CDP Data Center 7.1.1

Schema Registry Authorization

Date published: 2020-06-12
Date modified: 2020-06-12

CLOUDERA

Legal Notice

Contents

Schema Registry Authorization through Ranger Access Policies

User and group access to various Schema Registry functions is controlled through Apache Ranger.

Pre-defined access policies for Schema Registry allow the administrator to quickly add a user or user group to specify:

- Who can add/evolve schemas to a schema metadata.
- Who can view and edit schemas within a schema metadata.
- Who can upload the ser/des jar files.

If a higher level of granularity is necessary, the administrator can create an access policy and add the user or user-group to this custom policy.

Related Information

Pre-defined Access Policies for Schema Registry

Add the user or group to a pre-defined access policy

Create a Custom Access Policy

Pre-defined Access Policies for Schema Registry

Based on a user's responsibilities, you can add users or a user group to one or more of the following pre-defined access policies for Schema Registry and you can specify the type of permission such as Create, Read, Update, and Delete.

The following image shows the pre-defined access policies for Schema Registry:

The following table describes the pre-defined access policies for Schema Registry:

Access Policy	Description
all - serde	Allows users to store metadata for the format of how data should be read and how it should be written. Users can store JAR files for serializers and deserializers and then map the serdes to the schema.
all - schema-group, schema-metadata	Allows users to access the schema groups and schema metadata.
all - schema-group, schema-metadata, schema-branch	Allows users to access the schema groups, schema metadata, and schema branch.
all - registry-service	Allows users to access the schema registry service. If a user is added to this policy, the user can access all Schema Registry entities.
all - schema-group, schema-metadata, schema-branch, schema-version	Allows users to access the schema groups, schema metadata, schema branch, and schema version.

Add the user or group to a pre-defined access policy

When an authenticated user attempts to view, create, edit, or delete a Schema Registry entity, 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 the permissions required by a user or user group and accordingly add the user or group to the appropriate pre-defined access policy.

Each pre-defined access policy controls access to one or more Schema Registry entities.

Procedure

1. From the Cloudera Manager home page, click the Ranger link.
   The **Ranger** management page appears.
2. Click the Ranger Admin Web UI link.

   The **Ranger Log In** page appears.
3. Enter your user name and password to log in.
   The **Ranger Service Manager** page appears.

   The page is organized by service. Each cluster is listed under its respective service. For example, the Schema Registry clusters in the environment are listed under Schema Registry.

4. Select a cluster from the Schema Registry section.
The **List of Policies** page appears.

5. Click the ID for a policy.
The **Edit Policy** page appears.

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

7. From the Policy Conditions field, enter the appropriate IP address.

8. From the Permissions field, select the appropriate permission.

9. Click Save.

Results

The user now has the rights according to the policy and the permission you assigned to the user. These rights apply to all objects in the entities unless you specified otherwise in the Policy Conditions field.

Related Information

Schema Registry Authorization through Ranger Access Policies

Pre-defined Access Policies for Schema Registry

Create a Custom Access Policy

Create a Custom Access Policy

You can create a custom access policy for a specific Schema Registry entity, specify an access type, and add a user or user-group to the policy.

Before you begin

Determine the following information:

- The schema registry entity that the user needs access to.
- Whether the user requires all objects in the entity or specific objects.
- Whether the user needs read, view, edit, or delete permissions to the entity.
- If there are any IP addresses to include or exclude from the user's access.

About this task

With a custom policy you can specify the Schema Registry entity and the type of access the user requires.

Procedure

1. Go to the **Ranger List of Policies** page.
2. Click Add New Policy.
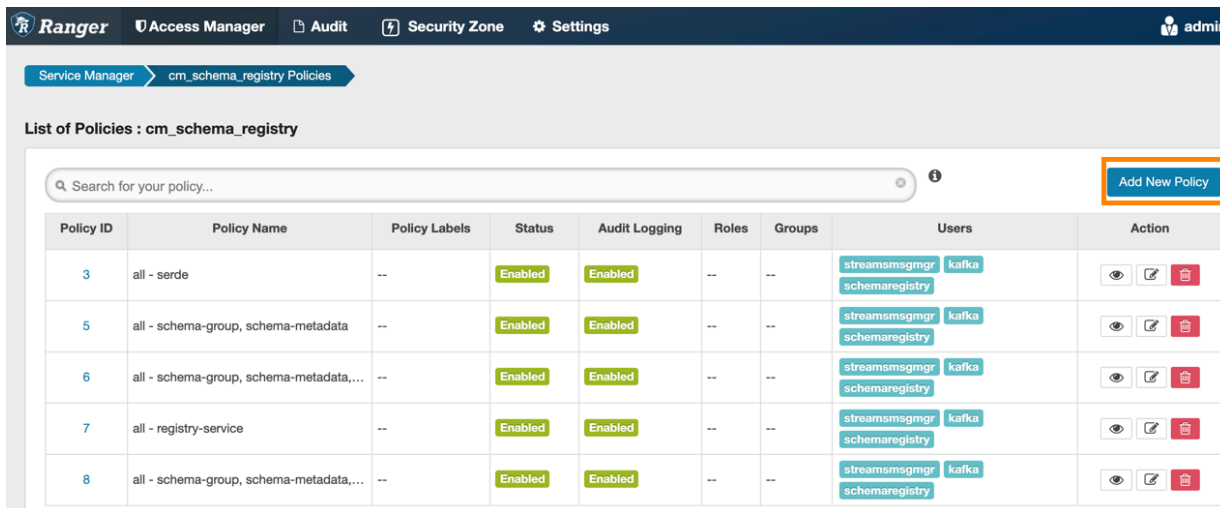
The **Create Policy** page appears.

3. Enter a unique name for the policy.
4. Optionally, enter a keyword in the Policy Label field to aid in searching for a policy.
5. Select a Schema Registry entity. You can choose the Schema Registry service, schema group, or serde. Then, do one of the following tasks:

   • If you want the user to access all the objects in the entity, enter *.
   • If you want to specify the objects in the entity that a user can access, enter the name of the object in the text field.

6. Optionally, enter a description.
7. In the Allow Conditions section, add the user or group to the respective Select User or Select Group field.
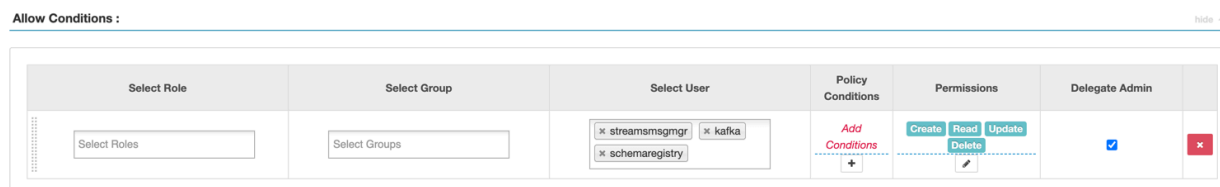
8. Optionally, from the Policy Conditions field, enter the appropriate IP address.
9. From the Permissions field, select the appropriate permission.
10. Click Save.

Results

The user now has the rights according to the policy and the permission you assigned to the user.

Related Information

Schema Registry Authorization through Ranger Access Policies

Pre-defined Access Policies for Schema Registry

Add the user or group to a pre-defined access policy