

Configuring Advanced Security Options for Apache Ranger

Date published: 2020-07-28

Date modified: 2023-09-07



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 pass JVM options to Ranger KMS KTS services.....	32
Recommended : Using the Ranger KMS KTS Client Java Opts field.....	32
Ranger KMS KTS Service Environment Advanced Configuration Snippet.....	33
How to clear Ranger Admin access logs.....	34
Configuring purge of x_auth_sess data.....	34
Enable Ranger Admin login using kerberos authentication.....	35

How to configure Ranger HDFS plugin configs per (NameNode) Role Group.....	36
How to add a coarse URI check for Hive agent.....	37
How to suppress database connection notifications.....	37
How to change the password for Ranger users.....	38

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 .

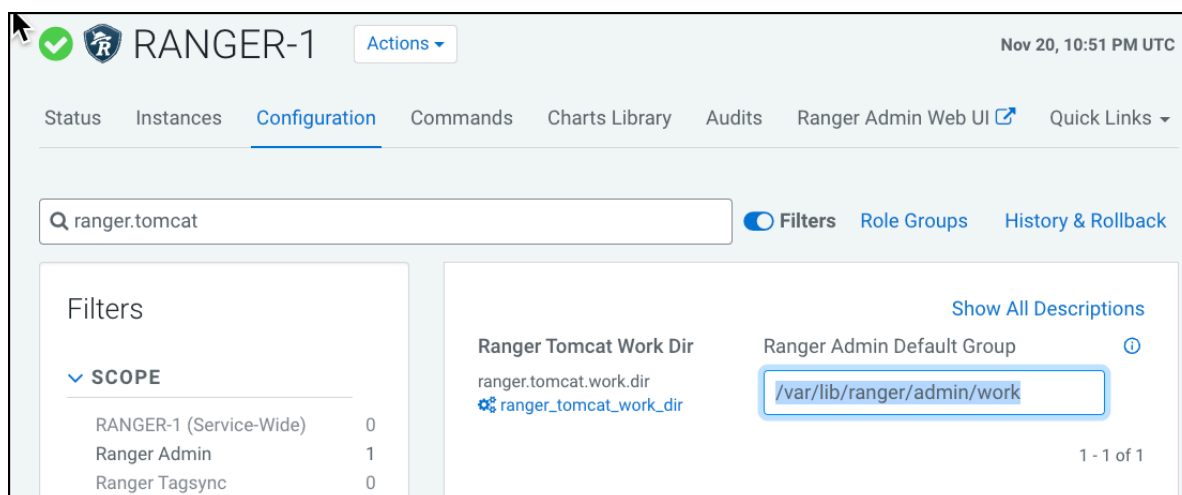
This is the Ranger Service Work Directory name.

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.
 - 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.

The screenshot displays the Cloudera Manager interface for configuring the Session Inactivity Timeout for Ranger Admin. The left sidebar shows the navigation menu with 'Clusters' selected. The main panel shows the configuration for 'RANGER-1' under the 'Configuration' tab. A search bar contains 'session'. The 'Filters' section shows 'SCOPE' with 'RANGER-1 (Service-Wide)' selected. The 'CATEGORY' section shows 'Main' selected. The configuration details for 'Session Inactivity Timeout For Ranger Admin' are shown, with the value '15' and unit 'minute(s)' set. The 'Ranger Admin Default Group' is also visible. A 'Save Changes(CTRL+S)' button is at the bottom right.

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	<p>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.</p> <p>Ranger Tagsync connects to Ranger Admin. If Ranger Admin is SSL enabled, make sure you add a Ranger Admin certificate in the trust store.</p> <p>If this parameter is not provided, the default list of well-known certificate authorities is used instead.</p>
Ranger Tagsync TLS/SSL Client Trust Store Password xasecure.policymgr.clientssl.truststore.password	<p>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.</p>
Ranger Usersync TLS/SSL Client Trust Store File ranger.usersync.truststore.file	<p>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).</p> <p>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.</p> <p>If this parameter is not provided, the default list of known certificate authorities is used.</p>
Ranger Usersync TLS/SSL Client Trust Store Password ranger.usersync.truststore.password	<p>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.</p>

- 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	<p>The alias used for the Ranger Admin TLS/SSL keystore file.</p> <p>If host FQDN is used as an alias while creating a keystore file, the default placeholder value <code>{{RANGER_ADMIN_HOST}}</code> is replaced with the host FQDN where Ranger Admin will be installed in the current cluster.</p> <p>The placeholder can be replaced to have a custom alias used while creating the keystore file.</p> <p>If using a custom alias which is the same as the host short name, use <code>{{RANGER_ADMIN_HOST_UQDN}}</code> placeholder as a value.</p>

- 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	<p>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.</p> <p>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.</p> <p>If this parameter is not provided, the default list of well-known certificate authorities is used instead.</p>
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	<p>The alias for the Ranger KMS Server TLS/SSL keystore file.</p> <p>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.</p> <p>The placeholder can be replaced to have a custom alias used while creating the keystore file.</p> <p>If using a custom alias which is the same as host short name then use {{HOST_UQDN}} placeholder as a value.</p>

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

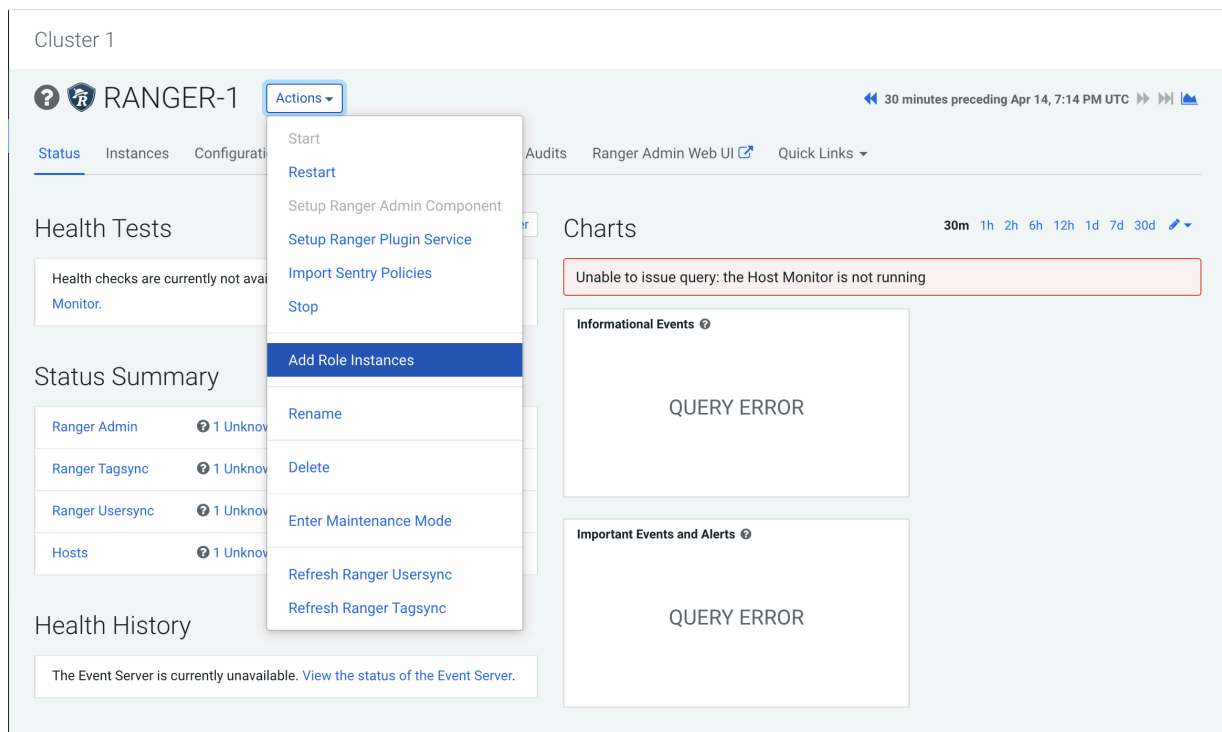
How to configure High Availability (HA) for Apache Ranger.

Configure Ranger Admin High Availability

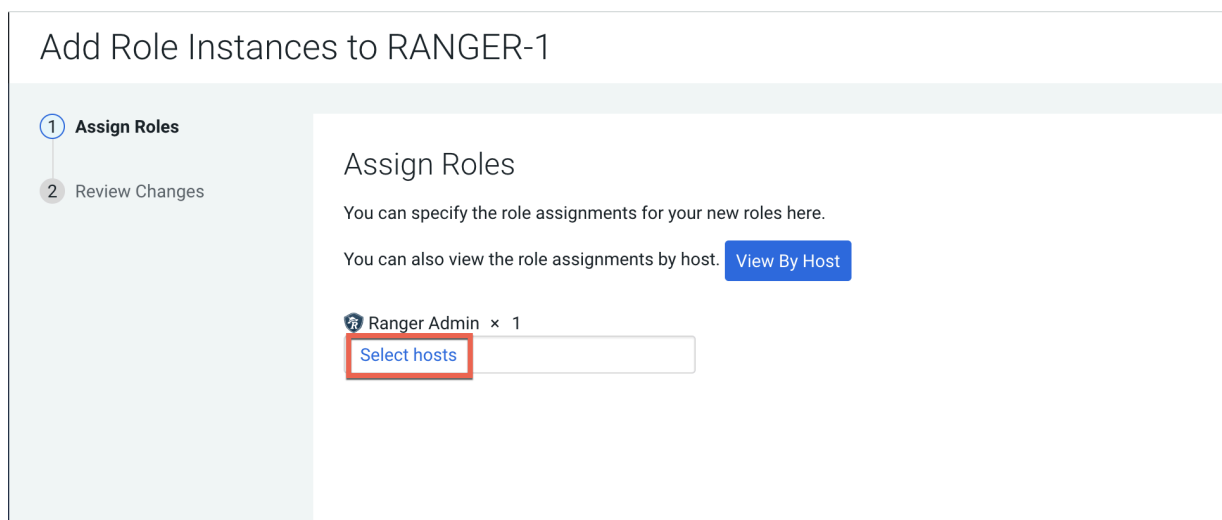
How to configure Ranger Admin High Availability (HA) by adding additional Ranger Admin role instances.

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.

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.

Q Enter hostnames: host01, host[01-10], IP addresses or rack.

Search

Tip: Click the first checkbox, hold down the Shift key and click the last checkbox to select a range.

<input type="checkbox"/>	Hostname ↑	IP Address	Rack	Cores	Physical Memory	Existing Roles	Added Roles
<input checked="" type="checkbox"/>	dhost-001 1 dhost-001 3 dhost-001,site	172.27.114.133	/default	88	251.6 GiB	AS G HB... RS DN G G G G ID KB KG M G LS RA RT RU G G G G NM ZS	
<input checked="" type="checkbox"/>	dhost-002 2 dhost-002 3 dhost-002,site	172.27.12.201	/default	32	251.6 GiB	M B NN NF... SNN G HMS G HS2 LB HS KTR ICS ISS KB LHBI TS G AP ES HM RM SM OS SS G HS G G JHS RM S	RA
<input type="checkbox"/>	dhost-003 3 dhost-003 3 dhost-003,site	172.27.109.135	/default	88	251.6 GiB	RS DN G G ID G KB TS G G G G NM	

1 - 3 of 3

CancelOK

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

Add Role Instances to RANGER-1

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

Ranger Admin × (1 + 1 New)

dhost-001-2.dhost-001,site...

Back

Continue

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

Add Role Instances to RANGER-1

✓ Assign Roles

2 Review Changes

Review Changes

Maximum Shards for Solr Collection of Ranger Audits ranger.audit.solr.max.shards.per.node	Ranger Admin Default Group	<input type="text" value="1"/>	?
Replicas for Solr Collection of Ranger Audits ranger.audit.solr.no.replica	Ranger Admin Default Group	<input type="text" value="1"/>	?
Shards for Solr Collection of Ranger Audits ranger.audit.solr.no.shards	Ranger Admin Default Group	<input type="text" value="1"/>	?
Ranger Database Host ranger_database_host	Ranger Admin Default Group	<input type="text" value="cloudera-0011-1.cloudera-0011.com:5432/ranger1"/>	?
Ranger Database Name ranger_database_name	Ranger Admin Default Group	<input type="text" value="ranger1"/>	?
Ranger Database User Password ranger.jpa.jdbc.password	Ranger Admin Default Group	<input type="password" value="....."/>	?
Ranger Database Type ranger_database_type	Ranger Admin Default Group	<input type="radio"/> MySQL <input type="radio"/> Oracle <input checked="" type="radio"/> PostgreSQL <input type="radio"/> MsSQL <input type="radio"/> SQLA	?
Ranger Database User ranger.jpa.jdbc.user	Ranger Admin Default Group	<input type="text" value="rangeradmin"/>	?
Ranger Admin TLS/SSL Client Trust Store File ranger.truststore.file	Ranger Admin Default Group	<input type="text"/>	?
Ranger Admin TLS/SSL Client Trust Store Password ranger.truststore.password	Ranger Admin Default Group	<input type="password"/>	?
Enable TLS/SSL for Ranger	<input type="checkbox"/> Ranger Admin Default Group		?

Back

Continue

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

Cluster 1 CDEP Deployment from 2020-Apr-28 09:23

RANGER-1 Actions

Stale Configuration: Restart

Status Instances Configuration Audits Ranger Admin Web UI Quick Links

Health Tests Create Trigger

Show 3 Good

Status Summary

Ranger Admin	1 Good Health	1 Stopped
Ranger Tagsync	1 Good Health	
Ranger Usersync	1 Good Health	
Hosts	2 Good Health	

Charts

Informational Events

Important Events and Alerts

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`.

The screenshot shows the Cloudera Manager interface for Cluster 1, specifically the Apache Ranger-1 service. The left sidebar contains navigation links for Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Private Cloud. The main content area is divided into several sections:

- Health Tests:** Shows 3 Good health tests.
- Status Summary:** A table listing the health of various components:

Component	Health Status
Ranger Admin	2 Good Health
Ranger Tagsync	1 Good Health
Ranger Usersync	1 Good Health
Hosts	2 Good Health
- Health History:** A list of recent health events:

Event	Time
> 3 Became Good	7:24:28 PM
> 3 Became Disabled	7:23:37 PM
> 2 Became Bad	7:23:32 PM
Ranger Admin Health Good	7:14:09 PM
> 1 Became Good	
- Web UI:** A dropdown menu is highlighted with a red box, showing links to 'Ranger Admin Web UI (cloudera-2-1)' and 'Ranger Admin Web UI (cloudera-2-2)'.
- Charts:** Two bar charts are shown: 'Informational Events' and 'Important Events and Alerts'. The 'Informational Events' chart shows 1 event at 07:15. The 'Important Events and Alerts' chart shows 1 event at 07:15.

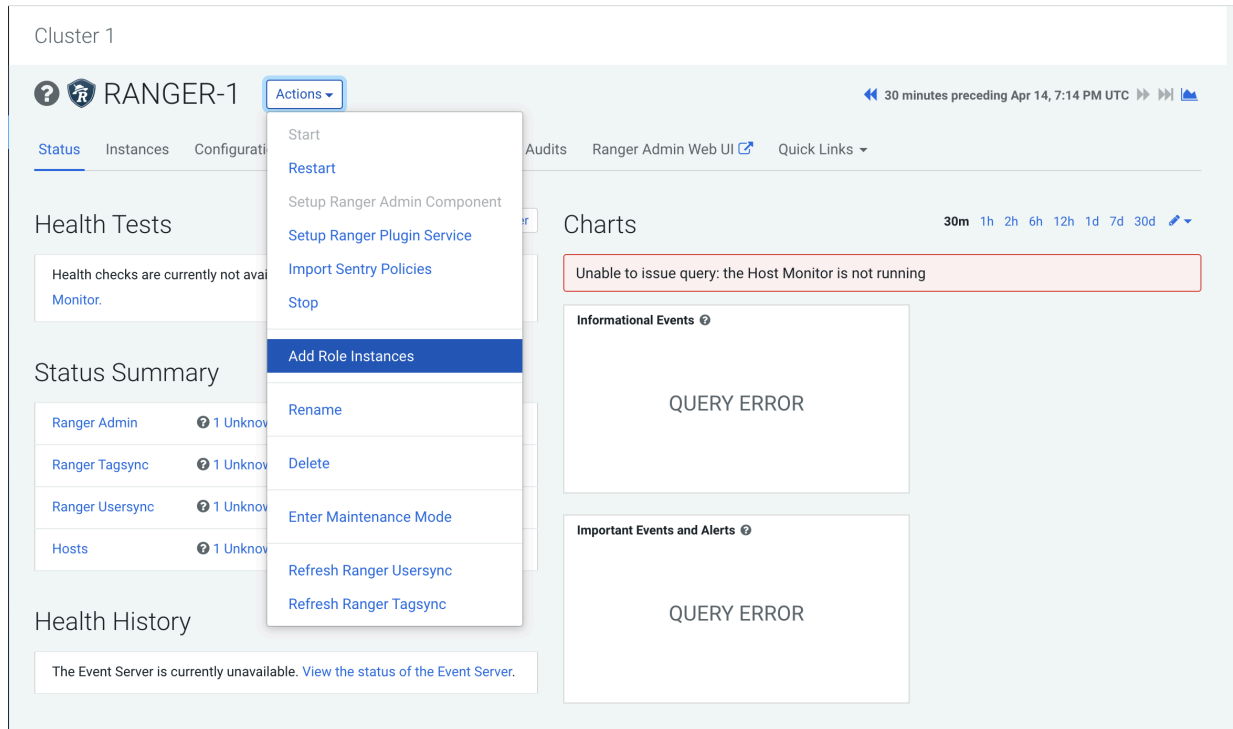
Configure Ranger Admin High Availability with a Load Balancer

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.

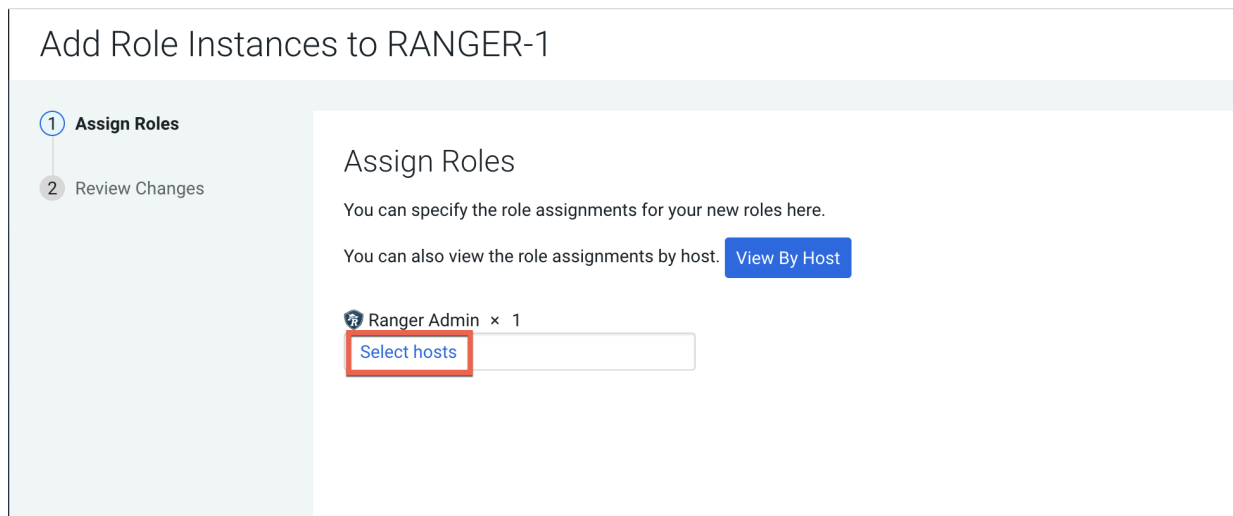
Procedure

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.

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.

Q Enter hostnames: host01, host[01-10], IP addresses or rack.

Search

Tip: Click the first checkbox, hold down the Shift key and click the last checkbox to select a range.

<input type="checkbox"/>	Hostname ↑	IP Address	Rack	Cores	Physical Memory	Existing Roles	Added Roles
<input checked="" type="checkbox"/>	d...-221 1 d... 3 d... 3 d... 3 d...	172.27.114.133	/default	88	251.6 GiB	AS G HB... RS DN G G G ID KB KG M L G LS RA RT RU G G G G NM ZS	
<input checked="" type="checkbox"/>	d...-221 2 d... 3 d... 3 d... 3 d...	172.27.12.201	/default	32	251.6 GiB	M B NN NF... SNN G HMS G HS2 LB HS KTR ICS ISS KB LHBI TS L G AP ES HM RM SM OS SS G HS G G JHS RM S	RA
<input type="checkbox"/>	d...-221 3 d... 3 d... 3 d...	172.27.109.135	/default	88	251.6 GiB	RS DN G G G ID G KB TS L G G G G NM	

1 - 3 of 3

CancelOK

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

Add Role Instances to RANGER-1

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

Ranger Admin × (1 + 1 New)

d...-2.d...
3 d...
3 d...

BackContinue

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

Add Role Instances to RANGER-1

✓ Assign Roles

2 Review Changes

Review Changes

Maximum Shards for Solr Collection of Ranger Audits <small>ranger.audit.solr.max.shards.per.node</small>	Ranger Admin Default Group	<input type="text" value="1"/>	?
Replicas for Solr Collection of Ranger Audits <small>ranger.audit.solr.no.replica</small>	Ranger Admin Default Group	<input type="text" value="1"/>	?
Shards for Solr Collection of Ranger Audits <small>ranger.audit.solr.no.shards</small>	Ranger Admin Default Group	<input type="text" value="1"/>	?
Ranger Database Host <small>ranger_database_host</small>	Ranger Admin Default Group	<input type="text" value="cloudera-0011-1.cloudera-0011.com:5432/ranger1"/>	?
Ranger Database Name <small>ranger_database_name</small>	Ranger Admin Default Group	<input type="text" value="ranger1"/>	?
Ranger Database User Password <small>ranger.jpa.jdbc.password</small>	Ranger Admin Default Group	<input type="password" value="....."/>	?
Ranger Database Type <small>ranger_database_type</small>	Ranger Admin Default Group	<input type="radio"/> MySQL <input type="radio"/> Oracle <input checked="" type="radio"/> PostgreSQL <input type="radio"/> MsSQL <input type="radio"/> SQLA	?
Ranger Database User <small>ranger.jpa.jdbc.user</small>	Ranger Admin Default Group	<input type="text" value="rangeradmin"/>	?
Ranger Admin TLS/SSL Client Trust Store File <small>ranger.truststore.file</small>	Ranger Admin Default Group	<input type="text"/>	?
Ranger Admin TLS/SSL Client Trust Store Password <small>ranger.truststore.password</small>	Ranger Admin Default Group	<input type="text"/>	?
Enable TLS/SSL for Ranger	<input type="checkbox"/> Ranger Admin Default Group		?

Back

Continue

- 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.

The screenshot shows the Cloudera Ranger Admin Web UI for the instance 'RANGER-1'. The 'Configuration' tab is active, and the 'Load Balancer' property is selected. The 'ranger.externalurl' property is being edited. The current value is 'http://', and the user is entering 'http://'. The 'SCOPE' filter shows 'RANGER-1 (Service-Wide)' with a count of 1. The 'CATEGORY' filter shows 'Main' with a count of 1. The 'Save Changes (CTRL+S)' button is visible at the bottom right.

SCOPE	Count
RANGER-1 (Service-Wide)	1
Ranger Admin	0
Ranger Tagsync	0
Ranger Usersync	0

CATEGORY	Count
Advanced	0
Logs	0
Main	1
Monitoring	0
Performance	0
Ports and Addresses	0

1 Edited Value Reason for change: Modified Load Balancer Address

Save Changes (CTRL+S)

- 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 check the list of principals for each domain where Ranger Admin and the load-balancer are installed.
 Note: This step assumes you are using an MIT KDC (and `kadmin.local`). 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.local`).

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-process>/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 the 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.

Cluster 1 CDEP Deployment from 2020-Apr-28 09:23

RANGER-1 Actions 30 minutes preceding Apr 28, 6:54 PM UTC

Stale Configuration: Restart needed

Status Instances Configuration Audits Ranger Admin Web UI Quick Links

Health Tests Create Trigger

Show 3 Good

Status Summary

Ranger Admin	1 Good Health	1 Stopped
Ranger Tagsync	1 Good Health	
Ranger Usersync	1 Good Health	
Hosts	2 Good Health	

Charts 30m 1h 2h 6h 12h 1d 7d 30d

Informational Events

events

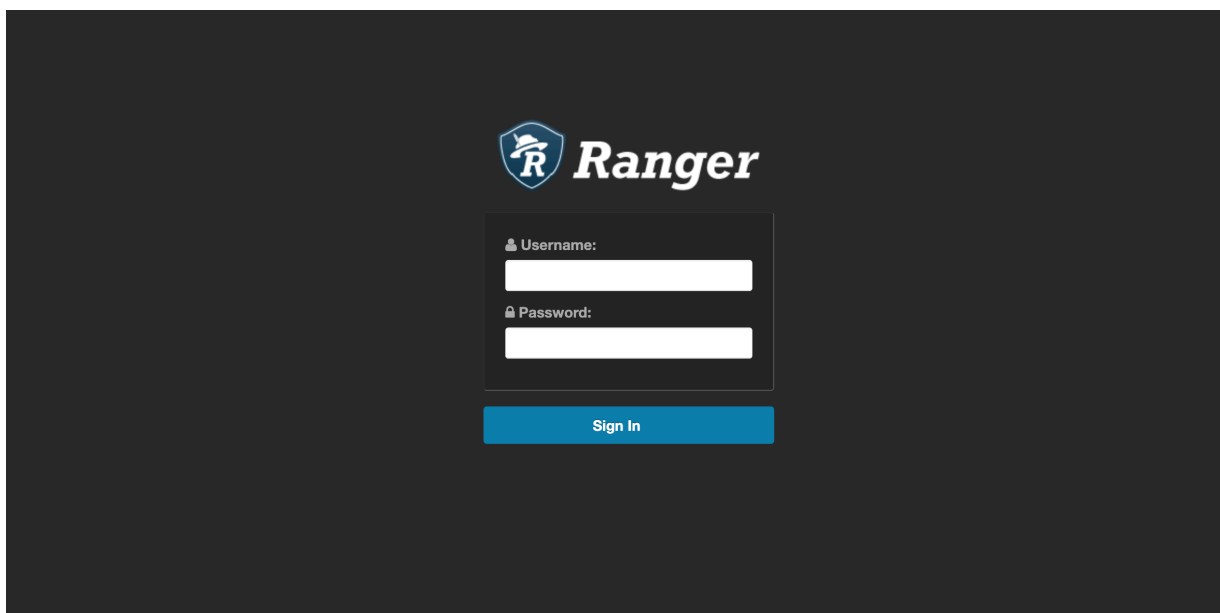
06:30 06:45

RANGER-1, Informational Events 0

Important Events and Alerts

events

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 availability of Ranger Usersync and Tagsync manually.

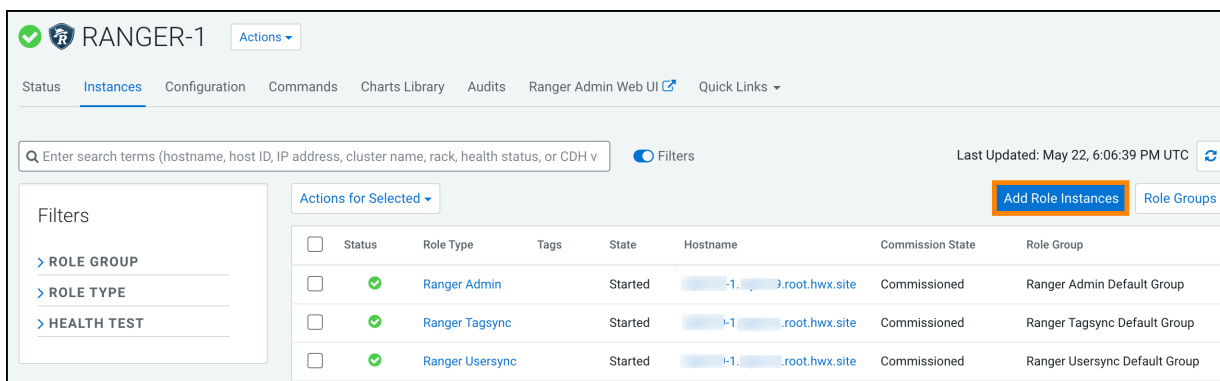
About this task

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 commissioned Usersync role along with an existing one

RANGER-1

Status **Instances** Configuration Commands Charts Library Audits Ranger Admin Web UI Quick Links

⚠ This entity is currently running with an outdated configuration. Restart the service (or the instance) for the changes to take effect.

Q Enter search terms (hostname, host ID, IP address, cluster name, rack, health status, or CDH version) se Filters Last Updated: May 22, 6:33:49 PM UTC

Filters

- STATUS
 - Stopped 2
 - Good Health 3
- ROLE GROUP
- ROLE TYPE
- STATE
- HEALTH TEST

Actions for Selected (2)

Status	Role Type	Tags	State	Hostname	Commission State	Role Group
<input type="checkbox"/>	Ranger Tagsync		Stopped	-2.100.100.root.hwx.site	Commissioned	Ranger Tagsync Default Group
<input checked="" type="checkbox"/>	Ranger Usersync		Stopped	-2.100.100.root.hwx.site	Commissioned	Ranger Usersync Default Group
<input type="checkbox"/>	Ranger Admin		Started with Outdated Configuration	-1.100.100.root.hwx.site	Commissioned	Ranger Admin Default Group
<input type="checkbox"/>	Ranger Tagsync		Started with Outdated Configuration	-1.100.100.root.hwx.site	Commissioned	Ranger Tagsync Default Group
<input checked="" type="checkbox"/>	Ranger Usersync		Started with Outdated Configuration	-1.100.100.root.hwx.site	Commissioned	Ranger Usersync Default Group

Add Role Instances Role Groups



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

RANGER-1

Status **Instances** Configuration Commands Charts Library Audits Ranger Admin Web UI Quick Links

Q Enter search terms (hostname, host ID, IP address, cluster name, rack, health status, or CDH version) se Filters Last Updated: May 22, 6:58:51 PM UTC

Filters

- ROLE GROUP
- ROLE TYPE
- HEALTH TEST

Actions for Selected

Status	Role Type	Tags	State	Hostname	Commission State	Role Group
<input type="checkbox"/>	Ranger Tagsync		Started	-2.100.100.root.hwx.site	Commissioned	Ranger Tagsync Default Group
<input type="checkbox"/>	Ranger Usersync		Started	-2.100.100.root.hwx.site	Commissioned	Ranger Usersync Default Group
<input type="checkbox"/>	Ranger Admin		Started	-1.100.100.root.hwx.site	Commissioned	Ranger Admin Default Group
<input type="checkbox"/>	Ranger Tagsync (Active)		Started	-1.100.100.root.hwx.site	Commissioned	Ranger Tagsync Default Group
<input type="checkbox"/>	Ranger Usersync (Active)		Started	-1.100.100.root.hwx.site	Commissioned	Ranger Usersync Default Group

Add Role Instances Role Groups

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

Create New Host Template For Cluster 1

Template Name:

Select Role Groups to Include:

Service Name	Role Groups
<input checked="" type="checkbox"/> RANGER-1 <input type="checkbox"/> Ranger Admin <input checked="" type="checkbox"/> Ranger Tagsync <input checked="" type="checkbox"/> Ranger Usersync	Ranger Tagsync Default Group Ranger Usersync Default Group
> RANGER_RAZ-1	
> SCHEMAREGISTRY-1	
> SOLR-1	
> SPARK_ON_YARN-1	
> SQOOP_CLIENT-1	
> STREAMS_MESSAGING_MANAGER-1	

Rows per page: 25 1 - 25 of 30

Cancel **Create**



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.

The screenshot shows the Cloudera Ranger Admin Web UI for 'RANGER-1'. The 'Instances' tab is active. A search bar and a 'Filters' sidebar are on the left. A table of roles is displayed with columns: Status, Role Type, State, Hostname, Commission State, and Role Group. Three roles are listed: Ranger Admin, Ranger Tagsync, and Ranger Usersync. The 'Actions for Selected (2)' dropdown is highlighted, and the 'Add Role Instances' button is also highlighted. The table data is as follows:

Status	Role Type	State	Hostname	Commission State	Role Group
<input type="checkbox"/>	Ranger Admin	Started	mjh7216-1.mjh7216.root.hwx.site	Commissioned	Ranger Admin Default Group
<input checked="" type="checkbox"/>	Ranger Tagsync	Started	mjh7216-1.mjh7216.root.hwx.site	Commissioned	Ranger Tagsync Default Group
<input checked="" type="checkbox"/>	Ranger Usersync	Started	mjh7216-1.mjh7216.root.hwx.site	Commissioned	Ranger Usersync Default Group

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.

The screenshot shows the Cloudera Manager interface for Cluster 1. The 'Configuration' tab is selected, and a search for 'Ranger Service Environment Advanced Configuration Snippet' is performed. The 'Filters' section on the left shows the following categories and counts:

SCOPE	Count
RANGER-1 (Service-Wide)	1
Ranger Admin	0
Ranger Tagsync	0
Ranger Usersync	0

The 'CATEGORY' section shows the following categories and counts:

CATEGORY	Count
Advanced	1
Database	0
Logs	0
Main	0
Monitoring	0
Performance	0
Ports and Addresses	0
Resource Management	0
Security	0
Stacks Collection	0

The 'STATUS' section shows the following statuses and counts:

STATUS	Count
Error	0
Warning	0
Edited	0
Non-Default	1
Include Overrides	0

The main configuration area shows a key-value pair for 'JAVA_OPTS' with the value '-XX:ErrorFile=file.log'. The configuration is for 'RANGER-1 (Service-Wide)' and is titled 'Ranger Service Environment Advanced Configuration Snippet (Safety Valve)'.

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.jmxremote.registry.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:

The screenshot shows the Cloudera Manager configuration page for the Ranger Admin role. On the left, a 'Filters (1)' sidebar shows 'SCOPE' with 'Ranger Admin' selected. The main area displays the 'Ranger Admin Environment Advanced Configuration Snippet (Safety Valve)' for the 'Ranger Admin Default Group'. The 'Key' field is 'JAVA_OPTS' and the 'Value' field is '-Dcom.sun.management.jmxremote.ssl=true -Dcom.sun.management.jmxremote.registry.ssl=true'.

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.

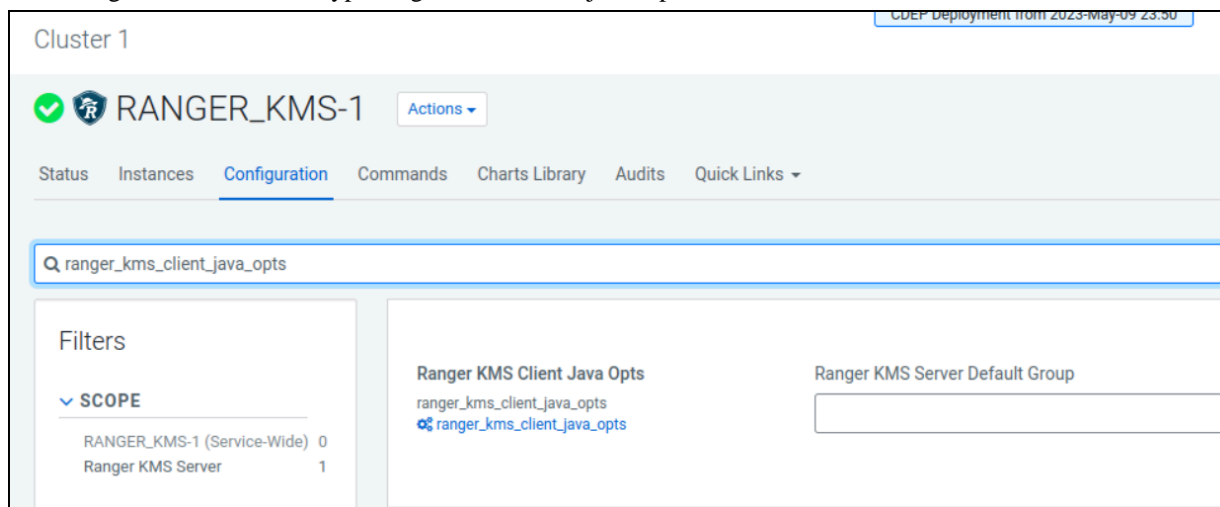
- Recommended : Using the Ranger KMS Client Java Opts field.
- Adding key/value pairs to the Ranger KMS Service Environment Advanced Configuration Snippet (Safety Valve).

Recommended : Using the Ranger KMS Client Java Opts field.

Procedure

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

- On Configuration, in Search, type `ranger_kms_client_java_opts`.



- 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.
- Click Save Changes.
After saving changes, the Stale Configuration icon appears on the Cloudera Manager UI. Optionally, click Stale Configuration to view details.
- 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

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

Key

`JAVA_OPTS`

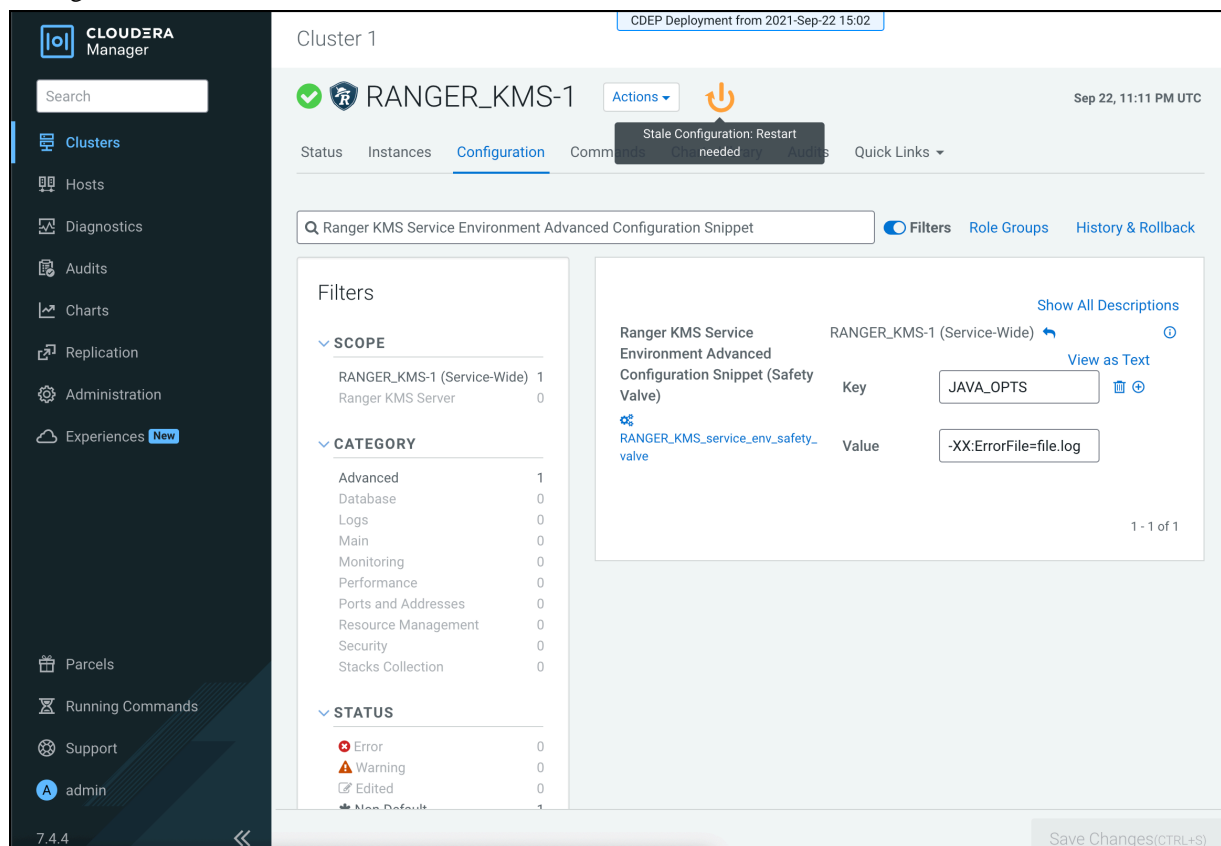
Value

`-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 pass JVM options to Ranger KMS KTS services

You can pass JVM options to Ranger KMS KTS to enable better debugging and tuning.

About this task

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

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

Recommended : Using the Ranger KMS KTS Client Java Opts field.

Procedure

1. In Cloudera Manager, select Ranger_KMS_KTS, then choose Configuration.
2. On Configuration, in Search, type ranger_kms_kts_client_java_opts.

- Enter the required JVM options in the Ranger KMS KTS 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.
- Click Save Changes.
After saving changes, the Stale Configuration icon appears on the Cloudera Manager UI. Optionally, click Stale Configuration to view details.
- Select Actions Restart .

Ranger KMS KTS Service Environment Advanced Configuration Snippet

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

Procedure

- In Cloudera Manager, select Ranger_KMS_KTS, then choose Configuration.
- On Configuration, in Search, type Ranger KMS with Key Trustee Server Service Environment Advanced Configuration Snippet.
- In RANGER_KMS_KTS_service_env_safety_valve, click + (Add).

The screenshot shows the Cloudera Manager Configuration page for the service RANGER_KMS_KTS-1. The 'Configuration' tab is active. A search bar contains the text 'safety_valve'. On the left, under 'Filters', the 'SCOPE' is set to 'RANGER_KMS_KTS-1 (Service-... 2' and the 'CATEGORY' is 'RANGER_KMS_KTS_service_env_safety_valve'. The main configuration area shows the snippet 'Ranger KMS with Key Trustee Server Service Environment Advanced Configuration Snippet (Safety Valve)' with a key-value pair 'RANGER_KMS_KTS_service_env_safety_valve'. The 'Key' field is empty and the 'Value' field is empty.

- Add a key-value pair that configures a JVM option for Ranger KMS KTS.

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 KTS service.

- 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 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`

Ranger Admin Advanced Configuration Snippet (Safety Valve) for `conf/ranger-admin-site.xml` [View as XML](#)

Ranger Admin Default Group [Undo](#)

Name	<input type="text" value="ranger.admin.init.purge.login_records"/>	🗑️ +
Value	<input type="text" value="true"/>	
Description	<input type="text"/>	
	<input type="checkbox"/> Final	
Name	<input type="text" value="ranger.admin.init.purge.login_records.retention.days"/>	🗑️ +
Value	<input type="text" value="5"/>	
Description	<input type="text"/>	

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: application/json" -X DELETE 'http://localhost:6080/service/public/v2/api/server/purge/records?type=login_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 add 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.

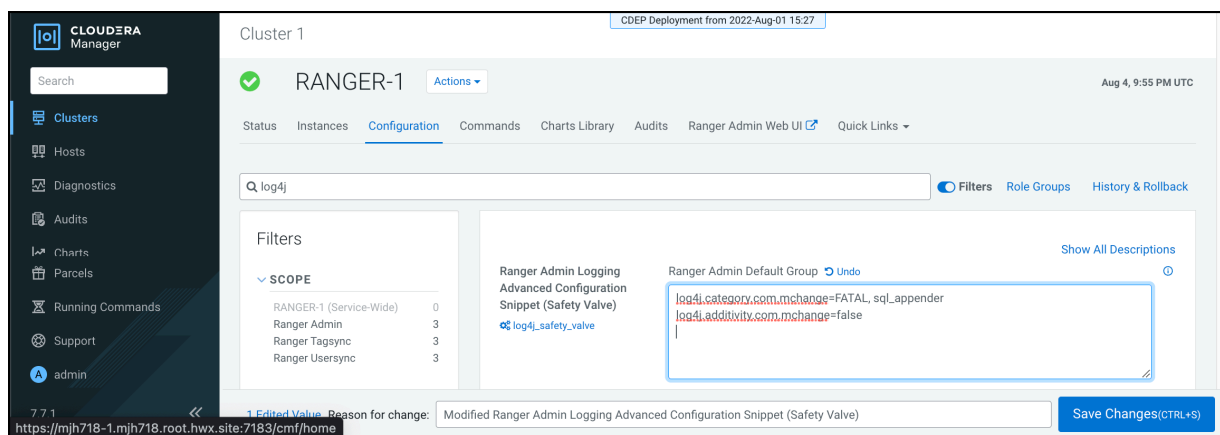
To limit the number of notifications to those that describe persistent db connections:

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)

- 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



- Click Save Changes.

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

- 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

- Set/export JAVA_HOME environment variable if not set.
`export JAVA_HOME=/usr/java/jdk1.8.0_232-cloudera`
- In the ranger-admin process run directory:
 - Find the proc.json file.
 - Search for HADOOP_CREDSTORE_PASSWORD.
 - Use that password to export it in the env variable.
`export HADOOP_CREDSTORE_PASSWORD=2fl2xmsd5zrp9homuqwww3it`
- 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/`
- Run the change password util command
`python changepasswordutil.py testuser1 Testuser1 Test12345`