# Red Hat Advanced Cluster Management for Kubernetes 2.10

## 액세스 제어

액세스 제어

Last Updated: 2024-09-05

액세스 제어

## 법적 공지

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 ® 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.

## 초록

사용자가 특정 역할을 수행하는 데 필요한 리소스에 액세스할 수 있는지 확인합니다.

# 차례

# 1장. 액세스 제어

액세스 제어를 수동으로 생성하고 관리해야 할 수 있습니다. Red Hat Advanced Cluster Management for Kubernetes의 *인증서비스* 요구 사항을 구성하여 IAM(Identity and Access Management)에 워크로드를 온보드해야 합니다. 자세한 내용은 OpenShift Container Platform 설명서의 인증 이해에서 인증 이해 를 참조하십시오.

*역할 기반 액세스 제어 및 인증은 사용자 관련 역할 및 클러스터 자격 증명을 식별합니다. 액세스 및 인증 정보에 대한 자세한 내용은 다음 설명서를 참조하십시오.*

***필수 액세스:*** *클러스터 관리자*

- *역할 기반 액세스 제어*
- *역할 기반 액세스 제어 구현*

## 1.1. 역할 기반 액세스 제어

*Red Hat Advanced Cluster Management for Kubernetes는 역할 기반 액세스 제어(RBAC)를 지원합니다. 역할에 따라 수행할 수 있는 작업이 결정됩니다. RBAC는 Red Hat OpenShift Container Platform과 유사하게 Kubernetes의 권한 부여 메커니즘을 기반으로 합니다. RBAC에 대한 자세한 내용은 OpenShift Container Platform 설명서의 OpenShift RBAC 개요를 참조하십시오.*

***참고:*** *사용자 역할 액세스가 허용되지 않는 경우 콘솔에서 동작 버튼이 비활성화됩니다.*

### 1.1.1. 역할 개요

*일부 제품 리소스는 클러스터 전체이며 일부는 네임스페이스 범위입니다. 일관된 액세스 제어를 위해 사용자에게 클러스터 역할 바인딩 및 네임스페이스 역할 바인딩을 적용해야 합니다. Red Hat Advanced Cluster Management for Kubernetes에서 지원되는 다음 역할 정의의 표 목록을 확인합니다.*

***표 1.1. 역할 정의 테이블***

| Role | 정의 |
|---|---|
| **cluster-admin** | OpenShift Container Platform 기본 역할입니다. **cluster-admin** 역할에 클러스터 바인딩이 있는 사용자는 모든 액세스 권한이 있는 OpenShift Container Platform 슈퍼 사용자입니다. |
| **open-cluster-management:cluster-manager-admin** | **open-cluster-management:cluster-manager-admin** 역할에 대한 클러스터 바인딩이 있는 사용자는 모든 액세스 권한이 있는 Kubernetes 슈퍼 사용자에 대한 Red Hat Advanced Cluster Management입니다. 이 역할을 사용하면 **ManagedCluster** 리소스를 생성할 수 있습니다. |
| **open-cluster-management:admin:<managed_cluster_name>** | **open-cluster-management:admin:<managed_cluster_name> 역할에 대한 클러스터** 바인딩 사용자는 <**managed_cluster_name**>이라는 **ManagedCluster** 리소스에 대한 관리자 액세스 권한이 있습니다. 사용자에게 관리 클러스터가 있으면 이 역할이 자동으로 생성됩니다. |

| | |
|---|---|
| **open-cluster-management:view:<managed_cluster_name>** | **open-cluster-management:view:<managed_cluster_name> 역할에 대한 클러스터** 바인딩 사용자는 <**managed_cluster_name** >이라는 **ManagedCluster** 리소스에 대한 보기 액세스 권한이 있습니다. |
| **open-cluster-management:managedclusterset:admin:<managed_clusterset_name>** | **open-cluster-management:managedclusterset:admin:<managed_clusterset_name> 역할에 대한 클러스터 바인딩 사용자는 <managed_ clusterset _name** >이라는 **ManagedCluster** 리소스에 대한 관리자 액세스 권한이 있습니다. 또한 사용자는 **관리 클러스터 세트 레이블이 cluster.open-cluster-management.io ,clusterclaim.hive.openshift.io,clusterdeployment.hive.openshift.io** 및 **clusterpool.hive.openshift.io** 리소스에 대한 관리자 액세스 권한도 있습니다. cluster **.open-cluster-management.io/clusterset=<managed_clusterset_name** > . 클러스터 세트를 사용하는 경우 역할 바인딩이 자동으로 생성됩니다. 리소스 를 관리하는 방법을 알아보려면 *ManagedClusterSet생성* 을 참조하십시오. |
| **open-cluster-management:managedclusterset:view:<managed_clusterset_name>** | **open-cluster-management:managedclusterset:view:<managed_clusterset_name** > 역할에 대한 클러스터 바인딩 사용자는 <managed_clusterset_name>'이라는 **ManagedCluster** 리소스에 대한 보기 액세스 권한이 있습니다. 또한 사용자는 **관리 클러스터 설정 라벨이 cluster.open-cluster-management.io,clusterclaim.hive.openshift.io,clusterdeployment.hive.openshift.io** 및 **clusterpool.hive.openshift.io** 에 대한 보기 액세스 권한도 있습니다. cluster.open-cluster-management.io , clusterset=<**managed_clusterset_name** > . 관리 클러스터 세트 리소스를 관리하는 방법에 대한 자세한 내용은 *ManagedClusterSet생성을* 참조하십시오. |
| **open-cluster-management:subscription-admin** | **open-cluster-management:subscription-admin** 역할의 사용자는 여러 네임스페이스에 리소스를 배포하는 Git 서브스크립션을 생성할 수 있습니다. 리소스는 구독한 Git 리포지토리의 Kubernetes 리소스 YAML 파일에 지정됩니다. **참고:** 서브스크립션 관리자가 아닌 사용자가 서브스크립션을 생성하면 리소스에 지정된 네임스페이스와 관계없이 모든 리소스가 서브스크립션 네임스페이스에 배포됩니다. 자세한 내용은 애플리케이션 라이프사이클 RBAC 섹션을 참조하십시오. |

| | |
|---|---|
| 관리자, 편집, 보기 | admin, edit, view는 OpenShift Container Platform 기본 역할입니다. 이러한 역할에 대한 네임스페이스 범위 바인딩이 있는 사용자는 특정 네임스페이스의 **open-cluster-management** 리소스에 액세스할 수 있지만 동일한 역할에 대한 클러스터 전체 바인딩은 클러스터 전체에서 모든 오픈 클러스터 관리 리소스에 액세스할 수 있습니다. |
| **open-cluster-management:managedclusterset:bind:<managed_clusterset_name>** | **open-cluster-management:managedclusterset:bind:<managed_clusterset_name>** 역할이 있는 사용자는 <managed_cluster **set_name>이라는 관리 클러스터** 리소스에 대한 보기 액세스 권한이 있습니다. 사용자는 < **managed_clusterset_name>을** 네임스페이스에 바인딩할 수 있습니다. 또한 사용자는 **관리 클러스터 세트 레이블이 cluster.open-cluster-management.io,clusterclaim.hive.openshift.io ,clusterdeployment.hive.openshift.io** 및 **clusterpool.hive.openshift.io** 리소스에 대한 보기 액세스 권한도 있습니다. cluster **.open-cluster-management.io/clusterset=<managed_clusterset_name>** . 리소스를 관리하는 방법을 알아보려면 *ManagedClusterSet생성* 을 참조하십시오. |

*중요:*

- *모든 사용자는 OpenShift Container Platform에서 프로젝트를 생성할 수 있으므로 네임스페이스에 대한 관리자 역할 권한이 부여됩니다.*
- *사용자에게 클러스터에 대한 역할 액세스 권한이 없는 경우 클러스터 이름이 표시되지 않습니다. 클러스터 이름은 다음 기호와 함께 표시될 수 있습니다. -.*

*자세한 내용은 역할 기반 액세스 제어 구현을 참조하십시오.*

## *1.2. 역할 기반 액세스 제어 구현*

*Red Hat Advanced Cluster Management for Kubernetes RBAC는 콘솔 수준 및 API 수준에서 검증됩니다. 콘솔의 작업은 사용자 액세스 역할 권한에 따라 활성화하거나 비활성화할 수 있습니다.*

*멀티 클러스터 엔진 Operator는 Red Hat Advanced Cluster Management의 사전 요구 사항과 클러스터 라이프사이클 기능입니다. 다중 클러스터 엔진 Operator를 사용하여 클러스터의 RBAC를 관리하려면 Kubernetes 운영자 역할 기반 액세스 제어 문서의 클러스터 라이프사이클 multicluster 엔진 의 RBAC 지침을 사용합니다.*

*Red Hat Advanced Cluster Management의 특정 라이프사이클에 대한 자세한 내용은 다음 섹션을 참조하십시오.*

- *애플리케이션 라이프사이클 RBAC*
  - *애플리케이션 라이프사이클을 위한 콘솔 및 API RBAC 테이블*

- 거버넌스 라이프사이클 RBAC
  - 거버넌스 라이프사이클을 위한 콘솔 및 API RBAC 테이블
- 관찰 가능성 RBAC
  - 관찰 가능 라이프사이클을 위한 콘솔 및 API RBAC 테이블

### 1.2.1. 애플리케이션 라이프사이클 RBAC

애플리케이션을 생성하면 **서브스크립션** 네임스페이스가 생성되고 **서브스크립션** 네임스페이스에 구성 맵이 생성됩니다. **채널** 네임스페이스에 대한 액세스 권한도 있어야 합니다. 서브스크립션을 적용하려면 서브스크립션 관리자여야 합니다. 애플리케이션 관리에 대한 자세한 내용은 서브스크립션 관리자로 허용 및 거부 목록 생성 을 참조하십시오.

다음 애플리케이션 라이프사이클 RBAC 작업을 확인합니다.

- **username** 이라는 사용자를 사용하여 모든 관리 클러스터에서 애플리케이션을 생성하고 관리합니다. 클러스터 역할 바인딩을 생성하여 사용자 이름에 바인딩해야 **합니다**. 다음 명령을 실행합니다.

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

  이 역할은 모든 리소스 및 작업에 액세스할 수 있는 슈퍼유저입니다. 이 역할을 사용하여 애플리케이션의 네임스페이스 및 네임스페이스의 모든 애플리케이션 리소스를 생성할 수 있습니다.

- 여러 네임스페이스에 리소스를 배포하는 애플리케이션을 생성합니다. **open-cluster-management:subscription-admin** 클러스터 역할에 대한 클러스터 역할 바인딩을 생성하여 **username** 이라는 사용자에게 바인딩해야 합니다. 다음 명령을 실행합니다.

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

- **username** 사용자를 사용하여 **클러스터 이름 관리** 클러스터에서 애플리케이션을 생성하고 관리합니다. **open-cluster-management:admin:<cluster-name> 클러스터** 역할에 대한 클러스터 역할 바인딩을 생성하고 다음 명령을 입력하여 **사용자** 이름에 바인딩해야 합니다.

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

  이 역할에는 관리 클러스터인 **cluster-name** 의 모든 **애플리케이션** 리소스에 대한 읽기 및 쓰기 권한이 있습니다. 다른 관리 클러스터에 대한 액세스가 필요한 경우 이 단계를 반복합니다.

- **admin** 역할을 사용하여 **애플리케이션** 네임스페이스에 대한 네임스페이스 역할 바인딩을 생성하고 다음 명령을 **입력하여 사용자** 이름에 바인딩합니다.

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

  이 역할에는 애플리케이션 namspace의 모든 **애플리케이션** 리소스에 대한 읽기 및 쓰기 권한이 있습니다. **다른 애플리케이션에 대한 액세스가 필요하거나 애플리케이션이 여러 네임스페이스에 배포하는 경우 이 과정을 반복합니다.**

- *여러 네임스페이스에 리소스를 배포하는 애플리케이션을 생성할 수 있습니다. **open-cluster-management:subscription-admin** 클러스터 역할에 대한 클러스터 역할 바인딩을 생성하고 다음 명령을 입력하여 사용자 이름에 바인딩합니다.*

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

- ***username** 이라는 사용자를 사용하여 **cluster-name** 이라는 관리 클러스터에서 애플리케이션을 보려면 **open-cluster-management:view: cluster** 역할에 클러스터 역할 바인딩을 생성하고 사용자 이름에 바인딩합니다. 다음 명령을 실행합니다.*

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

*이 역할은 관리 클러스터인 **cluster-name** 의 모든 애플리케이션 리소스에 대한 읽기 액세스 권한이 있습니다. 다른 관리 클러스터에 대한 액세스가 필요한 경우 이 단계를 반복합니다.*

- ***view** 역할을 사용하여 애플리케이션 네임스페이스에 대한 네임스페이스 역할 바인딩을 생성하고 사용자 이름에 바인딩 합니다. 다음 명령을 실행합니다.*

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

*이 역할은 애플리케이션 **namspace**의 모든 애플리케이션 리소스에 대한 읽기 액세스 권한이 있습니다. 다른 애플리케이션에 대한 액세스가 필요한 경우 이 작업을 반복합니다.*

#### *1.2.1.1. 애플리케이션 라이프사이클을 위한 콘솔 및 API RBAC 테이블*

*애플리케이션 라이프사이클에 대해 다음 콘솔 및 **API RBAC** 테이블을 확인합니다.*

*표 **1.2.** 애플리케이션 라이프사이클을 위한 콘솔 **RBAC** 테이블*

| 리소스 | 관리자 | edit | view |
|---|---|---|---|
| 애플리케이션 | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| 채널 | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |

| 리소스 | 관리자 | edit | view |
| --- | --- | --- | --- |
| 서브스크립션 | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |

*표 1.3. 애플리케이션 라이프사이클을 위한 API RBAC 테이블*

| API | 관리자 | edit | view |
| --- | --- | --- | --- |
| **applications.app.k8s.io** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **channels.apps.open-cluster-management.io** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **deployables.apps.open-cluster-management.io** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **helmreleases.apps.open-cluster-management.io** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **placements.apps.open-cluster-management.io** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **placementrules.apps.open-cluster-management.io** (더 이상 사용되지 않음) | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **subscriptions.apps.open-cluster-management.io** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **configmaps** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **secrets** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |
| **네임스페이스** | 생성, 읽기, 업데이트, 삭제 | 생성, 읽기, 업데이트, 삭제 | 읽기 |

### *1.2.2. 거버넌스 라이프사이클 RBAC*

*거버넌스 라이프사이클 작업을 수행하려면 정책이 생성되는 네임스페이스와 정책이 적용되는 관리 클러스터에 대한 액세스 권한이 있어야 합니다. 또한 관리되는 클러스터는 네임스페이스에 바인딩된 **ManagedClusterSet** 의 일부여야 합니다. **ManagedClusterSet** 에 대한 자세한 내용은 **ManagedClusterSets Introduction** 을 참조하십시오.*

*하나 이상의 바인딩된 **ManagedClusterSets** 가 있는 **rhacm-policies** 와 같은 네임스페이스를 선택하고 네임스페이스에서 **Placement** 오브젝트를 생성할 수 있는 액세스 권한이 있는 후 다음 작업을 확인합니다.*

- *__Policy ,PlacementBinding, Policy Automation edit__ 액세스 권한을 사용하여 **rhacm-edit-policy** 라는 **ClusterRole** 을 생성하려면 다음 명령을 실행합니다.*

```
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__ 네임스페이스에서 정책을 생성하려면 이전에 생성된 **ClusterRole** 을 사용하여 **rhacm-edit-policy** 와 같은 네임스페이스 **RoleBinding** 을 **rhacm-policies** 네임스페이스에 생성합니다. 다음 명령을 실행합니다.*

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

- *관리 클러스터의 정책 상태를 보려면 허브 클러스터의 관리 클러스터 네임스페이스에서 정책을 볼 수 있는 권한이 필요합니다. **OpenShift view ClusterRole** 을 통해와 같은 보기 액세스 권한이 없는 경우 다음 명령을 사용하여 정책에 대한 보기 액세스 권한을 사용하여 **rhacm- view -policy** 와 같은 **ClusterRole** 을 생성합니다.*

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

- *새 **ClusterRole** 을 관리 클러스터 네임스페이스에 바인딩하려면 다음 명령을 실행하여 네임스페이스 **RoleBinding** 을 생성합니다.*

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

#### *1.2.2.1. 거버넌스 라이프사이클을 위한 콘솔 및 API RBAC 테이블*

*거버넌스 라이프사이클을 위해 다음 콘솔 및 **API RBAC** 테이블을 확인합니다.*

*표 **1.4.** 거버넌스 라이프사이클을 위한 콘솔 **RBAC** 테이블*

| 리소스 | 관리자 | edit | view |
|---|---|---|---|
| Policies | 생성, 읽기, 업데이트, 삭제 | 읽기, 업데이트 | 읽기 |
| PlacementBindings | 생성, 읽기, 업데이트, 삭제 | 읽기, 업데이트 | 읽기 |
| 배치 | 생성, 읽기, 업데이트, 삭제 | 읽기, 업데이트 | 읽기 |
| PlacementRules (더 이상 사용되지 않음) | 생성, 읽기, 업데이트, 삭제 | 읽기, 업데이트 | 읽기 |
| PolicyAutomations | 생성, 읽기, 업데이트, 삭제 | 읽기, 업데이트 | 읽기 |

*표 **1.5.** 거버넌스 라이프사이클을 위한 **API RBAC** 테이블*

| API | 관리자 | edit | view |
|---|---|---|---|
| **policies.policy.open-cluster-management.io** | 생성, 읽기, 업데이트, 삭제 | 읽기, 업데이트 | 읽기 |
| **placementbindings.policy.open-cluster-management.io** | 생성, 읽기, 업데이트, 삭제 | 읽기, 업데이트 | 읽기 |
| **policyautomations.policy.open-cluster-management.io** | 생성, 읽기, 업데이트, 삭제 | 읽기, 업데이트 | 읽기 |

### *1.2.3. 관찰 가능성 RBAC*

*관리 클러스터의 관찰 가능 지표를 보려면 **hub** 클러스터에서 해당 관리 클러스터에 대한 보기 액세스 권한이 있어야 합니다. 다음 관찰 기능 목록을 확인합니다.*

- *관리되는 클러스터 메트릭에 액세스합니다.*

  ***hub** 클러스터에서 관리 클러스터의 **view** 역할에 할당되지 않은 경우 사용자는 관리 클러스*

터 메트릭에 대한 액세스가 거부됩니다. 다음 명령을 실행하여 관리 클러스터 네임스페이스에서 **managedClusterView** 역할을 생성할 권한이 있는지 확인합니다.

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

클러스터 관리자는 관리 클러스터 네임스페이스에서 **managedClusterView** 역할을 생성합니다. 다음 명령을 실행합니다.

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

그런 다음 역할 바인딩을 생성하여 역할을 사용자에게 적용하고 바인딩합니다. 다음 명령을 실행합니다.

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

- 리소스를 검색합니다.

  사용자가 리소스 유형에 액세스할 수 있는지 확인하려면 다음 명령을 사용합니다.

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

  참고: **& lt;resource-type>**은 복수형이어야 합니다.

- **Grafana**에서 관찰 가능한 데이터를 보려면 관리 클러스터의 동일한 네임스페이스에 **RoleBinding** 리소스가 있어야 합니다.

  다음 **RoleBinding** 예제를 확인합니다.

  ```
  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
```

*자세한 내용은 역할 바인딩 정책을 참조하십시오. 관찰 기능을 구성하려면 사용자 지정을 참조하십시오.*

#### *1.2.3.1. 관찰 가능 라이프사이클을 위한 콘솔 및 API RBAC 테이블*

*관찰 기능 구성 요소를 관리하려면 다음 API RBAC 표를 참조하십시오.*

*표 1.6. 관찰성을 위한 API RBAC 테이블*

| API | 관리자 | edit | view |
|---|---|---|---|
| **multiclusterobservabilities.observability.open-cluster-management.io** | 생성, 읽기, 업데이트 및 삭제 | 읽기, 업데이트 | 읽기 |
| **searchcustomizations.search.open-cluster-management.io** | 생성, get, list, watch, update, delete, patch | - | - |
| **policyreports.wgpolicyk8s.io** | get, list, watch | get, list, watch | get, list, watch |

*클러스터 보안에 대한 자세한 내용은 위험 및 규정 준수를 참조하십시오.*