Red Hat Advanced Cluster Management for Kubernetes 2.10

Access control

Access control

Last Updated: 2024-07-01

Red Hat Advanced Cluster Management for Kubernetes 2.10 Access control

Access control

法律通告

摘要

确保用户可以访问执行特定角色所需的资源。

目录

第 1 章 ACCESS CONTROL

可能需要手动创建和管理访问控制。您必须为 Red Hat Advanced Cluster Management for Kubernetes 配置*身份验证（authentication）*服务，以便将工作负载加载到 Identity and Access Management（IAM）。如需更多信息，请参阅 OpenShift Container Platform 文档中的了解身份验证中的*身份验证*。

基于角色的访问控制和身份验证用于标识用户关联的角色和集群凭据。有关访问和凭证的详情，请查看以下文档。

需要的访问权限：集群管理员

- 基于角色的访问控制
- 实施基于角色的访问控制

1.1. 基于角色的访问控制

Red Hat Advanced Cluster Management for Kubernetes 支持的基于角色的控制访问（RBAC）。您的角色决定了您可以执行的操作。RBAC 基于 Kubernetes 中的授权机制，类似于 Red Hat OpenShift Container Platform。如需有关 RBAC 的更多信息，请参阅 OpenShift Container Platform 文档中的 OpenShift *RBAC* 概述。

备注: 如果用户角色访问不可用，则控制台中的 Action 按钮会被禁用。

1.1.1. 角色概述

有些产品资源是基于集群范围的，有些则是命名空间范围。您必须将集群角色绑定和命名空间角色绑定应用到用户，以使访问控制具有一致性。查看 Red Hat Advanced Cluster Management for Kubernetes 支持的以下角色定义表列表：

表 1.1. 角色定义表

角色	定义
cluster-admin	这是 OpenShift Container Platform 的默认角色。具有集群范围内的绑定到 **cluster-admin** 角色的用户，是一个 OpenShift Container Platform 超级用户，其具有所有访问权限。
open-cluster-management:cluster-manager-admin	具有集群范围内的绑定到 **open-cluster-management:cluster-manager-admin** 角色的用户，是一个 Red Hat Advanced Cluster Management for Kubernetes 超级用户，其具有所有访问权限。此角色允许用户创建 **ManagedCluster** 资源。
open-cluster-management:admin:<managed_cluster_name>	具有集群范围内的绑定到 **open-cluster-management:admin:<managed_cluster_name>** 角色的用户，具有对名为 **<managed_cluster_name>** 的 **ManagedCluster** 资源的管理员访问权限。当用户具有受管集群时，会自动创建此角色。

open-cluster-management:view:<managed_cluster_name>	具有集群范围内的绑定到 **open-cluster-management:view:<managed_cluster_name>** 角色的用户，可以访问名为 **<managed_cluster_name>** 的 **ManagedCluster** 资源。
open-cluster-management:managedclusterset:admin:<managed_clusterset_name>	具有集群范围内的绑定到 **open-cluster-management:managedclusterset:admin:<managed_clusterset_name>** 角色的用户，具有对名为 **<managed_clusterset_name>** 的 **ManagedCluster** 资源的管理员访问权限。用户还有对 **managedcluster.cluster.open-cluster-management.io**、**clusterclaim.hive.openshift.io**、**clusterdeployment.hive.openshift.io** 和 **clusterpool.hive.openshift.io** 资源的管理员访问权限，这些资源具有受管集群集标签：**cluster.open-cluster-management.io/clusterset=<managed_clusterset_name>**。使用集群集时会自动生成角色绑定。请参阅创建 *ManagedClusterSet* 以了解如何管理该资源。
open-cluster-management:managedclusterset:view:<managed_clusterset_name>	具有集群范围内的绑定到 **open-cluster-management:managedclusterset:view:<managed_clusterset_name>** 角色的用户，可以访问名为 <managed_clusterset_name>' 的 **ManagedCluster** 资源。用户还有对 **managedcluster.cluster.open-cluster-management.io**、**clusterclaim.hive.openshift.io**、**clusterdeployment.hive.openshift.io** 和 **clusterpool.hive.openshift.io** 资源的查看访问权限，这些资源具有受管集群集标签：**cluster.open-cluster-management.io,clusterset=<managed_clusterset_name>**。有关如何管理受管集群设置资源的详情，请参阅创建 *ManagedClusterSet*。
open-cluster-management:subscription-admin	具有 **open-cluster-management:subscription-admin** 角色的用户，可以创建 Git 订阅将资源部署到多个命名空间中。资源在订阅的 Git 仓库中的 Kubernetes 资源 YAML 文件中指定。**备注**：当一个非 subscription-admin 用户创建订阅时，无论资源中的指定命名空间是什么，所有资源都会部署到订阅命名空间中。如需更多信息，请参阅应用程序生命周期 RBAC 部分。

admin, edit, view	admin、edit 和 view 是 OpenShift Container Platform 的默认角色。具有命名空间范围绑定的用户可以访问特定命名空间中的 **open-cluster-management** 资源，而集群范围的绑定到同一角色可以访问整个集群范围的 **open-cluster-management** 资源。
open-cluster-management:managedclusterset:bind:<managed_clusterset_name>	带有 **open-cluster-management:managedclusterset:bind:<managed_clusterset_name>** 角色的用户具有可以查看被称为 **<managed_clusterset_name>** 的受管集群资源的权限。用户可以将 **<managed_clusterset_name>** 绑定到一个命名空间。用户还有对 **managedcluster.cluster.open-cluster-management.io**、**clusterclaim.hive.openshift.io**、**clusterdeployment.hive.openshift.io** 和 **clusterpool.hive.openshift.io** 资源的查看访问权限，这些资源具有以下受管集群集标签：**cluster.open-cluster-management.io/clusterset=<managed_clusterset_name>**。请参阅*创建 ManagedClusterSet* 以了解如何管理该资源。

重要：

- 任何用户都可以从 OpenShift Container Platform 创建项目，这为命名空间授予管理员角色权限。
- 如果用户无法访问集群的角色，则不会显示集群名称。集群名称可能显示有以下符号： **-**。

如需了解更多详细信息，请参阅实现基于角色的访问控制。

1.2. 实施基于角色的访问控制

Red Hat Advanced Cluster Management for Kubernetes RBAC 在控制台级别和 API 级别进行验证。控制台中的操作可根据用户访问角色权限启用或禁用。

multicluster engine operator 是一个前提条件，Red Hat Advanced Cluster Management 的集群生命周期功能。要使用 multicluster engine operator 管理集群 RBAC，请参阅集群生命周期multicluster engine for Kubernetes operator Role-based access control 文档中的 RBAC 指导信息。

查看以下部分以了解有关 Red Hat Advanced Cluster Management 特定生命周期的 RBAC 的更多信息：

- 应用程序生命周期 RBAC
  - 应用程序生命周期的控制台和 API RBAC 表
- 监管生命周期 RBAC
  - 监管生命周期的控制台和 API RBAC 表
- Observability RBAC
  - Observability 生命周期的控制台和 API RBAC 表

1.2.1. 应用程序生命周期 RBAC

在创建应用程序时，***subscription*** 命名空间会被创建，配置映射会在 ***subscription*** 命名空间中创建。您还必须有权访问 ***channel*** 命名空间。如果需要应用订阅，则必须是订阅管理员。有关管理应用程序的更多信息，请参阅作为订阅管理员创建允许和拒绝列表。

查看以下应用程序生命周期 RBAC 操作：

- 使用名为 **username** 的用户在所有受管集群中创建和管理应用程序。您必须创建一个集群角色绑定，并将其绑定到 **username**。运行以下命令:

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

  这个角色是一个超级用户，可访问所有资源和操作。您可以使用此角色为应用程序和命名空间中的所有应用程序资源创建命名空间。

- 创建将资源部署到多个命名空间的应用程序。您必须创建一个集群角色绑定到 **open-cluster-management:subscription-admin** 集群角色，并将其绑定到名为 **username** 的用户。运行以下命令:

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

- 使用 **username** 用户在 **cluster-name** 受管集群中创建并管理应用程序。您必须输入以下命令创建一个到 **open-cluster-management:admin:<cluster-name>** 集群角色绑定的集群角色绑定，并将其绑定到 **username** ：

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

  此角色具有对受管集群 **cluster-name** 上所有 **application** 资源的读写访问权限。如果需要访问其他受管集群，请重复此操作。

- 输入以下命令，创建一个到使用 **admin** 角色的 **application** 命名空间的命名空间角色绑定，并把它绑定到 **username**：

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

  此角色具有对 **application** 命名空间中的所有 **application** 资源的读和写的访问权限。如果需要访问其他应用程序，或者应用部署到多个命名空间，请重复此操作。

- 您可以创建将资源部署到多个命名空间的应用程序。输入以下命令创建到 **open-cluster-management:subscription-admin** 集群角色的集群角色绑定，并将其绑定到 **username** ：

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

- 要使用名为 **username** 的用户查看在一个名为 **cluster-name** 的受管集群中的应用程序，请创建一个集群角色绑定到 **open-cluster-management:view:** 集群角色，并将其绑定到 **username**。输入以下命令：

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

-

此角色具有对受管集群 **cluster-name** 上所有 **application** 资源的读访问权限。如果需要访问其他受管集群，请重复此操作。

- 使用 **view** 角色创建到 **application** 命名空间的命名空间角色绑定，并将它绑定到 **username**。输入以下命令：

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

此角色具有对 **application** 命名空间中的 所有 **application** 资源的读访问权限。如果需要访问其他应用程序，请重复此操作。

1.2.1.1. 应用程序生命周期的控制台和 API RBAC 表

查看以下应用程序生命周期控制台和 API RBAC 表：

表 1.2. 应用程序生命周期的控制台 RBAC 表

资源	Admin	Edit	View
Application	创建、读取、更新、删除	创建、读取、更新、删除	读取
Channel	创建、读取、更新、删除	创建、读取、更新、删除	读取
Subscription	创建、读取、更新、删除	创建、读取、更新、删除	读取

表 1.3. 应用程序生命周期的 API RBAC 表

API	Admin	Edit	View
applications.app.k8s.io	创建、读取、更新、删除	创建、读取、更新、删除	读取
channels.apps.open-cluster-management.io	创建、读取、更新、删除	创建、读取、更新、删除	读取
deployables.apps.open-cluster-management.io	创建、读取、更新、删除	创建、读取、更新、删除	读取
helmreleases.apps.open-cluster-management.io	创建、读取、更新、删除	创建、读取、更新、删除	读取
placements.apps.open-cluster-management.io	创建、读取、更新、删除	创建、读取、更新、删除	读取

API	Admin	Edit	View
placementrules.apps.open-cluster-management.io （已弃用）	创建、读取、更新、删除	创建、读取、更新、删除	读取
subscriptions.apps.open-cluster-management.io	创建、读取、更新、删除	创建、读取、更新、删除	读取
configmaps	创建、读取、更新、删除	创建、读取、更新、删除	读取
secrets	创建、读取、更新、删除	创建、读取、更新、删除	读取
命名空间	创建、读取、更新、删除	创建、读取、更新、删除	读取

1.2.2. 监管生命周期 RBAC

要执行监管生命周期操作，您需要访问创建策略的命名空间，以及访问应用策略的受管集群。受管集群还必须是绑定到命名空间的 **ManagedClusterSet** 的一部分。要继续了解 **ManagedClusterSet**，请参阅 ManagedClusterSets Introduction。

选择命名空间后，如 **mvapich-policies**，带有一个或多个绑定的 **ManagedClusterSets**，并在命名空间中创建 **Placement** 对象后，查看以下操作：

- 要创建一个名为 mvapich **-edit-policy** 的 **ClusterRole**，以及 **Policy**、**PlacementBinding** 和 **PolicyAutomation** 编辑访问，请运行以下命令：

```
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
```

- 要在 mvapich **-policies** 命名空间中创建策略，请使用之前创建的 **ClusterRole** 创建一个命名空间 **RoleBinding**，如 mvapich **- edit-policy**。运行以下命令:

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

- 要查看受管集群的策略状态，您需要权限查看 hub 集群上的受管集群命名空间中的策略。如果您没有 查看 访问权限，如通过 OpenShift 视图 **ClusterRole**，使用以下命令创建一个 **ClusterRole**，如 **mvapich-view-policy**，并具有以下命令查看策略的访问权限：

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

- 要将新的 **ClusterRole** 绑定到受管集群命名空间，请运行以下命令来创建命名空间 **RoleBinding**：

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

1.2.2.1. 监管生命周期的控制台和 API RBAC 表

查看以下监管生命周期控制台和 API RBAC 表：

表 1.4. 监管生命周期的控制台 RBAC 表

资源	Admin	Edit	View
策略（policy）	创建、读取、更新、删除	读取、更新	读取
PlacementBindings	创建、读取、更新、删除	读取、更新	读取
放置	创建、读取、更新、删除	读取、更新	读取
PlacementRules (已弃用)	创建、读取、更新、删除	读取、更新	读取
PolicyAutomations	创建、读取、更新、删除	读取、更新	读取

表 1.5. 监管生命周期的 API RBAC 表

API	Admin	Edit	View
policies.policy.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取
placementbindings.policy.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取
policyautomations.policy.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取

1.2.3. Observability RBAC

要查看受管集群的可观察性指标，您必须具有对 hub 集群中该受管集群的 **view** 访问权限。查看以下可观察功能列表：

- 访问受管集群指标。
  如果没有将用户分配给 hub 集群上的受管集群的 **view** 角色，则拒绝用户访问受管集群的指标。运行以下命令，以验证用户是否有在受管集群命名空间中创建 **managedClusterView** 角色：

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

作为集群管理员，在受管集群命名空间中创建一个 **managedClusterView** 角色。运行以下命令:

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

然后，通过创建角色绑定来将角色应用到用户。运行以下命令:

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

- 搜索资源。
  要验证用户是否可以访问资源类型，请使用以下命令：

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

备注： <resource-type> 必须是复数。

- 要在 Grafana 中查看可观察性数据，则必须在受管集群相同的命名空间中有一个 **RoleBinding** 资源。
  查看以下 **RoleBinding** 示例：

```
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
```

如需更多信息，请参阅角色绑定策略。请参阅自定义可观察性以配置可观察性。

1.2.3.1. Observability 生命周期的控制台和 API RBAC 表

要管理可观察性组件，请查看以下 API RBAC 表：

表 1.6. 用于 observability 的 API RBAC 表

API	Admin	Edit	View
multiclusterobservabilities.observability.open-cluster-management.io	create、read、update 和 delete	读取、更新	读取

searchcustomizations.search.open-cluster-management.io	create, get, list, watch, update, delete, patch	-	-
policyreports.wgpolicyk8s.io	get、list、watch	get、list、watch	get、list、watch

要了解更多保护集群的信息，请参阅风险和合规性。