Cloudera Runtime 7.1.3

Configuring and Using Ranger KMS

Date published: 2019-11-01
Date modified:

https://docs.cloudera.com/

Legal Notice

Contents

Configuring Ranger KMS High Availability

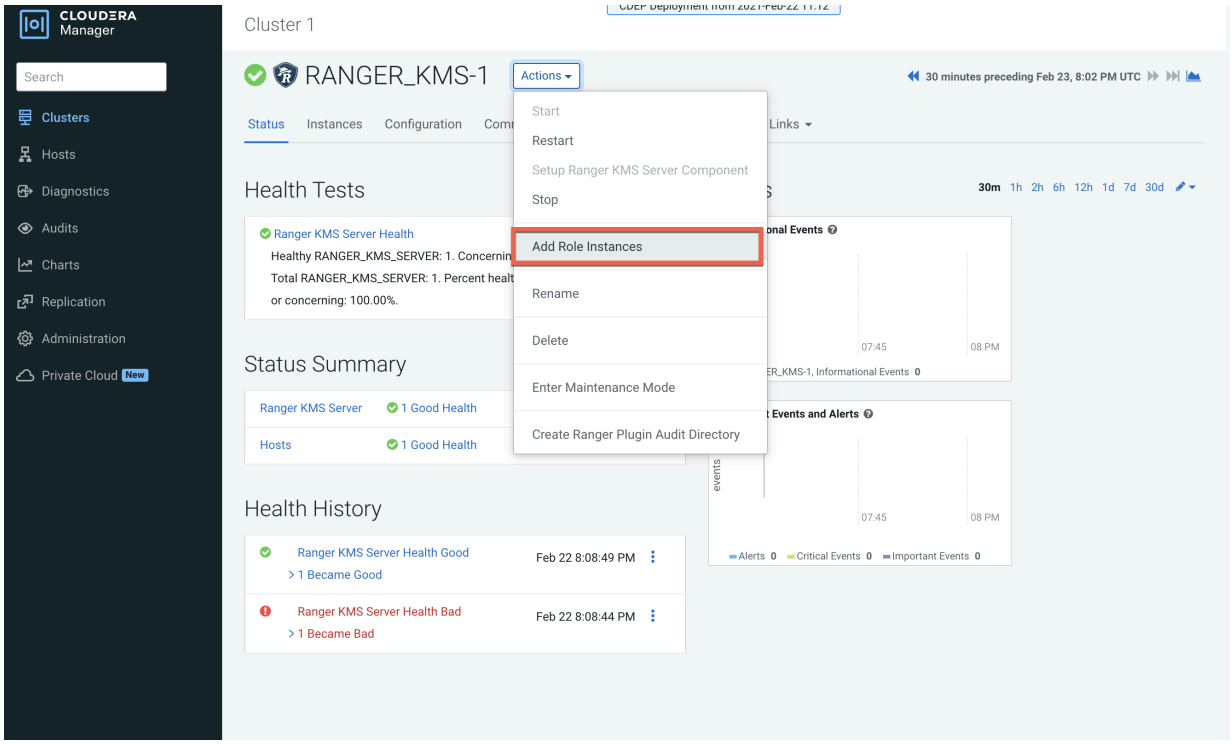
How to configure Ranger KMS high availability (HA) for Ranger KMS.

Configure High Availability for Ranger KMS with DB

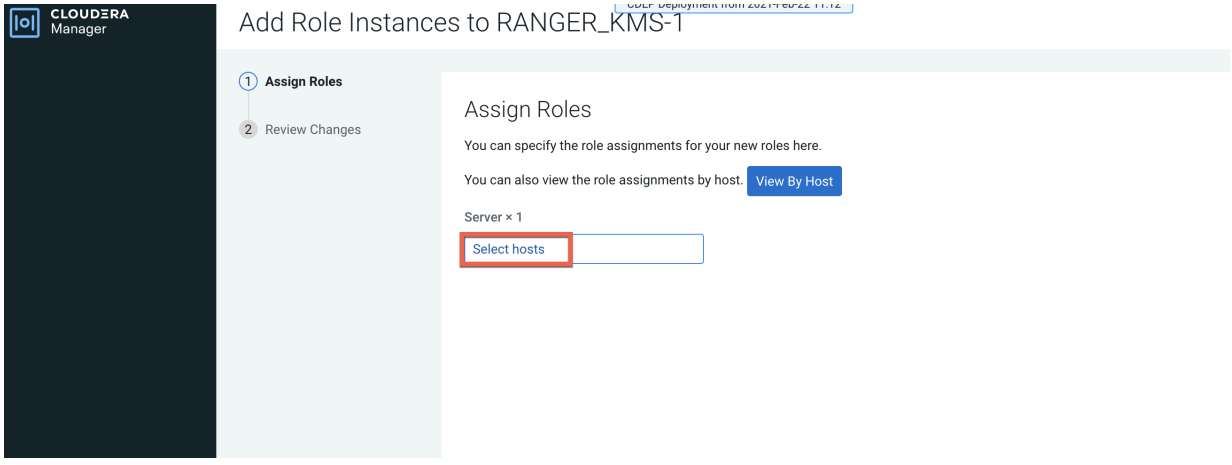
Use the following steps to configure high availability for Ranger KMS with an associated keystore database.

Procedure

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

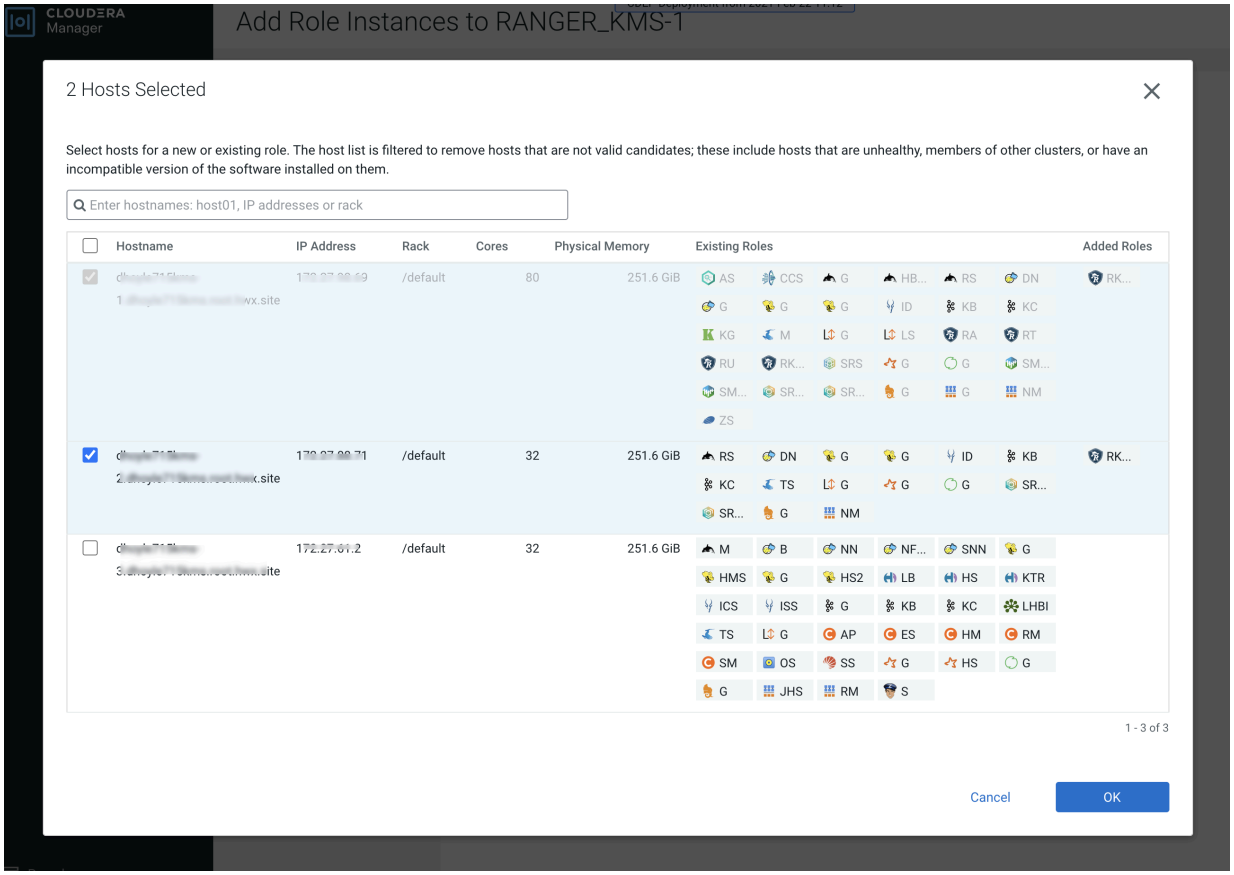


2. On the Assign Roles page, click Select hosts.

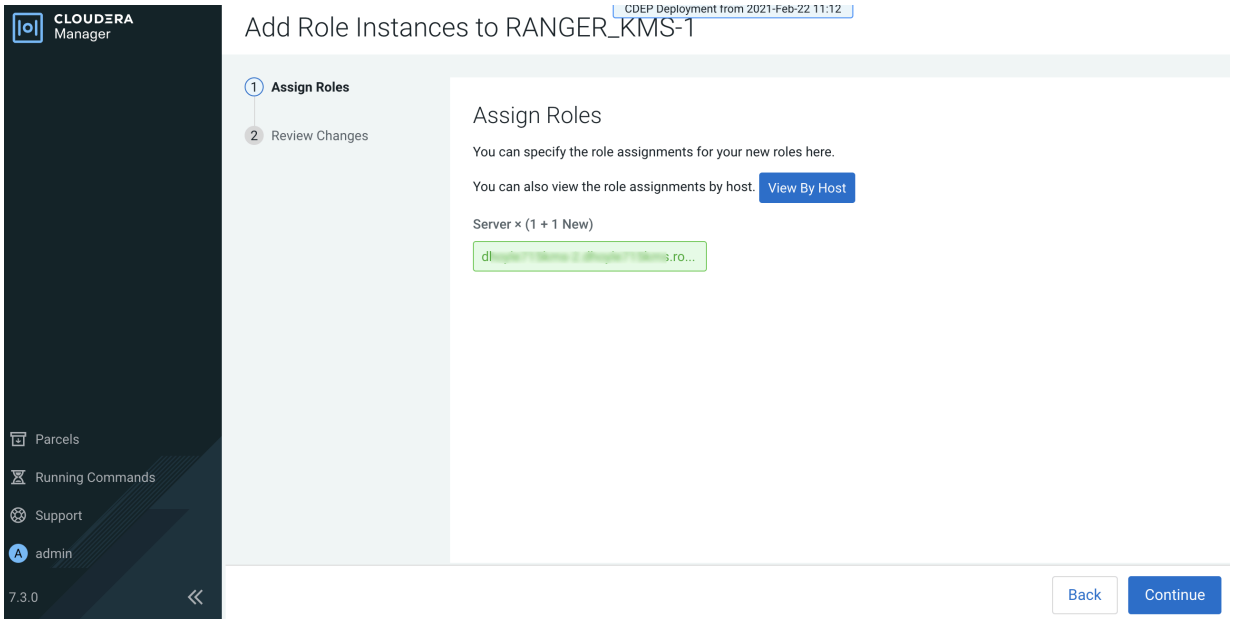


3. On the selected hosts page, select a backup Ranger KMS host. A Ranger KMS (RK) icon appears in the Added Roles column for the selected host. Click OK to continue.

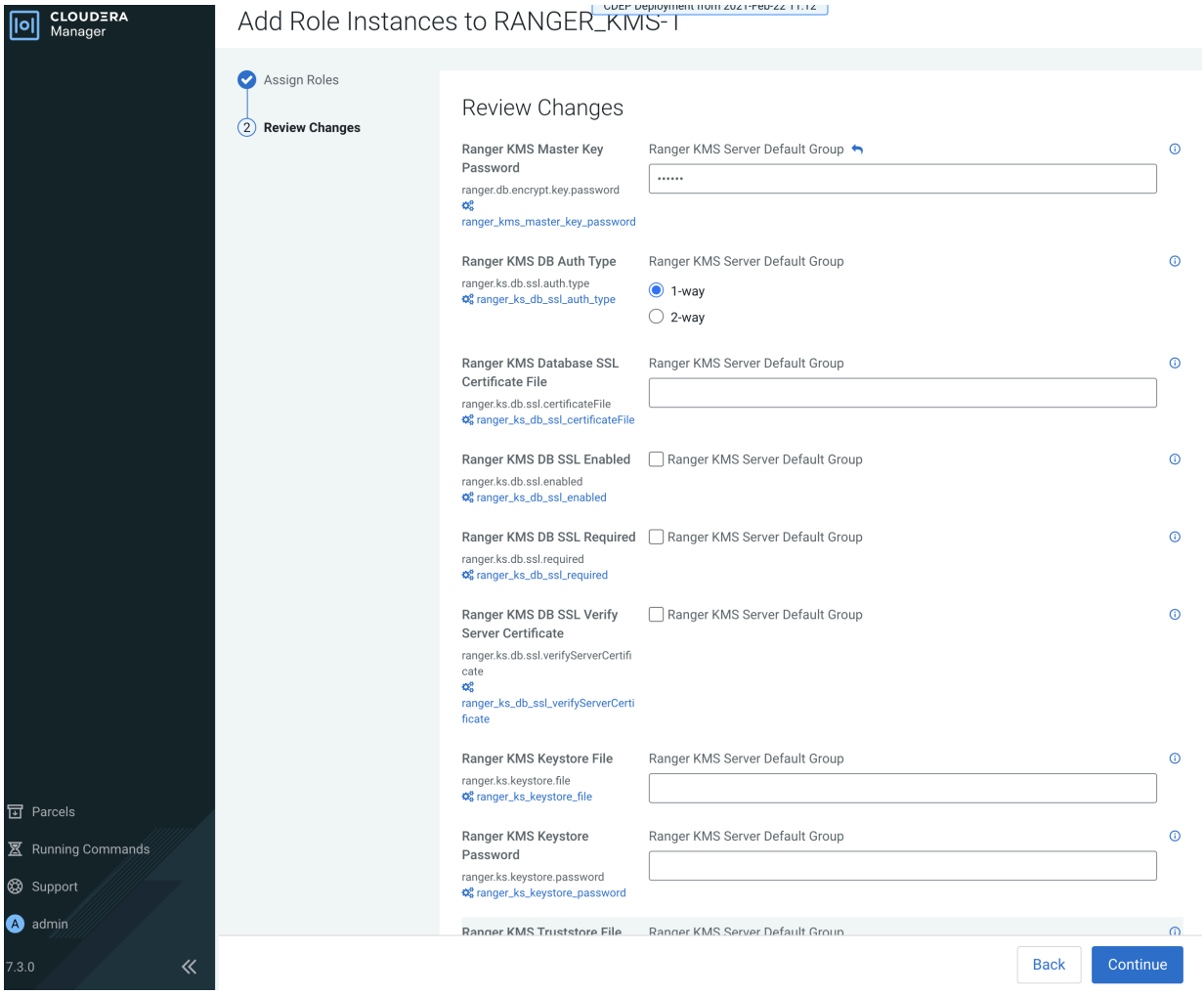
Note: These steps show how to add one additional backup Ranger KMS host, but you can use the same procedure to add multiple Ranger KMS hosts.



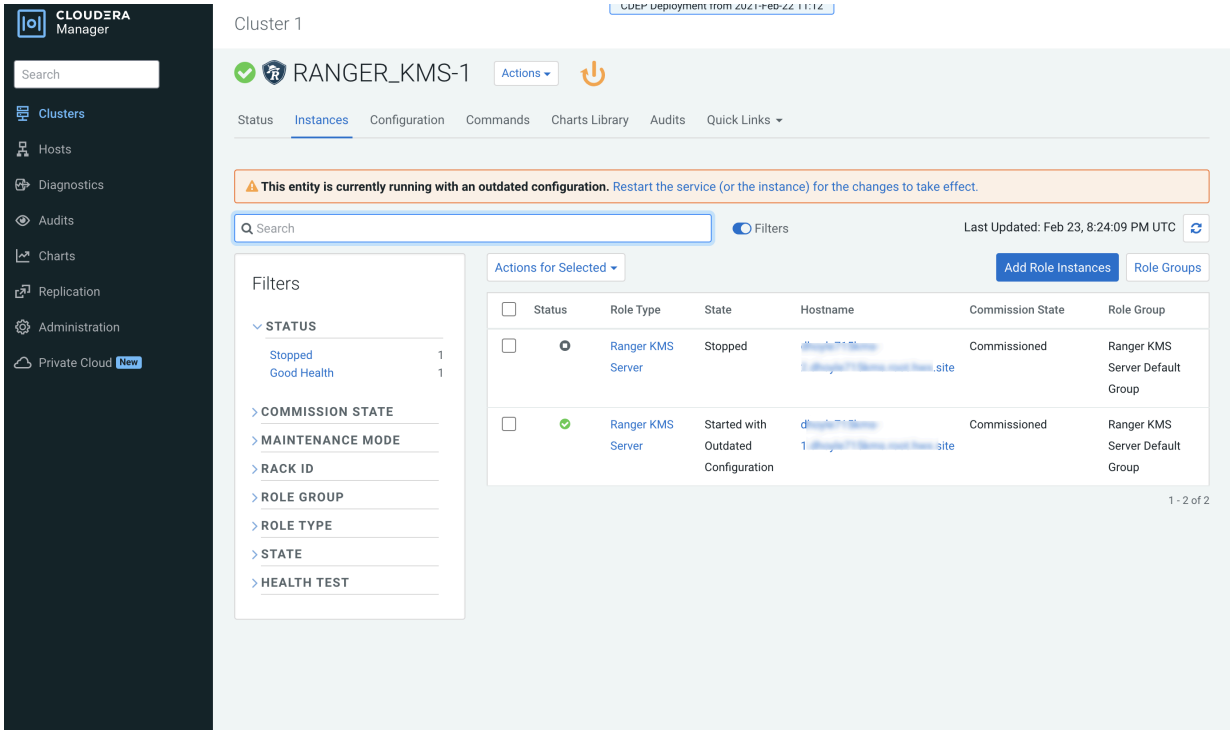
4. The Assign Roles page is redisplayed with the new backup host. Click Continue.



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.

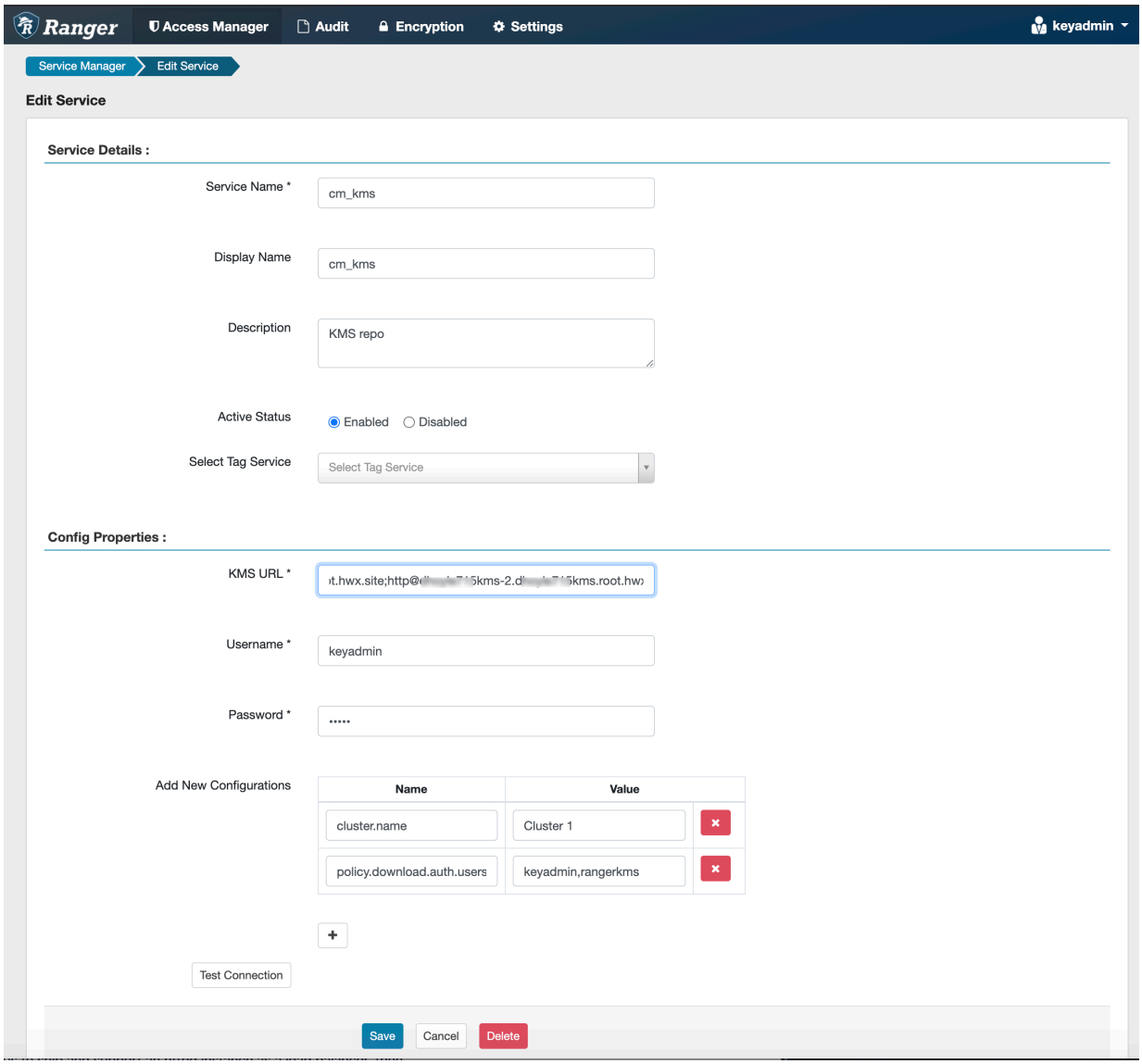
   - Add the new KMS host using the following format:

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

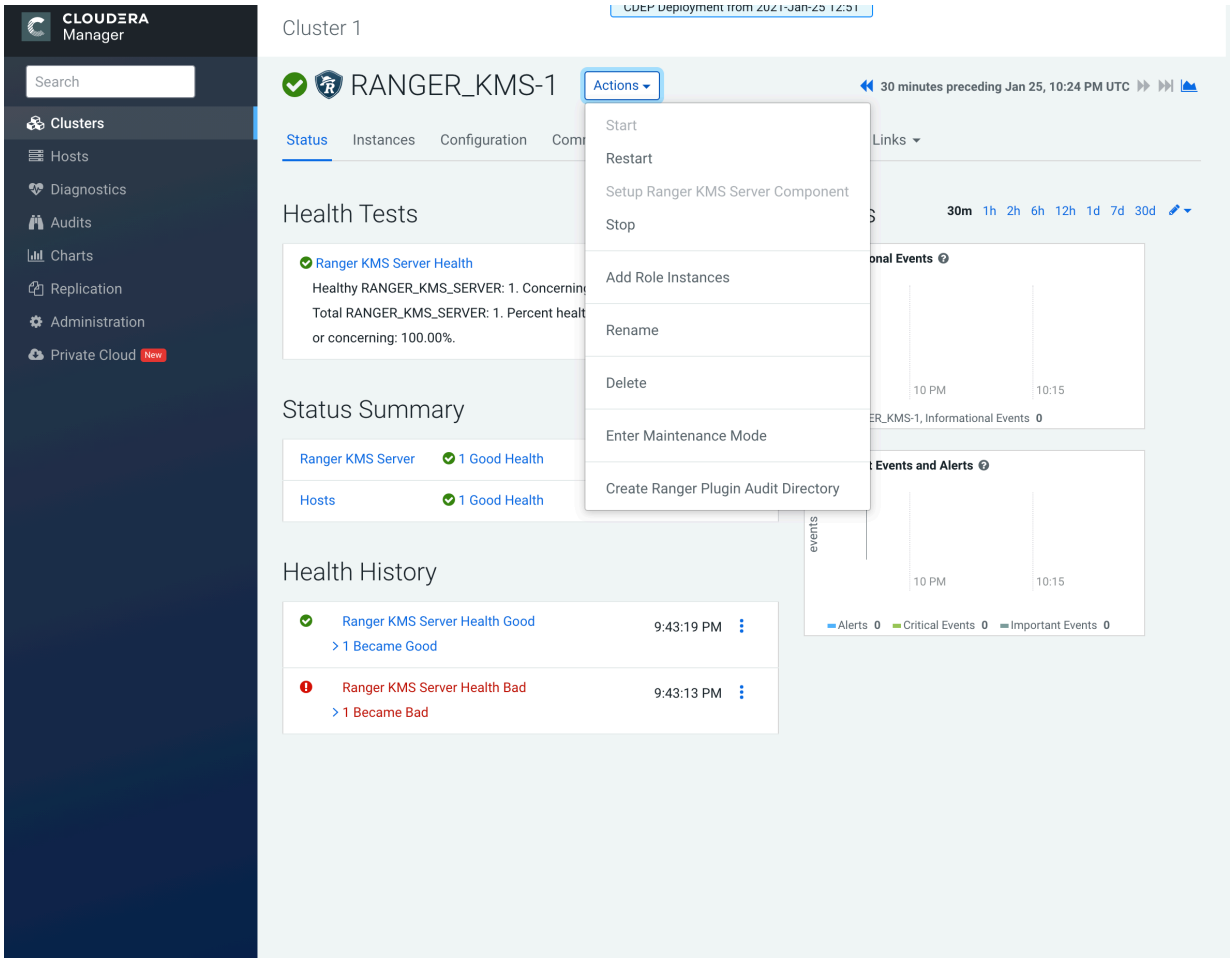
     kms://http@kms_host1;http@kms_host2:9292/kms
   - If SSL is enabled, use https and port 9494. For example:

     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.

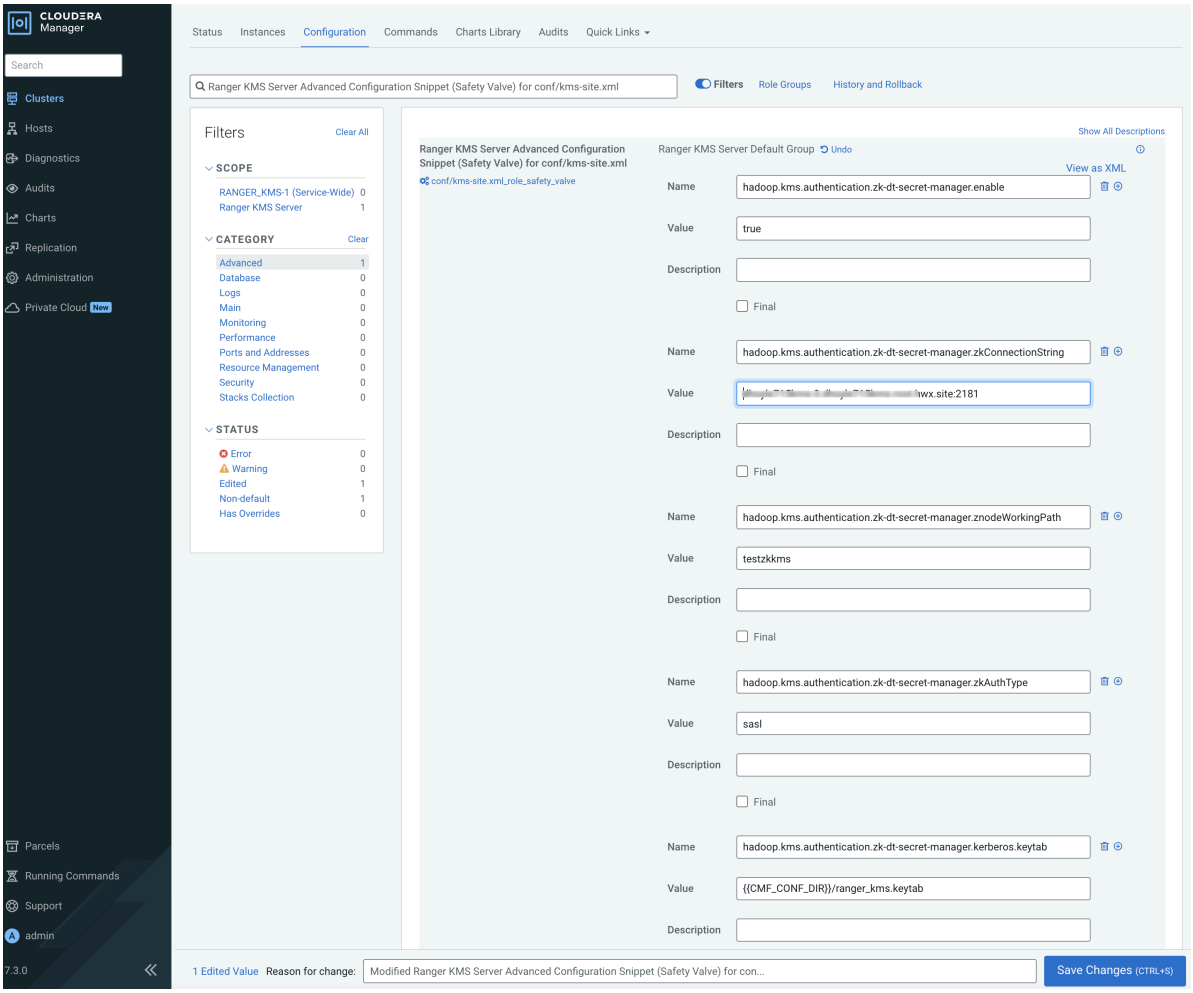
- hadoop.kms.authentication.zk-dt-secret-manager.enable = true
- hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString = <Zookeeper hostname>:2181

  Note: In a cluster with multiple ZK hosts, include them as a comma-seperated 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:

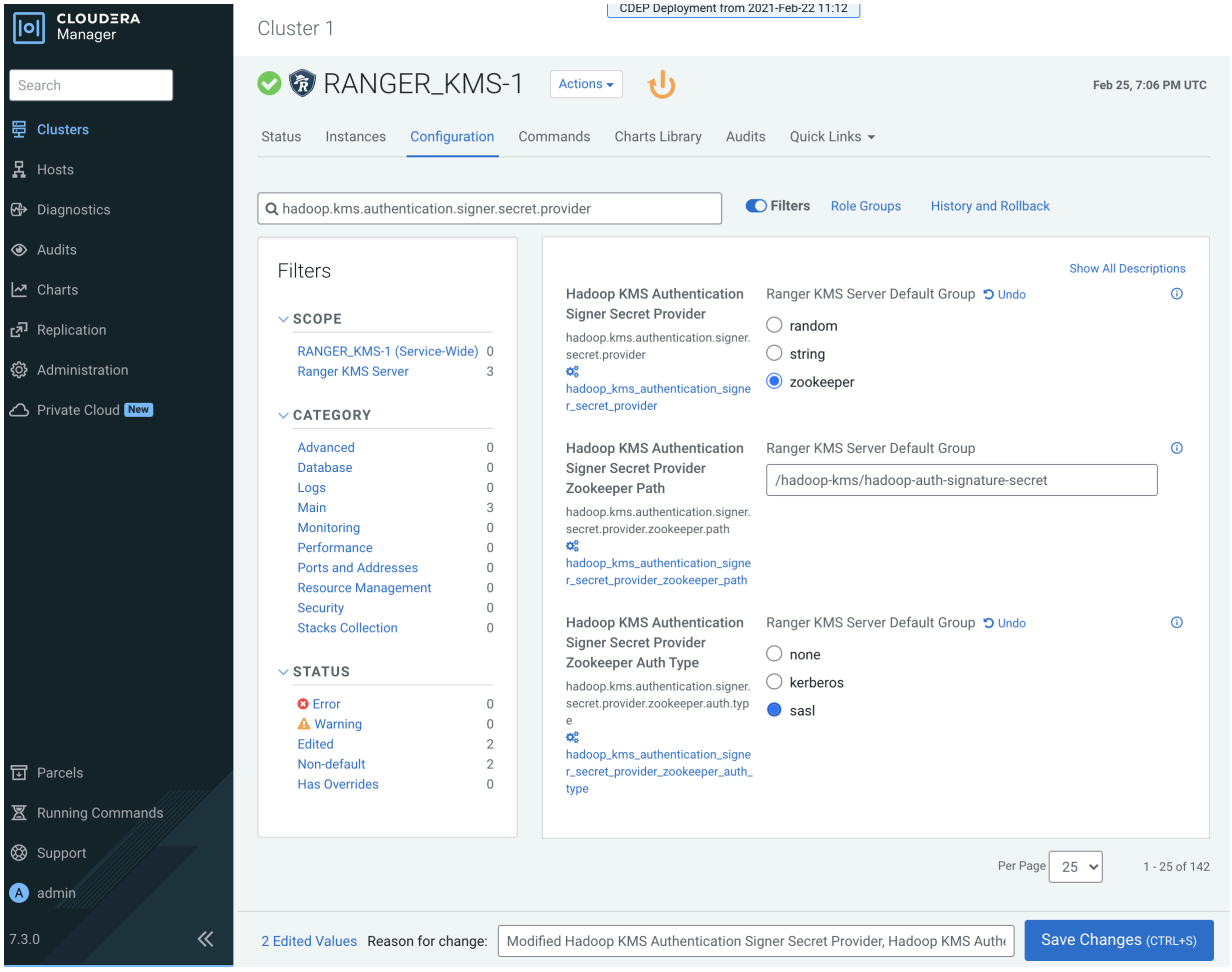
  hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath = testzkkms

  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

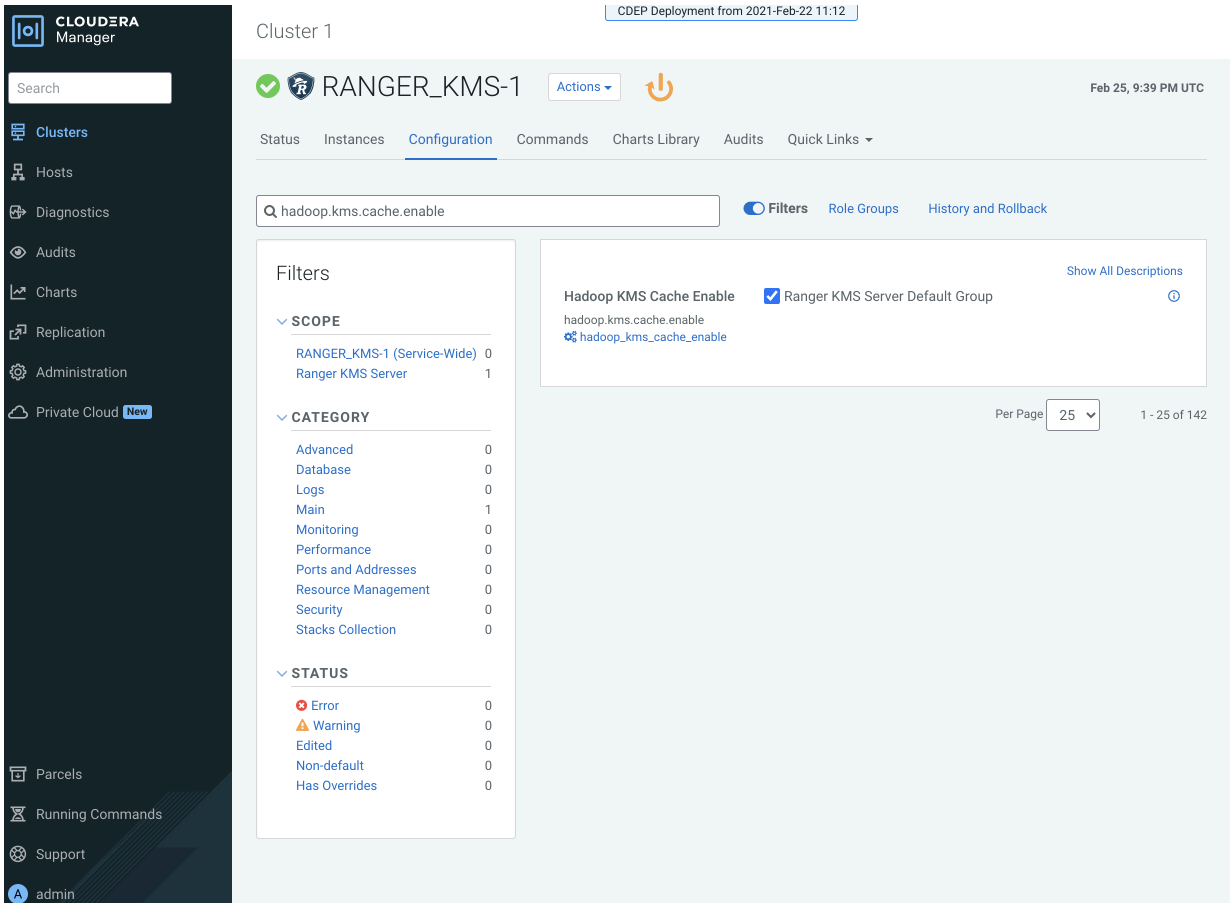


10. Update the following Ranger KMS configuration properties, then click Save Changes.

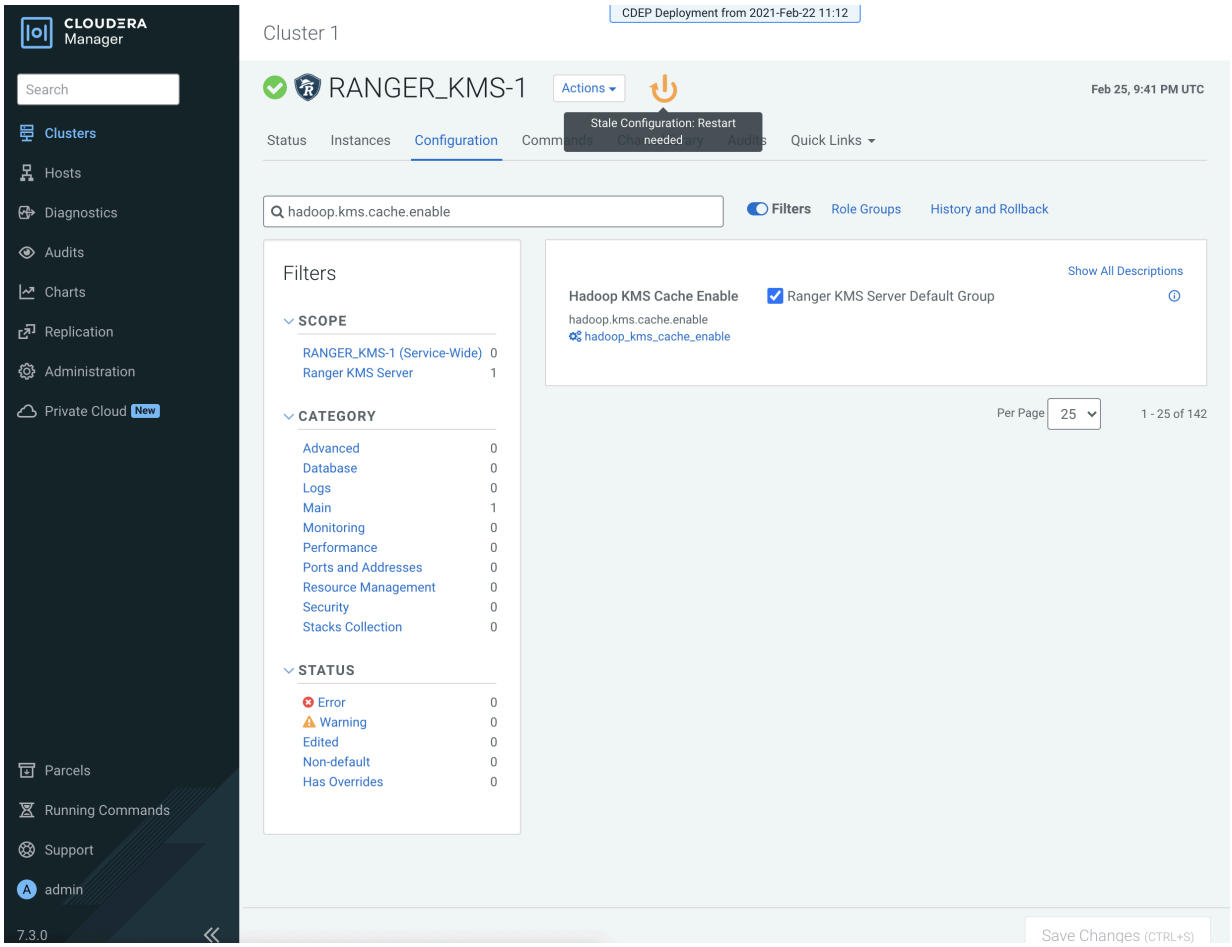
- hadoop.kms.authentication.signer.secret.provider = zookeeper
- hadoop.kms.authentication.signer.secret.provider.zookeeper.auth.type = sasl



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.



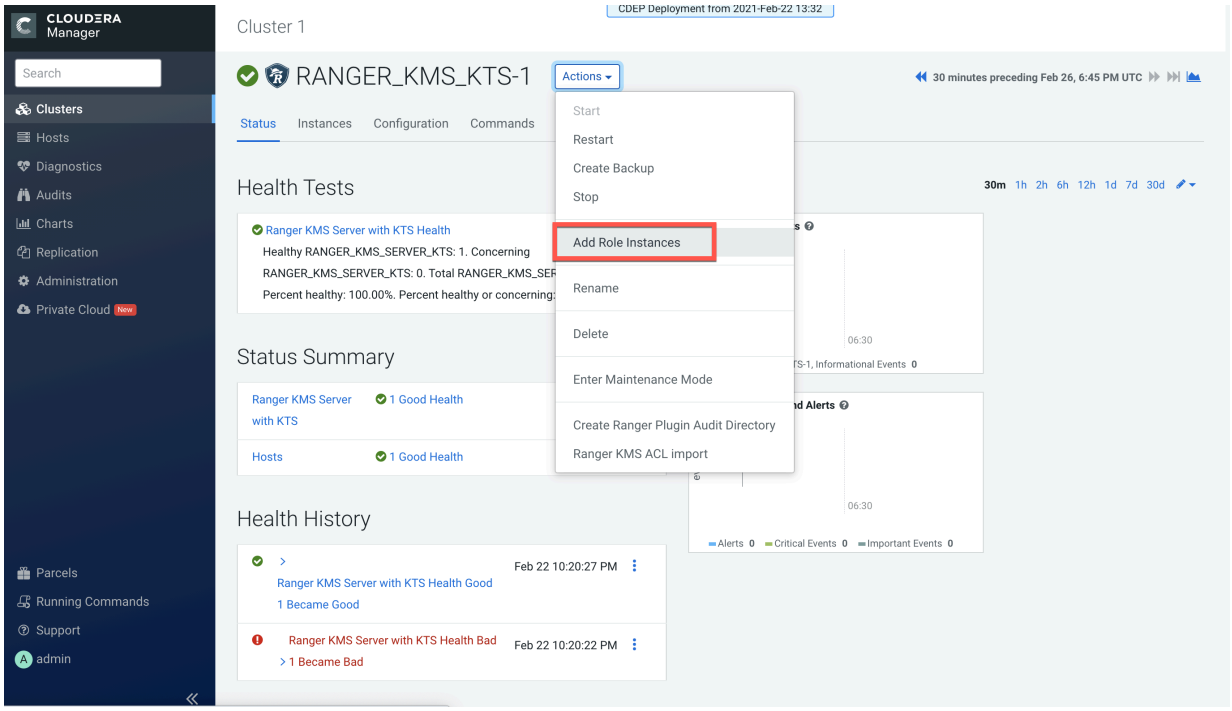
13. On the Stale Configurations page, click Restart Stale Services.
14. On the Restart Stale Services page, select the Re-deploy client configuration checkbox, then click Restart Now.
15. A progress indicator page appears while the services are being restarted. When the services have restarted, click Finish.

Configure High Availability for Ranger KMS with KTS

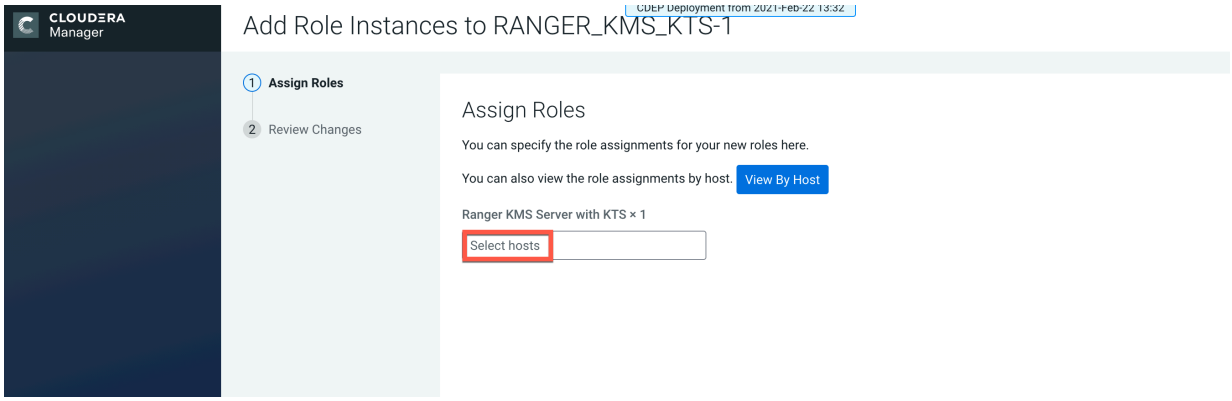
Use the following steps to configure high availability for Ranger KMS with Key Trustee Server as the backing key store.

Procedure

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

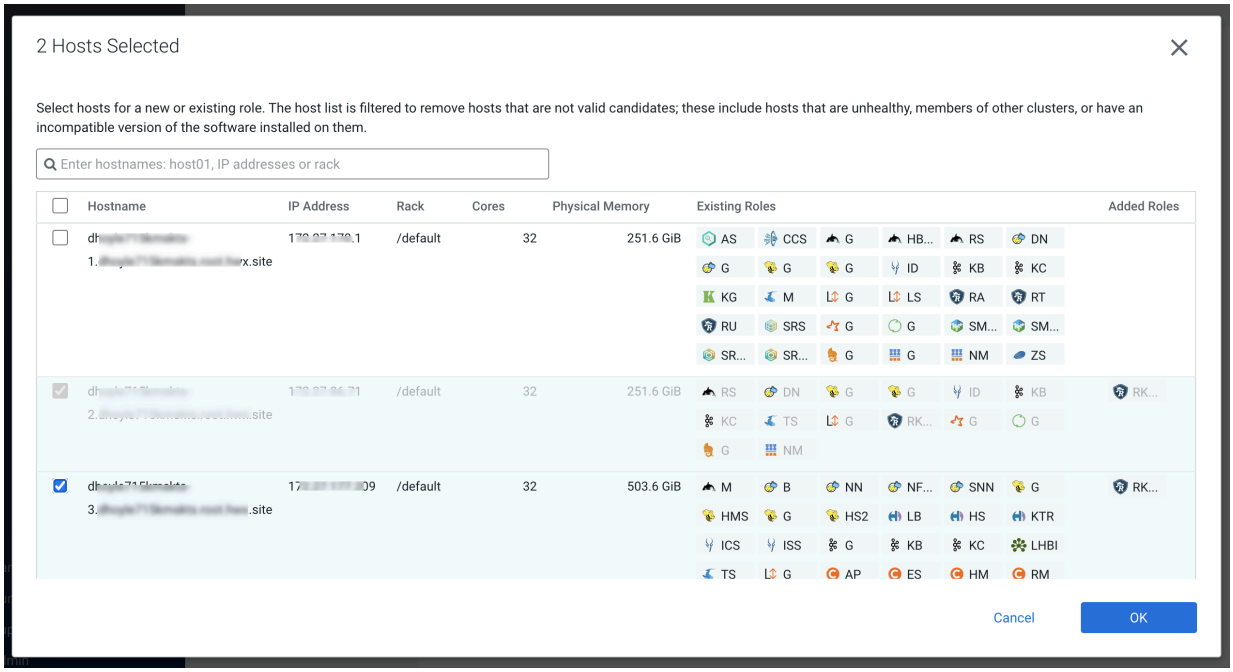


2. On the Assign Roles page, click Select hosts.

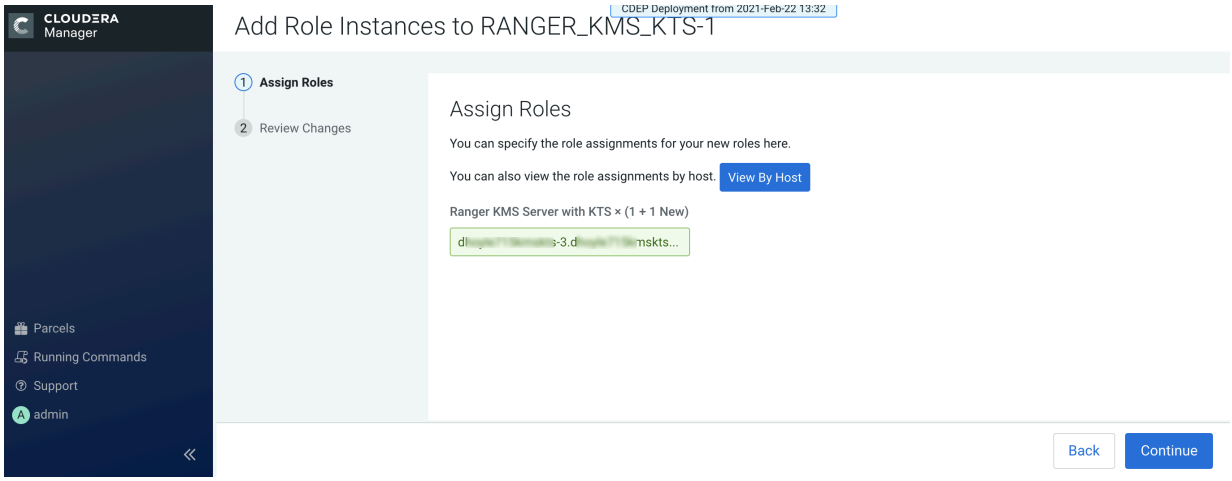


3. On the selected hosts page, select a backup Ranger KMS KTS host. A Ranger KMS KTS (RK) icon appears in the Added Roles column for the selected host. Click OK to continue.

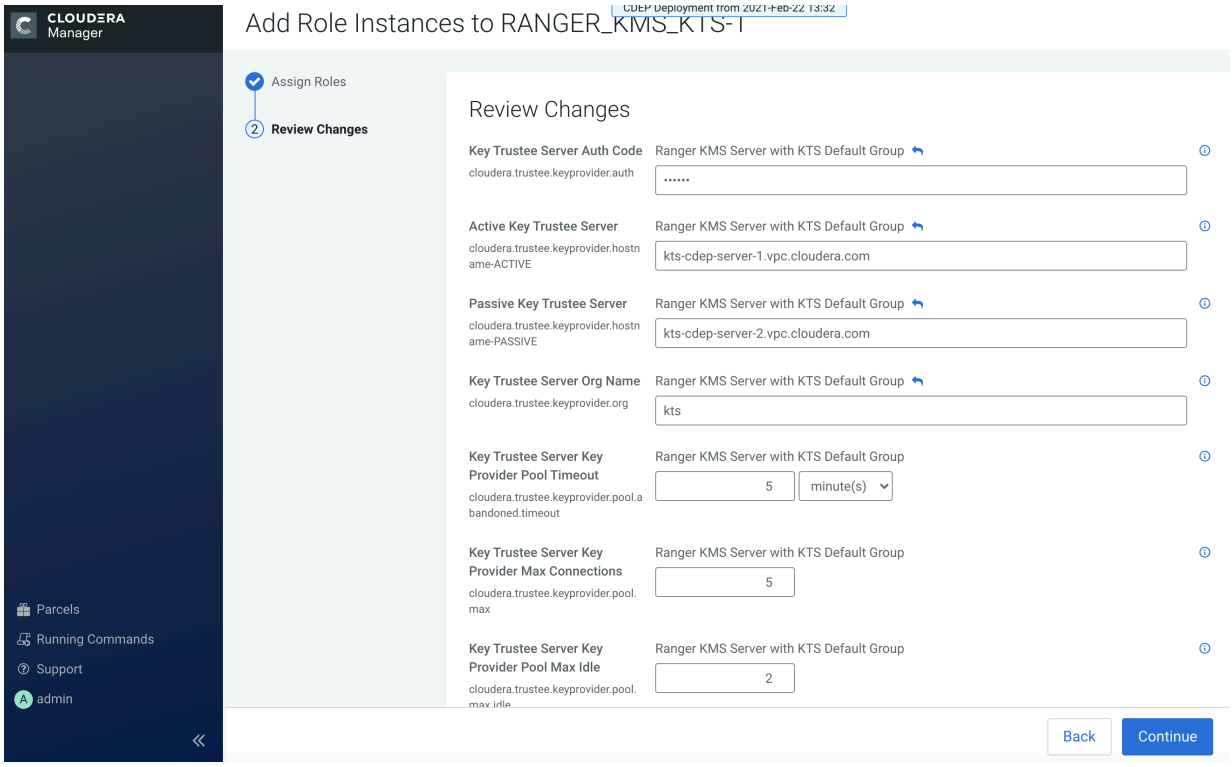
   Note: These steps show how to add one additional backup Ranger KMS KTS host, but you can use the same procedure to add multiple Ranger KMS KTS hosts.



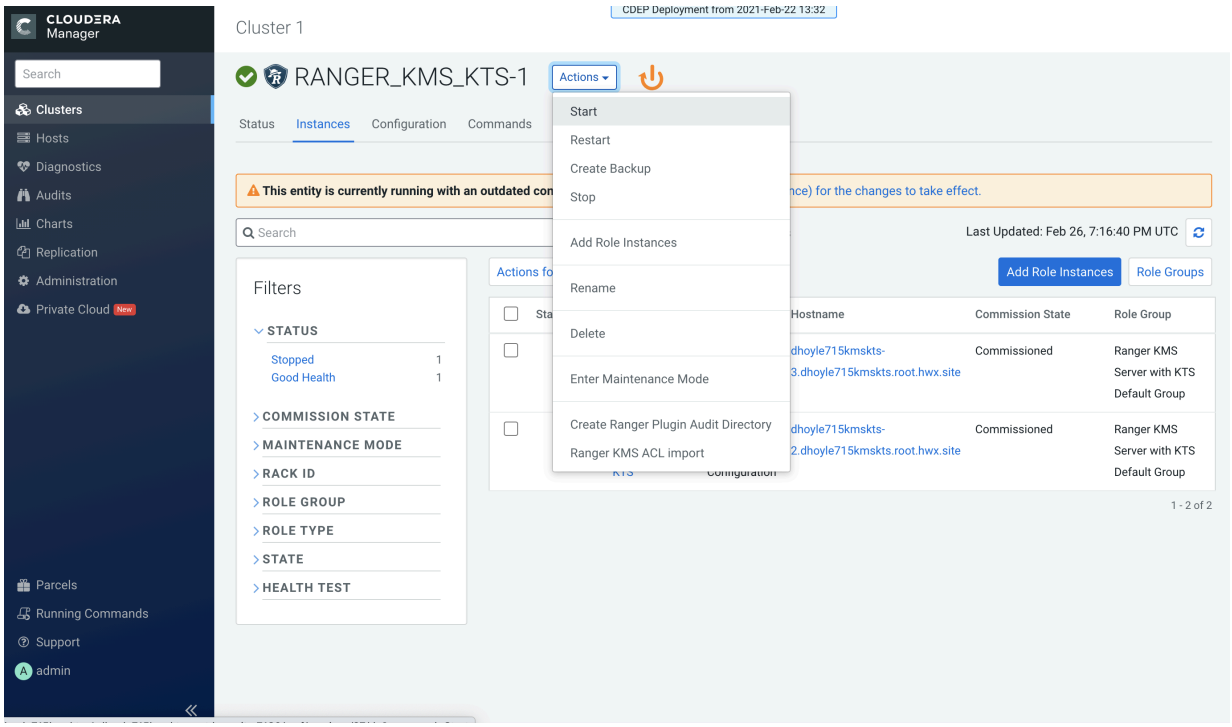
4. The Assign Roles page is redisplayed with the new backup host. Click Continue.



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



6. The new role instance appears on the Ranger KMS 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.

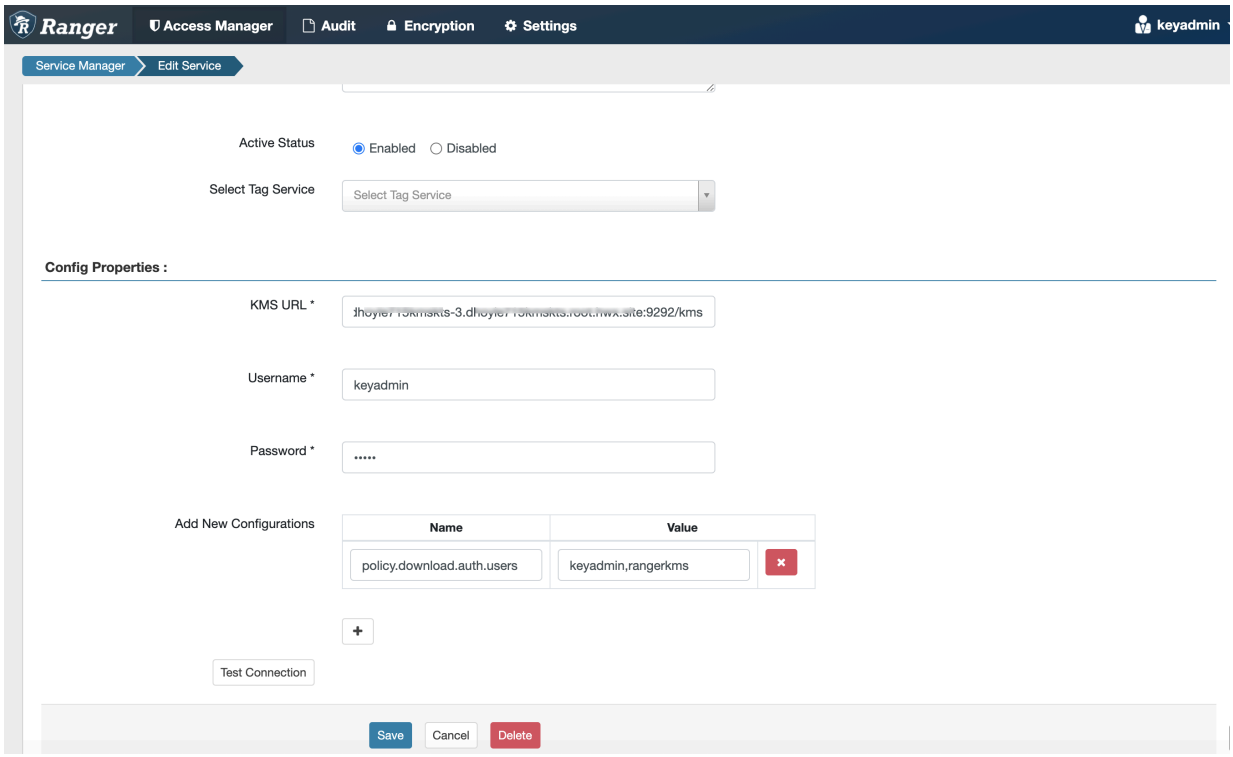
   - Add the new KMS host using the following format:

     kms://http@<kms_kts_host1>;http@<kms_kts_host2>:<kms_port>/kms
   - The default port is 9292. For example:

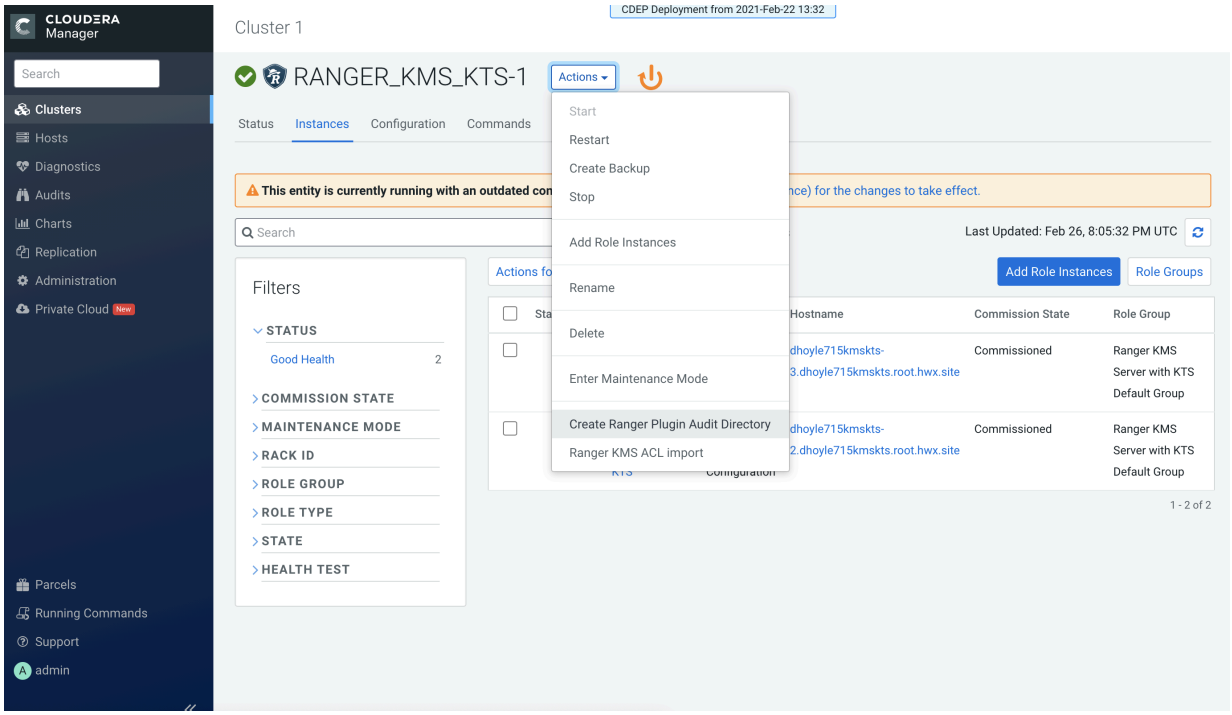
     kms://http@kms_kts_host1;http@kms_kts_host2:9292/kms
   - If SSL is enabled, use https and port 9494. For example:

     kms://http@kms_kts_host1;http@kms_kts_host2:9494/kms

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



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



11. In Cloudera Manager, select Ranger KMS KTS, 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.

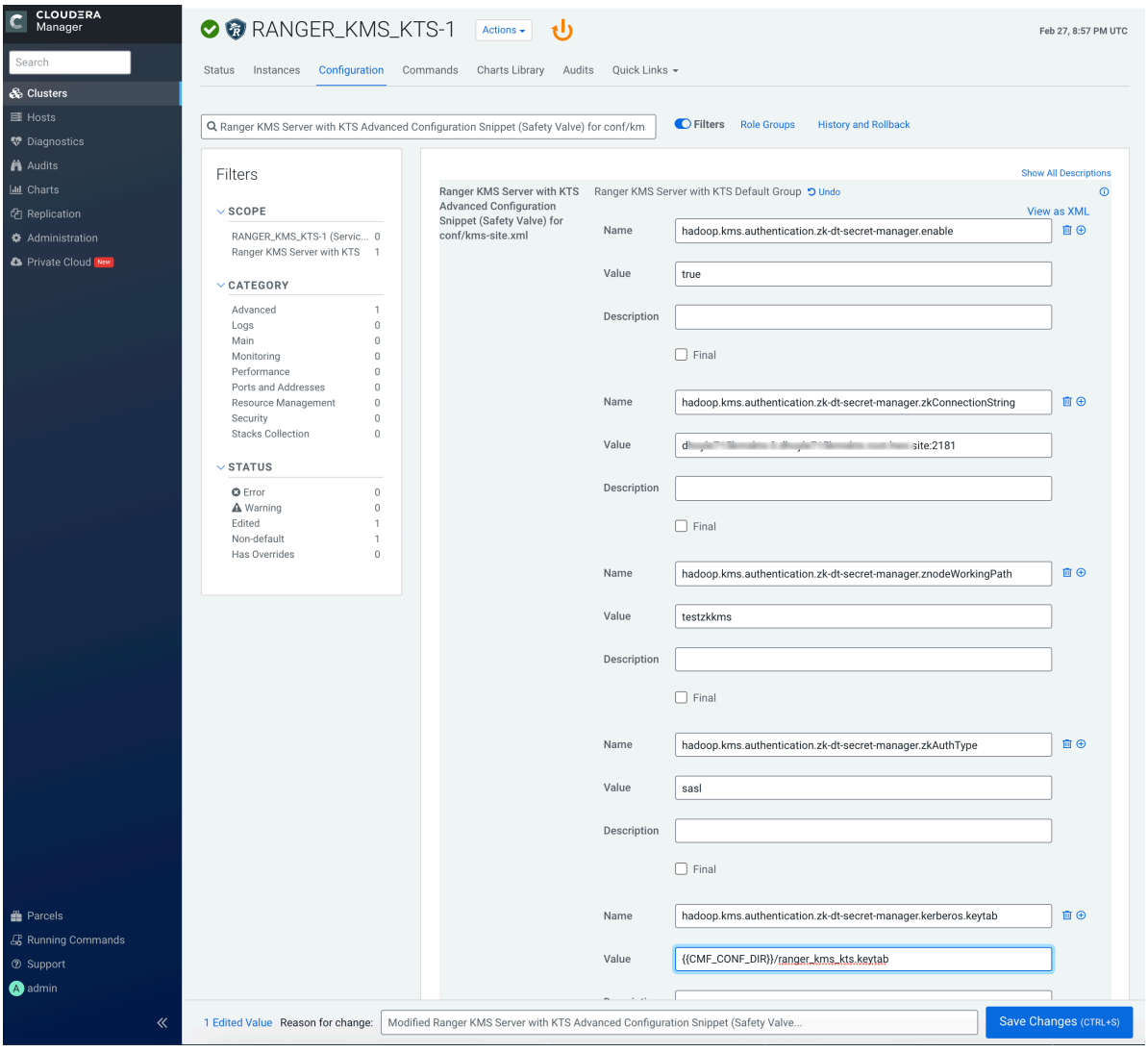
- hadoop.kms.authentication.zk-dt-secret-manager.enable = true
- hadoop.kms.authentication.zk-dt-secret-manager.zkConnectionString = <Zookeeper hostname>:2181
- hadoop.kms.authentication.zk-dt-secret-manager.znodeWorkingPath = <provide a znode working path other than /zkdtsm to avoid collision>

  For example:

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

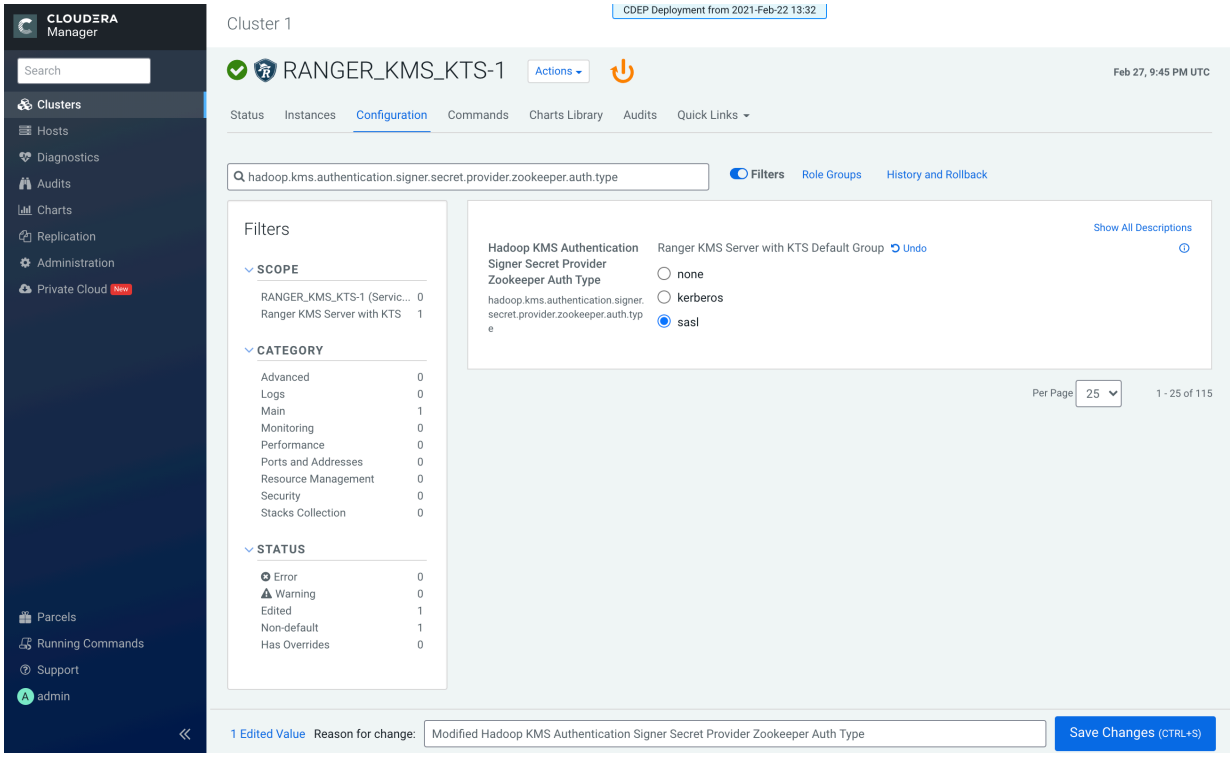
  Note: Do not put a leading slash at the beginning of the znode working path.

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

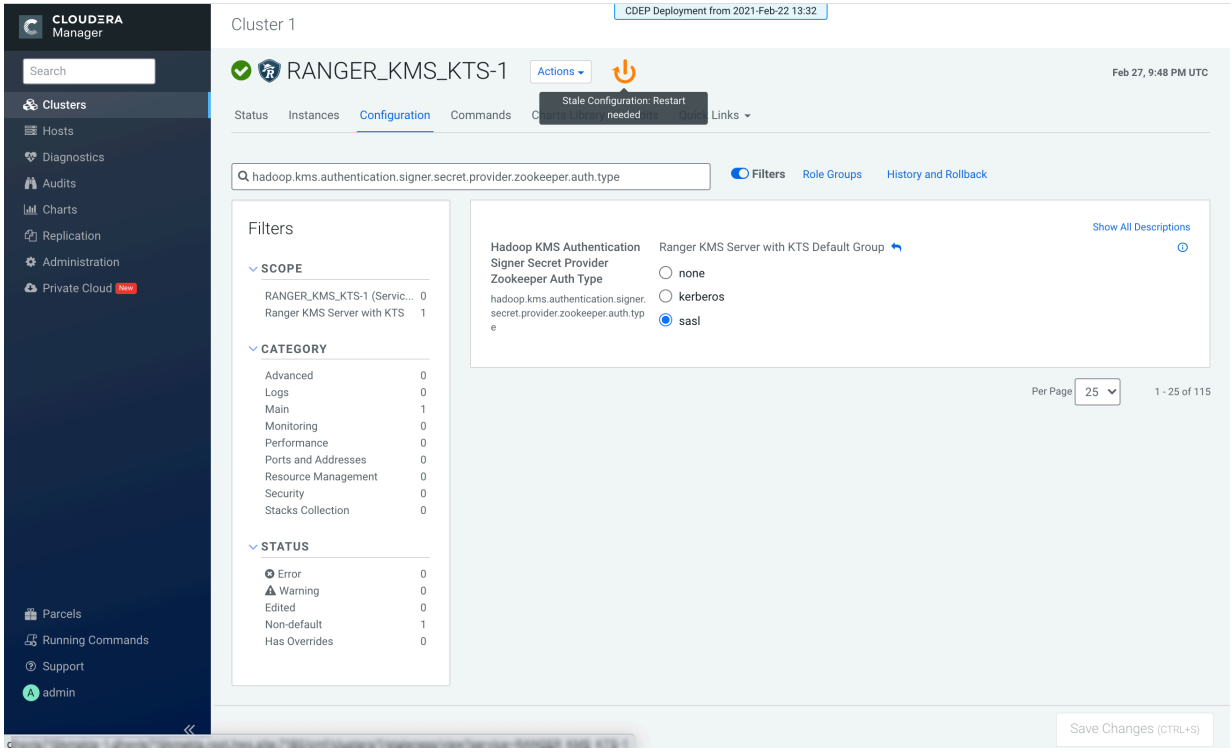


12. Update the following Ranger KMS configuration properties, then click Save Changes.

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



13. Click the Stale Configuration Restart icon.



14. On the Stale Configurations page, click Restart Stale Services.

15. On the Restart Stale Services page, select the Re-deploy client configuration checkbox, then click Restart Now.

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

Overriding custom keystore alias on a Ranger KMS Server

Use this procedure to override the custom keystore alias on a Ranger KMS server.

About this task

The custom keystore alias may need to be overridden in the following scenarios:

- User has manually enabled TLS/SSL during fresh installations of Ranger KMS and Ranger KMS with Key Trustee Server (KTS), and the keystore alias was not added to the hostname.
- User has upgraded from CDP-DC 7.0.3 with Key Trustee KMS and Ranger to CDP-DC 7.1.1 (where Ranger KMS with KTS is added during the upgrade) in a TLS/SSL environment in which TLS/SSL was manually enabled, and the keystore alias was not added to the hostname.

Overriding custom keystore alias while configuring TLS/SSL on a single instance of Ranger KMS Server

Procedure

1. In Cloudera Manager, select Ranger KMS > Configuration and use the Add (+) icon for the Ranger KMS Service Advanced Configuration Snippet (Safety valve) for conf/ranger-kms-site.xml property to add the following property:

   ```
   ranger.service.https.attrib.keystore.keyalias = <expected alias>
   ```

2. Click Save Changes.
3. Restart the Ranger KMS service.

Overriding custom keystore alias while configuring TLS/SSL on multiple instances of Ranger KMS Server

Procedure

1. In Cloudera Manager, select Ranger KMS > Instances and select Ranger KMS Server role > Configuration. Use the Add (+) icons for the Ranger KMS Server Advanced Configuration Snippet (Safety valve) for conf/ranger-kms-site.xml property to add the following property:

   ```
   ranger.service.https.attrib.keystore.keyalias = <expected alias>
   ```

   This overrides the configuration on the host on which the current Ranger KMS Server role is available.
2. Repeat Step 1 for all the other Ranger KMS Servers to override the configuration by using the Ranger KMS Server Advanced Configuration Snippet (Safety valve) for conf/ranger-kms-site.xml property.
3. Restart the Ranger KMS service.

Note: When high-availability has been enabled for Ranger KMS, the keystore may not have the same alias for different KMS instances. In such cases, use FQDN as the alias or add the custom key alias configuration in the Ranger KMS Server Advanced Configuration Snippet (Safety valve) for conf/ranger-kms-site.xml property of each host.