Security 3

Authorization with Ranger

Date of Publish: 2019-03-15

https://docs.hortonworks.com/

Contents

Authorization with Ranger

Creating Policies for NiFi Access

Once you have set up Ranger to manage NiFi authorization, you must create policies so that users can access and operate on the NiFi canvas.

Creating Policies to View NiFi

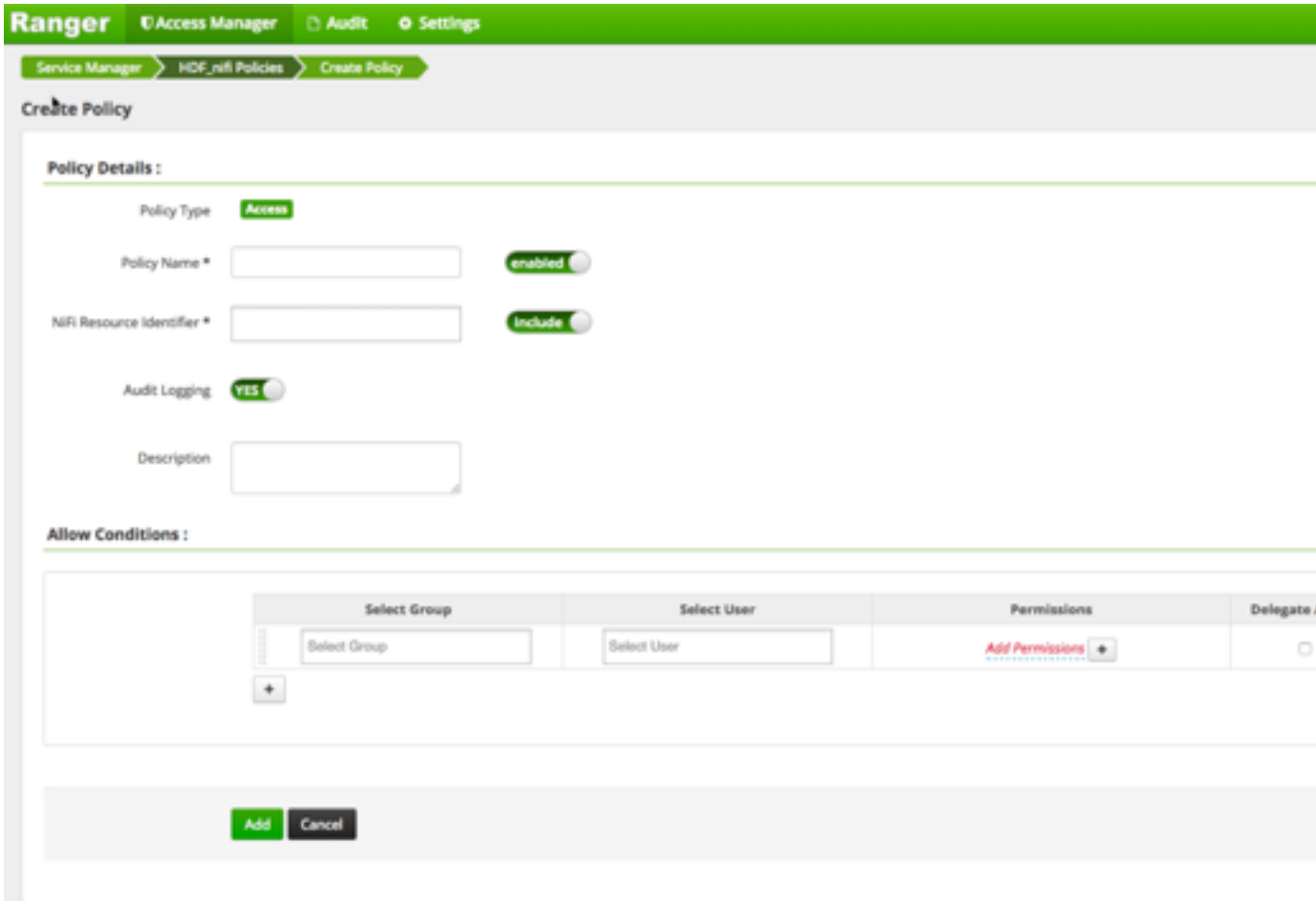
To allow users to view the NiFi UI, create the following policies for each host:

- /flow – read
- /proxy – read/write

To create policies:

1. From the Ranger console, click the NiFi Ranger plugin.

2. From the **List of Policies** page, click **Add New Policy**.
3. In the **Policy Details** dialog, create the /flow and /proxy policies.



4. To create the /flow policy:
   a. Provide the following information:
      - **Policy Name** – /flow
      - **NiFi Resource Identifier**- /flow
      - Select Users and Groups you want to immediately add.
      - Add **Read** permission
   b. Click **Add.**
5. To create the /proxy policy:
   a. Provide the following information:
      - **Policy Name** – /proxy
      - **NiFi Resource Identifier**- /proxy
      - Select Users and Groups you want to immediately add.
      - Add **Read** and **Write** permissions.
   b. Click **Add.**

Allowing Users Read and Write Access

To allow users complete read and write access to NiFi:

1. From the **Policy Details** page, select the global NiFi policy.
   - **Policy Name** – all - nifi-resource
   - **NiFi Resource Identifier** – x
2. Add users.

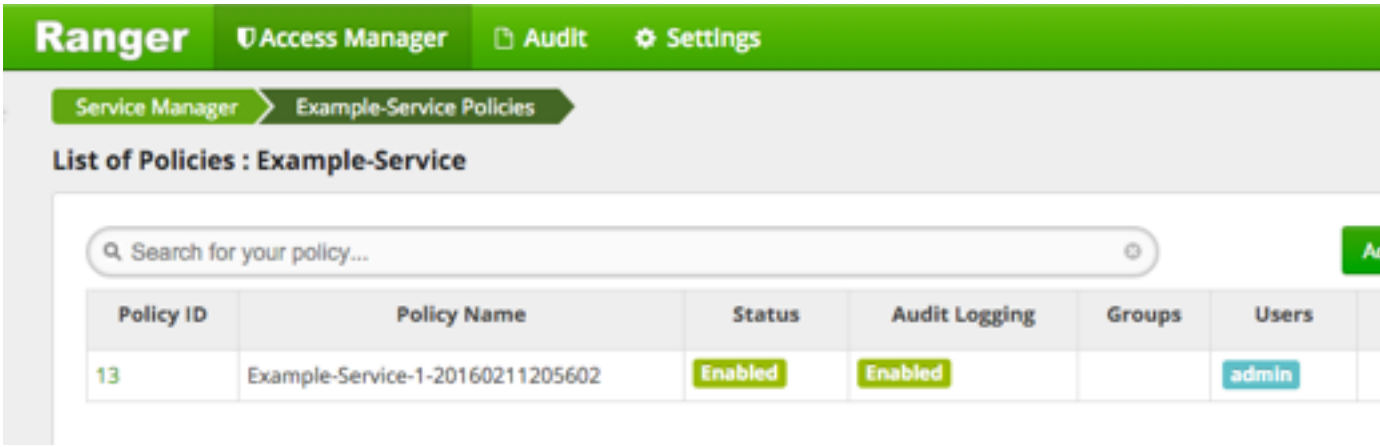
3. Add **Read** and **Write** permissions.

Create a Kafka Policy

To add a new policy to an existing Kafka service:

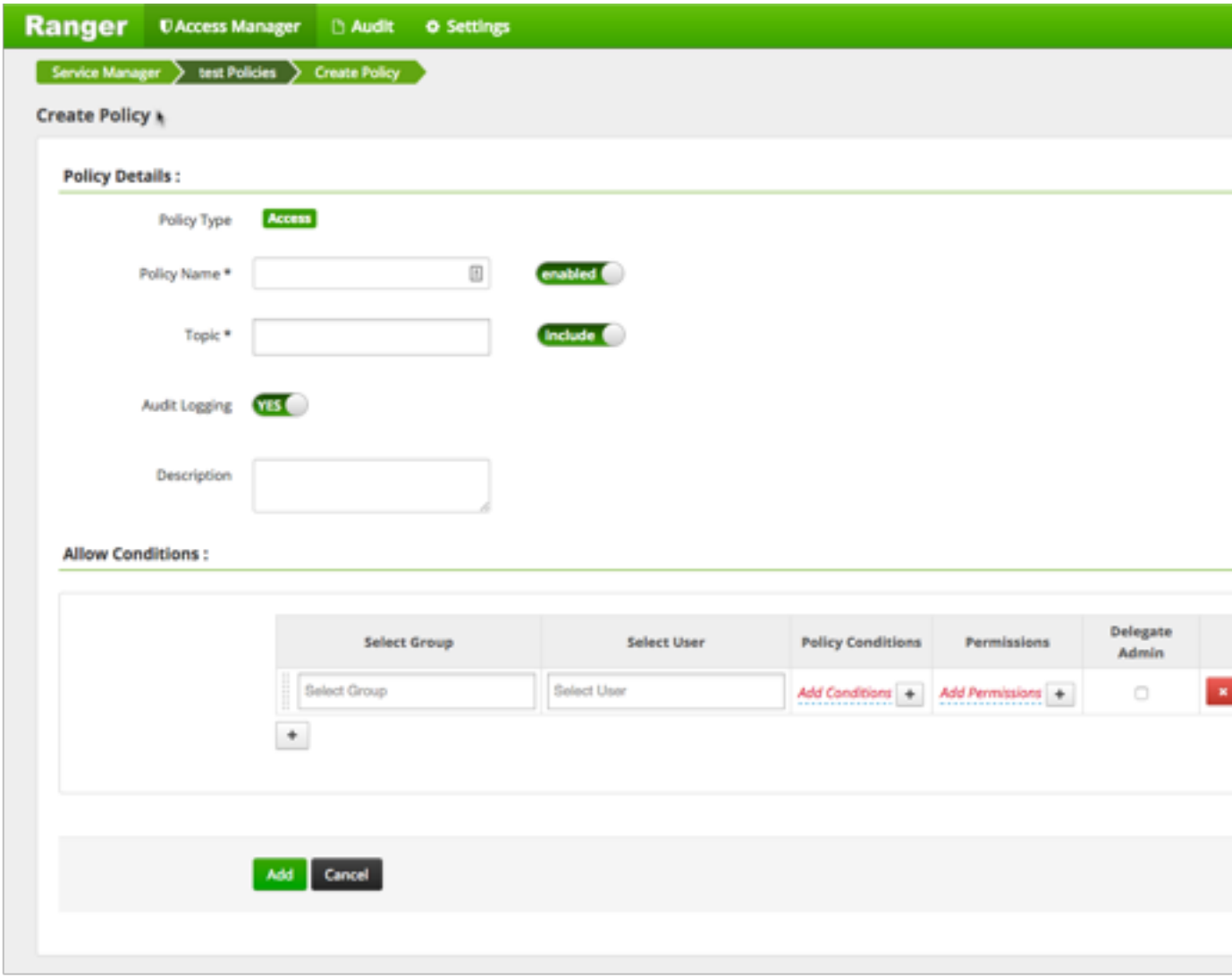
1. On the Service Manager page, select an existing service under Kafka.

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 1: Policy Details

Field	Description
Policy Name	Enter an appropriate policy name. This name cannot be duplicated across the system. This field is mandatory.
Topic	A topic is a category or feed name to which messages are published.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).

Table 2: Allow Conditions

Label	Description
Select Group	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). The public group contains all users, so granting access to the public group grants access to all users.
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	Specify IP address range.
Permissions	Add or edit permissions: Read, Write, Create, Admin, Select/ Deselect All.
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).

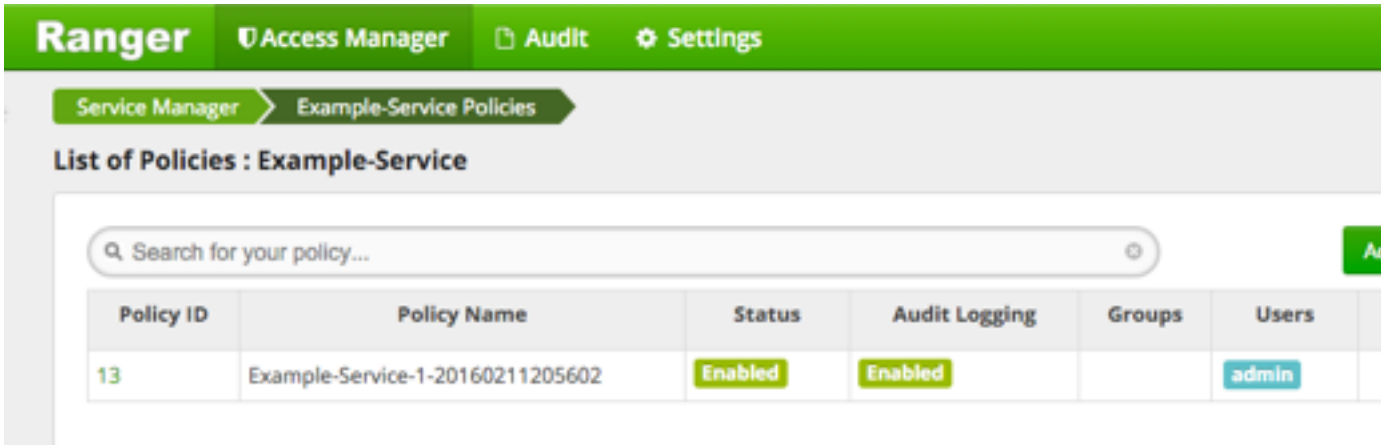
4. You can use the Plus (+) symbol to add additional conditions. Conditions are evaluated in the order listed in the policy. The condition at the top of the list is applied first, then the second, then the third, and so on.
5. Click **Add**.

Create a Storm Policy

To add a new policy to an existing Storm service:

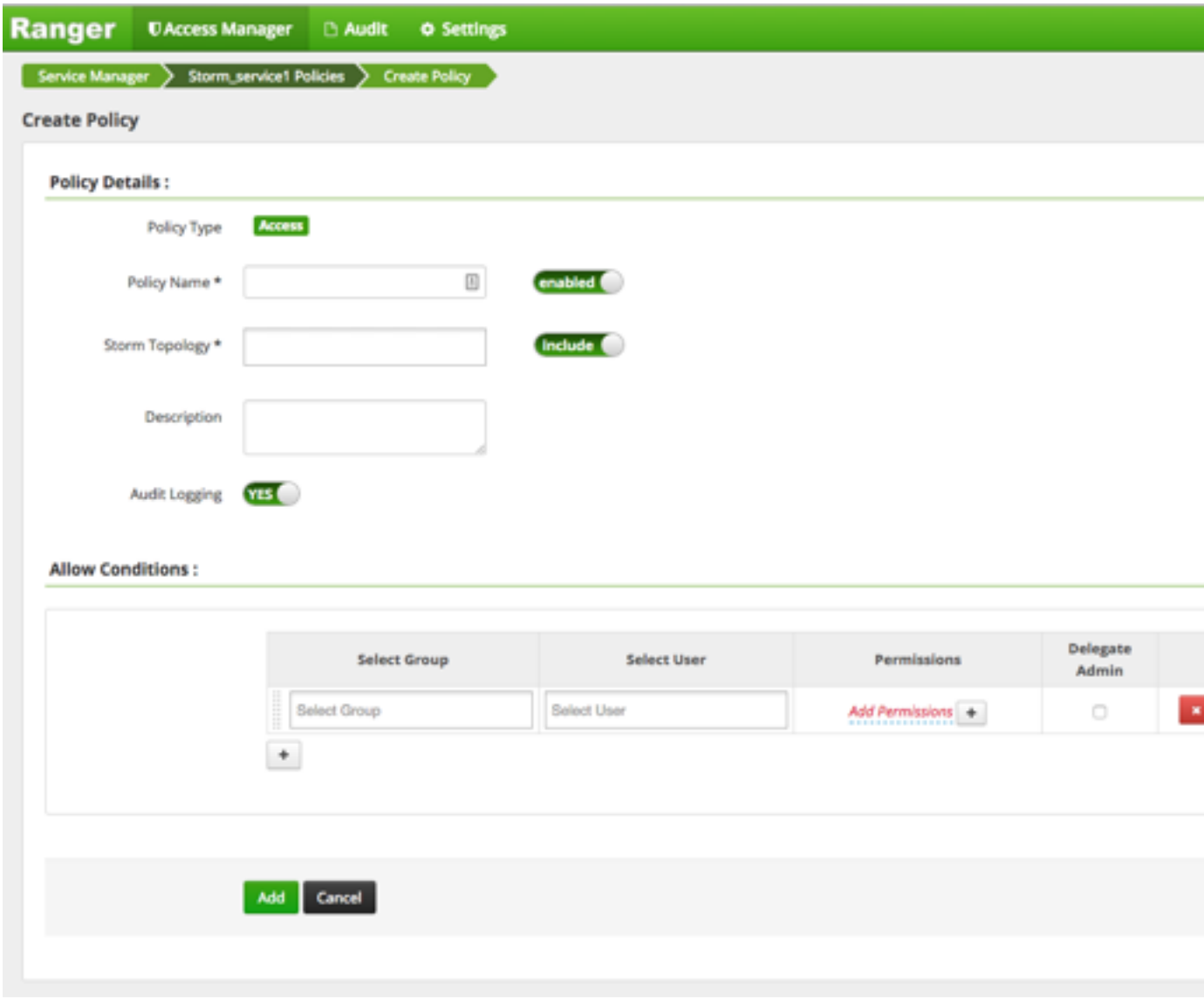
1. On the Service Manager page, select an existing service under Storm.

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 3: Policy Details

Label	Description
Policy Name	Enter an appropriate policy name. This name is cannot be duplicated across the system. This field is mandatory.
Storm Topology	Enter an appropriate Topology Name.
Description	(Optional) Describe the purpose of the policy.
Audit Logging	Specify whether this policy is audited. (De-select to disable auditing).

Table 4: Allow Conditions

Label	Description
Select Group	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). The public group contains all users, so granting access to the public group grants access to all users.
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).
Permissions	Add or edit permissions: Read, Write, Create, Admin, Select/ Deselect All.
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).

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

Table 5: Storm User and Group Permissions

Actions	Description
File upload	Allows a user to upload files.
Get Nimbus Conf	Allows a user to access Nimbus configurations.
Get Cluster Info	Allows a user to get cluster information.
File Download	Allows a user to download files.
Kill Topology	Allows a user to kill the topology.
Rebalance	Allows a user to rebalance topologies.
Activate	Allows a user to activate a topology.
Deactivate	Allows a user to deactivate a topology.
Get Topology Conf	Allows a user to access a topology configuration.
Get Topology	Allows a user to access a topology.
Get User Topology	Allows a user to access a user topology.
Get Topology Info	Allows a user to access topology information.
Upload New Credential	Allows a user to upload a new credential.
Admin	Provides a user with delegated admin access.

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. Click **Add**.