

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. 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
Rotating Ranger KMS access log files.....	13

Configuring Ranger KMS High Availability

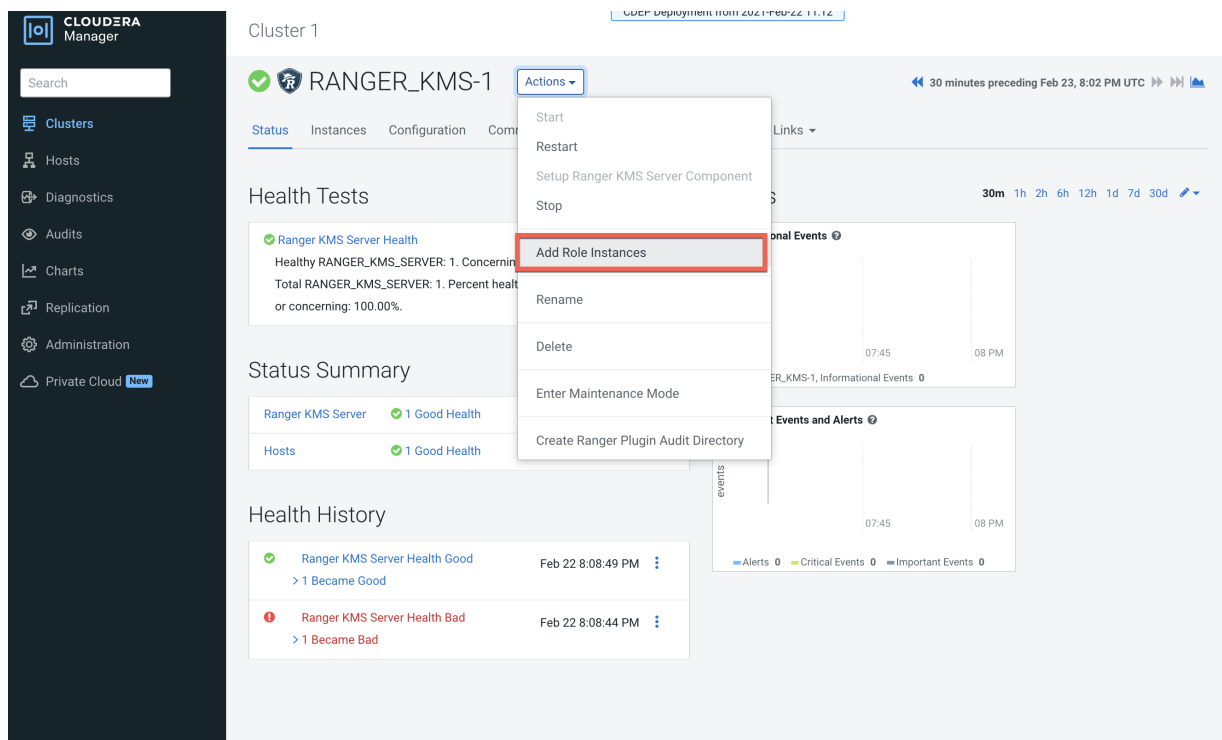
How to configure Ranger KMS high availability (HA) for Ranger KMS.

Configure High Availability for Ranger KMS with DB

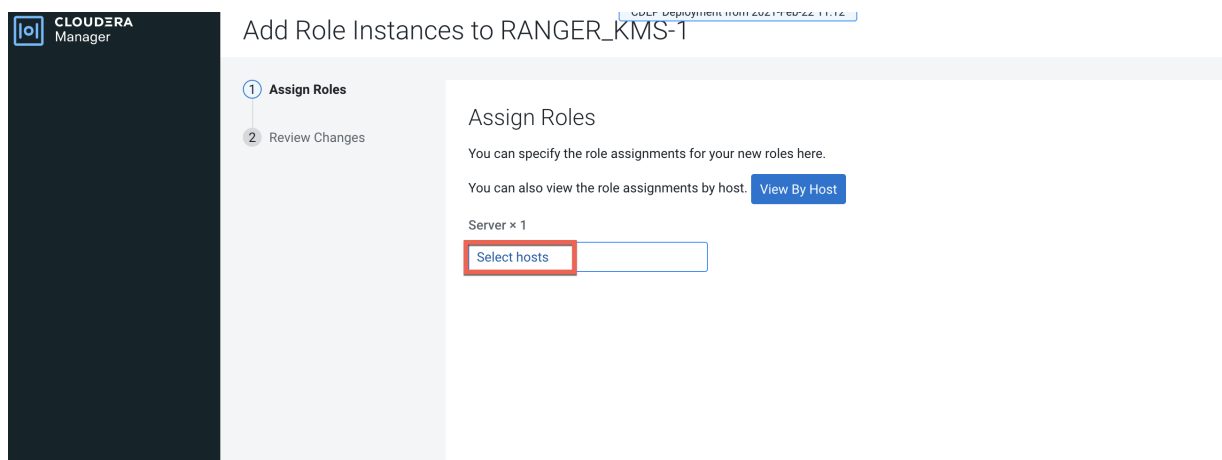
Use the following steps to configure high availability for Ranger KMS with an associated keystore database.

Procedure

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



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
☒	cloudera74-21name	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...
☒	cloudera74-21name	172.27.0.1	/default	32	251.6 GiB	RS, DN, G, G, ID, KB, KC, TS, L, G, G, G, SR..., G, NM	RK...
☐	cloudera74-21name	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.

Add Role Instances to RANGER_KMS-1

CDEP Deployment from 2021-Feb-22 11:12

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)

dlouder74-21name & dlouder74-21name3.ro...

Back Continue

- CLUSTERA
Manager

Parcels

Running Commands

Support

admin

7.3.0

Assign Roles

2 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.ks.truststore.file

ranger_ks_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

Ranger KMS Server Default Group

Ranger KMS Server Default Group

Ranger KMS Server Default Group

Back

Continue

- CLOUDERA**
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.](#)

Search

Filters

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

Actions for Selected

Add Role Instances

Role Groups

Filters

▼ STATUS

Stopped 1

Good Health 1

▼ COMMISSION STATE

▼ MAINTENANCE MODE

▼ RACK ID

▼ ROLE GROUP

▼ ROLE TYPE

▼ STATE

▼ HEALTH TEST

☐	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

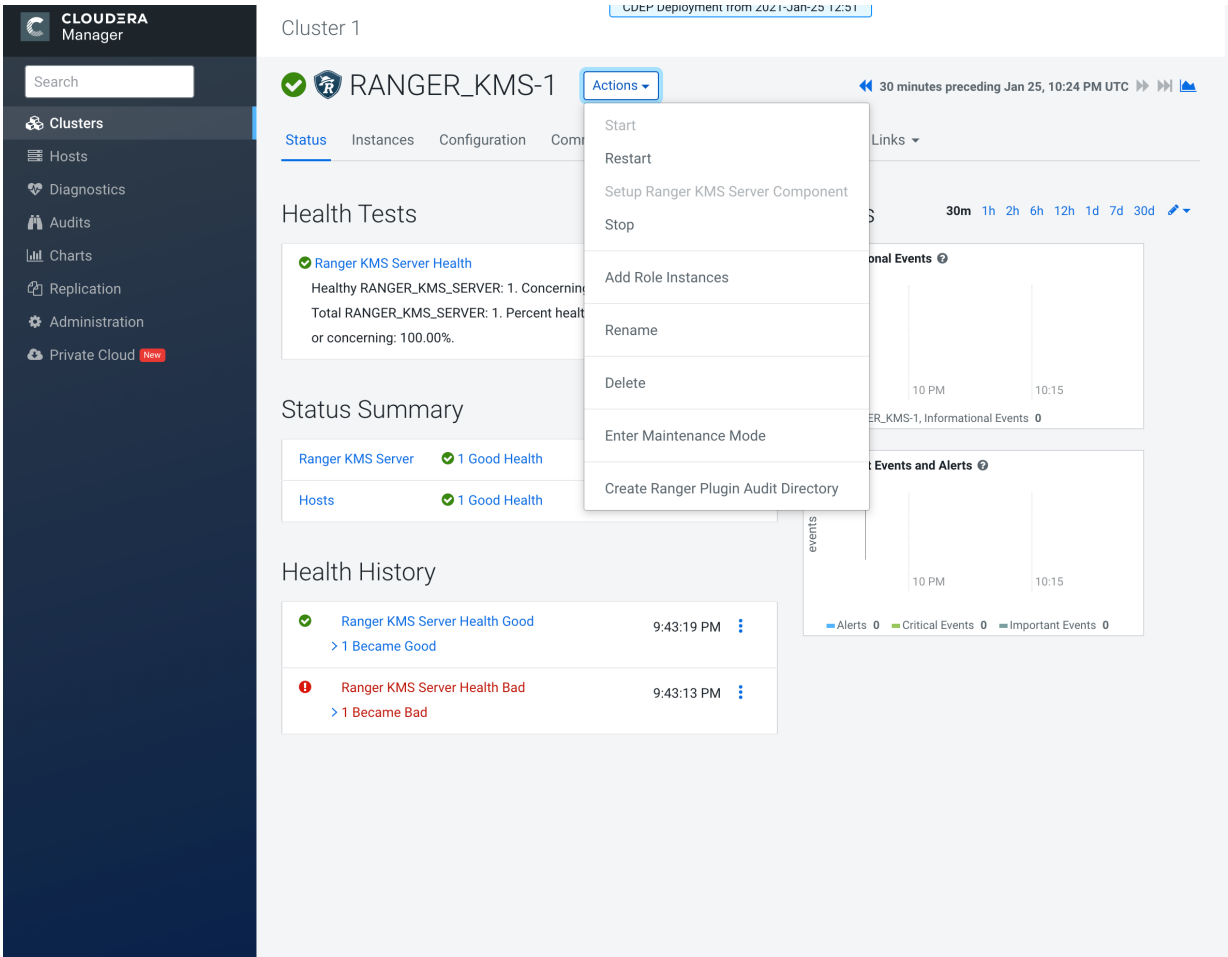
Name	Value	
cluster.name	Cluster 1	✕
policy.download.auth.users	keyadmin,rangerkms	✕

+

Test Connection

Save Cancel Delete

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



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

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

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



Note: In a cluster with multiple 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 /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
hadoop.kms.authentication.zk-dt-secret-manager.enable	true		☐
hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString	hwx.site:2181		☐
hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath	testzkms		☐
hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType	sasl		☐
hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab	{{CMF_CONF_DIR}}/ranger_kms.keytab		☐

At the bottom, a status bar indicates '1 Edited Value' and provides a 'Reason for change' field with the text 'Modified Ranger KMS Server Advanced Configuration Snippet (Safety Valve) for con...'. A 'Save Changes (CTRL+S)' button is located in the bottom right corner.

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

✓

RANGER_KMS-1

Actions

Feb 25, 9:39 PM UTC

Status

Instances

Configuration

Commands

Charts Library

Audits

Quick Links

hadoop.kms.cache.enable

Filters

Role Groups

History and Rollback

Filters

SCOPE

RANGER_KMS-1 (Service-Wide) 0

Ranger KMS Server 1

CATEGORY

Advanced 0

Database 0

Logs 0

Main 1

Monitoring 0

Performance 0

Ports and Addresses 0

Resource Management 0

Security 0

Stacks Collection 0

STATUS

Error 0

Warning 0

Edited 0

Non-default 0

Has Overrides 0

Hadoop KMS Cache Enable

hadoop.kms.cache.enable

[hadoop_kms_cache.enable](#)

☒ Ranger KMS Server Default Group

[Show All Descriptions](#)

Per Page 25

1 - 25 of 142

12. Click the Stale Configuration Restart icon.

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 .