



Red Hat Advanced Cluster Management for Kubernetes 2.3

アクセス制御

ロールベースのアクセス制御および認証の詳細は、「ロールベースのアクセス制御
および認証」を参照してください。

Red Hat Advanced Cluster Management for Kubernetes 2.3 アクセス制御

ロールベースのアクセス制御および認証の詳細は、「ロールベースのアクセス制御および認証」を参照してください。

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.

法律上の通知

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.

概要

ロールベースのアクセス制御および認証の詳細は、「ロールベースのアクセス制御および認証」を参照してください。

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
1.1.1. ロールの概要	3
1.1.2. RBAC 実装	5
1.1.2.1. クラスターライフサイクル RBAC	6
1.1.2.1.1. クラスタープール RBAC	7
1.1.2.2. 認証情報ロールベースのアクセス制御	10
1.1.2.3. アプリケーションライフサイクル RBAC	10
1.1.2.4. ガバナンスライフサイクル RBAC	13
1.1.2.5. 可観測性の RBAC	14

第1章 アクセス制御

アクセス制御の手動での作成および管理が必要な場合があります。Identity and Access Management (IAM) 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『[認証および認可](#)』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は、ユーザー関連のロールおよび認証情報を特定します。アクセス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](#)

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) をサポートします。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 の承認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権がない場合には、コンソールのアクションボタンが無効になります。

コンポーネントでサポートされる 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。

- [ロールの概要](#)
- [RBAC 実装](#)
- [クラスターライフサイクル RBAC](#)
- [アプリケーションライフサイクル RBAC](#)
- [ガバナンスライフサイクル RBAC](#)
- [可観測性の RBAC](#)

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 のロールバインド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
cluster-admin	これは OpenShift Container Platform のデフォルトのロールです。 cluster-admin ロールへのクラスターのバインディングのあるユーザーは、全アクセス権限のある OpenShift Container Platform スーパーユーザーです。

<p><code>open-cluster-management:cluster-manager-admin</code></p>	<p>open-cluster-management:cluster-manager-admin ロールへのクラスターバインディングのあるユーザーは、全アクセス権限のある 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 ManagedCluster リソースを作成できます。</p>
<p><code>open-cluster-management:admin:<managed_cluster_name></code></p>	<p>open-cluster-management:admin:<managed_cluster_name> ロールへのクラスターバインディングのあるユーザーには、managedcluster-<managed_cluster_name> という名前の ManagedCluster リソースに管理者アクセスが付与されます。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><code>open-cluster-management:view:<managed_cluster_name></code></p>	<p>open-cluster-management:view:<managed_cluster_name> ロールへのクラスターバインディングのあるユーザーには、managedcluster-<managed_cluster_name> という名前の ManagedCluster リソースに表示アクセスが付与されます。</p>
<p><code>open-cluster-management:managedclusterset:admin:<managed_clusterset_name></code></p>	<p>open-cluster-management:managedclusterset:admin:<managed_clusterset_name> ロールへのクラスターバインディングのあるユーザーには、<managed_clusterset_name> という名前の ManagedCluster リソースへの管理者アクセスがあります。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 リソースへの管理者アクセスがあり、cluster.open-cluster-management.io と 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。ロールバインドは、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、「ManagedClusterSets の作成および管理」 を参照してください。</p>

<p>open-cluster-management:managedclusterset:view: <managed_clusterset_name></p>	<p>open-cluster-management:managedclusterset:view: <managed_clusterset_name> ロールへのクラスターバインディングのあるユーザーには、<managed_clusterset_name> という名前の ManagedCluster リソースへの表示権限があります。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 リソースへの表示権限があり、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。マネージドクラスターセットの管理方法の詳細は、「ManagedClusterSets の作成と管理」 を参照してください。</p>
<p>open-cluster-management:subscription-admin</p>	<p>open-cluster-management:subscription-admin 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。注記: 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、「アプリケーションライフサイクル RBAC」の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 open-cluster-management 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には、クラスター全体の open-cluster-management リソースすべてにアクセス権があります。</p>

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 の管理者ロールパーミッションが付与されます。
- ユーザーにクラスターへのロールアクセスがない場合には、クラスター名は表示されません。クラスター名は、- の記号で表示されます。

1.1.2. RBAC 実装

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パーミッションに基づいて有効化/無効化できます。製品の特定期間ライフサイクルの RBAC の詳細は、以下のセクションを参照してください。

1.1.2.1. クラスターライフサイクル RBAC

以下のクラスターライフサイクル RBAC 操作を確認してください。

- 全マネージドクラスターを作成して管理する方法:

- 以下のコマンドを入力して、クラスターロール **open-cluster-management:cluster-manager-admin** にバインドするクラスターロールを作成します。

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

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す。このロールを使用すると、クラスターレベルの **managedcluster** リソース、マネージドクラスターを管理するリソースの namespace、namespace 内のリソースを作成できます。また、このロールで、プロバイダー接続、マネージドクラスター作成に使用するベアメタルアセットにアクセスできます。

- **cluster-name** という名前のマネージドクラスターを管理する方法:

- 以下のコマンドを入力して、クラスターロール **open-cluster-management:admin:<cluster-name>** にバインドするクラスターロールを作成します。

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

このロールを使用すると、クラスターレベルの **managedcluster** リソースに読み取り/書き込みアクセスができるようになります。**managedcluster** はクラスターレベルのリソースで、namespace レベルのリソースではないので、このロールが必要です。

- 以下のコマンドを入力して、クラスターロール **admin** にバインドする namespace ロールを作成します。

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

このロールでは、マネージドクラスターの namespace 内にあるリソースに対して読み取り/書き込みアクセスができるようになります。

- **cluster-name** という名前のマネージドクラスターを表示する方法:

- 以下のコマンドを入力して、クラスターロール **open-cluster-management:view:<cluster-name>** にバインドするクラスターロールを作成します。

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

このロールを使用すると、クラスターレベルの **managedcluster** リソースに読み取りアクセスができるようになります。**managedcluster** はクラスターレベルのリソースで、namespace レベルのリソースではないので、このロールが必要です。

- 以下のコマンドを入力して、クラスターロール **view** にバインドする namespace ロールを作成します。

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

このロールでは、マネージドクラスターの namespace 内にあるリソースに対して読み取り専用アクセスができるようになります。

- 以下のコマンドを入力して、アクセス可能なマネージドクラスターの一覧を表示します。

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

このコマンドは、クラスター管理者の権限のない管理者およびユーザーが使用します。

- 以下のコマンドを入力して、アクセス可能なマネージドクラスターセットの一覧を表示します。

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

このコマンドは、クラスター管理者の権限のない管理者およびユーザーが使用します。

1.1.2.1.1. クラスタープール RBAC

以下のクラスタープール RBAC 操作を確認してください。

- クラスタープールのプロビジョニングクラスターを使用するには、以下を実行します。
 - クラスタ管理者は、グループにロールを追加してマネージドクラスターセットを作成し、管理者権限をロールに付与します。
 - 以下のコマンドを使用して、**server-foundation-clusterset** マネージドクラスターセットに **admin** パーミッションを付与します。

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

- 以下のコマンドを使用して、**server-foundation-clusterset** マネージドクラスターセットに **view** パーミッションを付与します。

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

- クラスタープールの namespace (**server-foundation-clusterpool**) を作成します。
 - 以下のコマンドを実行して、**server-foundation-team-admin** の **server-foundation-clusterpool** に **admin** 権限を付与します。

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

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

- チーム管理者として、クラスタープール namespace にクラスターセットラベル **cluster.open-cluster-management.io/clusterset=server-foundation-clusterset** で、**ocp46-aws-clusterpool** という名前のクラスタープールを作成します。
 - **server-foundation-webhook** は、クラスタープールにクラスターセットラベルがある

かどうか、またユーザーにクラスターセットのクラスタープールを作成するパーミッションがあるかどうかを確認します。

- **server-foundation-controller** は、**server-foundation-team-user** の **server-foundation-clusterpool** namespace に **表示** パーミッションを付与します。
- クラスタープールが作成されると、クラスタープールは **clusterdeployment** を作成します。
 - **server-foundation-controller** は、**server-foundation-team-admin** の **clusterdeployment** namespace に **admin** パーミッションを付与します。
 - **server-foundation-controller** は、**server-foundation-team-user** の **clusterdeployment** namespace に **view** パーミッションを付与します。
注記: **team-admin** および **team-user** は、**clusterpool**、**clusterdeployment** および **clusterclaim** への **admin** 権限があります。

クラスター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 クラスター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
Clusters (クラスター)	read, update, delete	-	read
クラスターセット	get, update, bind, join	編集ロールなし	get
マネージドクラスター	read, update, delete	編集ロールなし	get
プロバイダー接続	create, read, update, delete	-	read
ベアメタルアセット	create, read, update, delete	-	read

表1.3 クラスターライフサイクルの API RBAC の表

API	管理	編集	表示
managedclusters.cluster .open-cluster- management.io	create, read, update, delete	read, update	read
この API のコマンドでは、 mcl (単数) または mcls (複数) を使用できます。			

API	管理	編集	表示
managedclusters.view.open-cluster-management.io この API のコマンドでは、mcv (単数) または mcvs (複数) を使用できます。	read	read	read
managedclusters.register.open-cluster-management.io/accept	更新	更新	
managedclusterset.cluster.open-cluster-management.io この API のコマンドでは、mclset (単数) または mclsets (複数) を使用できます。	create, read, update, delete	read, update	read
managedclustersets.view.open-cluster-management.io	read	read	read
managedclustersetbinding.cluster.open-cluster-management.io この API のコマンドでは、mclsetbinding (単数) または mclsetbindings (複数) を使用できます。	create, read, update, delete	read, update	read
baremetalassets.inventory.open-cluster-management.io	create, read, update, delete	read, update	read
klusterletaddonconfigs.agent.open-cluster-management.io	create, read, update, delete	read, update	read
managedclusteractions.action.open-cluster-management.io	create, read, update, delete	read, update	read

API	管理	編集	表示
managedclusterviews.v1ew.open-cluster-management.io	create, read, update, delete	read, update	read
managedclusterinfos.internal.open-cluster-management.io	create, read, update, delete	read, update	read
manifestworks.work.open-cluster-management.io	create, read, update, delete	read, update	read
submarinerconfigs.submarineraddon.open-cluster-management.io	create, read, update, delete	read, update	read
placements.cluster.open-cluster-management.io	create, read, update, delete	read, update	read

1.1.2.2. 認証情報ロールベースのアクセス制御

認証情報へのアクセスは Kubernetes で制御されます。認証情報は Kubernetes Secret として保存され、セキュリティを確保します。以下のパーミッションは、Red Hat Advanced Cluster Management for Kubernetes のシークレットのアクセスに関係します。

- namespace でシークレットの作成権限のあるユーザーは認証情報を作成できます。
- namespace でシークレットの読み取り権限のあるユーザーは、認証情報を表示することもできます。
- Kubernetes ロール **admin** と **edit** のあるユーザーは、シークレットの作成と編集が可能です。
- Kubernetes クラスターロール **view** のあるユーザーは、シークレットの内容を読み取ると、サービスアカウントの認証情報にアクセスできるようになるので、シークレットを表示できません。

1.1.2.3. 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、設定マップが **subscription** namespace に作成されます。**channel** namespace にもアクセスする必要があります。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の作成および管理](#)」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で、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して管理するには、以下を実行します。
 - 以下のコマンドを実行して、**open-cluster-management:cluster-manager-admin** クラスターロールへのクラスターロールのバインディングを作成して、**username** にバインドします。

```
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す。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。

- **オプション:** 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できます。
 - **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、これを **username** という名前のユーザーにバインドします。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** ユーザーで **cluster-name** マネージドクラスターに **application-name** という名前のアプリケーションを作成し、管理するには、以下を実行します。
 - 以下のコマンドを入力して、**open-cluster-management: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: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** リソースへの読み取りおよび書き込みアクセスがあります。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て、**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、これを **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** リソースへの読み取りおよび書き込みアクセスがあります。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。

- **オプション:** 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クラスターロールのバインディングを作成し、**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が **cluster-name** という名前のマネージドクラスターでアプリケーションを表示するには、以下を実行します。
 - 以下のコマンドを入力して、**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、これを **username** にバインドします。

```
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 **アプリケーション** リソースへの読み取りアクセスがあります。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、これを **username** にバインドします。以下のコマンドを実行します。

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

このロールは **application** の namespace にある全 **application** リソースへの読み取りアクセスがあります。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。

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1.4 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1.5 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	表示
applications.app.k8s.io	create, read, update, delete	create, read, update, delete	read
channels.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
deployables.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
helmreleases.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
placementrules.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read

API	管理	編集	表示
subscriptions.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
configmaps	create, read, update, delete	create, read, update, delete	read
secrets	create, read, update, delete	create, read, update, delete	read
namespace	create, read, update, delete	create, read, update, delete	read

1.1.2.4. 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のレベルは namespace 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。

ユーザーは、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。

以下の例を参照してください。

- **ポリシー namespace** でポリシーを作成し、これを **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、以下を実行します。
 - **open-cluster-management:admin:** 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=admin --user=<username>
```

- マネージドクラスターでポリシーを表示するには、以下を実行します。
 - 以下のコマンドを実行して、**open-cluster-management: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、これを **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>
```

ガバナンス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1.6 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

リソース	管理	編集	表示
PlacementBindings	create, read, update, delete	read, update	read
PlacementRules	create, read, update, delete	read, update	read
PolicyAutomations	create, read, update, delete	read, update	read

表1.7 ガバナンスライフサイクルの API RBAC の表

API	管理	編集	表示
policies.policy.open-cluster-management.io	create, read, update, delete	read, update	read
placementbindings.policy.open-cluster-management.io	create, read, update, delete	read, update	read
policyautomations.policy.open-cluster-management.io	create, read, update, delete	read, update	read

1.1.2.5. 可観測性の RBAC

マネージドクラスターの可観測性メトリクスを表示するには、ハブクラスターでそのマネージドクラスターへの **表示** アクセスが必要です。以下の可観測性機能のリスト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
ユーザーは、ハブクラスター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に、マネージドクラスターメトリクスへのアクセスが拒否されます。
- リソースの検索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。以下の **RoleBinding** の例を確認してください。

```
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、「[Role binding ポリシー](#)」を参照してください。「[可観測性のカスタマイズによる可観測性の設定](#)」を参照してください。

- Visual Web ターミナルの使用 (マネージドクラスターにアクセスできる場合)

可観測性のコンポーネントを管理するには、以下の API RBAC の表を確認します。

表1.8 可観測性の API RBAC の表

API	管理	編集	表示
multiclusterobservabilities.observability.open-cluster-management.io	create, read, update, delete	read, update	read
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

クラスターのセキュリティー保護に関する詳細の確認を続行するには、「[リスクおよびコンプライアンス](#)」を参照してください。