

Configuring and Using Ranger KMS

Date published: 2019-11-01

Date modified:



Legal Notice

© Cloudera Inc. 2025. 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

Configuring Ranger KMS High Availability.....	4
Configure High Availability for Ranger KMS with DB.....	4
Configure High Availability for Ranger KMS with KTS.....	13
 Overriding custom keystore alias on a Ranger KMS Server.....	 22
Overriding custom keystore alias while configuring TLS/SSL on a single instance of Ranger KMS Server.....	22
Overriding custom keystore alias while configuring TLS/SSL on multiple instances of Ranger KMS Server.....	22

Configuring Ranger KMS High Availability

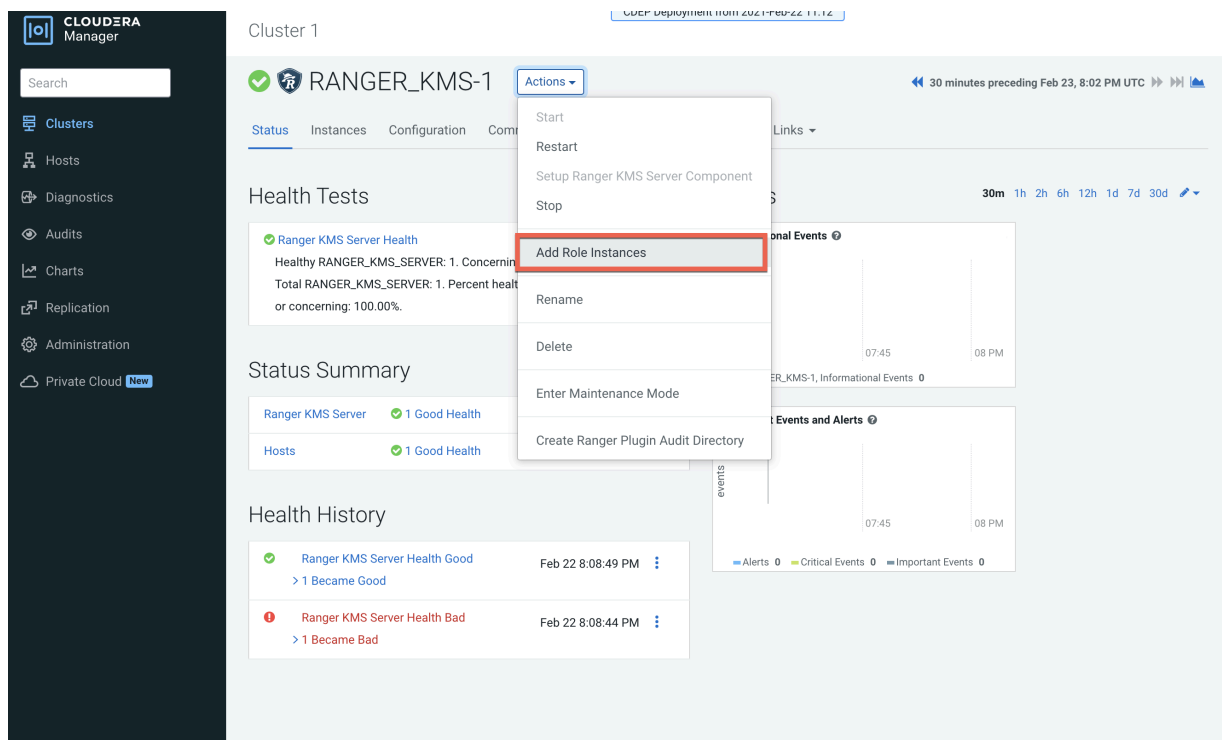
How to configure Ranger KMS high availability (HA) for Ranger KMS.

Configure High Availability for Ranger KMS with DB

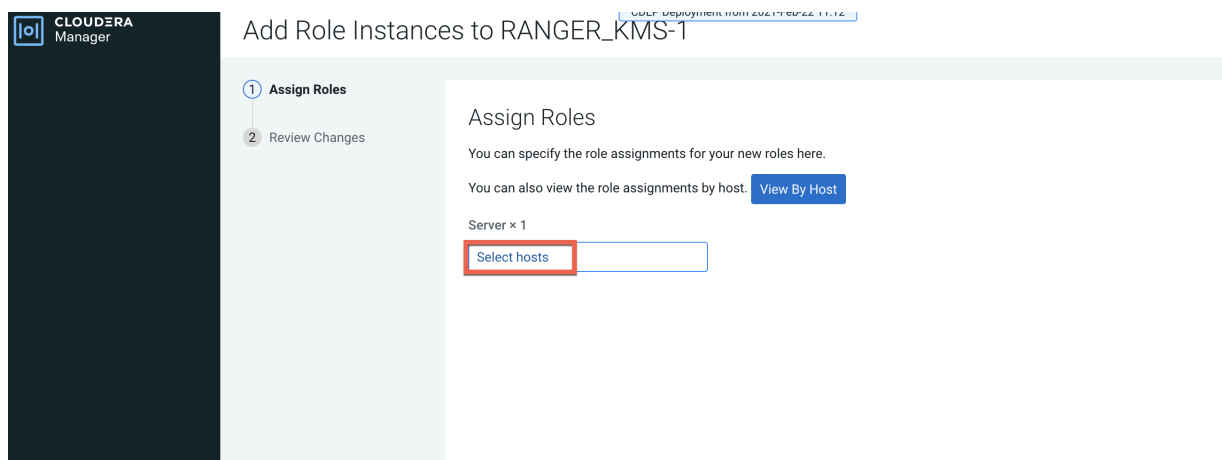
Use the following steps to configure high availability for Ranger KMS with an associated keystore database.

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

☐	Hostname	IP Address	Rack	Cores	Physical Memory	Existing Roles	Added Roles
☒	cloudera71-210...	172.27.0.1	/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...
☒	cloudera71-210...	172.27.0.1	/default	32	251.6 GiB	RS, DN, G, G, ID, KB, KC, TS, L, G, G, SR..., SR..., G, NM	RK...
☐	cloudera71-210...	172.27.0.2	/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.

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)

dlouder71-210... & dlouder71-210...3.ro...

Back Continue

- CLUSTER
Manager

Parcels

Running Commands

Support

admin

7.3.0

Assign Roles

Review Changes

Review Changes

Ranger KMS Master Key Password

ranger.db.encrypt.key.password

ranger_kms_master_key_password

Ranger KMS DB Auth Type

ranger.ks.db.ssl.auth.type

ranger_ks_db_ssl_auth_type

Ranger KMS Database SSL Certificate File

ranger.ks.db.ssl.certificateFile

ranger_ks_db_ssl_certificateFile

Ranger KMS DB SSL Enabled

ranger.ks.db.ssl.enabled

ranger_ks_db_ssl_enabled

Ranger KMS DB SSL Required

ranger.ks.db.ssl.required

ranger_ks_db_ssl_required

Ranger KMS DB SSL Verify Server Certificate

ranger.ks.db.ssl.verifyServerCertificate

ranger_ks_db_ssl_verifyServerCertificate

Ranger KMS Keystore File

ranger.ks.keystore.file

ranger_ks_keystore_file

Ranger KMS Keystore Password

ranger.ks.keystore.password

ranger_ks_keystore_password

Ranger KMS Truststore File

Ranger KMS Server Default Group

.....

Ranger KMS Server Default Group

1-way

2-way

Ranger KMS Server Default Group

Ranger KMS Server Default Group

☐

Ranger KMS Server Default Group

☐

Ranger KMS Server Default Group

☐

Ranger KMS Server Default Group

Ranger KMS Server Default Group

Ranger KMS Server Default Group

Back

Continue

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

CLUSTER

MANAGER

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Private Cloud New

Cluster 1

✓ RANGER_KMS-1

Actions

🔌

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.

Q 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

☐	Status	Role Type	State	Hostname	Commission State	Role Group
☐	⚠️	Ranger KMS Server	Stopped	10.10.10.10	Commissioned	Ranger KMS Server Default Group
☐	✓	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;http@kms_host2:9494/kms

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

Ranger Access Manager Audit Encryption Settings keyadmin

Service Manager Edit Service

Edit Service

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@10.10.10.15kms-2.dhgw15kms.root.hwx

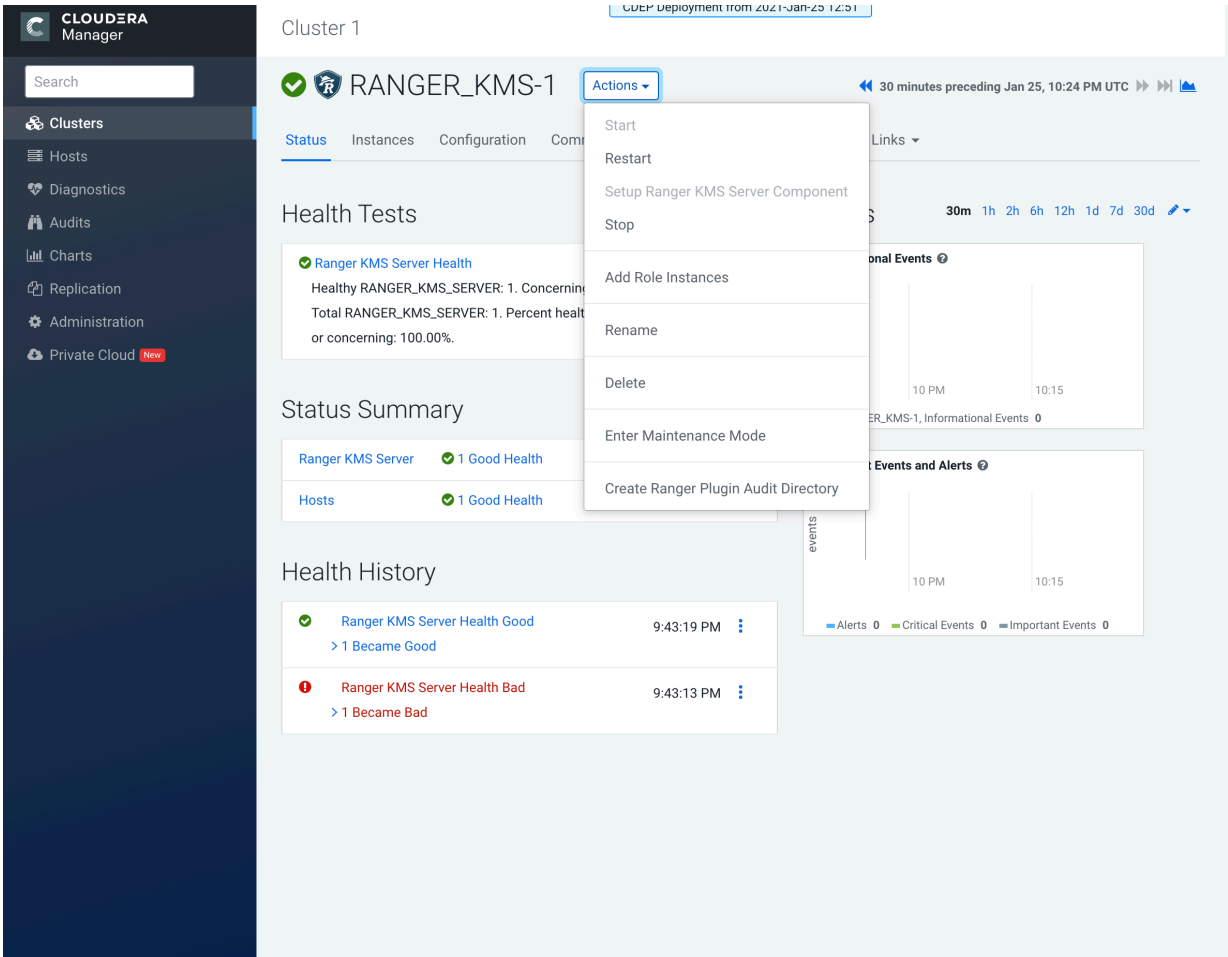
Username * keyadmin

Password *

Add New Configurations

Name	Value	
cluster.name	Cluster 1	x
policy.download.auth.users	keyadmin,rangerkms	x

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 (RANGER_KMS-1 (Service-Wide) 0, Ranger KMS Server 1), CATEGORY (Advanced 1, Database 0, Logs 0, Main 0, Monitoring 0, Performance 0, Ports and Addresses 0, Resource Management 0, Security 0, Stacks Collection 0), and STATUS (Error 0, Warning 0, Edited 1, Non-default 1, Has Overrides 0). The right panel displays a table of configuration properties:

Name	Value	Description	Final
<code>hadoop.kms.authentication.zk-dt-secret-manager.enable</code>	<code>true</code>		☐
<code>hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString</code>	<code>hwx.site:2181</code>		☐
<code>hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath</code>	<code>testzkms</code>		☐
<code>hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType</code>	<code>sasl</code>		☐
<code>hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab</code>	<code>{{CMF_CONF_DIR}}/ranger_kms.keytab</code>		☐

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

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

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

/hadoop-kms/hadoop-auth-signature-secret

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 Auth

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).

CloudEra

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

Feb 25, 9:39 PM UTC

✓

🛡️

RANGER_KMS-1

Actions

🔄

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. 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 displays the configuration for 'RANGER_KMS-1'. The 'Configuration' tab is selected, showing a search bar with the text 'hadoop.kms.cache.enable'. A 'Filters' sidebar on the left lists various categories and their counts. A 'Stale Configuration: Restart needed' tooltip is visible over the 'Actions' menu. The main content area shows the configuration for 'Hadoop KMS Cache Enable' with a checkbox for 'Ranger KMS Server Default Group' checked. 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.

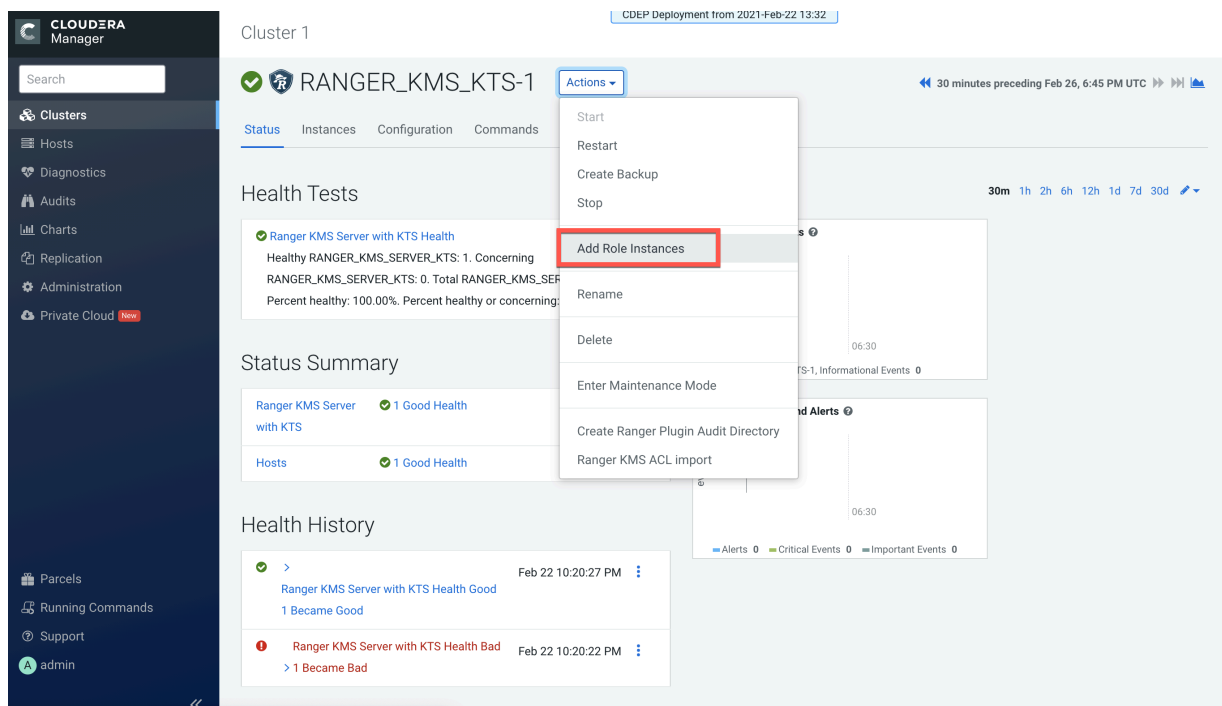
15. A progress indicator page appears while the services are being restarted. When the services have restarted, click Finish.

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.

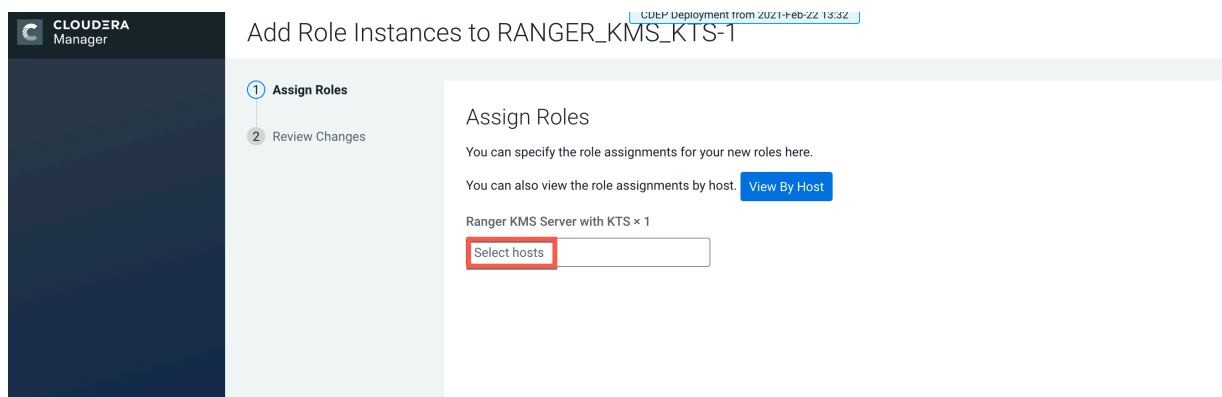
Procedure

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

☐	Hostname	IP Address	Rack	Cores	Physical Memory	Existing Roles	Added Roles
☐	dh...71... 1. dh...71...x.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..., SR..., SR..., G, G, NM, ZS	
☒	dh...71... 2. dh...71...x.site	172.27.130.71	/default	32	251.6 GiB	RS, DN, G, G, ID, KB, KC, TS, G, RK..., G, G, NM	RK...
☒	dh...71... 3. dh...71...x.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 MANAGER

Add Role Instances to RANGER_KMS_KTS-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](#)

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

dh...71...-3.d...mskts...

Back Continue

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

CLUSTERA
Manager

Parcels

Running Commands

Support

admin

CDP Deployment from ZUZI+ed-ZZ 13:32

Add Role Instances to RANGER_KMS_KTS-1

Assign Roles

2 Review Changes

Review Changes

Key Trustee Server Auth Code

cloudera.trustee.keyprovider.auth

Ranger KMS Server with KTS Default Group

.....

Active Key Trustee Server

cloudera.trustee.keyprovider.hostname=ACTIVE

Ranger KMS Server with KTS Default Group

kts-cdep-server-1.vpc.cloudera.com

Passive Key Trustee Server

cloudera.trustee.keyprovider.hostname=PASSIVE

Ranger KMS Server with KTS Default Group

kts-cdep-server-2.vpc.cloudera.com

Key Trustee Server Org Name

cloudera.trustee.keyprovider.org

Ranger KMS Server with KTS Default Group

kts

Key Trustee Server Key Provider Pool Timeout

cloudera.trustee.keyprovider.pool.abandoned.timeout

Ranger KMS Server with KTS Default Group

5

minute(s)

Key Trustee Server Key Provider Max Connections

cloudera.trustee.keyprovider.pool.max

Ranger KMS Server with KTS Default Group

5

Key Trustee Server Key Provider Pool Max Idle

cloudera.trustee.keyprovider.pool.max.idle

Ranger KMS Server with KTS Default Group

2

Back

Continue

- 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.

The screenshot displays the Cloudera Manager interface for the 'RANGER_KMS_KTS-1' cluster. The 'Instances' tab is selected, showing a table of roles and their status. A dropdown menu is open for the 'Actions' column, showing options like Start, Restart, Create Backup, Stop, Add Role Instances, Rename, Delete, Enter Maintenance Mode, Create Ranger Plugin Audit Directory, and Ranger KMS ACL import. The left sidebar shows navigation options like Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Private Cloud. The top navigation bar includes the Cloudera Manager logo and a search bar.

Hostname	Commission State	Role Group
dhoye715kmskts-	Commissioned	Ranger KMS
3.dhoye715kmskts.root.hwx.site	Commissioned	Server with KTS
		Default Group
dhoye715kmskts-	Commissioned	Ranger KMS
2.dhoye715kmskts.root.hwx.site	Commissioned	Server with KTS
		Default Group

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.

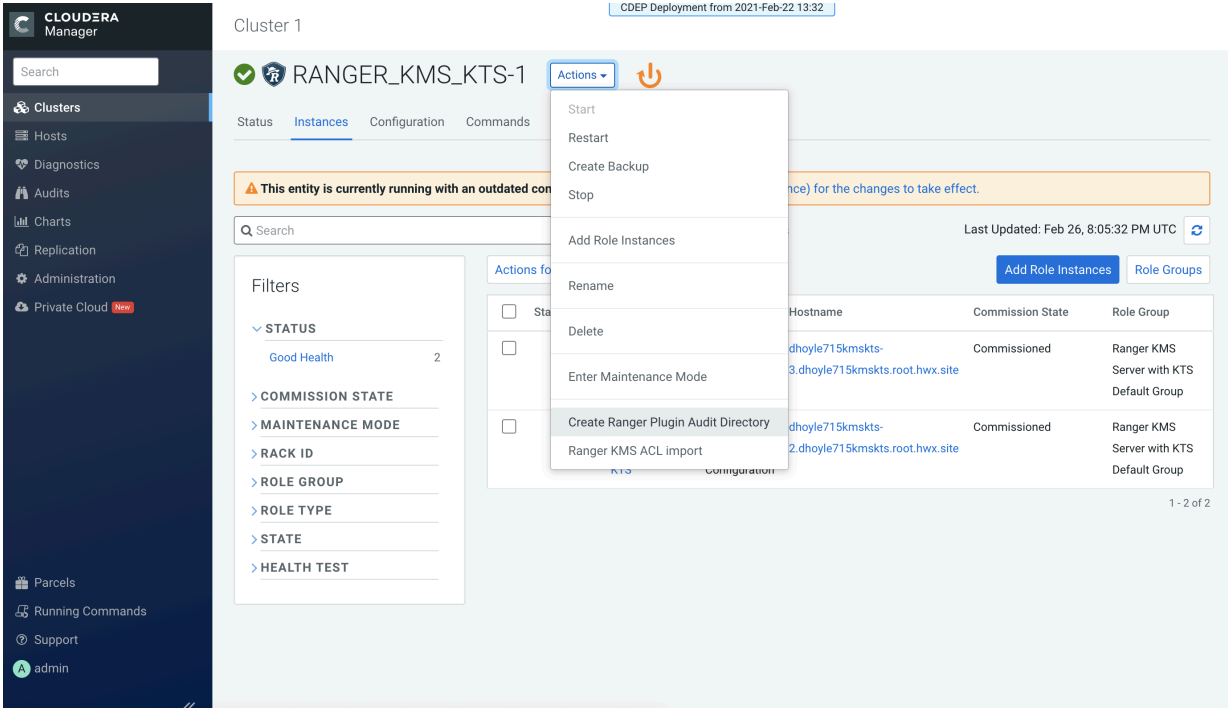
- Add the new KMS host using the following format:
kms://http@<kms_kts_host1>;http@<kms_kts_host2>:<kms_port>/kms
- The default port is 9292. For example:
kms://http@kms_kts_host1;http@kms_kts_host2:9292/kms
- If SSL is enabled, use https and port 9494. For example:
kms://https@kms_kts_host1;https@kms_kts_host2:9494/kms

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 'Ranger', 'Access Manager', 'Audit', 'Encryption', and 'Settings'. The user 'keyadmin' is logged in. The 'Edit Service' page for 'cm_kms' is displayed. It features an 'Active Status' section with 'Enabled' selected. Below is a 'Select Tag Service' dropdown. The 'Config Properties' section includes fields for 'KMS URL *', 'Username *', and 'Password *'. The 'KMS URL' is 'jhoyier.rangerkms-3.djhoyier.rangerkms.root.hwx.site:9292/kms', 'Username' is 'keyadmin', and 'Password' is masked. An 'Add New Configurations' table is shown with one entry: 'policy.download.auth.users' with value 'keyadmin,rangerkms'. A 'Test Connection' button is at the bottom left, and 'Save', 'Cancel', and 'Delete' buttons are at the bottom right.

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

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



11. In Cloudera Manager, select Ranger KMS KTS, 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.enable = true`
- `hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString = <Zookeeper hostname>:2181`
- `hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath = <provide a znode working path other than /zkdtsm to avoid collision>`

For example:

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



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_kts.keytab`

CLOUDERA
Manager

Search

Clusters

Hosts

Diagnostics

Audits

Charts

Replication

Administration

Private Cloud New

Parcels

Running Commands

Support

admin

RANGER_KMS_KTS-1Actions

Feb 27, 8:57 PM UTC

StatusInstancesConfigurationCommandsCharts LibraryAuditsQuick Links

Q Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve) for conf/kmFiltersRole GroupsHistory and Rollback

Filters

SCOPE

RANGER_KMS_KTS-1 (Service... 0
Ranger KMS Server with KTS 1

CATEGORY

Advanced 1
Logs 0
Main 0
Monitoring 0
Performance 0
Ports and Addresses 0
Resource Management 0
Security 0
Stacks Collection 0

STATUS

Error 0
Warning 0
Edited 1
Non-default 1
Has Overrides 0

Ranger KMS Server with KTS
Advanced Configuration
Snippet (Safety Valve) for
conf/kms-site.xml

Ranger KMS Server with KTS Default GroupUndoView as XML

Namehadoop.kms.authentication.zk-dt-secret-manager.enableValuetrueDescription☐ Final

Namehadoop.kms.authentication.zk-dt-secret-manager.zkConnectionStringValuelocalhost:2181Description☐ Final

Namehadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPathValuetestzkcmsDescription☐ Final

Namehadoop.kms.authentication.zk-dt-secret-manager.zkAuthTypeValuesaslDescription☐ Final

Namehadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytabValue{{CMF_CONF_DIR}}/ranger_kms_kts.keytabDescription☐ Final

1 Edited ValueReason for change:Modified Ranger KMS Server with KTS Advanced Configuration Snippet (Safety Valve...Save Changes (CTRL+S)

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

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

The screenshot shows the Cloudera Manager interface for Cluster 1, specifically the Configuration page for 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 a user profile for 'admin'. The main content area displays the configuration for the property `hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type`. The property is set to `sasl` under the 'Hadoop KMS Authentication Signer Secret Provider Zookeeper Auth Type' section. The 'Filters' panel on the left shows counts for SCOPE, CATEGORY, and STATUS. The 'Save Changes (CTRL+S)' button is located at the bottom right of the configuration area.

13. Click the Stale Configuration Restart icon.

This screenshot shows the same Cloudera Manager configuration page for RANGER_KMS_KTS-1. A dark button labeled 'Stale Configuration. Restart needed' has appeared above the configuration table. The configuration property `hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type` remains set to `sasl`. The 'Save Changes (CTRL+S)' button is still visible at the bottom right.

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

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

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

Overriding custom keystore alias on a Ranger KMS Server

Use this procedure to override the custom keystore alias on a Ranger KMS server.

About this task

The custom keystore alias may need to be overridden in the following scenarios:

- User has manually enabled TLS/SSL during fresh installations of Ranger KMS and Ranger KMS with Key Trustee Server (KTS), and the keystore alias was not added to the hostname.
- User has upgraded from CDP-DC 7.0.3 with Key Trustee KMS and Ranger to CDP-DC 7.1.1 (where Ranger KMS with KTS is added during the upgrade) in a TLS/SSL environment in which TLS/SSL was manually enabled, and the keystore alias was not added to the hostname.

Overriding custom keystore alias while configuring TLS/SSL on a single instance of Ranger KMS Server

Procedure

1. In Cloudera Manager, select Ranger KMS > Configuration and use the Add (+) icon for the Ranger KMS Service Advanced Configuration Snippet (Safety valve) for conf/ranger-kms-site.xml property to add the following property:

```
ranger.service.https.attrib.keystore.keyalias = <expected alias>
```

2. Click Save Changes.
3. Restart the Ranger KMS service.

Overriding custom keystore alias while configuring TLS/SSL on multiple instances of Ranger KMS Server

Procedure

1. In Cloudera Manager, select Ranger KMS > Instances and select Ranger KMS Server role > Configuration. Use the Add (+) icons for the Ranger KMS Server Advanced Configuration Snippet (Safety valve) for conf/ranger-kms-site.xml property to add the following property:

```
ranger.service.https.attrib.keystore.keyalias = <expected alias>
```

This overrides the configuration on the host on which the current Ranger KMS Server role is available.

2. Repeat Step 1 for all the other Ranger KMS Servers to override the configuration by using the Ranger KMS Server Advanced Configuration Snippet (Safety valve) for conf/ranger-kms-site.xml property.
3. Restart the Ranger KMS service.



Note: When high-availability has been enabled for Ranger KMS, the keystore may not have the same alias for different KMS instances. In such cases, use FQDN as the alias or add the custom key alias configuration in the Ranger KMS Server Advanced Configuration Snippet (Safety valve) for conf/ranger-kms-site.xml property of each host.