

Cloudera Runtime 7.3.1

Configuring and Using Ranger KMS

Date published: 2020-07-28

Date modified: 2024-12-10

CLOUdera

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

Legal Notice

© Cloudera Inc. 2024. All rights reserved.

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

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

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

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

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

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

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

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

Contents

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

Configuring Ranger KMS High Availability

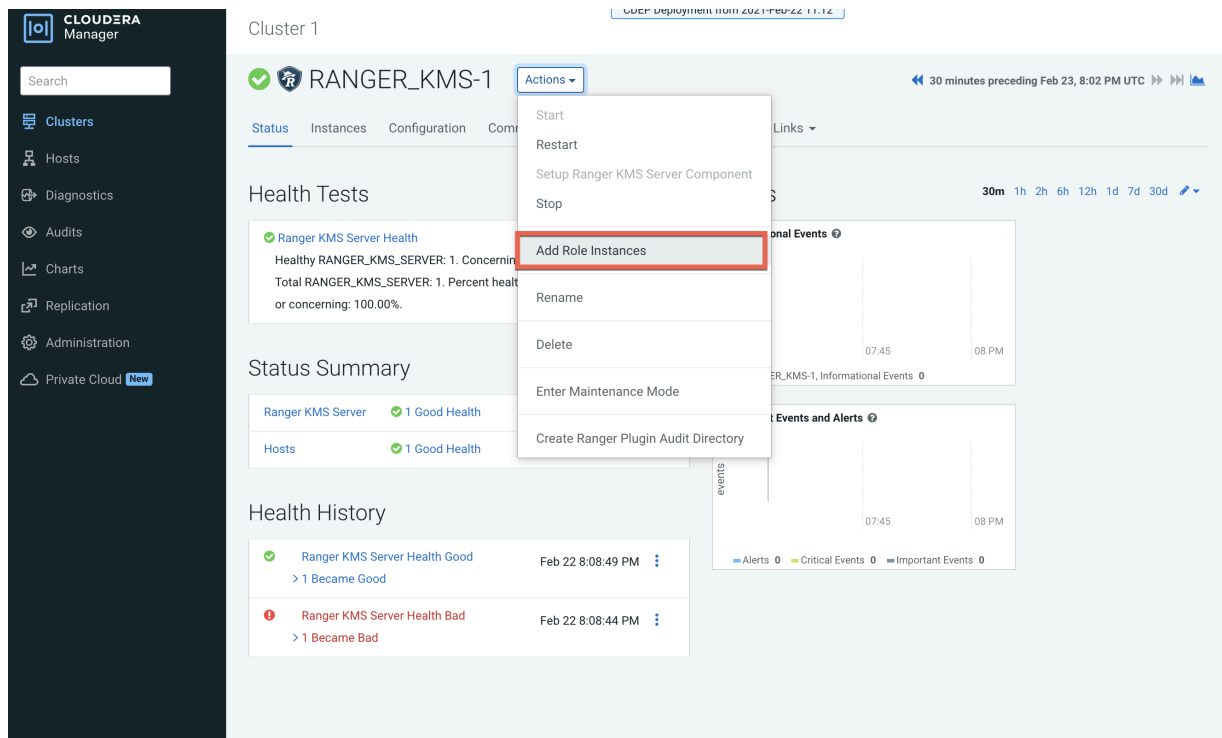
How to configure Ranger KMS high availability (HA) for Ranger KMS.

Configure High Availability for Ranger KMS with DB

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

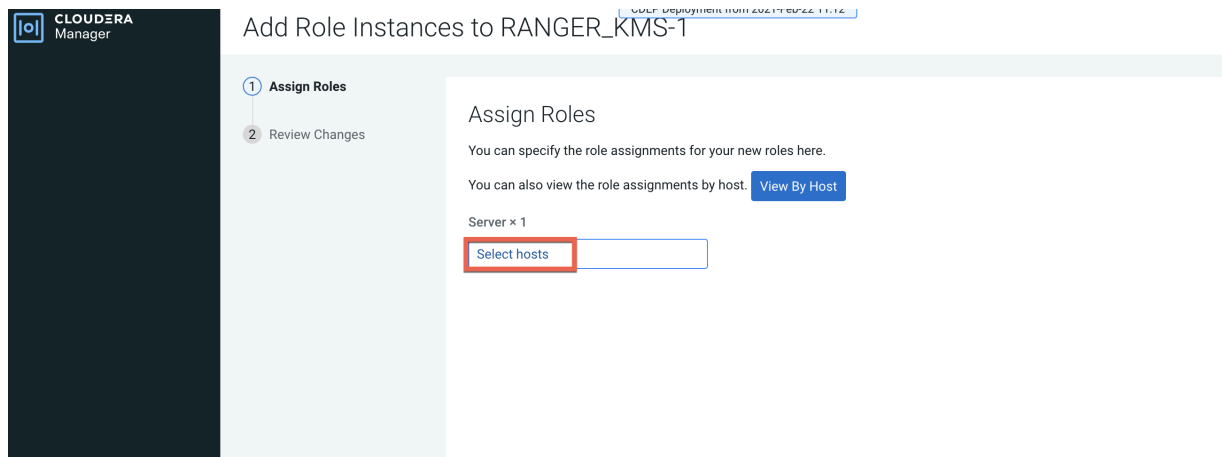
Procedure

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



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 table of health events.

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



The screenshot shows the Cloudera Manager interface for Cluster 1, specifically the 'Assign Roles' page for RANGER_KMS-1. The page title is 'Add Role Instances to RANGER_KMS-1'. The 'Assign Roles' section is active, and the 'Select hosts' button 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 'Assign Roles' section with a 'View By Host' button and a 'Server x 1' label.

- 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
<input type="checkbox"/> cloudera7151name 1. cloudera7151name.com.lax.site	172.27.00.69	/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"/> cloudera7151name 2. cloudera7151name.com.lax.site	172.27.00.71	/default	32	251.6 GiB	RS, DN, G, G, ID, KB, KC, TS, G, G, G, SR..., SR..., G, NM	RK...
<input type="checkbox"/> cloudera7151name 3. cloudera7151name.com.lax.site	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.

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)

- cloudera7151name.com.lax.site

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. Property: ranger_kms_master_key_password.
- Ranger KMS DB Auth Type:** Value is 'Ranger KMS Server Default Group'. Description: ranger.ks.db.ssl.auth.type. Property: ranger_ks_db_ssl_auth_type. Radio buttons for '1-way' (selected) and '2-way'.
- Ranger KMS Database SSL Certificate File:** Value is 'Ranger KMS Server Default Group'. Description: ranger.ks.db.ssl.certificateFile. Property: ranger_ks_db_ssl_certificateFile.
- Ranger KMS DB SSL Enabled:** Value is 'Ranger KMS Server Default Group'. Description: ranger.ks.db.ssl.enabled. Property: ranger_ks_db_ssl_enabled. Checkbox is unchecked.
- Ranger KMS DB SSL Required:** Value is 'Ranger KMS Server Default Group'. Description: ranger.ks.db.ssl.required. Property: ranger_ks_db_ssl_required. Checkbox is unchecked.
- Ranger KMS DB SSL Verify Server Certificate:** Value is 'Ranger KMS Server Default Group'. Description: ranger.ks.db.ssl.verifyServerCertificate. Property: ranger_ks_db_ssl_verifyServerCertificate. Checkbox is unchecked.
- Ranger KMS Keystore File:** Value is 'Ranger KMS Server Default Group'. Description: ranger.ks.keystore.file. Property: ranger_ks_keystore_file.
- Ranger KMS Keystore Password:** Value is 'Ranger KMS Server Default Group'. Description: ranger.ks.keystore.password. Property: 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 displays 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 '1 - 2 of 2' indicator is at the bottom right of the table.

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: `it.hwx.site;http@10.10.10.15kms-2.dhgw15kms.root.hwx` (highlighted with a blue border)
- Username: keyadmin
- Password:

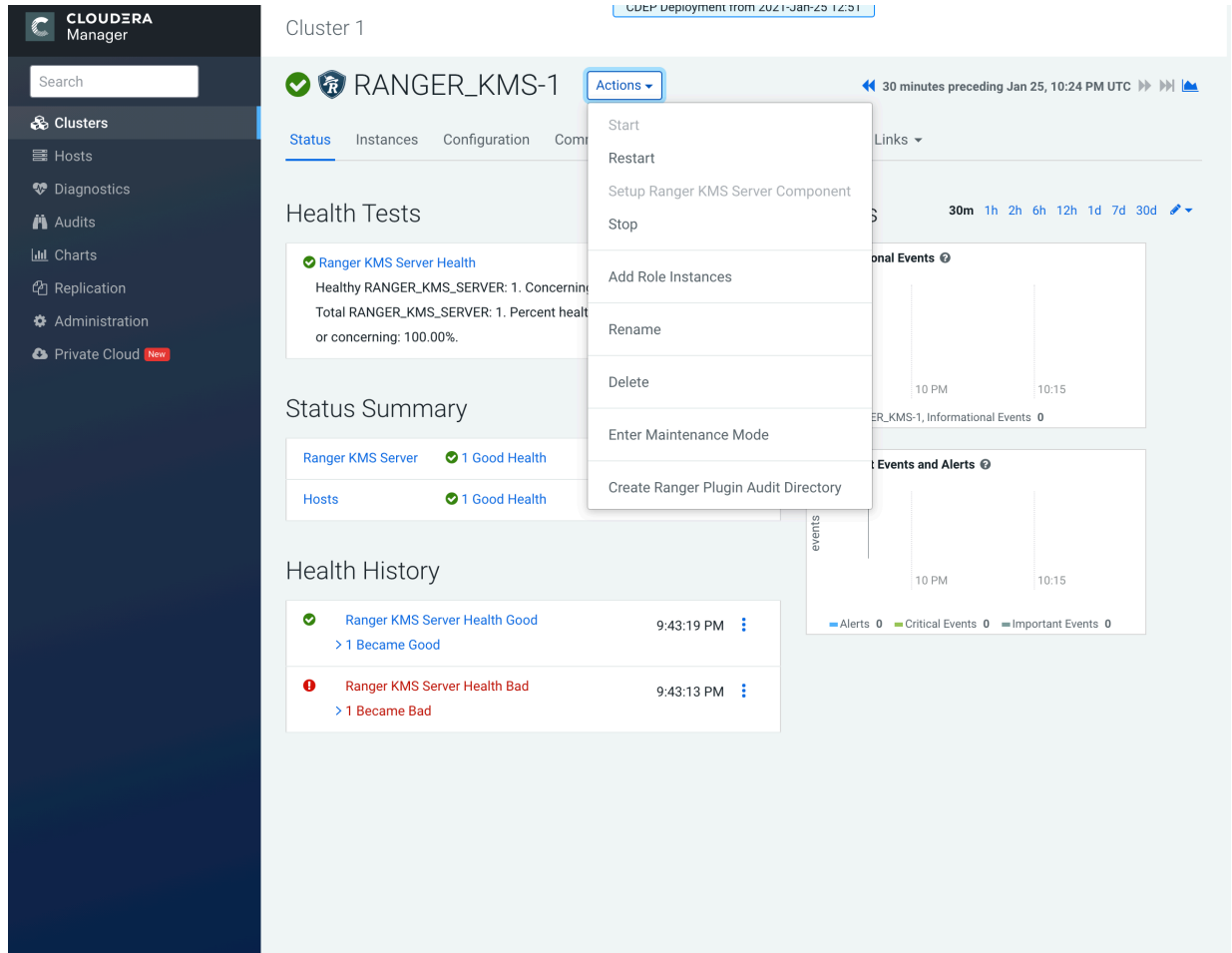
Add New Configurations:

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 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, 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

Ranger KMS Server Default Group Undo

hadoop.kms.authentication.signer.secret.provider

random

string

zookeeper

Hadoop KMS Authentication Signer Secret Provider Zookeeper Path

Ranger KMS Server Default Group

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

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

Hadoop KMS Authentication Signer Secret Provider Zookeeper Auth Type

Ranger KMS Server Default Group Undo

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 `hadoop.kms.cache.enable` property on cluster `RANGER_KMS-1`. 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 text 'hadoop.kms.cache.enable'. Below the search bar, there are tabs for 'Filters', 'Role Groups', and 'History and Rollback'. The 'Filters' section is expanded, showing a list of filters under three categories: SCOPE, CATEGORY, and STATUS. The SCOPE section lists 'RANGER_KMS-1 (Service-Wide)' with a count of 0 and 'Ranger KMS Server' with a count of 1. The CATEGORY section lists various categories like Advanced, Database, Logs, Main, Monitoring, Performance, Ports and Addresses, Resource Management, Security, and Stacks Collection, all with counts of 0. The STATUS section lists Error, Warning, Edited, Non-default, and Has Overrides, all with counts of 0. The main configuration area shows the property 'Hadoop KMS Cache Enable' with a checked checkbox and the label 'Ranger KMS Server Default Group'. Below this, the property name 'hadoop.kms.cache.enable' is listed with a link to 'hadoop_kms_cache_enable'. A 'Show All Descriptions' link is also visible. At the bottom right, 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 configuration page for RANGER_KMS-1 is displayed. The search bar contains the text 'hadoop.kms.cache.enable'. A tooltip 'Stale Configuration: Restart needed' is visible over the 'Actions' menu. The configuration table shows the following items:

Configuration Property	Value	Category	Status
hadoop.kms.cache.enable	Ranger KMS Server Default Group	Advanced	Warning
hadoop.kms.cache.enable	hadoop_kms_cache_enable	Advanced	Warning

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 .