

Cloudera Runtime 7.1.9

Configuring and Using Ranger KMS

Date published: 2020-07-28

Date modified: 2023-09-07

The Cloudera logo is displayed in a bold, orange, sans-serif font. The word "CLOUDERA" is written in all caps, with a stylized 'E' that has a horizontal bar extending to the right.

<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

| | |
|--|-----------|
| Configuring Ranger KMS High Availability..... | 4 |
| Configure High Availability for Ranger KMS with DB..... | 4 |
| Configure High Availability for Ranger KMS with KTS..... | 13 |
| | |
| Rotating Ranger KMS access log files..... | 22 |

Configuring Ranger KMS High Availability

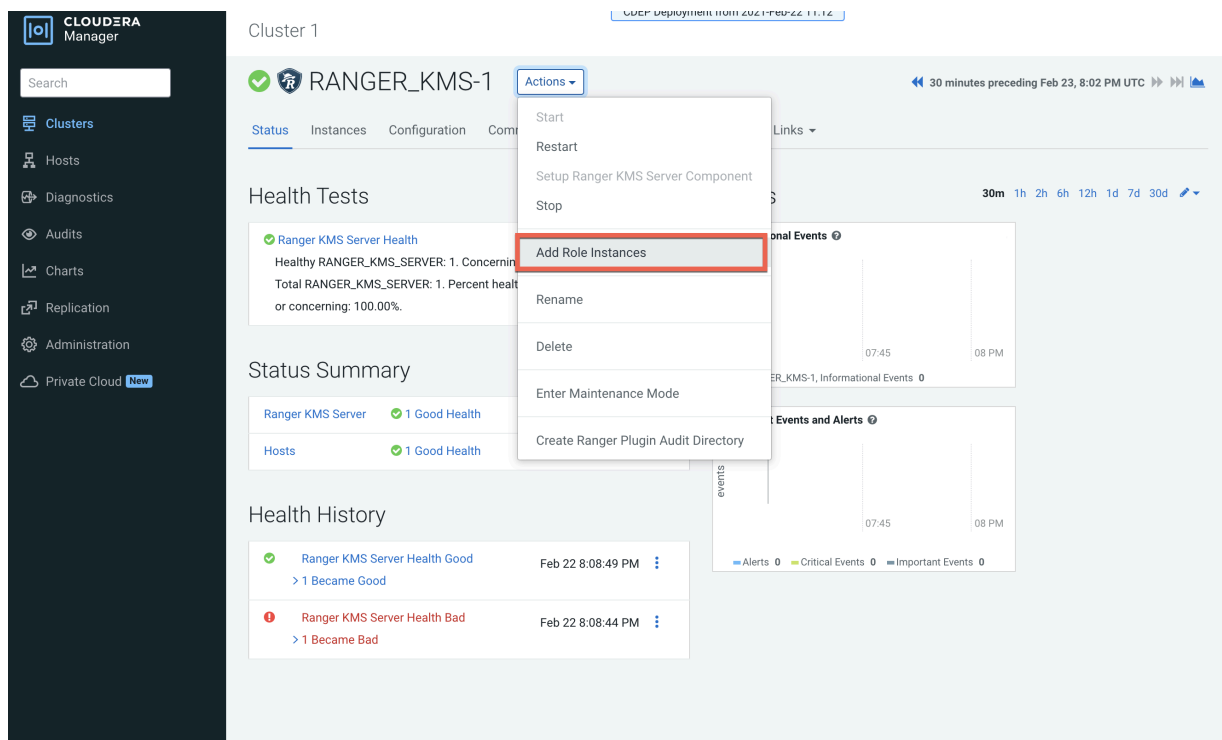
How to configure Ranger KMS high availability (HA) for Ranger KMS.

Configure High Availability for Ranger KMS with DB

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

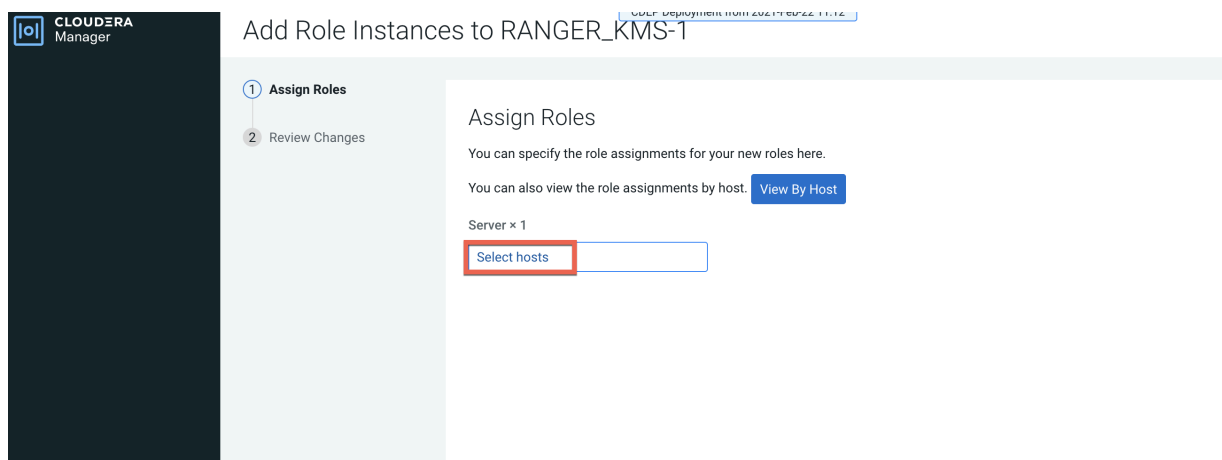
Procedure

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



The screenshot shows the Cloudera Manager interface for Cluster 1. The main content area displays the configuration for RANGER_KMS-1. The 'Actions' dropdown menu is open, and the 'Add Role Instances' option is highlighted with a red box. The interface includes a sidebar with navigation options like Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Private Cloud. The main content area shows the 'Health Tests' section with a 'Ranger KMS Server Health' test that is currently 'Good'. Below this is a 'Status Summary' section showing 'Ranger KMS Server' and 'Hosts' both in 'Good Health'. The 'Health History' section shows a log of health changes, including one that became 'Good' and one that became 'Bad' on Feb 22 at 8:08:49 PM and 8:08:44 PM respectively. On the right side, there are charts for 'Informational Events' and 'Events and Alerts', both showing zero events.

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



The screenshot shows the 'Assign Roles' page in Cloudera Manager for RANGER_KMS-1. The page title is 'Add Role Instances to RANGER_KMS-1'. The 'Assign Roles' section contains the text: 'You can specify the role assignments for your new roles here.' and 'You can also view the role assignments by host: View By Host'. Below this, there is a 'Server x 1' section with a 'Select hosts' button highlighted by a red box. The sidebar on the left shows the navigation menu with 'Assign Roles' selected.

- 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"/> | dl...@172.27.01.1 | 172.27.01.1 | /default | 80 | 251.6 GiB | AS, CCS, G, HB..., RS, DN, G, G, G, ID, KB, KC, KG, M, G, LS, RA, RT, RU, RK..., SRS, G, G, SM..., SM..., SR..., SR..., G, G, NM, ZS | RK... |
| <input checked="" type="checkbox"/> | dl...@172.27.01.1 | 172.27.01.1 | /default | 32 | 251.6 GiB | RS, DN, G, G, ID, KB, KC, TS, G, G, SR..., SR..., G, NM | RK... |
| <input type="checkbox"/> | dl...@172.27.01.2 | 172.27.01.2 | /default | 32 | 251.6 GiB | M, B, NN, NF..., SNN, G, HMS, G, HS2, LB, HS, KTR, ICS, ISS, G, KB, KC, LHBI, TS, 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.

CDEP Deployment from 2021-Feb-22 11:12

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)

- dl...@172.27.01.1

Back Continue

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

The screenshot shows the Cloudera Manager interface. On the left is a dark sidebar with the Cloudera Manager logo and navigation options: Parcels, Running Commands, Support, and a user profile for 'admin'. The main content area is titled 'Add Role Instances to RANGER_KMS-1'. Below the title is a progress indicator with two steps: 'Assign Roles' (completed) and 'Review Changes' (current step). The 'Review Changes' section contains several configuration items, each with a label, a description, a value, and a help icon:

- Ranger KMS Master Key Password:** Value is 'Ranger KMS Server Default Group'. Description: 'ranger.db.encrypt.key.password'. Link: 'ranger_kms_master_key_password'.
- Ranger KMS DB Auth Type:** Value is 'Ranger KMS Server Default Group'. Radio buttons for '1-way' (selected) and '2-way'. Description: 'ranger.ks.db.ssl.auth.type'. Link: 'ranger_ks_db_ssl_auth_type'.
- Ranger KMS Database SSL Certificate File:** Value is 'Ranger KMS Server Default Group'. Description: 'ranger.ks.db.ssl.certificateFile'. Link: 'ranger_ks_db_ssl_certificateFile'.
- Ranger KMS DB SSL Enabled:** Value is 'Ranger KMS Server Default Group'. Checkbox is unchecked. Description: 'ranger.ks.db.ssl.enabled'. Link: 'ranger_ks_db_ssl_enabled'.
- Ranger KMS DB SSL Required:** Value is 'Ranger KMS Server Default Group'. Checkbox is unchecked. Description: 'ranger.ks.db.ssl.required'. Link: 'ranger_ks_db_ssl_required'.
- Ranger KMS DB SSL Verify Server Certificate:** Value is 'Ranger KMS Server Default Group'. Checkbox is unchecked. Description: 'ranger.ks.db.ssl.verifyServerCertificate'. Link: 'ranger_ks_db_ssl_verifyServerCertificate'.
- Ranger KMS Keystore File:** Value is 'Ranger KMS Server Default Group'. Description: 'ranger.ks.keystore.file'. Link: 'ranger_ks_keystore_file'.
- Ranger KMS Keystore Password:** Value is 'Ranger KMS Server Default Group'. Description: 'ranger.ks.keystore.password'. Link: 'ranger_ks_keystore_password'.
- Ranger KMS Truststore File:** Value is 'Ranger KMS Server Default Group'.

At the bottom right of the configuration area are two buttons: 'Back' and 'Continue'.

- 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.

The screenshot shows the Cloudera Manager interface for a cluster named 'Cluster 1'. The main focus is on the 'RANGER_KMS-1' service. A warning banner at the top indicates that the entity is running with an outdated configuration. Below this, a table lists the instances of the service. The table has columns for Status, Role Type, State, Hostname, Commission State, and Role Group. Two instances are listed: one is 'Stopped' and the other is 'Started with Outdated Configuration'. A 'Filters' sidebar is visible on the left, and a 'Private Cloud' badge is at the bottom left of the sidebar.

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

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://https@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: rt.hwx.site;http@...;kms-2.d...;kms.root.hwx
- Username: keyadmin
- Password:

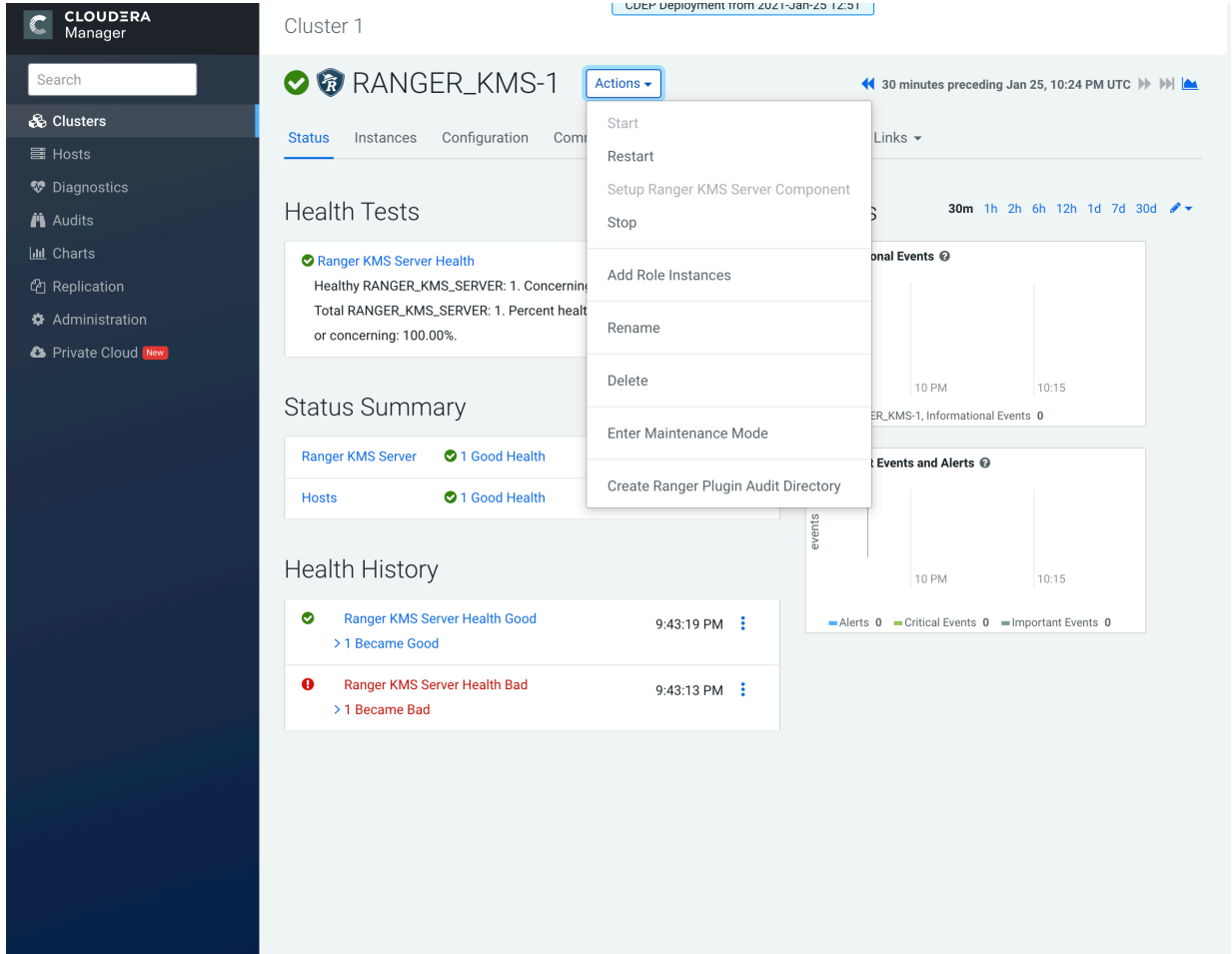
Add New Configurations:

| 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 new configurations and a 'Test Connection' button.

At the bottom of the page are three buttons: 'Save' (blue), 'Cancel' (grey), and 'Delete' (red).

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 = 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.keytab`

The screenshot shows the Cloudera Manager interface for configuring Ranger KMS. The left sidebar contains navigation options like 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 categories like 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`
- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString`, **Value:** `hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString:2181`
- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath`, **Value:** `testzkkms`
- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType`, **Value:** `sasl`
- Name:** `hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab`, **Value:** `{{CMF_CONF_DIR}}/ranger_kms.keytab`

At the bottom of the page, 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 Ranger KMS Server Default Group Undo

`hadoop.kms.authentication.signer.secret.provider`

`hadoop_kms_authentication_signer_secret_provider`

random

string

zookeeper

Hadoop KMS Authentication Signer Secret Provider Zookeeper Path Ranger KMS Server Default Group Undo

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

`hadoop_kms_authentication_signer_secret_provider_zookeeper_path`

Hadoop KMS Authentication Signer Secret Provider Zookeeper Auth Type Ranger KMS Server Default Group Undo

`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).

The screenshot shows the Cloudera Manager interface for configuring the `RANGER_KMS-1` cluster. The left sidebar contains navigation options like Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, Private Cloud, Parcels, Running Commands, Support, and a user profile for 'admin'. The main content area is titled 'Cluster 1' and shows the 'Configuration' tab for 'RANGER_KMS-1'. A search bar at the top contains the query 'hadoop.kms.cache.enable'. Below the search bar, there are filter options for 'Filters', 'Role Groups', and 'History and Rollback'. A 'Filters' panel on the left lists categories such as 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). The main configuration area displays the property 'Hadoop KMS Cache Enable' with a checked checkbox for 'Ranger KMS Server Default Group' and a link to 'Show All Descriptions'. Below this, the property name 'hadoop.kms.cache.enable' is listed with its corresponding configuration key 'hadoop_kms_cache_enable'. At the bottom right of the configuration area, there is a 'Per Page' dropdown set to '25' and a page indicator '1 - 25 of 142'.

12. Click the Stale Configuration Restart icon.

The screenshot shows the Cloudera Manager interface for Cluster 1. The main content area displays the configuration for RANGER_KMS-1. A search filter is applied for 'hadoop.kms.cache.enable'. The configuration results show a table with the following data:

| Configuration Name | Value |
|-------------------------|---|
| Hadoop KMS Cache Enable | <input checked="" type="checkbox"/> Ranger KMS Server Default Group |
| hadoop.kms.cache.enable | <input checked="" type="checkbox"/> hadoop_kms_cache_enable |

The 'Actions' menu is open, showing the 'Stale Configuration: Restart needed' option. The interface also includes a sidebar with navigation options like Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, Private Cloud, Parcels, Running Commands, Support, and admin. The bottom right corner 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.

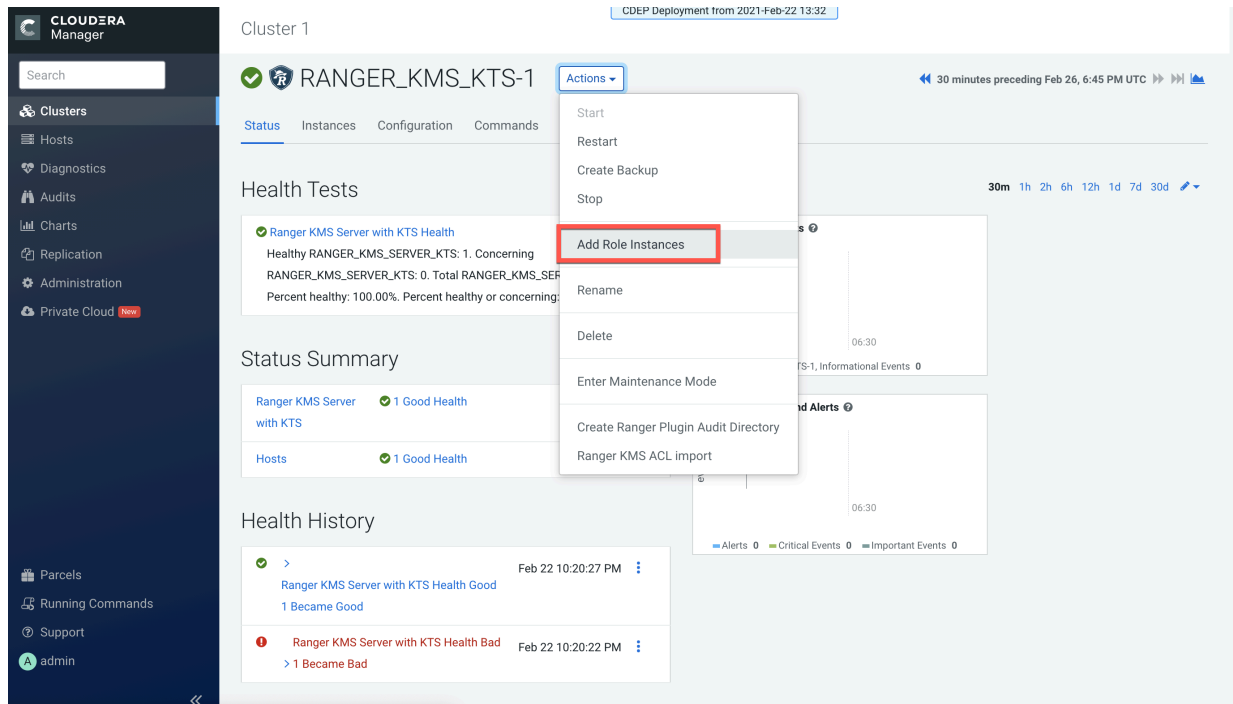
15. A progress indicator page appears while the services are being restarted. When the services have restarted, click Finish.

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.

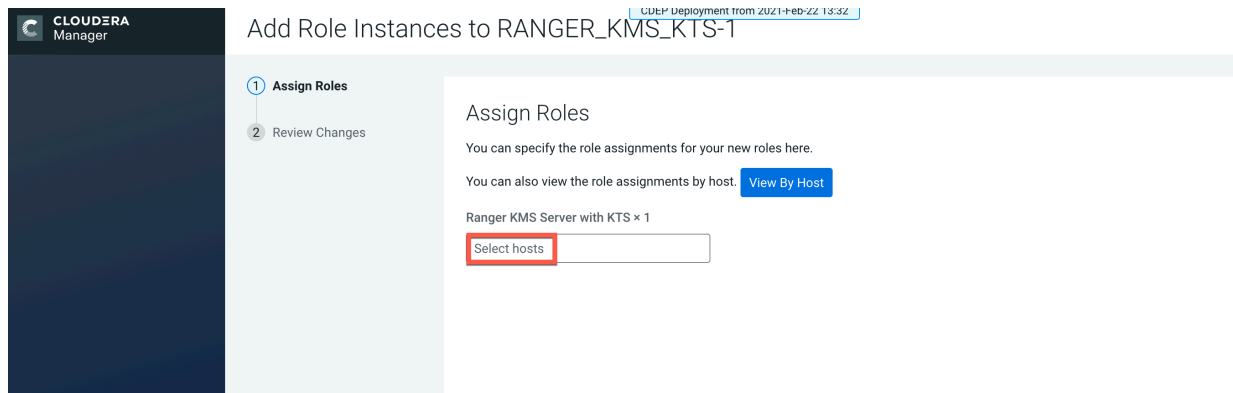
Procedure

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 'Cluster 1'. The main content area displays the 'RANGER_KMS_KTS-1' service. A dropdown menu is open over the 'Actions' button, with 'Add Role Instances' highlighted in red. The menu options include Start, Restart, Create Backup, Stop, Add Role Instances, Rename, Delete, Enter Maintenance Mode, Create Ranger Plugin Audit Directory, and Ranger KMS ACL import. The 'Health Tests' section shows 'Ranger KMS Server with KTS Health' as 'Healthy'. The 'Status Summary' shows 'Ranger KMS Server with KTS' and 'Hosts' both with '1 Good Health'. The 'Health History' shows a log of health changes.

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 '1 Assign Roles' and '2 Review Changes'. The main content area has the heading 'Assign Roles' and the text 'You can specify the role assignments for your new roles here.' Below this, it says 'You can also view the role assignments by host.' with a 'View By Host' button. The role 'Ranger KMS Server with KTS x 1' is listed, and a 'Select hosts' button is highlighted in red.

- 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.

🔍 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... 1. dh...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, G, LS, RA, RT, RU, SRS, G, G, SM..., SM..., SR..., SR..., G, G, NM, ZS | |
| <input checked="" type="checkbox"/> | dh... 2. dh...site | 172.27.130.71 | /default | 32 | 251.6 GiB | RS, DN, G, G, ID, KB, KC, TS, G, RK..., G, G, G, NM | RK... |
| <input checked="" type="checkbox"/> | dh... 3. dh...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, LHB, TS, G, AP, ES, HM, RM | RK... |

Cancel OK

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

CDEP Deployment from 2021-Feb-22 13:32

Add Role Instances to RANGER_KMS_KTS-1

1 Assign Roles

2 Review Changes

Parcels

Running Commands

Support

admin

Assign Roles

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

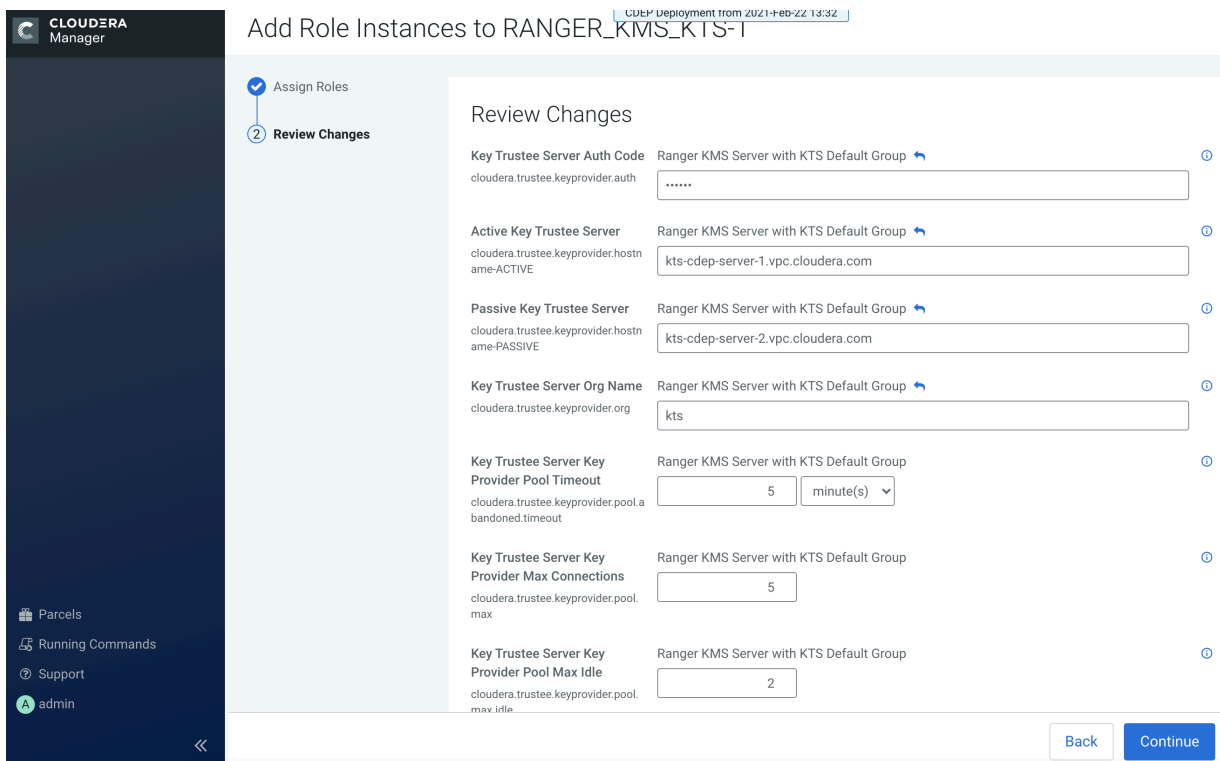
You can also view the role assignments by host. View By Host

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

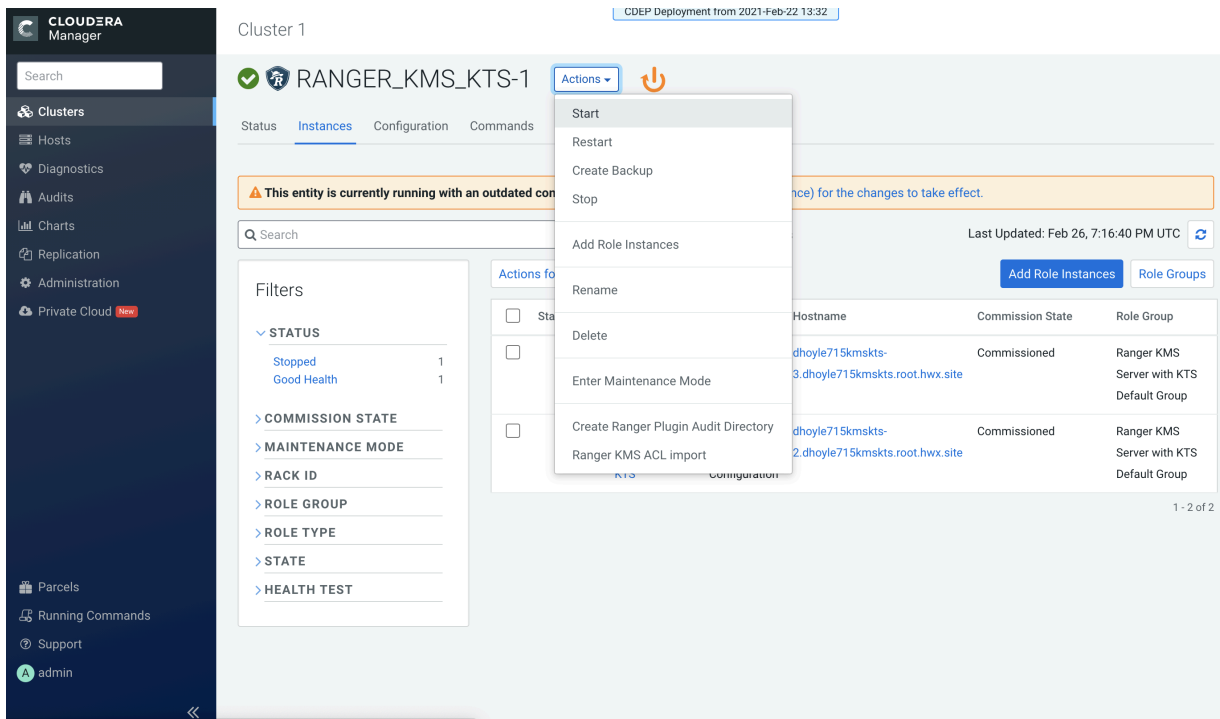
dh...-3.d...mks...

Back
Continue

- Review the settings on the Review Changes page, then click 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.



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@ktkms02.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 configuration page for the cm_kms service. The page is titled "Edit Service" and includes a navigation bar with "Ranger", "Access Manager", "Audit", "Encryption", and "Settings". The main content area shows the "Config Properties" section with the following fields:

- Active Status:** Enabled (selected), Disabled
- Select Tag Service:** Select Tag Service (dropdown)
- KMS URL *:** fhoyle1.rangerkms-3.dhoyle1.rangerkms.root.rwx.site:9292/kms
- Username *:** keyadmin
- Password *:**

Below the "Add New Configurations" section, there is a table with the following entry:

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

At the bottom of the page, there are buttons for "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 /zkdtms 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. 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`.

CLUSTER RANGER_KMS_KTS-1 Actions Feb 27, 8:57 PM UTC

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

Search

Clusters

- Hosts
- Diagnostics
- Audits
- Charts
- Replication
- Administration
- Private Cloud **NEW**

Parcels

Running Commands

Support

admin

Filters

SCOPE

- RANGER_KMS_KTS-1 (Servic... 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 Filters Role Groups History and Rollback Show All Descriptions

Ranger KMS Server with KTS Default Group Undo View as XML

Name hadoop.kms.authentication.zk-dt-secret-manager.enable 🗑️ 🔍

Value true

Description

Final

Name hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString 🗑️ 🔍

Value d... site:2181

Description

Final

Name hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath 🗑️ 🔍

Value testzkms

Description

Final

Name hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType 🗑️ 🔍

Value sasl

Description

Final

Name hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab 🗑️ 🔍

Value {{CMF_CONF_DIR}}/ranger_kms_kts.keytab

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

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 search bar contains the property name `hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type`. The configuration table shows the property is set to `sasl` for the 'Ranger KMS Server with KTS Default Group'. The 'Filters' sidebar on the left shows the current configuration is under the 'Main' category. At the bottom, a message indicates '1 Edited Value' and 'Reason for change: Modified Hadoop KMS Authentication Signer Secret Provider Zookeeper Auth Type'. A 'Save Changes (CTRL+S)' button is visible.

12. Click the Stale Configuration Restart icon.

This screenshot is identical to the previous one, but a 'Stale Configuration: Restart needed' icon (a power button with a lightning bolt) is now visible above the configuration table. This icon is used to restart the configuration for the selected property. The 'Save Changes (CTRL+S)' button is still present 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.

Rotating Ranger KMS access log files

How to configure properties that control access log file rotation in Ranger KMS service.

About this task

Ranger KMS access log files accrue in the following path: `/var/log/ranger/kms/access_log.yyyy-mm-dd.log`. By default, these files aren't removed which consumes free space in the `/var/` directory. Currently, Ranger KMS access log files get rotated every hour, which amounts to 24 files per day. You can configure it to rotate every 24 hours using the safety valve. To do so, you must add a configuration property to the `ranger-kms-site.xml` file.

Procedure

1. In Cloudera Manager, select `Ranger_KMS`, then choose Configuration.
2. On Configuration, in Search, type `ranger-kms-site`.
3. In Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for `conf/ranger-kms-site.xml`, click + (Add).
4. Add a key-value pair that configures the rotation of Ranger KMS access log files.

Name

`ranger.accesslog.dateformat`

Value

`yyyy-MM-dd`



Note: If not set, then the default value is `yyyy-MM-dd.HH`.

5. Click Save Changes.

After saving changes, the Stale Configuration icon appears on the Cloudera Manager UI. Optionally, click Stale Configuration to view details.

6. Select Actions Restart.