Cloudera Runtime 7.3.1

Configuring Advanced Security Options for Apache Ranger

Date published: 2020-07-28
Date modified: 2024-12-10

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 the server work directory path for a Ranger service..... 5

Configuring session inactivity timeout for Ranger Admin Web UI..... 6
Configuring http session timeout value for Tomcat server..... 7

Configure Kerberos authentication for Apache Ranger..... 7

Configure TLS/SSL encryption manually for Apache Ranger..... 8

Configure TLS/SSL encryption manually for Ranger KMS..... 9

Configure TLS/SSL encryption manually for Ranger RMS..... 10

Configuring Apache Ranger High Availability..... 11
Configure Ranger Admin High Availability..... 12
Configure Ranger Admin High Availability with a Load Balancer..... 16
Configuring Ranger Usersync and Tagsync High Availability..... 24
Migrating Ranger Usersync and Tagsync role groups..... 26

Configuring JVM options and system properties for Ranger services..... 28

How to pass JVM options to Ranger KMS services..... 30
Recommended : Using the Ranger KMS Client Java Opts field..... 30
Ranger KMS Service Environment Advanced Configuration Snippet..... 31

How to clear Ranger Admin access logs..... 32

Configuring purge of x_auth_sess data..... 33

Enable Ranger Admin login using kerberos authentication..... 34

How to configure Ranger HDFS plugin configs per (NameNode) Role Group..... 35

How to add a coarse URI check for Hive agent..... 36

How to suppress database connection notifications..... 36

How to change the password for Ranger users..... 37

Configuring the server work directory path for a Ranger service

A Ranger Administrator user can configure the server work directory path.

About this task

In versions prior to 7.1.7 (SP1) the server work directory path was hard-coded. A Ranger Admin user can now configure the Tomcat server directory for Ranger Admin, Ranger KMS, Ranger RMS and Ranger RAZ.

Procedure

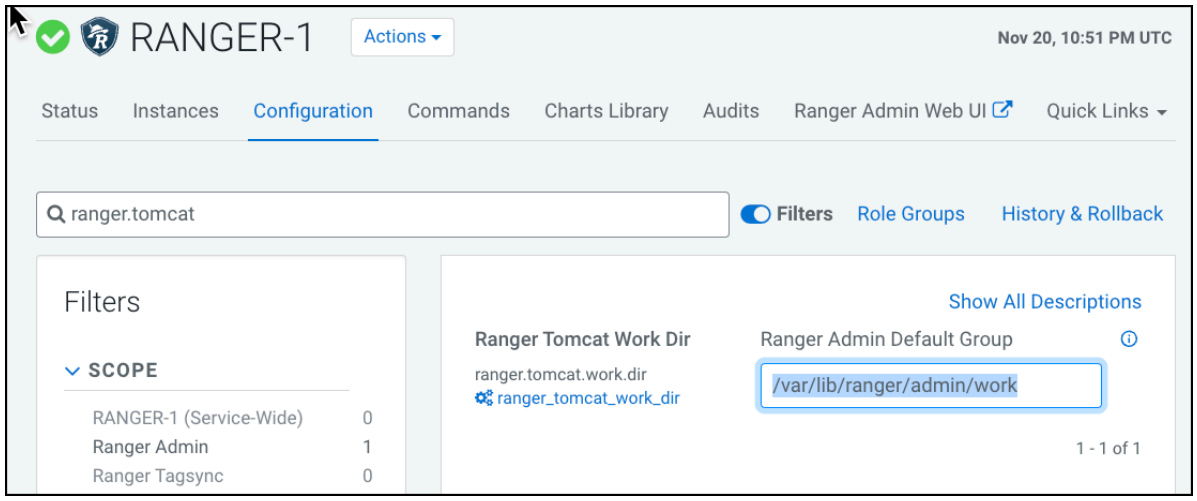
1. From Cloudera Manager <Service_Name> Configuration .
2. In Search, type <service_string>.tomcat.work.dir .
   This is the Ranger Service Work Directory name.

   Table 1: Ranger Service Work Directory Names

Ranger Service	Work Directory Name
Ranger Admin, KMS	ranger.tomcat.work.dir
Ranger RMS	ranger-rms.tomcat.work.dir
Ranger Raz	ranger.raz.tomcat.work.dir

3. Edit the path variable displayed for the Server Default Group.
4. Click Save Changes (CTRL+S).
5. Restart the Ranger service.
   For Ranger Admin and Ranger KMS:
   a) Go to Cloudera Manager Ranger Configuration .
   b) In Search, type ranger.tomcat.work.dir .
   c) In Ranger Admin Default Group, replace /var/lib/ranger/admin/work with a custom path.

   Figure 1: Editing the Ranger Admin Tomcat Server Work Directory Path



   d) Save Changes (CTRL+S).
   e) Restart the Ranger service.

Configuring session inactivity timeout for Ranger Admin Web UI

How to set a session inactivity timeout value for the Ranger Admin Web UI.

About this task

Ranger supports session inactivity timeout for the Ranger Admin web UI. User activity is monitored when a user logs in to the Ranger Admin web UI. If no user activity occurs during the set time period, Ranger Web UI prompts the user to either stay logged in or log out.

If the user chooses Stay Logged In, Ranger continues to use the same browser session and the session inactivity monitor resets. If the user chooses either Logout or no option, the browser redirects the user to either the Knox logout page (for a public cloud deployment) or the Ranger login page (for users who logged in to Ranger directly without using a Knox proxy).

ranger.service.inactivity.timeout has the value -1 second by default, which disables the session inactivity timeout.

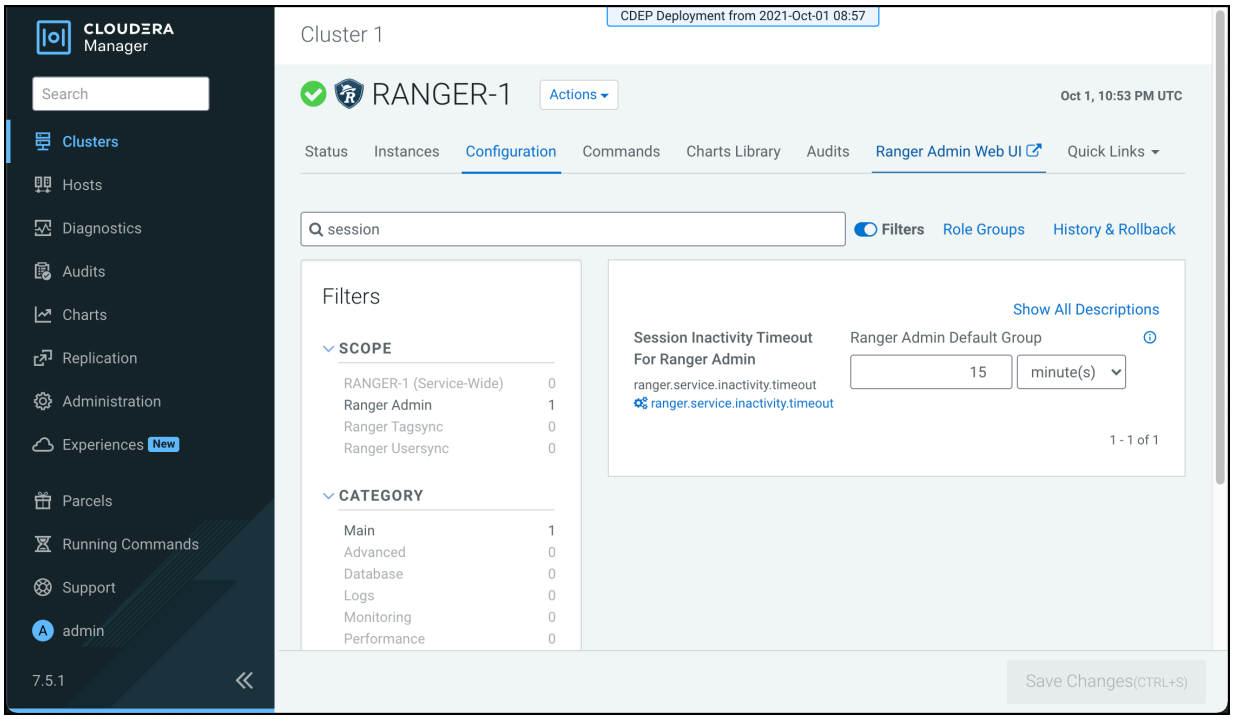
Note: Cloudera Manager also hides the Tomcat server timeout configuration by default. Refer to the instructions at the bottom of this page for those configuration details.

To enable session inactivity timeout and set a timeout value:

Procedure

1. In Cloudera Manager Ranger Configuration Search , type session.
2. In Session Inactivity Timeout for Ranger Admin: set a positive, integer value for the ranger.service.inactivity.timeout property, then choose a time unit.

   For example, setting ranger.service.inactivity.timeout to 30 seconds triggers the logout prompt after 30 seconds of inactivity in the Ranger Web UI. Choosing 30 days allows a month of inactivity before a logout prompt displays.



3. Click Save Changes (CTRL+S).

4. Choose Actions Restart to refresh session inactivity timeout configuration settings.

Configuring http session timeout value for Tomcat server

How to set a session timeout value for the UI and API requests from Ranger Admin Web UI's Tomcat server.

About this task

Ranger allows you to configure an http session timeout value for the UI and API requests from Ranger Admin Web UI's Tomcat server. This configuration ends the admin user's browser session after a specified duration. To set this configuration, use the command line editor to modify the session-timeout parameter in /web.xml.

Procedure

1. Login to your Ranger-Admin host.
2. Enter /opt/cloudera/parcels/CDH-[version]/lib/ranger-admin/ews/webapp/WEB-INF/ in the command line editor.
3. Backup the web.xml file in a safe place before making any changes.
4. Edit the web.xml file as follows:
   #vim web.xml
   a. Locate the value session-timeout = 60.
   b. Change this number to your desired value, in seconds. For example, setting session-timeout = 300seconds sets the session to end after 5 minutes.
5. Save the changes to the web.xml file.
6. Restart Ranger Service to refresh .

Configure Kerberos authentication for Apache Ranger

How to configure Kerberos Authentication for Apache Ranger

About this task

Kerberos authentication for Apache Ranger is automatically configured when HDFS Kerberos authentication is configured in Cloudera Manager (typically using the Cloudera Manager Kerberos Wizard). In this way, the actions that Ranger authorizes are sure to be requested by authenticated users.

Specifically, Ranger depends on the HDFS hadoop.security.authentication property to enable or disable Kerberos authentication. When the hadoop.security.authentication property is updated, the Ranger service gets a restart indicator for the core-site.xml file that resides inside the Ranger service conf directory generated by Cloudera Manager.

Important: Authorization through Apache Ranger is just one element of a secure production cluster: Cloudera supports Ranger only when it runs on a cluster where Kerberos is enabled to authenticate users.

Ranger Kerberos authentication is automatically enabled when HDFS Kerberos authentication is enabled.

To enable Kerberos Authentication for CDP, read the related information.

Related Information

Enabling Kerberos Authentication for CDP

Configure TLS/SSL encryption manually for Apache Ranger

How to manually configure TLS/SSL encryption for Apache Ranger

About this task

Use this procedure when you want to manage your TLS/SSL certificates manually.

Procedure

1. In Cloudera Manager, select Ranger, then click the Configuration tab.
2. Under Category, select Security.
3. Set the following properties:

Note: Ranger supports the following keystore formats:

- JKS
- BCFKS in a FIPS-enabled cluster.

Table 2: Apache Ranger TLS/SSL Settings

Configuration Property	Description
Enable TLS/SSL for Ranger Admin ranger.service.https.attrib.ssl.enabled	Select this option to encrypt communication between clients and Ranger Admin using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Ranger Admin TLS/SSL Server JKS Keystore File Location ranger.https.attrib.keystore.file	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger Admin is acting as a TLS/SSL server. The keystore must be in JKS or BCFKS format.
Ranger Admin TLS/SSL Server JKS Keystore File Password ranger.service.https.attrib.keystore.pass	The password for the Ranger Admin JKS keystore file.
Ranger Admin TLS/SSL Client Trust Store File ranger.truststore.file	The location on disk of the truststore used to confirm the authenticity of TLS/SSL servers that Ranger Admin might connect to. This is used when Ranger Admin is the client in a TLS/SSL connection. This truststore must contain the certificate(s) used to sign the connected service(s). If this parameter is not provided, the default list of known certificate authorities is used.
Ranger Admin TLS/SSL Client Trust Store Password ranger.truststore.password	The password for the Ranger Admin TLS/SSL Certificate truststore file. This password is not required to access the truststore; therefore, this field is optional. The contents of truststores are certificates, and certificates are public information. This password provides optional integrity checking of the file.
Enable TLS/SSL for Ranger Tagsync	Select this option to encrypt communication between clients and Ranger Tagsync using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Ranger Tagsync TLS/SSL Server JKS Keystore File Location xasecure.policymgr.clientssl.keystore	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger Tagsync is acting as a TLS/SSL server. The keystore must be in JKS or BCFKS format.
Ranger Tagsync TLS/SSL Server JKS Keystore File Password xasecure.policymgr.clientssl.keystore.password	The password for the Ranger Tagsync JKS keystore file.

Configuration Property	Description
Ranger Tagsync TLS/SSL Trust Store File xasecure.policymgr.clientssl.truststore	The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger Tagsync might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. Ranger Tagsync connects to Ranger Admin. If Ranger Admin is SSL enabled, make sure you add a Ranger Admin certificate in the trust store. If this parameter is not provided, the default list of well-known certificate authorities is used instead.
Ranger Tagsync TLS/SSL Client Trust Store Password xasecure.policymgr.clientssl.truststore.password	The password for the Ranger Tagsync TLS/SSL Certificate truststore file. This password is not mandatory to access the truststore. It is used to check the integrity of the file; this field is optional. The contents of truststores are certificates, and certificates are public information.
Ranger Usersync TLS/SSL Client Trust Store File ranger.usersync.truststore.file	The location on disk of the truststore, in JKS format, used to confirm the authenticity of TLS/SSL servers that Ranger Usersync might connect to. This is used when Ranger Usersync is the client in a TLS/SSL connection. This truststore must contain the certificate(s) used to sign the connected service(s). Ranger Usersync connects to Ranger Admin to sync users into Ranger. If Ranger Admin is SSL enabled, make sure you add a Ranger Admin certificate in the trust store. If this parameter is not provided, the default list of known certificate authorities is used.
Ranger Usersync TLS/SSL Client Trust Store Password ranger.usersync.truststore.password	The password for the Ranger Usersync TLS/SSL certificate truststore file. This password is not required to access the truststore; this field is optional. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

4. In Filters Search , type ranger.service.https.attrib.keystore.keyalias to set the Ranger Admin TLS/SSL Keystore File Alias property.

Table 3: Ranger Admin TLS/SSL Setting

Configuration Property	Description
Ranger Admin TLS/SSL Keystore File Alias ranger.service.https.attrib.keystore.keyalias	The alias used for the Ranger Admin TLS/SSL keystore file. If host FQDN is used as an alias while creating a keystore file, the default placeholder value {{RANGER_ADMIN_HOST}} is replaced with the host FQDN where Ranger Admin will be installed in the current cluster. The placeholder can be replaced to have a custom alias used while creating the keystore file. If using a custom alias which is the same as the host short name, use {{RANGER_ADMIN_HOST_UQDN}} placeholder as a value.

5. Click Save Changes.

Configure TLS/SSL encryption manually for Ranger KMS

How to manually configure TLS/SSL encryption for Ranger KMS

About this task

Procedure

1. In Cloudera Manager, select Ranger KMS, then click the Configuration tab.
2. Under Category, select Security.
3. Set the following properties:

Table 4: Ranger KMS TLS/SSL Settings

Configuration Property	Description
Enable TLS/SSL for Ranger KMS Server ranger.service.https.attrib.ssl.enabled	Encrypt communication between clients and Ranger KMS Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Ranger KMS Server TLS/SSL Server JKS Keystore File Location ranger.service.https.attrib.keystore.file	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger KMS Server is acting as a TLS/SSL server. The keystore must be in JKS format.
Ranger KMS Server TLS/SSL Server JKS Keystore File Password ranger.service.https.attrib.keystore.pass	The password for the Ranger KMS Server JKS keystore file.
Ranger KMS Server TLS/SSL Trust Store File xasecure.policymgr.clientssl.truststore	The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger KMS Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. The Ranger KMS plugin inside the Ranger KMS Server connects to Ranger Admin to download the authorization policies. If Ranger Admin is SSL enabled, make sure you add a Ranger Admin certificate in the trust store. If this parameter is not provided, the default list of well-known certificate authorities is used instead.
Ranger KMS Server TLS/SSL Trust Store Password xasecure.policymgr.clientssl.truststore.password	The password for the Ranger KMS Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

4. In Filters Search , type ranger.service.https.attrib.keystore.keyalias to set the Ranger KMS Server TLS/SSL Keystore File Alias property.

Table 5: Ranger KMS Server TLS/SSL Keystore Alias Property Settings

Configuration Property	Description
Ranger KMS Server TLS/SSL Keystore File Alias ranger.service.https.attrib.keystore.keyalias	The alias for the Ranger KMS Server TLS/SSL keystore file. If host FQDN is used as an alias while creating a keystore file, the {{HOST}} default placeholder value will be replaced with the host FQDN where Ranger KMS Server will be installed in the current cluster. The placeholder can be replaced to have a custom alias used while creating the keystore file. If using a custom alias which is the same as host short name then use {{HOST_UQDN}} placeholder as a value.

5. Click Save Changes.

Configure TLS/SSL encryption manually for Ranger RMS

How to manually configure TLS/SSL encryption for Ranger RMS

About this task

Procedure

1. In Cloudera Manager, select Ranger KMS, then click the Configuration tab.
2. Under Category, select Security.
3. Set the following properties:

Table 6: Ranger RMS TLS/SSL Settings

Configuration Property	Description
Enable TLS/SSL for Ranger RMS Server ranger-rms.service.https.attrib.ssl.enabled	Encrypt communication between clients and Ranger RMS Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Ranger RMS Server TLS/SSL Server JKS Keystore File Location ranger-rms.service.https.attrib.keystore.file	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger RMS Server is acting as a TLS/SSL server. The keystore must be in JKS format.
Ranger RMS Server TLS/SSL Server JKS Keystore File Password ranger-rms.service.https.attrib.keystore.pass	The password for the Ranger RMS Server JKS keystore file.
Ranger RMS Server TLS/SSL Trust Store File ranger-rms.truststore.file	The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger RMS Server might connect to. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.
Ranger RMS Server TLS/SSL Trust Store Password ranger-rms.truststore.password	The password for the Ranger RMS Server TLS/SSL Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.

4. In Filters Search , type ranger-rms.service.https.attrib.keystore.keyalias to set the Ranger RMS Server TLS/SSL Keystore File Alias property.

Table 7: Ranger RMS Server TLS/SSL Keystore File Alias Settings

Configuration Property	Description
Ranger RMS Server TLS/SSL Keystore File Alias ranger-rms.service.https.attrib.keystore.keyalias	The alias for the Ranger RMS Server TLS/SSL keystore file. If host FQDN is used as an alias while creating a keystore file, the {{HOST}} default placeholder value will be replaced with the host FQDN where Ranger RMS Server will be installed in the current cluster. The placeholder can be replaced to have a custom alias used while creating the keystore file. If using a custom alias which is the same as host short name then use {{HOST_UQDN}} placeholder as a value.

Configuring Apache Ranger High Availability

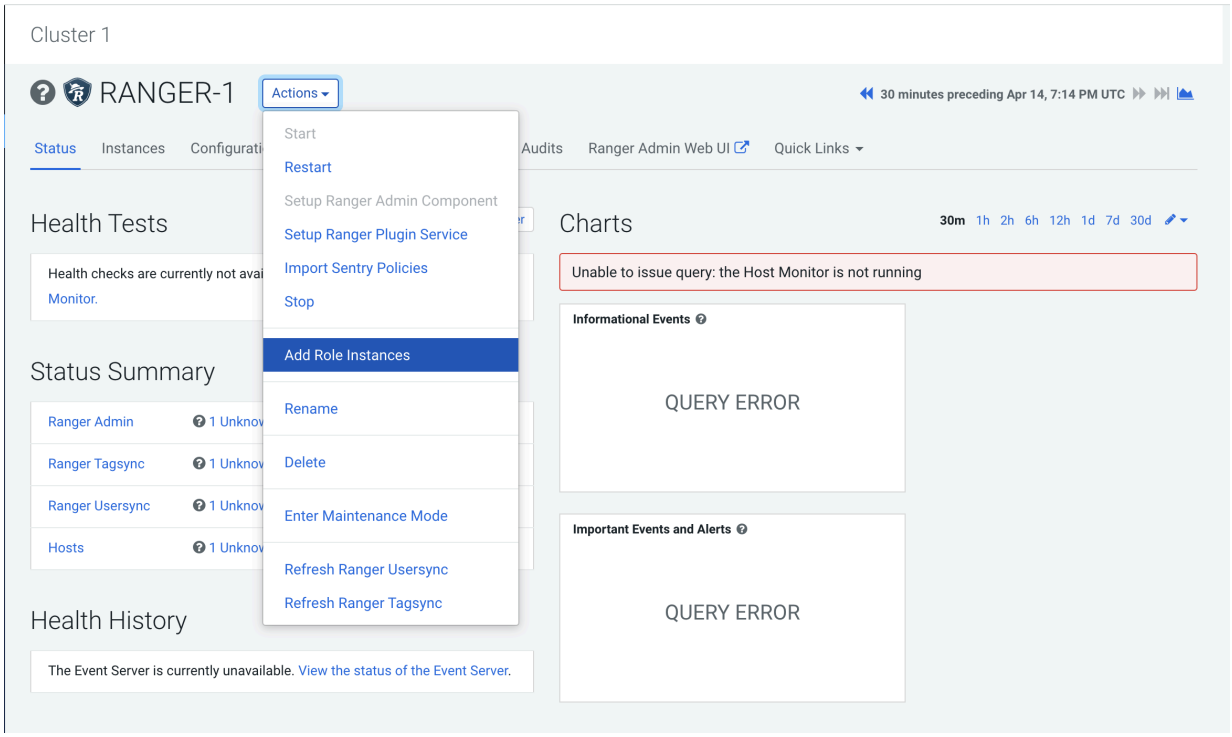
How to configure High Availability (HA) for Apache Ranger.

Configure Ranger Admin High Availability

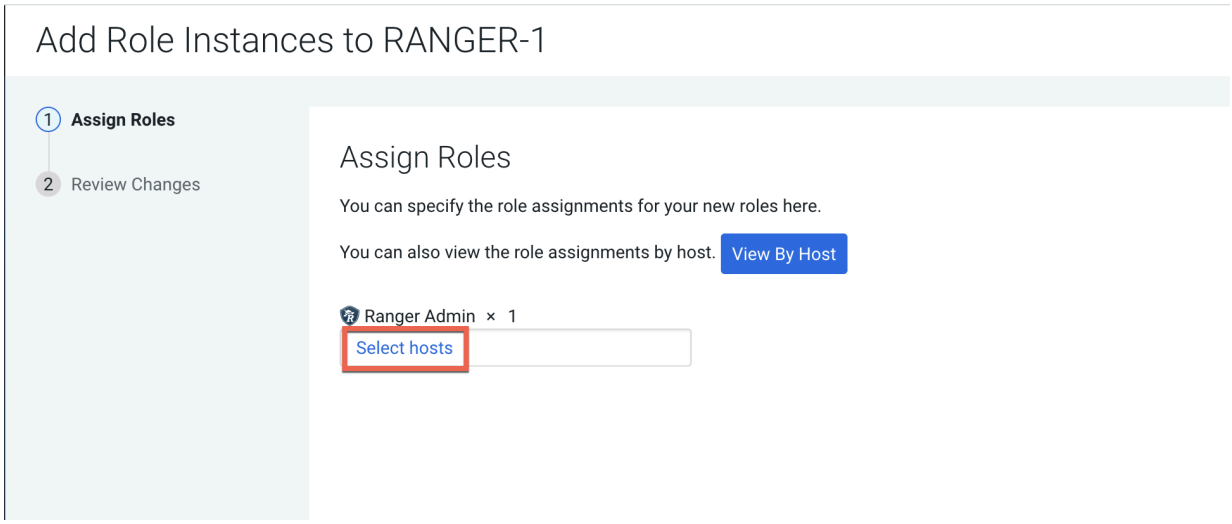
How to configure Ranger Admin High Availability (HA) by adding additional Ranger Admin role instances.

Procedure

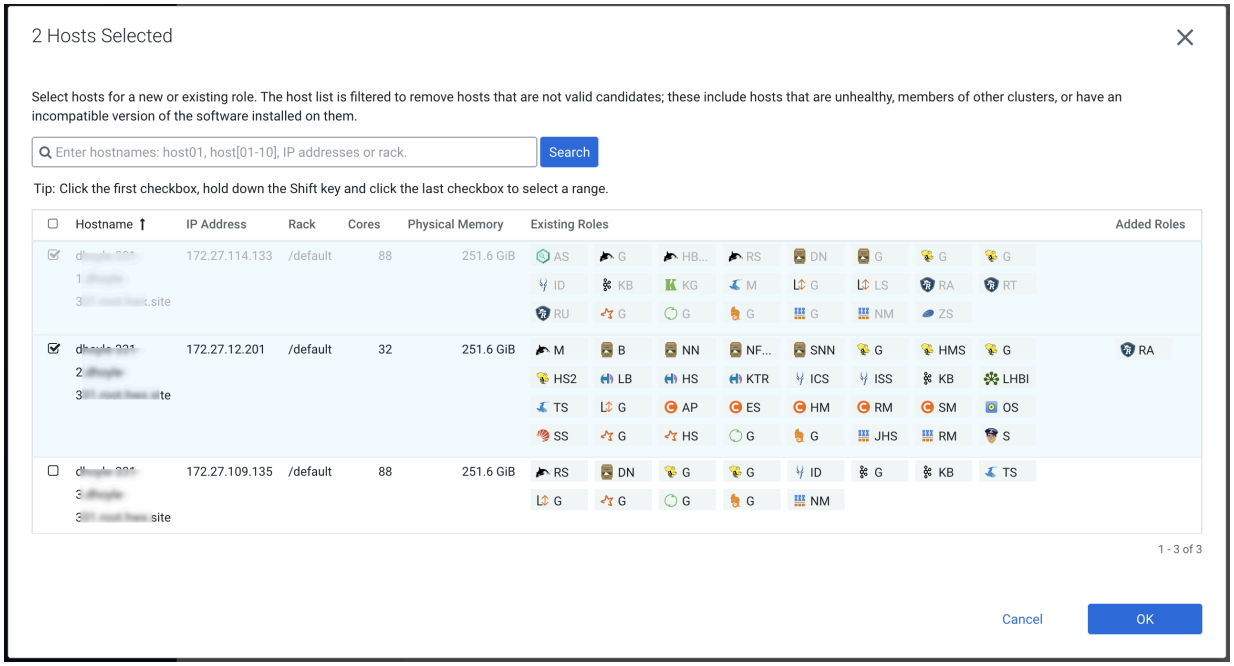
1. In Cloudera Manager, select Ranger Actions Add Role Instances .



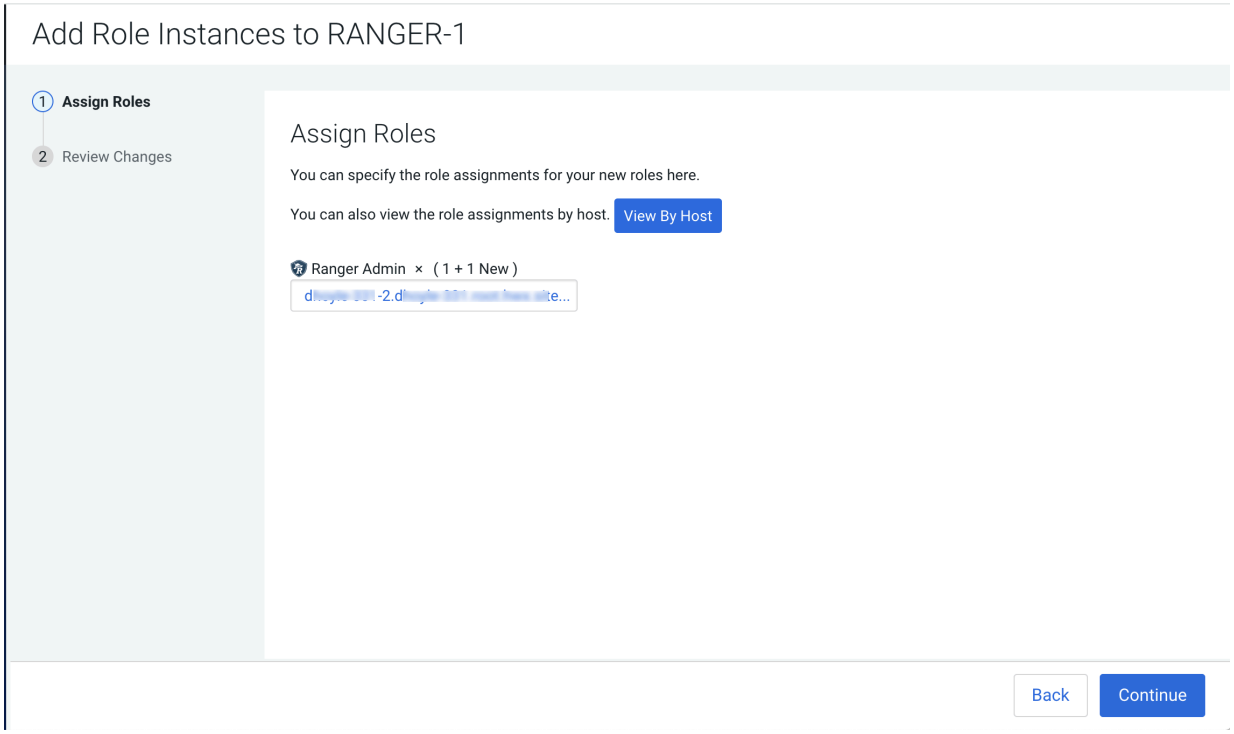
2. On **Add Role Instances**, click Select hosts.



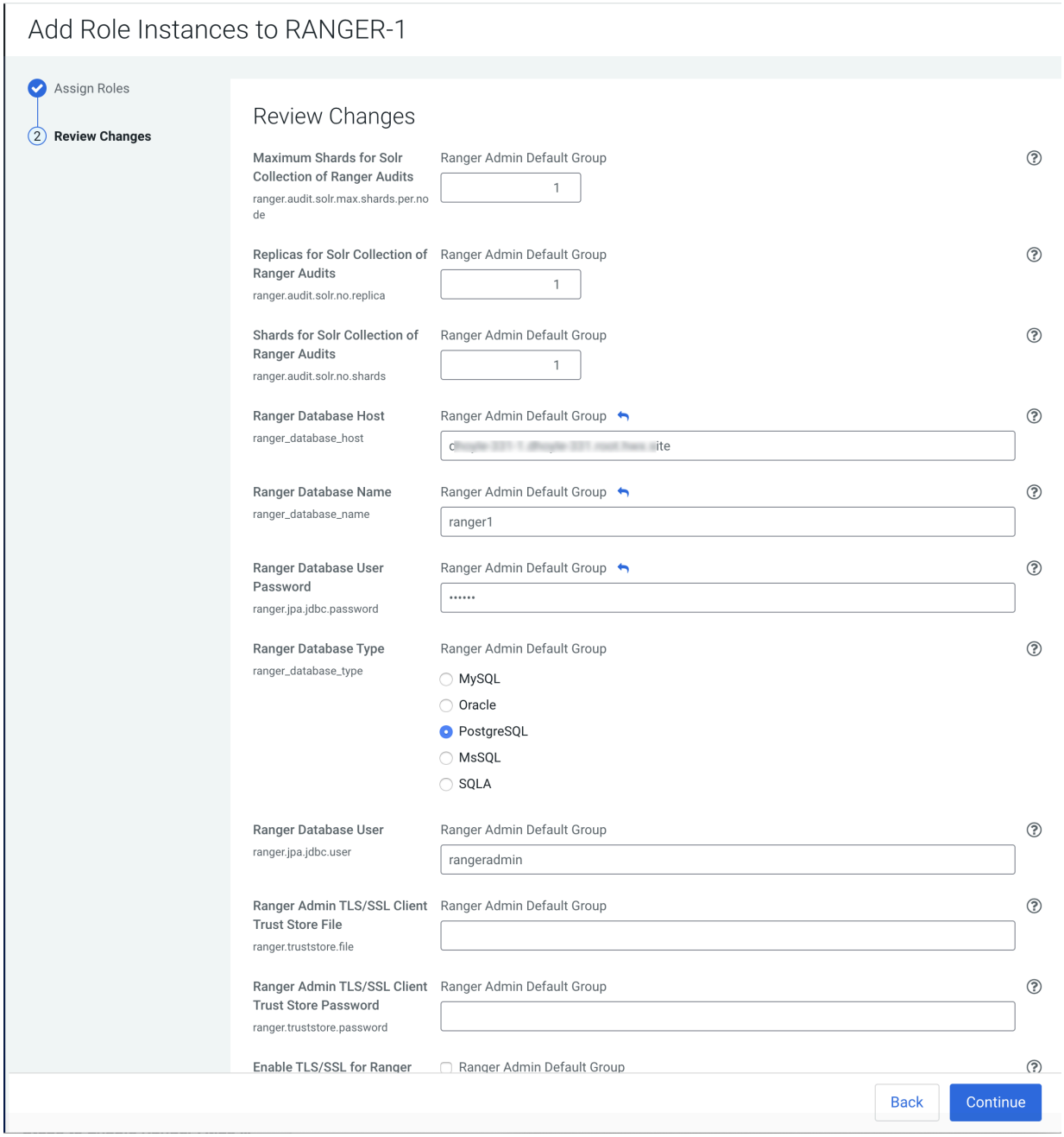
3. On **Hosts Selected**, the primary Ranger Admin host is selected by default. Select a backup Ranger host. A Ranger Admin (RA) icon appears in Added Roles for the selected backup host. Click OK to continue.



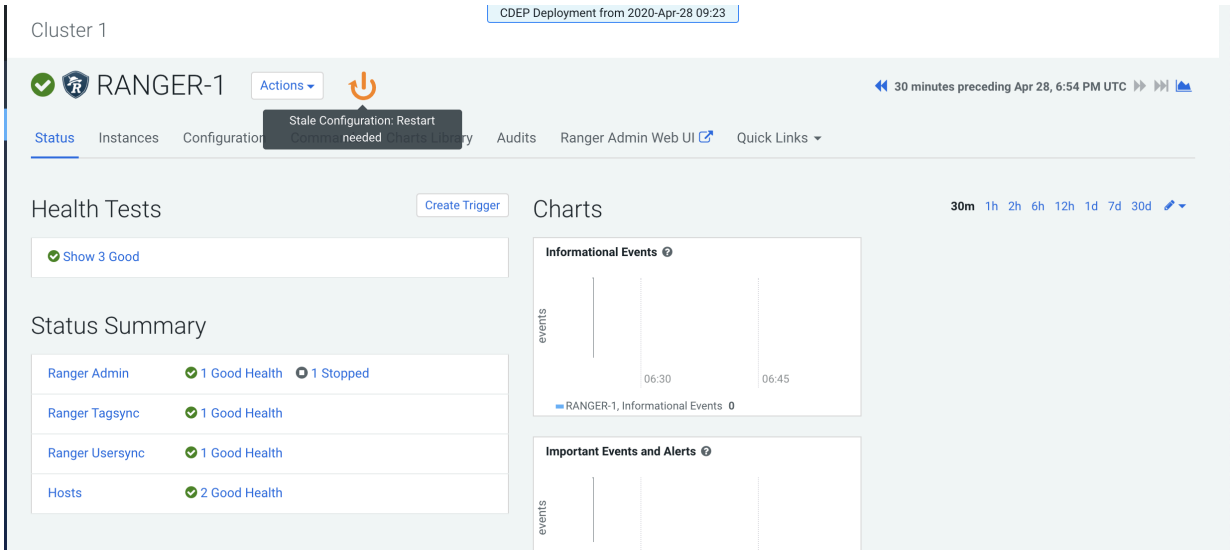
4. **Add Role Instances** refreshes, displaying the new backup host. Click Continue.



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



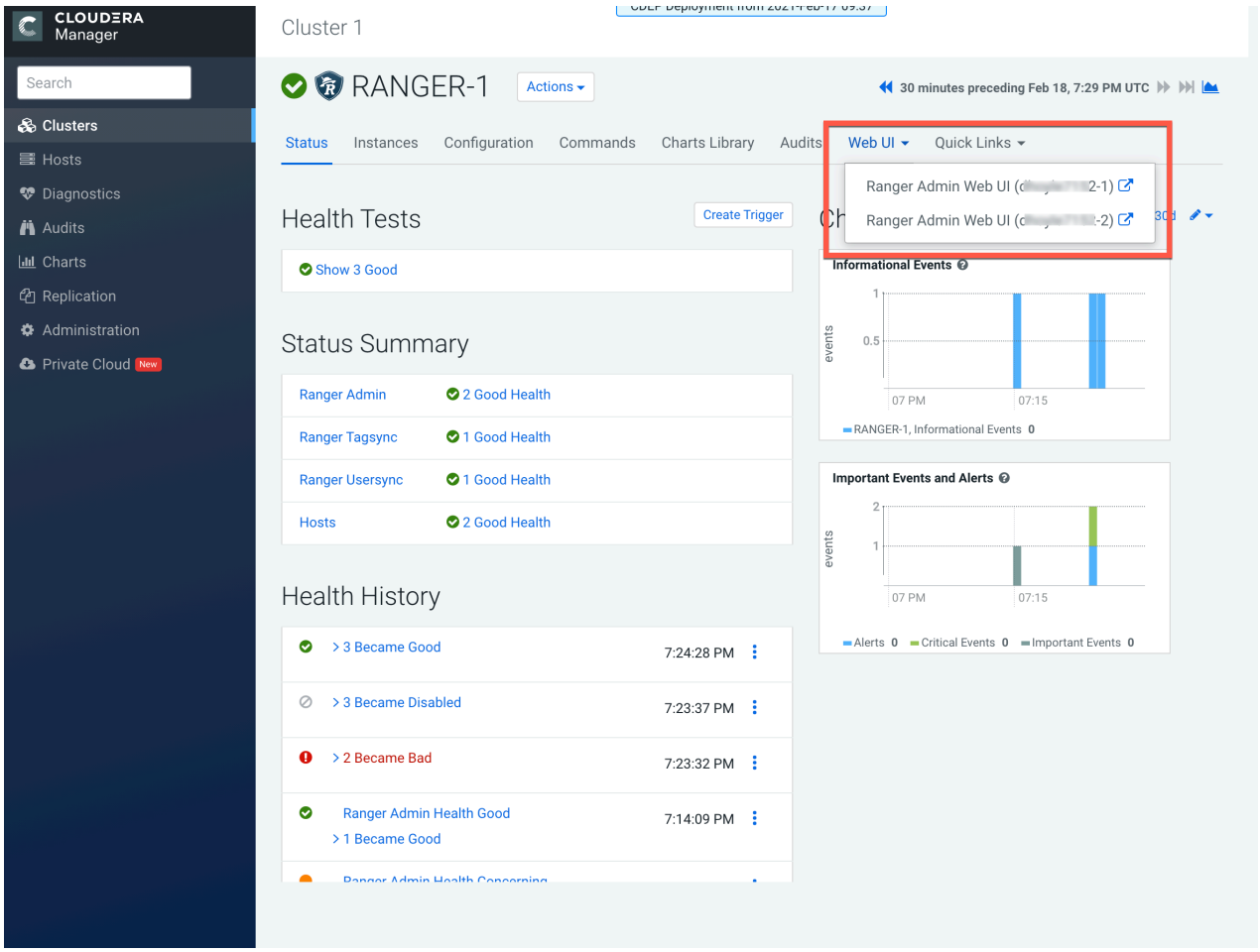
6. Restart the stale Ranger configuration, then click Finish.



Results

After restart you will see two URLs for the Ranger Admin Web UI.

- Requests are distributed to the multiple Ranger Admin instances in a round-robin fashion.
- If a connection is refused (indicating a failure), requests automatically reroute to the alternate Ranger Admin instance. However, you must manually switch to the alternate Ranger Admin Web UI.
- For all services that have the Ranger plugin enabled, the value of the ranger.plugin.<service>.policy.rest.url property changes to http://<RANGER-ADMIN-1>:6080,http://<RANGER-ADMIN-2>:6080.



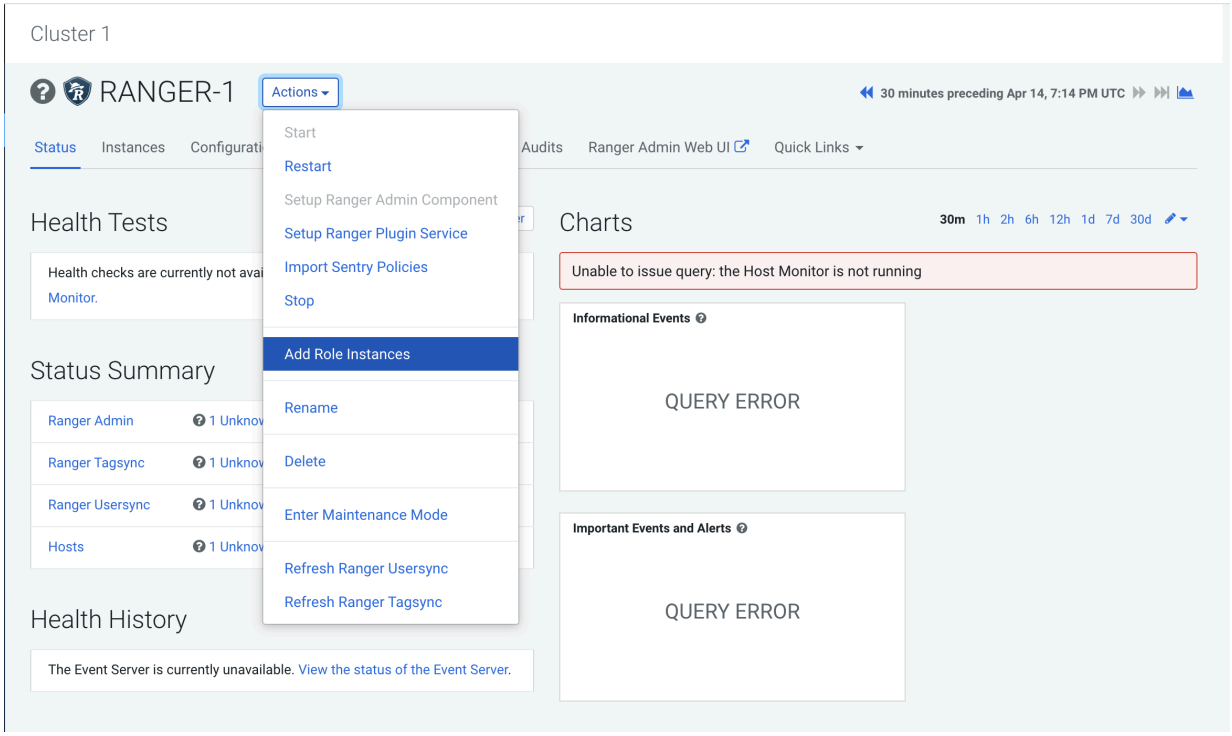
Configure Ranger Admin High Availability with a Load Balancer

For clusters that have multiple users and production availability requirements, you may want to configure Ranger high availability (HA) with a load-balancing proxy server to relay requests to and from Ranger.

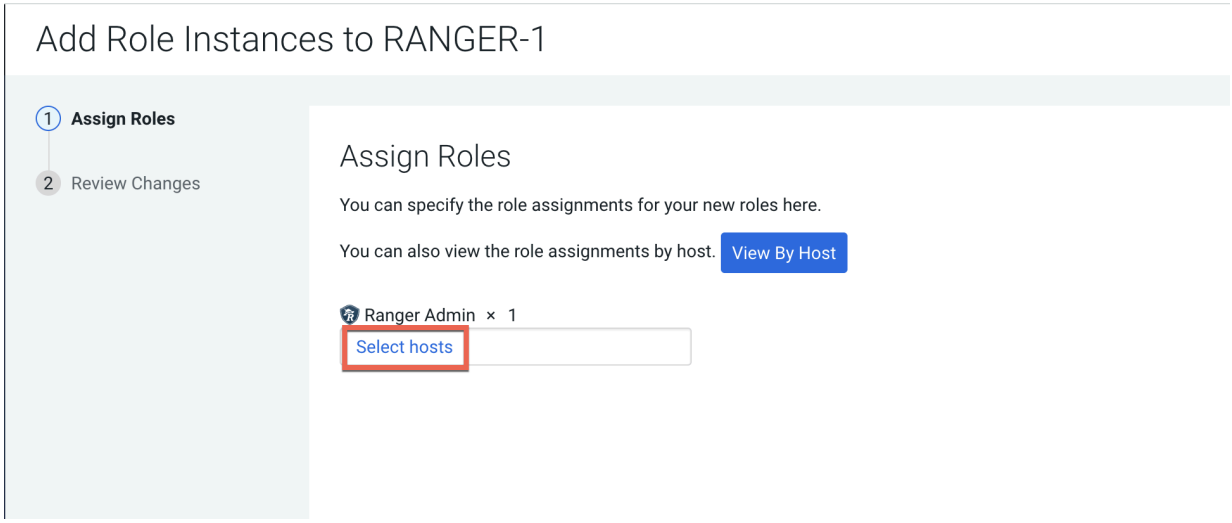
Procedure

1. Configure an external load balancer to use with Ranger HA.

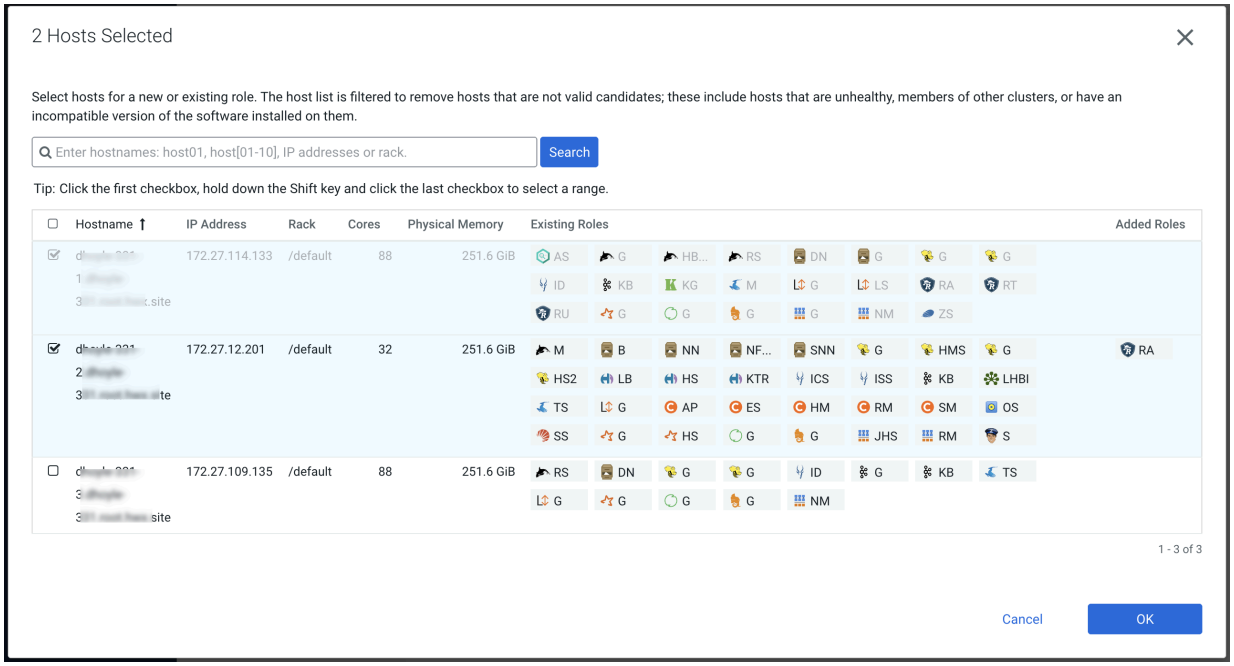
2. In Cloudera Manager, select Ranger Actions Add Role Instances .



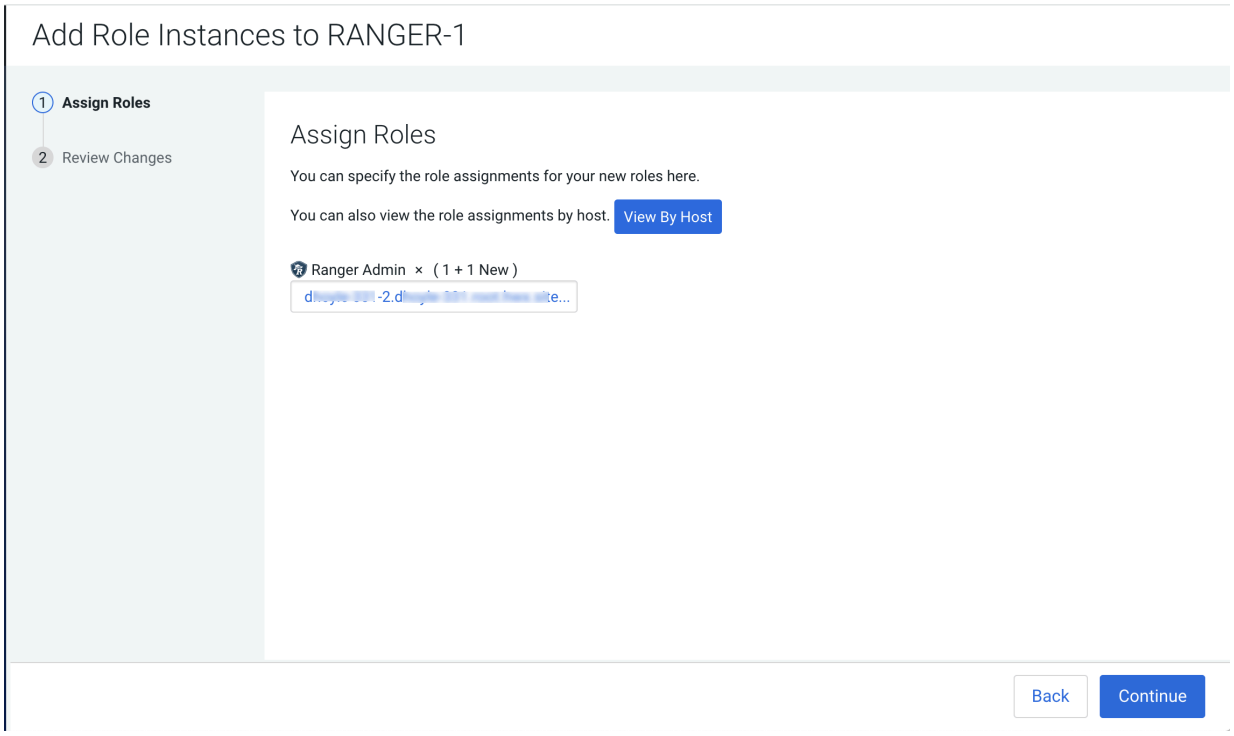
3. On **Add Role Instances**, click Select hosts.



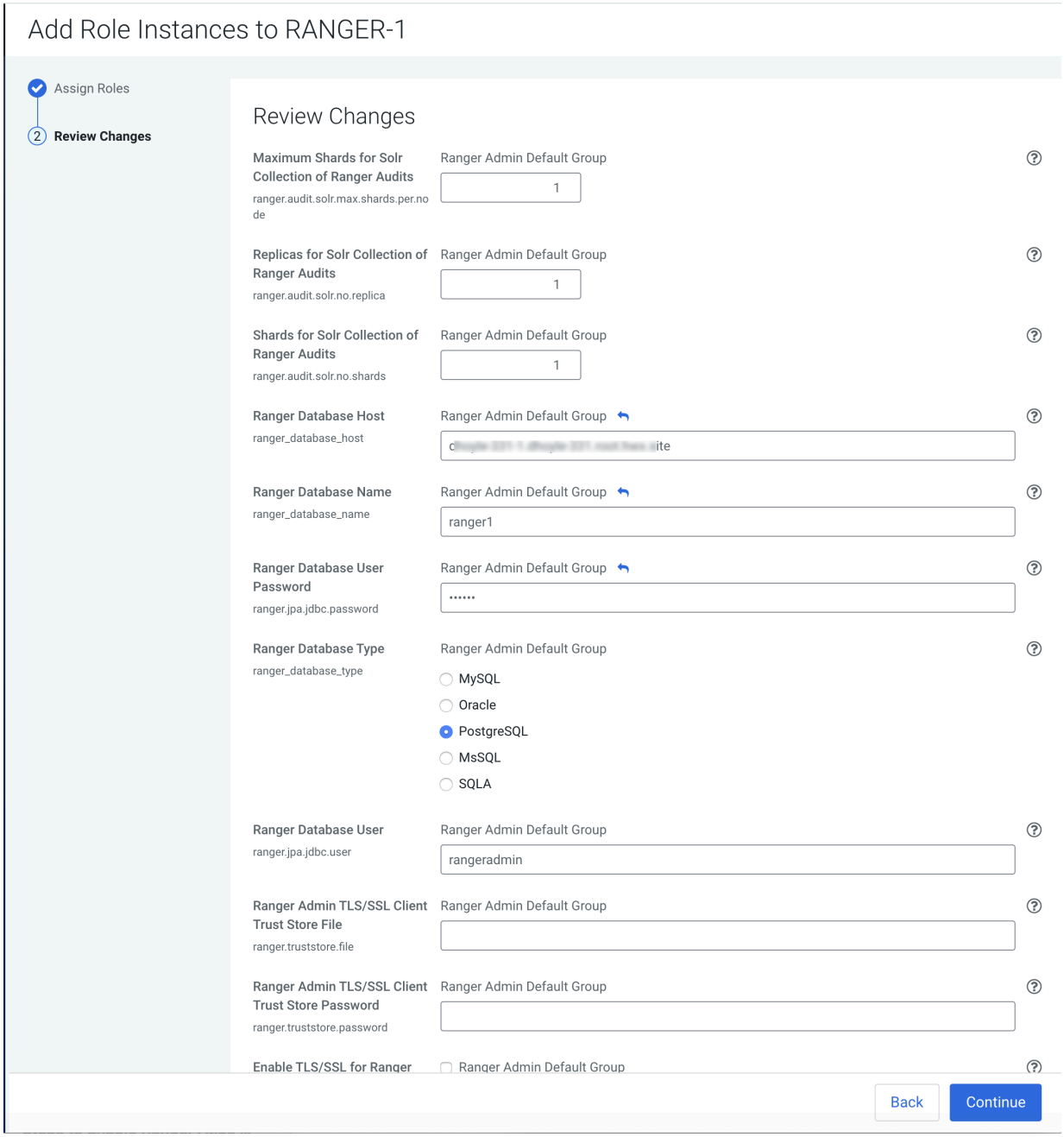
4. On **Hosts Selected**, the primary Ranger Admin host is selected by default. Select your configured backup Ranger host (ranger-host2-fqdn). A Ranger Admin (RA) icon appears in Added Roles for the selected backup host. Click OK to continue.



5. **Add Role Instances** refreshes, displaying the new backup host. Click Continue.

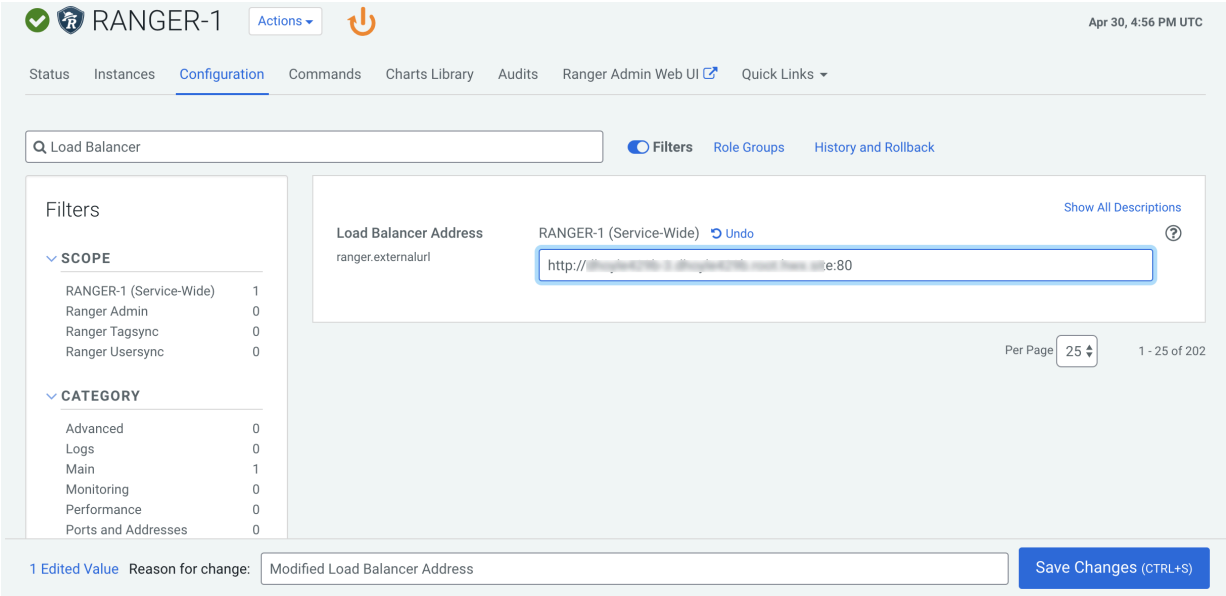


6. Review the settings on the Review Changes page, then click Continue.



7. Update the Ranger Load Balancer Address property (ranger.externalurl) with the load balancer host URL and port, then click Save Changes.

   Note: Do not use a trailing slash in the the load balancer host URL when updating the Ranger Load Balancer Address property.



8. Verify the load balancer principal is generated by CM. In Cloudera Manager Administration Security Kerberos credentials , search for the load balancer hostname. You should be able to search the principal in the format : HTTP/<loadbalancer-hostname>@EXAMPLE.COM. If the load balancer principal hostname entry is not

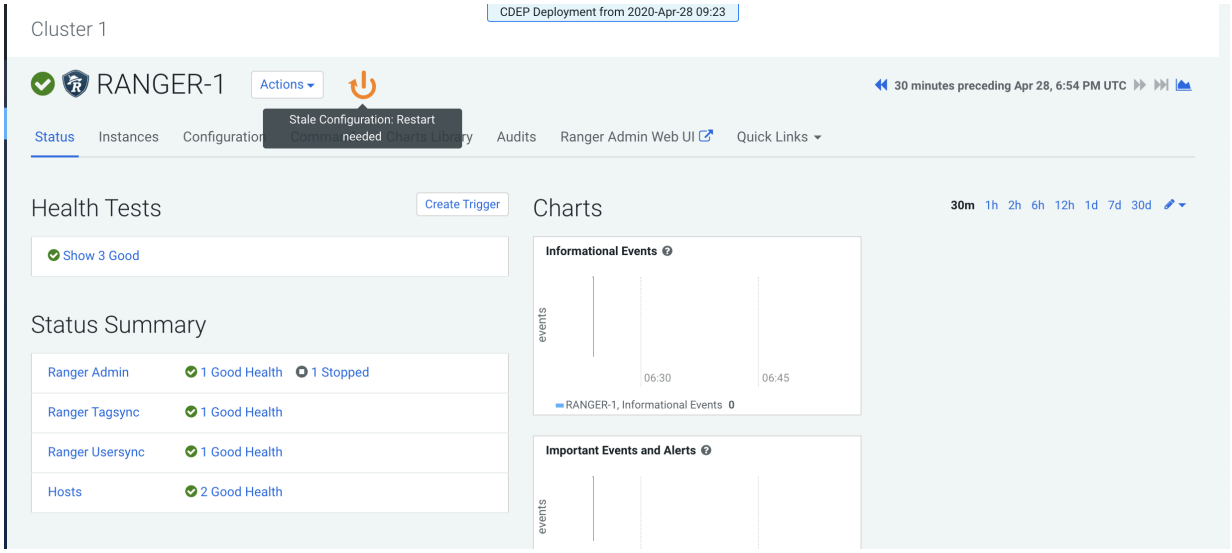
available, click Generate Missing Credentials on the same page and then search for the principal. After the load balancer principal is created by CM, restart the Ranger service after staleness.

Note: If load balancer principal hostname is not showing even after generating missing credentials, use the following manual steps to create composite keytab.

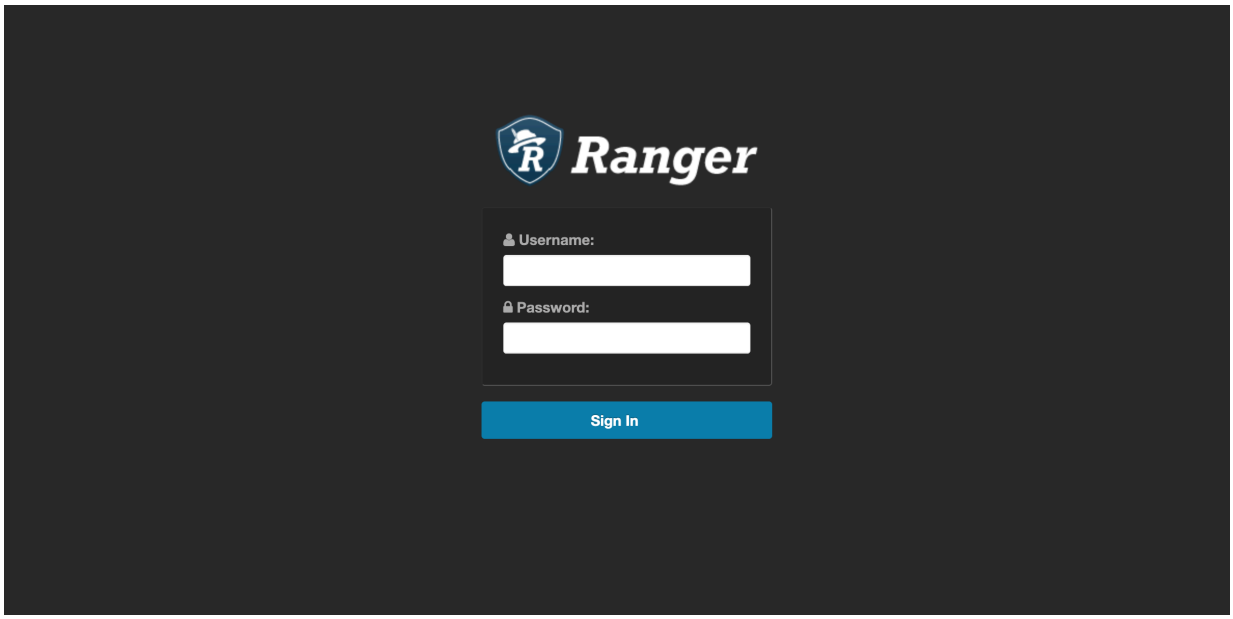
```
Manual Steps for creating a composite keytab:
1. If Kerberos is configured on your cluster, use SSH to connect to
 the KDC server host.
   Use the kadmin.local command to access the Kerberos CLI, then chec
k the list of principals
   for each domain where Ranger Admin and the load-balancer are ins
talled.
   Note: This step assumes you are using an MIT KDC (and kadmin.loc
al). This step will be different if you are using AD or IPA.

   kadmin.local
   kadmin.local: list_principals

   For example, if Ranger Admin is installed on <host1> and <host2>,
 and the load-balancer is installed on <host3>,
   the list returned should include the following entries:
    HTTP/ <host3>@EXAMPLE.COM
    HTTP/ <host2>@EXAMPLE.COM
    HTTP/ <host1>@EXAMPLE.COM

   If the HTTP principal for any of these hosts is not listed, use
the following command to add the principal:
   kadmin.local: addprinc -randkey HTTP/<host3>@EXAMPLE.COM

   Note: This step will need to be performed each time the Spnego
keytab is regenerated.

2. If Kerberos is configured on your cluster, complete the following
 steps to create a composite keytab:
   Note: These steps assume you are using an MIT KDC (and kadmin.lo
cal).
         These steps will be different if you are using AD or IPA.

   a. SSH into the Ranger Admin host, then create a keytabs directory
.
      mkdir /etc/security/keytabs/

   b. Copy the ranger.keytab from the current running process.
      cp /var/run/cloudera-scm-agent/process/<current-ranger-proce
ss>/ranger.keytab /etc/security/keytabs/ranger.ha.keytab

   c. Run the following command to invoke kadmin.local.
      kadmin.local

   d. Run the following command to add the SPNEGO principal entry on
 the load balancer node.
      ktadd -norandkey -kt /etc/security/keytabs/ranger.ha.keytab
HTTP/load-balancer-host@EXAMPLE.COM

      Note: As shown above, the domain portion of the URL must be in
 capital letters.
            You can use list_principals * to view a list of all of t
he principals.
   e. Run the following command to add the SPNEGO principal entry on
 the node where the first Ranger Admin is installed.
      ktadd -norandkey -kt /etc/security/keytabs/ranger.ha.keytab
HTTP/ranger-admin-host1@EXAMPLE.COM

   f. Run the following command to add the SPNEGO principal entry on
 the node where the second Ranger Admin is installed.
```

```
      ktadd -norandkey -kt /etc/security/keytabs/ranger.ha.keytab
HTTP/ranger-admin-host2@EXAMPLE.COM

   g. Run the following command to exit kadmin.local.
      exit

   h. Run the following command to verify that the /etc/security/k
eytabs/ranger.ha.keytab file has entries for all required
      SPNEGO principals.
      klist -kt /etc/security/keytabs/ranger.ha.keytab

   i. On the backup (ranger-admin-host2) Ranger Admin node, run the
 following command to create a keytabs folder.
      mkdir /etc/security/keytabs/

   j. Copy the ranger.ha.keytab file from the primary Ranger Admin
 node (ranger-admin-host1) to the backup (ranger-admin-host2) Ranger
 Admin node.
      scp /etc/security/keytabs/ranger.ha.keytab root@ranger-host2-
fqdn:/etc/security/keytabs/ranger.ha.keytab

   k. Run the following commands on all of the Ranger Admin nodes.
      chmod 440 /etc/security/keytabs/ranger.ha.keytab
      chown ranger:hadoop /etc/security/keytabs/ranger.ha.keytab

3. Update the following ranger-admin-site.xml configuration settings
 using the Safety Valve.
   ranger.spnego.kerberos.keytab=/etc/security/keytabs/ranger.ha.ke
ytab
   ranger.spnego.kerberos.principal=*
```

9. Restart all other cluster services that require a restart, then click Finish.



10. Use a browser to check the load-balancer host URL (with port). You should see the Ranger Admin page.



Configuring Ranger Usersync and Tagsync High Availability

How to configure high availabilty of Ranger Usersync and Tagsync manually.

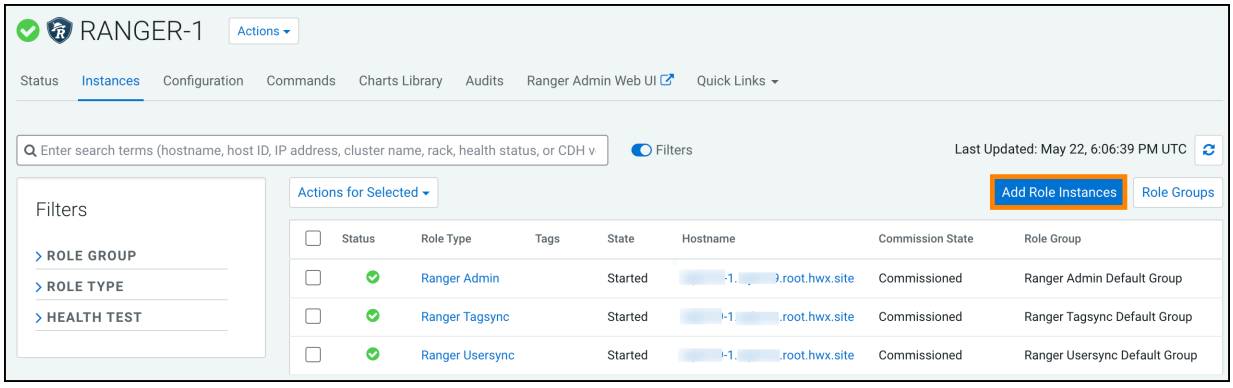
About this task

Ranger Usersync and Tagsync run on one host and belong to Ranger Usersync and Tagsync default groups by default. Configuring high availability adds another instance of each role to an additional host, which host continues to run the features if the default host fails.

Procedure

1. On Cloudera Manager Ranger Instances , select Add Role Instances, as shown.

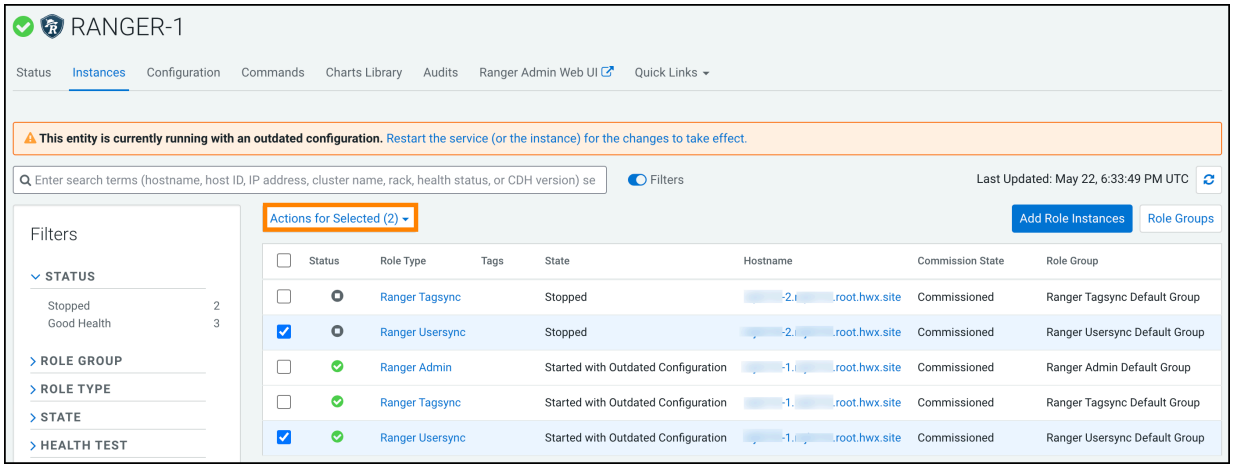
Figure 2: Adding UserSync and Tagsync role instances



2. Add Ranger Usersync and Tagsync roles to a new host, using Add Role Instance wizard.

3. Select the newly added roles along with the existing roles by checking the checkboxes.

Figure 3: Selecting a newly commissed Usersync role along with an existing one



Note: This example shows how to restart the newly added Usersync role only. You must also restart any stale configurations.

4. Verify that the port information for Usersync and Tagsync matches the following:
   a) Go to Cloudera Manager Ranger Configuration .

   Ranger Usersync HTTP port

   8280

   Ranger Usersync HTTPS port

   8283

   Ranger Tagsync HTTP port

   8180

   Ranger Tagsync HTTPS port

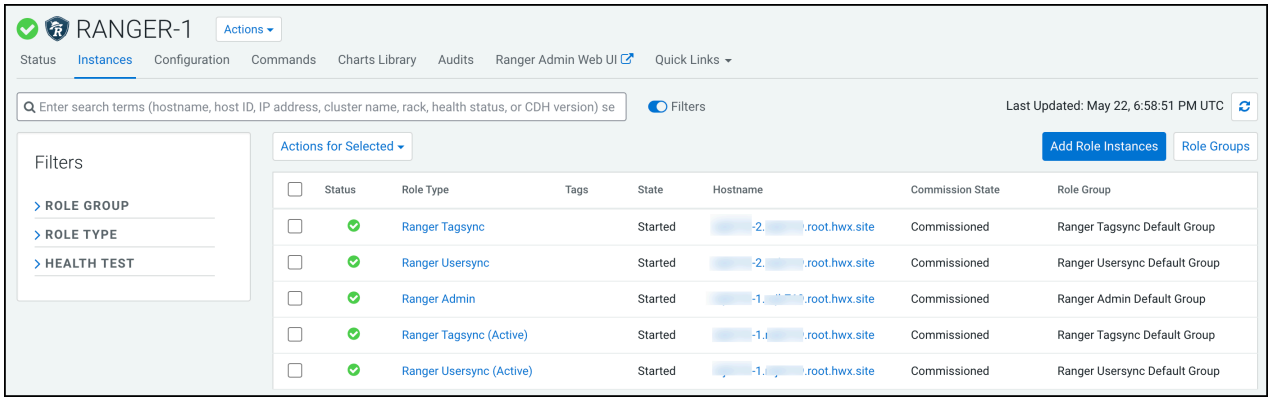
   8183

5. Select Actions for Selected Restart .

Results

- After successful restarts, Ranger Usersync and Ranger Tagsync run in High Availability mode.
- Active Ranger Usersync and Ranger Tagsync roles appear on Instances, as shown:

Figure 4: Usersync and Tagsync running in High Availability mode



Migrating Ranger Usersync and Tagsync role groups

You can use Host Templates to back up the existing usersync and tagsync role group configurations and migrate them to a new host.

About this task

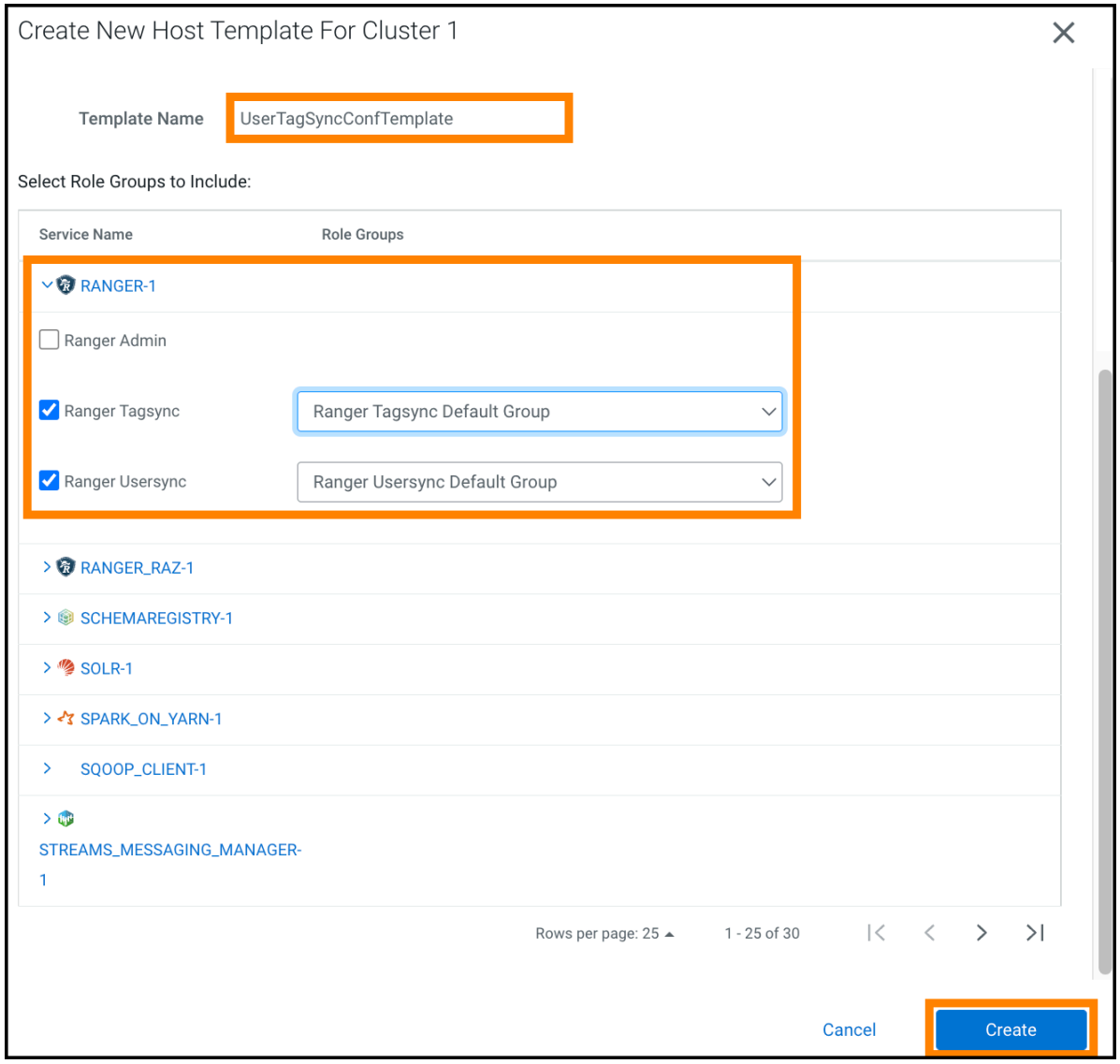
If the host on which your usersync and tagsync role groups run fails and cannot restart, you can migrate the role groups to a new host. You must stop usersync and tagsync and delete them from their original host before using them on the new one. Cloudera Manager Host Templates supports backing up, stopping, deleting, and migrating usersync and tagsync role groups from one host to another.

Procedure

1. Log in to your cluster as administrator, using Cloudera Manager.

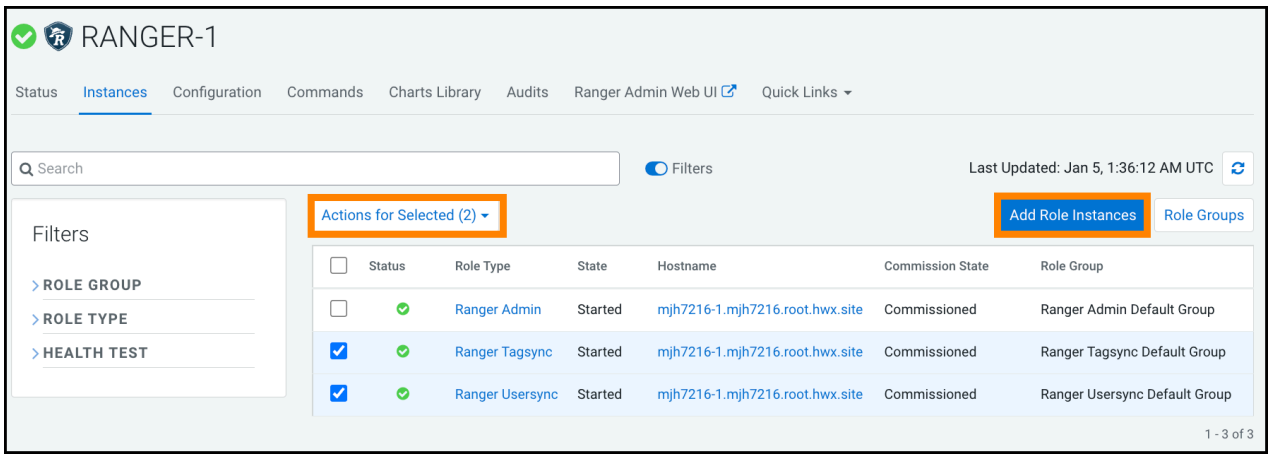
2. Back up you usersync and tagsync configurations.
   a) On Cloudera Manager Hosts , select Host Templates.
   b) On **Host Templates**, click Create.
   c) In Template Name, type a template name.
      This names a template in which you back up the usersync and tagsync role group configurations.
   d) On **Create New Host Template for Cluster** expand Ranger, select Ranger Tagsync and Ranger Usersync, then click Create, as shown in the following:

Figure 5: Creating a role groups template



Note: We recommend saving the actual config files used on the host for Ranger Usersync and Tagsync. You should verify the configs of the newly added role groups on the new host with the saved, old config files, ranger-ugsync-site.xml and ranger-tagsync-site.xml.

3. On Cloudera Manager Ranger Instances , select the Ranger Tagsync and Ranger Usersync role groups, as shown.



4. In Actions for Selected, select Stop.
5. In Actions for Selected, select Delete.
6. Click Add Role Instances.
   a) In Add Role Instances to Ranger Assign Roles Ranger Tagsync x 1 New , click Select Hosts.
   b) Choose a new host to which the Ranger Tagsync role will be added.
   c) In Add Role Instances to Ranger Assign Roles Ranger Usersync x 1 New , click Select Hosts.
   d) Choose a new host to which the Ranger Usersync role will be added.
   e) On Review Changes, click Finish.
   f) On Cloudera Manager Ranger Instances , select the Ranger Tagsync and Ranger Usersync role groups on the new host.
   g) With Usersync and Tagsync roles selected on the new host, in Actions, select Start.
7. Restart Ranger service.
8. Restart any stale services, if necessary.

Configuring JVM options and system properties for Ranger services

You can configure JVM options and system properties for Ranger, service-wide or to a specific Ranger role.

About this task

Adding key/value pairs to the Ranger Service Environment Advanced Configuration Snippet (Safety Valve) applies the values across all roles in the Ranger service except client configurations.

The `-D` option is used to set system properties in Java. System properties are key-value pairs that can be accessed by the Java application through the System.getProperty(key) method. Multiple -D params can be specified in the value field (space separated).

To configure JVM options or system properties for a specific role level, search and edit the following configurations:

Ranger Admin Environment Advanced Configuration Snippet

applies configurations to the Ranger Admin Default Group role only

Ranger Tagsync Environment Advanced Configuration Snippet

applies configurations to the Ranger Tagsync Default Group role only

Ranger Usersync Environment Advanced Configuration Snippet

applies configurations to the Ranger Usersync Default Group role only

Procedure

1. To set JVM options, in Cloudera Manager Home Ranger Configuration Search , type Ranger Service Environment Advanced Configuration Snippet.
2. In RANGER_service_env_safety_valve, click + (Add).
3. Add a key-value pair that configures a JVM option for Ranger.

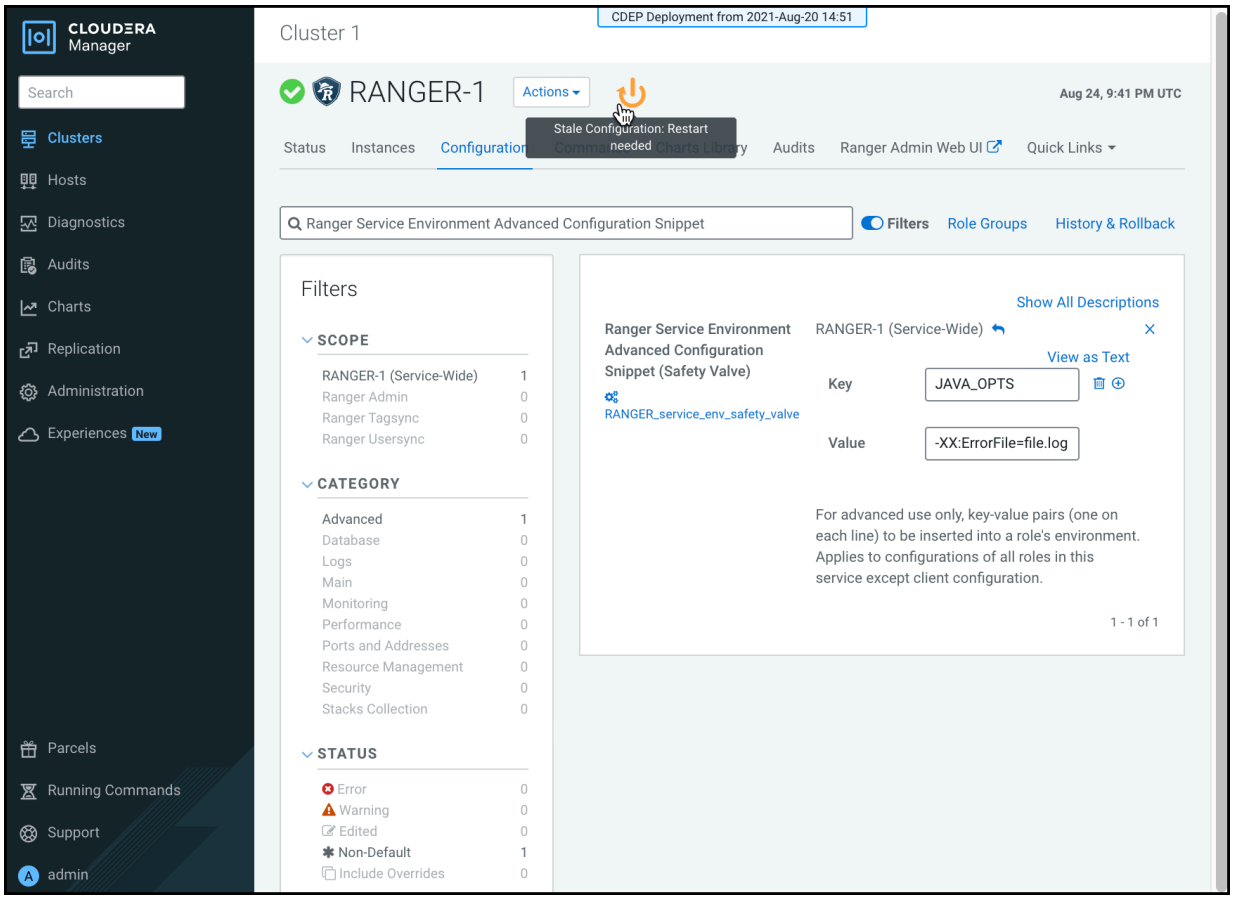
   Key

   JAVA_OPTS

   Value

   -XX:ErrorFile=file.log

   You can pass multiple JVM Options, each separated by a space, in the Value field. -XX:MetaspaceSize=100m -XX:MaxMetaspaceSize=200m represent default JVM options passed to the Ranger service.



4. To set system properties using the `-D` option: On Configuration, in Filters, choose Ranger Admin, in Search, type RANGER_ADMIN_Role.
5. In RANGER_ADMIN_role_env_safety_valve, click + (Add).

6. Add a key-value pair that configures system properties for the Ranger Admin role.

   Key

   JAVA_OPTS

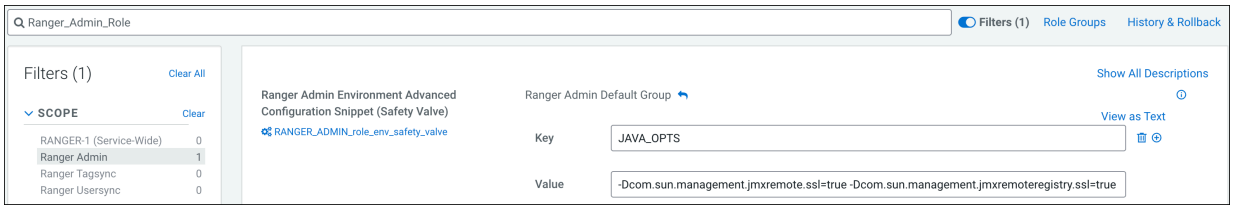
   Value

   -Dproperty.name=value

   You can pass multiple -D options, each separated by a space, in the Value field.

   -Dcom.sun.management.jmxremote.ssl=true -Dcom.sun.management.jmxremoteregistry.ssl=true -Dcom.sun.management.jmxremote.ssl.need.client.auth=true -Dcom.sun.management.jmxremote.ssl.enabled.protocols=TLS

   represent example system property values for the Ranger Admin role, two of which appear in the following example:



7. After completing configuration changes, click Save Changes.

   After saving configuration changes, the Stale Configuration icon appears on the Cloudera Manager UI. Optionally, click Stale Configuration to view details.

8. Select Actions Restart .

How to pass JVM options to Ranger KMS services

You can pass JVM options to Ranger KMS, service-wide or to a specific role within Ranger KMS service.

About this task

There are two ways you can pass JVM options to Ranger KMS.

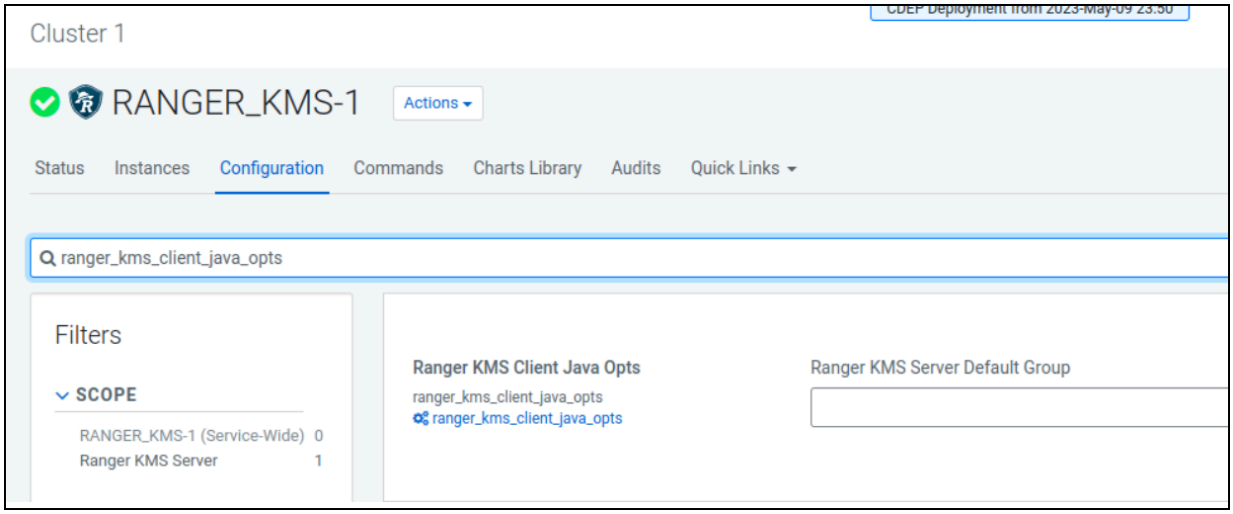
- Recommended : Using the Ranger KMS Client Java Opts field.
- Adding key/value pairs to the Ranger KMS Service Environment Advanced Configuration Snippet (Safety Valve).

Recommended : Using the Ranger KMS Client Java Opts field.

Procedure

1. In Cloudera Manager , select Ranger_KMS, then choose Configuration.

2. On Configuration, in Search, type ranger_kms_client_java_opts.



3. Enter the required JVM options in the Ranger KMS Client Java Opts.
   You can pass multiple JVM Options, each separated by a space : -XX:MetaspaceSize=100m -XX:MaxMetaspaceSize=256m Duser.timezone=UTC represent some JVM options passed to the Ranger KMS service.
4. Click Save Changes.

   After saving changes, the Stale Configuration icon appears on the Cloudera Manager UI. Optionally, click Stale Configuration to view details.
5. Select Actions Restart .

Ranger KMS Service Environment Advanced Configuration Snippet

Ranger KMS Service Environment Advanced Configuration Snippet (Safety Valve) applies the values across all roles in the Ranger KMS service except client configurations. Ranger KMS Server Environment Advanced Configuration Snippet applies configurations to the Ranger KMS Server Admin Default Group role only.

Procedure

1. In Cloudera Manager, select Ranger_KMS, then choose Configuration.
2. On Configuration, in Search, type Ranger KMS Service Environment Advanced Configuration Snippet.
3. In RANGER_KMS_service_env_safety_valve, click + (Add).
4. Add a key-value pair that configures a JVM option for Ranger KMS.

   Key

   JAVA_OPTS

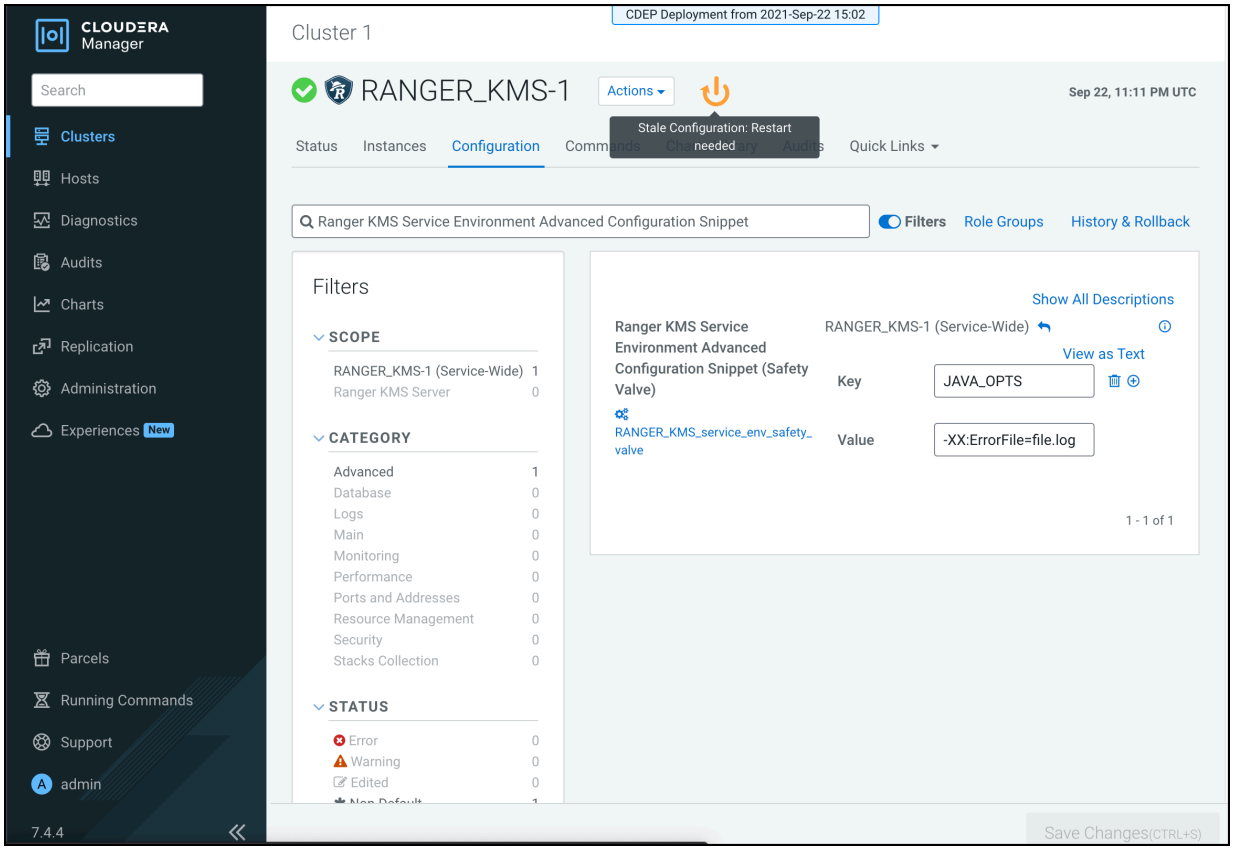
   Value

   -XX:ErrorFile=file.log

   You can pass multiple JVM Options, each separated by a space, in the Value field. -XX:MetaspaceSize=100m -XX:MaxMetaspaceSize=200m represent default JVM options passed to the Ranger KMS service.

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 .

How to clear Ranger Admin access logs

Starting with version 7.1.7sp1, you can set the max number of days to retain access logs in the Ranger Admin Web UI.

About this task

Ranger admin access log files accrue in the following path: /var/log/ranger/admin/access_log.yyyy-mm-dd.log. By default, these files aren't removed which consumes free space in the /var/ directory. You can set a maximum number of days for which these files are retained, after which they are deleted. To do so, you must add a configuration property to the ranger-admin-site.xml file.

Note: This feature is available in version 7.1.7sp1.

Procedure

1. In Cloudera Manager Home, select Ranger, then choose Configuration.
2. On Configuration, in Search, type ranger-admin.
3. In conf/ranger-admin-site.xml_role_safety_valve, click + (Add).

4. Add a key-value pair that configures the maximum number of days to retain Ranger Admin access log files.

   Name

   ranger.accesslog.rotate.max.days

   Value

   any suitable number of days

   To retain Ranger Admin access log files for 90 days, in the Value field, type 90
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 .

Configuring purge of x_auth_sess data

A Ranger administrator user can configure Ranger Admin service e to purge authentication login records during start-up.

Currently, Ranger stores authentication entries in x_auth_sess table which may accumulate lots of entries in a few days. You may need to manually remove the entries from x_auth_sess table regularly in order to maintain the disk space or handle the disk space issues in a production environment.

Option-1: Delete the entries during every start of ranger-admin service:

1. In Cloudera Manager Ranger Configuration Search , type conf/ .
2. In Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml, click +Add.

3. Add the following properties and values to conf/ranger-admin-site.xml_role_safety_valve:

   ranger.admin.init.purge.login_records

   true

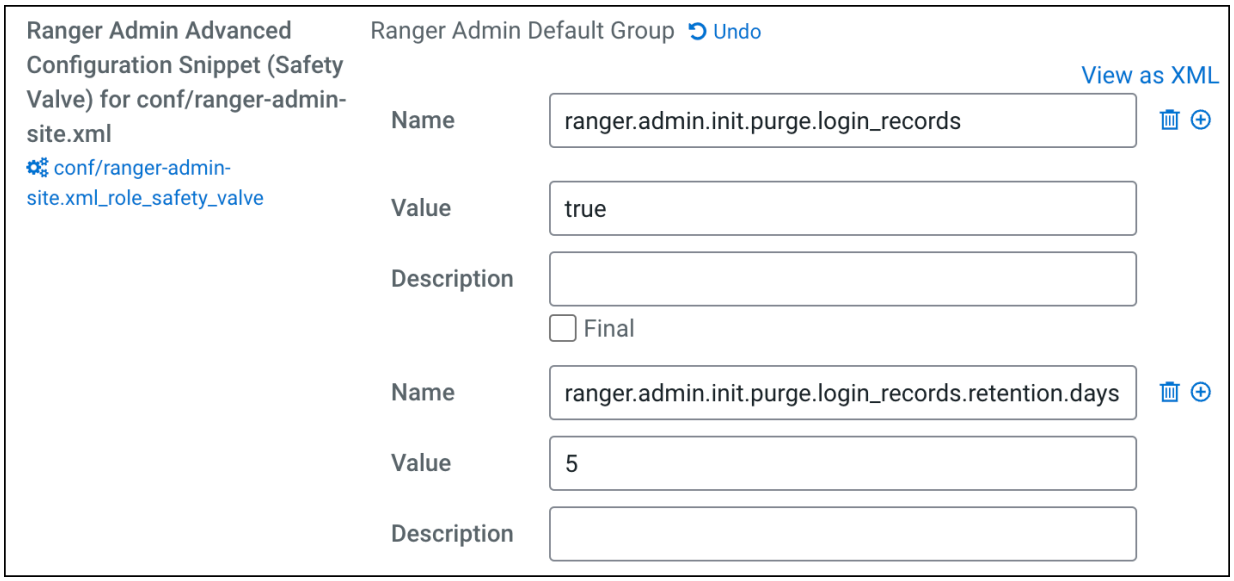
   default = false

   ranger.admin.init.purge.login_records.retention.days

   type a positive numerical value

   For example:

   Figure 6: Adding properties to Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml



   This example shows configuration properties that set ranger admin service to purge records older than 5 days from x_auth_sess table, during service (re)start.

4. Click Save Changes (CTRL+S).
5. Restart Ranger service.

Option-2: : Ranger Admin User can call REST-api to delete records from x_auth session table:

Login to Ranger Admin CLI using Ranger Admin role credentials that allow you to call this REST API:

```
curl -u admin:admin -H "Accept: application/json" -H "Content-Type: applicat
ion/json" -X DELETE
 'http://localhost:6080/service/public/v2/api/server/purge/records?type=logi
n_records&retentionDays=5'
```

if retentionDays parameter is not provided then default value 180 shall be considered.

Enable Ranger Admin login using kerberos authentication

You can enable the Ranger Admin web UI to use kerberos authentication for browser-based login.

About this task

The Ranger Admin web UI does not allow kerberos authentication by default. To allow users of specific web browsers to login to the Ranger Admin web UI, you must add configuration properties to the ranger-admin-site.xml file.

Procedure

1. In Cloudera Manager Home, select Ranger, then choose Configuration.
2. On Configuration, in Search, type ranger-admin.
3. In conf/ranger-admin-site.xml_role_safety_valve, click + (Add).
4. Add a key-value pair that configures the maximum number of days to retain Ranger Admin access log files.
   Name

   ranger.allow.kerberos.auth.login.browser

   Value

   true
5. Optionally, you can a another key-value pair that defines specific web browsers that allow kerberos authenticated login.
   Name

   ranger.krb.browser-useragents-regex

   Value

   Mozilla,Opera,Chrome
6. Click Save Changes.

   After saving changes, the Stale Configuration icon appears on the Cloudera Manager UI. Optionally, click Stale Configuration to view details.
7. Select Actions Restart .

Results

Users should now be able to login to Ranger Admin UI using kerberos authentication.

Note: Known Issue: If you have enabled browser login using kerberos authentication, and there is no valid ticket available to authenticate. In this case, your browser may display a blank page when you click the Ranger Admin URL. To redirect to the login page, you must refresh the page to view the login page. This issue is not found on Chrome browser as of now.

How to configure Ranger HDFS plugin configs per (NameNode) Role Group

You can override the service-level configurations, by setting configurations at the Role/Group level.

About this task

The Ranger HDFS plugin supports service-wide configuration using safety valves for auditing, policy management and security. Additionally, you can override service-wide security setting by configuring the NameNode Advanced Configuration Snippet (Safety Valve) which allows role/group specific configuration. This feature supports configuring security policies across a federated namespace environment.

Procedure

1. In Cloudera Manager Home, select HDFS, then choose Configuration.

2. On Configuration, in Search, type Ranger-hdfs.
3. In NameNode Advanced Configuration Snippet (Safety Valve), click + (Add).
4. Add key-value pairs that configure ranger-hdfs-security.xml per NameNode group.

Results

key-value pairs that you define in NameNode Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml override any defined in HDFS Service Advanced Configuration Snippet (Safety Valve) for ranger-hdfs-security.xml.

How to add a coarse URI check for Hive agent

You can set the Hive agent authorization check at the parent folder level using a safety valve configuration in Cloudera Manager.

Hive command performance deteriorates when the Hive URL location specified has a large number of folders and files. Performance suffers while the recursive check for permission occurs on all folders and files. One way to improve performance is to enable a Hive URL policy. Another way is to configure a coarse URI check that checks the parent folder permission only for authorization.

To avoid a URL recursive permission check, create the following configuration:

1. Go to CM Hive Configuration Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml .,
2. Click + to add a new configuration.
   a. In Name, type xasecure.hive.uri.permission.coarse.check.
   b. In Value, type true.
3. Click Save Changes.
4. Restart the Hive service.

How to suppress database connection notifications

You can limit the number of notifications to those about connection requests made from Ranger to an Oracle db.

About this task

Ranger Admin performs many interactions with its backend database (often Oracle), for example; policy updates, user/group info updates, etc. A customer can see audit logs that represent all activities at the Oracle side, not just connection attempts.

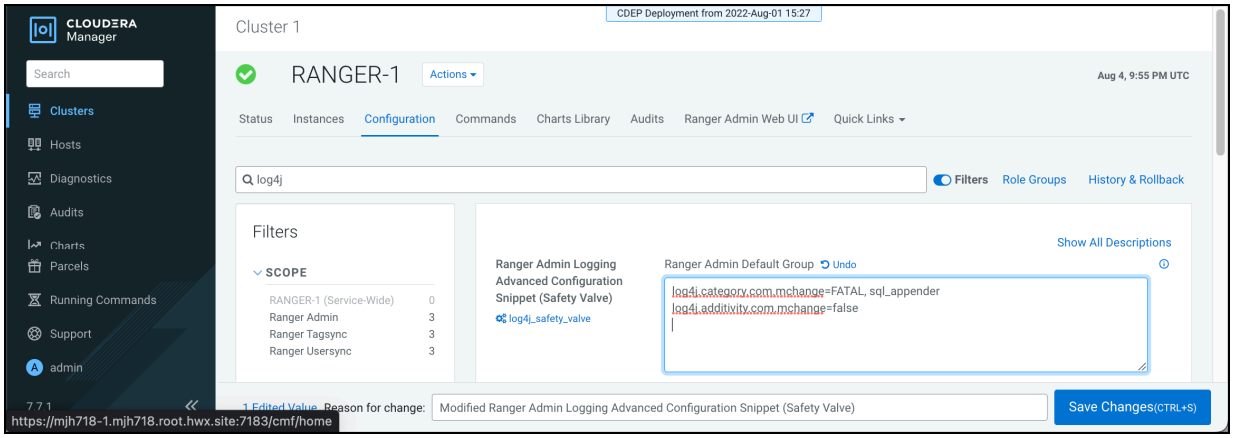
To limit the number of notifications to those that describe persistent db connections:

Procedure

1. In Cloudera Manager Home, select Ranger, then choose Configuration.
2. On Configuration, in Search, type log4j.
3. In Ranger Admin Logging Advanced Configuration Snippet (Safety Valve)

4. In Ranger Admin Default Group, type the following text:
   log4j.category.com.mchange=FATAL, sql_appender
   log4j.additivity.com.mchange=false

   Figure 7: Suppressing Ranger db connection notifications



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 .

How to change the password for Ranger users

You can change the password for multiple Ranger users without using the Ranger Admin Web UI.

About this task

To change the passwords of Ranger users defined in the Ranger Admin modules without using the Ranger Admin Web UI, use the following steps:

Before you begin

Change current working directory to the Ranger Admin installation directory.

Procedure

1. Set/export JAVA_HOME environment variable if not set.
   export JAVA_HOME=/usr/java/jdk1.8.0_232-cloudera
2. In the ranger-admin process run directory:
   a) Find the proc.json file.
   b) Search for HADOOP_CREDSTORE_PASSWORD.
   c) Use that password to export it in the env variable.

   export HADOOP_CREDSTORE_PASSWORD=2fl2xmsd5zrp9homuqwwwe3it
3. Copy the sql connector jar to ranger-admin ews/lib directory.
   cp /usr/share/java/mysql-connector-java.jar /opt/cloudera/parcels/CDH/lib/ranger-admin/ews/lib/
4. Run the change password util command
   python changepasswordutil.py testuser1 Testuser1 Test12345