Red Hat Advanced Cluster Management for Kubernetes 2.10

Access control

Access control
Red Hat Advanced Cluster Management for Kubernetes 2.10 Access control

Access control
Abstract

Ensure users have access to resources that are required to perform specific roles.
# Table of Contents

**CHAPTER 1. ACCESS CONTROL**  
1.1. ROLE-BASED ACCESS CONTROL  
1.1.1. Overview of roles  
3  
1.2. IMPLEMENTING ROLE-BASED ACCESS CONTROL  
1.2.1. Application lifecycle RBAC  
1.2.1.1. Console and API RBAC table for application lifecycle  
7  
1.2.2. Governance lifecycle RBAC  
1.2.2.1. Console and API RBAC table for governance lifecycle  
9  
1.2.3. Observability RBAC  
1.2.3.1. Console and API RBAC table for observability lifecycle  
11
CHAPTER 1. ACCESS CONTROL

Access control might need to manually be created and managed. You must configure **authentication** service requirements for Red Hat Advanced Cluster Management for Kubernetes to onboard workloads to Identity and Access Management (IAM). For more information see, *Understanding authentication* in the OpenShift Container Platform documentation.

Role-based access control and authentication identifies the user associated roles and cluster credentials. See the following documentation for information about access and credentials.

**Required access:** Cluster administrator

- Role-based access control
- Implementing role-based access control

1.1. ROLE-BASED ACCESS CONTROL

Red Hat Advanced Cluster Management for Kubernetes supports role-based access control (RBAC). Your role determines the actions that you can perform. RBAC is based on the authorization mechanisms in Kubernetes, similar to Red Hat OpenShift Container Platform. For more information about RBAC, see the OpenShift RBAC overview in the OpenShift Container Platform documentation.

**Note:** Action buttons are disabled from the console if the user-role access is impermissible.

1.1.1. Overview of roles

Some product resources are cluster-wide and some are namespace-scoped. You must apply cluster role bindings and namespace role bindings to your users for consistent access controls. View the table list of the following role definitions that are supported in Red Hat Advanced Cluster Management for Kubernetes:

<table>
<thead>
<tr>
<th>Role</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cluster-admin</strong></td>
<td>This is an OpenShift Container Platform default role. A user with cluster binding to the <code>cluster-admin</code> role is an OpenShift Container Platform super user, who has all access.</td>
</tr>
<tr>
<td><strong>open-cluster-management:cluster-manager-admin</strong></td>
<td>A user with cluster binding to the <code>open-cluster-management:cluster-manager-admin</code> role is a Red Hat Advanced Cluster Management for Kubernetes super user, who has all access. This role allows the user to create a ManagedCluster resource.</td>
</tr>
<tr>
<td>Role Description</td>
<td>Role Details</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| `open-cluster-management:admin:`<managed_cluster_name>` | A user with cluster binding to the `open-cluster-management:admin:`<managed_cluster_name>` role has administrator access to the ManagedCluster resource named, `<managed_cluster_name>`.

When a user has a managed cluster, this role is automatically created. |
| `open-cluster-management:view:`<managed_cluster_name>` | A user with cluster binding to the `open-cluster-management:view:`<managed_cluster_name>` role has view access to the ManagedCluster resource named, `<managed_cluster_name>`.
| `open-cluster-management:managedclusterset:admin:`<managed_clusterset_name>` | A user with cluster binding to the `open-cluster-management:managedclusterset:admin:`<managed_clusterset_name>` role has administrator access to ManagedCluster resource named `<managed_clusterset_name>`.

The user also has administrator access to `managedcluster.cluster.open-cluster-management.io`, `clusterclaim.hive.openshift.io`, `clusterdeployment.hive.openshift.io`, and `clusterpool.hive.openshift.io` resources, which has the managed cluster set label: `cluster.open-cluster-management.io/clusterset=<managed_clusterset_name>`. A role binding is automatically generated when you are using a cluster set. See Creating a ManagedClusterSet to learn how to manage the resource. |
| `open-cluster-management:managedclusterset:view:`<managed_clusterset_name>` | A user with cluster binding to the `open-cluster-management:managedclusterset:view:`<managed_clusterset_name>` role has view access to the ManagedCluster resource named, `<managed_clusterset_name>`.

The user also has view access to `managedcluster.cluster.open-cluster-management.io`, `clusterclaim.hive.openshift.io`, `clusterdeployment.hive.openshift.io`, and `clusterpool.hive.openshift.io` resources, which has the managed cluster set labels: `cluster.open-cluster-management.io clusterset=<managed_clusterset_name>`. For more details on how to manage managed cluster set resources, see Creating a ManagedClusterSet. |
<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>open-cluster-management:subscription-admin</code></td>
<td>A user with the <code>open-cluster-management:subscription-admin</code> role can create Git subscriptions that deploy resources to multiple namespaces. The resources are specified in Kubernetes resource YAML files in the subscribed Git repository. <strong>Note:</strong> When a non-subscription-admin user creates a subscription, all resources are deployed into the subscription namespace regardless of specified namespaces in the resources. For more information, see the Application lifecycle RBAC section.</td>
</tr>
<tr>
<td><code>admin, edit, view</code></td>
<td>Admin, edit, and view are OpenShift Container Platform default roles. A user with a namespace-scoped binding to these roles has access to <code>open-cluster-management</code> resources in a specific namespace, while cluster-wide binding to the same roles gives access to all of the <code>open-cluster-management</code> resources cluster-wide.</td>
</tr>
<tr>
<td><code>open-cluster-management:managedclusterset:bind:</code> <code>&lt;managed_clusterset_name&gt;</code></td>
<td>A user with the <code>open-cluster-management:managedclusterset:bind:</code> <code>&lt;managed_clusterset_name&gt;</code> role has view access to the managed cluster resource called <code>&lt;managed_clusterset_name&gt;</code>. The user can bind <code>&lt;managed_clusterset_name&gt;</code> to a namespace. The user also has view access to <code>managedcluster.cluster.open-cluster-management.io</code>, <code>clusterclaim.hive.openshift.io</code>, <code>clusterdeployment.hive.openshift.io</code>, and <code>clusterpool.hive.openshift.io</code> resources, which have the following managed cluster set label: <code>cluster.open-cluster-management.io/clusterset=</code> <code>&lt;managed_clusterset_name&gt;</code>. See Creating a ManagedClusterSet to learn how to manage the resource.</td>
</tr>
</tbody>
</table>

**Important:**

- Any user can create projects from OpenShift Container Platform, which gives administrator role permissions for the namespace.
- If a user does not have role access to a cluster, the cluster name is not displayed. The cluster name might be displayed with the following symbol: `•`.

See Implementing role-based access control for more details.

### 1.2. IMPLEMENTING ROLE-BASED ACCESS CONTROL

Red Hat Advanced Cluster Management for Kubernetes RBAC is validated at the console level and at the API level. Actions in the console can be enabled or disabled based on user access role permissions.
The multicluster engine operator is a prerequisite and the cluster lifecycle function of Red Hat Advanced Cluster Management. To manage RBAC for clusters with the multicluster engine operator, use the RBAC guidance from the cluster lifecycle multicluster engine for Kubernetes operator Role-based access control documentation.

View the following sections for more information on RBAC for specific lifecycles for Red Hat Advanced Cluster Management:

- Application lifecycle RBAC
  - Console and API RBAC table for application lifecycle
- Governance lifecycle RBAC
  - Console and API RBAC table for governance lifecycle
- Observability RBAC
  - Console and API RBAC table for observability lifecycle

1.2.1. Application lifecycle RBAC

When you create an application, the subscription namespace is created and the configuration map is created in the subscription namespace. You must also have access to the channel namespace. When you want to apply a subscription, you must be a subscription administrator. For more information on managing applications, see Creating an allow and deny list as subscription administrator.

View the following application lifecycle RBAC operations:

- Create and administer applications on all managed clusters with a user named username. You must create a cluster role binding and bind it to username. Run the following command:

  ```
  oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:cluster-manager-admin --user=<username>
  ```

  This role is a super user, which has access to all resources and actions. You can create the namespace for the application and all application resources in the namespace with this role.

- Create applications that deploy resources to multiple namespaces. You must create a cluster role binding to the open-cluster-management:subscription-admin cluster role, and bind it to a user named username. Run the following command:

  ```
  oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:subscription-admin --user=<username>
  ```

- Create and administer applications in the cluster-name managed cluster, with the username user. You must create a cluster role binding to the open-cluster-management:admin:cluster-name cluster role and bind it to username by entering the following command:

  ```
  oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:admin:cluster-name --user=<username>
  ```

  This role has read and write access to all application resources on the managed cluster, cluster-name. Repeat this if access for other managed clusters is required.
- Create a namespace role binding to the **application** namespace using the **admin** role and bind it to **username** by entering the following command:

  ```oc create rolebinding <role-binding-name> -n <application-namespace> --clusterrole=admin --user=<username>```

  This role has read and write access to all **application** resources in the **application** namespace. Repeat this if access for other applications is required or if the application deploys to multiple namespaces.

- You can create applications that deploy resources to multiple namespaces. Create a cluster role binding to the **open-cluster-management:subscription-admin** cluster role and bind it to **username** by entering the following command:

  ```oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:subscription-admin --user=<username>```

- To view an application on a managed cluster named **cluster-name** with the user named **username**, create a cluster role binding to the **open-cluster-management:view** cluster role and bind it to **username**. Enter the following command:

  ```oc create clusterrolebinding <role-binding-name> --clusterrole=open-cluster-management:view:<cluster-name> --user=<username>```

  This role has read access to all **application** resources on the managed cluster, **cluster-name**. Repeat this if access for other managed clusters is required.

- Create a namespace role binding to the **application** namespace using the **view** role and bind it to **username**. Enter the following command:

  ```oc create rolebinding <role-binding-name> -n <application-namespace> --clusterrole=view --user=<username>```

  This role has read access to all **application** resources in the **application** namespace. Repeat this if access for other applications is required.

### 1.2.1.1. Console and API RBAC table for application lifecycle

View the following console and API RBAC tables for Application lifecycle:

#### Table 1.2. Console RBAC table for application lifecycle

<table>
<thead>
<tr>
<th>Resource</th>
<th>Admin</th>
<th>Edit</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>Channel</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>Subscription</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
</tbody>
</table>
Table 1.3. API RBAC table for application lifecycle

<table>
<thead>
<tr>
<th>API</th>
<th>Admin</th>
<th>Edit</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>applications.app.k8s.io</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>channels.apps.open-cluster-management.io</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>deployables.apps.open-cluster-management.io</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>helmreleases.apps.open-cluster-management.io</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>placements.apps.open-cluster-management.io</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>placementrules.apps.open-cluster-management.io (Deprecated)</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>subscriptions.apps.open-cluster-management.io</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>configmaps</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>secrets</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
<tr>
<td>namespaces</td>
<td>create, read, update, delete</td>
<td>create, read, update, delete</td>
<td>read</td>
</tr>
</tbody>
</table>

1.2.2. Governance lifecycle RBAC

To perform governance lifecycle operations, you need access to the namespace where the policy is created, along with access to the managed cluster where the policy is applied. The managed cluster must also be part of a ManagedClusterSet that is bound to the namespace. To continue to learn about ManagedClusterSet, see ManagedClusterSets Introduction.

After you select a namespace, such as rhacm-policies, with one or more bound ManagedClusterSets, and after you have access to create Placement objects in the namespace, view the following operations:
To create a **ClusterRole** named `rhacm-edit-policy` with **Policy**, **PlacementBinding**, and **PolicyAutomation** edit access, run the following command:

```
oc create clusterrole rhacm-edit-policy --resource=policies.policy.open-cluster-management.io,placementbindings.policy.open-cluster-management.io,policyautomations.policy.open-cluster-management.io,policysets.policy.open-cluster-management.io --verb=create,delete,get,list,patch,update,watch
```

To create a policy in the `rhacm-policies` namespace, create a namespace **RoleBinding**, such as `rhacm-edit-policy`, to the `rhacm-policies` namespace using the **ClusterRole** created previously. Run the following command:

```
oc create rolebinding rhacm-edit-policy -n rhacm-policies --clusterrole=rhacm-edit-policy --user=<username>
```

To view policy status of a managed cluster, you need permission to view policies in the managed cluster namespace on the hub cluster. If you do not have **view** access, such as through the OpenShift **view ClusterRole**, create a **ClusterRole**, such as `rhacm-view-policy`, with **view** access to policies with the following command:

```
oc create clusterrole rhacm-view-policy --resource=policies.policy.open-cluster-management.io --verb=get,list,watch
```

To bind the new **ClusterRole** to the managed cluster namespace, run the following command to create a namespace **RoleBinding**:

```
oc create rolebinding rhacm-view-policy -n <cluster name> --clusterrole=rhacm-view-policy --user=<username>
```

### 1.2.2.1. Console and API RBAC table for governance lifecycle

View the following console and API RBAC tables for governance lifecycle:

**Table 1.4. Console RBAC table for governance lifecycle**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Admin</th>
<th>Edit</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>create, read, update, delete</td>
<td>read, update</td>
<td>read</td>
</tr>
<tr>
<td>PlacementBindings</td>
<td>create, read, update, delete</td>
<td>read, update</td>
<td>read</td>
</tr>
<tr>
<td>Placements</td>
<td>create, read, update, delete</td>
<td>read, update</td>
<td>read</td>
</tr>
<tr>
<td>PlacementRules (deprecated)</td>
<td>create, read, update, delete</td>
<td>read, update</td>
<td>read</td>
</tr>
<tr>
<td>PolicyAutomations</td>
<td>create, read, update, delete</td>
<td>read, update</td>
<td>read</td>
</tr>
</tbody>
</table>
Table 1.5. API RBAC table for governance lifecycle

<table>
<thead>
<tr>
<th>API</th>
<th>Admin</th>
<th>Edit</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policies.policy.open-cluster-management.io</code></td>
<td>create, read, update, delete</td>
<td>read, update</td>
<td>read</td>
</tr>
<tr>
<td><code>placementbindings.policy.open-cluster-management.io</code></td>
<td>create, read, update, delete</td>
<td>read, update</td>
<td>read</td>
</tr>
<tr>
<td><code>policyautomations.policy.open-cluster-management.io</code></td>
<td>create, read, update, delete</td>
<td>read, update</td>
<td>read</td>
</tr>
</tbody>
</table>

1.2.3. Observability RBAC

To view the observability metrics for a managed cluster, you must have `view` access to that managed cluster on the hub cluster. View the following list of observability features:

- **Access managed cluster metrics.**
  Users are denied access to managed cluster metrics, if they are not assigned to the `view` role for the managed cluster on the hub cluster. Run the following command to verify if a user has the authority to create a `managedClusterView` role in the managed cluster namespace:

  ```bash
  oc auth can-i create ManagedClusterView -n <managedClusterName> --as=<user>
  ```

  As a cluster administrator, create a `managedClusterView` role in the managed cluster namespace. Run the following command:

  ```bash
  oc create role create-managedclusterview --verb=create --resource=managedclusterviews -n <managedClusterName>
  ```

  Then apply and bind the role to a user by creating a role bind. Run the following command:

  ```bash
  oc create rolebinding user-create-managedclusterview-binding --role=create-managedclusterview --user=<user> -n <managedClusterName>
  ```

- **Search for resources.**
  To verify if a user has access to resource types, use the following command:

  ```bash
  oc auth can-i list <resource-type> -n <namespace> --as=<rbac-user>
  ```

  **Note:** `<resource-type>` must be plural.
To view observability data in Grafana, you must have a **RoleBinding** resource in the same namespace of the managed cluster. View the following **RoleBinding** example:

```yaml
kind: RoleBinding
apiversion: rbac.authorization.k8s.io/v1
metadata:
  name: <replace-with-name-of-rolebinding>
  namespace: <replace-with-name-of-managedcluster-namespace>
subjects:
  - kind: <replace with User|Group|ServiceAccount>
    apiGroup: rbac.authorization.k8s.io
    name: <replace with name of User|Group|ServiceAccount>
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: view
```

See [Role binding policy](#) for more information. See [Customizing observability](#) to configure observability.

### 1.2.3.1. Console and API RBAC table for observability lifecycle

To manage components of observability, view the following API RBAC table:

**Table 1.6. API RBAC table for observability**

<table>
<thead>
<tr>
<th>API</th>
<th>Admin</th>
<th>Edit</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>multiclusterobservabilities.observability.open-cluster-management.io</code></td>
<td>create, read, update, and delete</td>
<td>read, update</td>
<td>read</td>
</tr>
<tr>
<td><code>searchcustomization.s.search.open-cluster-management.io</code></td>
<td>create, get, list, watch, update, delete, patch</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><code>policyreports.wgpolicy.k8s.io</code></td>
<td>get, list, watch</td>
<td>get, list, watch</td>
<td>get, list, watch</td>
</tr>
</tbody>
</table>

Continue to learn about securing your cluster, see [Risk and compliance](#).