Cloudera Data Flow for Data Hub 7.2.0

Securing Flow Management Clusters

Date published: 2020-05-01
Date modified: 2020-06-16

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

Authorizing Access to Flow Management Clusters in CDP Public Cloud..... 4

User Authorization..... 4

Before you begin..... 4
Understanding the workflow..... 4
Authorization options..... 5
Option A. Assigning administrator-level permissions..... 6
Option B. Assigning selective permissions to a user..... 10
Step 1. Assign the EnvironmentUser role..... 10
Step 2. Add the user to pre-defined Ranger access policies..... 13
Step 3. Create a Custom Access Policy..... 15
Example..... 21

Pre-defined Ranger access policies for Apache NiFi..... 22

Pre-defined Ranger access policies for Apache NiFi Registry..... 23

Authorizing Access to Flow Management Clusters in CDP Public Cloud

Flow management users are authenticated automatically when they log into CDP. To access Apache NiFi and Apache NiFi Registry, a CDP administrator must assign the appropriate role and access policies to a new user.

CDP provides the following default security features for flow management users and clusters:

- Single-sign on (SSO) authorization with Apache Knox.
- Metadata management and governance capabilities with Apache Atlas.
- Flow versioning and management with Apache NiFi Registry.
- TLS encryption to secure communications over the network.
- Fine-grained authorization to do a specific action and/or operation with Apache Ranger.

For more information, see *CDP Security Overview*.

This document explains how to authorize a new user to access and manage NiFi and NiFi Registry.

Related Information
CDP Security Overview

User Authorization

When an administrator creates an environment, users cannot automatically access the environment, clusters, data lake, or flow management resources. To authorize a user, the administrator must assign the appropriate CDP resource role and one or more Ranger access policies to the user.

For more information about roles, see *Understanding roles and resource roles*.

For more information about Ranger access policies, see *Ranger Policies Overview*.

A Ranger access policy for flow management contains one or more access rights to NiFi or NiFi Registry resources.

Related Information
Understanding roles and resource roles
Ranger Policies Overview

Before you begin

Meet the prerequisites before you assign roles and policies to a user.

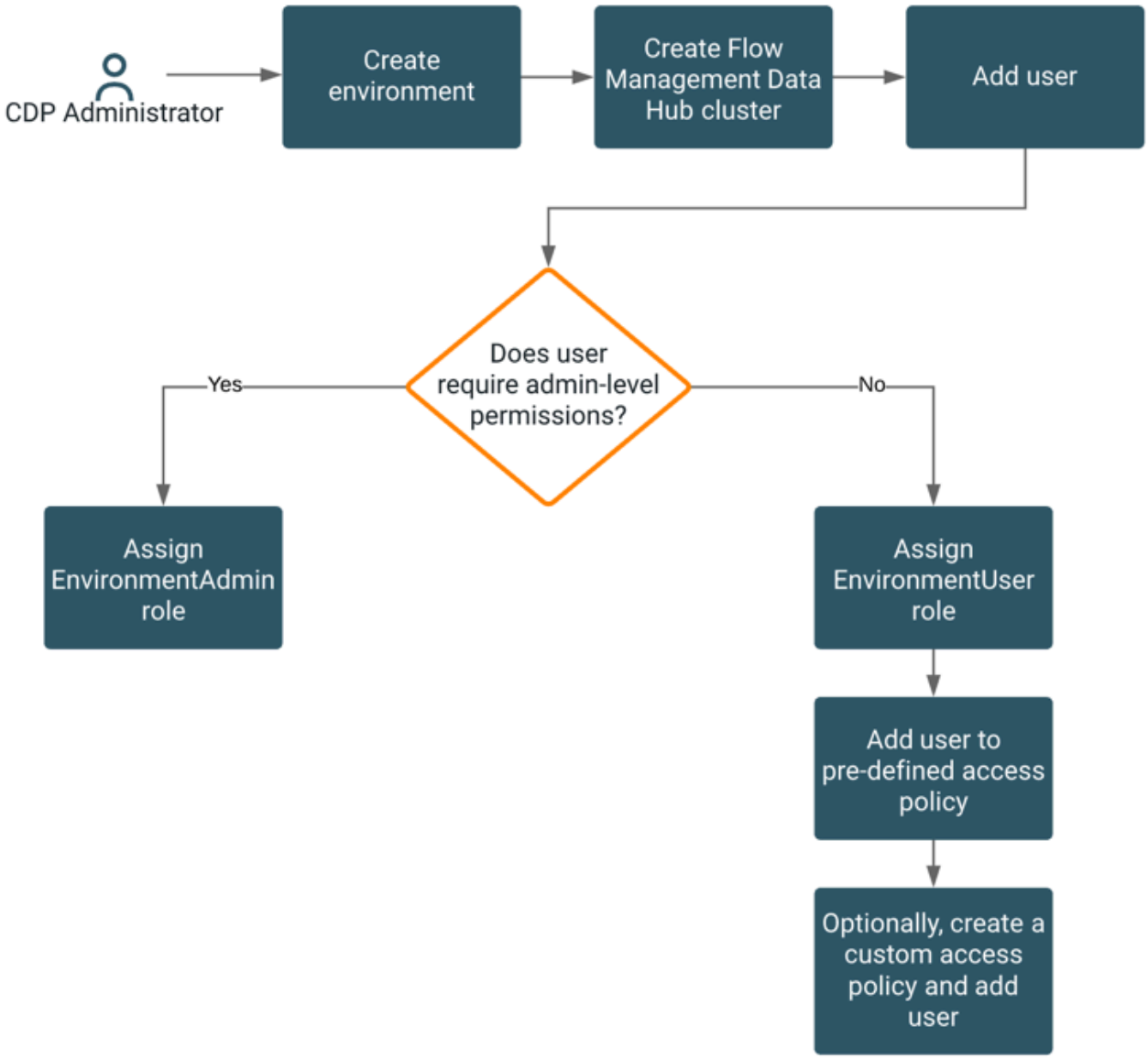
Ensure that you meet the following prerequisites:

- You are a CDP Administrator.
- You created an environment.
- You created a Flow Management Data Hub cluster.
- You determined the permission level for each user.

Understanding the workflow

The flow chart explains the process of authorizing flow management users.

The following diagram shows the prerequisites and the workflow involved in authorizing a flow management user:



Authorization options

Based on the permissions a user needs, assign a CDP role and add the user to access policies.

Select one of the following options:

Option A: If the user requires administrator-level permissions to NiFi and NiFi Registry, assign the EnvironmentAdmin role.

Option B: If the user requires selective permissions to NiFi and NiFi Registry, then do the following:

1. Assign the EnvironmentUser role to the user.
2. Add the user to the appropriate Ranger access policies for NiFi and NiFi Registry.
3. Optionally, create a custom policy and add the user to it.

Option A. Assigning administrator-level permissions

Assign the EnvironmentAdmin role to enable users to have administrator-level privileges to the environment. With the EnvironmentAdmin role, the user can access and manage environments, Flow Management clusters, and NiFi and NiFi Registry resources. Users can also authorize other users to access flow management resources.

About this task

When a user acquires the EnvironmentAdmin role, the following events happen:

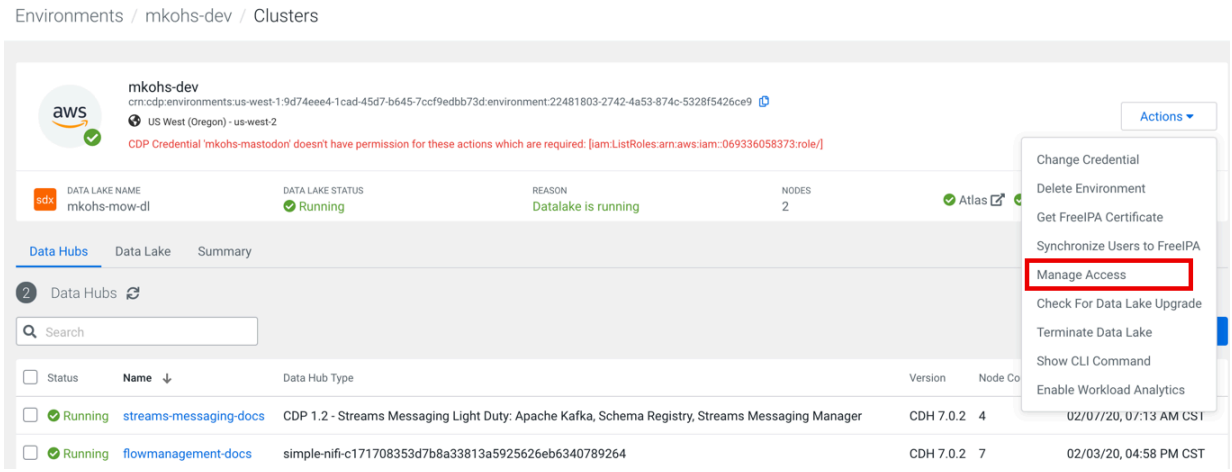
- The user acquires the datahub/adminNiFi and datahub/adminNiFiRegistry rights.
- The user is added to the following internal groups:
  - NiFi administrator group: _c_nifi_admins_[env-hash]

    This group is automatically added to the pre-defined Ranger access policies for NiFi.
  - NiFi Registry administrator group: _c_nifiregistry_admins_[env-hash]

    This group is automatically added to the pre-defined Ranger access policies for NiFi Registry.

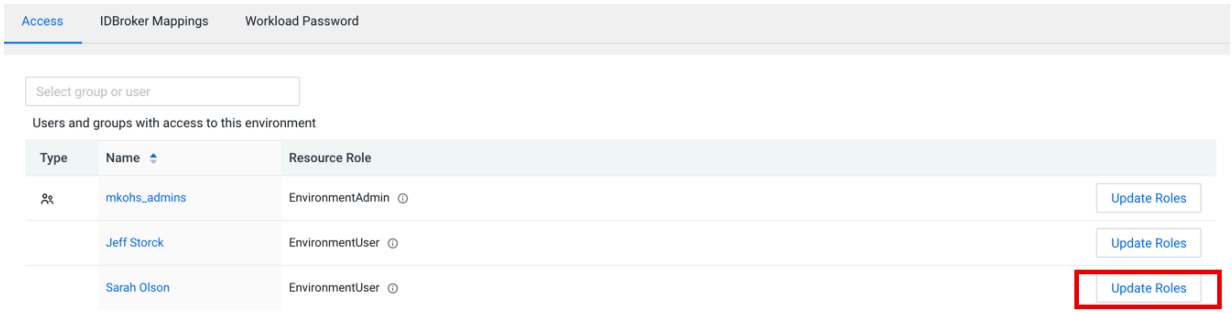
Procedure

1. Click the **Environments** tab.
2. Locate the environment.
3. Click the environment name.
4. Click Actions > Manage Access.



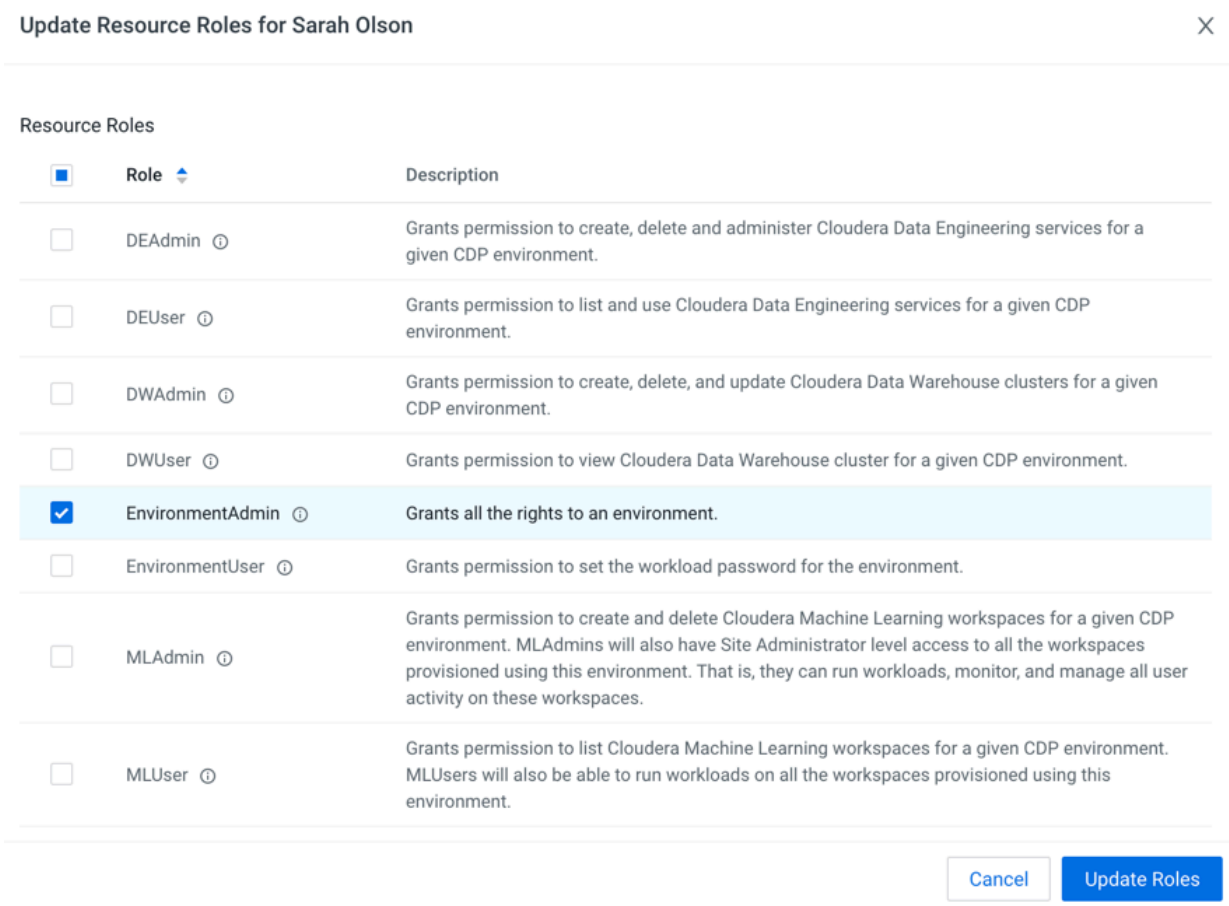
The **Access** page appears.

5. Locate the user and click Update Roles.



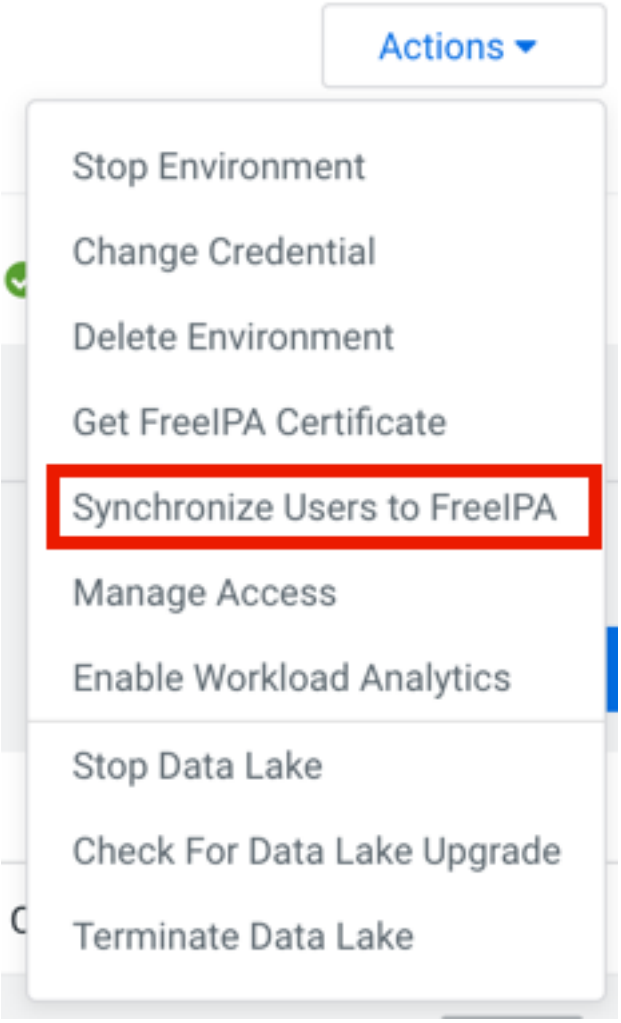
The **Update Resource Role** page for the user appears.

6. Check the EnvironmentAdmin option.



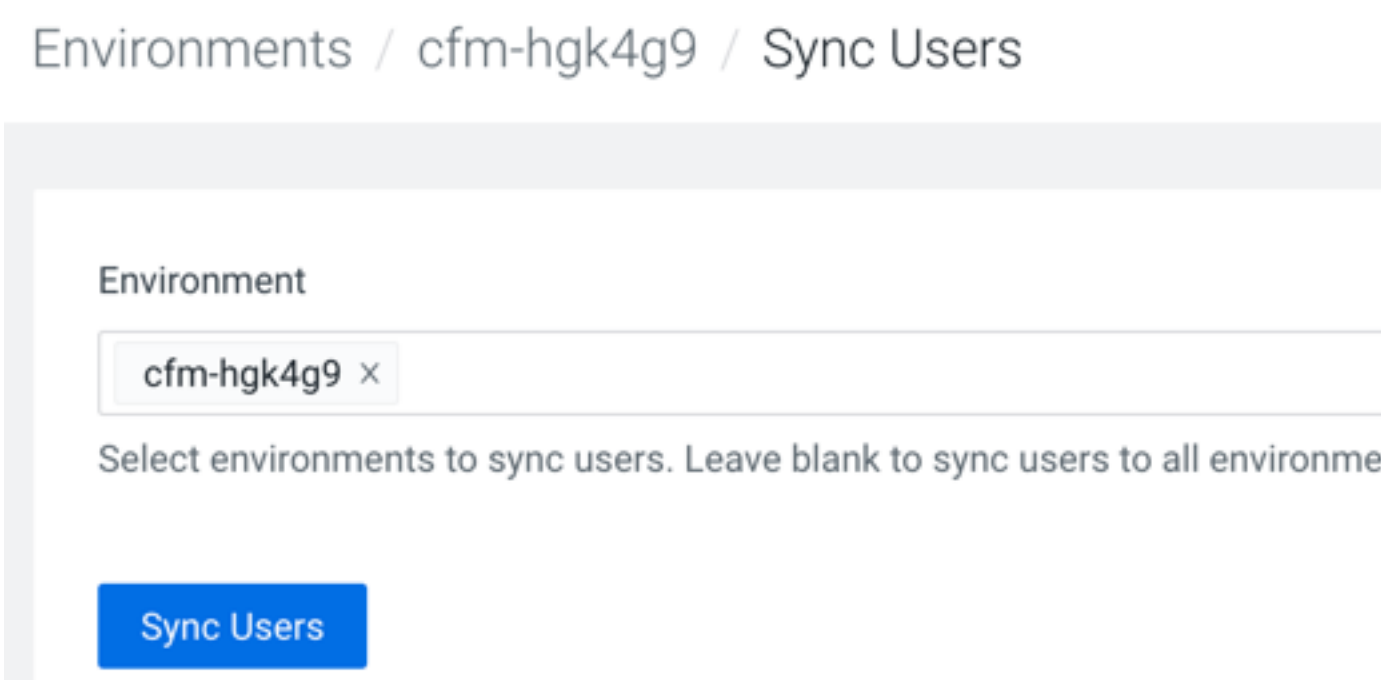
7. Click Update Roles.
8. Go back to the **Environments** tab and locate the environment.

9. Click Actions > Synchronize Users to FreeIPA.



The **Sync Users** window appears.

10. Click Sync Users.



This synchronizes the user to the FreeIPA identity management system to enable SSO.

Results

With the EnvironmentAdmin role and membership in the internal NiFi or NiFi Registry groups, the user has the ability to:

- Access and manage the environment and Flow Management clusters.
- Authorize users or groups by adding them to Ranger access polices.
- Modify or create conditions in pre-defined Ranger access policies.
- Create new Ranger access policies and create conditions that specify the desired level of access for each user or group.

Note: The EnvironmentAdmin role also gives a user the following privileges:

- Administrator rights to environments outside of NiFi.
- The right to modify pre-defined or custom Ranger access policies for any Ranger service in the environment.

For more information on roles, see *Understanding roles and resource roles*.

For more information about Ranger access policies, see *Ranger Policies Overview*.

To authorize flow management users who do not require administrator-level permission, add the users individually or as a group to specific Ranger access policies for selective access to NiFi and NiFi Registry resources. For more information, see *Option B. Assigning selective permissions to a user*.

Related Information

Understanding roles and resource roles

Ranger Policies Overview

Option B. Assigning selective permissions to a user

Option B. Assigning selective permissions to a user

Assign the EnvironmentUser role to users to access the environment and Flow Management clusters. Then, based on the user's access requirements, add the user or a group of users to the appropriate Ranger access policies for NiFi and NiFi Registry.

Perform the following steps to authorize access for a new user:

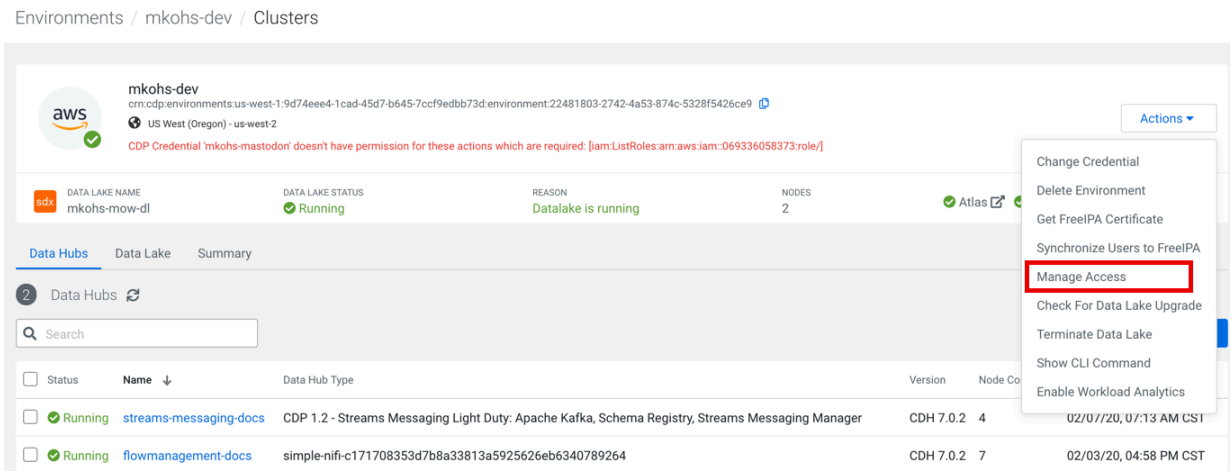
1. Assign the EnvironmentUser role.
2. Add the user or group to the appropriate pre-defined Ranger access policies.
3. Create a custom Ranger access policy and add the user or group.

Step 1. Assign the EnvironmentUser role

Assign the EnvironmentUser role to enable users to set their password and access the environment.

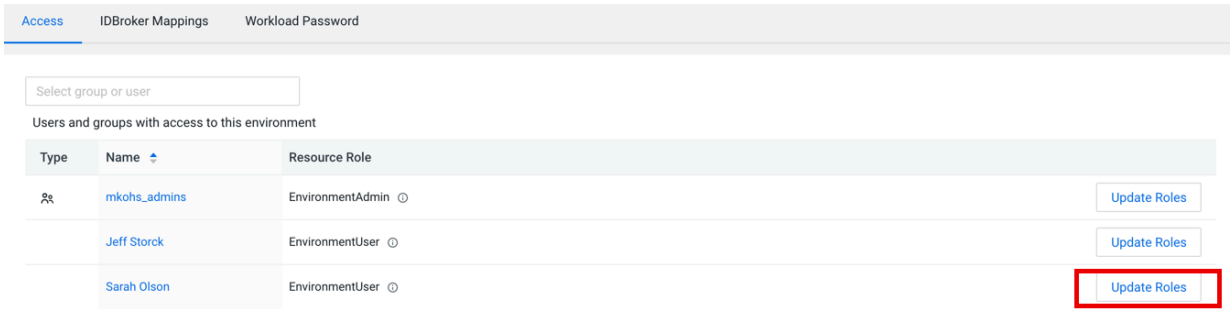
Procedure

1. From the Cloudera Management console, go to the Environments tab.
2. Use the Search bar to find the environment.
3. Click the environment name.
4. Click Actions > Manage Access.



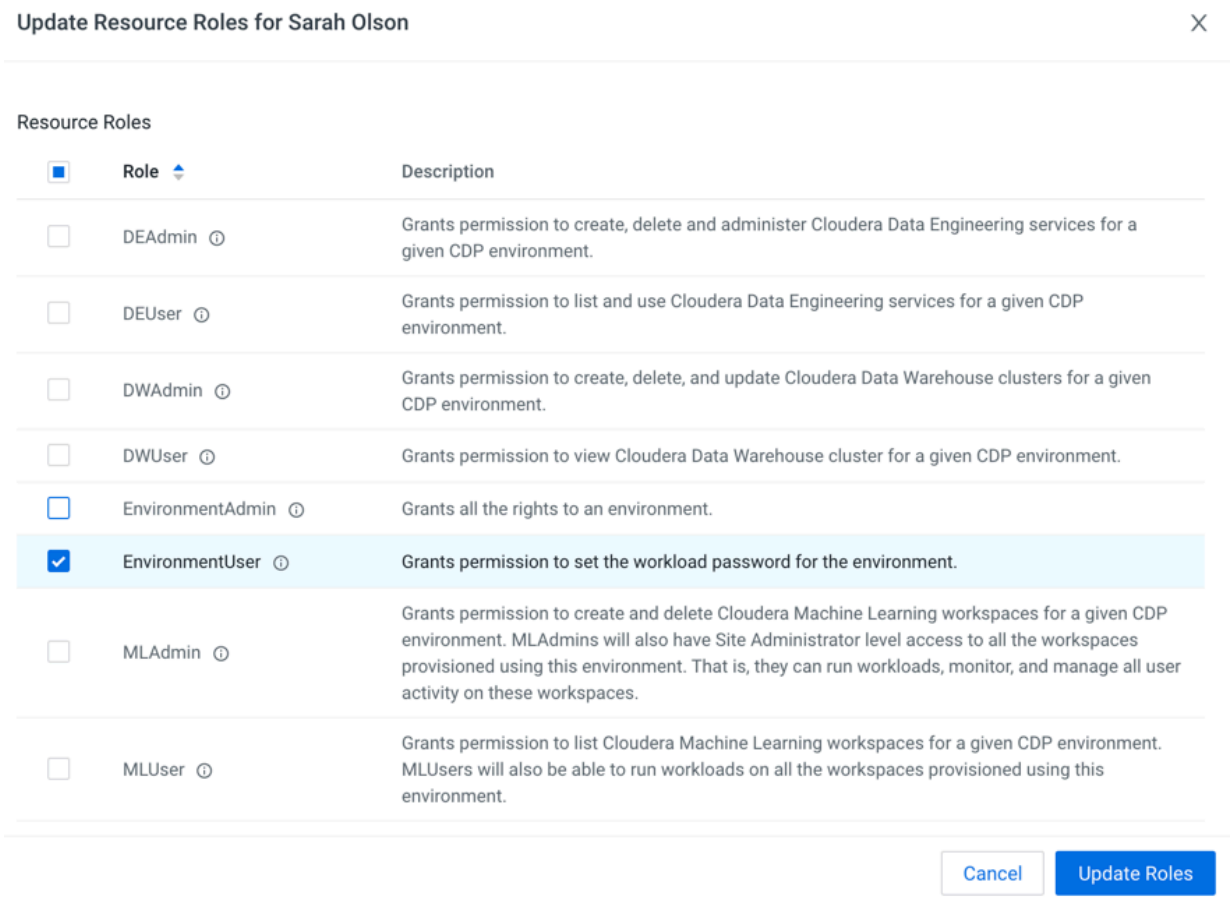
The **Access** page appears.

5. Locate the user and click Update Roles.



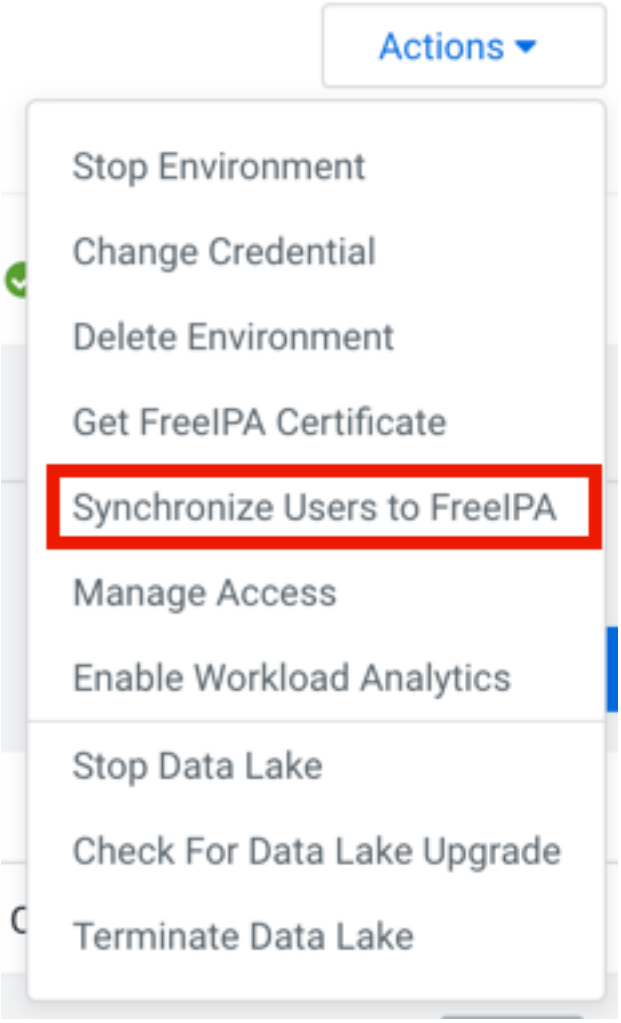
The **Update Resource Role** page for the user appears.

6. Check the EnvironmentUser option.



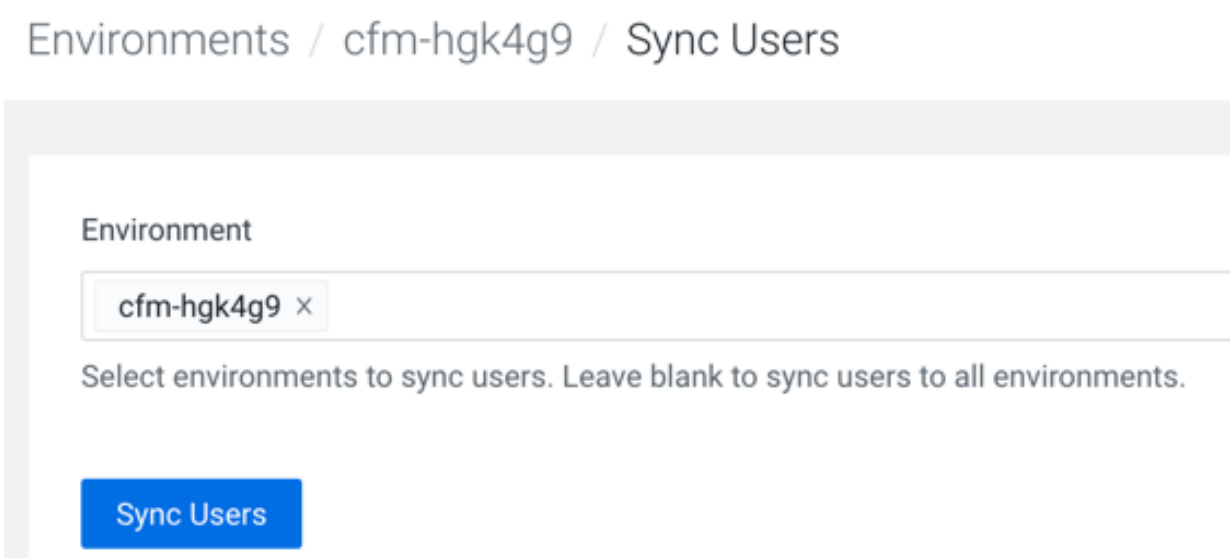
7. Click Update Roles.
8. Go back to the **Environments** tab and locate the environment.

9. Click Actions > Synchronize Users to FreeIPA.



The **Sync Users** window appears.

10. Click Sync Users.



This synchronizes the user to the FreeIPA identity management system to enable SSO.

Results

The user is added to the environment and can access the environment and Flow Management clusters. You can now add the user or a group of users to Ranger policies that allow access to NiFi and NiFi Registry resources.

What to do next

Complete the steps listed in *Step 2. Add the user to pre-defined Ranger access policies*.

Related Information

Step 2. Add the user to pre-defined Ranger access policies

Step 2. Add the user to pre-defined Ranger access policies

When an authenticated user attempts to view or modify a NiFi or NiFi Registry resource, the system checks whether the user has privileges to perform that action. These privileges are determined by the Ranger access policies that a user is associated with.

About this task

Determine what the user can command, control, and observe in a NiFi dataflow or in NiFi Registry and accordingly add the user or a group of users to the appropriate pre-defined Ranger access policies.

Each pre-defined Ranger access policy confers specific rights to NiFi or NiFi Registry resources.

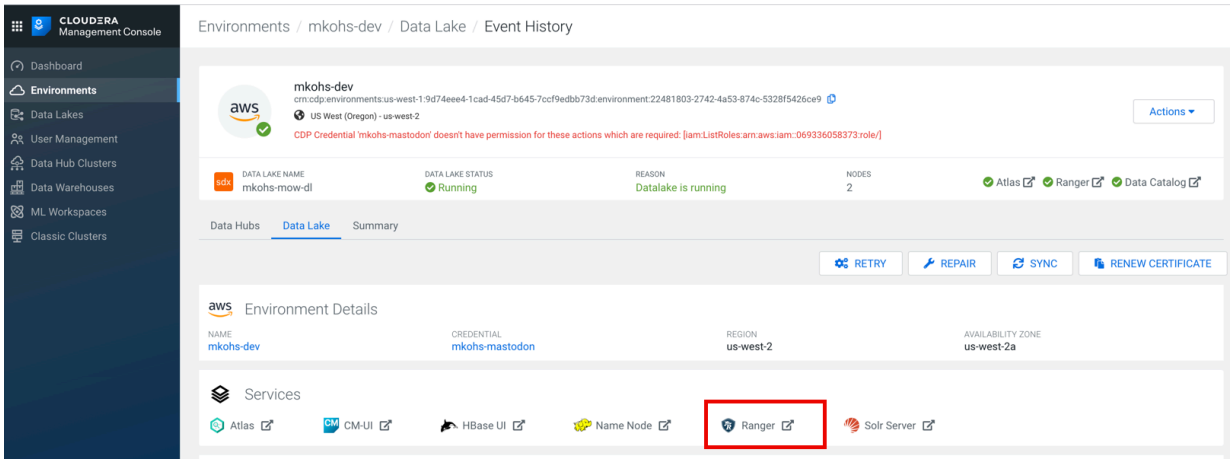
For more information, see:

- *Pre-defined Ranger access policies for NiFi resources*
- *Pre-defined Ranger access policies for NiFi Registry resources*

Procedure

1. Go to the environment.
2. Click the **Data Lake** tab.

3. Click the Ranger icon.

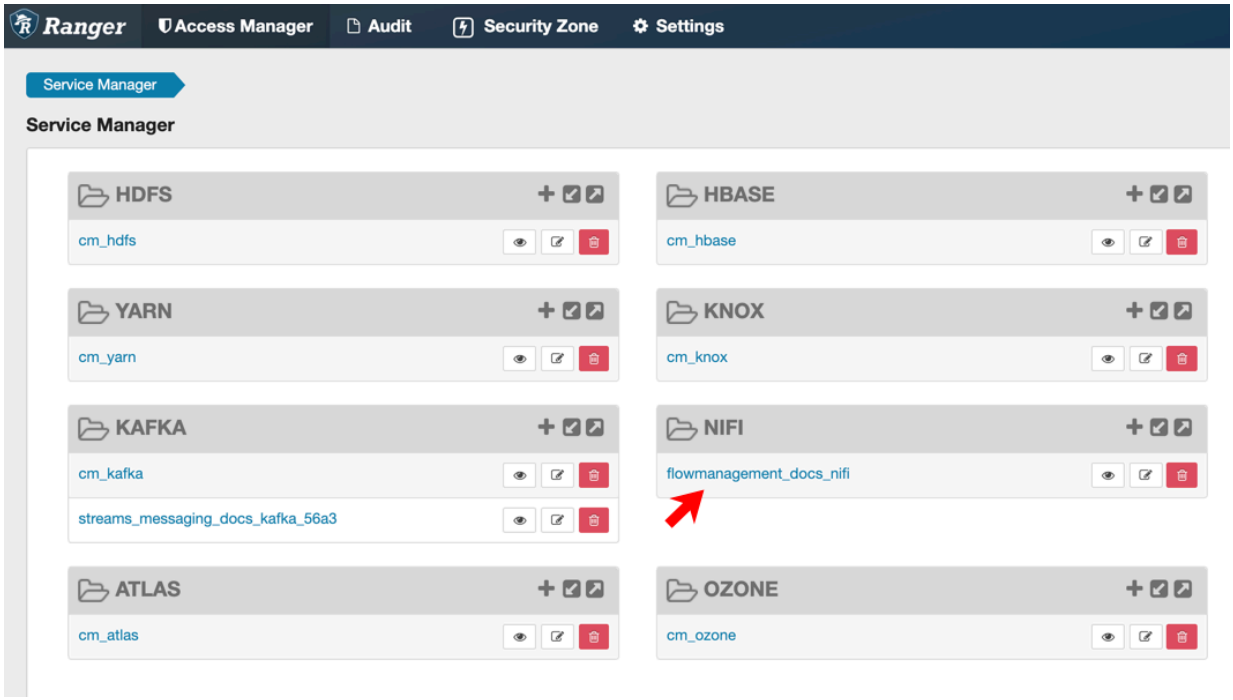


The **Ranger Service Manager** page appears.

Each cluster in the environment is listed under its respective service. For example, the NiFi clusters in the environment are listed under NiFi.

4. Select a cluster from either the NiFi or NiFi Registry section.

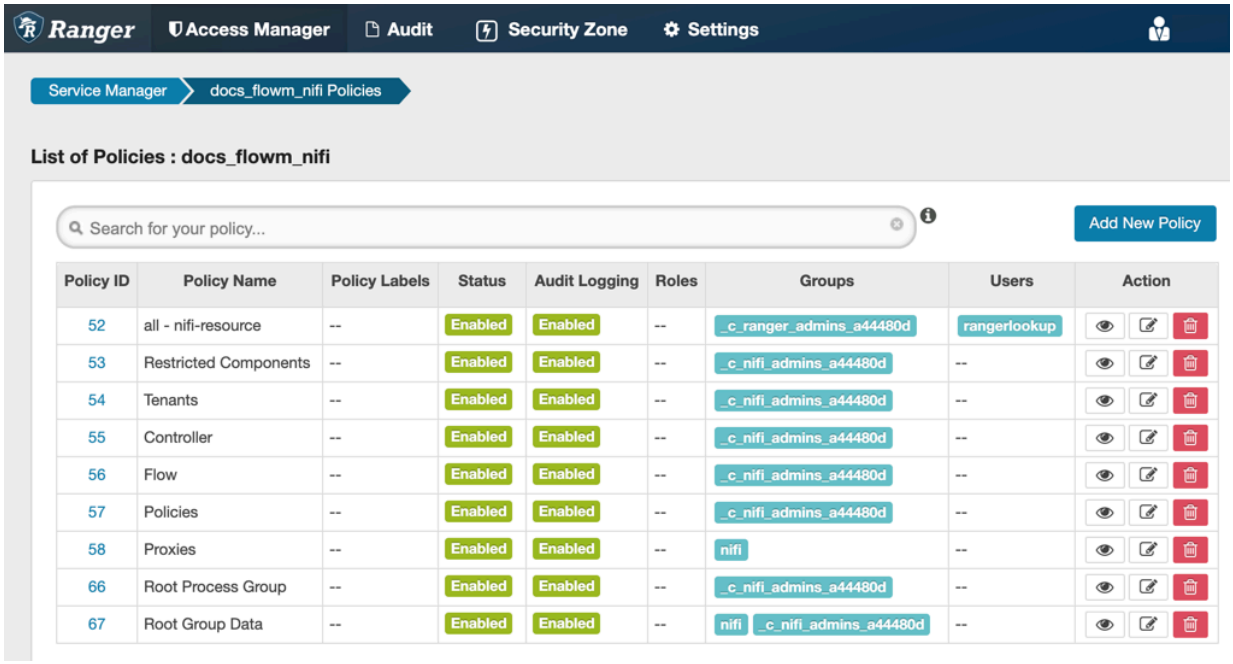
The following image shows the list of pre-defined policies for NiFi:



The **List of Policies** page appears.

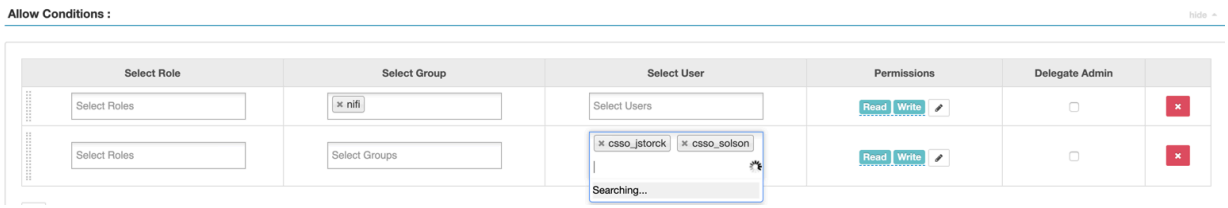
5. Click the ID for a policy.

   The following image shows the list of pre-defined policies for NiFi:



   The **Edit Policy** page appears.

6. In the Allow Conditions section, add the user or the user group to the Select User field.



7. Click Save.

Results

The user now has the NiFi and NiFi Registry rights according to the policies you added the user or user group to. These rights are inherited down the hierarchy unless there is a more specific policy on a component.

What to do next

Complete the steps listed in *Step 3. Create a Custom Access Policy*.

Related Information

Pre-defined Ranger access policies for Apache NiFi

Pre-defined Ranger access policies for Apache NiFi Registry

Step 3. Create a Custom Access Policy

Step 3. Create a Custom Access Policy

A user might need access to specific NiFi or NiFi Registry resources such as a processor, processor group, remote process group, funnel, label, controller service, or bucket. If the user cannot access the component through an inherited Ranger access policy, then you must create a custom Ranger access policy for the specific component and add the user to this policy. If all the users in a group require the same access, you can add the user group to the Ranger access policy.

About this task

Each custom Ranger access policy provides access to a specific component.

First determine which NiFi or NiFi Registry components a user needs access to. Then create a new policy for each component and add the user or user group to the new policy.

When you create a new policy, you must specify the ID of the component that the user requires access to.

Note:

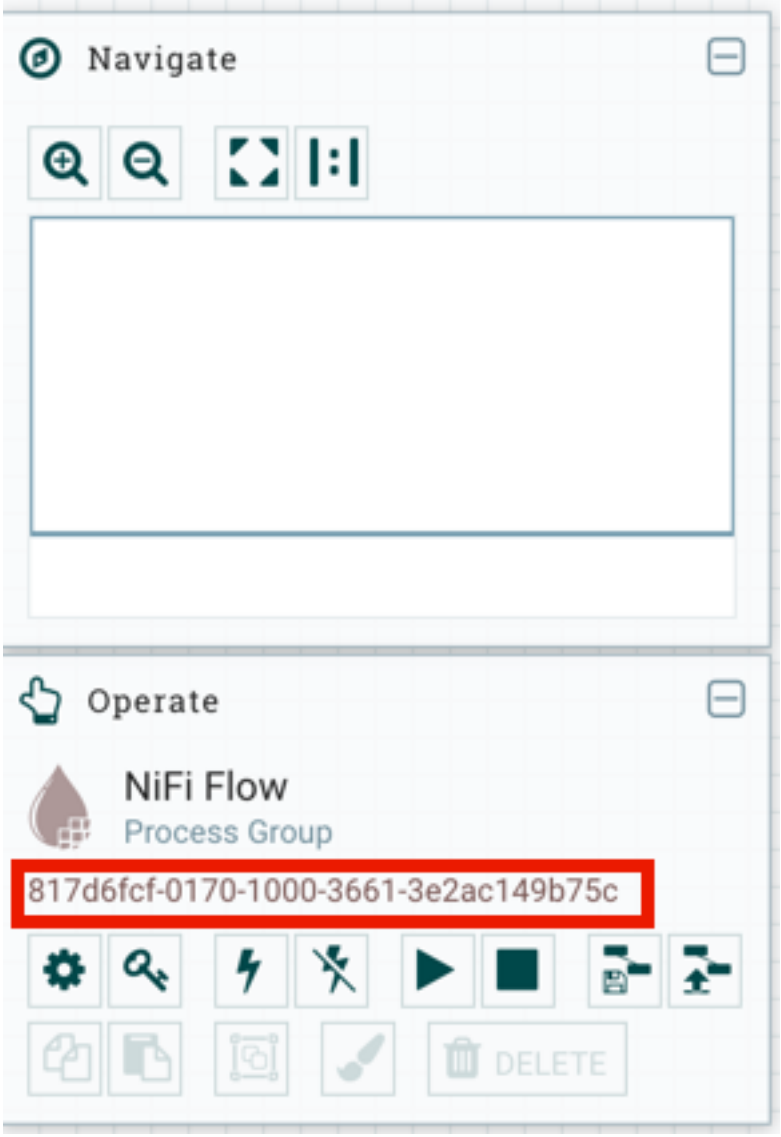
If a user requires permission to view or modify data for a specific component, you must create a custom data access policy and add the user and the nifi group to that policy.

The nifi group is a dynamically-managed group that exists on all Flow Management Data Hub hosts and contains the identities of NiFi and Knox nodes. When you add the nifi group to the data policy for a specific component, you authorize the nodes to access data on behalf of the user.

Procedure

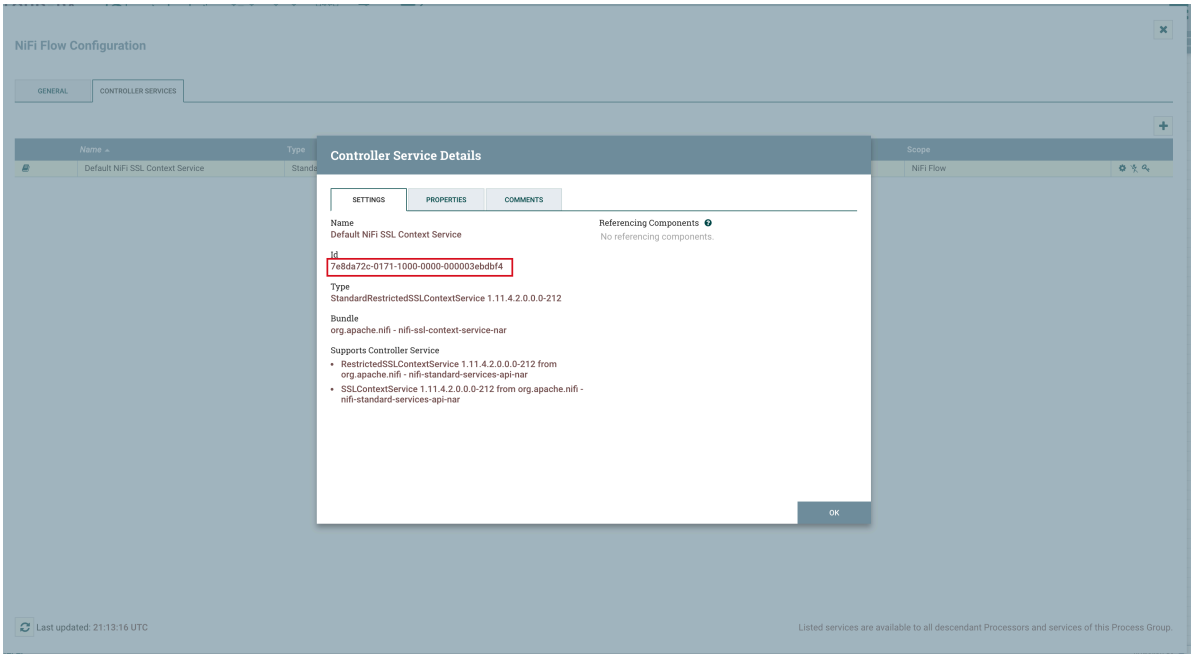
1. From the NiFi canvas, copy the ID of the process group, SSL Context Service, or controller service for reporting tasks that the user needs access to.

2. To locate the ID for a process group:
   a) Click the process group.
   The ID appears in the **Operate** pane.

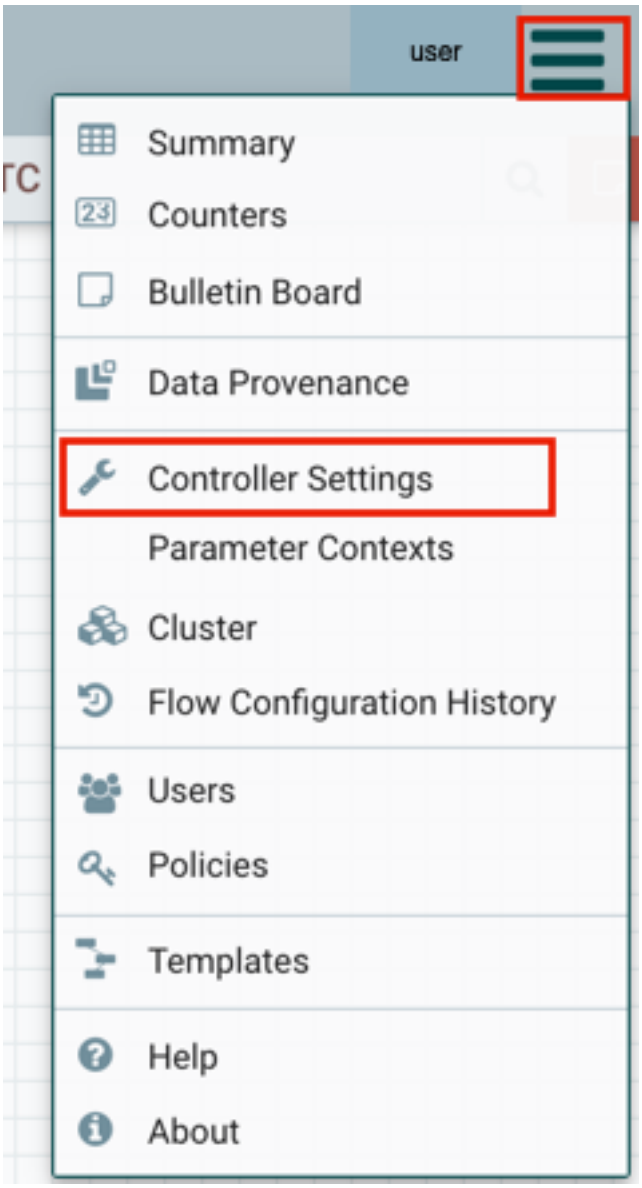


   b) Copy the ID.

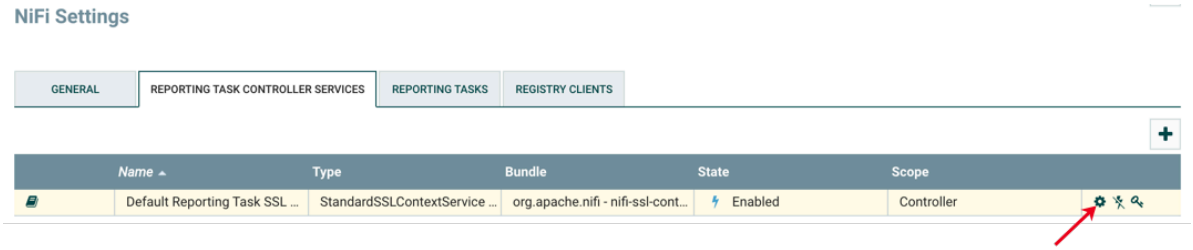
3. To locate the ID of the SSL Context Service:
   a) Click the settings icon on the process group.
      The **NiFi Flow Configuration** appears.
   b) Click the **Controller Services** tab.
   c) Click the **Settings** icon for the Default NiFi SSL Context Service.
      The **Controller Service Details** window appears.
   d) From the **Settings** tab, copy the ID from the Id field.



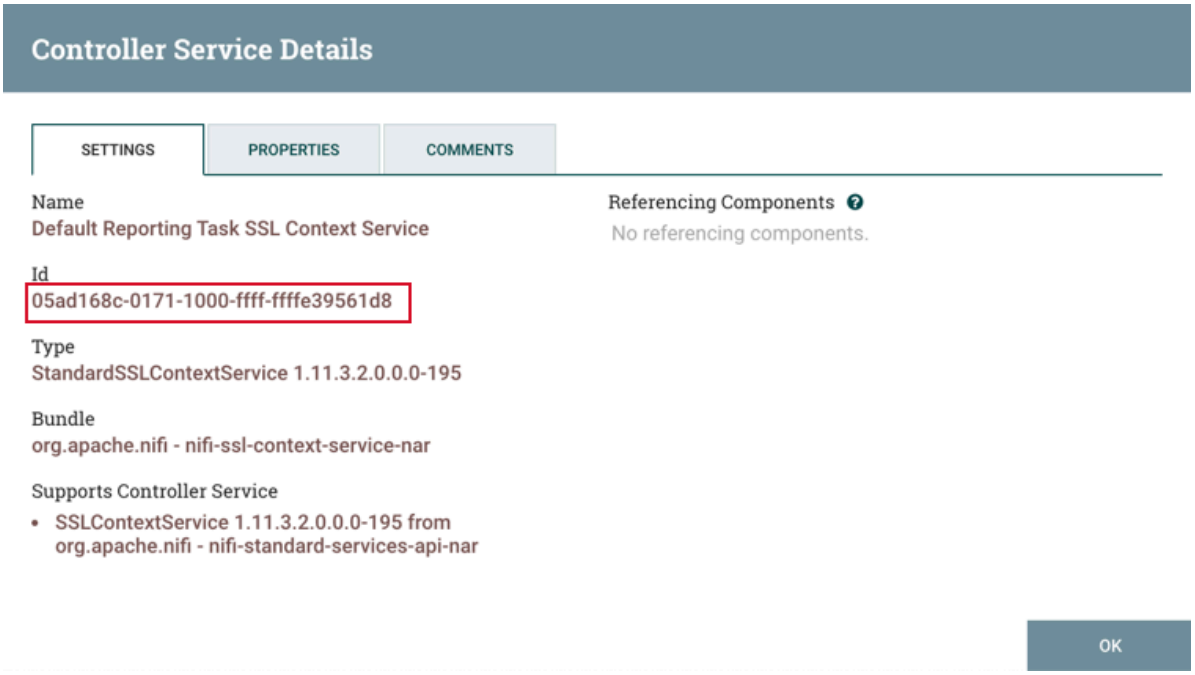
4. To locate the ID of a controller service for reporting tasks:
   a) Click the process group.
   b) Click the menu on the top right of the UI and select Controller Settings.



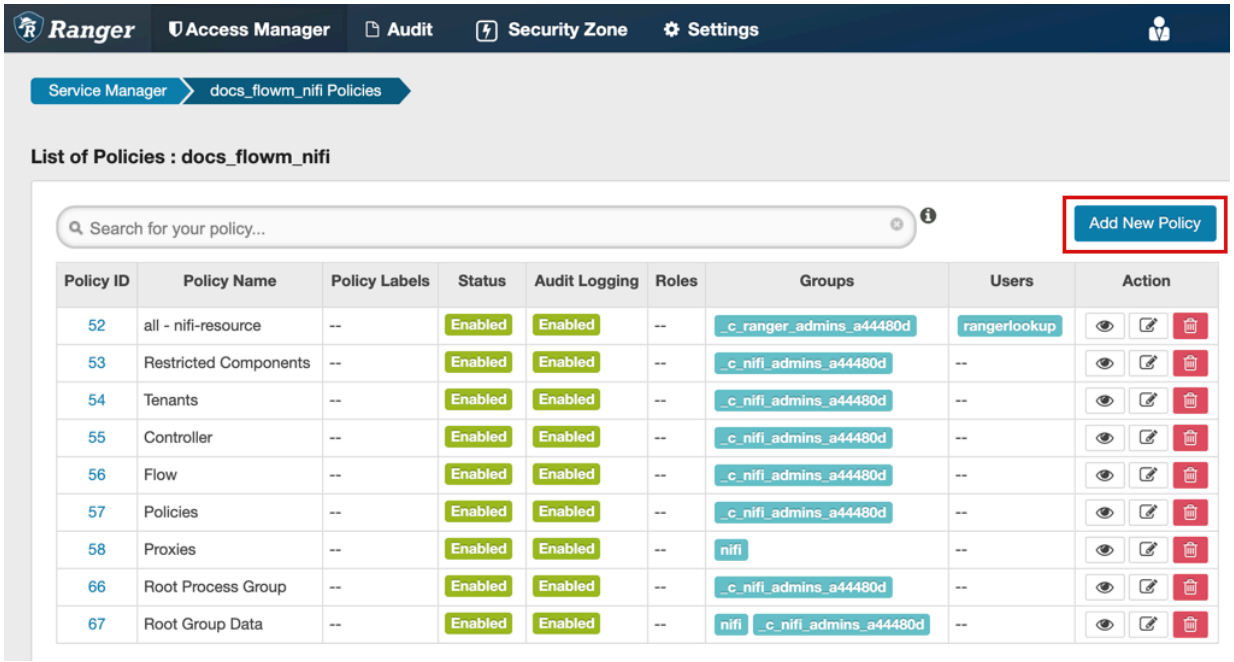
   The **NiFi Settings** page appears.
   c) Click the **Reporting Tasks Controller Services** tab.
   d) Click the Settings icon for the controller service.



   The **Controller Service Details** page appears.
   e) From the **Settings** tab, copy the ID from the Id field.



5. Go back to the **Ranger List of Policies** page.
6. Click Add New Policy.



The **Create Policy** page appears.

7. Enter a unique name for the policy.
8. Optionally, enter a keyword in the Policy Label field to aid in searching for a policy.
9. Enter the resource descriptor and the resource ID in the NiFi Resource Identifier or NiFi Registry Resource Identifier field in the following format: <resource descriptor>/<resource ID>

   To determine a NiFi resource descriptor, see *Pre-defined Ranger access policies for Apache NiFi*.

   To determine a NiFi Registry resource descriptor, see *Pre-defined Ranger access policies for Apache NiFI Registry*.
10. Optionally, enter a description.

11. Add a user or a group.

Note: If a user requires permission to view or modify the data for a specific component, you must create a data policy with /data/<component-type>/<component-UUID> as the resource identifier. Then add the user and the nifi group to the policy to authorize the NiFi and Knox nodes to access data on behalf of the user.

12. Set the permission level for the user or group.
13. Click Add.

Results

The user or group of users can now access the component specified in the custom policy.

Related Information

Pre-defined Ranger access policies for Apache NiFi

Pre-defined Ranger access policies for Apache NiFi Registry

Example

In the following scenario a user requires access to specific NiFi and NiFi resources. You must add the user to the appropriate access policies.

UserA must be able to do the following tasks:

- Access the NiFi UI.
- Export a flow.
- View data queued in connections.
- View data flowing through.
- Use a NiFi SSLContextService to connect to SSL-enabled systems.
- Set up version control for a flow.

Complete the following steps to enable UserA to perform the required tasks:

1. Add UserA to the pre-defined Ranger access policy for NiFi, Flow. Set the permissions to Read.

   The Flow policy gives the user the right to view the NiFi UI.
2. Create a Ranger access policy for NiFi with:

   - Resource descriptor: /data/process-groups/<ID of process-group>
   - Permission: Read and Write

   Add UserA to this custom policy. The policy gives the user the right to export the data, view the data that is queued and flowing through the connections.
3. Create a Ranger access policy for NiFi with:

   - Resource descriptor: /controller-service/<ID of SSL Context Service>
   - Permission: Read

   Add UserA to this custom policy. The policy gives the user the right to use the specified SSLContextService in their flows to connect to SSL-enabled systems.
4. Create a Ranger access policy for NiFi Registry with:

   - Resource descriptor: /buckets/<ID of bucket>
   - Permission: Read, Write, and Delete

   Add UserA to this custom policy. The policy gives the user the right to set up version control for a flow.

Pre-defined Ranger access policies for Apache NiFi

Based on a user's responsibilities, you can add users to one or more of the following Ranger access policies. When you create a custom policy, use the resource descriptor in the NiFi Resource Identifier field.

The following table lists the pre-defined Ranger access policies for NiFi:

Ranger Policy	Description	Resource Descriptor
Controller	Allows users to view and modify the controller including Reporting Tasks, Controller Services, Parameter Contexts and Nodes in the Cluster.	/controller
Flow	Allows users to view the NiFi UI.	/flow
Policies	Allows users to view the policies for all components.	/policies
Provenance	Allows users to submit a Provenance Search and request Event Lineage.	/provenance
Proxies	Allows NiFi and Knox hosts to proxy user requests. Does not apply to users or user groups.	/proxy
Restricted Components	Allows users to create/modify restricted components assuming other permissions are sufficient. The restricted components may indicate the specific permissions that are required. Permissions can be granted for specific restrictions or be granted regardless of restrictions. If permission is granted regardless of restrictions, the user can create/modify all restricted components. Some examples of restricted components are ExecuteScript, List/FetchHDFS, and TailFile.	/restricted-components
Root Group Data	Allows users and the nifi group to view and delete data from the root group and down the hierarchy unless there is a more specific policy on a component. **Note:** The nifi group is a dynamically managed list of Knox and NiFi node identities. The group exists on all Data Hub Flow Management hosts.	/data/process-groups
Root Group Provenance Data	Allows users to view provenance data.	/provenance-data/process-groups/
Root Process Group	Allows users to view and modify the root process group including adding/removing processors to the canvas. This policy is inherited down the hierarchy unless there is a more specific policy on a component.	/process-groups
Tenants	Allows users to view and modify user accounts and user groups.	/tenants

Pre-defined Ranger access policies for Apache NiFi Registry

Based on a user's responsibilities, you can add users to one or more of the following Ranger access policies. When you create a custom policy, use the resource descriptor in the NiFi Registry Resource Identifier field.

The following table lists the pre-defined Ranger access policies for NiFi Registry:

Ranger Policy	Description	Resource Descriptor
Actuator	Allows users to access the Spring Boot Actuator end-points.	/actuator
Buckets	Allows users to view and modify all buckets.	/buckets
Policies	Allows users to view the policies for all components.	/policies
Proxies	Allows proxy machines to send requests on behalf of others.	/proxy
Swagger	Allows users to access the self-hosted Swagger UI.	/swagger
Tenants	Allows users to view and modify user accounts and user groups.	/tenants