

Cloudera Runtime 7.3.2

## Configuring and Using Ranger KMS

Date published: 2020-07-28

Date modified: 2026-03-31

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. 2026. 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
<b>Rotating Ranger KMS access log files</b> .....	<b>13</b>

# Configuring Ranger KMS High Availability

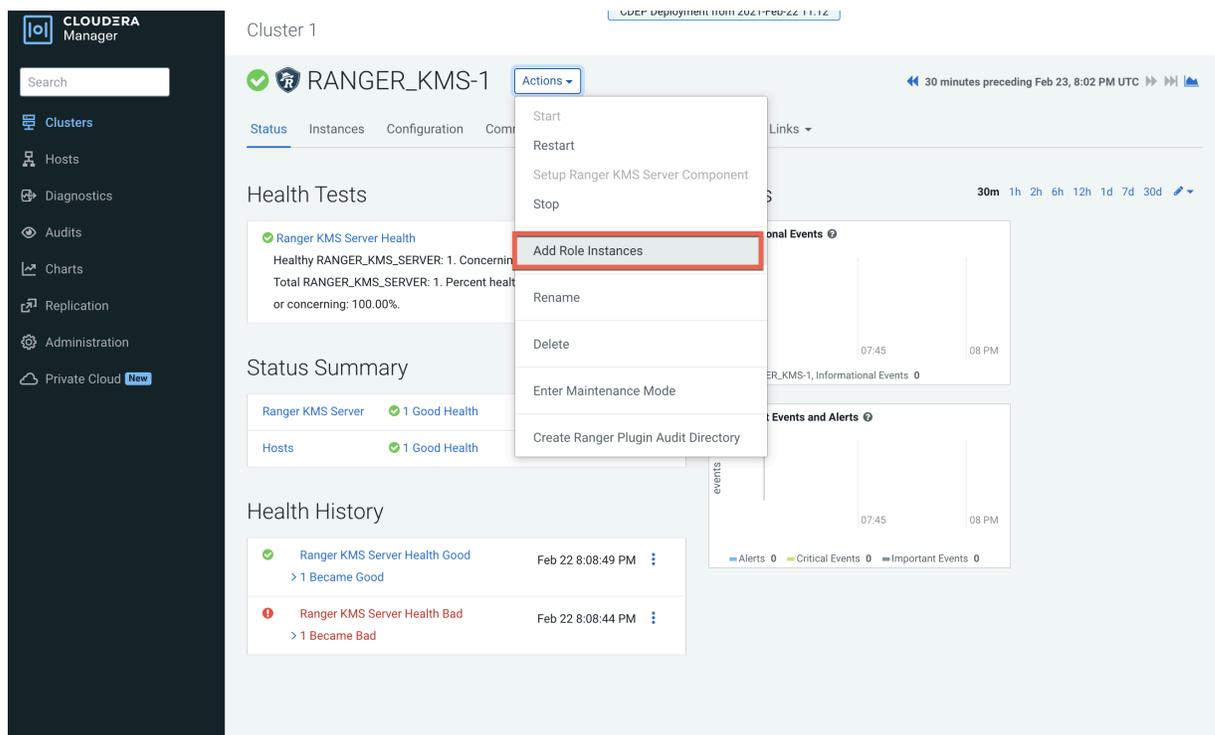
How to configure Ranger KMS high availability (HA) for Ranger KMS.

## Configure High Availability for Ranger KMS with DB

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

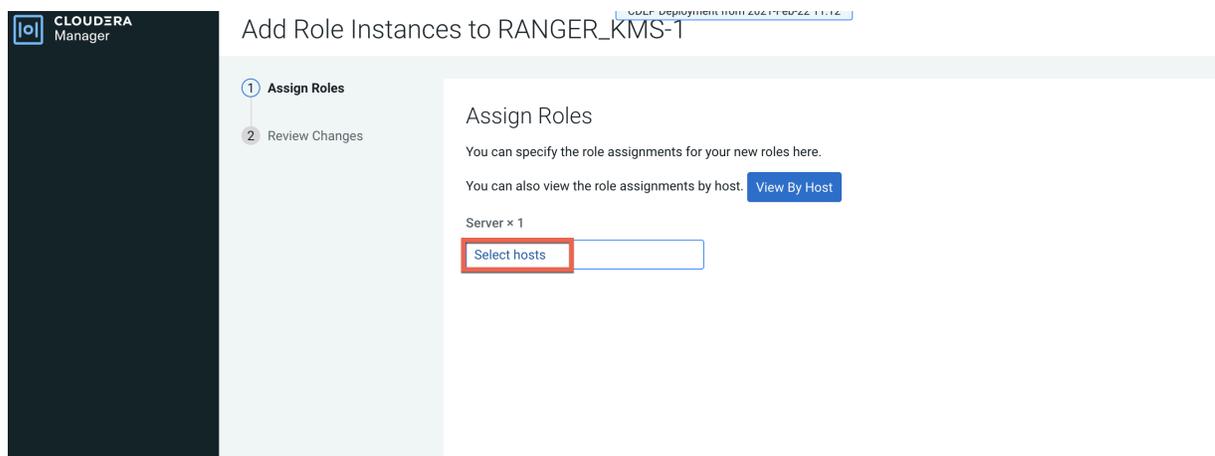
### Procedure

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' indicator, a 'Status Summary' section with 'Ranger KMS Server' and 'Hosts' both showing 'Good Health', and a 'Health History' section with a log of health changes.

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 instructions on how to specify role assignments and a 'View By Host' button. Below this, there is a 'Server x 1' section with a 'Select hosts' button highlighted by a red box.



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'. Options: '1-way' (selected), '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'. Description: 'ranger.ks.db.ssl.enabled'. Link: 'ranger\_ks\_db\_ssl\_enabled'.
- Ranger KMS DB SSL Required:** Value is 'Ranger KMS Server Default Group'. 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'. 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'.



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 Cloudera Manager. 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@10.10.10.15kms-2.dhgw.com;15kms.root.hwx` (highlighted with a blue border)
- Username: keyadmin
- Password: .....

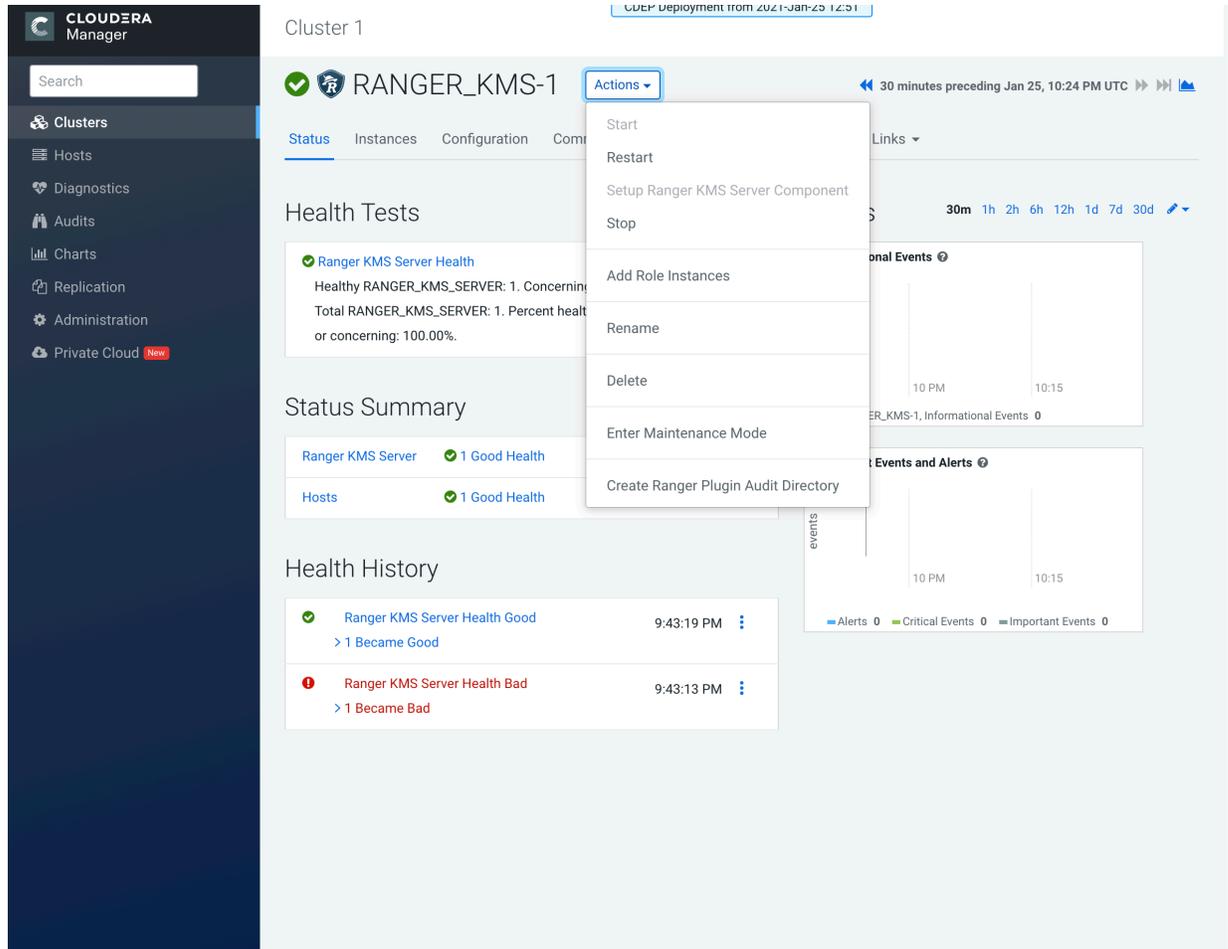
**Add New Configurations:**

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 ZooKeeper 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 /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.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, there is a status bar indicating '1 Edited Value' and a 'Save Changes (CTRL+S)' button.

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`

The screenshot shows the Cloudera Manager interface for configuring the RANGER\_KMS-1 cluster. The configuration page is titled "RANGER\_KMS-1" and shows the "Configuration" tab. The search bar contains the query "hadoop.kms.authentication.signer.secret.provider". The configuration is filtered by "SCOPE" (RANGER\_KMS-1 (Service-Wide) 0, Ranger KMS Server 3) and "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). The "STATUS" section shows 0 Errors, 0 Warnings, 2 Edited, 2 Non-default, and 0 Has Overrides. The configuration properties are:

- Hadoop KMS Authentication Signer Secret Provider:** Ranger KMS Server Default Group. Options:  random,  string,  zookeeper.
- Hadoop KMS Authentication Signer Secret Provider Zookeeper Path:** /hadoop-kms/hadoop-auth-signature-secret
- Hadoop KMS Authentication Signer Secret Provider Zookeeper Auth Type:** Ranger KMS Server Default Group. Options:  none,  kerberos,  sasl.

At the bottom, the "Reason for change" is "Modified Hadoop KMS Authentication Signer Secret Provider, Hadoop KMS Auth" and the "Save Changes (CTRL+S)" button is visible.

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 page for 'RANGER\_KMS-1'. A search bar at the top contains the query 'hadoop.kms.cache.enable'. Below the search bar, there are filter tabs for 'Filters', 'Role Groups', and 'History and Rollback'. A 'Filters' panel on the left lists various categories and their counts: 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 ID '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, specifically the Configuration page for RANGER\_KMS-1. The search bar contains the text 'hadoop.kms.cache.enable'. A tooltip 'Stale Configuration: Restart needed' is visible over the Actions menu. The left sidebar shows navigation options like Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, Private Cloud, Parcels, Running Commands, Support, and admin. The main content area shows filters for SCOPE, CATEGORY, and STATUS.

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 .