


# Custom RBAC Role



- Create Custom Azure RBAC role for AKS
- Assign Azure RBAC role to Namespace



# AKS authentication & authorization options

 **aks-cluster** | Cluster configuration

Kubernetes service

Search

Namespaces

Workloads

Services and ingresses

Storage

Configuration

Custom resources

Events

Run command

Settings

Node pools

Cluster configuration

Networking

Extensions + applications

Backup (preview)

Troubleshoot

upgrade only the control plane or to also upgrade all node pools. To upgrade individual node pools, go to the 'Node pools' menu item instead.

[Learn more about upgrading your AKS cluster](#)  
[View the Kubernetes changelog](#)  
[View the AKS changelog](#)

Kubernetes version

1.26.6

Manual upgrade

[Upgrade version](#)

AKS pricing tier

Enable secret store CSI driver

Authentication and Authorization

Choose between local accounts or Azure AD needs. [Learn more](#)

Authentication and Authorization

Azure AD authentication with Kubernetes RBAC

Use Azure AD for authentication and Kubernetes native RBAC for authorization.

Azure AD authentication with Azure RBAC

Use Azure role assignments for authorization checks on the cluster.

Local accounts with Kubernetes RBAC

Enabling Azure AD authentication is an irreversible action.

Azure AD authentication with Azure RBAC

Kubernetes local accounts

☐

# Azure RBAC built-in roles for AKS

Azure provides **built-in** roles for AKS.

Could be applied on **cluster level** or at **namespace level**.

| <input type="checkbox"/> Name ↑↓  | Description ↑↓  |
|---|---|
| <input type="checkbox"/> Azure Kubernetes Service Cluster Admin Role      | List cluster admin credential action.   |
| <input type="checkbox"/> Azure Kubernetes Service Cluster Monitoring User | List cluster monitoring user credential action.   |
| <input type="checkbox"/> Azure Kubernetes Service Cluster User Role       | List cluster user credential action.  |
| <input type="checkbox"/> Azure Kubernetes Service Contributor Role        | Grants access to read and write Azure Kubernetes Service clusters   |
| <input type="checkbox"/> Azure Kubernetes Service RBAC Admin              | Lets you manage all resources under cluster/namespace, except update or delete resource quotas and namespaces.            |
| <input type="checkbox"/> Azure Kubernetes Service RBAC Cluster Admin      | Lets you manage all resources in the cluster.   |
| <input type="checkbox"/> Azure Kubernetes Service RBAC Reader             | Allows read-only access to see most objects in a namespace. It does not allow viewing roles or role bindings. This role.. |
| <input type="checkbox"/> Azure Kubernetes Service RBAC Writer             | Allows read/write access to most objects in a namespace.This role does not allow viewing or modifying roles or role b..   |
| <input type="checkbox"/> Kubernetes Agentless Operator                    | Grants Microsoft Defender for Cloud access to Azure Kubernetes Services   |

# View roles in Portal

## Azure Kubernetes Service RBAC Writer

BuiltInRole

Permissions JSON Assignments

**Description:** Allows read/write access to most objects in a namespace.This role does not allow viewing or modifying roles or role bindings. However, this role allows accessing Secrets and running Pods as any ServiceAccount in the namespace, so it can be used to gain the API access levels of any ServiceAccount in the namespace. Applying this role at cluster scope will give access across all namespaces.

Search permissions

Type : All

☒ Actions ☐ DataActions

Showing 30 of 30 permissions

| Type                    | Permissions   | Description   |
|-------------------------|---|---|
| Microsoft.Authorization |   |   |
| Read                    | Get administrator ⓘ   | Reads the administrators for the subscription.                |
| Read                    | Get administrator operation statuses ⓘ                      | Gets the administrator opeation statuses of the subscription. |
| Read                    | Get deny assignment ⓘ                                       | Get information about a deny assignment.                      |
| Read                    | Read the information about diagnostic settings categories ⓘ | Get the information about diagnostic settings categories      |
| Read                    | Get information about diagnostics settings ⓘ                | Read the information about diagnostics settings               |
| Read                    | Get Role eligibility schedule instance ⓘ                    | Gets the role eligibility schedule instances at given scope.  |
| Read                    | Get management locks ⓘ                                      | Gets locks at the specified scope.                            |
| Read                    | Get operations ⓘ  | Gets the list of operations                                   |
| Read                    | List permissions ⓘ  | Lists all the permissions the caller has at a given scope.    |
| Read                    | Get policy assignment ⓘ                                     | Get information about a policy assignment.                    |

```
az role definition list --name "Azure Kubernetes Service RBAC Writer"
```

```
"roleName": "Azure Kubernetes Service RBAC Writer",  
"permissions": [  
  {  
    "actions": [  
      "Microsoft.Resources/subscriptions/read",  
      "Microsoft.Resources/subscriptions/resourceGroups/read"  
    ],  
    "dataActions": [  
      "Microsoft.ContainerService/managedClusters/apps/deployments/*",  
      "Microsoft.ContainerService/managedClusters/batch/jobs/*",  
      "Microsoft.ContainerService/managedClusters/secrets/*",  
      "Microsoft.ContainerService/managedClusters/configmaps/*",  
      "Microsoft.ContainerService/managedClusters/extensions/ingresses/*",  
      "Microsoft.ContainerService/managedClusters/extensions/networkpolicies/*",  
      "Microsoft.ContainerService/managedClusters/networking.k8s.io/  
      "Microsoft.ContainerService/managedClusters/pods/*",  
    ],  
    "notActions": [],  
    "notDataActions": []  
  }  
],  
...
```

# Azure RBAC roles vs Kubernetes RBAC

```
"roleName": "Azure Kubernetes Service Pod Reader",
"permissions": [
{
  "actions": [
    "Microsoft.Resources/subscriptions/read",
  ],
  "dataActions": [
    "Microsoft.ContainerService/managedClusters/pods/*",
  ],
  "notActions": [],
  "notDataActions": []
}
...
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: pod-reader-role
  namespace: my-namespace
rules:
- apiGroups:
  - ""
  resources:
  - pods
  verbs:
  - get
  - list
  - watch
```

# Creating and assigning custom RBAC role for AKS

```
az role definition create --role-definition deployment-reader.json
{
  "Name": "AKS Deployment Reader",
  "Description": "Lets you view all deployments in cluster/namespace.",
  "Actions": [],
  "NotActions": [],
  "DataActions": [
    "Microsoft.ContainerService/managedClusters/apps/deployments/read"
  ],
  "NotDataActions": [],
  "assignableScopes": [
    "/subscriptions/82f6d75e-85f4-434a-ab74-xxxxxxx"
  ]
}
```

```
az role assignment create --role "AKS Deployment Reader"
--assignee $USER_ID
--scope $AKS_ID/namespaces/kube-system
```