



# Red Hat Advanced Cluster Management for Kubernetes 2.7

## アクセス制御

ロールベースのアクセス制御と認証の詳細



ロールベースのアクセス制御と認証の詳細

## 法律上の通知

Copyright © 2024 Red Hat, Inc.

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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

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

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

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

Node.js<sup>®</sup> 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<sup>®</sup> 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.

## 概要

ロールベースのアクセス制御と認証の詳細について説明しています。

---

## 目次

第1章 アクセス制御 .....	3
1.1. ロールベースのアクセス制御	3
1.2. ロールベースのアクセス制御の実装	6



# 第1章 アクセス制御

手動でアクセス制御を作成、管理する必要がある場合もあります。IAM (Identity and Access Management) にワークロードをオンボードするには、Red Hat Advanced Cluster Management for Kubernetes の [認証](#) サービス要件を設定する必要があります。詳細は、OpenShift Container Platform ドキュメントの [認証についての認証について](#) を参照してください。

ロールベースのアクセス制御および認証では、ユーザーに関連付けられたロールおよび認証情報を識別します。アクセス権限と認証情報の詳細は、以下のファイルを参照してください。

**必要なアクセス権限:** クラスターの管理者

- [ロールベースのアクセス制御](#)
- [ロールベースのアクセス制御の実装](#)

## 1.1. ロールベースのアクセス制御

Red Hat Advanced Cluster Management for Kubernetes は、ロールベースのアクセス制御 (RBAC) に対応しています。ロールによって実行できるアクションが決まります。RBAC は、Red Hat OpenShift Container Platform と同様に Kubernetes の認可メカニズムに基づいています。RBAC の詳細は、[OpenShift Container Platform ドキュメント](#) の [RBAC](#) の概要を参照してください。

**注記:** ユーザーロールのアクセスが許可されていない場合、コンソールのアクションボタンは無効になります。

### 1.1.1. ロールの概要

クラスター別の製品リソースと、namespace がスコープの製品リソースがあります。アクセス制御に一貫性を持たせるため、クラスターのロールバインディングと、namespace のロールバインディングをユーザーに適用する必要があります。Red Hat Advanced Cluster Management for Kubernetes でサポートされている以下のロール定義の表を参照してください。

表1.1 ロール定義の表

ロール	定義
<b>cluster-admin</b>	これは OpenShift Container Platform のデフォルトのロールです。 <b>cluster-admin</b> ロールへのクラスターバインディングがあるユーザーは、すべてのアクセス権限を持つ OpenShift Container Platform のスーパーユーザーです。
<b>open-cluster-management:cluster-manager-admin</b>	<b>open-cluster-management:cluster-manager-admin</b> ロールへのクラスターバインディングがあるユーザーは、すべてのアクセス権限を持つ Red Hat Advanced Cluster Management for Kubernetes のスーパーユーザーです。このロールを指定すると、ユーザーは <b>ManagedCluster</b> リソースを作成できます。

<p><b>open-cluster-management:admin:</b> <b>&lt;managed_cluster_name&gt;</b></p>	<p><b>open-cluster-management:admin:</b> <b>&lt;managed_cluster_name&gt;</b> ロールへのクラスターバインディングがあるユーザーには、<b>managedcluster-&lt;managed_cluster_name&gt;</b> という名前の <b>ManagedCluster</b> リソースに管理者アクセス権が付与されます。ユーザーにマネージドクラスターがある場合は、このロールが自動的に作成されます。</p>
<p><b>open-cluster-management:view:</b> <b>&lt;managed_cluster_name&gt;</b></p>	<p><b>open-cluster-management:view:</b> <b>&lt;managed_cluster_name&gt;</b> ロールへのクラスターバインディングがあるユーザーには、<b>managedcluster-&lt;managed_cluster_name&gt;</b> という名前の <b>ManagedCluster</b> リソースの表示権限が付与されます。</p>
<p><b>open-cluster-management:managedclusterset:admin:</b> <b>&lt;managed_clusterset_name&gt;</b></p>	<p><b>open-cluster-management:managedclusterset:admin:</b> <b>&lt;managed_clusterset_name&gt;</b> ロールへのクラスターバインディングがあるユーザーには、<b>&lt;managed_clusterset_name&gt;</b> という名前の <b>ManagedCluster</b> リソースの管理者アクセス権が付与されます。また、ユーザーには <b>managedcluster.cluster.open-cluster-management.io</b>、<b>clusterclaim.hive.openshift.io</b>、<b>clusterdeployment.hive.openshift.io</b> および <b>clusterpool.hive.openshift.io</b> リソースへの管理者アクセス権があります。これには、<b>cluster.open-cluster-management.io/clusterset=&lt;managed_clusterset_name&gt;</b> のマネージドクラスターセットのラベルが付いています。ロールバインディングは、クラスターセットの使用時に自動的に生成されます。リソースの管理方法については、<a href="#">ManagedClusterSet の作成</a> を参照してください。</p>



<p><b>open-cluster-management:managedclusterset:view:</b> <b>&lt;managed_clusterset_name&gt;</b></p>	<p><b>open-cluster-management:managedclusterset:view:</b> <b>&lt;managed_clusterset_name&gt;</b> ロールへのクラスターバインディングがあるユーザーには、<b>&lt;managed_clusterset_name&gt;</b> という名前の <b>ManagedCluster</b> リソースへの表示権限が付与されます。また、ユーザーには <b>managedcluster.cluster.open-cluster-management.io</b>、<b>clusterclaim.hive.openshift.io</b>、<b>clusterdeployment.hive.openshift.io</b> および <b>clusterpool.hive.openshift.io</b> リソースの表示権限があります。これには、<b>cluster.open-cluster-management.io</b>、<b>clusterset=&lt;managed_clusterset_name&gt;</b> のマネージドクラスターセットのラベルが付いています。マネージドクラスターセットのリソース管理方法について、詳しくは <a href="#">ManagedClusterSet の作成</a> を参照してください。</p>
<p><b>open-cluster-management:subscription-admin</b></p>	<p><b>open-cluster-management:subscription-admin</b> ロールが割り当てられたユーザーは、Git サブスクリプションを作成して、リソースを複数の namespace にデプロイできます。リソースは、サブスクライブされた Git リポジトリー of Kubernetes リソース YAML ファイルで指定されます。<b>注記:</b> non-subscription-admin ユーザーがサブスクリプションを作成すると、リソースに指定された namespace に関係なく、すべてのリソースがサブスクリプションの namespace にデプロイされます。詳細は、<a href="#">アプリケーションライフサイクル RBAC</a> セクションを参照してください。</p>
<p>admin、edit、view</p>	<p>admin、edit、および view は OpenShift Container Platform のデフォルトロールです。これらのロールに対して namespace に限定されたバインディングが指定されているユーザーは特定の namespace 内の <b>open-cluster-management</b> リソースにアクセスでき、同じロールに対してクラスター全体のバインディングが指定されている場合はクラスター全体の全 <b>open-cluster-management</b> リソースにアクセスできます。</p>

```
open-cluster-
management:managedclusterset:bind:
<managed_clusterset_name>
```

```
open-cluster-
management:managedclusterset:bind:
<managed_clusterset_name> ロールが割り当て
られたユーザーに
は、<managed_clusterset_name> というマネー
ジドクラスターリソースの表示権限が付与されま
す。ユーザーは <managed_clusterset_name>
を namespace にバインドできます。また、ユーザー
には managedcluster.cluster.open-cluster-
management.io、clusterclaim.hive.openshift.
io、clusterdeployment.hive.openshift.io およ
び clusterpool.hive.openshift.io リソースの表示
権限があります。これは、cluster.open-cluster-
management.io/clusterset=
<managed_clusterset_name> のマネージドクラ
スターセットのラベルが付いています。リソースの
管理方法については、ManagedClusterSet の作成
を参照してください。
```

### 重要:

- ユーザーは OpenShift Container Platform からプロジェクトを作成できます。これにより、namespace の管理者ロール権が付与されます。
- ユーザーがクラスターへのロールアクセス権を持っていない場合、クラスター名は表示されません。クラスター名は、- の記号で表示される場合があります。

詳細は、[ロールベースのアクセス制御の実装](#) を参照してください。

## 1.2. ロールベースのアクセス制御の実装

Red Hat Advanced Cluster Management for Kubernetes RBAC は、コンソールレベルと API レベルで検証されます。コンソール内のアクションは、ユーザーのアクセスロールの権限に基づいて有効化/無効化できます。

マルチクラスターエンジン Operator は、Red Hat Advanced Cluster Management の前提条件であり、クラスターライフサイクル機能です。マルチクラスターエンジン Operator を使用してクラスターの RBAC を管理する場合は、[Kubernetes オペレーターのクラスターライフサイクルマルチクラスターエンジンのロールベースのアクセス制御](#) ドキュメントで RBAC ガイダンスを確認してください。

Red Hat Advanced Cluster Management の特定のライフサイクルにおける RBAC の詳細については、以下のセクションを参照してください。

- [アプリケーションライフサイクル RBAC](#)
  - [アプリケーションライフサイクルのコンソールと API RBAC テーブル](#)
- [ガバナンスライフサイクル RBAC](#)
  - [ガバナンスライフサイクルのコンソールと API RBAC テーブル](#)
- [可観測性の RBAC](#)
  - [可観測性ライフサイクルのコンソールと API RBAC テーブル](#)

### 1.2.1. アプリケーションライフサイクル RBAC

アプリケーションの作成時に、**subscription** namespace が作成され、configuration map が **subscription** namespace に作成されます。**channel** namespace へのアクセス権も必要です。サブスクリプションを適用する場合は、サブスクリプションの管理者である必要があります。アプリケーションの管理の詳細は、[サブスクリプション管理者としての許可および拒否リストの作成](#) を参照してください。

以下のアプリケーションライフサイクル RBAC 操作を確認してください。

- **username** という名前のユーザーを使用して、すべてのマネージドクラスターでアプリケーションを作成および管理します。クラスターロールバインディングを作成し、**username** にバインドする必要があります。以下のコマンドを実行します。

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

このロールはスーパーユーザーであるため、すべてのリソースとアクションにアクセスできません。このロールを使用して、アプリケーションの namespace および namespace 内のすべてのアプリケーションリソースを作成できます。

- 複数の namespace にリソースをデプロイするアプリケーションを作成します。**open-cluster-management:subscription-admin** クラスターロールにバインドするクラスターロールを作成し、**username** という名前のユーザーにバインドする必要があります。以下のコマンドを実行します。

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

- **username** ユーザーを使用して、**cluster-name** マネージドクラスター内に **application-name** という名前のアプリケーションを作成し、管理します。以下のコマンドを入力して、**open-cluster-management:admin:<cluster-name>** クラスターロールへのバインドを作成し、**username** にバインドする必要があります。

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

このロールには、マネージドクラスター **cluster-name** のすべての **application** リソースに対する読み取りおよび書き込み権限があります。他のマネージドクラスターへのアクセスが必要な場合は、この操作を繰り返します。

- 以下のコマンドを入力し、**admin** ロールを使用して **application** namespace にバインドする namespace ロールを作成し、それを **username** にバインドします。

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

このロールには、**application** namespace のすべての **application** リソースに対する読み取りおよび書き込み権限があります。他のアプリケーションへのアクセスが必要な場合や、アプリケーションが複数の namespace にデプロイされる場合は、これを繰り返します。

- リソースを複数の namespace にデプロイするアプリケーションを作成できます。以下のコマンドを入力して、**open-cluster-management:subscription-admin** クラスターロールへのバインドを作成し、**username** にバインドします。

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

- **username** という名前のユーザーで **cluster-name** という名前のマネージドクラスター上のアプリケーションを表示するには、**open-cluster-management:view**: クラスターロールにバインドするクラスターロールを作成し、**username** にバインドします。以下のコマンドを入力します。

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

このロールは、マネージドクラスター **cluster-name** のすべての **application** リソースに対する読み取り権限があります。他のマネージドクラスターへのアクセスが必要な場合は、この操作を繰り返します。

- **view** ロールを使用して **application** namespace にバインドする namespace ロールを作成し、それを **username** にバインドします。以下のコマンドを入力します。

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

このロールには、**application** の namespace にある全 **application** リソースに対する読み取り権限があります。他のアプリケーションへのアクセスが必要な場合は、この操作を繰り返します。

### 1.2.1.1. アプリケーションライフサイクルのコンソールと API RBAC テーブル

アプリケーションライフサイクルの以下のコンソールおよび API RBAC の表を表示します。

表1.2 アプリケーションライフサイクルのコンソール RBAC の表

リソース	管理	編集	表示
アプリケーション	create, read, update, delete	create, read, update, delete	read
チャンネル	create, read, update, delete	create, read, update, delete	read
サブスクリプション	create, read, update, delete	create, read, update, delete	read
配置ルール	create, read, update, delete	create, read, update, delete	read

表1.3 アプリケーションライフサイクルの API RBAC の表

API	管理	編集	View
<b>applications.app.k8s.io</b>	create, read, update, delete	create, read, update, delete	read

API	管理	編集	View
<b>channels.apps.open-cluster-management.io</b>	create, read, update, delete	create, read, update, delete	read
<b>deployables.apps.open-cluster-management.io</b>	create, read, update, delete	create, read, update, delete	read
<b>helmreleases.apps.open-cluster-management.io</b>	create, read, update, delete	create, read, update, delete	read
<b>placements.apps.open-cluster-management.io</b>	create, read, update, delete	create, read, update, delete	read
<b>placementrules.apps.open-cluster-management.io</b>	create, read, update, delete	create, read, update, delete	read
<b>subscriptions.apps.open-cluster-management.io</b>	create, read, update, delete	create, read, update, delete	read
<b>configmaps</b>	create, read, update, delete	create, read, update, delete	read
<b>secrets</b>	create, read, update, delete	create, read, update, delete	read
<b>namespace</b>	create, read, update, delete	create, read, update, delete	read

### 1.2.2. ガバナンスライフサイクル RBAC

ポリシーが作成されると、ポリシーはクラスターに作成されます。ガバナンスライフサイクルのロールは namespace-scoped です。ユーザーは、マネージドクラスターへのアクセス権も必要です。

ユーザーがガバナンスライフサイクル操作を実行するには、ポリシーが作成される namespace、およびポリシーが適用されるマネージドクラスターへのアクセス権が必要です。

次の操作を実行します。

- **policy** namespace にポリシーを作成し、それを **cluster-name** という名前のマネージドクラスターに適用するには、**open-cluster-management:admin:<cluster-name>** クラスターロールを使用して、**policy** namespace にバインドする namespace ロールを作成します。以下のコマンドを実行します。

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

- マネージドクラスターでポリシーを表示するには、**open-cluster-management:view:<cluster-name>** クラスターロールへのバインドを作成し、次のコマンドを使用して **view** ロールにバインドします。

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

### 1.2.2.1. ガバナンスライフサイクルのコンソールと API RBAC テーブル

以下は、ガバナンスライフサイクルのコンソールおよび API RBAC の表です。

表1.4 ガバナンスライフサイクルのコンソール RBAC の表

リソース	管理	編集	表示
ポリシー	create, read, update, delete	read, update	read
PlacementBindings	create, read, update, delete	read, update	read
Placements	create, read, update, delete	read, update	read
PlacementRules	create, read, update, delete	read, update	read
PolicyAutomations	create, read, update, delete	read, update	read

表1.5 ガバナンスライフサイクルの API RBAC の表

API	管理	編集	View
<b>policies.policy.open-cluster-management.io</b>	create, read, update, delete	read, update	read
<b>placementbindings.policy.open-cluster-management.io</b>	create, read, update, delete	read, update	read
<b>policyautomations.policy.open-cluster-management.io</b>	create, read, update, delete	read, update	read

### 1.2.3. 可観測性の RBAC

マネージドクラスターの可観測性メトリックを表示するには、ハブクラスター上のそのマネージドクラスターに対する **view** 権限が必要です。以下の可観測性機能の一覧を参照してください。

- マネージドクラスターのメトリクスへのアクセス  
ユーザーがハブクラスター上のマネージドクラスターの **view** ロールに割り当てられていない場合、ユーザーによるマネージドクラスターメトリックへのアクセスは拒否されます。次のコマンドを実行して、マネージドクラスターの namespace で **managedClusterView** ロールの作成権限がユーザーにあるか確認します。

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

クラスター管理者として、マネージドクラスターの namespace に **managedClusterView** ロールを作成します。以下のコマンドを実行します。

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

次に、ロールバインドを作成してロールをユーザーに適用し、バインドします。以下のコマンドを実行します。

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

- リソースの検索  
ユーザーがリソースタイプにアクセスできるか確認するには、次のコマンドを使用します。

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

**注記:** **<resource-type>** は複数形にする必要があります。

- Grafana で可観測性データを表示するには、マネージドクラスターの同じ namespace に **RoleBinding** リソースが必要です。以下は **RoleBinding** の例です。

```
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
```

詳細は、[ロールバインディングポリシー](#) を参照してください。可観測性を設定するには、[可観測性のカスタマイズ](#) を参照してください。

### 1.2.3.1. 可観測性ライフサイクルのコンソールと API RBAC テーブル

可観測性のコンポーネントを管理する場合は、以下の API RBAC の表を確認してください。

表1.6 可観測性の API RBAC の表

API	管理	編集	View
<b>multiclusterobservabilities.observability.open-cluster-management.io</b>	create, read, update, delete	read, update	read
<b>searchcustomizations.search.open-cluster-management.io</b>	create, get, list, watch, update, delete, patch	-	-
<b>policyreports.wgpolicyk8s.io</b>	get, list, watch	get, list, watch	get, list, watch

次は [リスクとコンプライアンス](#) でクラスターのセキュリティー保護について確認してください。