

Cloudera Runtime 7.2.13

Ranger Authorization

Date published: 2020-07-28

Date modified: 2021-12-13

The Cloudera logo is displayed in a bold, orange, sans-serif font. The word "CLOUDERA" is written in all caps, with a stylized 'E' that has a horizontal bar extending to the right.

<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

Using Ranger to Provide Authorization in CDP.....	5
Ranger special entities.....	5
Ranger Policies Overview.....	6
Ranger tag-based policies.....	6
Tags and policy evaluation.....	7
Ranger access conditions.....	8
Using the Ranger Console.....	10
Accessing the Ranger console.....	11
Ranger console navigation.....	12
Resource-based Services and Policies.....	15
Configuring resource-based services.....	15
Configure a resource-based service: Atlas.....	16
Configure a resource-based service: HBase.....	17
Configure a resource-based service: HDFS.....	19
Configure a resource-based service: HadoopSQL.....	21
Configure a resource-based service: Kafka.....	23
Configure a resource-based service: Knox.....	25
Configure a resource-based service: NiFi.....	27
Configure a resource-based service: NiFi Registry.....	29
Configure a resource-based service: Solr.....	31
Configure a resource-based service: YARN.....	33
Configuring resource-based policies.....	35
Configure a resource-based policy: Atlas.....	36
Configure a resource-based policy: HBase.....	37
Configure a resource-based policy: HDFS.....	40
Configure a resource-based policy: HadoopSQL.....	42
Configure a resource-based storage handler policy: HadoopSQL.....	46
Configure a resource-based policy: Kafka.....	49
Configure a resource-based policy: Knox.....	51
Configure a resource-based policy: NiFi.....	52
Configure a resource-based policy: NiFi Registry.....	54
Configure a resource-based policy: Solr.....	56
Configure a resource-based policy: YARN.....	58
Wildcards and variables in resource-based policies.....	60
Preloaded resource-based services and policies.....	61
Importing and exporting resource-based policies.....	67
Import resource-based policies for a specific service.....	69
Import resource-based policies for all services.....	71
Export resource-based policies for a specific service.....	74
Export all resource-based policies for all services.....	75
Row-level filtering and column masking in Hive.....	77

Row-level filtering in Hive with Ranger policies.....	77
Dynamic resource-based column masking in Hive with Ranger policies.....	81
Dynamic tag-based column masking in Hive with Ranger policies.....	85
Tag-based Services and Policies.....	89
Adding a tag-based service.....	89
Adding tag-based policies.....	90
Using tag attributes and values in Ranger tag-based policy conditions.....	93
Adding a tag-based PII policy.....	95
Default EXPIRES ON tag policy.....	99
Importing and exporting tag-based policies.....	102
Import tag-based policies.....	104
Export tag-based policies.....	106
Create a time-bound policy.....	108
Create a Hive authorizer URL policy.....	110
Ranger Security Zones.....	113
Security Zones Administration.....	113
Security Zones Example Use Cases.....	114
Adding a Ranger security zone.....	115
Administering Ranger Users, Groups, Roles, and Permissions.....	119
Add a user.....	121
Edit a user.....	122
Delete a user.....	124
Add a group.....	125
Edit a group.....	126
Delete a group.....	128
Add a role through Ranger.....	129
Add a role through Hive.....	131
Edit a role.....	133
Delete a role.....	135
Add or edit permissions.....	135
Administering Ranger Reports.....	137
View Ranger reports.....	137
Search Ranger reports.....	138
Export Ranger reports.....	139
Using Ranger client libraries.....	140
Using session cookies to validate Ranger policies.....	141

Using Ranger to Provide Authorization in CDP

Apache Ranger manages access control through a user interface that ensures consistent policy administration across Cloudera Data Platform (CDP) components. Security administrators can define security policies at the database, table, column, and file levels, and can administer permissions for specific LDAP-based groups or individual users. Rules based on dynamic conditions such as time or geolocation can also be added to an existing policy rule. The Ranger authorization model is pluggable and can be easily extended to any data source using a service-based definition.

Once a user has been authenticated, their access rights must be determined. Authorization defines user access rights to resources. For example, a user may be allowed to create a policy and view reports, but not allowed to edit users and groups. You can use Ranger to set up and manage access to Hadoop services.

Ranger enables you to create services for specific resources (HDFS, HBase, Hive, etc.) and add access policies to those services. Ranger security zones enable you to organize service resources into multiple security zones. You can also create tag-based services and add access policies to those services. Using tag-based policies enables you to control access to resources across multiple components without creating separate services and policies in each component. You can also use Ranger TagSync to synchronize the Ranger tag store with an external metadata service such as Apache Atlas.

**Note:**

You can configure authorization using the Ranger UI, REST APIs, or client libraries. For more information about:

- Ranger REST APIs, see <https://ranger.apache.org/apidocs/index.html>.
- Ranger client libraries, see [Using Ranger client libraries](#) on page 140.

Ranger special entities

Ranger in CDP has specific, internal groups and entities that affect user authorization and access to all services in CDP.

In addition to any users, group, roles and permissions that you define using Ranger, you must understand the following Ranger special entities:

"public" group

A special, internal group within Ranger that consists of all users, including future users. Membership is implicit and automatic.



Note: All users belong to "public" group. Any policies granted to this group provide access to everyone.

The following, default policies give permissions to members of group "public":

- all - database > public > create permission
- default database tables columns > public > create permission
- Information_schema database tables columns > public > select permission

You can remove "public" from these default policies to further restrict user access, based on your security requirements.

{OWNER} special entity

A special Ranger entity attached to a user based on their actions. For example, when a user "bob" creates a table, "bob" becomes the {OWNER} of that table and would get any permissions provided to {OWNER} on that table across all the policies. The following default policies have permissions for {OWNER}:

- all - database, table, column > {OWNER} > all permissions
- all - database, table > {OWNER} > all permissions
- all - database, udf > {OWNER} > all permissions
- all - database > {OWNER} > all permissions

Although not recommended, you can modify access to special entity {OWNER}, based on your security requirements. Removing the default {OWNER} permissions may require adding additional, specific policies for each object owner, which may increase your policy management operational burden.

Ranger Policies Overview

Ranger has two types of policies: resource-based and tag-based.

Resource-based policies

Ranger enables you to configure resource-based services (HDFS, HBase, Hive, etc.) and add access policies to those services.

Tag-based policies

Ranger enables you to create tag-based services and add access policies to those services.

Ranger tag-based policies

Ranger enables you to create tag-based services and add access policies to those services.

Tag-Based Policies Overview

- An important feature of Ranger tag-based authorization is the separation of resource-classification from access-authorization. For example, resources (HDFS file/directory, Hive database/table/column etc.) containing sensitive data such as social security numbers, credit card numbers, or sensitive health care data can be tagged with PII/PCI/PHI – either as the resource enters the Hadoop ecosystem or at a later time. Once a resource is tagged, the authorization for the tag would be automatically enforced, thus eliminating the need to create or update policies for the resource.
- Using tag-based policies also enables you to control access to resources across multiple Hadoop components without creating separate services and policies in each component.
- Tag details are stored in a tag store. Ranger TagSync can be used to synchronize the tag store with an external metadata service such as Apache Atlas.

Tag Store

Details of tags associated with resources are stored in a tag store. Apache Ranger plugins retrieve the tag details from the tag store for use during policy evaluation. To minimize the performance impact during policy evaluation (in finding tags for resources), Apache Ranger plugins cache the tags and periodically poll the tag store for any changes. When a change is detected, the plugins update the cache. In addition, the plugins store the tag details in a local cache file – just as the policies are stored in a local cache file. On component restart, the plugins will use the tag data from the local cache file if the tag store is not reachable.

Apache Ranger plugins download the tag details from the store managed by Ranger Admin. Ranger Admin persists the tag details in its policy store and provides a REST interface for the plugins to download the tag details.

Tags

Ranger Tags can have attributes. Tag attribute values can be used in Ranger tag-based policies to influence the authorization decision.

For example, to deny access to a resource after a specific date:

1. Add the EXPIRES_ON tag to the resource.
2. Add an expiry_date tag attribute and set its value to the expiry date.
3. Create a Ranger policy for the EXPIRES_ON tag.
4. Add a condition in this policy to deny access when the date specified the in expiry_date tag attribute is later than the current date.

Note that the EXPIRES_ON tag policy is created as the default policy in tag service instances.

TagSync

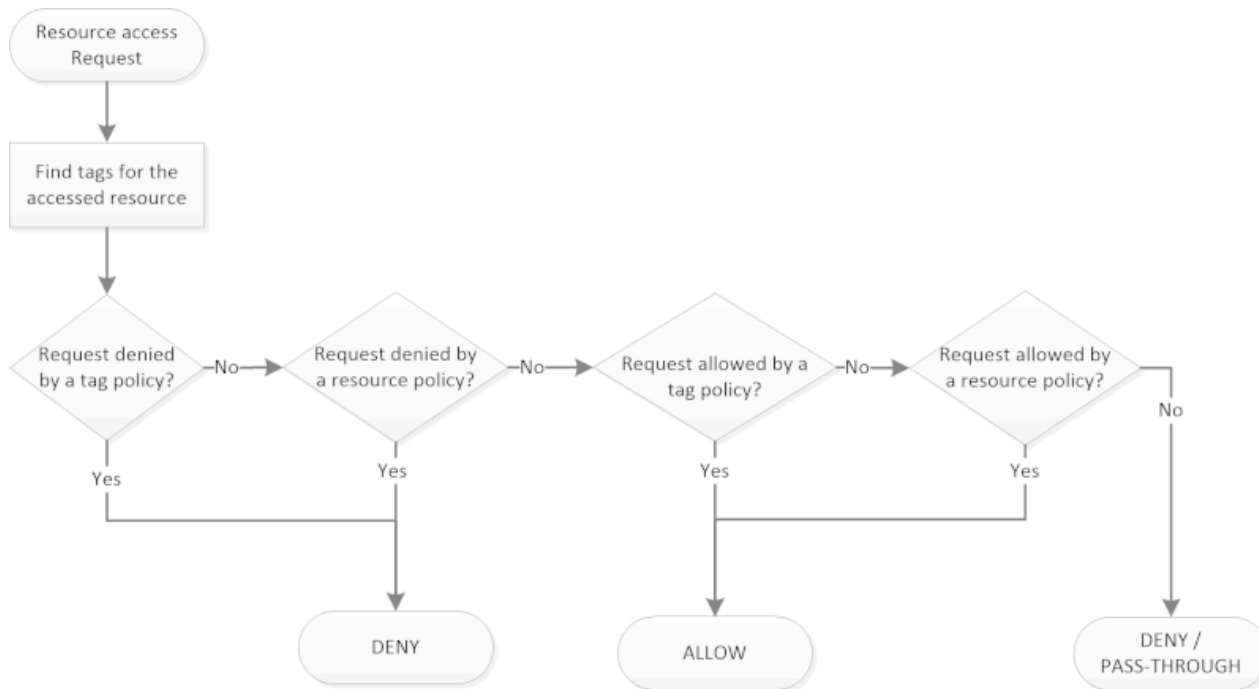
Ranger TagSync is used to synchronize the tag store with an external metadata service such as Apache Atlas. TagSync is a daemon process similar to the Ranger UserSync process.

Ranger TagSync receives tag details from Apache Atlas via change notifications. As tags are added to, updated, or deleted from resources in Apache Atlas, Ranger TagSync receives notifications and updates the tag store.

Tags and policy evaluation

When authorizing an access request, an Apache Ranger plugin evaluates applicable Ranger policies for the resource being accessed. The following diagram shows the details of the policy evaluation flow. More details on the steps in this workflow are provided in the subsequent sections.

Apache Ranger Policy Evaluation Flow with Tags



Apache Ranger Policy Evaluation Flow with Tags

Finding Tags

Apache Ranger supports a service to register context enrichers, which are used to update context data to the access request.

The Ranger Tag service, which is part of the tag-based policies feature, adds a context enricher named `RangerTagEnricher`. This context enricher is responsible for finding tags for the requested resource and adding the tag details to the request context. This context enricher keeps a cache of the available tags; while processing an access request, it finds the tags applicable for the requested resource and adds the tags to the request context. The context enricher keeps the cache updated by periodically polling Ranger Admin for changes.

Evaluating Tag-Based Policies

Once the list of tags for the requested resource is found, the Apache Ranger policy engine evaluates the tag-based policies applicable to the tags. If a policy for one of these tag results in a deny, access will be denied. If none of the tags are denied, and if a policy allows for one of the tags, access will be allowed. If there is no result for any tag, or if there are no tags for the resource, the policy engine will evaluate the resource-based policies to make the authorization decision.

Using Tags in Conditions

Apache Ranger allows the use of custom conditions while evaluating authorization policies. The Apache Ranger policy engine makes various request details – such as user, groups, resource, and context – available to the conditions. Tags in the request context, which are added by the enricher, are available to the conditions and can be used to influence the authorization decision.

The default policy in tag service instances, the `EXPIRES_ON` tag, uses such condition to check to see if the request date is later than the value specified in tag attribute `expiry_date`. This default policy does not work unless an `EXPIRES_ON` tag has been created in Atlas.

Related Information

[Apache Ranger Wiki > Context Enrichers](#)

Ranger access conditions

The Apache Ranger access policy model consists of two major components: specification of the resources a policy is applied to, such as HDFS files and directories, Hive databases, tables, and columns, HBase tables, column-families, and columns, and so on; and the specification of access conditions for specific users and groups

Allow Deny and Exclude Conditions

Apache Ranger supports the following access conditions:

- Allow
- Exclude from Allow
- Deny
- Exclude from Deny

These access conditions enable you to set up fine-grained access control policies.

For example, you can allow access to a "finance" database to all users in the "finance" group, but deny access to all users in the "interns" group. Let's say that one of the members of the "interns" group, "scott", needs to work on an assignment that requires access to the "finance" database. In that case, you can add an Exclude from Deny condition that will allow user "scott" to access the "finance" database. The following image shows how this policy would be set up in Apache Ranger:

Policy Details :

Policy ID **15**

Policy Name * enabled

Hive Database * Include

table * Include **Resource**

Hive Column * Include

Description

Audit Logging YES

Allow Conditions :

Select Group	Select User	Permissions	Delegate Admin	
<input type="text" value="finance"/>	<input type="text" value="Select User"/>	<input type="checkbox"/> All <input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Exclude from Allow Conditions :

Deny Conditions :

Select Group	Select User	Permissions	Delegate Admin	
<input type="text" value="interns"/>	<input type="text" value="Select User"/>	<input type="checkbox"/> All <input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

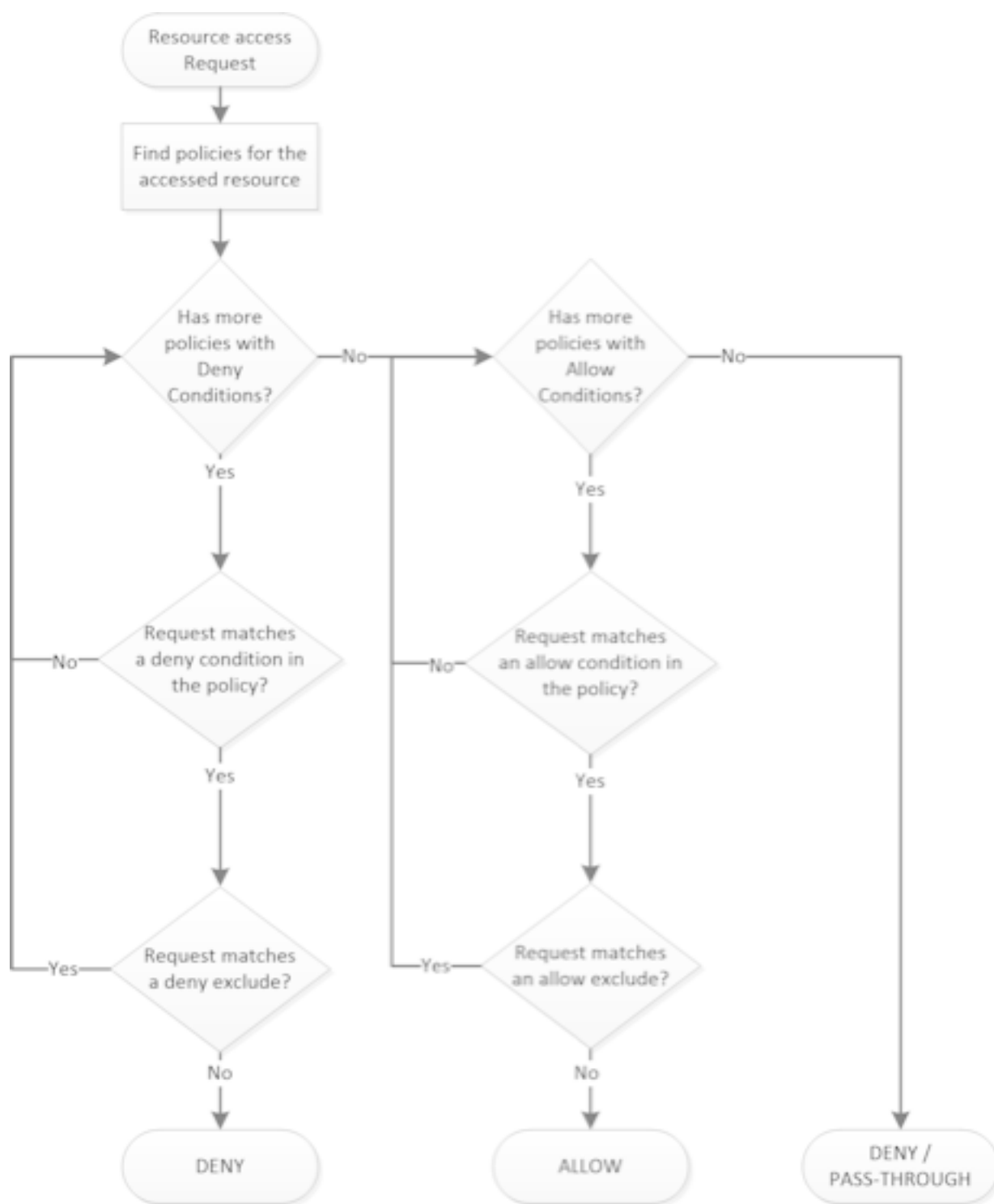
Exclude from Deny Conditions :

Select Group	Select User	Permissions	Delegate Admin	
<input type="text" value="Select Group"/>	<input type="text" value="SCOR"/>	<input type="checkbox"/> select <input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Deny Excludes

Policy Evaluation of Access Conditions

Apache Ranger policies are evaluated in a specific order to ensure predictable results (if there is no access policy that allows access, the authorization request will typically be denied). The following diagram shows the policy evaluation work-flow:



Apache Ranger Policy Evaluation Flow

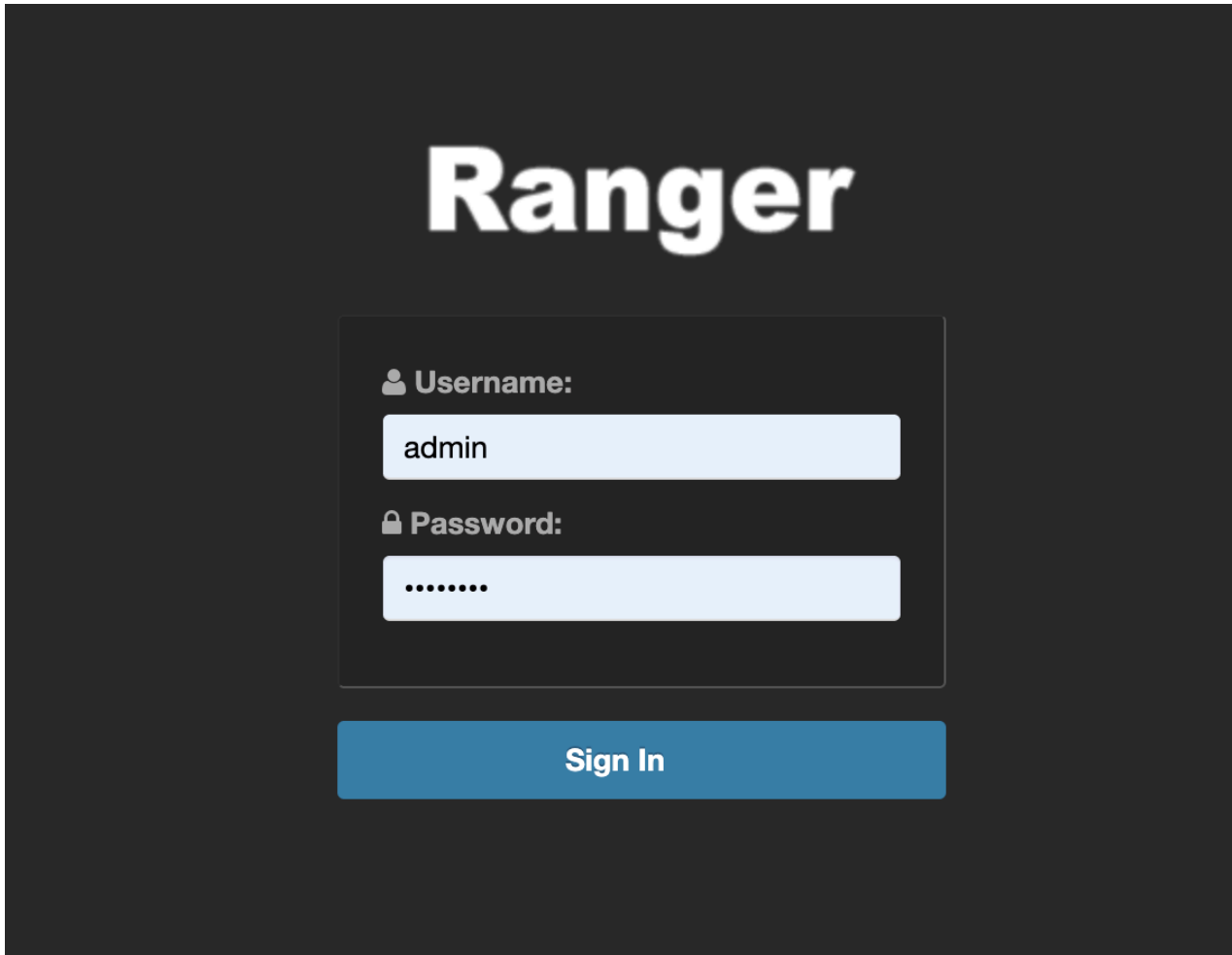
Using the Ranger Console

This chapter contains an overview of the Ranger console.

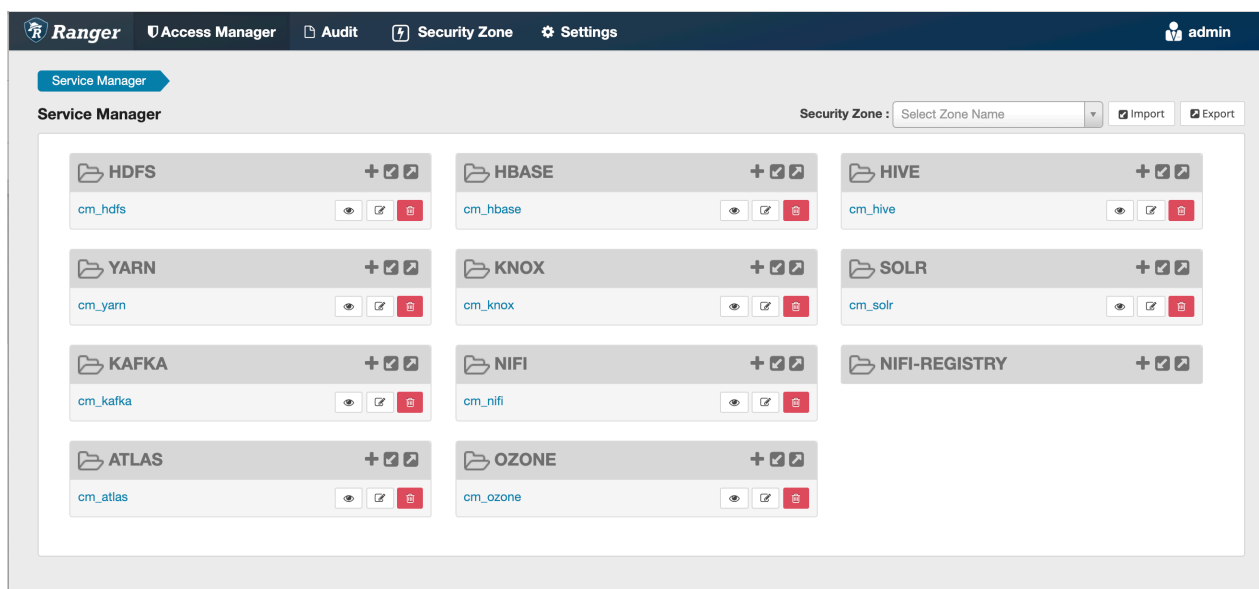
Accessing the Ranger console

How to access the Ranger console.

To access the Ranger Console, click the Ranger Admin web UI link, enter your user name and password, then click Sign In.

The image shows the Ranger Console Home Page. At the top, the word "Ranger" is displayed in a large, white, sans-serif font against a dark background. Below this, there is a login form with a dark background and light-colored text and input fields. The form contains two labels: "Username:" with a person icon and "Password:" with a lock icon. The Username input field contains the text "admin". The Password input field contains seven dots. Below the input fields is a blue button with the text "Sign In" in white.

Ranger Console Home Page

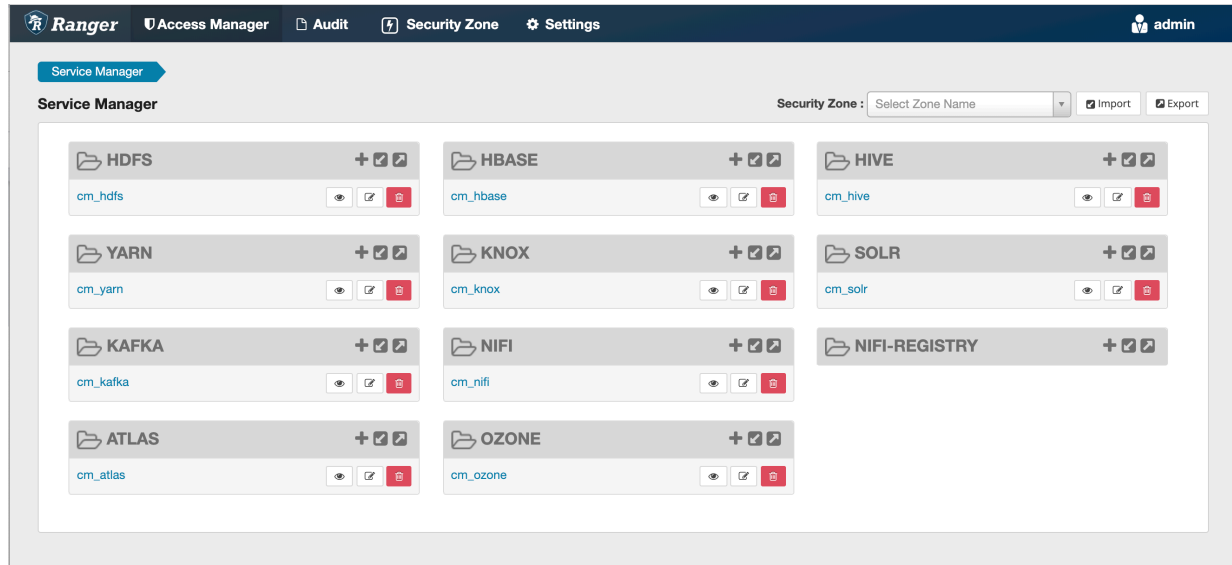


After you log in, your user name is displayed at the top right of the Ranger Console.

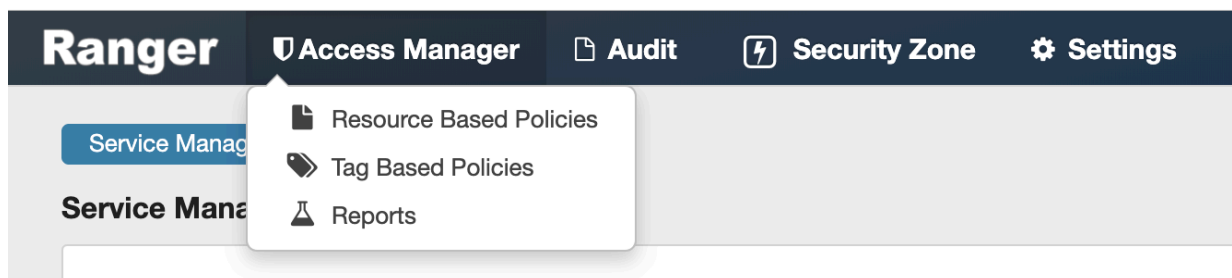
Ranger console navigation

Explains the basic Ranger console/GUI.

- The Service Manager for Resource Based Policies page is displayed when you log in to the Ranger Console. You can use this page to create services for Hadoop resources (HDFS, HBase, Hive, etc.) and add access policies to those resources.

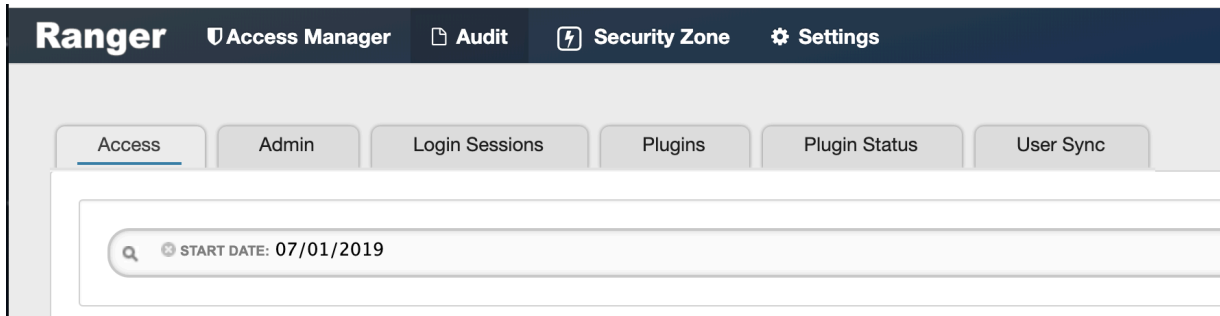


Clicking Access Manager in the top menu opens the Service Manager for Resource Based Policies page, and also displays a submenu with links to Resource Based Policies, Tag Based Policies, and Reports (this submenu is also displayed when you pass the mouse over the Access Manager link).

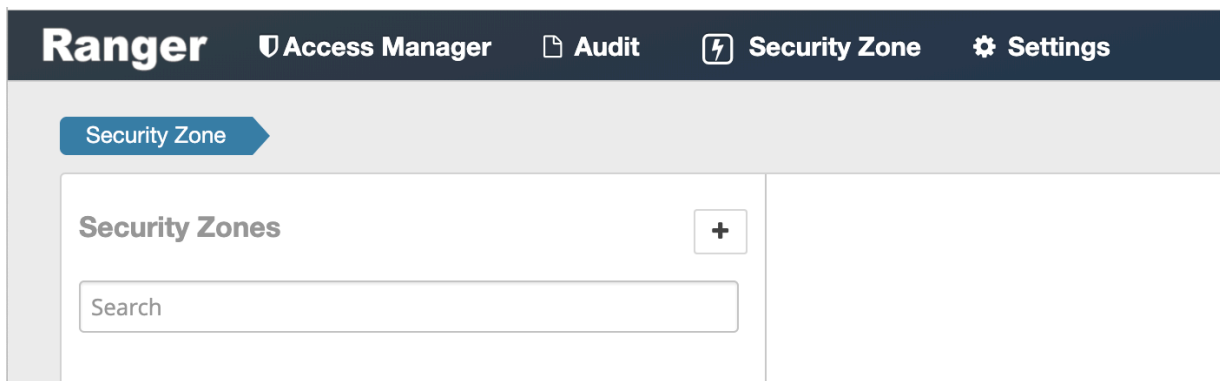


- Access Manager > Resource Based Policies -- Opens the Service Manager for Resource Based Policies page. You can use this page to create services for resources (HDFS, HBase, Hive, etc.) and add access policies to those services.
- Access Manager > Tag Based Policies -- Opens the Service Manager for Tag Based Policies page. You can use this page to create tag-based services and add access policies to those services. Using tag-based policies enables you to control access to resources across multiple components without creating separate services and policies in each component.
- Access Manager > Reports -- Opens the Reports page. You can use this page to generate user access reports for resource and tag-based policies based on search criteria such as policy name, resource, group, and user name.

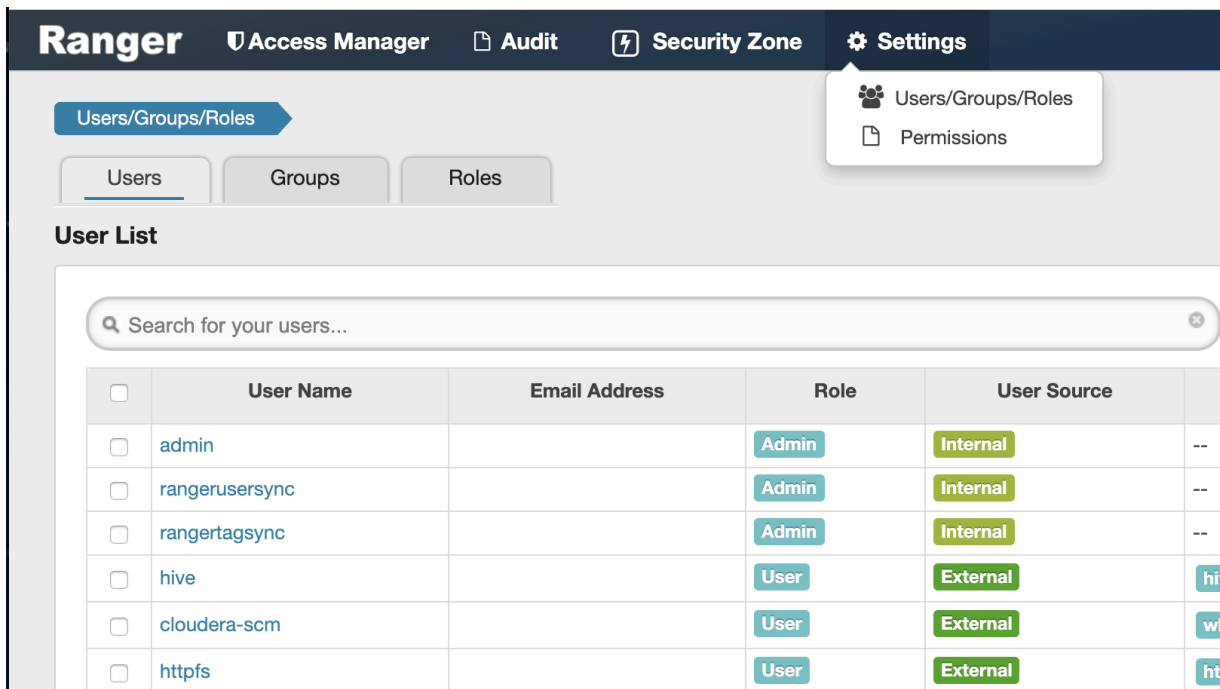
- Audit -- You can use the Audit page to monitor user activity at the resource level, and also to set up conditional auditing based on users, groups, or time. The Audit page includes the Access, Admin, Login Sessions, Plugins, Plugin Status, and User Sync tabs.



- Security Zone -- Lets you organize resource and tag-based services and policies into separate security zones. You can assign one or more administrators for each security zone. Security zone administrators can then create and update policies for their security zone.



- Settings -- Enables you to manage and assign policy permissions to users and groups. Clicking or passing the mouse over Settings displays a submenu with links to the Users/Groups/Roles and Permissions pages.






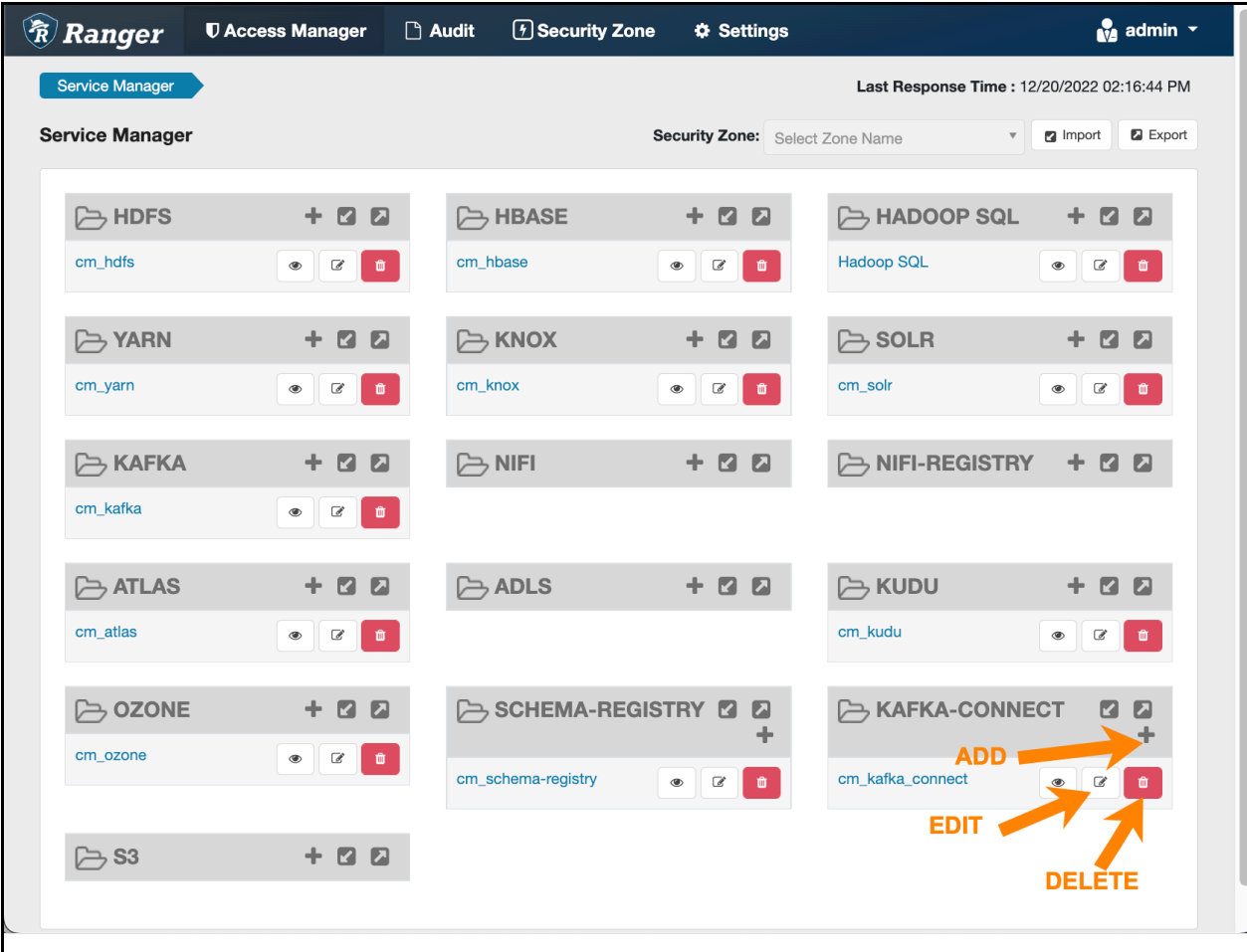
Resource-based Services and Policies

Ranger enables you to configure resource-based services for Hadoop components (e.g. HBase, Kafka, Storm, etc.) and add access policies to those services.

Configuring resource-based services

The Service Manager for Resource Based Policies page displays when you log in to the Ranger Admin Web UI. You can also access this page by selecting **Access Manager** **Resource Based Policies**. You can use this page to create services for Hadoop resources (HDFS, HBase, HadoopSQL, etc.) and add access policies to those resources.

- To add a new resource-based service, click the Add icon () in the applicable box on the Service Manager page. Enter the required configuration settings, then click Add.
- To edit a resource-based service, click the Edit icon () at the right of the service. Edit the service settings, then click Save to save your changes.
- To delete a resource-based service, click the Delete icon () at the right of the service. Deleting a service also deletes all of the policies for that service.




The screenshot shows the Ranger Service Manager interface. At the top, there is a navigation bar with the Ranger logo, 'Access Manager', 'Audit', 'Security Zone', and 'Settings' tabs, and a user profile 'admin'. Below the navigation bar, the 'Service Manager' section is displayed. It includes a 'Security Zone' dropdown menu set to 'Select Zone Name', and 'Import' and 'Export' buttons. The main area contains a grid of service cards for various Hadoop components. Each card has a plus icon for adding, an eye icon for visibility, a pencil icon for editing, and a trash can icon for deleting. Orange arrows point to the plus, pencil, and trash can icons for the 'KAFKA-CONNECT' service, with labels 'ADD', 'EDIT', and 'DELETE' respectively.

Configure a resource-based service: Atlas

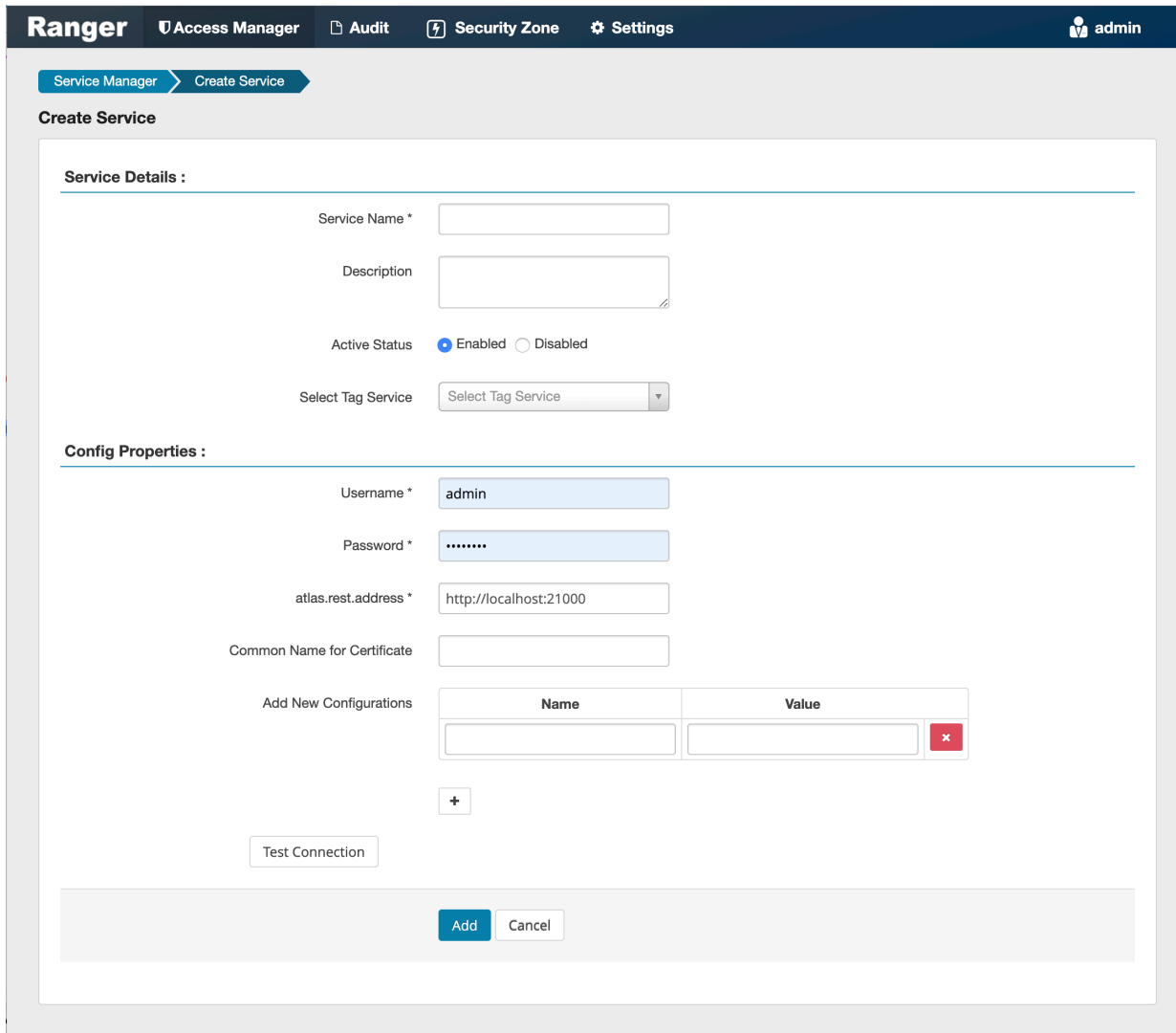
How to add an Atlas service.

Procedure

1.

On the Service Manager page, click the Add icon () next to Atlas.

The Create Service page appears.



The screenshot shows the 'Create Service' page in the Ranger interface. The page is titled 'Create Service' and has a breadcrumb trail 'Service Manager > Create Service'. The 'Service Details' section includes:

- Service Name * (text input)
- Description (text area)
- Active Status: Enabled Disabled
- Select Tag Service (dropdown menu)

 The 'Config Properties' section includes:

- Username * (text input with value 'admin')
- Password * (password input with masked characters)
- atlas.rest.address * (text input with value 'http://localhost:21000')
- Common Name for Certificate (text input)
- Add New Configurations: A table with columns 'Name' and 'Value', and a red 'x' button to remove entries.
- A '+' button to add new configurations.
- Test Connection (button)
- At the bottom, there are 'Add' and 'Cancel' buttons.

2. Enter the following information on the Create Service page:

Table 1: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.
Active Status	Enabled or Disabled.

Field name	Description
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to Atlas.

Table 2: Configuration Properties

Field name	Description
Username	The end system username that can be used for connection.
Password	The password for the username entered above.
atlas.rest.address	Atlas host and port: : http://atlas_host_FQDN:21000.
Common Name For Certificate	The name of the certificate. This field is interchangeably named Common Name For Certificate and Ranger Plugin SSL CName in Create Service pages.
Add New Configurations	Add any other new configuration(s).


3. Click Test Connection.
4. Click Add.

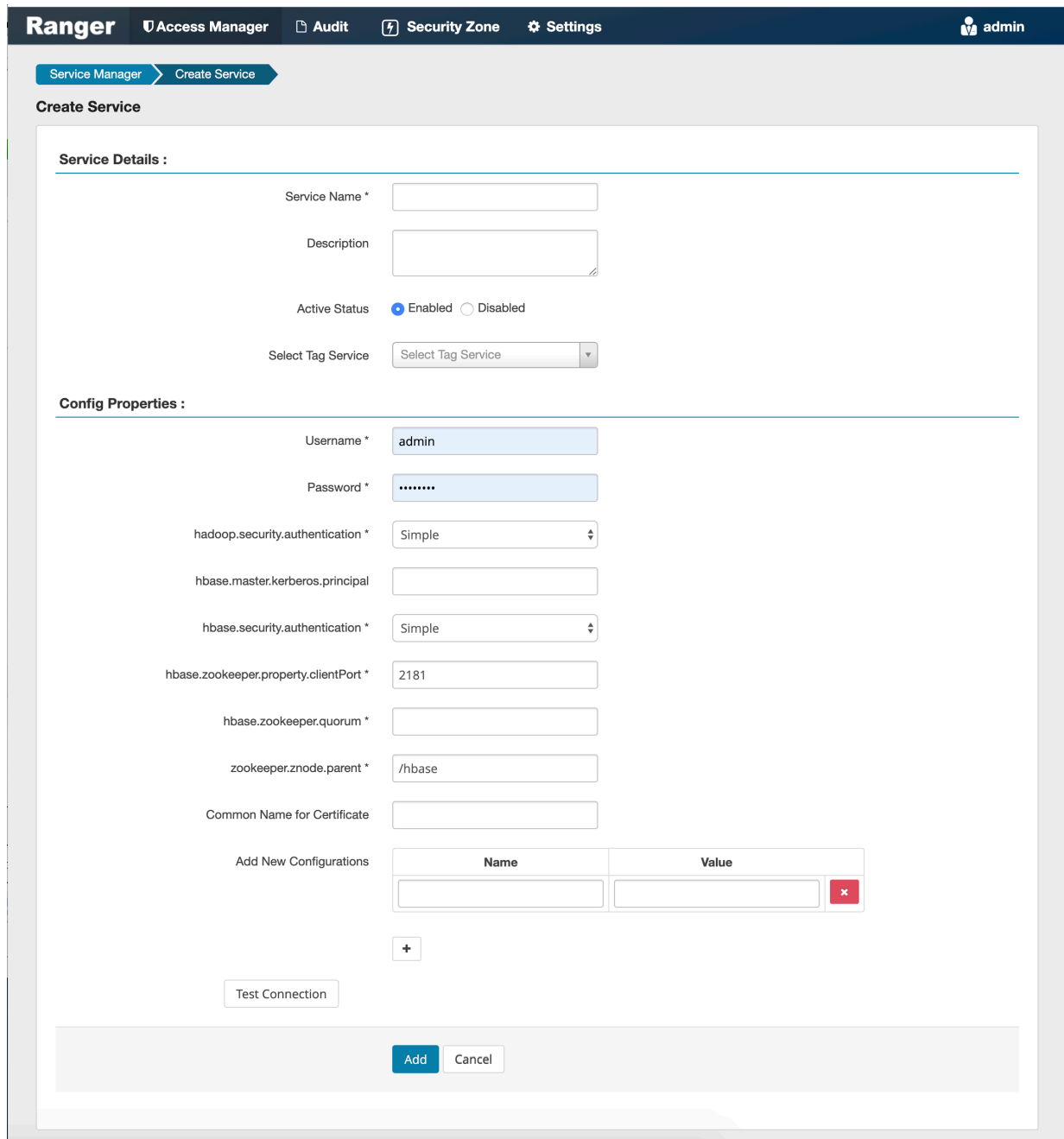
Configure a resource-based service: HBase

How to add an HBase service.

Procedure

1.

On the Service Manager page, click the Add icon () next to HBase. The Create Service page appears.



2. Enter the following information on the Create Service page:

Table 3: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.

Field name	Description
Active Status	Enabled or Disabled.
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to HBase.

Table 4: Configuration Properties


Field name	Description
Username	The end system username that can be used for connection.
Password	The password for the username entered above.
hadoop.security.authorization	The complete connection URL, including port and database name. (Default port: 10000.) For example, on the sandbox, jdbc:hive2://sandbox:10000/.
hbase.master.kerberos.principal	The Kerberos principal for the HBase Master. (Required only if Kerberos authentication is enabled.)
hbase.security.authentication	As noted in the hadoop configuration file hbase-site.xml.
hbase.zookeeper.property.clientPort	As noted in the hadoop configuration file hbase-site.xml.
hbase.zookeeper.quorum	As noted in the hadoop configuration file hbase-site.xml.
zookeeper.znode.parent	As noted in the hadoop configuration file hbase-site.xml.
Common Name for Certificate	The name of the certificate. This field is interchangeably named Common Name For Certificate and Ranger Plugin SSL CName in Create Service pages.
Add New Configurations	Add any other new configuration(s).

3. Click Test Connection.
4. Click Add.

Configure a resource-based service: HDFS

How to add an HDFS service.

Procedure

1. On the Service Manager page, click the Add icon () next to HDFS. The Create Service page appears.

2. Enter the following information on the Create Service page:

Table 5: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.

Field name	Description
Description	A description of the service.
Active Status	Enabled or Disabled.
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to HDFS.

Table 6: Configuration Properties


Field name	Description
Username	The end system username that can be used for connection.
Password	The password for the username entered above.
NameNode URL	hdfs://NAMENODE_FQDN:8020 The location of the Hadoop HDFS service, as noted in the hadoop configuration file core-site.xml OR (if this is a HA environment) the path for the primary NameNode. This field was formerly named fs.defaultFS.
Authorization Enabled	Authorization involves restricting access to resources. If enabled, user need authorization credentials.
Authentication Type	The type of authorization in use, as noted in the hadoop configuration file core-site.xml; either simple or Kerberos. (Required only if authorization is enabled). This field was formerly named hadoop.security.authorization.
hadoop.security.auth_to_local	Maps the login credential to a username with Hadoop; use the value noted in the hadoop configuration file, core-site.xml.
dfs.datanode.kerberos.principal	The principal associated with the datanode where the service resides, as noted in the hadoop configuration file hdfs-site.xml. (Required only if Kerberos authentication is enabled).
dfs.namenode.kerberos.principal	The principal associated with the NameNode where the service resides, as noted in the hadoop configuration file hdfs-site.xml. (Required only if Kerberos authentication is enabled).
dfs.secondary.namenode.kerberos.principal	The principal associated with the secondary NameNode where the service resides, as noted in the hadoop configuration file hdfs-site.xml. (Required only if Kerberos authentication is enabled).
RPC Protection Type	Only authorised user can view, use, and contribute to a dataset. A list of protection values for secured SASL connections. Values: Authentication, Integrity, Privacy
Common Name For Certificate	The name of the certificate. This field is interchangeably named Common Name For Certificate and Ranger Plugin SSL CName in Create Service pages.
Add New Configurations	Add any other new configuration(s).

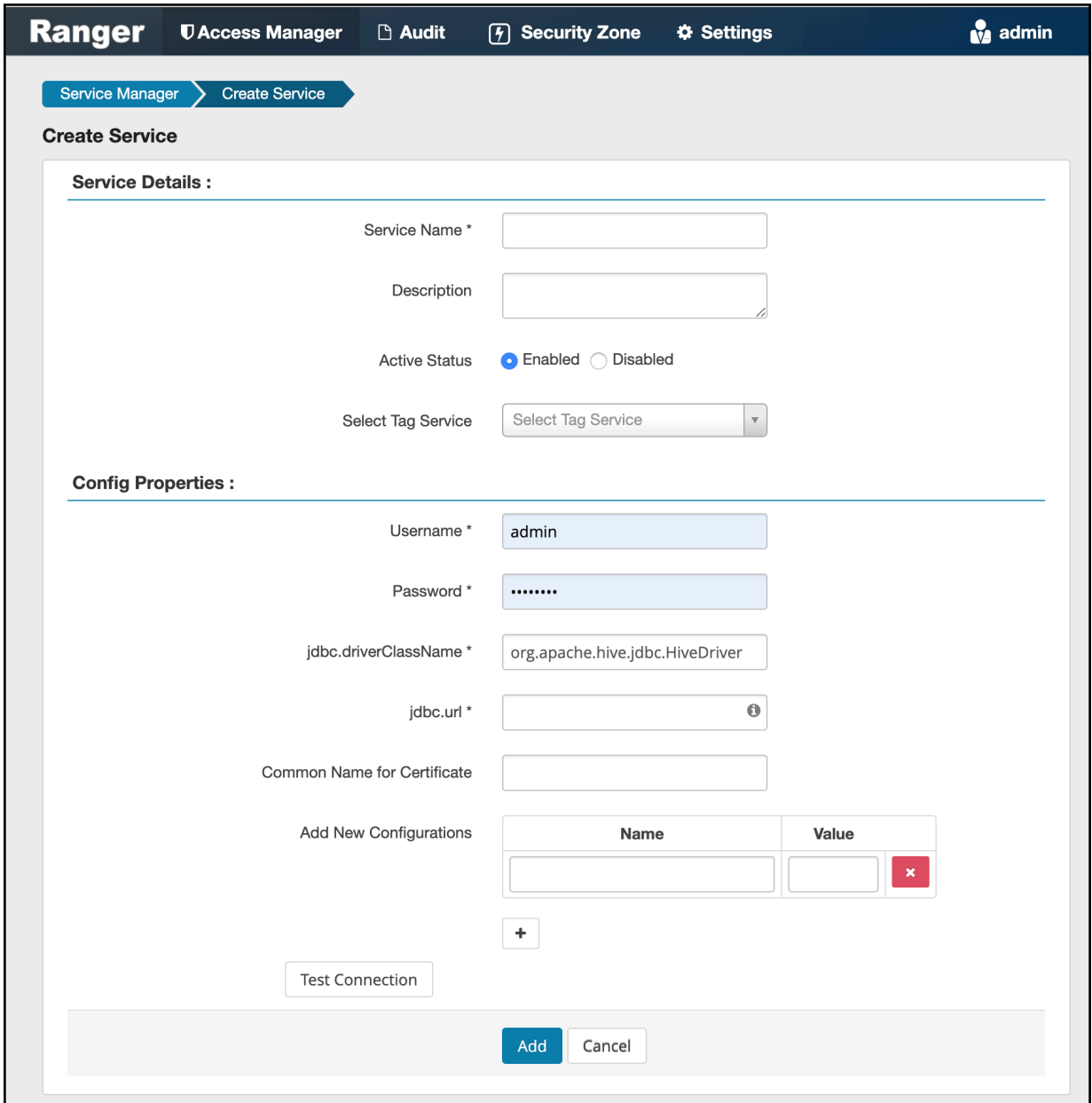
3. Click Test Connection.
4. Click Add.

Configure a resource-based service: HadoopSQL

How to add a HadoopSQL service.

Procedure

1. On Service Manager, click Add () next to HadoopSQL.
Create Service appears.



Ranger Access Manager Audit Security Zone Settings admin

Service Manager Create Service

Create Service

Service Details :

Service Name *

Description

Active Status Enabled Disabled

Select Tag Service

Config Properties :

Username *

Password *

jdbc.driverClassName *

jdbc.url *

Common Name for Certificate

Add New Configurations

Name	Value
<input type="text"/>	<input type="text"/>

2. On Create Service, enter the following information:

Table 7: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.
Active Status	Enabled or Disabled.

Field name	Description
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to Hive.

Table 8: Configuration Properties

Field name	Description
Username	The end system username that can be used for connection.
Password	The password for the username entered above.
jdbc.driver ClassName	The full classname of the driver used for Hive connections. Default: org.apache.hive.jdbc.HiveDriver
jdbc.url	The complete connection URL, including port and database name. (Default port: 10000.) For example, on the sandbox, jdbc:hive2://sandbox:10000/.
Common Name For Certificate	The name of the certificate. This field is interchangeably named Common Name For Certificate and Ranger Plugin SSL CName in Create Service pages.
Add New Configurations	Add any other new configuration(s).


3. Click Test Connection.
4. Click Add.

Configure a resource-based service: Kafka

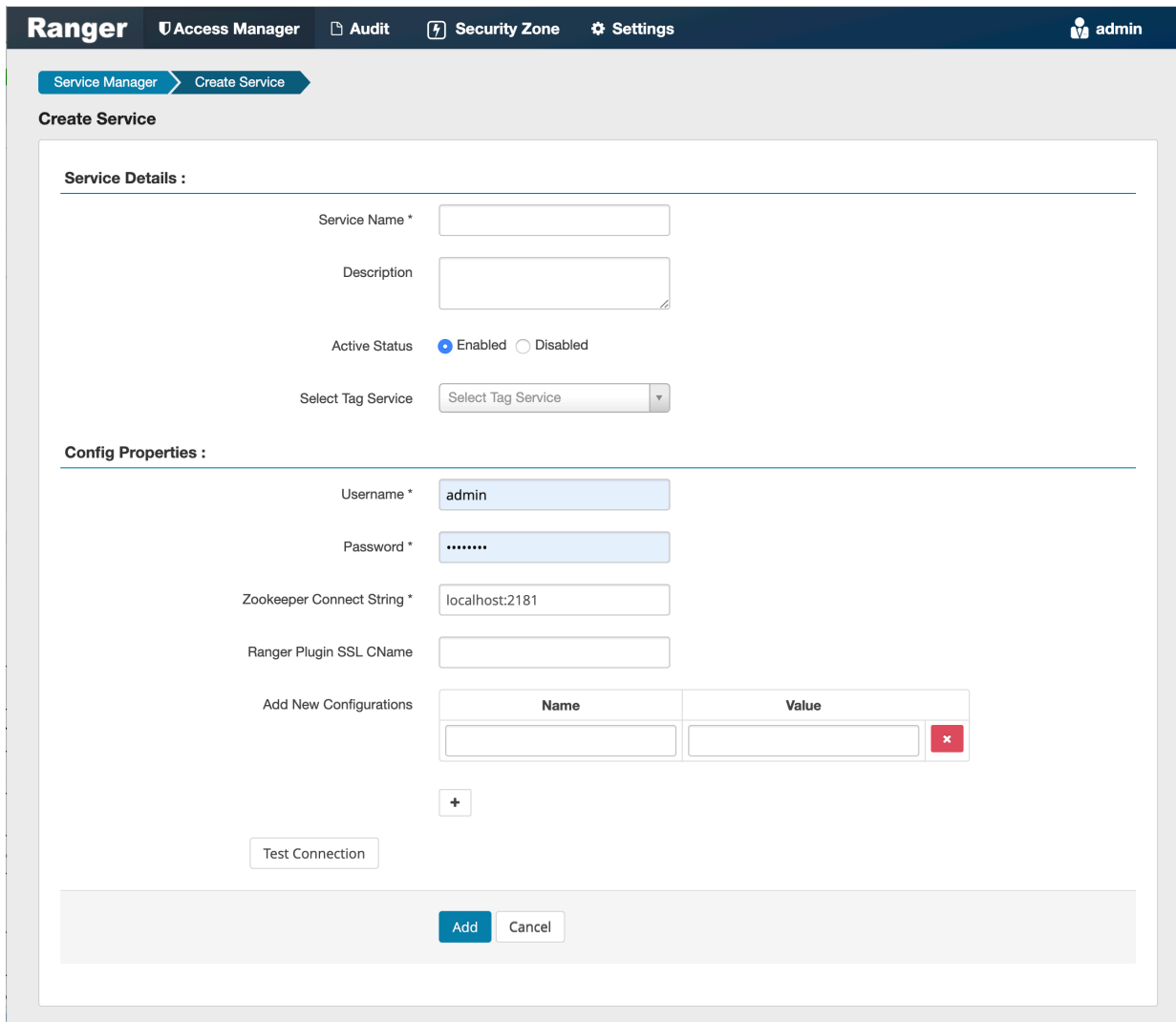
How to add a Kafka service.

Procedure

1.

On the Service Manager page, click the Add icon () next to Kafka.

The Create Service page appears.



2. Enter the following information on the Create Service page:

Table 9: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.
Active Status	Enabled or Disabled.

Field name	Description
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to Kafka.

Table 10: Configuration Properties


Field name	Description
Username	The end system username that can be used for connection.
Password	The password for the username entered above.
ZooKeeper Connect String	Defaults to localhost:2181 (Provide FQDN of zookeeper host : 2181).
Ranger Plugin SSL CName	Provide common.name.for.certificate which is registered with Ranger (in Wire Encryption environment). This field is interchangeably named Common Name For Certificate and Ranger Plugin SSL CName in Create Service pages.
Add New Configurations	Add any other new configuration(s).

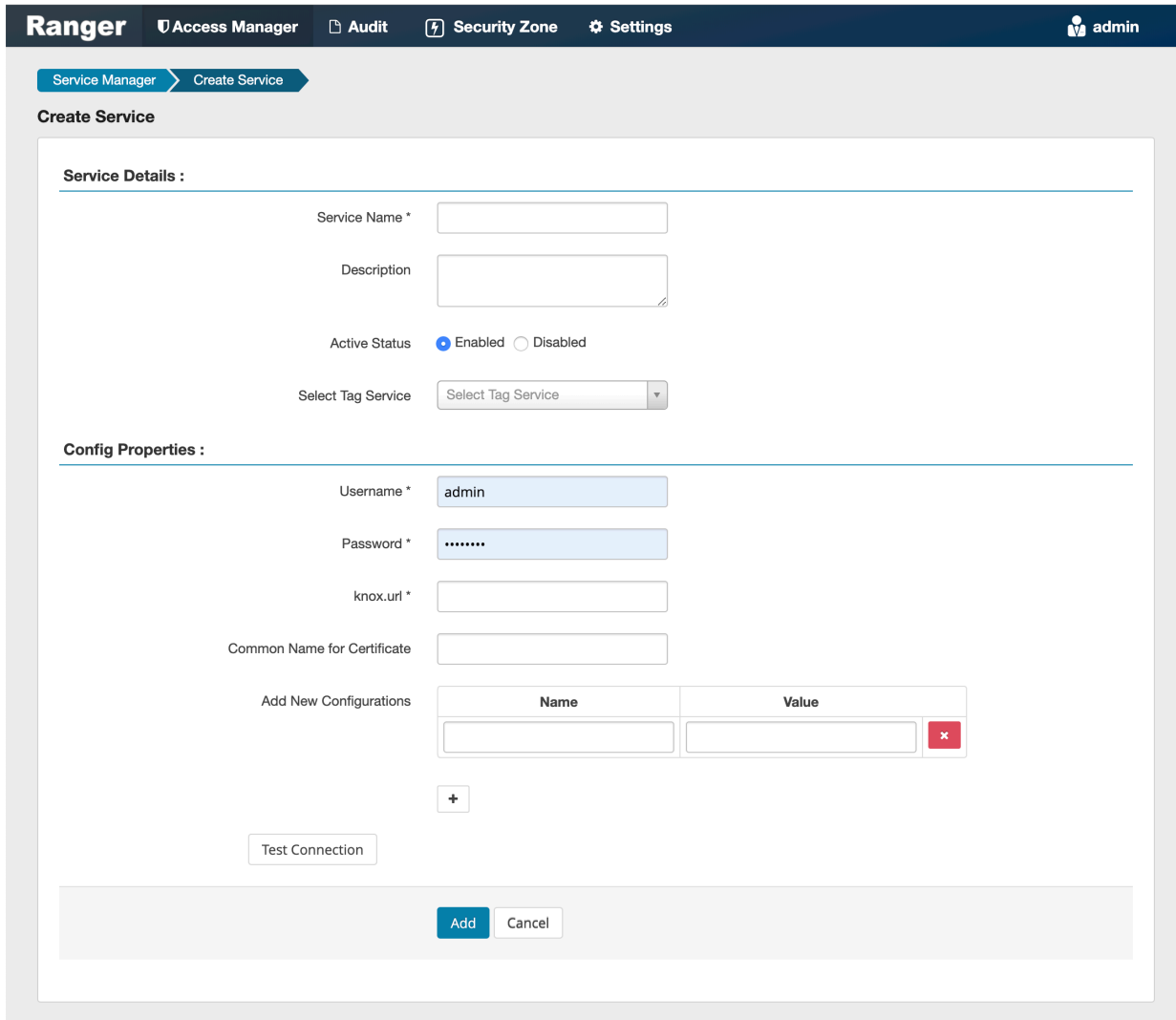
3. Click Test Connection.
4. Click Add.

Configure a resource-based service: Knox

How to add a Knox service.

Procedure

1. On the Service Manager page, click the Add icon () next to Knox.
The Create Service page appears.



2. Enter the following information on the Create Service page:

Table 11: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.
Active Status	Enabled or Disabled.

Field name	Description
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to Knox.

Table 12: Configuration Properties

Field name	Description
Username	The end system username that can be used for connection.
Password	The password for the username entered above.
knox.url	The Gateway URL for Knox.
Common Name For Certificate	The name of the certificate. This field is interchangeably named Common Name For Certificate and Ranger Plugin SSL CName in Create Service pages.
Add New Configurations	Add any other new configuration(s).


3. Click Test Connection.
4. Click Add.

Configure a resource-based service: NiFi

How to add a NiFi service.

Procedure

1.

On the Service Manager page, click the Add icon () next to NiFi. The Create Service page appears.

2. Enter the following information on the Create Service page:

Table 13: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.
Active Status	Enabled or Disabled.

Field name	Description
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to NiFi.

Table 14: Configuration Properties

Field name	Description
NiFi URL	The complete NiFi host URL.
Authentication Type	None or SSL.
Keystore	The keystore to use when Ranger makes an https connection to NiFi. This keystore contains the certificate that represents the Ranger server.
Keystore Type	The keystore type (JKS or PKCS12).
Keystore Password	The keystore password.
Truststore	The truststore to use when Ranger makes an https connection to NiFi. This truststore contains the public key of the certificate authority that signed the NiFi server certificates.
Truststore Type	The truststore type (JKS or PKCS12).
Truststore Password	The truststore password.
Add New Configurations	Add any other new configuration(s).


3. Click Test Connection.
4. Click Add.

Configure a resource-based service: NiFi Registry

How to add a NiFi Registry service.

Procedure

1.

On the Service Manager page, click the Add icon () next to NiFi Registry. The Create Service page appears.

2. Enter the following information on the Create Service page:

Table 15: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.
Active Status	Enabled or Disabled.

Field name	Description
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to NiFi.

Table 16: Configuration Properties


Field name	Description
NiFi Registry URL	The complete NiFi Registry URL.
Authentication Type	None or SSL.
Keystore	The keystore to use when Ranger makes an https connection to the NiFi Registry. This keystore contains the certificate that represents the Ranger server.
Keystore Type	The keystore type (JKS or PKCS12).
Keystore Password	The keystore password.
Truststore	The truststore to use when Ranger makes an https connection to the NiFi Registry. This truststore contains the public key of the certificate authority that signed the NiFi server certificates.
Truststore Type	The truststore type (JKS or PKCS12).
Truststore Password	The truststore password.
Add New Configurations	Add any other new configuration(s).

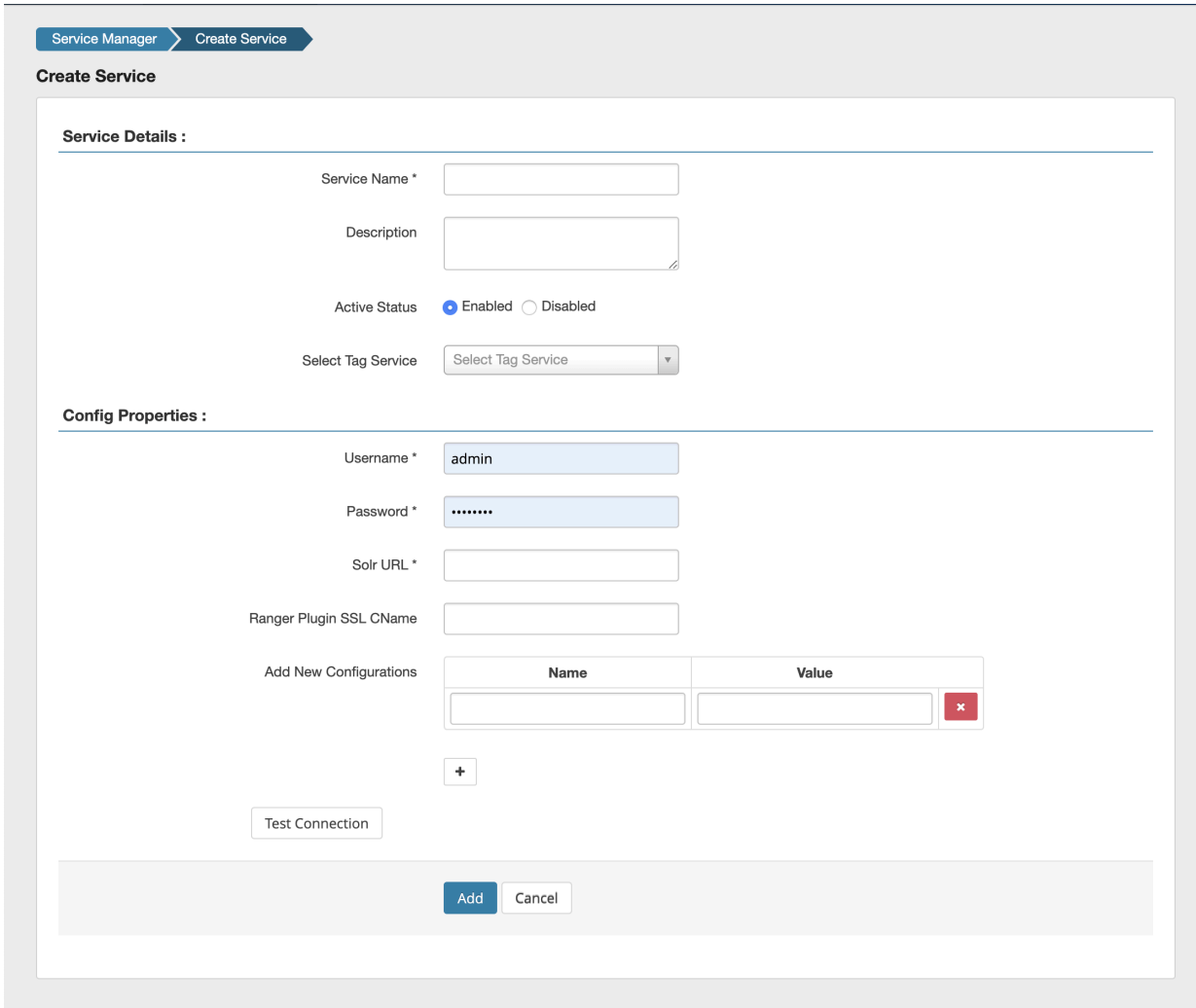
3. Click Test Connection.
4. Click Add.

Configure a resource-based service: Solr

How to add a Solr service.

Procedure

1. On the Service Manager page, click the Add icon () next to Solr.
The Create Service page appears.



Service Manager > **Create Service**

Create Service

Service Details :

Service Name *

Description

Active Status Enabled Disabled

Select Tag Service

Config Properties :

Username *

Password *

Solr URL *

Ranger Plugin SSL CName

Add New Configurations

Name	Value
<input type="text"/>	<input type="text"/>

2. Enter the following information on the Create Service page:

Table 17: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.
Active Status	Enabled or Disabled.

Field name	Description
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to Solr.

Table 18: Configuration Properties

Field name	Description
Username	The end system username that can be used for connection.
Password	The password for the username entered above.
Solr URL	http://Solr_host:8983
Ranger Plugin SSL CName	Provide common.name.for.certificate which is registered with Ranger (in Wire Encryption environment). This field is interchangeably named Common Name For Certificate and Ranger Plugin SSL CName in Create Service pages.
Add New Configurations	Add any other new configuration(s).


3. Click Test Connection.
4. Click Add.

Configure a resource-based service: YARN

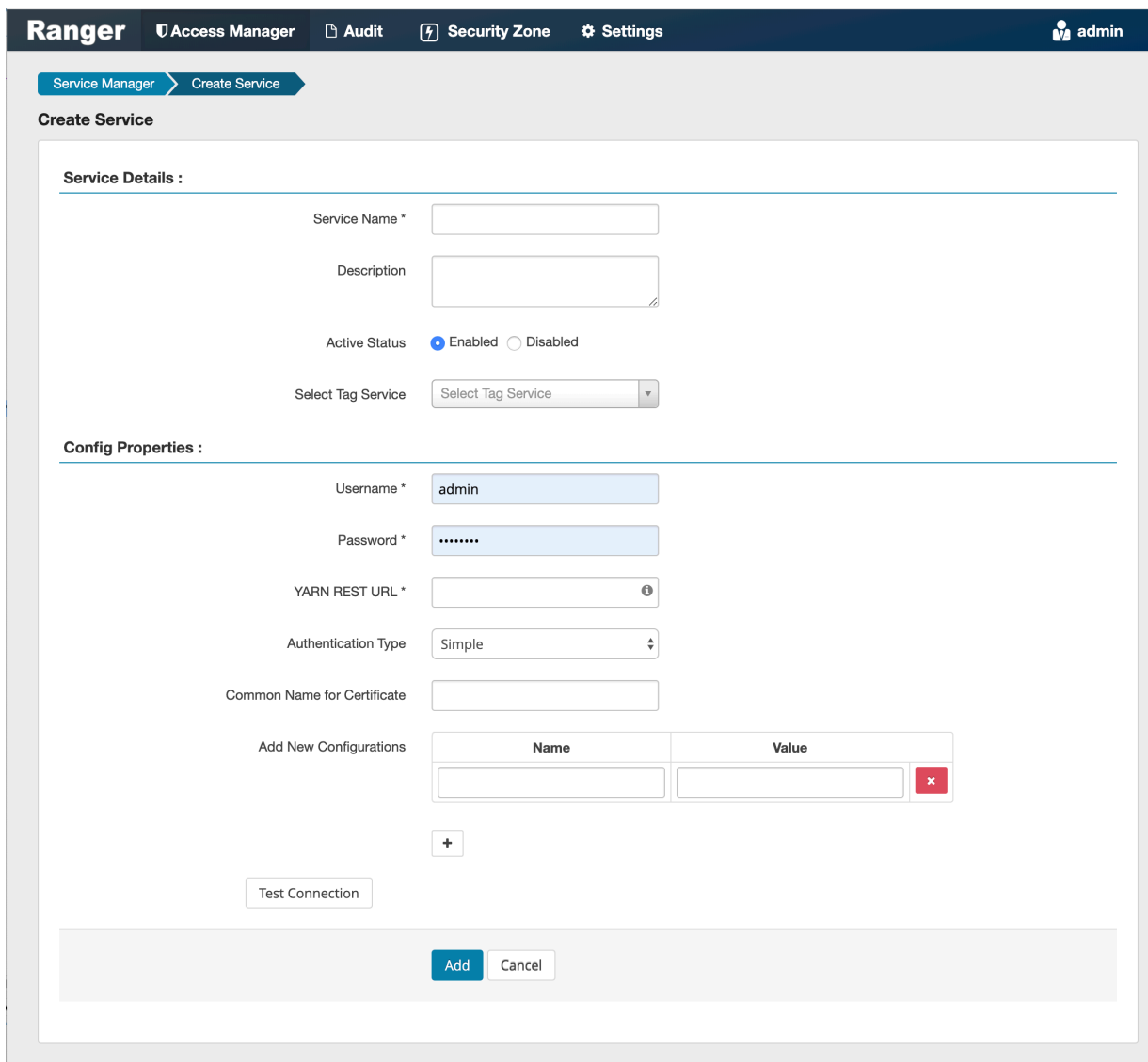
How to add a YARN service.

Procedure

1.

On the Service Manager page, click the Add icon () next to YARN.

The Create Service page appears.



2. Enter the following information on the Create Service page:

Table 19: Service Details

Field name	Description
Service Name	The name of the service; required when configuring agents.
Description	A description of the service.
Active Status	Enabled or Disabled.

Field name	Description
Select Tag Service	Select a tag-based service to apply the service and its tag-based policies to YARN.



Table 20: Configuration Properties

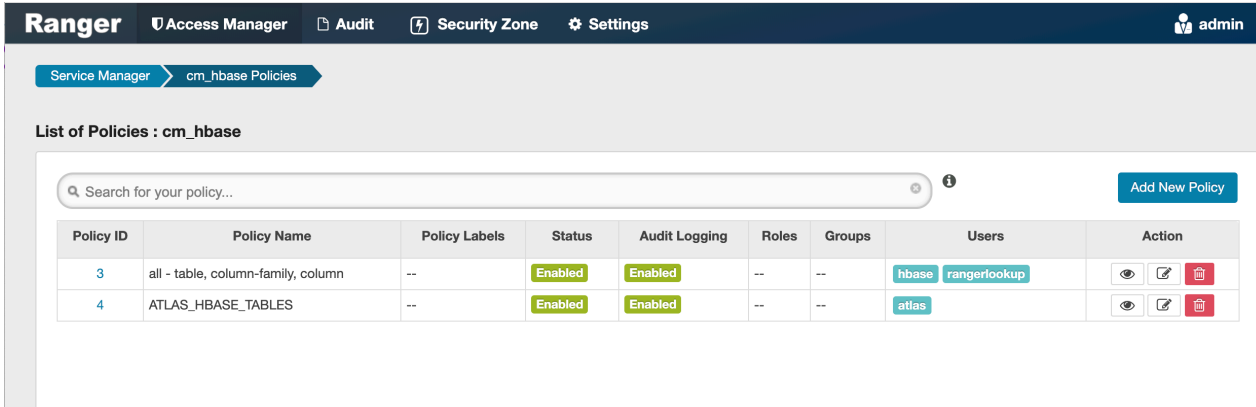
Field name	Description
Username	The end system username that can be used for connection.
Password	The password for the username entered above.
YARN REST URL	Http or https://RESOURCEMANAGER_FQDN:8088.
Authentication Type	The type of authorization in use, as noted in the hadoop configuration file core-site.xml; either simple or Kerberos. (Required only if authorization is enabled). This field was formerly named hadoop.security.authorization.
Common Name For Certificate	The name of the certificate. This field is interchangeably named Common Name For Certificate and Ranger Plugin SSL CName in Create Service pages.
Add New Configurations	Add any other new configuration(s).

3. Click Test Connection.
4. Click Add.

Configuring resource-based policies

To view the policies associated with a service, click the service name on the Resource Based Policies Service Manager page. The policies for that service will be displayed in a list, along with a search box.

- To add a new resource-based policy to the service, click Add New Policy.
- To edit a resource-based policy, click the Edit icon () for the service. Edit the policy settings, then click Save to save your changes.
- To delete a resource-based policy, click the Delete icon () for the service.









Ranger Access Manager Audit Security Zone Settings admin

Service Manager cm_hbase Policies

List of Policies : cm_hbase

Search for your policy... + i Add New Policy

Policy ID	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
3	all - table, column-family, column	--	Enabled	Enabled	--	--	hbase rangerlookup	  
4	ATLAS_HBASE_TABLES	--	Enabled	Enabled	--	--	atlas	  

Related Information

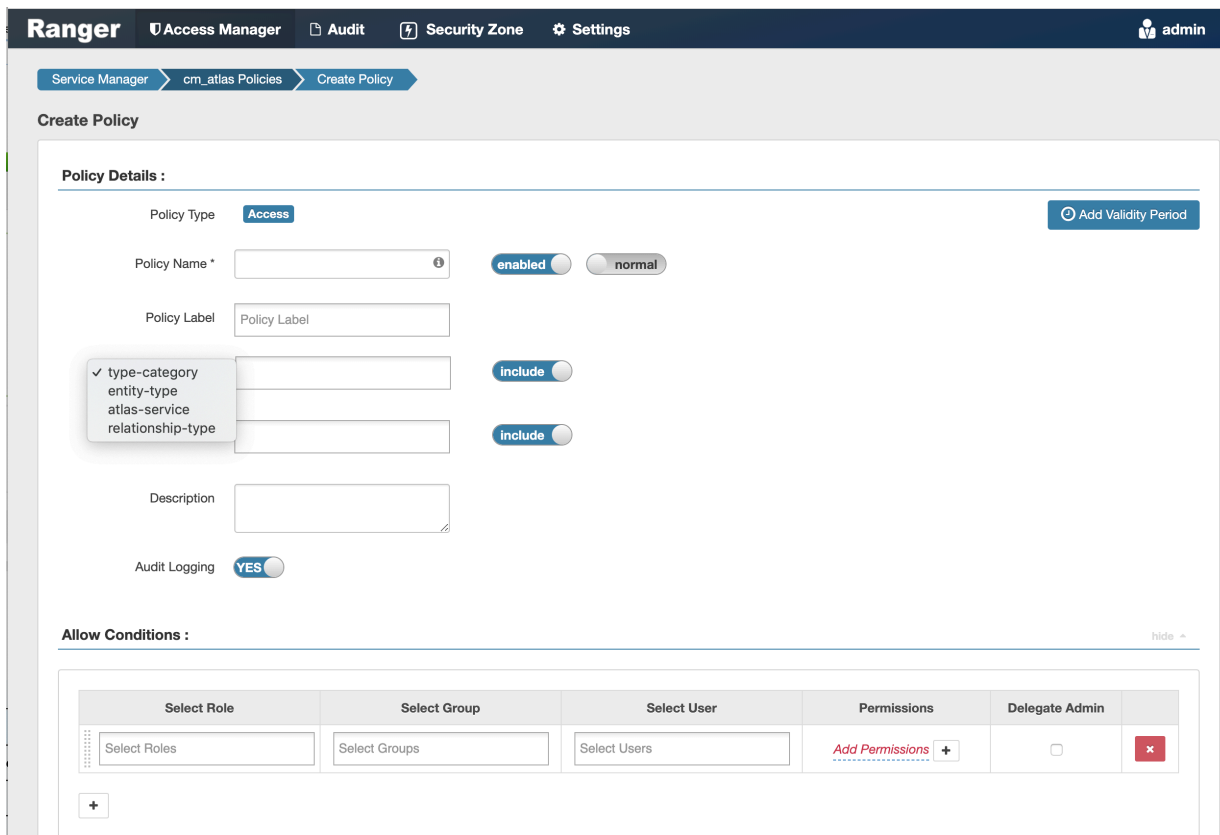
[Importing and exporting resource-based policies](#)

Configure a resource-based policy: Atlas

How to add a new policy to an existing Atlas service.

Procedure

1. On the Service Manager page, select an existing Atlas service. The List of Policies page appears.
2. Click Add New Policy. The Create Policy page appears.



3. Complete the Create Policy page as follows:

Table 21: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
type-category	Select type-category, entity-type, atlas-service, or relationship-type.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.

Field	Description
Add Validity Period	Specify a start and end time for the policy.

Table 22: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Permissions	Add or edit permissions: Create Type, Update Type, Delete Type, Select/Deselect All.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

- You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
- You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
- Click Add.

Related Information

[Wildcards and variables in resource-based policies](#)

Configure a resource-based policy: HBase

How to add a new policy to an existing HBase service.

Procedure

- On the Service Manager page, select an existing HBase service.

The List of Policies page appears.

2. Click Add New Policy.

The Create Policy page appears.

The screenshot shows the Ranger 'Create Policy' page. The navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The breadcrumb trail is 'Service Manager > cm_hbase Policies > Create Policy'. The page title is 'Create Policy'. The 'Policy Details' section contains the following fields and controls:


- Policy Type:** Access (selected)
- Policy Name *:** Text input field with a search icon.
- Policy Label:** Text input field with the value 'Policy Label'.
- HBase Table *:** Text input field.
- HBase Column-family *:** Text input field.
- HBase Column *:** Text input field.
- Description:** Text area.
- Audit Logging:** YES (selected)
- enabled/normal:** Toggle switch, currently on 'enabled'.
- include:** Toggle switch, currently on 'include'.
- include:** Toggle switch, currently on 'include'.
- include:** Toggle switch, currently on 'include'.
- Add Validity Period:** Button with a clock icon.

The 'Allow Conditions' section is expanded, showing a table with the following columns and controls:

Select Role	Select Group	Select User	Permissions	Delegate Admin	
Select Roles	Select Groups	Select Users	Add Permissions +	<input type="checkbox"/>	<input type="button" value="x"/>

3. Complete the Create Policy page as follows:

Table 23: Policy Details

Label	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
HBase Table	<p>Select the appropriate database. Multiple databases can be selected for a particular policy. This field is mandatory.</p> <p> Note: Policies must use '<namespace>:*' for the table name to apply to the namespace as a whole. You can define a namespace in the HBase table field. Valid formats for a namespace-specific, HBase policy include: <namespace>:<table> for example, "myNameSpace:table1"</p> <p>Further, note that <namespace>:<tablePrefix>* (default value) does not work, per https://issues.apache.org/jira/browse/RANGER-1226. All other namespaces except the default one work.</p>

Label	Description
HBase Column-family	For the selected table, specify the column families to which the policy applies.
HBase Column	For the selected table and column families, specify the columns to which the policy applies.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.
Add Validity Period	Specify a start and end time for the policy.

Table 24: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Permissions	Add or edit permissions: Read, Write, Create, Admin, Select/ Deselect All.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

4. You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
5. You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
6. Click Add.

What to do next

Provide User Access to HBase Database Tables from the Command Line

HBase provides the means to manage user access to HBase database tables directly from the command line. The most commonly-used commands are:

- GRANT

Syntax:

```
grant '<user-or-group>', '<permissions>', '<table>
```

For example, to create a policy that grants user1 read/write permission on the table usertable, the command would be:

```
grant 'user1', 'RW', 'usertable'
```

The syntax is the same for granting CREATE and ADMIN rights.

- REVOKE

Syntax:

```
revoke '<user-or-group>', '<usertable>'
```

For example, to revoke the read/write access of user1 to the table usertable, the command would be:

```
revoke 'user1', 'usertable'
```



Note:

Unlike Hive, HBase has no specific revoke commands for each user privilege.

Related Information

[Wildcards and variables in resource-based policies](#)

Configure a resource-based policy: HDFS

How to add a new policy to an existing HDFS service.

About this task

Through configuration, Apache Ranger enables both Ranger policies and HDFS permissions to be checked for a user request. When the NameNode receives a user request, the Ranger plugin checks for policies set through the Ranger Service Manager. If there are no policies, the Ranger plugin checks for permissions set in HDFS.

We recommend that permissions be created at the Ranger Service Manager, and to have restrictive permissions at the HDFS level.

Procedure

1. On the Service Manager page, select an existing HDFS service.

The List of Policies page appears.

- Click Add New Policy.
The Create Policy page appears.

The screenshot shows the Ranger 'Create Policy' page. The page is titled 'Create Policy' and is part of the 'cm_hdfs Policies' section. The 'Policy Details' section includes the following fields and controls:

- Policy Type:** Access (selected)
- Policy Name:** A text input field with a lock icon and a toggle switch for 'enabled' (selected) and 'normal'.
- Policy Label:** A text input field with the placeholder 'Policy Label'.
- Resource Path:** A text input field with a toggle switch for 'recursive' (selected).
- Description:** A text area.
- Audit Logging:** A toggle switch for 'YES' (selected).
- add/edit permissions:** A dropdown menu showing options: Read (selected), Write, Execute, and Select/Deselect All.

The 'Allow Conditions' section includes the following controls:

- Select Role:** A dropdown menu with the placeholder 'Select Roles'.
- Select Group:** A dropdown menu with the placeholder 'Select Groups'.
- Select User:** A dropdown menu with the placeholder 'Select Users'.
- Add Permissions:** A button with a plus sign.
- Delegate Admin:** A checkbox.

- Complete the Create Policy page as follows:

Table 25: Policy Details

Field	Description
Policy Name	Enter a unique name for this policy. The name cannot be duplicated anywhere in the system.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Resource Path	Define the resource path for the policy folder/file. The default recursive setting specifies that the resource path is recursive; you can also specify a non-recursive path.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.

Field	Description
Add Validity Period	Specify a start and end time for the policy.

Table 26: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Permissions	Add or edit permissions: Read, Write, Execute, Select/Deselect All.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

- You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
- You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
- Click Add.

Related Information

[Wildcards and variables in resource-based policies](#)

Configure a resource-based policy: HadoopSQL

How to add a new policy to an existing Hive service.

Procedure

- On the Service Manager page, select an existing HadoopSQL service.

The List of Policies page appears.



Note: Service_name remains cm_hive. Display name is HadoopSQL.

2. Click Add New Policy.

The Create Policy page appears.

The screenshot displays the 'Create Policy' interface in Cloudera Ranger. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The breadcrumb trail shows 'Service Manager > Hadoop SQL Policies > Create Policy'. The 'Policy Details' section contains the following elements:

- Policy Type:** Set to 'Access'.
- Policy Name:** A text input field with a dropdown arrow.
- Policy Label:** A text input field containing 'Policy Label'.
- Database:** A dropdown menu set to 'database' with an 'Include' toggle.
- Table:** A dropdown menu set to 'table' with an 'Include' toggle.
- Column:** A dropdown menu set to 'column' with an 'Include' toggle.
- Description:** A text area for entering a description.
- Audit Logging:** A toggle switch set to 'Yes'.
- Buttons:** 'Add Validity Period' and 'Enabled/Normal' toggle.

An 'add/edit permissions' modal is open, listing various permissions with checkboxes. Below the modal, a table is partially visible with columns for 'Permissions', 'Delegate Admin', and a delete button.

3. Complete the Create Policy page as follows:

Table 27: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory. The policy is enabled by default.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Database	Type in the applicable database name. The autocomplete feature displays available databases based on the entered text. Include is selected by default to allow access. Select Exclude to deny access..

Field	Description
table/udf	Specifies a table-based or UDF-based policy. Select table or udf, then type in the applicable table or UDF name. The autocomplete feature displays available tables based on the entered text. Include is selected by default to allow access. Select Exclude to deny access.
column	Type in the applicable column name. The autocomplete feature displays available columns based on the entered text. Include is selected by default to allow access. Select Exclude to deny access.
URL	Specify the cloud storage path (for example s3a://dev-admin/demo/campaigns.txt) where the end-user permission is needed to read/write the Hive data from/to a cloud storage path. Permissions: READ operation on the URL permits the user to perform HiveServer2 operations which use S3 as data source for Hive tables. WRITE operation on the URL permits the user to perform HiveServer2 operations which write data to the specified S3 location.
URI	Hive INSERT OVERWRITE queries require a Ranger URI policy to allow write operations, even if the user has write privilege granted through HDFS policy. Failure to specify this field will result in the following error: Error while compiling statement: FAILED: HiveAccessControlException Permission denied: user [jdoe] does not have [WRITE] privilege on [tmp/*] (state=42000,code=40000) Example value: /tmp/*
Description	(Optional) Describe the purpose of the policy.
Hive Service Name	hiveservice is used only in conjunction with Permissions=Service Admin. Enables a user who has Service Admin permission in Ranger to run the kill query API: kill query <queryID> . Supported value: *. (Required)
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.
Add Validity Period	Specify a start and end time for the policy.

Table 28: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.

Label	Description
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Permissions	Add or edit permissions: Select, Update, Create, Drop, Alter, Index, Lock, All, ReplAdmin, Service Admin, Temp UDF Admin, Refresh, RW Storage, Select/Deselect All. Service Admin is used in conjunction with Hive Service Name and the kill query API: kill query <queryID> .
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

- You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
- You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
- Click Add.

What to do next

Provide User Access to Hive Database Tables from the Command Line

Hive provides the means to manage user access to Hive database tables directly from the command line. The most commonly-used commands are:

- GRANT

Syntax:

```
grant <permissions> on table <table> to user <user or group>;
```

For example, to create a policy that grants user1 SELECT permission on the table default-hivesmoke22074, the command would be:

```
grant select on table default.hivesmoke22074 to user user1;
```

The syntax is the same for granting UPDATE, CREATE, DROP, ALTER, INDEX, LOCK, ALL, and ADMIN rights.

- REVOKE

Syntax:

```
revoke <permissions> on table <table> from user <user or group>;
```

For example, to revoke the SELECT rights of user1 to the table default.hivesmoke22074, the command would be:

```
revoke select on table default.hivesmoke22074 from user user1;
```

The syntax is the same for revoking UPDATE, CREATE, DROP, ALTER, INDEX, LOCK, ALL, and ADMIN rights.

Related Information

[Wildcards and variables in resource-based policies](#)

Configure a resource-based storage handler policy: HadoopSQL

How to configure a policy that allows authorized users to create data tables using storage-handlers.

About this task

Ranger includes “storage-type” and “storage-url” resources in HadoopSQL Service that support only the permission “RW Storage” permission. Ranger authorizes a user that creates or alters a table against this resource policy. A user having the required “RW Storage” permission on the resource representing the storage-type and storage-url, is allowed to create/alter the table in the respective storage.

Procedure

1. On the Service Manager page, select HadoopSQL service.

The List of Policies HadoopSQL page appears.



Note: Service_name remains cm_hive. Display name is HadoopSQL.

2. To create a new policy, click Add New Policy.

- a) On Create Policy click storage-type as shown in the following example:

Policy Details:

Policy Type: **Access** Add Validity Period

Policy Name *: test storage handler policy Enabled Normal

Policy Label:
 dropdown: database, uri, hiveservice, global, **storage-type**

Storage URL *: Include

Description: storage handler policy for HadoopSQL

Audit Logging: **Yes**

Allow Conditions: hide

Select Role	Select Group	Select User	Permissions	Delegate Admin
<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/> hive <input checked="" type="checkbox"/> beacon <input checked="" type="checkbox"/> dpprofiler <input checked="" type="checkbox"/> hue <input checked="" type="checkbox"/> admin <input checked="" type="checkbox"/> impala	RW Storage	<input checked="" type="checkbox"/>

- b) Complete the required* fields.

- c) In Allow Conditions, select users, then add the RW Storage permission, as shown in the preceding example.

- d) Scroll to the bottom of Create Policy, then click Add.

- To configure an existing policy named all - storage-type, storage-url, click Edit.

The Edit Policy page appears.

Edit Policy Last Response Time
11/29/2023 03:22:15 PM

Service Manager > Hadoop SQL Policies > Edit Policy

Policy ID* 11

Policy Name* Enabled Normal

Policy Label

Storage Type Include

Storage URL* Include

Description

Audit Logging* Yes

Allow Conditions: hide ^

Select Roles	Select Groups	Select Users	Permissions	Delegate Admin
<input type="text" value="Select..."/>	<input type="text" value="Select..."/>	hive x beacon x dpprofiler x hue x admin x impala x systest x	RW Storage	<input checked="" type="checkbox"/>

- Complete the Edit Policy page as shown in the preceding example using the follow policy detail descriptions:

Table 29: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory. The policy is enabled by default.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.
storage-type	Type in the applicable storage type. * allows athenizes users to create any table in the spcified storage type..
storage url	Type in the applicable storage URL. * allows athenizes users to create any table in the spcified storage URL. Select Exclude to deny access.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).

Field	Description
Add Validity Period	Specify a start and end time for the policy.

Table 30: Allow Conditions

Label	Description
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Permissions	Add or edit permissions: RW Storage, You can assign read and select permissions to rangerlookup user.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

Example

Example StorageHandler Policy Definitions:

HBase StorageHandler policy:

Storage Type: hbase

Storage URL: hbase-cluster:port/hbase-table

Storage create table command:

```
CREATE [EXTERNAL] table foo(...)
STORED BY 'org.apache.hadoop.hive.hbase.HBaseStorageHandler'
TBLPROPERTIES ('hbase.table.name' = 'bar');
```

```
e.g:
CREATE TABLE hive_hbase_test_1(key int, value string) STORED BY
'org.apache.hadoop.hive.hbase.HBaseStorageHandler' WITH SERDEPR
OPERTIES ("hbase.columns.mapping" = "cf:string", "hbase.table.na
me" = "hive_hbase_test_1");
```

Kafka StorageHandler policy:

Storage Type: kafka

Storage URL: bootstrap-server:port/kafka-topic

JDBC StorageHandler policy:

Storage Type: jdbc:mysql

Storage URL: mysql-host:port/DBname/Table , or

Sorage URL: mysql-host:port/DBname/*

**Note:**

Policy and table definitions must be in sync regarding the port definition, even for default port numbers. For example, if port number 3306 is defined in the policy for mysql and this port number is left out from the URL as default value for the JDBC Driver, you must use the same reference as defined in the policy when creating the external table.

Using an explicit table name allows only to reference that specific table with `hive.sql.table` while using `*` allows not only to reference any tables from the database but also allows you to write a custom query against this database, for example using `hive.sql.query`.

Configure a resource-based policy: Kafka

How to add a new policy to an existing Kafka service.

Procedure

1. On the Service Manager page, select an existing Kafka service.
The List of Policies page appears.
2. Click Add New Policy.
The Create Policy page appears.

The screenshot shows the 'Create Policy' page in the Ranger interface. The page is titled 'Create Policy' and is part of the 'cm_kafka Policies' service manager. The 'Policy Details' section includes the following fields and controls:

- Policy Type:** Access (selected)
- Policy Name:** A text input field with a required field indicator.
- Policy Label:** A text input field.
- Topic Selection:** A dropdown menu with options: topic (checked), transactionalid, cluster, and delegationtoken.
- Enabled:** A toggle switch set to 'enabled'.
- Normal:** A toggle switch set to 'normal'.
- Include:** A toggle switch set to 'include'.
- Audit Logging:** A toggle switch set to 'YES'.
- Add Validity Period:** A button to add a validity period.
- Policy Conditions:** A section with a '+' button and 'No Conditions' listed.

The 'Allow Conditions' section is currently hidden, showing a table with the following columns:

Select Role	Select Group	Select User	Policy Conditions	Permissions	Delegate Admin	
Select Roles	Select Groups	Select Users	Add Conditions	Add Permissions	<input type="checkbox"/>	<input type="button" value="x"/>

3. Complete the Create Policy page as follows:

Table 31: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.

Field	Description
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.
Topic	Kafka resource type. A topic is a category or feed name to which messages are published.
Transactional ID	Kafka resource type, uniquely identifies producers in a persistent way.
Cluster	Kafka resource type.
Delegation Token	Kafka resource type for authentication.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Add Validity Period	Specify a start and end time for the policy.
Policy Conditions (applied at the policy level)	Click the + icon, then specify an IP address range.

Table 32: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Policy Conditions (applied at the item level)	Specify an IP address range.
Permissions	Add or edit permissions: Publish, Consume, Configure, Describe, Create, Delete, Describe Configs, Alter Configs, Select/Deselect All.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

4. You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
5. You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
6. Click Add.

Related Information

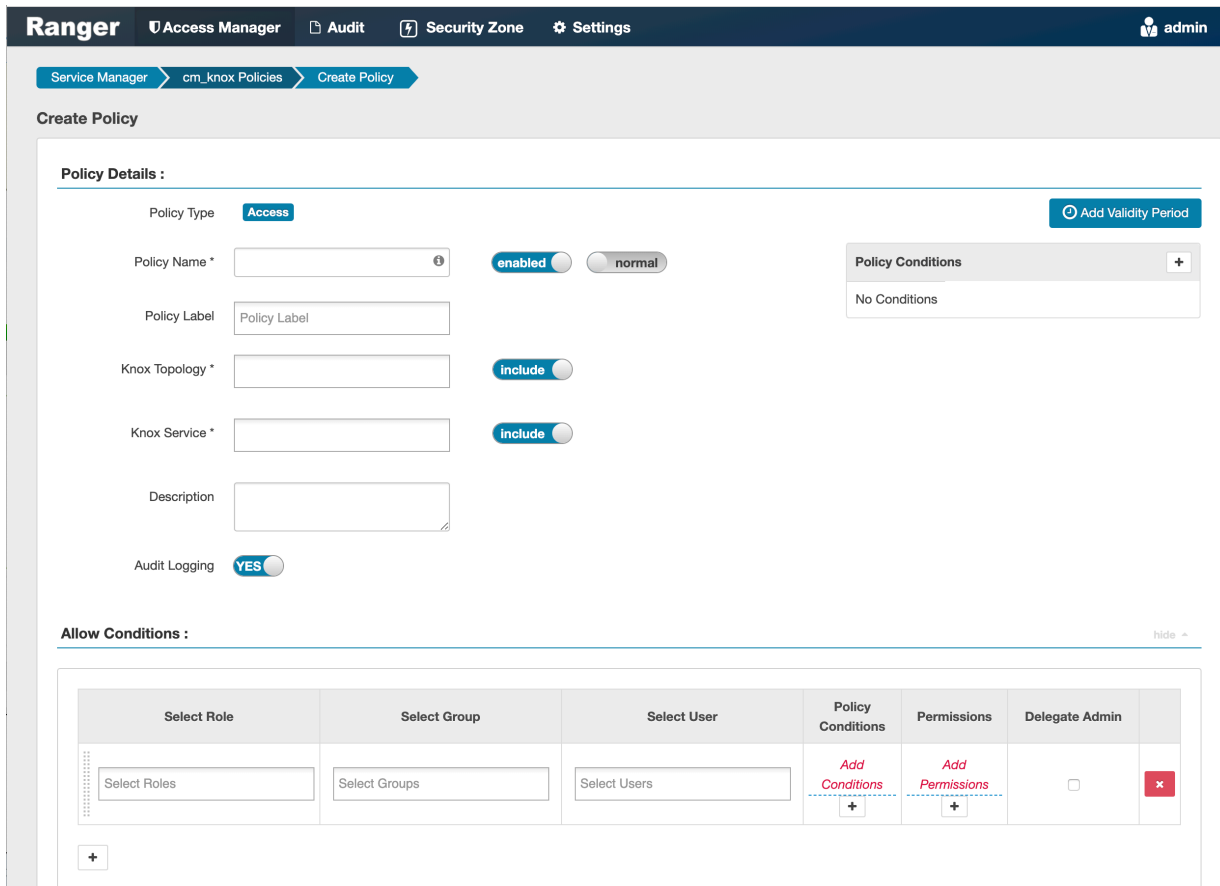
[Wildcards and variables in resource-based policies](#)

Configure a resource-based policy: Knox

How to add a new policy to an existing Knox service.

Procedure

1. On the Service Manager page, select an existing Knox service.
The List of Policies page appears.
2. Click Add New Policy.
The Create Policy page appears.



3. Complete the Create Policy page as follows:

Table 33: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Knox Topology	Enter an appropriate Topology Name.
Knox Service	Enter an appropriate Service Name.

Field	Description
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.
Add Validity Period	Specify a start and end time for the policy.
Policy Conditions (applied at the policy level)	Click the + icon, then specify an IP address range.

Table 34: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Policy Conditions (applied at the item level)	Specify an IP address range.
Permissions	Add or edit permissions: Allow
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

Since Knox does not provide a command line methodology for assigning privileges or roles to users, the User and Group Permissions portion of the Knox Create Policy form is especially important.

4. You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
5. You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
6. Click Add.

Related Information

[Wildcards and variables in resource-based policies](#)

Configure a resource-based policy: NiFi

How to add a new policy to an existing Atlas service.

Procedure

1. On the Service Manager page, select an existing NiFi service.
The List of Policies page appears.

- Click Add New Policy.
The Create Policy page appears.

The screenshot shows the 'Create Policy' page in the Ranger interface. The page is titled 'Create Policy' and is part of the 'Service Manager' > 'cm_nifi Policies' > 'Create Policy' path. The 'Policy Details' section includes the following fields and controls:

- Policy Type:** Set to 'Access'. There is an 'Add Validity Period' button to the right.
- Policy Name *:** A text input field with a dropdown arrow. To its right are two toggle buttons: 'enabled' (selected) and 'normal'.
- Policy Label:** A text input field with the value 'Policy Label'.
- NiFi Resource Identifier *:** A text input field.
- Description:** A text area.
- Audit Logging:** A toggle button set to 'YES'.

The 'Allow Conditions' section is partially visible, showing a table with the following columns:

Select Role	Select Group	Select User	Permissions	Delegate Admin	
Select Roles	Select Groups	Select Users	Add Permissions +	<input type="checkbox"/>	x

- Complete the Create Policy page as follows:

Table 35: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
NiFi Resource Identifier	In a NiFi cluster, all nodes must be granted the ability to view and modify component data in order for user to list or empty queues in processor component outbound connections. With Ranger this can be accomplished by using a wildcard to grant all of the NiFi nodes read and write access to the /data/* NiFi resource.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.

Field	Description
Add Validity Period	Specify a start and end time for the policy.

Table 36: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Permissions	Add or edit permissions: Read, Write, Select/Deselect All.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

- You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
- You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
- Click Add.

Configure a resource-based policy: NiFi Registry

How to add a new policy to an existing Atlas service.

Procedure

- On the Service Manager page, select an existing NiFi Registry service.
The List of Policies page appears.

- Click Add New Policy.
The Create Policy page appears.

The screenshot shows the 'Create Policy' page in the Ranger interface. The page is titled 'Create Policy' and is part of the 'cm_nifi_registry Policies' section. The 'Policy Details' section includes the following fields and controls:

- Policy Type:** Access (selected)
- Policy Name:** A text input field with a search icon.
- Policy Label:** A text input field with the value 'Policy Label'.
- NiFi Registry Resource Identifier:** A text input field.
- Description:** A text area.
- Audit Logging:** YES (selected)
- enabled/normal:** Toggle switches, with 'enabled' selected.
- Add Validity Period:** A button.

The 'Allow Conditions' section shows a table with the following columns and controls:

Select Role	Select Group	Select User	Permissions	Delegate Admin	
Select Roles	Select Groups	Select Users	Add Permissions +	<input type="checkbox"/>	X

- Complete the Create Policy page as follows:

Table 37: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
NiFi Registry Resource Identifier	In a NiFi cluster, all nodes must be granted the ability to view and modify component data in order for user to list or empty queues in processor component outbound connections. With Ranger this can be accomplished by using a wildcard to grant all of the NiFi nodes read and write access to the /data/* NiFi resource.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.

Field	Description
Add Validity Period	Specify a start and end time for the policy.

Table 38: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Permissions	Add or edit permissions: Read, Write, Delete, Select/Deselect All.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

- You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
- You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
- Click Add.

Related Information

[SQL Standard Based Hive Authorization](#)

Configure a resource-based policy: Solr

How to add a new policy to an existing Solr service.

Procedure

- On the Service Manager page, select an existing Solr service.
The List of Policies page appears.

- Click Add New Policy.
The Create Policy page appears.

Policy Details :

Policy Type: **Access** Add Validity Period

Policy Name * enabled normal

Policy Label:

Solr Collection * include

Description:

Audit Logging: **YES**

Policy Conditions +

No Conditions

Allow Conditions : hide -

Select Role	Select Group	Select User	Policy Conditions	Permissions	Delegate Admin	
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="Select Users"/>	Add Conditions +	Add Permissions +	<input type="checkbox"/>	<input checked="" type="checkbox"/>

+

- Complete the Create Policy page as follows:

Table 39: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Solr Collection	Non-SSL: http:<host_ip>:8983/solr SSL: https:<host_ip>:8985/solr
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.
Add Validity Period	Specify a start and end time for the policy.

Field	Description
Policy Conditions (applied at the policy level)	Click the + icon, then specify an IP address range.

Table 40: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Policy Conditions (applied at the item level)	Specify an IP address range.
Permissions	Add or edit permissions: Query, Update, Others, Solr Admin, Select/Deselect All.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

- You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
- You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
- Click Add.

Related Information

[Wildcards and variables in resource-based policies](#)

Configure a resource-based policy: YARN

How to add a new policy to an existing YARN service.

Procedure

- On the Service Manager page, select an existing YARN service.
The List of Policies page appears.

- Click Add New Policy.
The Create Policy page appears.

Ranger Access Manager Audit Security Zone Settings admin

Service Manager > cm_yarn Policies > Create Policy

Create Policy

Policy Details :

Policy Type: **Access** Add Validity Period

Policy Name * enabled normal

Policy Label:

Queue * recursive

Description:

Audit Logging: **YES**

Allow Conditions : Hide

Select Role	Select Group	Select User	Permissions	Delegate Admin	
Select Roles	Select Groups	Select Users	Add Permissions +	<input type="checkbox"/>	X
+					

- Complete the Create Policy page as follows:

Table 41: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Queue	The YARN queue to which the policy applies.
Recursive	The default recursive setting specifies that the policy will also be applied to all sub-queues; you can also specify a non-recursive path.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.

Field	Description
Add Validity Period	Specify a start and end time for the policy.

Table 42: Allow Conditions

Label	Description
Select Role	Specify the roles to which this policy applies. To designate a role as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Select Group	Specify the groups to which this policy applies. To designate a group as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify the users to which this policy applies. To designate a user as an Administrator, select the Delegate Admin check box. Administrators can edit or delete the policy, and can also create child policies based on the original policy.
Permissions	Add or edit permissions: submit-app, admin-queue, Select/Deselect All.
Delegate Admin	You can use Delegate Admin to assign administrator privileges to the roles, groups, or users specified in the policy. Administrators can edit or delete the policy, and can also create child policies based on the original policy.

- You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
- You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
- Click Add.

Related Information

[Wildcard and variables in resource-based policies](#)

Wildcard and variables in resource-based policies

Reference for wildcards and variables in resource-based policies.

Ranger Authorization Resource Policy Wildcard Characters

Wildcard characters can be included in the resource path, the database name, the table name, or the column name:

- * indicates zero or more occurrences of characters
- ? indicates a single character

Ranger Authorization Resource Policy {USER} Variable

The variable {USER} can be used to autofill the accessing user, for example:

In Select User, choose {USER}.

In Resource Path, enter data_{USER}.

Ranger Authorization Resource Policy {USER} Variable Recommended Practices and Customizability

Ranger requires that string '{USER}' is used to represent accessing user as the user in the policy-item in a Ranger policy. However, Ranger provides flexible way of customizing the string that is used as shorthand to represent the

accessing user's name in the policy resource specification. By default, Ranger policy resource specification expects characters '{' and '}' as delimiters for string 'USER', however, ranger supports customizable way of specifying delimiter characters, escaping those delimiters, and the string 'USER' itself by prefixing it with another, user-specified string on a per resource-level basis in the service definition of each component supported by Ranger.

For example, if for a certain HDFS installation, if the path names may contain '{' or '}' as valid characters, but not '%' character, then the service-definition for HDFS can be specified as:

```
"resources": [
  {
    "itemId": 1,
    "name": "path",
    "type": "path",
    "level": 10,
    "parent": "",
    "mandatory": true,
    "lookupSupported": true,
    "recursiveSupported": true,
    "excludesSupported": false,
    "matcher": "org.apache.ranger.plugin.resourcematcher.RangerPathResourceMatcher",
    "matcherOptions": {"wildcard": true, "ignoreCase": false}, "replaceTokens": true, "tokenDelimiterStart": "%", "tokenDelimiterEnd": "%", "tokenDelimiterPrefix": "rangerToken:" }
    "validationRegex": "",
    "validationMessage": "",
    "uiHint": "",
    "label": "Resource Path",
    "description": "HDFS file or directory"
  }
]
```

Corresponding ranger policy for the use case for HDFS will be written as follow:

```
resource: path=/home/%rangerToken:USER%
user: {USER}
permissions: all, delegateAdmin=true
```

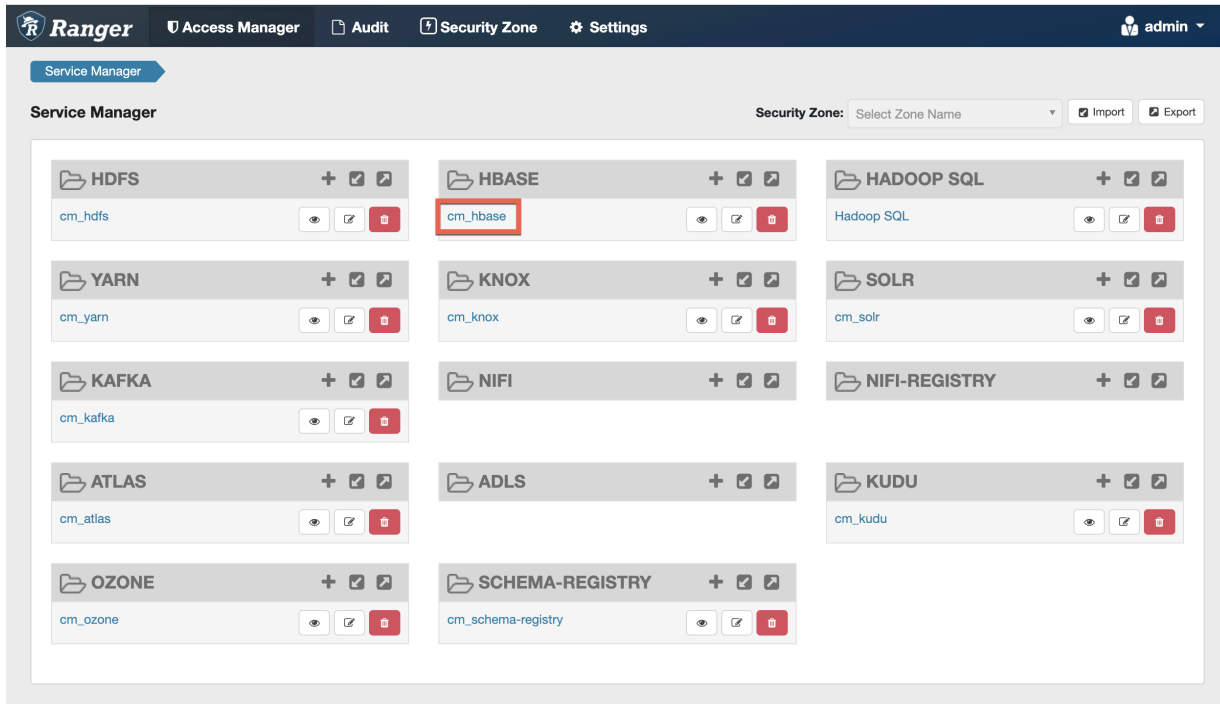
The following customizable matcherOptions are available for this feature:

- `replaceTokens`: true if short-hand for user in resource-spec needs to be replaced at run-time with current-user's name; false if the resource-spec needs to be interpreted as it is. Default value: true.
- `tokenDelimiterStart`: Identifies start character of short-hand for current-user in resource specification. Default value: {.
- `tokenDelimiterEnd`: Identifies end character of short-hand for current-user in resource specification. Default value: }.
- `tokenDelimiterEscape`: Identifies escape character for escaping `tokenDelimiterStart` or `tokenDelimiterEnd` values in resource specification. Default value: \.
- `tokenDelimiterPrefix`: Identifies special prefix which together with string 'USER' makes up short-hand for current-user's name in the resource specification. Default value: .

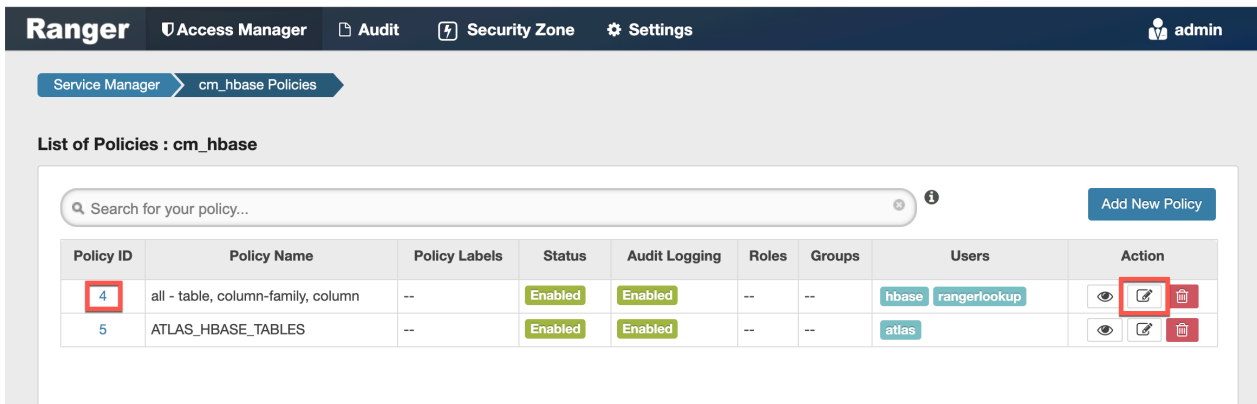
Preloaded resource-based services and policies

Apache Ranger includes preloaded resource-based services and policies.

- The preloaded resource-based services appear on the Service Manager page for resource-based policies, and are prefixed with "cm_", with the exception of Hadoop SQL, which applies to multiple SQL stack components (Hive, Impala, and Hue).



- To view the policies for each preloaded service, click the service name. To view policy details, click the applicable edit icon or policy ID number.



Index

- [cm_atlas](#)
- [cm_hbase](#)
- [cm_hdfs](#)
- [cm_kafka](#)
- [cm_knox](#)
- [cm_nifi](#)
- [cm_solr](#)
- [cm_yarn](#)

Hadoop SQL

cm_atlas

all - entity-type, entity-classification, entity, entity-business-metadata

This is a default policy of type "entity" that gives access to all entities and their business metadata attributes for the following users and groups, with the specified permissions:

- admin, dpprofiler, beacon – Update Business Metadata
- rangertagsync, rangerlookup – Read entity
- public group – Read entity

all - entity-type, entity-classification, entity

This is a default policy of type "entity" that gives access to all entities and their classifications for the following users and groups, with the specified permissions:

- admin, dpprofiler, beacon – Read, Create, Update, Delete entity & Add, Update, Remove classification
- rangertagsync, rangerlookup – Read entity
- public group – Read entity

all - entity-type, entity-classification, entity, entity-label

This is a default policy of type "entity" that gives access to all entities and classifications and their labels for the following users and groups, with the specified permissions:

- admin, dpprofiler, beacon – Add, Remove label
- rangertagsync, rangerlookup – Read entity
- public group – Read entity

all - relationship-type, end-one-entity-type, end-one-entity-classification, end-one-entity, end-two-entity-type, end-two-entity-classification, end-two-entity

This is a default policy of type "relationship" that gives access to all to all Entity-Relationships between End1-Entity-Type, End1-Entity-Classification, End1-Entity-ID and End2-Entity-Type, End2-Entity-Classification, End2-Entity-ID for the following users and groups, with the specified permissions:

- admin, dpprofiler, beacon – Add, Update, and Remove relationship
- public group – Add, Update, and Remove relationship

all - atlas-service

This is a default policy of type "atlas-service" that gives access to all atlas-services [export, import, purge, server] for the following users, with the specified permissions:

- admin, dpprofiler, beacon – Admin Export and Admin Import

all - type-category, type

This is a default policy of type "type-category" that gives access to all type categories [ENUM, ENTITY, CLASSIFICATION, RELATIONSHIP, STRUCT] and type names for the following users, with the specified permissions:

- admin, dpprofiler, beacon – Create, Update, and Delete type

Allow users to manage favorite searches

This is a default policy of type "entity-type" that gives access to __AtlasUserProfile and __AtlasUserSavedSearch resources which are internal types for favorite search. This policy provides Read, Create, Update, and Delete Entity permissions to validated users who create a favorite search.

cm_hbase

all - table, column-family, column

Provides access to all HBase tables, column-families, and columns to the following users, with the specified permissions:

- hbase, rangerlookup – Read, Write, Create, Admin

ATLAS_HBASE_TABLES

Provides access to all HBase column-families and columns in the atlas_janus and ATLAS_ENTITY_AUDIT_EVENTS HBase tables, to the following user, with the specified permissions:

- atlas – Read, Write, Create, Admin

cm_hdfs

all - path

Provides access to all HDFS resource paths to the following users, with the specified permissions:

- hdfs, rangerlookup – Read, Write, Execute

kms-audit-path

Provides access to the /ranger/audit/kms resource path to the following user, with the specified permissions:

- keyadmin – Read, Write, Execute

cm_kafka

all - topic

Provides access to all topics to the following users, with the specified permissions:

- kafka, rangerlookup, streamsmgmgr, streamsrepmgr – Publish, Consume, Configure, Describe, Create, Delete, Describe Configs, Alter Configs

all - cluster

Provides access to all clusters to the following users, with the specified permissions:

- kafka, rangerlookup, streamsmgmgr, streamsrepmgr – Configure, Describe, Create, Kafka Admin, Idempotent Write, Describe Configs, Alter Configs

all - transactionalid

Provides transactionalid access to the following users, with the specified permissions:

- kafka, rangerlookup, streamsmgmgr, streamsrepmgr – Publish, Describe

all - delegationtoken

Provides delegationtoken access to the following users, with the specified permissions:

- kafka, rangerlookup, streamsmgmgr, streamsrepmgr – Describe

ATLAS_HOOK

Provides ATLAS_HOOK topic access to the following users, with the specified permissions:

- hbase, hive, impala, mlgov – Publish
- atlas – Create, Configure, and Consume

ATLAS_ENTITIES

Provides ATLAS_ENTITIES topic access to the following users, with the specified permissions:

- atlas – Create, Configure, and Publish
- rangertagsync – Consume

ATLAS_SPARK_HOOK

Provides ATLAS_SPARK_HOOK topic access to the following user, with the specified permissions:

- atlas – Create, Configure, and Consume

Also provides ATLAS_SPARK_HOOK topic access to the following group, with the specified permissions:

- public – Publish

cm_knox

all - topology, service

Provides access to all Knox topologies and services to the following users, with the specified permissions:

- admin, rangerlookup – Allow

cm_nifi

all - nifi-resource

Provides access to all NiFi resource identifiers to the following user, with the specified permissions:

- rangerlookup – Read, Write

cm_solr

all - collection

Provides access to all Solr collections to the following users, with the specified permissions:

- solr, rangerlookup, ranger, atlas – Query, Update, Others, Solr Admin

RANGER_AUDITS_COLLECTION

Provides access to the RANGER_AUDITS_COLLECTION Solr collection to the following users, with the specified permissions:

- atlas, hbase, hdfs, hive, impala, kafka, knox, nifi, ranger, storm, yarn – Query, Update, Others
- ranger – Query, Update, Others, Solr Admin

cm_yarn

all - queue

Provides access to all YARN queues to the following users, with the specified permissions:

- yarn, rangerlookup – submit-app, admin-queue

Hadoop SQL

all - global

Provides global access to the following users, with the specified permission:

- hive, beacon, dpprofiler, hue, admin, impala, rangerlookup – Temporary UDF Admin



Note: The Ranger web UI may show additional permissions for the all-global policy, but the only valid permission is Temporary UDF Admin.

all - database, table, column

Provides access to all databases, tables, and columns to the following users, with the specified permissions:

- hive, rangerlookup, impala – Select, Update, Create, Drop, Alter, Index, Lock, All, Read, Write, ReplAdmin, Service Admin, Temporary UDF Admin, Refresh
- {OWNER} – All

all - database, table

Provides access to all databases and tables to the following users, with the specified permissions:

- hive, rangerlookup, impala – Select, Update, Create, Drop, Alter, Index, Lock, All, Read, Write, ReplAdmin, Service Admin, Temporary UDF Admin, Refresh
- {OWNER} – All

all - storage-type, storage-url

Ranger introduces new resources “storage-type” and “storage-url” in HadoopSQL Service and supports only one permission “RW Storage”. When a user creates / alters a table, they will be authorized against this resource policy. Users granted “RW Storage” permission on the resource representing the storage-type + storage-url, can create/alter the table in the respective storage. Provides access to all databases to the following users, with the RW Storage permission only:

- hive, rangerlookup, impala, beacon, dpprofiler, hue, admin



Note: {OWNER} macro should NOT be configured for StorageHandler policies.

all - database

Provides access to all databases to the following users, with the specified permissions:

- hive, rangerlookup, impala – Select, Update, Create, Drop, Alter, Index, Lock, All, Read, Write, ReplAdmin, Service Admin, Temporary UDF Admin, Refresh
- {OWNER} – All

Also provides access to all databases to the following group, with the specified permissions:

- public – Create

all - hiveservice

Provides hiveservice access to the following users, with the specified permissions:

- hive, rangerlookup, impala – Select, Update, Create, Drop, Alter, Index, Lock, All, Read, Write, ReplAdmin, Service Admin, Temporary UDF Admin, Refresh

all - database, udf

Provides database and udf access to the following users, with the specified permissions:

- hive, rangerlookup, impala – Select, Update, Create, Drop, Alter, Index, Lock, All, Read, Write, ReplAdmin, Service Admin, Temporary UDF Admin, Refresh
- {OWNER} – All

all - url

Provides url access to the following users, with the specified permissions:

- hive, rangerlookup, impala – Select, Update, Create, Drop, Alter, Index, Lock, All, Read, Write, ReplAdmin, Service Admin, Temporary UDF Admin, Refresh

default database tables columns

Provides access to all tables and columns in the default database to the following user, with the specified permissions:

- impala – Create

Also provides access to all tables and columns in the default database to the following group, with the specified permissions:

- public – Create

information_schema database tables columns

Provides access to all tables and columns in the information_schema database to the following user, with the specified permissions:

- impala – Select

Also provides access to all tables and columns in the information_schema database to the following group, with the specified permissions:

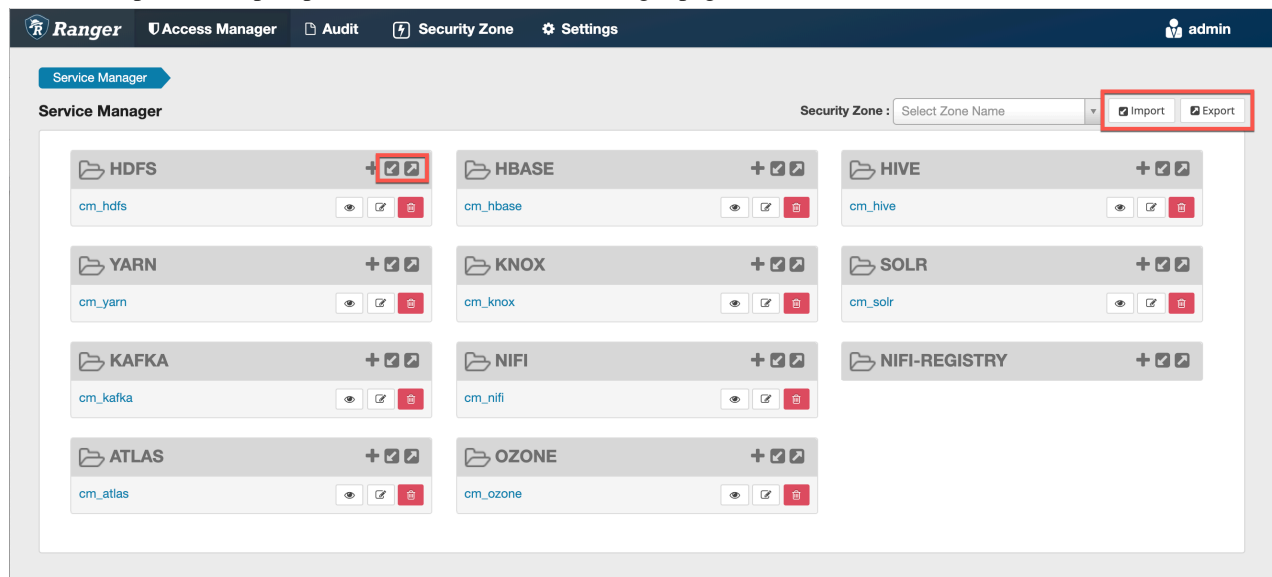
- public – Select

Importing and exporting resource-based policies

You can export and import policies from the Ranger Admin UI for cluster resiliency (backups), during recovery operations, or when moving policies from test clusters to production clusters. You can export/import a specific subset of policies (such as those that pertain to specific resources or user/groups) or clone the entire repository (or multiple repositories) via Ranger Admin UI.

Interfaces

You can import and export policies from the Service Manager page:



You can also export policies from the Reports page:

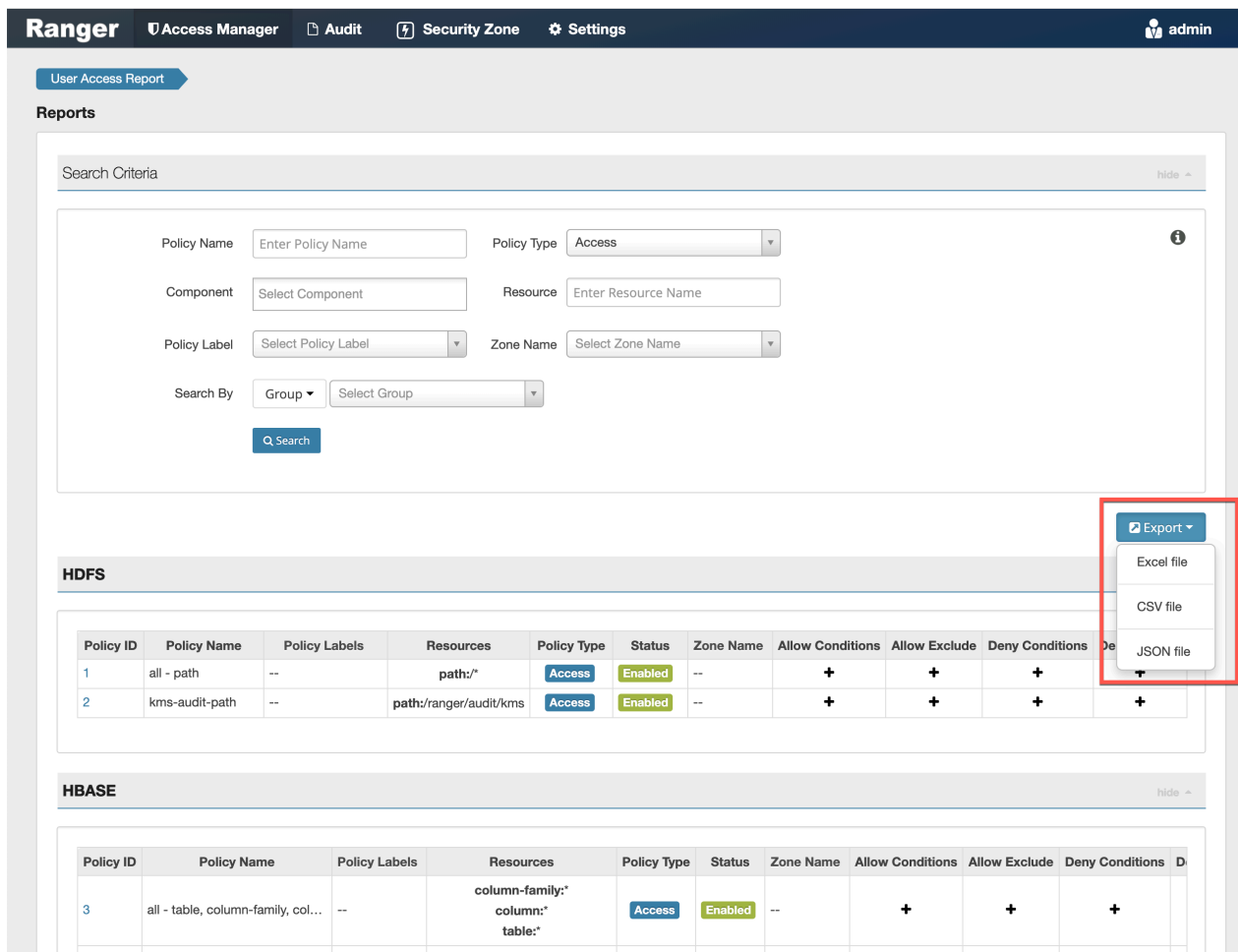


Table 43: Export Policy Options

	Service Manager Page	Reports Page
Formats	JSON	JSON Excel CSV
Filtering Supported	No	Yes
Specific Service Export	Yes	Via filtering

Filtering

When exporting from the Reports page, you can apply filters before saving the file.

Export Formats

You can export policies in the following formats:

- Excel
- JSON
- CSV

Note: CSV format is not supported for importing policies.

When you export policies from the Service Manager page, the policies are automatically downloaded in JSON format. If you wish to export in Excel or CSV format, export the policies from the Reports page dropdown menu.

Required User Roles

The Ranger admin user can import and export only Resource & Tag based policies. The credentials for this user are set in Ranger Configs > Advanced ranger-env in the fields labeled admin_username (default: admin/admin).

The Ranger KMS keyadmin user can import and export only KMS policies. The default credentials for this user are keyadmin/keyadmin.

Limitations

To successfully import policies, use the following database versions:

- MariaDB: 10.1.16+
- MySQL: 5.6.x+
- Oracle: 11gR2+
- PostgreSQL: 8.4+
- MS SQL: 2008 R2+

Partial import is not supported.

Related Information

[Importing and exporting tag-based policies](#)

Import resource-based policies for a specific service

How to import resource-based policies for a specific service (HBase, YARN, etc.).

Procedure

1. On the Service Manager page, click the Import icon for the service:



The Import Policy page appears.


2. Select the file to import.

You can only import policies in JSON format.


Security Zone : Select

Import Policy ✕

Select File :

Select file  Override Policy :

Ranger_Policies_20190717_190622.json ✕

 All services gets listed on service destination when Zone destination is blank. When zone is selected at destination, then only services associated with that zone will be listed.

Specify Zone Mapping :

Source	To	Destination
	To	No zone selected ▼

Specify Service Mapping :

Source	To	Destination
cm_hdfs ✕ ▼	To	Select service name ▼ ✕

CancelImport

3. (Optional) Configure the import operation:
 - a) The Override Policy option deletes all policies of the destination repositories.
 - b) Zone Mapping – when no destination is selected, all services are imported. When a destination is selected, only the services associated with that security zone are imported.
 - c) Service Mapping maps the downloaded file repository, i.e. source repository to destination repository. You can use the red x symbols to remove services from the import. Scroll down to view all service mappings.

Import Policy

Specify Zone Mapping :

Source: [] To Destination: [No zone selected]

Specify Service Mapping :

Source	To	Destination	
cm_hdfs	To	cm_hdfs	X
cm_hbase	To	cm_hbase	X
cm_yarn	To	cm_yarn	X
cm_hive	To	cm_hive	X
cm_knox	To	cm_knox	X
cm_storm	To	cm_storm	X

Buttons: Cancel, Import

4. Click Import.
A confirmation message appears after the file is imported.

Related Information

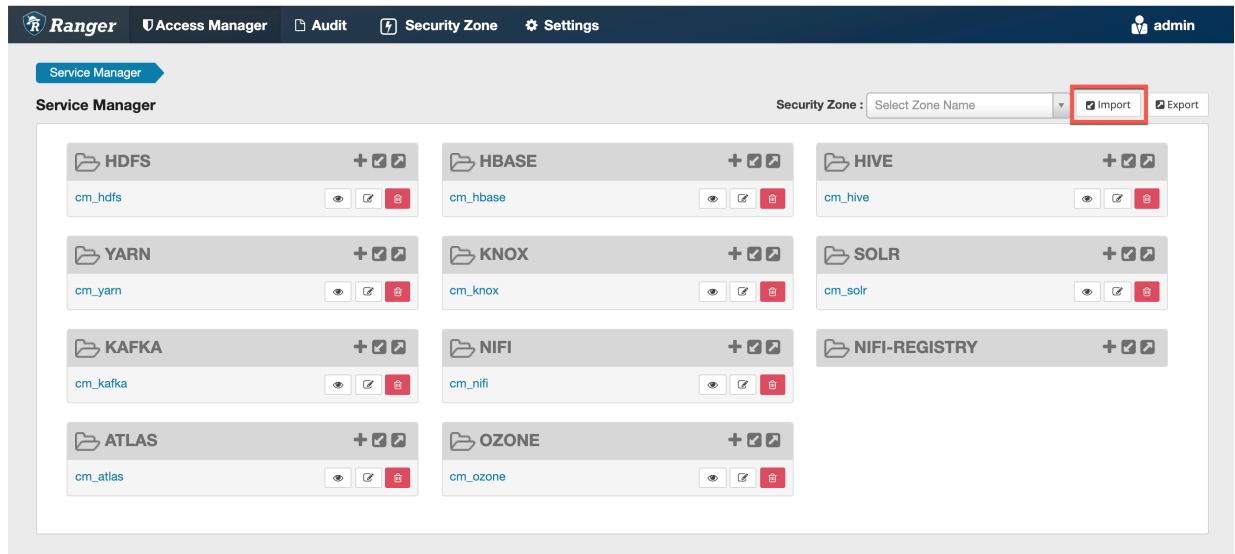
[Import resource-based policies for all services](#)

Import resource-based policies for all services

How to import policies for all services.

Procedure


1. On the Service Manager page, click Import.



The Import Policy page appears.

Import Policy ✕

Select File :

Select file  Override Policy :

Ranger_Policies_20190717_190622.json ✕

i All services gets listed on service destination when Zone destination is blank. When zone is selected at destination, then only services associated with that zone will be listed.

Specify Zone Mapping :

Source		Destination
<input type="text"/>	To	<input type="text" value="No zone selected"/>

Specify Service Mapping :

Source		Destination
<input type="text" value="cm_hdfs"/>	To	<input type="text" value="cm_hdfs"/>

Cancel Import

2. Select the file to import.
You can only import policies in JSON format.

3. (Optional) Configure the import operation:
 - a) The Override Policy option deletes all policies of the destination repositories.
 - b) Zone Mapping – when no destination is selected, all services are imported. When a destination is selected, only the services associated with that security zone are imported.
 - c) Service Mapping maps the downloaded file repository, i.e. source repository to destination repository. You can use the red x symbols to remove services from the import. Scroll down to view all service mappings.

Import Policy [Close]

Specify Zone Mapping :

Source: [] To Destination: [No zone selected]

Specify Service Mapping :

Source	To	Destination	Action
cm_hdfs	To	cm_hdfs	X
cm_hbase	To	cm_hbase	X
cm_yarn	To	cm_yarn	X
cm_hive	To	cm_hive	X
cm_knox	To	cm_knox	X
cm_storm	To	cm_storm	X

[Cancel] [Import]

4. Click Import.
A confirmation message appears after the file is imported.

Related Information

[Import resource-based policies for a specific service](#)

Export resource-based policies for a specific service

How to export the policies for a specific service (HBase, YARN, etc).

About this task

If you would like to export in Excel or CSV format, export the policies from the Reports page dropdown menu.

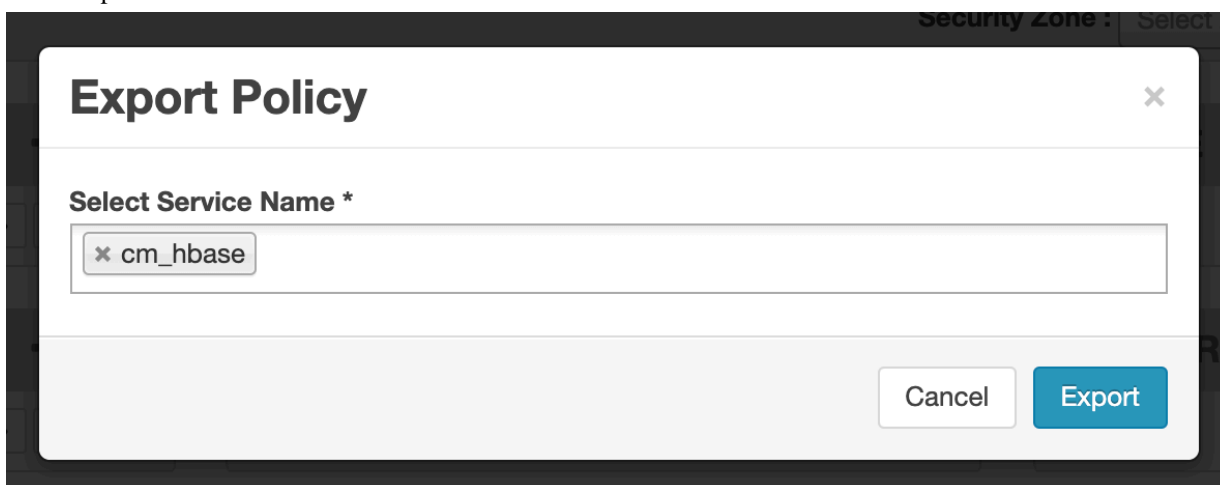
Procedure

1. On the Service Manager page, click the Export icon for the service:



The Export Policy page appears.

2. Click Export.



The file downloads in your browser as a JSON file.

Related Information

[Export all resource-based policies for all services](#)

Export all resource-based policies for all services

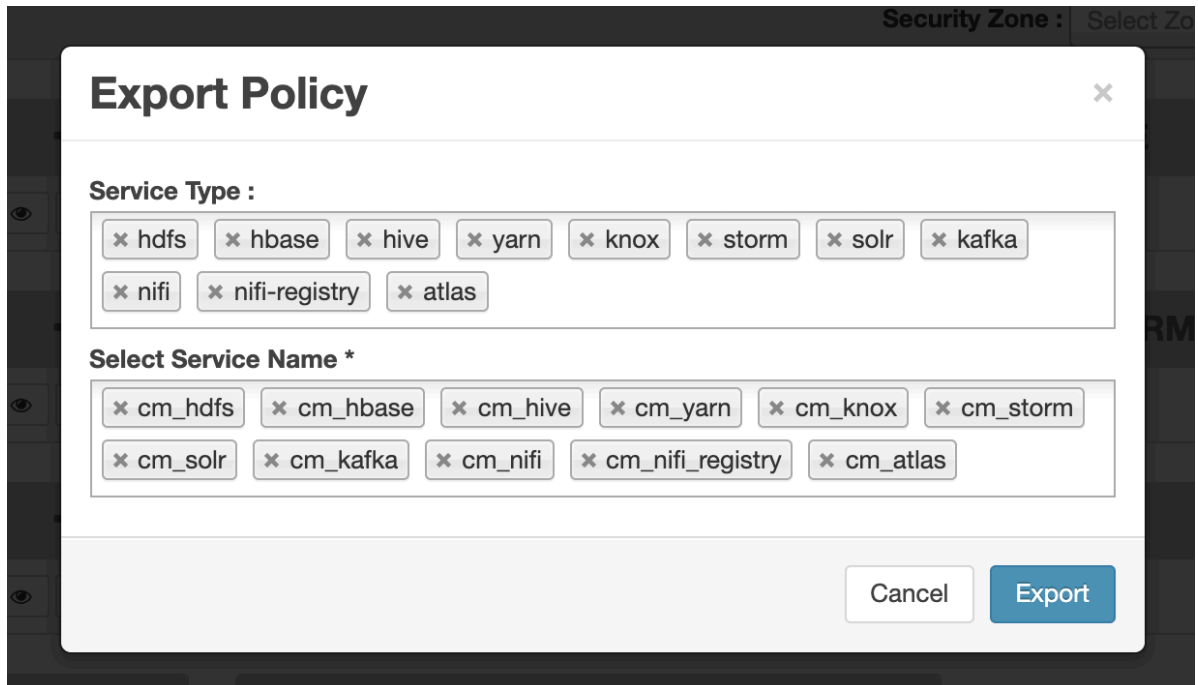
How to export the policies for all service.

About this task

If you would like to export in Excel or CSV format, export the policies from the Reports page drop-down menu.

Procedure

- From the Service Manager page:
 - a) Click Export.
The Export Policy page appears.
 - b) Remove components or specific services, then click Export.



The file downloads in your browser as a JSON file.

- From the Reports page:
 - Apply filters before exporting the file.
 - Open the Export drop-down menu:

The screenshot shows the Ranger 'User Access Report' page. At the top, there are navigation tabs for 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The 'Reports' section contains a 'Search Criteria' form with fields for Policy Name, Component, Policy Label, Resource, and Zone Name, along with a 'Search By' dropdown and a search button. Below the search criteria are two tables: 'HDFS' and 'HBASE'. The 'HDFS' table has two rows of policies, and the 'HBASE' table has one row. An 'Export' dropdown menu is open on the right side of the 'HDFS' table, showing options for 'Excel file', 'CSV file', and 'JSON file'.

- Select the file format.
The file downloads in your browser.

Related Information

[Export resource-based policies for a specific service](#)

Row-level filtering and column masking in Hive

You can use Apache Ranger row-level filters to set access policies for rows in Hive tables. You can also use Ranger column masking to set policies that mask data in Hive columns, for example to show only the first or last four characters of column data.



Note: To prevent possible data loss, row filtering and masking policies must exclude users that run compaction. For more information about excluding compaction users from Ranger policies, see [Compaction prerequisites in Managing Apache Hive](#).

Related Information

[Compaction prerequisites](#)

Row-level filtering in Hive with Ranger policies

Row-level filtering helps simplify Hive queries. By moving the access restriction logic down into the Hive layer, Hive applies the access restrictions every time data access is attempted. This helps simplify authoring of the Hive query, and provides seamless behind-the-scenes enforcement of row-level segmentation without having to add this logic to the predicate of the query.

About this task

Row-level filtering also improves the reliability and robustness of Hadoop. By providing row-level security to Hive tables and reducing the security surface area, Hive data access can be restricted to specific rows based on user characteristics (such as group membership) and the runtime context in which this request is issued.

Typical use cases where row-level filtering can be beneficial include:

- A hospital can create a security policy that allows doctors to view data rows only for their own patients, and that allows insurance claims administrators to view only specific rows for their specific site.
- A bank can create a policy to restrict access to rows of financial data based on the employee's business division, locale, or based on the employee's role (for example: only employees in the finance department are allowed to see customer invoices, payments, and accrual data; only European HR employees can see European employee data).
- A multi-tenant application can create logical separation of each tenant's data so that each tenant can see only their own data rows.

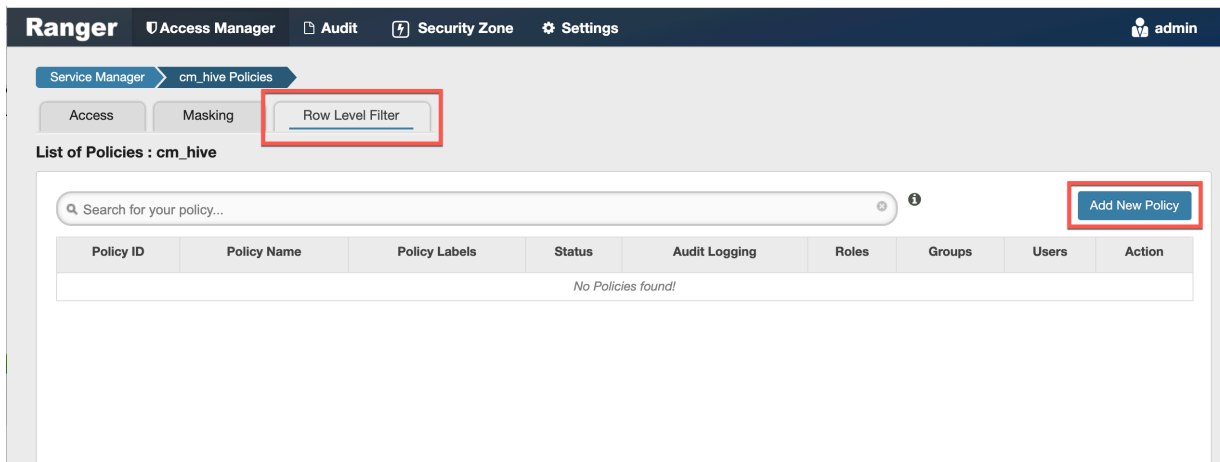
You can use Apache Ranger row-level filters to set access policies for rows in Hive tables. Row-level filter policies are similar to other Ranger access policies. You can set filters for specific users, groups, and conditions.

The following conditions apply when using row-level filters:

- The filter expression must be a valid WHERE clause for the table or view.
- Each table or view should have its own row-level filter policy.
- Wildcard matching is not supported on database or table names.
- Filters are evaluated in the order listed in the policy.
- An audit log entry is generated each time a row-level filter is applied to a table or view.

Procedure

1. On the Service Manager page, select an existing Hive Service.
2. Select the Row Level Filter tab, then click Add New Policy.



3. On the Create Policy page, add the following information for the row-level filter:

Table 44: Policy Details

Field	Description
Policy Name (required)	Enter an appropriate policy name. This name cannot be duplicated across the system. The policy is enabled by default.

Field	Description
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Hive Database (required)	Type in the applicable database name. The auto-complete feature displays available databases based on the entered text.
Hive Table (required)	Type in the applicable table name. The auto-complete feature displays available tables based on the entered text.
Audit Logging	Audit Logging is set to Yes by default. Select No to turn off audit logging.
Description	Enter an optional description for the policy.
Add Validity Period	Specify a start and end time for the policy.

Table 45: Row Filter Conditions

Label	Description
Select Role	Specify the roles to which this policy applies.
Select Group	Specify the groups to which this policy applies. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify one or more users to which this policy applies.
Access Types	Currently select is the only available access type. This will be used in conjunction with the WHERE clause specified in the Row Level Filter field.

Label	Description
Add Row Filter	<ul style="list-style-type: none"> To create a row filter for the specified users, groups, and roles, Click Add Row Filter, then type a valid WHERE clause in the Enter filter expression box. To allow Select access for the specified users and groups without row-level restrictions, do not add a row filter (leave the setting as "Add Row Filter"). Filters are evaluated in the order listed in the policy. The filter at the top of the Row Filter Conditions list is applied first, then the second, then the third, and so on.

Ranger
Access Manager
Audit
Security Zone
Settings
admin

Service Manager
cm_hive Policies
Create Policy

Create Policy

i Please ensure that users/groups listed in this policy have access to the table via an Access Policy. This policy does not implicitly grant access to the table. x

Policy Details :

Policy Type Row Level Filter Add Validity Period

Policy Name * enabled normal

Policy Label

Hive Database *

Hive Table *

Description

Audit Logging YES

Row Filter Conditions :

Select Role	Select Group	Select User	Access Types	
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="x admin"/>	Add Permissions +	Add Row Filter +
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="x systest"/>	Add Permissions +	Add Row Filter +
<input type="text" value="Select Roles"/>	<input type="text" value="x public"/>	<input type="text" value="Select Users"/>	Add Permissions +	Add Row Filter +

Add
Cancel

Enter filter expression

✓
x

- To move a condition in the Row Filter Conditions list (and therefore change the order in which it is evaluated), click the dotted rows icon at the left of the condition row, then drag the condition to a new position in the list.

Ranger Access Manager Audit Security Zone Settings admin

Service Manager cm_hive Policies Create Policy

Create Policy

Please ensure that users/groups listed in this policy have access to the table via an Access Policy. This policy does not implicitly grant access to the table.

Policy Details :

Policy Type **Row Level Filter** Add Validity Period

Policy Name * **enabled** **normal**

Policy Label

Hive Database *

Hive Table *

Description

Audit Logging **YES**

Row Filter Conditions : hide

Select Role	Select Group	Select User	Access Types	Row Level Filter	
Select Roles	Select Groups	* admin	Add Permissions +	Add Row Filter +	✕
Select Roles	Select Groups	* systest	Add Permissions +	Add Row Filter +	✕
Select Roles	* public	Select Users	Add Permissions +	Add Row Filter +	✕

+ Add Cancel

- Click Add to add the new row-level filter policy.

Dynamic resource-based column masking in Hive with Ranger policies

You can use Apache Ranger dynamic resource-based column masking capabilities to protect sensitive data in Hive in near real-time. You can set policies that mask or anonymize sensitive data columns (such as PII, PCI, and PHI) dynamically from Hive query output. For example, you can mask sensitive data within a column to show only the first or last four characters.

About this task

Dynamic column masking policies are similar to other Ranger access policies for Hive. You can set filters for specific users, groups, and conditions. With dynamic column-level masking, sensitive information never leaves Hive, and no changes are required at the consuming application or the Hive layer. There is also no need to produce additional protected duplicate versions of datasets.

The following conditions apply when using Ranger column masking policies to mask data returned in Hive query results:

- A variety of masking types are available, such as show last 4 characters, show first 4 characters, Hash, Nullify, and date masks (show only year).

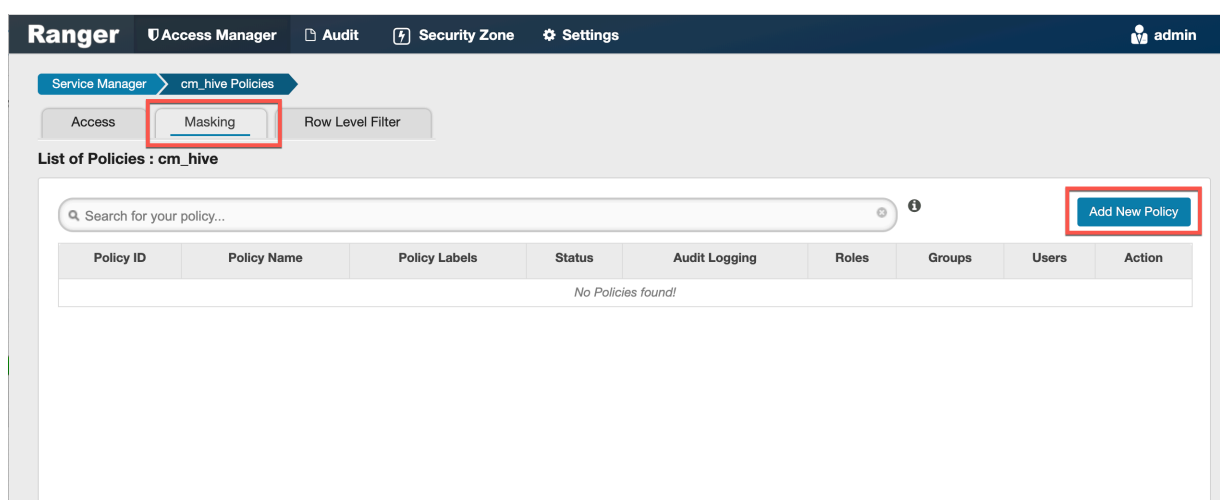


Note: Ranger depends on Hive/Impala's hashing functions for hash masking.

- Impala uses sha512 in FIPS mode, sha256 in non-FIPS mode.
- Hive uses sha256. Plans to update to sha512 in FIPS mode.
- You can specify a masking type for specific users, groups, and conditions.
- Wildcard matching is not supported.
- Each column should have its own masking policy.
- Masks are evaluated in the order listed in the policy.
- An audit log entry is generated each time a masking policy is applied to a column.

Procedure

1. In Service Manager, select an existing Hive Service.
2. Select the Masking tab, then click Add New Policy.



3. In Create Policy, add the following information for the column-masking filter:

Table 46: Policy Details

Field	Description
Policy Name (required)	Enter an appropriate policy name. This name cannot be duplicated across the system. The policy is enabled by default.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
Hive Database (required)	Type in the applicable database name. The auto-complete feature displays available databases based on the entered text.
Hive Table (required)	Type in the applicable table name. The auto-complete feature displays available tables based on the entered text.
Hive Column (required)	Type in the applicable column name. The auto-complete feature displays available columns based on the entered text.
Audit Logging	Audit Logging is set to Yes by default. Select No to turn off audit logging.

Field	Description
Description	Enter an optional description for the policy.
Add Validity Period	Specify a start and end time for the policy.

Table 47: Mask Conditions

Label	Description
Select Role	Specify the roles to which this policy applies.
Select Group	Specify the groups to which this policy applies. The public group contains all users, so granting access to the public group grants access to all users.
Select User	Specify one or more users to which this policy applies.
Access Types	Currently, select is the only available access type.

Label	Description
<p>Select Masking Type</p>	<p>To create a row filter for the specified users, groups, and roles, click Select Masking Option, then select a masking type:</p> <ul style="list-style-type: none"> • Redact – mask all alphabetic characters with "x" and all numeric characters with "n". • Partial mask: show last 4 – Show only the last four characters. • Partial mask: show first 4 – Show only the first four characters. • Hash – Replace all characters with a hash of entire cell value. • Nullify – Replace all characters with a NULL value. • Unmasked (retain original value) – No masking is applied. • Date: show only year – Show only the year portion of a date string and default the month and day to 01/01 • Custom – Specify a custom masked value or expression. Custom masking can use any valid Hive UDF (Hive that returns the same data type as the data type in the column being masked). <p>Masking conditions are evaluated in the order listed in the policy. The condition at the top of the Masking Conditions list is applied first, then the second, then the third, and so on.</p>

- To move a condition in the Mask Conditions list (and therefore change the order in which it is evaluated), click the dotted rows icon at the left of the condition row, then drag the condition to a new position in the list.

The screenshot shows the Ranger web interface for creating a policy. The 'Policy Details' section includes fields for Policy Type (Masking), Policy Name, Policy Label, Hive Database, Hive Table, Hive Column, Description, and Audit Logging (set to YES). The 'Mask Conditions' section is a table with columns: Select Role, Select Group, Select User, Access Types, and Select Masking Option. The table contains three rows of conditions. A red box highlights the dotted rows icon in the first column of the third row, which is highlighted in yellow. Below the table are 'Add' and 'Cancel' buttons.

Select Role	Select Group	Select User	Access Types	Select Masking Option
Select Roles	Select Groups	× hive	Add Permissions +	Unmasked (retain original value) ✕
Select Roles	Select Groups	× systest	Add Permissions +	Partial mask: show last 4 ✕
Select Roles	× public	Select Users	Add Permissions +	Select Masking Option + ✕

- Click Add to add the new column masking filter policy.

Dynamic tag-based column masking in Hive with Ranger policies

Where Ranger resource-based masking policy for Hive anonymizes data from a Hive column identified by the database, table, and column, Ranger tag-based masking policy anonymizes Hive column data based on tags and tag attribute values associated with Hive column (usually specified as metadata classification in Atlas).

About this task

The following conditions apply when using Ranger column masking policies to mask data returned in Hive query results:

- A variety of masking types are available, such as show last 4 characters, show first 4 characters, Hash, Nullify, and date masks (show only year).



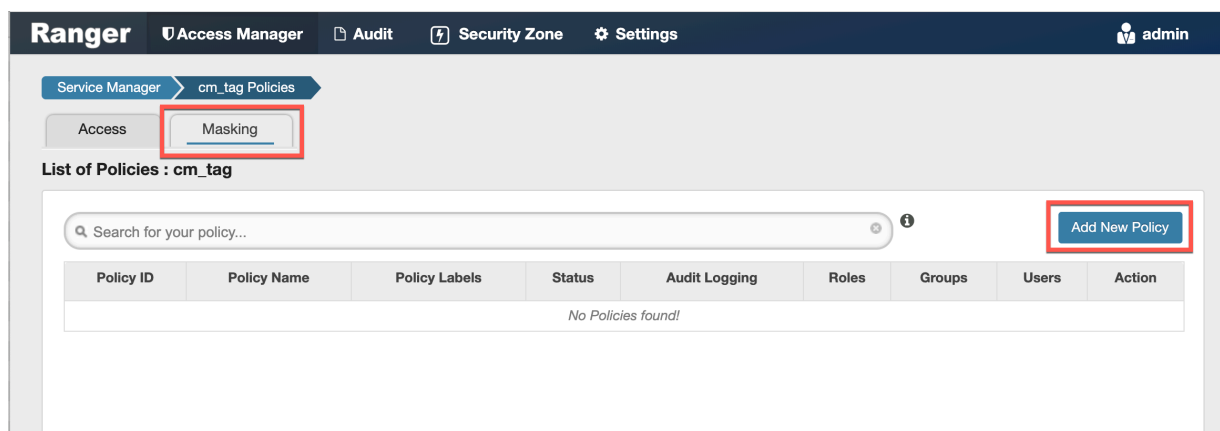
Note: Ranger depends on Hive/Impala's hashing functions for hash masking.

- Impala uses sha512 in FIPS mode, sha256 in non-FIPS mode.
- Hive uses sha256. Plans to update to sha512 in FIPS mode.

- You can specify a masking type for specific users, groups, and conditions.
- Wildcard matching is not supported.
- If there are multiple tag masking policies applied to the same Hive column, the masking policy with the lexicographically smallest policy-name is chosen for enforcement, E.G., policy "a" is enforced before policy "aa".
- Masks are evaluated in the order listed in the policy.
- An audit log entry is generated each time a masking policy is applied to a column.

Procedure

1. Select Access Manager Tag Based Policies , then select a tag-based service.
2. Select the Masking tab, then click Add New Policy.



3. In Create Policy, add the following information for the column-masking filter:

Table 48: Policy Details

Field	Description
Policy Type (required)	Set to Masking by default.
Policy Name (required)	Enter an appropriate policy name. This name cannot be duplicated across the system. The policy is enabled by default.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
TAG (required)	Enter the applicable tag name, for example MASK.
Audit Logging	Audit Logging is set to Yes by default. Select No to turn off audit logging.
Description	Enter an optional description for the policy.
Add Validity Period	Specify a start and end time for the policy.

Field	Description
Policy Conditions (applied at the policy level)	<p>Click the + icon to add policy conditions. Currently "Accessed after expiry_date? (yes/no)" is the only available policy condition.</p> <p>"Accessed after expiry_date (yes/no)": To set this condition, type yes in the text box, then click check mark to add the condition.</p> <p>Enter boolean expression: Available for allow or deny conditions on tag-based policies. For examples and details, see "Using Tag Attributes and Values in Ranger Tag-Based Policy Conditions".</p> <p>Click Save to save the policy condition.</p>

Table 49: Mask Conditions

Label	Description
Select Role	Specify the roles to which this policy applies.
Select Group	<p>Specify the groups to which this policy applies.</p> <p>The public group contains all users, so granting access to the public group grants access to all users.</p>
Select User	Specify one or more users to which this policy applies.
Policy Conditions (applied at the item level)	<p>Click Add Conditions to add policy conditions. Currently "Accessed after expiry_date? (yes/no)" is the only available policy condition.</p> <p>"Accessed after expiry_date (yes/no)": To set this condition, type yes in the text box, then click check mark to add the condition.</p> <p>Enter boolean expression: Available for allow or deny conditions on tag-based policies. For examples and details, see "Using Tag Attributes and Values in Ranger Tag-Based Policy Conditions".</p>
Access Types	Currently select is the only available access type for the hive component.

Label	Description
Select Masking Option	<p>To create a row filter for the specified users, groups, and roles, click Select Masking Option, then select a masking type:</p> <ul style="list-style-type: none"> • Redact – mask all alphabetic characters with "x" and all numeric characters with "n". • Partial mask: show last 4 – Show only the last four characters. • Partial mask: show first 4 – Show only the first four characters. • Hash – Replace all characters with a hash of entire cell value. • Nullify – Replace all characters with a NULL value. • Unmasked (retain original value) – No masking is applied. • Date: show only year – Show only the year portion of a date string and default the month and day to 01/01 • Custom – Specify a custom masked value or expression. Custom masking can use any valid Hive UDF (Hive that returns the same data type as the data type in the column being masked). <p>Masking conditions are evaluated in the order listed in the policy. The condition at the top of the Masking Conditions list is applied first, then the second, then the third, and so on.</p>

4. Click + to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
5. Click Add to add the new policy.

Related Information

[Using tag attributes and values in Ranger tag-based policy conditions](#)

Tag-based Services and Policies

Ranger enables you to create tag-based services and add access policies to those services.

Adding a tag-based service


How to add a tag-based service to Ranger.

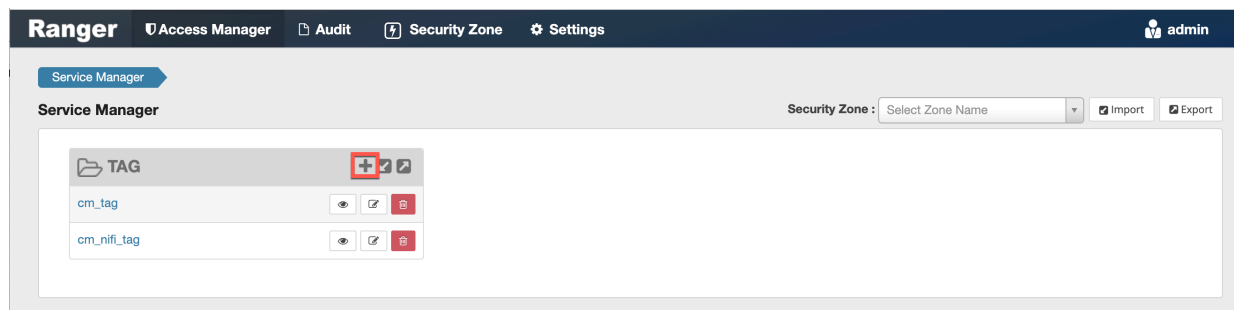
About this task

You can use the Service Manager for Tag-Based Policies page to create tag-based services and add tag-based access policies that can be applied to Hadoop resources. Using tag-based policies enables you to control access to resources across multiple Hadoop components without creating separate services and policies in each component. You can also use Ranger TagSync to synchronize the Ranger tag store with an external metadata service such as Apache Atlas.

Procedure

1.

Select Access Manager > Tag Based Policies, then click the Add icon () in the TAG box on the Service Manager page.



- On the Create Service page, type in a service name and an optional description. The service is enabled by default, but you can disable it by selecting Disabled. To add the service, click Add.

The screenshot shows the 'Create Service' page in the Ranger interface. The page has a dark blue header with the 'Ranger' logo and navigation links for 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. The main content area is titled 'Create Service' and contains two sections: 'Service Details' and 'Config Properties'.

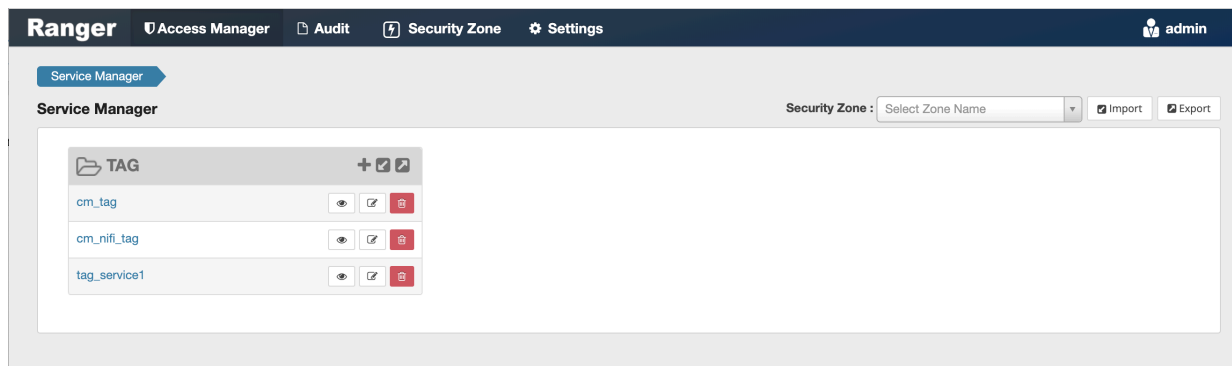
Service Details:

- Service Name *:** tag_service1
- Description:** (empty text area)
- Active Status:** Enabled Disabled

Config Properties:

Below this section is a table with columns 'Name' and 'Value'. There is a '+ Add New Configurations' button and a 'Test Connection' button. At the bottom of the form are 'Add' and 'Cancel' buttons.

- The new tag service appears on the Service Manager page.



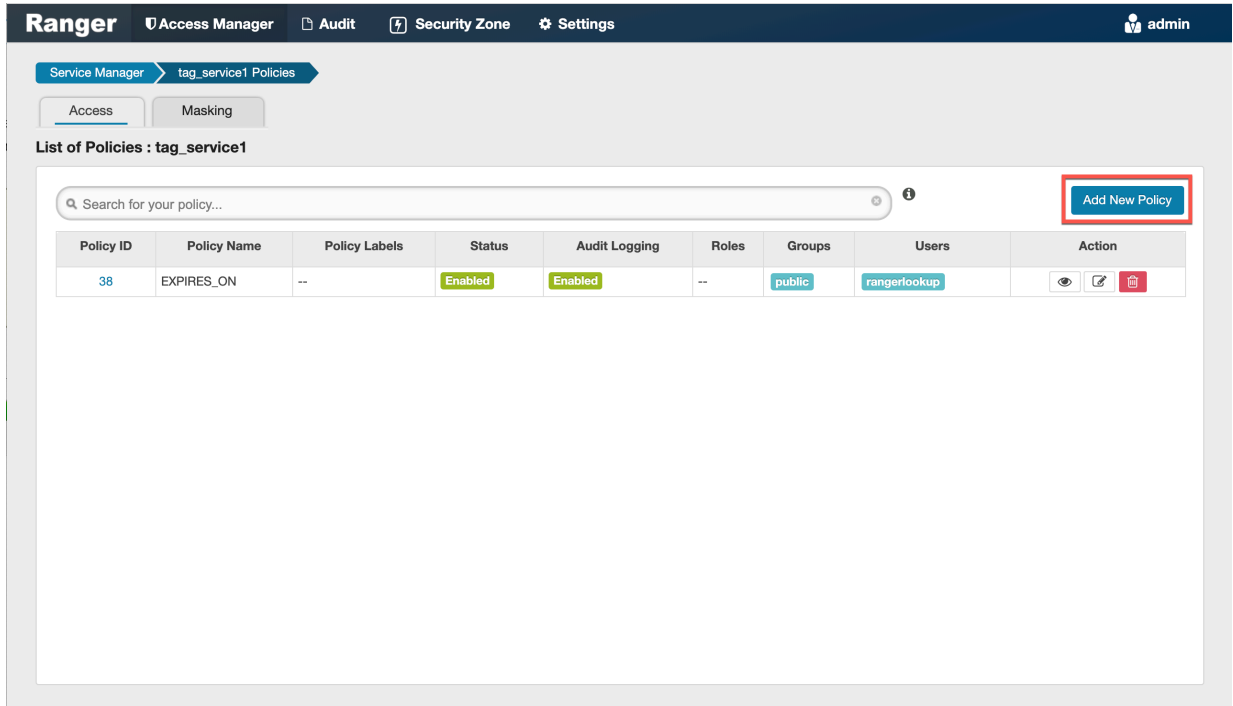
Adding tag-based policies

Tag-based policies enable you to control access to resources across multiple Hadoop components without creating separate services and policies in each component. You can also use Ranger TagSync to synchronize the Ranger tag store with an external metadata service such as Apache Atlas.




Procedure

- Select Access Manager > Tag Based Policies, then select a tag-based service.

2. The List of Policies page appears with the Access tab selected by default. Click Add New Policy.



The screenshot shows the Ranger Access Manager interface. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user is logged in as 'admin'. The breadcrumb trail shows 'Service Manager > tag_service1 Policies'. There are two tabs: 'Access' (selected) and 'Masking'. Below the tabs, the title is 'List of Policies : tag_service1'. A search bar is present with the placeholder text 'Search for your policy...'. To the right of the search bar is an 'Add New Policy' button, which is highlighted with a red rectangular box. Below the search bar is a table with the following data:

Policy ID	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
38	EXPIRES_ON	--	Enabled	Enabled	--	public	rangerlookup	  

The Create Policy page appears:

Ranger Access Manager Audit Security Zone Settings admin

Service Manager > tag_service1 Policies > Create Policy

Create Policy

Policy Details :

Policy Type: **Access** Add Validity Period

Policy Name * enabled normal

Policy Label:

TAG *

Description:

Audit Logging: **YES**

Policy Conditions +

No Conditions

Allow Conditions : hide -

Select Role	Select Group	Select User	Policy Conditions	Component Permissions	
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="Select Users"/>	Add Conditions +	Add Permissions +	<input type="button" value="x"/>
+ hide -					
⚠ Exclude from Allow Conditions :					
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="Select Users"/>	Add Conditions +	Add Permissions +	<input type="button" value="x"/>
+					

Deny Conditions : hide -

Select Role	Select Group	Select User	Policy Conditions	Component Permissions	
<input type="text" value="Select Roles"/>	<input type="text" value="Select Groups"/>	<input type="text" value="Select Users"/>	Add Conditions +	Add Permissions +	<input type="button" value="x"/>

3. Enter information on the Create Policy page as follows:

Table 50: Policy Details

Field	Description
Policy Type	Set to Access by default.
Policy Name	Enter a unique policy name. This name cannot be duplicated across the system. This field is mandatory.
normal/override	Enables you to specify an override policy. When override is selected, the access permissions in the policy override the access permissions in existing policies. This feature can be used with Add Validity Period to create temporary access policies that override existing policies.
TAG	Enter the applicable tag name.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).

Field	Description
Policy Label	Specify a label for this policy. You can search reports and filter policies based on these labels.
Add Validity Period	Specify a start and end time for the policy.
Policy Conditions (applied at the policy level)	<p>Click the + icon to add policy conditions. Currently "Accessed after expiry_date? (yes/no)" is the only available policy condition.</p> <p>"Accessed after expiry_date (yes/no)?: To set this condition, type yes in the text box, then click the check mark button to add the condition.</p> <p>Enter boolean expression: Available for allow or deny conditions on tag-based policies. For examples and details, see "Using Tag Attributes and Values in Ranger Tag-Based Policy Conditions".</p> <p>Click Save to save the policy condition.</p>

Table 51: Allow, Exclude from Allow, Deny, and Exclude from Deny Conditions

Label	Description
Select Role	Specify the roles to which this policy applies.
Select Group	<p>Specify the group to which this policy applies. To designate the group as an Administrator for the chosen resource, specify Admin permissions. (Administrators can create child policies based on existing policies).</p> <p>The public group contains all users, so setting a condition for the public group applies to all users.</p>
Select User	Specify a particular user to which this policy applies (outside of an already-specified group) OR designate a particular user as Admin for this policy. (Administrators can create child policies based on existing policies).
Policy Conditions (applied at the item level)	<p>Click Add Conditions to add policy conditions. Currently "Accessed after expiry_date? (yes/no)" is the only available policy condition.</p> <p>"Accessed after expiry_date (yes/no)?: To set this condition, type yes in the text box, then click the check mark button to add the condition.</p> <p>Enter boolean expression: Available for allow or deny conditions on tag-based policies. For examples and details, see "Using Tag Attributes and Values in Ranger Tag-Based Policy Conditions".</p>
Component Permissions	Click Add Permissions to add or edit component conditions. To add component permissions, enter the component name in the text box, then use the check boxes to specify component permissions. Click the check mark button to add the chosen component conditions to the policy.

- You can use the Plus (+) symbols to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
- You can use Deny All Other Accesses to deny access to all other users, groups, and roles other than those specified in the allow conditions for the policy.
- Click Add to add the new policy.

Related Information

[Using tag attributes and values in Ranger tag-based policy conditions](#)

Using tag attributes and values in Ranger tag-based policy conditions

Enter boolean expression allows Ranger to use tag attributes and values when configuring tag-based policy Allow or Deny conditions. It allows admins to provide boolean expression(s) using tag attributes.

The policy condition is introduced in the tag service definition:

```
{
  "itemId":2,
  "name":"expression",
  "evaluator": "org.apache.ranger.plugin.conditionevaluator.RangerScriptConditionEvaluator",
  "evaluatorOptions" : {"engineName":"JavaScript", "ui.isMultiline":"true"},
  "label":"Enter boolean expression",
  "description": "Boolean expression"
}
```

The following variables can be referenced in the boolean expression:

- `ctx`: Context handler containing APIs to access metadata information from the request.
- `tag`: Information about the current tag.
- `tagAttr`: Map containing all the current tag attributes and corresponding values.

The following APIs available from the request:

- `getUser()`: Returns a string.
- `getUserGroups()`: Returns a set of strings containing groups.
- `getClientIPAddress()`: Returns a string containing client IP address.
- `getAction()`: Returns a string containing information about the action being requested.

For two scenarios:

- User “sam” needs to be denied a policy based on the IP address of the machine from where the resources are accessed.

Set the deny condition for user sam with the following boolean expression:

```
if ( tagAttr.get('ipAddr').equals(ctx.getClientIPAddress()) ) {
  ctx.result = true;
}
```

- Deny one particular user, “bob” from a group, “users”, only when this user is accessing resources from a particular IP defined as an tag attribute in Atlas.

Set the deny condition for group users with the following boolean expression:

```
if (tagAttr.get('ipAddr').equals(ctx.getClientIPAddress()) && ctx.getUser().equals("bob")) {
  ctx.result=true;
}
```

Deny Conditions :

Select Group	Select User	Policy Conditions	Component Permissions
Select Group [X] users [X] bob	[X] saml Select User	expression: JavaScript Condition	deny [X]
		expression: JavaScript Condition	deny [X]

(tagAttr.get("ipAddr").equals(ctx.getClientIPAddress())) {
ctx.result = true;}

(tagAttr.get("ipAddr").equals(ctx.getClientIPAddress()) &&
ctx.getUser().equals("bob")) {
ctx.result=true;}

Adding a tag-based PII policy




Example of how to add a PII tag-based policy. In this example we create a tag-based policy for objects tagged "PII" in Atlas. Access to objects tagged "PII" is allowed for members of the "audit" group. All other users (the "public" group) are denied access.

Procedure

1. Select Access Manager > Tag Based Policies, then select a tag-based service.

2. On the List of Policies page, click Add New Policy.

The screenshot shows the Ranger web interface. At the top, there is a navigation bar with 'Ranger' and 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. Below this, there are tabs for 'Service Manager' and 'tag_service1 Policies'. There are also buttons for 'Access' and 'Masking'. The main content area is titled 'List of Policies : tag_service1' and contains a search bar and an 'Add New Policy' button (highlighted with a red box). Below the search bar is a table with the following data:

Policy ID	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
38	EXPIRES_ON	--	Enabled	Enabled	--	public	rangerlookup	  

The Create Policy page appears:

3. Enter the following information on the Create Policy page:

Table 52: Policy Details

Field	Description
Policy Type	Set to Access by default.
Policy Name	PII
TAG	PII
Audit Logging	YES
Description	Restrict access to resources with the PII tag.

Table 53: Allow Conditions

Label	Description
Select Group	audit
Select User	<none>

Label	Description
Policy Conditions	<none>
Component Permissions	hive (select all permissions)

Table 54: Deny Conditions

Label	Description
Select Group	public
Select User	<none>
Policy Conditions	<none>
Component Permissions	hive (select all permissions)

Table 55: Exclude from Deny Conditions

Label	Description
Select Group	audit
Select User	<none>
Policy Conditions	<none>

Label	Description
Component Permissions	hive (select all permissions)

Ranger
Access Manager
Audit
Security Zone
Settings
admin

Service Manager > cm_tag Policies > Create Policy

Create Policy

Policy Details :

Policy Type: Access Add Validity Period

Policy Name: enabled normal

Policy Label:

TAG:

Description:

Audit Logging: YES

Policy Conditions +

No Conditions

Allow Conditions : hide

Select Role	Select Group	Select User	Policy Conditions	Component Permissions	
<input type="text" value="Select Roles"/>	<input type="text" value="audit"/>	<input type="text" value="Select Users"/>	Add Conditions +	HIVE <input type="text"/>	<input checked="" type="checkbox"/>
+ show					
⚠ Exclude from Allow Conditions :					

Deny Conditions : hide

Select Role	Select Group	Select User	Policy Conditions	Component Permissions	
<input type="text" value="Select Roles"/>	<input type="text" value="public"/>	<input type="text" value="Select Users"/>	Add Conditions +	HIVE <input type="text"/>	<input checked="" type="checkbox"/>
+ hide					
⚠ Exclude from Deny Conditions :					

Select Role	Select Group	Select User	Policy Conditions	Component Permissions	
<input type="text" value="Select Roles"/>	<input type="text" value="audit"/>	<input type="text" value="Select Users"/>	Add Conditions +	HIVE <input type="text"/>	<input checked="" type="checkbox"/>

In this example we used Allow Conditions to grant access to the "audit" group, and then used Deny Conditions to deny access to the "public" group. Because the "public" group includes all users, we then used Exclude from Deny Conditions to exclude the "audit" group, in effect reinstating the "audit" group's original Allow access condition.

- Click Add to add the new policy.

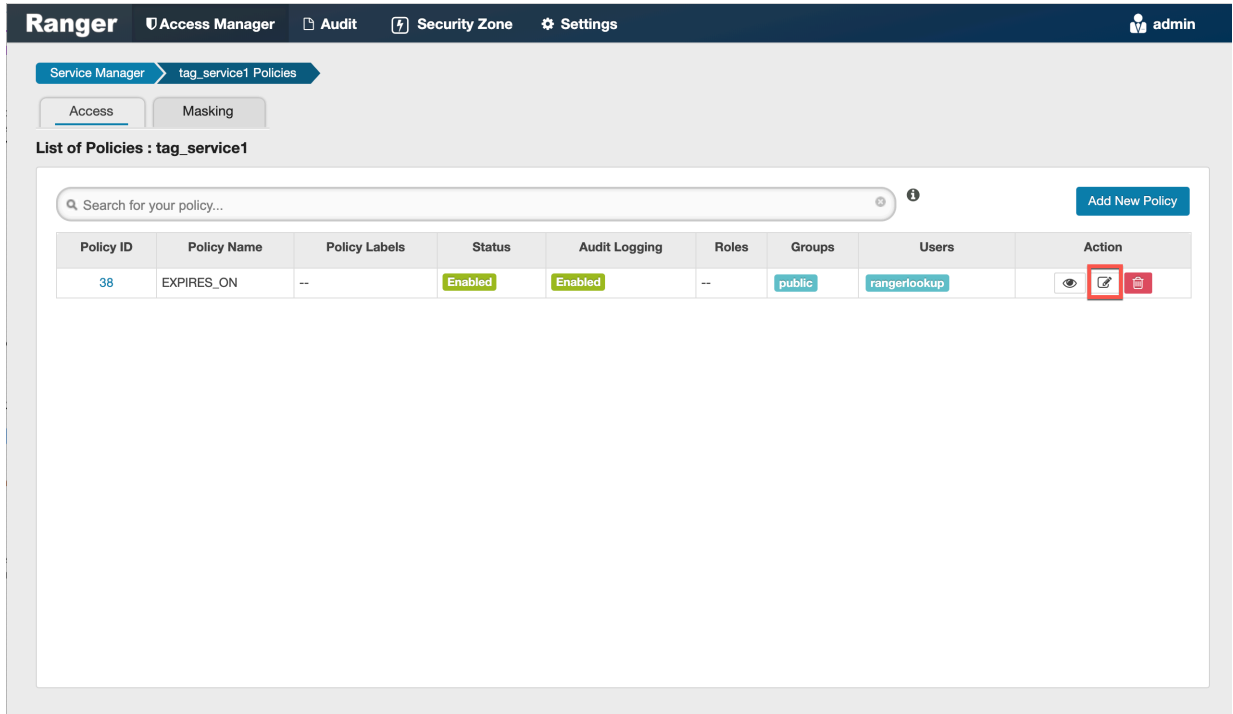
Default EXPIRES_ON tag policy

An EXPIRES_ON tag-based policy is created automatically when a tag service instance created. This default policy denies access to objects tagged with EXPIRES_ON after the expiry date specified in the Atlas tag attribute. You can use the following steps to review the default EXPIRES_ON policy.




Procedure

1. Select Access Manager > Tag Based Policies, then select a tag-based service.

2. On the List of Policies page, click the Edit icon for the default EXPIRES_ON policy.



The screenshot shows the Ranger Access Manager interface. The top navigation bar includes "Ranger", "Access Manager", "Audit", "Security Zone", and "Settings". The user is logged in as "admin". The breadcrumb trail shows "Service Manager" > "tag_service1 Policies". There are tabs for "Access" and "Masking". The main heading is "List of Policies : tag_service1". Below this is a search bar and an "Add New Policy" button. A table lists the policies:

Policy ID	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
38	EXPIRES_ON	--	Enabled	Enabled	--	public	rangerlookup	  

The Edit Policy page appears:

The screenshot shows the Ranger Admin UI for editing a policy. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. The breadcrumb trail is 'Service Manager > tag_service1 Policies > Edit Policy'.

Policy Details:

- Policy Type: Access
- Policy ID: 38
- Policy Name: EXPIRES_ON (with a tooltip icon)
- Policy Label: Policy Label
- TAG: EXPIRES_ON
- Description: Policy for data with EXPIRES_ON tag
- Audit Logging: YES
- Buttons: 'Add Validity Period', 'enabled' (selected), 'normal'
- Policy Conditions: No Conditions

Allow Conditions:

Select Role	Select Group	Select User	Policy Conditions	Component Permissions	
Select Roles	Select Groups	Select Users	Add Conditions +	Add Permissions +	✖
+ Exclude from Allow Conditions : show					

Deny Conditions:

Select Role	Select Group	Select User	Policy Conditions	Component Permissions	
Select Roles	public	rangerlookup	accessed-after-expiry: yes	HDFS, HBASE, HIVE, KMS, KNOX, STORM, YARN, KAFKA, SOLR, NIFI, NIFI-REGISTRY, ATLAS	✖
+					

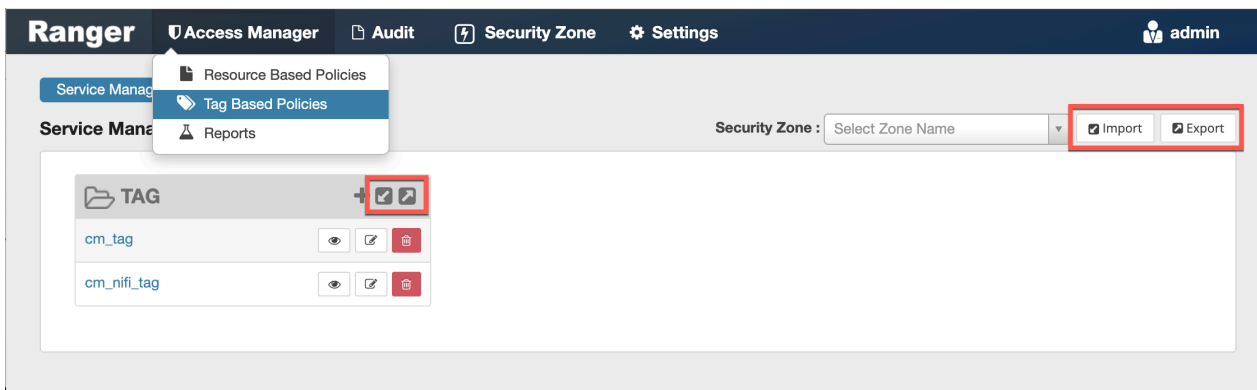
- We can see that the default EXPIRES_ON policy denies access to all users, and for all components, after the expiry date specified in the Atlas tag attribute.

Importing and exporting tag-based policies

You can export and import policies from the Ranger Admin UI for cluster resiliency (backups), during recovery operations, or when moving policies from test clusters to production clusters. You can import or export a specific subset of policies (such as those that pertain to specific resources or user/groups) or clone the entire repository (or multiple repositories) via the Ranger Admin UI.

Interfaces

You can import and export policies from the Tag Based Policies page:



You can also export policies from the Reports page:

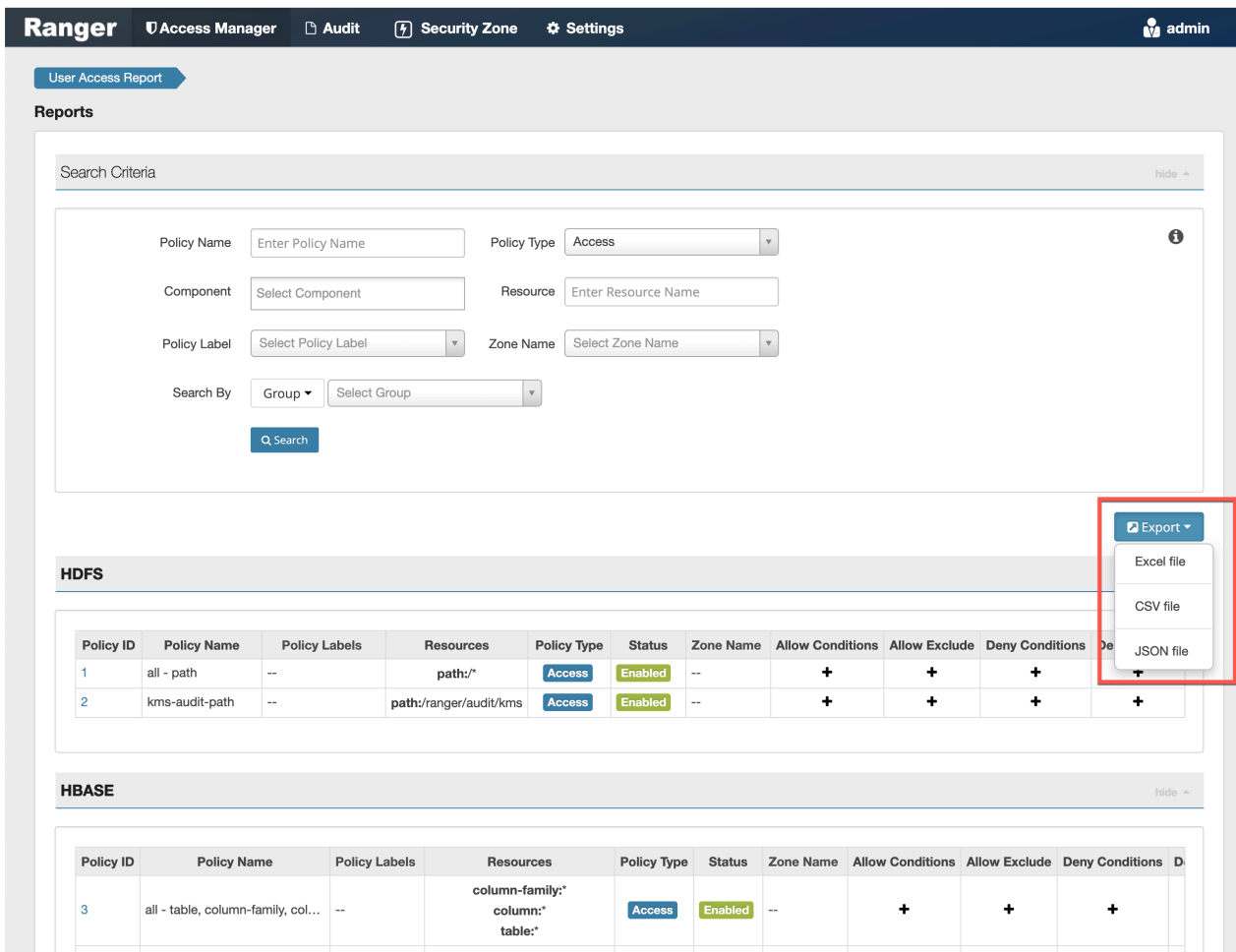


Table 56: Export Policy Options

	Service Manager Page	Reports Page
Formats	JSON	JSON Excel CSV
Filtering Supported	No	Yes
Specific Service Export	Yes	Via filtering

Filtering

When exporting from the Reports page, you can apply filters before saving the file.

Export Formats

You can export policies in the following formats:

- Excel
- JSON
- CSV

Note: CSV format is not supported for importing policies.

When you export policies from the Service Manager page, the policies are automatically downloaded in JSON format. If you wish to export in Excel or CSV format, export the policies from the Reports page dropdown menu.

Required User Roles

The Ranger admin user can import and export only Resource & Tag based policies. The credentials for this user are set in Ranger Configs > Advanced ranger-env in the fields labeled admin_username (default: admin/admin).

The Ranger KMS keyadmin user can import and export only KMS policies. The default credentials for this user are keyadmin/keyadmin.

Limitations

To successfully import policies, use the following database versions:

- MariaDB: 10.1.16+
- MySQL: 5.6.x+
- Oracle: 11gR2+
- PostgreSQL: 8.4+
- MS SQL: 2008 R2+

Partial policy import is not supported.

Related Information

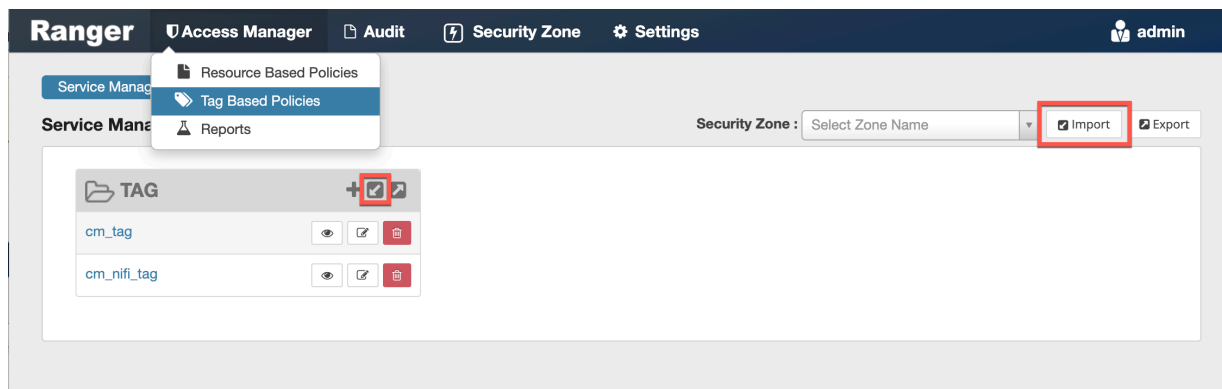
[Importing and exporting resource-based policies](#)

Import tag-based policies

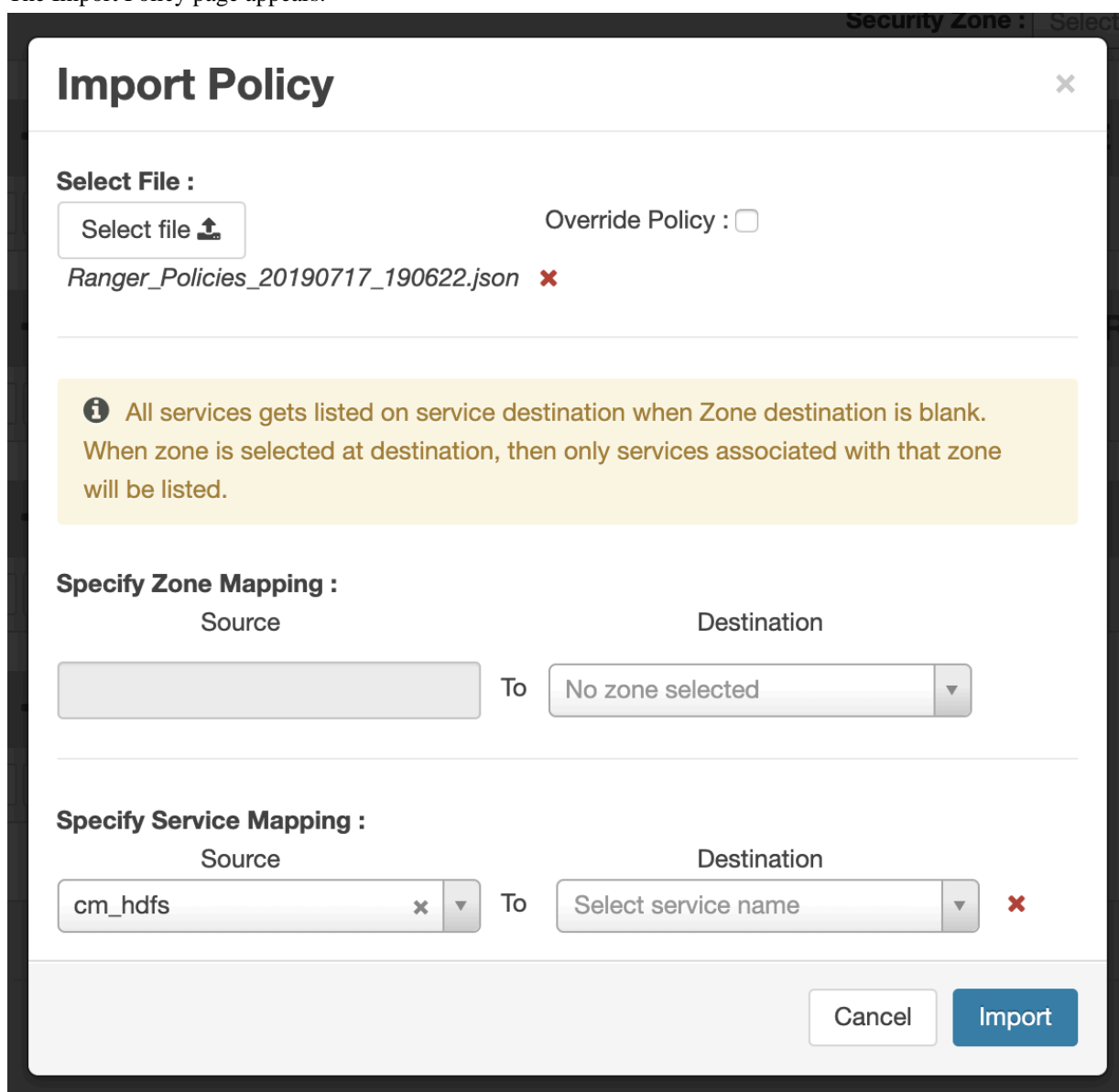
How to import tag-based policies.

Procedure

1. On the Tag Based Policies page, click one of the Import icons:



The Import Policy page appears.



2. Select the file to import.
You can only import policies in JSON format.

3. (Optional) Configure the import operation:
 - a) The Override Policy option deletes all policies of the destination repositories.
 - b) Zone Mapping – when no destination is selected, all services are imported. When a destination is selected, only the services associated with that security zone are imported.
 - c) Service Mapping maps the downloaded file repository, i.e. source repository to destination repository. You can use the red x symbols to remove services from the import. Scroll down to view all service mappings.

Import Policy

Specify Zone Mapping :

Source: [] To Destination: [No zone selected]

Specify Service Mapping :

Source	To	Destination
cm_hdfs	To	cm_hdfs
cm_hbase	To	cm_hbase
cm_yarn	To	cm_yarn
cm_hive	To	cm_hive
cm_knox	To	cm_knox
cm_storm	To	cm_storm

Buttons: Cancel, Import

4. Click Import.
A confirmation message appears after the file is imported.

Related Information

[Export tag-based policies](#)

Export tag-based policies

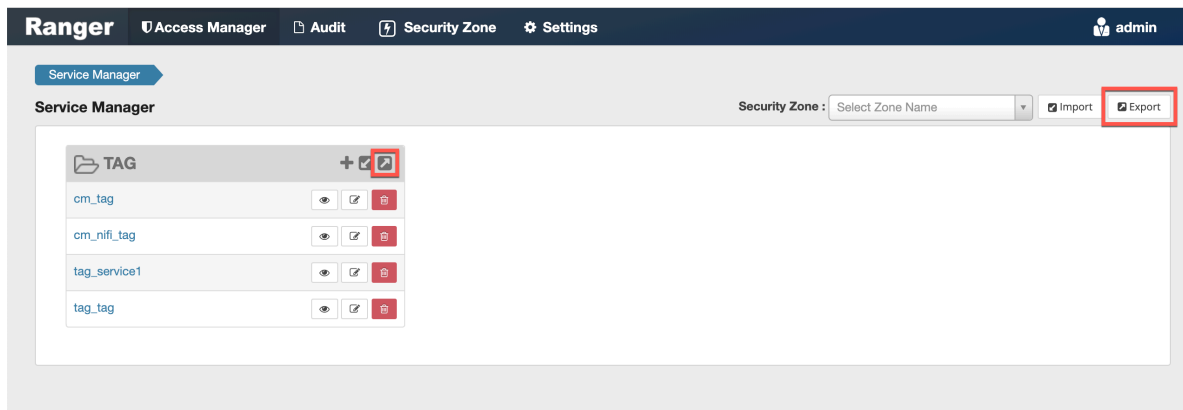
How to export all tag-based policies.

About this task

You can only export policies in JSON format from the Tag-based policies page. If you would like to export in Excel or CSV format, export the policies from the Reports page drop-down menu.

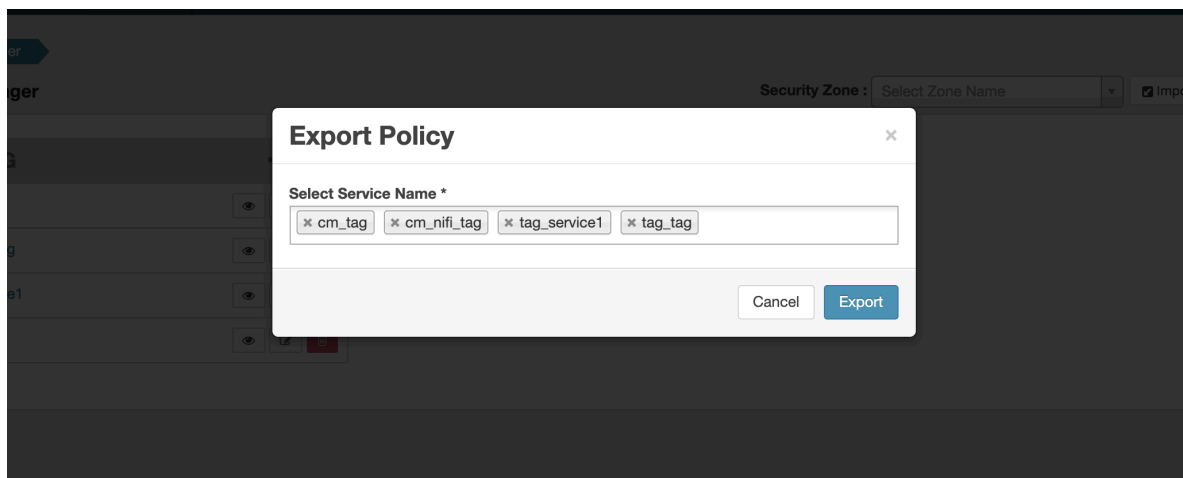
Procedure

- From the Access Manager > Tag Based Policies page:
 - Click the Export button or icon:



The Export Policy page appears.

- Remove components or specific services, then click Export.



- The file downloads in your browser as a JSON file.

- From the Reports page:
 - Filter Component to tag and click Search.
 - (Optional) Apply filters before exporting the file.
 - Open the Export drop-down menu:

The screenshot shows the Ranger 'User Access Report' interface. The 'Reports' section has a search criteria form with the following fields: Policy Name (text input), Policy Type (dropdown set to 'Access'), Component (text input with 'tag'), Resource (text input), Policy Label (dropdown), Zone Name (dropdown), and Search By (dropdown set to 'Group'). A 'Search' button is present. Below the form is a table titled 'TAG' with columns: Policy ID, Policy Name, Policy Labels, Resources, Policy Type, Status, Zone Name, Allow Conditions, Allow Exclude, Deny Conditions, and Deny. The table contains four rows of data for 'EXPIRES_ON' policies. An 'Export' dropdown menu is open, showing options for 'Excel file', 'CSV file', and 'JSON file'.

- Select the file format.
The file downloads in your browser.

Create a time-bound policy

Ranger policy validity periods enable you to configure a policy to be effective for a specified time range. You can add a validity period to both resource-based and tag-based policies.

About this task

Time-bound policy use-case examples:

- To restrict access to sensitive financial information until the earnings release date.
- To block a certain user for a specific time period (e.g., a compromised user account being investigated needs to be put on "hold" from accessing resources in Hadoop services).
- To block a certain group for a specific time (e.g., excluding temporary employees from writing on resources during the holiday season).



Note: The following procedure shows how to create a time-bound resource-based policy. The procedure is essentially the same for a tag-based resource policy.

Procedure

1. On the Ranger Service Manger page, select a service, then click Add New Policy.
2. Complete the fields on the **Create Policy** page.
3. Click Add Validity Period.
4. On the **Policy Validity Period** pop-up, specify a start time, end time, and time zone. To add additional validity periods, click the + symbol. Click Save to save the specified validity periods.

The screenshot shows a "Policy Validity Period" dialog box overlaid on a "Create Policy" page. The dialog box has a title bar with a close button (X) and contains three columns: "Start Time", "End Time", and "Time zone".

Start Time	End Time	Time zone
2019/07/22 09:00:15	2019/08/31 09:09:15	America/Los_Angel...
+		

At the bottom right of the dialog box are "Cancel" and "Save" buttons. The background page shows breadcrumb navigation: "om_hbase Policies" > "Create Policy".

- If you would like the policy to override all other policies during its validity period, select override.

Ranger Access Manager Audit Security Zone Settings admin

Service Manager > cm_hbase Policies > Create Policy

Create Policy

Policy Details :

Policy Type: Access Add Validity Period

Policy Name *: Temp Employees Override enabled **override**

Policy Label: Policy Label

HBase Table *: sales include

HBase Column-family *: include

HBase Column *: include

Description:

Audit Logging: YES

Allow Conditions : hide

Select Role	Select Group	Select User	Permissions	Delegate Admin	
Select Roles	temp_employees	Select Users	Read	<input type="checkbox"/>	<input type="button" value="x"/>

+ show

Exclude from Allow Conditions : show

Deny Conditions : show

Add Cancel

- Click Add.

Create a Hive authorizer URL policy

You can create a Hive Authorizer URL policy in Ranger that maintains Read and Write permissions for a location or folder.

About this task

Hive supports several commands that include URLs which refer to a current or future data location. Such locations must authorize end user access to that location. Currently, you can create a Ranger HDFS policy that grants "All" permissions for a location, recursively. If no such policy exists, HDFS authorization "falls back" to the current ACL that defines access to a location or folder. By default the value of the parameter is "hdfs:,file:". If you remove "hdfs:", access requests will be authorized against the HIVE URL policy and won't check for hdfs plugin or Hadoop ACL. This solution requires maintaining many policies or ACLs at the storage level. You can create a Hive Authorizer URL policy in Ranger that maintains Read and Write permissions for a location or folder.

To create a Hive Authorizer policy:

Procedure

1. In Cloudera Manager HIVE-1 Configuration Search . type ranger-hive.
2. In Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml, click +.
 - a) Under HIVE-1, in Name, type: ranger.plugin.hive.urlauth.filesystem.schemes.
 - b) In Value, type: file:
 - c) Click Save Changes.
3. In Cloudera Manager Hive_On_Tez-1 Configuration Search . type ranger-hive.
4. In Hive Service Advanced Configuration Snippet (Safety Valve) for ranger-hive-security.xml, click +.
 - a) Under HIVE_ON_TEZ-1, in Name, type: ranger.plugin.hive.urlauth.filesystem.schemes.
 - b) In Value, type: file:
 - c) Click Save Changes.
5. In HIVE-1 Actions , click Restart.
6. In HIVE_ON_TEZ-1 Actions , click Restart.

By default the value of the parameter is “hdfs:file:”. If you remove “hdfs:”, access requests will be authorized against the HIVE URL policy and won't check for hdfs plugin or Hadoop ACL.
7. In Ranger Resource Policies Hadoop SQL , click Add New Policy.
8. In Policy Details, select URL, then type the URL represents the location or folder to which you want Ranger to authorize access: hdfs://<hostname>.root.hwx.site:8020/demo/data.

9. In Allow Conditions, select user(s), then choose Read and Write permissions, as shown in the following example:

Figure 1: Creating a Hive Authorizer URL Policy

The screenshot shows the 'Create Policy' interface in Cloudera Service Manager. The 'Policy Details' section includes the following fields and controls:

- Policy Type:** Access (selected)
- Policy Name:** (empty text field)
- Policy Label:** Policy Label
- url:** hdfs://<hostname>.hwx.site:8020/demo/data
- Audit Logging:** Yes (selected)

The 'Allow Conditions' section is expanded to show a table with the following columns and values:

Select Role	Select Group	Select User	Permissions	Delegate Admin
Select Roles	Select Groups	hive	Read Write	<input type="checkbox"/>

This policy allows the user to READ / WRITE into the location defined by the URL.

```
CREATE EXTERNAL TABLE IF NOT EXISTS STUDENT (student_ID INT, FirstName STRING, LastName STRING, year STRING, Major STRING) COMMENT 'Student Names' ROW FORMAT DELIMITED FIELDS TERMINATED BY ',' STORED AS TEXTFILE LOCATION '/demo/data';
```

This will create a table reading data from the location /demo/data provided user will have the necessary READ permission to the location along with CREATE permission for table STUDENT

If the storage system is S3A or ADFS, then URL policy would be maintained for the scheme. For example, s3a://<folder>, abfs://<folder>.

Hive supports URL policies for the following commands that have URLs defined for the respective location:

CREATE TABLE

external table location

ALTER TABLE LOCATION

new location

ALTER PARTITION LOCATION

new partition location

ALTER TABLE ADD PARTITION

for partition location

LOAD

input location

For additional information about creating Hive commands with URL, see <https://cwiki.apache.org/confluence/display/RANGER/Hive+Commands+to+Ranger+Permission+Mapping>.

Ranger Security Zones

Ranger security zones let you organize service resources into multiple security zones.

Security Zones allow carving/bucketing of resources in a service into multiple zones for better administration of security policies. Defining Security Zones can enable multiple administrators to setup security policies for a service – based on the zones to which they have been granted administration rights.

Security Zones Administration

A Security Zone enables a Ranger administrator to separate resource policies into different administrative zones.

What is a Security Zone?

Security Zones help simplify security policy administration, and allow a limited amount of policies to be checked when doing authorization against certain resources. Only policies under a particular zone that contains the requested resource are loaded and checked by Ranger.

For example, let us consider two security zones: finance and sales:

- Security zone finance includes all content in a Hive database named finance.
- Security zone sales includes all content in a sales database.
- Policies defined in a security zone apply only to resources of that zone.
- A zone can be extended to include resources from multiple services such as HDFS, Hive, HBase, Kafka, etc. Extending a zone across multiple services allows zone administrators to set up policies for resources owned by their organization across multiple services.

For example:

```
Zone: finance
  service: prod_hdfs; path=/finance/*, /taxes/*
  service: prod_hive; database=finance
  service: prod_kafka; topic=FIN_*
  service: test_hadoop; path=/finance/*, /taxes/*
Zone: sales
  service: prod_hadoop; path=/sales/*
  service: prod_hive; database=sales
  service: prod_kafka; topic=SALES_*
```

- As shown above, resources can be specified using wildcards (FIN_*, SALES_*).
- Sets of users and groups are designated as administrators in each security zone.
- Users are allowed to set up policies only in security zones in which they are administrators.
- A resource cannot map to more than one security zone. Ranger does not allow creating security zones that specify resources that match resources in another zone. For example, an attempt to update the finance zone in the above example with the HDFS path /sales/finance/* is not permitted, because this conflicts with the HDFS path /sales/* specified in the sales zone.
- A set of users and groups can be designated as administrators of a security zone. Administrators can create, update, and delete security policies for the resources in that security zone.
- A set of users and groups can be authorized to view audit logs for that security zone's resources. Other users are not allowed to view access-audit logs for that security zone's resources.
- The security zone name appears in the zonename column of the access-audit log.

Security Zone Administration

- Security zones can only be created, updated, or deleted by a user with the ROLE_SYS_ADMIN role in Ranger.

- Users can view, retrieve, and update policies only in security zones in which they have administrator privileges.
- Users can view/retrieve and cannot update zone policies for which they have zone auditor permission.

How are Security Zones Used in Authorization?

When a Ranger authorization plugin authorizes a resource access request, it first determines the zone in which the accessed resource resides. If the resource matches a security zone, only the policies of that security zone are used to authorize the access. If resource does not match any security zone, the policies in the default (unnamed) security zone are used to authorize the access.

Tag-based Policies in Security Zones

In a given service, each security zone can be configured to use tag-based policies from a specific security zone in a tag-service. This enables different tag-based authorization policies to be used, based on the security zone of the resource.

Audit Logs

Audit logs generated by Ranger include the name of the security zone in which the accessed resource resides. Only users who have been assigned as an Admin or Auditor for the security zone are allowed to view the audit logs.

Security Zones Example Use Cases

Four example use cases for administering security zones.

Based on the following example:

```
Zone: finance
    service: prod_hdfs; path=/finance/*, /taxes/*
    service: prod_hive; database=finance
    service: prod_kafka; topic=FIN_*
    service: test_hadoop; path=/finance/*, /taxes/*
Zone: sales
    service: prod_hadoop; path=/sales/*
    service: prod_hive; database=sales
    service: prod_kafka; topic=SALES_*
```

Use case 1 : Access HDFS path using zone policy

For example, let us access hdfs path using unixuser1 user from finance zone.

Finance zone resource:

Ranger Service : prod_hdfs

Resource : /finance/*

Finance zone policy:

Resource Path : /finance/*

User : unixuser1

Permission : read, write, execute

Now, when unixuser1 user tries to create dir in /finance dir, Ranger checks for zone with resource /finance and policy for that user in that zone and then allows access for that user. Also, access-audit logs for that operation appear in the Ranger Admin Web UI, Access Audit tab.

Use case 2 : Hive access policy and tag masking policy

For example, we want to manage access policies and masking policy for taxation-related information in multiple finance databases for an organization.

Zone Resource :

Zone Tag service: cm_tag
Ranger Service : prod_hive
Resource :
Database : finance

Zone policy resource

Tag policy
resource:TDS
Hive policy
Resource :
Database : finance

Now, the Admin and security zone admin can create access policies and masking policies for all the resources associated with tag TDS and as and when new tables on Hive / Hbase are created for saving any taxation related data. They can associate a TDS tag with a related Hive / Hbase column. This will enable zone admin to create policies for masking the confidential data of its organization.

Use case 3 : Knox topologies

For example, suppose we want to manage access to a service. We can manage access to a service using topology.

Zone Resource :

Ranger Service : prod_knox
Resource:
Knox Topology:cdp-proxy-api
Knox Service:WEBHDFS

Zone deny policy Resource:

Knox Topology:cdp-proxy-api
Knox Service:WEBHDFS

Without a security zone, access to webhdfs is allowed since the default policy has a 'public' group in it.

Use case 4 : Import and export of zone policy

We can import and export zone policies from stage to prod.

Suppose we want to have the same policy in production that exists on stage. We can export the zone policy from the stage where the exported json has a zone name as a parameter in the json. While importing, we can map the zone name of stage to prod and then import the policies.

Adding a Ranger security zone

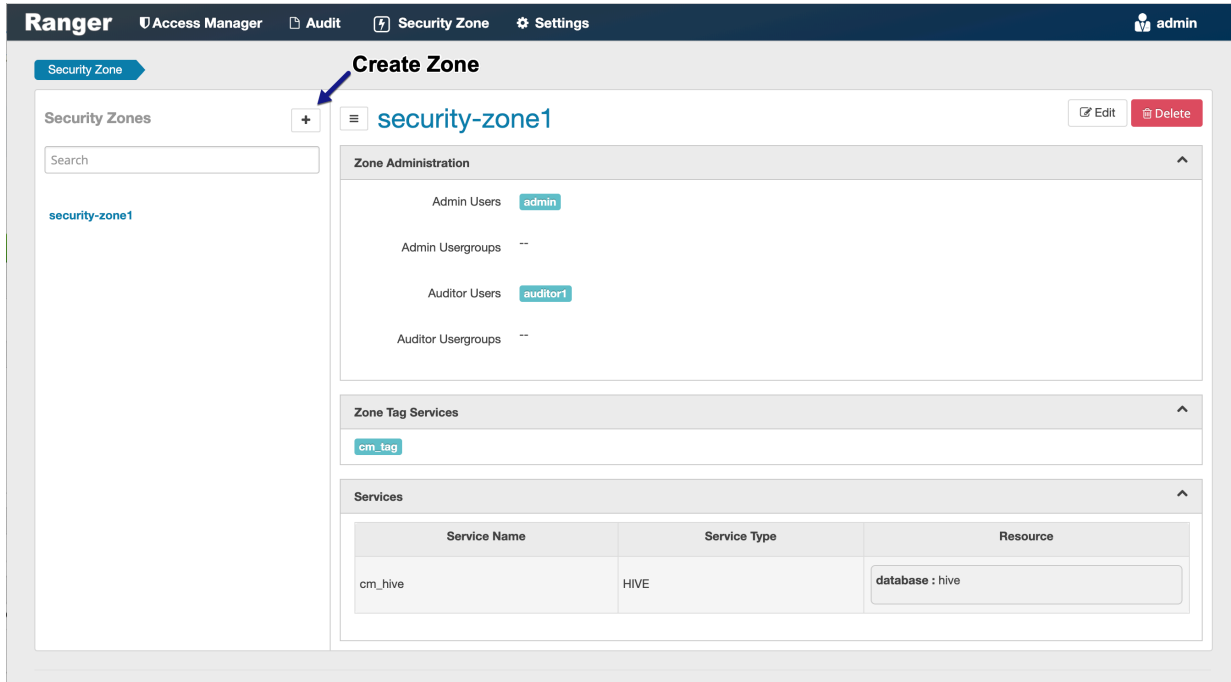
How to add a new Ranger Security Zone.

Procedure

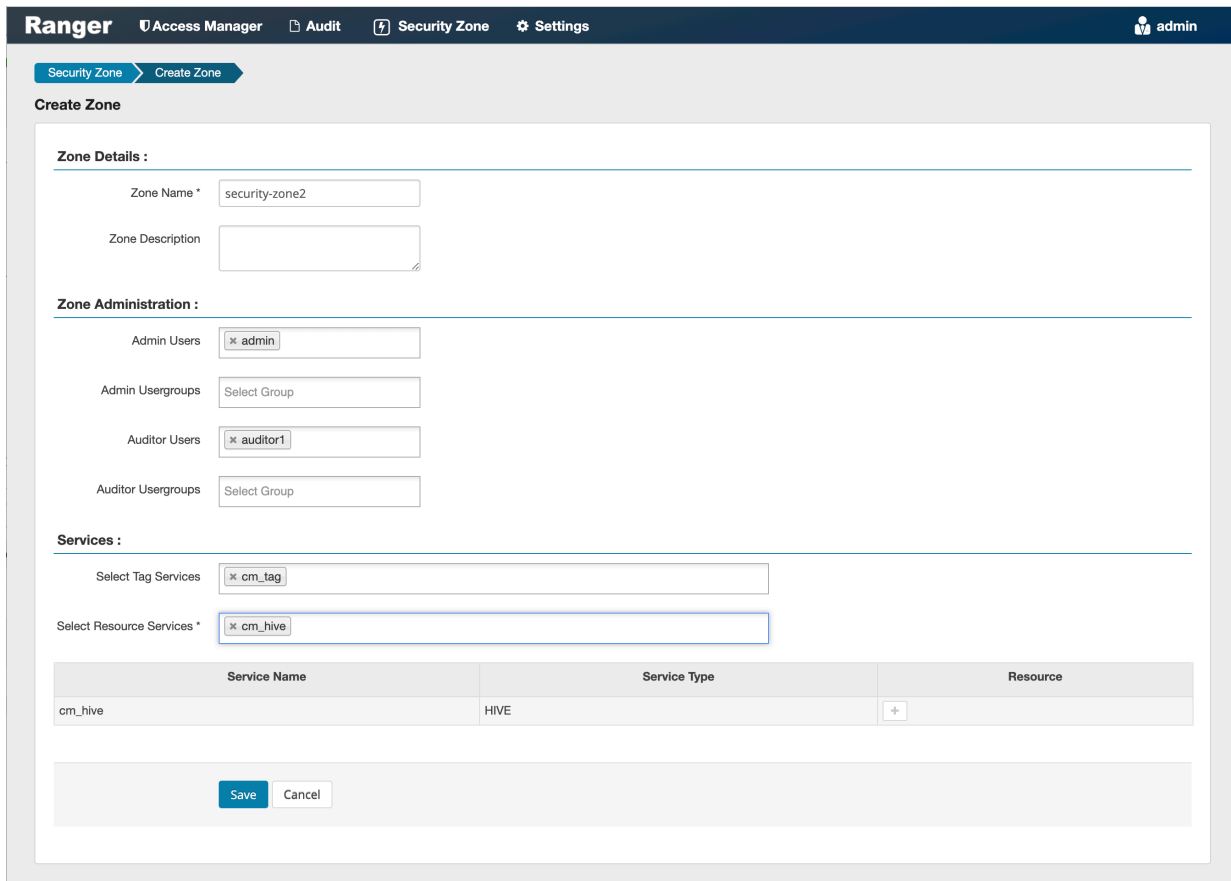
1. Click Security Zone in the top menu.

The Security Zone page appears.

- On the Security Zone page, click the + icon.



The Create Zone page appears.



3. Complete the Create Zone page as follows:

Table 57: Zone Details

Field	Description
Zone Name	The security zone name.
Zone Description	An optional description.

Table 58: Zone Administration

Field	Description
Admin Users	The Admin users for the security zone.
Admin Usergroups	The Admin user groups for the security zone.
Auditor Users	The Auditor users for the security zone.
Auditor Usergroups	The Auditor user groups for the security zone.

Table 59: Services

Label	Description
Select Tag Services	Select tag-based services for the security zone.
Select Resource Services	Select resource-based services for the security zone.

4. Selected Services are listed in the Services table. To add resources for each selected service, click the + icon in the Resources column for the applicable service.

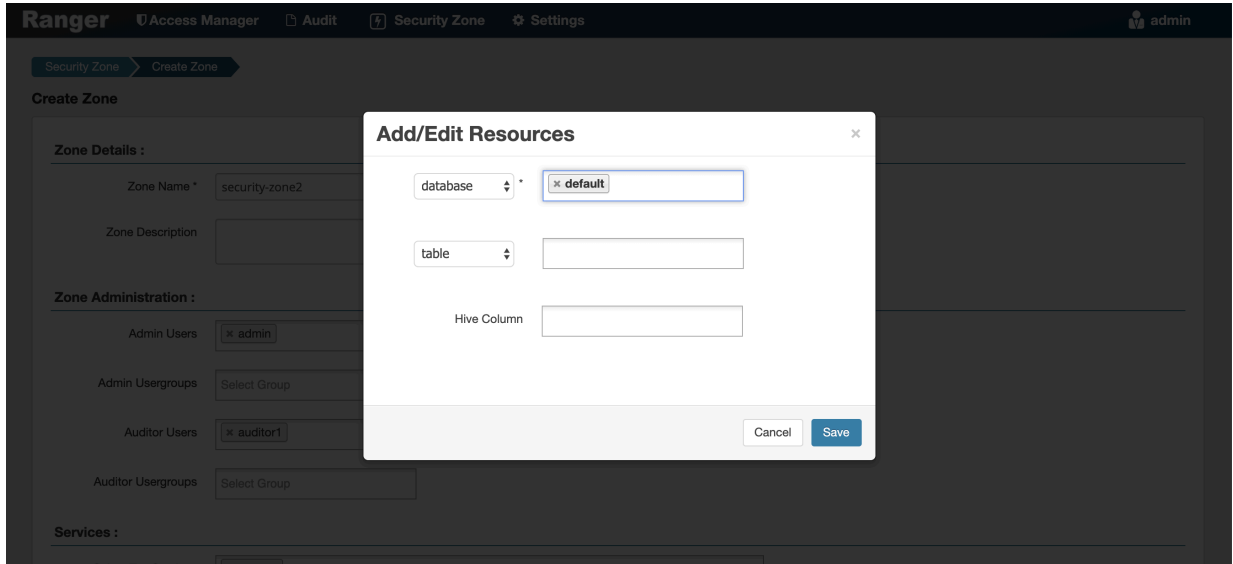
The screenshot shows the 'Create Zone' page in the Ranger interface. The page is divided into several sections:

- Zone Details:** Zone Name * (security-zone2), Zone Description.
- Zone Administration:** Admin Users (admin), Admin Usergroups (Select Group), Auditor Users (auditor1), Auditor Usergroups (Select Group).
- Services:** Select Tag Services (cm_tag), Select Resource Services * (cm_hive).
- Services Table:**

Service Name	Service Type	Resource
cm_hive	HIVE	+

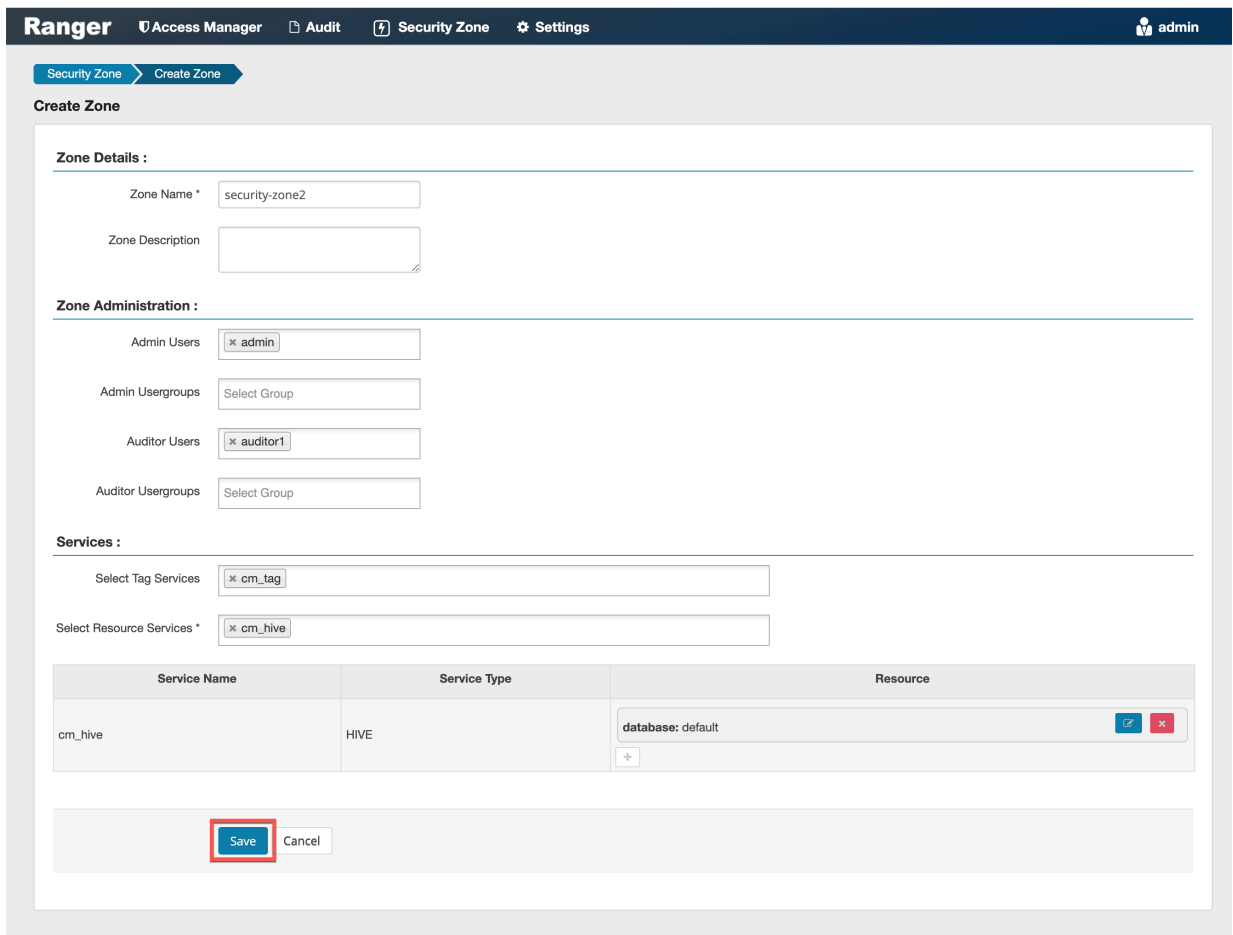
A blue arrow points to the '+' icon in the Resource column of the Services table, with the text 'Add Resources' next to it. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

- Use the Add/Edit Resources pop-up to specify resources for the service, then click Save.



The resources are listed in the Resources column of the Services table.

- Click Save at the bottom of the Create Zone page to save the new security zone.



7. The new security zone is listed on the Security Zone page.

The screenshot shows the Ranger Security Zone page. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. The main content area is titled 'Security Zone' and shows a list of security zones on the left: 'security-zone1' and 'security-zone2'. The 'security-zone2' zone is selected and its details are shown on the right. The 'Zone Administration' section lists 'Admin Users' as 'admin', 'Admin Usergroups' as '--', 'Auditor Users' as 'auditor1', and 'Auditor Usergroups' as '--'. The 'Zone Tag Services' section shows 'cm_tag'. The 'Services' section contains a table with the following data:

Service Name	Service Type	Resource
cm_hive	HIVE	database : default

8. To edit a security zone, click the security zone name in the Security Zones list, then click Edit.
9. After security zones have been created, you can use the Security Zone selection box on the Service Manager page to display the services assigned to the selected security zone. A Zone Name column appears in the table on the Audit > Access page, and also in the Access Manager > Reports tables.

The screenshot shows the Ranger Service Manager page. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. The main content area is titled 'Service Manager' and shows a grid of service cards for HDFS, HBASE, YARN, KNOX, SOLR, KAFKA, NIFI, NIFI-REGISTRY, and ATLAS. A dropdown menu is open for the 'Security Zone' selection, showing 'security-zone1' and 'security-zone2' as options. The 'security-zone2' option is highlighted.

Administering Ranger Users, Groups, Roles, and Permissions

To view a list of the users, groups, and roles that can access the Ranger portal or its services, select Settings > Users/Groups/Roles from the Ranger top menu.

What is a Role ?

A role is a set of permissions that you assign to a user, group, or another role. You assign a role by adding a user, group or role to it. By adding multiple roles, you create a role hierarchy in which you manage permission sets at the role level. For example, your workflow to create a role hierarchy:

1. Create a new role.
2. Add permissions to the role. For example, in Hadoop SQL, create a policy for a table that provides necessary permissions and add the role in the Role selector of Allow.
3. Repeat #2 until you have assigned all permissions.
4. Add users, groups, or other roles to the new role, which assigns the permission set to that role.

Benefits that roles provide in a large environment:

- A role may include many permissions, all of which may be granted or revoked to a user or group using a single command.
- Adding or revoking a single permission to or from a role requires a single command, which also applies to all users and groups with that role.
- Roles allow for some documentation about why a permission is granted or revoked.

In other words, a role is a collection of permissions. A group is a collection of users. You create a role and add permissions to it. Then, you grant that role to a group. Roles present an easier way to manage a set of permissions based on specific access criteria.

Example Ranger Role hierarchy

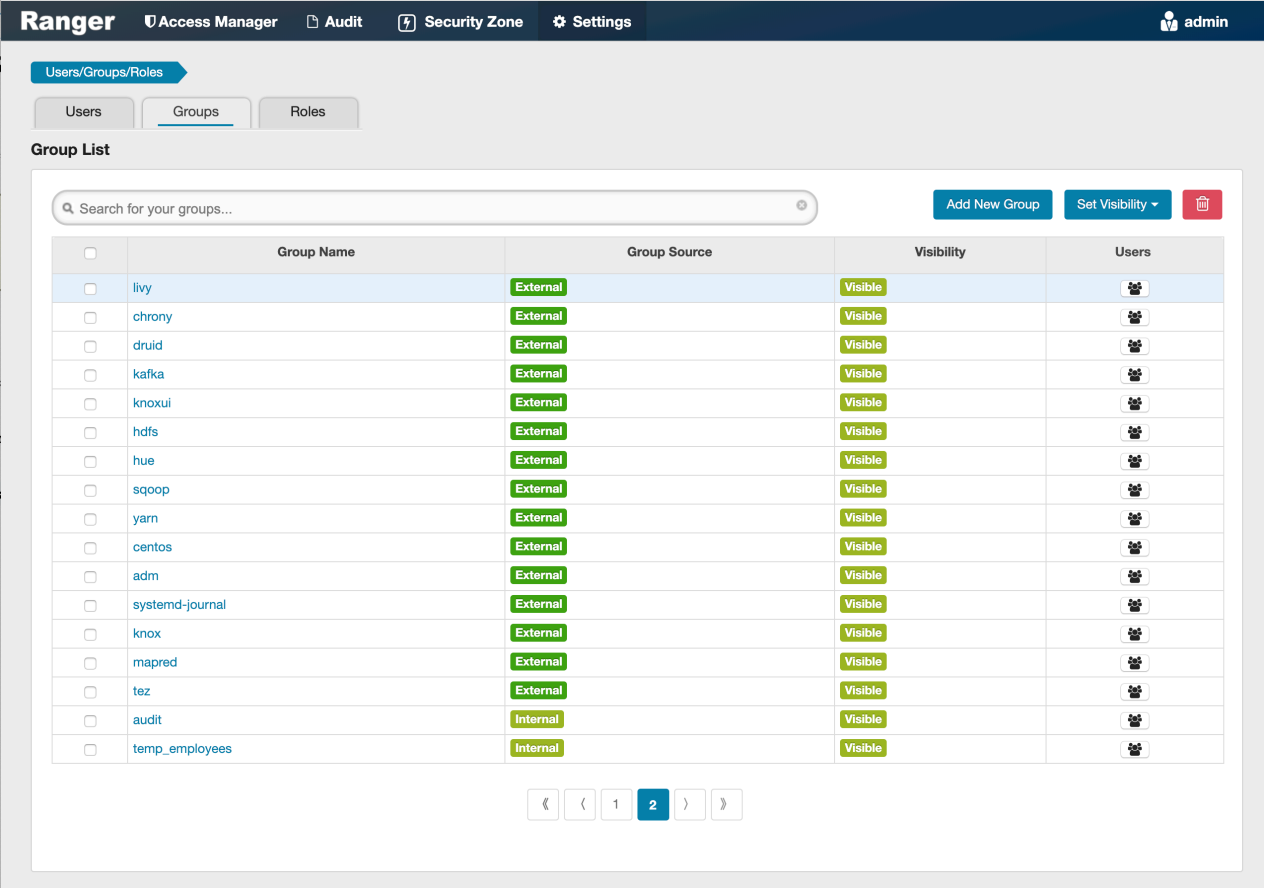
A simple example of a role heirarchy follows:

- FinReadOnly role, which gives read permission on all tables in the Finance database and is defined by a Ranger policy that grants read on database:Finance, table:* to the FinReadOnly role.
- FinWrite role, which gives write permission on all tables in the Finance database and is defined by a Ranger policy that grants write on database:Finance, table:* to the FinWrite role.
- FinReadWrite role, which role is granted both the FinRead and FinWrite roles and thereby inherits read and write permission to all tables in the Finance database.
- FinReporting group whose users require only read permission to the Finance tables. FinReporting group is added to FinReadOnly role in Ranger.
- FinDataPrep group whose users require only write permission to the Finance tables. FinDataPrep group is added to the FinWrite role in Ranger.
- FinPowerUser group whose users require read and write permission to all Finance tables. FinPowerUsers group is added to the FinReadWrite role in Ranger.

Overview of the Ranger Roles feature

The Users/Groups/Roles page lists:

- Internal users who can log in to the Ranger portal; created by the Ranger console Service Manager.
- External users who can access services controlled by the Ranger portal; created at other systems such as Active Directory, LDAP, or UNIX, and synched with those systems.
- Admin users who are the only users with permission to create users and services, run reports, and perform other administrative tasks. Admin users can also create child policies based on the original policy (base policy).
- On the Groups page, you can click the people icons in the Users column to view the members of the applicable group.
- On the Roles page, you can view the roles that have been mapped to users and groups. Roles are application-managed and are easier to apply changes than users and groups.



The screenshot shows the Ranger Admin console interface. At the top, there is a navigation bar with the 'Ranger' logo and menu items: 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. Below the navigation bar, there are tabs for 'Users/Groups/Roles', 'Users', 'Groups', and 'Roles'. The 'Groups' tab is selected, and the 'Group List' section is displayed. A search bar is present with the placeholder text 'Search for your groups...'. To the right of the search bar are buttons for 'Add New Group', 'Set Visibility', and a trash icon. The main content is a table with the following columns: Group Name, Group Source, Visibility, and Users. The table lists 20 groups, with 19 being 'External' and 1 being 'Internal'. Each group has a checkbox in the 'Users' column.

<input type="checkbox"/>	Group Name	Group Source	Visibility	Users
<input type="checkbox"/>	livy	External	Visible	
<input type="checkbox"/>	chrony	External	Visible	
<input type="checkbox"/>	druid	External	Visible	
<input type="checkbox"/>	kafka	External	Visible	
<input type="checkbox"/>	knoxui	External	Visible	
<input type="checkbox"/>	hdfs	External	Visible	
<input type="checkbox"/>	hue	External	Visible	
<input type="checkbox"/>	sqoop	External	Visible	
<input type="checkbox"/>	yarn	External	Visible	
<input type="checkbox"/>	centos	External	Visible	
<input type="checkbox"/>	adm	External	Visible	
<input type="checkbox"/>	systemd-journal	External	Visible	
<input type="checkbox"/>	knox	External	Visible	
<input type="checkbox"/>	mapred	External	Visible	
<input type="checkbox"/>	tez	External	Visible	
<input type="checkbox"/>	audit	Internal	Visible	
<input type="checkbox"/>	temp_employees	Internal	Visible	

Add a user

How to add a new Ranger user.

Procedure

1. Select Settings > Users/Groups/Roles.

The Users/Groups/Roles page appears.

<input type="checkbox"/>	User Name	Email Address	Role	User Source	Groups	Visibility
<input type="checkbox"/>	admin		Admin	Internal	--	Visible
<input type="checkbox"/>	rangerusersync		Admin	Internal	--	Visible
<input type="checkbox"/>	rangertagsync		Admin	Internal	--	Visible
<input type="checkbox"/>	hive		User	External	hive	Visible
<input type="checkbox"/>	cloudera-scm		User	External	wheel cloudera-scm	Visible
<input type="checkbox"/>	https		User	External	https	Visible
<input type="checkbox"/>	superset		User	External	superset	Visible
<input type="checkbox"/>	atlas		User	External	hadoop atlas	Visible
<input type="checkbox"/>	ranger		User	External	hadoop ranger	Visible
<input type="checkbox"/>	kudu		User	External	kudu	Visible
<input type="checkbox"/>	kms		User	External	kms	Visible
<input type="checkbox"/>	accumulo		User	External	accumulo	Visible

2. Click Add New User .

The User Detail page appears.

3. Add the required user details, then click Save.
The user is immediately added to the list.

Edit a user

How to edit a user in Ranger.

Procedure

1. Select Settings > Users/Groups/Roles.
The Users/Groups page opens to the Users tab.

The screenshot shows the Ranger Admin console interface. At the top, there is a navigation bar with 'Ranger' and several menu items: 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. Below the navigation bar, there are tabs for 'Users/Groups/Roles', 'Users', 'Groups', and 'Roles'. The 'Users' tab is currently selected. Underneath, there is a search bar labeled 'Search for your users...' and two buttons: 'Add New User' and 'Set Visibility'. The main content area is titled 'User List' and contains a table with the following data:

<input type="checkbox"/>	User Name	Email Address	Role	User Source	Groups	Visibility
<input type="checkbox"/>	admin		Admin	Internal	--	Visible
<input type="checkbox"/>	rangerusersync		Admin	Internal	--	Visible
<input type="checkbox"/>	rangertagsync		Admin	Internal	--	Visible
<input type="checkbox"/>	hive		User	External	hive	Visible
<input type="checkbox"/>	cloudera-scm		User	External	wheel cloudera-scm	Visible
<input type="checkbox"/>	https		User	External	https	Visible
<input type="checkbox"/>	superset		User	External	superset	Visible
<input type="checkbox"/>	atlas		User	External	hadoop atlas	Visible
<input type="checkbox"/>	ranger		User	External	hadoop ranger	Visible
<input type="checkbox"/>	kudu		User	External	kudu	Visible
<input type="checkbox"/>	kms		User	External	kms	Visible
<input type="checkbox"/>	accumulo		User	External	accumulo	Visible

- Select a user profile to edit. To edit your own profile, select your user name, then click Profile.

User List

	User Name	Email Address	Role	User Source	Groups	Visibility
<input type="checkbox"/>	admin		Admin	Internal	--	Visible
<input type="checkbox"/>	rangerusersync		Admin	Internal	--	Visible
<input type="checkbox"/>	rangertagsync		Admin	Internal	--	Visible
<input type="checkbox"/>	hive		User	External	hive	Visible
<input type="checkbox"/>	cloudera-scm		User	External	wheel cloudera-scm	Visible
<input type="checkbox"/>	httpfs		User	External	httpfs	Visible
<input type="checkbox"/>	superset		User	External	superset	Visible
<input type="checkbox"/>	atlas		User	External	hadoop atlas	Visible
<input type="checkbox"/>	ranger		User	External	hadoop ranger	Visible
<input type="checkbox"/>	kudu		User	External	kudu	Visible

The User Detail page appears.

User Detail

Basic Info | Change Password

User Name * rangerusersync

First Name * rangerusersync

Last Name

Email Address

Select Role * Admin

Group Please select

Save Cancel



Note:

You can only fully edit internal users. For external users, you can only edit the user role.

- Edit the user details, then click Save.

Delete a user

How to delete a user in Ranger.

Before you begin


Only users with the "admin" role can delete a user.

Procedure

1. Select Settings > Users/Groups.
The Users/Groups page appears.

The screenshot shows the Ranger interface with the 'Users/Groups/Roles' section selected. The 'Users' tab is active, displaying a 'User List' table. The table has columns for User Name, Email Address, Role, User Source, Groups, and Visibility. A search bar is at the top, and buttons for 'Add New User', 'Set Visibility', and a delete icon are on the right.

<input type="checkbox"/>	User Name	Email Address	Role	User Source	Groups	Visibility
<input type="checkbox"/>	admin		Admin	Internal	--	Visible
<input type="checkbox"/>	rangerusersync		Admin	Internal	--	Visible
<input type="checkbox"/>	rangertagsync		Admin	Internal	--	Visible
<input type="checkbox"/>	hive		User	External	hive	Visible
<input type="checkbox"/>	cloudera-scm		User	External	wheel cloudera-scm	Visible
<input type="checkbox"/>	https		User	External	https	Visible
<input type="checkbox"/>	superset		User	External	superset	Visible
<input type="checkbox"/>	atlas		User	External	hadoop atlas	Visible
<input type="checkbox"/>	ranger		User	External	hadoop ranger	Visible
<input type="checkbox"/>	kudu		User	External	kudu	Visible
<input type="checkbox"/>	kms		User	External	kms	Visible
<input type="checkbox"/>	accumulo		User	External	accumulo	Visible

2. Select the check box of the user you want to delete, then click the Delete icon () at the right of the User List menu bar.

The screenshot shows the same Ranger interface as above, but with the 'rangertagsync' user selected. The checkbox in the first column of the 'rangertagsync' row is checked and highlighted with a red box. The delete icon in the top right corner is also highlighted with a red box.

<input type="checkbox"/>	User Name	Email Address	Role	User Source	Groups	Visibility
<input type="checkbox"/>	admin		Admin	Internal	--	Visible
<input type="checkbox"/>	rangerusersync		Admin	Internal	--	Visible
<input checked="" type="checkbox"/>	rangertagsync		Admin	Internal	--	Visible
<input type="checkbox"/>	hive		User	External	hive	Visible
<input type="checkbox"/>	cloudera-scm		User	External	wheel cloudera-scm	Visible
<input type="checkbox"/>	https		User	External	https	Visible
<input type="checkbox"/>	superset		User	External	superset	Visible
<input type="checkbox"/>	atlas		User	External	hadoop atlas	Visible
<input type="checkbox"/>	ranger		User	External	hadoop ranger	Visible
<input type="checkbox"/>	kudu		User	External	kudu	Visible

3. Click OK on the confirmation pop-up.

Add a group

How to add a group in Ranger.

Procedure

1. Select Settings > Users/Groups/Roles, then click the Groups tab.
The Groups page appears.

	Group Name	Group Source	Visibility	Users
<input type="checkbox"/>	lvy	External	Visible	
<input type="checkbox"/>	chrony	External	Visible	
<input type="checkbox"/>	druid	External	Visible	
<input type="checkbox"/>	kafka	External	Visible	
<input type="checkbox"/>	knoxui	External	Visible	
<input type="checkbox"/>	hdfs	External	Visible	
<input type="checkbox"/>	hue	External	Visible	
<input type="checkbox"/>	sqoop	External	Visible	
<input type="checkbox"/>	yam	External	Visible	
<input type="checkbox"/>	centos	External	Visible	
<input type="checkbox"/>	adm	External	Visible	
<input type="checkbox"/>	systemd-journal	External	Visible	
<input type="checkbox"/>	knox	External	Visible	
<input type="checkbox"/>	mapred	External	Visible	
<input type="checkbox"/>	tez	External	Visible	
<input type="checkbox"/>	audit	Internal	Visible	
<input type="checkbox"/>	temp_employees	Internal	Visible	

2. Click Add New Group.
The Group Create page appears.

3. Enter a unique name for the group and an optional description, then click Save.

Edit a group

How to edit a group in Ranger.

Procedure

1. Select Settings > Users/Groups/Roles, then click the Groups tab.
The Groups page appears.

The screenshot shows the Ranger Admin console interface. At the top, there's a navigation bar with 'Ranger' and links for 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user 'admin' is logged in. Below the navigation bar, there's a breadcrumb 'Users/Groups/Roles' and three tabs: 'Users', 'Groups', and 'Roles'. The 'Groups' tab is active. The main content area is titled 'Group List' and contains a search bar 'Search for your groups...', an 'Add New Group' button, a 'Set Visibility' dropdown, and a trash icon. Below this is a table with the following data:

<input type="checkbox"/>	Group Name	Group Source	Visibility	Users
<input type="checkbox"/>	lvy	External	Visible	
<input type="checkbox"/>	chrony	External	Visible	
<input type="checkbox"/>	druid	External	Visible	
<input type="checkbox"/>	kafka	External	Visible	
<input type="checkbox"/>	knoxui	External	Visible	
<input type="checkbox"/>	hdfs	External	Visible	
<input type="checkbox"/>	hue	External	Visible	
<input type="checkbox"/>	sqoop	External	Visible	
<input type="checkbox"/>	yarn	External	Visible	
<input type="checkbox"/>	centos	External	Visible	
<input type="checkbox"/>	adm	External	Visible	
<input type="checkbox"/>	systemd-journal	External	Visible	
<input type="checkbox"/>	knox	External	Visible	
<input type="checkbox"/>	mapred	External	Visible	
<input type="checkbox"/>	tez	External	Visible	
<input type="checkbox"/>	audit	Internal	Visible	
<input type="checkbox"/>	temp_employees	Internal	Visible	

At the bottom of the table, there are pagination controls showing page 2 of 2.

2. Select a group name to edit.

The screenshot shows the Ranger Admin console interface, similar to the previous one. The 'Groups' tab is active. The main content area is titled 'Group List' and contains a search bar 'Search for your groups...', an 'Add New Group' button, a 'Set Visibility' dropdown, and a trash icon. Below this is a table with the following data:

<input type="checkbox"/>	Group Name	Group Source	Visibility	Users
<input type="checkbox"/>	public	Internal	Visible	
<input type="checkbox"/>	hive	External	Visible	
<input type="checkbox"/>	cloudera-scm	External	Visible	
<input type="checkbox"/>	wheel	External	Visible	
<input type="checkbox"/>	httpfs	External	Visible	
<input type="checkbox"/>	superset	External	Visible	
<input type="checkbox"/>	atlas	External	Visible	
<input type="checkbox"/>	hadoop	External	Visible	
<input type="checkbox"/>	ranger	External	Visible	
<input type="checkbox"/>	kudu	External	Visible	
<input type="checkbox"/>	kms	External	Visible	
<input type="checkbox"/>	accumulo	External	Visible	

The 'public' group name in the first row is highlighted with a red rectangular box.

- The Group Edit page appears.

The screenshot shows the Ranger interface with the 'Group Edit' page. The breadcrumb navigation is 'Users/Groups/Roles > Group Edit'. The 'Group Detail' section contains a form with the following fields:

- Group Name *: public
- Description: public group

At the bottom of the form are 'Save' and 'Cancel' buttons.

- Edit the group details, then click Save.

Delete a group

How to delete a group in Ranger.

Before you begin

Only users with the "admin" role can delete a group.


Procedure

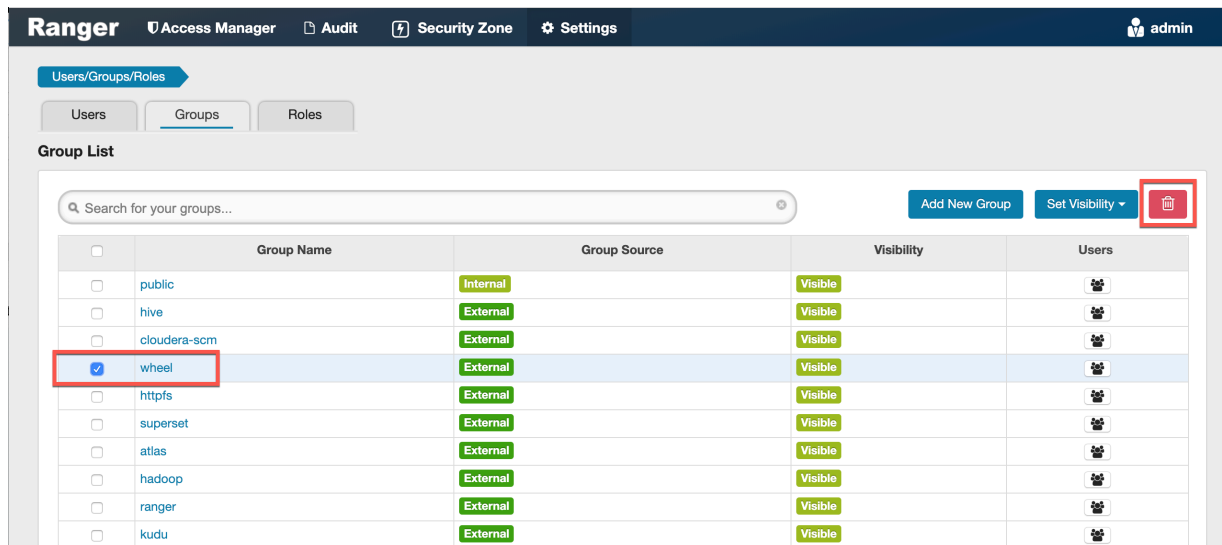
- Select Settings > Users/Groups/Roles, then click the Groups tab. The Groups page appears.

The screenshot shows the Ranger interface with the 'Groups' page. The breadcrumb navigation is 'Users/Groups/Roles > Groups'. The 'Group List' section contains a table with the following columns: Group Name, Group Source, Visibility, and Users. The table lists 20 groups, all with 'Visible' visibility and 'External' source, except for 'audit' and 'temp_employees' which are 'Internal'. There are 'Add New Group', 'Set Visibility', and 'Delete' buttons at the top right of the table.











	Group Name	Group Source	Visibility	Users
<input type="checkbox"/>	livy	External	Visible	
<input type="checkbox"/>	chrony	External	Visible	
<input type="checkbox"/>	druid	External	Visible	
<input type="checkbox"/>	kafka	External	Visible	
<input type="checkbox"/>	knoxui	External	Visible	
<input type="checkbox"/>	hdfs	External	Visible	
<input type="checkbox"/>	hue	External	Visible	
<input type="checkbox"/>	sqoop	External	Visible	
<input type="checkbox"/>	yarn	External	Visible	
<input type="checkbox"/>	centos	External	Visible	
<input type="checkbox"/>	adm	External	Visible	
<input type="checkbox"/>	systemd-journal	External	Visible	
<input type="checkbox"/>	knox	External	Visible	
<input type="checkbox"/>	mapred	External	Visible	
<input type="checkbox"/>	tez	External	Visible	
<input type="checkbox"/>	audit	Internal	Visible	
<input type="checkbox"/>	temp_employees	Internal	Visible	

2.

Select the check box of the group you want to delete, then click the Delete icon () at the right of the Group List menu bar.



The screenshot shows the Ranger Admin console interface. At the top, there is a navigation bar with 'Ranger' and several menu items: 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. A user profile 'admin' is visible in the top right. Below the navigation bar, there are tabs for 'Users', 'Groups', and 'Roles', with 'Groups' currently selected. The main content area is titled 'Group List' and contains a search bar, 'Add New Group' button, 'Set Visibility' dropdown, and a 'Delete' icon (a trash can) which is highlighted with a red box. Below this is a table with the following columns: 'Group Name', 'Group Source', 'Visibility', and 'Users'. The 'wheel' group is selected, indicated by a blue highlight and a checked checkbox in the first column.

<input type="checkbox"/>	Group Name	Group Source	Visibility	Users
<input type="checkbox"/>	public	Internal	Visible	
<input type="checkbox"/>	hive	External	Visible	
<input type="checkbox"/>	cloudera-scm	External	Visible	
<input checked="" type="checkbox"/>	wheel	External	Visible	
<input type="checkbox"/>	https	External	Visible	
<input type="checkbox"/>	superset	External	Visible	
<input type="checkbox"/>	atlas	External	Visible	
<input type="checkbox"/>	hadoop	External	Visible	
<input type="checkbox"/>	ranger	External	Visible	
<input type="checkbox"/>	kudu	External	Visible	

3. Click OK on the confirmation pop-up.

What to do next

Users in a deleted group will be reassigned to no group. You can edit these users and reassign them to other groups.

Related Information

[Edit a user](#)

Add a role through Ranger

How to add a role in Ranger.

About this task

You can create a role either through Ranger, or through Hive.

Procedure

To create a role through Ranger:

1. Select Settings > Users/Groups/Roles, then click the Roles tab.
The Role List page appears.

The screenshot shows the Ranger web interface. At the top, there is a dark blue navigation bar with the Ranger logo and menu items: Access Manager, Audit, Security Zone, and Settings. The user 'admin' is logged in. Below the navigation bar, there is a breadcrumb 'Users/Groups/Roles' and three tabs: Users, Groups, and Roles. The Roles tab is active. The main content area is titled 'Role List' and features a search bar with the placeholder text 'Search for your roles'. To the right of the search bar are two buttons: 'Add New Role' and a red trash icon. Below the search bar is a table with columns: Role Name, Users, Groups, and Roles. The table is currently empty, displaying the message 'No roles found!'.

<input type="checkbox"/>	Role Name	Users	Groups	Roles
No roles found!				

Licensed under the Apache License, Version 2.0

- Click Add New Role.
The Role Detail page appears.

Ranger Access Manager Audit Security Zone Settings admin

Users/Groups/Roles > Role Create

Role Detail

Role Name *

Description

Users:

User Name	Is Role Admin	Action
No users found		

Select User

Groups:

Group Name	Is Role Admin	Action
No groups found		

Select Group

Roles:

Role Name	Is Role Admin	Action
No roles found		

Select Role

- Enter a unique name for the role. Optionally, add users, groups and/or roles to be associated with the role, then click Save.

Add a role through Hive

How to add a role in Hive.

About this task

You can create a role either through Ranger, or through Hive.

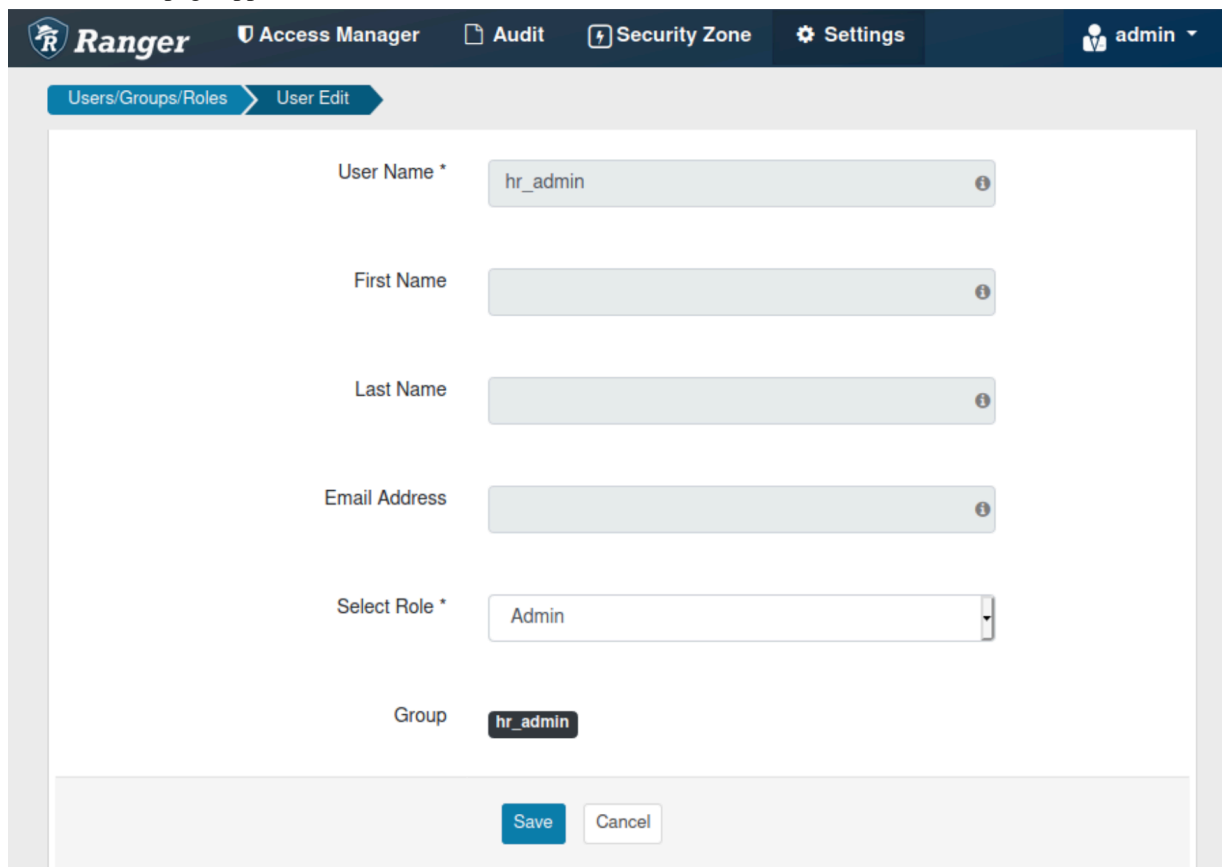
Before you begin

To add a role through Hive, the user must have Admin_Role privilege in Ranger.

Procedure

To grant the Admin_Role privilege, in Ranger:

1. Select Settings > Users/Groups/Roles, then click the Users tab.
2. Click the user name to which you want the Admin_Role privilege granted.
The User Edit page appears.



The screenshot displays the Ranger web interface for editing a user. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', 'Settings', and a user profile 'admin'. The breadcrumb trail shows 'Users/Groups/Roles' > 'User Edit'. The form contains the following fields:

- User Name *: hr_admin
- First Name
- Last Name
- Email Address
- Select Role *: Admin
- Group: hr_admin

At the bottom of the form are 'Save' and 'Cancel' buttons.

3. From the Select Role list, select Admin, then click Save.

In Hive:

4. Log in as a user with Admin_Role privilege.

5. Type the following command:

```
CREATE ROLE external_hr_role_01;
```

Any user with Is_Role_Admin privilege has the ability to assign the role to other users in Hive.

For example, to grant this new role to the user hr_user01, type:

```
GRANT ROLE external_hr_role_01 TO USER hr_user01;
```

hr_user01 appears in Ranger having the external_hr_role_01 role.

You can also grant Is_Role_Admin privilege to a specific user by typing:

```
GRANT ROLE external_hr_role_01 TO USER hr_user02 WITH ADMIN OPTION;
```

The role you create appears in Ranger and is recognized by Hive. The user that creates the role adds automatically to the list of users having that role. The added user has the Is_Role_Admin privilege, as shown in Ranger:

The screenshot shows the Ranger web interface. At the top, there is a navigation bar with 'Ranger', 'Access Manager', 'Audit', 'Security Zone', 'Settings', and a user profile 'admin'. Below the navigation bar, there are breadcrumb links 'Users/Groups/Roles' and 'Role Edit'. The main content area is titled 'Role Detail' and contains a form for editing the role. The 'Role Name' field is filled with 'external_hr_role_01'. Below it is a 'Description' field. Underneath is a 'Users:' section with a table. The table has three columns: 'User Name', 'Is Role Admin', and 'Action'. The first row shows 'hr_admin' in the 'User Name' column, a checked checkbox in the 'Is Role Admin' column, and a red 'X' icon in the 'Action' column. The 'Is Role Admin' column is highlighted with an orange box. At the bottom of the table, there is a 'Select User' input field and an 'Add Users' button.

User Name	Is Role Admin	Action
hr_admin	<input checked="" type="checkbox"/>	

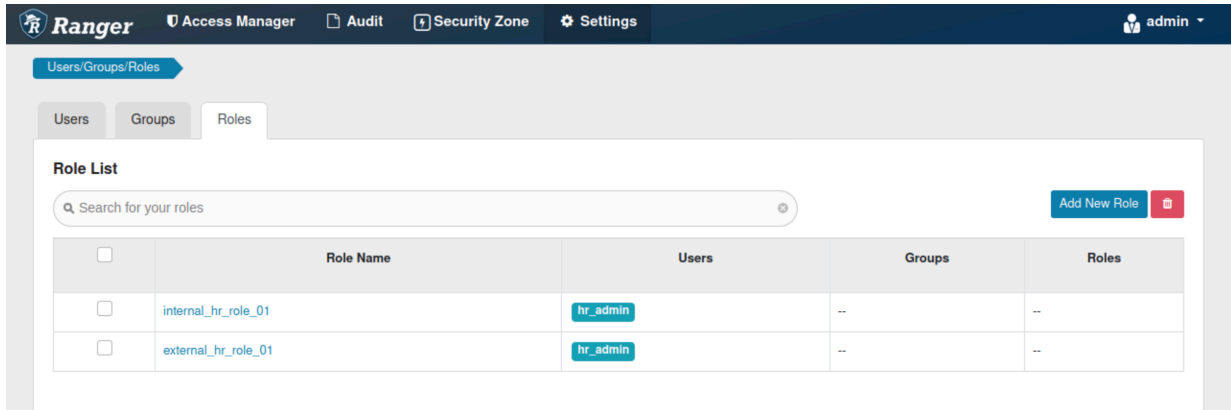
Edit a role

How to edit a role in Ranger.

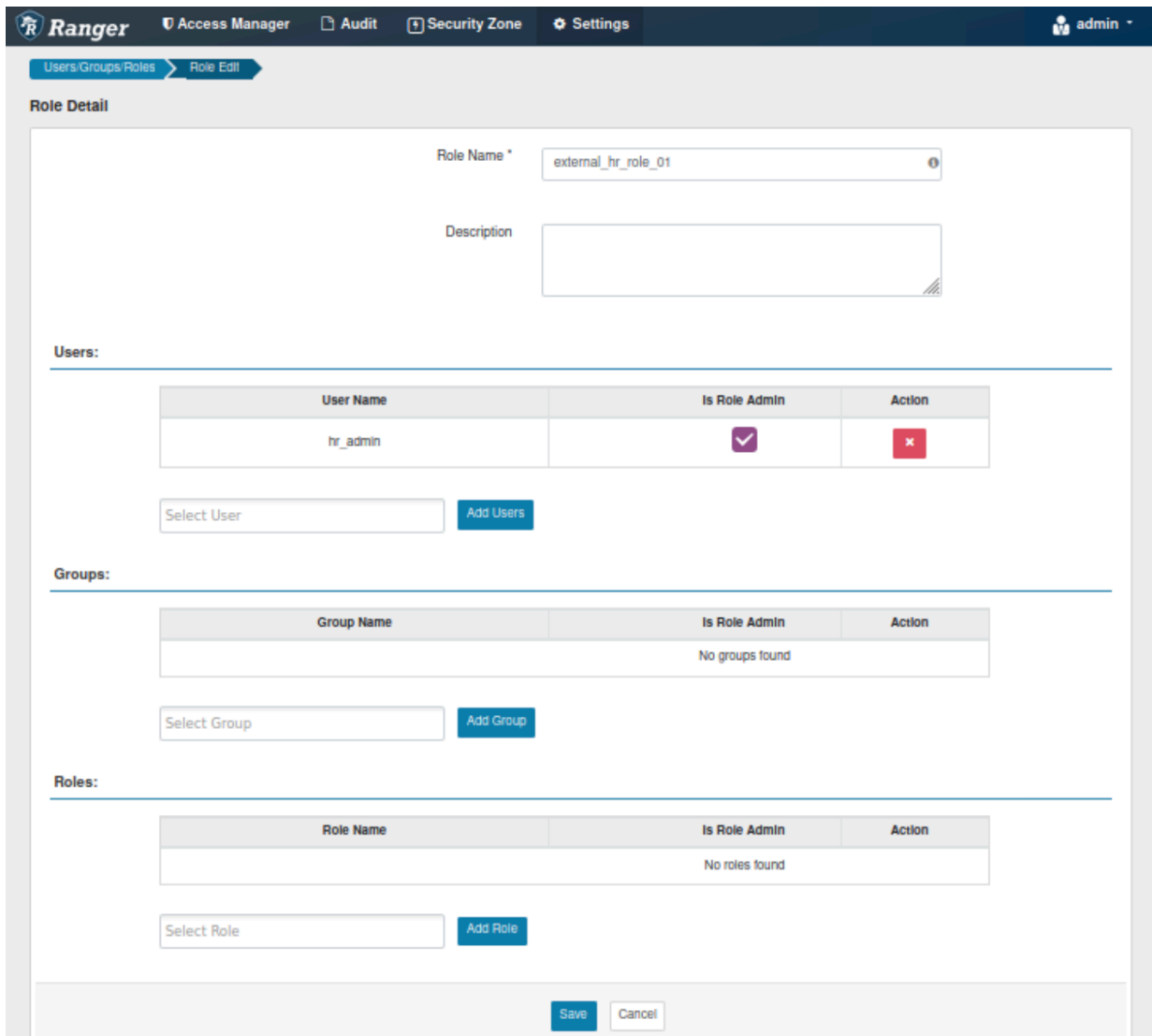
Procedure

1. Select Settings > Users/Groups/Roles.

- Click the Roles tab.
The Users/Groups/Roles page opens to the Roles tab.



- Click the role name to edit.
The selected role opens for editing in Role Detail.



4. Add users, groups and roles to the existing role, then click Save.

If the role was created in Hive, you can add other users in Hive using the GRANT command:

```
GRANT ROLE external_hr_role_01 TO USER hr_user02;
```

Delete a role

How to delete a role in Ranger.

Procedure

1. Select Settings > Users/Groups/Roles.

2. Click the Roles tab.

The Users/Groups/Roles page opens to the Roles tab.

The screenshot shows the Ranger web interface with the 'Roles' tab selected. The 'Role List' table contains the following data:

<input type="checkbox"/>	Role Name	Users	Groups	Roles
<input type="checkbox"/>	internal_hr_role_01	hr_admin	--	--
<input type="checkbox"/>	external_hr_role_01	hr_admin	--	--
<input type="checkbox"/>	external_hr_role_02	hr_admin	--	--
<input checked="" type="checkbox"/>	internal_hr_table_02	hr_admin	--	--

3. Click the checkbox for the role you want to delete, then select the Trash icon.

4. After deleting any roles, click Save .

If the role was created in Hive, you can delete the role through Hive using the Drop command:

```
DROP ROLE internal_hr_role_02;
```

Add or edit permissions


How to add or edit user or group permissions in Ranger.

Procedure

1. Select Settings > Permissions.
The Permissions page appears.

The screenshot shows the Ranger interface with the 'Permissions' page selected. The table below represents the data shown in the interface:

Modules	Groups	Users	Action
Resource Based Policies		admin rangerusersync keyadmin rangertagsync + More..	
Users/Groups		admin rangerusersync rangertagsync keyadmin + More..	
Reports		admin rangerusersync keyadmin rangertagsync + More..	
Audit		admin rangerusersync rangertagsync keyadmin + More..	
Key Manager		keyadmin	
Tag Based Policies		admin rangerusersync rangertagsync auditor1	
Security Zone		admin rangerusersync rangertagsync hive + More..	

2. Click the Edit icon () for the permission you would like to edit.
The Edit Permission page appears.

The screenshot shows the 'Edit Permission' page in Ranger. The 'Module Name' is 'Users/Groups'. The 'User and Group Permissions' section is active, showing a list of users: admin, rangerusersync, rangertagsync, keyadmin, and auditor1. The 'Select and Add Group' column is currently empty, showing 'No Selected Groups'.

3. Edit the permission settings, then click Save.
You can select multiple users and groups using the + icons.

Administering Ranger Reports

You can use the Reports page to help manage policies more efficiently as the number of policies increases. This page lists all resource-based and tag-based policies.

The screenshot shows the Ranger Reports page. The top navigation bar includes 'Ranger', 'Access Manager', 'Audit', 'Security Zone', and 'Settings'. The user is logged in as 'admin'. A dropdown menu is open under 'Access Manager', showing 'Resource Based Policies', 'Tag Based Policies', and 'Reports'. The 'Reports' section is active, displaying search criteria and a table of HDFS policies.

Search Criteria

Policy Name: Policy Type:

Component: Resource:

Policy Label: Zone Name:

Search By:


HDFS

Policy ID	Policy Name	Policy Labels	Resources	Policy Type	Status	Zone Name	Allow Conditions	Allow Exclude	Deny Conditions	Deny Exclude
1	all - path	--	path:/*	Access	Enabled	--	-	+	+	+
Allow Conditions		Groups		Users		Accesses				
		--		hdfs rangerlookup		read write execute				
2	kms-audit-path	--	path:/ranger/audit/kms	Access	Enabled	--	+	+	+	+

View Ranger reports

How to view reports for Ranger policies.

To view reports for one or more policies, select Access Manager > Reports.

- To view Allow Condition details for each policy, click the  icon in the Allow Conditions column. You can use the same method to view details for other policy conditions (Allow Exclude, Deny Conditions, etc.).
- To edit a policy from the Reports page, click the Policy ID.

The screenshot shows the Ranger Admin console interface. At the top, there are navigation tabs for Access Manager, Audit, Security Zone, and Settings. The user is logged in as 'admin'. A dropdown menu is open under 'Reports', showing options for Resource Based Policies, Tag Based Policies, and Reports. The main content area is titled 'Search Criteria' and contains several search filters: Policy Name (text input), Policy Type (dropdown menu set to 'Access'), Component (dropdown menu), Resource (text input), Policy Label (dropdown menu), Zone Name (dropdown menu), and Search By (dropdown menu set to 'Group'). A 'Q Search' button is located below the filters. An 'Export' button is visible on the right side of the search criteria section. Below the search criteria is a section titled 'HDFS' which contains a table of policy details.

Policy ID	Policy Name	Policy Labels	Resources	Policy Type	Status	Zone Name	Allow Conditions	Allow Exclude	Deny Conditions	Deny Exclude
1	all - path	--	path/*	Access	Enabled	--	-	+	+	+
Allow Conditions		Groups		Users		Accesses				
		--		hdfs rangerlookup		read write execute				
2	kms-audit-path	--	path/ranger/audit/kms	Access	Enabled	--	+	+	+	+

Search Ranger reports

Reference information for searching Ranger reports on one or more policies.

You can search based on:

- Policy Name – The policy name.
- Policy Type – The policy type (Access, Masking, or Row Level Filter).
- Policy Label – The policy label.
- Component – The policy resource or tag component.
- Resource – The resource path used when creating the policy.
- Zone Name – The security zone name.
- Group, Username – The group or user name assigned to the policy.

The screenshot shows the Ranger Reports interface. At the top, there are navigation tabs: Access Manager, Audit, Security Zone, and Settings. The user is logged in as 'admin'. A dropdown menu is open under 'Reports', showing 'Resource Based Policies', 'Tag Based Policies', and 'Reports'. The 'Reports' section is active, displaying a search criteria form and a table of HDFS policies.

Search Criteria

Policy Name: Policy Type: ?

Component: Resource:

Policy Label: Zone Name:

Search By:

HDFS

Policy ID	Policy Name	Policy Labels	Resources	Policy Type	Status	Zone Name	Allow Conditions	Allow Exclude	Deny Conditions	Deny Exclude
1	all - path	--	path:/	Access	Enabled	--	-	+	+	+
Allow Conditions	Groups		Users			Accesses				
	--		hdfs	rangerlookup	read	write	execute			
2	kms-audit-path	--	path:/ranger/audit/kms	Access	Enabled	--	+	+	+	+

Export Ranger reports

Reference information for exporting Ranger reports on one or more policies.

You can export a list of reports in three file formats:

- CSV file
- Excel file
- JSON

The screenshot shows the Ranger web interface. At the top, there are navigation tabs: Access Manager, Audit, Security Zone, and Settings. The user is logged in as 'admin'. The main section is titled 'User Access Report' and contains a 'Reports' tab. Below this is a search criteria form with fields for Policy Name, Policy Type (set to 'Access'), Component, Resource, Policy Label, Zone Name, and Search By (set to 'Group'). A 'Q Search' button is present. Below the search form is an 'HDFS' table with columns: Policy ID, Policy Name, Policy Labels, Resources, Policy Type, Status, Zone Name, Allow Conditions, Allow Exclude, Deny Conditions, and Deny Exclude. Two policies are listed: 'all - path' and 'kms-audit-path'. An 'Export' dropdown menu is open, showing options for 'Excel file', 'CSV file', and 'JSON file'.

Related Information

[Export tag-based policies](#)

[Export resource-based policies for a specific service](#)

[Export all resource-based policies for all services](#)

Using Ranger client libraries

Ranger now supports clients written in java and python which enable applications to access Ranger REST APIs programmatically. Using client library code simplifies access using java or python, compared with making direct HTTP requests to Ranger REST APIs.

Summary

Ranger client libraries:

- Provide idiomatic, hand-written code in Java and Python, making Ranger REST APIs simple and intuitive to use.
- Handle all low-level details of communication with the server including complexities involved in JSON parsing.
- Support installing the python client using the familiar package management tool pip.

Table 60: Ranger Client Installation Repo and Library Reference Links

Language	Installation	Library Reference
java	github source repository	java library reference
python	github source repository	python library reference

Authentication

The Apache Ranger release 2.2 client supports two authentication types:

- Basic authentication (username/password)
- Kerberos authentication

Java client prompts for the authentication mode to be used at runtime. For Kerberos-based authentications, a principal and keytab file path is required.

SSL

Java and Python clients support SSL/TLS-enabled ranger. To connect to HTTPS ranger using java client, provide the path to the SSL configuration file, as shown in this example:

```
$ ./run-sample-client.sh -n <ranger_admin_url>  
SSL Configuration File: /path/to/config.xml
```

Sample SSL configuration file which requires values to be populated:

```
<configuration>  
  <property>  
    <name>xasecure.policymgr.clientssl.truststore</name>  
    <value></value>  
  </property>  
  <property>  
    <name>xasecure.policymgr.clientssl.truststore.credential.file</name>  
    <value></value>  
  </property>  
  <property>  
    <name>xasecure.policymgr.clientssl.truststore.type</name>  
    <value></value>  
  </property>  
</configuration>
```

Environment variables

The Java client requires that you initialize the following environment variables:

```
$ export JAVA_HOME=/usr/java/<jdk_version>/bin  
$ export PATH=$PATH:$JAVA_HOME  
$ export HADOOP_CREDSTORE_PASSWORD=<hadoop_credstore_password>
```

Using session cookies to validate Ranger policies

Apache Ranger REST Client uses cookie sessions to download policies, tags and roles from Ranger Admin.

In earlier versions, each Ranger plugin used a kerberos login to request a ticket granting ticket (TGT) from the KDC/AD server in order to download policies, tags and roles. This caused high traffic levels when multiple Ranger plugins requested downloads.

Starting with version 7.1.7 sp2, Ranger Admin now supports cookie-based sessions. The flag used to enable cookie sessions, `ranger.plugin.<service-name>.policy.rest.client.cookie.enabled`, where `<service-name>` is the name of the service for which a Ranger plugin is enabled, such as `hive`, `solr`, or `kafka`, is set to "enabled" by default.

To check whether the cookie session is used, open the Ranger Admin `access.log` in the `/var/log/ranger/admin` folder. Any policy, tag, or role download call to Ranger Admin displays either a 200 or 304 value as response status. A 401 value for response status indicates the call to the KDC server for a TGT for authentication at service start or when the session cookie expires.