Cloudera Runtime 7.3.2

Configuring and Using Ranger KMS

Date published: 2020-07-28
Date modified: 2026-03-31

https://docs.cloudera.com/

Legal Notice

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

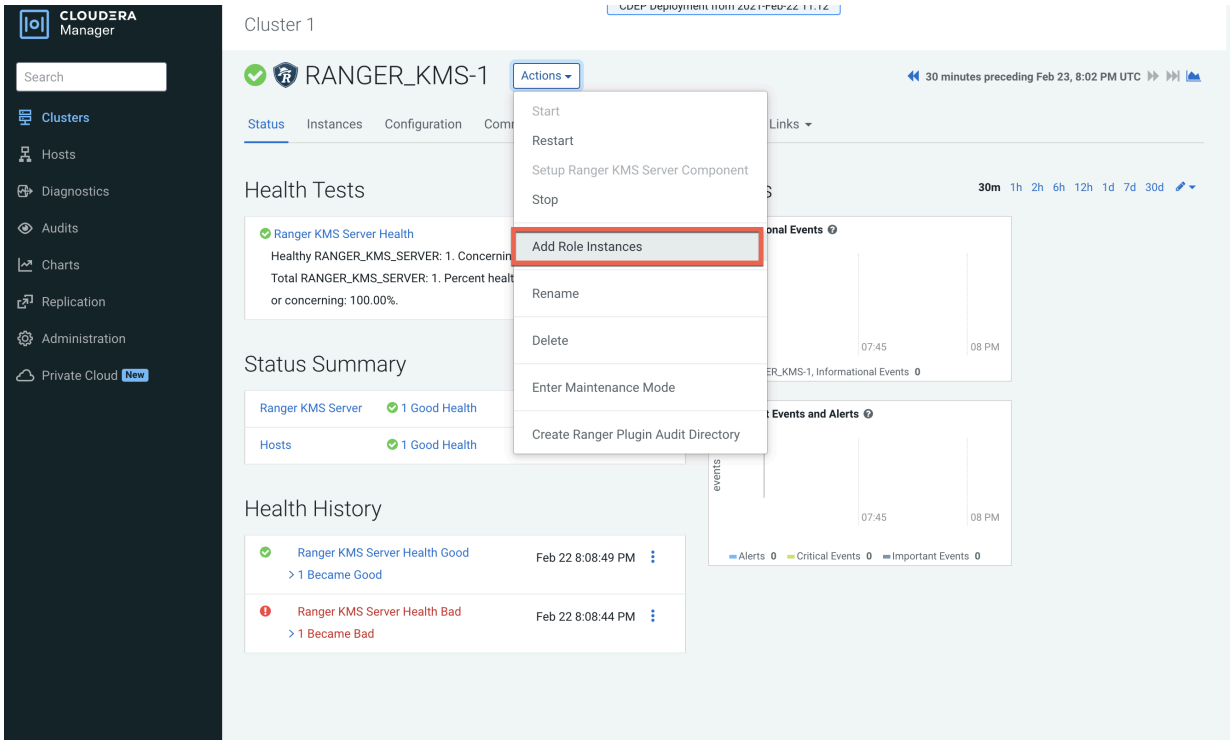
How to configure Ranger KMS high availability (HA) for Ranger KMS.

Configure High Availability for Ranger KMS with DB

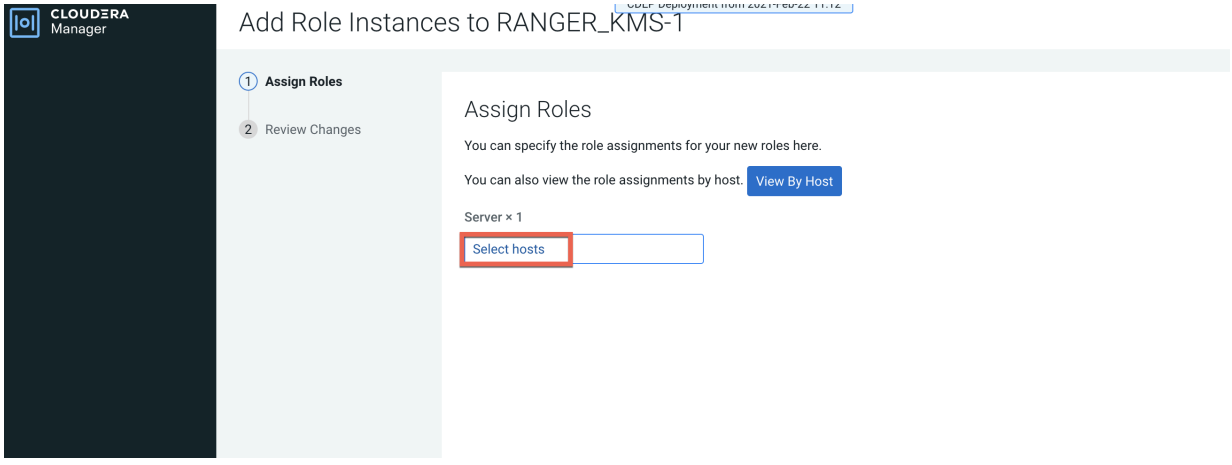
Use the following steps to configure high availability for Ranger KMS with an associated keystore database.

Procedure

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

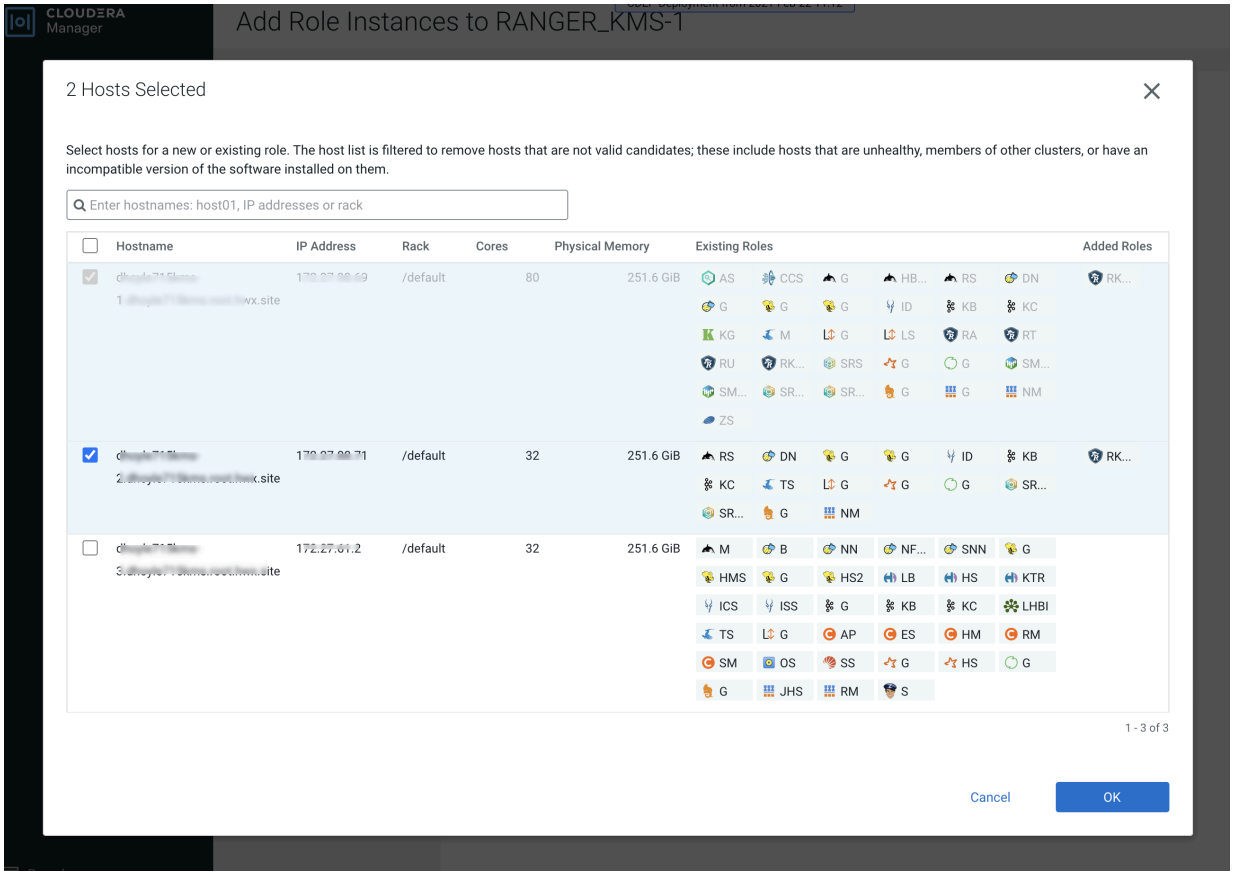


2. On the Assign Roles page, click Select hosts.

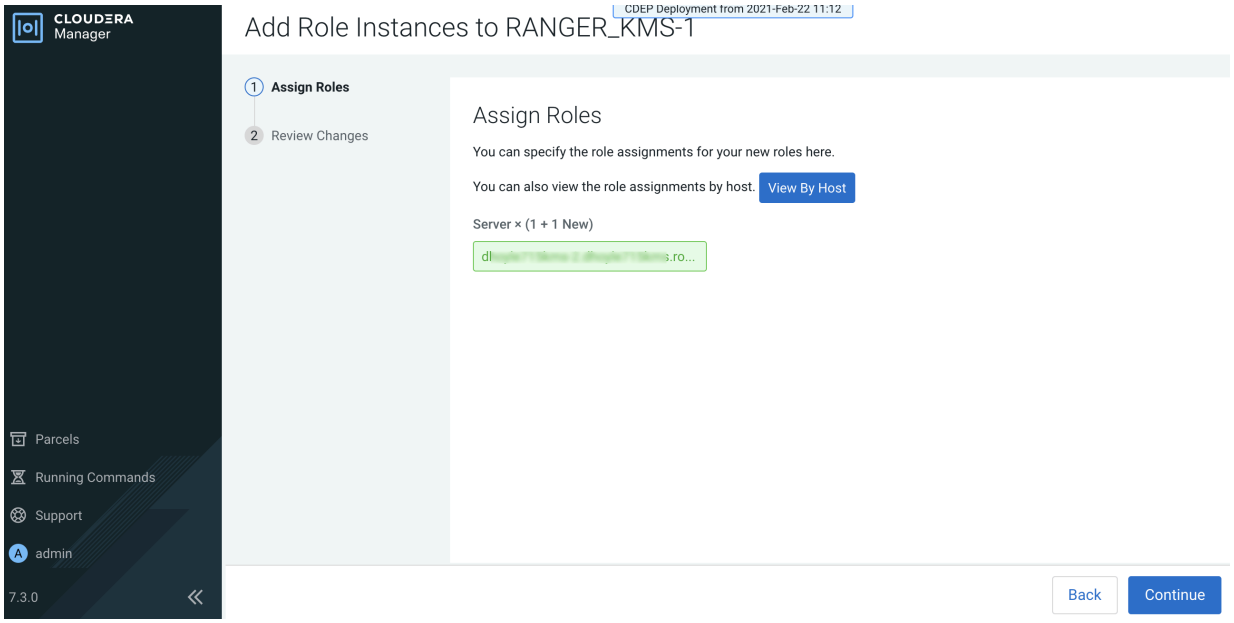


3. On the selected hosts page, select a backup Ranger KMS host. A Ranger KMS (RK) icon appears in the Added Roles column for the selected host. Click OK to continue.

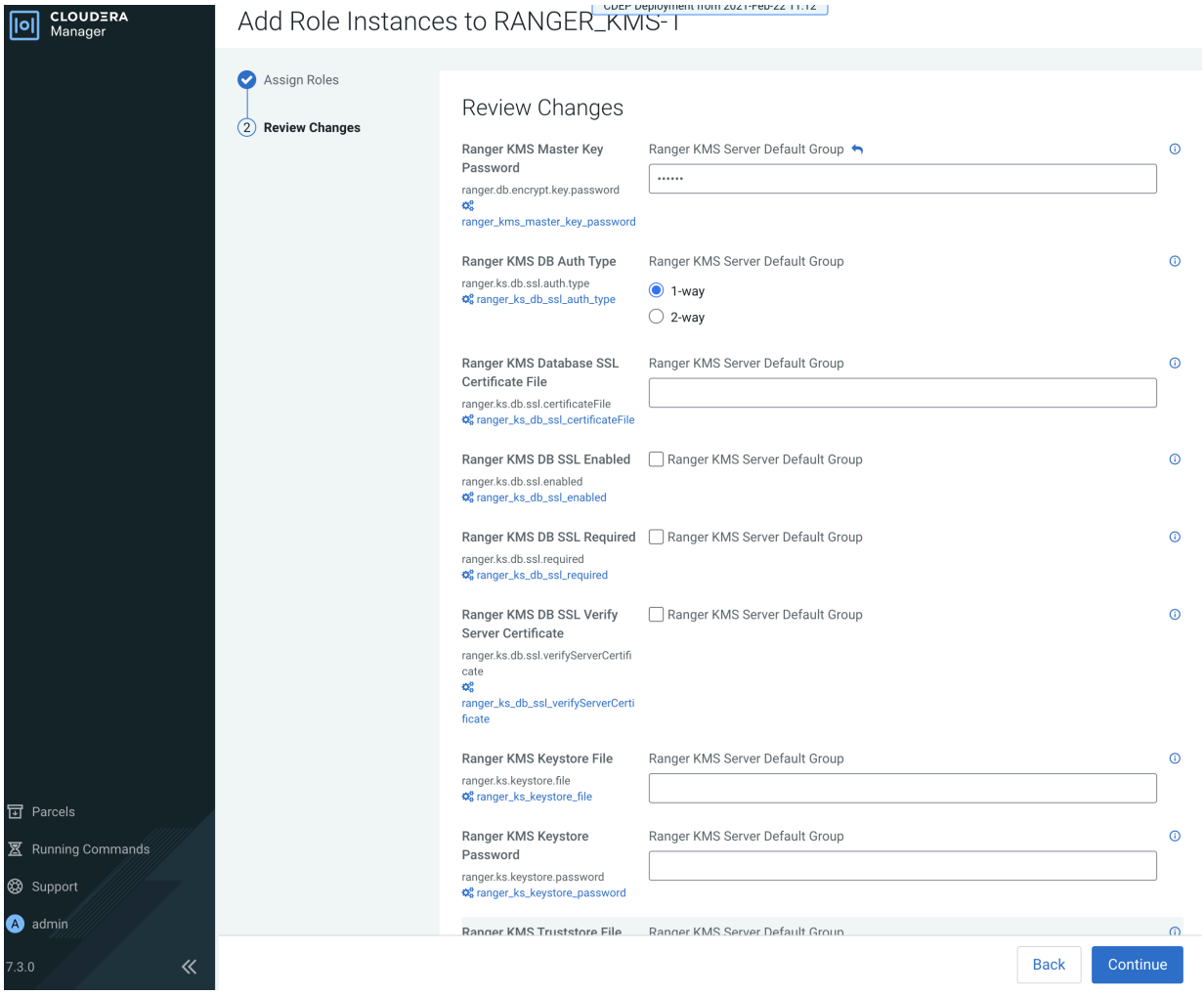
Note: These steps show how to add one additional backup Ranger KMS host, but you can use the same procedure to add multiple Ranger KMS hosts.



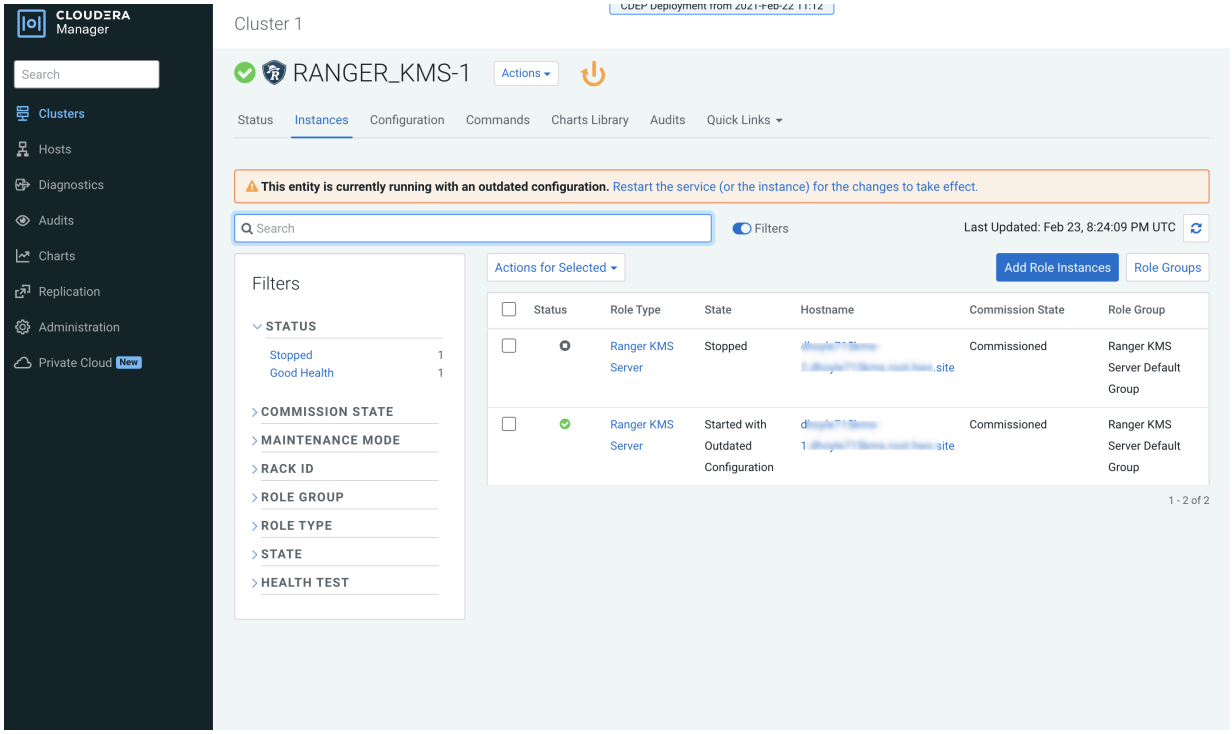
4. The Assign Roles page is redisplayed with the new backup host. Click Continue.



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



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.

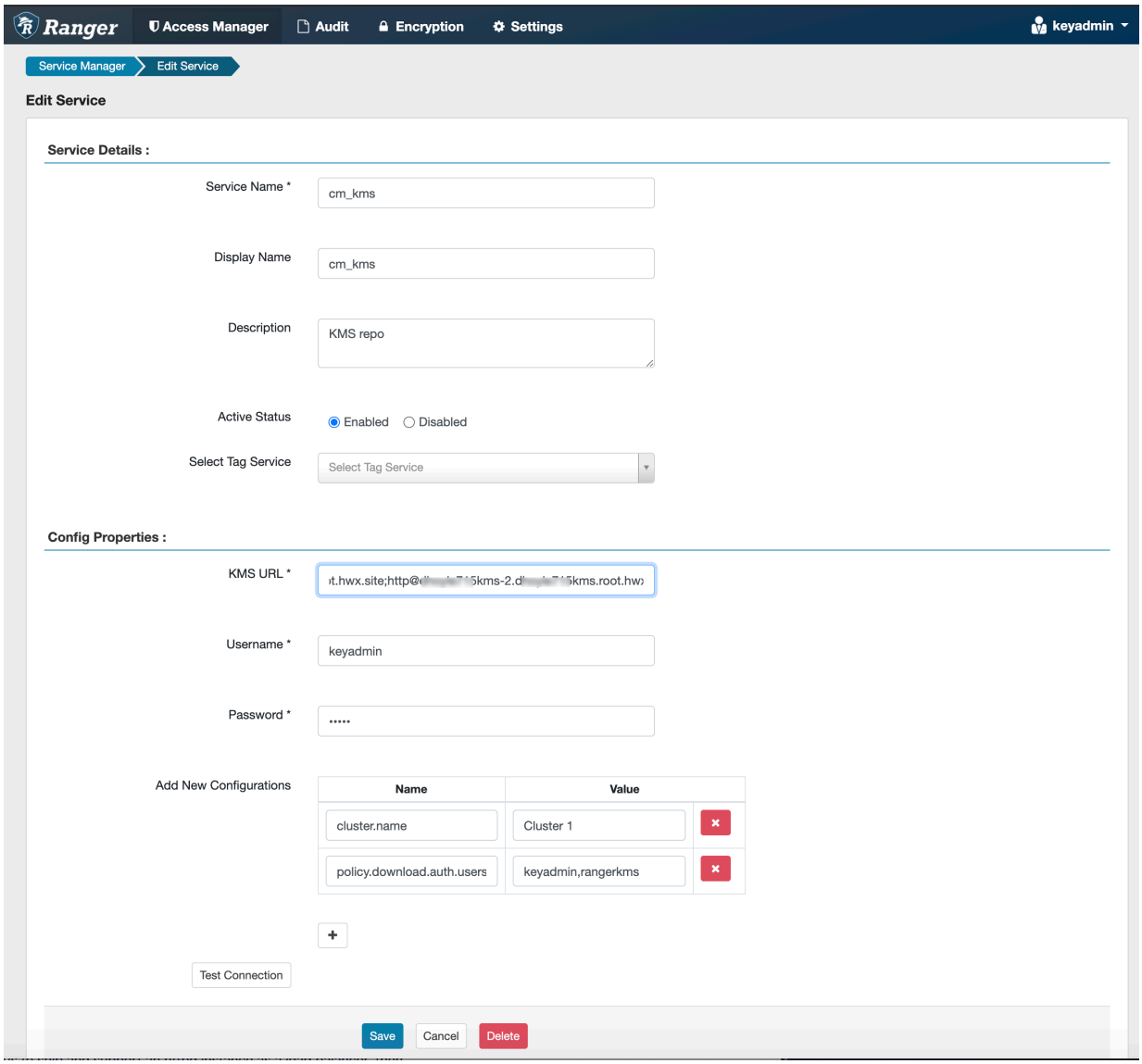
   - Add the new KMS host using the following format:

     kms://http@<kms_host1>;http@<kms_host2>:<kms_port>/kms
   - The default port is 9292. For example:

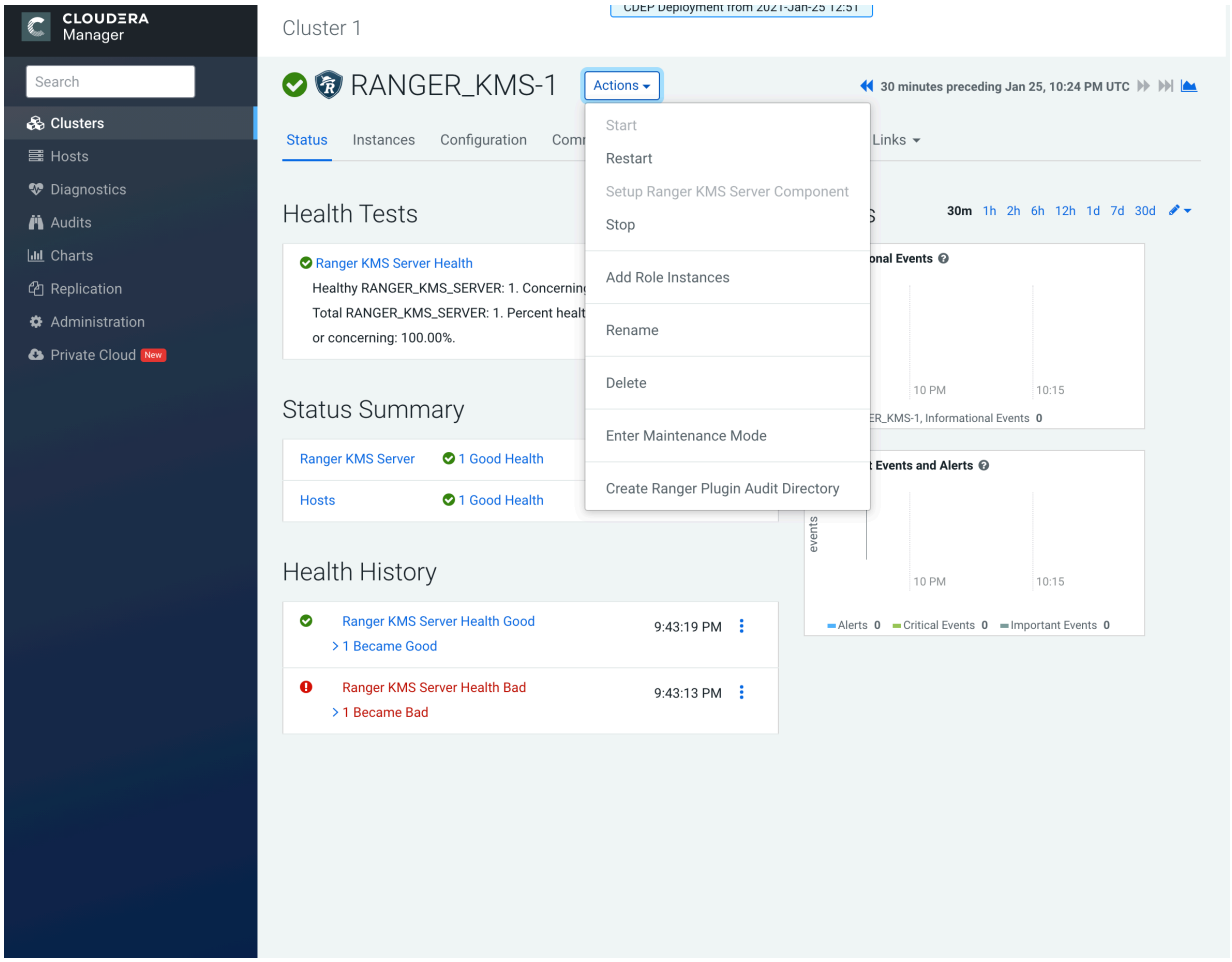
     kms://http@kms_host1;http@kms_host2:9292/kms
   - If SSL is enabled, use https and port 9494. For example:

     kms://http@kms_host1;http@kms_host2:9494/kms

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



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 .

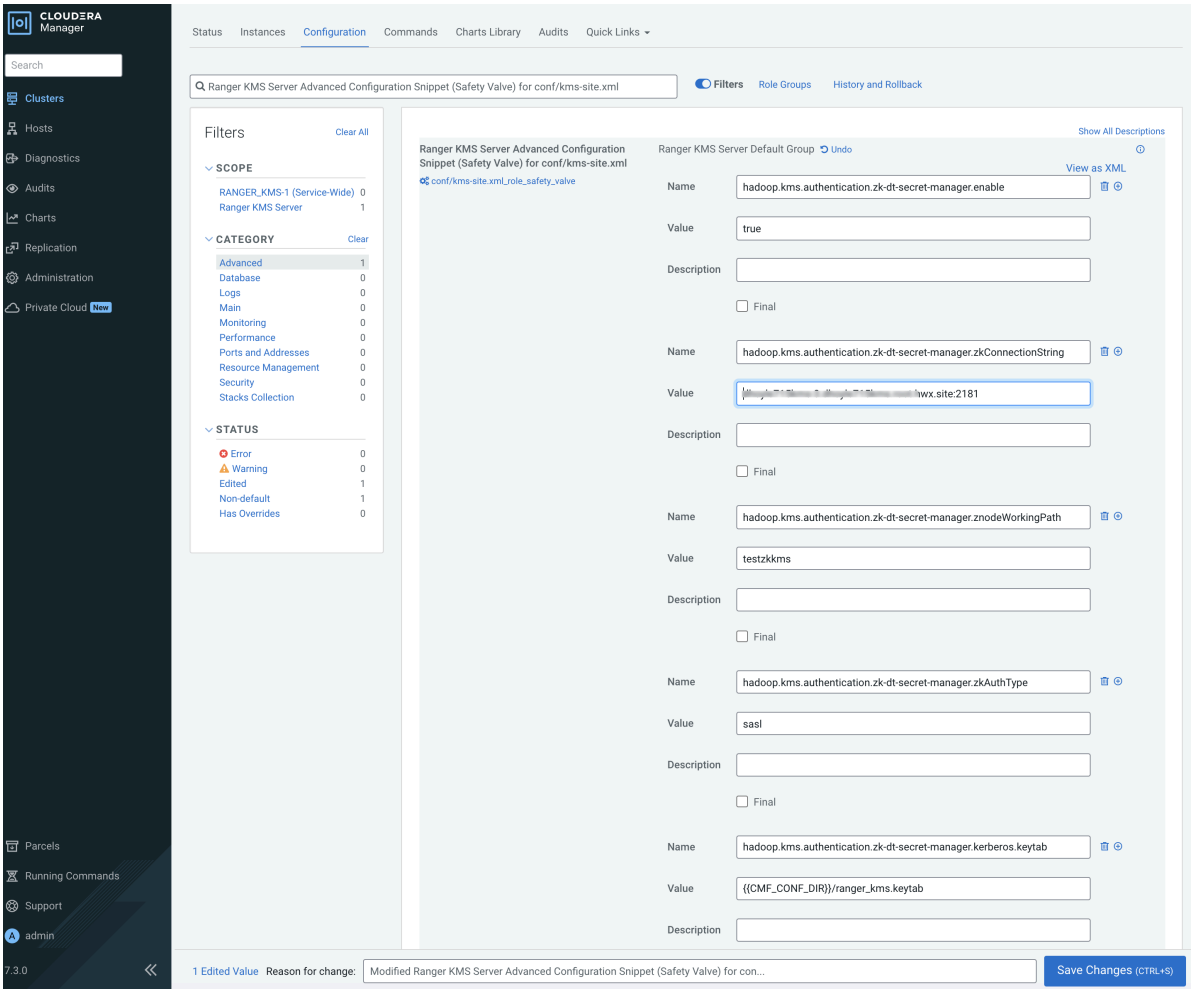
- hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath = <provide a znode working path other than /zkdtsm to avoid collision>

  For example:

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

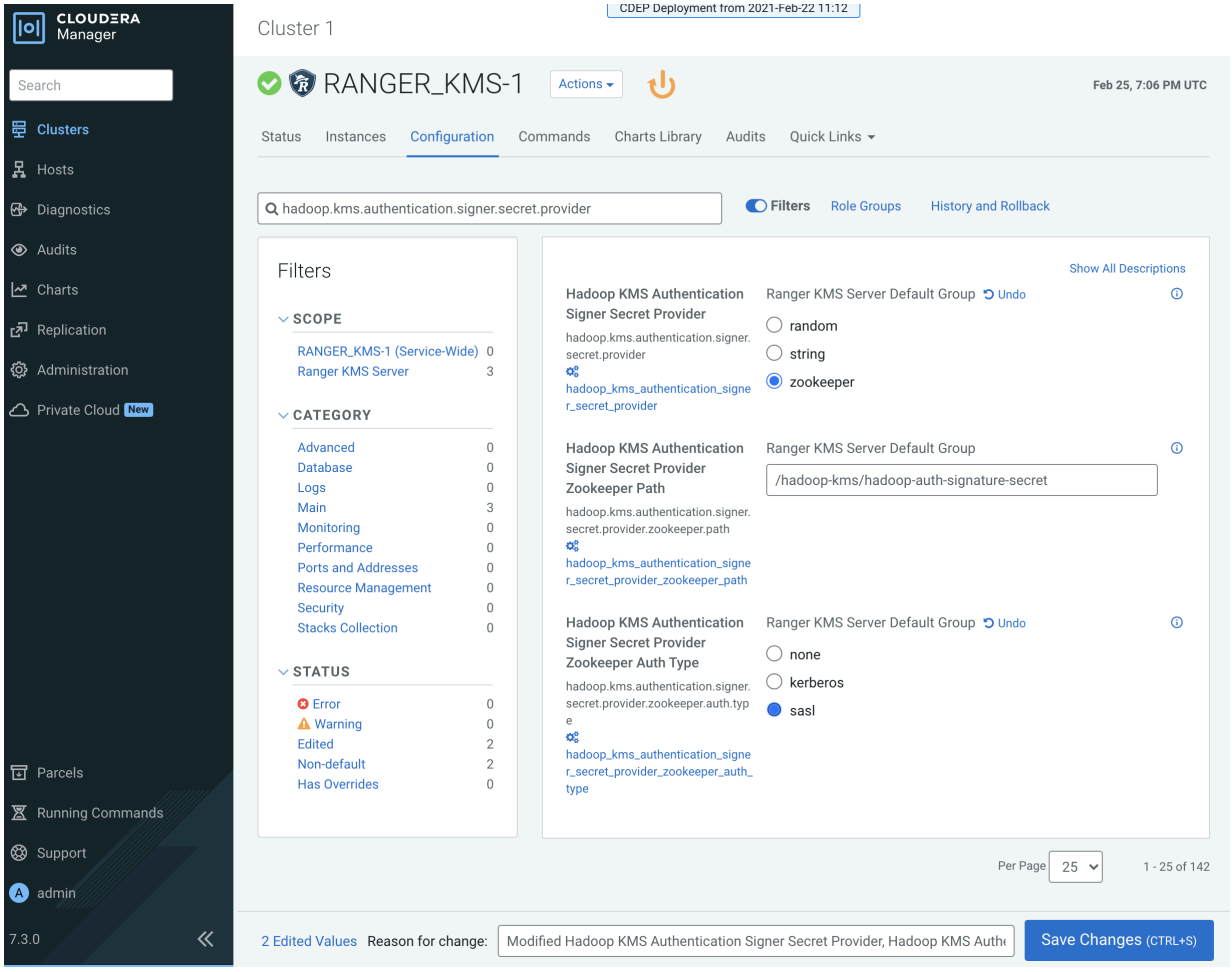
> **Note:** Do not put a leading slash at the beginning of the znode working path.

- hadoop.kms.authentication.zk-dt-secret-manager.zkAuthType = sasl
- hadoop.kms.authentication.zk-dt-secret-manager.kerberos.keytab = {{CMF_CONF_DIR}}/ranger_kms.keytab

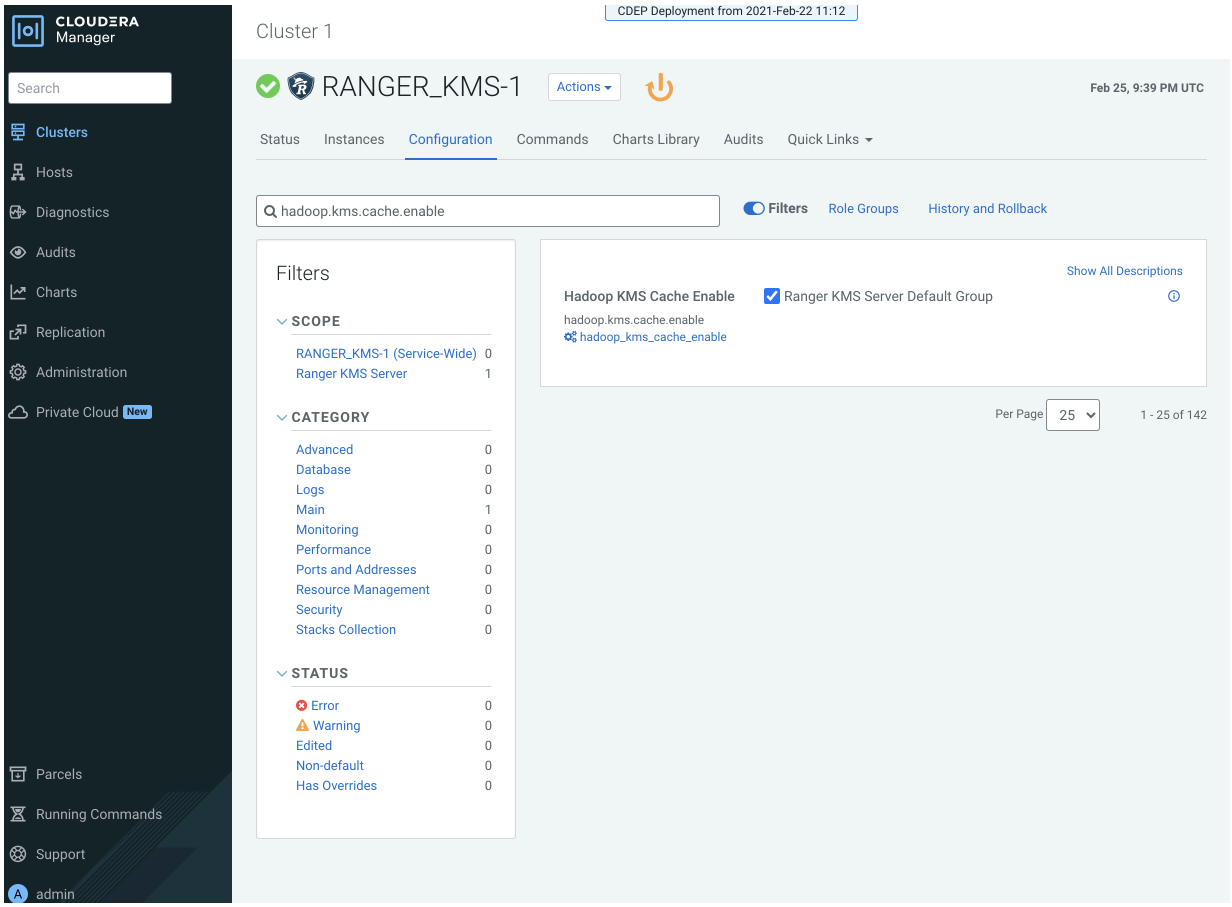


10. Update the following Ranger KMS configuration properties, then click Save Changes.

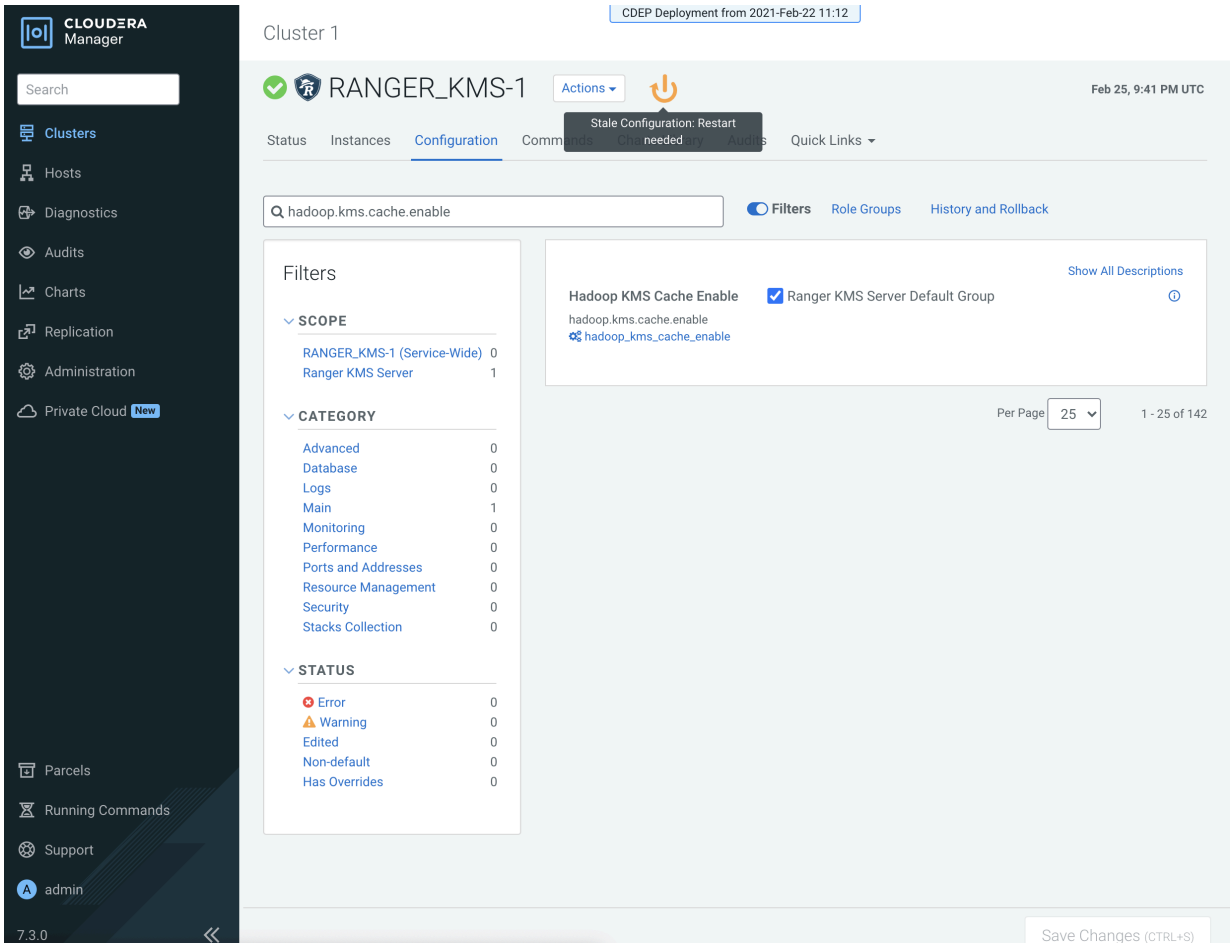
- hadoop.kms.authentication.signer.secret.provider = zookeeper
- hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type = sasl



11. Verify that the hadoop.kms.cache.enable property is set to the default value of true (the check box is selected).



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 .