Red Hat Advanced Cluster Management for Kubernetes 2.10

アクセス制御

アクセス制御

Last Updated: 2024-05-24

Red Hat Advanced Cluster Management for Kubernetes 2.10 アクセス制御

アクセス制御

法律上の通知

概要

ユーザーによる、特定のロールを実行するために必要なリソースへのアクセスを可能にします。

目次

第1章 アクセス制御

手動によるアクセス制御の作成および管理が必要になる場合もあります。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。アクセスおよび認証情報の詳細は、以下のドキュメント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、スコープに namespace が指定されている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
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。
open-cluster-management:cluster-manager-admin	**open-cluster-management:cluster-manager-admin** 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 **ManagedCluster** リソースを作成できます。

open-cluster-management:admin:<managed_cluster_name>	**open-cluster-management:admin:<managed_cluster_name>** 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、**managedcluster-<managed_cluster_name>** という名前の **ManagedCluster** 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。
open-cluster-management:view:<managed_cluster_name>	**open-cluster-management:view:<managed_cluster_name>** 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、**managedcluster-<managed_cluster_name>** という名前の **ManagedCluster** リソースの表示権限が付与されます。
open-cluster-management:managedclusterset:admin:<managed_clusterset_name>	**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があるユーザーには、**<managed_clusterset_name>** という名前の **ManagedCluster** 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 **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権があります。これには、**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。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は、ManagedClusterSet の作成 を参照してください。

open-cluster-management:managedclusterset:view:<managed_clusterset_name>	**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があるユーザーには、<managed_clusterset_name>` という名前の **ManagedCluster** リソースへの表示権限が付与されます。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。これには、**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。マネージドクラスターセットのリソース管理方法の詳細は、ManagedClusterSet の作成 を参照してください。
open-cluster-management:subscription-admin	**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 リポジトリーの 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 セクションを参照してください。
admin、edit、view	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は、クラスター全体の全 **open-cluster-management** リソースにアクセスできます。

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 に対する管理者ロールの権限が付与されます。
- 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 ドキュメントの RBAC ガイダンスを使用してください。

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。

- 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でアプリケーションを作成および管理します。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** namspace 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 namspace にあるすべての **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

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	表示
applications.app.k8s.io	create, read, update, delete	create, read, update, delete	read

API	管理	編集	表示
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
placements.apps.open-cluster-management.io	create, read, update, delete	create, read, update, delete	read
placementrules.apps.open-cluster-management.io (非推奨)	create, read, update, delete	create, read, update, delete	read
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

1.2.2. 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。マネージドクラスターは、namespace にバインドされる **ManagedClusterSet** の一部でもある必要があります。**ManagedClusterSet** の詳細は、ManagedClusterSets の概要 を参照してください。

1 つ以上の **ManagedClusterSets** がバインドされた **rhacm-policies** などの namespace を選択し、namespace 内に **Placement** オブジェクトを作成するためのアクセス権を取得したら、次の操作を表示します。

- **Policy**、**PlacementBinding**、および **PolicyAutomation** の編集アクセス権を指定して **rhacm-edit-policy** という名前の **ClusterRole** を作成するには、次のコマンドを実行します。

```
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
```

- **rhacm-policies** namespace にポリシーを作成するには、以前に作成した **ClusterRole** を使用して、**rhacm-policies** namespace に **rhacm-edit-policy** などの namespace **RoleBinding** を作成します。以下のコマンドを実行します。

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

- マネージドクラスターのポリシーステータスを表示するには、ハブクラスターのマネージドクラスターの namespace でポリシーを表示するパーミッションが必要です。OpenShift **viewClusterRole** などの **view** アクセス権がない場合は、次のコマンドを使用して、ポリシーへの表示アクセス権を持つ **ClusterRole** (**rhacm-view-policy** など) を作成します。

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

- 新しい **ClusterRole** をマネージドクラスターの namespace にバインドするには、次のコマンドを実行して namespace **RoleBinding** を作成します。

```
oc create rolebinding rhacm-view-policy -n <cluster name> --clusterrole=rhacm-view-policy --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 (非推奨)	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	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

1.2.3. 可観測性の RBAC

マネージドクラスターの可観測性メトリクスを表示するには、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クス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を確認します。

  ```
  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	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

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。