

Cloudera Runtime 7.1.3

# Configuring Advanced Security Options for Apache Ranger

Date published: 2019-11-08

Date modified: 2020-08-10

# CLouDERA

<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

<b>Configure Kerberos authentication for Apache Ranger.....</b>	<b>4</b>
<b>Configure TLS/SSL for Apache Ranger.....</b>	<b>4</b>
<b>Configuring Apache Ranger High Availability.....</b>	<b>7</b>
Configure Ranger Admin High Availability.....	7
Configure Ranger Admin High Availability with a Load Balancer.....	11
<b>Configure Usersync assignment of Admin users.....</b>	<b>17</b>
<b>How to pass JVM options to Ranger services.....</b>	<b>18</b>
<b>How to pass JVM options to Ranger KMS services.....</b>	<b>19</b>

# 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.

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

## Related Information

[Enabling Kerberos Authentication for CDP](#)

# Configure TLS/SSL for Apache Ranger

How to configure TLS/SSL for Apache Ranger

## About this task

## Procedure

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

**Table 1: Apache Ranger TLS/SSL Settings**

Configuration Property	Description
Enable TLS/SSL for Ranger Admin <code>ranger.service.https.attrib.ssl.enabled</code>	Select this check box 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 <code>ranger.https.attrib.keystore.file</code>	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 format.
Ranger Admin TLS/SSL Server JKS Keystore File Password <code>ranger.service.https.attrib.keystore.pass</code>	The password for the Ranger Admin JKS keystore file.
Ranger Admin TLS/SSL Client Trust Store File <code>ranger.truststore.file</code>	The location on disk of the trust store, in .jks format, 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 trust store must contain the certificate(s) used to sign the connected service(s). If this parameter is not provided, the default list of well known certificate authorities is used.

Configuration Property	Description
Ranger Admin TLS/SSL Client Trust Store Password ranger.truststore.password	The password for the Ranger Admin TLS/SSL Certificate 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.
Enable TLS/SSL for Ranger Tagsync	Select this check box 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.clientsssl.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 format.
Ranger Tagsync TLS/SSL Server JKS Keystore File Password xasecure.policymgr.clientsssl.keystore.password	The password for the Ranger Tagsync JKS keystore file.
Ranger Tagsync TLS/SSL Client Trust Store Password xasecure.policymgr.clientsssl.truststore.password	The password for the Ranger Tagsync TLS/SSL Certificate 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.
Ranger Usersync TLS/SSL Client Trust Store File ranger.usersync.truststore.file	The location on disk of the trust store, 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 trust store must contain the certificate(s) used to sign the connected service(s). If this parameter is not provided, the default list of well 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 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. Click Save Changes.

5. In order for services to communicate successfully with Ranger, you must set the following properties in each service that has Ranger authorization enabled to ensure that the Ranger Admin certificate is imported into the trust store.

- TLS/SSL Client Trust Store File
- TLS/SSL Client Trust Store Password

For example, for HDFS select HDFS > Configuration in Cloudera Manager, then search for "HDFS NameNode TLS/SSL Client Trust Store", or use the Security Category to find and set the following properties:

- HDFS NameNode TLS/SSL Client Trust Store File
- HDFS NameNode TLS/SSL Client Trust Store Password



**Important:** Repeat this procedure for all services that have Ranger authorization enabled.

The screenshot shows the Cloudera Manager interface for configuring HDFS-1. The left sidebar contains navigation options like Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Private Cloud. The main area displays the configuration for HDFS-1, with the 'Configuration' tab selected. A search bar at the top of the configuration area contains the text 'HDFS NameNode TLS/SSL Client Trust Store'. Below the search bar, there are filters for SCOPE, CATEGORY, and STATUS. The SCOPE filter shows 'HDFS-1 (Service-Wide)' selected. The CATEGORY filter shows 'Security' selected. The STATUS filter shows 'Warning' selected. The configuration table shows two properties: 'HDFS NameNode TLS/SSL Client Trust Store File' and 'HDFS NameNode TLS/SSL Client Trust Store Password'. Both properties are set to 'NameNode Default Group' and have an 'Undo' button. The 'Client Trust Store File' property has a value of '/etc/hadoop/conf/ranger-plugin-truststore.jks'. The 'Client Trust Store Password' property has a masked value '.....'. At the bottom of the configuration area, there is a 'Save Changes (CTRL+S)' button and a 'Reason for change' field containing 'Modified HDFS NameNode TLS/SSL Client Trust Store File, HDFS NameNode'.

6. Click Save Changes.

# Configuring Apache Ranger High Availability

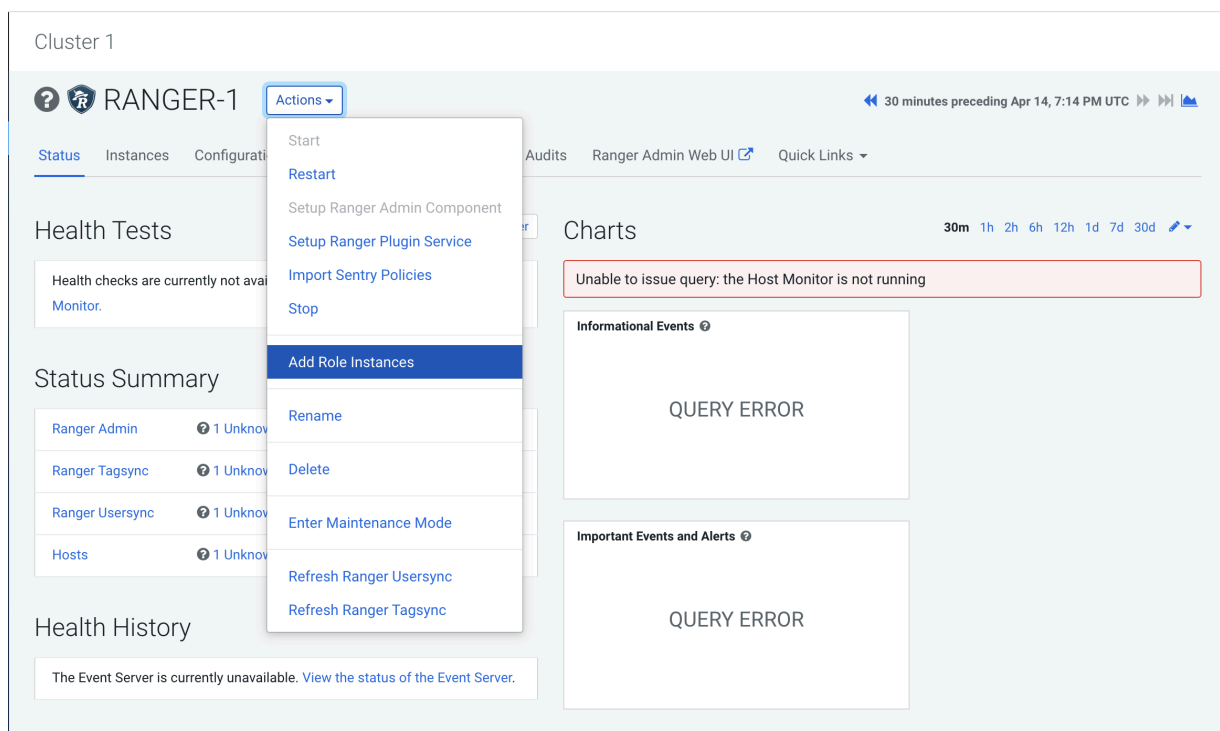
How to configure High Availability (HA) for Apache Ranger.

## Configure Ranger Admin High Availability

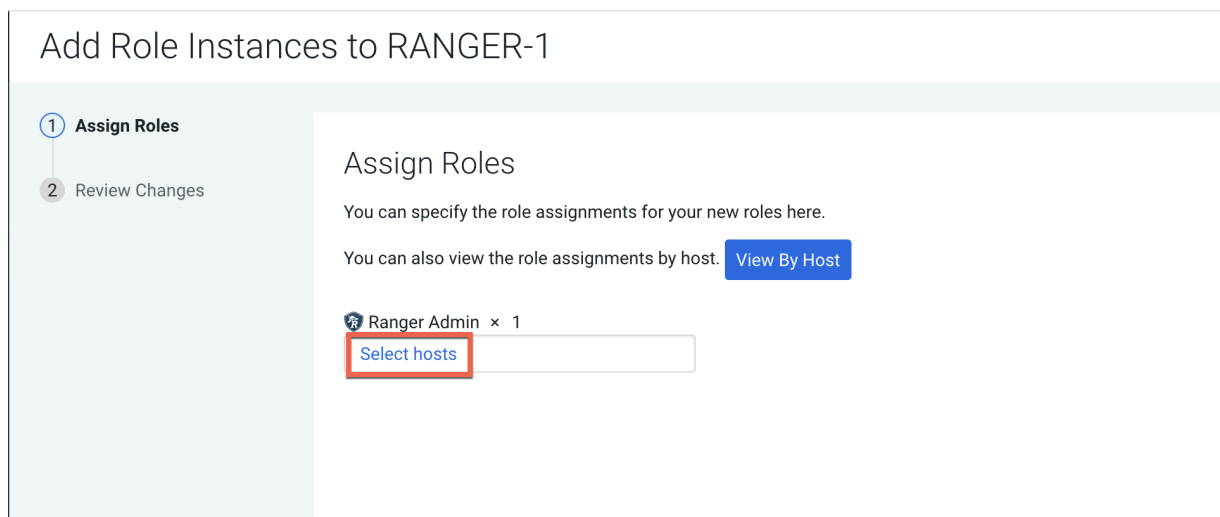
How to configure Ranger Admin High Availability (HA) by adding additional Ranger Admin role instances.

### Procedure

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



2. On the Add Role Instances page, click Select hosts.



- On the selected hosts page, the primary Ranger Admin host is selected by default. Select a backup Ranger host. A Ranger Admin (RA) icon appears in the Added Roles column 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.

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 G	
<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 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 G, ID G, KB TS, G G, G G, NM	

1 - 3 of 3

Cancel OK

- The Add Role Instances page is redisplayed with 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



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

### Add Role Instances to RANGER-1

**Assign Roles**

**Review Changes**

#### Review Changes

<b>Maximum Shards for Solr Collection of Ranger Audits</b> ranger.audit.solr.max.shards.per.node	Ranger Admin Default Group	<input type="text" value="1"/>	?
<b>Replicas for Solr Collection of Ranger Audits</b> ranger.audit.solr.no.replica	Ranger Admin Default Group	<input type="text" value="1"/>	?
<b>Shards for Solr Collection of Ranger Audits</b> ranger.audit.solr.no.shards	Ranger Admin Default Group	<input type="text" value="1"/>	?
<b>Ranger Database Host</b> ranger_database_host	Ranger Admin Default Group	<input type="text" value="cloudera10011-0000000001-cloudera10011-site"/>	?
<b>Ranger Database Name</b> ranger_database_name	Ranger Admin Default Group	<input type="text" value="ranger1"/>	?
<b>Ranger Database User Password</b> ranger.jpa.jdbc.password	Ranger Admin Default Group	<input type="password" value="....."/>	?
<b>Ranger Database Type</b> 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	?
<b>Ranger Database User</b> ranger.jpa.jdbc.user	Ranger Admin Default Group	<input type="text" value="rangeradmin"/>	?
<b>Ranger Admin TLS/SSL Client Trust Store File</b> ranger.truststore.file	Ranger Admin Default Group	<input type="text"/>	?
<b>Ranger Admin TLS/SSL Client Trust Store Password</b> ranger.truststore.password	Ranger Admin Default Group	<input type="text"/>	?
<b>Enable TLS/SSL for Ranger</b>	<input type="checkbox"/> Ranger Admin Default Group		?

## 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 Command needed

Status Instances Configuration Audits Ranger Admin Web UI Quick Links

Health Tests 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

## 7. 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 are automatically rerouted 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`.

CLUSTER MANAGER

Cluster 1 CDEP Deployment from 2021-Feb-17 09:37

RANGER-1 Actions

Web UI Quick Links

Ranger Admin Web UI (c...-2-1)

Ranger Admin Web UI (c...-2)

Health Tests Show 3 Good

Status Summary

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

Health History

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	
Ranger Admin Health Concerning	

Informational Events

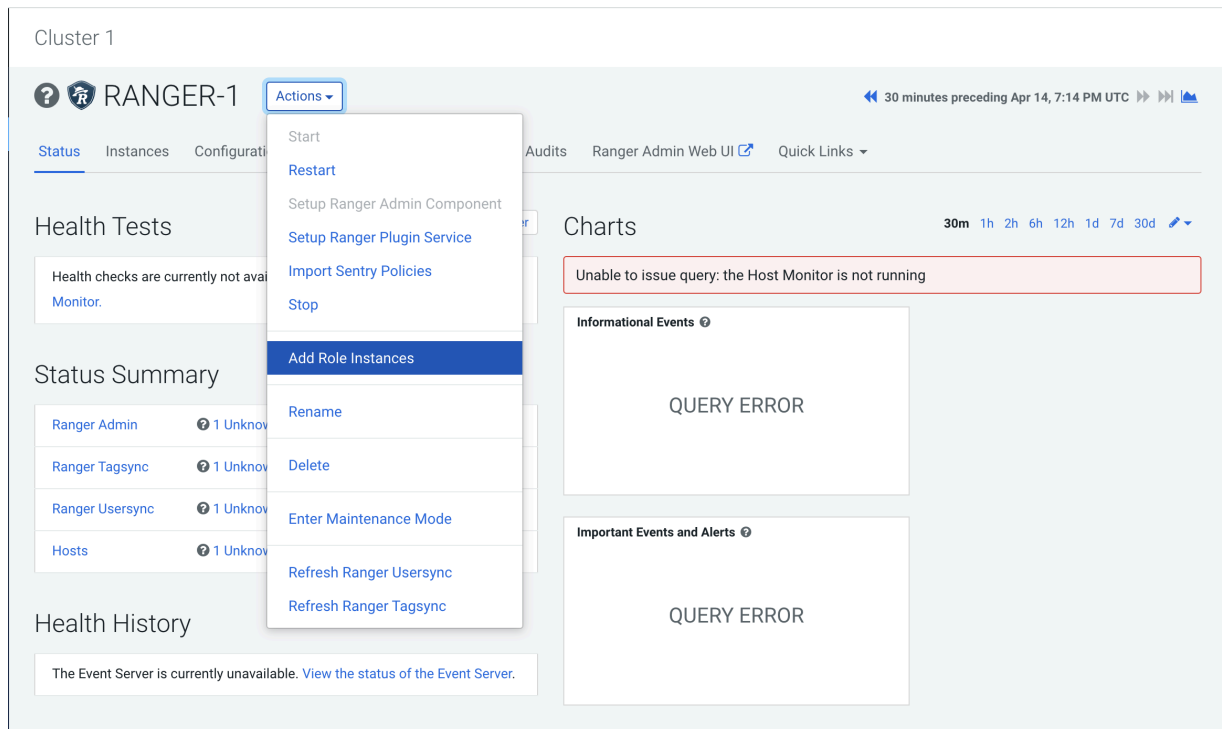
Important Events and Alerts

## Configure Ranger Admin High Availability with a Load Balancer

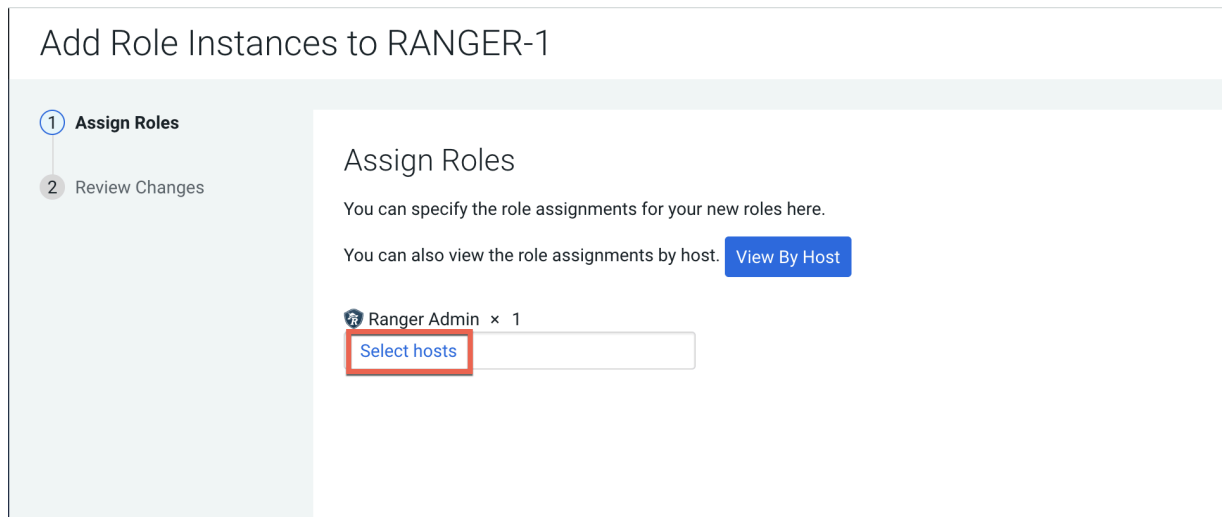
For clusters that have multiple users and production availability requirements, you may want to configure Ranger high availability (HA) with a load-balancing proxy server to relay requests to and from Ranger.

### Procedure

1. Configure an external load balancer to use with Ranger HA.
2. In Cloudera Manager, select Ranger, then select Actions > Add Role Instances.



3. On the Add Role Instances page, click Select hosts.



- On the selected hosts page, 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 the Added Roles column 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.

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	RA RT
<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 G ID G KB TS G G G NM	

1 - 3 of 3

Cancel
OK

- The Add Role Instances page is redisplayed with 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

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

### Add Role Instances to RANGER-1

Assign Roles

**Review Changes**

#### Review Changes

<p><b>Maximum Shards for Solr Collection of Ranger Audits</b> ranger.audit.solr.max.shards.per.node</p>	<p>Ranger Admin Default Group</p> <input type="text" value="1"/>	?
<p><b>Replicas for Solr Collection of Ranger Audits</b> ranger.audit.solr.no.replica</p>	<p>Ranger Admin Default Group</p> <input type="text" value="1"/>	?
<p><b>Shards for Solr Collection of Ranger Audits</b> ranger.audit.solr.no.shards</p>	<p>Ranger Admin Default Group</p> <input type="text" value="1"/>	?
<p><b>Ranger Database Host</b> ranger_database_host</p>	<p>Ranger Admin Default Group <a href="#">↩</a></p> <input type="text" value="cloudera.com:22111:cloudera.com:22111:cloudera.com:22111"/>	?
<p><b>Ranger Database Name</b> ranger_database_name</p>	<p>Ranger Admin Default Group <a href="#">↩</a></p> <input type="text" value="ranger1"/>	?
<p><b>Ranger Database User Password</b> ranger.jpa.jdbc.password</p>	<p>Ranger Admin Default Group <a href="#">↩</a></p> <input type="password" value="....."/>	?
<p><b>Ranger Database Type</b> ranger_database_type</p>	<p>Ranger Admin Default Group</p> <p> <input type="radio"/> MySQL  <input type="radio"/> Oracle  <input checked="" type="radio"/> PostgreSQL  <input type="radio"/> MsSQL  <input type="radio"/> SQLA         </p>	?
<p><b>Ranger Database User</b> ranger.jpa.jdbc.user</p>	<p>Ranger Admin Default Group</p> <input type="text" value="rangeradmin"/>	?
<p><b>Ranger Admin TLS/SSL Client Trust Store File</b> ranger.truststore.file</p>	<p>Ranger Admin Default Group</p> <input type="text"/>	?
<p><b>Ranger Admin TLS/SSL Client Trust Store Password</b> ranger.truststore.password</p>	<p>Ranger Admin Default Group</p> <input type="text"/>	?
<p><b>Enable TLS/SSL for Ranger</b></p>	<p><input type="checkbox"/> Ranger Admin Default Group</p>	?

- 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.

- 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.

9. 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/keytabs/ranger.ha.keytab` file has entries for all of the 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
```

10. Update the following ranger-admin-site.xml configuration settings using the Safety Valve.

```
ranger.spnego.kerberos.keytab=/etc/security/keytabs/ranger.ha.keytab
ranger.spnego.kerberos.principal=*
```

The screenshot displays the Cloudera Ranger Admin console for instance RANGER-1. The 'Configuration' tab is active, and a search for 'Safety Valve' is performed. The configuration editor shows two configuration items:

- Item 1:** Name: `ranger.spnego.kerberos.keytab`, Value: `/etc/security/keytabs/ranger.ha.keytab`. It includes a description field and a 'Final' checkbox.
- Item 2:** Name: `ranger.spnego.kerberos.principal`, Value: `*`. It includes a description field and a 'Final' checkbox.

The status bar at the bottom indicates '1 Edited Value' and provides a 'Reason for change' field with the text 'Modified Ranger Admin Advanced Configuration Snippet (Safety Valve) for conf/ranger-admin-site.xml'. A 'Save Changes(CTRL+S)' button is also present.



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

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

## Configure Usersync assignment of Admin users

How to automatically assign Admin and Key Admin roles for external users

### About this task

Usersync pulls in users/groups from your external user repository, such as LDAP/AD, and populates the Ranger database with these users/groups. Use this procedure to automatically assign roles to specific users/groups. The example properties shown in this topic automatically assign the ADMIN/KEYADMIN role .

### Procedure

1. In Search, type `role.assignmentnet`.

- In Ranger Usersync Default Group: verify that the following default delimiter values appear for each property:

Property Name	Delimiter Value
ranger.usersync.role.assignment.list.delimiter	&
ranger.usersync.users.groups.assignment.list.delimiter	:
ranger.usersync.username.groupname.assignment.list.delimiter	,
ranger.usersync.group.based.role.assignment.rules	

- In Ranger UserSync Group Based Role Assignment Rules, type the following value as one string:  
 ROLE\_SYS\_ADMIN:u:User1,User2&ROLE\_SYS\_ADMIN:g:Group1,Group2&  
 ROLE\_KEY\_ADMIN:u:kmsUser&ROLE\_KEY\_ADMIN:g:kmsGroup&  
 ROLE\_USER:u:User3,User4&ROLE\_USER:g:Group3,Group4&  
 ROLE\_ADMIN\_AUDITOR:u:auditorUsers,auditors&  
 ROLE\_ADMIN\_AUDITOR:g:adminAuditorGroup,rangerAuditors&  
 ROLE\_KEY\_ADMIN\_AUDITOR:u:kmsAuditors&ROLE\_KEY\_ADMIN\_AUDITOR:g:kmsAuditorGroup  
 where "u" indicates user and "g" indicates group
- Click Save Changes (CTRL+S).
- If Usersync requires no other changes, choose Actions Restart Usersync .

## How to pass JVM options to Ranger services

You can pass JVM options to 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. To pass JVM Options to 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

- In Cloudera Manager Home, select Ranger, then choose Configuration.
- On Configuration, in Search, type Ranger Service Environment Advanced Configuration Snippet.
- In RANGER\_service\_env\_safety\_valve, click + (Add).
- 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.

### 5. Click Save Changes.

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

The screenshot shows the Cloudera Manager interface for Cluster 1. The left sidebar contains navigation options like Clusters, Hosts, Diagnostics, Audits, Charts, Replication, Administration, and Experiences. The main content area displays the configuration for RANGER-1. A search bar contains 'Ranger Service Environment Advanced Configuration Snippet'. The configuration is categorized by SCOPE (RANGER-1 (Service-Wide) with 1 instance) and STATUS (Non-Default with 1 instance). The configuration snippet for 'RANGER\_service\_env\_safety\_valve' is shown with a key 'JAVA\_OPTS' and a value '-XX:ErrorFile=file.log'. A tooltip indicates that a stale configuration needs to be restarted.

### 6. 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

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. To pass JVM Options to a specific role level, search and edit the following 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 Home, 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).

- 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.

- Click Save Changes.

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

The screenshot shows the Cloudera Manager interface for Cluster 1. The configuration page for RANGER\_KMS-1 is displayed, showing the configuration snippet for RANGER\_KMS\_service\_env\_safety\_valve. The key is JAVA\_OPTS and the value is -XX:ErrorFile=file.log. A tooltip indicates that the configuration is stale and needs to be restarted. The interface also shows a search bar, filters, and a status section.

- Select Actions Restart .