Cost Management Service 2021

Limiting access to cost management resources

Learn how to secure your cost information
Cost Management Service 2021 Limiting access to cost management resources

Learn how to secure your cost information
Abstract

You may not want users to have access to all cost data, but instead only data specific to their projects or organization.
# Table of Contents

CHAPTER 1. LIMITING ACCESS TO COST MANAGEMENT RESOURCES  ........................................ 3
  1.1. DEFAULT USER ROLES IN COST MANAGEMENT .............................................. 3
  1.2. ADDING A ROLE ......................................................................................... 3
  1.3. ADDING A ROLE TO A GROUP ................................................................. 5
CHAPTER 1. LIMITING ACCESS TO COST MANAGEMENT RESOURCES

You may not want users to have access to all cost data, but instead only data specific to their projects or organization. Using role-based access control, you can limit the visibility of resources involved in cost management reports. For example, you may want to restrict a user’s view to only AWS sources, instead of the entire environment.

Role-based access control works by organizing users into groups, which can be associated with one or more roles. A role defines a permission and a set of resource definitions.

By default, a user who is not an account administrator will not have access to data, but instead must be granted access to resources. Account administrators can view all data without any further role-based access control configuration.

NOTE

A Red Hat account user with Organization Administrator entitlements is required to configure Red Hat account users. This Red Hat login allows you to look up users, add them to groups, and to assign roles that control visibility to resources.

For more information about Red Hat account roles, see Roles and Permissions for Red Hat Subscription Management and How To Create and Manage Users.

1.1. DEFAULT USER ROLES IN COST MANAGEMENT

You can configure custom user access roles for cost management, or assign each user a predefined role.

To use a default role, determine the required level of access to permit your users based on the following predefined roles in cost management:

**Administrator roles**

- Cost Administrator: has read and write permissions to all resources in cost management
- Cost Price List Administrator: has read and write permissions on price list rates

**Viewer roles**

- Cost Cloud Viewer: has read permissions on cost reports related to cloud sources
- Cost OpenShift Viewer: has read permissions on cost reports related to OpenShift sources
- Cost Price List Viewer: has read permissions on price list rates

1.2. ADDING A ROLE

Create a new role to manage and limit the scope of information that users can see within cost management.

Prerequisites
You must be an Account Administrator or a member of a group with the RBAC Administrator role to create a role.

Procedure

1. From cost management, click (Settings) to navigate to User Access.

2. Click the Roles tab.

3. Click Create Role to open the Add role wizard.

4. In the Name and Description screen, enter a name for the new role, and optionally, a description. Click Next.

5. In the Permission screen, specify the Red Hat Cloud Services application you are creating the role for (in this case, cost management) as well as the resource and permission type:
   a. For Application, enter cost-management.
   b. For Resource type, specify the resource this permission will be used to access from the following list:
      - aws.account
      - aws.organizational_unit
      - azure.subscription_guid
      - openshift.cluster
      - openshift.node
      - openshift.project
   
   **NOTE**
   When you add an AWS organizational unit as a Resource Type, any user who has access to the parent node also has access to all children and sub-children of the parent node.
   c. For Permission, specify read as all cost resource data is read-only.
      For example, to create a role with read-only permissions to AWS account data, set aws.account as the Resource type and read as the Permission. In the next step, you can specify the AWS account to apply this role to.

6. In the Resource definitions screen, you can provide more details about the resources the permission will be used for. For example, to grant this role access to a specific AWS account, enter the following and click Add to definitions:
   - **Key**: aws.account
     - Options for Key are: aws.account, aws.organizational_unit, azure.subscription_guid, openshift.cluster, openshift.node, openshift.project
   - **Operation**: equal
     - Use equal if you know the exact value, or list to see a list of values that will work for this role.
• **Value:** Your AWS account number or account alias.
  
  - This is specific to the resource defined in the **Key** field. Examples include the AWS account ID or alias, AWS organizational unit, Azure subscription ID, OpenShift cluster ID, OpenShift node name, or OpenShift project name.
  
  You can also enter * in this field as a wildcard to create a role that matches everything of the resource type defined in **Key**.

7. Add more resource definitions if desired and click **Next** when finished.

8. Review the details for this role and click **Confirm** to create the role.

Your new role will be listed in the **Roles** tab on the **User Access Management** screen.

**Next steps**

- Add this role to a group to provide the role with access to resources.

### 1.3. ADDING A ROLE TO A GROUP

Add your role to a group to manage and limit the scope of information that users in that group can see within cost management.

**Prerequisites**

- You must be an Account Administrator or a member of a group with the **RBAC Administrator** role to create a role.

**Procedure**

1. From cost management, click **(Settings)** to navigate to **User Access**.

2. Click the **Groups** tab.

3. Click **Create group**.

4. In the **General information** screen, enter a name for the new group, and optionally, a description. Click **Next**.

5. In the **Add members** screen, select the user(s) in your organization to add to the new group. Click **Next**.

6. (Optional) In the **Select roles** screen, select one or more role(s) to add to the group. Default roles available for cost management are:

   - **Cost Administrator**: grants read and write permissions
   - **Cost Cloud Viewer**: grants read permissions on cost reports related to cloud sources
   - **Cost OpenShift Viewer**: grants read permissions on cost reports related to OpenShift sources
   - **Cost Price List Administrator**: grants read and write permissions on price list rates

7. Review the details for this group and click **Confirm** to create the group.
Your new group will be listed in the **Groups** list on the **User Access** screen.

To verify your configuration, log out of the cost management application and log back in as a user added to the group.