

Configure Security by Using the Azure Kubernetes Service

Understand the scenario

You are an Azure® administrator. You need to deploy secure, containerized applications by using the Azure Kubernetes Service (AKS). First, you will create an AKS cluster, and then you will assign a role-based access control (RBAC) role to the cluster. Next, you will connect to the AKS cluster as the administrator by using Azure Cloud Shell. Finally, you will deploy an application as a developer in the AKS cluster, and then you will verify the security of the cluster.

Understand your environment

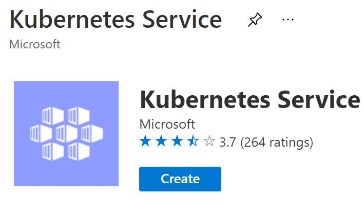
You will be using an Azure resource group named corp-datalod26434135 that initially contains no resources.

# **Deploy an AKS cluster that uses RBAC**

* Sign in to the Azure portal
* Create an Azure Kubernetes Service (AKS) cluster by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434135** |
| Cluster preset configuration | **Standard** |
| Kubernetes cluster name | aks |
| Availability zones | **None** |
| Node size | **Standard DS2\_v2** - 2 vcpus, 8 GiB memory |
| Node count (range end value) | 2 |
| Authentication and Authorization | **Local accounts with Kubernetes RBAC** |
| Container monitoring | **Disabled** |

* Expand this hint for guidance on creating an AKS cluster.
  + On the Azure portal home page, select **Create a resource** to display the Azure Marketplace.
  + In Search services and marketplace, search for and select Kubernetes Service.
  + On the Kubernetes Service page, select **Create**.



* + On the Create Kubernetes cluster blade, on the Basics page, in Resource group, select **corp-datalod26434135**.
  + In Cluster preset configuration, ensure that **Standard** is selected.
  + In Kubernetes cluster name, enter aks.
  + In Availability zones, clear the **1**, **2**, and **3** check boxes, and then ensure that **None** is selected.
  + In Primary node pool, In Node size, ensure that **Standard DS2 v2** is selected.
  + On the Basics page, in Node count, in the range end value, enter 2.
  + On the Access page, in Authentication and Authorization, select **Local accounts with Kubernetes RBAC**.
  + On the Integrations page, in Container monitoring, select **Disabled**.
  + Select **Review + create**, review the specifications, and then select **Create** to create the Kubernetes cluster.

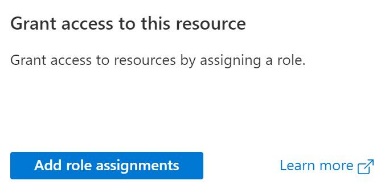
It will take approximately 3–5 minutes to deploy the AKS cluster.

[Azure Kubernetes Service](https://docs.microsoft.com/en-us/azure/aks/intro-kubernetes) creates a fully managed hosting cluster for containerized applications. AKS supports the open source Kubernetes platform.

* Assign the Azure Kubernetes Service Cluster User Role to the User1-26434135@cloudslice.onmicrosoft.com user at the resource scope.

Expand this hint for guidance on assigning a role to a user.

* + On the Azure portal home page, select **All resources**, and then select **aks**.
  + On the aks resource menu, select **Access control (IAM)**.
  + On the Access control (IAM) page, in Grant access to this resource, select **Add role assignment**.



* + On the Add role assignment blade, on the Role page, search for and select Azure Kubernetes Service Cluster User Role, and then select **Next**.
  + On the Members page, select **Select members**.
  + On the Select members blade, search for and select User1-26434135@cloudslice.onmicrosoft.com, and then select **Select**.
  + Select **Next**, and then select **Review + assign**.

Ignore any authorization errors when viewing the Kubernetes Service blade. This is expected as the AKS cluster will be used for testing only.



## Check your work

* Confirm that you created an AKS cluster named aks.
* Confirm that you assigned the Azure Kubernetes Service Cluster User Role to a user at the resource scope.

# **Connect to the AKS cluster as the administrator**

* Launch an Azure **Cloud Shell** **Bash** session by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434135** |
| Cloud Shell region | **East US** |
| Storage account | cs26434135 |
| File share | cloudshell |

* Expand this hint for guidance on creating an Azure Cloud Shell session.
  + On the Azure portal page header, in the global controls section, select the **Cloud Shell** icon.



* + On the Welcome to Azure Cloud Shell page, select **Bash**.
  + On the You have no storage mounted page, select **Show advanced settings**.
  + In Resource group, ensure that **Use existing** is selected, and then ensure that **corp-datalod26434135** is selected.
  + In Cloud Shell region, select **East US**.
  + In Storage account, ensure that **Create new** is selected, and then enter cs26434135.
  + In File share, ensure that **Create new** is selected, and then enter cloudshell,
  + Select **Create storage**, and then wait for the Cloud Shell session to initialize.

It will take approximately 1–2 minutes to initialize the Cloud Shell.

* Connect to the aks cluster in the corp-datalod26434135 resource group as admin by using the [az aks get-credentials](https://docs.microsoft.com/en-us/cli/azure/aks?view=azure-cli-latest#az_aks_get_credentials) Azure command-line interface (Azure CLI) command.

Expand this hint for guidance on connecting to the AKS cluster.

* + Run the following command to connect to the cluster:

az aks get-credentials --resource-group corp-datalod26434135 --name aks --admin

Cloud Shell does not support the keyboard shortcut Ctrl+V for paste. Instead, select the command prompt, and then use **Ctrl+Shift+V** to paste.

* Verify that the current context of the connection to the cluster is **aks-admin** by using the [kubectl config](https://kubernetes.io/docs/reference/kubectl/cheatsheet/#kubectl-context-and-configuration) command.

Expand this hint for guidance on verifying the current context of the connection to the cluster.

* + Run the following command to verify that the current context of the connection to the cluster is aks-admin:

kubectl config current-context

* Display a list of the cluster nodes by using the [kubectl get](https://kubernetes.io/docs/reference/kubectl/cheatsheet/#viewing-finding-resources) command.

Expand this hint for guidance on displaying a list of the cluster nodes.

* + Run the following command to display a list of the cluster nodes:

kubectl get nodes

There should be two nodes in the cluster.

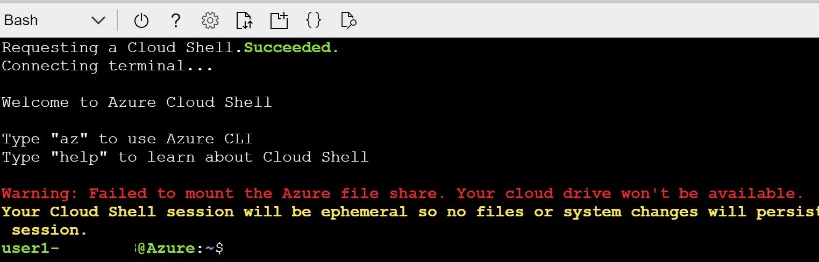
## Check your work

* Confirm that you connected to the aks cluster by using administrator credentials.
* Confirm that you displayed a list of the cluster nodes.

# **Deploy a container in the AKS cluster as a non-administrative user**

* Open an InPrivate or incognito browser window, go to the Azure portal at https://portal.azure.com/, and then sign in
* Launch a **Cloud Shell** **Bash** session by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-datalod26434135** |
| Cloud Shell region | **East US** |
| Storage account | **cs26434135** |
| File share | cloudshell |

* Ignore any file share mount warnings. This is expected because the user has read-only access in the Azure portal. You can access the AKS cluster as a non-administrative user.
* 
* Connect to the aks cluster in the corp-datalod26434135 resource group by using the az aks get-credentials CLI command.

Expand this hint for guidance on connecting to the AKS cluster.

* + Run the following command to connect to the aks cluster:

az aks get-credentials --resource-group corp-datalod26434135 --name aks

* Verify that the current context of the connection to the cluster is **aks** by using the kubectl config command.

Expand this hint for guidance on verifying the current context of the connection to the cluster.

* + Run the following command to verify that the current context of the connection to the cluster is aks:

kubectl config current-context

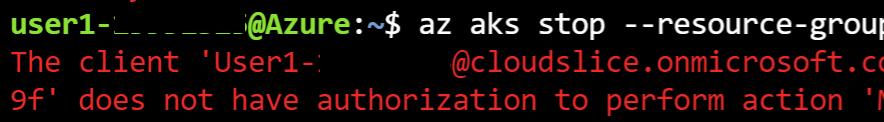
* Attempt to stop the aks cluster in the corp-datalod26434135 resource group by using the [az aks stop](https://docs.microsoft.com/en-us/cli/azure/aks?view=azure-cli-latest#az_aks_stop) CLI command.

Expand this hint for guidance on attempting to stop a cluster.

* + Run the following command to attempt to stop the cluster:

az aks stop --resource-group corp-datalod26434135 --name aks

This operation should fail as you are not authorized to stop the AKS cluster as a non-admin user.



* Deploy an application named nginx-26434135 that uses the nginx container image from Docker Hub by using the [kubectl create deployment](https://kubernetes.io/docs/reference/kubectl/cheatsheet/#creating-objects) command.

Expand this hint for guidance on deploying an application.

* + Run the following command to deploy the application:

kubectl create deployment nginx-26434135 --image=nginx

* Verify that an AKS pod was created for the application by using the kubectl get command.

Expand this hint for guidance on verifying that an AKS pod was created.

* + Run the following command to verify that a pod was created:

kubectl get pods

There should be one pod running in the AKS cluster.

* Expose the pod in the nginx-26434135 deployment to the internet for testing by using the [kubectl expose deployment](https://kubernetes.io/docs/reference/kubectl/cheatsheet/#updating-resources) command.

Expand this hint for guidance on exposing a pod in a deployment to the internet.

* + Run the following command to expose the nginx-26434135 deployment to the internet:

kubectl expose deployment nginx-26434135 --port=80 --type=LoadBalancer

* Run the following command to identify the public IP address of the application, and then re-run the command until the value in the **EXTERNAL-IP** column for **nginx-26434135** changes from **<pending>** to a public IP address:

kubectl get services

* Record the public IP address in the following **Public IP Address** text box:

**Public IP Address**  


* Go to the public IP address http://<PublicIP>, and then verify that the browser displays **Welcome to nginx!**



## Check your work

* Confirm that you connected to the AKS cluster by using non-administrative credentials.
* Confirm that you deployed an application that uses the nginx container image to the AKS cluster.
* Confirm that you accessed the nginx application in a browser.

# **Summary**

Congratulations, you have completed the **Configure Security by Using the Azure Kubernetes Service** challenge.

You have accomplished the following:

* Deployed an AKS cluster.
* Enabled RBAC on an AKS cluster.
* Connected to an AKS cluster as an administrator.
* Deployed an application in the AKS cluster as a non-administrative user.