Red Hat Advanced Cluster Management for Kubernetes 2.3

访问控制

更多有关基于角色的访问控制和身份验证的信息。

Last Updated: 2023-02-24

Red Hat Advanced Cluster Management for Kubernetes 2.3 访问控制

更多有关基于角色的访问控制和身份验证的信息。

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Access_control.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

更多有关基于角色的访问控制和身份验证的信息。

目录

第 1 章 访问控制

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 文档中的身份验证中的 *了解身份验证*。

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。有关访问和凭据的详情，请查看以下文件。

需要的访问权限： 集群管理员

- 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。有关 RBAC 的更多信息，请参阅 OpenShift Container Platform 文档中的 *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。

如需组件支持的 RBAC 的详细信息，参阅以下小节。

- 角色概述
- RBAC 的实施
- 集群生命周期 RBAC
- 应用程序生命周期 RBAC
- 监管生命周期 RBAC
- Observability RBAC

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** 和 **clusterset=<managed_clusterset_name>**。使用集群集时会自动生成角色绑定。请参阅创建和管理 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>**。如需有关如何管理受管集群设置资源的更多详细信息，请参阅创建和管理 ManagedClusterSets。

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。**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。

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，则无法看到集群名称。集群名称显示有以下符号： **-**。

1.1.2. RBAC 的实施

RBAC 在控制台和 API 一级进行验证。控制台中的操作可根据用户访问角色权限启用或禁用。查看以下部分以了解有关产品中特定生命周期的 RBAC 的更多信息。

1.1.2.1. 集群生命周期 RBAC

查看以下集群生命周期 RBAC 操作。

- 创建和管理所有受管集群：
  - 输入以下命令，创建到集群角色 **open-cluster-management:cluster-manager-admin** 的集群角色绑定：

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

    这个角色是一个超级用户，可访问所有资源和操作。您可以创建集群范围的 **managedcluster** 资源、用于管理受管集群的资源的命名空间，以及使用此角色的命名空间中的资源。您还可以访问用于创建具有此角色的受管集群的供应商连接和裸机资产。

- 管理名为 **cluster-name** 的受管集群：
  - 输入以下命令，创建到集群角色 **open-cluster-management:admin:<cluster-name>** 的集群角色绑定：

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

此角色对集群范围的 **managedcluster** 资源具有读写访问权限。这是必要的，因为 **managedcluster** 是一个集群范围的资源，而不是命名空间范围的资源。

- 输入以下命令，创建到集群角色 **admin** 的命名空间角色绑定：

```
oc create rolebinding <role-binding-name> -n <cluster-name> --clusterrole=admin
```

此角色对受管集群命名空间中的资源具有读写访问权限。

- 查看名为 **cluster-name** 的受管集群：
  - 输入以下命令，创建到集群角色 **open-cluster-management:view:<cluster-name>** 的集群角色绑定：

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

此角色具有对集群范围的 **managedcluster** 资源的读取访问权限。这是必要的，因为 **managedcluster** 是一个集群范围的资源，而不是命名空间范围的资源。

  - 输入以下命令，创建到集群角色 **view** 的命名空间角色绑定：

```
oc create rolebinding <role-binding-name> -n <cluster-name> --clusterrole=view
```

此角色对受管集群命名空间中的资源具有只读访问权限。

- 输入以下命令来查看您可以访问的受管集群列表：

```
oc get managedclusters.clusterview.open-cluster-management.io
```

此命令供没有集群管理员特权的管理员和用户使用。

- 输入以下命令来查看您可以访问的受管集群集列表：

```
oc get managedclustersets.clusterview.open-cluster-management.io
```

此命令供没有集群管理员特权的管理员和用户使用。

1.1.2.1.1. 集群池 RBAC

查看以下集群池 RBAC 操作。

- 使用集群池置备集群：
  - 以集群管理员身份，通过将角色添加到组来创建受管集群集，并将管理员权限授予角色。
    - 使用以下命令为 **server-foundation-clusterset** 受管集群集授予 **admin** 权限：

```
oc adm policy add-cluster-role-to-group open-cluster-management:clusterset-admin:server-foundation-clusterset
server-foundation-team-admin
```

    - 使用以下命令为 **server-foundation-clusterset** 受管集群授予 **view** 权限：

```
oc adm policy add-cluster-role-to-group open-cluster-management:clusterset-view:server-foundation-clusterset server-foundation-team-user
```

- 为集群池 **server-foundation-clusterpool** 创建命名空间。
  - 运行以下命令，为 **server-foundation-team-admin** 授予 **server-foundation-clusterpool** 的 **admin** 权限：

```
oc adm new-project server-foundation-clusterpool

oc adm policy add-role-to-group admin server-foundation-team-admin --namespace server-foundation-clusterpool
```

- 作为团队管理员，在集群池命名空间中创建一个名为 **ocp46-aws-clusterpool** 的集群池，带有集群设置标签 **cluster.open-cluster-management.io/clusterset=server-foundation-clusterset**。
  - **server-foundation-webhook** 检查集群池是否有集群设置标签，以及用户是否有权在集群集中创建集群池。
  - **server-foundation-controller** 为 **server-foundation-team-user** 授予对 **server-foundation-clusterpool** 命名空间的 **view** 权限。
- 创建集群池时，集群池会创建一个 **clusterdeployment**。
  - **server-foundation-controller** 为 **server-foundation-team-admin** 授予对 **clusterdeployment** 命名空间的 **admin** 权限。
  - **server-foundation-controller** 为 **server-foundation-team-user** 授予对 **clusterdeployment** 名空间的 **view** 权限。
    注 ：作为 **team-admin** 和 **team-user**，您有 **clusterpool**、**clusterdeplyment** 和 **clusterclaim** 的 **admin** 权限

查看以下集群生命周期控制台和 API RBAC 表：

表 1.2. 集群生命周期的控制台 RBAC 表

资源	Admin	Edit	View
Clusters	read、update、delete	-	读取
集群集	get、update、bind、join	未提及 edit 角色	get
受管集群	read、update、delete	未提及 edit 角色	get
AWS 供应商连接。	create、read、update 和 delete	-	读取
裸机资产	创建、读取、更新、删除	-	读取

表 1.3. 集群生命周期的 API RBAC 表

API	Admin	Edit	View
managedclusters.cluster.open-cluster-management.io *对于这个 API 您可以使用 **mcl**（单数形式）或 **mcls**（复数形式）。*	创建、读取、更新、删除	读取、更新	读取
managedclusters.view.open-cluster-management.io *对于这个 API 您可以使用 **mcv**（单数形式）或 **mcvs**（复数形式）。*	读取	读取	读取
managedclusters.register.open-cluster-management.io/accept	update	update	
managedclusterset.cluster.open-cluster-management.io *对于这个 API 您可以使用 **mclset**（单数形式）或 **mclsets**（复数形式）。*	创建、读取、更新、删除	读取、更新	读取
managedclustersets.view.open-cluster-management.io	读取	读取	读取
managedclustersetbinding.cluster.open-cluster-management.io *对于这个 API 您可以使用 **mclsetbinding**（单数形式）或 **mclsetbindings**（复数形式）。*	创建、读取、更新、删除	读取、更新	读取
baremetalassets.inventory.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取
klusterletaddonconfigs.agent.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取

API	Admin	Edit	View
managedclusteractions.action.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取
managedclusterviews.view.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取
managedclusterinfos.internal.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取
manifestworks.work.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取
submarinerconfigs.submarineraddon.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取
placements.cluster.open-cluster-management.io	创建、读取、更新、删除	读取、更新	读取

1.1.2.2. 基于角色的凭证访问控制

对凭证的访问由 Kubernetes 控制。凭据作为 Kubernetes secret 存储和保护。以下权限适用于在 Red Hat Advanced Cluster Management for Kubernetes 中访问 secret：

- 有权在命名空间中创建 secret 的用户可以创建凭证。
- 有权读取命名空间中的 secret 的用户也可以查看凭证。
- 具有 Kubernetes 集群角色 **admin** 和 **edit** 的用户可以创建和编辑 secret。
- 具有 Kubernetes 集群角色 **view** 的用户无法查看 secret，因为读取 secret 的内容可以访问服务帐户凭证。

1.1.2.3. 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，请参阅创建和管理订阅。

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：

- 创建到 **open-cluster-management:cluster-manager-admin** 集群角色绑定的集群角色绑定，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。

- 选项 ：您可以创建应用程序将资源部署到多个命名空间中：
  - 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>
```

- 要在 **cluster-name** 受管集群中创建并管理一个名为 **application-name** 的应用程序，以 **username** 用户：
  - 输入以下命令创建一个绑定到 **open-cluster-management:admin:** 的一个集群角色，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。

- 选项 ：您可以创建应用程序将资源部署到多个命名空间中：
  - 输入以下命令创建一个到 open-cluster-management:subscription-admin 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:subscription-admin --user=<username>
```

- 使用名为 **username** 的用户在名为 **cluster-name** 的受管集群中查看应用程序：
  - 输入以下命令创建一个绑定到 **open-cluster-management:view:** 的一个集群角色，并将其绑定到 **username**：

```
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**。使用以下命令：

```
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。

查看以下应用程序生命周期控制台和 API RBAC 表：

表 1.4. 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
放置规则（Placement rule）	创建、读取、更新、删除	创建、读取、更新、删除	读取

表 1.5. 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
placementrules.apps.open-cluster-management.io	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

API	Admin	Edit	View
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

1.1.2.4. 监管生命周期 RBAC

创建策略时，会在集群中创建策略。监管生命周期的角色是命名空间范围的。用户还必须有权访问受管集群。

要执行监管生命周期操作，用户必须有权访问创建策略的命名空间，以及访问应用策略的受管集群。

请参见以下示例：

- 要在 **policy** 命名空间中创建策略，并将其应用到名为 **cluster-name** 的受管集群中：
  - 使用 **open-cluster-management:admin:** 角色，创建到 **policy** 命名空间的命名空间角色绑定。运行以下命令：

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

- 查看受管集群中的策略：
  - 输入以下命令创建一个到 **open-cluster-management:admin:** 集群角色的集群角色绑定，并将其绑定到 **view** 角色：

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

查看以下监管生命周期控制台和 API RBAC 表：

表 1.6. 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
PlacementRules	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 1.7. 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

1.1.2.5. 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。
- 搜索资源。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 Role binding policy。请参阅 自定义可观察性 来配置可观察性。

- 如果您有权限可以访问受管集群，请使用 Visual Web Terminal。

要管理可观察性组件，请查看以下 API RBAC 表：

表 1.8. 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

要继续了解更多有关保护集群的信息，请参阅风险和合规性。