Apache Ranger 0.5 - User Guide

USER GUIDE

Version : 0.5.0

September 2015

About this document

- This user guide is for Ranger Policy Admin. The URL information can be found in the install guide or from your system administrator.

Getting started

General Features

Login to the system:

- You can Login to the system by providing your username and password. For simplicity, your username is also displayed on your home page. Be aware that the login is case sensitive.You must use capital letters,numbers where appropriate in your username and password.

Log out to the system:

- Your username is also displayed on your homepage, on top right. Option to logout is provided under the drop list there.

Service Manager (Access Manager)

- The Access Manager is accessible from the top menu bar. The top menu bar shows a list of modules supported by Ranger Admin.
- The Access Manager module helps in adding and administering various supported Services and Policies under those services.

Add Service

- You can add a service by clicking on the plus icon next to each column on the Service Manager page. Details of the service and other config properties can be added in this step. The added service will be listed as shown below.
- **Step 1 :** Click on the Plus button to add a service
- **Step 2 :** Fill all the properties related to the service type on the "Create Service" screen shown below

HDFS

Label	Description
Service name	Name of the service, you will need to specify the service name in the agent config
Description	Give service description for reference
Active Status	You can choose this option to enable or disable the service
User name	Specify the end system username that can be used for connection
Password	Add the password for username above
Namenode URL	hdfs://NAMENODE_FQDN:8020
Authorization Enabled	Authorization involves restricting access to resources. If enabled, user need authorization credentials.
Authentication Type	Specify the authentication type (Simple, Kerberos)
hadoop.security. auth_to_local	It should be taken from hadoop configuration file, core-site.xml; Mapping of login credential to a username with hadoop
dfs.datanode.kerberos. principal	It should be taken from hadoop configuration file, hdfs-site.xml; Provide only if kerberos authentication is enabled; Principle associated with datanode
dfs.namenode.kerberos. principal	It should be taken from hadoop configuration file, hdfs-site.xml; Provide only if kerberos authentication is enabled; Principle associated with namenode
dfs.secondary.namenode. kerberos.principal	Should be taken from hadoop configuration file, hdfs-site.xml; Provide only if kerberos authentication is enabled; principal associated with secondary- namenode
RPC Protection Type	Only authorised user can view,use and contribute to a dataset
Common Name for certificate	Specify the name of the certificate
Add new Configurations	Specify any other new configurations

HIVE

Label	Description
Service Name	Name of the service, you will need to specify the service name in the agents config
Description	Give service description for reference.
Active Status	You can choose this option to enable or disable the service
Username	Specify the end system user name that can be used for connection
Password	Add the password for username above
jdbc.driverClassName	Specify the full classname of the driver used for Hive connections. The default HiveServer2 classname is : *org.apache.hive.jdbc.HiveDriver*
jdbc.url	jdbc:hive2://HIVE_FQDN:10000
Common name for certificate	Specify common name for certificate
Add new configurations	Specify any other new configurations

HBASE

Label	Description
Service Name	Name of the Service, you will need to specify the service name in the agents config
Description	Give any description for reference
Active Status	You can choose this option to enable or disable the service
Username	Specify the end system user name that can be used for connection
Password	Add the password for the username above
hadoop.security.authentication	Specify the authentication type (Simple, Kerberos)
hbase.master.kerberos.principal	Specify the Kerberos principal for the HBase Master (Applicable only for Kerberos enabled environment)
hbase.security.authentication	Setting must match the hbase-site.xml setting for this property (Simple, Kerberos).
hbase.zookeeper.property.clientPort	Setting must match the hbase-site.xml setting for this property (default is : 2181).
hbase.zookeeper.quorum	Setting must match the hbase-site.xml setting for this property.

zookeeper.znode.parent	Setting must match the hbase-site.xml setting for this property.
Common Name for Certificate	Specify common name for certificate
Add New Configurations	Specify any other new configurations

KNOX

Label	Description
Service Name	Name of the Service, you will need to specify the service name in the agents config
Description	Give service description for reference
Active Status	You can choose this option to enable or disable the service
Username	Specify the end system user name that can be used for connection
Password	Add the password for the username above
knox.url	gateway url for knox
common name for certificate	Specify the name of the certificate
Add New configurations	Specify any other new configuration

5.YARN

Label	Description
Service Name	Name of the Service, you will need to specify the service name in the agents config
Description	Give service description for reference
Active Status	You can choose this option to enable or disable the service
Username	Specify the end system user name that can be used for connection
Password	Add the password for the username above
YARN REST URL	Http or https://RESOURCEMANAGER_FQDN:8088
Common name for certificate	Specify common name for certificate
Add new configurations	Specify new configurations

STORM

Label	Description
Service Name	Name of the Service, you will need to specify the service name in the agents config
Description	Give service description for reference
Active Status	You can choose this option to enable or disable the service
Username	Specify the end system user name that can be used for connection
Password	Add the password for the username above
Nimbus URL	hostname of nimbus format http://<ipaddress>:8080
Common name for certificate	Specify common name of the certificate
Add New Configuration	Specify any other new configurations

SOLR

Label	Description
Service name	Name of the Service, you will need to specify the service name in the agents config
Description	Give any description for reference
Active Status	You can choose this option to enable or disable the service
Username	Specify the end system user name that can be used for connection
Password	Add the password for the username above
solr URL	http://Solr_host:6083
Ranger Plugin SSL Cname	Provide common.name.for.certificate which is registered with Ranger (in Wire Encryption environment)
Add New Configurations	Specify new configuration

KAFKA

Label	Description
Service name	Name of the Service, you will need to specify the service name in the agents config
Description	Give service description for reference
Active Status	You can choose this option to enable or disable the service
Username	Specify the end system user name that can be used for connection
Password	Add the password for the username 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)
Add New Configuration	Specify any other new configurations

Edit Service

- You can edit service details, including the config properties from the edit icon next to each service name.

Delete Service

- You can delete a service by clicking on the delete button next to each service name listed on the Manage service page.

Ranger Policies

HDFS

- **Adding HDFS policies**

  You can add a new policy from the HDFS policy listing page for a particular service. On add , the policy should be listed in the table below. You can search a Policy by search filters provided.

Step 1 : Click on the Add New Policy button on listing page

<u>Step 2</u> : Create Policy Form

Label	Description
Policy Name	Enter an appropriate policy name. This name is cannot be duplicated for the same Service type (HDFS). This field is mandatory.
Resource path	Define the resource path for folder/file. You can add wildcard characters like /home* to avoid writing the full path as well as to enable the policy for all sub folders or files
Description	You can include the description for the policy you are creating
Recursive	You can indicate whether all files or folders within the existing folder comes under the policy. Can be used instead of wildcard characters
Audit Logging	Indicate whether this policy would be audited or not

Group Permissions	From a user group list, pick a particular group and choose permissions for that group.
Enable /disable	By default the policy is enabled.You can disable a policy to restrict user/group access for that policy.
User Permissions	From a user list, pick a particular user and choose permissions for that user.
Delegate Admin	When a policy is assigned to a user or a group of users those users become the delegated admin.The delegated admin can update, delete the policies. It can also create child policies based on the original policy (base policy)

- Permissions while creating policy

Permissions	Description
Read	Allows user to perform read operation
Write	Allows user to perform write operation
Execute	Allows user to perform execute operation

Step 3 : Policy is created with unique id

Edit/Delete HDFS Policies

- You can edit/delete a policy from the HDFS Policy Listing page by clicking on the edit/delete button next to policy row.

HDFS Policy Examples

- Ranger allows (through configuration) to allow both Ranger policies and HDFS permissions to be checked for a user request. When a user request is received in namenode. Ranger plugin will check for policies set through Ranger admin. If there are no policies, Ranger plugin will check for permission set in HDFS. It is recommended to have restrictive permission at HDFS level and create permission in Ranger security admin.

Example 1: Policy in Ranger

<u>Step 1</u> : In the below example we create a policy 'HDFS_POLICY' with Resource path /home with read ,write,execute,delegate admin rights and assign it to *mark*.

- Login as '*mark*' user and try to create a directory home.The user will be allowed to create the directory since it has read, write, execute rights to the policy ‘HDFS_POLICY’ with Resource path /home

- Logs For the operations. Result will come as ‘allowed’ if permission is granted and ‘denied’ if permission is denied.

- In the below example we create a policy ‘HDFS_POLICY’ with Resource path /hadoop with read permission and assign it to user ‘mark’.

- When the user tries to create a directory in Resource path then application throws an error of permission denied.

- Result will come as ‘denied’ in the logs generated for operations as user does not have write permission. Please note the “Access Enforcer” column will show the enforcer (ranger-acl or hadoop-acl)

Example 2: No Policies in Ranger,permission in HDFS

- There are no policies in service of HDFS component

- When user ‘mark’ tries to create a directory with name ‘directory’ in the resource path application throws an error.

- Result will come as ‘denied’ if permission is denied in the logs generated for operations.

HIVE

- ## Adding HIVE policies

You can add a new policy from the Hive Policy Listing Page. On add , the policy should be listed in the table below. You can search a Policy by ‘Database Name’, ‘Table’ , ‘Column’, ‘Groups name’, ’policy name’, ’status’, ’user name’, ’udf’

<u>**Step 1**</u> **:** Click on the Add New Policy button on listing page.

Step 2 : Add policy form

- **TABLE :-**

- You can create a policy for a combination for hive database, hive table and hive column name.

Label	Description
policy name	Enter an appropriate policy name. This name is cannot be duplicated for the same Service type (Hive). This field is mandatory.
Hive database name	Select the appropriate database. Multiple databases can be selected for a particular policy. This field is mandatory.
table name	For the selected database, select table(s) for the which the policy will be applicable
Hive column name	For the selected database and table(s), select columns for the which the policy will be applicable
Audit logging	Choose whether the particular policy will be audited or not.
Group permission	From a user group list, pick a particular group and choose permissions for that group.

User permission	From a user list, pick a particular user and choose permissions for that user.
include /exclude	The include flag means it will consider the values entered in the field. The default value is set as include. The exclude Flag will exclude all the table names or column names entered in that particular field.
Enable /disable	By default the policy is enabled.You can disable a policy to restrict user/group access for that policy.

- **UDF :-**

Label	Description
Policy name	Enter an appropriate policy name. This name can not be duplicated across the system.This field is mandatory.
Hive database	Select the appropriate database. Multiple databases can be selected for a particular policy. This field is mandatory.
UDF	We can also set policies for UDF.User Defined Function.Enter an appropriate udf.
Audit Logging	Choose whether the particular policy will be audited or not.
Group permissions	From a user group list, pick a particular group and choose permissions for that group. Choosing admin permission will designate the group as admin for chosen resource
User Permissions	From a user list, pick a particular group and choose permissions for that group. Choosing admin permission will designate the user as admin for the chosen resource
Include /exclude	The include flag means it will consider the values entered in the field.The default value is set as include. The exclude Flag will exclude all the table names or column names entered in that particular field.
Enable /disable	By default the policy is enabled. You can disable a policy to restrict user/group access for that policy.

Wildcards: Wildcards can be included in resource path.’*’ indicates zero or more occurs of characters.’?‘ indicates single character.You can use wildcards in the database name ,table name ,column name.for e.g database name as *,table name as ? and column name as ?.

In case of UDF we can use for e.g. database name as *,UDF as ?.

Permission	Description
Select	Allows users to perform a select operation
Update	Allows users to perform an update operation
Create	Allows users to perform a Create operation
Drop	Allows users to perform a Drop operation
Alter	Allows users to perform a Alter operation
Index	Allows users to perform an indexing operation
Lock	Allows users to perform an lock operation on specified resource
All	Allows users to perform all operations

GRANT: Hive GRANT is a command used to provide access or privileges on Hive database tables to the users.

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

i.e   : grant select on table default.newtable to user mark;
```

This will create a policy and give select rights to user1.

Edit / Delete / Revoke HIVE policies

- You can edit/delete a policy from the HIVE Policy Listing page by clicking on the edit/delete button next to policy row.

REVOKE: Hive REVOKE is a command used to revoke access or privileges on Hive database tables from the users.

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

i.e.  : revoke select on table default.newtable from user mark;
```

This will revoke select rights from user1.

- Similarly we can write it for (Update,Create,Drop,Alter,Index,Lock,All,Admin)

HBASE

- **Adding HBASE Policies**

You can add a new policy from the HBASE Policy Listing Page. On add , the policy should be listed in the table below. You can search a Policy by ‘column’, ’column family’, ’Group name’, ’Policy name’, ’Status', 'Table', ’Username’.

Step 1 **:** Click on the Add New Policy button on listing page.

Step 2 **:** Create Hbase Policy

Label	Description
Policy Name	Enter an appropriate policy name. This name is cannot be duplicated for same Service type (Hbase). This field is mandatory.
Hbase Table	Select the appropriate table. Multiple tables can be selected for a particular policy. This field is mandatory
Hbase column-family	For the selected table, select column families for the which the policy will be applicable
Hbase column	For the selected table and column family, select columns for the which the policy will be applicable
Audit Logging	Choose whether the particular policy will be audited or not.
Group permission	From a user group list, pick a particular group and choose permissions for that group. Choosing admin permission will designate the group as admin for the chosen resource
User Permission	From a user list, pick a particular user and choose permissions for that user. Choosing admin permission will designate the user as admin for the chosen resource

Enable /Disable	By default the policy is enabled.You can disable a policy to restrict user/group access for that policy.

Wildcards: Wildcards can be included in resource path.’*’ indicates zero or more occurs of characters.’?‘ indicates single character. You can use wildcards in the table name, column name, column families. for e.g table name as *, column family as ? and column name as ?.

Permission	Description
Read	Allows user to perform a read operation
Write	Allows user to perform a write operation
Create	Allows user to perform a create operation
Admin	This gives the delegated admin access to user

GRANT: HBase GRANT is a command used to provide access or privileges on Hbase database tables to the users.

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

i.e   : grant 'mark’' , 'RW' , 'testtable2'
```

This will create a policy and give read and write access to user1 on testtable2 .Similarly we can grant create and admin writes

Edit / Delete / Revoke HBASE Policies

- You can edit/delete a policy from the HBASE Policy Listing page by clicking on the edit/delete button next to policy row.

REVOKE: Hbase REVOKE is a command used to revoke access or privileges on Hbase database tables from the users.

```
Syntax: revoke ‘<user-or-group>','<table>'

i.e   : revoke 'mark','testtable2'
```

This will revoke all rights from mark

In hbase you don't have specific revoke commands for each privilege as we had in Hbase.

KNOX

- ## Adding KNOX Policies

  You can add a new policy from the KNOX Policy Listing Page. On add , the policy should be listed in the table below. You can search a Policy by ‘Policy Name’, ‘Topology Name’, ‘Service Name’ and ‘Groups’.

<u>Step 1</u> : Click on the Add New Policy button on listing page

Step 2 : Add knox policy

- Topology name: A topology is a graph of computation. Each node in a topology contains processing logic, and links between nodes indicate how data should be passed around between nodes.
- Service Name: Binds a Hadoop service with an internal URL that the gateway uses to proxy requests from external clients to the internal cluster services.

Label	Description
Policy name	Enter an appropriate policy name. This name is cannot be duplicated in the same Service type (Knox).
Knox topology	Enter an appropriate Topology Name
Knox service	Enter an appropriate Service Name
Audit Logging	Choose whether the particular policy will be audited or not.

Group permissions	From a group list, pick a particular group and choose permissions for that group.
User permissions	From a user user list, pick a particular user and choose permissions for that user.
Enable /disable	By default the policy is enabled. You can disable a policy to restrict user/group access for that policy.
Include /Exclude	The include flag means it will consider the values entered in the field. The default value is set as include. The exclude Flag will exclude all the table names or column names entered in that particular field.

Wildcards: Wildcards can be included in resource path.’*’ indicates zero or more occurs of characters.’?‘ indicates single character. You can use wildcards in the 'topology name', 'service name'. for e.g topology name as *, service name as ?.

Permission	Description
IP Address Range	Specify ip address range
Allow	Allow permission allows users to access topology that is specified in topology name

- ## Edit/Delete Knox policies

  You can edit/delete a policy from the KNOX Policy Listing page by clicking on the edit/delete button next to policy row.

STORM

- ## Adding STORM Policies

  You can add a new policy from the STORM Policy Listing Page. On add , the policy should be listed in the table below. You can search a Policy by ‘Policy Name’, ‘Topology Name’ and ‘Groups’.

Step 1 : Click on the Add New Policy button on listing page

Step 2 : Add STORM Policy

Topology name: A topology is a graph of computation. Each node in a topology contains processing logic, and links between nodes indicate how data should be passed around between nodes.

Label	Description
Policy name	Enter an appropriate policy name. This name is cannot be duplicated across the system.
Storm topology	Enter an appropriate Topology Name
Audit logging	Choose whether the particular policy will be audited or not.
Group permis sion	From a user group list, pick a particular group and choose permissions for that group.
User permis sion	From a user list, pick a particular group and choose permissions for that group.
Enable /disable	By default the policy is enabled.You can disable a policy to restrict user/group access for that policy.

Include /Exclude	The include flag means it will consider the values entered in the field. The default value is set as include. The exclude Flag will exclude all the table names or column names entered in that particular field.

Wildcards: Wildcards can be included in resource path.’*’ indicates zero or more occurs of characters.’?‘ indicates single character. You can use wildcards in the topology name.for e.g topology name as ?.

Permission	Description
Submit Topology	Allows user to submit a topology
File upload	Allows user to upload files
Get Nimbus Conf	Allows user to access Nimbus Configuration
Get Cluster info	Allows user to get Cluster Information
File Download	Allows user to Download Files
Kill Topology	Allows user to kill a topology
Rebalance	Allows user to Rebalance topologies
Activate	Allows user to Activate topology
Deactivate	Allows user to Deactivate topology
Get Topology Conf	Allows user to access Topology Configuration
Get Topology	Allows user to access Topology
Get User Topology	Allows user to access user Topology
Get Topology Info	Allows user to access Topology Information
Upload New Credential	Allows user to upload new credential

• Edit / Delete STORM Policies

You can edit/delete a policy from the STORM Policy Listing page by clicking on the edit/delete button next to policy row.

YARN

• Adding Yarn policies

You can add a new policy from the YARN Policy Listing Page. On add , the policy should be listed in the table below. You can search a Policy by ‘Group name’, ’Policy name’, ’Queue’, ’Status’, ’username’.

Step 1 : Click on the Add New Policy button on listing page

Step 2 : Add YARN Policy

Label	Description
Policy Name	Enter an appropriate policy name. This name is cannot be duplicated across the system.
Queue	The fundamental unit of scheduling in yarn
Audit Logging	Choose whether the particular policy will be audited or not.
Enable /disable	By default the policy is enabled.You can disable a policy to restrict user/group access for that policy.
Recursive	You can indicate whether all files or folders within the existing folder comes under the policy.Can be used instead of wildcard characters
User Permission	From a user list, pick a particular user and choose permissions for that user.

Group Permission	From a group list, pick a particular group and choose permissions for that group.

Wildcards: Wildcards can be included in resource path.’*’ indicates zero or more occurs of characters.’?‘ indicates single character.You can use wildcards in the topology name.for e.g topology name as ?.

Permission	Description
Submit-job	Allows user to submit a job on a defined queue
Admin-queue	Allows user to manage admin queue

Edit/Delete YARN policies

- You can edit/delete a policy from the YARN Policy Listing page by clicking on the edit/delete button next to policy row.

SOLR

- Adding SOLR Policies

You can add a new policy from the Solr Policy Listing Page. On add , the policy should be listed in the table below. You can search a Policy by 'Collection', 'Group name', 'Policy name', 'status', 'user name'.

Step 1 : Click on the Add New Policy button on listing page

Step 2 : Add SOLR policy

Label	Description
Policy Name	Enter an appropriate policy name. This name is cannot be duplicated for the same Service type (Solr)
Solr connection	http:<host_ip>:6083/solr
Audit logging	Choose whether the particular policy will be audited or not.
Group permission	From a user list, pick a particular group and choose permissions for that group. Choosing solr admin permission will designate the group as admin for chosen resource
User Permission	From a user list, pick a particular user and choose permissions for that user. Choosing solr admin permission will designate the user as admin for the chosen resource

Enabled /disabled	By default the policy is enabled.You can disable a policy to restrict user/group access for that policy.
Include /Exclude	The include flag means it will consider the values entered in the field.The default value is set as include.The exclude Flag will exclude all the table names or column names entered in that particular field.

Permission	Description
Querry	Permission to fetch records from Solr DB.
Update	Permission to update records in Solr
Others	
Solr Admin	Permission to manage user accounts and

Edit / Delete SOLR Policies

- You can edit/delete a policy from the SOLR Policy Listing page by clicking on the edit/delete button next to policy row.

KAFKA

- **Adding KAFKA Policies**

You can add a new policy from the KAFKA Policy Listing Page. On add , the policy should be listed in the table below. You can search a Policy by ‘Group name’,’Policy name’,Status,topic,’username’.

Step 1 : Click on the Add New Policy button on listing page

Step 2 : Add KAFKA Policy

Label	Description
Policy name	Enter an appropriate policy name. This name is cannot be duplicated for the same Service type (Kafka)
Topic	A topic is a category or feed name to which messages are published.
Audit logging	Choose whether the particular policy will be audited or not.
User permis sion	From a user list, pick a particular user and choose permissions for that user. Choosing Kafka Admin permission will designate the user as admin for the chosen resource
Group permis sion	From a user group list, pick a particular group and choose permissions for that group. Choosing Kafka Admin permission will designate the group as admin for chosen resource
Enable /Disable	By default the policy is enabled.You can disable a policy to restrict user/group access for that policy.
Include /Exclude	The include flag means it will consider the values entered in the field. The default value is set as include. The exclude Flag will exclude all the table names or column names entered in that particular file

Wildcards: Wildcards can be included in resource path.'*' indicates zero or more occurs of characters.'?' indicates single character. You can use wildcards in the topic name.for e.g topic name as ?.

Permission	Description
Publish	A process that publish message to kafka topic producers.
Consume	Consume only a subset of the partitions in a topic in a process
Configure	Configure the kafka broker/cluster
Describe	Permission to fetch metadata on the topic
Kafka Admin	

USERS/GROUPS

Policy permissions are assigned to users and groups.

- ## Users

These are users who can login into the Ranger portal and perform administrative and reporting tasks.Roles can be assigned while adding the users. Only admins are allowed to create users and create services. The role of the ‘admin’/’admin user’ dictates what roles can be assigned to the new users.

Internal Vs External Users

- Internal users are those users which are created by ranger Admin i.e XA Policy Manager. External users are those users which are synced from other system like Active Directory(AD), LDAP or unix system.

- ### Add Users

You can add a new group from the User Listing Page. On add, the user should be listed in the table below. The users that are created in the system are You can search a User by ‘Email Address’, ‘Role’ , ‘User Name’, ‘ User Source’, ’user status’, ’visibility’.

Step 1 : Click on the Add New User button on the user listing page

Step 2 : Enter the details and save.

Label	Description
User Name	Enter an appropriate user name. This name cannot be duplicated across the system.
New Password	Enter an appropriate password.
Password Confirm	Confirm the entered password
First Name	Enter an appropriate first name.
Last Name	Enter an appropriate last name
Email address	Enter an appropriate first email address in the required format
Select Role	Select appropriate Role (Admin, User). This is a mandatory field.
Group	Select group/s to which user belongs.

Step 3 **:** Set visibility (i.e. Visible/Hidden)

After clicking on hidden button user get hide from policy listing page. For hiding functionality user must need to select check box located near User Name column.

Step 4 **:** Set visibility (Visible)

- After clicking on Visible option selected user get visible in users listing page.

Step 5 **:** Set status of the user.

- If the status of the user is enable then that user can login to the application.If user status is disable then that particular user is not able to login to the application.

- ## Edit Users
    - We can edit only internal users.For the external users,only the role can be changed.

Admin Login:

- You can edit a user from the users Listing page by clicking on the user name.

User Login:

- You can edit a user from the users Listing page by clicking on profile.

Groups

- Ranger allows assigning permissions at group level too.
- **Add Groups**

You can add a new group from the group Listing Page. On add , the group should be listed in the table below. You can search a group by ‘Group Name’ and ‘ Group Source’,visibility

Step 1: Click on the Add New Group button on the group listing page.

Step 2 **:** Enter the details and save.

Label	Description
Group Name	Enter an appropriate user name. This name cannot be duplicated across the system.This is a mandatory field.
Description	Give any description for reference.

- **Edit Groups**
  - You can edit a group from the groups Listing page by clicking on the name of the group.(Can only be performed by an admin)

Visibility of Groups

- Hidden group does not appears in group listing page.To make the group hide select the check box near group group name.

Reports

- The Reports module is used to manage the policies more efficiently as the number of policies grow.This page will list all the policies from HDFS, HIVE,HBASE,KNOX,YARN,KAFKA,SOLR and STORM. You can perform search based on

- **Policy Name :** The policy name assigned to the policy while creating it.
- **Resource Path :** The resource path used while creating the policy.
- ‘Group’ / ‘User Name’: The group and the users to which the policy is assigned

Audit

- Currently Ranger supports regular auditing. This includes logging at the resource level.It will support conditional auditing based on users, groups or date/time, etc.

Access

- Provides Service activity data for all Policies that have Audit set to On. The default service Policy is configured to log all user activity within the Service. This default policy does not contain user and group access rules.You can filter the data based on the following criteria:

Search Criteria	Description
Access Enforcer	Access enforcer indicates who made the decision to allow or deny. In case of HDFS, the enforcer would XA (Ranger) or Hadoop.

Access Type	Type of access user has for e.g read,write
Start date,End date	Time and date is stored for each access.A date range is used to filter the results for that particular date range.
Service Name	The name of the service which the user tries to access
Service Type	The type of the service which the user tries to access
Result	This shows whether the operation was successfull or not
User	Name of the user which tried to access the resource
Client ip	Ip address of the user system which tried to access the resource

---

Admin

- This module Contains all events for the HDP Security Administration Web UI, including Service, Policy Manager, Log in, etc. (actions like create, update,delete,password change).You can filter the data based on the following

Search Criteria	Description
Action	These are operations performed on resources e.g(actions like create,update,delete,password change)
Audit Type	There are three values Resource,asset and xa user according to operations performed on Service,policy and users.
Session id	The session count increments each time you try to login to the system
Start Date	Login time and date is stored for each session.A date range is used to filter the results for that particular date range
User	Username who has performed create,update,delete operation.

- Difference view when we click on an operation (Update operation in this case)

Logging Session

- This module logs the information related to the sessions for each login.You can filter the data based on

Search Criteria	Description
End Date,Start Date	Login time and date is stored for each session.A date range is used to filter the results for that particular date range
Ip	The IP of the system through which we log in
Login id	The user name through which you login to the system
Login Type	The mode through which the user tries to login.(By entering username and password)
Result	Result based on login pass or fail

Session id	The session count increments each time you try to login to the system
User Agent	Login time and date is stored for each session

- Click on session id for session details.

Plugins

- This module shows the upload history of the Security Agents.This module displays all the services Exported from the system.You can filter the data based on the followin.

Search Criteria	Description
Http Response Code	The http code which you get when you try to export the Services
Plugin IP	Ip of the agent which tries to export the service
Plugin Id	Name of the agent which tries to export the service
Start Date,End Date	Export time and date is stored for each agent. A date range is used to filter the results for that particular date range.
Service Name	The service name we are trying to export.

- Plugins tab is useful to check components are communicating successfully with ranger or not.

Permissions

- ## Permissions Module

  The aim of permission module is to provide flexibility of user roles.With the help of permission model, Admin can restrict access or assign permission to any module for non-admin users.The main purpose of Permission model is to assign dedicated roles to non-admin users based on services such as policy manager, audit, reporting, user management,Key Manager.

Step 1: Put the pointer on Settings tab. Click on ‘Permissions’ from dropdown.

Step 2 : You can search the permissions by Group Name,Module Name,User Name.

- Add / Edit Permission

Step 3 : Click on edit button under Action column for access of particular module to selected user on permissions listing page.

<u>Step 4</u> : You can select multiple users and groups from drop down.

a. **User Permission**

b. **Group Permission**

<u>Step 5</u> : If Steve user is having permission of only Audit and Reports tab then only this two module will be visible to to mark user on his login.

a. Admin Login

b. Steve user Login