

Contents

Azure Kubernetes Service (AKS)

Overview

[About AKS](#)

[Quotas and regional limits](#)

[Supported Kubernetes version](#)

[Add-ons, extensions, and other integrations](#)

[Solution architectures](#)

Quickstarts

[Deploy a Linux-based AKS Cluster](#)

[Use the Azure CLI](#)

[Use Azure PowerShell](#)

[Use the Azure portal](#)

[Use Bicep](#)

[Use ARM template](#)

[Deploy a Windows-based AKS Cluster](#)

[Use the Azure CLI](#)

[Use Azure PowerShell](#)

Develop applications

[Develop with Helm](#)

[Develop with Dapr](#)

Subscribe to AKS events with Event Grid

Tutorials

[1 - Prepare application for AKS](#)

[2 - Create container registry](#)

[3 - Create Kubernetes cluster](#)

[4 - Run application](#)

[5 - Scale application](#)

[6 - Update application](#)

[7 - Upgrade cluster](#)

Security

Configure application to use workload identity

Concepts

Core concepts

Security

Security Baseline

Container Security

Security controls by Azure Policy

Compliance

CIS Baseline overview

CIS Kubernetes benchmark

CIS Ubuntu benchmark

Access and identity

Networking

Storage

Scale

Node auto-repair

Multi-instance GPU Node pool

Service meshes

Sustainable software engineering

Dapr

GitOps

Best practices

Overview

Baseline architecture for an AKS cluster

Security

Authentication and authorization

Cluster security

Container image management

For cluster operators

Multi-tenancy and cluster isolation

Basic scheduler features

- Run AKS clusters at scale
- Advanced scheduler features
- Networking
- Storage
- Business continuity (BC) and disaster recovery (DR)
- For application developers
 - Resource management
 - Pod security

Migrate to AKS

- Plan and execute a migration
- Spring Boot
- Tomcat
- Wildfly
- WebLogic
- WebSphere
- JBoss EAP
- Java web app containerization and migration
- ASP.NET app containerization and migration

How-to guides

- Cluster operations
 - Abort long running operations
 - Automatically upgrade an AKS cluster
 - Configure an AKS cluster
 - Custom node configuration
 - Use cluster snapshots (preview)
 - Integrate ACR with an AKS cluster
 - Use Vertical Pod Autoscaler (preview)
 - Scale an AKS cluster
 - Stop/Deallocate nodes with Scale-down Mode
 - Stop an AKS cluster
 - Use planned maintenance (preview)
 - Planned Maintenance for AKS weekly releases (preview)

[Cloud Controller Manager](#)

[Upgrade an AKS cluster](#)

[Use Uptime SLA](#)

[Use Draft \(preview\)](#)

[Use proximity placement groups](#)

[Upgrade the node image](#)

[Upgrade the node image automatically with GitHub Actions](#)

[Process node OS updates](#)

[Connect to cluster nodes](#)

[Create virtual nodes](#)

[Use virtual nodes](#)

[Use the Azure CLI](#)

[Use the Azure portal](#)

[Use Cluster Autoscaler](#)

[Use Availability Zones](#)

[Use node pools](#)

[Node pool snapshot](#)

[Use Dedicated Hosts with AKS \(preview\)](#)

[Use multiple node pools](#)

[Use spot node pools](#)

[Use Confidential Virtual Machines](#)

[Use system node pools](#)

[Use WebAssembly System Interface \(WASI\) node pools](#)

[Start/stop node pools](#)

[Resize node pools](#)

[Use the Mariner container host](#)

[Deploy AKS with Terraform](#)

[Azure portal Kubernetes resource view](#)

[Use tags](#)

[Use labels](#)

[Security and authentication](#)

[Overview of Defender for Containers](#)

[Enable Defender for Containers](#)

[Build security](#)

[Scan images in your CI/CD Workflow](#)

[Registry security](#)

[Scanning images in ACR registries](#)

[Cluster security](#)

[Create service principal](#)

[Use managed identities](#)

[Remove vulnerable images with ImageCleaner \(preview\)](#)

[Limit access to cluster configuration file](#)

[Define API server authorized IP ranges](#)

[Use KMS etcd encryption](#)

[Update cluster credentials](#)

[Enable Azure Active Directory integration](#)

[AKS-managed Azure AD](#)

[Azure AD integration \(legacy\)](#)

[Enable GMSA integration](#)

[Use Azure RBAC for Kubernetes authorization](#)

[Use Kubernetes RBAC with Azure AD integration](#)

[Use custom certificate authorities \(preview\)](#)

[Rotate certificates](#)

[Use Azure Policy](#)

[Control deployments with Azure Policy](#)

[Node security](#)

[BYOK for disks](#)

[Enable host-based encryption](#)

[Enable FIPS](#)

[Application security](#)

[Workload identity \(preview\)](#)

[Overview](#)

[Deploy and configure cluster](#)

[Modernize your app with workload identity sidecar](#)

- [Use Azure AD pod identity \(preview\)](#)
- [Secure pod traffic with network policies](#)
- [Use pod security policies \(preview\)](#)
- [Use Pod Security Admission](#)
- [Secrets Store CSI Driver](#)
 - [Secrets Store CSI Driver configuration](#)
 - [Provide Azure Key Vault access](#)
 - [Configure TLS for NGINX ingress controller](#)
- [Configure private clusters](#)
 - [Create a private cluster](#)
 - [Access a private cluster remotely](#)
- [Configure networking](#)
 - [Create or use existing virtual network](#)
 - [Use kubenet](#)
 - [Use kubenet with dual-stack networking](#)
 - [Use Azure-CNI](#)
 - [Use Azure-CNI Overlay \(Preview\)](#)
- [Use API Server VNet Integration](#)
- [Bring your own CNI](#)
- [Use Azure CNI Powered by Cilium \(Preview\)](#)
- [Create an internal load balancer](#)
 - [Use a Standard Load Balancer](#)
 - [Use kube-proxy configuration \(IPVS\)](#)
 - [Use a static IP address and DNS label](#)
 - [Use an HTTP proxy](#)
- [Ingress](#)
 - [Use ingress-nginx](#)
 - [Create an ingress controller](#)
 - [Use TLS with an ingress controller](#)
 - [Use HTTP application routing](#)
 - [Enable the AGIC add-on for an existing AKS cluster](#)
- [Egress](#)

- [Restrict and control cluster egress traffic](#)
- [Use a user defined route for egress](#)
- [Managed NAT Gateway](#)
- [Customize CoreDNS](#)
- [Configure storage](#)
 - [CSI storage drivers](#)
 - [CSI storage drivers overview](#)
 - [Azure Disks CSI driver](#)
 - [Azure Files CSI driver](#)
 - [Azure Blob CSI driver](#)
 - [Azure NetApp Files](#)
 - [Use Azure Ultra Disks](#)
 - [Configure storage](#)
 - [Azure Blob - dynamic](#)
 - [Azure Blob - static](#)
 - [Azure Disks - dynamic](#)
 - [Azure Disks - static](#)
 - [Azure Files - dynamic](#)
 - [Azure Files - static](#)
 - [Azure HPC Cache](#)
 - [NFS Server - static](#)
- [Monitoring and logging](#)
 - [Monitor AKS](#)
 - [Monitor reference](#)
 - [View the kubelet logs](#)
 - [View container data real-time](#)
- [Use Windows Server containers](#)
 - [Connect remotely](#)
 - [Use HostProcess containers](#)
 - [Windows Server containers FAQ](#)
 - [Upgrade from Windows Server 2019 to 2022](#)
 - [Create Dockerfiles for Windows Server containers](#)

[Optimize Dockerfiles for Windows Server containers](#)

[Develop and run applications](#)

[Use Bridge to Kubernetes with Visual Studio Code](#)

[Use Bridge to Kubernetes with Visual Studio](#)

[Install existing applications with Helm](#)

[Use OpenFaaS](#)

[Use GPUs](#)

[Build Django app with PostgreSQL](#)

[Build Java app with WebSphere Liberty or Open Liberty](#)

[Build WordPress app with MySQL](#)

[Use Azure API Management](#)

[Use Dapr](#)

[How to use the Dapr extension](#)

[Migrate from Dapr OSS](#)

[Troubleshoot the Dapr extension](#)

[Use GitOps](#)

[Deploy Kubernetes applications from Azure Marketplace](#)

[Deploy the Open Service Mesh AKS add-on](#)

[About Open Service Mesh](#)

[Use the Azure CLI](#)

[Use Bicep template](#)

[Install the OSM CLI](#)

[Open Service Mesh integrations](#)

[Troubleshoot Open Service Mesh](#)

[Uninstall the Open Service Mesh AKS add-on](#)

[Track releases and region availability](#)

[Deploy the Kubernetes Event-driven Autoscaler \(KEDA\) add-on \(preview\)](#)

[About Kubernetes Event-driven Autoscaler \(KEDA\)](#)

[Use ARM template](#)

[Use Azure CLI](#)

[Kubernetes Event-driven Autoscaler \(KEDA\) integrations](#)

[Troubleshoot Kubernetes Event-driven Autoscaler \(KEDA\)](#)

[Use Web Application Routing \(preview\)](#)

[Use cluster extensions](#)

[DevOps](#)

[Use Ansible to create AKS clusters](#)

[Jenkins continuous deployment](#)

[Azure DevOps Project](#)

[Deployment Center Launcher](#)

[GitHub Actions for Kubernetes](#)

[Configure automated deployments \(preview\)](#)

[CI/CD with Azure Pipelines](#)

[Reference](#)

[Azure CLI](#)

[REST](#)

[PowerShell](#)

[.NET](#)

[Python](#)

[Java](#)

[Node.js](#)

[Resource Manager template](#)

[Azure Policy built-ins](#)

[Resources](#)

[Build your skills with Microsoft Learn training](#)

[Region availability](#)

[Pricing](#)

[Support policies](#)

[Azure Roadmap](#)

[AKS Roadmap](#)

[Stack Overflow](#)

[Videos](#)

[FAQ](#)

[Support and troubleshooting](#)

Azure Kubernetes Service

10/27/2022 • 5 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) simplifies deploying a managed Kubernetes cluster in Azure by offloading the operational overhead to Azure. As a hosted Kubernetes service, Azure handles critical tasks, like health monitoring and maintenance. Since Kubernetes masters are managed by Azure, you only manage and maintain the agent nodes. Thus, AKS is free; you only pay for the agent nodes within your clusters, not for the masters.

You can create an AKS cluster using:

- [The Azure CLI](#)
- [The Azure portal](#)
- [Azure PowerShell](#)
- Using template-driven deployment options, like [Azure Resource Manager templates](#), [Bicep](#) and [Terraform](#).

When you deploy an AKS cluster, the Kubernetes master and all nodes are deployed and configured for you. Advanced networking, Azure Active Directory (Azure AD) integration, monitoring, and other features can be configured during the deployment process.

For more information on Kubernetes basics, see [Kubernetes core concepts for AKS](#).

NOTE

This service supports [Azure Lighthouse](#), which lets service providers sign in to their own tenant to manage subscriptions and resource groups that customers have delegated.

AKS also supports Windows Server containers.

Access, security, and monitoring

For improved security and management, AKS lets you integrate with Azure AD to:

- Use Kubernetes role-based access control (Kubernetes RBAC).
- Monitor the health of your cluster and resources.

Identity and security management

Kubernetes RBAC

To limit access to cluster resources, AKS supports [Kubernetes RBAC](#). Kubernetes RBAC controls access and permissions to Kubernetes resources and namespaces.

Azure AD

You can configure an AKS cluster to integrate with Azure AD. With Azure AD integration, you can set up Kubernetes access based on existing identity and group membership. Your existing Azure AD users and groups can be provided with an integrated sign-on experience and access to AKS resources.

For more information on identity, see [Access and identity options for AKS](#).

To secure your AKS clusters, see [Integrate Azure Active Directory with AKS](#).

Integrated logging and monitoring

Azure Monitor for Container Health collects memory and processor performance metrics from containers, nodes, and controllers within your AKS cluster and deployed applications. You can review both container logs

and [the Kubernetes master logs](#), which are:

- Stored in an Azure Log Analytics workspace.
- Available through the Azure portal, Azure CLI, or a REST endpoint.

For more information, see [Monitor Azure Kubernetes Service container health](#).

Clusters and nodes

AKS nodes run on Azure virtual machines (VMs). With AKS nodes, you can connect storage to nodes and pods, upgrade cluster components, and use GPUs. AKS supports Kubernetes clusters that run multiple node pools to support mixed operating systems and Windows Server containers.

For more information about Kubernetes cluster, node, and node pool capabilities, see [Kubernetes core concepts for AKS](#).

Cluster node and pod scaling

As demand for resources change, the number of cluster nodes or pods that run your services automatically scales up or down. You can adjust both the horizontal pod autoscaler or the cluster autoscaler to adjust to demands and only run necessary resources.

For more information, see [Scale an Azure Kubernetes Service \(AKS\) cluster](#).

Cluster node upgrades

AKS offers multiple Kubernetes versions. As new versions become available in AKS, you can upgrade your cluster using the Azure portal or Azure CLI. During the upgrade process, nodes are carefully cordoned and drained to minimize disruption to running applications.

To learn more about lifecycle versions, see [Supported Kubernetes versions in AKS](#). For steps on how to upgrade, see [Upgrade an Azure Kubernetes Service \(AKS\) cluster](#).

GPU-enabled nodes

AKS supports the creation of GPU-enabled node pools. Azure currently provides single or multiple GPU-enabled VMs. GPU-enabled VMs are designed for compute-intensive, graphics-intensive, and visualization workloads.

For more information, see [Using GPUs on AKS](#).

Confidential computing nodes (public preview)

AKS supports the creation of Intel SGX-based, confidential computing node pools (DCSv2 VMs). Confidential computing nodes allow containers to run in a hardware-based, trusted execution environment (enclaves). Isolation between containers, combined with code integrity through attestation, can help with your defense-in-depth container security strategy. Confidential computing nodes support both confidential containers (existing Docker apps) and enclave-aware containers.

For more information, see [Confidential computing nodes on AKS](#).

Mariner nodes

Mariner is an open-source Linux distribution created by Microsoft, and it's now available for preview as a container host on Azure Kubernetes Service (AKS). The Mariner container host provides reliability and consistency from cloud to edge across the AKS, AKS-HCI, and Arc products. You can deploy Mariner node pools in a new cluster, add Mariner node pools to your existing Ubuntu clusters, or migrate your Ubuntu nodes to Mariner nodes.

For more information, see [Use the Mariner container host on Azure Kubernetes Service \(AKS\)](#)

Storage volume support

To support application workloads, you can mount static or dynamic storage volumes for persistent data.

Depending on the number of connected pods expected to share the storage volumes, you can use storage backed by either:

- Azure Disks for single pod access, or
- Azure Files for multiple, concurrent pod access.

For more information, see [Storage options for applications in AKS](#).

Get started with dynamic persistent volumes using [Azure Disks](#) or [Azure Files](#).

Virtual networks and ingress

An AKS cluster can be deployed into an existing virtual network. In this configuration, every pod in the cluster is assigned an IP address in the virtual network, and can directly communicate with:

- Other pods in the cluster
- Other nodes in the virtual network.

Pods can also connect to other services in a peered virtual network and to on-premises networks over ExpressRoute or site-to-site (S2S) VPN connections.

For more information, see the [Network concepts for applications in AKS](#).

Ingress with HTTP application routing

The HTTP application routing add-on helps you easily access applications deployed to your AKS cluster. When enabled, the HTTP application routing solution configures an ingress controller in your AKS cluster.

As applications are deployed, publicly accessible DNS names are autoconfigured. The HTTP application routing sets up a DNS zone and integrates it with the AKS cluster. You can then deploy Kubernetes ingress resources as normal.

To get started with ingress traffic, see [HTTP application routing](#).

Development tooling integration

Kubernetes has a rich ecosystem of development and management tools that work seamlessly with AKS. These tools include Helm and the Kubernetes extension for Visual Studio Code.

Azure provides several tools that help streamline Kubernetes, such as DevOps Starter.

DevOps Starter

DevOps Starter provides a simple solution for bringing existing code and Git repositories into Azure. DevOps Starter automatically:

- Creates Azure resources (such as AKS);
- Configures a release pipeline in Azure DevOps Services that includes a build pipeline for CI;
- Sets up a release pipeline for CD; and,
- Generates an Azure Application Insights resource for monitoring.

For more information, see [DevOps Starter](#).

Docker image support and private container registry

AKS supports the Docker image format. For private storage of your Docker images, you can integrate AKS with Azure Container Registry (ACR).

To create a private image store, see [Azure Container Registry](#).

Kubernetes certification

AKS has been CNCF-certified as Kubernetes conformant.

Regulatory compliance

AKS is compliant with SOC, ISO, PCI DSS, and HIPAA. For more information, see [Overview of Microsoft Azure compliance](#).

Next steps

Learn more about deploying and managing AKS with the Azure CLI Quickstart.

[Deploy an AKS Cluster using Azure CLI](#)

Quotas, virtual machine size restrictions, and region availability in Azure Kubernetes Service (AKS)

10/27/2022 • 3 minutes to read • [Edit Online](#)

All Azure services set default limits and quotas for resources and features, including usage restrictions for certain virtual machine (VM) SKUs.

This article details the default resource limits for Azure Kubernetes Service (AKS) resources and the availability of AKS in Azure regions.

Service quotas and limits

RESOURCE	LIMIT
Maximum clusters per subscription	5000 Note: spread clusters across different regions to account for Azure API throttling limits
Maximum nodes per cluster with Virtual Machine Scale Sets and Standard Load Balancer SKU	5000 across all node-pools (default limit: 1000) Note: Running more than a 1000 nodes per cluster requires increasing the default node limit quota. Contact support for assistance.
Maximum nodes per node pool (Virtual Machine Scale Sets node pools)	1000
Maximum node pools per cluster	100
Maximum pods per node: with Kubenet networking plug-in	Maximum: 250 Azure CLI default: 110 Azure Resource Manager template default: 110 Azure portal deployment default: 30
Maximum pods per node: with Azure Container Networking Interface	Maximum: 250 Default: 30
Open Service Mesh (OSM) AKS addon	Kubernetes Cluster Version: AKS Supported Versions OSM controllers per cluster: 1 Pods per OSM controller: 1600 Kubernetes service accounts managed by OSM: 160
Maximum load-balanced kubernetes services per cluster with Standard Load Balancer SKU	300
Maximum nodes per cluster with Virtual Machine Availability Sets and Basic Load Balancer SKU	100
KUBERNETES CONTROL PLANE TIER	LIMIT
Paid tier	Automatically scales out based on the load

KUBERNETES CONTROL PLANE TIER	LIMIT
Free tier	Limited resources with inflight requests limit of 50 mutating and 100 read-only calls

Provisioned infrastructure

All other network, compute, and storage limitations apply to the provisioned infrastructure. For the relevant limits, see [Azure subscription and service limits](#).

IMPORTANT

When you upgrade an AKS cluster, extra resources are temporarily consumed. These resources include available IP addresses in a virtual network subnet or virtual machine vCPU quota.

For Windows Server containers, you can perform an upgrade operation to apply the latest node updates. If you don't have the available IP address space or vCPU quota to handle these temporary resources, the cluster upgrade process will fail. For more information on the Windows Server node upgrade process, see [Upgrade a node pool in AKS](#).

Supported VM sizes

The list of supported VM sizes in AKS is evolving with the release of new VM SKUs in Azure. Please follow the [AKS release notes](#) to stay informed of new supported SKUs.

Restricted VM sizes

VM sizes with less than 2 CPUs may not be used with AKS.

Each node in an AKS cluster contains a fixed amount of compute resources such as vCPU and memory. If an AKS node contains insufficient compute resources, pods might fail to run correctly. To ensure the required *kube-system* pods and your applications can be reliably scheduled, AKS requires nodes use VM sizes with at least 2 CPUs.

For more information on VM types and their compute resources, see [Sizes for virtual machines in Azure](#).

Region availability

For the latest list of where you can deploy and run clusters, see [AKS region availability](#).

Cluster configuration presets in the Azure portal

When you create a cluster using the Azure portal, you can choose a preset configuration to quickly customize based on your scenario. You can modify any of the preset values at any time.

PRESET	DESCRIPTION
Standard	Best if you're not sure what to choose. Works well with most applications.
Dev/Test	Best for experimenting with AKS or deploying a test application.
Cost-optimized	Best for reducing costs on production workloads that can tolerate interruptions.

PRESET	DESCRIPTION
Batch processing	Best for machine learning, compute-intensive, and graphics-intensive workloads. Suited for applications requiring fast scale-up and scale-out of the cluster.
Hardened access	Best for large enterprises that need full control of security and stability.

Next steps

You can increase certain default limits and quotas. If your resource supports an increase, request the increase through an [Azure support request](#) (for **Issue type**, select **Quota**).

Supported Kubernetes versions in Azure Kubernetes Service (AKS)

10/27/2022 • 9 minutes to read • [Edit Online](#)

The Kubernetes community releases minor versions roughly every three months. Recently, the Kubernetes community has [increased the support window for each version from 9 months to 12 months](#), starting with version 1.19.

Minor version releases include new features and improvements. Patch releases are more frequent (sometimes weekly) and are intended for critical bug fixes within a minor version. Patch releases include fixes for security vulnerabilities or major bugs.

Kubernetes versions

Kubernetes uses the standard [Semantic Versioning](#) versioning scheme for each version:

[major].[minor].[patch]

Example:

1.17.7
1.17.8

Each number in the version indicates general compatibility with the previous version:

- **Major versions** change when incompatible API updates or backwards compatibility may be broken.
- **Minor versions** change when functionality updates are made that are backwards compatible to the other minor releases.
- **Patch versions** change when backwards-compatible bug fixes are made.

Aim to run the latest patch release of the minor version you're running. For example, your production cluster is on `1.17.7`. `1.17.8` is the latest available patch version available for the `1.17` series. You should upgrade to `1.17.8` as soon as possible to ensure your cluster is fully patched and supported.

Alias minor version

NOTE

Alias minor version requires Azure CLI version 2.37 or above. Use `az upgrade` to install the latest version of the CLI.

Azure Kubernetes Service allows for you to create a cluster without specifying the exact patch version. When creating a cluster without designating a patch, the cluster will run the minor version's latest GA patch. For example, if you create a cluster with `1.21`, your cluster will be running `1.21.7`, which is the latest GA patch version of `1.21`.

When upgrading by alias minor version, only a higher minor version is supported. For example, upgrading from `1.14.x` to `1.14` will not trigger an upgrade to the latest GA `1.14` patch, but upgrading to `1.15` will trigger an upgrade to the latest GA `1.15` patch.

To see what patch you are on, run the `az aks show --resource-group myResourceGroup --name myAKSCluster`

command. The property `currentKubernetesVersion` shows the whole Kubernetes version.

```
{  
    "apiServerAccessProfile": null,  
    "autoScalerProfile": null,  
    "autoUpgradeProfile": null,  
    "azurePortalFqdn": "myaksclust-myresourcegroup.portal.hcp.eastus.azmk8s.io",  
    "currentKubernetesVersion": "1.21.7",  
}
```

Kubernetes version support policy

AKS defines a generally available version as a version enabled in all SLO or SLA measurements and available in all regions. AKS supports three GA minor versions of Kubernetes:

- The latest GA minor version that is released in AKS (which we'll refer to as N).
- Two previous minor versions.
 - Each supported minor version also supports a maximum of two (2) stable patches.

AKS may also support preview versions, which are explicitly labeled and subject to [Preview terms and conditions](#).

NOTE

AKS uses safe deployment practices which involve gradual region deployment. This means it may take up to 10 business days for a new release or a new version to be available in all regions.

The supported window of Kubernetes versions on AKS is known as "N-2": (N (Latest release) - 2 (minor versions)).

For example, if AKS introduces *1.17.a* today, support is provided for the following versions:

NEW MINOR VERSION	SUPPORTED VERSION LIST
1.17.a	1.17.a, 1.17.b, 1.16.c, 1.16.d, 1.15.e, 1.15.f

Where ".letter" is representative of patch versions.

When a new minor version is introduced, the oldest minor version and patch releases supported are deprecated and removed. For example, the current supported version list is:

```
1.17.a  
1.17.b  
1.16.c  
1.16.d  
1.15.e  
1.15.f
```

AKS releases *1.18.**, removing all the *1.15.** versions out of support in 30 days.

NOTE

If customers are running an unsupported Kubernetes version, they will be asked to upgrade when requesting support for the cluster. Clusters running unsupported Kubernetes releases are not covered by the [AKS support policies](#).

In addition to the above, AKS supports a maximum of two **patch** releases of a given minor version. So given the following supported versions:

Current Supported Version List

1.17.8, 1.17.7, 1.16.10, 1.16.9

If AKS releases `1.17.9` and `1.16.11`, the oldest patch versions are deprecated and removed, and the supported version list becomes:

New Supported Version List

1.17.*9*, 1.17.*8*, 1.16.*11*, 1.16.*10*

Supported `kubectl` versions

You can use one minor version older or newer of `kubectl` relative to your *kube-apiserver* version, consistent with the [Kubernetes support policy for kubectl](#).

For example, if your *kube-apiserver* is at `1.17`, then you can use versions `1.16` to `1.18` of `kubectl` with that *kube-apiserver*.

To install or update `kubectl` to the latest version, run:

- [Azure CLI](#)
- [Azure PowerShell](#)

```
az aks install-cli
```

Release and deprecation process

You can reference upcoming version releases and deprecations on the [AKS Kubernetes Release Calendar](#).

For new **minor** versions of Kubernetes:

- AKS publishes a pre-announcement with the planned date of a new version release and respective old version deprecation on the [AKS Release notes](#) at least 30 days prior to removal.
- AKS uses [Azure Advisor](#) to alert users if a new version will cause issues in their cluster because of deprecated APIs. Azure Advisor is also used to alert the user if they are currently out of support.
- AKS publishes a [service health notification](#) available to all users with AKS and portal access, and sends an email to the subscription administrators with the planned version removal dates.

NOTE

To find out who is your subscription administrators or to change it, please refer to [manage Azure subscriptions](#).

- Users have **30 days** from version removal to upgrade to a supported minor version release to continue receiving support.

For new **patch** versions of Kubernetes:

- Because of the urgent nature of patch versions, they can be introduced into the service as they become available. Once available, patches will have a two month minimum lifecycle.

- In general, AKS does not broadly communicate the release of new patch versions. However, AKS constantly monitors and validates available CVE patches to support them in AKS in a timely manner. If a critical patch is found or user action is required, AKS will notify users to upgrade to the newly available patch.
- Users have **30 days** from a patch release's removal from AKS to upgrade into a supported patch and continue receiving support. However, you will **no longer be able to create clusters or node pools once the version is deprecated/removed**.

Supported versions policy exceptions

AKS reserves the right to add or remove new/existing versions with one or more critical production-impacting bugs or security issues without advance notice.

Specific patch releases may be skipped or rollout accelerated, depending on the severity of the bug or security issue.

Azure portal and CLI versions

When you deploy an AKS cluster in the portal, with the Azure CLI, or with Azure PowerShell, the cluster defaults to the N-1 minor version and latest patch. For example, if AKS supports *1.17.a*, *1.17.b*, *1.16.c*, *1.16.d*, *1.15.e*, and *1.15.f*, the default version selected is *1.16.c*.

- [Azure CLI](#)
- [Azure PowerShell](#)

To find out what versions are currently available for your subscription and region, use the `az aks get-versions` command. The following example lists the available Kubernetes versions for the *EastUS* region:

```
az aks get-versions --location eastus --output table
```

AKS Kubernetes Release Calendar

For the past release history, see [Kubernetes](#).

K8S VERSION	UPSTREAM RELEASE	AKS PREVIEW	AKS GA	END OF LIFE
1.21	Apr-08-21	May 2021	Jul 2021	1.24 GA
1.22	Aug-04-21	Sept 2021	Dec 2021	1.25 GA
1.23	Dec 2021	Jan 2022	Apr 2022	1.26 GA
1.24	Apr-22-22	May 2022	Jul 2022	1.27 GA
1.25	Aug 2022	Oct 2022	Dec 2022	1.28 GA
1.26	Dec 2022	Jan 2023	Mar 2023	1.29 GA

FAQ

How does Microsoft notify me of new Kubernetes versions?

The AKS team publishes pre-announcements with planned dates of the new Kubernetes versions in our documentation, our [GitHub](#) as well as emails to subscription administrators who own clusters that are going to fall out of support. In addition to announcements, AKS also uses [Azure Advisor](#) to notify the customer inside the

Azure portal to alert users if they are out of support, as well as alerting them of deprecated APIs that will affect their application or development process.

How often should I expect to upgrade Kubernetes versions to stay in support?

Starting with Kubernetes 1.19, the [open source community has expanded support to 1 year](#). AKS commits to enabling patches and support matching the upstream commitments. For AKS clusters on 1.19 and greater, you will be able to upgrade at a minimum of once a year to stay on a supported version.

What happens when a user upgrades a Kubernetes cluster with a minor version that isn't supported?

If you're on the *n-3* version or older, it means you're outside of support and will be asked to upgrade. When your upgrade from version *n-3* to *n-2* succeeds, you're back within our support policies. For example:

- If the oldest supported AKS version is *1.15.a* and you are on *1.14.b* or older, you're outside of support.
- When you successfully upgrade from *1.14.b* to *1.15.a* or higher, you're back within our support policies.

Downgrades are not supported.

What does 'Outside of Support' mean

'Outside of Support' means that:

- The version you're running is outside of the supported versions list.
- You'll be asked to upgrade the cluster to a supported version when requesting support, unless you're within the 30-day grace period after version deprecation.

Additionally, AKS doesn't make any runtime or other guarantees for clusters outside of the supported versions list.

What happens when a user scales a Kubernetes cluster with a minor version that isn't supported?

For minor versions not supported by AKS, scaling in or out should continue to work. Since there are no Quality of Service guarantees, we recommend upgrading to bring your cluster back into support.

Can a user stay on a Kubernetes version forever?

If a cluster has been out of support for more than three (3) minor versions and has been found to carry security risks, Azure proactively contacts you to upgrade your cluster. If you do not take further action, Azure reserves the right to automatically upgrade your cluster on your behalf.

What version does the control plane support if the node pool is not in one of the supported AKS versions?

The control plane must be within a window of versions from all node pools. For details on upgrading the control plane or node pools, visit documentation on [upgrading node pools](#).

Can I skip multiple AKS versions during cluster upgrade?

When you upgrade a supported AKS cluster, Kubernetes minor versions cannot be skipped. Kubernetes control planes [version skew policy](#) does not support minor version skipping. For example, upgrades between:

- *1.12.x-> 1.13.x*: allowed.
- *1.13.x-> 1.14.x*: allowed.
- *1.12.x-> 1.14.x*: not allowed.

To upgrade from *1.12.x-> 1.14.x*:

1. Upgrade from *1.12.x-> 1.13.x*.

2. Upgrade from 1.13.x-> 1.14.x

Skipping multiple versions can only be done when upgrading from an unsupported version back into the minimum supported version. For example, you can upgrade from an unsupported 1.10.x to a supported 1.15.x if 1.15 is the minimum supported minor version.

Can I create a new 1.xx.x cluster during its 30 day support window?

No. Once a version is deprecated/removed, you cannot create a cluster with that version. As the change rolls out, you will start to see the old version removed from your version list. This process may take up to two weeks from announcement, progressively by region.

I am on a freshly deprecated version, can I still add new node pools? Or will I have to upgrade?

No. You will not be allowed to add node pools of the deprecated version to your cluster. You can add node pools of a new version. However, this may require you to update the control plane first.

How often do you update patches?

Patches have a two month minimum lifecycle. To keep up to date when new patches are released, follow the [AKS Release Notes](#).

Next steps

For information on how to upgrade your cluster, see [Upgrade an Azure Kubernetes Service \(AKS\) cluster](#).

Add-ons, extensions, and other integrations with Azure Kubernetes Service

10/27/2022 • 4 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) provides additional, supported functionality for your cluster using add-ons and extensions. There are also many more integrations provided by open-source projects and third parties that are commonly used with AKS. These open-source and third-party integrations are not covered by the [AKS support policy](#).

Add-ons

Add-ons are a fully supported way to provide extra capabilities for your AKS cluster. Add-ons' installation, configuration, and lifecycle is managed by AKS. Use `az aks enable-addons` to install an add-on or manage the add-ons for your cluster.

The following rules are used by AKS for applying updates to installed add-ons:

- Only an add-on's patch version can be upgraded within a Kubernetes minor version. The add-on's major/minor version will not be upgraded within the same Kubernetes minor version.
- The major/minor version of the add-on will only be upgraded when moving to a later Kubernetes minor version.
- Any breaking or behavior changes to the add-on will be announced well before, usually 60 days, for a GA minor version of Kubernetes on AKS.
- Add-ons can be patched weekly with every new release of AKS which will be announced in the release notes. AKS releases can be controlled using [maintenance windows](#) and followed using [release tracker](#).

Exceptions

- Add-ons will be upgraded to a new major/minor version (or breaking change) within a Kubernetes minor version if either the cluster's Kubernetes version or the add-on version are in preview.
- It is also possible, in unavoidable circumstances such as CVE security patches or critical bug fixes, that there may be times when an add-on needs to be updated within a GA minor version.

Available add-ons

The below table shows the available add-ons.

NAME	DESCRIPTION	MORE DETAILS
http_application_routing	Configure ingress with automatic public DNS name creation for your AKS cluster.	HTTP application routing add-on on Azure Kubernetes Service (AKS)
monitoring	Use Container Insights monitoring with your AKS cluster.	Container insights overview
virtual-node	Use virtual nodes with your AKS cluster.	Use virtual nodes

Name	Description	More Details
azure-policy	Use Azure Policy for AKS, which enables at-scale enforcements and safeguards on your clusters in a centralized, consistent manner.	Understand Azure Policy for Kubernetes clusters
ingress-appgw	Use Application Gateway Ingress Controller with your AKS cluster.	What is Application Gateway Ingress Controller?
open-service-mesh	Use Open Service Mesh with your AKS cluster.	Open Service Mesh AKS add-on
azure-keyvault-secrets-provider	Use Azure Keyvault Secrets Provider addon.	Use the Azure Key Vault Provider for Secrets Store CSI Driver in an AKS cluster
web_application_routing	Use a managed NGINX ingress Controller with your AKS cluster.	Web Application Routing Overview
keda	Event-driven autoscaling for the applications on your AKS cluster.	Simplified application autoscaling with Kubernetes Event-driven Autoscaling (KEDA) add-on

Extensions

Cluster extensions build on top of certain Helm charts and provide an Azure Resource Manager-driven experience for installation and lifecycle management of different Azure capabilities on top of your Kubernetes cluster. For more details on the specific cluster extensions for AKS, see [Deploy and manage cluster extensions for Azure Kubernetes Service \(AKS\)](#). For more details on the currently available cluster extensions, see [Currently available extensions](#).

Difference between extensions and add-ons

Both extensions and add-ons are supported ways to add functionality to your AKS cluster. When you install an add-on, the functionality is added as part of the AKS resource provider in the Azure API. When you install an extension, the functionality is added as part of a separate resource provider in the Azure API.

GitHub Actions

GitHub Actions helps you automate your software development workflows from within GitHub. For more details on using GitHub Actions with Azure, see [What is GitHub Actions for Azure](#). For an example of using GitHub Actions with an AKS cluster, see [Build, test, and deploy containers to Azure Kubernetes Service using GitHub Actions](#).

Open source and third-party integrations

You can install many open source and third-party integrations on your AKS cluster, but these open-source and third-party integrations are not covered by the [AKS support policy](#).

The below table shows a few examples of open-source and third-party integrations.

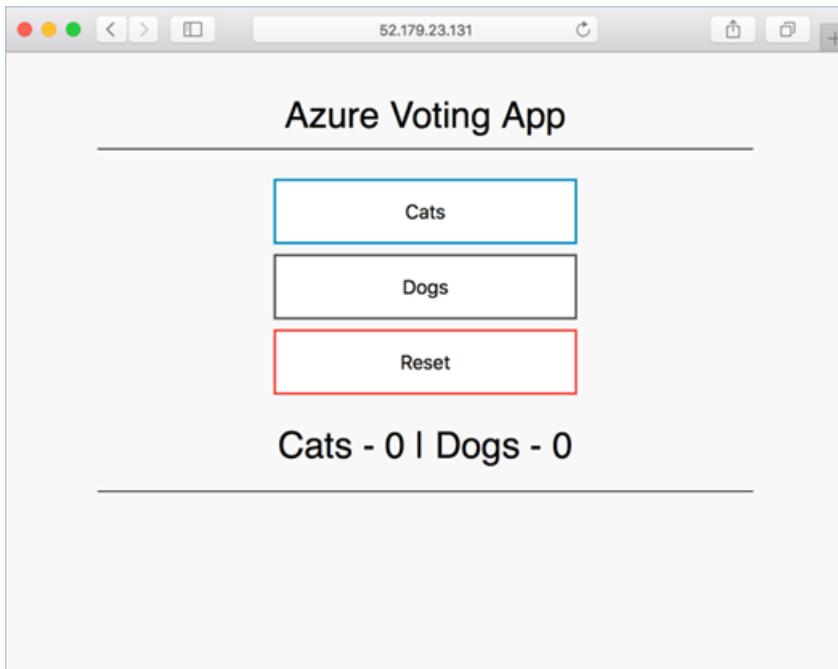
NAME	DESCRIPTION	MORE DETAILS
Helm	An open-source packaging tool that helps you install and manage the lifecycle of Kubernetes applications.	Quickstart: Develop on Azure Kubernetes Service (AKS) with Helm
Prometheus	An open source monitoring and alerting toolkit.	Container insights with metrics in Prometheus format, Prometheus Helm chart
Grafana	An open-source dashboard for observability.	Deploy Grafana on Kubernetes or use Managed Grafana
Couchbase	A distributed NoSQL cloud database.	Install Couchbase and the Operator on AKS
OpenFaaS	An open-source framework for building serverless functions by using containers.	Use OpenFaaS with AKS
Apache Spark	An open source, fast engine for large-scale data processing.	Running Apache Spark jobs requires a minimum node size of <i>Standard_D3_v2</i> . See running Spark on Kubernetes for more details on running Spark jobs on Kubernetes.
Istio	An open-source service mesh.	Istio Installation Guides
Linkerd	An open-source service mesh.	Linkerd Getting Started
Consul	An open source, identity-based networking solution.	Getting Started with Consul Service Mesh for Kubernetes

Quickstart: Deploy an Azure Kubernetes Service cluster using the Azure CLI

10/27/2022 • 6 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage clusters. In this quickstart, you will:

- Deploy an AKS cluster using the Azure CLI.
- Run a sample multi-container application with a web front-end and a Redis instance in the cluster.



This quickstart assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

To learn more about creating a Windows Server node pool, see [Create an AKS cluster that supports Windows Server containers](#).

Prerequisites

- Use the Bash environment in [Azure Cloud Shell](#). For more information, see [Azure Cloud Shell Quickstart - Bash](#).
[Launch Cloud Shell](#)
- If you prefer to run CLI reference commands locally, [install](#) the Azure CLI. If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a Docker container](#).
 - If you're using a local installation, sign in to the Azure CLI by using the `az login` command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).
 - When you're prompted, install the Azure CLI extension on first use. For more information about extensions, see [Use extensions with the Azure CLI](#).

- Run [az version](#) to find the version and dependent libraries that are installed. To upgrade to the latest version, run [az upgrade](#).
- This article requires version 2.0.64 or later of the Azure CLI. If using Azure Cloud Shell, the latest version is already installed.
- The identity you are using to create your cluster has the appropriate minimum permissions. For more details on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).
- If you have multiple Azure subscriptions, select the appropriate subscription ID in which the resources should be billed using the [az account](#) command.
- Verify *Microsoft.OperationsManagement* and *Microsoft.OperationalInsights* providers are registered on your subscription. These are Azure resource providers required to support [Container insights](#). To check the registration status, run the following commands:

```
az provider show -n Microsoft.OperationsManagement -o table  
az provider show -n Microsoft.OperationalInsights -o table
```

If they are not registered, register *Microsoft.OperationsManagement* and *Microsoft.OperationalInsights* using the following commands:

```
az provider register --namespace Microsoft.OperationsManagement  
az provider register --namespace Microsoft.OperationalInsights
```

NOTE

Run the commands with administrative privileges if you plan to run the commands in this quickstart locally instead of in Azure Cloud Shell.

Create a resource group

An [Azure resource group](#) is a logical group in which Azure resources are deployed and managed. When you create a resource group, you are prompted to specify a location. This location is:

- The storage location of your resource group metadata.
- Where your resources will run in Azure if you don't specify another region during resource creation.

The following example creates a resource group named *myResourceGroup* in the *eastus* location.

Create a resource group using the [az group create](#) command.

```
az group create --name myResourceGroup --location eastus
```

The following output example resembles successful creation of the resource group:

```
{  
  "id": "/subscriptions/<guid>/resourceGroups/myResourceGroup",  
  "location": "eastus",  
  "managedBy": null,  
  "name": "myResourceGroup",  
  "properties": {  
    "provisioningState": "Succeeded"  
  },  
  "tags": null  
}
```

Create AKS cluster

Create an AKS cluster using the `az aks create` command with the `--enable-addons monitoring` and `--enable-msi-auth-for-monitoring` parameter to enable [Azure Monitor Container insights](#) with managed identity authentication (preview). The following example creates a cluster named *myAKSCluster* with one node and enables a system-assigned managed identity:

```
az aks create -g myResourceGroup -n myAKSCluster --enable-managed-identity --node-count 1 --enable-addons monitoring --enable-msi-auth-for-monitoring --generate-ssh-keys
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

NOTE

When you create an AKS cluster, a second resource group is automatically created to store the AKS resources. For more information, see [Why are two resource groups created with AKS?](#)

Connect to the cluster

To manage a Kubernetes cluster, use the Kubernetes command-line client, `kubectl`. `kubectl` is already installed if you use Azure Cloud Shell.

1. Install `kubectl` locally using the `az aks install-cli` command:

```
az aks install-cli
```

2. Configure `kubectl` to connect to your Kubernetes cluster using the `az aks get-credentials` command. The following command:

- Downloads credentials and configures the Kubernetes CLI to use them.
- Uses `~/.kube/config`, the default location for the [Kubernetes configuration file](#). Specify a different location for your Kubernetes configuration file using `--file` argument.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

3. Verify the connection to your cluster using the `kubectl get` command. This command returns a list of the cluster nodes.

```
kubectl get nodes
```

The following output example shows the single node created in the previous steps. Make sure the node

status is *Ready*:

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-31718369-0	Ready	agent	6m44s	v1.12.8

Deploy the application

A [Kubernetes manifest file](#) defines a cluster's desired state, such as which container images to run.

In this quickstart, you will use a manifest to create all objects needed to run the [Azure Vote application](#). This manifest includes two [Kubernetes deployments](#):

- The sample Azure Vote Python applications.
- A Redis instance.

Two [Kubernetes Services](#) are also created:

- An internal service for the Redis instance.
- An external service to access the Azure Vote application from the internet.

1. Create a file named `azure-vote.yaml` and copy in the following manifest.

- If you use the Azure Cloud Shell, this file can be created using `code`, `vi`, or `nano` as if working on a virtual or physical system.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-back
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-back
  template:
    metadata:
      labels:
        app: azure-vote-back
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
        - name: azure-vote-back
          image: mcr.microsoft.com/oss/bitnami/redis:6.0.8
          env:
            - name: ALLOW_EMPTY_PASSWORD
              value: "yes"
          resources:
            requests:
              cpu: 100m
              memory: 128Mi
            limits:
              cpu: 250m
              memory: 256Mi
          ports:
            - containerPort: 6379
              name: redis
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-back
spec:
```

```

ports:
- port: 6379
selector:
  app: azure-vote-back
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-front
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-front
  template:
    metadata:
      labels:
        app: azure-vote-front
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
        - name: azure-vote-front
          image: mcr.microsoft.com/azuredocs/azure-vote-front:v1
          resources:
            requests:
              cpu: 100m
              memory: 128Mi
            limits:
              cpu: 250m
              memory: 256Mi
          ports:
            - containerPort: 80
          env:
            - name: REDIS
              value: "azure-vote-back"
      ---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-front
spec:
  type: LoadBalancer
  ports:
    - port: 80
  selector:
    app: azure-vote-front

```

2. Deploy the application using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f azure-vote.yaml
```

The following example resembles output showing the successfully created deployments and services:

```

deployment "azure-vote-back" created
service "azure-vote-back" created
deployment "azure-vote-front" created
service "azure-vote-front" created

```

Test the application

When the application runs, a Kubernetes service exposes the application front-end to the internet. This process

can take a few minutes to complete.

Monitor progress using the `kubectl get service` command with the `--watch` argument.

```
kubectl get service azure-vote-front --watch
```

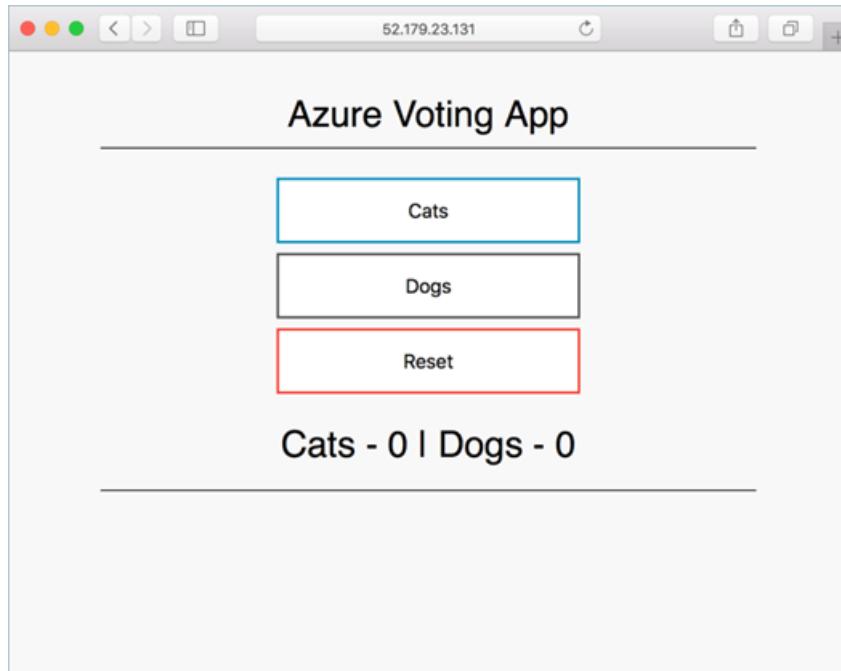
The EXTERNAL-IP output for the `azure-vote-front` service will initially show as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
azure-vote-front	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

Once the EXTERNAL-IP address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
azure-vote-front LoadBalancer 10.0.37.27 52.179.23.131 80:30572/TCP 2m
```

To see the Azure Vote app in action, open a web browser to the external IP address of your service.



Delete the cluster

To avoid Azure charges, if you don't plan on going through the tutorials that follow, clean up your unnecessary resources. Use the `az group delete` command to remove the resource group, container service, and all related resources.

```
az group delete --name myResourceGroup --yes --no-wait
```

NOTE

The AKS cluster was created with system-assigned managed identity (default identity option used in this quickstart), the identity is managed by the platform and does not require removal.

Next steps

In this quickstart, you deployed a Kubernetes cluster and then deployed a simple multi-container application to it.

To learn more about AKS, and walk through a complete code to deployment example, continue to the Kubernetes cluster tutorial.

[AKS tutorial](#)

This quickstart is for introductory purposes. For guidance on creating full solutions with AKS for production, see [AKS solution guidance](#).

Quickstart: Deploy an Azure Kubernetes Service cluster using PowerShell

10/27/2022 • 6 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage clusters. In this quickstart, you will:

- Deploy an AKS cluster using PowerShell.
- Run a sample multi-container application with a web front-end and a Redis instance in the cluster.



This quickstart assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

Prerequisites

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

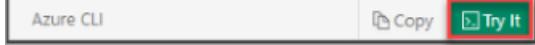
- If you're running PowerShell locally, install the Az PowerShell module and connect to your Azure account using the [Connect-AzAccount](#) cmdlet. For more information about installing the Az PowerShell module, see [Install Azure PowerShell](#).
- The identity you are using to create your cluster has the appropriate minimum permissions. For more details on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).
- If you have multiple Azure subscriptions, select the appropriate subscription ID in which the resources should be billed using the [Set-AzContext](#) cmdlet.

```
Set-AzContext -SubscriptionId 00000000-0000-0000-0000-000000000000
```

Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article, without having to install anything on your local environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code or command block. Selecting Try It doesn't automatically copy the code or command to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To use Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block (or command block) to copy the code or command.
3. Paste the code or command into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux, or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code or command.

Create a resource group

An [Azure resource group](#) is a logical group in which Azure resources are deployed and managed. When you create a resource group, you will be prompted to specify a location. This location is:

- The storage location of your resource group metadata.
- Where your resources will run in Azure if you don't specify another region during resource creation.

The following example creates a resource group named *myResourceGroup* in the *eastus* region.

Create a resource group using the [New-AzResourceGroup](#) cmdlet.

```
New-AzResourceGroup -Name myResourceGroup -Location eastus
```

The following output example resembles successful creation of the resource group:

```
ResourceGroupName : myResourceGroup
Location        : eastus
ProvisioningState : Succeeded
Tags            :
ResourceId      : /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/myResourceGroup
```

Create AKS cluster

Create an AKS cluster using the [New-AzAksCluster](#) cmdlet with the *-WorkspaceResourceId* parameter to enable [Azure Monitor container insights](#).

1. Create an AKS cluster named **myAKSCluster** with one node.

```
New-AzAksCluster -ResourceGroupName myResourceGroup -Name myAKSCluster -NodeCount 1 -GenerateSshKey -  
WorkspaceResourceId <WORKSPACE_RESOURCE_ID>
```

After a few minutes, the command completes and returns information about the cluster.

NOTE

When you create an AKS cluster, a second resource group is automatically created to store the AKS resources. For more information, see [Why are two resource groups created with AKS?](#)

Connect to the cluster

To manage a Kubernetes cluster, use the Kubernetes command-line client, `kubectl`. `kubectl` is already installed if you use Azure Cloud Shell.

1. Install `kubectl` locally using the `Install-AzAksKubectl` cmdlet:

```
Install-AzAksKubectl
```

2. Configure `kubectl` to connect to your Kubernetes cluster using the `Import-AzAksCredential` cmdlet. The following cmdlet downloads credentials and configures the Kubernetes CLI to use them.

```
Import-AzAksCredential -ResourceGroupName myResourceGroup -Name myAKSCluster
```

3. Verify the connection to your cluster using the `kubectl get` command. This command returns a list of the cluster nodes.

```
kubectl get nodes
```

The following output example shows the single node created in the previous steps. Make sure the node status is *Ready*:

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-31718369-0	Ready	agent	6m44s	v1.15.10

Deploy the application

A [Kubernetes manifest file](#) defines a cluster's desired state, such as which container images to run.

In this quickstart, you will use a manifest to create all objects needed to run the [Azure Vote application](#). This manifest includes two [Kubernetes deployments](#):

- The sample Azure Vote Python applications.
- A Redis instance.

Two [Kubernetes Services](#) are also created:

- An internal service for the Redis instance.
- An external service to access the Azure Vote application from the internet.

1. Create a file named `azure-vote.yaml`.

- If you use the Azure Cloud Shell, this file can be created using `code`, `vi`, or `nano` as if working on a virtual or physical system

2. Copy in the following YAML definition:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-back
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-back
  template:
    metadata:
      labels:
        app: azure-vote-back
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
        - name: azure-vote-back
          image: mcr.microsoft.com/oss/bitnami/redis:6.0.8
          env:
            - name: ALLOW_EMPTY_PASSWORD
              value: "yes"
          resources:
            requests:
              cpu: 100m
              memory: 128Mi
            limits:
              cpu: 250m
              memory: 256Mi
          ports:
            - containerPort: 6379
              name: redis
      ---
      apiVersion: v1
      kind: Service
      metadata:
        name: azure-vote-back
      spec:
        ports:
          - port: 6379
        selector:
          app: azure-vote-back
      ---
      apiVersion: apps/v1
      kind: Deployment
      metadata:
        name: azure-vote-front
      spec:
        replicas: 1
        selector:
          matchLabels:
            app: azure-vote-front
        template:
          metadata:
            labels:
              app: azure-vote-front
        spec:
          nodeSelector:
            "kubernetes.io/os": linux
          containers:
            - name: azure-vote-front
```

```

image: mcr.microsoft.com/azuredocs/azure-vote-front:v1
resources:
  requests:
    cpu: 100m
    memory: 128Mi
  limits:
    cpu: 250m
    memory: 256Mi
ports:
- containerPort: 80
env:
- name: REDIS
  value: "azure-vote-back"
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-front
spec:
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: azure-vote-front

```

- Deploy the application using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f azure-vote.yaml
```

The following example resembles output showing the successfully created deployments and services:

```

deployment.apps/azure-vote-back created
service/azure-vote-back created
deployment.apps/azure-vote-front created
service/azure-vote-front created

```

Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete.

Monitor progress using the [kubectl get service](#) command with the `--watch` argument.

```
kubectl get service azure-vote-front --watch
```

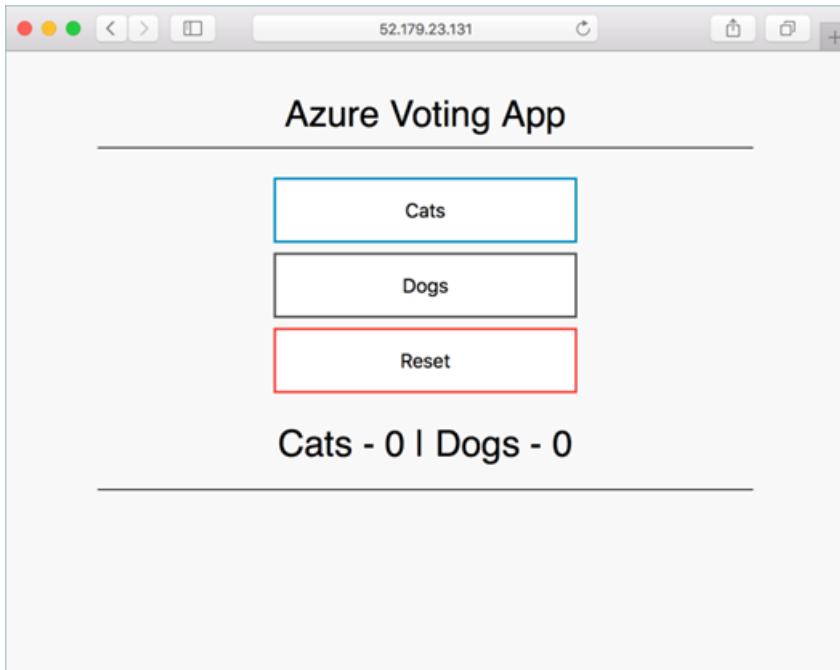
The **EXTERNAL-IP** output for the `azure-vote-front` service will initially show as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
azure-vote-front	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

Once the **EXTERNAL-IP** address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the [kubectl](#) watch process. The following example output shows a valid public IP address assigned to the service:

```
azure-vote-front  LoadBalancer  10.0.37.27  52.179.23.131  80:30572/TCP  2m
```

To see the Azure Vote app in action, open a web browser to the external IP address of your service.



Delete the cluster

To avoid Azure charges, if you don't plan on going through the tutorials that follow, clean up your unnecessary resources. Use the [Remove-AzResourceGroup](#) cmdlet to remove the resource group, container service, and all related resources.

```
Remove-AzResourceGroup -Name myResourceGroup
```

NOTE

The AKS cluster was created with system-assigned managed identity (default identity option used in this quickstart), the identity is managed by the platform and does not require removal.

Next steps

In this quickstart, you deployed a Kubernetes cluster and then deployed a sample multi-container application to it.

To learn more about AKS, and walk through a complete code to deployment example, continue to the Kubernetes cluster tutorial.

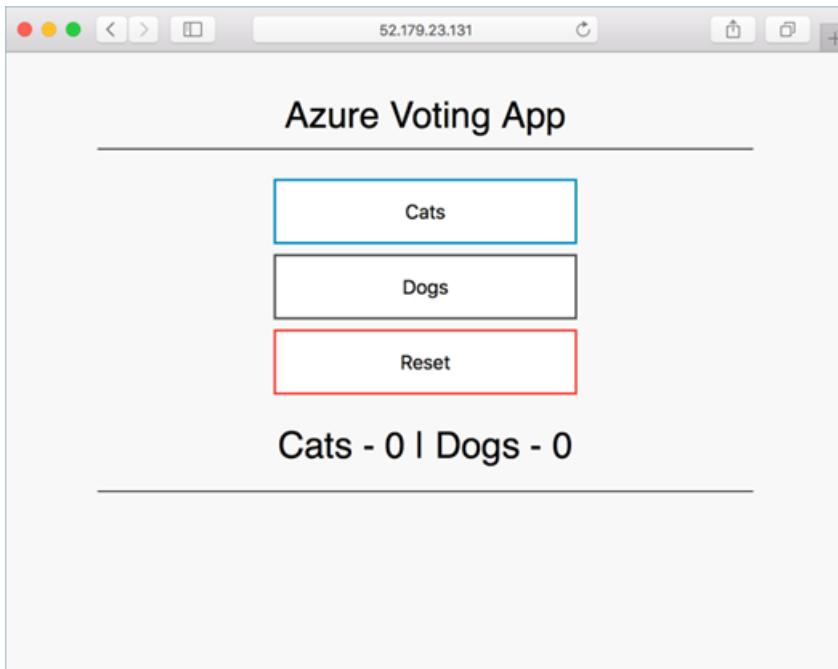
[AKS tutorial](#)

Quickstart: Deploy an Azure Kubernetes Service (AKS) cluster using the Azure portal

10/27/2022 • 6 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage clusters. In this quickstart, you will:

- Deploy an AKS cluster using the Azure portal.
- Run a sample multi-container application with a web front-end and a Redis instance in the cluster.



This quickstart assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

Prerequisites

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

- If you're unfamiliar with the Azure Cloud Shell, review [Overview of Azure Cloud Shell](#).
- The identity you're using to create your cluster has the appropriate minimum permissions. For more details on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).

Create an AKS cluster

1. Sign in to the [Azure portal](#).
2. On the Azure portal menu or from the Home page, select **Create a resource**.
3. Select **Containers > Kubernetes Service**.
4. On the **Basics** page, configure the following options:
 - **Project details:**

- Select an Azure Subscription.
- Select or create an Azure Resource group, such as *myResourceGroup*.
- Cluster details:
 - Ensure the the Preset configuration is *Standard (\$\$)*. For more details on preset configurations, see [Cluster configuration presets in the Azure portal](#).
 - Enter a **Kubernetes cluster name**, such as *myAKSCluster*.
 - Select a **Region** for the AKS cluster, and leave the default value selected for **Kubernetes version**.
 - Select **99.5% for API server availability**.
- Primary node pool:
 - Leave the default values selected.

The screenshot shows the 'Create Kubernetes cluster' wizard in the Microsoft Azure portal. The current step is 'Cluster details'. The configuration includes:

- Kubernetes cluster name:** myAKSCluster
- Region:** (US) East US
- Availability zones:** Zones 1,2,3
- Kubernetes version:** 1.22.6 (default)
- API server availability:** 99.5% (selected)
- Primary node pool:**
 - Node size:** Standard DS2 v2 (2 vcpus, 7 GiB memory)
 - Scale method:** Autoscale (selected)
 - Node count range:** 1 to 5 (set to 1)

At the bottom, there are navigation buttons: 'Review + create', '< Previous', 'Next : Node pools >', and a horizontal scroll bar.

NOTE

You can change the preset configuration when creating your cluster by selecting *Learn more and compare presets* and choosing a different option.

Presets	System node pool node size	User node pool node size	Cluster autoscaling	Private cluster	Availability zones	Azure Policy	Azure Monitor
Standard (\$\$)	DS2_v2	-	✓	-	✓	-	✓
Dev/Test (\$)	-	-	-	-	-	-	-
Cost-optimized (\$)	-	-	-	-	-	-	-
Batch processing (\$\$\$)	-	-	-	-	-	-	-
Hardened access (\$\$\$\$)	-	-	-	-	-	-	-

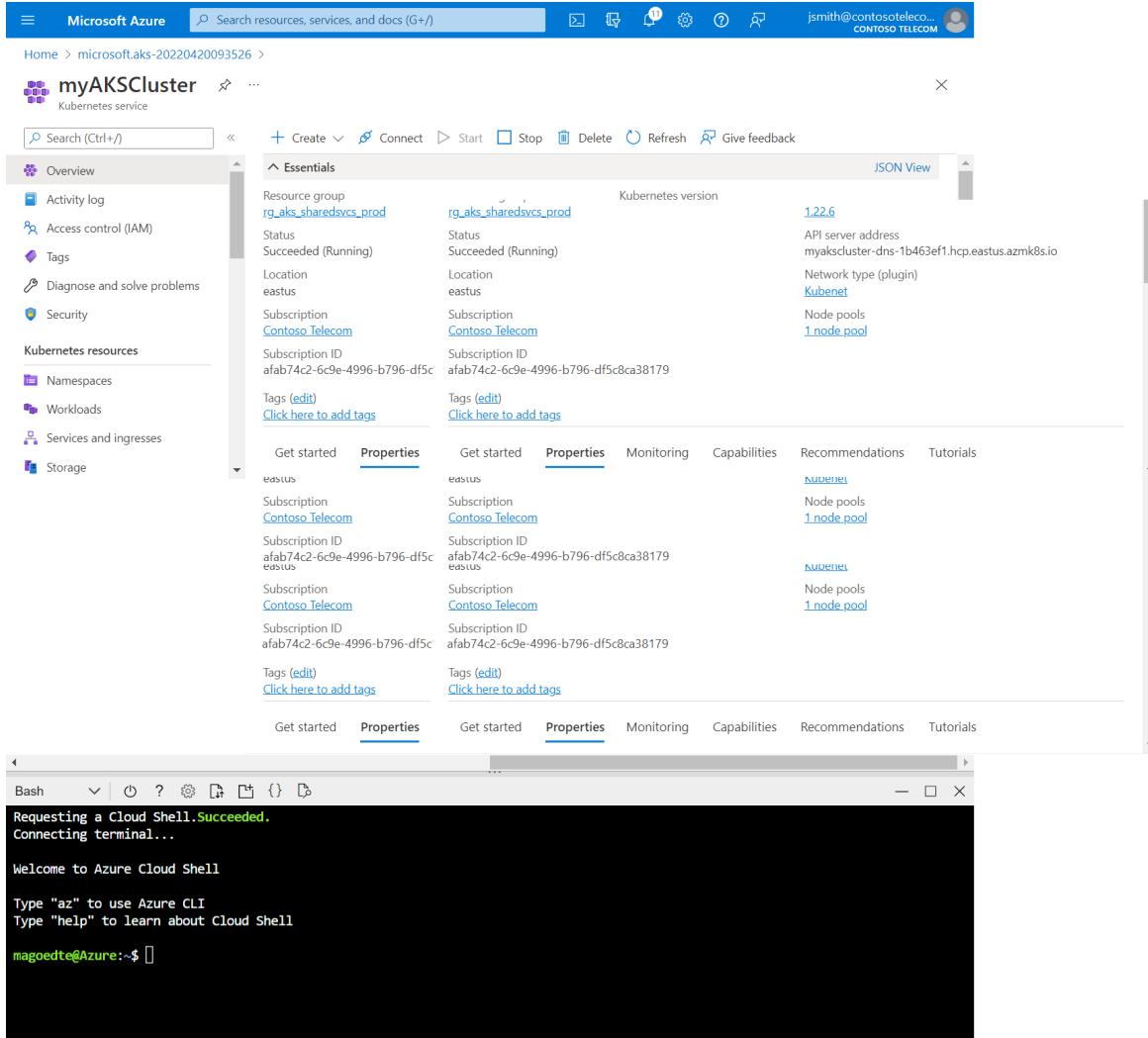
5. Select **Next: Node pools** when complete.
6. Keep the default **Node pools** options. At the bottom of the screen, click **Next: Access**.
7. On the **Access** page, configure the following options:
 - The default value for **Resource identity** is **System-assigned managed identity**. Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. For more details about managed identities, see [What are managed identities for Azure resources?](#).
 - The Kubernetes role-based access control (RBAC) option is the default value to provide more fine-grained control over access to the Kubernetes resources deployed in your AKS cluster.By default, *Basic* networking is used, and [Container insights](#) is enabled.
8. Click **Review + create**. When you navigate to the **Review + create** tab, Azure runs validation on the settings that you have chosen. If validation passes, you can proceed to create the AKS cluster by selecting **Create**. If validation fails, then it indicates which settings need to be modified.
9. It takes a few minutes to create the AKS cluster. When your deployment is complete, navigate to your resource by either:
 - Selecting **Go to resource**, or
 - Browsing to the AKS cluster resource group and selecting the AKS resource. In this example you browse for *myResourceGroup* and select the resource *myAKSCluster*.

Essentials	Kubernetes version	API server address
Resource group : rg_aks_shardsvcs_prod	: 1.22	: myakscluster-dns-1b463ef1.hcp.eastus.azmk8s.io
Status : Succeeded (Running)		
Location : eastus		
Subscription : Contoso Telecom		
Subscription ID : afab74c2-6c9e-4996-b796-df5c8ca38179		
Tags (edit) : Click here to add tags		
Node pools	: 1 node pool	

Connect to the cluster

To manage a Kubernetes cluster, use the Kubernetes command-line client, `kubectl`. `kubectl` is already installed if you use Azure Cloud Shell. If you're unfamiliar with the Cloud Shell, review [Overview of Azure Cloud Shell](#).

1. Open Cloud Shell using the  button on the top of the Azure portal.



The screenshot shows the Azure portal interface for managing a Kubernetes cluster named "myAKSCluster". The "Properties" tab is active in the main content area, displaying details such as the resource group ("rg_aks_sharedsvcs_prod"), Kubernetes version ("1.22.6"), and API server address ("myakscluster-dns-1b463ef1.hcp.eastus.azmk8s.io"). The "Essentials" section also lists the location ("eastus"), subscription ("Contoso Telecom"), and node pool ("1_node_pool"). On the left sidebar, there are sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Kubernetes resources (Namespaces, Workloads, Services and ingresses, Storage), and a Get started button. Below the main content, a terminal window titled "Bash" shows the output of a command: "Requesting a Cloud Shell. Succeeded. Connecting terminal... Welcome to Azure Cloud Shell Type "az" to use Azure CLI Type "help" to learn about Cloud Shell magoedte@Azure:< \$ ". The terminal window has a dark background with white text.

NOTE

To perform these operations in a local shell installation:

1. Verify Azure CLI or Azure PowerShell is installed.
2. Connect to Azure via the `az login` or `Connect-AzAccount` command.

- [Azure CLI](#)
 - [Azure PowerShell](#)
2. Configure `kubectl` to connect to your Kubernetes cluster using the `az aks get-credentials` command. The following command downloads credentials and configures the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

3. Verify the connection to your cluster using `kubectl get` to return a list of the cluster nodes.

```
kubectl get nodes
```

Output shows the single node created in the previous steps. Make sure the node status is *Ready*.

NAME	STATUS	ROLES	AGE	VERSION
aks-agentpool-12345678-vmss000000	Ready	agent	23m	v1.19.11
aks-agentpool-12345678-vmss000001	Ready	agent	24m	v1.19.11

Deploy the application

A Kubernetes manifest file defines a cluster's desired state, like which container images to run.

In this quickstart, you will use a manifest to create all objects needed to run the Azure Vote application. This manifest includes two Kubernetes deployments:

- The sample Azure Vote Python applications.
 - A Redis instance.

Two Kubernetes Services are also created:

- An internal service for the Redis instance.
 - An external service to access the Azure Vote application from the internet.

1. In the Cloud Shell, use an editor to create a file named `azure-vote.yaml`, such as

- code azure-vote.yaml
 - nano azure-vote.yaml , or
 - vi azure-vote.yaml .

2. Copy in the following YAML definition:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-back
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-back
  template:
    metadata:
      labels:
        app: azure-vote-back
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
        - name: azure-vote-back
          image: mcr.microsoft.com/oss/bitnami/redis:6.0.8
          env:
            - name: ALLOW_EMPTY_PASSWORD
              value: "yes"
          resources:
            requests:
              cpu: 100m
              memory: 128Mi
            limits:
              cpu: 250m
              memory: 256Mi
          ports:
            - containerPort: 6379
              name: redis
---
apiVersion: v1
kind: Service
metadata:
```

```

metadata:
  name: azure-vote-back
spec:
  ports:
  - port: 6379
  selector:
    app: azure-vote-back
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-front
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-front
  template:
    metadata:
      labels:
        app: azure-vote-front
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
      - name: azure-vote-front
        image: mcr.microsoft.com/azuredocs/azure-vote-front:v1
        resources:
          requests:
            cpu: 100m
            memory: 128Mi
          limits:
            cpu: 250m
            memory: 256Mi
      ports:
      - containerPort: 80
      env:
      - name: REDIS
        value: "azure-vote-back"
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-front
spec:
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: azure-vote-front

```

3. Deploy the application using the `kubectl apply` command and specify the name of your YAML manifest:

```
kubectl apply -f azure-vote.yaml
```

Output shows the successfully created deployments and services:

```

deployment "azure-vote-back" created
service "azure-vote-back" created
deployment "azure-vote-front" created
service "azure-vote-front" created

```

Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete.

To monitor progress, use the `kubectl get service` command with the `--watch` argument.

```
kubectl get service azure-vote-front --watch
```

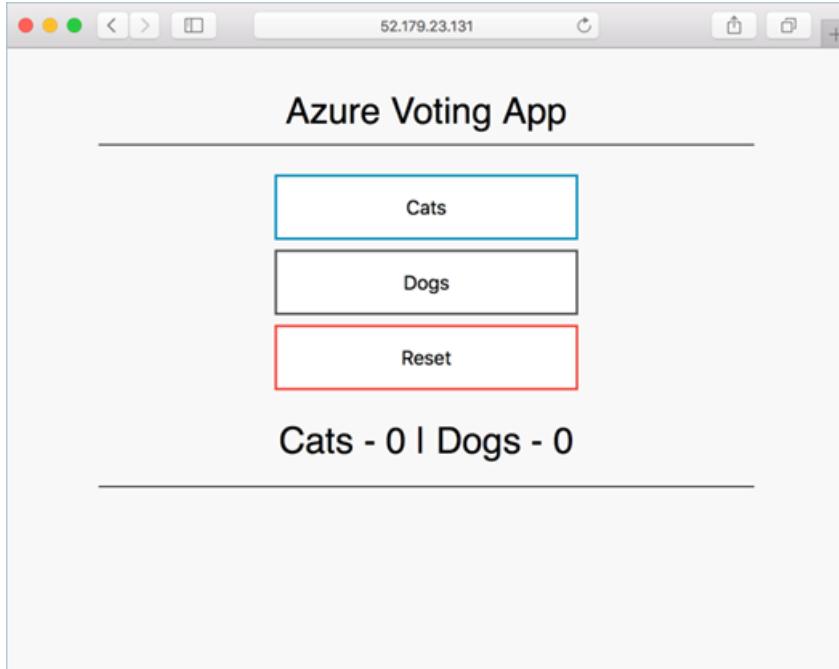
The EXTERNAL-IP output for the `azure-vote-front` service will initially show as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
azure-vote-front	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

Once the EXTERNAL-IP address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
azure-vote-front LoadBalancer 10.0.37.27 52.179.23.131 80:30572/TCP 2m
```

To see the Azure Vote app in action, open a web browser to the external IP address of your service.



Delete cluster

To avoid Azure charges, if you don't plan on going through the tutorials that follow, clean up your unnecessary resources. Select the **Delete** button on the AKS cluster dashboard. You can also use the [az group delete](#) command or the [Remove-AzResourceGroup](#) cmdlet to remove the resource group, container service, and all related resources.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
az group delete --name myResourceGroup --yes --no-wait
```

NOTE

The AKS cluster was created with a system-assigned managed identity. This identity is managed by the platform and doesn't require removal.

Next steps

In this quickstart, you deployed a Kubernetes cluster and then deployed a sample multi-container application to it.

To learn more about AKS by walking through a complete example, including building an application, deploying from Azure Container Registry, updating a running application, and scaling and upgrading your cluster, continue to the Kubernetes cluster tutorial.

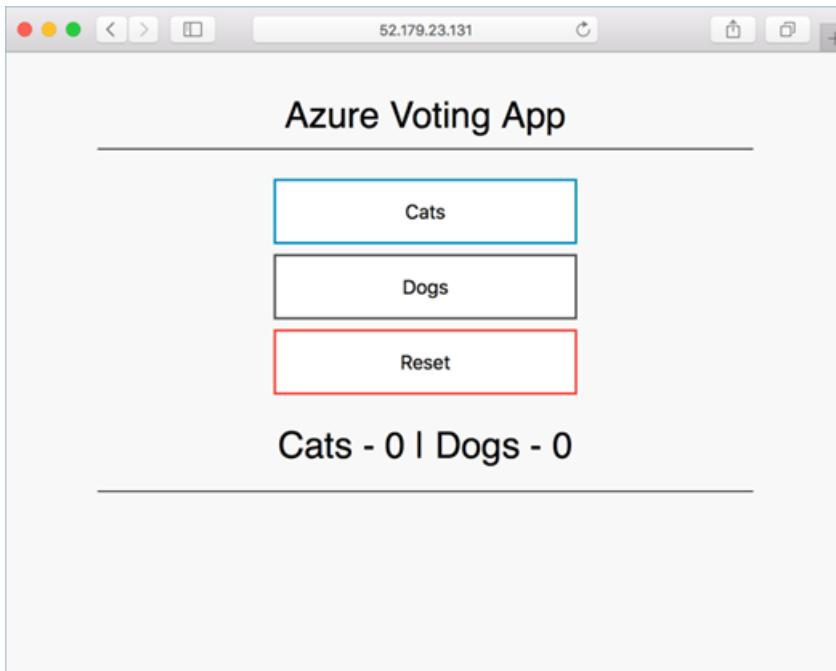
[AKS tutorial](#)

Quickstart: Deploy an Azure Kubernetes Service (AKS) cluster using Bicep

10/27/2022 • 8 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage clusters. In this quickstart, you'll:

- Deploy an AKS cluster using a Bicep file.
- Run a sample multi-container application with a web front-end and a Redis instance in the cluster.



[Bicep](#) is a domain-specific language (DSL) that uses declarative syntax to deploy Azure resources. It provides concise syntax, reliable type safety, and support for code reuse. Bicep offers the best authoring experience for your infrastructure-as-code solutions in Azure.

This quickstart assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

Prerequisites

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

- [Azure CLI](#)
- [Azure PowerShell](#)
- Use the Bash environment in [Azure Cloud Shell](#). For more information, see [Azure Cloud Shell Quickstart - Bash](#).
[Launch Cloud Shell](#)
- If you prefer to run CLI reference commands locally, [install](#) the Azure CLI. If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a Docker container](#).
 - If you're using a local installation, sign in to the Azure CLI by using the `az login` command. To finish

the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).

- When you're prompted, install the Azure CLI extension on first use. For more information about extensions, see [Use extensions with the Azure CLI](#).
- Run `az version` to find the version and dependent libraries that are installed. To upgrade to the latest version, run `az upgrade`.
- This article requires version 2.20.0 or later of the Azure CLI. If using Azure Cloud Shell, the latest version is already installed.
- To create an AKS cluster using a Bicep file, you provide an SSH public key. If you need this resource, see the following section; otherwise skip to the [Review the Bicep file](#) section.
- The identity you're using to create your cluster has the appropriate minimum permissions. For more details on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).
- To deploy a Bicep file, you need write access on the resources you're deploying and access to all operations on the Microsoft.Resources/deployments resource type. For example, to deploy a virtual machine, you need Microsoft.Compute/virtualMachines/write and Microsoft.Resources/deployments/* permissions. For a list of roles and permissions, see [Azure built-in roles](#).

Create an SSH key pair

To access AKS nodes, you connect using an SSH key pair (public and private), which you generate using the `ssh-keygen` command. By default, these files are created in the `~/.ssh` directory. Running the `ssh-keygen` command will overwrite any SSH key pair with the same name already existing in the given location.

1. Go to <https://shell.azure.com> to open Cloud Shell in your browser.
2. Run the `ssh-keygen` command. The following example creates an SSH key pair using RSA encryption and a bit length of 4096:

```
ssh-keygen -t rsa -b 4096
```

For more information about creating SSH keys, see [Create and manage SSH keys for authentication in Azure](#).

Review the Bicep file

The Bicep file used in this quickstart is from [Azure Quickstart Templates](#).

```

@description('The name of the Managed Cluster resource.')
param clusterName string = 'aks101cluster'

@description('The location of the Managed Cluster resource.')
param location string = resourceGroup().location

@description('Optional DNS prefix to use with hosted Kubernetes API server FQDN.')
param dnsPrefix string

@description('Disk size (in GB) to provision for each of the agent pool nodes. This value ranges from 0 to 1023. Specifying 0 will apply the default disk size for that agentVMSize.')
@param minValue(0)
@param maxValue(1023)
param osDiskSizeGB int = 0

@description('The number of nodes for the cluster.')
@param minValue(1)
@param maxValue(50)
param agentCount int = 3

@description('The size of the Virtual Machine.')
param agentVMSize string = 'standard_d2s_v3'

@description('User name for the Linux Virtual Machines.')
param linuxAdminUsername string

@description('Configure all linux machines with the SSH RSA public key string. Your key should include three parts, for example \'ssh-rsa AAAAB...snip...UcyupgH azureuser@linuxvm\'')
param sshRSAPublicKey string

resource aks 'Microsoft.ContainerService/managedClusters@2022-05-02-preview' = {
    name: clusterName
    location: location
    identity: {
        type: 'SystemAssigned'
    }
    properties: {
        dnsPrefix: dnsPrefix
        agentPoolProfiles: [
            {
                name: 'agentpool'
                osDiskSizeGB: osDiskSizeGB
                count: agentCount
                vmSize: agentVMSize
                osType: 'Linux'
                mode: 'System'
            }
        ]
        linuxProfile: {
            adminUsername: linuxAdminUsername
            ssh: {
                publicKeys: [
                    {
                        keyData: sshRSAPublicKey
                    }
                ]
            }
        }
    }
}

output controlPlaneFQDN string = aks.properties.fqdn

```

The resource defined in the Bicep file:

- [Microsoft.ContainerService/managedClusters](#)

For more AKS samples, see the [AKS quickstart templates](#) site.

Deploy the Bicep file

1. Save the Bicep file as `main.bicep` to your local computer.
2. Deploy the Bicep file using either Azure CLI or Azure PowerShell.

- [CLI](#)
- [PowerShell](#)

```
az group create --name myResourceGroup --location eastus
az deployment group create --resource-group myResourceGroup --template-file main.bicep --parameters
clusterName=<cluster-name> dnsPrefix=<dns-prefix> linuxAdminUsername=<linux-admin-username>
sshRSAPublicKey='<ssh-key>'
```

Provide the following values in the commands:

- **Cluster name:** Enter a unique name for the AKS cluster, such as *myAKSCluster*.
- **DNS prefix:** Enter a unique DNS prefix for your cluster, such as *myakscluster*.
- **Linux Admin Username:** Enter a username to connect using SSH, such as *azureuser*.
- **SSH RSA Public Key:** Copy and paste the *public* part of your SSH key pair (by default, the contents of `~/.ssh/id_rsa.pub`).

It takes a few minutes to create the AKS cluster. Wait for the cluster to be successfully deployed before you move on to the next step.

Validate the Bicep deployment

Connect to the cluster

To manage a Kubernetes cluster, use the Kubernetes command-line client, `kubectl`. `kubectl` is already installed if you use Azure Cloud Shell.

- [Azure CLI](#)
- [Azure PowerShell](#)

1. Install `kubectl` locally using the `az aks install-cli` command:

```
az aks install-cli
```

2. Configure `kubectl` to connect to your Kubernetes cluster using the `az aks get-credentials` command. This command downloads credentials and configures the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

3. Verify the connection to your cluster using the `kubectl get` command. This command returns a list of the cluster nodes.

```
kubectl get nodes
```

The following output example shows the three nodes created in the previous steps. Make sure the node status is *Ready*:

NAME	STATUS	ROLES	AGE	VERSION
aks-agentpool-41324942-0	Ready	agent	6m44s	v1.12.6
aks-agentpool-41324942-1	Ready	agent	6m46s	v1.12.6
aks-agentpool-41324942-2	Ready	agent	6m45s	v1.12.6

Deploy the application

A [Kubernetes manifest file](#) defines a cluster's desired state, such as which container images to run.

In this quickstart, you'll use a manifest to create all objects needed to run the [Azure Vote application](#). This manifest includes two [Kubernetes deployments](#):

- The sample Azure Vote Python applications.
- A Redis instance.

Two [Kubernetes Services](#) are also created:

- An internal service for the Redis instance.
- An external service to access the Azure Vote application from the internet.

1. Create a file named `azure-vote.yaml`.

- If you use the Azure Cloud Shell, this file can be created using `code`, `vi`, or `nano` as if working on a virtual or physical system

2. Copy in the following YAML definition:

```

apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-back
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-back
  template:
    metadata:
      labels:
        app: azure-vote-back
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
        - name: azure-vote-back
          image: mcr.microsoft.com/oss/bitnami/redis:6.0.8
          env:
            - name: ALLOW_EMPTY_PASSWORD
              value: "yes"
          resources:
            requests:
              cpu: 100m
              memory: 128Mi
            limits:
              cpu: 250m
              memory: 256Mi
          ports:
            - containerPort: 6379
              name: redis
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-ingress
spec:
  type: LoadBalancer
  selector:
    app: azure-vote-back
  ports:
    - port: 80
      targetPort: 6379
      protocol: TCP
  externalIPs:
    - <IP>

```

```

name: azure-vote-back
spec:
  ports:
    - port: 6379
  selector:
    app: azure-vote-back
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-front
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-front
  template:
    metadata:
      labels:
        app: azure-vote-front
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
        - name: azure-vote-front
          image: mcr.microsoft.com/azuredocs/azure-vote-front:v1
          resources:
            requests:
              cpu: 100m
              memory: 128Mi
            limits:
              cpu: 250m
              memory: 256Mi
          ports:
            - containerPort: 80
          env:
            - name: REDIS
              value: "azure-vote-back"
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-front
spec:
  type: LoadBalancer
  ports:
    - port: 80
  selector:
    app: azure-vote-front

```

- Deploy the application using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f azure-vote.yaml
```

The following example resembles output showing the successfully created deployments and services:

```

deployment "azure-vote-back" created
service "azure-vote-back" created
deployment "azure-vote-front" created
service "azure-vote-front" created

```

Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process

can take a few minutes to complete.

Monitor progress using the `kubectl get service` command with the `--watch` argument.

```
kubectl get service azure-vote-front --watch
```

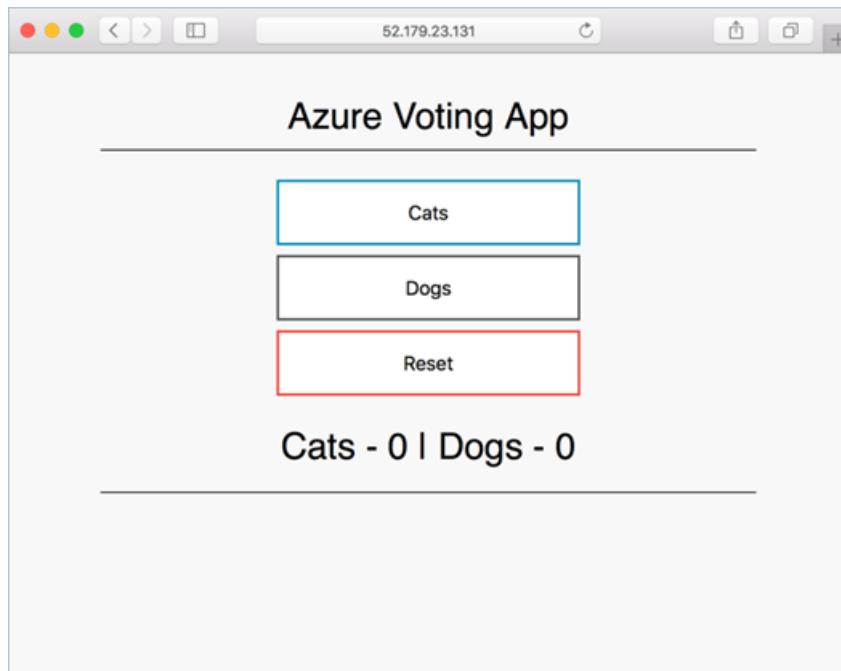
The **EXTERNAL-IP** output for the `azure-vote-front` service will initially show as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
azure-vote-front	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

Once the **EXTERNAL-IP** address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
azure-vote-front LoadBalancer 10.0.37.27 52.179.23.131 80:30572/TCP 2m
```

To see the Azure Vote app in action, open a web browser to the external IP address of your service.



Clean up resources

- [Azure CLI](#)
- [Azure PowerShell](#)

To avoid Azure charges, if you don't plan on going through the tutorials that follow, clean up your unnecessary resources. Use the `az group delete` command to remove the resource group, container service, and all related resources.

```
az group delete --name myResourceGroup --yes --no-wait
```

NOTE

In this quickstart, the AKS cluster was created with a system-assigned managed identity (the default identity option). This identity is managed by the platform and does not require removal.

Next steps

In this quickstart, you deployed a Kubernetes cluster and then deployed a sample multi-container application to it.

To learn more about AKS, and walk through a complete code to deployment example, continue to the Kubernetes cluster tutorial.

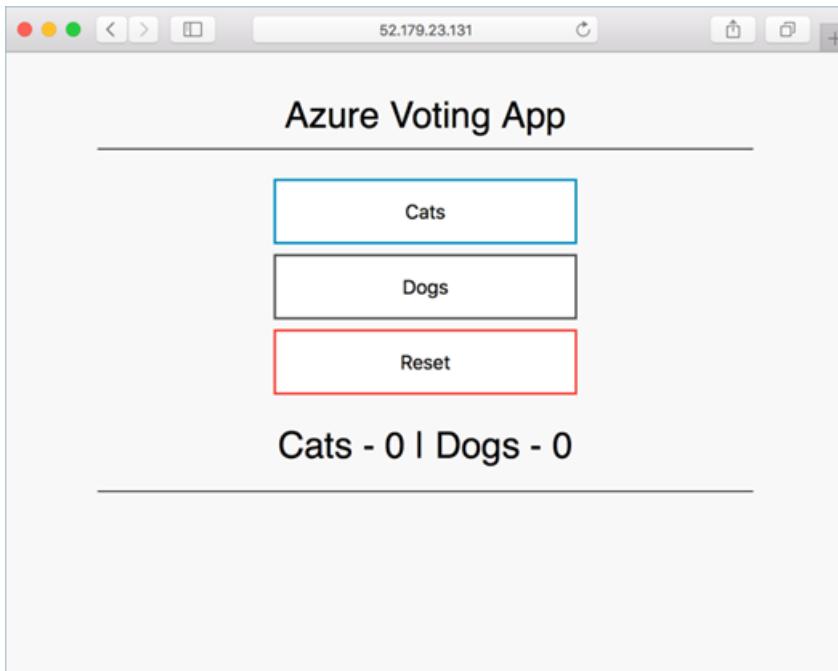
[AKS tutorial](#)

Quickstart: Deploy an Azure Kubernetes Service (AKS) cluster using an ARM template

10/27/2022 • 9 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage clusters. In this quickstart, you will:

- Deploy an AKS cluster using an Azure Resource Manager template.
- Run a sample multi-container application with a web front-end and a Redis instance in the cluster.



An [ARM template](#) is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration for your project. The template uses declarative syntax. In declarative syntax, you describe your intended deployment without writing the sequence of programming commands to create the deployment.

This quickstart assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

If your environment meets the prerequisites and you're familiar with using ARM templates, select the **Deploy to Azure** button. The template will open in the Azure portal.

 [Deploy to Azure](#)

Prerequisites

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

- [Azure CLI](#)
- [Azure PowerShell](#)
- Use the Bash environment in [Azure Cloud Shell](#). For more information, see [Azure Cloud Shell Quickstart - Bash](#).  [Launch Cloud Shell](#)

- If you prefer to run CLI reference commands locally, [install](#) the Azure CLI. If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a Docker container](#).
 - If you're using a local installation, sign in to the Azure CLI by using the `az login` command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).
 - When you're prompted, install the Azure CLI extension on first use. For more information about extensions, see [Use extensions with the Azure CLI](#).
 - Run `az version` to find the version and dependent libraries that are installed. To upgrade to the latest version, run `az upgrade`.
- This article requires version 2.0.64 or later of the Azure CLI. If using Azure Cloud Shell, the latest version is already installed.
- To create an AKS cluster using a Resource Manager template, you provide an SSH public key. If you need this resource, see the following section; otherwise skip to the [Review the template](#) section.
- The identity you are using to create your cluster has the appropriate minimum permissions. For more details on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).
- To deploy a Bicep file or ARM template, you need write access on the resources you're deploying and access to all operations on the Microsoft.Resources/deployments resource type. For example, to deploy a virtual machine, you need Microsoft.Compute/virtualMachines/write and Microsoft.Resources/deployments/* permissions. For a list of roles and permissions, see [Azure built-in roles](#).

Create an SSH key pair

To access AKS nodes, you connect using an SSH key pair (public and private), which you generate using the `ssh-keygen` command. By default, these files are created in the `~/.ssh` directory. Running the `ssh-keygen` command will overwrite any SSH key pair with the same name already existing in the given location.

1. Go to <https://shell.azure.com> to open Cloud Shell in your browser.
2. Run the `ssh-keygen` command. The following example creates an SSH key pair using RSA encryption and a bit length of 4096:

```
ssh-keygen -t rsa -b 4096
```

For more information about creating SSH keys, see [Create and manage SSH keys for authentication in Azure](#).

Review the template

The template used in this quickstart is from [Azure Quickstart Templates](#).

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "metadata": {
    "_generator": {
      "name": "bicep",
      "version": "0.9.1.41621",
      "templateHash": "2637152180661081755"
    }
  },
}
```

```
"parameters": {
    "clusterName": {
        "type": "string",
        "defaultValue": "aks101cluster",
        "metadata": {
            "description": "The name of the Managed Cluster resource."
        }
    },
    "location": {
        "type": "string",
        "defaultValue": "[resourceGroup().location]",
        "metadata": {
            "description": "The location of the Managed Cluster resource."
        }
    },
    "dnsPrefix": {
        "type": "string",
        "metadata": {
            "description": "Optional DNS prefix to use with hosted Kubernetes API server FQDN."
        }
    },
    "osDiskSizeGB": {
        "type": "int",
        "defaultValue": 0,
        "maxValue": 1023,
        "minValue": 0,
        "metadata": {
            "description": "Disk size (in GB) to provision for each of the agent pool nodes. This value ranges from 0 to 1023. Specifying 0 will apply the default disk size for that agentVMSize."
        }
    },
    "agentCount": {
        "type": "int",
        "defaultValue": 3,
        "maxValue": 50,
        "minValue": 1,
        "metadata": {
            "description": "The number of nodes for the cluster."
        }
    },
    "agentVMSize": {
        "type": "string",
        "defaultValue": "standard_d2s_v3",
        "metadata": {
            "description": "The size of the Virtual Machine."
        }
    },
    "linuxAdminUsername": {
        "type": "string",
        "metadata": {
            "description": "User name for the Linux Virtual Machines."
        }
    },
    "sshRSAPublicKey": {
        "type": "string",
        "metadata": {
            "description": "Configure all linux machines with the SSH RSA public key string. Your key should include three parts, for example 'ssh-rsa AAAAB...snip...UcyupgH azureuser@linuxvm'"
        }
    }
},
"resources": [
{
    "type": "Microsoft.ContainerService/managedClusters",
    "apiVersion": "2022-05-02-preview",
    "name": "[parameters('clusterName')]",
    "location": "[parameters('location')]",
    "identity": {
        "type": "SystemAssigned"
    }
}
```

```

},
"properties": {
    "dnsPrefix": "[parameters('dnsPrefix')]",
    "agentPoolProfiles": [
        {
            "name": "agentpool",
            "osDiskSizeGB": "[parameters('osDiskSizeGB')]",
            "count": "[parameters('agentCount')]",
            "vmSize": "[parameters('agentVMSize')]",
            "osType": "Linux",
            "mode": "System"
        }
    ],
    "linuxProfile": {
        "adminUsername": "[parameters('linuxAdminUsername')]",
        "ssh": {
            "publicKeys": [
                {
                    "keyData": "[parameters('sshRSAPublicKey')]"
                }
            ]
        }
    }
},
"outputs": {
    "controlPlaneFQDN": {
        "type": "string",
        "value": "[reference(resourceId('Microsoft.ContainerService/managedClusters', parameters('clusterName'))).fqdn]"
    }
}
}

```

The resource defined in the ARM template includes:

- [Microsoft.ContainerService/managedClusters](#)

For more AKS samples, see the [AKS quickstart templates](#) site.

Deploy the template

1. Select the following button to sign in to Azure and open a template.



2. Select or enter the following values.

For this quickstart, leave the default values for the *OS Disk Size GB*, *Agent Count*, *Agent VM Size*, *OS Type*, and *Kubernetes Version*. Provide your own values for the following template parameters:

- **Subscription:** Select an Azure subscription.
- **Resource group:** Select **Create new**. Enter a unique name for the resource group, such as *myResourceGroup*, then choose **OK**.
- **Location:** Select a location, such as **East US**.
- **Cluster name:** Enter a unique name for the AKS cluster, such as *myAKSCluster*.
- **DNS prefix:** Enter a unique DNS prefix for your cluster, such as *myakscluster*.
- **Linux Admin Username:** Enter a username to connect using SSH, such as *azureuser*.
- **SSH RSA Public Key:** Copy and paste the *public* part of your SSH key pair (by default, the contents of *~/.ssh/id_rsa.pub*).

The screenshot shows the Azure Container Service (AKS) quickstart template configuration page. It includes fields for Deployment scope (Subscription: East US, Resource group: myResourceGroup), Parameters (Region: East US, Cluster Name: myAKSCluster, Location: [resourceGroup()].location, Dns Prefix: myakscluster, Os Disk Size GB: 0, Agent Count: 3, Agent VM Size: Standard_DS2_v2, Linux Admin Username: azureuser, Ssh RSA Public Key: empty, Os Type: Linux), and navigation buttons (Review + create, < Previous, Next : Review + create >).

3. Select **Review + Create**.

It takes a few minutes to create the AKS cluster. Wait for the cluster to be successfully deployed before you move on to the next step.

Validate the deployment

Connect to the cluster

To manage a Kubernetes cluster, use the Kubernetes command-line client, `kubectl`. `kubectl` is already installed if you use Azure Cloud Shell.

- [Azure CLI](#)
- [Azure PowerShell](#)

1. Install `kubectl` locally using the `az aks install-cli` command:

```
az aks install-cli
```

2. Configure `kubectl` to connect to your Kubernetes cluster using the `az aks get-credentials` command. This command downloads credentials and configures the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group myResourceGroup --name myAKScluster
```

3. Verify the connection to your cluster using the [kubectl get](#) command. This command returns a list of the cluster nodes.

```
kubectl get nodes
```

The following output example shows the three nodes created in the previous steps. Make sure the node status is *Ready*:

NAME	STATUS	ROLES	AGE	VERSION
aks-agentpool-41324942-0	Ready	agent	6m44s	v1.12.6
aks-agentpool-41324942-1	Ready	agent	6m46s	v1.12.6
aks-agentpool-41324942-2	Ready	agent	6m45s	v1.12.6

Deploy the application

A [Kubernetes manifest file](#) defines a cluster's desired state, such as which container images to run.

In this quickstart, you will use a manifest to create all objects needed to run the [Azure Vote application](#). This manifest includes two [Kubernetes deployments](#):

- The sample Azure Vote Python applications.
- A Redis instance.

Two [Kubernetes Services](#) are also created:

- An internal service for the Redis instance.
- An external service to access the Azure Vote application from the internet.

1. Create a file named `azure-vote.yaml`.

- If you use the Azure Cloud Shell, this file can be created using `code`, `vi`, or `nano` as if working on a virtual or physical system

2. Copy in the following YAML definition:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-back
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-back
  template:
    metadata:
      labels:
        app: azure-vote-back
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
        - name: azure-vote-back
          image: mcr.microsoft.com/oss/bitnami/redis:6.0.8
          env:
            - name: ALLOW_EMPTY_PASSWORD
              value: "yes"
      resources:
```

```

requests:
  cpu: 100m
  memory: 128Mi
limits:
  cpu: 250m
  memory: 256Mi
ports:
- containerPort: 6379
  name: redis
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-back
spec:
  ports:
  - port: 6379
  selector:
    app: azure-vote-back
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-front
spec:
  replicas: 1
  selector:
    matchLabels:
      app: azure-vote-front
  template:
    metadata:
      labels:
        app: azure-vote-front
    spec:
      nodeSelector:
        "kubernetes.io/os": linux
      containers:
      - name: azure-vote-front
        image: mcr.microsoft.com/azuredocs/azure-vote-front:v1
        resources:
          requests:
            cpu: 100m
            memory: 128Mi
          limits:
            cpu: 250m
            memory: 256Mi
        ports:
        - containerPort: 80
        env:
        - name: REDIS
          value: "azure-vote-back"
---
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-front
spec:
  type: LoadBalancer
  ports:
  - port: 80
  selector:
    app: azure-vote-front

```

3. Deploy the application using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f azure-vote.yaml
```

The following example resembles output showing the successfully created deployments and services:

```
deployment "azure-vote-back" created
service "azure-vote-back" created
deployment "azure-vote-front" created
service "azure-vote-front" created
```

Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete.

Monitor progress using the [kubectl get service](#) command with the `--watch` argument.

```
kubectl get service azure-vote-front --watch
```

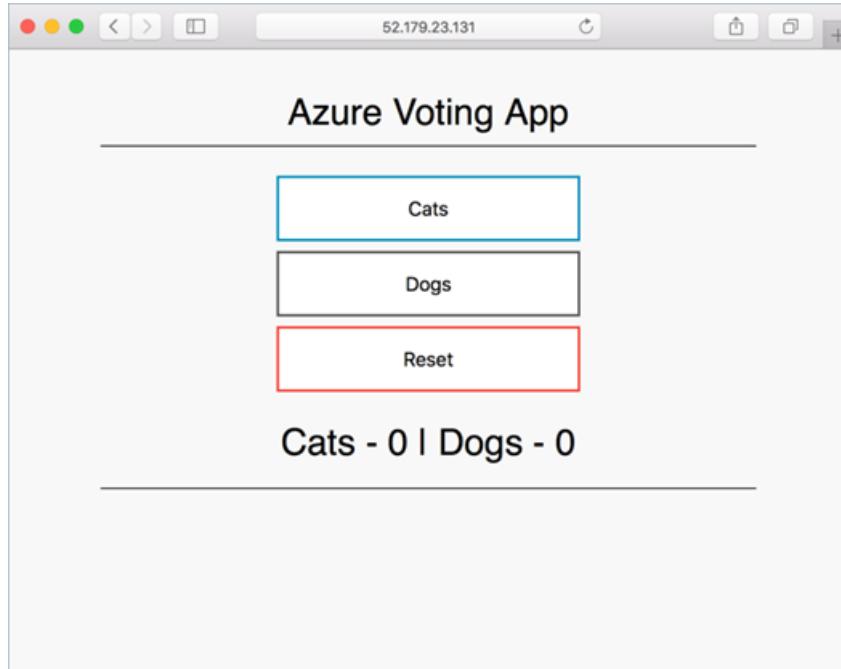
The **EXTERNAL-IP** output for the `azure-vote-front` service will initially show as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
azure-vote-front	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

Once the **EXTERNAL-IP** address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the [kubectl](#) watch process. The following example output shows a valid public IP address assigned to the service:

```
azure-vote-front    LoadBalancer    10.0.37.27    52.179.23.131    80:30572/TCP    2m
```

To see the Azure Vote app in action, open a web browser to the external IP address of your service.



Clean up resources

- [Azure CLI](#)
- [Azure PowerShell](#)

To avoid Azure charges, if you don't plan on going through the tutorials that follow, clean up your unnecessary resources. Use the [az group delete](#) command to remove the resource group, container service, and all related

resources.

```
az group delete --name myResourceGroup --yes --no-wait
```

NOTE

The AKS cluster was created with system-assigned managed identity (default identity option used in this quickstart), the identity is managed by the platform and does not require removal.

Next steps

In this quickstart, you deployed a Kubernetes cluster and then deployed a sample multi-container application to it.

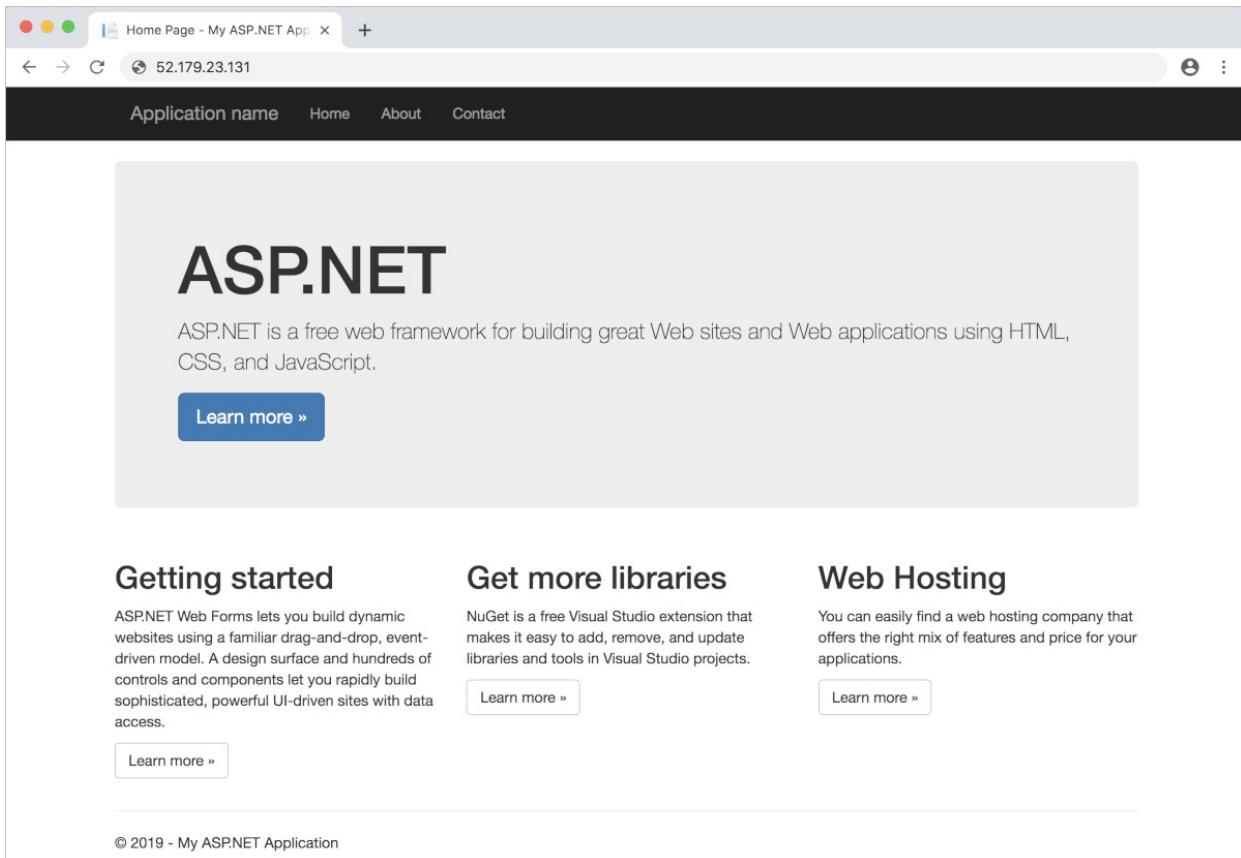
To learn more about AKS, and walk through a complete code to deployment example, continue to the Kubernetes cluster tutorial.

[AKS tutorial](#)

Create a Windows Server container on an Azure Kubernetes Service (AKS) cluster using the Azure CLI

10/27/2022 • 11 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage clusters. In this article, you deploy an AKS cluster that runs Windows Server 2019 containers using the Azure CLI. You also deploy an ASP.NET sample application in a Windows Server container to the cluster.



This article assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

Prerequisites

- Use the Bash environment in [Azure Cloud Shell](#). For more information, see [Azure Cloud Shell Quickstart - Bash](#).
[Launch Cloud Shell](#)
- If you prefer to run CLI reference commands locally, [install](#) the Azure CLI. If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a Docker container](#).
 - If you're using a local installation, sign in to the Azure CLI by using the [az login](#) command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).

- When you're prompted, install the Azure CLI extension on first use. For more information about extensions, see [Use extensions with the Azure CLI](#).
- Run `az version` to find the version and dependent libraries that are installed. To upgrade to the latest version, run `az upgrade`.
- This article requires version 2.0.64 or later of the Azure CLI. If using Azure Cloud Shell, the latest version is already installed.
- The identity you're using to create your cluster has the appropriate minimum permissions. For more details on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).
- If you have multiple Azure subscriptions, select the appropriate subscription ID in which the resources should be billed using the `az account` command.

Limitations

The following limitations apply when you create and manage AKS clusters that support multiple node pools:

- You can't delete the first node pool.

The following additional limitations apply to Windows Server node pools:

- The AKS cluster can have a maximum of 10 node pools.
- The AKS cluster can have a maximum of 100 nodes in each node pool.
- The Windows Server node pool name has a limit of 6 characters.

Create a resource group

An Azure resource group is a logical group in which Azure resources are deployed and managed. When you create a resource group, you're asked to specify a location. This location is where resource group metadata is stored, it is also where your resources run in Azure if you don't specify another region during resource creation. Create a resource group using the `az group create` command.

The following example creates a resource group named `myResourceGroup` in the `eastus` location.

NOTE

This article uses Bash syntax for the commands in this tutorial. If you're using Azure Cloud Shell, ensure that the dropdown in the upper-left of the Cloud Shell window is set to **Bash**.

```
az group create --name myResourceGroup --location eastus
```

The following example output shows the resource group created successfully:

```
{
  "id": "/subscriptions/<guid>/resourceGroups/myResourceGroup",
  "location": "eastus",
  "managedBy": null,
  "name": "myResourceGroup",
  "properties": {
    "provisioningState": "Succeeded"
  },
  "tags": null,
  "type": null
}
```

Create an AKS cluster

To run an AKS cluster that supports node pools for Windows Server containers, your cluster needs to use a network policy that uses [Azure CNI \(advanced\)](#) network plugin. For more detailed information to help plan out the required subnet ranges and network considerations, see [configure Azure CNI networking](#). Use the `az aks create` command to create an AKS cluster named *myAKSCluster*. This command will create the necessary network resources if they don't exist.

- The cluster is configured with two nodes.
- The `--windows-admin-password` and `--windows-admin-username` parameters set the administrator credentials for any Windows Server nodes on the cluster and must meet [Windows Server password requirements](#). If you don't specify the `--windows-admin-password` parameter, you will be prompted to provide a value.
- The node pool uses `VirtualMachineScaleSets`.

NOTE

To ensure your cluster to operate reliably, you should run at least 2 (two) nodes in the default node pool.

Create a username to use as administrator credentials for the Windows Server nodes on your cluster. The following commands prompt you for a username and set it to *WINDOWS_USERNAME* for use in a later command (remember that the commands in this article are entered into a BASH shell).

```
echo "Please enter the username to use as administrator credentials for Windows Server nodes on your cluster: " && read WINDOWS_USERNAME
```

Create your cluster ensuring you specify `--windows-admin-username` parameter. The following example command creates a cluster using the value from *WINDOWS_USERNAME* you set in the previous command. Alternatively you can provide a different username directly in the parameter instead of using *WINDOWS_USERNAME*. The following command will also prompt you to create a password for the administrator credentials for the Windows Server nodes on your cluster. Alternatively, you can use the `--windows-admin-password` parameter and specify your own value there.

```
az aks create \
--resource-group myResourceGroup \
--name myAKSCluster \
--node-count 2 \
--enable-addons monitoring \
--generate-ssh-keys \
--windows-admin-username $WINDOWS_USERNAME \
--vm-set-type VirtualMachineScaleSets \
--network-plugin azure
```

NOTE

If you get a password validation error, verify the password you set meets the [Windows Server password requirements](#). If your password meets the requirements, try creating your resource group in another region. Then try creating the cluster with the new resource group.

If you do not specify an administrator username and password when setting `--vm-set-type VirtualMachineScaleSets` and `--network-plugin azure`, the username is set to *azureuser* and the password is set to a random value.

The administrator username can't be changed, but you can change the administrator password your AKS cluster uses for Windows Server nodes using `az aks update`. For more details, see [Windows Server node pools FAQ](#).

After a few minutes, the command completes and returns JSON-formatted information about the cluster. Occasionally the cluster can take longer than a few minutes to provision. Allow up to 10 minutes in these cases.

Add a Windows Server 2019 node pool

By default, an AKS cluster is created with a node pool that can run Linux containers. Use `az aks nodepool add` command to add an additional node pool that can run Windows Server containers alongside the Linux node pool.

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--os-type Windows \
--name npwin \
--node-count 1
```

The above command creates a new node pool named `npwin` and adds it to the `myAKSCluster`. The above command also uses the default subnet in the default vnet created when running `az aks create`.

Add a Windows Server 2022 node pool

When creating a Windows node pool, the default operating system will be Windows Server 2019. To use Windows Server 2022 nodes, you will need to specify an OS SKU type of `Windows2022`.

NOTE

Windows Server 2022 requires Kubernetes version "1.23.0" or higher.

Use `az aks nodepool add` command to add a Windows Server 2022 node pool:

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--os-type Windows \
--os-sku Windows2022 \
--name npwin \
--node-count 1
```

Optional: Using `containerd` with Windows Server node pools

Beginning in Kubernetes version 1.20 and greater, you can specify `containerd` as the container runtime for Windows Server 2019 node pools. From Kubernetes 1.23, `containerd` will be the default container runtime for Windows.

IMPORTANT

When using `containerd` with Windows Server 2019 node pools:

- Both the control plane and Windows Server 2019 node pools must use Kubernetes version 1.20 or greater.
- When creating or updating a node pool to run Windows Server containers, the default value for `--node-vm-size` is `Standard_D2s_v3` which was minimum recommended size for Windows Server 2019 node pools prior to Kubernetes 1.20. The minimum recommended size for Windows Server 2019 node pools using `containerd` is `Standard_D4s_v3`. When setting the `--node-vm-size` parameter, please check the list of [restricted VM sizes](#).
- It is highly recommended that you use [taints or labels](#) with your Windows Server 2019 node pools running `containerd` and tolerations or node selectors with your deployments to guarantee your workloads are scheduled correctly.

Add a Windows Server node pool with `containerd`

Use the `az aks nodepool add` command to add a node pool that can run Windows Server containers with the `containerd` runtime.

NOTE

If you do not specify the `WindowsContainerRuntime=containerd` custom header, the node pool will still use `containerd` as the container runtime by default.

```
az aks nodepool add \
  --resource-group myResourceGroup \
  --cluster-name myAKSCluster \
  --os-type Windows \
  --name npwcd \
  --node-vm-size Standard_D4s_v3 \
  --kubernetes-version 1.20.5 \
  --aks-custom-headers WindowsContainerRuntime=containerd \
  --node-count 1
```

The above command creates a new Windows Server node pool using `containerd` as the runtime named `npwcd` and adds it to the `myAKSCluster`. The above command also uses the default subnet in the default vnet created when running `az aks create`.

Upgrade an existing Windows Server node pool to `containerd`

Use the `az aks nodepool upgrade` command to upgrade a specific node pool from Docker to `containerd`.

```
az aks nodepool upgrade \
  --resource-group myResourceGroup \
  --cluster-name myAKSCluster \
  --name npwd \
  --kubernetes-version 1.20.7 \
  --aks-custom-headers WindowsContainerRuntime=containerd
```

The above command upgrades a node pool named `npwd` to the `containerd` runtime.

To upgrade all existing node pools in a cluster to use the `containerd` runtime for all Windows Server node pools:

```
az aks upgrade \
--resource-group myResourceGroup \
--name myAKScluster \
--kubernetes-version 1.20.7 \
--aks-custom-headers WindowsContainerRuntime=containerd
```

The above command upgrades all Windows Server node pools in the *myAKScluster* to use the `containerd` runtime.

NOTE

When running the upgrade command, the `--kubernetes-version` specified must be a higher version than the node pool's current version.

Connect to the cluster

To manage a Kubernetes cluster, you use `kubectl`, the Kubernetes command-line client. If you use Azure Cloud Shell, `kubectl` is already installed. To install `kubectl` locally, use the [az aks install-cli](#) command:

```
az aks install-cli
```

To configure `kubectl` to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command. This command downloads credentials and configures the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group myResourceGroup --name myAKScluster
```

To verify the connection to your cluster, use the `kubectl get` command to return a list of the cluster nodes.

```
kubectl get nodes -o wide
```

The following example output shows all nodes in the cluster. Make sure that the status of all nodes is *Ready*:

NAME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE
KERNEL-VERSION	CONTAINER-RUNTIME						
aks-nodepool1-12345678-vmss00000	Ready	agent	34m	v1.20.7	10.240.0.4	<none>	Ubuntu
18.04.5 LTS	5.4.0-1046-azure				containerd://1.4.4+azure		
aks-nodepool1-12345678-vmss00001	Ready	agent	34m	v1.20.7	10.240.0.35	<none>	Ubuntu
18.04.5 LTS	5.4.0-1046-azure				containerd://1.4.4+azure		
aksnpwcd123456	Ready	agent	9m6s	v1.20.7	10.240.0.97	<none>	Windows
Server 2019 Datacenter	10.0.17763.1879				containerd://1.4.4+unknown		
aksnpwin987654	Ready	agent	25m	v1.20.7	10.240.0.66	<none>	Windows
Server 2019 Datacenter	10.0.17763.1879				docker://19.3.14		

NOTE

The container runtime for each node pool is shown under *CONTAINER-RUNTIME*. Notice `aksnpwin987654` begins with `docker://` which means it is using Docker for the container runtime. Notice `aksnpwcd123456` begins with `containerd://` which means it is using `containerd` for the container runtime.

Deploy the application

A Kubernetes manifest file defines a desired state for the cluster, such as what container images to run. In this

article, a manifest is used to create all objects needed to run the ASP.NET sample application in a Windows Server container. This manifest includes a [Kubernetes deployment](#) for the ASP.NET sample application and an external [Kubernetes service](#) to access the application from the internet.

The ASP.NET sample application is provided as part of the [.NET Framework Samples](#) and runs in a Windows Server container. AKS requires Windows Server containers to be based on images of *Windows Server 2019* or greater. The Kubernetes manifest file must also define a [node selector](#) to tell your AKS cluster to run your ASP.NET sample application's pod on a node that can run Windows Server containers.

Create a file named `sample.yaml` and copy in the following YAML definition. If you use the Azure Cloud Shell, this file can be created using `code`, `vi`, or `nano` as if working on a virtual or physical system:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: sample
  labels:
    app: sample
spec:
  replicas: 1
  template:
    metadata:
      name: sample
      labels:
        app: sample
    spec:
      nodeSelector:
        "kubernetes.io/os": windows
      containers:
        - name: sample
          image: mcr.microsoft.com/dotnet/framework/samples:aspnetapp
          resources:
            limits:
              cpu: 1
              memory: 800M
            ports:
              - containerPort: 80
      selector:
        matchLabels:
          app: sample
---
apiVersion: v1
kind: Service
metadata:
  name: sample
spec:
  type: LoadBalancer
  ports:
    - protocol: TCP
      port: 80
  selector:
    app: sample
```

Deploy the application using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f sample.yaml
```

The following example output shows the Deployment and Service created successfully:

```
deployment.apps/sample created
service/sample created
```

Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete. Occasionally the service can take longer than a few minutes to provision. Allow up to 10 minutes in these cases.

To monitor progress, use the `kubectl get service` command with the `--watch` argument.

```
kubectl get service sample --watch
```

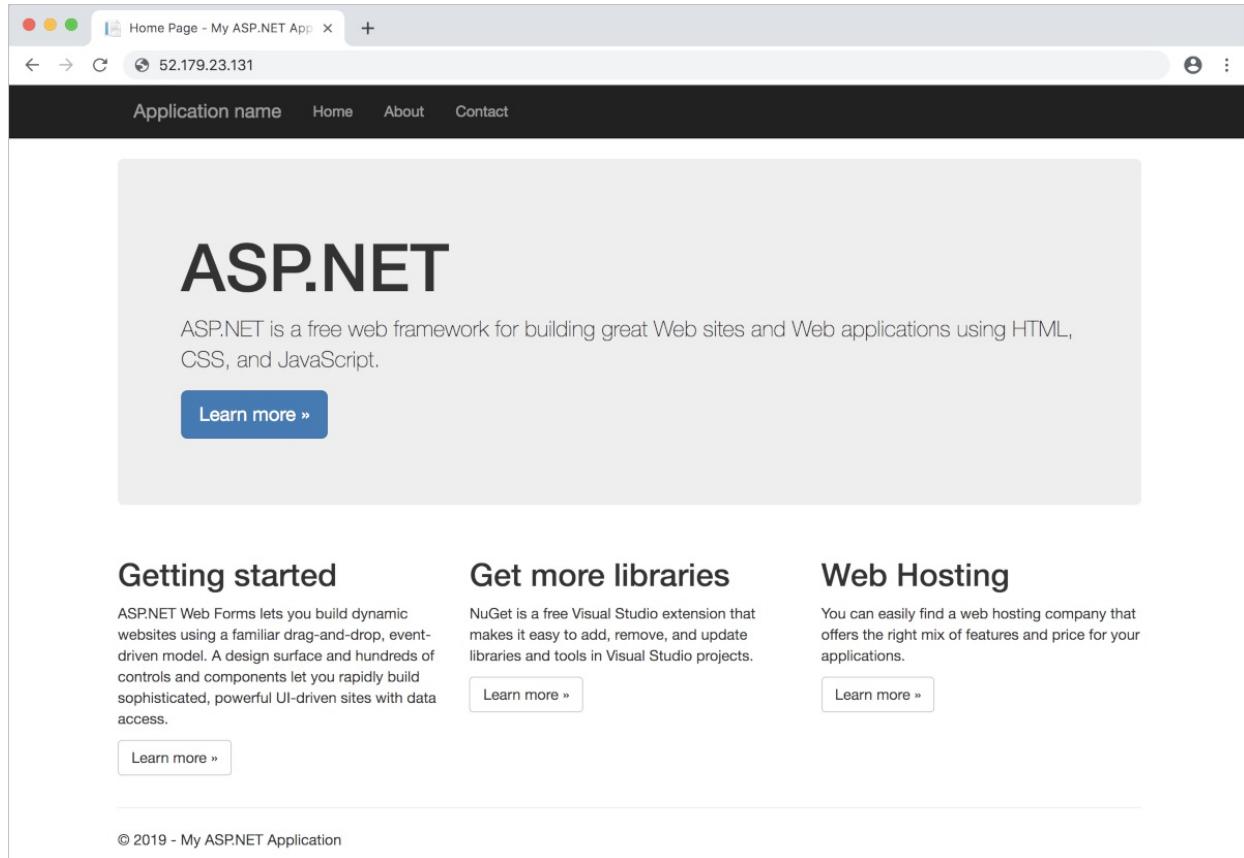
Initially the *EXTERNAL-IP* for the *sample* service is shown as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
sample	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

When the *EXTERNAL-IP* address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
sample  LoadBalancer  10.0.37.27  52.179.23.131  80:30572/TCP  2m
```

To see the sample app in action, open a web browser to the external IP address of your service.



The screenshot shows a web browser window with the title "Home Page - My ASP.NET App". The address bar displays "52.179.23.131". The page content is the ASP.NET welcome page, featuring the "ASP.NET" logo and a brief description: "ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS, and JavaScript." A blue "Learn more »" button is visible. Below this, there are three sections: "Getting started", "Get more libraries", and "Web Hosting", each with a "Learn more »" button. At the bottom of the page, a copyright notice reads "© 2019 - My ASPNET Application".

NOTE

If you receive a connection timeout when trying to load the page then you should verify the sample app is ready with the following command [`kubectl get pods --watch`]. Sometimes the Windows container will not be started by the time your external IP address is available.

Delete cluster

To avoid Azure charges, if you don't plan on going through the tutorials that follow, use the [az group delete](#) command to remove the resource group, container service, and all related resources.

```
az group delete --name myResourceGroup --yes --no-wait
```

NOTE

The AKS cluster was created with system-assigned managed identity (default identity option used in this quickstart), the identity is managed by the platform and does not require removal.

Next steps

In this article, you deployed a Kubernetes cluster and deployed an ASP.NET sample application in a Windows Server container to it.

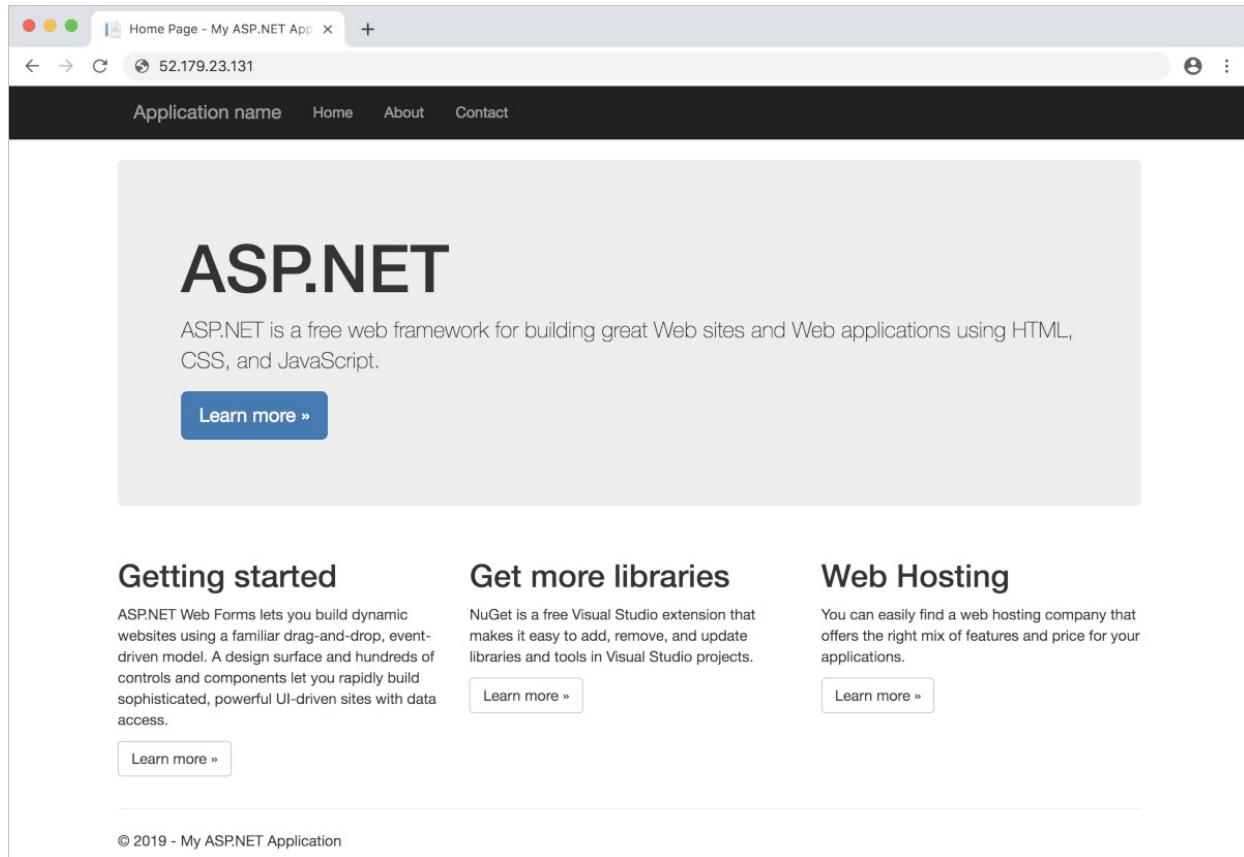
To learn more about AKS, and walk through a complete code to deployment example, continue to the Kubernetes cluster tutorial.

[AKS tutorial](#)

Create a Windows Server container on an Azure Kubernetes Service (AKS) cluster using PowerShell

10/27/2022 • 8 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage clusters. In this article, you deploy an AKS cluster running Windows Server 2019 containers using PowerShell. You also deploy an [ASP.NET](#) sample application in a Windows Server container to the cluster.



This article assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

Prerequisites

If you don't have an Azure subscription, create a [free](#) account before you begin.

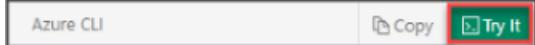
- The identity you are using to create your cluster has the appropriate minimum permissions. For more details on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).
- If you choose to use PowerShell locally, you need to install the [Az PowerShell](#) module and connect to your Azure account using the [Connect-AzAccount](#) cmdlet. For more information about installing the Az PowerShell module, see [Install Azure PowerShell](#).

Azure Cloud Shell

Azure hosts Azure Cloud Shell, an interactive shell environment that you can use through your browser. You can use either Bash or PowerShell with Cloud Shell to work with Azure services. You can use the Cloud Shell preinstalled commands to run the code in this article, without having to install anything on your local

environment.

To start Azure Cloud Shell:

OPTION	EXAMPLE/LINK
Select Try It in the upper-right corner of a code or command block. Selecting Try It doesn't automatically copy the code or command to Cloud Shell.	
Go to https://shell.azure.com , or select the Launch Cloud Shell button to open Cloud Shell in your browser.	
Select the Cloud Shell button on the menu bar at the upper right in the Azure portal .	

To use Azure Cloud Shell:

1. Start Cloud Shell.
2. Select the **Copy** button on a code block (or command block) to copy the code or command.
3. Paste the code or command into the Cloud Shell session by selecting **Ctrl+Shift+V** on Windows and Linux, or by selecting **Cmd+Shift+V** on macOS.
4. Select **Enter** to run the code or command.

If you have multiple Azure subscriptions, choose the appropriate subscription in which the resources should be billed. Select a specific subscription ID using the [Set-AzContext](#) cmdlet.

```
Set-AzContext -SubscriptionId 00000000-0000-0000-0000-000000000000
```

Limitations

The following limitations apply when you create and manage AKS clusters that support multiple node pools:

- You can't delete the first node pool.

The following additional limitations apply to Windows Server node pools:

- The AKS cluster can have a maximum of 10 node pools.
- The AKS cluster can have a maximum of 100 nodes in each node pool.
- The Windows Server node pool name has a limit of 6 characters.

Create a resource group

An [Azure resource group](#) is a logical group in which Azure resources are deployed and managed. When you create a resource group, you are asked to specify a location. This location is where resource group metadata is stored, it is also where your resources run in Azure if you don't specify another region during resource creation. Create a resource group using the [New-AzResourceGroup](#) cmdlet.

The following example creates a resource group named **myResourceGroup** in the **eastus** location.

NOTE

This article uses PowerShell syntax for the commands in this tutorial. If you are using Azure Cloud Shell, ensure that the dropdown in the upper-left of the Cloud Shell window is set to **PowerShell**.

```
New-AzResourceGroup -Name myResourceGroup -Location eastus
```

The following example output shows the resource group created successfully:

```
ResourceGroupName : myResourceGroup
Location         : eastus
ProvisioningState : Succeeded
Tags             :
ResourceId       : /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/myResourceGroup
```

Create an AKS cluster

To run an AKS cluster that supports node pools for Windows Server containers, your cluster needs to use a network policy that uses [Azure CNI](#) (advanced) network plugin. For more detailed information to help plan out the required subnet ranges and network considerations, see [configure Azure CNI networking](#). Use the [New-AzAksCluster](#) cmdlet below to create an AKS cluster named **myAKSCluster**. The following example creates the necessary network resources if they don't exist.

NOTE

To ensure your cluster operates reliably, you should run at least 2 (two) nodes in the default node pool.

```
$AdminCreds = Get-Credential -Message 'Please create the administrator credentials for your Windows Server
containers'
New-AzAksCluster -ResourceGroupName myResourceGroup -Name myAKSCluster -NodeCount 2 -NetworkPlugin azure -
NodeVmSetType VirtualMachineScaleSets -WindowsProfileAdminUserName $AdminCreds.UserName -
WindowsProfileAdminUserPassword $AdminCreds.Password -GenerateSshKey
```

NOTE

If you are unable to create the AKS cluster because the version is not supported in this region then you can use the `Get-AzAksVersion -Location eastus` command to find the supported version list for this region.

After a few minutes, the command completes and returns information about the cluster. Occasionally the cluster can take longer than a few minutes to provision. Allow up to 10 minutes in these cases.

Add a Windows Server node pool

By default, an AKS cluster is created with a node pool that can run Linux containers. Use `New-AzAksNodePool` cmdlet to add a node pool that can run Windows Server containers alongside the Linux node pool.

```
New-AzAksNodePool -ResourceGroupName myResourceGroup -ClusterName myAKSCluster -VmSetType
VirtualMachineScaleSets -OsType Windows -Name npwin
```

The above command creates a new node pool named **npwin** and adds it to the **myAKSCluster**. When creating

a node pool to run Windows Server containers, the default value for `-VmSize` is **Standard_D2s_v3**. If you choose to set the `-VmSize` parameter, check the list of [restricted VM sizes](#). The minimum recommended size is **Standard_D2s_v3**. The previous command also uses the default subnet in the default vnet created when running `New-AzAksCluster`.

Connect to the cluster

To manage a Kubernetes cluster, you use [kubectl](#), the Kubernetes command-line client. If you use Azure Cloud Shell, `kubectl` is already installed. To install `kubectl` locally, use the `Install-AzAksKubectl` cmdlet:

```
Install-AzAksKubectl
```

To configure `kubectl` to connect to your Kubernetes cluster, use the [Import-AzAksCredential](#) cmdlet. This command downloads credentials and configures the Kubernetes CLI to use them.

```
Import-AzAksCredential -ResourceGroupName myResourceGroup -Name myAKSCluster
```

To verify the connection to your cluster, use the [kubectl get](#) command to return a list of the cluster nodes.

```
kubectl get nodes
```

The following example output shows all the nodes in the cluster. Make sure that the status of all nodes is **Ready**:

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-12345678-vmssfedcba	Ready	agent	13m	v1.16.7
aksnpwin987654	Ready	agent	108s	v1.16.7

Deploy the application

A Kubernetes manifest file defines a desired state for the cluster, such as what container images to run. In this article, a manifest is used to create all objects needed to run the ASP.NET sample application in a Windows Server container. This manifest includes a [Kubernetes deployment](#) for the ASP.NET sample application and an external [Kubernetes service](#) to access the application from the internet.

The ASP.NET sample application is provided as part of the [.NET Framework Samples](#) and runs in a Windows Server container. AKS requires Windows Server containers to be based on images of **Windows Server 2019** or greater. The Kubernetes manifest file must also define a [node selector](#) to tell your AKS cluster to run your ASP.NET sample application's pod on a node that can run Windows Server containers.

Create a file named `sample.yaml` and copy in the following YAML definition. If you use the Azure Cloud Shell, this file can be created using `code`, `vi`, or `nano` as if working on a virtual or physical system:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: sample
  labels:
    app: sample
spec:
  replicas: 1
  template:
    metadata:
      name: sample
      labels:
        app: sample
    spec:
      nodeSelector:
        "kubernetes.io/os": windows
      containers:
        - name: sample
          image: mcr.microsoft.com/dotnet/framework/samples:aspnetapp
          resources:
            limits:
              cpu: 1
              memory: 800M
            ports:
              - containerPort: 80
      selector:
        matchLabels:
          app: sample
---
apiVersion: v1
kind: Service
metadata:
  name: sample
spec:
  type: LoadBalancer
  ports:
    - protocol: TCP
      port: 80
  selector:
    app: sample
```

Deploy the application using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f sample.yaml
```

The following example output shows the Deployment and Service created successfully:

```
deployment.apps/sample created
service/sample created
```

Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete. Occasionally the service can take longer than a few minutes to provision. Allow up to 10 minutes in these cases.

To monitor progress, use the [kubectl get service](#) command with the `--watch` argument.

```
kubectl get service sample --watch
```

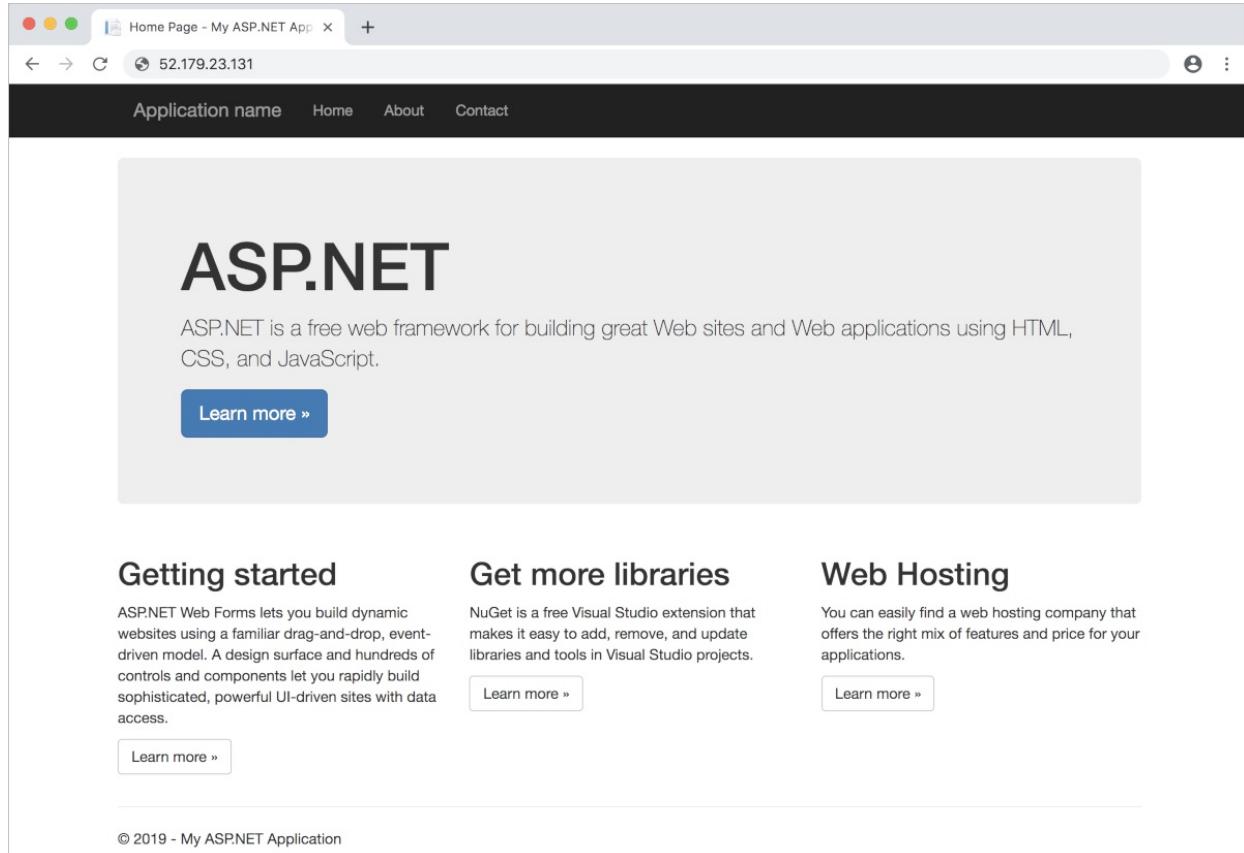
Initially the EXTERNAL-IP for the **sample** service is shown as **pending**.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
sample	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

When the EXTERNAL-IP address changes from **pending** to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
sample  LoadBalancer  10.0.37.27  52.179.23.131  80:30572/TCP  2m
```

To see the sample app in action, open a web browser to the external IP address of your service.



NOTE

If you receive a connection timeout when trying to load the page then you should verify the sample app is ready with the following command `kubectl get pods --watch`. Sometimes the Windows container will not be started by the time your external IP address is available.

Delete cluster

To avoid Azure charges, if you don't plan on going through the tutorials that follow, use the [Remove-AzResourceGroup](#) cmdlet to remove the resource group, container service, and all related resources.

```
Remove-AzResourceGroup -Name myResourceGroup
```

NOTE

The AKS cluster was created with system-assigned managed identity (default identity option used in this quickstart), the identity is managed by the platform and does not require removal.

Next steps

In this article, you deployed a Kubernetes cluster and deployed an [ASP .NET](#) sample application in a Windows Server container to it.

To learn more about AKS, and walk through a complete code to deployment example, continue to the Kubernetes cluster tutorial.

[AKS tutorial](#)

Quickstart: Develop on Azure Kubernetes Service (AKS) with Helm

10/27/2022 • 5 minutes to read • [Edit Online](#)

[Helm](#) is an open-source packaging tool that helps you install and manage the lifecycle of Kubernetes applications. Similar to Linux package managers like *APT* and *Yum*, Helm manages Kubernetes charts, which are packages of pre-configured Kubernetes resources.

In this quickstart, you'll use Helm to package and run an application on AKS. For more details on installing an existing application using Helm, see the [Install existing applications with Helm in AKS](#) how-to guide.

Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI](#) or [Azure PowerShell](#) installed.
- [Helm v3](#) installed.

Create an Azure Container Registry

You'll need to store your container images in an Azure Container Registry (ACR) to run your application in your AKS cluster using Helm. Provide your own registry name unique within Azure and containing 5-50 alphanumeric characters. The *Basic* SKU is a cost-optimized entry point for development purposes that provides a balance of storage and throughput.

- [Azure CLI](#)
- [Azure PowerShell](#)

The below example uses `az acr create` to create an ACR named *MyHelmACR* in *MyResourceGroup* with the *Basic* SKU.

```
az group create --name MyResourceGroup --location eastus
az acr create --resource-group MyResourceGroup --name MyHelmACR --sku Basic
```

Output will be similar to the following example. Take note of your *loginServer* value for your ACR since you'll use it in a later step. In the below example, *myhelmacr.azurecr.io* is the *loginServer* for *MyHelmACR*.

```
{  
    "adminUserEnabled": false,  
    "creationDate": "2019-06-11T13:35:17.998425+00:00",  
    "id":  
        "/subscriptions/<ID>/resourceGroups/MyResourceGroup/providers/Microsoft.ContainerRegistry/registries/MyHelmACR",  
    "location": "eastus",  
    "loginServer": "myhelmacr.azurecr.io",  
    "name": "MyHelmACR",  
    "networkRuleSet": null,  
    "provisioningState": "Succeeded",  
    "resourceGroup": "MyResourceGroup",  
    "sku": {  
        "name": "Basic",  
        "tier": "Basic"  
    },  
    "status": null,  
    "storageAccount": null,  
    "tags": {},  
    "type": "Microsoft.ContainerRegistry/registries"  
}
```

Create an AKS cluster

Your new AKS cluster needs access to your ACR to pull the container images and run them. Use the following command to:

- Create an AKS cluster called *MyAKS* and attach *MyHelmACR*.
- Grant the *MyAKS* cluster access to your *MyHelmACR* ACR.
- [Azure CLI](#)
- [Azure PowerShell](#)

```
az aks create --resource-group MyResourceGroup --name MyAKS --location eastus --attach-acr MyHelmACR --generate-ssh-keys
```

Connect to your AKS cluster

To connect a Kubernetes cluster locally, use the Kubernetes command-line client, `kubectl`. `kubectl` is already installed if you use Azure Cloud Shell.

- [Azure CLI](#)
- [Azure PowerShell](#)

1. Install `kubectl` locally using the `az aks install-cli` command:

```
az aks install-cli
```

2. Configure `kubectl` to connect to your Kubernetes cluster using the `az aks get-credentials` command. The following command example gets credentials for the AKS cluster named *MyAKS* in the *MyResourceGroup*:

```
az aks get-credentials --resource-group MyResourceGroup --name MyAKS
```

Download the sample application

This quickstart uses the [Azure Vote application](#). Clone the application from GitHub and navigate to the `azure-vote` directory.

```
git clone https://github.com/Azure-Samples/azure-voting-app-redis.git
cd azure-voting-app-redis/azure-vote/
```

Build and push the sample application to the ACR

Using the preceding Dockerfile, run the `az acr build` command to build and push an image to the registry. The `.` at the end of the command provides the location of the source code directory path (in this case, the current directory). The `--file` parameter takes in the path of the Dockerfile relative to this source code directory path.

```
az acr build --image azure-vote-front:v1 --registry MyHelmACR --file Dockerfile .
```

NOTE

In addition to importing container images into your ACR, you can also import Helm charts into your ACR. For more information, see [Push and pull Helm charts to an Azure container registry](#).

Create your Helm chart

Generate your Helm chart using the `helm create` command.

```
helm create azure-vote-front
```

Update `azure-vote-front/Chart.yaml` to add a dependency for the `redis` chart from the <https://charts.bitnami.com/bitnami> chart repository and update `appVersion` to `v1`. For example:

NOTE

The container image versions shown in this guide have been tested to work with this example but may not be the latest version available.

```
apiVersion: v2
name: azure-vote-front
description: A Helm chart for Kubernetes

dependencies:
  - name: redis
    version: 14.7.1
    repository: https://charts.bitnami.com/bitnami

...
# This is the version number of the application being deployed. This version number should be
# incremented each time you make changes to the application.
appVersion: v1
```

Update your helm chart dependencies using `helm dependency update`:

```
helm dependency update azure-vote-front
```

Update *azure-vote-front/values.yaml*:

- Add a *redis* section to set the image details, container port, and deployment name.
- Add a *backendName* for connecting the frontend portion to the *redis* deployment.
- Change *image.repository* to <loginServer>/azure-vote-front .
- Change *image.tag* to v1 .
- Change *service.type* to *LoadBalancer*.

For example:

```
# Default values for azure-vote-front.
# This is a YAML-formatted file.
# Declare variables to be passed into your templates.

replicaCount: 1
backendName: azure-vote-backend-master
redis:
  image:
    registry: mcr.microsoft.com
    repository: oss/bitnami/redis
    tag: 6.0.8
  fullnameOverride: azure-vote-backend
  auth:
    enabled: false

  image:
    repository: myhelmacr.azurecr.io/azure-vote-front
    pullPolicy: IfNotPresent
    tag: "v1"
...
service:
  type: LoadBalancer
  port: 80
...
```

Add an `env` section to *azure-vote-front/templates/deployment.yaml* for passing the name of the *redis* deployment.

```
...
  containers:
    - name: {{ .Chart.Name }}
      securityContext:
        {{- toYaml .Values.securityContext | nindent 12 --}}
      image: "{{ .Values.image.repository }}:{{ .Values.image.tag | default .Chart.AppVersion }}"
      imagePullPolicy: {{ .Values.image.pullPolicy }}
      env:
        - name: REDIS
          value: {{ .Values.backendName }}
...

```

Run your Helm chart

Install your application using your Helm chart using the `helm install` command.

```
helm install azure-vote-front azure-vote-front/
```

It takes a few minutes for the service to return a public IP address. Monitor progress using the `kubectl get service` command with the `--watch` argument.

```
$ kubectl get service azure-vote-front --watch
NAME           TYPE      CLUSTER-IP   EXTERNAL-IP     PORT(S)        AGE
azure-vote-front  LoadBalancer  10.0.18.228 <pending>    80:32021/TCP  6s
...
azure-vote-front  LoadBalancer  10.0.18.228  52.188.140.81  80:32021/TCP  2m6s
```

Navigate to your application's load balancer in a browser using the `<EXTERNAL-IP>` to see the sample application.

Delete the cluster

- [Azure CLI](#)
- [Azure PowerShell](#)

Use the `az group delete` command to remove the resource group, the AKS cluster, the container registry, the container images stored in the ACR, and all related resources.

```
az group delete --name MyResourceGroup --yes --no-wait
```

NOTE

If the AKS cluster was created with system-assigned managed identity (default identity option used in this quickstart), the identity is managed by the platform and does not require removal.

If the AKS cluster was created with service principal as the identity option instead, then when you delete the cluster, the service principal used by the AKS cluster is not removed. For steps on how to remove the service principal, see [AKS service principal considerations and deletion](#).

Next steps

For more information about using Helm, see the Helm documentation.

[Helm documentation](#)

Quickstart: Deploy an application using the Dapr cluster extension for Azure Kubernetes Service (AKS) or Arc-enabled Kubernetes

10/27/2022 • 4 minutes to read • [Edit Online](#)

In this quickstart, you will get familiar with using the [Dapr cluster extension](#) in an AKS or Arc-enabled Kubernetes cluster. You will be deploying a hello world example, consisting of a Python application that generates messages and a Node application that consumes and persists them.

Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI](#) or [Azure PowerShell](#) installed.
- An AKS or Arc-enabled Kubernetes cluster with the [Dapr cluster extension](#) enabled

Clone the repository

To obtain the files you'll be using to deploy the sample application, clone the [Quickstarts repository](#) and change to the `hello-kubernetes` directory:

```
git clone https://github.com/dapr/quickstarts.git
cd quickstarts/hello-kubernetes
```

Create and configure a state store

Dapr can use a number of different state stores (Redis, Azure Cosmos DB, DynamoDB, Cassandra, etc.) to persist and retrieve state. For this example, we will use Redis.

Create a Redis store

1. Open the [Azure portal](#) to start the Azure Redis Cache creation flow.
2. Fill out the necessary information
3. Click "Create" to kickoff deployment of your Redis instance.
4. Take note of the hostname of your Redis instance, which you can retrieve from the "Overview" in Azure. It should look like `xxxxxx.redis.cache.windows.net:6380`.
5. Once your instance is created, you'll need to grab your access key. Navigate to "Access Keys" under "Settings" and create a Kubernetes secret to store your Redis password:

```
kubectl create secret generic redis --from-literal=redis-password=<your-redis-password>
```

Configure the Dapr components

Once your store is created, you will need to add the keys to the `redis.yaml` file in the `deploy` directory of the Hello World repository. Replace the `redisHost` value with your own Redis master address, and the `redisPassword` with your own Secret. You can learn more [here](#).

You will also need to add the following two lines below `redisPassword` to enable connection over TLS:

```
- name: redisPassword
  secretKeyRef:
    name: redis
    key: redis-password
- name: enableTLS
  value: true
```

Apply the configuration

Apply the `redis.yaml` file:

```
kubectl apply -f ./deploy/redis.yaml
```

And verify that your state store was successfully configured in the output:

```
component.dapr.io/statestore created
```

Deploy the Node.js app with the Dapr sidecar

Apply the Node.js app's deployment to your cluster:

```
kubectl apply -f ./deploy/node.yaml
```

NOTE

Kubernetes deployments are asynchronous. This means you'll need to wait for the deployment to complete before moving on to the next steps. You can do so with the following command:

```
kubectl rollout status deploy/nodeapp
```

This will deploy the Node.js app to Kubernetes. The Dapr control plane will automatically inject the Dapr sidecar to the Pod. If you take a look at the `node.yaml` file, you will see how Dapr is enabled for that deployment:

- `dapr.io/enabled: true` - this tells the Dapr control plane to inject a sidecar to this deployment.
- `dapr.io/app-id: nodeapp` - this assigns a unique ID or name to the Dapr application, so it can be sent messages to and communicated with by other Dapr apps.

To access your service, obtain and make note of the `EXTERNAL-IP` via `kubectl`:

```
kubectl get svc nodeapp
```

Verify the service

To call the service, run:

```
curl $EXTERNAL_IP/ports
```

You should see output similar to the following:

```
{"DAPR_HTTP_PORT": "3500", "DAPR_GRPC_PORT": "50001"}
```

Next, submit an order to the application:

```
curl --request POST --data "@sample.json" --header Content-Type:application/json $EXTERNAL_IP/neworder
```

Confirm the order has been persisted by requesting it:

```
curl $EXTERNAL_IP/order
```

You should see output similar to the following:

```
{ "orderId": "42" }
```

TIP

This is a good time to get acquainted with the Dapr dashboard- a convenient interface to check status, information and logs of applications running on Dapr. The following command will make it available on <http://localhost:8080> :

```
kubectl port-forward svc/dapr-dashboard -n dapr-system 8080:8080
```

Deploy the Python app with the Dapr sidecar

Take a quick look at the Python app. Navigate to the Python app directory in the [hello-kubernetes](#) quickstart and open [app.py](#).

This is a basic Python app that posts JSON messages to <localhost:3500>, which is the default listening port for Dapr. You can invoke the Node.js application's [neworder](#) endpoint by posting to

[v1.0/invoke/nodeapp/method/neworder](#). The message contains some data with an [orderId](#) that increments once per second:

```
n = 0
while True:
    n += 1
    message = {"data": {"orderId": n}}

    try:
        response = requests.post(dapr_url, json=message)
    except Exception as e:
        print(e)

    time.sleep(1)
```

Deploy the Python app to your Kubernetes cluster:

```
kubectl apply -f ./deploy/python.yaml
```

NOTE

As with above, the following command will wait for the deployment to complete:

```
kubectl rollout status deploy/pythonapp
```

Observe messages and confirm persistence

Now that both the Node.js and Python applications are deployed, watch messages come through.

Get the logs of the Node.js app:

```
kubectl logs --selector=app=node -c node --tail=-1
```

If the deployments were successful, you should see logs like this:

```
Got a new order! Order ID: 1
Successfully persisted state
Got a new order! Order ID: 2
Successfully persisted state
Got a new order! Order ID: 3
Successfully persisted state
```

Call the Node.js app's order endpoint to get the latest order. Grab the external IP address that you saved before and, append "/order" and perform a GET request against it (enter it into your browser, use Postman, or `curl` it!):

```
curl $EXTERNAL_IP/order
{"orderID": "42"}
```

You should see the latest JSON in the response.

Clean up resources

- [Azure CLI](#)
- [Azure PowerShell](#)

Use the `az group delete` command to remove the resource group, the cluster, the namespace, and all related resources.

```
az group delete --name MyResourceGroup
```

Next steps

After successfully deploying this sample application:

[Learn more about other cluster extensions](#)

Quickstart: Subscribe to Azure Kubernetes Service (AKS) events with Azure Event Grid

10/27/2022 • 3 minutes to read • [Edit Online](#)

Azure Event Grid is a fully managed event routing service that provides uniform event consumption using a publish-subscribe model.

In this quickstart, you'll create an AKS cluster and subscribe to AKS events.

Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI](#) or [Azure PowerShell](#) installed.

Create an AKS cluster

- [Azure CLI](#)
- [Azure PowerShell](#)

Create an AKS cluster using the `az aks create` command. The following example creates a resource group *MyResourceGroup* and a cluster named *MyAKS* with one node in the *MyResourceGroup* resource group:

```
az group create --name MyResourceGroup --location eastus
az aks create -g MyResourceGroup -n MyAKS --location eastus --node-count 1 --generate-ssh-keys
```

Subscribe to AKS events

- [Azure CLI](#)
- [Azure PowerShell](#)

Create a namespace and event hub using `az eventhubs namespace create` and `az eventhubs eventhub create`.

The following example creates a namespace *MyNamespace* and an event hub *MyEventGridHub* in *MyNamespace*, both in the *MyResourceGroup* resource group.

```
az eventhubs namespace create --location eastus --name MyNamespace -g MyResourceGroup
az eventhubs eventhub create --name MyEventGridHub --namespace-name MyNamespace -g MyResourceGroup
```

NOTE

The *name* of your namespace must be unique.

Subscribe to the AKS events using `az eventgrid event-subscription create`:

```
SOURCE_RESOURCE_ID=$(az aks show -g MyResourceGroup -n MyAKS --query id --output tsv)
ENDPOINT=$(az eventhubs eventhub show -g MyResourceGroup -n MyEventGridHub --namespace-name MyNamespace --
query id --output tsv)
az eventgrid event-subscription create --name MyEventGridSubscription \
--source-resource-id $SOURCE_RESOURCE_ID \
--endpoint-type eventhub \
--endpoint $ENDPOINT
```

Verify your subscription to AKS events using `az eventgrid event-subscription list`:

```
az eventgrid event-subscription list --source-resource-id $SOURCE_RESOURCE_ID
```

The following example output shows you're subscribed to events from the *MyAKS* cluster and those events are delivered to the *MyEventGridHub* event hub:

```
[  
 {  
   "deadLetterDestination": null,  
   "deadLetterWithResourceIdentity": null,  
   "deliveryWithResourceIdentity": null,  
   "destination": {  
     "deliveryAttributeMappings": null,  
     "endpointType": "EventHub",  
     "resourceId":  
       "/subscriptions/SUBSCRIPTION_ID/resourceGroups/MyResourceGroup/providers/Microsoft.EventHub/namespaces/MyName  
space/eventhubs/MyEventGridHub"  
   },  
   "eventDeliverySchema": "EventGridSchema",  
   "expirationTimeUtc": null,  
   "filter": {  
     "advancedFilters": null,  
     "enableAdvancedFilteringOnArrays": null,  
     "includedEventTypes": [  
       "Microsoft.ContainerService.NewKubernetesVersionAvailable"  
     ],  
     "isSubjectCaseSensitive": null,  
     "subjectBeginsWith": "",  
     "subjectEndsWith": ""  
   },  
   "id":  
     "/subscriptions/SUBSCRIPTION_ID/resourceGroups/MyResourceGroup/providers/Microsoft.ContainerService/managedC  
lusters/MyAKS/providers/Microsoft.EventGrid/eventSubscriptions/MyEventGridSubscription",  
   "labels": null,  
   "name": "MyEventGridSubscription",  
   "provisioningState": "Succeeded",  
   "resourceGroup": "MyResourceGroup",  
   "retryPolicy": {  
     "eventTimeToLiveInMinutes": 1440,  
     "maxDeliveryAttempts": 30  
   },  
   "systemData": null,  
   "topic":  
     "/subscriptions/SUBSCRIPTION_ID/resourceGroups/MyResourceGroup/providers/microsoft.containerservice/managedc  
lusters/MyAKS",  
     "type": "Microsoft.EventGrid/eventSubscriptions"  
   }  
 ]
```

When AKS events occur, you'll see those events appear in your event hub. For example, when the list of available Kubernetes versions for your clusters changes, you'll see a

`Microsoft.ContainerService.NewKubernetesVersionAvailable` event. For more information on the events AKS

emits, see [Azure Kubernetes Service \(AKS\) as an Event Grid source](#).

Delete the cluster and subscriptions

- [Azure CLI](#)
- [Azure PowerShell](#)

Use the `az group delete` command to remove the resource group, the AKS cluster, namespace, and event hub, and all related resources.

```
az group delete --name MyResourceGroup --yes --no-wait
```

NOTE

When you delete the cluster, the Azure Active Directory service principal used by the AKS cluster is not removed. For steps on how to remove the service principal, see [AKS service principal considerations and deletion](#).

If you used a managed identity, the identity is managed by the platform and does not require removal.

Next steps

In this quickstart, you deployed a Kubernetes cluster and then subscribed to AKS events in Azure Event Hubs.

To learn more about AKS, and walk through a complete code to deployment example, continue to the Kubernetes cluster tutorial.

[AKS tutorial](#)

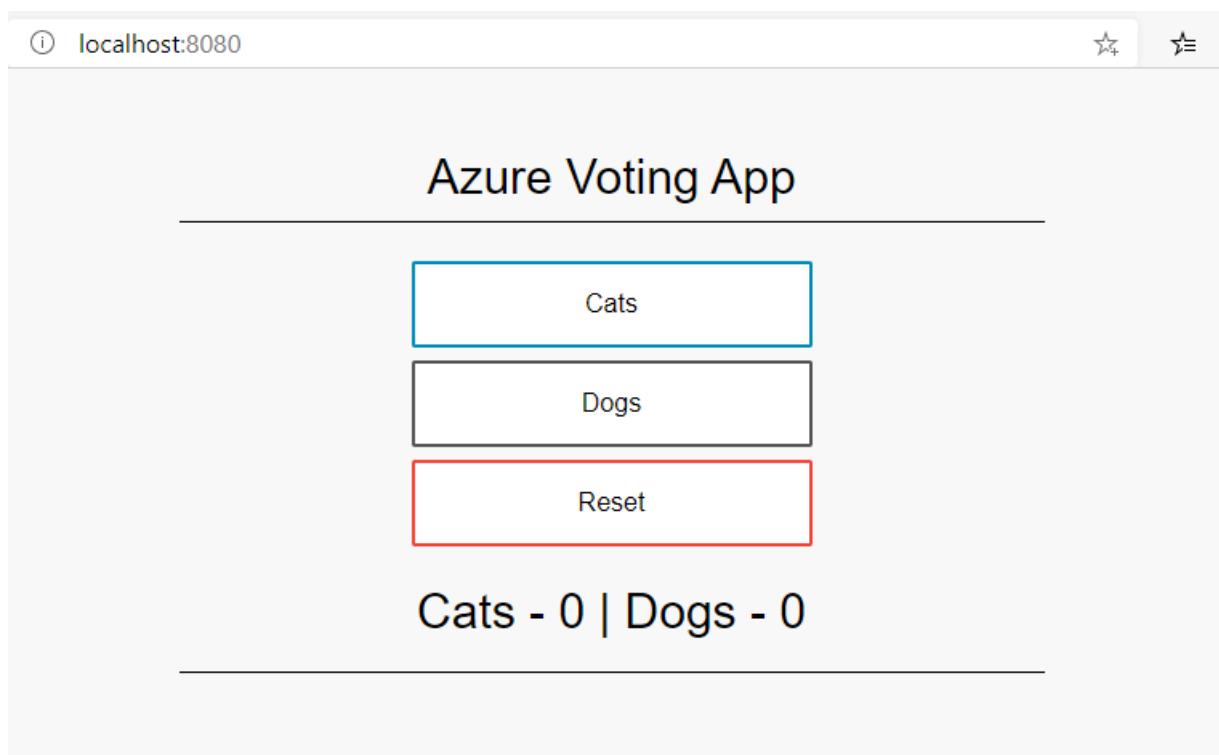
Tutorial: Prepare an application for Azure Kubernetes Service (AKS)

10/27/2022 • 3 minutes to read • [Edit Online](#)

In this tutorial, part one of seven, a multi-container application is prepared for use in Kubernetes. Existing development tools such as Docker Compose are used to locally build and test an application. You learn how to:

- Clone a sample application source from GitHub
- Create a container image from the sample application source
- Test the multi-container application in a local Docker environment

Once completed, the following application runs in your local development environment:



In later tutorials, the container image is uploaded to an Azure Container Registry, and then deployed into an AKS cluster.

Before you begin

This tutorial assumes a basic understanding of core Docker concepts such as containers, container images, and `docker` commands. For a primer on container basics, see [Get started with Docker](#).

To complete this tutorial, you need a local Docker development environment running Linux containers. Docker provides packages that configure Docker on a [Mac](#), [Windows](#), or [Linux](#) system.

NOTE

Azure Cloud Shell does not include the Docker components required to complete every step in these tutorials. Therefore, we recommend using a full Docker development environment.

Get application code

The [sample application](#) used in this tutorial is a basic voting app consisting of a front-end web component and a back-end Redis instance. The web component is packaged into a custom container image. The Redis instance uses an unmodified image from Docker Hub.

Use [git](#) to clone the sample application to your development environment:

```
git clone https://github.com/Azure-Samples/azure-voting-app-redis.git
```

Change into the cloned directory.

```
cd azure-voting-app-redis
```

Inside the directory is the application source code, a pre-created Docker compose file, and a Kubernetes manifest file. These files are used throughout the tutorial set. The contents and structure of the directory are as follows:

```
azure-voting-app-redis
|   azure-vote-all-in-one-redis.yaml
|   docker-compose.yaml
|   LICENSE
|   README.md

|-- azure-vote
|   |   app_init.supervisord.conf
|   |   Dockerfile
|   |   Dockerfile-for-app-service
|   |   sshd_config

|   |-- azure-vote
|       |       config_file.cfg
|       |       main.py

|       |       static
|           |           default.css

|       |       templates
|           |           index.html

|-- jenkins-tutorial
    |       config-jenkins.sh
    |       deploy-jenkins-vm.sh
```

Create container images

[Docker Compose](#) can be used to automate building container images and the deployment of multi-container applications.

Use the sample `docker-compose.yaml` file to create the container image, download the Redis image, and start the application:

```
docker-compose up -d
```

When completed, use the [docker images](#) command to see the created images. Three images have been downloaded or created. The *azure-vote-front* image contains the front-end application and uses the *nginx-flask* image as a base. The *redis* image is used to start a Redis instance.

```
$ docker images
```

REPOSITORY SIZE	TAG	IMAGE ID	CREATED
mcr.microsoft.com/azuredocs/azure-vote-front 944MB	v1	84b41c268ad9	9 seconds ago
mcr.microsoft.com/oss/bitnami/redis 103MB	6.0.8	3a54a920bb6c	2 days ago
tiangolo/uwsgi-nginx-flask 944MB	python3.6	a16ce562e863	6 weeks ago

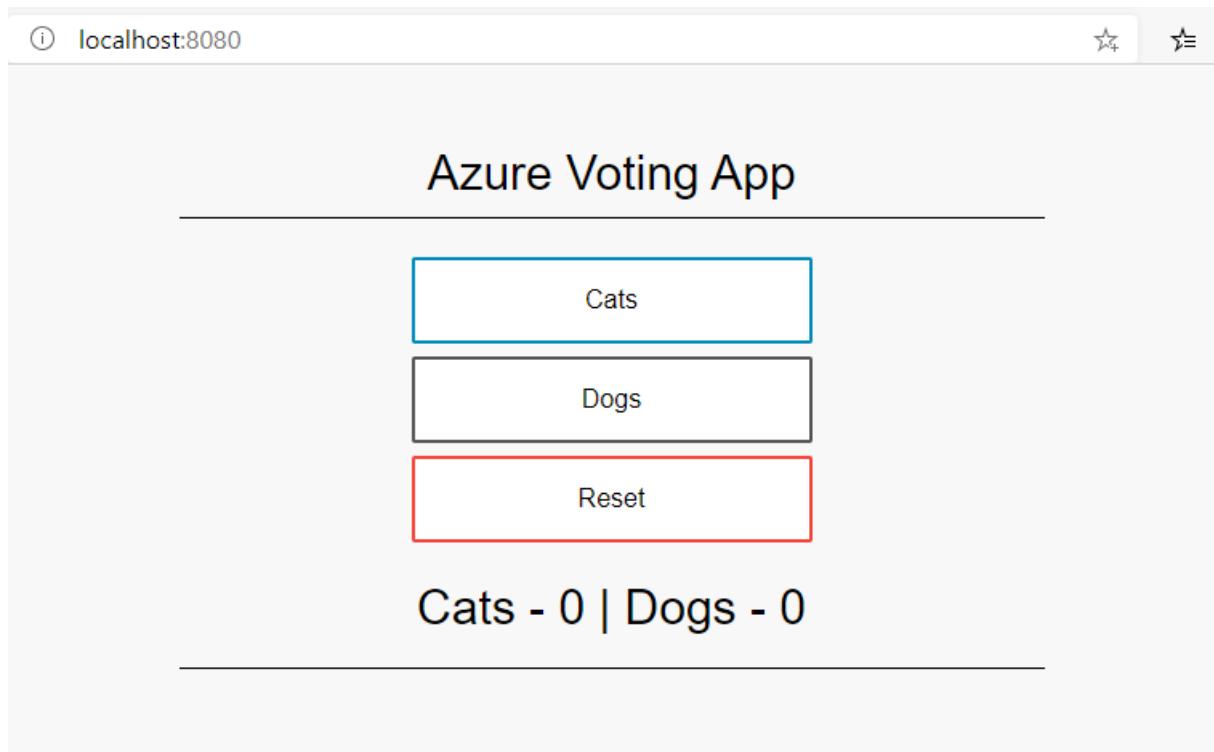
Run the [docker ps](#) command to see the running containers:

```
$ docker ps
```

CONTAINER ID STATUS	IMAGE PORTS	NAMES	COMMAND	CREATED
d10e5244f237 Up 3 minutes	mcr.microsoft.com/azuredocs/azure-vote-front:v1 443/tcp, 0.0.0.0:8080->80/tcp	azure-vote-front	"/entrypoint.sh /sta..."	3 minutes ago
21574cb38c1f Up 3 minutes	mcr.microsoft.com/oss/bitnami/redis:6.0.8 0.0.0.0:6379->6379/tcp	azure-vote-back	"/opt/bitnami/script..."	3 minutes ago

Test application locally

To see the running application, enter <http://localhost:8080> in a local web browser. The sample application loads, as shown in the following example:



Clean up resources

Now that the application's functionality has been validated, the running containers can be stopped and removed. ***Do not delete the container images*** - in the next tutorial, the *azure-vote-front* image is uploaded to an Azure Container Registry instance.

Stop and remove the container instances and resources with the [docker-compose down](#) command:

```
docker-compose down
```

When the local application has been removed, you have a Docker image that contains the Azure Vote application, *azure-vote-front*, for use with the next tutorial.

Next steps

In this tutorial, an application was tested and container images created for the application. You learned how to:

- Clone a sample application source from GitHub
- Create a container image from the sample application source
- Test the multi-container application in a local Docker environment

Advance to the next tutorial to learn how to store container images in Azure Container Registry.

[Push images to Azure Container Registry](#)

Tutorial: Deploy and use Azure Container Registry

10/27/2022 • 5 minutes to read • [Edit Online](#)

Azure Container Registry (ACR) is a private registry for container images. A private container registry lets you securely build and deploy your applications and custom code. In this tutorial, part two of seven, you deploy an ACR instance and push a container image to it. You learn how to:

- Create an Azure Container Registry (ACR) instance
- Tag a container image for ACR
- Upload the image to ACR
- View images in your registry

In later tutorials, this ACR instance is integrated with a Kubernetes cluster in AKS, and an application is deployed from the image.

Before you begin

In the [previous tutorial](#), a container image was created for a simple Azure Voting application. If you have not created the Azure Voting app image, return to [Tutorial 1 – Create container images](#).

- [Azure CLI](#)
- [Azure PowerShell](#)

This tutorial requires that you're running the Azure CLI version 2.0.53 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create an Azure Container Registry

To create an Azure Container Registry, you first need a resource group. An Azure resource group is a logical container into which Azure resources are deployed and managed.

- [Azure CLI](#)
- [Azure PowerShell](#)

Create a resource group with the `az group create` command. In the following example, a resource group named `myResourceGroup` is created in the `eastus` region:

```
az group create --name myResourceGroup --location eastus
```

Create an Azure Container Registry instance with the `az acr create` command and provide your own registry name. The registry name must be unique within Azure, and contain 5-50 alphanumeric characters. In the rest of this tutorial, `<acrName>` is used as a placeholder for the container registry name. Provide your own unique registry name. The `Basic` SKU is a cost-optimized entry point for development purposes that provides a balance of storage and throughput.

```
az acr create --resource-group myResourceGroup --name <acrName> --sku Basic
```

Log in to the container registry

- [Azure CLI](#)
- [Azure PowerShell](#)

To use the ACR instance, you must first log in. Use the `az acr login` command and provide the unique name given to the container registry in the previous step.

```
az acr login --name <acrName>
```

The command returns a *Login Succeeded* message once completed.

Tag a container image

To see a list of your current local images, use the `docker images` command:

```
docker images
```

The above command's output shows list of your current local images:

REPOSITORY	TAG	IMAGE ID	CREATED
mcr.microsoft.com/azuredocs/azure-vote-front	v1	84b41c268ad9	7 minutes ago
944MB			
mcr.microsoft.com/oss/bitnami/redis	6.0.8	3a54a920bb6c	2 days ago
103MB			
tiangolo/uwsgi-nginx-flask	python3.6	a16ce562e863	6 weeks ago
944MB			

To use the *azure-vote-front* container image with ACR, the image needs to be tagged with the login server address of your registry. This tag is used for routing when pushing container images to an image registry.

- [Azure CLI](#)
- [Azure PowerShell](#)

To get the login server address, use the `az acr list` command and query for the *loginServer* as follows:

```
az acr list --resource-group myResourceGroup --query "[].{acrLoginServer:loginServer}" --output table
```

Now, tag your local *azure-vote-front* image with the *acrLoginServer* address of the container registry. To indicate the image version, add *.v1* to the end of the image name:

```
docker tag mcr.microsoft.com/azuredocs/azure-vote-front:v1 <acrLoginServer>/azure-vote-front:v1
```

To verify the tags are applied, run `docker images` again.

```
docker images
```

An image is tagged with the ACR instance address and a version number.

REPOSITORY	TAG	IMAGE ID	CREATED
SIZE			
mcr.microsoft.com/azuredocs/azure-vote-front	v1	84b41c268ad9	16 minutes ago
944MB			
mycontainerregistry.azurecr.io/azure-vote-front	v1	84b41c268ad9	16 minutes ago
944MB			
mcr.microsoft.com/oss/bitnami/redis	6.0.8	3a54a920bb6c	2 days ago
103MB			
tiangolo/uwsgi-nginx-flask	python3.6	a16ce562e863	6 weeks ago
944MB			

Push images to registry

With your image built and tagged, push the *azure-vote-front* image to your ACR instance. Use [docker push](#) and provide your own *acrLoginServer* address for the image name as follows:

```
docker push <acrLoginServer>/azure-vote-front:v1
```

It may take a few minutes to complete the image push to ACR.

List images in registry

- [Azure CLI](#)
- [Azure PowerShell](#)

To return a list of images that have been pushed to your ACR instance, use the [az acr repository list](#) command.

Provide your own `<acrName>` as follows:

```
az acr repository list --name <acrName> --output table
```

The following example output lists the *azure-vote-front* image as available in the registry:

```
Result
-----
azure-vote-front
```

To see the tags for a specific image, use the [az acr repository show-tags](#) command as follows:

```
az acr repository show-tags --name <acrName> --repository azure-vote-front --output table
```

The following example output shows the *v1* image tagged in a previous step:

```
Result
-----
v1
```

You now have a container image that is stored in a private Azure Container Registry instance. This image is deployed from ACR to a Kubernetes cluster in the next tutorial.

Next steps

In this tutorial, you created an Azure Container Registry and pushed an image for use in an AKS cluster. You

learned how to:

- Create an Azure Container Registry (ACR) instance
- Tag a container image for ACR
- Upload the image to ACR
- View images in your registry

Advance to the next tutorial to learn how to deploy a Kubernetes cluster in Azure.

[Deploy Kubernetes cluster](#)

Tutorial: Deploy an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 4 minutes to read • [Edit Online](#)

Kubernetes provides a distributed platform for containerized applications. With AKS, you can quickly create a production ready Kubernetes cluster. In this tutorial, part three of seven, a Kubernetes cluster is deployed in AKS. You learn how to:

- Deploy a Kubernetes AKS cluster that can authenticate to an Azure container registry
- Install the Kubernetes CLI (kubectl)
- Configure kubectl to connect to your AKS cluster

In later tutorials, the Azure Vote application is deployed to the cluster, scaled, and updated.

Before you begin

In previous tutorials, a container image was created and uploaded to an Azure Container Registry instance. If you haven't done these steps, and would like to follow along, start at [Tutorial 1 – Create container images](#).

- [Azure CLI](#)
- [Azure PowerShell](#)

This tutorial requires that you're running the Azure CLI version 2.0.53 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create a Kubernetes cluster

AKS clusters can use Kubernetes role-based access control (Kubernetes RBAC). These controls let you define access to resources based on roles assigned to users. Permissions are combined if a user is assigned multiple roles, and permissions can be scoped to either a single namespace or across the whole cluster. By default, the Azure CLI automatically enables Kubernetes RBAC when you create an AKS cluster.

- [Azure CLI](#)
- [Azure PowerShell](#)

Create an AKS cluster using `az aks create`. The following example creates a cluster named *myAKSCluster* in the resource group named *myResourceGroup*. This resource group was created in the [previous tutorial](#) in the *eastus* region. The following example does not specify a region so the AKS cluster is also created in the *eastus* region. For more information, see [Quotas, virtual machine size restrictions, and region availability in Azure Kubernetes Service \(AKS\)](#) for more information about resource limits and region availability for AKS.

To allow an AKS cluster to interact with other Azure resources, a cluster identity is automatically created, since you did not specify one. Here, this cluster identity is [granted the right to pull images](#) from the Azure Container Registry (ACR) instance you created in the previous tutorial. To execute the command successfully, you're required to have an **Owner** or **Azure account administrator** role on the Azure subscription.

```
az aks create \
--resource-group myResourceGroup \
--name myAKSCluster \
--node-count 2 \
--generate-ssh-keys \
--attach-acr <acrName>
```

To avoid needing an **Owner** or **Azure account administrator** role, you can also manually configure a service principal to pull images from ACR. For more information, see [ACR authentication with service principals](#) or [Authenticate from Kubernetes with a pull secret](#). Alternatively, you can use a [managed identity](#) instead of a service principal for easier management.

After a few minutes, the deployment completes, and returns JSON-formatted information about the AKS deployment.

NOTE

To ensure your cluster to operate reliably, you should run at least 2 (two) nodes.

Install the Kubernetes CLI

To connect to the Kubernetes cluster from your local computer, you use [kubectl](#), the Kubernetes command-line client.

- [Azure CLI](#)
- [Azure PowerShell](#)

If you use the Azure Cloud Shell, `kubectl` is already installed. You can also install it locally using the [az aks install-cli](#) command:

```
az aks install-cli
```

Connect to cluster using kubectl

- [Azure CLI](#)
- [Azure PowerShell](#)

To configure `kubectl` to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command. The following example gets credentials for the AKS cluster named *myAKSCluster* in the *myResourceGroup*:

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

To verify the connection to your cluster, run the [kubectl get nodes](#) command to return a list of the cluster nodes:

```
kubectl get nodes
```

The following example output shows the list of cluster nodes.

```
$ kubectl get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-37463671-vmss000000	Ready	agent	2m37s	v1.18.10
aks-nodepool1-37463671-vmss000001	Ready	agent	2m28s	v1.18.10

Next steps

In this tutorial, a Kubernetes cluster was deployed in AKS, and you configured `kubectl` to connect to it. You learned how to:

- Deploy a Kubernetes AKS cluster that can authenticate to an Azure container registry
- Install the Kubernetes CLI (`kubectl`)
- Configure `kubectl` to connect to your AKS cluster

Advance to the next tutorial to learn how to deploy an application to the cluster.

[Deploy application in Kubernetes](#)

Tutorial: Run applications in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

Kubernetes provides a distributed platform for containerized applications. You build and deploy your own applications and services into a Kubernetes cluster, and let the cluster manage the availability and connectivity. In this tutorial, part four of seven, a sample application is deployed into a Kubernetes cluster. You learn how to:

- Update a Kubernetes manifest file
- Run an application in Kubernetes
- Test the application

In later tutorials, this application is scaled out and updated.

This quickstart assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

TIP

AKS clusters can use GitOps for configuration management. This enables declarations of your cluster's state, which are pushed to source control, to be applied to the cluster automatically. To learn how to use GitOps to deploy an application with an AKS cluster, see the tutorial [Use GitOps with Flux v2](#) and follow the [prerequisites for Azure Kubernetes Service clusters](#).

Before you begin

In previous tutorials, an application was packaged into a container image, this image was uploaded to Azure Container Registry, and a Kubernetes cluster was created.

To complete this tutorial, you need the pre-created `azure-vote-all-in-one-redis.yaml` Kubernetes manifest file. This file was downloaded with the application source code in a previous tutorial. Verify that you've cloned the repo, and that you have changed directories into the cloned repo. If you haven't done these steps, and would like to follow along, start with [Tutorial 1 – Create container images](#).

- [Azure CLI](#)
- [Azure PowerShell](#)

This tutorial requires that you're running the Azure CLI version 2.0.53 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Update the manifest file

In these tutorials, an Azure Container Registry (ACR) instance stores the container image for the sample application. To deploy the application, you must update the image name in the Kubernetes manifest file to include the ACR login server name.

- [Azure CLI](#)
- [Azure PowerShell](#)

Get the ACR login server name using the `az acr list` command as follows:

```
az acr list --resource-group myResourceGroup --query "[].{acrLoginServer:loginServer}" --output table
```

The sample manifest file from the git repo cloned in the first tutorial uses the images from Microsoft Container Registry (mcr.microsoft.com). Make sure that you're in the cloned `azure-voting-app-redis` directory, then open the manifest file with a text editor, such as `vi`:

```
vi azure-vote-all-in-one-redis.yaml
```

Replace `mcr.microsoft.com` with your ACR login server name. The image name is found on line 60 of the manifest file. The following example shows the default image name:

```
containers:
- name: azure-vote-front
  image: mcr.microsoft.com/azuredocs/azure-vote-front:v1
```

Provide your own ACR login server name so that your manifest file looks like the following example:

```
containers:
- name: azure-vote-front
  image: <acrName>.azurecr.io/azure-vote-front:v1
```

Save and close the file. In `vi`, use `:wq`.

Deploy the application

To deploy your application, use the [kubectl apply](#) command. This command parses the manifest file and creates the defined Kubernetes objects. Specify the sample manifest file, as shown in the following example:

```
kubectl apply -f azure-vote-all-in-one-redis.yaml
```

The following example output shows the resources successfully created in the AKS cluster:

```
$ kubectl apply -f azure-vote-all-in-one-redis.yaml

deployment "azure-vote-back" created
service "azure-vote-back" created
deployment "azure-vote-front" created
service "azure-vote-front" created
```

Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete.

To monitor progress, use the [kubectl get service](#) command with the `--watch` argument.

```
kubectl get service azure-vote-front --watch
```

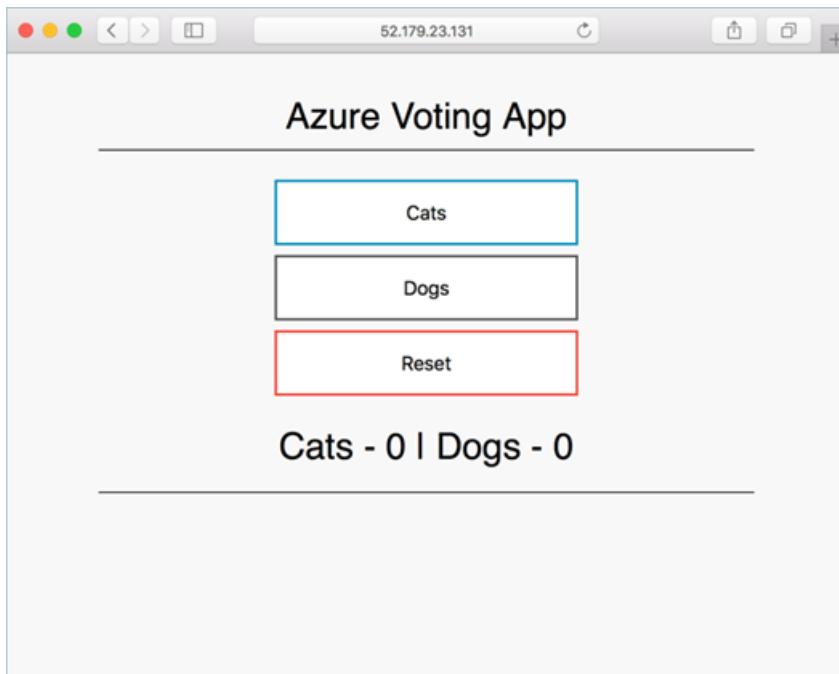
Initially the `EXTERNAL-IP` for the `azure-vote-front` service is shown as *pending*.

```
azure-vote-front LoadBalancer 10.0.34.242 <pending> 80:30676/TCP 5s
```

When the *EXTERNAL-IP* address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
azure-vote-front LoadBalancer 10.0.34.242 52.179.23.131 80:30676/TCP 67s
```

To see the application in action, open a web browser to the external IP address of your service:



If the application didn't load, it might be due to an authorization problem with your image registry. To view the status of your containers, use the `kubectl get pods` command. If the container images can't be pulled, see [Authenticate with Azure Container Registry from Azure Kubernetes Service](#).

Next steps

In this tutorial, a sample Azure vote application was deployed to a Kubernetes cluster in AKS. You learned how to:

- Update a Kubernetes manifest files
- Run an application in Kubernetes
- Test the application

Advance to the next tutorial to learn how to scale a Kubernetes application and the underlying Kubernetes infrastructure.

[Scale Kubernetes application and infrastructure](#)

Tutorial: Scale applications in Azure Kubernetes Service (AKS)

10/27/2022 • 5 minutes to read • [Edit Online](#)

If you've followed the tutorials, you have a working Kubernetes cluster in AKS and you deployed the sample Azure Voting app. In this tutorial, part five of seven, you scale out the pods in the app and try pod autoscaling. You also learn how to scale the number of Azure VM nodes to change the cluster's capacity for hosting workloads. You learn how to:

- Scale the Kubernetes nodes
- Manually scale Kubernetes pods that run your application
- Configure autoscaling pods that run the app front-end

In later tutorials, the Azure Vote application is updated to a new version.

Before you begin

In previous tutorials, an application was packaged into a container image. This image was uploaded to Azure Container Registry, and you created an AKS cluster. The application was then deployed to the AKS cluster. If you haven't done these steps, and would like to follow along, start with [Tutorial 1 – Create container images](#).

- [Azure CLI](#)
- [Azure PowerShell](#)

This tutorial requires that you're running the Azure CLI version 2.0.53 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Manually scale pods

When the Azure Vote front-end and Redis instance were deployed in previous tutorials, a single replica was created. To see the number and state of pods in your cluster, use the `kubectl get` command as follows:

```
kubectl get pods
```

The following example output shows one front-end pod and one back-end pod:

NAME	READY	STATUS	RESTARTS	AGE
azure-vote-back-2549686872-4d2r5	1/1	Running	0	31m
azure-vote-front-848767080-tf34m	1/1	Running	0	31m

To manually change the number of pods in the `azure-vote-front` deployment, use the `kubectl scale` command. The following example increases the number of front-end pods to 5:

```
kubectl scale --replicas=5 deployment/azure-vote-front
```

Run `kubectl get pods` again to verify that AKS successfully creates the additional pods. After a minute or so, the pods are available in your cluster:

```
kubectl get pods
```

	READY	STATUS	RESTARTS	AGE
azure-vote-back-2606967446-nmpcf	1/1	Running	0	15m
azure-vote-front-3309479140-2hfh0	1/1	Running	0	3m
azure-vote-front-3309479140-bzt05	1/1	Running	0	3m
azure-vote-front-3309479140-fvcvm	1/1	Running	0	3m
azure-vote-front-3309479140-hrbf2	1/1	Running	0	15m
azure-vote-front-3309479140-qphz8	1/1	Running	0	3m

Autoscale pods

- [Azure CLI](#)
- [Azure PowerShell](#)

Kubernetes supports [horizontal pod autoscaling](#) to adjust the number of pods in a deployment depending on CPU utilization or other select metrics. The [Metrics Server](#) is used to provide resource utilization to Kubernetes, and is automatically deployed in AKS clusters versions 1.10 and higher. To see the version of your AKS cluster, use the `az aks show` command, as shown in the following example:

```
az aks show --resource-group myResourceGroup --name myAKSCluster --query kubernetesVersion --output table
```

NOTE

If your AKS cluster is less than 1.10, the Metrics Server is not automatically installed. Metrics Server installation manifests are available as a `components.yaml` asset on Metrics Server releases, which means you can install them via a url. To learn more about these YAML definitions, see the [Deployment](#) section of the readme.

Example installation:

```
kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/releases/download/v0.3.6/components.yaml
```

To use the autoscaler, all containers in your pods and your pods must have CPU requests and limits defined. In the `azure-vote-front` deployment, the front-end container already requests 0.25 CPU, with a limit of 0.5 CPU.

These resource requests and limits are defined for each container as shown in the following example snippet:

```
containers:
- name: azure-vote-front
  image: mcr.microsoft.com/azuredocs/azure-vote-front:v1
  ports:
  - containerPort: 80
  resources:
    requests:
      cpu: 250m
    limits:
      cpu: 500m
```

The following example uses the `kubectl autoscale` command to autoscale the number of pods in the `azure-vote-front` deployment. If average CPU utilization across all pods exceeds 50% of their requested usage, the autoscaler increases the pods up to a maximum of 10 instances. A minimum of 3 instances is then defined for the deployment:

```
kubectl autoscale deployment azure-vote-front --cpu-percent=50 --min=3 --max=10
```

Alternatively, you can create a manifest file to define the autoscaler behavior and resource limits. The following is an example of a manifest file named `azure-vote-hpa.yaml`.

```
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: azure-vote-back-hpa
spec:
  maxReplicas: 10 # define max replica count
  minReplicas: 3 # define min replica count
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: azure-vote-back
  targetCPUUtilizationPercentage: 50 # target CPU utilization

---
apiVersion: autoscaling/v1
kind: HorizontalPodAutoscaler
metadata:
  name: azure-vote-front-hpa
spec:
  maxReplicas: 10 # define max replica count
  minReplicas: 3 # define min replica count
  scaleTargetRef:
    apiVersion: apps/v1
    kind: Deployment
    name: azure-vote-front
  targetCPUUtilizationPercentage: 50 # target CPU utilization
```

Use `kubectl apply` to apply the autoscaler defined in the `azure-vote-hpa.yaml` manifest file.

```
kubectl apply -f azure-vote-hpa.yaml
```

To see the status of the autoscaler, use the `kubectl get hpa` command as follows:

```
kubectl get hpa
NAME          REFERENCE          TARGETS      MINPODS   MAXPODS   REPLICAS   AGE
azure-vote-front  Deployment/azure-vote-front  0% / 50%   3         10        3          2m
```

After a few minutes, with minimal load on the Azure Vote app, the number of pod replicas decreases automatically to three. You can use `kubectl get pods` again to see the unneeded pods being removed.

NOTE

For additional examples on using the horizontal pod autoscaler, see [HorizontalPodAutoscaler Walkthrough](#).

Manually scale AKS nodes

If you created your Kubernetes cluster using the commands in the previous tutorial, it has two nodes. You can adjust the number of nodes manually if you plan more or fewer container workloads on your cluster.

The following example increases the number of nodes to three in the Kubernetes cluster named `myAKSCluster`.

The command takes a couple of minutes to complete.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
az aks scale --resource-group myResourceGroup --name myAKSCluster --node-count 3
```

When the cluster has successfully scaled, the output is similar to following example:

```
"agentPoolProfiles": [  
  {  
    "count": 3,  
    "dnsPrefix": null,  
    "fqdn": null,  
    "name": "myAKSCluster",  
    "osDiskSizeGb": null,  
    "osType": "Linux",  
    "ports": null,  
    "storageProfile": "ManagedDisks",  
    "vmSize": "Standard_D2_v2",  
    "vnetSubnetId": null  
  }]
```

Next steps

In this tutorial, you used different scaling features in your Kubernetes cluster. You learned how to:

- Manually scale Kubernetes pods that run your application
- Configure autoscaling pods that run the app front-end
- Manually scale the Kubernetes nodes

Advance to the next tutorial to learn how to update application in Kubernetes.

[Update an application in Kubernetes](#)

Tutorial: Update an application in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

After an application has been deployed in Kubernetes, it can be updated by specifying a new container image or image version. An update is staged so that only a portion of the deployment is updated at the same time. This staged update enables the application to keep running during the update. It also provides a rollback mechanism if a deployment failure occurs.

In this tutorial, part six of seven, the sample Azure Vote app is updated. You learn how to:

- Update the front-end application code
- Create an updated container image
- Push the container image to Azure Container Registry
- Deploy the updated container image

Before you begin

In previous tutorials, an application was packaged into a container image. This image was uploaded to Azure Container Registry, and you created an AKS cluster. The application was then deployed to the AKS cluster.

An application repository was also cloned that includes the application source code, and a pre-created Docker Compose file used in this tutorial. Verify that you've created a clone of the repo, and have changed directories into the cloned directory. If you haven't completed these steps, and want to follow along, start with [Tutorial 1 – Create container images](#).

- [Azure CLI](#)
- [Azure PowerShell](#)

This tutorial requires that you're running the Azure CLI version 2.0.53 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Update an application

Let's make a change to the sample application, then update the version already deployed to your AKS cluster. Make sure that you're in the cloned `azure-voting-app-redis` directory. The sample application source code can then be found inside the `azure-vote` directory. Open the `config_file.cfg` file with an editor, such as `vi`:

```
vi azure-vote/azure-vote/config_file.cfg
```

Change the values for `VOTE1VALUE` and `VOTE2VALUE` to different values, such as colors. The following example shows the updated values:

```
# UI Configurations
TITLE = 'Azure Voting App'
VOTE1VALUE = 'Blue'
VOTE2VALUE = 'Purple'
SHOWHOST = 'false'
```

Save and close the file. In `vi`, use `:wq`.

Update the container image

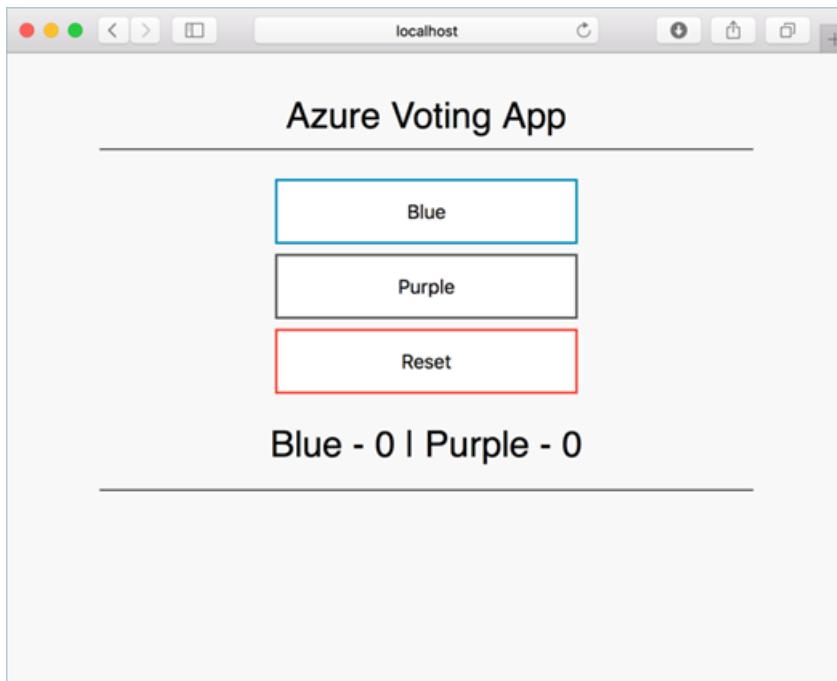
To re-create the front-end image and test the updated application, use `docker-compose`. The `--build` argument is used to instruct Docker Compose to re-create the application image:

```
docker-compose up --build -d
```

Test the application locally

To verify that the updated container image shows your changes, open a local web browser to

```
http://localhost:8080 .
```



The updated values provided in the `config_file.cfg` file are displayed in your running application.

Tag and push the image

- [Azure CLI](#)
- [Azure PowerShell](#)

To correctly use the updated image, tag the `azure-vote-front` image with the login server name of your ACR registry. Get the login server name with the `az acr list` command:

```
az acr list --resource-group myResourceGroup --query "[].{acrLoginServer:loginServer}" --output table
```

Use `docker tag` to tag the image. Replace `<acrLoginServer>` with your ACR login server name or public registry hostname, and update the image version to `.v2` as follows:

```
docker tag mcr.microsoft.com/azuredocs/azure-vote-front:v1 <acrLoginServer>/azure-vote-front:v2
```

Now use `docker push` to upload the image to your registry. Replace `<acrLoginServer>` with your ACR login server name.

- [Azure CLI](#)
- [Azure PowerShell](#)

NOTE

If you experience issues pushing to your ACR registry, make sure that you are still logged in. Run the `az acr login` command using the name of your Azure Container Registry that you created in the [Create an Azure Container Registry](#) step. For example, `az acr login --name <azure container registry name>`.

```
docker push <acrLoginServer>/azure-vote-front:v2
```

Deploy the updated application

To provide maximum uptime, multiple instances of the application pod must be running. Verify the number of running front-end instances with the [kubectl get pods](#) command:

```
$ kubectl get pods

NAME                  READY   STATUS    RESTARTS   AGE
azure-vote-back-217588096-5w632  1/1     Running   0          10m
azure-vote-front-233282510-b5pkz  1/1     Running   0          10m
azure-vote-front-233282510-dhrtr  1/1     Running   0          10m
azure-vote-front-233282510-pqbfk  1/1     Running   0          10m
```

If you don't have multiple front-end pods, scale the *azure-vote-front* deployment as follows:

```
kubectl scale --replicas=3 deployment/azure-vote-front
```

To update the application, use the [kubectl set](#) command. Update `<acrLoginServer>` with the login server or host name of your container registry, and specify the *v2* application version:

```
kubectl set image deployment azure-vote-front azure-vote-front=<acrLoginServer>/azure-vote-front:v2
```

To monitor the deployment, use the [kubectl get pod](#) command. As the updated application is deployed, your pods are terminated and re-created with the new container image.

```
kubectl get pods
```

The following example output shows pods terminating and new instances running as the deployment progresses:

```
$ kubectl get pods

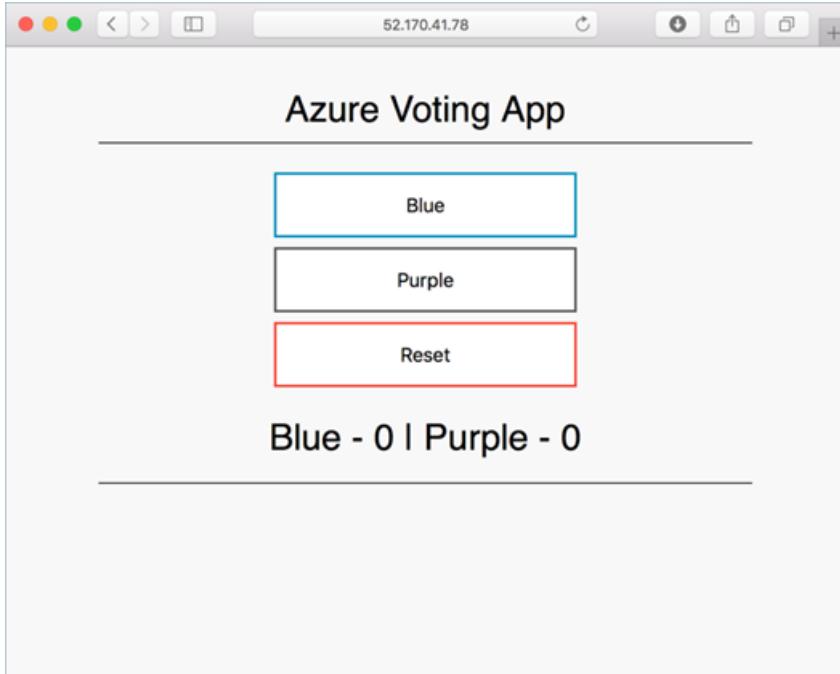
NAME                  READY   STATUS    RESTARTS   AGE
azure-vote-back-2978095810-gq9g0  1/1     Running   0          5m
azure-vote-front-1297194256-tpjlg  1/1     Running   0          1m
azure-vote-front-1297194256-tptnx  1/1     Running   0          5m
azure-vote-front-1297194256-zktw9  1/1     Terminating   0          1m
```

Test the updated application

To view the update application, first get the external IP address of the `azure-vote-front` service:

```
kubectl get service azure-vote-front
```

Now open a web browser to the IP address of your service:



Next steps

In this tutorial, you updated an application and rolled out this update to your AKS cluster. You learned how to:

- Update the front-end application code
- Create an updated container image
- Push the container image to Azure Container Registry
- Deploy the updated container image

Advance to the next tutorial to learn how to upgrade an AKS cluster to a new version of Kubernetes.

[Upgrade Kubernetes](#)

Tutorial: Upgrade Kubernetes in Azure Kubernetes Service (AKS)

10/27/2022 • 6 minutes to read • [Edit Online](#)

As part of the application and cluster lifecycle, you may wish to upgrade to the latest available version of Kubernetes and use new features. An Azure Kubernetes Service (AKS) cluster can be upgraded using the Azure CLI.

In this tutorial, part seven of seven, a Kubernetes cluster is upgraded. You learn how to:

- Identify current and available Kubernetes versions
- Upgrade the Kubernetes nodes
- Validate a successful upgrade

Before you begin

In previous tutorials, an application was packaged into a container image. This image was uploaded to Azure Container Registry, and you created an AKS cluster. The application was then deployed to the AKS cluster. If you have not done these steps, and would like to follow along, start with [Tutorial 1 – Create container images](#).

- [Azure CLI](#)
- [Azure PowerShell](#)

This tutorial requires that you are running the Azure CLI version 2.0.53 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Get available cluster versions

- [Azure CLI](#)
- [Azure PowerShell](#)

Before you upgrade a cluster, use the `az aks get-upgrades` command to check which Kubernetes releases are available for upgrade:

```
az aks get-upgrades --resource-group myResourceGroup --name myAKSCluster
```

In the following example, the current version is *1.18.10*, and the available versions are shown under *upgrades*.

```
{  
  "agentPoolProfiles": null,  
  "controlPlaneProfile": {  
    "kubernetesVersion": "1.18.10",  
    ...  
    "upgrades": [  
      {  
        "isPreview": null,  
        "kubernetesVersion": "1.19.1"  
      },  
      {  
        "isPreview": null,  
        "kubernetesVersion": "1.19.3"  
      }  
    ]  
  },  
  ...  
}
```

Upgrade a cluster

To minimize disruption to running applications, AKS nodes are carefully cordoned and drained. In this process, the following steps are performed:

1. The Kubernetes scheduler prevents additional pods being scheduled on a node that is to be upgraded.
2. Running pods on the node are scheduled on other nodes in the cluster.
3. A node is created that runs the latest Kubernetes components.
4. When the new node is ready and joined to the cluster, the Kubernetes scheduler begins to run pods on it.
5. The old node is deleted, and the next node in the cluster begins the cordon and drain process.

NOTE

If no patch is specified, the cluster will automatically be upgraded to the specified minor version's latest GA patch. For example, setting `--kubernetes-version` to `1.21` will result in the cluster upgrading to `1.21.9`.

When upgrading by alias minor version, only a higher minor version is supported. For example, upgrading from `1.20.x` to `1.20` will not trigger an upgrade to the latest GA `1.20` patch, but upgrading to `1.21` will trigger an upgrade to the latest GA `1.21` patch.

- [Azure CLI](#)
- [Azure PowerShell](#)

Use the `az aks upgrade` command to upgrade the AKS cluster.

```
az aks upgrade \  
  --resource-group myResourceGroup \  
  --name myAKScluster \  
  --kubernetes-version KUBERNETES_VERSION
```

NOTE

You can only upgrade one minor version at a time. For example, you can upgrade from `1.14.x` to `1.15.x`, but cannot upgrade from `1.14.x` to `1.16.x` directly. To upgrade from `1.14.x` to `1.16.x`, first upgrade from `1.14.x` to `1.15.x`, then perform another upgrade from `1.15.x` to `1.16.x`.

The following condensed example output shows the result of upgrading to 1.19.1. Notice the *kubernetesVersion* now reports 1.19.1:

```
{  
  "agentPoolProfiles": [  
    {  
      "count": 3,  
      "maxPods": 110,  
      "name": "nodepool1",  
      "osType": "Linux",  
      "storageProfile": "ManagedDisks",  
      "vmSize": "Standard_DS1_v2",  
    }  
  ],  
  "dnsPrefix": "myAKSclust-myResourceGroup-19da35",  
  "enableRbac": false,  
  "fqdn": "myaksclust-myresourcegroup-19da35-bd54a4be.hcp.eastus.azurek8s.io",  
  "id": "/subscriptions/<Subscription  
ID>/resourcegroups/myResourceGroup/providers/Microsoft.ContainerService/managedClusters/myAKSCluster",  
  "kubernetesVersion": "1.19.1",  
  "location": "eastus",  
  "name": "myAKSCluster",  
  "type": "Microsoft.ContainerService/ManagedClusters"  
}  
}
```

View the upgrade events

When you upgrade your cluster, the following Kubernetes events may occur on each node:

- Surge – Create surge node.
- Drain – Pods are being evicted from the node. Each pod has a 5 minute timeout to complete the eviction.
- Update – Update of a node has succeeded or failed.
- Delete – Deleted a surge node.

Use `kubectl get events` to show events in the default namespaces while running an upgrade. For example:

```
kubectl get events
```

The following example output shows some of the above events listed during an upgrade.

```
...  
default 2m1s Normal Drain node/aks-nodepool1-96663640-vmss000001 Draining node: [aks-nodepool1-96663640-  
vmss000001]  
...  
default 9m22s Normal Surge node/aks-nodepool1-96663640-vmss000002 Created a surge node [aks-nodepool1-  
96663640-vmss000002 nodepool1] for agentpool %!(MISSING)  
...
```

Validate an upgrade

- [Azure CLI](#)
- [Azure PowerShell](#)

Confirm that the upgrade was successful using the `az aks show` command as follows:

```
az aks show --resource-group myResourceGroup --name myAKSCluster --output table
```

The following example output shows the AKS cluster runs *KubernetesVersion 1.19.1*:

Name	Location	ResourceGroup	KubernetesVersion	ProvisioningState	Fqdn
myAKScluster	eastus	myResourceGroup	1.19.1	Succeeded	myaksclust-
			myresourcegroup-19da35-bd54a4be.hcp.eastus.azmk8s.io		

Delete the cluster

- [Azure CLI](#)
- [Azure PowerShell](#)

As this tutorial is the last part of the series, you may want to delete the AKS cluster. As the Kubernetes nodes run on Azure virtual machines (VMs), they continue to incur charges even if you don't use the cluster. Use the [az group delete](#) command to remove the resource group, container service, and all related resources.

```
az group delete --name myResourceGroup --yes --no-wait
```

NOTE

When you delete the cluster, the Azure Active Directory service principal used by the AKS cluster is not removed. For steps on how to remove the service principal, see [AKS service principal considerations and deletion](#). If you used a managed identity, the identity is managed by the platform and does not require you to provision or rotate any secrets.

Next steps

In this tutorial, you upgraded Kubernetes in an AKS cluster. You learned how to:

- Identify current and available Kubernetes versions
- Upgrade the Kubernetes nodes
- Validate a successful upgrade

For more information on AKS, see [AKS overview](#). For guidance on creating full solutions with AKS, see [AKS solution guidance](#).

Tutorial: Use a workload identity with an application on Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage Kubernetes clusters. In this tutorial, you will:

- Deploy an AKS cluster using the Azure CLI with OpenID Connect Issuer and managed identity.
- Create an Azure Key Vault and secret.
- Create an Azure Active Directory workload identity and Kubernetes service account
- Configure the managed identity for token federation
- Deploy the workload and verify authentication with the workload identity.

This tutorial assumes a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

- This article requires version 2.40.0 or later of the Azure CLI. If using Azure Cloud Shell, the latest version is already installed.
- You have installed the latest version of the `aks-preview` extension, version 0.5.102 or later.
- The identity you are using to create your cluster has the appropriate minimum permissions. For more information on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).
- If you have multiple Azure subscriptions, select the appropriate subscription ID in which the resources should be billed using the `az account` command.

Create a resource group

An [Azure resource group](#) is a logical group in which Azure resources are deployed and managed. When you create a resource group, you are prompted to specify a location. This location is:

- The storage location of your resource group metadata.
- Where your resources will run in Azure if you don't specify another region during resource creation.

The following example creates a resource group named `myResourceGroup` in the `eastus` location.

Create a resource group using the `az group create` command.

```
az group create --name myResourceGroup --location eastus
```

The following output example resembles successful creation of the resource group:

```
{  
  "id": "/subscriptions/<guid>/resourceGroups/myResourceGroup",  
  "location": "eastus",  
  "managedBy": null,  
  "name": "myResourceGroup",  
  "properties": {  
    "provisioningState": "Succeeded"  
  },  
  "tags": null  
}
```

Install the aks-preview Azure CLI extension

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

To install the aks-preview extension, run the following command:

```
az extension add --name aks-preview
```

Run the following command to update to the latest version of the extension released:

```
az extension update --name aks-preview
```

Create AKS cluster

Create an AKS cluster using the [az aks create](#) command with the `--enable-oidc-issuer` parameter to use the OIDC Issuer. The following example creates a cluster named *myAKSCluster* with one node in the *myResourceGroup*:

```
az aks create -g myResourceGroup -n myAKSCluster --node-count 1 --enable-oidc-issuer --enable-workload-identity --generate-ssh-keys
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

NOTE

When you create an AKS cluster, a second resource group is automatically created to store the AKS resources. For more information, see [Why are two resource groups created with AKS?](#)

To get the OIDC Issuer URL and save it to an environmental variable, run the following command. Replace the default value for the arguments `-n`, which is the name of the cluster and `-g`, the resource group name:

```
export AKS_OIDC_ISSUER=$(az aks show -n myAKScluster -g myResourceGroup --query "oidcIssuerProfile.issuerUrl" -otsv)"
```

Export environmental variables

To help simplify steps to configure creating Azure Key Vault and other identities required, the steps below define environmental variables for reference on the cluster.

Run the following commands to create these variables. Replace the default values for `RESOURCE_GROUP`, `LOCATION`, `KEYVAULT_SECRET_NAME`, `SERVICE_ACCOUNT_NAME`, `SUBSCRIPTION`, `UAID`, and `FICID`.

```
# environment variables for the Azure Key Vault resource
export KEYVAULT_NAME="azwi-kv-tutorial"
export KEYVAULT_SECRET_NAME="my-secret"
export RESOURCE_GROUP="resourceGroupName"
export LOCATION="westcentralus"

# environment variables for the Kubernetes Service account & federated identity credential
export SERVICE_ACCOUNT_NAMESPACE="default"
export SERVICE_ACCOUNT_NAME="workload-identity-sa"

# environment variables for the Federated Identity
export SUBSCRIPTION="{your subscription ID}"
# user assigned identity name
export UAID="fic-test-ua"
# federated identity name
export FICID="fic-test-fic-name"
```

Create an Azure Key Vault and secret

Use the Azure CLI `az keyvault create` command to create a Key Vault in the resource group created earlier.

```
az keyvault create --resource-group "${RESOURCE_GROUP}" --location "${LOCATION}" --name "${KEYVAULT_NAME}"
```

The output of this command shows properties of the newly created key vault. Take note of the two properties listed below:

- **Name:** The Vault name you provided to the `--name` parameter above.
- **vaultUri:** In the example, this is `https://<your-unique-keyvault-name>.vault.azure.net/`. Applications that use your vault through its REST API must use this URI.

At this point, your Azure account is the only one authorized to perform any operations on this new vault.

To add a secret to the vault, you need to run the Azure CLI `az keyvault secret set` command to create it. The password is the value you specified for the environment variable `KEYVAULT_SECRET_NAME` and stores the value of `Hello!` in it.

```
az keyvault secret set --vault-name "${KEYVAULT_NAME}" --name "${KEYVAULT_SECRET_NAME}" --value 'Hello!'
```

Create a managed identity and grant permissions to access the secret

Use the Azure CLI [az account set](#) command to set a specific subscription to be the current active subscription. Then use the [az identity create](#) command to create a managed identity.

```
az account set --subscription "${SUBSCRIPTION}"
```

```
az identity create --name "${UAID}" --resource-group "${RESOURCE_GROUP}" --location "${LOCATION}" --subscription "${SUBSCRIPTION}"
```

Next, you need to set an access policy for the managed identity to access the Key Vault secret by running the following commands:

```
export USER_ASSIGNED_CLIENT_ID=$(az identity show --resource-group "${RESOURCE_GROUP}" --name "${UAID}" --query 'clientId' -otsv)"
```

```
az keyvault set-policy --name "${KEYVAULT_NAME}" --secret-permissions get --spn "${USER_ASSIGNED_CLIENT_ID}"
```

Create Kubernetes service account

Create a Kubernetes service account and annotate it with the client ID of the Managed Identity created in the previous step. Use the [az aks get-credentials](#) command and replace the default value for the cluster name and the resource group name.

```
az aks get-credentials -n myAKScluster -g "${RESOURCE_GROUP}"
```

Copy and paste the following multi-line input in the Azure CLI.

```
cat <<EOF | kubectl apply -f -
apiVersion: v1
kind: ServiceAccount
metadata:
  annotations:
    azure.workload.identity/client-id: ${USER_ASSIGNED_CLIENT_ID}
  labels:
    azure.workload.identity/use: "true"
  name: ${SERVICE_ACCOUNT_NAME}
  namespace: ${SERVICE_ACCOUNT_NAMESPACE}
EOF
```

The following output resembles successful creation of the identity:

```
Serviceaccount/workload-identity-sa created
```

Establish federated identity credential

Use the [az identity federated-credential create](#) command to create the federated identity credential between the managed identity, the service account issuer, and the subject.

```
az identity federated-credential create --name ${FICID} --identity-name ${UAID} --resource-group ${RESOURCE_GROUP} --issuer ${AKS_OIDC_ISSUER} --subject system:serviceaccount:${SERVICE_ACCOUNT_NAMESPACE}: ${SERVICE_ACCOUNT_NAME}
```

NOTE

It takes a few seconds for the federated identity credential to be propagated after being initially added. If a token request is made immediately after adding the federated identity credential, it might lead to failure for a couple of minutes as the cache is populated in the directory with old data. To avoid this issue, you can add a slight delay after adding the federated identity credential.

Deploy the workload

Run the following to deploy a pod that references the service account created in the previous step.

```
cat <<EOF | kubectl apply -f -
apiVersion: v1
kind: Pod
metadata:
  name: quick-start
  namespace: ${SERVICE_ACCOUNT_NAMESPACE}
spec:
  serviceAccountName: ${SERVICE_ACCOUNT_NAME}
  containers:
    - image: ghcr.io/azure/azure-workload-identity/msal-go
      name: oidc
      env:
        - name: KEYVAULT_NAME
          value: ${KEYVAULT_NAME}
        - name: SECRET_NAME
          value: ${KEYVAULT_SECRET_NAME}
  nodeSelector:
    kubernetes.io/os: linux
EOF
```

The following output resembles successful creation of the pod:

```
pod/quick-start created
```

To check whether all properties are injected properly by the webhook, use the [kubectl describe](#) command:

```
kubectl describe pod quick-start
```

To verify that pod is able to get a token and access the secret from the Key Vault, use the [kubectl logs](#) command:

```
kubectl logs quick-start
```

The following output resembles successful access of the token:

```
I1013 22:49:29.872708      1 main.go:30] "successfully got secret" secret="Hello!"
```

Clean up resources

If you plan to continue on to work with subsequent tutorials, you may wish to leave these resources in place.

When no longer needed, you can run the following Kubectl and the Azure CLI commands to remove the resource group and all related resources.

```
kubectl delete pod quick-start
```

```
kubectl delete sa "${SERVICE_ACCOUNT_NAME}" --namespace "${SERVICE_ACCOUNT_NAMESPACE}"
```

```
az group delete --name "${RESOURCE_GROUP}"
```

Next steps

In this tutorial, you deployed a Kubernetes cluster and then deployed a simple container application to test working with an Azure AD workload identity (preview).

This tutorial is for introductory purposes. For guidance on creating full solutions with AKS for production, see [AKS solution guidance](#).

Kubernetes core concepts for Azure Kubernetes Service (AKS)

10/27/2022 • 14 minutes to read • [Edit Online](#)

Application development continues to move toward a container-based approach, increasing our need to orchestrate and manage resources. As the leading platform, Kubernetes provides reliable scheduling of fault-tolerant application workloads. Azure Kubernetes Service (AKS), a managed Kubernetes offering, further simplifies container-based application deployment and management.

This article introduces:

- Core Kubernetes infrastructure components:
 - *control plane*
 - *nodes*
 - *node pools*
- Workload resources:
 - *pods*
 - *deployments*
 - *sets*
- How to group resources into *namespaces*.

What is Kubernetes?

Kubernetes is a rapidly evolving platform that manages container-based applications and their associated networking and storage components. Kubernetes focuses on the application workloads, not the underlying infrastructure components. Kubernetes provides a declarative approach to deployments, backed by a robust set of APIs for management operations.

You can build and run modern, portable, microservices-based applications, using Kubernetes to orchestrate and manage the availability of the application components. Kubernetes supports both stateless and stateful applications as teams progress through the adoption of microservices-based applications.

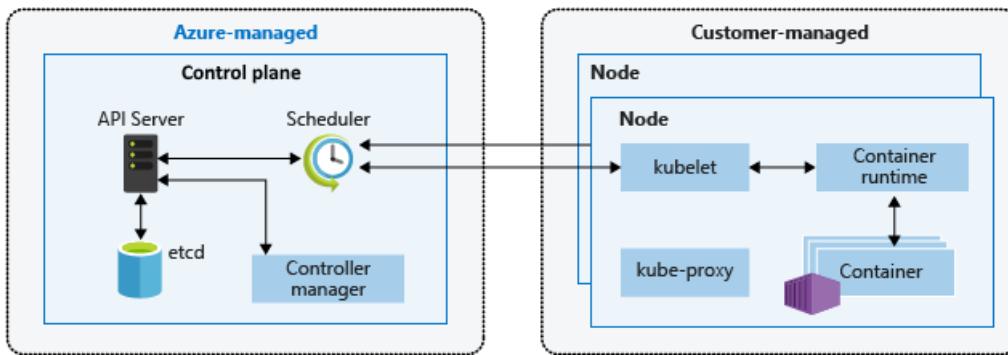
As an open platform, Kubernetes allows you to build your applications with your preferred programming language, OS, libraries, or messaging bus. Existing continuous integration and continuous delivery (CI/CD) tools can integrate with Kubernetes to schedule and deploy releases.

AKS provides a managed Kubernetes service that reduces the complexity of deployment and core management tasks, like upgrade coordination. The Azure platform manages the AKS control plane, and you only pay for the AKS nodes that run your applications.

Kubernetes cluster architecture

A Kubernetes cluster is divided into two components:

- *Control plane*: provides the core Kubernetes services and orchestration of application workloads.
- *Nodes*: run your application workloads.



Control plane

When you create an AKS cluster, a control plane is automatically created and configured. This control plane is provided at no cost as a managed Azure resource abstracted from the user. You only pay for the nodes attached to the AKS cluster. The control plane and its resources reside only on the region where you created the cluster.

The control plane includes the following core Kubernetes components:

COMPONENT	DESCRIPTION
<i>kube-apiserver</i>	The API server is how the underlying Kubernetes APIs are exposed. This component provides the interaction for management tools, such as <code>kubectl</code> or the Kubernetes dashboard.
<i>etcd</i>	To maintain the state of your Kubernetes cluster and configuration, the highly available <i>etcd</i> is a key value store within Kubernetes.
<i>kube-scheduler</i>	When you create or scale applications, the Scheduler determines what nodes can run the workload and starts them.
<i>kube-controller-manager</i>	The Controller Manager oversees a number of smaller Controllers that perform actions such as replicating pods and handling node operations.

AKS provides a single-tenant control plane, with a dedicated API server, scheduler, etc. You define the number and size of the nodes, and the Azure platform configures the secure communication between the control plane and nodes. Interaction with the control plane occurs through Kubernetes APIs, such as `kubectl` or the Kubernetes dashboard.

While you don't need to configure components (like a highly available *etcd* store) with this managed control plane, you can't access the control plane directly. Kubernetes control plane and node upgrades are orchestrated through the Azure CLI or Azure portal. To troubleshoot possible issues, you can review the control plane logs through Azure Monitor logs.

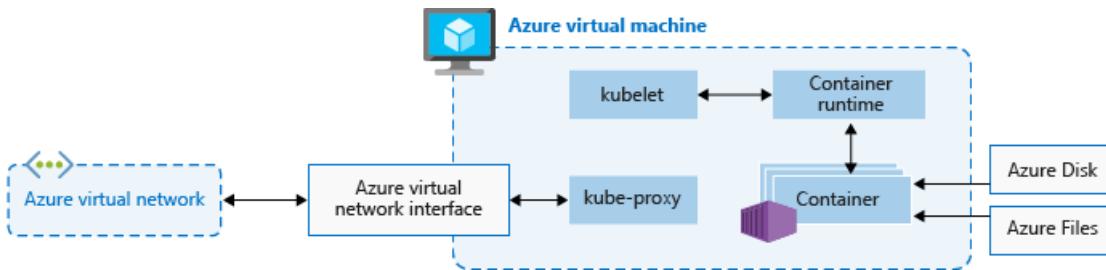
To configure or directly access a control plane, deploy a self-managed Kubernetes cluster using [Cluster API Provider Azure](#).

For associated best practices, see [Best practices for cluster security and upgrades in AKS](#).

Nodes and node pools

To run your applications and supporting services, you need a Kubernetes *node*. An AKS cluster has at least one node, an Azure virtual machine (VM) that runs the Kubernetes node components and container runtime.

COMPONENT	DESCRIPTION
kubelet	The Kubernetes agent that processes the orchestration requests from the control plane along with scheduling and running the requested containers.
<i>kube-proxy</i>	Handles virtual networking on each node. The proxy routes network traffic and manages IP addressing for services and pods.
<i>container runtime</i>	Allows containerized applications to run and interact with additional resources, such as the virtual network and storage. AKS clusters using Kubernetes version 1.19+ for Linux node pools use <code>containerd</code> as their container runtime. Beginning in Kubernetes version 1.20 for Windows node pools, <code>containerd</code> can be used in preview for the container runtime, but Docker is still the default container runtime. AKS clusters using prior versions of Kubernetes for node pools use Docker as their container runtime.



The Azure VM size for your nodes defines the storage CPUs, memory, size, and type available (such as high-performance SSD or regular HDD). Plan the node size around whether your applications may require large amounts of CPU and memory or high-performance storage. Scale out the number of nodes in your AKS cluster to meet demand.

In AKS, the VM image for your cluster's nodes is based on Ubuntu Linux or Windows Server 2019. When you create an AKS cluster or scale out the number of nodes, the Azure platform automatically creates and configures the requested number of VMs. Agent nodes are billed as standard VMs, so any VM size discounts (including [Azure reservations](#)) are automatically applied.

For managed disks, the default disk size and performance will be assigned according to the selected VM SKU and vCPU count. For more information, see [Default OS disk sizing](#).

If you need advanced configuration and control on your Kubernetes node container runtime and OS, you can deploy a self-managed cluster using [Cluster API Provider Azure](#).

Resource reservations

AKS uses node resources to help the node function as part of your cluster. This usage can create a discrepancy between your node's total resources and the allocatable resources in AKS. Remember this information when setting requests and limits for user deployed pods.

To find a node's allocatable resources, run:

```
kubectl describe node [NODE_NAME]
```

To maintain node performance and functionality, AKS reserves resources on each node. As a node grows larger in resources, the resource reservation grows due to a higher need for management of user-deployed pods.

NOTE

Using AKS add-ons such as Container Insights (OMS) will consume additional node resources.

Two types of resources are reserved:

- **CPU**

Reserved CPU is dependent on node type and cluster configuration, which may cause less allocatable CPU due to running additional features.

CPU CORES ON HOST	1	2	4	8	16	32	64
Kube-reserved (millicores)	60	100	140	180	260	420	740

- **Memory**

Memory utilized by AKS includes the sum of two values.

1. **kubelet daemon**

The `kubelet` daemon is installed on all Kubernetes agent nodes to manage container creation and termination.

By default on AKS, `kubelet` daemon has the `memory.available<750Mi` eviction rule, ensuring a node must always have at least 750 Mi allocatable at all times. When a host is below that available memory threshold, the `kubelet` will trigger to terminate one of the running pods and free up memory on the host machine.

2. **A regressive rate of memory reservations** for the kubelet daemon to properly function (*kube-reserved*).

- 25% of the first 4 GB of memory
- 20% of the next 4 GB of memory (up to 8 GB)
- 10% of the next 8 GB of memory (up to 16 GB)
- 6% of the next 112 GB of memory (up to 128 GB)
- 2% of any memory above 128 GB

NOTE

AKS reserves an additional 2GB for system process in Windows nodes that are not part of the calculated memory.

Memory and CPU allocation rules:

- Keep agent nodes healthy, including some hosting system pods critical to cluster health.
- Cause the node to report less allocatable memory and CPU than it would if it were not part of a Kubernetes cluster.

The above resource reservations can't be changed.

For example, if a node offers 7 GB, it will report 34% of memory not allocatable including the 750Mi hard eviction threshold.

$$0.75 + (0.25*4) + (0.20*3) = 0.75\text{GB} + 1\text{GB} + 0.6\text{GB} = 2.35\text{GB} / 7\text{GB} = 33.57\% \text{ reserved}$$

In addition to reservations for Kubernetes itself, the underlying node OS also reserves an amount of CPU and memory resources to maintain OS functions.

For associated best practices, see [Best practices for basic scheduler features in AKS](#).

Node pools

Nodes of the same configuration are grouped together into *node pools*. A Kubernetes cluster contains at least one node pool. The initial number of nodes and size are defined when you create an AKS cluster, which creates a *default node pool*. This default node pool in AKS contains the underlying VMs that run your agent nodes.

NOTE

To ensure your cluster operates reliably, you should run at least two (2) nodes in the default node pool.

You scale or upgrade an AKS cluster against the default node pool. You can choose to scale or upgrade a specific node pool. For upgrade operations, running containers are scheduled on other nodes in the node pool until all the nodes are successfully upgraded.

For more information about how to use multiple node pools in AKS, see [Create and manage multiple node pools for a cluster in AKS](#).

Node selectors

In an AKS cluster with multiple node pools, you may need to tell the Kubernetes Scheduler which node pool to use for a given resource. For example, ingress controllers shouldn't run on Windows Server nodes.

Node selectors let you define various parameters, like node OS, to control where a pod should be scheduled.

The following basic example schedules an NGINX instance on a Linux node using the node selector `"kubernetes.io/os": "linux"`.

```
kind: Pod
apiVersion: v1
metadata:
  name: nginx
spec:
  containers:
    - name: myfrontend
      image: mcr.microsoft.com/oss/nginx/nginx:1.15.12-alpine
  nodeSelector:
    "kubernetes.io/os": linux
```

For more information on how to control where pods are scheduled, see [Best practices for advanced scheduler features in AKS](#).

Pods

Kubernetes uses *pods* to run an instance of your application. A pod represents a single instance of your application.

Pods typically have a 1:1 mapping with a container. In advanced scenarios, a pod may contain multiple containers. Multi-container pods are scheduled together on the same node, and allow containers to share related resources.

When you create a pod, you can define *resource requests* to request a certain amount of CPU or memory resources. The Kubernetes Scheduler tries to meet the request by scheduling the pods to run on a node with available resources. You can also specify maximum resource limits to prevent a pod from consuming too much compute resource from the underlying node. Best practice is to include resource limits for all pods to help the

Kubernetes Scheduler identify necessary, permitted resources.

For more information, see [Kubernetes pods](#) and [Kubernetes pod lifecycle](#).

A pod is a logical resource, but application workloads run on the containers. Pods are typically ephemeral, disposable resources. Individually scheduled pods miss some of the high availability and redundancy Kubernetes features. Instead, pods are deployed and managed by Kubernetes *Controllers*, such as the Deployment Controller.

Deployments and YAML manifests

A *deployment* represents identical pods managed by the Kubernetes Deployment Controller. A deployment defines the number of pod *replicas* to create. The Kubernetes Scheduler ensures that additional pods are scheduled on healthy nodes if pods or nodes encounter problems.

You can update deployments to change the configuration of pods, container image used, or attached storage. The Deployment Controller:

- Drains and terminates a given number of replicas.
- Creates replicas from the new deployment definition.
- Continues the process until all replicas in the deployment are updated.

Most stateless applications in AKS should use the deployment model rather than scheduling individual pods. Kubernetes can monitor deployment health and status to ensure that the required number of replicas run within the cluster. When scheduled individually, pods aren't restarted if they encounter a problem, and aren't rescheduled on healthy nodes if their current node encounters a problem.

You don't want to disrupt management decisions with an update process if your application requires a minimum number of available instances. *Pod Disruption Budgets* define how many replicas in a deployment can be taken down during an update or node upgrade. For example, if you have *five (5)* replicas in your deployment, you can define a pod disruption of *4 (four)* to only allow one replica to be deleted or rescheduled at a time. As with pod resource limits, best practice is to define pod disruption budgets on applications that require a minimum number of replicas to always be present.

Deployments are typically created and managed with `kubectl create` or `kubectl apply`. Create a deployment by defining a manifest file in the YAML format.

The following example creates a basic deployment of the NGINX web server. The deployment specifies *three (3)* replicas to be created, and requires port *80* to be open on the container. Resource requests and limits are also defined for CPU and memory.

```

apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
        - name: nginx
          image: mcr.microsoft.com/oss/nginx/nginx:1.15.2-alpine
          ports:
            - containerPort: 80
          resources:
            requests:
              cpu: 250m
              memory: 64Mi
            limits:
              cpu: 500m
              memory: 256Mi

```

More complex applications can be created by including services (such as load balancers) within the YAML manifest.

For more information, see [Kubernetes deployments](#).

Package management with Helm

[Helm](#) is commonly used to manage applications in Kubernetes. You can deploy resources by building and using existing public Helm *charts* that contain a packaged version of application code and Kubernetes YAML manifests. You can store Helm charts either locally or in a remote repository, such as an [Azure Container Registry Helm chart repo](#).

To use Helm, install the Helm client on your computer, or use the Helm client in the [Azure Cloud Shell](#). Search for or create Helm charts, and then install them to your Kubernetes cluster. For more information, see [Install existing applications with Helm in AKS](#).

StatefulSets and DaemonSets

Using the Kubernetes Scheduler, the Deployment Controller runs replicas on any available node with available resources. While this approach may be sufficient for stateless applications, The Deployment Controller is not ideal for applications that require:

- A persistent naming convention or storage.
- A replica to exist on each select node within a cluster.

Two Kubernetes resources, however, let you manage these types of applications:

- *StatefulSets* maintain the state of applications beyond an individual pod lifecycle, such as storage.
- *DaemonSets* ensure a running instance on each node, early in the Kubernetes bootstrap process.

StatefulSets

Modern application development often aims for stateless applications. For stateful applications, like those that include database components, you can use *StatefulSets*. Like deployments, a StatefulSet creates and manages at least one identical pod. Replicas in a StatefulSet follow a graceful, sequential approach to deployment, scale,

upgrade, and termination. The naming convention, network names, and storage persist as replicas are rescheduled with a StatefulSet.

Define the application in YAML format using `kind: StatefulSet`. From there, the StatefulSet Controller handles the deployment and management of the required replicas. Data is written to persistent storage, provided by Azure Managed Disks or Azure Files. With StatefulSets, the underlying persistent storage remains, even when the StatefulSet is deleted.

For more information, see [Kubernetes StatefulSets](#).

Replicas in a StatefulSet are scheduled and run across any available node in an AKS cluster. To ensure at least one pod in your set runs on a node, you use a DaemonSet instead.

DaemonSets

For specific log collection or monitoring, you may need to run a pod on all, or selected, nodes. You can use `DaemonSet` deploy on one or more identical pods, but the DaemonSet Controller ensures that each node specified runs an instance of the pod.

The DaemonSet Controller can schedule pods on nodes early in the cluster boot process, before the default Kubernetes scheduler has started. This ability ensures that the pods in a DaemonSet are started before traditional pods in a Deployment or StatefulSet are scheduled.

Like StatefulSets, a DaemonSet is defined as part of a YAML definition using `kind: DaemonSet`.

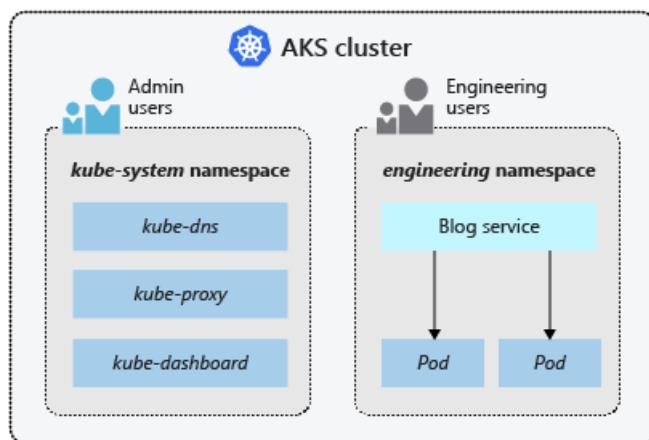
For more information, see [Kubernetes DaemonSets](#).

NOTE

If using the [Virtual Nodes add-on](#), DaemonSets will not create pods on the virtual node.

Namespaces

Kubernetes resources, such as pods and deployments, are logically grouped into a *namespace* to divide an AKS cluster and restrict create, view, or manage access to resources. For example, you can create namespaces to separate business groups. Users can only interact with resources within their assigned namespaces.



When you create an AKS cluster, the following namespaces are available:

NAMESPACE	DESCRIPTION
-----------	-------------

NAMESPACE	DESCRIPTION
<i>default</i>	Where pods and deployments are created by default when none is provided. In smaller environments, you can deploy applications directly into the default namespace without creating additional logical separations. When you interact with the Kubernetes API, such as with <code>kubectl get pods</code> , the default namespace is used when none is specified.
<i>kube-system</i>	Where core resources exist, such as network features like DNS and proxy, or the Kubernetes dashboard. You typically don't deploy your own applications into this namespace.
<i>kube-public</i>	Typically not used, but can be used for resources to be visible across the whole cluster, and can be viewed by any user.

For more information, see [Kubernetes namespaces](#).

Next steps

This article covers some of the core Kubernetes components and how they apply to AKS clusters. For more information on core Kubernetes and AKS concepts, see the following articles:

- [Kubernetes / AKS access and identity](#)
- [Kubernetes / AKS security](#)
- [Kubernetes / AKS virtual networks](#)
- [Kubernetes / AKS storage](#)
- [Kubernetes / AKS scale](#)

Security concepts for applications and clusters in Azure Kubernetes Service (AKS)

10/27/2022 • 8 minutes to read • [Edit Online](#)

Container security protects the entire end-to-end pipeline from build to the application workloads running in Azure Kubernetes Service (AKS).

The Secure Supply Chain includes the build environment and registry.

Kubernetes includes security components, such as *pod security standards* and *Secrets*. Meanwhile, Azure includes components like Active Directory, Microsoft Defender for Containers, Azure Policy, Azure Key Vault, network security groups and orchestrated cluster upgrades. AKS combines these security components to:

- Provide a complete Authentication and Authorization story.
- Leverage AKS Built-in Azure Policy to secure your applications.
- End-to-End insight from build through your application with Microsoft Defender for Containers.
- Keep your AKS cluster running the latest OS security updates and Kubernetes releases.
- Provide secure pod traffic and access to sensitive credentials.

This article introduces the core concepts that secure your applications in AKS:

- [Security concepts for applications and clusters in Azure Kubernetes Service \(AKS\)](#)
 - [Build security](#)
 - [Registry security](#)
 - [Cluster security](#)
 - [Node security](#)
 - [Compute isolation](#)
 - [Cluster upgrades](#)
 - [Cordon and drain](#)
 - [Network security](#)
 - [Azure network security groups](#)
 - [Application Security](#)
 - [Kubernetes Secrets](#)
 - [Next steps](#)

Build Security

As the entry point for the Supply Chain, it is important to conduct static analysis of image builds before they are promoted down the pipeline. This includes vulnerability and compliance assessment. It is not about failing a build because it has a vulnerability, as that will break development. It is about looking at the "Vendor Status" to segment based on vulnerabilities that are actionable by the development teams. Also leverage "Grace Periods" to allow developers time to remediate identified issues.

Registry Security

Assessing the vulnerability state of the image in the Registry will detect drift and will also catch images that didn't come from your build environment. Use [Notary V2](#) to attach signatures to your images to ensure deployments are coming from a trusted location.

Cluster security

In AKS, the Kubernetes master components are part of the managed service provided, managed, and maintained by Microsoft. Each AKS cluster has its own single-tenanted, dedicated Kubernetes master to provide the API Server, Scheduler, etc.

By default, the Kubernetes API server uses a public IP address and a fully qualified domain name (FQDN). You can limit access to the API server endpoint using [authorized IP ranges](#). You can also create a fully [private cluster](#) to limit API server access to your virtual network.

You can control access to the API server using Kubernetes role-based access control (Kubernetes RBAC) and Azure RBAC. For more information, see [Azure AD integration with AKS](#).

Node security

AKS nodes are Azure virtual machines (VMs) that you manage and maintain.

- Linux nodes run an optimized Ubuntu distribution using the `containerd` or Docker container runtime.
- Windows Server nodes run an optimized Windows Server 2019 release using the `containerd` or Docker container runtime.

When an AKS cluster is created or scaled up, the nodes are automatically deployed with the latest OS security updates and configurations.

NOTE

AKS clusters using:

- Kubernetes version 1.19 and greater for Linux node pools use `containerd` as its container runtime. Using `containerd` with Windows Server 2019 node pools is currently in preview. For more details, see [Add a Windows Server node pool with containerd](#).
- Kubernetes prior to v1.19 for Linux node pools use Docker as its container runtime. For Windows Server 2019 node pools, Docker is the default container runtime.

Node security patches

Linux nodes

Each evening, Linux nodes in AKS get security patches through their distro security update channel. This behavior is automatically configured as the nodes are deployed in an AKS cluster. To minimize disruption and potential impact to running workloads, nodes are not automatically rebooted if a security patch or kernel update requires it. For more information about how to handle node reboots, see [Apply security and kernel updates to nodes in AKS](#).

Nightly updates apply security updates to the OS on the node, but the node image used to create nodes for your cluster remains unchanged. If a new Linux node is added to your cluster, the original image is used to create the node. This new node will receive all the security and kernel updates available during the automatic check every night but will remain unpatched until all checks and restarts are complete. You can use node image upgrade to check for and update node images used by your cluster. For more details on node image upgrade, see [Azure Kubernetes Service \(AKS\) node image upgrade](#).

Windows Server nodes

For Windows Server nodes, Windows Update doesn't automatically run and apply the latest updates. Schedule Windows Server node pool upgrades in your AKS cluster around the regular Windows Update release cycle and your own validation process. This upgrade process creates nodes that run the latest Windows Server image and patches, then removes the older nodes. For more information on this process, see [Upgrade a node pool in AKS](#).

Node authorization

Node authorization is a special-purpose authorization mode that specifically authorizes API requests made by kubelets to protect against East-West attacks. Node authorization is enabled by default on AKS 1.24 + clusters.

Node deployment

Nodes are deployed into a private virtual network subnet, with no public IP addresses assigned. For troubleshooting and management purposes, SSH is enabled by default and only accessible using the internal IP address.

Node storage

To provide storage, the nodes use Azure Managed Disks. For most VM node sizes, Azure Managed Disks are Premium disks backed by high-performance SSDs. The data stored on managed disks is automatically encrypted at rest within the Azure platform. To improve redundancy, Azure Managed Disks are securely replicated within the Azure datacenter.

Hostile multi-tenant workloads

Currently, Kubernetes environments aren't safe for hostile multi-tenant usage. Extra security features, like *Pod Security Policies* or Kubernetes RBAC for nodes, efficiently block exploits. For true security when running hostile multi-tenant workloads, only trust a hypervisor. The security domain for Kubernetes becomes the entire cluster, not an individual node.

For these types of hostile multi-tenant workloads, you should use physically isolated clusters. For more information on ways to isolate workloads, see [Best practices for cluster isolation in AKS](#).

Compute isolation

Because of compliance or regulatory requirements, certain workloads may require a high degree of isolation from other customer workloads. For these workloads, Azure provides [isolated VMs](#) to use as the agent nodes in an AKS cluster. These VMs are isolated to a specific hardware type and dedicated to a single customer.

Select [one of the isolated VMs sizes](#) as the **node size** when creating an AKS cluster or adding a node pool.

Cluster upgrades

Azure provides upgrade orchestration tools to upgrade of an AKS cluster and components, maintain security and compliance, and access the latest features. This upgrade orchestration includes both the Kubernetes master and agent components.

To start the upgrade process, specify one of the [listed available Kubernetes versions](#). Azure then safely cordons and drains each AKS node and upgrades.

Cordon and drain

During the upgrade process, AKS nodes are individually cordoned from the cluster to prevent new pods from being scheduled on them. The nodes are then drained and upgraded as follows:

1. A new node is deployed into the node pool.
 - This node runs the latest OS image and patches.
2. One of the existing nodes is identified for upgrade.
3. Pods on the identified node are gracefully terminated and scheduled on the other nodes in the node pool.
4. The emptied node is deleted from the AKS cluster.
5. Steps 1-4 are repeated until all nodes are successfully replaced as part of the upgrade process.

For more information, see [Upgrade an AKS cluster](#).

Network security

For connectivity and security with on-premises networks, you can deploy your AKS cluster into existing Azure

virtual network subnets. These virtual networks connect back to your on-premises network using Azure Site-to-Site VPN or Express Route. Define Kubernetes ingress controllers with private, internal IP addresses to limit services access to the internal network connection.

Azure network security groups

To filter virtual network traffic flow, Azure uses network security group rules. These rules define the source and destination IP ranges, ports, and protocols allowed or denied access to resources. Default rules are created to allow TLS traffic to the Kubernetes API server. You create services with load balancers, port mappings, or ingress routes. AKS automatically modifies the network security group for traffic flow.

If you provide your own subnet for your AKS cluster (whether using Azure CNI or Kubenet), **do not** modify the NIC-level network security group managed by AKS. Instead, create more subnet-level network security groups to modify the flow of traffic. Make sure they don't interfere with necessary traffic managing the cluster, such as load balancer access, communication with the control plane, and [egress](#).

Kubernetes network policy

To limit network traffic between pods in your cluster, AKS offers support for [Kubernetes network policies](#). With network policies, you can allow or deny specific network paths within the cluster based on namespaces and label selectors.

Application Security

To protect pods running on AKS leverage [Microsoft Defender for Containers](#) to detect and restrict cyber attacks against your applications running in your pods. Run continual scanning to detect drift in the vulnerability state of your application and implement a "blue/green/canary" process to patch and replace the vulnerable images.

Kubernetes Secrets

With a Kubernetes *Secret*, you inject sensitive data into pods, such as access credentials or keys.

1. Create a Secret using the Kubernetes API.
2. Define your pod or deployment and request a specific Secret.
 - Secrets are only provided to nodes with a scheduled pod that requires them.
 - The Secret is stored in `tmpfs`, not written to disk.
3. When you delete the last pod on a node requiring a Secret, the Secret is deleted from the node's `tmpfs`.
 - Secrets are stored within a given namespace and can only be accessed by pods within the same namespace.

Using Secrets reduces the sensitive information defined in the pod or service YAML manifest. Instead, you request the Secret stored in Kubernetes API Server as part of your YAML manifest. This approach only provides the specific pod access to the Secret.

NOTE

The raw secret manifest files contain the secret data in base64 format (see the [official documentation](#) for more details). Treat these files as sensitive information, and never commit them to source control.

Kubernetes secrets are stored in etcd, a distributed key-value store. Etcd store is fully managed by AKS and [data is encrypted at rest within the Azure platform](#).

Next steps

To get started with securing your AKS clusters, see [Upgrade an AKS cluster](#).

For associated best practices, see [Best practices for cluster security and upgrades in AKS](#) and [Best practices for pod security in AKS](#).

For more information on core Kubernetes and AKS concepts, see:

- [Kubernetes / AKS clusters and workloads](#)
- [Kubernetes / AKS identity](#)
- [Kubernetes / AKS virtual networks](#)
- [Kubernetes / AKS storage](#)
- [Kubernetes / AKS scale](#)

Azure Policy Regulatory Compliance controls for Azure Kubernetes Service (AKS)

10/27/2022 • 22 minutes to read • [Edit Online](#)

Regulatory Compliance in Azure Policy provides initiative definitions (*built-ins*) created and managed by Microsoft, for the compliance domains and security controls related to different compliance standards. This page lists the Azure Kubernetes Service (AKS) compliance domains and security controls.

You can assign the built-ins for a **security control** individually to help make your Azure resources compliant with the specific standard.

The title of each built-in policy definition links to the policy definition in the Azure portal. Use the link in the **Policy Version** column to view the source on the [Azure Policy GitHub repo](#).

IMPORTANT

Each control is associated with one or more [Azure Policy](#) definitions. These policies might help you [assess compliance](#) with the control. However, there often isn't a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policies themselves. This doesn't ensure that you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between controls and Azure Policy Regulatory Compliance definitions for these compliance standards can change over time.

Azure Security Benchmark

The [Azure Security Benchmark](#) provides recommendations on how you can secure your cloud solutions on Azure. To see how this service completely maps to the Azure Security Benchmark, see the [Azure Security Benchmark mapping files](#).

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - Azure Security Benchmark](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Network Security	NS-2	Secure cloud services with network controls	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Privileged Access	PA-7	Follow just enough administration (least privilege) principle	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Data Protection	DP-3	Encrypt sensitive data in transit	Kubernetes clusters should be accessible only over HTTPS	8.0.0

Domain	Control ID	Control Title	Policy	Policy Version
Logging and Threat Detection	LT-1	Enable threat detection capabilities	Azure Kubernetes Service clusters should have Defender profile enabled	2.0.0
Logging and Threat Detection	LT-2	Enable threat detection for identity and access management	Azure Kubernetes Service clusters should have Defender profile enabled	2.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	[Preview]: Kubernetes clusters should gate deployment of vulnerable images	2.0.0-preview
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters	1.0.2
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits	9.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster containers should not share host process ID or host IPC namespace	5.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster containers should only use allowed AppArmor profiles	6.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster containers should only use allowed capabilities	6.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster containers should only use allowed images	9.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster containers should run with a read only root file system	6.0.0

Domain	Control ID	Control Title	Policy	Policy Version
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster pod hostPath volumes should only use allowed host paths	6.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster pods and containers should only run with approved user and group IDs	6.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster pods should only use approved host network and port range	6.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster services should listen only on allowed ports	8.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes cluster should not allow privileged containers	9.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes clusters should disable automounting API credentials	4.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes clusters should not allow container privilege escalation	7.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes clusters should not grant CAP_SYS_ADMIN security capabilities	5.0.0
Posture and Vulnerability Management	PV-2	Audit and enforce secure configurations	Kubernetes clusters should not use the default namespace	4.0.0
Posture and Vulnerability Management	PV-6	Rapidly and automatically remediate vulnerabilities	Running container images should have vulnerability findings resolved	1.0.1
DevOps Security	DS-6	Enforce security of workload throughout DevOps lifecycle	Running container images should have vulnerability findings resolved	1.0.1

Azure Security Benchmark v1

The [Azure Security Benchmark](#) provides recommendations on how you can secure your cloud solutions on Azure. To see how this service completely maps to the Azure Security Benchmark, see the [Azure Security Benchmark mapping files](#).

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - Azure Security Benchmark](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Network Security	1.1	Protect resources using Network Security Groups or Azure Firewall on your Virtual Network	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Data Protection	4.6	Use Azure RBAC to control access to resources	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Vulnerability Management	5.3	Deploy automated third-party software patch management solution	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2

CIS Microsoft Azure Foundations Benchmark 1.1.0

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - CIS Microsoft Azure Foundations Benchmark 1.1.0](#). For more information about this compliance standard, see [CIS Microsoft Azure Foundations Benchmark](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
8 Other Security Considerations	CIS Microsoft Azure Foundations Benchmark recommendation 8.5	Enable role-based access control (RBAC) within Azure Kubernetes Services	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2

CIS Microsoft Azure Foundations Benchmark 1.3.0

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - CIS Microsoft Azure Foundations Benchmark 1.3.0](#). For more information about this compliance standard, see [CIS Microsoft Azure Foundations Benchmark](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
8 Other Security Considerations	CIS Microsoft Azure Foundations Benchmark recommendation 8.5	Enable role-based access control (RBAC) within Azure Kubernetes Services	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2

CMMC Level 3

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - CMMC Level 3](#). For more information about this compliance standard, see [Cybersecurity Maturity Model Certification \(CMMC\)](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems).	Kubernetes cluster pods should only use approved host network and port range	6.0.0
Access Control	AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, and devices (including other information systems).	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Access Control	AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Kubernetes cluster pods should only use approved host network and port range	6.0.0
Access Control	AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Access Control	AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Access Control	AC.2.016	Control the flow of CUI in accordance with approved authorizations.	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Configuration Management	CM.2.062	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2

Domain	Control ID	Control Title	Policy	Policy Version
Configuration Management	CM.3.068	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Kubernetes cluster pods should only use approved host network and port range	6.0.0
Risk Assessment	RM.2.143	Remediate vulnerabilities in accordance with risk assessments.	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2
System and Communications Protection	SC.1.175	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	Kubernetes cluster pods should only use approved host network and port range	6.0.0
System and Communications Protection	SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys	1.0.0
System and Communications Protection	SC.3.183	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Kubernetes cluster pods should only use approved host network and port range	6.0.0
System and Information Integrity	SI.1.210	Identify, report, and correct information and information system flaws in a timely manner.	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2

FedRAMP High

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - FedRAMP High](#). For more information about this compliance standard, see [FedRAMP High](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC-4	Information Flow Enforcement	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Configuration Management	CM-6	Configuration Settings	Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters	1.0.2
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should not share host process ID or host IPC namespace	5.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed AppArmor profiles	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed capabilities	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed images	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should run with a read only root file system	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pod hostPath volumes should only use allowed host paths	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pods and containers should only run with approved user and group IDs	6.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pods should only use approved host network and port range	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster services should listen only on allowed ports	8.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster should not allow privileged containers	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes clusters should not allow container privilege escalation	7.0.0
System And Communications Protection	SC-7	Boundary Protection	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
System And Communications Protection	SC-7 (3)	Access Points	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
System And Communications Protection	SC-8	Transmission Confidentiality And Integrity	Kubernetes clusters should be accessible only over HTTPS	8.0.0
System And Communications Protection	SC-8 (1)	Cryptographic Or Alternate Physical Protection	Kubernetes clusters should be accessible only over HTTPS	8.0.0
System And Communications Protection	SC-12	Cryptographic Key Establishment And Management	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys	1.0.0
System And Communications Protection	SC-28	Protection Of Information At Rest	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host	1.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System And Communications Protection	SC-28 (1)	Cryptographic Protection	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host	1.0.0
System And Information Integrity	SI-2	Flaw Remediation	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2

FedRAMP Moderate

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - FedRAMP Moderate](#). For more information about this compliance standard, see [FedRAMP Moderate](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC-4	Information Flow Enforcement	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Configuration Management	CM-6	Configuration Settings	Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters	1.0.2
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should not share host process ID or host IPC namespace	5.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed AppArmor profiles	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed capabilities	6.0.0

Domain	Control ID	Control Title	Policy	Policy Version
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed images	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should run with a read only root file system	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pod hostPath volumes should only use allowed host paths	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pods and containers should only run with approved user and group IDs	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pods should only use approved host network and port range	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster services should listen only on allowed ports	8.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster should not allow privileged containers	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes clusters should not allow container privilege escalation	7.0.0
System And Communications Protection	SC-7	Boundary Protection	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
System And Communications Protection	SC-7 (3)	Access Points	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
System And Communications Protection	SC-8	Transmission Confidentiality And Integrity	Kubernetes clusters should be accessible only over HTTPS	8.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System And Communications Protection	SC-8 (1)	Cryptographic Or Alternate Physical Protection	Kubernetes clusters should be accessible only over HTTPS	8.0.0
System And Communications Protection	SC-12	Cryptographic Key Establishment And Management	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys	1.0.0
System And Communications Protection	SC-28	Protection Of Information At Rest	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host	1.0.0
System And Communications Protection	SC-28 (1)	Cryptographic Protection	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host	1.0.0
System And Information Integrity	SI-2	Flaw Remediation	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2

HIPAA HITRUST 9.2

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - HIPAA HITRUST 9.2](#). For more information about this compliance standard, see [HIPAA HITRUST 9.2](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Privilege Management	1149.01c2System.9 - 01.c	The organization facilitates information sharing by enabling authorized users to determine a business partner's access when discretion is allowed as defined by the organization and by employing manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions.	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
11 Access Control	1153.01c3System.35 -01.c	01.02 Authorized Access to Information Systems	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
12 Audit Logging & Monitoring	1229.09c1Organizational.1-09.c	09.01 Documented Operating Procedures	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2

NIST SP 800-53 Rev. 5

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - NIST SP 800-53 Rev. 5](#). For more information about this compliance standard, see [NIST SP 800-53 Rev. 5](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control	AC-3 (7)	Role-based Access Control	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Access Control	AC-4	Information Flow Enforcement	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Configuration Management	CM-6	Configuration Settings	Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters	1.0.2

Domain	Control ID	Control Title	Policy	Policy Version
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should not share host process ID or host IPC namespace	5.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed AppArmor profiles	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed capabilities	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should only use allowed images	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster containers should run with a read only root file system	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pod hostPath volumes should only use allowed host paths	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pods and containers should only run with approved user and group IDs	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster pods should only use approved host network and port range	6.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster services should listen only on allowed ports	8.0.0

Domain	Control ID	Control Title	Policy	Policy Version
Configuration Management	CM-6	Configuration Settings	Kubernetes cluster should not allow privileged containers	9.0.0
Configuration Management	CM-6	Configuration Settings	Kubernetes clusters should not allow container privilege escalation	7.0.0
System and Communications Protection	SC-7	Boundary Protection	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
System and Communications Protection	SC-7 (3)	Access Points	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
System and Communications Protection	SC-8	Transmission Confidentiality and Integrity	Kubernetes clusters should be accessible only over HTTPS	8.0.0
System and Communications Protection	SC-8 (1)	Cryptographic Protection	Kubernetes clusters should be accessible only over HTTPS	8.0.0
System and Communications Protection	SC-12	Cryptographic Key Establishment and Management	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys	1.0.0
System and Communications Protection	SC-28	Protection of Information at Rest	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host	1.0.0
System and Communications Protection	SC-28 (1)	Cryptographic Protection	Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host	1.0.0
System and Information Integrity	SI-2	Flaw Remediation	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
System and Information Integrity	SI-2 (6)	Removal of Previous Versions of Software and Firmware	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2

NZ ISM Restricted v3.5

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - NZ ISM Restricted v3.5](#). For more information about this compliance standard, see [NZ ISM Restricted v3.5](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Access Control and Passwords	NZISM Security Benchmark AC-18	16.6.9 Events to be logged	Resource logs in Azure Kubernetes Service should be enabled	1.0.0
Gateway security	NZISM Security Benchmark GS-2	19.1.11 Using Gateways	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Infrastructure	NZISM Security Benchmark INF-9	10.8.35 Security Architecture	Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters	1.0.2
Infrastructure	NZISM Security Benchmark INF-9	10.8.35 Security Architecture	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Software security	NZISM Security Benchmark SS-3	14.1.9 Maintaining hardened SOEs	Kubernetes cluster containers should not share host process ID or host IPC namespace	5.0.0
Software security	NZISM Security Benchmark SS-3	14.1.9 Maintaining hardened SOEs	Kubernetes cluster containers should run with a read only root file system	6.0.0
Software security	NZISM Security Benchmark SS-3	14.1.9 Maintaining hardened SOEs	Kubernetes cluster should not allow privileged containers	9.0.0
Software security	NZISM Security Benchmark SS-3	14.1.9 Maintaining hardened SOEs	Kubernetes clusters should be accessible only over HTTPS	8.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Software security	NZISM Security Benchmark SS-3	14.1.9 Maintaining hardened SOEs	Kubernetes clusters should disable automounting API credentials	4.0.0
Software security	NZISM Security Benchmark SS-3	14.1.9 Maintaining hardened SOEs	Kubernetes clusters should not allow container privilege escalation	7.0.0
Software security	NZISM Security Benchmark SS-3	14.1.9 Maintaining hardened SOEs	Kubernetes clusters should not grant CAP_SYS_ADMIN security capabilities	5.0.0
Software security	NZISM Security Benchmark SS-3	14.1.9 Maintaining hardened SOEs	Kubernetes clusters should not use the default namespace	4.0.0

Reserve Bank of India - IT Framework for NBFC

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - Reserve Bank of India - IT Framework for NBFC](#). For more information about this compliance standard, see [Reserve Bank of India - IT Framework for NBFC](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
IT Governance	RBI IT Framework 1	IT Governance-1	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2
Information and Cyber Security	RBI IT Framework 3.1.a	Identification and Classification of Information Assets-3.1	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Information and Cyber Security	RBI IT Framework 3.1.c	Role based Access Control-3.1	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Information and Cyber Security	RBI IT Framework 3.1.g	Trails-3.1	Azure Kubernetes Service clusters should have Defender profile enabled	2.0.0
Information and Cyber Security	RBI IT Framework 3.3	Vulnerability Management-3.3	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Information and Cyber Security	RBI IT Framework 3.3	Vulnerability Management-3.3	Running container images should have vulnerability findings resolved	1.0.1

Reserve Bank of India IT Framework for Banks v2016

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - RBI ITF Banks v2016](#). For more information about this compliance standard, see [RBI ITF Banks v2016 \(PDF\)](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Patch/Vulnerability & Change Management		Patch/Vulnerability & Change Management-7.7	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Patch/Vulnerability & Change Management		Patch/Vulnerability & Change Management-7.7	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Anti-Phishing		Anti-Phishing-14.1	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Advanced Real-Timethreat Defenceand Management		Advanced Real-Timethreat Defenceand Management-13.2	Azure Kubernetes Service clusters should have Defender profile enabled	2.0.0
User Access Control / Management		User Access Control / Management-8.5	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
User Access Control / Management		User Access Control / Management-8.1	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
User Access Control / Management		User Access Control / Management-8.8	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Application Security Life Cycle (Aslc)		Application Security Life Cycle (Aslc)-6.3	Running container images should have vulnerability findings resolved	1.0.1

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Application Security Life Cycle (Aslc)		Application Security Life Cycle (Aslc)-6.1	Running container images should have vulnerability findings resolved	1.0.1
Application Security Life Cycle (Aslc)		Application Security Life Cycle (Aslc)-6.7	Running container images should have vulnerability findings resolved	1.0.1
Application Security Life Cycle (Aslc)		Application Security Life Cycle (Aslc)-6.6	Running container images should have vulnerability findings resolved	1.0.1
Application Security Life Cycle (Aslc)		Application Security Life Cycle (Aslc)-6.3	Running container images should have vulnerability findings resolved	1.0.1
Application Security Life Cycle (Aslc)		Application Security Life Cycle (Aslc)-6.1	Running container images should have vulnerability findings resolved	1.0.1
Preventing Execution Of Unauthorised Software		Security Update Management-2.3	Running container images should have vulnerability findings resolved	1.0.1
Patch/Vulnerability & Change Management		Patch/Vulnerability & Change Management-7.6	Running container images should have vulnerability findings resolved	1.0.1
Patch/Vulnerability & Change Management		Patch/Vulnerability & Change Management-7.2	Running container images should have vulnerability findings resolved	1.0.1
Patch/Vulnerability & Change Management		Patch/Vulnerability & Change Management-7.1	Running container images should have vulnerability findings resolved	1.0.1
Patch/Vulnerability & Change Management		Patch/Vulnerability & Change Management-7.6	Running container images should have vulnerability findings resolved	1.0.1
Patch/Vulnerability & Change Management		Patch/Vulnerability & Change Management-7.2	Running container images should have vulnerability findings resolved	1.0.1

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Patch/Vulnerability & Change Management		Patch/Vulnerability & Change Management-7.1	Running container images should have vulnerability findings resolved	1.0.1
Application Security Life Cycle (Aslc)		Application Security Life Cycle (Aslc)-6.6	Running container images should have vulnerability findings resolved	1.0.1
Application Security Life Cycle (Aslc)		Application Security Life Cycle (Aslc)-6.7	Running container images should have vulnerability findings resolved	1.0.1

RMIT Malaysia

To review how the available Azure Policy built-ins for all Azure services map to this compliance standard, see [Azure Policy Regulatory Compliance - RMIT Malaysia](#). For more information about this compliance standard, see [RMIT Malaysia](#).

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY (AZURE PORTAL)	POLICY VERSION (GITHUB)
Cryptography	RMiT 10.19	Cryptography - 10.19	Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys	1.0.0
Access Control	RMiT 10.54	Access Control - 10.54	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Access Control	RMiT 10.55	Access Control - 10.55	Kubernetes cluster containers should only use allowed capabilities	6.0.0
Access Control	RMiT 10.55	Access Control - 10.55	Kubernetes cluster containers should run with a read only root file system	6.0.0
Access Control	RMiT 10.55	Access Control - 10.55	Kubernetes cluster pods and containers should only run with approved user and group IDs	6.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION
Access Control	RMiT 10.55	Access Control - 10.55	Kubernetes cluster should not allow privileged containers	9.0.0
Access Control	RMiT 10.55	Access Control - 10.55	Kubernetes clusters should not allow container privilege escalation	7.0.0
Access Control	RMiT 10.60	Access Control - 10.60	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Access Control	RMiT 10.61	Access Control - 10.61	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Access Control	RMiT 10.62	Access Control - 10.62	Role-Based Access Control (RBAC) should be used on Kubernetes Services	1.0.2
Patch and End-of-Life System Management	RMiT 10.65	Patch and End-of-Life System Management - 10.65	Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version	1.0.2
Security Operations Centre (SOC)	RMiT 11.17	Security Operations Centre (SOC) - 11.17	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Security Operations Centre (SOC)	RMiT 11.17	Security Operations Centre (SOC) - 11.17	Authorized IP ranges should be defined on Kubernetes Services	2.0.1
Control Measures on Cybersecurity	RMiT Appendix 5.5	Control Measures on Cybersecurity - Appendix 5.5	Kubernetes cluster services should only use allowed external IPs	5.0.0
Control Measures on Cybersecurity	RMiT Appendix 5.6	Control Measures on Cybersecurity - Appendix 5.6	Kubernetes cluster pods should only use approved host network and port range	6.0.0
Control Measures on Cybersecurity	RMiT Appendix 5.6	Control Measures on Cybersecurity - Appendix 5.6	Kubernetes cluster services should listen only on allowed ports	8.0.0
Control Measures on Cybersecurity	RMiT Appendix 5.6	Control Measures on Cybersecurity - Appendix 5.6	Kubernetes clusters should be accessible only over HTTPS	8.0.0

DOMAIN	CONTROL ID	CONTROL TITLE	POLICY	POLICY VERSION

Next steps

- Learn more about [Azure Policy Regulatory Compliance](#).
- See the built-ins on the [Azure Policy GitHub repo](#).

Center for Internet Security (CIS) Kubernetes benchmark

10/27/2022 • 11 minutes to read • [Edit Online](#)

As a secure service, Azure Kubernetes Service (AKS) complies with SOC, ISO, PCI DSS, and HIPAA standards. This article covers the security hardening applied to AKS based on the CIS Kubernetes benchmark. For more information about AKS security, see [Security concepts for applications and clusters in Azure Kubernetes Service \(AKS\)](#). For more information on the CIS benchmark, see [Center for Internet Security \(CIS\) Benchmarks](#).

Kubernetes CIS benchmark

The following are the results from the [CIS Kubernetes V1.20 Benchmark v1.0.0](#) recommendations on AKS.

Scored recommendations affect the benchmark score if they are not applied, while *Not Scored* recommendations don't.

CIS benchmarks provide two levels of security settings:

- *L1*, or Level 1, recommends essential basic security requirements that can be configured on any system and should cause little or no interruption of service or reduced functionality.
- *L2*, or Level 2, recommends security settings for environments requiring greater security that could result in some reduced functionality.

Recommendations can have one of the following statuses:

- *Pass* - The recommendation has been applied.
- *Fail* - The recommendation has not been applied.
- *N/A* - The recommendation relates to manifest file permission requirements that are not relevant to AKS. Kubernetes clusters by default use a manifest model to deploy the control plane pods, which rely on files from the node VM. The CIS Kubernetes benchmark recommends these files must have certain permission requirements. AKS clusters use a Helm chart to deploy control plane pods and don't rely on files in the node VM.
- *Depends on Environment* - The recommendation is applied in the user's specific environment and is not controlled by AKS. *Scored* recommendations affect the benchmark score whether the recommendation applies to the user's specific environment or not.
- *Equivalent Control* - The recommendation has been implemented in a different, equivalent manner.

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1	Control Plane Components			
1.1	Control Plane Node Configuration Files			

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1.1.1	Ensure that the API server pod specification file permissions are set to 644 or more restrictive	Scored	L1	N/A
1.1.2	Ensure that the API server pod specification file ownership is set to root:root	Scored	L1	N/A
1.1.3	Ensure that the controller manager pod specification file permissions are set to 644 or more restrictive	Scored	L1	N/A
1.1.4	Ensure that the controller manager pod specification file ownership is set to root:root	Scored	L1	N/A
1.1.5	Ensure that the scheduler pod specification file permissions are set to 644 or more restrictive	Scored	L1	N/A
1.1.6	Ensure that the scheduler pod specification file ownership is set to root:root	Scored	L1	N/A
1.1.7	Ensure that the etcd pod specification file permissions are set to 644 or more restrictive	Scored	L1	N/A
1.1.8	Ensure that the etcd pod specification file ownership is set to root:root	Scored	L1	N/A
1.1.9	Ensure that the Container Network Interface file permissions are set to 644 or more restrictive	Not Scored	L1	N/A

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1.1.10	Ensure that the Container Network Interface file ownership is set to root:root	Not Scored	L1	N/A
1.1.11	Ensure that the etcd data directory permissions are set to 700 or more restrictive	Scored	L1	N/A
1.1.12	Ensure that the etcd data directory ownership is set to etcd:etcd	Scored	L1	N/A
1.1.13	Ensure that the admin.conf file permissions are set to 644 or more restrictive	Scored	L1	N/A
1.1.14	Ensure that the admin.conf file ownership is set to root:root	Scored	L1	N/A
1.1.15	Ensure that the scheduler.conf file permissions are set to 644 or more restrictive	Scored	L1	N/A
1.1.16	Ensure that the scheduler.conf file ownership is set to root:root	Scored	L1	N/A
1.1.17	Ensure that the controller-manager.conf file permissions are set to 644 or more restrictive	Scored	L1	N/A
1.1.18	Ensure that the controller-manager.conf file ownership is set to root:root	Scored	L1	N/A

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1.1.19	Ensure that the Kubernetes PKI directory and file ownership is set to root:root	Scored	L1	N/A
1.1.20	Ensure that the Kubernetes PKI certificate file permissions are set to 644 or more restrictive	Scored	L1	N/A
1.1.21	Ensure that the Kubernetes PKI key file permissions are set to 600	Scored	L1	N/A
1.2	API Server			
1.2.1	Ensure that the <code>--anonymous-auth</code> argument is set to false	Not Scored	L1	Pass
1.2.2	Ensure that the <code>--basic-auth-file</code> argument is not set	Scored	L1	Pass
1.2.3	Ensure that the <code>--token-auth-file</code> parameter is not set	Scored	L1	Fail
1.2.4	Ensure that the <code>--kubelet-https</code> argument is set to true	Scored	L1	Equivalent Control
1.2.5	Ensure that the <code>--kubelet-client-certificate</code> and <code>--kubelet-client-key</code> arguments are set as appropriate	Scored	L1	Pass
1.2.6	Ensure that the <code>--kubelet-certificate-authority</code> argument is set as appropriate	Scored	L1	Equivalent Control

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1.2.7	Ensure that the --authorization-mode argument is not set to AlwaysAllow	Scored	L1	Pass
1.2.8	Ensure that the --authorization-mode argument includes Node	Scored	L1	Pass
1.2.9	Ensure that the --authorization-mode argument includes RBAC	Scored	L1	Pass
1.2.10	Ensure that the admission control plugin EventRateLimit is set	Not Scored	L1	Fail
1.2.11	Ensure that the admission control plugin AlwaysAdmit is not set	Scored	L1	Pass
1.2.12	Ensure that the admission control plugin AlwaysPullImages is set	Not Scored	L1	Fail
1.2.13	Ensure that the admission control plugin SecurityContextDeny is set if PodSecurityPolicy is not used	Not Scored	L1	Fail
1.2.14	Ensure that the admission control plugin ServiceAccount is set	Scored	L1	Pass
1.2.15	Ensure that the admission control plugin NamespaceLifecycle is set	Scored	L1	Pass

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1.2.16	Ensure that the admission control plugin PodSecurityPolicy is set	Scored	L1	Fail
1.2.17	Ensure that the admission control plugin NodeRestriction is set	Scored	L1	Fail
1.2.18	Ensure that the <code>--insecure-bind-address</code> argument is not set	Scored	L1	Fail
1.2.19	Ensure that the <code>--insecure-port</code> argument is set to 0	Scored	L1	Pass
1.2.20	Ensure that the <code>--secure-port</code> argument is not set to 0	Scored	L1	Pass
1.2.21	Ensure that the <code>--profiling</code> argument is set to false	Scored	L1	Pass
1.2.22	Ensure that the <code>--audit-log-path</code> argument is set	Scored	L1	Pass
1.2.23	Ensure that the <code>--audit-log-maxage</code> argument is set to 30 or as appropriate	Scored	L1	Equivalent Control
1.2.24	Ensure that the <code>--audit-log-maxbackup</code> argument is set to 10 or as appropriate	Scored	L1	Equivalent Control
1.2.25	Ensure that the <code>--audit-log-maxsize</code> argument is set to 100 or as appropriate	Scored	L1	Pass

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1.2.26	Ensure that the --request-timeout argument is set as appropriate	Scored	L1	Pass
1.2.27	Ensure that the --service-account-lookup argument is set to true	Scored	L1	Pass
1.2.28	Ensure that the --service-account-key-file argument is set as appropriate	Scored	L1	Pass
1.2.29	Ensure that the --etcd-certfile and --etcd-keyfile arguments are set as appropriate	Scored	L1	Pass
1.2.30	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate	Scored	L1	Pass
1.2.31	Ensure that the --client-ca-file argument is set as appropriate	Scored	L1	Pass
1.2.32	Ensure that the --etcd-cafile argument is set as appropriate	Scored	L1	Pass
1.2.33	Ensure that the --encryption-provider-config argument is set as appropriate	Scored	L1	Fail
1.2.34	Ensure that encryption providers are appropriately configured	Scored	L1	Fail

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1.2.35	Ensure that the API Server only makes use of Strong Cryptographic Ciphers	Not Scored	L1	Pass
1.3	Controller Manager			
1.3.1	Ensure that the <code>--terminated-pod-gc-threshold</code> argument is set as appropriate	Scored	L1	Pass
1.3.2	Ensure that the <code>--profiling</code> argument is set to false	Scored	L1	Pass
1.3.3	Ensure that the <code>--use-service-account-credentials</code> argument is set to true	Scored	L1	Pass
1.3.4	Ensure that the <code>--service-account-private-key-file</code> argument is set as appropriate	Scored	L1	Pass
1.3.5	Ensure that the <code>--root-ca-file</code> argument is set as appropriate	Scored	L1	Pass
1.3.6	Ensure that the RotateKubeletServer Certificate argument is set to true	Scored	L2	Pass
1.3.7	Ensure that the <code>--bind-address</code> argument is set to 127.0.0.1	Scored	L1	Fail
1.4	Scheduler			
1.4.1	Ensure that the <code>--profiling</code> argument is set to false	Scored	L1	Pass

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
1.4.2	Ensure that the <code>--bind-address</code> argument is set to 127.0.0.1	Scored	L1	Fail
2	etcd			
2.1	Ensure that the <code>--cert-file</code> and <code>--key-file</code> arguments are set as appropriate	Scored	L1	Pass
2.2	Ensure that the <code>--client-cert-auth</code> argument is set to true	Scored	L1	Pass
2.3	Ensure that the <code>--auto-tls</code> argument is not set to true	Scored	L1	Pass
2.4	Ensure that the <code>--peer-cert-file</code> and <code>--peer-key-file</code> arguments are set as appropriate	Scored	L1	Pass
2.5	Ensure that the <code>--peer-client-cert-auth</code> argument is set to true	Scored	L1	Pass
2.6	Ensure that the <code>--peer-auto-tls</code> argument is not set to true	Scored	L1	Pass
2.7	Ensure that a unique Certificate Authority is used for etcd	Not Scored	L2	Pass
3	Control Plane Configuration			
3.1	Authentication and Authorization			

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
3.1.1	Client certificate authentication should not be used for users	Not Scored	L2	Pass
3.2	Logging			
3.2.1	Ensure that a minimal audit policy is created	Scored	L1	Pass
3.2.2	Ensure that the audit policy covers key security concerns	Not Scored	L2	Pass
4	Worker Nodes			
4.1	Worker Node Configuration Files			
4.1.1	Ensure that the kubelet service file permissions are set to 644 or more restrictive	Scored	L1	Pass
4.1.2	Ensure that the kubelet service file ownership is set to root:root	Scored	L1	Pass
4.1.3	Ensure that the proxy kubeconfig file permissions are set to 644 or more restrictive	Scored	L1	Pass
4.1.4	Ensure that the proxy kubeconfig file ownership is set to root:root	Scored	L1	Pass
4.1.5	Ensure that the kubelet.conf file permissions are set to 644 or more restrictive	Scored	L1	Pass
4.1.6	Ensure that the kubelet.conf file ownership is set to root:root	Scored	L1	Pass

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
4.1.7	Ensure that the certificate authorities file permissions are set to 644 or more restrictive	Scored	L1	Pass
4.1.8	Ensure that the client certificate authorities file ownership is set to root:root	Scored	L1	Pass
4.1.9	Ensure that the kubelet configuration file has permissions set to 644 or more restrictive	Scored	L1	Pass
4.1.10	Ensure that the kubelet configuration file ownership is set to root:root	Scored	L1	Pass
4.2	Kubelet			
4.2.1	Ensure that the <code>--anonymous-auth</code> argument is set to false	Scored	L1	Pass
4.2.2	Ensure that the <code>--authorization-mode</code> argument is not set to AlwaysAllow	Scored	L1	Pass
4.2.3	Ensure that the <code>--client-ca-file</code> argument is set as appropriate	Scored	L1	Pass
4.2.4	Ensure that the <code>--read-only-port</code> argument is set to 0	Scored	L1	Pass
4.2.5	Ensure that the <code>--streaming-connection-idle-timeout</code> argument is not set to 0	Scored	L1	Pass
4.2.6	Ensure that the <code>--protect-kernel-defaults</code> argument is set to true	Scored	L1	Pass

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
4.2.7	Ensure that the --make-iptables-util-chains argument is set to true	Scored	L1	Pass
4.2.8	Ensure that the --hostname-override argument is not set	Not Scored	L1	Pass
4.2.9	Ensure that the --event-qps argument is set to 0 or a level which ensures appropriate event capture	Not Scored	L2	Pass
4.2.10	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate	Scored	L1	Equivalent Control
4.2.11	Ensure that the --rotate-certificates argument is not set to false	Scored	L1	Pass
4.2.12	Ensure that the RotateKubeletServer Certificate argument is set to true	Scored	L1	Fail
4.2.13	Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers	Not Scored	L1	Pass
5	Policies			
5.1	RBAC and Service Accounts			
5.1.1	Ensure that the cluster-admin role is only used where required	Not Scored	L1	Depends on Environment
5.1.2	Minimize access to secrets	Not Scored	L1	Depends on Environment

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
5.1.3	Minimize wildcard use in Roles and ClusterRoles	Not Scored	L1	Depends on Environment
5.1.4	Minimize access to create pods	Not Scored	L1	Depends on Environment
5.1.5	Ensure that default service accounts are not actively used	Scored	L1	Depends on Environment
5.1.6	Ensure that Service Account Tokens are only mounted where necessary	Not Scored	L1	Depends on Environment
5.2	Pod Security Policies			
5.2.1	Minimize the admission of privileged containers	Not Scored	L1	Depends on Environment
5.2.2	Minimize the admission of containers wishing to share the host process ID namespace	Scored	L1	Depends on Environment
5.2.3	Minimize the admission of containers wishing to share the host IPC namespace	Scored	L1	Depends on Environment
5.2.4	Minimize the admission of containers wishing to share the host network namespace	Scored	L1	Depends on Environment
5.2.5	Minimize the admission of containers with allowPrivilegeEscalation	Scored	L1	Depends on Environment
5.2.6	Minimize the admission of root containers	Not Scored	L2	Depends on Environment
5.2.7	Minimize the admission of containers with the NET_RAW capability	Not Scored	L1	Depends on Environment

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
5.2.8	Minimize the admission of containers with added capabilities	Not Scored	L1	Depends on Environment
5.2.9	Minimize the admission of containers with capabilities assigned	Not Scored	L2	Depends on Environment
5.3	Network Policies and CNI			
5.3.1	Ensure that the CNI in use supports Network Policies	Not Scored	L1	Pass
5.3.2	Ensure that all Namespaces have Network Policies defined	Scored	L2	Depends on Environment
5.4	Secrets Management			
5.4.1	Prefer using secrets as files over secrets as environment variables	Not Scored	L1	Depends on Environment
5.4.2	Consider external secret storage	Not Scored	L2	Depends on Environment
5.5	Extensible Admission Control			
5.5.1	Configure Image Provenance using ImagePolicyWebhook admission controller	Not Scored	L2	Depends on Environment
5.6	General Policies			
5.6.1	Create administrative boundaries between resources using namespaces	Not Scored	L1	Depends on Environment
5.6.2	Ensure that the seccomp profile is set to docker/default in your pod definitions	Not Scored	L2	Depends on Environment
5.6.3	Apply Security Context to Your Pods and Containers	Not Scored	L2	Depends on Environment

CIS ID	RECOMMENDATION DESCRIPTION	SCORING TYPE	LEVEL	STATUS
5.6.4	The default namespace should not be used	Scored	L2	Depends on Environment

NOTE

In addition to the Kubernetes CIS benchmark, there is an [AKS CIS benchmark](#) available as well.

Additional notes

- The security hardened OS is built and maintained specifically for AKS and is **not** supported outside of the AKS platform.
- To further reduce the attack surface area, some unnecessary kernel module drivers have been disabled in the OS.

Next steps

For more information about AKS security, see the following articles:

- [Azure Kubernetes Service \(AKS\)](#)
- [AKS security considerations](#)
- [AKS best practices](#)

Azure Kubernetes Service (AKS) Ubuntu image alignment with Center for Internet Security (CIS) benchmark

10/27/2022 • 11 minutes to read • [Edit Online](#)

As a secure service, Azure Kubernetes Service (AKS) complies with SOC, ISO, PCI DSS, and HIPAA standards. This article covers the security OS configuration applied to Ubuntu imaged used by AKS. This security configuration is based on the Azure Linux security baseline which aligns with CIS benchmark. For more information about AKS security, see [Security concepts for applications and clusters in Azure Kubernetes Service \(AKS\)](#). For more information about AKS security, see [Security concepts for applications and clusters in Azure Kubernetes Service \(AKS\)](#). For more information on the CIS benchmark, see [Center for Internet Security \(CIS\) Benchmarks](#). For more information on the Azure security baselines for Linux, see [Linux security baseline](#).

Ubuntu LTS 18.04

AKS clusters are deployed on host virtual machines, which run an operating system with built-in secure configurations. This operating system is used for containers running on AKS. This host operating system is based on an **Ubuntu 18.04.LTS** image with security configurations applied.

As a part of the security-optimized operating system:

- AKS provides a security-optimized host OS by default, but no option to select an alternate operating system.
- The security-optimized host OS is built and maintained specifically for AKS and is **not** supported outside of the AKS platform.
- Some unnecessary kernel module drivers have been disabled in the OS to reduce the attack surface area.

NOTE

Unrelated to the CIS benchmarks, Azure applies daily patches, including security patches, to AKS virtual machine hosts.

The goal of the secure configuration built into the host OS is to reduce the surface area of attack and optimize for the deployment of containers in a secure manner.

The following are the results from the [CIS Ubuntu 18.04 LTS Benchmark v2.1.0](#) recommendations.

Recommendations can have one of the following reasons:

- *Potential Operation Impact* - Recommendation was not applied because it would have a negative effect on the service.
- *Covered Elsewhere* - Recommendation is covered by another control in Azure cloud compute.

The following are CIS rules implemented:

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
1	Initial Setup		
1.1	Filesystem Configuration		

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
1.1.1	Disable unused filesystems		
1.1.1.1	Ensure mounting of cramfs filesystems is disabled	Pass	
1.1.1.2	Ensure mounting of freevxf filesystems is disabled	Pass	
1.1.1.3	Ensure mounting of jffs2 filesystems is disabled	Pass	
1.1.1.4	Ensure mounting of hfs filesystems is disabled	Pass	
1.1.1.5	Ensure mounting of hfsplus filesystems is disabled	Pass	
1.1.1.6	Ensure mounting of udf filesystems is disabled	Fail	Potential Operational Impact
1.1.2	Ensure /tmp is configured	Fail	
1.1.3	Ensure nodev option set on /tmp partition	Fail	
1.1.4	Ensure nosuid option set on /tmp partition	Pass	
1.1.5	Ensure noexec option set on /tmp partition	Pass	
1.1.6	Ensure /dev/shm is configured	Pass	
1.1.7	Ensure nodev option set on /dev/shm partition	Pass	
1.1.8	Ensure nosuid option set on /dev/shm partition	Pass	
1.1.9	Ensure noexec option set on /dev/shm partition	Fail	Potential Operational Impact
1.1.12	Ensure /var/tmp partition includes the nodev option	Pass	
1.1.13	Ensure /var/tmp partition includes the nosuid option	Pass	
1.1.14	Ensure /var/tmp partition includes the noexec option	Pass	

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
1.1.18	Ensure /home partition includes the nodev option	Pass	
1.1.19	Ensure nodev option set on removable media partitions	Not Applicable	
1.1.20	Ensure nosuid option set on removable media partitions	Not Applicable	
1.1.21	Ensure noexec option set on removable media partitions	Not Applicable	
1.1.22	Ensure sticky bit is set on all world-writable directories	Fail	Potential Operation Impact
1.1.23	Disable Automounting	Pass	
1.1.24	Disable USB Storage	Pass	
1.2	Configure Software Updates		
1.2.1	Ensure package manager repositories are configured	Pass	Covered Elsewhere
1.2.2	Ensure GPG keys are configured	Not Applicable	
1.3	Filesystem Integrity Checking		
1.3.1	Ensure AIDE is installed	Fail	Covered Elsewhere
1.3.2	Ensure filesystem integrity is regularly checked	Fail	Covered Elsewhere
1.4	Secure Boot Settings		
1.4.1	Ensure permissions on bootloader config are not overridden	Fail	
1.4.2	Ensure bootloader password is set	Fail	Not Applicable
1.4.3	Ensure permissions on bootloader config are configured	Fail	
1.4.4	Ensure authentication required for single user mode	Fail	Not Applicable

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
1.5	Additional Process Hardening		
1.5.1	Ensure XD/NX support is enabled	Not Applicable	
1.5.2	Ensure address space layout randomization (ASLR) is enabled	Pass	
1.5.3	Ensure prelink is disabled	Pass	
1.5.4	Ensure core dumps are restricted	Pass	
1.6	Mandatory Access Control		
1.6.1	Configure AppArmor		
1.6.1.1	Ensure AppArmor is installed	Pass	
1.6.1.2	Ensure AppArmor is enabled in the bootloader configuration	Fail	Potential Operation Impact
1.6.1.3	Ensure all AppArmor Profiles are in enforce or complain mode	Pass	
1.7	Command Line Warning Banners		
1.7.1	Ensure message of the day is configured properly	Pass	
1.7.2	Ensure permissions on /etc/issue.net are configured	Pass	
1.7.3	Ensure permissions on /etc/issue are configured	Pass	
1.7.4	Ensure permissions on /etc/motd are configured	Pass	
1.7.5	Ensure remote login warning banner is configured properly	Pass	
1.7.6	Ensure local login warning banner is configured properly	Pass	

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
1.8	GNOME Display Manager		
1.8.2	Ensure GDM login banner is configured	Pass	
1.8.3	Ensure disable-user-list is enabled	Pass	
1.8.4	Ensure XDCMP is not enabled	Pass	
1.9	Ensure updates, patches, and additional security software are installed	Pass	
2	Services		
2.1	Special Purpose Services		
2.1.1	Time Synchronization		
2.1.1.1	Ensure time synchronization is in use	Pass	
2.1.1.2	Ensure systemd-timesyncd is configured	Not Applicable	AKS uses ntpd for timesync
2.1.1.3	Ensure chrony is configured	Fail	Covered Elsewhere
2.1.1.4	Ensure ntp is configured	Pass	
2.1.2	Ensure X Window System is not installed	Pass	
2.1.3	Ensure Avahi Server is not installed	Pass	
2.1.4	Ensure CUPS is not installed	Pass	
2.1.5	Ensure DHCP Server is not installed	Pass	
2.1.6	Ensure LDAP server is not installed	Pass	
2.1.7	Ensure NFS is not installed	Pass	
2.1.8	Ensure DNS Server is not installed	Pass	
2.1.9	Ensure FTP Server is not installed	Pass	

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
2.1.10	Ensure HTTP server is not installed	Pass	
2.1.11	Ensure IMAP and POP3 server are not installed	Pass	
2.1.12	Ensure Samba is not installed	Pass	
2.1.13	Ensure HTTP Proxy Server is not installed	Pass	
2.1.14	Ensure SNMP Server is not installed	Pass	
2.1.15	Ensure mail transfer agent is configured for local-only mode	Pass	
2.1.16	Ensure rsync service is not installed	Fail	
2.1.17	Ensure NIS Server is not installed	Pass	
2.2	Service Clients		
2.2.1	Ensure NIS Client is not installed	Pass	
2.2.2	Ensure rsh client is not installed	Pass	
2.2.3	Ensure talk client is not installed	Pass	
2.2.4	Ensure telnet client is not installed	Fail	
2.2.5	Ensure LDAP client is not installed	Pass	
2.2.6	Ensure RPC is not installed	Fail	Potential Operational Impact
2.3	Ensure nonessential services are removed or masked	Pass	
3	Network Configuration		
3.1	Disable unused network protocols and devices		

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
3.1.2	Ensure wireless interfaces are disabled	Pass	
3.2	Network Parameters (Host Only)		
3.2.1	Ensure packet redirect sending is disabled	Pass	
3.2.2	Ensure IP forwarding is disabled	Fail	Not Applicable
3.3	Network Parameters (Host and Router)		
3.3.1	Ensure source routed packets are not accepted	Pass	
3.3.2	Ensure ICMP redirects are not accepted	Pass	
3.3.3	Ensure secure ICMP redirects are not accepted	Pass	
3.3.4	Ensure suspicious packets are logged	Pass	
3.3.5	Ensure broadcast ICMP requests are ignored	Pass	
3.3.6	Ensure bogus ICMP responses are ignored	Pass	
3.3.7	Ensure Reverse Path Filtering is enabled	Pass	
3.3.8	Ensure TCP SYN Cookies is enabled	Pass	
3.3.9	Ensure IPv6 router advertisements are not accepted	Pass	
3.4	Uncommon Network Protocols		
3.5	Firewall Configuration		
3.5.1	Configure UncomplicatedFirewall		
3.5.1.1	Ensure ufw is installed	Pass	

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
3.5.1.2	Ensure iptables-persistent is not installed with ufw	Pass	
3.5.1.3	Ensure ufw service is enabled	Fail	Covered Elsewhere
3.5.1.4	Ensure ufw loopback traffic is configured	Fail	Covered Elsewhere
3.5.1.5	Ensure ufw outbound connections are configured	Not Applicable	Covered Elsewhere
3.5.1.6	Ensure ufw firewall rules exist for all open ports	Not Applicable	Covered Elsewhere
3.5.1.7	Ensure ufw default deny firewall policy	Fail	Covered Elsewhere
3.5.2	Configure nftables		
3.5.2.1	Ensure nftables is installed	Fail	Covered Elsewhere
3.5.2.2	Ensure ufw is uninstalled or disabled with nftables	Fail	Covered Elsewhere
3.5.2.3	Ensure iptables are flushed with nftables	Not Applicable	Covered Elsewhere
3.5.2.4	Ensure a nftables table exists	Fail	Covered Elsewhere
3.5.2.5	Ensure nftables base chains exist	Fail	Covered Elsewhere
3.5.2.6	Ensure nftables loopback traffic is configured	Fail	Covered Elsewhere
3.5.2.7	Ensure nftables outbound and established connections are configured	Not Applicable	Covered Elsewhere
3.5.2.8	Ensure nftables default deny firewall policy	Fail	Covered Elsewhere
3.5.2.9	Ensure nftables service is enabled	Fail	Covered Elsewhere
3.5.2.10	Ensure nftables rules are permanent	Fail	Covered Elsewhere
3.5.3	Configure iptables		

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
3.5.3.1	Configure iptables software		
3.5.3.1.1	Ensure iptables packages are installed	Fail	Covered Elsewhere
3.5.3.1.2	Ensure nftables is not installed with iptables	Pass	
3.5.3.1.3	Ensure ufw is uninstalled or disabled with iptables	Fail	Covered Elsewhere
3.5.3.2	Configure IPv4 iptables		
3.5.3.2.1	Ensure iptables default deny firewall policy	Fail	Covered Elsewhere
3.5.3.2.2	Ensure iptables loopback traffic is configured	Fail	Not Applicable
3.5.3.2.3	Ensure iptables outbound and established connections are configured	Not Applicable	
3.5.3.2.4	Ensure iptables firewall rules exist for all open ports	Fail	Potential Operation Impact
3.5.3.3	Configure IPv6 ip6tables		
3.5.3.3.1	Ensure ip6tables default deny firewall policy	Fail	Covered Elsewhere
3.5.3.3.2	Ensure ip6tables loopback traffic is configured	Fail	Covered Elsewhere
3.5.3.3.3	Ensure ip6tables outbound and established connections are configured	Not Applicable	Covered Elsewhere
3.5.3.3.4	Ensure ip6tables firewall rules exist for all open ports	Fail	Covered Elsewhere
4	Logging and Auditing		
4.1	Configure System Accounting (auditd)		
4.1.1.2	Ensure auditing is enabled		
4.1.2	Configure Data Retention		
4.2	Configure Logging		

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
4.2.1	Configure rsyslog		
4.2.1.1	Ensure rsyslog is installed	Pass	
4.2.1.2	Ensure rsyslog Service is enabled	Pass	
4.2.1.3	Ensure logging is configured	Pass	
4.2.1.4	Ensure rsyslog default file permissions configured	Pass	
4.2.1.5	Ensure rsyslog is configured to send logs to a remote log host	Fail	Covered Elsewhere
4.2.1.6	Ensure remote rsyslog messages are only accepted on designated log hosts.	Not Applicable	
4.2.2	Configure journald		
4.2.2.1	Ensure journald is configured to send logs to rsyslog	Pass	
4.2.2.2	Ensure journald is configured to compress large log files	Fail	
4.2.2.3	Ensure journald is configured to write logfiles to persistent disk	Pass	
4.2.3	Ensure permissions on all logfiles are configured	Fail	
4.3	Ensure logrotate is configured	Pass	
4.4	Ensure logrotate assigns appropriate permissions	Fail	
5	Access, Authentication, and Authorization		
5.1	Configure time-based job schedulers		
5.1.1	Ensure cron daemon is enabled and running	Pass	

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
5.1.2	Ensure permissions on /etc/crontab are configured	Pass	
5.1.3	Ensure permissions on /etc/cron.hourly are configured	Pass	
5.1.4	Ensure permissions on /etc/cron.daily are configured	Pass	
5.1.5	Ensure permissions on /etc/cron.weekly are configured	Pass	
5.1.6	Ensure permissions on /etc/cron.monthly are configured	Pass	
5.1.7	Ensure permissions on /etc/cron.d are configured	Pass	
5.1.8	Ensure cron is restricted to authorized users	Fail	
5.1.9	Ensure at is restricted to authorized users	Fail	
5.2	Configure sudo		
5.2.1	Ensure sudo is installed	Pass	
5.2.2	Ensure sudo commands use pty	Fail	Potential Operational Impact
5.2.3	Ensure sudo log file exists	Fail	
5.3	Configure SSH Server		
5.3.1	Ensure permissions on /etc/ssh/sshd_config are configured	Pass	
5.3.2	Ensure permissions on SSH private host key files are configured	Pass	
5.3.3	Ensure permissions on SSH public host key files are configured	Pass	
5.3.4	Ensure SSH access is limited	Pass	

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
5.3.5	Ensure SSH LogLevel is appropriate	Pass	
5.3.7	Ensure SSH MaxAuthTries is set to 4 or less	Pass	
5.3.8	Ensure SSH IgnoreRhosts is enabled	Pass	
5.3.9	Ensure SSH HostbasedAuthentication is disabled	Pass	
5.3.10	Ensure SSH root login is disabled	Pass	
5.3.11	Ensure SSH PermitEmptyPasswords is disabled	Pass	
5.3.12	Ensure SSH PermitUserEnvironment is disabled	Pass	
5.3.13	Ensure only strong Ciphers are used	Pass	
5.3.14	Ensure only strong MAC algorithms are used	Pass	
5.3.15	Ensure only strong Key Exchange algorithms are used	Pass	
5.3.16	Ensure SSH Idle Timeout Interval is configured	Fail	
5.3.17	Ensure SSH LoginGraceTime is set to one minute or less	Pass	
5.3.18	Ensure SSH warning banner is configured	Pass	
5.3.19	Ensure SSH PAM is enabled	Pass	
5.3.21	Ensure SSH MaxStartups is configured	Fail	
5.3.22	Ensure SSH MaxSessions is limited	Pass	
5.4	Configure PAM		

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
5.4.1	Ensure password creation requirements are configured	Pass	
5.4.2	Ensure lockout for failed password attempts is configured	Fail	
5.4.3	Ensure password reuse is limited	Fail	
5.4.4	Ensure password hashing algorithm is SHA-512	Pass	
5.5	User Accounts and Environment		
5.5.1	Set Shadow Password Suite Parameters		
5.5.1.1	Ensure minimum days between password changes is configured	Pass	
5.5.1.2	Ensure password expiration is 365 days or less	Pass	
5.5.1.3	Ensure password expiration warning days is 7 or more	Pass	
5.5.1.4	Ensure inactive password lock is 30 days or less	Pass	
5.5.1.5	Ensure all users last password change date is in the past	Fail	
5.5.2	Ensure system accounts are secured	Pass	
5.5.3	Ensure default group for the root account is GID 0	Pass	
5.5.4	Ensure default user umask is 027 or more restrictive	Pass	
5.5.5	Ensure default user shell timeout is 900 seconds or less	Fail	
5.6	Ensure root login is restricted to system console	Not Applicable	

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
5.7	Ensure access to the su command is restricted	Fail	Potential Operation Impact
6	System Maintenance		
6.1	System File Permissions		
6.1.2	Ensure permissions on /etc/passwd are configured	Pass	
6.1.3	Ensure permissions on /etc/passwd- are configured	Pass	
6.1.4	Ensure permissions on /etc/group are configured	Pass	
6.1.5	Ensure permissions on /etc/group- are configured	Pass	
6.1.6	Ensure permissions on /etc/shadow are configured	Pass	
6.1.7	Ensure permissions on /etc/shadow- are configured	Pass	
6.1.8	Ensure permissions on /etc/gshadow are configured	Pass	
6.1.9	Ensure permissions on /etc/gshadow- are configured	Pass	
6.1.10	Ensure no world writable files exist	Fail	Potential Operation Impact
6.1.11	Ensure no unowned files or directories exist	Fail	Potential Operation Impact
6.1.12	Ensure no ungrouped files or directories exist	Fail	Potential Operation Impact
6.1.13	Audit SUID executables	Not Applicable	
6.1.14	Audit SGID executables	Not Applicable	
6.2	User and Group Settings		
6.2.1	Ensure accounts in /etc/passwd use shadowed passwords	Pass	

CIS PARAGRAPH NUMBER	RECOMMENDATION DESCRIPTION	STATUS	REASON
6.2.2	Ensure password fields are not empty	Pass	
6.2.3	Ensure all groups in /etc/passwd exist in /etc/group	Pass	
6.2.4	Ensure all users' home directories exist	Pass	
6.2.5	Ensure users own their home directories	Pass	
6.2.6	Ensure users' home directories permissions are 750 or more restrictive	Pass	
6.2.7	Ensure users' dot files are not group or world writable	Pass	
6.2.8	Ensure no users have .netrc files	Pass	
6.2.9	Ensure no users have .forward files	Pass	
6.2.10	Ensure no users have .rhosts files	Pass	
6.2.11	Ensure root is the only UID 0 account	Pass	
6.2.12	Ensure root PATH Integrity	Pass	
6.2.13	Ensure no duplicate UIDs exist	Pass	
6.2.14	Ensure no duplicate GIDs exist	Pass	
6.2.15	Ensure no duplicate user names exist	Pass	
6.2.16	Ensure no duplicate group names exist	Pass	
6.2.17	Ensure shadow group is empty	Pass	

Next steps

For more information about AKS security, see the following articles:

- Azure Kubernetes Service (AKS)
- AKS security considerations
- AKS best practices

Access and identity options for Azure Kubernetes Service (AKS)

10/27/2022 • 15 minutes to read • [Edit Online](#)

You can authenticate, authorize, secure, and control access to Kubernetes clusters in a variety of ways:

- Using Kubernetes role-based access control (Kubernetes RBAC), you can grant users, groups, and service accounts access to only the resources they need.
- With Azure Kubernetes Service (AKS), you can further enhance the security and permissions structure using Azure Active Directory and Azure RBAC.

Kubernetes RBAC and AKS help you secure your cluster access and provide only the minimum required permissions to developers and operators.

This article introduces the core concepts that help you authenticate and assign permissions in AKS.

Kubernetes RBAC

Kubernetes RBAC provides granular filtering of user actions. With this control mechanism:

- You assign users or user groups permission to create and modify resources or view logs from running application workloads.
- You can scope permissions to a single namespace or across the entire AKS cluster.
- You create *roles* to define permissions, and then assign those roles to users with *role bindings*.

For more information, see [Using Kubernetes RBAC authorization](#).

Roles and ClusterRoles

Roles

Before assigning permissions to users with Kubernetes RBAC, you'll define user permissions as a *Role*. Grant permissions within a namespace using roles.

NOTE

Kubernetes roles *grant* permissions; they don't *deny* permissions.

To grant permissions across the entire cluster or to cluster resources outside a given namespace, you can instead use *ClusterRoles*.

ClusterRoles

A ClusterRole grants and applies permissions to resources across the entire cluster, not a specific namespace.

RoleBindings and ClusterRoleBindings

Once you've defined roles to grant permissions to resources, you assign those Kubernetes RBAC permissions with a *RoleBinding*. If your AKS cluster [integrates with Azure Active Directory \(Azure AD\)](#), RoleBindings grant permissions to Azure AD users to perform actions within the cluster. See how in [Control access to cluster resources using Kubernetes role-based access control and Azure Active Directory identities](#).

RoleBindings

Assign roles to users for a given namespace using RoleBindings. With RoleBindings, you can logically segregate a single AKS cluster, only enabling users to access the application resources in their assigned namespace.

To bind roles across the entire cluster, or to cluster resources outside a given namespace, you instead use [ClusterRoleBindings](#).

ClusterRoleBinding

With a ClusterRoleBinding, you bind roles to users and apply to resources across the entire cluster, not a specific namespace. This approach lets you grant administrators or support engineers access to all resources in the AKS cluster.

NOTE

Microsoft/AKS performs any cluster actions with user consent under a built-in Kubernetes role `aks-service` and built-in role binding `aks-service-rolebinding`.

This role enables AKS to troubleshoot and diagnose cluster issues, but can't modify permissions nor create roles or role bindings, or other high privilege actions. Role access is only enabled under active support tickets with just-in-time (JIT) access. Read more about [AKS support policies](#).

Kubernetes service accounts

Service accounts are one of the primary user types in Kubernetes. The Kubernetes API holds and manages service accounts. Service account credentials are stored as Kubernetes secrets, allowing them to be used by authorized pods to communicate with the API Server. Most API requests provide an authentication token for a service account or a normal user account.

Normal user accounts allow more traditional access for human administrators or developers, not just services and processes. While Kubernetes doesn't provide an identity management solution to store regular user accounts and passwords, you can integrate external identity solutions into Kubernetes. For AKS clusters, this integrated identity solution is Azure AD.

For more information on the identity options in Kubernetes, see [Kubernetes authentication](#).

Azure role-based access control

Azure role-based access control (RBAC) is an authorization system built on [Azure Resource Manager](#) that provides fine-grained access management of Azure resources.

RBAC SYSTEM	DESCRIPTION
Kubernetes RBAC	Designed to work on Kubernetes resources within your AKS cluster.
Azure RBAC	Designed to work on resources within your Azure subscription.

With Azure RBAC, you create a *role definition* that outlines the permissions to be applied. You then assign a user or group this role definition via a *role assignment* for a particular *scope*. The scope can be an individual resource, a resource group, or across the subscription.

For more information, see [What is Azure role-based access control \(Azure RBAC\)?](#)

There are two levels of access needed to fully operate an AKS cluster:

- [Access the AKS resource in your Azure subscription](#).
 - Control scaling or upgrading your cluster using the AKS APIs.
 - Pull your `kubeconfig`.
- Access to the Kubernetes API. This access is controlled by either:
 - [Kubernetes RBAC](#) (traditionally).

- Integrating Azure RBAC with AKS for Kubernetes authorization.

Azure RBAC to authorize access to the AKS resource

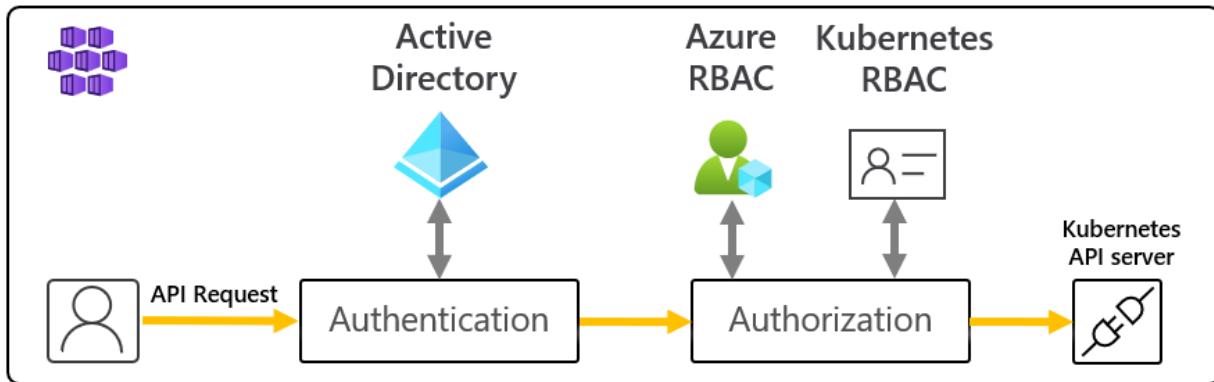
With Azure RBAC, you can provide your users (or identities) with granular access to AKS resources across one or more subscriptions. For example, you could use the [Azure Kubernetes Service Contributor role](#) to scale and upgrade your cluster. Meanwhile, another user with the [Azure Kubernetes Service Cluster Admin role](#) only has permission to pull the Admin `kubeconfig`.

Alternatively, you could give your user the general [Contributor](#) role. With the general Contributor role, users can perform the above permissions and every action possible on the AKS resource, except managing permissions.

[Use Azure RBAC to define access to the Kubernetes configuration file in AKS.](#)

Azure RBAC for Kubernetes Authorization

With the Azure RBAC integration, AKS will use a Kubernetes Authorization webhook server so you can manage Azure AD-integrated Kubernetes cluster resource permissions and assignments using Azure role definition and role assignments.



As shown in the above diagram, when using the Azure RBAC integration, all requests to the Kubernetes API will follow the same authentication flow as explained on the [Azure Active Directory integration section](#).

If the identity making the request exists in Azure AD, Azure will team with Kubernetes RBAC to authorize the request. If the identity exists outside of Azure AD (i.e., a Kubernetes service account), authorization will defer to the normal Kubernetes RBAC.

In this scenario, you use Azure RBAC mechanisms and APIs to assign users built-in roles or create custom roles, just as you would with Kubernetes roles.

With this feature, you not only give users permissions to the AKS resource across subscriptions, but you also configure the role and permissions for inside each of those clusters controlling Kubernetes API access. For example, you can grant the [Azure Kubernetes Service RBAC Reader](#) role on the subscription scope. The role recipient will be able to list and get all Kubernetes objects from all clusters without modifying them.

IMPORTANT

You need to enable Azure RBAC for Kubernetes authorization before using this feature. For more details and step by step guidance, follow our [Use Azure RBAC for Kubernetes Authorization](#) how-to guide.

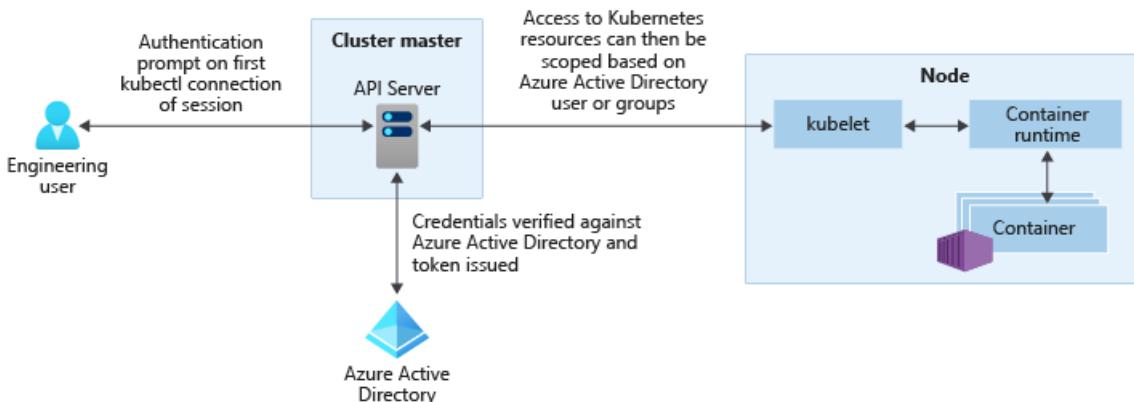
Built-in roles

AKS provides the following four built-in roles. They are similar to the [Kubernetes built-in roles](#) with a few differences, like supporting CRDs. See the full list of actions allowed by each [Azure built-in role](#).

ROLE	DESCRIPTION
Azure Kubernetes Service RBAC Reader	Allows read-only access to see most objects in a namespace. Doesn't allow viewing roles or role bindings. Doesn't allow viewing <code>Secrets</code> . Reading the <code>Secrets</code> contents enables access to <code>ServiceAccount</code> credentials in the namespace, which would allow API access as any <code>ServiceAccount</code> in the namespace (a form of privilege escalation).
Azure Kubernetes Service RBAC Writer	Allows read/write access to most objects in a namespace. Doesn't allow viewing or modifying roles, or role bindings. Allows accessing <code>Secrets</code> and running pods as any <code>ServiceAccount</code> in the namespace, so it can be used to gain the API access levels of any <code>ServiceAccount</code> in the namespace.
Azure Kubernetes Service RBAC Admin	Allows admin access, intended to be granted within a namespace. Allows read/write access to most resources in a namespace (or cluster scope), including the ability to create roles and role bindings within the namespace. Doesn't allow write access to resource quota or to the namespace itself.
Azure Kubernetes Service RBAC Cluster Admin	Allows super-user access to perform any action on any resource. Gives full control over every resource in the cluster and in all namespaces.

Azure AD integration

Enhance your AKS cluster security with Azure AD integration. Built on decades of enterprise identity management, Azure AD is a multi-tenant, cloud-based directory and identity management service that combines core directory services, application access management, and identity protection. With Azure AD, you can integrate on-premises identities into AKS clusters to provide a single source for account management and security.



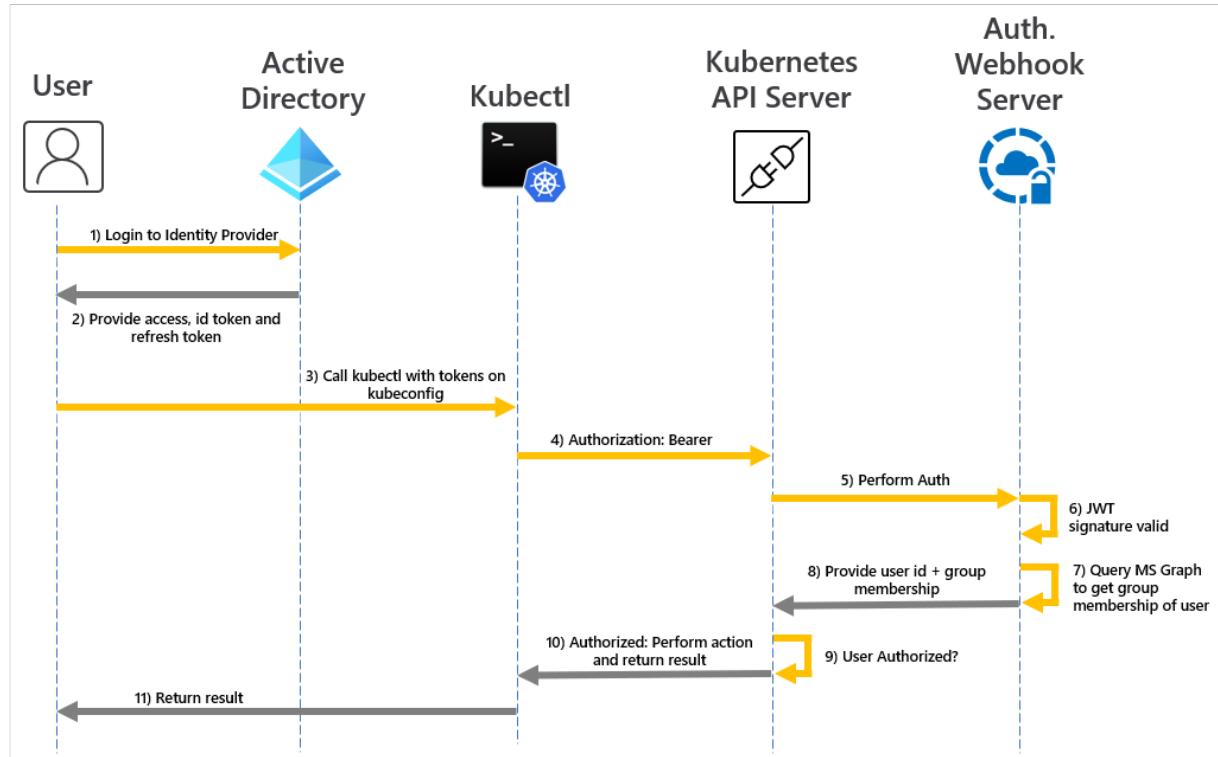
With Azure AD-integrated AKS clusters, you can grant users or groups access to Kubernetes resources within a namespace or across the cluster.

1. To obtain a `kubectl` configuration context, a user runs the `az aks get-credentials` command.
2. When a user interacts with the AKS cluster with `kubectl`, they're prompted to sign in with their Azure AD credentials.

This approach provides a single source for user account management and password credentials. The user can only access the resources as defined by the cluster administrator.

Azure AD authentication is provided to AKS clusters with OpenID Connect. OpenID Connect is an identity layer built on top of the OAuth 2.0 protocol. For more information on OpenID Connect, see the [Open ID connect documentation](#). From inside of the Kubernetes cluster, [Webhook Token Authentication](#) is used to verify authentication tokens. Webhook token authentication is configured and managed as part of the AKS cluster.

Webhook and API server



As shown in the graphic above, the API server calls the AKS webhook server and performs the following steps:

1. `kubectl` uses the Azure AD client application to sign in users with [OAuth 2.0 device authorization grant flow](#).
2. Azure AD provides an `access_token`, `id_token`, and a `refresh_token`.
3. The user makes a request to `kubectl` with an `access_token` from `kubeconfig`.
4. `kubectl` sends the `access_token` to API Server.
5. The API Server is configured with the Auth WebHook Server to perform validation.
6. The authentication webhook server confirms the JSON Web Token signature is valid by checking the Azure AD public signing key.
7. The server application uses user-provided credentials to query group memberships of the logged-in user from the MS Graph API.
8. A response is sent to the API Server with user information such as the user principal name (UPN) claim of the access token, and the group membership of the user based on the object ID.
9. The API performs an authorization decision based on the Kubernetes Role/RoleBinding.
10. Once authorized, the API server returns a response to `kubectl`.
11. `kubectl` provides feedback to the user.

Learn how to integrate AKS with Azure AD with our [AKS-managed Azure AD integration how-to guide](#).

AKS service permissions

When creating a cluster, AKS generates or modifies resources it needs (like VMs and NICs) to create and run the cluster on behalf of the user. This identity is distinct from the cluster's identity permission, which is created

during cluster creation.

Identity creating and operating the cluster permissions

The following permissions are needed by the identity creating and operating the cluster.

PERMISSION	REASON
Microsoft.Compute/diskEncryptionSets/read	Required to read disk encryption set ID.
Microsoft.Compute/proximityPlacementGroups/write	Required for updating proximity placement groups.
Microsoft.Network/applicationGateways/read Microsoft.Network/applicationGateways/write Microsoft.Network/virtualNetworks/subnets/join/action	Required to configure application gateways and join the subnet.
Microsoft.Network/virtualNetworks/subnets/join/action	Required to configure the Network Security Group for the subnet when using a custom VNET.
Microsoft.Network/publicIPAddresses/join/action Microsoft.Network/publicIPPrefixes/join/action	Required to configure the outbound public IPs on the Standard Load Balancer.
Microsoft.OperationalInsights/workspaces/sharedkeys/read Microsoft.OperationalInsights/workspaces/read Microsoft.OperationsManagement/solutions/write Microsoft.OperationsManagement/solutions/read Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	Required to create and update Log Analytics workspaces and Azure monitoring for containers.
Microsoft.Network/virtualNetworks/joinLoadBalancer/action	Required to configure the IP-based Load Balancer Backend Pools.

AKS cluster identity permissions

The following permissions are used by the AKS cluster identity, which is created and associated with the AKS cluster. Each permission is used for the reasons below:

PERMISSION	REASON
Microsoft.ContainerService/managedClusters/*	Required for creating users and operating the cluster
Microsoft.Network/loadBalancers/delete Microsoft.Network/loadBalancers/read Microsoft.Network/loadBalancers/write	Required to configure the load balancer for a LoadBalancer service.
Microsoft.Network/publicIPAddresses/delete Microsoft.Network/publicIPAddresses/read Microsoft.Network/publicIPAddresses/write	Required to find and configure public IPs for a LoadBalancer service.
Microsoft.Network/publicIPAddresses/join/action	Required for configuring public IPs for a LoadBalancer service.
Microsoft.Network/networkSecurityGroups/read Microsoft.Network/networkSecurityGroups/write	Required to create or delete security rules for a LoadBalancer service.

PERMISSION	REASON
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/disks/delete</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/disks/read</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/disks/write</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/locations/DiskOperations/read</div>	Required to configure AzureDisks.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Storage/storageAccounts/delete</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Storage/storageAccounts/listKeys/action</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Storage/storageAccounts/read</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Storage/storageAccounts/write</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Storage/operations/read</div>	Required to configure storage accounts for AzureFile or AzureDisk.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Network/routeTables/read</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Network/routeTables/routes/delete</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Network/routeTables/routes/read</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Network/routeTables/routes/write</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Network/routeTables/write</div>	Required to configure route tables and routes for nodes.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachines/read</div>	Required to find information for virtual machines in a VMAS, such as zones, fault domain, size, and data disks.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachines/write</div>	Required to attach AzureDisks to a virtual machine in a VMAS.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachineScaleSets/read</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachineScaleSets/virtualMachines/write</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachineScaleSets/virtualmachines/instanceView/read</div>	Required to find information for virtual machines in a virtual machine scale set, such as zones, fault domain, size, and data disks.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Network/networkInterfaces/write</div>	Required to add a virtual machine in a VMAS to a load balancer backend address pool.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachineScaleSets/write</div>	Required to add a virtual machine scale set to a load balancer backend address pools and scale out nodes in a virtual machine scale set.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachineScaleSets/delete</div>	Required to delete a virtual machine scale set to a load balancer backend address pools and scale down nodes in a virtual machine scale set.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachineScaleSets/virtualmachines/write</div>	Required to attach AzureDisks and add a virtual machine from a virtual machine scale set to the load balancer.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Network/networkInterfaces/read</div>	Required to search internal IPs and load balancer backend address pools for virtual machines in a VMAS.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read</div>	Required to search internal IPs and load balancer backend address pools for a virtual machine in a virtual machine scale set.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Compute/virtualMachineScaleSets/virtualMachines/publicIPAddresses/read</div>	Required to find public IP for a virtual machine in a virtual machine scale set.
<div style="border: 1px solid black; padding: 2px;">Microsoft.Network/virtualNetworks/read</div> <div style="border: 1px solid black; padding: 2px;">Microsoft.Network/virtualNetworks/subnets/read</div>	Required to verify if a subnet exists for the internal load balancer in another resource group.

PERMISSION	REASON
Microsoft.Compute/snapshots/delete Microsoft.Compute/snapshots/read Microsoft.Compute/snapshots/write	Required to configure snapshots for AzureDisk.
Microsoft.Compute/locations/vmSizes/read Microsoft.Compute/locations/operations/read	Required to find virtual machine sizes for finding AzureDisk volume limits.

Additional cluster identity permissions

When creating a cluster with specific attributes, you will need the following additional permissions for the cluster identity. Since these permissions are not automatically assigned, you must add them to the cluster identity after it's created.

PERMISSION	REASON
Microsoft.Network/networkSecurityGroups/write Microsoft.Network/networkSecurityGroups/read	Required if using a network security group in another resource group. Required to configure security rules for a LoadBalancer service.
Microsoft.Network/virtualNetworks/subnets/read Microsoft.Network/virtualNetworks/subnets/join/action	Required if using a subnet in another resource group such as a custom VNET.
Microsoft.Network/routeTables/routes/read Microsoft.Network/routeTables/routes/write	Required if using a subnet associated with a route table in another resource group such as a custom VNET with a custom route table. Required to verify if a subnet already exists for the subnet in the other resource group.
Microsoft.Network/virtualNetworks/subnets/read	Required if using an internal load balancer in another resource group. Required to verify if a subnet already exists for the internal load balancer in the resource group.
Microsoft.Network/privateDnszones/*	Required if using a private DNS zone in another resource group such as a custom privateDNSZone.

AKS Node Access

By default Node Access is not required for AKS. The following access is needed for the node if a specific component is leveraged.

ACCESS	REASON
kubelet	Required to grant MSI access to ACR.
http app routing	Required for write permission to "random name".aksapp.io.
container insights	Required to grant permission to the Log Analytics workspace.

Summary

View the table for a quick summary of how users can authenticate to Kubernetes when Azure AD integration is enabled. In all cases, the user's sequence of commands is:

1. Run `az login` to authenticate to Azure.
2. Run `az aks get-credentials` to download credentials for the cluster into `.kube/config`.
3. Run `kubectl` commands.

- The first command may trigger browser-based authentication to authenticate to the cluster, as described in the following table.

In the Azure portal, you can find:

- The *Role Grant* (Azure RBAC role grant) referred to in the second column is shown on the **Access Control** tab.
- The Cluster Admin Azure AD Group is shown on the **Configuration** tab.
 - Also found with parameter name `--aad-admin-group-object-ids` in the Azure CLI.

DESCRIPTION	ROLE GRANT REQUIRED	CLUSTER ADMIN AZURE AD GROUP(S)	WHEN TO USE
Legacy admin login using client certificate	Azure Kubernetes Admin Role. This role allows <code>az aks get-credentials</code> to be used with the <code>--admin</code> flag, which downloads a legacy (non-Azure AD) cluster admin certificate into the user's <code>.kube/config</code> . This is the only purpose of "Azure Kubernetes Admin Role".	n/a	If you're permanently blocked by not having access to a valid Azure AD group with access to your cluster.
Azure AD with manual (Cluster)RoleBindings	Azure Kubernetes User Role. The "User" role allows <code>az aks get-credentials</code> to be used without the <code>--admin</code> flag. (This is the only purpose of "Azure Kubernetes User Role".) The result, on an Azure AD-enabled cluster, is the download of an empty entry into <code>.kube/config</code> , which triggers browser-based authentication when it's first used by <code>kubectl</code> .	User is not in any of these groups. Because the user is not in any Cluster Admin groups, their rights will be controlled entirely by any RoleBindings or ClusterRoleBindings that have been set up by cluster admins. The (Cluster)RoleBindings nominate Azure AD users or Azure AD groups as their <code>subjects</code> . If no such bindings have been set up, the user will not be able to execute any <code>kubectl</code> commands.	If you want fine-grained access control, and you're not using Azure RBAC for Kubernetes Authorization. Note that the user who sets up the bindings must log in by one of the other methods listed in this table.

DESCRIPTION	ROLE GRANT REQUIRED	CLUSTER ADMIN AZURE AD GROUP(S)	WHEN TO USE
Azure AD by member of admin group	Same as above	User is a member of one of the groups listed here. AKS automatically generates a ClusterRoleBinding that binds all of the listed groups to the <code>cluster-admin</code> Kubernetes role. So users in these groups can run all <code>kubectl</code> commands as <code>cluster-admin</code> .	If you want to conveniently grant users full admin rights, and are <i>not</i> using Azure RBAC for Kubernetes authorization.
Azure AD with Azure RBAC for Kubernetes Authorization	Two roles: First, Azure Kubernetes User Role (as above). Second, one of the "Azure Kubernetes Service RBAC..." roles listed above, or your own custom alternative.	The admin roles field on the Configuration tab is irrelevant when Azure RBAC for Kubernetes Authorization is enabled.	You are using Azure RBAC for Kubernetes authorization. This approach gives you fine-grained control, without the need to set up RoleBindings or ClusterRoleBindings.

Next steps

- To get started with Azure AD and Kubernetes RBAC, see [Integrate Azure Active Directory with AKS](#).
- For associated best practices, see [Best practices for authentication and authorization in AKS](#).
- To get started with Azure RBAC for Kubernetes Authorization, see [Use Azure RBAC to authorize access within the Azure Kubernetes Service \(AKS\) Cluster](#).
- To get started securing your `kubeconfig` file, see [Limit access to cluster configuration file](#)

For more information on core Kubernetes and AKS concepts, see the following articles:

- [Kubernetes / AKS clusters and workloads](#)
- [Kubernetes / AKS security](#)
- [Kubernetes / AKS virtual networks](#)
- [Kubernetes / AKS storage](#)
- [Kubernetes / AKS scale](#)

Network concepts for applications in Azure Kubernetes Service (AKS)

10/27/2022 • 9 minutes to read • [Edit Online](#)

In a container-based, microservices approach to application development, application components work together to process their tasks. Kubernetes provides various resources enabling this cooperation:

- You can connect to and expose applications internally or externally.
- You can build highly available applications by load balancing your applications.
- For your more complex applications, you can configure ingress traffic for SSL/TLS termination or routing of multiple components.
- For security reasons, you can restrict the flow of network traffic into or between pods and nodes.

This article introduces the core concepts that provide networking to your applications in AKS:

- [Services](#)
- [Azure virtual networks](#)
- [Ingress controllers](#)
- [Network policies](#)

Kubernetes basics

To allow access to your applications or between application components, Kubernetes provides an abstraction layer to virtual networking. Kubernetes nodes connect to a virtual network, providing inbound and outbound connectivity for pods. The *kube-proxy* component runs on each node to provide these network features.

In Kubernetes:

- *Services* logically group pods to allow for direct access on a specific port via an IP address or DNS name.
- You can distribute traffic using a *load balancer*.
- More complex routing of application traffic can also be achieved with *Ingress Controllers*.
- Security and filtering of the network traffic for pods is possible with Kubernetes *network policies*.

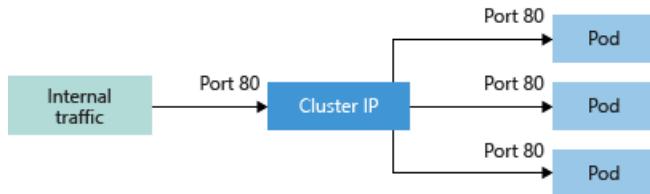
The Azure platform also simplifies virtual networking for AKS clusters. When you create a Kubernetes load balancer, you also create and configure the underlying Azure load balancer resource. As you open network ports to pods, the corresponding Azure network security group rules are configured. For HTTP application routing, Azure can also configure *external DNS* as new ingress routes are configured.

Services

To simplify the network configuration for application workloads, Kubernetes uses *Services* to logically group a set of pods together and provide network connectivity. The following Service types are available:

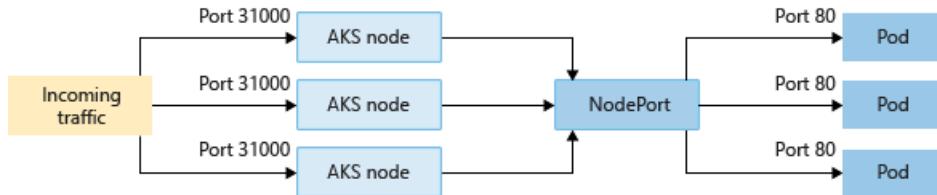
- **Cluster IP**

Creates an internal IP address for use within the AKS cluster. Good for internal-only applications that support other workloads within the cluster.



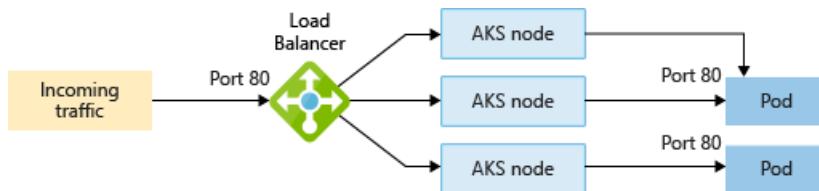
- **NodePort**

Creates a port mapping on the underlying node that allows the application to be accessed directly with the node IP address and port.



- **LoadBalancer**

Creates an Azure load balancer resource, configures an external IP address, and connects the requested pods to the load balancer backend pool. To allow customers' traffic to reach the application, load balancing rules are created on the desired ports.



For extra control and routing of the inbound traffic, you may instead use an [Ingress controller](#).

- **ExternalName**

Creates a specific DNS entry for easier application access.

Either the load balancers and services IP address can be dynamically assigned, or you can specify an existing static IP address. You can assign both internal and external static IP addresses. Existing static IP addresses are often tied to a DNS entry.

You can create both *internal* and *external* load balancers. Internal load balancers are only assigned a private IP address, so they can't be accessed from the Internet.

Azure virtual networks

In AKS, you can deploy a cluster that uses one of the following two network models:

- *Kubenet* networking

The network resources are typically created and configured as the AKS cluster is deployed.

- *Azure Container Networking Interface (CNI)* networking

The AKS cluster is connected to existing virtual network resources and configurations.

Kubenet (basic) networking

The *kubenet* networking option is the default configuration for AKS cluster creation. With *kubenet*

1. Nodes receive an IP address from the Azure virtual network subnet.
2. Pods receive an IP address from a logically different address space than the nodes' Azure virtual network

subnet.

3. Network address translation (NAT) is then configured so that the pods can reach resources on the Azure virtual network.
4. The source IP address of the traffic is translated to the node's primary IP address.

Nodes use the [kubenet](#) Kubernetes plugin. You can:

- Let the Azure platform create and configure the virtual networks for you, or
- Choose to deploy your AKS cluster into an existing virtual network subnet.

Remember, only the nodes receive a routable IP address. The pods use NAT to communicate with other resources outside the AKS cluster. This approach reduces the number of IP addresses you need to reserve in your network space for pods to use.

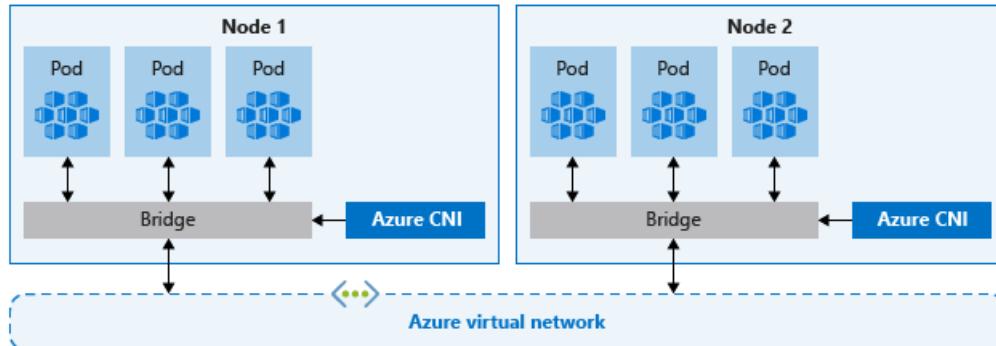
For more information, see [Configure kubenet networking for an AKS cluster](#).

Azure CNI (advanced) networking

With Azure CNI, every pod gets an IP address from the subnet and can be accessed directly. These IP addresses must be planned in advance and unique across your network space. Each node has a configuration parameter for the maximum number of pods it supports. The equivalent number of IP addresses per node are then reserved up front. Without planning, this approach can lead to IP address exhaustion or the need to rebuild clusters in a larger subnet as your application demands grow.

Unlike kubenet, traffic to endpoints in the same virtual network isn't NAT'd to the node's primary IP. The source address for traffic inside the virtual network is the pod IP. Traffic that's external to the virtual network still NATs to the node's primary IP.

Nodes use the [Azure CNI](#) Kubernetes plugin.



For more information, see [Configure Azure CNI for an AKS cluster](#).

Compare network models

Both kubenet and Azure CNI provide network connectivity for your AKS clusters. However, there are advantages and disadvantages to each. At a high level, the following considerations apply:

- **kubenet**
 - Conserves IP address space.
 - Uses Kubernetes internal or external load balancer to reach pods from outside of the cluster.
 - You manually manage and maintain user-defined routes (UDRs).
 - Maximum of 400 nodes per cluster.
- **Azure CNI**
 - Pods get full virtual network connectivity and can be directly reached via their private IP address from connected networks.
 - Requires more IP address space.

The following behavior differences exist between kubenet and Azure CNI:

Capability	Kubenet	Azure CNI
Deploy cluster in existing or new virtual network	Supported - UDRs manually applied	Supported
Pod-pod connectivity	Supported	Supported
Pod-VM connectivity; VM in the same virtual network	Works when initiated by pod	Works both ways
Pod-VM connectivity; VM in peered virtual network	Works when initiated by pod	Works both ways
On-premises access using VPN or Express Route	Works when initiated by pod	Works both ways
Access to resources secured by service endpoints	Supported	Supported
Expose Kubernetes services using a load balancer service, App Gateway, or ingress controller	Supported	Supported
Default Azure DNS and Private Zones	Supported	Supported
Support for Windows node pools	Not Supported	Supported

Regarding DNS, with both kubenet and Azure CNI plugins DNS are offered by CoreDNS, a deployment running in AKS with its own autoscaler. For more information on CoreDNS on Kubernetes, see [Customizing DNS Service](#). CoreDNS by default is configured to forward unknown domains to the DNS functionality of the Azure Virtual Network where the AKS cluster is deployed. Hence, Azure DNS and Private Zones will work for pods running in AKS.

Support scope between network models

Whatever network model you use, both kubenet and Azure CNI can be deployed in one of the following ways:

- The Azure platform can automatically create and configure the virtual network resources when you create an AKS cluster.
- You can manually create and configure the virtual network resources and attach to those resources when you create your AKS cluster.

Although capabilities like service endpoints or UDRs are supported with both kubenet and Azure CNI, the [support policies for AKS](#) define what changes you can make. For example:

- If you manually create the virtual network resources for an AKS cluster, you're supported when configuring your own UDRs or service endpoints.
- If the Azure platform automatically creates the virtual network resources for your AKS cluster, you can't manually change those AKS-managed resources to configure your own UDRs or service endpoints.

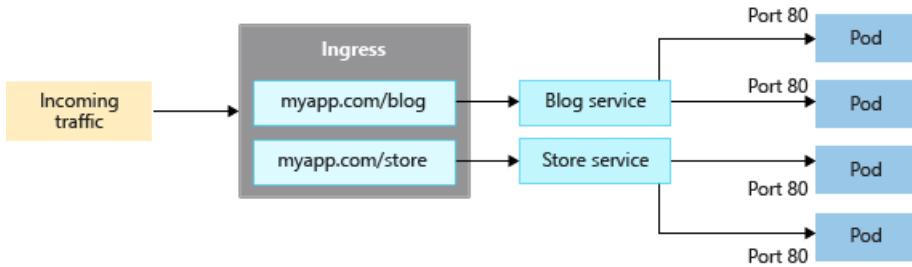
Ingress controllers

When you create a LoadBalancer-type Service, you also create an underlying Azure load balancer resource. The load balancer is configured to distribute traffic to the pods in your Service on a given port.

The LoadBalancer only works at layer 4. At layer 4, the Service is unaware of the actual applications, and can't

make any more routing considerations.

Ingress controllers work at layer 7, and can use more intelligent rules to distribute application traffic. Ingress controllers typically route HTTP traffic to different applications based on the inbound URL.



Create an ingress resource

In AKS, you can create an Ingress resource using NGINX, a similar tool, or the AKS HTTP application routing feature. When you enable HTTP application routing for an AKS cluster, the Azure platform creates the Ingress controller and an *External-DNS* controller. As new Ingress resources are created in Kubernetes, the required DNS A records are created in a cluster-specific DNS zone.

For more information, see [Deploy HTTP application routing](#).

Application Gateway Ingress Controller (AGIC)

With the Application Gateway Ingress Controller (AGIC) add-on, AKS customers leverage Azure's native Application Gateway level 7 load-balancer to expose cloud software to the Internet. AGIC monitors the host Kubernetes cluster and continuously updates an Application Gateway, exposing selected services to the Internet.

To learn more about the AGIC add-on for AKS, see [What is Application Gateway Ingress Controller?](#).

SSL/TLS termination

SSL/TLS termination is another common feature of Ingress. On large web applications accessed via HTTPS, the Ingress resource handles the TLS termination rather than within the application itself. To provide automatic TLS certification generation and configuration, you can configure the Ingress resource to use providers such as "Let's Encrypt".

For more information on configuring an NGINX Ingress controller with Let's Encrypt, see [Ingress and TLS](#).

Client source IP preservation

Configure your ingress controller to preserve the client source IP on requests to containers in your AKS cluster. When your ingress controller routes a client's request to a container in your AKS cluster, the original source IP of that request is unavailable to the target container. When you enable *client source IP preservation*, the source IP for the client is available in the request header under *X-Forwarded-For*.

If you're using client source IP preservation on your ingress controller, you can't use TLS pass-through. Client source IP preservation and TLS pass-through can be used with other services, such as the *LoadBalancer* type.

Network security groups

A network security group filters traffic for VMs like the AKS nodes. As you create Services, such as a LoadBalancer, the Azure platform automatically configures any necessary network security group rules.

You don't need to manually configure network security group rules to filter traffic for pods in an AKS cluster. Simply define any required ports and forwarding as part of your Kubernetes Service manifests. Let the Azure platform create or update the appropriate rules.

You can also use network policies to automatically apply traffic filter rules to pods.

Network policies

By default, all pods in an AKS cluster can send and receive traffic without limitations. For improved security, define rules that control the flow of traffic, like:

- Backend applications are only exposed to required frontend services.
- Database components are only accessible to the application tiers that connect to them.

Network policy is a Kubernetes feature available in AKS that lets you control the traffic flow between pods. You allow or deny traffic to the pod based on settings such as assigned labels, namespace, or traffic port. While network security groups are better for AKS nodes, network policies are a more suited, cloud-native way to control the flow of traffic for pods. As pods are dynamically created in an AKS cluster, required network policies can be automatically applied.

For more information, see [Secure traffic between pods using network policies in Azure Kubernetes Service \(AKS\)](#).

Next steps

To get started with AKS networking, create and configure an AKS cluster with your own IP address ranges using [kubenet](#) or [Azure CNI](#).

For associated best practices, see [Best practices for network connectivity and security in AKS](#).

For more information on core Kubernetes and AKS concepts, see the following articles:

- [Kubernetes / AKS clusters and workloads](#)
- [Kubernetes / AKS access and identity](#)
- [Kubernetes / AKS security](#)
- [Kubernetes / AKS storage](#)
- [Kubernetes / AKS scale](#)

Storage options for applications in Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

Applications running in Azure Kubernetes Service (AKS) may need to store and retrieve data. While some application workloads can use local, fast storage on unneeded, emptied nodes, others require storage that persists on more regular data volumes within the Azure platform.

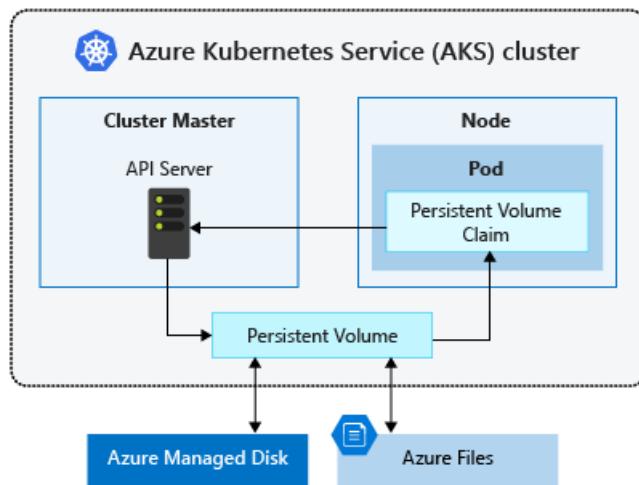
Multiple pods may need to:

- Share the same data volumes.
- Reattach data volumes if the pod is rescheduled on a different node.

Finally, you might need to collect and store sensitive data or application configuration information into pods.

This article introduces the core concepts that provide storage to your applications in AKS:

- [Volumes](#)
- [Persistent volumes](#)
- [Storage classes](#)
- [Persistent volume claims](#)



Volumes

Kubernetes typically treats individual pods as ephemeral, disposable resources. Applications have different approaches available to them for using and persisting data. A *volume* represents a way to store, retrieve, and persist data across pods and through the application lifecycle.

Traditional volumes are created as Kubernetes resources backed by Azure Storage. You can manually create data volumes to be assigned to pods directly, or have Kubernetes automatically create them. Data volumes can use: [Azure Disks](#), [Azure Files](#), [Azure NetApp Files](#), or [Azure Blobs](#).

Azure Disks

Use [Azure Disks](#) to create a Kubernetes *DataDisk* resource. Disks types include:

- Ultra Disks
- Premium SSDs

- Standard SSDs
- Standard HDDs

TIP

For most production and development workloads, use Premium SSD.

Since Azure Disks are mounted as *ReadWriteOnce*, they're only available to a single node. For storage volumes that can be accessed by pods on multiple nodes simultaneously, use Azure Files.

Azure Files

Use *Azure Files* to mount a Server Message Block (SMB) version 3.1.1 share or Network File System (NFS) version 4.1 share backed by an Azure storage accounts to pods. Files let you share data across multiple nodes and pods and can use:

- Azure Premium storage backed by high-performance SSDs
- Azure Standard storage backed by regular HDDs

Azure NetApp Files

- Ultra Storage
- Premium Storage
- Standard Storage

Azure Blob Storage

Use *Azure Blob Storage* to create a blob storage container and mount it using the NFS v3.0 protocol or BlobFuse.

- Block Blobs

Volume types

Kubernetes volumes represent more than just a traditional disk for storing and retrieving information. Kubernetes volumes can also be used as a way to inject data into a pod for use by the containers.

Common volume types in Kubernetes include:

emptyDir

Commonly used as temporary space for a pod. All containers within a pod can access the data on the volume. Data written to this volume type persists only for the lifespan of the pod. Once you delete the pod, the volume is deleted. This volume typically uses the underlying local node disk storage, though it can also exist only in the node's memory.

secret

You can use *secret* volumes to inject sensitive data into pods, such as passwords.

1. Create a Secret using the Kubernetes API.
2. Define your pod or deployment and request a specific Secret.
 - Secrets are only provided to nodes with a scheduled pod that requires them.
 - The Secret is stored in *tmpfs*, not written to disk.
3. When you delete the last pod on a node requiring a Secret, the Secret is deleted from the node's *tmpfs*.
 - Secrets are stored within a given namespace and can only be accessed by pods within the same namespace.

configMap

You can use *configMap* to inject key-value pair properties into pods, such as application configuration information. Define application configuration information as a Kubernetes resource, easily updated and applied

to new instances of pods as they're deployed.

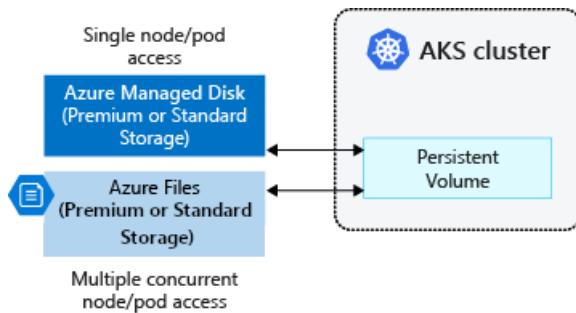
Like using a secret:

1. Create a ConfigMap using the Kubernetes API.
2. Request the ConfigMap when you define a pod or deployment.
 - ConfigMaps are stored within a given namespace and can only be accessed by pods within the same namespace.

Persistent volumes

Volumes defined and created as part of the pod lifecycle only exist until you delete the pod. Pods often expect their storage to remain if a pod is rescheduled on a different host during a maintenance event, especially in StatefulSets. A *persistent volume* (PV) is a storage resource created and managed by the Kubernetes API that can exist beyond the lifetime of an individual pod.

You can use Azure Disks or Files to provide the PersistentVolume. As noted in the [Volumes](#) section, the choice of Disks or Files is often determined by the need for concurrent access to the data or the performance tier.



A PersistentVolume can be *statically* created by a cluster administrator, or *dynamically* created by the Kubernetes API server. If a pod is scheduled and requests currently unavailable storage, Kubernetes can create the underlying Azure Disk or Files storage and attach it to the pod. Dynamic provisioning uses a *StorageClass* to identify what type of Azure storage needs to be created.

Storage classes

To define different tiers of storage, such as Premium and Standard, you can create a *StorageClass*.

The StorageClass also defines the *reclaimPolicy*. When you delete the pod and the persistent volume is no longer required, the reclaimPolicy controls the behavior of the underlying Azure storage resource. The underlying storage resource can either be deleted or kept for use with a future pod.

For clusters using the [Container Storage Interface \(CSI\) drivers](#) the following extra `StorageClasses` are created:

PERMISSION	REASON
<code>managed-csi</code>	Uses Azure StandardSSD locally redundant storage (LRS) to create a Managed Disk. The reclaim policy ensures that the underlying Azure Disk is deleted when the persistent volume that used it is deleted. The storage class also configures the persistent volumes to be expandable, you just need to edit the persistent volume claim with the new size.

PERMISSION	REASON
managed-csi-premium	Uses Azure Premium locally redundant storage (LRS) to create a Managed Disk. The reclaim policy again ensures that the underlying Azure Disk is deleted when the persistent volume that used it is deleted. Similarly, this storage class allows for persistent volumes to be expanded.
azurefile-csi	Uses Azure Standard storage to create an Azure File Share. The reclaim policy ensures that the underlying Azure File Share is deleted when the persistent volume that used it is deleted.
azurefile-csi-premium	Uses Azure Premium storage to create an Azure File Share. The reclaim policy ensures that the underlying Azure File Share is deleted when the persistent volume that used it is deleted.
azureblob-nfs-premium	Uses Azure Premium storage to create an Azure Blob storage container and connect using the NFS v3 protocol. The reclaim policy ensures that the underlying Azure Blob storage container is deleted when the persistent volume that used it is deleted.
azureblob-fuse-premium	Uses Azure Premium storage to create an Azure Blob storage container and connect using BlobFuse. The reclaim policy ensures that the underlying Azure Blob storage container is deleted when the persistent volume that used it is deleted.

Unless you specify a StorageClass for a persistent volume, the default StorageClass will be used. Ensure volumes use the appropriate storage you need when requesting persistent volumes.

IMPORTANT

Starting in Kubernetes version 1.21, AKS will use CSI drivers only and by default. The `default` class will be the same as `managed-csi`

You can create a StorageClass for additional needs using `kubectl`. The following example uses Premium Managed Disks and specifies that the underlying Azure Disk should be *retained* when you delete the pod:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: managed-premium-retain
provisioner: disk.csi.azure.com
parameters:
  skuName: Premium_LRS
reclaimPolicy: Retain
volumeBindingMode: WaitForFirstConsumer
allowVolumeExpansion: true
```

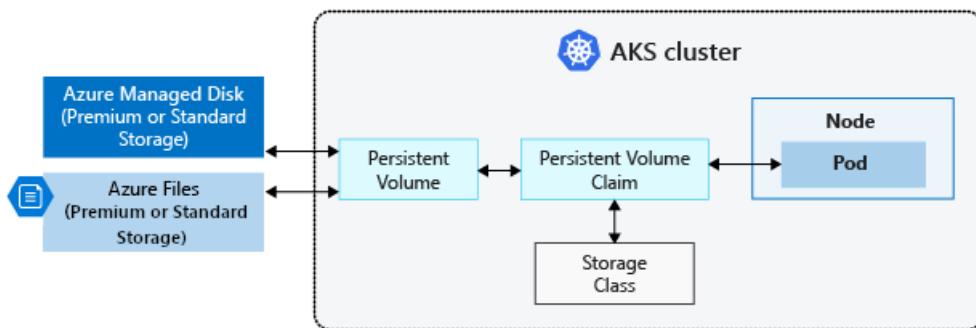
NOTE

AKS reconciles the default storage classes and will overwrite any changes you make to those storage classes.

Persistent volume claims

A PersistentVolumeClaim requests storage of a particular StorageClass, access mode, and size. The Kubernetes API server can dynamically provision the underlying Azure storage resource if no existing resource can fulfill the claim based on the defined StorageClass.

The pod definition includes the volume mount once the volume has been connected to the pod.



Once an available storage resource has been assigned to the pod requesting storage, PersistentVolume is *bound* to a PersistentVolumeClaim. Persistent volumes are 1:1 mapped to claims.

The following example YAML manifest shows a persistent volume claim that uses the *managed-premium* StorageClass and requests a Disk 5Gi in size:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: azure-managed-disk
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: managed-premium-retain
  resources:
    requests:
      storage: 5Gi
```

When you create a pod definition, you also specify:

- The persistent volume claim to request the desired storage.
- The *volumeMount* for your applications to read and write data.

The following example YAML manifest shows how the previous persistent volume claim can be used to mount a volume at */mnt/azure*.

```
kind: Pod
apiVersion: v1
metadata:
  name: nginx
spec:
  containers:
    - name: myfrontend
      image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
      volumeMounts:
        - mountPath: "/mnt/azure"
          name: volume
  volumes:
    - name: volume
      persistentVolumeClaim:
        claimName: azure-managed-disk
```

For mounting a volume in a Windows container, specify the drive letter and path. For example:

```
...
  volumeMounts:
    - mountPath: "d:"
      name: volume
    - mountPath: "c:\k"
      name: k-dir
...

```

Next steps

For associated best practices, see [Best practices for storage and backups in AKS](#).

To see how to use CSI drivers, see the following how-to articles:

- [Enable Container Storage Interface \(CSI\) drivers for Azure Disks, Azure Files, and Azure Blob storage on Azure Kubernetes Service](#)
- [Use Azure Disks CSI driver in Azure Kubernetes Service](#)
- [Use Azure Files CSI driver in Azure Kubernetes Service](#)
- [Use Azure Blob storage CSI driver \(preview\) in Azure Kubernetes Service](#)
- [Integrate Azure NetApp Files with Azure Kubernetes Service](#)

For more information on core Kubernetes and AKS concepts, see the following articles:

- [Kubernetes / AKS clusters and workloads](#)
- [Kubernetes / AKS identity](#)
- [Kubernetes / AKS security](#)
- [Kubernetes / AKS virtual networks](#)
- [Kubernetes / AKS scale](#)

Scaling options for applications in Azure Kubernetes Service (AKS)

10/27/2022 • 6 minutes to read • [Edit Online](#)

As you run applications in Azure Kubernetes Service (AKS), you may need to increase or decrease the amount of compute resources. As the number of application instances you need change, the number of underlying Kubernetes nodes may also need to change. You also might need to quickly provision a large number of additional application instances.

This article introduces the core concepts that help you scale applications in AKS:

- [Manually scale](#)
- [Horizontal pod autoscaler \(HPA\)](#)
- [Cluster autoscaler](#)
- [Azure Container Instance \(ACI\) integration with AKS](#)

Manually scale pods or nodes

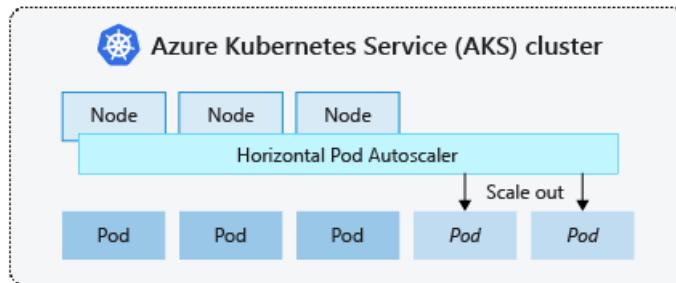
You can manually scale replicas (pods) and nodes to test how your application responds to a change in available resources and state. Manually scaling resources also lets you define a set amount of resources to use to maintain a fixed cost, such as the number of nodes. To manually scale, you define the replica or node count. The Kubernetes API then schedules creating additional pods or draining nodes based on that replica or node count.

When scaling down nodes, the Kubernetes API calls the relevant Azure Compute API tied to the compute type used by your cluster. For example, for clusters built on VM Scale Sets the logic for selecting which nodes to remove is determined by the VM Scale Sets API. To learn more about how nodes are selected for removal on scale down, see the [VMSS FAQ](#).

To get started with manually scaling pods and nodes see [Scale applications in AKS](#).

Horizontal pod autoscaler

Kubernetes uses the horizontal pod autoscaler (HPA) to monitor the resource demand and automatically scale the number of replicas. By default, the horizontal pod autoscaler checks the Metrics API every 15 seconds for any required changes in replica count, but the Metrics API retrieves data from the Kubelet every 60 seconds. Effectively, the HPA is updated every 60 seconds. When changes are required, the number of replicas is increased or decreased accordingly. Horizontal pod autoscaler works with AKS clusters that have deployed the Metrics Server for Kubernetes 1.8+.



When you configure the horizontal pod autoscaler for a given deployment, you define the minimum and maximum number of replicas that can run. You also define the metric to monitor and base any scaling decisions on, such as CPU usage.

To get started with the horizontal pod autoscaler in AKS, see [Autoscale pods in AKS](#).

Cooldown of scaling events

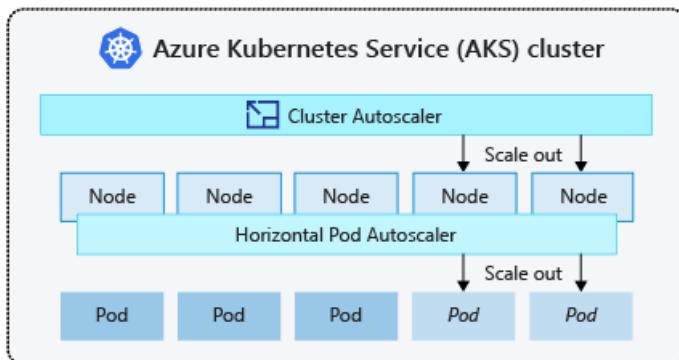
As the horizontal pod autoscaler is effectively updated every 60 seconds, previous scale events may not have successfully completed before another check is made. This behavior could cause the horizontal pod autoscaler to change the number of replicas before the previous scale event could receive application workload and the resource demands to adjust accordingly.

To minimize race events, a delay value is set. This value defines how long the horizontal pod autoscaler must wait after a scale event before another scale event can be triggered. This behavior allows the new replica count to take effect and the Metrics API to reflect the distributed workload. There is [no delay for scale-up events as of Kubernetes 1.12](#), however the delay on scale down events is defaulted to 5 minutes.

Currently, you can't tune these cooldown values from the default.

Cluster autoscaler

To respond to changing pod demands, Kubernetes has a cluster autoscaler, that adjusts the number of nodes based on the requested compute resources in the node pool. By default, the cluster autoscaler checks the Metrics API server every 10 seconds for any required changes in node count. If the cluster autoscale determines that a change is required, the number of nodes in your AKS cluster is increased or decreased accordingly. The cluster autoscaler works with Kubernetes RBAC-enabled AKS clusters that run Kubernetes 1.10.x or higher.



Cluster autoscaler is typically used alongside the horizontal pod autoscaler. When combined, the horizontal pod autoscaler increases or decreases the number of pods based on application demand, and the cluster autoscaler adjusts the number of nodes as needed to run those additional pods accordingly.

To get started with the cluster autoscaler in AKS, see [Cluster Autoscaler on AKS](#).

Scale out events

If a node doesn't have sufficient compute resources to run a requested pod, that pod can't progress through the scheduling process. The pod can't start unless additional compute resources are available within the node pool.

When the cluster autoscaler notices pods that can't be scheduled because of node pool resource constraints, the number of nodes within the node pool is increased to provide the additional compute resources. When those additional nodes are successfully deployed and available for use within the node pool, the pods are then scheduled to run on them.

If your application needs to scale rapidly, some pods may remain in a state waiting to be scheduled until the additional nodes deployed by the cluster autoscaler can accept the scheduled pods. For applications that have high burst demands, you can scale with virtual nodes and Azure Container Instances.

Scale in events

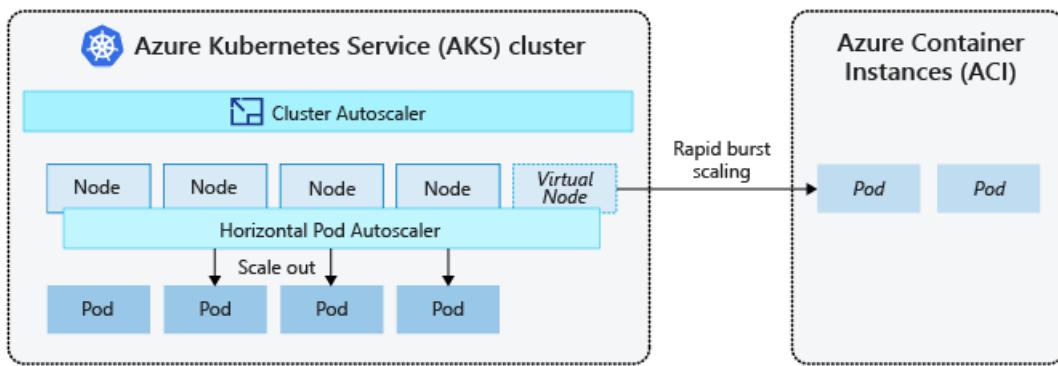
The cluster autoscaler also monitors the pod scheduling status for nodes that haven't recently received new scheduling requests. This scenario indicates the node pool has more compute resources than are required, and the number of nodes can be decreased.

A node that passes a threshold for no longer being needed for 10 minutes by default is scheduled for deletion. When this situation occurs, pods are scheduled to run on other nodes within the node pool, and the cluster autoscaler decreases the number of nodes.

Your applications may experience some disruption as pods are scheduled on different nodes when the cluster autoscaler decreases the number of nodes. To minimize disruption, avoid applications that use a single pod instance.

Burst to Azure Container Instances

To rapidly scale your AKS cluster, you can integrate with Azure Container Instances (ACI). Kubernetes has built-in components to scale the replica and node count. However, if your application needs to rapidly scale, the horizontal pod autoscaler may schedule more pods than can be provided by the existing compute resources in the node pool. If configured, this scenario would then trigger the cluster autoscaler to deploy additional nodes in the node pool, but it may take a few minutes for those nodes to successfully provision and allow the Kubernetes scheduler to run pods on them.



ACI lets you quickly deploy container instances without additional infrastructure overhead. When you connect with AKS, ACI becomes a secured, logical extension of your AKS cluster. The [virtual nodes](#) component, which is based on [Virtual Kubelet](#), is installed in your AKS cluster that presents ACI as a virtual Kubernetes node.

Kubernetes can then schedule pods that run as ACI instances through virtual nodes, not as pods on VM nodes directly in your AKS cluster.

Your application requires no modification to use virtual nodes. Deployments can scale across AKS and ACI and with no delay as cluster autoscaler deploys new nodes in your AKS cluster.

Virtual nodes are deployed to an additional subnet in the same virtual network as your AKS cluster. This virtual network configuration allows the traffic between ACI and AKS to be secured. Like an AKS cluster, an ACI instance is a secure, logical compute resource that is isolated from other users.

Next steps

To get started with scaling applications, first follow the [quickstart to create an AKS cluster with the Azure CLI](#). You can then start to manually or automatically scale applications in your AKS cluster:

- Manually scale [pods](#) or [nodes](#)
- Use the [horizontal pod autoscaler](#)
- Use the [cluster autoscaler](#)

For more information on core Kubernetes and AKS concepts, see the following articles:

- [Kubernetes / AKS clusters and workloads](#)
- [Kubernetes / AKS access and identity](#)
- [Kubernetes / AKS security](#)
- [Kubernetes / AKS virtual networks](#)

- Kubernetes / AKS storage

Azure Kubernetes Service (AKS) node auto-repair

10/27/2022 • 2 minutes to read • [Edit Online](#)

AKS continuously monitors the health state of worker nodes and performs automatic node repair if they become unhealthy. The Azure virtual machine (VM) platform [performs maintenance on VMs](#) experiencing issues.

AKS and Azure VMs work together to minimize service disruptions for clusters.

In this document, you'll learn how automatic node repair functionality behaves for both Windows and Linux nodes.

How AKS checks for unhealthy nodes

AKS uses the following rules to determine if a node is unhealthy and needs repair:

- The node reports **NotReady** status on consecutive checks within a 10-minute timeframe.
- The node doesn't report any status within 10 minutes.

You can manually check the health state of your nodes with kubectl.

```
kubectl get nodes
```

How automatic repair works

NOTE

AKS initiates repair operations with the user account **aks-remediator**.

If AKS identifies an unhealthy node that remains unhealthy for 10 minutes, AKS takes the following actions:

1. Reboot the node.
2. If the reboot is unsuccessful, reimagine the node.
3. If the reimagine is unsuccessful, redeploy the node.

Alternative remediations are investigated by AKS engineers if auto-repair is unsuccessful.

If AKS finds multiple unhealthy nodes during a health check, each node is repaired individually before another repair begins.

Node Autodrain

[Scheduled Events](#) can occur on the underlying virtual machines (VMs) in any of your node pools. For [spot node pools](#), scheduled events may cause a *preempt* node event for the node. Certain node events, such as *preempt*, cause AKS node autodrain to attempt a cordon and drain of the affected node, which allows for a graceful reschedule of any affected workloads on that node. When this happens, you might notice the node to receive a taint with `"remediator.aks.microsoft.com/unschedulable"`, because of `"kubernetes.azure.com/scalesetpriority: spot"`.

The following table shows the node events, and the actions they cause for AKS node autodrain.

EVENT	DESCRIPTION	ACTION
Freeze	The VM is scheduled to pause for a few seconds. CPU and network connectivity may be suspended, but there is no impact on memory or open files	No action
Reboot	The VM is scheduled for reboot. The VM's non-persistent memory is lost.	No action
Redeploy	The VM is scheduled to move to another node. The VM's ephemeral disks are lost.	Cordon and drain
Preempt	The spot VM is being deleted. The VM's ephemeral disks are lost.	Cordon and drain
Terminate	The VM is scheduled to be deleted.	Cordon and drain

Limitations

In many cases, AKS can determine if a node is unhealthy and attempt to repair the issue, but there are cases where AKS either can't repair the issue or can't detect that there is an issue. For example, AKS can't detect issues if a node status is not being reported due to error in network configuration, or has failed to initially register as a healthy node.

Next steps

Use [Availability Zones](#) to increase high availability with your AKS cluster workloads.

Multi-instance GPU Node pool

10/27/2022 • 3 minutes to read • [Edit Online](#)

Nvidia's A100 GPU can be divided in up to seven independent instances. Each instance has their own memory and Stream Multiprocessor (SM). For more information on the Nvidia A100, follow [Nvidia A100 GPU](#).

This article will walk you through how to create a multi-instance GPU node pool on Azure Kubernetes Service clusters and schedule tasks.

GPU Instance Profile

GPU Instance Profiles define how a GPU will be partitioned. The following table shows the available GPU Instance Profile for the `Standard_ND96asr_v4`, the only instance type that supports the A100 GPU at this time.

PROFILE NAME	FRACTION OF SM	FRACTION OF MEMORY	NUMBER OF INSTANCES CREATED
MIG 1g.5gb	1/7	1/8	7
MIG 2g.10gb	2/7	2/8	3
MIG 3g.20gb	3/7	4/8	2
MIG 4g.20gb	4/7	4/8	1
MIG 7g.40gb	7/7	8/8	1

As an example, the GPU Instance Profile of `MIG 1g.5gb` indicates that each GPU instance will have 1g SM(Computing resource) and 5gb memory. In this case, the GPU will be partitioned into seven instances.

The available GPU Instance Profiles available for this instance size are `MIG1g`, `MIG2g`, `MIG3g`, `MIG4g`, `MIG7g`

IMPORTANT

The applied GPU Instance Profile cannot be changed after node pool creation.

Create an AKS cluster

To get started, create a resource group and an AKS cluster. If you already have a cluster, you can skip this step. Follow the example below to the resource group name `myresourcegroup` in the `southcentralus` region:

```
az group create --name myresourcegroup --location southcentralus
```

```
az aks create \
  --resource-group myresourcegroup \
  --name migcluster \
  --node-count 1
```

Create a multi-instance GPU node pool

You can choose to either use the `az` command line or http request to the ARM API to create the node pool

Azure CLI

If you're using command line, use the `az aks nodepool add` command to create the node pool and specify the GPU instance profile through `--gpu-instance-profile`

```
az aks nodepool add \
  --name mignode \
  --resourcegroup myresourcegroup \
  --cluster-name migcluster \
  --node-vm-size Standard_ND96asr_v4 \
  --gpu-instance-profile MIG1g
```

HTTP request

If you're using http request, you can place GPU instance profile in the request body:

```
{
  "properties": {
    "count": 1,
    "vmSize": "Standard_ND96asr_v4",
    "type": "VirtualMachineScaleSets",
    "gpuInstanceProfile": "MIG1g"
  }
}
```

Run tasks using kubectl

MIG strategy

Before you install the Nvidia plugins, you need to specify which strategy to use for GPU partitioning.

The two strategies "Single" and "Mixed" won't affect how you execute CPU workloads, but how GPU resources will be displayed.

- Single Strategy

The single strategy treats every GPU instance as a GPU. If you're using this strategy, the GPU resources will be displayed as:

```
nvidia.com/gpu: 1
```

- Mixed Strategy

The mixed strategy will expose the GPU instances and the GPU instance profile. If you use this strategy, the GPU resource will be displayed as:

```
nvidia.com/mig1g.5gb: 1
```

Install the NVIDIA device plugin and GPU feature discovery

Set your MIG Strategy

```
export MIG_STRATEGY=single
```

or

```
export MIG_STRATEGY=mixed
```

Install the Nvidia device plugin and GPU feature discovery using helm

```
helm repo add nvdp https://nvidia.github.io/k8s-device-plugin
helm repo add nvgfd https://nvidia.github.io/gpu-feature-discovery
helm repo update #do not forget to update the helm repo
```

```
helm install \
--version=0.7.0 \
--generate-name \
--set migStrategy=${MIG_STRATEGY} \
nvdp/nvidia-device-plugin
```

```
helm install \
--version=0.2.0 \
--generate-name \
--set migStrategy=${MIG_STRATEGY} \
nvgfd/gpu-feature-discovery
```

Confirm multi-instance GPU capability

As an example, if you used MIG1g as the GPU instance profile, confirm the node has multi-instance GPU capability by running:

```
kubectl describe mignode
```

If you're using single strategy, you'll see:

```
Allocable:
nvidia.com/gpu: 56
```

If you're using mixed strategy, you'll see:

```
Allocable:
nvidia.com/mig-1g.5gb: 56
```

Schedule work

Use the `kubectl` run command to schedule work using single strategy:

```
kubectl run -it --rm \
--image=nvidia/cuda:11.0-base \
--restart=Never \
--limits=nvidia.com/gpu=1 \
single-strategy-example -- nvidia-smi -L
```

Use the `kubectl` run command to schedule work using mixed strategy:

```
kubectl run -it --rm \
--image=nvidia/cuda:11.0-base \
--restart=Never \
--limits=nvidia.com/mig-1g.5gb=1 \
mixed-strategy-example -- nvidia-smi -L
```

Troubleshooting

- If you do not see multi-instance GPU capability after the node pool has been created, confirm the API version is not older than 2021-08-01.

About service meshes

10/27/2022 • 2 minutes to read • [Edit Online](#)

A service mesh provides capabilities like traffic management, resiliency, policy, security, strong identity, and observability to your workloads. Your application is decoupled from these operational capabilities and the service mesh moves them out of the application layer, and down to the infrastructure layer.

Scenarios

These are some of the scenarios that can be enabled for your workloads when you use a service mesh:

- **Encrypt all traffic in cluster** - Enable mutual TLS between specified services in the cluster. This can be extended to ingress and egress at the network perimeter, and provides a secure by default option with no changes needed for application code and infrastructure.
- **Canary and phased rollouts** - Specify conditions for a subset of traffic to be routed to a set of new services in the cluster. On successful test of canary release, remove conditional routing and phase gradually increasing % of all traffic to new service. Eventually all traffic will be directed to new service.
- **Traffic management and manipulation** - Create a policy on a service that will rate limit all traffic to a version of a service from a specific origin, or a policy that applies a retry strategy to classes of failures between specified services. Mirror live traffic to new versions of services during a migration or to debug issues. Inject faults between services in a test environment to test resiliency.
- **Observability** - Gain insight into how your services are connected and the traffic that flows between them. Obtain metrics, logs, and traces for all traffic in cluster, including ingress/egress. Add distributed tracing abilities to your applications.

Selection criteria

Before you select a service mesh, ensure that you understand your requirements and the reasons for installing a service mesh. Ask the following questions:

- **Is an Ingress Controller sufficient for my needs?** - Sometimes having a capability like A/B testing or traffic splitting at the ingress is sufficient to support the required scenario. Don't add complexity to your environment with no upside.
- **Can my workloads and environment tolerate the additional overheads?** - All the additional components required to support the service mesh require additional resources like CPU and memory. In addition, all the proxies and their associated policy checks add latency to your traffic. If you have workloads that are very sensitive to latency or cannot provide the additional resources to cover the service mesh components, then re-consider.
- **Is this adding additional complexity unnecessarily?** - If the reason for installing a service mesh is to gain a capability that is not necessarily critical to the business or operational teams, then consider whether the additional complexity of installation, maintenance, and configuration is worth it.
- **Can this be adopted in an incremental approach?** - Some of the service meshes that provide a lot of capabilities can be adopted in a more incremental approach. Install just the components you need to ensure your success. Once you are more confident and additional capabilities are required, then explore those. Resist the urge to install *everything* from the start.

Next steps

Open Service Mesh (OSM) is a supported service mesh that runs Azure Kubernetes Service (AKS):

[Learn more about OSM ...](#)

There are also service meshes provided by open-source projects and third parties that are commonly used with AKS. These open-source and third-party service meshes are not covered by the [AKS support policy](#).

- [Istio](#)
- [Linkerd](#)
- [Consul Connect](#)

For more details on the service mesh landscape, see [Layer 5's Service Mesh Landscape](#).

For more details service mesh standardization efforts:

- [Service Mesh Interface \(SMI\)](#)
- [Service Mesh Federation](#)
- [Service Mesh Performance \(SMP\)](#)

Sustainable software engineering practices in Azure Kubernetes Service (AKS)

10/27/2022 • 10 minutes to read • [Edit Online](#)

The sustainable software engineering principles are a set of competencies to help you define, build, and run sustainable applications. The overall goal is to reduce the carbon footprint in every aspect of your application. The Azure Well-Architected Framework guidance for sustainability aligns with the [The Principles of Sustainable Software Engineering](#) from the [Green Software Foundation](#), and provides an overview of the principles of sustainable software engineering.

Sustainable software engineering is a shift in priorities and focus. In many cases, the way most software is designed and run highlights fast performance and low latency. Meanwhile, sustainable software engineering focuses on reducing as much carbon emission as possible. Consider the following:

- Applying sustainable software engineering principles can give you faster performance or lower latency, such as by lowering total network traversal.
- Reducing carbon emissions may cause slower performance or increased latency, such as delaying low-priority workloads.

The guidance found in this article is focused on Azure Kubernetes Services you're building or operating on Azure and includes design and configuration checklists, recommended design, and configuration options. Before applying sustainable software engineering principles to your application, review the priorities, needs, and trade-offs of your application.

Prerequisites

- Understanding the Well-Architected Framework sustainability guidance can help you produce a high quality, stable, and efficient cloud architecture. We recommend that you start by reading more about [sustainable workloads](#) and reviewing your workload using the [Microsoft Azure Well-Architected Review](#) assessment.
- Having clearly defined business requirements is crucial when building applications, as they might have a direct impact on both cluster and workload architectures and configurations. When building or updating existing applications, review the Well-Architected Framework sustainability design areas, alongside your application's holistic lifecycle.

Understanding the shared responsibility model

Sustainability – just like security – is a shared responsibility between the cloud provider and the customer or partner designing and deploying AKS clusters on the platform. Deploying AKS does not automatically make it sustainable, even if the [data centers are optimized for sustainability](#). Applications that aren't optimized may still emit more carbon than necessary.

Learn more about the [shared responsibility model for sustainability](#).

Design principles

Carbon Efficiency: Emit the least amount of carbon possible.

A carbon efficient cloud application is one that is optimized, and the starting point is the cost optimization.

Energy Efficiency: Use the least amount of energy possible.

One way to increase energy efficiency, is to run the application on as few servers as possible, with the servers running at the highest utilization rate; thereby increasing hardware efficiency as well.

Hardware Efficiency: Use the least amount of embodied carbon possible.

There are two main approaches to hardware efficiency:

- For end-user devices, it's extending the lifespan of the hardware.
- For cloud computing, it's increasing the utilization of the resource.

Carbon Awareness: Do more when the electricity is cleaner and do less when the electricity is dirtier.

Being carbon aware means responding to shifts in carbon intensity by increasing or decreasing your demand.

Design patterns and practices

We recommend careful consideration of these design patterns for building a sustainable workload on Azure Kubernetes Service, before reviewing the detailed recommendations in each of the design areas.

DESIGN PATTERN	APPLIES TO WORKLOAD	APPLIES TO CLUSTER
Design for independent scaling of logical components	✓	
Design for event-driven scaling	✓	
Aim for stateless design	✓	
Enable cluster and node auto-updates		✓
Install supported add-ons and extensions	✓	✓
Containerize your workload where applicable	✓	
Use energy efficient hardware		✓
Match the scalability needs and utilize auto-scaling and bursting capabilities		✓
Turn off workloads and node pools outside of business hours	✓	✓
Delete unused resources	✓	✓
Tag your resources	✓	✓
Optimize storage utilization	✓	✓
Choose a region that is closest to users		✓
Reduce network traversal between nodes		✓

DESIGN PATTERN	APPLIES TO WORKLOAD	APPLIES TO CLUSTER
Evaluate using a service mesh		✓
Optimize log collection	✓	✓
Cache static data	✓	✓
Evaluate whether to use TLS termination	✓	✓
Use cloud native network security tools and controls	✓	✓
Scan for vulnerabilities	✓	✓

Application design

Explore this section to learn more about how to optimize your applications for a more sustainable application design.

Design for independent scaling of logical components

A microservice architecture may reduce the compute resources required, as it allows for independent scaling of its logical components and ensures they are scaled according to the demand.

- Consider using [Dapr Framework](#) or [other CNCF projects](#) to help you separate your application functionality into different microservices, to allow independent scaling of its logical components.

Design for event-driven scaling

Scaling your workload based on relevant business metrics such as HTTP requests, queue length, and cloud events can help reduce its resource utilization, hence its carbon emissions.

- Use [Keda](#) when building event-driven applications to allow scaling down to zero when there is no demand.

Aim for stateless design

Removing state from your design reduces the in-memory or on-disk data required by the workload to function.

- Consider [stateless design](#) to reduce unnecessary network load, data processing, and compute resources.

Application platform

Explore this section to learn how to make better informed platform-related decisions around sustainability.

Enable cluster and node auto-updates

An up-to-date cluster avoids unnecessary performance issues and ensures you benefit from the latest performance improvements and compute optimizations.

- Enable [cluster auto-upgrade](#) and [apply security updates to nodes automatically using GitHub Actions](#), to ensure your cluster has the latest improvements.

Install supported add-ons and extensions

Add-ons and extensions covered by the [AKS support policy](#) provide additional and supported functionality to your cluster while allowing you to benefit from the latest performance improvements and energy optimizations throughout your cluster lifecycle.

- Ensure you install [KEDA](#) as an add-on and [GitOps & Dapr](#) as extensions.

Containerize your workload where applicable

Containers allow for reducing unnecessary resource allocation and making better use of the resources deployed as they allow for bin packing and require less compute resources than virtual machines.

- Use [Draft](#) to simplify application containerization by generating Dockerfiles and Kubernetes manifests.

Use energy efficient hardware

Ampere's Cloud Native Processors are uniquely designed to meet both the high performance and power efficiency needs of the cloud.

- Evaluate if nodes with [Ampere Altra Arm-based processors](#) are a good option for your workloads.

Match the scalability needs and utilize auto-scaling and bursting capabilities

An oversized cluster does not maximize utilization of compute resources and can lead to a waste of energy. Separate your applications into different node pools to allow for cluster right sizing and independent scaling according to the application requirements. As you run out of capacity in your AKS cluster, grow from AKS to ACI to scale out additional pods to serverless nodes and ensure your workload uses all the allocated resources efficiently.

- Size your cluster to match the scalability needs of your application and [use cluster autoscaler](#) in combination with [virtual nodes](#) to rapidly scale and maximize compute resource utilization. Additionally, [enforce resource quotas](#) at the namespace level and [scale user node pools to 0](#) when there is no demand.

Turn off workloads and node pools outside of business hours

Workloads may not need to run continuously and could be turned off to reduce energy waste, hence carbon emissions. You can completely turn off (stop) your node pools in your AKS cluster, allowing you to also save on compute costs.

- Use the [node pool stop / start](#) to turn off your node pools outside of business hours, and [KEDA CRON scaler](#) to scale down your workloads (pods) based on time.

Operational procedures

Explore this section to set up your environment for measuring and continuously improving your workloads cost and carbon efficiency.

Delete unused resources

Unused resources such as unreferenced images and storage resources should be identified and deleted as they have a direct impact on hardware and energy efficiency. Identifying and deleting unused resources must be treated as a process, rather than a point-in-time activity to ensure continuous energy optimization.

- Use [Azure Advisor](#) to identify unused resources and [ImageCleaner](#) to clean up stale images and remove an area of risk in your cluster.

Tag your resources

Getting the right information and insights at the right time is important for producing reports about performance and resource utilization.

- Set [Azure tags on your cluster](#) to enable monitoring of your workloads.

Storage

Explore this section to learn how to design a more sustainable data storage architecture and optimize existing deployments.

Optimize storage utilization

The data retrieval and data storage operations can have a significant impact on both energy and hardware efficiency. Designing solutions with the correct data access pattern can reduce energy consumption and embodied carbon.

- Understand the needs of your application to [choose the appropriate storage](#) and define it using [storage classes](#) to avoid storage underutilization. Additionally, consider [provisioning volumes dynamically](#) to automatically scale the number of storage resources.

Network and connectivity

Explore this section to learn how to enhance and optimize network efficiency to reduce unnecessary carbon emissions.

Choose a region that is closest to users

The distance from a data center to the users has a significant impact on energy consumption and carbon emissions. Shortening the distance a network packet travels improves both your energy and carbon efficiency.

- Review your application requirements and [Azure geographies](#) to choose a region that is the closest to the majority of where the network packets are going.

Reduce network traversal between nodes

Placing nodes in a single region or a single availability zone reduces the physical distance between the instances. However, for business critical workloads, you need to ensure your cluster is spread across multiple availability-zones, which may result in more network traversal and increase in your carbon footprint.

- Consider deploying your nodes within a [proximity placement group](#) to reduce the network traversal by ensuring your compute resources are physically located close to each other. For critical workloads configure [proximity placement groups with availability zones](#).

Evaluate using a service mesh

A service mesh deploys additional containers for communication, typically in a [sidecar pattern](#), to provide more operational capabilities leading to an increase in CPU usage and network traffic. Nevertheless, it allows you to decouple your application from these capabilities as it moves them out from the application layer, and down to the infrastructure layer.

- Carefully consider the increase in CPU usage and network traffic generated by [service mesh](#) communication components before making the decision to use one.

Optimize log collection

Sending and storing all logs from all possible sources (workloads, services, diagnostics and platform activity) can considerably increase storage and network traffic, which would impact higher costs and carbon emissions.

- Make sure you are collecting and retaining only the log data necessary to support your requirements. [Configure data collection rules for your AKS workloads](#) and implement design considerations for [optimizing your Log Analytics costs](#).

Cache static data

Using Content Delivery Network (CDN) is a sustainable approach to optimizing network traffic because it reduces the data movement across a network. It minimizes latency through storing frequently read static data closer to users, and helps reduce network traffic and server load.

- Ensure you [follow best practices](#) for CDN and consider using [Azure CDN](#) to lower the consumed bandwidth and keep costs down.

Security

Explore this section to learn more about the recommendations leading to a sustainable, right-sized security posture.

Evaluate whether to use TLS termination

Transport Layer Security (TLS) ensures that all data passed between the web server and web browsers remain private and encrypted. However, terminating and re-establishing TLS increases CPU utilization and might be unnecessary in certain architectures. A balanced level of security can offer a more sustainable and energy efficient workload, while a higher level of security may increase the compute resource requirements.

- Review the information on TLS termination when using [Application Gateway](#) or [Azure Front Door](#). Consider if you can terminate TLS at your border gateway and continue with non-TLS to your workload load balancer and onwards to your workload.

Use cloud native network security tools and controls

Azure Font Door and Application Gateway help manage traffic from web applications while Azure Web Application Firewall provides protection against OWASP top 10 attacks and load shedding bad bots. Using these capabilities helps remove unnecessary data transmission and reduces the burden on the cloud infrastructure, with lower bandwidth and less infrastructure requirements.

- Use [Application Gateway Ingress Controller \(AGIC\) in AKS](#) to filter and offload traffic at the network edge from reaching your origin to reduce energy consumption and carbon emissions.

Scan for vulnerabilities

Many attacks on cloud infrastructure seek to misuse deployed resources for the attacker's direct gain leading to an unnecessary spike in usage and cost. Vulnerability scanning tools help minimize the window of opportunity for attackers and mitigate any potential malicious usage of resources.

- Follow recommendations from [Microsoft Defender for Cloud](#) and run automated vulnerability scanning tools such as [Defender for Containers](#) to avoid unnecessary resource usage by identifying vulnerabilities in your images and minimizing the window of opportunity for attackers.

Next steps

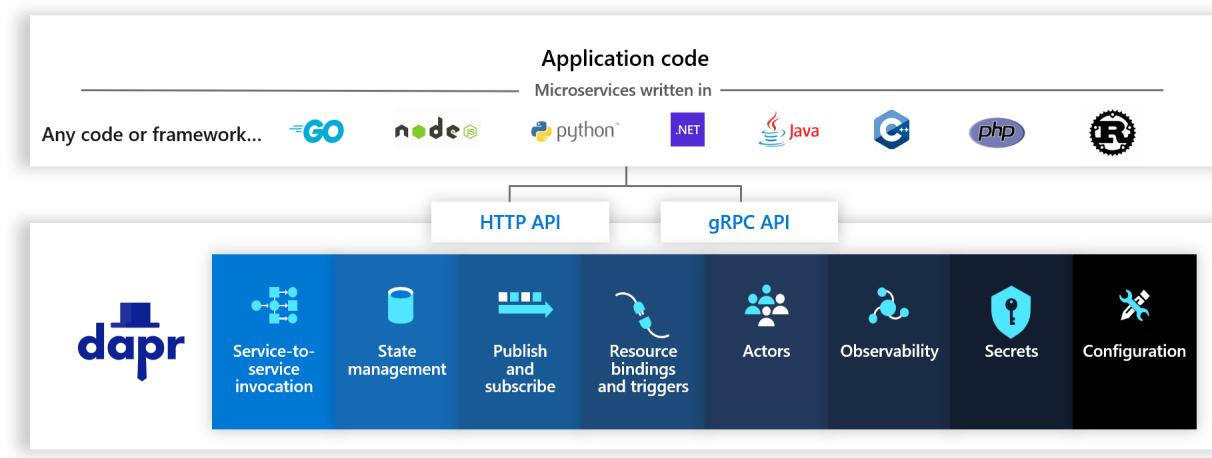
[Azure Well-Architected Framework review of AKS](#)

Dapr

10/27/2022 • 4 minutes to read • [Edit Online](#)

Distributed Application Runtime (Dapr) offers APIs that simplify microservice development and implementation. Running as a sidecar process in tandem with your applications, Dapr APIs abstract away common complexities developers regularly encounter when building distributed applications, such as service discovery, message broker integration, encryption, observability, and secret management. Whether your inter-application communication is direct service-to-service, or pub/sub messaging, Dapr helps you write simple, portable, resilient, and secured microservices.

Dapr is incrementally adoptable – the API building blocks can be used as the need arises. Use one, several, or all to develop your application faster.



Capabilities and features

Dapr provides the following set of capabilities to help with your microservice development on AKS:

- Easy provisioning of Dapr on AKS through [cluster extensions](#).
- Portability enabled through HTTP and gRPC APIs which abstract underlying technologies choices
- Reliable, secure, and resilient service-to-service calls through HTTP and gRPC APIs
- Publish and subscribe messaging made easy with support for CloudEvent filtering and “at-least-once” semantics for message delivery
- Pluggable observability and monitoring through Open Telemetry API collector
- Works independent of language, while also offering language specific SDKs
- Integration with VS Code through the Dapr extension
- [More APIs for solving distributed application challenges](#)

Frequently asked questions

How do Dapr and Service meshes compare?

A: Where a service mesh is defined as a networking service mesh, Dapr is not a service mesh. While Dapr and service meshes do offer some overlapping capabilities, a service mesh is focused on networking concerns, whereas Dapr is focused on providing building blocks that make it easier for developers to build applications as microservices. Dapr is developer-centric, while service meshes are infrastructure-centric.

Some common capabilities that Dapr shares with service meshes include:

- Secure service-to-service communication with mTLS encryption
- Service-to-service metric collection
- Service-to-service distributed tracing
- Resiliency through retries

In addition, Dapr provides other application-level building blocks for state management, pub/sub messaging, actors, and more. However, Dapr does not provide capabilities for traffic behavior such as routing or traffic splitting. If your solution would benefit from the traffic splitting a service mesh provides, consider using [Open Service Mesh](#).

For more information on Dapr and service meshes, and how they can be used together, visit the [Dapr documentation](#).

How does the Dapr secrets API compare to the Secrets Store CSI driver?

Both the Dapr secrets API and the managed Secrets Store CSI driver allow for the integration of secrets held in an external store, abstracting secret store technology from application code. The Secrets Store CSI driver mounts secrets held in Azure Key Vault as a CSI volume for consumption by an application. Dapr exposes secrets via a RESTful API that can be called by application code and can be configured with assorted secret stores. The following table lists the capabilities of each offering:

	DAPR SECRETS API	SECRETS STORE CSI DRIVER
Supported secrets stores	Local environment variables (for Development); Local file (for Development); Kubernetes Secrets; AWS Secrets Manager; Azure Key Vault secret store; Azure Key Vault with Managed Identities on Kubernetes; GCP Secret Manager; HashiCorp Vault	Azure Key Vault secret store
Accessing secrets in application code	Call the Dapr secrets API	Access the mounted volume or sync mounted content as a Kubernetes secret and set an environment variable
Secret rotation	New API calls obtain the updated secrets	Polls for secrets and updates the mount at a configurable interval
Logging and metrics	The Dapr sidecar generates logs, which can be configured with collectors such as Azure Monitor, emits metrics via Prometheus, and exposes an HTTP endpoint for health checks	Emits driver and Azure Key Vault provider metrics via Prometheus

For more information on the secret management in Dapr, see the [secrets management building block overview](#).

For more information on the Secrets Store CSI driver and Azure Key Vault provider, see the [Secrets Store CSI driver overview](#).

How does the managed Dapr cluster extension compare to the open source Dapr offering?

The managed Dapr cluster extension is the easiest method to provision Dapr on an AKS cluster. With the extension, you're able to offload management of the Dapr runtime version by opting into automatic upgrades. Additionally, the extension installs Dapr with smart defaults (for example, provisioning the Dapr control plane in high availability mode).

When installing Dapr OSS via helm or the Dapr CLI, runtime versions and configuration options are the responsibility of developers and cluster maintainers.

Lastly, the Dapr extension is an extension of AKS, therefore you can expect the same support policy as other AKS features.

[Learn more about migrating from Dapr OSS to the Dapr extension for AKS.](#)

How can I authenticate Dapr components with Azure AD using managed identities?

- Learn how [Dapr components authenticate with Azure AD](#).
- Learn about [using managed identities with AKS](#).

How can I switch to using the Dapr extension if I've already installed Dapr via a method, such as Helm?

Recommended guidance is to completely uninstall Dapr from the AKS cluster and reinstall it via the cluster extension.

If you install Dapr through the AKS extension, our recommendation is to continue using the extension for future management of Dapr instead of the Dapr CLI. Combining the two tools can cause conflicts and result in undesired behavior.

Next Steps

After learning about Dapr and some of the challenges it solves, try [Deploying an application with the Dapr cluster extension](#).

GitOps Flux v2 configurations with AKS and Azure Arc-enabled Kubernetes

10/27/2022 • 6 minutes to read • [Edit Online](#)

Azure provides configuration management capability using GitOps in Azure Kubernetes Service (AKS) and Azure Arc-enabled Kubernetes clusters. You can easily enable and use GitOps in these clusters.

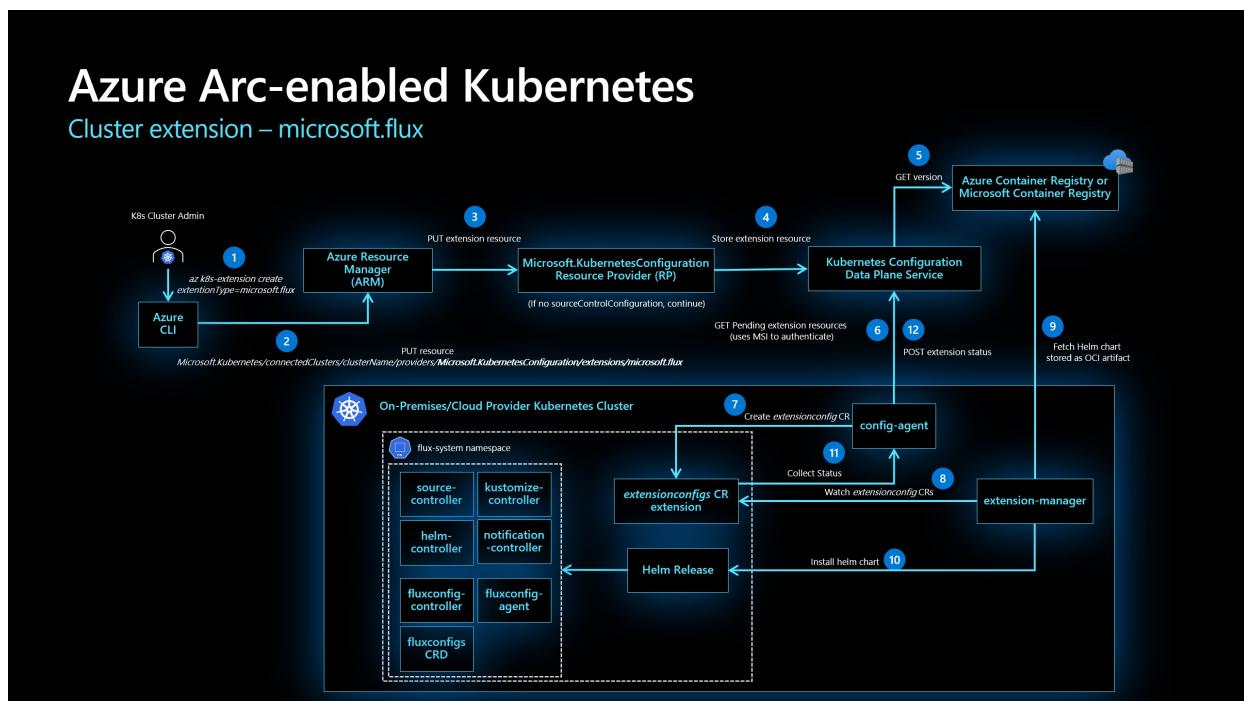
With GitOps, you declare the desired state of your Kubernetes clusters in files in Git repositories. The Git repositories may contain the following files:

- [YAML-formatted manifests](#) that describe Kubernetes resources (such as Namespaces, Secrets, Deployments, and others)
- [Helm charts](#) for deploying applications
- [Kustomize files](#) to describe environment-specific changes

Because these files are stored in a Git repository, they're versioned, and changes between versions are easily tracked. Kubernetes controllers run in the clusters and continually reconcile the cluster state with the desired state declared in the Git repository. These operators pull the files from the Git repositories and apply the desired state to the clusters. The operators also continuously assure that the cluster remains in the desired state.

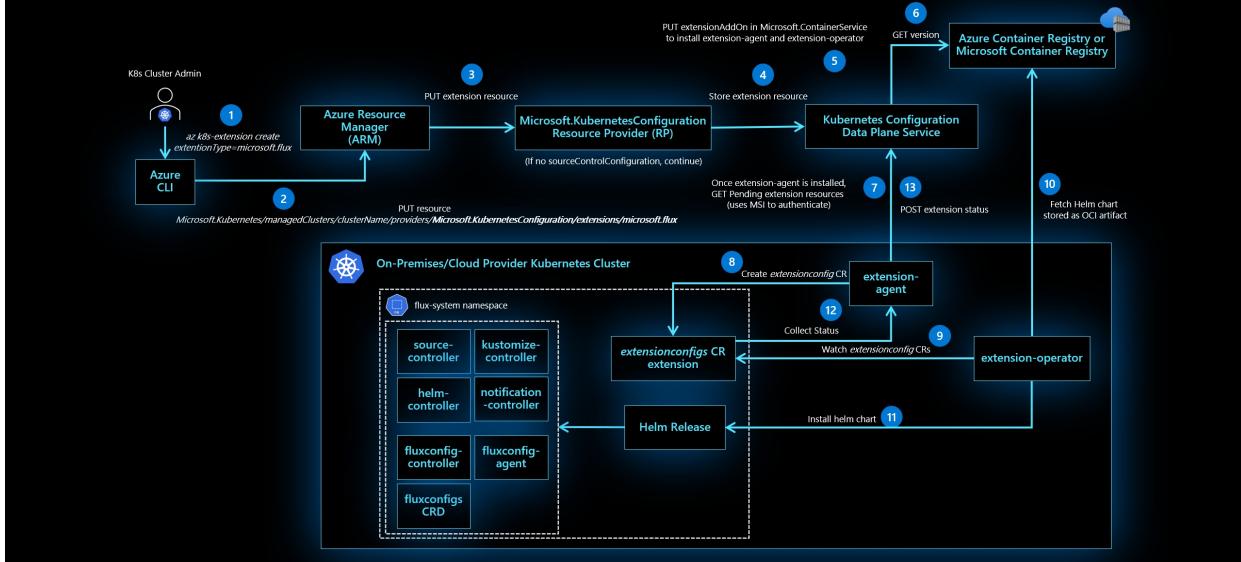
GitOps on Azure Arc-enabled Kubernetes or Azure Kubernetes Service uses [Flux](#), a popular open-source tool set. Flux provides support for common file sources (Git and Helm repositories, Buckets, Azure Blob Storage) and template types (YAML, Helm, and Kustomize). Flux also supports multi-tenancy and deployment dependency management, among [other features](#).

Flux cluster extension



Azure Kubernetes Service (AKS)

Cluster extension – microsoft.flux



GitOps is enabled in an Azure Arc-enabled Kubernetes or AKS cluster as a

`Microsoft.KubernetesConfiguration/extensions/microsoft.flux` cluster extension resource. The `microsoft.flux` extension must be installed in the cluster before one or more `fluxConfigurations` can be created. The extension will be installed automatically when you create the first `Microsoft.KubernetesConfiguration/fluxConfigurations` in a cluster, or you can install it manually using the portal, the Azure CLI (`az k8s-extension create --extensionType=microsoft.flux`), ARM template, or REST API.

Version support

The most recent version of the Flux v2 extension and the two previous versions (N-2) are supported. We generally recommend that you use the most recent version of the extension.

Controllers

The `microsoft.flux` extension installs by default the **Flux controllers** (Source, Kustomize, Helm, Notification) and the FluxConfig CRD, fluxconfig-agent, and fluxconfig-controller. You can control which of these controllers is installed and can optionally install the Flux image-automation and image-reflector controllers, which provide functionality around updating and retrieving Docker images.

- **Flux Source controller:** Watches the `source.toolkit.fluxcd.io` custom resources. Handles the synchronization between the Git repositories, Helm repositories, Buckets and Azure Blob storage. Handles authorization with the source for private Git, Helm repos and Azure blob storage accounts. Surfaces the latest changes to the source through a tar archive file.
- **Flux Kustomize controller:** Watches the `kustomization.toolkit.fluxcd.io` custom resources. Applies Kustomize or raw YAML files from the source onto the cluster.
- **Flux Helm controller:** Watches the `helm.toolkit.fluxcd.io` custom resources. Retrieves the associated chart from the Helm Repository source surfaced by the Source controller. Creates the `HelmChart` custom resource and applies the `HelmRelease` with given version, name, and customer-defined values to the cluster.
- **Flux Notification controller:** Watches the `notification.toolkit.fluxcd.io` custom resources. Receives notifications from all Flux controllers. Pushes notifications to user-defined webhook endpoints.
- **Flux Custom Resource Definitions:**
 - `kustomizations.kustomize.toolkit.fluxcd.io`

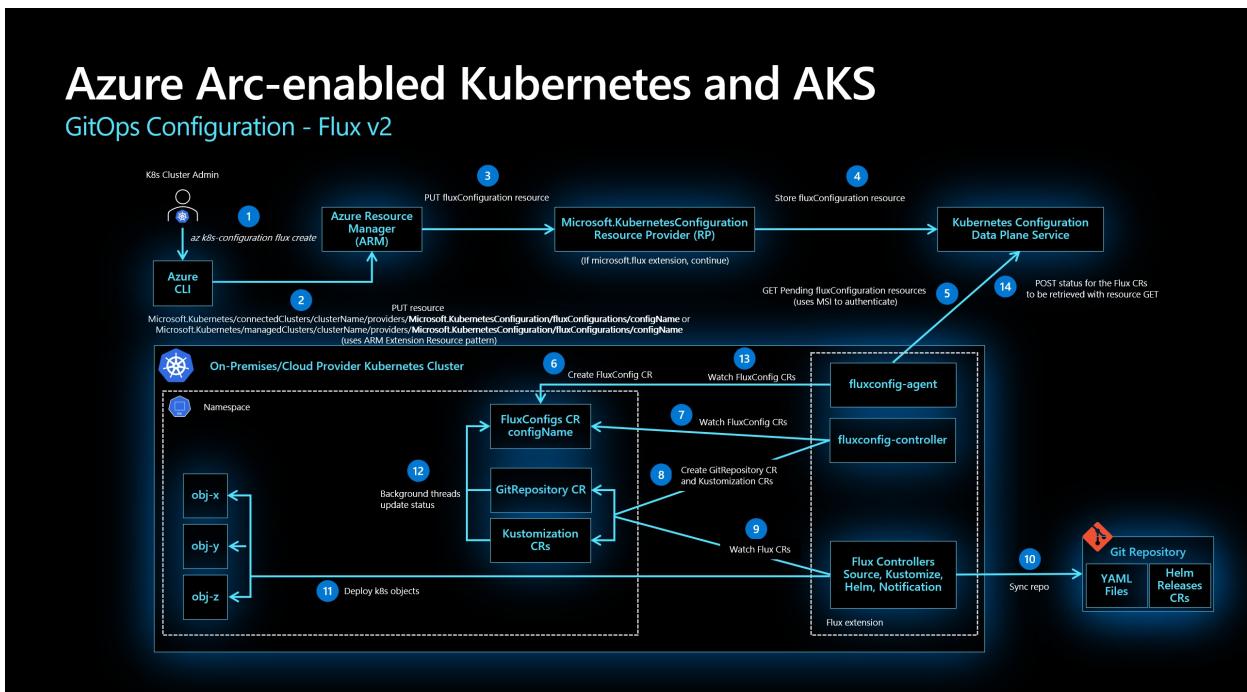
- `imagepolicies.image.toolkit.fluxcd.io`
- `imagerepositories.image.toolkit.fluxcd.io`
- `imageupdateautomations.image.toolkit.fluxcd.io`
- `alerts.notification.toolkit.fluxcd.io`
- `providers.notification.toolkit.fluxcd.io`
- `receivers.notification.toolkit.fluxcd.io`
- `buckets.source.toolkit.fluxcd.io`
- `gitrepositories.source.toolkit.fluxcd.io`
- `helmcharts.source.toolkit.fluxcd.io`
- `helmrepositories.source.toolkit.fluxcd.io`
- `helmreleases.helm.toolkit.fluxcd.io`
- `fluxconfigs.clusterconfig.azure.com`

- **FluxConfig CRD:** Custom Resource Definition for `fluxconfigs.clusterconfig.azure.com` custom resources that define `FluxConfig` Kubernetes objects.
- **fluxconfig-agent:** Responsible for watching Azure for new or updated `fluxConfigurations` resources, and for starting the associated Flux configuration in the cluster. Also, is responsible for pushing Flux status changes in the cluster back to Azure for each `fluxConfigurations` resource.
- **fluxconfig-controller:** Watches the `fluxconfigs.clusterconfig.azure.com` custom resources and responds to changes with new or updated configuration of GitOps machinery in the cluster.

NOTE

The `microsoft.flux` extension is installed in the `flux-system` namespace and has cluster-wide scope. The option to install this extension at the namespace scope is not available, and attempt to install at namespace scope will fail with 400 error.

Flux configurations



You create Flux configuration resources (`Microsoft.KubernetesConfiguration/fluxConfigurations`) to enable GitOps management of the cluster from your Git repos, Bucket sources or Azure Blob Storage. When you create

a `fluxConfigurations` resource, the values you supply for the parameters, such as the target Git repo, are used to create and configure the Kubernetes objects that enable the GitOps process in that cluster. To ensure data security, the `fluxConfigurations` resource data is stored encrypted at rest in an Azure Cosmos DB database by the Cluster Configuration service.

The `fluxconfig-agent` and `fluxconfig-controller` agents, installed with the `microsoft.flux` extension, manage the GitOps configuration process.

`fluxconfig-agent` is responsible for:

- Polls the Kubernetes Configuration data plane service for new or updated `fluxConfigurations` resources.
- Creates or updates `FluxConfig` custom resources in the cluster with the configuration information.
- Watches `FluxConfig` custom resources and pushes status changes back to the associated Azure `fluxConfiguration` resources.

`fluxconfig-controller` is responsible for:

- Watches status updates to the Flux custom resources created by the managed `fluxConfigurations`.
- Creates private/public key pair that exists for the lifetime of the `fluxConfigurations`. This key is used for authentication if the URL is SSH based and if the user doesn't provide their own private key during creation of the configuration.
- Creates custom authentication secret based on user-provided private-key/http basic-auth/known-hosts/no-auth data.
- Sets up RBAC (service account provisioned, role binding created/assigned, role created/assigned).
- Creates `GitRepository` or `Bucket` custom resource and `Kustomization` custom resources from the information in the `FluxConfig` custom resource.

Each `fluxConfigurations` resource in Azure will be associated in a Kubernetes cluster with one Flux `GitRepository` or `Bucket` custom resource and one or more `Kustomization` custom resources. When you create a `fluxConfigurations` resource, you'll specify, among other information, the URL to the source (Git repository, Bucket or Azure Blob storage) and the sync target in the source for each `Kustomization`. You can configure dependencies between `Kustomization` custom resources to control deployment sequencing. Also, you can create multiple namespace-scoped `fluxConfigurations` resources on the same cluster for different applications and app teams.

NOTE

The `fluxconfig-agent` monitors for new or updated `fluxConfiguration` resources in Azure. The agent requires connectivity to Azure for the desired state of the `fluxConfiguration` to be applied to the cluster. If the agent is unable to connect to Azure, there will be a delay in making the changes in the cluster until the agent can connect. If the cluster is disconnected from Azure for more than 48 hours, then the request to the cluster will time-out, and the changes will need to be re-applied in Azure.

Sensitive customer inputs like private key and token/password are stored for less than 48 hours in the Kubernetes Configuration service. If you update any of these values in Azure, make sure that your clusters connect with Azure within 48 hours.

GitOps with Private Link

If you've added support for [private link to an Azure Arc-enabled Kubernetes cluster](#), then the `microsoft.flux` extension works out-of-the-box with communication back to Azure. For connections to your Git repository, Helm repository, or any other endpoints that are needed to deploy your Kubernetes manifests, you will need to provision these endpoints behind your firewall or list them on your firewall so that the Flux Source controller can successfully reach them.

Data residency

The Azure GitOps service (Azure Kubernetes Configuration Management) stores/processes customer data. By default, customer data is replicated to the paired region. For the regions Singapore, East Asia, and Brazil South, all customer data is stored and processed in the region.

Apply Flux configurations at scale

Because Azure Resource Manager manages your configurations, you can automate creating the same configuration across all Azure Kubernetes Service and Azure Arc-enabled Kubernetes resources using Azure Policy, within the scope of a subscription or a resource group. This at-scale enforcement ensures that specific configurations will be applied consistently across entire groups of clusters.

[Learn how to use the built-in policies for Flux v2.](#)

Next steps

Advance to the next tutorial to learn how to enable GitOps on your AKS or Azure Arc-enabled Kubernetes clusters:

- [Enable GitOps with Flux](#)

Cluster operator and developer best practices to build and manage applications on Azure Kubernetes Service (AKS)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Building and running applications successfully in Azure Kubernetes Service (AKS) require understanding and implementation of some key considerations, including:

- Multi-tenancy and scheduler features.
- Cluster and pod security.
- Business continuity and disaster recovery.

The AKS product group, engineering teams, and field teams (including global black belts [GBBs]) contributed to, wrote, and grouped the following best practices and conceptual articles. Their purpose is to help cluster operators and developers understand the considerations above and implement the appropriate features.

Cluster operator best practices

As a cluster operator, work together with application owners and developers to understand their needs. You can then use the following best practices to configure your AKS clusters as needed.

Multi-tenancy

- [Best practices for cluster isolation](#)
 - Includes multi-tenancy core components and logical isolation with namespaces.
- [Best practices for basic scheduler features](#)
 - Includes using resource quotas and pod disruption budgets.
- [Best practices for advanced scheduler features](#)
 - Includes using taints and tolerations, node selectors and affinity, and inter-pod affinity and anti-affinity.
- [Best practices for authentication and authorization](#)
 - Includes integration with Azure Active Directory, using Kubernetes role-based access control (Kubernetes RBAC), using Azure RBAC, and pod identities.

Security

- [Best practices for cluster security and upgrades](#)
 - Includes securing access to the API server, limiting container access, and managing upgrades and node reboots.
- [Best practices for container image management and security](#)
 - Includes securing the image and runtimes and automated builds on base image updates.
- [Best practices for pod security](#)
 - Includes securing access to resources, limiting credential exposure, and using pod identities and digital key vaults.

Network and storage

- [Best practices for network connectivity](#)
 - Includes different network models, using ingress and web application firewalls (WAF), and securing

node SSH access.

- [Best practices for storage and backups](#)
 - Includes choosing the appropriate storage type and node size, dynamically provisioning volumes, and data backups.

Running enterprise-ready workloads

- [Best practices for business continuity and disaster recovery](#)
 - Includes using region pairs, multiple clusters with Azure Traffic Manager, and geo-replication of container images.

Developer best practices

As a developer or application owner, you can simplify your development experience and define requirements for application performance needs.

- [Best practices for application developers to manage resources](#)
 - Includes defining pod resource requests and limits, configuring development tools, and checking for application issues.
- [Best practices for pod security](#)
 - Includes securing access to resources, limiting credential exposure, and using pod identities and digital key vaults.

Kubernetes / AKS concepts

To help understand some of the features and components of these best practices, you can also see the following conceptual articles for clusters in Azure Kubernetes Service (AKS):

- [Kubernetes core concepts](#)
- [Access and identity](#)
- [Security concepts](#)
- [Network concepts](#)
- [Storage options](#)
- [Scaling options](#)

Next steps

If you need to get started with AKS, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

Best practices for authentication and authorization in Azure Kubernetes Service (AKS)

10/27/2022 • 8 minutes to read • [Edit Online](#)

As you deploy and maintain clusters in Azure Kubernetes Service (AKS), you implement ways to manage access to resources and services. Without these controls:

- Accounts could have access to unnecessary resources and services.
- Tracking credentials used to make changes can be difficult.

In this article, we discuss what recommended practices a cluster operator can follow to manage access and identity for AKS clusters. You'll learn how to:

- Authenticate AKS cluster users with Azure Active Directory (Azure AD).
- Control access to resources with Kubernetes role-based access control (Kubernetes RBAC).
- Use Azure RBAC to granularly control access to the AKS resource, the Kubernetes API at scale, and the `kubeconfig`.
- Use a [managed identity](#) to authenticate pods with other services.

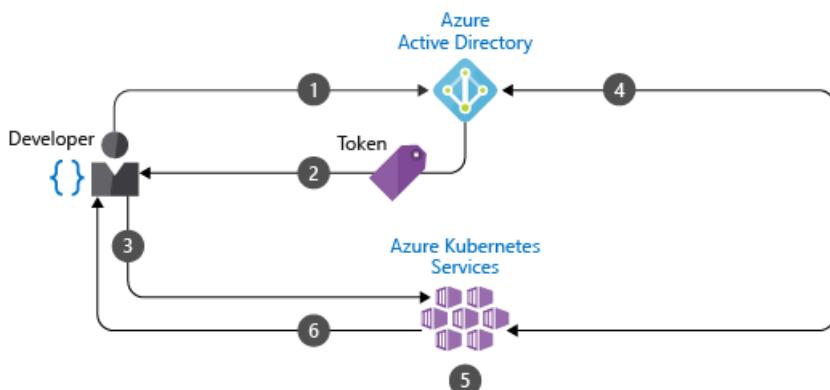
Use Azure Active Directory (Azure AD)

Best practice guidance

Deploy AKS clusters with [Azure AD integration](#). Using Azure AD centralizes the identity management layer. Any change in user account or group status is automatically updated in access to the AKS cluster. Scope users or groups to the minimum permissions amount using [Roles, ClusterRoles, or Bindings](#).

Your Kubernetes cluster developers and application owners need access to different resources. Kubernetes lacks an identity management solution for you to control the resources with which users can interact. Instead, you can integrate your cluster with an existing identity solution like Azure AD, an enterprise-ready identity management solution.

With Azure AD-integrated clusters in AKS, you create *Roles* or *ClusterRoles* defining access permissions to resources. You then *bind* the roles to users or groups from Azure AD. Learn more about these Kubernetes RBAC in [the next section](#). Azure AD integration and how you control access to resources can be seen in the following diagram:



1. Developer authenticates with Azure AD.
2. The Azure AD token issuance endpoint issues the access token.

3. The developer performs an action using the Azure AD token, such as `kubectl create pod`.
4. Kubernetes validates the token with Azure AD and fetches the developer's group memberships.
5. Kubernetes RBAC and cluster policies are applied.
6. The developer's request is successful based on previous validation of Azure AD group membership and Kubernetes RBAC and policies.

To create an AKS cluster that uses Azure AD, see [Integrate Azure Active Directory with AKS](#).

Use Kubernetes role-based access control (Kubernetes RBAC)

Best practice guidance

Define user or group permissions to cluster resources with Kubernetes RBAC. Create roles and bindings that assign the least amount of permissions required. Integrate with Azure AD to automatically update any user status or group membership change and keep access to cluster resources current.

In Kubernetes, you provide granular access control to cluster resources. You define permissions at the cluster level, or to specific namespaces. You determine what resources can be managed and with what permissions. You then apply these roles to users or groups with a binding. For more information about *Roles*, *ClusterRoles*, and *Bindings*, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).

For example, you create a role with full access to resources in the namespace named *finance-app*, as shown in the following example YAML manifest:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: finance-app-full-access-role
  namespace: finance-app
rules:
- apiGroups: [""]
  resources: ["*"]
  verbs: ["*"]
```

You then create a *RoleBinding* and bind the Azure AD user *developer1@contoso.com* to it, as shown in the following YAML manifest:

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: finance-app-full-access-role-binding
  namespace: finance-app
subjects:
- kind: User
  name: developer1@contoso.com
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: finance-app-full-access-role
  apiGroup: rbac.authorization.k8s.io
```

When *developer1@contoso.com* is authenticated against the AKS cluster, they have full permissions to resources in the *finance-app* namespace. In this way, you logically separate and control access to resources. Use Kubernetes RBAC with Azure AD-integration.

To learn how to use Azure AD groups to control access to Kubernetes resources using Kubernetes RBAC, see [Control access to cluster resources using role-based access control and Azure Active Directory identities in AKS](#).

Use Azure RBAC

Best practice guidance

Use Azure RBAC to define the minimum required user and group permissions to AKS resources in one or more subscriptions.

There are two levels of access needed to fully operate an AKS cluster:

- Access the AKS resource on your Azure subscription.

This access level allows you to:

- Control scaling or upgrading your cluster using the AKS APIs
- Pull your `kubeconfig`.

To learn how to control access to the AKS resource and the `kubeconfig`, see [Limit access to cluster configuration file](#).

- Access to the Kubernetes API.

This access level is controlled either by:

- [Kubernetes RBAC](#) (traditionally) or
- By integrating Azure RBAC with AKS for Kubernetes authorization.

To learn how to granularly grant permissions to the Kubernetes API using Azure RBAC, see [Use Azure RBAC for Kubernetes authorization](#).

Use pod-managed identities

Best practice guidance

Don't use fixed credentials within pods or container images, as they are at risk of exposure or abuse. Instead, use *pod identities* to automatically request access using Azure AD.

NOTE

Pod identities are intended for use with Linux pods and container images only. Pod-managed identities support for Windows containers is coming soon.

To access other Azure resources, like Azure Cosmos DB, Key Vault, or Blob storage, the pod needs authentication credentials. You could define authentication credentials with the container image or inject them as a Kubernetes secret. Either way, you would need to manually create and assign them. Usually, these credentials are reused across pods and aren't regularly rotated.

With pod-managed identities (preview) for Azure resources, you automatically request access to services through Azure AD. Pod-managed identities is currently in preview for AKS. Refer to the [Use Azure Active Directory pod-managed identities in Azure Kubernetes Service \(Preview\)](#) documentation to get started.

NOTE

If you have enabled [Azure AD pod-managed identity](#) on your AKS cluster or are considering implementing it, we recommend you first review the [workload identity overview](#) article to understand our recommendations and options to set up your cluster to use an Azure AD workload identity (preview). This authentication method replaces pod-managed identity (preview), which integrates with the Kubernetes native capabilities to federate with any external identity providers.

Azure Active Directory pod-managed identity (preview) supports two modes of operation:

- **Standard** mode: In this mode, the following 2 components are deployed to the AKS cluster:
 - **Managed Identity Controller(MIC)**: A Kubernetes controller that watches for changes to pods, [AzureIdentity](#) and [AzureIdentityBinding](#) through the Kubernetes API Server. When it detects a relevant change, the MIC adds or deletes [AzureAssignedIdentity](#) as needed. Specifically, when a pod is scheduled, the MIC assigns the managed identity on Azure to the underlying virtual machine scale set used by the node pool during the creation phase. When all pods using the identity are deleted, it removes the identity from the virtual machine scale set of the node pool, unless the same managed identity is used by other pods. The MIC takes similar actions when [AzureIdentity](#) or [AzureIdentityBinding](#) are created or deleted.
 - **Node Managed Identity (NMI)**: is a pod that runs as a DaemonSet on each node in the AKS cluster. NMI intercepts security token requests to the [Azure Instance Metadata Service](#) on each node. It redirects requests to itself and validates if the pod has access to the identity it's requesting a token for, and fetch the token from the Azure Active Directory tenant on behalf of the application.
- **Managed** mode: In this mode, there's only NMI. The identity needs to be manually assigned and managed by the user. For more information, see [Pod Identity in Managed Mode](#). In this mode, when you use the `az aks pod-identity add` command to add a pod identity to an Azure Kubernetes Service (AKS) cluster, it creates the [AzureIdentity](#) and [AzureIdentityBinding](#) in the namespace specified by the `--namespace` parameter, while the AKS resource provider assigns the managed identity specified by the `--identity-resource-id` parameter to virtual machine scale set of each node pool in the AKS cluster.

NOTE

If you instead decide to install the Azure Active Directory pod-managed identity using the [AKS cluster add-on](#), setup uses the `managed` mode.

The `managed` mode provides the following advantages over the `standard`:

- Identity assignment on the virtual machine scale set of a node pool can take up 40-60s. With cronjobs or applications that require access to the identity and can't tolerate the assignment delay, it's best to use `managed` mode as the identity is pre-assigned to the virtual machine scale set of the node pool. Either manually or using the `az aks pod-identity add` command.
- In `standard` mode, MIC requires write permissions on the virtual machine scale set used by the AKS cluster and `Managed Identity Operator` permission on the user-assigned managed identities. When running in `managed mode`, since there's no MIC, the role assignments aren't required.

Instead of manually defining credentials for pods, pod-managed identities request an access token in real time, using it to access only their assigned resources. In AKS, there are two components that handle the operations to allow pods to use managed identities:

- **The Node Management Identity (NMI) server** is a pod that runs as a DaemonSet on each node in the AKS cluster. The NMI server listens for pod requests to Azure services.
- **The Azure Resource Provider** queries the Kubernetes API server and checks for an Azure identity mapping that corresponds to a pod.

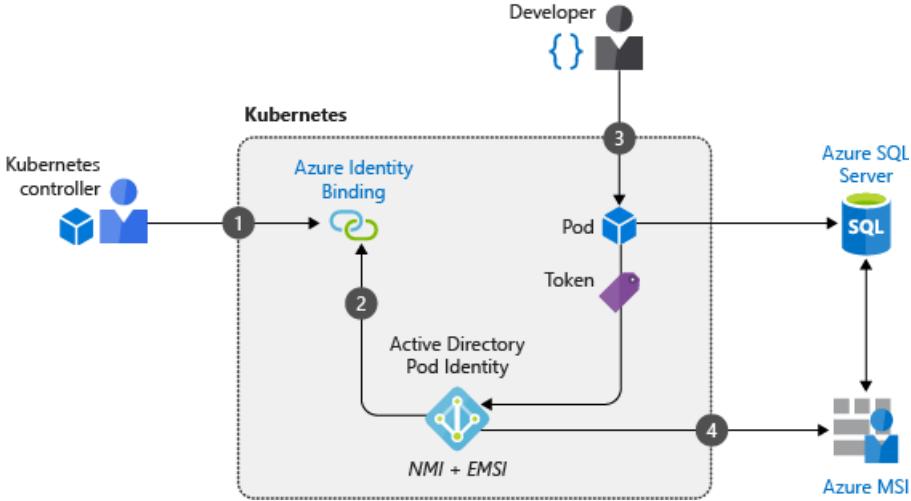
When pods request a security token from Azure Active Directory to access to an Azure resource, network rules redirect the traffic to the NMI server.

1. The NMI server:

- Identifies pods requesting access to Azure resources based on their remote address.

- Queries the Azure Resource Provider.
2. The Azure Resource Provider checks for Azure identity mappings in the AKS cluster.
 3. The NMI server requests an access token from Azure AD based on the pod's identity mapping.
 4. Azure AD provides access to the NMI server, which is returned to the pod.
 - This access token can be used by the pod to then request access to resources in Azure.

In the following example, a developer creates a pod that uses a managed identity to request access to Azure SQL Database:



1. Cluster operator creates a service account to map identities when pods request access to resources.
2. The NMI server is deployed to relay any pod requests, along with the Azure Resource Provider, for access tokens to Azure AD.
3. A developer deploys a pod with a managed identity that requests an access token through the NMI server.
4. The token is returned to the pod and used to access Azure SQL Database

To use Pod-managed identities, see [Use Azure Active Directory pod-managed identities in Azure Kubernetes Service \(preview\)](#).

Next steps

This best practices article focused on authentication and authorization for your cluster and resources. To implement some of these best practices, see the following articles:

- [Integrate Azure Active Directory with AKS](#)
- [Use Azure Active Directory pod-managed identities in Azure Kubernetes Service \(preview\)](#)

For more information about cluster operations in AKS, see the following best practices:

- [Multi-tenancy and cluster isolation](#)
- [Basic Kubernetes scheduler features](#)
- [Advanced Kubernetes scheduler features](#)

Best practices for cluster security and upgrades in Azure Kubernetes Service (AKS)

10/27/2022 • 10 minutes to read • [Edit Online](#)

As you manage clusters in Azure Kubernetes Service (AKS), workload and data security is a key consideration. When you run multi-tenant clusters using logical isolation, you especially need to secure resource and workload access. Minimize the risk of attack by applying the latest Kubernetes and node OS security updates.

This article focuses on how to secure your AKS cluster. You learn how to:

- Use Azure Active Directory and Kubernetes role-based access control (Kubernetes RBAC) to secure API server access.
- Secure container access to node resources.
- Upgrade an AKS cluster to the latest Kubernetes version.
- Keep nodes up to date and automatically apply security patches.

You can also read the best practices for [container image management](#) and for [pod security](#).

Enable threat protection

Best practice guidance

You can enable [Defender for Containers](#) to help secure your containers. Defender for Containers can assess cluster configurations and provide security recommendations, run vulnerability scans, and provide real-time protection and alerting for Kubernetes nodes and clusters.

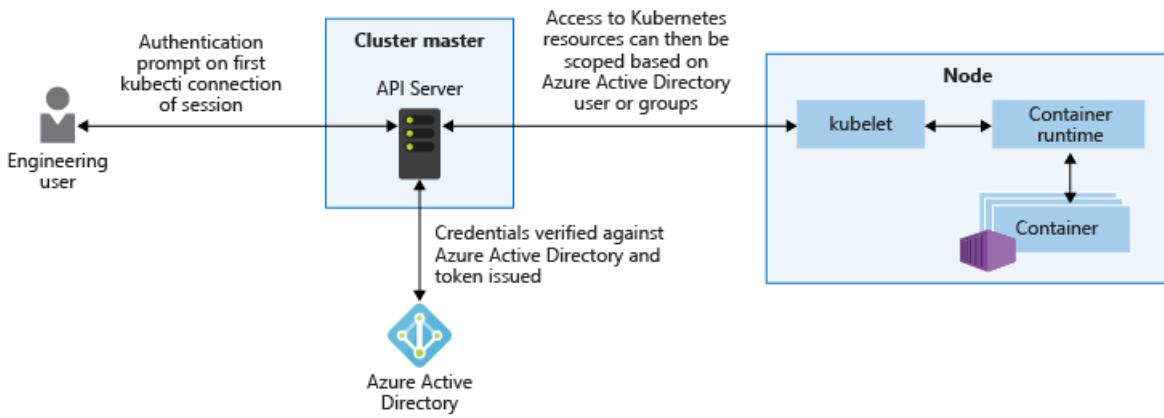
Secure access to the API server and cluster nodes

Best practice guidance

One of the most important ways to secure your cluster is to secure access to the Kubernetes API server. To control access to the API server, integrate Kubernetes RBAC with Azure Active Directory (Azure AD). With these controls, you secure AKS the same way that you secure access to your Azure subscriptions.

The Kubernetes API server provides a single connection point for requests to perform actions within a cluster. To secure and audit access to the API server, limit access and provide the lowest possible permission levels. While this approach isn't unique to Kubernetes, it's especially important when you've logically isolated your AKS cluster for multi-tenant use.

Azure AD provides an enterprise-ready identity management solution that integrates with AKS clusters. Since Kubernetes doesn't provide an identity management solution, you may be hard-pressed to granularly restrict access to the API server. With Azure AD-integrated clusters in AKS, you use your existing user and group accounts to authenticate users to the API server.



Using Kubernetes RBAC and Azure AD-integration, you can secure the API server and provide the minimum permissions required to a scoped resource set, like a single namespace. You can grant different Azure AD users or groups different Kubernetes roles. With granular permissions, you can restrict access to the API server and provide a clear audit trail of actions performed.

The recommended best practice is to use *groups* to provide access to files and folders instead of individual identities. For example, use an Azure AD *group* membership to bind users to Kubernetes roles rather than individual *users*. As a user's group membership changes, their access permissions on the AKS cluster change accordingly.

Meanwhile, let's say you bind the individual user directly to a role and their job function changes. While the Azure AD group memberships update, their permissions on the AKS cluster would not. In this scenario, the user ends up with more permissions than they require.

For more information about Azure AD integration, Kubernetes RBAC, and Azure RBAC, see [Best practices for authentication and authorization in AKS](#).

Restrict access to Instance Metadata API

Best practice guidance

Add a network policy in all user namespaces to block pod egress to the metadata endpoint.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: restrict-instance-metadata
spec:
  podSelector:
    matchLabels: {}
  policyTypes:
  - Egress
  egress:
  - to:
    - ipBlock:
        cidr: 10.10.0.0/0#example
      except:
      - 169.254.169.254/32
```

NOTE

Alternatively you can use [Pod Identity](#) though this is in Public Preview. It has a pod (NMI) that runs as a DaemonSet on each node in the AKS cluster. NMI intercepts security token requests to the Azure Instance Metadata Service on each node, redirect them to itself and validates if the pod has access to the identity it's requesting a token for and fetch the token from the Azure AD tenant on behalf of the application.

Secure container access to resources

Best practice guidance

Limit access to actions that containers can perform. Provide the least number of permissions, and avoid the use of root access or privileged escalation.

In the same way that you should grant users or groups the minimum privileges required, you should also limit containers to only necessary actions and processes. To minimize the risk of attack, avoid configuring applications and containers that require escalated privileges or root access.

For example, set `allowPrivilegeEscalation: false` in the pod manifest. These built-in Kubernetes *pod security contexts* let you define additional permissions, such as the user or group to run as, or the Linux capabilities to expose. For more best practices, see [Secure pod access to resources](#).

For even more granular control of container actions, you can also use built-in Linux security features such as *AppArmor* and *seccomp*.

1. Define Linux security features at the node level.
2. Implement features through a pod manifest.

Built-in Linux security features are only available on Linux nodes and pods.

NOTE

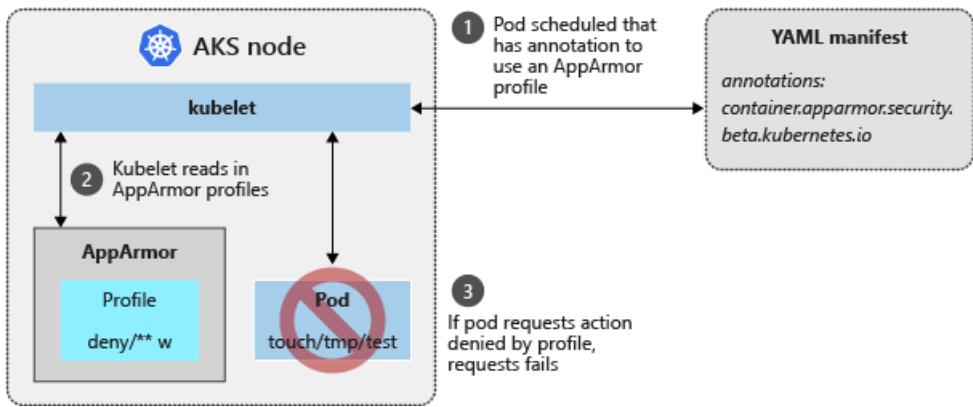
Currently, Kubernetes environments aren't completely safe for hostile multi-tenant usage. Additional security features, like *Microsoft Defender for Containers AppArmor*, *seccomp*, *Pod Security Admission*, or Kubernetes RBAC for nodes, efficiently block exploits.

For true security when running hostile multi-tenant workloads, only trust a hypervisor. The security domain for Kubernetes becomes the entire cluster, not an individual node.

For these types of hostile multi-tenant workloads, you should use physically isolated clusters.

App Armor

To limit container actions, you can use the [AppArmor](#) Linux kernel security module. AppArmor is available as part of the underlying AKS node OS, and is enabled by default. You create AppArmor profiles that restrict read, write, or execute actions, or system functions like mounting filesystems. Default AppArmor profiles restrict access to various `/proc` and `/sys` locations, and provide a means to logically isolate containers from the underlying node. AppArmor works for any application that runs on Linux, not just Kubernetes pods.



To see AppArmor in action, the following example creates a profile that prevents writing to files.

1. [SSH](#) to an AKS node.
2. Create a file named `deny-write.profile`.
3. Copy and paste the following content:

```
#include <tunables/global>
profile k8s-apparmor-example-deny-write flags=(attach_disconnected) {
    #include <abstractions/base>

    file,
    # Deny all file writes.
    deny /** w,
}
```

AppArmor profiles are added using the `apparmor_parser` command.

1. Add the profile to AppArmor.
2. Specify the name of the profile created in the previous step:

```
sudo apparmor_parser deny-write.profile
```

If the profile is correctly parsed and applied to AppArmor, you won't see any output and you'll be returned to the command prompt.

3. From your local machine, create a pod manifest named `aks-apparmor.yaml`. This manifest:
 - Defines an annotation for `container.apparmor.security.beta.kubernetes.io`.
 - References the `deny-write` profile created in the previous steps.

```
apiVersion: v1
kind: Pod
metadata:
  name: hello-apparmor
  annotations:
    container.apparmor.security.beta.kubernetes.io/hello: localhost/k8s-apparmor-example-deny-write
spec:
  containers:
  - name: hello
    image: mcr.microsoft.com/dotnet/runtime-deps:6.0
    command: [ "sh", "-c", "echo 'Hello AppArmor!' && sleep 1h" ]
```

4. With the pod deployed, verify the `hello-apparmor` pod shows a *blocked* status by running the following command:

```
kubectl get pods

NAME        READY   STATUS    RESTARTS   AGE
aks-ssh     1/1     Running   0          4m2s
hello-apparmor 0/1     Blocked   0          50s
```

For more information about AppArmor, see [AppArmor profiles in Kubernetes](#).

Secure computing

While AppArmor works for any Linux application, [seccomp \(secure computing\)](#) works at the process level. Seccomp is also a Linux kernel security module, and is natively supported by the Docker runtime used by AKS nodes. With seccomp, you can limit container process calls. Align to the best practice of granting the container minimal permission only to run by:

- Defining with filters what actions to allow or deny.
- Annotating within a pod YAML manifest to associate with the seccomp filter.

To see seccomp in action, create a filter that prevents changing permissions on a file.

1. [SSH](#) to an AKS node.
2. Create a seccomp filter named `/var/lib/kubelet/seccomp/prevent-chmod`.
3. Copy and paste the following content:

```
{
  "defaultAction": "SCMP_ACT_ALLOW",
  "syscalls": [
    {
      "name": "chmod",
      "action": "SCMP_ACT_ERRNO"
    },
    {
      "name": "fchmodat",
      "action": "SCMP_ACT_ERRNO"
    },
    {
      "name": "chmodat",
      "action": "SCMP_ACT_ERRNO"
    }
  ]
}
```

In version 1.19 and later, you need to configure the following:

```
{
  "defaultAction": "SCMP_ACT_ALLOW",
  "syscalls": [
    {
      "names": ["chmod","fchmodat","chmodat"],
      "action": "SCMP_ACT_ERRNO"
    }
  ]
}
```

4. From your local machine, create a pod manifest named `aks-seccomp.yaml` and paste the following content. This manifest:

- Defines an annotation for `seccomp.security.alpha.kubernetes.io`.

- References the `prevent-chmod` filter created in the previous step.

```
apiVersion: v1
kind: Pod
metadata:
  name: chmod-prevented
  annotations:
    seccomp.security.alpha.kubernetes.io/pod: localhost/prevent-chmod
spec:
  containers:
    - name: chmod
      image: mcr.microsoft.com/dotnet/runtime-deps:6.0
      command:
        - "chmod"
      args:
        - "777"
        - /etc/hostname
  restartPolicy: Never
```

In version 1.19 and later, you need to configure the following:

```
apiVersion: v1
kind: Pod
metadata:
  name: chmod-prevented
spec:
  securityContext:
    seccompProfile:
      type: Localhost
      localhostProfile: prevent-chmod
  containers:
    - name: chmod
      image: mcr.microsoft.com/dotnet/runtime-deps:6.0
      command:
        - "chmod"
      args:
        - "777"
        - /etc/hostname
  restartPolicy: Never
```

5. Deploy the sample pod using the [kubectl apply](#) command:

```
kubectl apply -f ./aks-seccomp.yaml
```

6. View pod status using the [kubectl get pods](#) command.

- The pod reports an error.
- The `chmod` command is prevented from running by the seccomp filter, as shown in the following example output:

kubectl get pods				
NAME	READY	STATUS	RESTARTS	AGE
chmod-prevented	0/1	Error	0	7s

For more information about available filters, see [Seccomp security profiles for Docker](#).

Regularly update to the latest version of Kubernetes

Best practice guidance

To stay current on new features and bug fixes, regularly upgrade the Kubernetes version in your AKS cluster.

Kubernetes releases new features at a quicker pace than more traditional infrastructure platforms. Kubernetes updates include:

- New features
- Bug or security fixes

New features typically move through *alpha* and *beta* status before they become *stable*. Once stable, are generally available and recommended for production use. Kubernetes new feature release cycle allows you to update Kubernetes without regularly encountering breaking changes or adjusting your deployments and templates.

AKS supports three minor versions of Kubernetes. Once a new minor patch version is introduced, the oldest minor version and patch releases supported are retired. Minor Kubernetes updates happen on a periodic basis. To stay within support, ensure you have a governance process to check for necessary upgrades. For more information, see [Supported Kubernetes versions AKS](#).

- [Azure CLI](#)
- [Azure PowerShell](#)

To check the versions that are available for your cluster, use the `az aks get-upgrades` command as shown in the following example:

```
az aks get-upgrades --resource-group myResourceGroup --name myAKSCluster --output table
```

You can then upgrade your AKS cluster using the `az aks upgrade` command. The upgrade process safely:

- Cordons and drains one node at a time.
- Schedules pods on remaining nodes.
- Deploys a new node running the latest OS and Kubernetes versions.

IMPORTANT

Test new minor versions in a dev/test environment and validate that your workload remains healthy with the new Kubernetes version.

Kubernetes may deprecate APIs (like in version 1.16) that your workloads rely on. When bringing new versions into production, consider using [multiple node pools on separate versions](#) and upgrade individual pools one at a time to progressively roll the update across a cluster. If running multiple clusters, upgrade one cluster at a time to progressively monitor for impact or changes.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
az aks upgrade --resource-group myResourceGroup --name myAKSCluster --kubernetes-version  
KUBERNETES_VERSION
```

For more information about upgrades in AKS, see [Supported Kubernetes versions in AKS](#) and [Upgrade an AKS cluster](#).

Process Linux node updates

Each evening, Linux nodes in AKS get security patches through their distro update channel. This behavior is automatically configured as the nodes are deployed in an AKS cluster. To minimize disruption and potential impact to running workloads, nodes are not automatically rebooted if a security patch or kernel update requires it. For more information about how to handle node reboots, see [Apply security and kernel updates to nodes in AKS](#).

Node image upgrades

Unattended upgrades apply updates to the Linux node OS, but the image used to create nodes for your cluster remains unchanged. If a new Linux node is added to your cluster, the original image is used to create the node. This new node will receive all the security and kernel updates available during the automatic check every night but will remain unpatched until all checks and restarts are complete. You can use node image upgrade to check for and update node images used by your cluster. For more information on node image upgrade, see [Azure Kubernetes Service \(AKS\) node image upgrade](#).

Process Windows Server node updates

For Windows Server nodes, regularly perform a node image upgrade operation to safely cordon and drain pods and deploy updated nodes.

Best practices for container image management and security in Azure Kubernetes Service (AKS)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Container and container image security is a major priority while you develop and run applications in Azure Kubernetes Service (AKS). Containers with outdated base images or unpatched application runtimes introduce a security risk and possible attack vector.

Minimize risks by integrating and running scan and remediation tools in your containers at build and runtime. The earlier you catch the vulnerability or outdated base image, the more secure your cluster.

In this article, "*containers*" means both:

- The container images stored in a container registry.
- The running containers.

This article focuses on how to secure your containers in AKS. You learn how to:

- Scan for and remediate image vulnerabilities.
- Automatically trigger and redeploy container images when a base image is updated.

You can also read the best practices for [cluster security](#) and for [pod security](#).

You can also use [Container security in Defender for Cloud](#) to help scan your containers for vulnerabilities. [Azure Container Registry integration](#) with Defender for Cloud helps protect your images and registry from vulnerabilities.

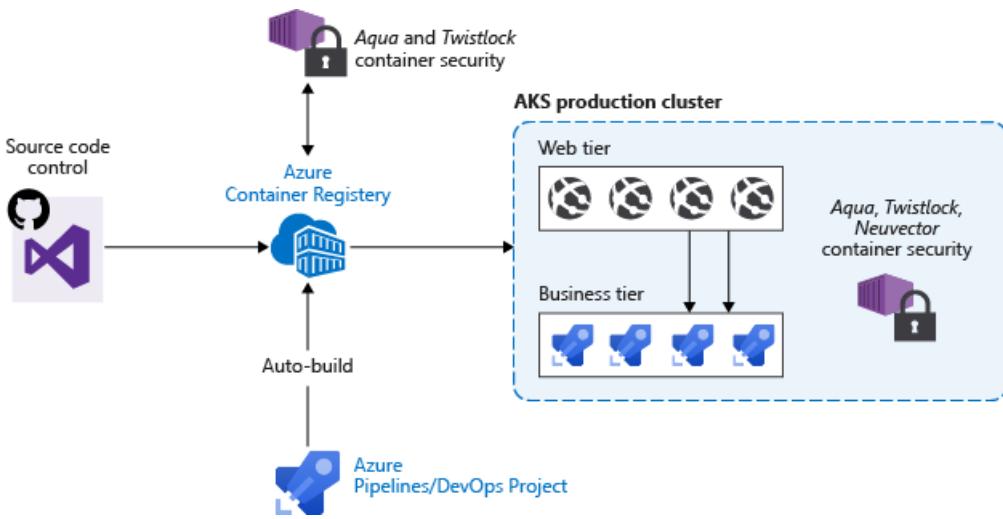
Secure the images and run time

Best practice guidance

Scan your container images for vulnerabilities. Only deploy validated images. Regularly update the base images and application runtime. Redeploy workloads in the AKS cluster.

When adopting container-based workloads, you'll want to verify the security of images and runtime used to build your own applications. How do you avoid introducing security vulnerabilities into your deployments?

- Include in your deployment workflow a process to scan container images using tools such as [Twistlock](#) or [Aqua](#).
- Only allow verified images to be deployed.



For example, you can use a continuous integration and continuous deployment (CI/CD) pipeline to automate the image scans, verification, and deployments. Azure Container Registry includes these vulnerabilities scanning capabilities.

Automatically build new images on base image update

Best practice guidance

As you use base images for application images, use automation to build new images when the base image is updated. Since updated base images typically include security fixes, update any downstream application container images.

Each time a base image is updated, you should also update any downstream container images. Integrate this build process into validation and deployment pipelines such as [Azure Pipelines](#) or Jenkins. These pipelines make sure that your applications continue to run on the updated based images. Once your application container images are validated, the AKS deployments can then be updated to run the latest, secure images.

Azure Container Registry Tasks can also automatically update container images when the base image is updated. With this feature, you build a few base images and keep them updated with bug and security fixes.

For more information about base image updates, see [Automate image builds on base image update with Azure Container Registry Tasks](#).

Next steps

This article focused on how to secure your containers. To implement some of these areas, see the following articles:

- [Automate image builds on base image update with Azure Container Registry Tasks](#)

Best practices for cluster isolation in Azure Kubernetes Service (AKS)

10/27/2022 • 3 minutes to read • [Edit Online](#)

As you manage clusters in Azure Kubernetes Service (AKS), you often need to isolate teams and workloads. AKS provides flexibility in how you can run multi-tenant clusters and isolate resources. To maximize your investment in Kubernetes, first understand and implement AKS multi-tenancy and isolation features.

This best practices article focuses on isolation for cluster operators. In this article, you learn how to:

- Plan for multi-tenant clusters and separation of resources
- Use logical or physical isolation in your AKS clusters

Design clusters for multi-tenancy

Kubernetes lets you logically isolate teams and workloads in the same cluster. The goal is to provide the least number of privileges, scoped to the resources each team needs. A Kubernetes [Namespace](#) creates a logical isolation boundary. Additional Kubernetes features and considerations for isolation and multi-tenancy include the following areas:

Scheduling

Scheduling uses basic features such as resource quotas and pod disruption budgets. For more information about these features, see [Best practices for basic scheduler features in AKS](#).

More advanced scheduler features include:

- Taints and tolerations
- Node selectors
- Node and pod affinity or anti-affinity.

For more information about these features, see [Best practices for advanced scheduler features in AKS](#).

Networking

Networking uses network policies to control the flow of traffic in and out of pods.

Authentication and authorization

Authentication and authorization uses:

- Role-based access control (RBAC)
- Azure Active Directory (AD) integration
- Pod identities
- Secrets in Azure Key Vault

For more information about these features, see [Best practices for authentication and authorization in AKS](#).

Containers

Containers include:

- The Azure Policy Add-on for AKS to enforce pod security.
- The use of pod security admission.
- Scanning both images and the runtime for vulnerabilities.

- Using App Armor or Seccomp (Secure Computing) to restrict container access to the underlying node.

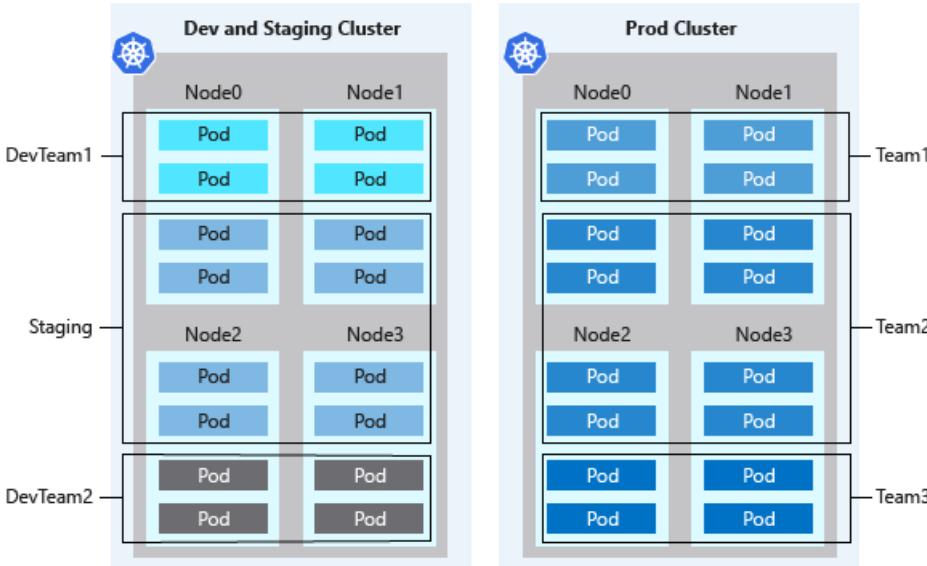
Logically isolate clusters

Best practice guidance

Separate teams and projects using *logical isolation*. Minimize the number of physical AKS clusters you deploy to isolate teams or applications.

With logical isolation, a single AKS cluster can be used for multiple workloads, teams, or environments.

Kubernetes [Namespaces](#) form the logical isolation boundary for workloads and resources.



Logical separation of clusters usually provides a higher pod density than physically isolated clusters, with less excess compute capacity sitting idle in the cluster. When combined with the Kubernetes cluster autoscaler, you can scale the number of nodes up or down to meet demands. This best practice approach to autoscaling minimizes costs by running only the number of nodes required.

Currently, Kubernetes environments aren't completely safe for hostile multi-tenant usage. In a multi-tenant environment, multiple tenants are working on a common, shared infrastructure. If all tenants cannot be trusted, you will need extra planning to prevent tenants from impacting the security and service of others.

Additional security features, like Kubernetes RBAC for nodes, efficiently block exploits. For true security when running hostile multi-tenant workloads, you should only trust a hypervisor. The security domain for Kubernetes becomes the entire cluster, not an individual node.

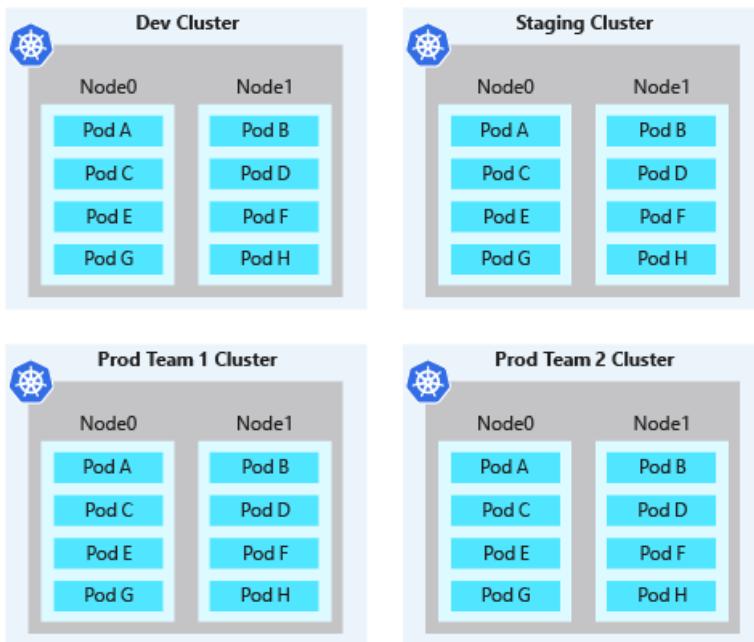
For these types of hostile multi-tenant workloads, you should use physically isolated clusters.

Physically isolate clusters

Best practice guidance

Minimize the use of physical isolation for each separate team or application deployment. Instead, use *logical* isolation, as discussed in the previous section.

Physically separating AKS clusters is a common approach to cluster isolation. In this isolation model, teams or workloads are assigned their own AKS cluster. While physical isolation might look like the easiest way to isolate workloads or teams, it adds management and financial overhead. Now, you must maintain these multiple clusters and individually provide access and assign permissions. You'll also be billed for each the individual node.



Physically separate clusters usually have a low pod density. Since each team or workload has their own AKS cluster, the cluster is often over-provisioned with compute resources. Often, a small number of pods are scheduled on those nodes. Unclaimed node capacity can't be used for applications or services in development by other teams. These excess resources contribute to the additional costs in physically separate clusters.

Next steps

This article focused on cluster isolation. For more information about cluster operations in AKS, see the following best practices:

- [Basic Kubernetes scheduler features](#)
- [Advanced Kubernetes scheduler features](#)
- [Authentication and authorization](#)

Best practices for basic scheduler features in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

As you manage clusters in Azure Kubernetes Service (AKS), you often need to isolate teams and workloads. The Kubernetes scheduler lets you control the distribution of compute resources, or limit the impact of maintenance events.

This best practices article focuses on basic Kubernetes scheduling features for cluster operators. In this article, you learn how to:

- Use resource quotas to provide a fixed amount of resources to teams or workloads
- Limit the impact of scheduled maintenance using pod disruption budgets

Enforce resource quotas

Best practice guidance

Plan and apply resource quotas at the namespace level. If pods don't define resource requests and limits, reject the deployment. Monitor resource usage and adjust quotas as needed.

Resource requests and limits are placed in the pod specification. Limits are used by the Kubernetes scheduler at deployment time to find an available node in the cluster. Limits and requests work at the individual pod level. For more information about how to define these values, see [Define pod resource requests and limits](#)

To provide a way to reserve and limit resources across a development team or project, you should use *resource quotas*. These quotas are defined on a namespace, and can be used to set quotas on the following basis:

- **Compute resources**, such as CPU and memory, or GPUs.
- **Storage resources**, including the total number of volumes or amount of disk space for a given storage class.
- **Object count**, such as maximum number of secrets, services, or jobs can be created.

Kubernetes doesn't overcommit resources. Once your cumulative resource request total passes the assigned quota, all further deployments will be unsuccessful.

When you define resource quotas, all pods created in the namespace must provide limits or requests in their pod specifications. If they don't provide these values, you can reject the deployment. Instead, you can [configure default requests and limits for a namespace](#).

The following example YAML manifest named *dev-app-team-quotas.yaml* sets a hard limit of a total of 10 CPUs, 20Gi of memory, and 10 pods:

```
apiVersion: v1
kind: ResourceQuota
metadata:
  name: dev-app-team
spec:
  hard:
    cpu: "10"
    memory: 20Gi
    pods: "10"
```

This resource quota can be applied by specifying the namespace, such as *dev-apps*:

```
kubectl apply -f dev-app-team-quotas.yaml --namespace dev-apps
```

Work with your application developers and owners to understand their needs and apply the appropriate resource quotas.

For more information about available resource objects, scopes, and priorities, see [Resource quotas in Kubernetes](#).

Plan for availability using pod disruption budgets

Best practice guidance

To maintain the availability of applications, define Pod Disruption Budgets (PDBs) to make sure that a minimum number of pods are available in the cluster.

There are two disruptive events that cause pods to be removed:

Involuntary disruptions

Involuntary disruptions are events beyond the typical control of the cluster operator or application owner. Include:

- Hardware failure on the physical machine
- Kernel panic
- Deletion of a node VM

Involuntary disruptions can be mitigated by:

- Using multiple replicas of your pods in a deployment.
- Running multiple nodes in the AKS cluster.

Voluntary disruptions

Voluntary disruptions are events requested by the cluster operator or application owner. Include:

- Cluster upgrades
- Updated deployment template
- Accidentally deleting a pod

Kubernetes provides *pod disruption budgets* for voluntary disruptions, letting you plan for how deployments or replica sets respond when a voluntary disruption event occurs. Using pod disruption budgets, cluster operators can define a minimum available or maximum unavailable resource count.

If you upgrade a cluster or update a deployment template, the Kubernetes scheduler will schedule extra pods on other nodes before allowing voluntary disruption events to continue. The scheduler waits to reboot a node until

the defined number of pods are successfully scheduled on other nodes in the cluster.

Let's look at an example of a replica set with five pods that run NGINX. The pods in the replica set are assigned the label `app: nginx-frontend`. During a voluntary disruption event, such as a cluster upgrade, you want to make sure at least three pods continue to run. The following YAML manifest for a `PodDisruptionBudget` object defines these requirements:

```
apiVersion: policy/v1
kind: PodDisruptionBudget
metadata:
  name: nginx-pdb
spec:
  minAvailable: 3
  selector:
    matchLabels:
      app: nginx-frontend
```

You can also define a percentage, such as `60%`, which allows you to automatically compensate for the replica set scaling up the number of pods.

You can define a maximum number of unavailable instances in a replica set. Again, a percentage for the maximum unavailable pods can also be defined. The following pod disruption budget YAML manifest defines that no more than two pods in the replica set be unavailable:

```
apiVersion: policy/v1
kind: PodDisruptionBudget
metadata:
  name: nginx-pdb
spec:
  maxUnavailable: 2
  selector:
    matchLabels:
      app: nginx-frontend
```

Once your pod disruption budget is defined, you create it in your AKS cluster as with any other Kubernetes object:

```
kubectl apply -f nginx-pdb.yaml
```

Work with your application developers and owners to understand their needs and apply the appropriate pod disruption budgets.

For more information about using pod disruption budgets, see [Specify a disruption budget for your application](#).

Next steps

This article focused on basic Kubernetes scheduler features. For more information about cluster operations in AKS, see the following best practices:

- [Multi-tenancy and cluster isolation](#)
- [Advanced Kubernetes scheduler features](#)
- [Authentication and authorization](#)

Best practices for creating and running Azure Kubernetes Service (AKS) clusters at scale

10/27/2022 • 3 minutes to read • [Edit Online](#)

AKS clusters that satisfy any of the below criteria should use the [Uptime SLA](#) feature for higher reliability and scalability of the Kubernetes control plane:

- Clusters running greater than 10 nodes on average
- Clusters that need to scale beyond 1000 nodes
- Clusters running production workloads or availability sensitive mission critical workloads

To scale AKS clusters beyond 1000 nodes, you need to request a node limit quota increase by raising a support ticket via the [portal](#) up-to a maximum of 5000 nodes per cluster.

To increase the node limit beyond 1000, you must have the following pre-requisites:

- An existing AKS cluster that needs the node limit increase. This cluster shouldn't be deleted as that will remove the limit increase.
- Uptime SLA enabled on your cluster.
- Clusters should use Kubernetes version 1.23 or above

NOTE

It may take up to a week to enable your clusters with the larger node limit.

IMPORTANT

Raising the node limit does not increase other AKS service quota limits, such as the number of pods per node. For more details, [Limits for resources, SKUs, regions](#).

Networking considerations and best practices

- Use Managed NAT for cluster egress with at least 2 public IPs on the NAT Gateway. For more information, see [Managed NAT Gateway - Azure Kubernetes Service](#).
- Use Azure CNI with Dynamic IP allocation for optimum IP utilization and scale up to 50k application pods per cluster with one routable IP per pod. For more information, see [Configure Azure CNI networking in Azure Kubernetes Service \(AKS\)](#).
- When using internal Kubernetes services behind an internal load balancer, it's recommended to create an internal load balancer or internal service below 750 node scale for best scaling performance and load balancer elasticity.

NOTE

You can't use NPM with clusters greater than 500 Nodes

Node pool scaling considerations and best practices

- For system node pools, use the *Standard_D16ds_v5* SKU or equivalent core/memory VM SKUs with ephemeral OS disks to provide sufficient compute resources for *kube-system* pods.
- Create at-least five user node pools to scale up to 5,000 nodes since there's a 1000 nodes per node pool limit.
- Use cluster autoscaler wherever possible when running at-scale AKS clusters to ensure dynamic scaling of node pools based on the demand for compute resources.
- When scaling beyond 1000 nodes without cluster autoscaler, it's recommended to scale in batches of a maximum 500 to 700 nodes at a time. These scaling operations should also have 2 mins to 5-mins sleep time between consecutive scale-ups to prevent Azure API throttling.

NOTE

You can't use [Stop and Start feature](#) on clusters enabled with the greater than 1000 node limit

Cluster upgrade best practices

- AKS clusters have a hard limit of 5000 nodes. This limit prevents clusters from upgrading that are running at this limit since there's no more capacity do a rolling update with the max surge property. We recommend scaling the cluster down below 3000 nodes before doing cluster upgrades to provide extra capacity for node churn and minimize control plane load.
- By default, AKS configures upgrades to surge with one extra node through the max surge settings. This default value allows AKS to minimize workload disruption by creating an extra node before the cordon/drain of existing applications to replace an older versioned node. When you are upgrading clusters with a large number of nodes, using the default max surge settings can force an upgrade to take several hours to complete as the upgrade churns through a large number of nodes. You can customize the max surge settings per node pool to enable a trade-off between upgrade speed and upgrade disruption. By increasing the max surge settings, the upgrade process completes faster but may cause disruptions during the upgrade process.
- It isn't recommended to upgrade a cluster with greater than 500 nodes with the default max-surge configuration of one node. We suggest increasing the max surge settings to between 10 to 20 percent with up to a maximum of 500 nodes max-surge based on your workload disruption tolerance.
- For more information, see [Upgrade an Azure Kubernetes Service \(AKS\) cluster](#).

Best practices for advanced scheduler features in Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

As you manage clusters in Azure Kubernetes Service (AKS), you often need to isolate teams and workloads. Advanced features provided by the Kubernetes scheduler let you control:

- Which pods can be scheduled on certain nodes.
- How multi-pod applications can be appropriately distributed across the cluster.

This best practices article focuses on advanced Kubernetes scheduling features for cluster operators. In this article, you learn how to:

- Use taints and tolerations to limit what pods can be scheduled on nodes.
- Give preference to pods to run on certain nodes with node selectors or node affinity.
- Split apart or group together pods with inter-pod affinity or anti-affinity.

Provide dedicated nodes using taints and tolerations

Best practice guidance:

Limit access for resource-intensive applications, such as ingress controllers, to specific nodes. Keep node resources available for workloads that require them, and don't allow scheduling of other workloads on the nodes.

When you create your AKS cluster, you can deploy nodes with GPU support or a large number of powerful CPUs. You can use these nodes for large data processing workloads such as machine learning (ML) or artificial intelligence (AI).

Since this node resource hardware is typically expensive to deploy, limit the workloads that can be scheduled on these nodes. Instead, you'd dedicate some nodes in the cluster to run ingress services and prevent other workloads.

This support for different nodes is provided by using multiple node pools. An AKS cluster provides one or more node pools.

The Kubernetes scheduler uses taints and tolerations to restrict what workloads can run on nodes.

- Apply a **taint** to a node to indicate only specific pods can be scheduled on them.
- Then apply a **toleration** to a pod, allowing them to *tolerate* a node's taint.

When you deploy a pod to an AKS cluster, Kubernetes only schedules pods on nodes whose taint aligns with the toleration. For example, assume you added a node pool in your AKS cluster for nodes with GPU support. You define name, such as *gpu*, then a value for scheduling. Setting this value to *NoSchedule* restricts the Kubernetes scheduler from scheduling pods with undefined toleration on the node.

```
az aks nodepool add \
    --resource-group myResourceGroup \
    --cluster-name myAKSCluster \
    --name taintnp \
    --node-taints sku=gpu:NoSchedule \
    --no-wait
```

With a taint applied to nodes in the node pool, you'll define a toleration in the pod specification that allows scheduling on the nodes. The following example defines the `sku: gpu` and `effect: NoSchedule` to tolerate the taint applied to the node pool in the previous step:

```
kind: Pod
apiVersion: v1
metadata:
  name: tf-mnist
spec:
  containers:
  - name: tf-mnist
    image: mcr.microsoft.com/azuredocs/samples-tf-mnist-demo:gpu
    resources:
      requests:
        cpu: 0.5
        memory: 2Gi
      limits:
        cpu: 4.0
        memory: 16Gi
    tolerations:
    - key: "sku"
      operator: "Equal"
      value: "gpu"
      effect: "NoSchedule"
```

When this pod is deployed using `kubectl apply -f gpu-toleration.yaml`, Kubernetes can successfully schedule the pod on the nodes with the taint applied. This logical isolation lets you control access to resources within a cluster.

When you apply taints, work with your application developers and owners to allow them to define the required tolerations in their deployments.

For more information about how to use multiple node pools in AKS, see [Create and manage multiple node pools for a cluster in AKS](#).

Behavior of taints and tolerations in AKS

When you upgrade a node pool in AKS, taints and tolerations follow a set pattern as they're applied to new nodes:

Default clusters that use VM scale sets

You can [taint a node pool](#) from the AKS API to have newly scaled out nodes receive API specified node taints.

Let's assume:

1. You begin with a two-node cluster: `node1` and `node2`.
2. You upgrade the node pool.
3. Two additional nodes are created: `node3` and `node4`.
4. The taints are passed on respectively.
5. The original `node1` and `node2` are deleted.

Clusters without VM scale set support

Again, let's assume:

1. You have a two-node cluster: *node1* and *node2*.
2. You upgrade then node pool.
3. An additional node is created: *node3*.
4. The taints from *node1* are applied to *node3*.
5. *node1* is deleted.
6. A new *node1* is created to replace to original *node1*.
7. The *node2* taints are applied to the new *node1*.
8. *node2* is deleted.

In essence *node1* becomes *node3*, and *node2* becomes the new *node1*.

When you scale a node pool in AKS, taints and tolerations do not carry over by design.

Control pod scheduling using node selectors and affinity

Best practice guidance

Control the scheduling of pods on nodes using node selectors, node affinity, or inter-pod affinity. These settings allow the Kubernetes scheduler to logically isolate workloads, such as by hardware in the node.

Taints and tolerations logically isolate resources with a hard cut-off. If the pod doesn't tolerate a node's taint, it isn't scheduled on the node.

Alternatively, you can use node selectors. For example, you label nodes to indicate locally attached SSD storage or a large amount of memory, and then define in the pod specification a node selector. Kubernetes schedules those pods on a matching node.

Unlike tolerations, pods without a matching node selector can still be scheduled on labeled nodes. This behavior allows unused resources on the nodes to consume, but prioritizes pods that define the matching node selector.

Let's look at an example of nodes with a high amount of memory. These nodes prioritize pods that request a high amount of memory. To ensure the resources don't sit idle, they also allow other pods to run. The follow example command adds a node pool with the label *hardware=highmem* to the *myAKSCluster* in the *myResourceGroup*. All nodes in that node pool will have this label.

```
az aks nodepool add \
    --resource-group myResourceGroup \
    --cluster-name myAKSCluster \
    --name labelnp \
    --node-count 1 \
    --labels hardware=highmem \
    --no-wait
```

A pod specification then adds the `nodeSelector` property to define a node selector that matches the label set on a node:

```

kind: Pod
apiVersion: v1
metadata:
  name: tf-mnist
spec:
  containers:
    - name: tf-mnist
      image: mcr.microsoft.com/azuredocs/samples-tf-mnist-demo:gpu
      resources:
        requests:
          cpu: 0.5
          memory: 2Gi
        limits:
          cpu: 4.0
          memory: 16Gi
  nodeSelector:
    hardware: highmem

```

When you use these scheduler options, work with your application developers and owners to allow them to correctly define their pod specifications.

For more information about using node selectors, see [Assigning Pods to Nodes](#).

Node affinity

A node selector is a basic solution for assigning pods to a given node. *Node affinity* provides more flexibility, allowing you to define what happens if the pod can't be matched with a node. You can:

- *Require* that Kubernetes scheduler matches a pod with a labeled host. Or,
- *Prefer* a match but allow the pod to be scheduled on a different host if no match is available.

The following example sets the node affinity to *requiredDuringSchedulingIgnoredDuringExecution*. This affinity requires the Kubernetes schedule to use a node with a matching label. If no node is available, the pod has to wait for scheduling to continue. To allow the pod to be scheduled on a different node, you can instead set the value to *preferredDuringSchedulingIgnoreDuringExecution*.

```

kind: Pod
apiVersion: v1
metadata:
  name: tf-mnist
spec:
  containers:
    - name: tf-mnist
      image: mcr.microsoft.com/azuredocs/samples-tf-mnist-demo:gpu
      resources:
        requests:
          cpu: 0.5
          memory: 2Gi
        limits:
          cpu: 4.0
          memory: 16Gi
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
          - matchExpressions:
              - key: hardware
                operator: In
                values: highmem

```

The *IgnoredDuringExecution* part of the setting indicates that the pod shouldn't be evicted from the node if the node labels change. The Kubernetes scheduler only uses the updated node labels for new pods being scheduled,

not pods already scheduled on the nodes.

For more information, see [Affinity and anti-affinity](#).

Inter-pod affinity and anti-affinity

One final approach for the Kubernetes scheduler to logically isolate workloads is using inter-pod affinity or anti-affinity. These settings define that pods either *shouldn't* or *should* be scheduled on a node that has an existing matching pod. By default, the Kubernetes scheduler tries to schedule multiple pods in a replica set across nodes. You can define more specific rules around this behavior.

For example, you have a web application that also uses an Azure Cache for Redis.

1. You use pod anti-affinity rules to request that the Kubernetes scheduler distributes replicas across nodes.
2. You use affinity rules to ensure each web app component is scheduled on the same host as a corresponding cache.

The distribution of pods across nodes looks like the following example:

NODE 1	NODE 2	NODE 3
webapp-1	webapp-2	webapp-3
cache-1	cache-2	cache-3

Inter-pod affinity and anti-affinity provide a more complex deployment than node selectors or node affinity. With the deployment, you logically isolate resources and control how Kubernetes schedules pods on nodes.

For a complete example of this web application with Azure Cache for Redis example, see [Co-locate pods on the same node](#).

Next steps

This article focused on advanced Kubernetes scheduler features. For more information about cluster operations in AKS, see the following best practices:

- [Multi-tenancy and cluster isolation](#)
- [Basic Kubernetes scheduler features](#)
- [Authentication and authorization](#)

Best practices for network connectivity and security in Azure Kubernetes Service (AKS)

10/27/2022 • 10 minutes to read • [Edit Online](#)

As you create and manage clusters in Azure Kubernetes Service (AKS), you provide network connectivity for your nodes and applications. These network resources include IP address ranges, load balancers, and ingress controllers. To maintain a high quality of service for your applications, you need to strategize and configure these resources.

This best practices article focuses on network connectivity and security for cluster operators. In this article, you learn how to:

- Compare the kubenet and Azure Container Networking Interface (CNI) network modes in AKS.
- Plan for required IP addressing and connectivity.
- Distribute traffic using load balancers, ingress controllers, or a web application firewall (WAF).
- Securely connect to cluster nodes.

Choose the appropriate network model

Best practice guidance

Use Azure CNI networking in AKS for integration with existing virtual networks or on-premises networks. This network model allows greater separation of resources and controls in an enterprise environment.

Virtual networks provide the basic connectivity for AKS nodes and customers to access your applications. There are two different ways to deploy AKS clusters into virtual networks:

- **Azure CNI networking**

Deploys into a virtual network and uses the [Azure CNI](#) Kubernetes plugin. Pods receive individual IPs that can route to other network services or on-premises resources.

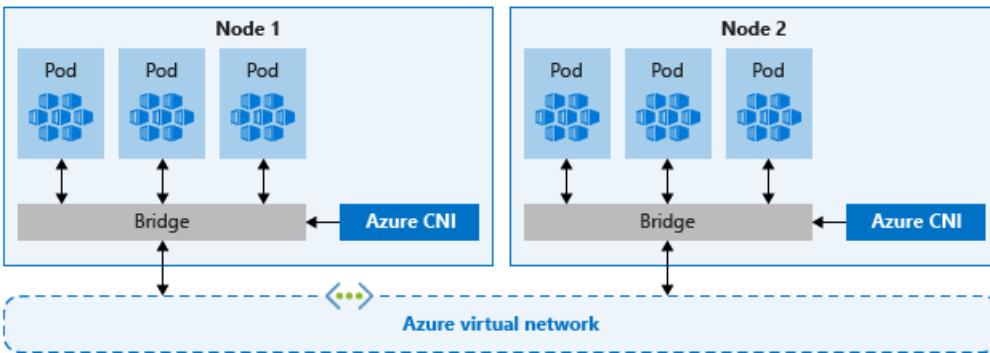
- **Kubenet networking**

Azure manages the virtual network resources as the cluster is deployed and uses the [kubenet](#) Kubernetes plugin.

For production deployments, both kubenet and Azure CNI are valid options.

CNI Networking

Azure CNI is a vendor-neutral protocol that lets the container runtime make requests to a network provider. It assigns IP addresses to pods and nodes, and provides IP address management (IPAM) features as you connect to existing Azure virtual networks. Each node and pod resource receives an IP address in the Azure virtual network - no need for extra routing to communicate with other resources or services.



Notably, Azure CNI networking for production allows for separation of control and management of resources. From a security perspective, you often want different teams to manage and secure those resources. With Azure CNI networking, you connect to existing Azure resources, on-premises resources, or other services directly via IP addresses assigned to each pod.

When you use Azure CNI networking, the virtual network resource is in a separate resource group to the AKS cluster. Delegate permissions for the AKS cluster identity to access and manage these resources. The cluster identity used by the AKS cluster must have at least [Network Contributor](#) permissions on the subnet within your virtual network.

If you wish to define a [custom role](#) instead of using the built-in Network Contributor role, the following permissions are required:

- `Microsoft.Network/virtualNetworks/subnets/join/action`
- `Microsoft.Network/virtualNetworks/subnets/read`

By default, AKS uses a managed identity for its cluster identity. However, you are able to use a service principal instead. For more information about:

- AKS service principal delegation, see [Delegate access to other Azure resources](#).
- Managed identities, see [Use managed identities](#).

As each node and pod receives its own IP address, plan out the address ranges for the AKS subnets. Keep in mind:

- The subnet must be large enough to provide IP addresses for every node, pods, and network resource that you deploy.
 - With both kubenet and Azure CNI networking, each node running has default limits to the number of pods.
- Each AKS cluster must be placed in its own subnet.
- Avoid using IP address ranges that overlap with existing network resources.
 - Necessary to allow connectivity to on-premises or peered networks in Azure.
- To handle scale out events or cluster upgrades, you need extra IP addresses available in the assigned subnet.
 - This extra address space is especially important if you use Windows Server containers, as those node pools require an upgrade to apply the latest security patches. For more information on Windows Server nodes, see [Upgrade a node pool in AKS](#).

To calculate the IP address required, see [Configure Azure CNI networking in AKS](#).

When creating a cluster with Azure CNI networking, you specify other address ranges for the cluster, such as the Docker bridge address, DNS service IP, and service address range. In general, make sure these address ranges:

- Don't overlap each other.
- Don't overlap with any networks associated with the cluster, including any virtual networks, subnets, on-premises and peered networks.

For the specific details around limits and sizing for these address ranges, see [Configure Azure CNI networking in AKS](#).

Kubenet networking

Although kubenet doesn't require you to set up the virtual networks before the cluster is deployed, there are disadvantages to waiting:

- Since nodes and pods are placed on different IP subnets, User Defined Routing (UDR) and IP forwarding routes traffic between pods and nodes. This extra routing may reduce network performance.
- Connections to existing on-premises networks or peering to other Azure virtual networks can be complex.

Since you don't create the virtual network and subnets separately from the AKS cluster, Kubenet is ideal for:

- Small development or test workloads.
- Simple websites with low traffic.
- Lifting and shifting workloads into containers.

For most production deployments, you should plan for and use Azure CNI networking.

You can also [configure your own IP address ranges and virtual networks using kubenet](#). Like Azure CNI networking, these address ranges shouldn't overlap each other and shouldn't overlap with any networks associated with the cluster (virtual networks, subnets, on-premises and peered networks).

For the specific details around limits and sizing for these address ranges, see [Use kubenet networking with your own IP address ranges in AKS](#).

Distribute ingress traffic

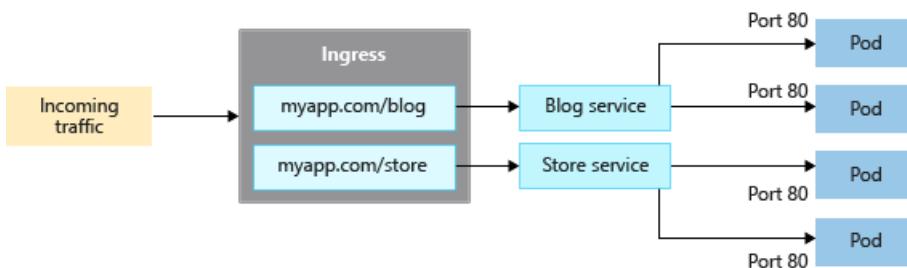
Best practice guidance

To distribute HTTP or HTTPS traffic to your applications, use ingress resources and controllers. Compared to an Azure load balancer, ingress controllers provide extra features and can be managed as native Kubernetes resources.

While an Azure load balancer can distribute customer traffic to applications in your AKS cluster, it's limited in understanding that traffic. A load balancer resource works at layer 4, and distributes traffic based on protocol or ports.

Most web applications using HTTP or HTTPS should use Kubernetes ingress resources and controllers, which work at layer 7. Ingress can distribute traffic based on the URL of the application and handle TLS/SSL termination. Ingress also reduces the number of IP addresses you expose and map.

With a load balancer, each application typically needs a public IP address assigned and mapped to the service in the AKS cluster. With an ingress resource, a single IP address can distribute traffic to multiple applications.



There are two components for ingress:

- An ingress *resource*
- An ingress *controller*

Ingress resource

The *ingress resource* is a YAML manifest of `kind: Ingress`. It defines the host, certificates, and rules to route traffic to services running in your AKS cluster.

The following example YAML manifest would distribute traffic for *myapp.com* to one of two services, *blogservice* or *storeservice*. The customer is directed to one service or the other based on the URL they access.

```
kind: Ingress
metadata:
  name: myapp-ingress
  annotations: kubernetes.io/ingress.class: "PublicIngress"
spec:
  tls:
    - hosts:
        - myapp.com
      secretName: myapp-secret
  rules:
    - host: myapp.com
      http:
        paths:
          - path: /blog
            backend:
              serviceName: blogservice
              servicePort: 80
          - path: /store
            backend:
              serviceName: storeservice
              servicePort: 80
```

Ingress controller

An *ingress controller* is a daemon that runs on an AKS node and watches for incoming requests. Traffic is then distributed based on the rules defined in the ingress resource. While the most common ingress controller is based on [NGINX](#), AKS doesn't restrict you to a specific controller. You can use [Contour](#), [HAProxy](#), [Traefik](#), etc.

Ingress controllers must be scheduled on a Linux node. Indicate that the resource should run on a Linux-based node using a node selector in your YAML manifest or Helm chart deployment. For more information, see [Use node selectors to control where pods are scheduled in AKS](#).

NOTE

Windows Server nodes shouldn't run the ingress controller.

There are many scenarios for ingress, including the following how-to guides:

- [Create a basic ingress controller with external network connectivity](#)
- [Create an ingress controller that uses an internal, private network and IP address](#)
- [Create an ingress controller that uses your own TLS certificates](#)
- [Create an ingress controller that uses Let's Encrypt to automatically generate TLS certificates with a dynamic public IP address or with a static public IP address](#)

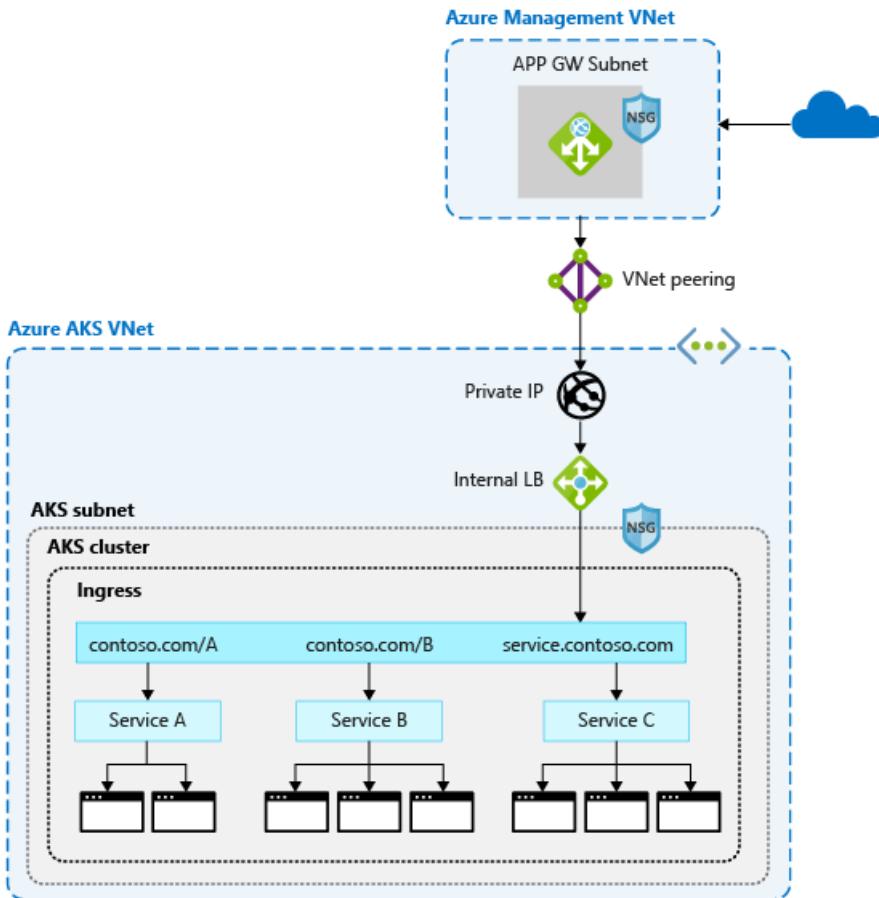
Secure traffic with a web application firewall (WAF)

Best practice guidance

To scan incoming traffic for potential attacks, use a web application firewall (WAF) such as [Barracuda WAF for Azure](#) or Azure Application Gateway. These more advanced network resources can also route traffic beyond just HTTP and HTTPS connections or basic TLS termination.

Typically, an ingress controller is a Kubernetes resource in your AKS cluster that distributes traffic to services and applications. The controller runs as a daemon on an AKS node, and consumes some of the node's resources, like CPU, memory, and network bandwidth. In larger environments, you'll want to:

- Offload some of this traffic routing or TLS termination to a network resource outside of the AKS cluster.
- Scan incoming traffic for potential attacks.



For that extra layer of security, a web application firewall (WAF) filters the incoming traffic. With a set of rules, the Open Web Application Security Project (OWASP) watches for attacks like cross-site scripting or cookie poisoning. [Azure Application Gateway](#) (currently in preview in AKS) is a WAF that integrates with AKS clusters, locking in these security features before the traffic reaches your AKS cluster and applications.

Since other third-party solutions also perform these functions, you can continue to use existing investments or expertise in your preferred product.

Load balancer or ingress resources continually run in your AKS cluster and refine the traffic distribution. App Gateway can be centrally managed as an ingress controller with a resource definition. To get started, [create an Application Gateway Ingress controller](#).

Control traffic flow with network policies

Best practice guidance

Use network policies to allow or deny traffic to pods. By default, all traffic is allowed between pods within a cluster. For improved security, define rules that limit pod communication.

Network policy is a Kubernetes feature available in AKS that lets you control the traffic flow between pods. You allow or deny traffic to the pod based on settings such as assigned labels, namespace, or traffic port. Network policies are a cloud-native way to control the flow of traffic for pods. As pods are dynamically created in an AKS cluster, required network policies can be automatically applied.

To use network policy, enable the feature when you create a new AKS cluster. You can't enable network policy on an existing AKS cluster. Plan ahead to enable network policy on the necessary clusters.

NOTE

Network policy should only be used for Linux-based nodes and pods in AKS.

You create a network policy as a Kubernetes resource using a YAML manifest. Policies are applied to defined pods, with ingress or egress rules defining traffic flow.

The following example applies a network policy to pods with the *app: backend* label applied to them. The ingress rule only allows traffic from pods with the *app: frontend* label:

```
kind: NetworkPolicy
apiVersion: networking.k8s.io/v1
metadata:
  name: backend-policy
spec:
  podSelector:
    matchLabels:
      app: backend
  ingress:
  - from:
    - podSelector:
        matchLabels:
          app: frontend
```

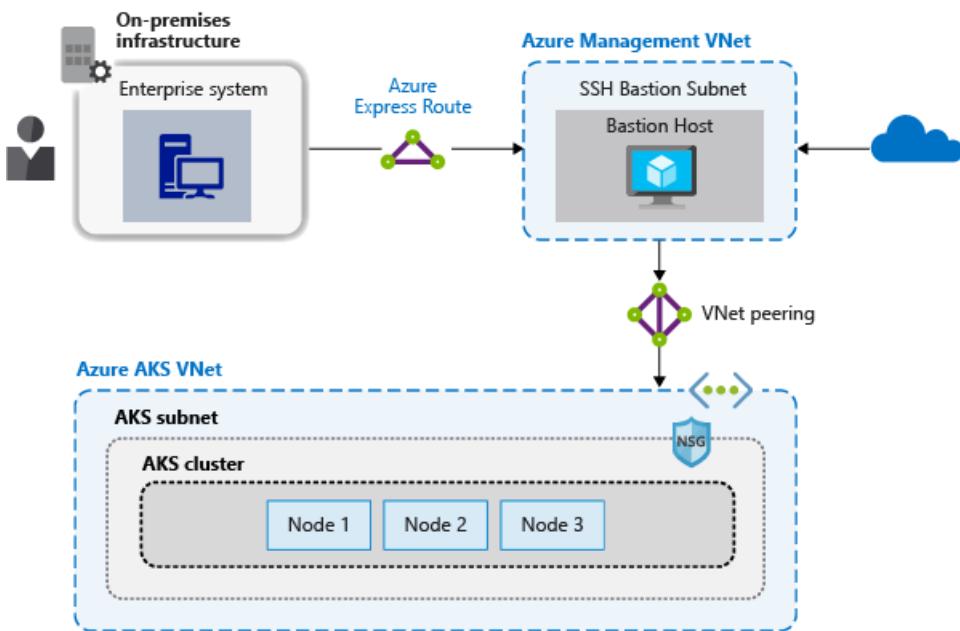
To get started with policies, see [Secure traffic between pods using network policies in Azure Kubernetes Service \(AKS\)](#).

Securely connect to nodes through a bastion host

Best practice guidance

Don't expose remote connectivity to your AKS nodes. Create a bastion host, or jump box, in a management virtual network. Use the bastion host to securely route traffic into your AKS cluster to remote management tasks.

You can complete most operations in AKS using the Azure management tools or through the Kubernetes API server. AKS nodes are only available on a private network and aren't connected to the public internet. To connect to nodes and provide maintenance and support, route your connections through a bastion host, or jump box. Verify this host lives in a separate, securely-peered management virtual network to the AKS cluster virtual network.



The management network for the bastion host should be secured, too. Use an [Azure ExpressRoute](#) or [VPN gateway](#) to connect to an on-premises network, and control access using network security groups.

Next steps

This article focused on network connectivity and security. For more information about network basics in Kubernetes, see [Network concepts for applications in Azure Kubernetes Service \(AKS\)](#)

Best practices for storage and backups in Azure Kubernetes Service (AKS)

10/27/2022 • 6 minutes to read • [Edit Online](#)

As you create and manage clusters in Azure Kubernetes Service (AKS), your applications often need storage. Make sure you understand pod performance needs and access methods so that you can select the best storage for your application. The AKS node size may impact your storage choices. Plan for ways to back up and test the restore process for attached storage.

This best practices article focuses on storage considerations for cluster operators. In this article, you learn:

- What types of storage are available.
- How to correctly size AKS nodes for storage performance.
- Differences between dynamic and static provisioning of volumes.
- Ways to back up and secure your data volumes.

Choose the appropriate storage type

Best practice guidance

Understand the needs of your application to pick the right storage. Use high performance, SSD-backed storage for production workloads. Plan for network-based storage when you need multiple concurrent connections.

Applications often require different types and speeds of storage. Determine the most appropriate storage type by asking the following questions.

- Do your applications need storage that connects to individual pods?
- Do your applications need storage shared across multiple pods?
- Is the storage for read-only access to data?
- Will the storage be used to write large amounts of structured data?

The following table outlines the available storage types and their capabilities:

USE CASE	VOLUME PLUGIN	READ/WRITE ONCE	READ-ONLY MANY	READ/WRITE MANY	WINDOWS SERVER CONTAINER SUPPORT
Shared configuration	Azure Files	Yes	Yes	Yes	Yes
Structured app data	Azure Disks	Yes	No	No	Yes
Unstructured data, file system operations	BlobFuse	Yes	Yes	Yes	No

AKS provides two primary types of secure storage for volumes backed by Azure Disks or Azure Files. Both use the default Azure Storage Service Encryption (SSE) that encrypts data at rest. Disks cannot be encrypted using

Azure Disk Encryption at the AKS node level.

Both Azure Files and Azure Disks are available in Standard and Premium performance tiers:

- *Premium* disks
 - Backed by high-performance solid-state disks (SSDs).
 - Recommended for all production workloads.
- *Standard* disks
 - Backed by regular spinning disks (HDDs).
 - Good for archival or infrequently accessed data.

Understand the application performance needs and access patterns to choose the appropriate storage tier. For more information about Managed Disks sizes and performance tiers, see [Azure Managed Disks overview](#)

Create and use storage classes to define application needs

Define the type of storage you want using Kubernetes *storage classes*. The storage class is then referenced in the pod or deployment specification. Storage class definitions work together to create the appropriate storage and connect it to pods.

For more information, see [Storage classes in AKS](#).

Size the nodes for storage needs

Best practice guidance

Each node size supports a maximum number of disks. Different node sizes also provide different amounts of local storage and network bandwidth. Plan appropriately for your application demands to deploy the right size of nodes.

AKS nodes run as various Azure VM types and sizes. Each VM size provides:

- A different amount of core resources such as CPU and memory.
- A maximum number of disks that can be attached.

Storage performance also varies between VM sizes for the maximum local and attached disk IOPS (input/output operations per second).

If your applications require Azure Disks as their storage solution, strategize an appropriate node VM size.

Storage capabilities and CPU and memory amounts play a major role when deciding on a VM size.

For example, while both the *Standard_B2ms* and *Standard_DS2_v2* VM sizes include a similar amount of CPU and memory resources, their potential storage performance is different:

NODE TYPE AND SIZE	VCPU	MEMORY (GIB)	MAX DATA DISKS	MAX UNCACHED DISK IOPS	MAX UNCACHED THROUGHPUT (MBPS)
Standard_B2ms	2	8	4	1,920	22.5
Standard_DS2_v2	2	7	8	6,400	96

In this example, the *Standard_DS2_v2* offers twice as many attached disks, and three to four times the amount of IOPS and disk throughput. If you only compared core compute resources and compared costs, you might have chosen the *Standard_B2ms* VM size with poor storage performance and limitations.

Work with your application development team to understand their storage capacity and performance needs.

Choose the appropriate VM size for the AKS nodes to meet or exceed their performance needs. Regularly baseline applications to adjust VM size as needed.

NOTE

By default, disk size and performance for managed disks is assigned according to the selected VM SKU and vCPU count. Default OS disk sizing is only used on new clusters or node pools when Ephemeral OS disks are not supported and a default OS disk size is not specified. For more information, see [Default OS disk sizing](#).

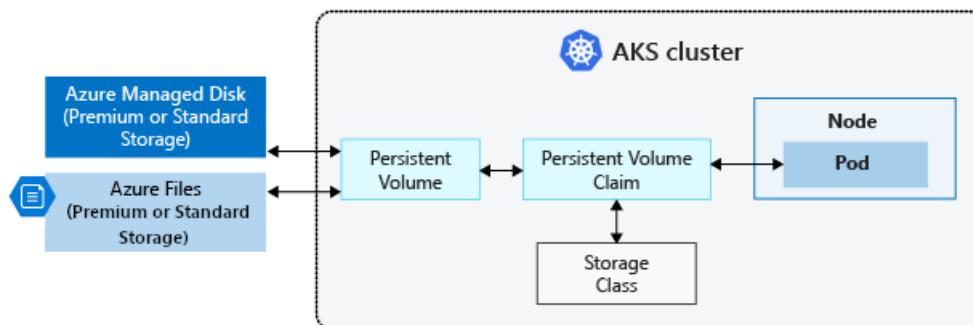
For more information about available VM sizes, see [Sizes for Linux virtual machines in Azure](#).

Dynamically provision volumes

Best practice guidance

To reduce management overhead and enable scaling, avoid statically create and assign persistent volumes. Use dynamic provisioning. In your storage classes, define the appropriate reclaim policy to minimize unneeded storage costs once pods are deleted.

To attach storage to pods, use persistent volumes. Persistent volumes can be created manually or dynamically. Creating persistent volumes manually adds management overhead and limits your ability to scale. Instead, provision persistent volume dynamically to simplify storage management and allow your applications to grow and scale as needed.



A persistent volume claim (PVC) lets you dynamically create storage as needed. Underlying Azure disks are created as pods request them. In the pod definition, request a volume to be created and attached to a designated mount path.

For the concepts on how to dynamically create and use volumes, see [Persistent Volumes Claims](#).

To see these volumes in action, see how to dynamically create and use a persistent volume with [Azure Disks](#) or [Azure Files](#).

As part of your storage class definitions, set the appropriate *reclaimPolicy*. This reclaimPolicy controls the behavior of the underlying Azure storage resource when the pod is deleted. The underlying storage resource can either be deleted or retained for future pod use. Set the reclaimPolicy to *retain* or *delete*.

Understand your application needs, and implement regular checks for retained storage to minimize the amount of unused and billed storage.

For more information about storage class options, see [storage reclaim policies](#).

Secure and back up your data

Best practice guidance

Back up your data using an appropriate tool for your storage type, such as Velero or Azure Backup. Verify the integrity and security of those backups.

When your applications store and consume data persisted on disks or in files, you need to take regular backups or snapshots of that data. Azure Disks can use built-in snapshot technologies. Your applications may need to flush writes-to-disk before you perform the snapshot operation. [Velero](#) can back up persistent volumes along with additional cluster resources and configurations. If you can't [remove state from your applications](#), back up the data from persistent volumes and regularly test the restore operations to verify data integrity and the processes required.

Understand the limitations of the different approaches to data backups and if you need to quiesce your data prior to snapshot. Data backups don't necessarily let you restore your application environment of cluster deployment. For more information about those scenarios, see [Best practices for business continuity and disaster recovery in AKS](#).

Next steps

This article focused on storage best practices in AKS. For more information about storage basics in Kubernetes, see [Storage concepts for applications in AKS](#).

Best practices for business continuity and disaster recovery in Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

As you manage clusters in Azure Kubernetes Service (AKS), application uptime becomes important. By default, AKS provides high availability by using multiple nodes in a [Virtual Machine Scale Set \(VMSS\)](#). But these multiple nodes don't protect your system from a region failure. To maximize your uptime, plan ahead to maintain business continuity and prepare for disaster recovery.

This article focuses on how to plan for business continuity and disaster recovery in AKS. You learn how to:

- Plan for AKS clusters in multiple regions.
- Route traffic across multiple clusters by using Azure Traffic Manager.
- Use geo-replication for your container image registries.
- Plan for application state across multiple clusters.
- Replicate storage across multiple regions.

Plan for multiregion deployment

Best practice

When you deploy multiple AKS clusters, choose regions where AKS is available. Use paired regions.

An AKS cluster is deployed into a single region. To protect your system from region failure, deploy your application into multiple AKS clusters across different regions. When planning where to deploy your AKS cluster, consider:

- [AKS region availability](#)
 - Choose regions close to your users.
 - AKS continually expands into new regions.
- [Azure paired regions](#)
 - For your geographic area, choose two regions paired together.
 - AKS platform updates (planned maintenance) are serialized with a delay of at least 24 hours between paired regions.
 - Recovery efforts for paired regions are prioritized where needed.
- [Service availability](#)
 - Decide whether your paired regions should be hot/hot, hot/warm, or hot/cold.
 - Do you want to run both regions at the same time, with one region *ready* to start serving traffic? Or,
 - Do you want to give one region time to get ready to serve traffic?

AKS region availability and paired regions are a joint consideration. Deploy your AKS clusters into paired regions designed to manage region disaster recovery together. For example, AKS is available in East US and West US. These regions are paired. Choose these two regions when you're creating an AKS BC/DR strategy.

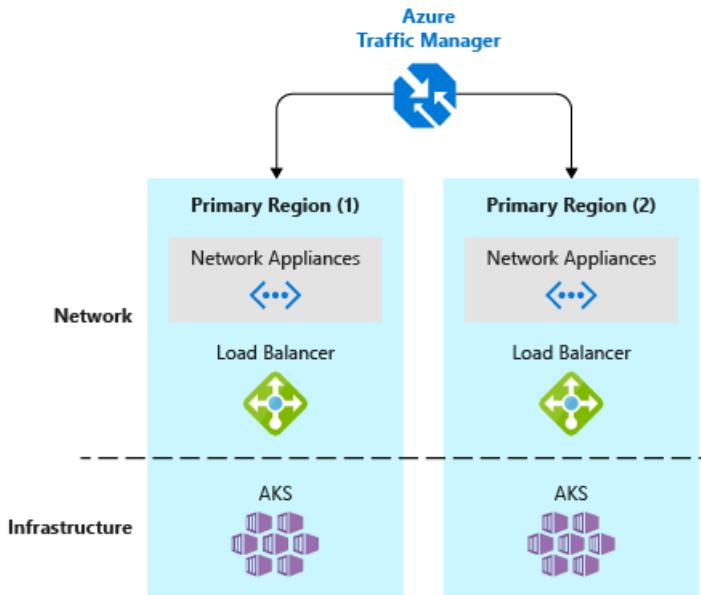
When you deploy your application, add another step to your CI/CD pipeline to deploy to these multiple AKS clusters. Updating your deployment pipelines prevents applications from deploying into only one of your regions and AKS clusters. In that scenario, customer traffic directed to a secondary region won't receive the latest code updates.

Use Azure Traffic Manager to route traffic

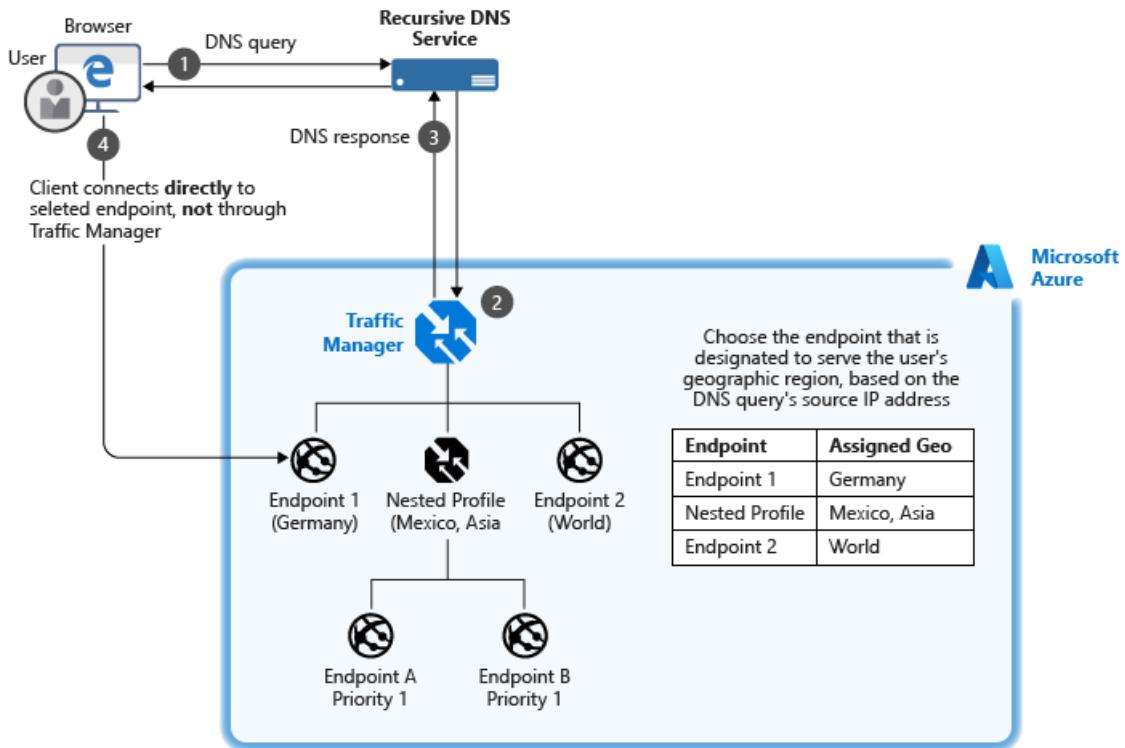
Best practice

Azure Traffic Manager can direct you to your closest AKS cluster and application instance. For the best performance and redundancy, direct all application traffic through Traffic Manager before it goes to your AKS cluster.

If you have multiple AKS clusters in different regions, use Traffic Manager to control traffic flow to the applications running in each cluster. [Azure Traffic Manager](#) is a DNS-based traffic load balancer that can distribute network traffic across regions. Use Traffic Manager to route users based on cluster response time or based on geography.



If you have a single AKS cluster, you typically connect to the service IP or DNS name of a given application. In a multi-cluster deployment, you should connect to a Traffic Manager DNS name that points to the services on each AKS cluster. Define these services by using Traffic Manager endpoints. Each endpoint is the *service load balancer IP*. Use this configuration to direct network traffic from the Traffic Manager endpoint in one region to the endpoint in a different region.



Traffic Manager performs DNS lookups and returns your most appropriate endpoint. Nested profiles can prioritize a primary location. For example, you should connect to their closest geographic region. If that region has a problem, Traffic Manager directs you to a secondary region. This approach ensures that you can connect to an application instance even if your closest geographic region is unavailable.

For information on how to set up endpoints and routing, see [Configure the geographic traffic routing method by using Traffic Manager](#).

Application routing with Azure Front Door Service

Using split TCP-based anycast protocol, [Azure Front Door Service](#) promptly connects your end users to the nearest Front Door POP (Point of Presence). More features of Azure Front Door Service:

- TLS termination
- Custom domain
- Web application firewall
- URL Rewrite
- Session affinity

Review the needs of your application traffic to understand which solution is the most suitable.

Interconnect regions with global virtual network peering

Connect both virtual networks to each other through [virtual network peering](#) to enable communication between clusters. Virtual network peering interconnects virtual networks, providing high bandwidth across Microsoft's backbone network - even across different geographic regions.

Before peering virtual networks with running AKS clusters, use the standard Load Balancer in your AKS cluster. This prerequisite makes Kubernetes services reachable across the virtual network peering.

Enable geo-replication for container images

Best practice

Store your container images in Azure Container Registry and geo-replicate the registry to each AKS region.

To deploy and run your applications in AKS, you need a way to store and pull the container images. Container Registry integrates with AKS, so it can securely store your container images or Helm charts. Container Registry supports multimaster geo-replication to automatically replicate your images to Azure regions around the world.

To improve performance and availability:

1. Use Container Registry geo-replication to create a registry in each region where you have an AKS cluster.
2. Each AKS cluster then pulls container images from the local container registry in the same region:



When you use Container Registry geo-replication to pull images from the same region, the results are:

- **Faster:** Pull images from high-speed, low-latency network connections within the same Azure region.
- **More reliable:** If a region is unavailable, your AKS cluster pulls the images from an available container registry.
- **Cheaper:** No network egress charge between datacenters.

Geo-replication is a *Premium* SKU container registry feature. For information on how to configure geo-replication, see [Container Registry geo-replication](#).

Remove service state from inside containers

Best practice

Avoid storing service state inside the container. Instead, use an Azure platform as a service (PaaS) that supports multi-region replication.

Service state refers to the in-memory or on-disk data required by a service to function. State includes the data structures and member variables that the service reads and writes. Depending on how the service is architected, the state might also include files or other resources stored on the disk. For example, the state might include the files a database uses to store data and transaction logs.

State can be either externalized or co-located with the code that manipulates the state. Typically, you externalize state by using a database or other data store that runs on different machines over the network or that runs out of process on the same machine.

Containers and microservices are most resilient when the processes that run inside them don't retain state. Since applications almost always contain some state, use a PaaS solution, such as:

- Azure Cosmos DB
- Azure Database for PostgreSQL
- Azure Database for MySQL
- Azure SQL Database

To build portable applications, see the following guidelines:

- [The 12-factor app methodology](#)
- [Run a web application in multiple Azure regions](#)

Create a storage migration plan

Best practice

If you use Azure Storage, prepare and test how to migrate your storage from the primary region to the backup region.

Your applications might use Azure Storage for their data. If so, your applications are spread across multiple AKS clusters in different regions. You need to keep the storage synchronized. Here are two common ways to replicate storage:

- Infrastructure-based asynchronous replication
- Application-based asynchronous replication

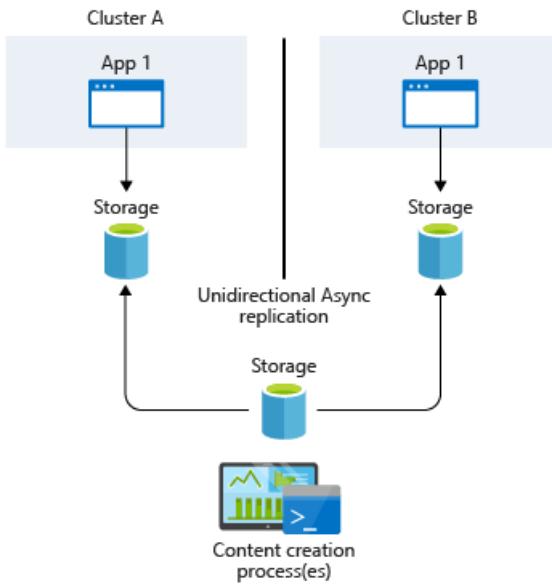
Infrastructure-based asynchronous replication

Your applications might require persistent storage even after a pod is deleted. In Kubernetes, you can use persistent volumes to persist data storage. Persistent volumes are mounted to a node VM and then exposed to the pods. Persistent volumes follow pods even if the pods are moved to a different node inside the same cluster.

The replication strategy you use depends on your storage solution. The following common storage solutions provide their own guidance about disaster recovery and replication:

- [Gluster](#)
- [Ceph](#)
- [Rook](#)
- [Portworx](#)

Typically, you provide a common storage point where applications write their data. This data is then replicated across regions and accessed locally.

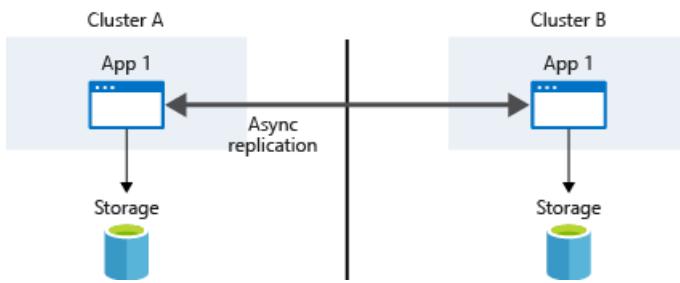


If you use Azure Managed Disks, you can use [Velero on Azure](#) and [Kasten](#) to handle replication and disaster recovery. These options are back up solutions native to but unsupported by Kubernetes.

Application-based asynchronous replication

Kubernetes currently provides no native implementation for application-based asynchronous replication. Since containers and Kubernetes are loosely coupled, any traditional application or language approach should work.

Typically, the applications themselves replicate the storage requests, which are then written to each cluster's underlying data storage.



Next steps

This article focuses on business continuity and disaster recovery considerations for AKS clusters. For more information about cluster operations in AKS, see these articles about best practices:

- [Multitenancy and cluster isolation](#)
- [Basic Kubernetes scheduler features](#)

Best practices for application developers to manage resources in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

As you develop and run applications in Azure Kubernetes Service (AKS), there are a few key areas to consider. How you manage your application deployments can negatively impact the end-user experience of services that you provide. To succeed, keep in mind some best practices you can follow as you develop and run applications in AKS.

This article focuses on running your cluster and workloads from an application developer perspective. For information about administrative best practices, see [Cluster operator best practices for isolation and resource management in Azure Kubernetes Service \(AKS\)](#). In this article, you learn:

- Pod resource requests and limits.
- Ways to develop and deploy applications with Bridge to Kubernetes and Visual Studio Code.

Define pod resource requests and limits

Best practice guidance

Set pod requests and limits on all pods in your YAML manifests. If the AKS cluster uses *resource quotas* and you don't define these values, your deployment may be rejected.

Use pod requests and limits to manage the compute resources within an AKS cluster. Pod requests and limits inform the Kubernetes scheduler which compute resources to assign to a pod.

Pod CPU/Memory requests

Pod requests define a set amount of CPU and memory that the pod needs regularly.

In your pod specifications, it's **best practice and very important** to define these requests and limits based on the above information. If you don't include these values, the Kubernetes scheduler cannot take into account the resources your applications require to aid in scheduling decisions.

Monitor the performance of your application to adjust pod requests.

- If you underestimate pod requests, your application may receive degraded performance due to over-scheduling a node.
- If requests are overestimated, your application may have increased difficulty getting scheduled.

Pod CPU/Memory limits**

Pod limits set the maximum amount of CPU and memory that a pod can use.

- *Memory limits* define which pods should be killed when nodes are unstable due to insufficient resources. Without proper limits set, pods will be killed until resource pressure is lifted.
- While a pod may exceed the *CPU limit* periodically, the pod will not be killed for exceeding the CPU limit.

Pod limits define when a pod has lost control of resource consumption. When it exceeds the limit, the pod is marked for killing. This behavior maintains node health and minimizes impact to pods sharing the node. Not setting a pod limit defaults it to the highest available value on a given node.

Avoid setting a pod limit higher than your nodes can support. Each AKS node reserves a set amount of CPU and

memory for the core Kubernetes components. Your application may try to consume too many resources on the node for other pods to successfully run.

Monitor the performance of your application at different times during the day or week. Determine peak demand times and align the pod limits to the resources required to meet maximum needs.

IMPORTANT

In your pod specifications, define these requests and limits based on the above information. Failing to include these values prevents the Kubernetes scheduler from accounting for resources your applications require to aid in scheduling decisions.

If the scheduler places a pod on a node with insufficient resources, application performance will be degraded. Cluster administrators **must** set *resource quotas* on a namespace that requires you to set resource requests and limits. For more information, see [resource quotas on AKS clusters](#).

When you define a CPU request or limit, the value is measured in CPU units.

- 1.0 CPU equates to one underlying virtual CPU core on the node.
 - The same measurement is used for GPUs.
- You can define fractions measured in millicores. For example, *100m* is *0.1* of an underlying vCPU core.

In the following basic example for a single NGINX pod, the pod requests *100m* of CPU time, and *128Mi* of memory. The resource limits for the pod are set to *250m* CPU and *256Mi* memory:

```
kind: Pod
apiVersion: v1
metadata:
  name: mypod
spec:
  containers:
  - name: mypod
    image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
    resources:
      requests:
        cpu: 100m
        memory: 128Mi
      limits:
        cpu: 250m
        memory: 256Mi
```

For more information about resource measurements and assignments, see [Managing compute resources for containers](#).

Develop and debug applications against an AKS cluster

Best practice guidance

Development teams should deploy and debug against an AKS cluster using Bridge to Kubernetes.

With Bridge to Kubernetes, you can develop, debug, and test applications directly against an AKS cluster. Developers within a team collaborate to build and test throughout the application lifecycle. You can continue to use existing tools such as Visual Studio or Visual Studio Code with the Bridge to Kubernetes extension.

Using integrated development and test process with Bridge to Kubernetes reduces the need for local test environments like [minikube](#). Instead, you develop and test against an AKS cluster, even secured and isolated clusters.

NOTE

Bridge to Kubernetes is intended for use with applications that run on Linux pods and nodes.

Use the Visual Studio Code (VS Code) extension for Kubernetes

Best practice guidance

Install and use the VS Code extension for Kubernetes when you write YAML manifests. You can also use the extension for integrated deployment solution, which may help application owners that infrequently interact with the AKS cluster.

The [Visual Studio Code extension for Kubernetes](#) helps you develop and deploy applications to AKS. The extension provides:

- Intellisense for Kubernetes resources, Helm charts, and templates.
- Browse, deploy, and edit capabilities for Kubernetes resources from within VS Code.
- An intellisense check for resource requests or limits being set in the pod specifications:

```
1 kind: Pod
2 apiVersion: v1
3 metadata:
4   name: mypod
5 spec:
6   containers:
7     - name: mypod
8       image: nginx:1.15.5
9       resources:
10         requests:
11           cpu: 100m
12           No memory limit specified for this container - this could starve other processes
13
14         limits:
15           cpu: 250m
```

Next steps

This article focused on how to run your cluster and workloads from a cluster operator perspective. For information about administrative best practices, see [Cluster operator best practices for isolation and resource management in Azure Kubernetes Service \(AKS\)](#).

To implement some of these best practices, see the following articles:

- [Develop with Bridge to Kubernetes](#)

Best practices for pod security in Azure Kubernetes Service (AKS)

10/27/2022 • 5 minutes to read • [Edit Online](#)

As you develop and run applications in Azure Kubernetes Service (AKS), the security of your pods is a key consideration. Your applications should be designed for the principle of least number of privileges required. Keeping private data secure is top of mind for customers. You don't want credentials like database connection strings, keys, or secrets and certificates exposed to the outside world where an attacker could take advantage of those secrets for malicious purposes. Don't add them to your code or embed them in your container images. This approach would create a risk for exposure and limit the ability to rotate those credentials as the container images will need to be rebuilt.

This best practices article focuses on how to secure pods in AKS. You learn how to:

- Use pod security context to limit access to processes and services or privilege escalation
- Authenticate with other Azure resources using pod managed identities
- Request and retrieve credentials from a digital vault such as Azure Key Vault

You can also read the best practices for [cluster security](#) and for [container image management](#).

Secure pod access to resources

Best practice guidance - To run as a different user or group and limit access to the underlying node processes and services, define pod security context settings. Assign the least number of privileges required.

For your applications to run correctly, pods should run as a defined user or group and not as *root*. The `securityContext` for a pod or container lets you define settings such as `runAsUser` or `fsGroup` to assume the appropriate permissions. Only assign the required user or group permissions, and don't use the security context as a means to assume additional permissions. The `runAsUser`, privilege escalation, and other Linux capabilities settings are only available on Linux nodes and pods.

When you run as a non-root user, containers cannot bind to the privileged ports under 1024. In this scenario, Kubernetes Services can be used to disguise the fact that an app is running on a particular port.

A pod security context can also define additional capabilities or permissions for accessing processes and services. The following common security context definitions can be set:

- **allowPrivilegeEscalation** defines if the pod can assume *root* privileges. Design your applications so this setting is always set to *false*.
- **Linux capabilities** let the pod access underlying node processes. Take care with assigning these capabilities. Assign the least number of privileges needed. For more information, see [Linux capabilities](#).
- **SELinux labels** is a Linux kernel security module that lets you define access policies for services, processes, and filesystem access. Again, assign the least number of privileges needed. For more information, see [SELinux options in Kubernetes](#)

The following example pod YAML manifest sets security context settings to define:

- Pod runs as user ID *1000* and part of group ID *2000*
- Can't escalate privileges to use `root`
- Allows Linux capabilities to access network interfaces and the host's real-time (hardware) clock

```
apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo
spec:
  securityContext:
    fsGroup: 2000
  containers:
    - name: security-context-demo
      image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
      securityContext:
        runAsUser: 1000
        allowPrivilegeEscalation: false
        capabilities:
          add: ["NET_ADMIN", "SYS_TIME"]
```

Work with your cluster operator to determine what security context settings you need. Try to design your applications to minimize additional permissions and access the pod requires. There are additional security features to limit access using AppArmor and seccomp (secure computing) that can be implemented by cluster operators. For more information, see [Secure container access to resources](#).

Limit credential exposure

Best practice guidance - Don't define credentials in your application code. Use managed identities for Azure resources to let your pod request access to other resources. A digital vault, such as Azure Key Vault, should also be used to store and retrieve digital keys and credentials. Pod-managed identities are intended for use with Linux pods and container images only.

To limit the risk of credentials being exposed in your application code, avoid the use of fixed or shared credentials. Credentials or keys shouldn't be included directly in your code. If these credentials are exposed, the application needs to be updated and redeployed. A better approach is to give pods their own identity and way to authenticate themselves, or automatically retrieve credentials from a digital vault.

Use Azure Container Compute Upstream projects

IMPORTANT

Associated AKS open source projects are not supported by Azure technical support. They are provided for users to self-install into clusters and gather feedback from our community.

The following [associated AKS open source projects](#) let you automatically authenticate pods or request credentials and keys from a digital vault. These projects are maintained by the Azure Container Compute Upstream team and are part of a [broader list of projects available for use](#).

- [Azure Active Directory workload identity](#) (preview)
- [Azure Key Vault Provider for Secrets Store CSI Driver](#)

Use an Azure AD workload identity (preview)

A workload identity is an identity used by an application running on a pod that can authenticate itself against other Azure services that support it, such as Storage or SQL. It integrates with the capabilities native to Kubernetes to federate with external identity providers. In this security model, the AKS cluster acts as token issuer, Azure Active Directory uses OpenID Connect to discover public signing keys and verify the authenticity of the service account token before exchanging it for an Azure AD token. Your workload can exchange a service account token projected to its volume for an Azure AD token using the Azure Identity client library using the [Azure SDK](#) or the [Microsoft Authentication Library](#) (MSAL).

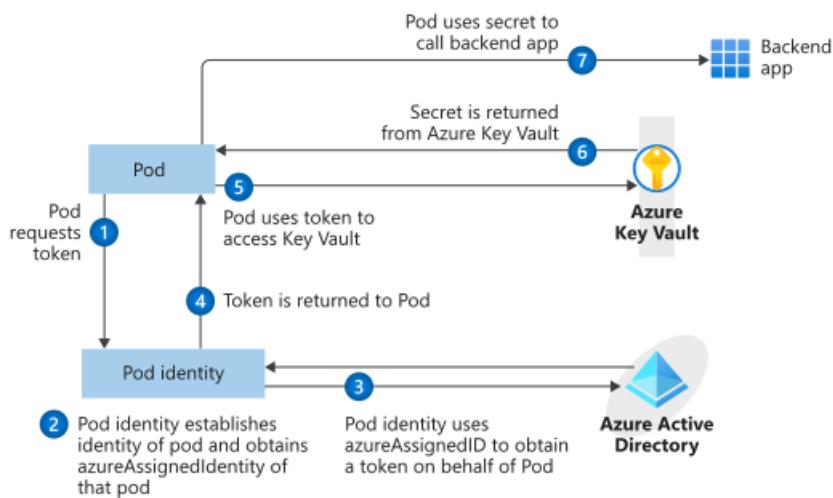
For more information about workload identities, see [Configure an AKS cluster to use Azure AD workload](#)

identities with your applications

Use Azure Key Vault with Secrets Store CSI Driver

Using the pod identity project enables authentication against supporting Azure services. For your own services or applications without managed identities for Azure resources, you can still authenticate using credentials or keys. A digital vault can be used to store these secret contents.

When applications need a credential, they communicate with the digital vault, retrieve the latest secret contents, and then connect to the required service. Azure Key Vault can be this digital vault. The simplified workflow for retrieving a credential from Azure Key Vault using pod managed identities is shown in the following diagram:



With Key Vault, you store and regularly rotate secrets such as credentials, storage account keys, or certificates. You can integrate Azure Key Vault with an AKS cluster using the [Azure Key Vault provider for the Secrets Store CSI Driver](#). The Secrets Store CSI driver enables the AKS cluster to natively retrieve secret contents from Key Vault and securely provide them only to the requesting pod. Work with your cluster operator to deploy the Secrets Store CSI Driver onto AKS worker nodes. You can use a pod managed identity to request access to Key Vault and retrieve the secret contents needed through the Secrets Store CSI Driver.

Next steps

This article focused on how to secure your pods. To implement some of these areas, see the following articles:

- [Use workload managed identities for Azure resources with AKS \(preview\)](#)
- [Integrate Azure Key Vault with AKS](#)

Migrate to Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

To help you plan and execute a successful migration to Azure Kubernetes Service (AKS), this guide provides details for the current recommended AKS configuration. While this article doesn't cover every scenario, it contains links to more detailed information for planning a successful migration.

This document helps support the following scenarios:

- Containerizing certain applications and migrating them to AKS using [Azure Migrate](#).
- Migrating an AKS Cluster backed by [Availability Sets](#) to [Virtual Machine Scale Sets](#).
- Migrating an AKS cluster to use a [Standard SKU load balancer](#).
- Migrating from [Azure Container Service \(ACS\) - retiring January 31, 2020](#) to AKS.
- Migrating from [AKS engine](#) to AKS.
- Migrating from non-Azure based Kubernetes clusters to AKS.
- Moving existing resources to a different region.

When migrating, ensure your target Kubernetes version is within the supported window for AKS. Older versions may not be within the supported range and will require a version upgrade to be supported by AKS. For more information, see [AKS supported Kubernetes versions](#).

If you're migrating to a newer version of Kubernetes, review [Kubernetes version and version skew support policy](#).

Several open-source tools can help with your migration, depending on your scenario:

- [Velero](#) (Requires Kubernetes 1.7+)
- [Azure Kube CLI extension](#)
- [ReShifter](#)

In this article we will summarize migration details for:

- Containerizing applications through Azure Migrate
- AKS with Standard Load Balancer and Virtual Machine Scale Sets
- Existing attached Azure Services
- Ensure valid quotas
- High Availability and business continuity
- Considerations for stateless applications
- Considerations for stateful applications
- Deployment of your cluster configuration

Use Azure Migrate to migrate your applications to AKS

Azure Migrate offers a unified platform to assess and migrate to Azure on-premises servers, infrastructure, applications, and data. For AKS, you can use Azure Migrate for the following tasks:

- [Containerize ASP.NET applications and migrate to AKS](#)
- [Containerize Java web applications and migrate to AKS](#)

AKS with Standard Load Balancer and Virtual Machine Scale Sets

AKS is a managed service offering unique capabilities with lower management overhead. Since AKS is a managed service, you must select from a set of [regions](#) which AKS supports. You may need to modify your existing applications to keep them healthy on the AKS-managed control plane during the transition from your existing cluster to AKS.

We recommend using AKS clusters backed by [Virtual Machine Scale Sets](#) and the [Azure Standard Load Balancer](#) to ensure you get features such as:

- [Multiple node pools](#),
- [Availability Zones](#),
- [Authorized IP ranges](#),
- [Cluster Autoscaler](#),
- [Azure Policy for AKS](#), and
- Other new features as they are released.

AKS clusters backed by [Virtual Machine Availability Sets](#) lack support for many of these features.

The following example creates an AKS cluster with single node pool backed by a virtual machine (VM) scale set. The cluster:

- Uses a standard load balancer.
- Enables the cluster autoscaler on the node pool for the cluster.
- Sets a minimum of 1 and maximum of 3 nodes.

```
# First create a resource group
az group create --name myResourceGroup --location eastus

# Now create the AKS cluster and enable the cluster autoscaler
az aks create \
    --resource-group myResourceGroup \
    --name myAKSCluster \
    --node-count 1 \
    --vm-set-type VirtualMachineScaleSets \
    --load-balancer-sku standard \
    --enable-cluster-autoscaler \
    --min-count 1 \
    --max-count 3
```

Existing attached Azure Services

When migrating clusters, you may have attached external Azure services. While the following services don't require resource recreation, they will require updating connections from previous to new clusters to maintain functionality.

- Azure Container Registry
- Log Analytics
- Application Insights
- Traffic Manager
- Storage Account
- External Databases

Ensure valid quotas

Since other VMs will be deployed into your subscription during migration, you should verify that your quotas and limits are sufficient for these resources. If necessary, request an increase in [vCPU quota](#).

You may need to request an increase for [Network quotas](#) to ensure you don't exhaust IPs. For more information, see [networking and IP ranges for AKS](#).

For more information, see [Azure subscription and service limits](#). To check your current quotas, in the Azure portal, go to the [subscriptions blade](#), select your subscription, and then select [Usage + quotas](#).

High Availability and Business Continuity

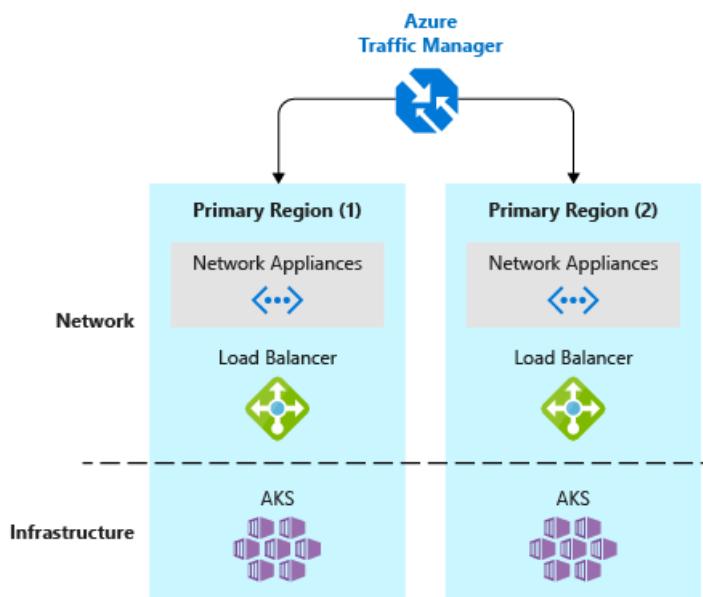
If your application can't handle downtime, you will need to follow best practices for high availability migration scenarios. Read more about [Best practices for complex business continuity planning, disaster recovery, and maximizing uptime in Azure Kubernetes Service \(AKS\)](#).

For complex applications, you'll typically migrate over time rather than all at once, meaning the old and new environments might need to communicate over the network. Applications previously using `ClusterIP` services to communicate might need to be exposed as type `LoadBalancer` and be secured appropriately.

To complete the migration, you'll want to point clients to the new services that are running on AKS. We recommend that you redirect traffic by updating DNS to point to the Load Balancer sitting in front of your AKS cluster.

[Azure Traffic Manager](#) can direct customers to the desired Kubernetes cluster and application instance. Traffic Manager is a DNS-based traffic load balancer that can distribute network traffic across regions. For the best performance and redundancy, direct all application traffic through Traffic Manager before it goes to your AKS cluster.

In a multi-cluster deployment, customers should connect to a Traffic Manager DNS name that points to the services on each AKS cluster. Define these services by using Traffic Manager endpoints. Each endpoint is the *service load balancer IP*. Use this configuration to direct network traffic from the Traffic Manager endpoint in one region to the endpoint in a different region.



[Azure Front Door Service](#) is another option for routing traffic for AKS clusters. With Azure Front Door Service, you can define, manage, and monitor the global routing for your web traffic by optimizing for best performance and instant global failover for high availability.

Considerations for stateless applications

Stateless application migration is the most straightforward case:

1. Apply your resource definitions (YAML or Helm) to the new cluster.
2. Ensure everything works as expected.
3. Redirect traffic to activate your new cluster.

Considerations for stateful applications

Carefully plan your migration of stateful applications to avoid data loss or unexpected downtime.

- If you use Azure Files, you can mount the file share as a volume into the new cluster. See [Mount Static Azure Files as a Volume](#).
- If you use Azure Managed Disks, you can only mount the disk if unattached to any VM. See [Mount Static Azure Disk as a Volume](#).
- If neither of those approaches work, you can use a backup and restore options. See [Velero on Azure](#).

Azure Files

Unlike disks, Azure Files can be mounted to multiple hosts concurrently. In your AKS cluster, Azure and Kubernetes don't prevent you from creating a pod that your AKS cluster still uses. To prevent data loss and unexpected behavior, ensure that the clusters don't write to the same files simultaneously.

If your application can host multiple replicas that point to the same file share, follow the stateless migration steps and deploy your YAML definitions to your new cluster.

If not, one possible migration approach involves the following steps:

1. Validate your application is working correctly.
2. Point your live traffic to your new AKS cluster.
3. Disconnect the old cluster.

If you want to start with an empty share and make a copy of the source data, you can use the [`az storage file copy`](#) commands to migrate your data.

Migrating persistent volumes

If you're migrating existing persistent volumes to AKS, you'll generally follow these steps:

1. Quiesce writes to the application.
 - This step is optional and requires downtime.
2. Take snapshots of the disks.
3. Create new managed disks from the snapshots.
4. Create persistent volumes in AKS.
5. Update pod specifications to [use existing volumes](#) rather than PersistentVolumeClaims (static provisioning).
6. Deploy your application to AKS.
7. Validate your application is working correctly.
8. Point your live traffic to your new AKS cluster.

IMPORTANT

If you choose not to quiesce writes, you'll need to replicate data to the new deployment. Otherwise you'll miss the data that was written after you took the disk snapshots.

Some open-source tools can help you create managed disks and migrate volumes between Kubernetes clusters:

- [Azure CLI Disk Copy extension](#) copies and converts disks across resource groups and Azure regions.
- [Azure Kube CLI extension](#) enumerates ACS Kubernetes volumes and migrates them to an AKS cluster.

Deployment of your cluster configuration

We recommend that you use your existing Continuous Integration (CI) and Continuous Deliver (CD) pipeline to deploy a known-good configuration to AKS. You can use Azure Pipelines to [build and deploy your applications to AKS](#). Clone your existing deployment tasks and ensure that `kubeconfig` points to the new AKS cluster.

If that's not possible, export resource definitions from your existing Kubernetes cluster and then apply them to AKS. You can use `kubectl` to export objects. For example:

```
kubectl get deployment -o yaml > deployments.yaml
```

Be sure to examine the output and remove any unnecessary live data fields.

Moving existing resources to another region

You may want to move your AKS cluster to a [different region supported by AKS](#). We recommend that you create a new cluster in the other region, then deploy your resources and applications to your new cluster.

In addition, if you have any services running on your AKS cluster, you will need to install and configure those services on your cluster in the new region.

In this article, we summarized migration details for:

- AKS with Standard Load Balancer and Virtual Machine Scale Sets
- Existing attached Azure Services
- Ensure valid quotas
- High Availability and business continuity
- Considerations for stateless applications
- Considerations for stateful applications
- Deployment of your cluster configuration

Java web app containerization and migration to Azure Kubernetes Service

10/27/2022 • 15 minutes to read • [Edit Online](#)

In this article, you'll learn how to containerize Java web applications (running on Apache Tomcat) and migrate them to [Azure Kubernetes Service \(AKS\)](#) using the Azure Migrate: App Containerization tool. The containerization process doesn't require access to your codebase and provides an easy way to containerize existing applications. The tool works by using the running state of the applications on a server to determine the application components and helps you package them in a container image. The containerized application can then be deployed on Azure Kubernetes Service (AKS).

The Azure Migrate: App Containerization tool currently supports -

- Containerizing Java Web Apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on AKS.
- Containerizing Java Web Apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on App Service. [Learn more](#)
- Containerizing ASP.NET apps and deploying them on Windows containers on AKS. [Learn more](#)
- Containerizing ASP.NET apps and deploying them on Windows containers on App Service. [Learn more](#)

The Azure Migrate: App Containerization tool helps you to -

- **Discover your application:** The tool remotely connects to the application servers running your Java web application (running on Apache Tomcat) and discovers the application components. The tool creates a Dockerfile that can be used to create a container image for the application.
- **Build the container image:** You can inspect and further customize the Dockerfile as per your application requirements and use that to build your application container image. The application container image is pushed to an Azure Container Registry you specify.
- **Deploy to Azure Kubernetes Service:** The tool then generates the Kubernetes resource definition YAML files needed to deploy the containerized application to your Azure Kubernetes Service cluster. You can customize the YAML files and use them to deploy the application on AKS.

NOTE

The Azure Migrate: App Containerization tool helps you discover specific application types (ASP.NET and Java web apps on Apache Tomcat) and their components on an application server. To discover servers and the inventory of apps, roles, and features running on on-premises machines, use Azure Migrate: Discovery and assessment capability. [Learn more](#)

While all applications won't benefit from a straight shift to containers without significant rearchitecting, some of the benefits of moving existing apps to containers without rewriting include:

- **Improved infrastructure utilization:** With containers, multiple applications can share resources and be hosted on the same infrastructure. This can help you consolidate infrastructure and improve utilization.
- **Simplified management:** By hosting your applications on a modern managed platform like AKS and App Service, you can simplify your management practices. You can achieve this by retiring or reducing the infrastructure maintenance and management processes that you'd traditionally perform with owned infrastructure.
- **Application portability:** With increased adoption and standardization of container specification formats and platforms, application portability is no longer a concern.

- **Adopt modern management with DevOps:** Helps you adopt and standardize on modern practices for management and security and transition to DevOps.

In this tutorial, you'll learn how to:

- Set up an Azure account.
- Install the Azure Migrate: App Containerization tool.
- Discover your Java web application.
- Build the container image.
- Deploy the containerized application on AKS.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths.

Prerequisites

Before you begin this tutorial, you should:

REQUIREMENT	DETAILS
Identify a machine to install the tool	<p>A Windows machine to install and run the Azure Migrate: App Containerization tool. The Windows machine could be a server (Windows Server 2016 or later) or client (Windows 10) operating system, meaning that the tool can run on your desktop as well.</p> <p>The Windows machine running the tool should have network connectivity to the servers/virtual machines hosting the Java web applications to be containerized.</p> <p>Ensure that 6-GB space is available on the Windows machine running the Azure Migrate: App Containerization tool for storing application artifacts.</p> <p>The Windows machine should have internet access, directly or via a proxy.</p>
Application servers	- Enable Secure Shell (SSH) connection on port 22 on the server(s) running the Java application(s) to be containerized.
Java web application	<p>The tool currently supports</p> <ul style="list-style-type: none"> - Applications running on Tomcat 8 or later. - Application servers on Ubuntu Linux 16.04/18.04/20.04, Debian 7/8, CentOS 6/7, Red Hat Enterprise Linux 5/6/7. - Applications using Java version 7 or later. <p>The tool currently doesn't support</p> <ul style="list-style-type: none"> - Applications servers running multiple Tomcat instances

Prepare an Azure user account

If you don't have an Azure subscription, create a [free account](#) before you begin.

Once your subscription is set up, you'll need an Azure user account with:

- Owner permissions on the Azure subscription
- Permissions to register Azure Active Directory apps

If you just created a free Azure account, you're the owner of your subscription. If you're not the subscription owner, work with the owner to assign the permissions as follows:

1. In the Azure portal, search for "subscriptions", and under **Services**, select **Subscriptions**.

The screenshot shows the Microsoft Azure portal interface. The search bar at the top has 'subscriptions' typed into it. Below the search bar, the 'Services' section is expanded, and 'Subscriptions' is highlighted with a red box. Other options in the Services list include Event Grid Subscriptions, Service Bus, and Resource groups. The 'Resources' section shows 'No results were found.' The 'Marketplace' section lists SharpCloud Subscriptions, Barracuda WAF Add On Subscriptions, Stratum CSP Subscription Management, and Managed Azure Subscription. The 'Documentation' section includes links to 'Subscription decision guide - Cloud Adoption Fram...' and 'How to find your Azure subscription - Azure Media...'. At the bottom of the search results, there are links for 'Try searching in Activity Log' and 'Try searching in Azure Active Directory'. To the right of the search results, there are icons for Azure Synapse Analytics, Virtual machines, App Services, All resources, and Security Center.

2. In the **Subscriptions** page, select the subscription in which you want to create an Azure Migrate project.
3. Select **Access control (IAM)**.
4. Select **Add > Add role assignment** to open the **Add role assignment** page.
5. Assign the following role. For detailed steps, see [Assign Azure roles using the Azure portal](#).

SETTING	VALUE
Role	Owner
Assign access to	User
Members	azmigrateuser (in this example)

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to a...	BuiltinRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you ...	BuiltinRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltinRole	General	View
AcrDelete	acr delete	BuiltinRole	Containers	View
AcrImageSigner	acr image signer	BuiltinRole	Containers	View
AcrPull	acr pull	BuiltinRole	Containers	View
AcrPush	acr push	BuiltinRole	Containers	View
AcrQuarantineReader	acr quarantine data reader	BuiltinRole	Containers	View
AcrQuarantineWriter	acr quarantine data writer	BuiltinRole	Containers	View

[Review + assign](#) [Previous](#) [Next](#)

6. Your Azure account also needs permissions to register Azure Active Directory apps.
7. In Azure portal, navigate to Azure Active Directory > Users > User Settings.
8. In User settings, verify that Azure AD users can register applications (set to Yes by default).

Home > Default Directory > Users

Users | User settings

Default Directory - Azure Active Directory

« Save Discard

- [All users \(Preview\)](#)
- [Deleted users \(Preview\)](#)
- [Password reset](#)
- [User settings](#)
- [Diagnose and solve problems](#)

Activity

- [Sign-ins](#)
- [Audit logs](#)
- [Bulk operation results](#)

Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications [\(i\)](#)

Yes No

Administration portal

Restrict access to Azure AD administration portal [\(i\)](#)

Yes No

9. In case the 'App registrations' settings is set to 'No', request the tenant/global admin to assign the required permission. Alternately, the tenant/global admin can assign the **Application Developer** role to an account to allow the registration of Azure Active Directory App. [Learn more](#).

Download and install Azure Migrate: App Containerization tool

1. [Download](#) the Azure Migrate: App Containerization installer on a Windows machine.
2. Launch PowerShell in administrator mode and change the PowerShell directory to the folder containing the installer.

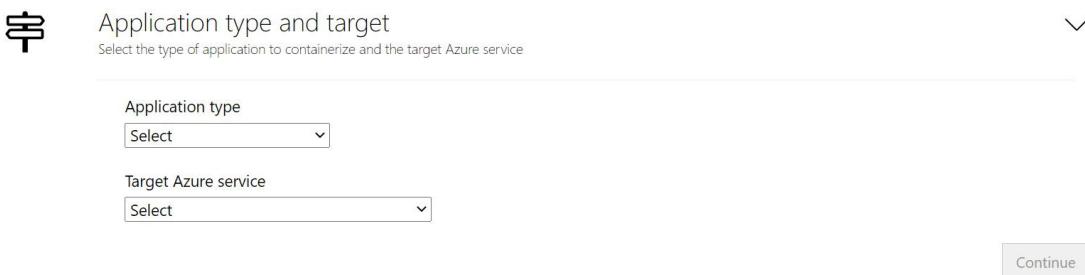
- Run the installation script using the command

```
.\AppContainerizationInstaller.ps1
```

Launch the App Containerization tool

- Open a browser on any machine that can connect to the Windows machine running the App Containerization tool, and open the tool URL: <https://machine name or IP address: 44369>.
Alternately, you can open the app from the desktop by selecting the app shortcut.
- If you see a warning stating that says your connection isn't private, click Advanced and choose to proceed to the website. This warning appears as the web interface uses a self-signed TLS/SSL certificate.
- At the sign-in screen, use the local administrator account on the machine to sign-in.
- Select **Java web apps on Tomcat** as the type of application you want to containerize.
- To specify target Azure service, select **Containers on Azure Kubernetes Service**.

Azure Migrate: App Containerization helper (Preview)



Complete tool pre-requisites

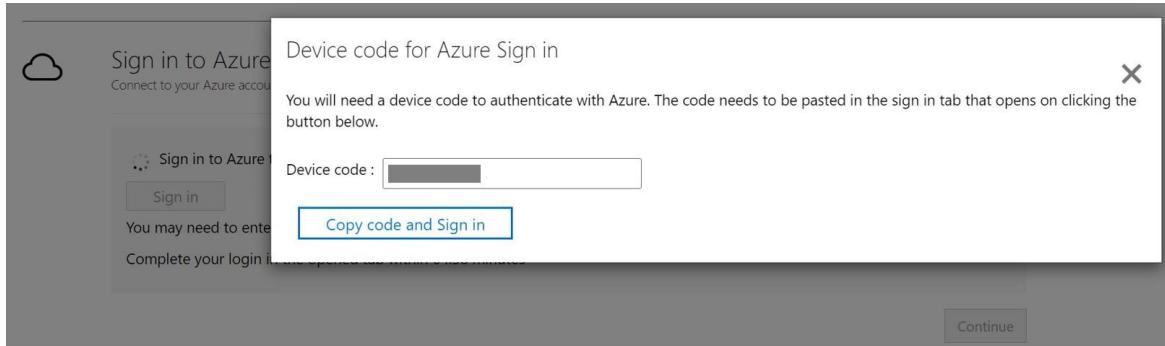
- Accept the **license terms**, and read the third-party information.
- In the tool web app > **Set up prerequisites**, do the following steps:
 - Connectivity:** The tool checks that the Windows machine has internet access. If the machine uses a proxy:
 - Click on **Set up proxy** to specify the proxy address (in the form IP address or FQDN) and listening port.
 - Specify credentials if the proxy needs authentication.
 - Only HTTP proxy is supported.
 - If you've added proxy details or disabled the proxy and/or authentication, click on **Save** to trigger connectivity check again.
 - Install updates:** The tool will automatically check for latest updates and install them. You can also manually install the latest version of the tool from [here](#).
 - Enable Secure Shell (SSH):** The tool will inform you to ensure that Secure Shell (SSH) is enabled on the application servers running the Java web applications to be containerized.

Sign in to Azure

Click **Sign in** to log in to your Azure account.

- You'll need a device code to authenticate with Azure. Clicking on sign in will open a modal with the device code.
- Click on **Copy code & sign in** to copy the device code and open an Azure sign in prompt in a new

browser tab. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.



3. On the new tab, paste the device code and complete sign in using your Azure account credentials. You can close the browser tab after sign in is complete and return to the App Containerization tool's web interface.
4. Select the **Azure tenant** that you want to use.
5. Specify the **Azure subscription** that you want to use.

Discover Java web applications

The App Containerization helper tool connects remotely to the application servers using the provided credentials and attempts to discover Java web applications (running on Apache Tomcat) hosted on the application servers.

1. Specify the **IP address/FQDN** and the **credentials** of the server running the Java web application that should be used to remotely connect to the server for application discovery.
 - The credentials provided must be for a root account (Linux) on the application server.
 - For domain accounts (the user must be an administrator on the application server), prefix the username with the domain name in the format <domain\username>.
 - You can run application discovery for upto five servers at a time.
2. Click **Validate** to verify that the application server is reachable from the machine running the tool and that the credentials are valid. Upon successful validation, the status column will show the status as **Mapped**.

A screenshot of the "Discover applications" wizard. The first step, "Provide server details", shows a table with one row for a server. The columns are "Server IP / FQDN", "Username", "Password", and "Status". The values are 10.0.0.1, root, redacted, and Mapped (with a green checkmark). Buttons for "Add server", "Validate", and "Review" are visible. Below this is a "Review discovered applications" step with a "Review" button.

3. Click **Continue** to start application discovery on the selected application servers.
4. Upon successful completion of application discovery, you can select the list of applications to

containerize.

The screenshot shows a table with one application entry:

Name	Server IP/ FQDN	Target container	Application configurations	Application folders
javaapp	10.0.0.1	(empty)	3 app configuration(s)	Edit

Below the table is a 'Continue' button.

5. Use the checkbox to select the applications to containerize.
6. **Specify container name:** Specify a name for the target container for each selected application. The container name should be specified as `<name:tag>` where the tag is used for container image. For example, you can specify the target container name as `appname:v1`.

Parameterize application configurations

Parameterizing the configuration makes it available as a deployment time parameter. This allows you to configure this setting while deploying the application as opposed to having it hard-coded to a specific value in the container image. For example, this option is useful for parameters like database connection strings.

1. Click **app configurations** to review detected configurations.
2. Select the checkbox to parameterize the detected application configurations.
3. Click **Apply** after selecting the configurations to parameterize.

The screenshot shows a modal dialog with the following content:

Discover applications

Provide server details and run configuration

Review discovered applications

Select applications

File name	Section tag	Attribute name
/opt/tomcat9/webapps/javaapp/META-INF/context.xml	/Context/Resource[@name='jdbc/appname']/@username	username
/opt/tomcat9/webapps/javaapp/META-INF/context.xml	/Context/Resource[@name='jdbc/appname']/@password	password
/opt/tomcat9/webapps/javaapp/META-INF/context.xml	/Context/Resource[@name='jdbc/appname']/@url	url

Buttons: Apply, Continue

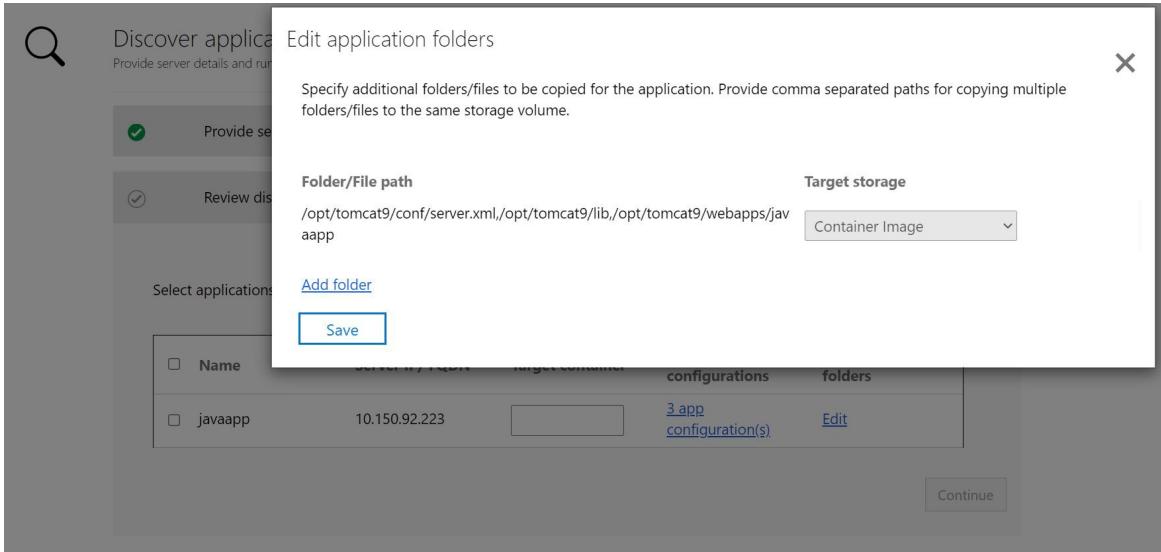
Externalize file system dependencies

You can add other folders that your application uses. Specify if they should be part of the container image or are to be externalized through persistent volumes on Azure file share. Using persistent volumes works great for stateful applications that store state outside the container or have other static content stored on the file system.

[Learn more](#)

1. Click **Edit** under App Folders to review the detected application folders. The detected application folders have been identified as mandatory artifacts needed by the application and will be copied into the container image.

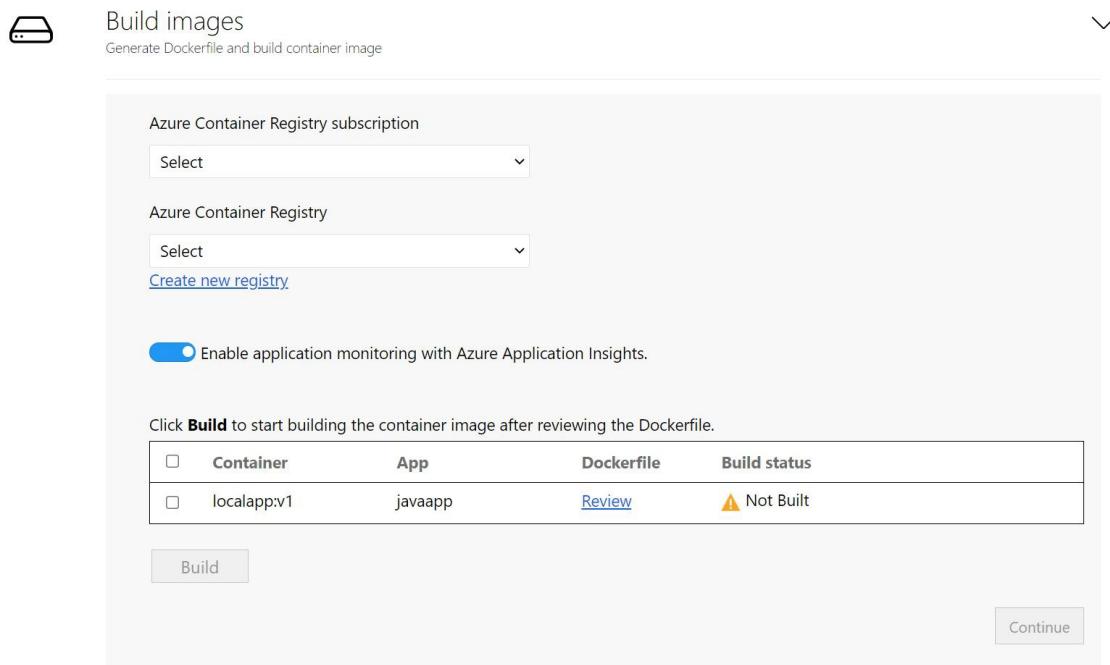
2. Click **Add folders** and specify the folder paths to be added.
3. To add multiple folders to the same volume, provide comma (,) separated values.
4. Select **Persistent Volume** as the storage option if you want the folders to be stored outside the container on a Persistent Volume.
5. Click **Save** after reviewing the application folders.



6. Click **Continue** to proceed to the container image build phase.

Build container image

1. **Select Azure Container Registry:** Use the dropdown to select an [Azure Container Registry](#) that will be used to build and store the container images for the apps. You can use an existing Azure Container Registry or choose to create a new one using the [Create new registry](#) option.



2. **Review the Dockerfile:** The Dockerfile needed to build the container images for each selected application are generated at the beginning of the build step. Click **Review** to review the Dockerfile. You can also add any necessary customizations to the Dockerfile in the review step and save the changes before starting the build process.

3. **Configure Application Insights:** You can enable monitoring for your Java apps running on App Service without instrumenting your code. The tool will install the Java standalone agent as part of the container image. Once configured during deployment, the Java agent will automatically collect a multitude of requests, dependencies, logs, and metrics for your application that can be used for monitoring with Application Insights. This option is enabled by default for all Java applications.
4. **Trigger build process:** Select the applications to build images for and click **Build**. Clicking build will start the container image build for each application. The tool keeps monitoring the build status continuously and will let you proceed to the next step upon successful completion of the build.
5. **Track build status:** You can also monitor progress of the build step by clicking the **Build in Progress** link under the status column. The link takes a couple of minutes to be active after you've triggered the build process.
6. Once the build is completed, click **Continue** to specify deployment settings.

Click **Build** to start building the container image after reviewing the Dockerfile.

<input type="checkbox"/>	Container	App	Dockerfile	Build status
<input checked="" type="checkbox"/>	localapp:v1	javaapp	Review	✓ Successful

Build **Continue**

Deploy the containerized app on AKS

Once the container image is built, the next step is to deploy the application as a container on [Azure Kubernetes Service \(AKS\)](#).

1. **Select the Azure Kubernetes Service Cluster:** Specify the AKS cluster that the application should be deployed to.

- The selected AKS cluster must have a Linux node pool.
- The cluster must be configured to allow pulling of images from the Azure Container Registry that was selected to store the images.
 - Run the following command in Azure CLI to attach the AKS cluster to the ACR.

```
az aks update -n <cluster-name> -g <cluster-resource-group> --attach-acr <acr-name>
```

- If you don't have an AKS cluster or would like to create a new AKS cluster to deploy the application to, you can choose to create one from the tool by clicking **Create new AKS cluster**.
 - The AKS cluster created using the tool will be created with a Linux node pool. The cluster will be configured to allow it to pull images from the Azure Container Registry that was created earlier (if create new registry option was chosen).
- Click **Continue** after selecting the AKS cluster.

2. **Specify secret store and monitoring workspace:** If you had opted to parameterize application configurations, then specify the secret store to be used for the application. You can choose Azure Key Vault or Kubernetes Secrets for managing your application secrets.

- If you've selected Kubernetes secrets for managing secrets, then click **Continue**.
- If you'd like to use an Azure Key Vault for managing your application secrets, then specify the Azure Key Vault that you'd want to use.
 - If you don't have an Azure Key Vault or would like to create a new Key Vault, you can choose to

create on from the tool by clicking **Create new**.

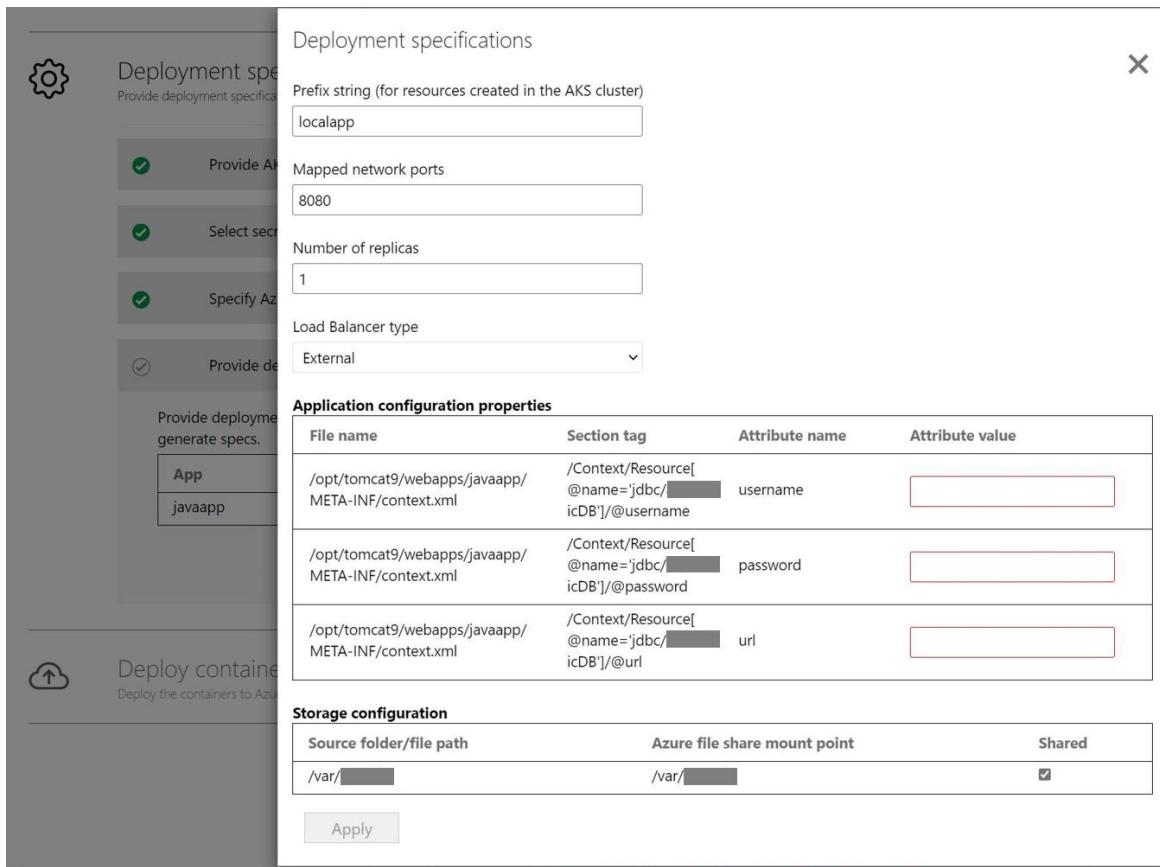
- The tool will automatically assign the necessary permissions for managing secrets through the Key Vault.
- **Monitoring workspace:** If you'd selected to enabled monitoring with Application Insights, then specify the Application Insights resource that you'd want to use. This option won't be visible if you had disabled monitoring integration.
 - If you don't have an Application Insights resource or would like to create a new resource, you can choose to create on from the tool by clicking **Create new**.

3. **Specify Azure file share:** If you had added more folders and selected the Persistent Volume option, then specify the Azure file share that should be used by Azure Migrate: App Containerization tool during the deployment process. The tool will create new directories in this Azure file share to copy over the application folders that are configured for Persistent Volume storage. Once the application deployment is complete, the tool will clean up the Azure file share by deleting the directories it had created.

- If you don't have an Azure file share or would like to create a new Azure file share, you can choose to create on from the tool by clicking **Create new Storage Account and file share**.

4. **Application deployment configuration:** Once you've completed the steps above, you'll need to specify the deployment configuration for the application. Click **Configure** to customize the deployment for the application. In the configure step you can provide the following customizations:

- **Prefix string:** Specify a prefix string to use in the name for all resources that are created for the containerized application in the AKS cluster.
- **Replica Sets:** Specify the number of application instances (pods) that should run inside the containers.
- **Load balancer type:** Select *External* if the containerized application should be reachable from public networks.
- **Application Configuration:** For any application configurations that were parameterized, provide the values to use for the current deployment.
- **Storage:** For any application folders that were configured for Persistent Volume storage, specify whether the volume should be shared across application instances or should be initialized individually with each instance in the container. By default, all application folders on Persistent Volumes are configured as shared.
- Click **Apply** to save the deployment configuration.
- Click **Continue** to deploy the application.



5. Deploy the application: Once the deployment configuration for the application is saved, the tool will generate the Kubernetes deployment YAML for the application.

- Click **Review** to review and customize the Kubernetes deployment YAML for the applications.
- Select the application to deploy.
- Click **Deploy** to start deployments for the selected applications

The screenshot shows the 'Deploy containers' screen. It displays a table with columns for Container, App, Deployment Spec, and Deployment status. One row is shown for 'localapp:v1' associated with the 'javaapp' app and the 'Edit' link. The deployment status is 'Not deployed'. A large blue 'Deploy' button is visible at the bottom right.

- Once the application is deployed, you can click the *Deployment status* column to track the resources that were deployed for the application.

Download generated artifacts

All artifacts that are used to build and deploy the application into AKS, including the Dockerfile and Kubernetes YAML specification files, are stored on the machine running the tool. The artifacts are located at `C:\ProgramData\Microsoft Azure Migrate App Containerization`.

A single folder is created for each application server. You can view and download all intermediate artifacts used in the containerization process by navigating to this folder. The folder, corresponding to the application server, will be cleaned up at the start of each run of the tool for a particular server.

Troubleshoot issues

To troubleshoot any issues with the tool, you can look at the log files on the Windows machine running the App Containerization tool. Tool log files are located at *C:\ProgramData\Microsoft Azure Migrate App Containerization\Logs* folder.

Next steps

- Containerizing Java web apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on App Service. [Learn more](#)
- Containerizing ASP.NET web apps and deploying them on Windows containers on AKS. [Learn more](#)
- Containerizing ASP.NET web apps and deploying them on Windows containers on Azure App Service. [Learn more](#)

ASP.NET app containerization and migration to Azure Kubernetes Service

10/27/2022 • 15 minutes to read • [Edit Online](#)

In this article, you'll learn how to containerize ASP.NET applications and migrate them to [Azure Kubernetes Service \(AKS\)](#) using the Azure Migrate: App Containerization tool. The containerization process doesn't require access to your codebase and provides an easy way to containerize existing applications. The tool works by using the running state of the applications on a server to determine the application components and helps you package them in a container image. The containerized application can then be deployed on Azure Kubernetes Service (AKS).

The Azure Migrate: App Containerization tool currently supports -

- Containerizing ASP.NET apps and deploying them on Windows containers on Azure Kubernetes Service.
- Containerizing ASP.NET apps and deploying them on Windows containers on Azure App Service. [Learn more](#)
- Containerizing Java Web Apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on AKS. [Learn more](#)
- Containerizing Java Web Apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on App Service. [Learn more](#)

The Azure Migrate: App Containerization tool helps you to -

- **Discover your application:** The tool remotely connects to the application servers running your ASP.NET application and discovers the application components. The tool creates a Dockerfile that can be used to create a container image for the application.
- **Build the container image:** You can inspect and further customize the Dockerfile as per your application requirements and use that to build your application container image. The application container image is pushed to an Azure Container Registry you specify.
- **Deploy to Azure Kubernetes Service:** The tool then generates the Kubernetes resource definition YAML files needed to deploy the containerized application to your Azure Kubernetes Service cluster. You can customize the YAML files and use them to deploy the application on AKS.

NOTE

The Azure Migrate: App Containerization tool helps you discover specific application types (ASP.NET and Java web apps on Apache Tomcat) and their components on an application server. To discover servers and the inventory of apps, roles, and features running on on-premises machines, use Azure Migrate: Discovery and assessment capability. [Learn more](#)

While all applications won't benefit from a straight shift to containers without significant rearchitecting, some of the benefits of moving existing apps to containers without rewriting include:

- **Improved infrastructure utilization:** With containers, multiple applications can share resources and be hosted on the same infrastructure. This can help you consolidate infrastructure and improve utilization.
- **Simplified management:** By hosting your applications on a modern managed platform like AKS and App Service, you can simplify your management practices. You can achieve this by retiring or reducing the infrastructure maintenance and management processes that you'd traditionally perform with owned infrastructure.
- **Application portability:** With increased adoption and standardization of container specification formats and platforms, application portability is no longer a concern.

- **Adopt modern management with DevOps:** Helps you adopt and standardize on modern practices for management and security and transition to DevOps.

In this tutorial, you'll learn how to:

- Set up an Azure account.
- Install the Azure Migrate: App Containerization tool.
- Discover your ASP.NET application.
- Build the container image.
- Deploy the containerized application on AKS.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths.

Prerequisites

Before you begin this tutorial, you should:

REQUIREMENT	DETAILS
Identify a machine to install the tool	<p>A Windows machine to install and run the Azure Migrate: App Containerization tool. The Windows machine could be a server (Windows Server 2016 or later) or client (Windows 10) operating system, meaning that the tool can run on your desktop as well.</p> <p>The Windows machine running the tool should have network connectivity to the servers/virtual machines hosting the ASP.NET applications to be containerized.</p> <p>Ensure that 6-GB space is available on the Windows machine running the Azure Migrate: App Containerization tool for storing application artifacts.</p> <p>The Windows machine should have internet access, directly or via a proxy.</p> <p>Install the Microsoft Web Deploy tool on the machine running the App Containerization helper tool and application server if not already installed. You can download the tool from here</p>
Application servers	<p>Enable PowerShell remoting on the application servers: Log in to the application server and Follow these instructions to turn on PowerShell remoting.</p> <p>If the application server is running Window Server 2008 R2, ensure that PowerShell 5.1 is installed on the application server. Follow the instruction here to download and install PowerShell 5.1 on the application server.</p> <p>Install the Microsoft Web Deploy tool on the machine running the App Containerization helper tool and application server if not already installed. You can download the tool from here</p>

REQUIREMENT	DETAILS
ASP.NET application	<p>The tool currently supports</p> <ul style="list-style-type: none"> - ASP.NET applications using Microsoft .NET framework 3.5 or later. - Application servers running Windows Server 2008 R2 or later (application servers should be running PowerShell version 5.1). - Applications running on Internet Information Services (IIS) 7.5 or later. <p>The tool currently doesn't support</p> <ul style="list-style-type: none"> - Applications requiring Windows authentication (AKS doesn't support gMSA currently). - Applications that depend on other Windows services hosted outside IIS.

Prepare an Azure user account

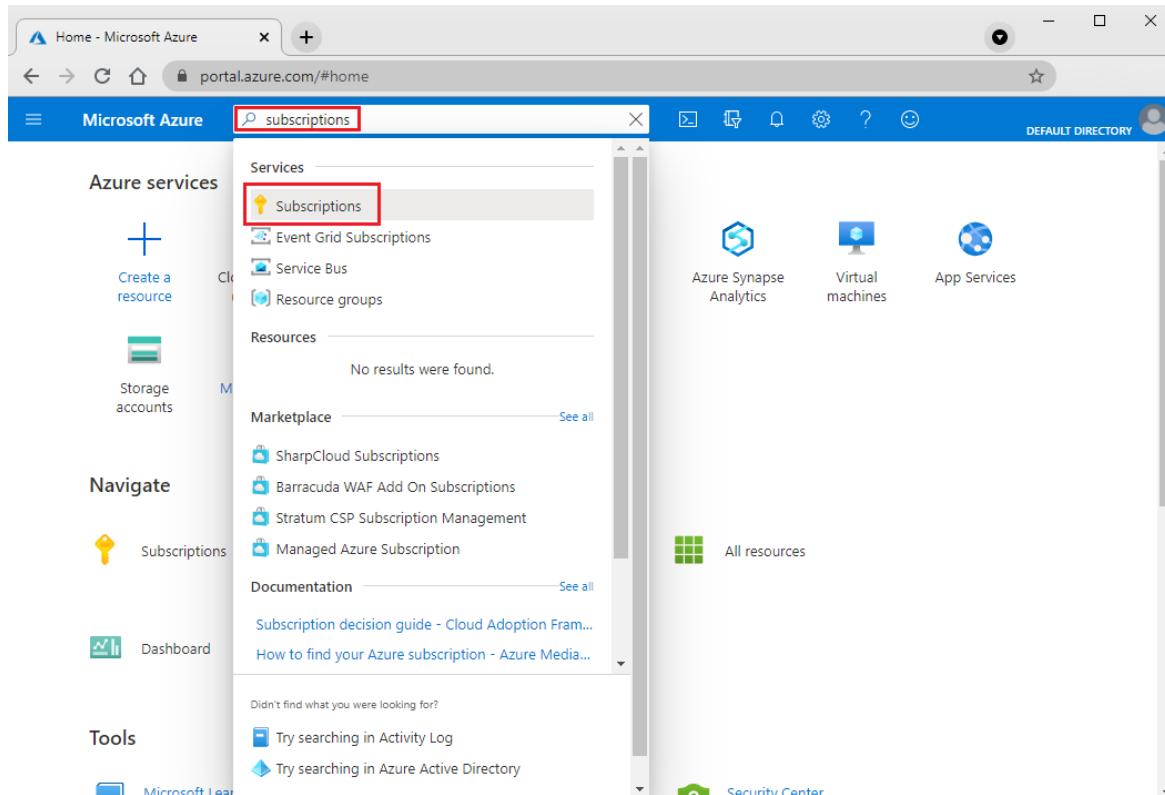
If you don't have an Azure subscription, create a [free account](#) before you begin.

Once your subscription is set up, you'll need an Azure user account with:

- Owner permissions on the Azure subscription
- Permissions to register Azure Active Directory apps

If you just created a free Azure account, you're the owner of your subscription. If you're not the subscription owner, work with the owner to assign the permissions as follows:

1. In the Azure portal, search for "subscriptions", and under **Services**, select **Subscriptions**.



2. In the **Subscriptions** page, select the subscription in which you want to create an Azure Migrate project.
3. Select **Access control (IAM)**.

4. Select **Add > Add role assignment** to open the **Add role assignment** page.
5. Assign the following role. For detailed steps, see [Assign Azure roles using the Azure portal](#).

SETTING	VALUE
Role	Owner
Assign access to	User
Members	azmigrateuser (in this example)

The screenshot shows the 'Add role assignment' interface. At the top, there's a breadcrumb navigation: Home > Add role assignment. Below that, there are three tabs: Role (which is selected), Members, and Review + assign. A search bar and filters for Type (All) and Category (All) are also present. The main area displays a table of roles with columns for Name, Description, Type, Category, and Details. The 'Owner' role is selected and highlighted in blue. Other roles listed include Contributor, Reader, AcrDelete, AcrImageSigner, AcrPull, AcrPush, AcrQuarantineReader, and AcrQuarantineWriter. At the bottom, there are buttons for 'Review + assign', 'Previous', and 'Next'.

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Owner	Grants full access to manage all resources, including the ability to a...	BuiltinRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you ...	BuiltinRole	General	View
Reader	View all resources, but does not allow you to make any changes.	BuiltinRole	General	View
AcrDelete	acr delete	BuiltinRole	Containers	View
AcrImageSigner	acr image signer	BuiltinRole	Containers	View
AcrPull	acr pull	BuiltinRole	Containers	View
AcrPush	acr push	BuiltinRole	Containers	View
AcrQuarantineReader	acr quarantine data reader	BuiltinRole	Containers	View
AcrQuarantineWriter	acr quarantine data writer	BuiltinRole	Containers	View

6. Your Azure account also needs permissions to register Azure Active Directory apps.
7. In Azure portal, navigate to **Azure Active Directory > Users > User Settings**.
8. In **User settings**, verify that Azure AD users can register applications (set to **Yes** by default).

Users | User settings

All users (Preview)

Deleted users (Preview)

Password reset

User settings

Diagnose and solve problems

Activity

Sign-ins

Audit logs

Bulk operation results

Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications

Yes No

Administration portal

Restrict access to Azure AD administration portal

Yes No

9. In case the 'App registrations' settings is set to 'No', request the tenant/global admin to assign the required permission. Alternately, the tenant/global admin can assign the **Application Developer** role to an account to allow the registration of Azure Active Directory App. [Learn more](#).

Download and install Azure Migrate: App Containerization tool

1. [Download](#) the Azure Migrate: App Containerization installer on a Windows machine.
2. Launch PowerShell in administrator mode and change the PowerShell directory to the folder containing the installer.
3. Run the installation script using the command

```
.\AppContainerizationInstaller.ps1
```

Launch the App Containerization tool

1. Open a browser on any machine that can connect to the Windows machine running the App Containerization tool, and open the tool URL: <https://machine name or IP address: 44369>.
Alternately, you can open the app from the desktop by selecting the app shortcut.
2. If you see a warning stating that says your connection isn't private, click Advanced and choose to proceed to the website. This warning appears as the web interface uses a self-signed TLS/SSL certificate.
3. At the sign in screen, use the local administrator account on the machine to sign in.
4. Select **ASP.NET web apps** as the type of application you want to containerize.
5. To specify target Azure service, select **Containers on Azure Kubernetes Service**.

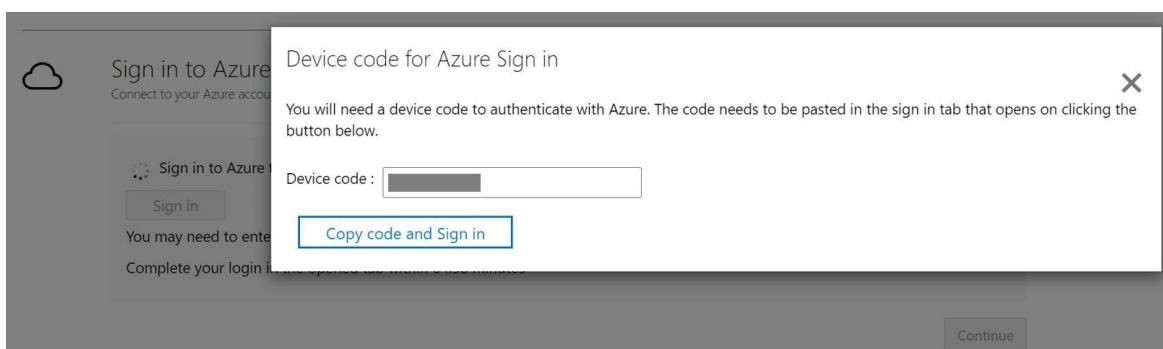
Complete tool pre-requisites

1. Accept the **license terms**, and read the third-party information.
2. In the tool web app > **Set up prerequisites**, do the following steps:
 - **Connectivity:** The tool checks that the Windows machine has internet access. If the machine uses a proxy:
 - Click on **Set up proxy** to specify the proxy address (in the form IP address or FQDN) and listening port.
 - Specify credentials if the proxy needs authentication.
 - Only HTTP proxy is supported.
 - If you've added proxy details or disabled the proxy and/or authentication, click on **Save** to trigger connectivity check again.
 - **Install updates:** The tool will automatically check for latest updates and install them. You can also manually install the latest version of the tool from [here](#).
 - **Install Microsoft Web Deploy tool:** The tool will check that the Microsoft Web Deploy tool is installed on the Windows machine running the Azure Migrate: App Containerization tool.
 - **Enable PowerShell remoting:** The tool will inform you to ensure that PowerShell remoting is enabled on the application servers running the ASP.NET applications to be containerized.

Sign in to Azure

Click **Sign in** to log in to your Azure account.

1. You'll need a device code to authenticate with Azure. Clicking on sign in will open a modal with the device code.
2. Click on **Copy code & sign in** to copy the device code and open an Azure sign in prompt in a new browser tab. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.



3. On the new tab, paste the device code and complete sign in using your Azure account credentials. You can close the browser tab after sign in is complete and return to the App Containerization tool's web interface.
4. Select the **Azure tenant** that you want to use.

5. Specify the Azure subscription that you want to use.

Discover ASP.NET applications

The App Containerization helper tool connects remotely to the application servers using the provided credentials and attempts to discover ASP.NET applications hosted on the application servers.

1. Specify the IP address/FQDN and the credentials of the server running the ASP.NET application that should be used to remotely connect to the server for application discovery.

- The credentials provided must be for a local administrator (Windows) on the application server.
- For domain accounts (the user must be an administrator on the application server), prefix the username with the domain name in the format <domain\username>.
- You can run application discovery for upto five servers at a time.

2. Click **Validate** to verify that the application server is reachable from the machine running the tool and that the credentials are valid. Upon successful validation, the status column will show the status as **Mapped**.

The screenshot shows the 'Discover applications' wizard with the following steps:

- Step 1: Provide server details**
 - Contains fields for Server IP/ FQDN (127.0.0.1), Username (webvm\demouser), and Password (redacted).
 - Status: Mapped (green checkmark).
 - Buttons: Add server, Validate (highlighted in blue), and Continue.
- Step 2: Review discovered applications**
 - Contains a message: 1 application(s) discovered.
 - Instructions: Select applications to containerize, configurations to parameterize, and folders to migrate.
 - Table:

Name	Server IP/ FQDN	Target container	Application configurations	Application folders
localapp	127.0.0.1	(empty)	1 app configuration(s)	Edit
 - Buttons: Continue.

3. Click **Continue** to start application discovery on the selected application servers.

4. Upon successful completion of application discovery, you can select the list of applications to containerize.

The screenshot shows the 'Discover applications' wizard with the following steps:

- Step 1: Provide server details** (not visible in this screenshot)
- Step 2: Review discovered applications**
 - Contains a message: 1 application(s) discovered.
 - Instructions: Select applications to containerize, configurations to parameterize, and folders to migrate.
 - Table:

Name	Server IP/ FQDN	Target container	Application configurations	Application folders
localapp	127.0.0.1	(empty)	1 app configuration(s)	Edit
 - Buttons: Continue.

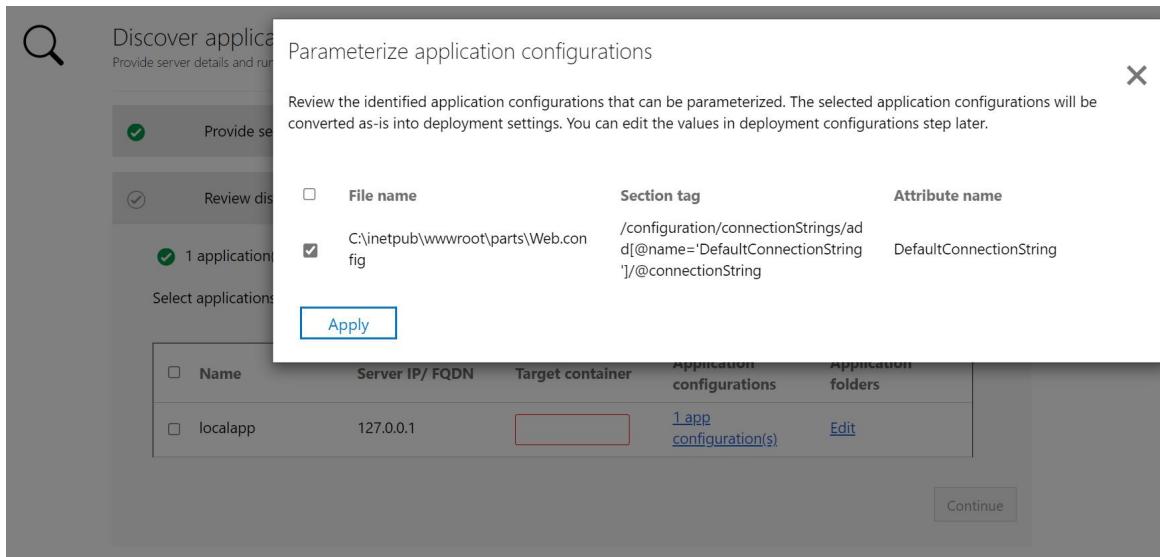
5. Use the checkbox to select the applications to containerize.

6. **Specify container name:** Specify a name for the target container for each selected application. The container name should be specified as <name:tag> where the tag is used for container image. For example, you can specify the target container name as *appname:v1*.

Parameterize application configurations

Parameterizing the configuration makes it available as a deployment time parameter. This allows you to configure this setting while deploying the application as opposed to having it hard-coded to a specific value in the container image. For example, this option is useful for parameters like database connection strings.

1. Click **app configurations** to review detected configurations.
2. Select the checkbox to parameterize the detected application configurations.
3. Click **Apply** after selecting the configurations to parameterize.

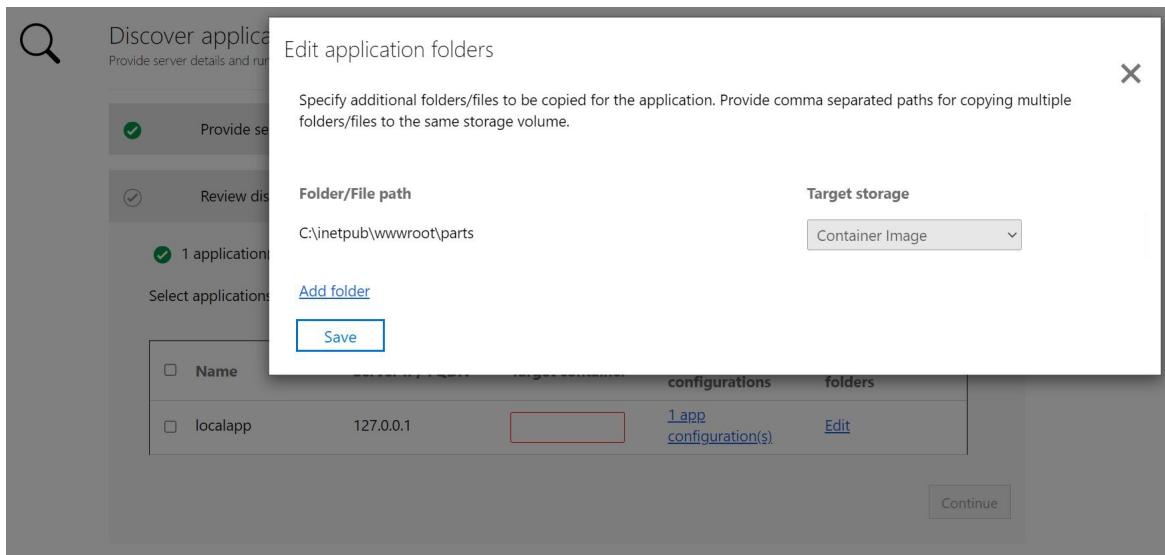


Externalize file system dependencies

You can add other folders that your application uses. Specify if they should be part of the container image or are to be externalized through persistent volumes on Azure file share. Using persistent volumes works great for stateful applications that store state outside the container or have other static content stored on the file system.

[Learn more](#)

1. Click **Edit** under App Folders to review the detected application folders. The detected application folders have been identified as mandatory artifacts needed by the application and will be copied into the container image.
2. Click **Add folders** and specify the folder paths to be added.
3. To add multiple folders to the same volume, provide comma (,) separated values.
4. Select **Persistent Volume** as the storage option if you want the folders to be stored outside the container on a Persistent Volume.
5. Click **Save** after reviewing the application folders.



6. Click **Continue** to proceed to the container image build phase.

Build container image

1. **Select Azure Container Registry:** Use the dropdown to select an [Azure Container Registry](#) that will be used to build and store the container images for the apps. You can use an existing Azure Container Registry or choose to create a new one using the Create new registry option.

Container	App	Dockerfile	Build status
localapp:v1	localapp	Review	⚠ Not Built

2. **Review the Dockerfile:** The Dockerfile needed to build the container images for each selected application are generated at the beginning of the build step. Click **Review** to review the Dockerfile. You can also add any necessary customizations to the Dockerfile in the review step and save the changes before starting the build process.
3. **Trigger build process:** Select the applications to build images for and click **Build**. Clicking build will start the container image build for each application. The tool keeps monitoring the build status continuously and will let you proceed to the next step upon successful completion of the build.
4. **Track build status:** You can also monitor progress of the build step by clicking the **Build in Progress** link under the status column. The link takes a couple of minutes to be active after you've triggered the build process.
5. Once the build is completed, click **Continue** to specify deployment settings.

Review the generated Dockerfile. Select applications and click **Build** to start building the container image.

<input type="checkbox"/> Container	App	Dockerfile	Build status
<input checked="" type="checkbox"/> localapp:v1	localapp	Review	Successful

[Build](#)

[Continue](#)

Deploy the containerized app on AKS

Once the container image is built, the next step is to deploy the application as a container on [Azure Kubernetes Service \(AKS\)](#).

1. **Select the Azure Kubernetes Service Cluster:** Specify the AKS cluster that the application should be deployed to.

- The selected AKS cluster must have a Windows node pool.
- The cluster must be configured to allow pulling of images from the Azure Container Registry that was selected to store the images.
 - Run the following command in Azure CLI to attach the AKS cluster to the ACR.

```
az aks update -n <cluster-name> -g <cluster-resource-group> --attach-acr <acr-name>
```

- If you don't have an AKS cluster or would like to create a new AKS cluster to deploy the application to, you can choose to create one from the tool by clicking **Create new AKS cluster**.
 - The AKS cluster created using the tool will be created with a Windows node pool. The cluster will be configured to allow it to pull images from the Azure Container Registry that was created earlier (if create new registry option was chosen).
- Click **Continue** after selecting the AKS cluster.

2. **Specify secret store:** If you had opted to parameterize application configurations, then specify the secret store to be used for the application. You can choose Azure Key Vault or App Service application settings for managing your application secrets. [Learn more](#)

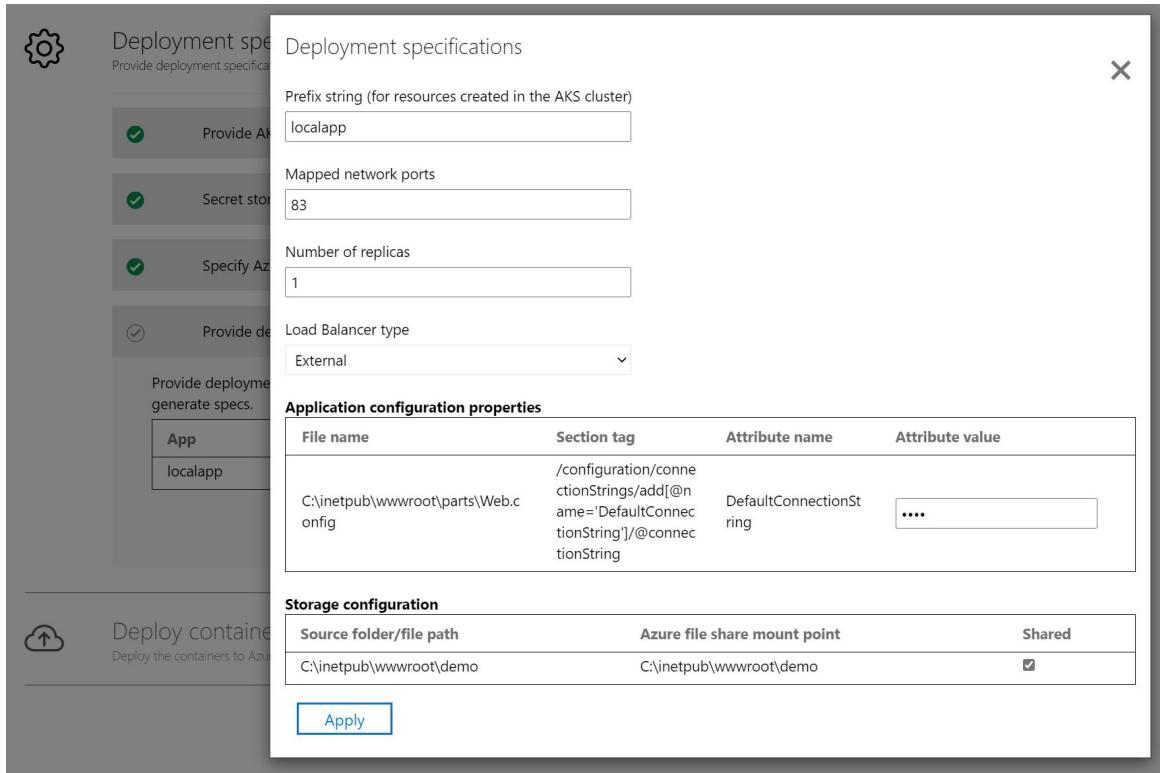
- If you've selected App Service application settings for managing secrets, then click **Continue**.
- If you'd like to use an Azure Key Vault for managing your application secrets, then specify the Azure Key Vault that you'd want to use.
 - If you don't have an Azure Key Vault or would like to create a new Key Vault, you can choose to create one from the tool by clicking **Create new Azure Key Vault**.
 - The tool will automatically assign the necessary permissions for managing secrets through the Key Vault.

3. **Specify Azure file share:** If you had added more folders and selected the Persistent Volume option, then specify the Azure file share that should be used by Azure Migrate: App Containerization tool during the deployment process. The tool will create new directories in this Azure file share to copy over the application folders that are configured for Persistent Volume storage. Once the application deployment is complete, the tool will clean up the Azure file share by deleting the directories it had created.

- If you don't have an Azure file share or would like to create a new Azure file share, you can choose to create one from the tool by clicking **Create new Storage Account and file share**.

4. **Application deployment configuration:** Once you've completed the steps above, you'll need to specify the deployment configuration for the application. Click **Configure** to customize the deployment for the application. In the configure step you can provide the following customizations:

- **Prefix string:** Specify a prefix string to use in the name for all resources that are created for the containerized application in the AKS cluster.
- **SSL certificate:** If your application requires an https site binding, specify the PFX file that contains the certificate to be used for the binding. The PFX file shouldn't be password protected and the original site shouldn't have multiple bindings.
- **Replica Sets:** Specify the number of application instances (pods) that should run inside the containers.
- **Load balancer type:** Select *External* if the containerized application should be reachable from public networks.
- **Application Configuration:** For any application configurations that were parameterized, provide the values to use for the current deployment.
- **Storage:** For any application folders that were configured for Persistent Volume storage, specify whether the volume should be shared across application instances or should be initialized individually with each instance in the container. By default, all application folders on Persistent Volumes are configured as shared.
- Click **Apply** to save the deployment configuration.
- Click **Continue** to deploy the application.



5. **Deploy the application:** Once the deployment configuration for the application is saved, the tool will generate the Kubernetes deployment YAML for the application.

- Click **Review** to review and customize the Kubernetes deployment YAML for the applications.
- Select the application to deploy.
- Click **Deploy** to start deployments for the selected applications

The screenshot shows a user interface for deploying containers to Azure Kubernetes Service (AKS). At the top, there's a cloud icon with an upward arrow and the text "Deploy containers". Below it, a sub-header says "Deploy the containers to Azure". A large callout box contains instructions: "Review the deployment spec and click **Deploy** to deploy container to AKS". Inside this box is a table:

<input type="checkbox"/> Container	App	Deployment Spec	Deployment status
<input checked="" type="checkbox"/> localapp:v1	localapp	Edit	⚠ Not deployed

At the bottom right of the callout box is a blue "Deploy" button.

- Once the application is deployed, you can click the *Deployment status* column to track the resources that were deployed for the application.

Download generated artifacts

All artifacts that are used to build and deploy the application into AKS, including the Dockerfile and Kubernetes YAML specification files, are stored on the machine running the tool. The artifacts are located at *C:\ProgramData\Microsoft Azure Migrate App Containerization*.

A single folder is created for each application server. You can view and download all intermediate artifacts used in the containerization process by navigating to this folder. The folder, corresponding to the application server, will be cleaned up at the start of each run of the tool for a particular server.

Troubleshoot issues

To troubleshoot any issues with the tool, you can look at the log files on the Windows machine running the App Containerization tool. Tool log files are located at *C:\ProgramData\Microsoft Azure Migrate App Containerization\Logs* folder.

Next steps

- Containerizing ASP.NET web apps and deploying them on Windows containers on App Service. [Learn more](#)
- Containerizing Java web apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on AKS. [Learn more](#)
- Containerizing Java web apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on App Service. [Learn more](#)

Terminate a long running operation on an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 2 minutes to read • [Edit Online](#)

Sometimes deployment or other processes running within pods on nodes in a cluster can run for periods of time longer than expected due to various reasons. While it's important to allow those processes to gracefully terminate when they're no longer needed, there are circumstances where you need to release control of node pools and clusters with long running operations using an *abort* command.

AKS now supports aborting a long running operation, allowing you to take back control and run another operation seamlessly. This design is supported using the [Azure REST API](#) or the [Azure CLI](#).

The abort operation supports the following scenarios:

- If a long running operation is stuck or suspected to be in a bad state or failing, the operation can be aborted provided it's the last running operation on the Managed Cluster or agent pool.
- If a long running operation is stuck or failing, that operation can be aborted.
- An operation that was triggered in error can be aborted as long as the operation doesn't reach a terminal state first.

Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, start with reviewing our guidance on how to design, secure, and operate an AKS cluster to support your production-ready workloads. For more information, see [AKS architecture guidance](#).

Abort a long running operation

- [Azure CLI](#)
- [Azure REST API](#)

You can use the `az aks nodepool` command with the `operation-abort` argument to abort an operation on a node pool or a managed cluster.

The following example terminates an operation on a node pool on a specified cluster by its name and resource group that holds the cluster.

```
az aks nodepool operation-abort --resource-group myResourceGroup --cluster-name myAKSCluster --name myNodePool
```

The following example terminates an operation against a specified managed cluster its name and resource group that holds the cluster.

```
az aks operation-abort --name myAKSCluster --resource-group myResourceGroup
```

In the response, an HTTP status code of 204 is returned.

The provisioning state on the managed cluster or agent pool should be **Canceled**. Use the REST API [Get Managed Clusters](#) or [Get Agent Pools](#) to verify the operation. The provisioning state should update to **Canceled**

within a few seconds of the abort request being accepted. Operation status of last running operation ID on the managed cluster/agent pool, which can be retrieved by performing a GET operation against the Managed Cluster or agent pool, should show a status of **C canceling**.

Next steps

Learn more about [Container insights](#) to understand how it helps you monitor the performance and health of your Kubernetes cluster and container workloads.

Automatically upgrade an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 3 minutes to read • [Edit Online](#)

Part of the AKS cluster lifecycle involves performing periodic upgrades to the latest Kubernetes version. It's important you apply the latest security releases, or upgrade to get the latest features. Before learning about auto-upgrade, make sure you understand upgrade fundamentals by reading [Upgrade an AKS cluster](#).

Why use auto-upgrade

Auto-upgrade provides a set once and forget mechanism that yields tangible time and operational cost benefits. By enabling auto-upgrade, you can ensure your clusters are up to date and don't miss the latest AKS features or patches from AKS and upstream Kubernetes.

AKS follows a strict versioning window with regard to supportability. With properly selected auto-upgrade channels, you can avoid clusters falling into an unsupported version. For more on the AKS support window, see [Supported Kubernetes versions](#).

Using auto-upgrade

Automatically completed upgrades are functionally the same as manual upgrades. The timing of upgrades is determined by the selected channel.

The following upgrade channels are available:

CHANNEL	ACTION	EXAMPLE
<code>none</code>	disables auto-upgrades and keeps the cluster at its current version of Kubernetes	Default setting if left unchanged
<code>patch</code>	automatically upgrade the cluster to the latest supported patch version when it becomes available while keeping the minor version the same.	For example, if a cluster is running version <code>1.17.7</code> and versions <code>1.17.9</code> , <code>1.18.4</code> , <code>1.18.6</code> , and <code>1.19.1</code> are available, your cluster is upgraded to <code>1.17.9</code>
<code>stable</code>	automatically upgrade the cluster to the latest supported patch release on minor version $N-1$, where N is the latest supported minor version.	For example, if a cluster is running version <code>1.17.7</code> and versions <code>1.17.9</code> , <code>1.18.4</code> , <code>1.18.6</code> , and <code>1.19.1</code> are available, your cluster is upgraded to <code>1.18.6</code> .
<code>rapid</code>	automatically upgrade the cluster to the latest supported patch release on the latest supported minor version.	In cases where the cluster is at a version of Kubernetes that is at an $N-2$ minor version where N is the latest supported minor version, the cluster first upgrades to the latest supported patch version on $N-1$ minor version. For example, if a cluster is running version <code>1.17.7</code> and versions <code>1.17.9</code> , <code>1.18.4</code> , <code>1.18.6</code> , and <code>1.19.1</code> are available, your cluster first is upgraded to <code>1.18.6</code> , then is upgraded to <code>1.19.1</code> .

CHANNEL	ACTION	EXAMPLE
node-image	automatically upgrade the node image to the latest version available.	Microsoft provides patches and new images for image nodes frequently (usually weekly), but your running nodes won't get the new images unless you do a node image upgrade. Turning on the node-image channel will automatically update your node images whenever a new version is available.

NOTE

Cluster auto-upgrade only updates to GA versions of Kubernetes and will not update to preview versions.

Automatically upgrading a cluster follows the same process as manually upgrading a cluster. For more information, see [Upgrade an AKS cluster](#).

To set the auto-upgrade channel when creating a cluster, use the *auto-upgrade-channel* parameter, similar to the following example.

```
az aks create --resource-group myResourceGroup --name myAKSCluster --auto-upgrade-channel stable --generate-ssh-keys
```

To set the auto-upgrade channel on existing cluster, update the *auto-upgrade-channel* parameter, similar to the following example.

```
az aks update --resource-group myResourceGroup --name myAKSCluster --auto-upgrade-channel stable
```

Using auto-upgrade with Planned Maintenance

If you're using Planned Maintenance and Auto-Upgrade, your upgrade will start during your specified maintenance window. For more information on Planned Maintenance, see [Use Planned Maintenance to schedule maintenance windows for your Azure Kubernetes Service \(AKS\) cluster](#).

Best practices for auto-upgrade

The following best practices will help maximize your success when using auto-upgrade:

- In order to keep your cluster always in a supported version (i.e within the N-2 rule), choose either `stable` or `rapid` channels.
- If you're interested in getting the latest patches as soon as possible, use the `patch` channel. The `node-image` channel is a good fit if you want your agent pools to always be running the most recent node images.
- Follow [Operator best practices](#).
- Follow [PDB best practices](#).

Configure an AKS cluster

10/27/2022 • 15 minutes to read • [Edit Online](#)

As part of creating an AKS cluster, you may need to customize your cluster configuration to suit your needs. This article introduces a few options for customizing your AKS cluster.

OS configuration

AKS supports Ubuntu 18.04 as the default node operating system (OS) in general availability (GA) for clusters.

Container runtime configuration

A container runtime is software that executes containers and manages container images on a node. The runtime helps abstract away sys-calls or operating system (OS) specific functionality to run containers on Linux or Windows. For Linux node pools, `containerd` is used for node pools using Kubernetes version 1.19 and greater. For Windows Server 2019 node pools, `containerd` is generally available and will be the only container runtime option in Kubernetes 1.21 and greater. Docker is no longer supported as of September 2022. For more information about this deprecation, see the [AKS release notes](#).

`Containerd` is an [OCI](#) (Open Container Initiative) compliant core container runtime that provides the minimum set of required functionality to execute containers and manage images on a node. It was [donated](#) to the Cloud Native Compute Foundation (CNCF) in March of 2017. The current Moby (upstream Docker) version that AKS uses already uses and is built on top of `containerd`, as shown above.

With a `containerd`-based node and node pools, instead of talking to the `dockershim`, the kubelet will talk directly to `containerd` via the CRI (container runtime interface) plugin, removing extra hops on the flow when compared to the Docker CRI implementation. As such, you'll see better pod startup latency and less resource (CPU and memory) usage.

By using `containerd` for AKS nodes, pod startup latency improves and node resource consumption by the container runtime decreases. These improvements are enabled by this new architecture where kubelet talks directly to `containerd` through the CRI plugin while in Moby/docker architecture kubelet would talk to the `dockershim` and docker engine before reaching `containerd`, thus having extra hops on the flow.



`Containerd` works on every GA version of Kubernetes in AKS, and in every upstream kubernetes version above v1.19, and supports all Kubernetes and AKS features.

IMPORTANT

Clusters with Linux node pools created on Kubernetes v1.19 or greater default to `containerd` for its container runtime. Clusters with node pools on earlier supported Kubernetes versions receive Docker for their container runtime. Linux node pools will be updated to `containerd` once the node pool Kubernetes version is updated to a version that supports `containerd`.

`containerd` with Windows Server 2019 node pools is generally available, and is the only container runtime option in Kubernetes 1.21 and higher. You can continue using Docker node pools and clusters on versions earlier than 1.23, but Docker is no longer supported as of September 2022. For more information, see [Add a Windows Server node pool with containerd](#).

It is highly recommended you test your workloads on AKS node pools with `containerd` before using clusters with a Kubernetes version that supports `containerd` for your node pools.

`Containerd` limitations/differences

- For `containerd`, we recommend using `cricctl` as a replacement CLI instead of the Docker CLI for troubleshooting pods, containers, and container images on Kubernetes nodes (for example, `cricctl ps`).
 - It doesn't provide the complete functionality of the docker CLI. It's intended for troubleshooting only.
 - `cricctl` offers a more kubernetes-friendly view of containers, with concepts like pods, etc. being present.
- `Containerd` sets up logging using the standardized `cri` logging format (which is different from what you currently get from docker's json driver). Your logging solution needs to support the `cri` logging format (like [Azure Monitor for Containers](#))
- You can no longer access the docker engine, `/var/run/docker.sock`, or use Docker-in-Docker (DinD).
 - If you currently extract application logs or monitoring data from Docker Engine, use [Container insights](#) instead. Additionally AKS doesn't support running any out of band commands on the agent nodes that could cause instability.
 - Building images and directly using the Docker engine using the methods above isn't recommended. Kubernetes isn't fully aware of those consumed resources, and those approaches present numerous issues detailed [here](#) and [here](#), for example.
- Building images - You can continue to use your current docker build workflow as normal, unless you're building images inside your AKS cluster. In this case, consider switching to the recommended approach for building images using [ACR Tasks](#), or a more secure in-cluster option like `docker buildx`.

Generation 2 virtual machines

Azure supports [Generation 2 \(Gen2\) virtual machines \(VMs\)](#). Generation 2 VMs support key features that aren't supported in generation 1 VMs (Gen1). These features include increased memory, Intel Software Guard Extensions (Intel SGX), and virtualized persistent memory (vPMEM).

Generation 2 VMs use the new UEFI-based boot architecture rather than the BIOS-based architecture used by generation 1 VMs. Only specific SKUs and sizes support Gen2 VMs. Check the [list of supported sizes](#), to see if your SKU supports or requires Gen2.

Additionally not all VM images support Gen2, on AKS Gen2 VMs will use the new [AKS Ubuntu 18.04 image](#). This image supports all Gen2 SKUs and sizes.

Default OS disk sizing

By default, when creating a new cluster or adding a new node pool to an existing cluster, the disk size is determined by the number of vCPUs, which is based on the VM SKU. The default values are shown in the following table:

VM SKU CORES (VCPU)	DEFAULT OS DISK TIER	PROVISIONED IOPS	PROVISIONED THROUGHPUT (MPBS)
1 - 7	P10/128G	500	100
8 - 15	P15/256G	1100	125
16 - 63	P20/512G	2300	150
64+	P30/1024G	5000	200

IMPORTANT

Default OS disk sizing is only used on new clusters or node pools when Ephemeral OS disks are not supported and a default OS disk size isn't specified. The default OS disk size may impact the performance or cost of your cluster, but you can change the sizing of the OS disk at any time after cluster or node pool creation. This default disk sizing affects clusters or node pools created in July 2022 or later.

Ephemeral OS

By default, Azure automatically replicates the operating system disk for a virtual machine to Azure storage to avoid data loss if the VM needs to be relocated to another host. However, since containers aren't designed to have local state persisted, this behavior offers limited value while providing some drawbacks, including slower node provisioning and higher read/write latency.

By contrast, ephemeral OS disks are stored only on the host machine, just like a temporary disk. This provides lower read/write latency, along with faster node scaling and cluster upgrades.

Like the temporary disk, an ephemeral OS disk is included in the price of the virtual machine, so you don't incur more storage costs.

IMPORTANT

When you don't explicitly request managed disks for the OS, AKS will default to ephemeral OS if possible for a given node pool configuration.

If you chose to use an ephemeral OS, the OS disk must fit in the VM cache. The sizes for VM cache are available in the [Azure documentation](#) in parentheses next to IO throughput ("cache size in GiB").

If you chose to use the AKS default VM size [Standard_DS2_v2](#) SKU with the default OS disk size of 100 GB, this VM size supports ephemeral OS but only has 86 GB of cache size. This configuration would default to managed disks if you don't explicitly specify it. If you do request an ephemeral OS, you'll receive a validation error.

If you request the same [Standard_DS2_v2](#) SKU with a 60GB OS disk, this configuration would default to ephemeral OS: the requested size of 60GB is smaller than the maximum cache size of 86 GB.

If you select the [Standard_D8s_v3](#) SKU with 100 GB OS disk, this VM size supports ephemeral OS and has 200 GB of cache space. If you don't specify the OS disk type, the node pool would receive ephemeral OS by default.

The latest generation of VM series doesn't have a dedicated cache, but only temporary storage. Let's assume to use the [Standard_E2bds_v5](#) VM size with the default OS disk size of 100 GiB as an example. This VM size

supports ephemeral OS disks but only has 75 GiB of temporary storage. This configuration would default to managed OS disks if you don't explicitly specify it. If you do request an ephemeral OS disk, you'll receive a validation error.

If you request the same [Standard_E2bds_v5](#) VM size with a 60 GiB OS disk, this configuration would default to ephemeral OS disks. The requested size of 60 GiB is smaller than the maximum temporary storage of 75 GiB.

If you chose to use [Standard_E4bds_v5](#) SKU with 100 GiB OS disk, this VM size supports ephemeral OS and has 150 GiB of temporary storage. If you don't specify the OS disk type, the node pool is provisioned with an ephemeral OS by default.

Ephemeral OS requires at least version 2.15.0 of the Azure CLI.

Use Ephemeral OS on new clusters

Configure the cluster to use Ephemeral OS disks when the cluster is created. Use the `--node-osdisk-type` flag to set Ephemeral OS as the OS disk type for the new cluster.

```
az aks create --name myAKSCluster --resource-group myResourceGroup -s Standard_DS3_v2 --node-osdisk-type Ephemeral
```

If you want to create a regular cluster using network-attached OS disks, you can do so by specifying `--node-osdisk-type=Managed`. You can also choose to add more ephemeral OS node pools as per below.

Use Ephemeral OS on existing clusters

Configure a new node pool to use Ephemeral OS disks. Use the `--node-osdisk-type` flag to set as the OS disk type as the OS disk type for that node pool.

```
az aks nodepool add --name ephemeral --cluster-name myAKSCluster --resource-group myResourceGroup -s Standard_DS3_v2 --node-osdisk-type Ephemeral
```

IMPORTANT

With ephemeral OS you can deploy VM and instance images up to the size of the VM cache. In the AKS case, the default node OS disk configuration uses 128 GB, which means that you need a VM size that has a cache larger than 128 GB. The default Standard_DS2_v2 has a cache size of 86 GB, which isn't large enough. The Standard_DS3_v2 has a cache size of 172 GB, which is large enough. You can also reduce the default size of the OS disk by using `--node-osdisk-size`. The minimum size for AKS images is 30 GB.

If you want to create node pools with network-attached OS disks, you can do so by specifying `--node-osdisk-type Managed`.

Mariner OS

Mariner can be deployed on AKS through Azure CLI or ARM templates.

Prerequisites

1. You need the latest version of Azure CLI. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).
2. You need the `aks-preview` Azure CLI extension for the ability to select the Mariner 2.0 operating system SKU. Run `az extension remove --name aks-preview` to clear any previous versions, then run `az extension add --name aks-preview`.
3. If you don't already have kubectl installed, install it through Azure CLI using `az aks install-cli` or follow the [upstream instructions](#).

Deploy an AKS Mariner cluster with Azure CLI

Use the following example commands to create a Mariner cluster.

```
az group create --name MarinerTest --location eastus  
  
az aks create --name testMarinerCluster --resource-group MarinerTest --os-sku mariner  
  
az aks get-credentials --resource-group MarinerTest --name testMarinerCluster  
  
kubectl get pods --all-namespaces
```

Deploy an AKS Mariner cluster with an ARM template

To add Mariner to an existing ARM template, you need to add `"osSKU": "mariner"` and `"mode": "System"` to `agentPoolProfiles` and set the `apiVersion` to 2021-03-01 or newer (`"apiVersion": "2021-03-01"`). The following deployment uses the ARM template "marineraksarm.yml".

```
{  
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.1",  
    "parameters": {  
        "clusterName": {  
            "type": "string",  
            "defaultValue": "marinerakscluster",  
            "metadata": {  
                "description": "The name of the Managed Cluster resource."  
            }  
        },  
        "location": {  
            "type": "string",  
            "defaultValue": "[resourceGroup().location]",  
            "metadata": {  
                "description": "The location of the Managed Cluster resource."  
            }  
        },  
        "dnsPrefix": {  
            "type": "string",  
            "metadata": {  
                "description": "Optional DNS prefix to use with hosted Kubernetes API server FQDN."  
            }  
        },  
        "osDiskSizeGB": {  
            "type": "int",  
            "defaultValue": 0,  
            "minValue": 0,  
            "maxValue": 1023,  
            "metadata": {  
                "description": "Disk size (in GB) to provision for each of the agent pool nodes. This value ranges from 0 to 1023. Specifying 0 will apply the default disk size for that agentVMSize."  
            }  
        },  
        "agentCount": {  
            "type": "int",  
            "defaultValue": 3,  
            "minValue": 1,  
            "maxValue": 50,  
            "metadata": {  
                "description": "The number of nodes for the cluster."  
            }  
        },  
        "agentVMSize": {  
            "type": "string",  
            "defaultValue": "Standard_DS2_v2",  
            "metadata": {  
                "description": "The size of the Virtual Machine."  
            }  
        }  
    },  
    "variables": {},  
    "resources": [],  
    "outputs": {}  
}
```

```
        },
    },
    "linuxAdminUsername": {
        "type": "string",
        "metadata": {
            "description": "User name for the Linux Virtual Machines."
        }
    },
    "sshRSAPublicKey": {
        "type": "string",
        "metadata": {
            "description": "Configure all linux machines with the SSH RSA public key string. Your key should include three parts, for example 'ssh-rsa AAAAB...snip...UcyupgH azureuser@linuxvm'"
        }
    },
    "osType": {
        "type": "string",
        "defaultValue": "Linux",
        "allowedValues": [
            "Linux"
        ],
        "metadata": {
            "description": "The type of operating system."
        }
    },
    "osSKU": {
        "type": "string",
        "defaultValue": "mariner",
        "allowedValues": [
            "mariner",
            "Ubuntu",
        ],
        "metadata": {
            "description": "The Linux SKU to use."
        }
    }
},
"resources": [
{
    "type": "Microsoft.ContainerService/managedClusters",
    "apiVersion": "2021-03-01",
    "name": "[parameters('clusterName')]",
    "location": "[parameters('location')]",
    "properties": {
        "dnsPrefix": "[parameters('dnsPrefix')]",
        "agentPoolProfiles": [
            {
                "name": "agentpool",
                "mode": "System",
                "osDiskSizeGB": "[parameters('osDiskSizeGB')]",
                "count": "[parameters('agentCount')]",
                "vmSize": "[parameters('agentVMSize')]",
                "osType": "[parameters('osType')]",
                "osSKU": "[parameters('osSKU')]",
                "storageProfile": "ManagedDisks"
            }
        ],
        "linuxProfile": {
            "adminUsername": "[parameters('linuxAdminUsername')]",
            "ssh": {
                "publicKeys": [
                    {
                        "keyData": "[parameters('sshRSAPublicKey')]"
                    }
                ]
            }
        }
    }
},
"identity": {
```

```

        "type": "SystemAssigned"
    }
}
],
"outputs": {
    "controlPlaneFQDN": {
        "type": "string",
        "value": "[reference(parameters('clusterName')).fqdn]"
    }
}
}

```

Create this file on your system and fill it with the contents of the Mariner AKS YAML file.

```

az group create --name MarinerTest --location eastus

az deployment group create --resource-group MarinerTest --template-file marineraksarm.yml --parameters
clusterName=testMarinerCluster dnsPrefix=marineraks1 linuxAdminUsername=azureuser sshRSAPublicKey=`<contents
of your id_rsa.pub>` 

az aks get-credentials --resource-group MarinerTest --name testMarinerCluster

kubectl get pods --all-namespaces

```

Custom resource group name

When you deploy an Azure Kubernetes Service cluster in Azure, a second resource group gets created for the worker nodes. By default, AKS will name the node resource group `MC_resourcegroupname_clustername_location`, but you can also provide your own name.

To specify your own resource group name, install the `aks-preview` Azure CLI extension version 0.3.2 or later. Using the Azure CLI, use the `--node-resource-group` parameter of the `az aks create` command to specify a custom name for the resource group. If you use an Azure Resource Manager template to deploy an AKS cluster, you can define the resource group name by using the `nodeResourceGroup` property.

```
az aks create --name myAKSCluster --resource-group myResourceGroup --node-resource-group myNodeResourceGroup
```

The secondary resource group is automatically created by the Azure resource provider in your own subscription. You can only specify the custom resource group name when the cluster is created.

As you work with the node resource group, keep in mind that you can't:

- Specify an existing resource group for the node resource group.
- Specify a different subscription for the node resource group.
- Change the node resource group name after the cluster has been created.
- Specify names for the managed resources within the node resource group.
- Modify or delete Azure-created tags of managed resources within the node resource group.

Node Restriction (Preview)

The [Node Restriction](#) admission controller limits the Node and Pod objects a kubelet can modify. Node Restriction is on by default in AKS 1.24+ clusters. If you're using an older version, use the below commands to create a cluster with Node Restriction or update an existing cluster to add Node Restriction.

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

Before you begin

You must have the following resource installed:

- The Azure CLI
- The `aks-preview` extension version 0.5.95 or later

Install the `aks-preview` CLI extension

```
# Install the aks-preview extension
az extension add --name aks-preview

# Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

Create an AKS cluster with Node Restriction

To create a cluster using Node Restriction.

```
az aks create -n aks -g myResourceGroup --enable-node-restriction
```

Update an AKS cluster with Node Restriction

To update a cluster to use Node Restriction.

```
az aks update -n aks -g myResourceGroup --enable-node-restriction
```

Remove Node Restriction from an AKS cluster

To remove Node Restriction from a cluster.

```
az aks update -n aks -g myResourceGroup --disable-node-restriction
```

OIDC Issuer

This enables an OIDC Issuer URL of the provider which allows the API server to discover public signing keys.

WARNING

Enable or disable OIDC Issuer changes the current service account token issuer to a new value, which can cause downtime and restarts the API server. If the application pods using a service token remain in a failed state after you enable or disable the OIDC Issuer, we recommend you manually restart the pods.

Prerequisites

- The Azure CLI version 2.40.0 or higher. Run `az --version` to find your version. If you need to install or

upgrade, see [Install Azure CLI](#).

- AKS version 1.22 and higher. If your cluster is running version 1.21 and the OIDC Issuer preview is enabled, we recommend you upgrade the cluster to the minimum required version supported.

Create an AKS cluster with OIDC Issuer

Create an AKS cluster using the `az aks create` command with the `--enable-oidc-issuer` parameter to use the OIDC Issuer (preview). The following example creates a cluster named *myAKScluster* with one node in the *myResourceGroup*.

```
az aks create -g myResourceGroup -n myAKScluster --node-count 1 --enable-oidc-issuer
```

Update an AKS cluster with OIDC Issuer

Update an AKS cluster using the `az aks update` command with the `--enable-oidc-issuer` parameter to use the OIDC Issuer (preview). The following example updates a cluster named *myAKScluster*.

```
az aks update -g myResourceGroup -n myAKScluster --enable-oidc-issuer
```

Show the OIDC Issuer URL

To get the OIDC Issuer URL, run the following command. Replace the default values for the cluster name and the resource group name.

```
az aks show -n myAKScluster -g myResourceGroup --query "oidcIssuerProfile.issuerUrl" -otsv
```

Rotate the OIDC key

To rotate the OIDC key, perform the following command. Replace the default values for the cluster name and the resource group name.

```
az aks oidc-issuer rotate-signing-keys -n myAKScluster -g myResourceGroup
```

IMPORTANT

Once you rotate the key, the old key (key1) expires after 24 hours. This means that both the old key (key1) and the new key (key2) are valid within the 24-hour period. If you want to invalidate the old key (key1) immediately, you need to rotate the OIDC key twice. Then key2 and key3 are valid, and key1 is invalid.

Next steps

- Learn how to [upgrade the node images](#) in your cluster.
- See [Upgrade an Azure Kubernetes Service \(AKS\) cluster](#) to learn how to upgrade your cluster to the latest version of Kubernetes.
- Read more about `containerd` and [Kubernetes](#)
- See the list of [Frequently asked questions about AKS](#) to find answers to some common AKS questions.
- Read more about [Ephemeral OS disks](#).

Customize node configuration for Azure Kubernetes Service (AKS) node pools

10/27/2022 • 9 minutes to read • [Edit Online](#)

Customizing your node configuration allows you to configure or tune your operating system (OS) settings or the kubelet parameters to match the needs of the workloads. When you create an AKS cluster or add a node pool to your cluster, you can customize a subset of commonly used OS and kubelet settings. To configure settings beyond this subset, [use a daemon set to customize your needed configurations without losing AKS support for your nodes.](#)

Use custom node configuration

Kubelet custom configuration

The supported Kubelet parameters and accepted values are listed below.

PARAMETER	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>cpuManagerPolicy</code>	none, static	none	The static policy allows containers in Guaranteed pods with integer CPU requests access to exclusive CPUs on the node.
<code>cpuCfsQuota</code>	true, false	true	Enable/Disable CPU CFS quota enforcement for containers that specify CPU limits.
<code>cpuCfsQuotaPeriod</code>	Interval in milliseconds (ms)	<code>100ms</code>	Sets CPU CFS quota period value.
<code>imageGcHighThreshold</code>	0-100	85	The percent of disk usage after which image garbage collection is always run. Minimum disk usage that will trigger garbage collection. To disable image garbage collection, set to 100.
<code>imageGcLowThreshold</code>	0-100, no higher than <code>imageGcHighThreshold</code>	80	The percent of disk usage before which image garbage collection is never run. Minimum disk usage that can trigger garbage collection.
<code>topologyManagerPolicy</code>	none, best-effort, restricted, single-numa-node	none	Optimize NUMA node alignment, see more here .

PARAMETER	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>allowedUnsafeSysctls</code>	<code>kernel.shm*</code> , <code>kernel.msg*</code> , <code>kernel.sem</code> , <code>fs.mqueue.*</code> , <code>net.*</code>	None	Allowed list of unsafe sysctls or unsafe sysctl patterns.
<code>containerLogMaxSizeMB</code>	Size in megabytes (MB)	10 MB	The maximum size (for example, 10 MB) of a container log file before it's rotated.
<code>containerLogMaxFiles</code>	≥ 2	5	The maximum number of container log files that can be present for a container.
<code>podMaxPids</code>	-1 to kernel PID limit	-1 (°)	The maximum amount of process IDs that can be running in a Pod

Linux OS custom configuration

The supported OS settings and accepted values are listed below.

File handle limits

When you're serving a lot of traffic, it's common that the traffic you're serving is coming from a large number of local files. You can tweak the below kernel settings and built-in limits to allow you to handle more, at the cost of some system memory.

SETTING	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>fs.file-max</code>	8192 - 12000500	709620	Maximum number of file-handles that the Linux kernel will allocate, by increasing this value you can increase the maximum number of open files permitted.
<code>fs.inotify.max_user_watches</code>	781250 - 2097152	1048576	Maximum number of file watches allowed by the system. Each <i>watch</i> is roughly 90 bytes on a 32-bit kernel, and roughly 160 bytes on a 64-bit kernel.
<code>fs.aio-max-nr</code>	65536 - 6553500	65536	The aio-nr shows the current system-wide number of asynchronous io requests. aio-max-nr allows you to change the maximum value aio-nr can grow to.
<code>fs.nr_open</code>	8192 - 20000500	1048576	The maximum number of file-handles a process can allocate.

Socket and network tuning

For agent nodes, which are expected to handle very large numbers of concurrent sessions, you can use the subset of TCP and network options below that you can tweak per node pool.

SETTING	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>net.core.somaxconn</code>	4096 - 3240000	16384	Maximum number of connection requests that can be queued for any given listening socket. An upper limit for the value of the backlog parameter passed to the listen(2) function. If the backlog argument is greater than the <code>somaxconn</code> , then it's silently truncated to this limit.
<code>net.core.netdev_max_backlog</code>	1000 - 3240000	1000	Maximum number of packets, queued on the INPUT side, when the interface receives packets faster than kernel can process them.
<code>net.core.rmem_max</code>	212992 - 134217728	212992	The maximum receive socket buffer size in bytes.
<code>net.core.wmem_max</code>	212992 - 134217728	212992	The maximum send socket buffer size in bytes.
<code>net.core.optmem_max</code>	20480 - 4194304	20480	Maximum ancillary buffer size (option memory buffer) allowed per socket. Socket option memory is used in a few cases to store extra structures relating to usage of the socket.
<code>net.ipv4.tcp_max_syn_backlog</code>	128 - 3240000	16384	The maximum number of queued connection requests that have still not received an acknowledgment from the connecting client. If this number is exceeded, the kernel will begin dropping requests.
<code>net.ipv4.tcp_max_tw_buckets</code>	8000 - 1440000	32768	Maximal number of <code>timewait</code> sockets held by system simultaneously. If this number is exceeded, time-wait socket is immediately destroyed and warning is printed.

SETTING	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>net.ipv4.tcp_fin_timeout</code>	5 - 120	60	The length of time an orphaned (no longer referenced by any application) connection will remain in the FIN_WAIT_2 state before it's aborted at the local end.
<code>net.ipv4.tcp_keepalive_time</code>	30 - 432000	7200	How often TCP sends out <code>keepalive</code> messages when <code>keepalive</code> is enabled.
<code>net.ipv4.tcp_keepalive_probes</code>	1 - 15	9	How many <code>keepalive</code> probes TCP sends out, until it decides that the connection is broken.
<code>net.ipv4.tcp_keepalive_intvl</code>	1 - 75	75	How frequently the probes are sent out. Multiplied by <code>tcp_keepalive_probes</code> it makes up the time to kill a connection that isn't responding, after probes started.
<code>net.ipv4.tcp_tw_reuse</code>	0 or 1	0	Allow to reuse <code>TIME-WAIT</code> sockets for new connections when it's safe from protocol viewpoint.
<code>net.ipv4.ip_local_port_range</code>	First: 1024 - 60999 and Last: 32768 - 65000]	First: 32768 and Last: 60999	The local port range that is used by TCP and UDP traffic to choose the local port. Comprised of two numbers: The first number is the first local port allowed for TCP and UDP traffic on the agent node, the second is the last local port number.
<code>net.ipv4.neigh.default.gc_thresh1</code>	80000	4096	Minimum number of entries that may be in the ARP cache. Garbage collection won't be triggered if the number of entries is below this setting.
<code>net.ipv4.neigh.default.gc_thresh2</code>	90000	8192	Soft maximum number of entries that may be in the ARP cache. This setting is arguably the most important, as ARP garbage collection will be triggered about 5 seconds after reaching this soft maximum.

SETTING	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>net.ipv4.neigh.default.gc_thresh1</code>	1024 - 100000	16384	Hard maximum number of entries in the ARP cache.
<code>net.netfilter.nf_conntrack_max</code>	1024 - 1048576	131072	<code>nf_conntrack</code> is a module that tracks connection entries for NAT within Linux. The <code>nf_conntrack</code> module uses a hash table to record the <i>established connection</i> record of the TCP protocol. <code>nf_conntrack_max</code> is the maximum number of nodes in the hash table, that is, the maximum number of connections supported by the <code>nf_conntrack</code> module or the size of connection tracking table.
<code>net.netfilter.nf_conntrack_buckets</code>	65536 - 147456	65536	<code>nf_conntrack</code> is a module that tracks connection entries for NAT within Linux. The <code>nf_conntrack</code> module uses a hash table to record the <i>established connection</i> record of the TCP protocol. <code>nf_conntrack_buckets</code> is the size of hash table.

Worker limits

Like file descriptor limits, the number of workers or threads that a process can create are limited by both a kernel setting and user limits. The user limit on AKS is unlimited.

SETTING	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>kernel.threads-max</code>	20 - 513785	55601	Processes can spin up worker threads. The maximum number of all threads that can be created is set with the kernel setting <code>kernel.threads-max</code> .

Virtual memory

The settings below can be used to tune the operation of the virtual memory (VM) subsystem of the Linux kernel and the `writeout` of dirty data to disk.

SETTING	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION

SETTING	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>vm.max_map_count</code>	65530 - 262144	65530	This file contains the maximum number of memory map areas a process may have. Memory map areas are used as a side-effect of calling <code>malloc</code> , directly by <code>mmap</code> , <code>mprotect</code> , and <code>madvice</code> , and also when loading shared libraries.
<code>vm.vfs_cache_pressure</code>	1 - 500	100	This percentage value controls the tendency of the kernel to reclaim the memory, which is used for caching of directory and inode objects.
<code>vm.swappiness</code>	0 - 100	60	This control is used to define how aggressive the kernel will swap memory pages. Higher values will increase aggressiveness, lower values decrease the amount of swap. A value of 0 instructs the kernel not to initiate swap until the amount of free and file-backed pages is less than the high water mark in a zone.
<code>swapFileSizeMB</code>	1 MB - Size of the temporary disk (/dev/sdb)	None	SwapFileSizeMB specifies size in MB of a swap file will be created on the agent nodes from this node pool.

SETTING	ALLOWED VALUES/INTERVAL	DEFAULT	DESCRIPTION
<code>transparentHugePageEnabled</code>	<code>always</code> , <code>madvise</code> , <code>never</code>	<code>always</code>	<p><code>Transparent Hugepages</code> is a Linux kernel feature intended to improve performance by making more efficient use of your processor's memory-mapping hardware. When enabled the kernel attempts to allocate <code>hugepages</code> whenever possible and any Linux process will receive 2-MB pages if the <code>mmap</code> region is 2 MB naturally aligned. In certain cases when <code>hugepages</code> are enabled system wide, applications may end up allocating more memory resources. An application may <code>mmap</code> a large region but only touch 1 byte of it, in that case a 2-MB page might be allocated instead of a 4k page for no good reason. This scenario is why it's possible to disable <code>hugepages</code> system-wide or to only have them inside <code>MADV_HUGEPAGE madvise</code> regions.</p>
<code>transparentHugePageDefrag</code>	<code>always</code> , <code>defer</code> , <code>defer+madvise</code> , <code>madvise</code> , <code>never</code>	<code>madvise</code>	This value controls whether the kernel should make aggressive use of memory compaction to make more <code>hugepages</code> available.

IMPORTANT

For ease of search and readability the OS settings are displayed in this document by their name but should be added to the configuration json file or AKS API using [camelCase capitalization convention](#).

Create a `kubeletconfig.json` file with the following contents:

```
{  
    "cpuManagerPolicy": "static",  
    "cpuCfsQuota": true,  
    "cpuCfsQuotaPeriod": "200ms",  
    "imageGcHighThreshold": 90,  
    "imageGcLowThreshold": 70,  
    "topologyManagerPolicy": "best-effort",  
    "allowedUnsafeSysctls": [  
        "kernel.msg*",  
        "net.*"  
    ],  
    "failSwapOn": false  
}
```

Create a `linuxosconfig.json` file with the following contents:

```
{  
    "transparentHugePageEnabled": "madvise",  
    "transparentHugePageDefrag": "defer+madvise",  
    "swapFileSizeMB": 1500,  
    "sysctls": {  
        "netCoreSOMAXCONN": 163849,  
        "netIpv4TcpTwReuse": true,  
        "netIpv4IpLocalPortRange": "32000 60000"  
    }  
}
```

Create a new cluster specifying the kubelet and OS configurations using the JSON files created in the previous step.

NOTE

When you create a cluster, you can specify the kubelet configuration, OS configuration, or both. If you specify a configuration when creating a cluster, only the nodes in the initial node pool will have that configuration applied. Any settings not configured in the JSON file will retain the default value.

```
az aks create --name myAKSCluster --resource-group myResourceGroup --kubelet-config ./kubeletconfig.json --linux-os-config ./linuxosconfig.json
```

Add a new node pool specifying the Kubelet parameters using the JSON file you created.

NOTE

When you add a node pool to an existing cluster, you can specify the kubelet configuration, OS configuration, or both. If you specify a configuration when adding a node pool, only the nodes in the new node pool will have that configuration applied. Any settings not configured in the JSON file will retain the default value.

```
az aks nodepool add --name mynodepool1 --cluster-name myAKSCluster --resource-group myResourceGroup --kubelet-config ./kubeletconfig.json
```

Other configuration

The settings below can be used to modify other Operating System settings.

Message of the Day

Pass the `--message-of-the-day` flag with the location of the file to replace the Message of the Day on Linux nodes at cluster creation or node pool creation.

Cluster creation

```
az aks create --cluster-name myAKSCluster --resource-group myResourceGroup --message-of-the-day  
./newMOTD.txt
```

Nodepool creation

```
az aks nodepool add --name mynodepool1 --cluster-name myAKSCluster --resource-group myResourceGroup --  
message-of-the-day ./newMOTD.txt
```

Confirm settings have been applied

After you have applied custom node configuration, you can confirm the settings have been applied to the nodes by [connecting to the host](#) and verifying `sysctl` or configuration changes have been made on the filesystem.

Next steps

- Learn [how to configure your AKS cluster](#).
- Learn how [upgrade the node images](#) in your cluster.
- See [Upgrade an Azure Kubernetes Service \(AKS\) cluster](#) to learn how to upgrade your cluster to the latest version of Kubernetes.
- See the list of [Frequently asked questions about AKS](#) to find answers to some common AKS questions.

Use cluster snapshots to save and apply Azure Kubernetes Service cluster configuration (preview)

10/27/2022 • 3 minutes to read • [Edit Online](#)

Cluster snapshots allow you to save configuration from an Azure Kubernetes Service (AKS) cluster, which can then be used to easily apply the configuration to other clusters. Currently, we snapshot the following properties:

- `ManagedClusterSKU`
- `EnableRbac`
- `KubernetesVersion`
- `LoadBalancersSKU`
- `NetworkMode`
- `NetworkPolicy`
- `NetworkPlugin`

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

Prerequisite

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- The latest version of the [Azure CLI](#) installed.
- Your cluster must be running successfully.
- Your cluster must have been created with the `AddonManagerV2Preview` and `CSIControllersV2Preview` custom header feature values:

```
az aks create -g $RESOURCE_GROUP -n $CLUSTER_NAME --aks-custom-headers  
AKSHTTPCustomFeatures=AddonManagerV2Preview,AKSHTTPCustomFeatures=CSIControllersV2Preview
```

Install the `aks-preview` Azure CLI extension

Install the latest version of the `aks-preview` Azure CLI extension using the following command:

```
az extension add --upgrade --name aks-preview
```

Register the `ManagedClusterSnapshotPreview` feature flag

To use the KEDA, you must enable the `ManagedClusterSnapshotPreview` feature flag on your subscription.

```
az feature register --name ManagedClusterSnapshotPreview --namespace Microsoft.ContainerService
```

You can check on the registration status by using the `az feature list` command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/ManagedClusterSnapshotPreview')].{Name:name,State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider by using the `az provider register` command:

```
az provider register --namespace Microsoft.ContainerService
```

Take a snapshot of your cluster

To begin, get the `id` of the cluster you want to take a snapshot of using `az aks show`:

```
az aks show -g $RESOURCE_GROUP -n $CLUSTER_NAME
```

Using the `id` you just obtained, create a snapshot using `az aks snapshot create`:

```
az aks snapshot create -g $RESOURCE_GROUP -n snapshot1 --cluster-id $CLUSTER_ID
```

Your output will look similar to the following example:

```
{
  "creationData": {
    "sourceResourceId": "$CLUSTER_ID"
  },
  "id": "/subscriptions/$SUBSCRIPTION/resourceGroups/$RESOURCE_GROUP/providers/Microsoft.ContainerService/managedclustersnapshots/snapshot1",
  "location": "eastus2",
  "managedClusterPropertiesReadOnly": {
    "enableRbac": true,
    "kubernetesVersion": "1.22.6",
    "networkProfile": {
      "loadBalancerSku": "Standard",
      "networkMode": null,
      "networkPlugin": "kubenet",
      "networkPolicy": null
    },
    "sku": {
      "name": "Basic",
      "tier": "Paid"
    }
  },
  "name": "snapshot1",
  "resourceGroup": "$RESOURCE_GROUP",
  "snapshotType": "ManagedCluster",
  "systemData": {
    "createdAt": "2022-04-21T00:47:49.041399+00:00",
    "createdBy": "user@contoso.com",
    "createdByType": "User",
    "lastModifiedAt": "2022-04-21T00:47:49.041399+00:00",
    "lastModifiedBy": "user@contoso.com",
    "lastModifiedByType": "User"
  },
  "tags": null,
  "type": "Microsoft.ContainerService/ManagedClusterSnapshots"
}
```

View a snapshot

To list all available snapshots, use the `az aks snapshot list` command:

```
az aks snapshot list -g $RESOURCE_GROUP
```

To view details for an individual snapshot, reference it by name in the `az aks snapshot show` command. For example, to view the snapshot `snapshot1` created in the steps above:

```
az aks snapshot show -g $RESOURCE_GROUP -n snapshot1 -o table
```

Your output will look similar to the following example:

Name	Location	ResourceGroup	Sku	EnableRbac	KubernetesVersion	NetworkPlugin
<hr/>						
snapshot1	eastus2	qizhe-rg	Paid	True	1.22.6	kubenet Standard

Delete a snapshot

Removing a snapshot can be done by referencing the snapshot's name in the `az aks snapshot delete` command. For example, to delete the snapshot `snapshot1` created in the above steps:

```
az aks snapshot delete -g $RESOURCE_GROUP -n snapshot1
```

Create a cluster from a snapshot

New AKS clusters can be created based on the configuration captured in a snapshot. To do so, first obtain the `id` of the desired snapshot. Next, use `az aks create`, using the snapshot's `id` with the `--cluster-snapshot-id` flag. Be sure to include the `addonManagerV2` and `CSIControllersV2Preview` feature flag custom header values. For example:

```
az aks create -g $RESOURCE_GROUP -n aks-from-snapshot --cluster-snapshot-id
"/subscriptions/$SUBSCRIPTION/resourceGroups/$RESOURCE_GROUP/providers/Microsoft.ContainerService/managedclustersnapshots/snapshot1" --aks-custom-headers
AKSHTTPCustomFeatures=AddonManagerV2Preview,AKSHTTPCustomFeatures=CSIControllersV2Preview
```

NOTE

The cluster can be created with other allowed parameters that are not captured in the snapshot, such as `vm-sku-size` or `--node-count`. However, no configuration arguments for parameters that are part of the snapshot should be included. If the values passed in these arguments differs from the snapshot's values, cluster creation will fail.

Update or upgrade a cluster using a snapshot

Clusters can also be updated and upgraded while using a snapshot by using the snapshot's `id` with the `--cluster-snapshot-id` flag:

```
az aks update -g $RESOURCE_GROUP -n aks-from-snapshot --cluster-snapshot-id
"/subscriptions/$SUBSCRIPTION/resourceGroups/$RESOURCE_GROUP/providers/Microsoft.ContainerService/managedclustersnapshots/snapshot1" --aks-custom-headers
AKSHTTPCustomFeatures=AddonManagerV2Preview,AKSHTTPCustomFeatures=CSIControllersV2Preview
```

```
az aks upgrade -g $RESOURCE_GROUP -n aks-from-snapshot --cluster-snapshot-id
"/subscriptions/$SUBSCRIPTION/resourceGroups/$RESOURCE_GROUP/providers/Microsoft.ContainerService/managedclustersnapshots/snapshot1" --aks-custom-headers
AKSHTTPCustomFeatures=AddonManagerV2Preview,AKSHTTPCustomFeatures=CSIControllersV2Preview
```

Next steps

- Learn [how to use node pool snapshots](#)

Authenticate with Azure Container Registry from Azure Kubernetes Service

10/27/2022 • 4 minutes to read • [Edit Online](#)

When you're using Azure Container Registry (ACR) with Azure Kubernetes Service (AKS), an authentication mechanism needs to be established. This operation is implemented as part of the CLI, PowerShell, and Portal experience by granting the required permissions to your ACR. This article provides examples for configuring authentication between these two Azure services.

You can set up the AKS to ACR integration in a few simple commands with the Azure CLI or Azure PowerShell. This integration assigns the `AcrPull` role to the managed identity associated to the AKS Cluster.

NOTE

This article covers automatic authentication between AKS and ACR. If you need to pull an image from a private external registry, use an [image pull secret](#).

Before you begin

These examples require:

- [Azure CLI](#)
- [Azure PowerShell](#)
- **Owner, Azure account administrator, or Azure co-administrator** role on the **Azure subscription**
- Azure CLI version 2.7.0 or later

To avoid needing an **Owner, Azure account administrator, or Azure co-administrator** role, you can use an existing managed identity to authenticate ACR from AKS. For more information, see [Use an Azure managed identity to authenticate to an Azure container registry](#).

Create a new AKS cluster with ACR integration

You can set up AKS and ACR integration during the initial creation of your AKS cluster. To allow an AKS cluster to interact with ACR, an Azure Active Directory **managed identity** is used. The following command allows you to authorize an existing ACR in your subscription and configures the appropriate **ACRPull** role for the managed identity. Supply valid values for your parameters below.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
# set this to the name of your Azure Container Registry. It must be globally unique
MYACR=myContainerRegistry

# Run the following line to create an Azure Container Registry if you do not already have one
az acr create -n $MYACR -g myContainerRegistryResourceGroup --sku basic

# Create an AKS cluster with ACR integration
az aks create -n myAKScluster -g myResourceGroup --generate-ssh-keys --attach-acr $MYACR
```

Alternatively, you can specify the ACR name using an ACR resource ID, which has the following format:

```
/subscriptions/\<subscription-id\>/resourceGroups/\<resource-group-name\>/providers/Microsoft.ContainerRegistry/registries/\<name\>
```

NOTE

If you are using an ACR that is located in a different subscription from your AKS cluster, use the ACR resource ID when attaching or detaching from an AKS cluster.

```
az aks create -n myAKSCluster -g myResourceGroup --generate-ssh-keys --attach-acr  
/subscriptions/<subscription-id>/resourceGroups/myContainerRegistryResourceGroup/providers/Microsoft.ContainerRegistry/registries/myContainerRegistry
```

This step may take several minutes to complete.

Configure ACR integration for existing AKS clusters

- [Azure CLI](#)
- [Azure PowerShell](#)

Integrate an existing ACR with existing AKS clusters by supplying valid values for **acr-name** or **acr-resource-id** as below.

```
az aks update -n myAKSCluster -g myResourceGroup --attach-acr <acr-name>
```

or,

```
az aks update -n myAKSCluster -g myResourceGroup --attach-acr <acr-resource-id>
```

NOTE

Running `az aks update --attach-acr` uses the permissions of the user running the command to create the role ACR assignment. This role is assigned to the kubelet managed identity. For more information on the AKS managed identities, see [Summary of managed identities](#).

You can also remove the integration between an ACR and an AKS cluster with the following

```
az aks update -n myAKSCluster -g myResourceGroup --detach-acr <acr-name>
```

or

```
az aks update -n myAKSCluster -g myResourceGroup --detach-acr <acr-resource-id>
```

Working with ACR & AKS

Import an image into your ACR

Import an image from docker hub into your ACR by running the following:

- [Azure CLI](#)

- [Azure PowerShell](#)

```
az acr import -n <acr-name> --source docker.io/library/nginx:latest --image nginx:v1
```

Deploy the sample image from ACR to AKS

Ensure you have the proper AKS credentials

- [Azure CLI](#)
- [Azure PowerShell](#)

```
az aks get-credentials -g myResourceGroup -n myAKSCluster
```

Create a file called `acr-nginx.yaml` that contains the following. Substitute the resource name of your registry for `acr-name`. Example: *myContainerRegistry*.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx0-deployment
  labels:
    app: nginx0-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app: nginx0
  template:
    metadata:
      labels:
        app: nginx0
    spec:
      containers:
        - name: nginx
          image: <acr-name>.azurecr.io/nginx:v1
          ports:
            - containerPort: 80
```

Next, run this deployment in your AKS cluster:

```
kubectl apply -f acr-nginx.yaml
```

You can monitor the deployment by running:

```
kubectl get pods
```

You should have two running pods.

NAME	READY	STATUS	RESTARTS	AGE
nginx0-deployment-669dfc4d4b-x74kr	1/1	Running	0	20s
nginx0-deployment-669dfc4d4b-xdpd6	1/1	Running	0	20s

Troubleshooting

- Run the `az aks check-acr` command to validate that the registry is accessible from the AKS cluster.

- Learn more about [ACR Monitoring](#)
- Learn more about [ACR Health](#)

Vertical Pod Autoscaling (preview) in Azure Kubernetes Service (AKS)

10/27/2022 • 9 minutes to read • [Edit Online](#)

This article provides an overview of Vertical Pod Autoscaler (VPA) (preview) in Azure Kubernetes Service (AKS), which is based on the open source [Kubernetes](#) version. When configured, it automatically sets resource requests and limits on containers per workload based on past usage. This ensures pods are scheduled onto nodes that have the required CPU and memory resources.

Benefits

Vertical Pod Autoscaler provides the following benefits:

- It analyzes and adjusts processor and memory resources to *right size* your applications. VPA isn't only responsible for scaling up, but also for scaling down based on their resource use over time.
- A Pod is evicted if it needs to change its resource requests if its scaling mode is set to *auto* or *recreate*.
- Set CPU and memory constraints for individual containers by specifying a resource policy
- Ensures nodes have correct resources for pod scheduling
- Configurable logging of any adjustments to processor or memory resources made
- Improve cluster resource utilization and frees up CPU and memory for other pods.

Limitations

- Vertical Pod autoscaling supports a maximum of 500 `VerticalPodAutoscaler` objects per cluster.
- With this preview release, you can't change the `controlledValue` and `updateMode` of `managedCluster` object.

Before you begin

- AKS cluster is running Kubernetes version 1.24 and higher.
- The Azure CLI version 2.0.64 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).
- The `aks-preview` extension version 0.5.102 or later.
- `kubectl` should be connected to the cluster you want to install VPA.

API Object

The Vertical Pod Autoscaler is an API resource in the Kubernetes autoscaling API group. The version supported in this preview release is 0.11 can be found in the [Kubernetes autoscaler repo](#).

Register the VPA provider feature

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

To install the aks-vpapreview preview feature, run the following command:

```
az feature register --namespace Microsoft.ContainerService --name AKS-VPAPreview
```

Deploy, upgrade, or disable VPA on a cluster

In this section, you deploy, upgrade, or disable the Vertical Pod Autoscaler on your cluster.

1. To enable VPA on a new cluster, use `--enable-vpa` parameter with the [az aks create](#) command.

```
az aks create -n myAKSCluster -g myResourceGroup --enable-vpa
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

2. Optionally, to enable VPA on an existing cluster, use the `--enable-vpa` with the [az aks upgrade](#) command.

```
az aks update -n myAKSCluster -g myResourceGroup --enable-vpa
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

3. Optionally, to disable VPA on an existing cluster, use the `--disable-vpa` with the [az aks upgrade](#) command.

```
az aks update -n myAKSCluster -g myResourceGroup --disable-vpa
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

4. To verify that the Vertical Pod Autoscaler pods have been created successfully, use the [kubectl get](#) command.

```
kubectl get pods -n kube-system
```

The output of the command includes the following results specific to the VPA pods. The pods should show a *running* status.

NAME	READY	STATUS	RESTARTS	AGE
vpa-admission-controller-7867874bc5-vjfxk	1/1	Running	0	41m
vpa-recommender-5fd94767fb-ggjr2	1/1	Running	0	41m
vpa-updater-56f9bfc96f-jgq2g	1/1	Running	0	41m

Test your Vertical Pod Autoscaler installation

The following steps create a deployment with two pods, each running a single container that requests 100 millicores and tries to utilize slightly above 500 millicores. Also created is a VPA config pointing at the deployment. The VPA observes the behavior of the pods, and after about five minutes, they're updated with a higher CPU request.

1. Create a file named `hamster.yaml` and copy in the following manifest of the Vertical Pod Autoscaler example from the [kubernetes/autoscaler](#) GitHub repository.
2. Deploy the `hamster.yaml` Vertical Pod Autoscaler example using the `kubectl apply` command and specify the name of your YAML manifest:

```
kubectl apply -f hamster.yaml
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

3. Run the following `kubectl get` command to get the pods from the hamster example application:

```
kubectl get pods -l app=hamster
```

The example output resembles the following:

```
hamster-78f9dcdd4c-hf7gk  1/1    Running   0          24s
hamster-78f9dcdd4c-j9mc7  1/1    Running   0          24s
```

4. Use the `kubectl describe` command on one of the pods to view its CPU and memory reservation. Replace "exampleID" with one of the pod IDs returned in your output from the previous step.

```
kubectl describe pod hamster-exampleID
```

The example output is a snippet of the information about the cluster:

```
hamster:
  Container ID:  containerd://
  Image:         k8s.gcr.io/ubuntu-slim:0.1
  Image ID:      sha256:
  Port:          <none>
  Host Port:    <none>
  Command:
    /bin/sh
  Args:
    -c
    while true; do timeout 0.5s yes >/dev/null; sleep 0.5s; done
  State:        Running
  Started:     Wed, 28 Sep 2022 15:06:14 -0400
  Ready:        True
  Restart Count: 0
  Requests:
    cpu:        100m
    memory:    50Mi
  Environment: <none>
```

The pod has 100 millicpu and 50 Mibibytes of memory reserved in this example. For this sample application, the pod needs less than 100 millicpu to run, so there's no CPU capacity available. The pods also reserves much less memory than needed. The Vertical Pod Autoscaler *vpa-recommender* deployment analyzes the pods hosting the hamster application to see if the CPU and memory requirements are appropriate. If adjustments are needed, the vpa-updater relaunches the pods with

updated values.

5. Wait for the vpa-updater to launch a new hamster pod. This should take a few minutes. You can monitor the pods using the [kubectl get](#) command.

```
kubectl get --watch pods -l app=hamster
```

6. When a new hamster pod is started, describe the pod running the [kubectl describe](#) command and view the updated CPU and memory reservations.

```
kubectl describe pod hamster-<exampleID>
```

The example output is a snippet of the information describing the pod:

```
State:          Running
Started:       Wed, 28 Sep 2022 15:09:51 -0400
Ready:          True
Restart Count: 0
Requests:
  cpu:        587m
  memory:     262144k
Environment:   <none>
```

In the previous output, you can see that the CPU reservation increased to 587 millicpu, which is over five times the original value. The memory increased to 262,144 Kilobytes, which is around 250 Mibabytes, or five times the original value. This pod was under-resourced, and the Vertical Pod Autoscaler corrected the estimate with a much more appropriate value.

7. To view updated recommendations from VPA, run the [kubectl describe](#) command to describe the hamster-vpa resource information.

```
kubectl describe vpa/hamster-vpa
```

The example output is a snippet of the information about the resource utilization:

```
State:          Running
Started:       Wed, 28 Sep 2022 15:09:51 -0400
Ready:          True
Restart Count: 0
Requests:
  cpu:        587m
  memory:     262144k
Environment:   <none>
```

Set Pod Autoscaler requests automatically

Vertical Pod autoscaling uses the `VerticalPodAutoscaler` object to automatically set resource requests on Pods when the updateMode is set to `Auto` or `Recreate`.

1. Enable VPA for your cluster by running the following command. Replace cluster name `myAKScluster` with the name of your AKS cluster and replace `myResourceGroup` with the name of the resource group the cluster is hosted in.

```
az aks update -n myAKSCluster -g myResourceGroup --enable-vpa
```

2. Create a file named `azure-autodeploy.yaml`, and copy in the following manifest.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: vpa-auto-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app: vpa-auto-deployment
  template:
    metadata:
      labels:
        app: vpa-auto-deployment
    spec:
      containers:
        - name: mycontainer
          image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
          resources:
            requests:
              cpu: 100m
              memory: 50Mi
          command: ["/bin/sh"]
          args: ["-c", "while true; do timeout 0.5s yes >/dev/null; sleep 0.5s; done"]
```

This manifest describes a deployment that has two Pods. Each Pod has one container that requests 100 milliCPU and 50 MiB of memory.

3. Create the pod with the `kubectl create` command, as shown in the following example:

```
kubectl create -f azure-autodeploy.yaml
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

4. Run the following `kubectl get` command to get the pods:

```
kubectl get pods
```

The output resembles the following example showing the name and status of the pods:

NAME	READY	STATUS	RESTARTS	AGE
vpa-auto-deployment-54465fb978-kchc5	1/1	Running	0	52s
vpa-auto-deployment-54465fb978-nhtmj	1/1	Running	0	52s

5. Create a file named `azure-vpa-auto.yaml`, and copy in the following manifest that describes a

`VerticalPodAutoscaler`:

```
apiVersion: autoscaling.k8s.io/v1
kind: VerticalPodAutoscaler
metadata:
  name: vpa-auto
spec:
  targetRef:
    apiVersion: "apps/v1"
    kind: Deployment
    name: vpa-auto-deployment
  updatePolicy:
    updateMode: "Auto"
```

The `targetRef.name` value specifies that any Pod that is controlled by a deployment named `vpa-auto-deployment` belongs to this `VerticalPodAutoscaler`. The `updateMode` value of `Auto` means that the Vertical Pod Autoscaler controller can delete a Pod, adjust the CPU and memory requests, and then start a new Pod.

6. Apply the manifest to the cluster using the [kubectl apply](#) command:

```
kubectl create -f azure-vpa-auto.yaml
```

7. Wait a few minutes, and view the running Pods again by running the following [kubectl get](#) command:

```
kubectl get pods
```

The output resembles the following example showing the pod names have changed and status of the pods:

NAME	READY	STATUS	RESTARTS	AGE
vpa-auto-deployment-54465fb978-qbhc4	1/1	Running	0	2m49s
vpa-auto-deployment-54465fb978-vbj68	1/1	Running	0	109s

8. Get detailed information about one of your running Pods by using the [Kubectl get](#) command. Replace `podName` with the name of one of your Pods that you retrieved in the previous step.

```
kubectl get pod podName --output yaml
```

The output resembles the following example, showing that the Vertical Pod Autoscaler controller has increased the memory request to 262144k and CPU request to 25 milliCPU.

```

apiVersion: v1
kind: Pod
metadata:
  annotations:
    vpaObservedContainers: mycontainer
    vpaUpdates: 'Pod resources updated by vpa-auto: container 0: cpu request, memory
      request'
  creationTimestamp: "2022-09-29T16:44:37Z"
  generateName: vpa-auto-deployment-54465fb978-
  labels:
    app: vpa-auto-deployment

spec:
  containers:
  - args:
    - -c
    - - while true; do timeout 0.5s yes >/dev/null; sleep 0.5s; done
    command:
    - /bin/sh
    image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
    imagePullPolicy: IfNotPresent
    name: mycontainer
    resources:
      requests:
        cpu: 25m
        memory: 262144k

```

9. To get detailed information about the Vertical Pod Autoscaler and its recommendations for CPU and memory, use the [kubectl get](#) command:

```
kubectl get vpa vpa-auto --output yaml
```

The output resembles the following example:

```

recommendation:
  containerRecommendations:
  - containerName: mycontainer
    lowerBound:
      cpu: 25m
      memory: 262144k
    target:
      cpu: 25m
      memory: 262144k
    uncappedTarget:
      cpu: 25m
      memory: 262144k
    upperBound:
      cpu: 230m
      memory: 262144k

```

The results show the `target` attribute specifies that for the container to run optimally, it doesn't need to change the CPU or the memory target. Your results may vary where the target CPU and memory recommendation are higher.

The Vertical Pod Autoscaler uses the `lowerBound` and `upperBound` attributes to decide whether to delete a Pod and replace it with a new Pod. If a Pod has requests less than the lower bound or greater than the upper bound, the Vertical Pod Autoscaler deletes the Pod and replaces it with a Pod that meets the target attribute.

Next steps

This article showed you how to automatically scale resource utilization, such as CPU and memory, of cluster nodes to match application requirements. You can also use the horizontal pod autoscaler to automatically adjust the number of pods that run your application. For steps on using the horizontal pod autoscaler, see [Scale applications in AKS](#).

Scale the node count in an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 3 minutes to read • [Edit Online](#)

If the resource needs of your applications change, your cluster performance may be impacted due to low capacity on CPU, memory, PID space, or disk sizes. To address these changes, you can manually scale your AKS cluster to run a different number of nodes. When you scale down, nodes are carefully [cordoned and drained](#) to minimize disruption to running applications. When you scale up, AKS waits until nodes are marked **Ready** by the Kubernetes cluster before pods are scheduled on them.

Scale the cluster nodes

NOTE

Removing nodes from a node pool using the `kubectl` command is not supported. Doing so can create scaling issues with your AKS cluster.

- [Azure CLI](#)
- [Azure PowerShell](#)

First, get the *name* of your node pool using the `az aks show` command. The following example gets the node pool name for the cluster named *myAKSCluster* in the *myResourceGroup* resource group:

```
az aks show --resource-group myResourceGroup --name myAKSCluster --query agentPoolProfiles
```

The following example output shows that the *name* is *nodepool1*:

```
[  
 {  
   "count": 1,  
   "maxPods": 110,  
   "name": "nodepool1",  
   "osDiskSizeGb": 30,  
   "osType": "Linux",  
   "storageProfile": "ManagedDisks",  
   "vmSize": "Standard_DS2_v2"  
 }  
]
```

Use the `az aks scale` command to scale the cluster nodes. The following example scales a cluster named *myAKSCluster* to a single node. Provide your own `--nodepool-name` from the previous command, such as *nodepool1*:

```
az aks scale --resource-group myResourceGroup --name myAKSCluster --node-count 1 --nodepool-name <your node  
pool name>
```

The following example output shows the cluster has successfully scaled to one node, as shown in the *agentPoolProfiles* section:

```
{  
  "aadProfile": null,  
  "addonProfiles": null,  
  "agentPoolProfiles": [  
    {  
      "count": 1,  
      "maxPods": 110,  
      "name": "nodepool1",  
      "osDiskSizeGb": 30,  
      "osType": "Linux",  
      "storageProfile": "ManagedDisks",  
      "vmSize": "Standard_DS2_v2",  
      "vnetSubnetId": null  
    }  
  ],  
  [...]  
}
```

Scale `User` node pools to 0

Unlike `System` node pools that always require running nodes, `User` node pools allow you to scale to 0. To learn more on the differences between system and user node pools, see [System and user node pools](#).

- [Azure CLI](#)
- [Azure PowerShell](#)

To scale a user pool to 0, you can use the `az aks nodepool scale` in alternative to the above `az aks scale` command, and set 0 as your node count.

```
az aks nodepool scale --name <your node pool name> --cluster-name myAKSCluster --resource-group  
myResourceGroup --node-count 0
```

You can also autoscale `User` node pools to 0 nodes, by setting the `--min-count` parameter of the [Cluster Autoscaler](#) to 0.

Next steps

In this article, you manually scaled an AKS cluster to increase or decrease the number of nodes. You can also use the [cluster autoscaler](#) to automatically scale your cluster.

Use Scale-down Mode to delete/deallocate nodes in Azure Kubernetes Service (AKS)

10/27/2022 • 2 minutes to read • [Edit Online](#)

By default, scale-up operations performed manually or by the cluster autoscaler require the allocation and provisioning of new nodes, and scale-down operations delete nodes. Scale-down Mode allows you to decide whether you would like to delete or deallocate the nodes in your Azure Kubernetes Service (AKS) cluster upon scaling down.

When an Azure VM is in the `Stopped` (deallocated) state, you will not be charged for the VM compute resources. However, you'll still need to pay for any OS and data storage disks attached to the VM. This also means that the container images will be preserved on those nodes. For more information, see [States and billing of Azure Virtual Machines](#). This behavior allows for faster operation speeds, as your deployment uses cached images. Scale-down Mode removes the need to pre-provision nodes and pre-pull container images, saving you compute cost.

Before you begin

WARNING

In order to preserve any deallocated VMs, you must set Scale-down Mode to Deallocation. That includes VMs that have been deallocated using IaaS APIs (Virtual Machine Scale Set APIs). Setting Scale-down Mode to Delete will remove any deallocated VMs. Once applied the deallocated mode and scale down operation occurred, those nodes keep registered in APIserver and appear as NotReady state.

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart using the [Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

Limitations

- [Ephemeral OS](#) disks aren't supported. Be sure to specify managed OS disks via `--node-osdisk-type Managed` when creating a cluster or node pool.

NOTE

Previously, while Scale-down Mode was in preview, [spot node pools](#) were unsupported. Now that Scale-down Mode is Generally Available, this limitation no longer applies.

Using Scale-down Mode to deallocate nodes on scale-down

By setting `--scale-down-mode Deallocation`, nodes will be deallocated during a scale-down of your cluster/node pool. All deallocated nodes are stopped. When your cluster/node pool needs to scale up, the deallocated nodes will be started first before any new nodes are provisioned.

In this example, we create a new node pool with 20 nodes and specify that upon scale-down, nodes are to be deallocated via `--scale-down-mode Deallocation`.

```
az aks nodepool add --node-count 20 --scale-down-mode Deallocation --node-osdisk-type Managed --max-pods 10 --name nodepool2 --cluster-name myAKSCluster --resource-group myResourceGroup
```

By scaling the node pool and changing the node count to 5, we'll deallocate 15 nodes.

```
az aks nodepool scale --node-count 5 --name nodepool2 --cluster-name myAKSCluster --resource-group myResourceGroup
```

Deleting previously deallocated nodes

To delete your deallocated nodes, you can change your Scale-down Mode to `Delete` by setting `--scale-down-mode Delete`. The 15 deallocated nodes will now be deleted.

```
az aks nodepool update --scale-down-mode Delete --name nodepool2 --cluster-name myAKSCluster --resource-group myResourceGroup
```

NOTE

Changing your scale-down mode from `Deallocate` to `Delete` then back to `Deallocate` will delete all deallocated nodes while keeping your node pool in `Deallocate` scale-down mode.

Using Scale-down Mode to delete nodes on scale-down

The default behavior of AKS without using Scale-down Mode is to delete your nodes when you scale-down your cluster. With Scale-down Mode, this behavior can be explicitly achieved by setting `--scale-down-mode Delete`.

In this example, we create a new node pool and specify that our nodes will be deleted upon scale-down via `--scale-down-mode Delete`. Scaling operations will be handled via the cluster autoscaler.

```
az aks nodepool add --enable-cluster-autoscaler --min-count 1 --max-count 10 --max-pods 10 --node-osdisk-type Managed --scale-down-mode Delete --name nodepool3 --cluster-name myAKSCluster --resource-group myResourceGroup
```

Next steps

- To learn more about upgrading your AKS cluster, see [Upgrade an AKS cluster](#)
- To learn more about the cluster autoscaler, see [Automatically scale a cluster to meet application demands on AKS](#)

Stop and Start an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 4 minutes to read • [Edit Online](#)

Your AKS workloads may not need to run continuously, for example a development cluster that is used only during business hours. This leads to times where your Azure Kubernetes Service (AKS) cluster might be idle, running no more than the system components. You can reduce the cluster footprint by scaling all the [User node pools to 0](#), but your [System pool](#) is still required to run the system components while the cluster is running. To optimize your costs further during these periods, you can completely turn off (stop) your cluster. This action will stop your control plane and agent nodes altogether, allowing you to save on all the compute costs, while maintaining all your objects (except standalone pods) and cluster state stored for when you start it again. You can then pick up right where you left off after a weekend or to have your cluster running only while you run your batch jobs.

Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

Limitations

When using the cluster start/stop feature, the following restrictions apply:

- This feature is only supported for Virtual Machine Scale Sets backed clusters.
- The cluster state of a stopped AKS cluster is preserved for up to 12 months. If your cluster is stopped for more than 12 months, the cluster state cannot be recovered. For more information, see the [AKS Support Policies](#).
- You can only start or delete a stopped AKS cluster. To perform any operation like scale or upgrade, start your cluster first.
- The customer provisioned PrivateEndpoints linked to private cluster need to be deleted and recreated again when you start a stopped AKS cluster.
- Because the stop process drains all nodes, any standalone pods (i.e. pods not managed by a Deployment, StatefulSet, DaemonSet, Job, etc.) will be deleted.

Stop an AKS Cluster

- [Azure CLI](#)
- [Azure PowerShell](#)

You can use the `az aks stop` command to stop a running AKS cluster's nodes and control plane. The following example stops a cluster named *myAKSCluster*.

```
az aks stop --name myAKSCluster --resource-group myResourceGroup
```

You can verify when your cluster is stopped by using the `az aks show` command and confirming the [powerState](#) shows as [Stopped](#) as on the below output:

```
{  
[...]  
  "nodeResourceGroup": "MC_myResourceGroup_myAKSCluster_westus2",  
  "powerState":{  
    "code":"Stopped"  
  },  
  "privateFqdn": null,  
  "provisioningState": "Succeeded",  
  "resourceGroup": "myResourceGroup",  
[...]  
}
```

If the `provisioningState` shows `Stopping` that means your cluster hasn't fully stopped yet.

IMPORTANT

If you are using [Pod Disruption Budgets](#) the stop operation can take longer as the drain process will take more time to complete.

Start an AKS Cluster

Caution

It is important that you don't repeatedly start/stop your cluster. Repeatedly starting/stopping your cluster may result in errors. Once your cluster is stopped, you should wait 15-30 minutes before starting it up again.

- [Azure CLI](#)
- [Azure PowerShell](#)

You can use the `az aks start` command to start a stopped AKS cluster's nodes and control plane. The cluster is restarted with the previous control plane state and number of agent nodes. The following example starts a cluster named *myAKSCluster*.

```
az aks start --name myAKSCluster --resource-group myResourceGroup
```

You can verify when your cluster has started by using the `az aks show` command and confirming the `powerState` shows `Running` as on the below output:

```
{  
[...]  
  "nodeResourceGroup": "MC_myResourceGroup_myAKSCluster_westus2",  
  "powerState":{  
    "code":"Running"  
  },  
  "privateFqdn": null,  
  "provisioningState": "Succeeded",  
  "resourceGroup": "myResourceGroup",  
[...]  
}
```

If the `provisioningState` shows `Starting` that means your cluster hasn't fully started yet.

NOTE

When you start your cluster back up, the following is expected behavior:

- The IP address of your API server may change.
- If you are using cluster autoscaler, when you start your cluster back up your current node count may not be between the min and max range values you set. The cluster starts with the number of nodes it needs to run its workloads, which isn't impacted by your autoscaler settings. When your cluster performs scaling operations, the min and max values will impact your current node count and your cluster will eventually enter and remain in that desired range until you stop your cluster.

Next steps

- To learn how to scale `user` pools to 0, see [Scale `user` pools to 0](#).
- To learn how to save costs using Spot instances, see [Add a spot node pool to AKS](#).
- To learn more about the AKS support policies, see [AKS support policies](#).

Use Planned Maintenance to schedule maintenance windows for your Azure Kubernetes Service (AKS) cluster (preview)

10/27/2022 • 4 minutes to read • [Edit Online](#)

Your AKS cluster has regular maintenance performed on it automatically. By default, this work can happen at any time. Planned Maintenance allows you to schedule weekly maintenance windows that will update your control plane as well as your kube-system Pods on a VMSS instance and minimize workload impact. Once scheduled, all your maintenance will occur during the window you selected. You can schedule one or more weekly windows on your cluster by specifying a day or time range on a specific day. Maintenance Windows are configured using the Azure CLI.

Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

Limitations

When using Planned Maintenance, the following restrictions apply:

- AKS reserves the right to break these windows for unplanned/reactive maintenance operations that are urgent or critical.
- Currently, performing maintenance operations are considered *best-effort only* and are not guaranteed to occur within a specified window.
- Updates cannot be blocked for more than seven days.

Install `aks-preview` CLI extension

You also need the `aks-preview` Azure CLI extension version 0.5.4 or later. Install the `aks-preview` Azure CLI extension by using the [az extension add](#) command. Or install any available updates by using the [az extension update](#) command.

```
# Install the aks-preview extension
az extension add --name aks-preview

# Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

Allow maintenance on every Monday at 1:00am to 2:00am

To add a maintenance window, you can use the `az aks maintenanceconfiguration add` command.

IMPORTANT

At this time, you must set `default` as the value for `--name`. Using any other name will cause your maintenance window to not run.

Planned Maintenance windows are specified in Coordinated Universal Time (UTC).

```
az aks maintenanceconfiguration add -g MyResourceGroup --cluster-name myAKSCluster --name default --weekday Monday --start-hour 1
```

The following example output shows the maintenance window from 1:00am to 2:00am every Monday.

```
{
  "id": "/subscriptions/<subscriptionID>/resourcegroups/MyResourceGroup/providers/Microsoft.ContainerService/managedClusters/myAKSCluster/maintenanceConfigurations/default",
  "name": "default",
  "notAllowedTime": null,
  "resourceGroup": "MyResourceGroup",
  "systemData": null,
  "timeInWeek": [
    {
      "day": "Monday",
      "hourSlots": [
        1
      ]
    }
  ],
  "type": null
}
```

To allow maintenance any time during a day, omit the `start-hour` parameter. For example, the following command sets the maintenance window for the full day every Monday:

```
az aks maintenanceconfiguration add -g MyResourceGroup --cluster-name myAKSCluster --name default --weekday Monday
```

Add a maintenance configuration with a JSON file

You can also use a JSON file to create a maintenance window instead of using parameters. Create a `test.json` file with the following contents:

```
{  
    "timeInWeek": [  
        {  
            "day": "Tuesday",  
            "hour_slots": [  
                1,  
                2  
            ]  
        },  
        {  
            "day": "Wednesday",  
            "hour_slots": [  
                1,  
                6  
            ]  
        }  
    ],  
    "notAllowedTime": [  
        {  
            "start": "2021-05-26T03:00:00Z",  
            "end": "2021-05-30T12:00:00Z"  
        }  
    ]  
}
```

The above JSON file specifies maintenance windows every Tuesday at 1:00am - 3:00am and every Wednesday at 1:00am - 2:00am and at 6:00am - 7:00am. There is also an exception from `2021-05-26T03:00:00Z` to `2021-05-30T12:00:00Z` where maintenance isn't allowed even if it overlaps with a maintenance window. The following command adds the maintenance windows from `test.json`.

```
az aks maintenanceconfiguration add -g MyResourceGroup --cluster-name myAKSCluster --name default --config-file ./test.json
```

Update an existing maintenance window

To update an existing maintenance configuration, use the `az aks maintenanceconfiguration update` command.

```
az aks maintenanceconfiguration update -g MyResourceGroup --cluster-name myAKSCluster --name default --weekday Monday --start-hour 1
```

List all maintenance windows in an existing cluster

To see all current maintenance configuration windows in your AKS cluster, use the

```
az aks maintenanceconfiguration list
```

```
az aks maintenanceconfiguration list -g MyResourceGroup --cluster-name myAKSCluster
```

In the output below, you can see that there are two maintenance windows configured for myAKSCluster. One window is on Mondays at 1:00am and another window is on Friday at 4:00am.

```
[  
  {  
    "id":  
      "/subscriptions/<subscriptionID>/resourcegroups/MyResourceGroup/providers/Microsoft.ContainerService/managedClusters/myAKSCluster/maintenanceConfigurations/default",  
      "name": "default",  
      "notAllowedTime": null,  
      "resourceGroup": "MyResourceGroup",  
      "systemData": null,  
      "timeInWeek": [  
        {  
          "day": "Monday",  
          "hourSlots": [  
            1  
          ]  
        }  
      ],  
      "type": null  
    },  
    {  
      "id":  
        "/subscriptions/<subscriptionID>/resourcegroups/MyResourceGroup/providers/Microsoft.ContainerService/managedClusters/myAKSCluster/maintenanceConfigurations/testConfiguration",  
        "name": "testConfiguration",  
        "notAllowedTime": null,  
        "resourceGroup": "MyResourceGroup",  
        "systemData": null,  
        "timeInWeek": [  
          {  
            "day": "Friday",  
            "hourSlots": [  
              4  
            ]  
          }  
        ],  
        "type": null  
      }  
  ]
```

Show a specific maintenance configuration window in an AKS cluster

To see a specific maintenance configuration window in your AKS Cluster, use the

```
az aks maintenanceconfiguration show
```

```
az aks maintenanceconfiguration show -g MyResourceGroup --cluster-name myAKSCluster --name default
```

The following example output shows the maintenance window for *default*.

```
{  
  "id":  
    "/subscriptions/<subscriptionID>/resourcegroups/MyResourceGroup/providers/Microsoft.ContainerService/managed  
Clusters/myAKSCluster/maintenanceConfigurations/default",  
  "name": "default",  
  "notAllowedTime": null,  
  "resourceGroup": "MyResourceGroup",  
  "systemData": null,  
  "timeInWeek": [  
    {  
      "day": "Monday",  
      "hourSlots": [  
        1  
      ]  
    }  
  ],  
  "type": null  
}
```

Delete a certain maintenance configuration window in an existing AKS Cluster

To delete a certain maintenance configuration window in your AKS Cluster, use the

```
az aks maintenanceconfiguration delete
```

```
az aks maintenanceconfiguration delete -g MyResourceGroup --cluster-name myAKSCluster --name default
```

Using Planned Maintenance with Cluster Auto-Upgrade

Planned Maintenance will detect if you are using Cluster Auto-Upgrade and schedule your upgrades during your maintenance window automatically. For more details on about Cluster Auto-Upgrade, see [Upgrade an Azure Kubernetes Service \(AKS\) cluster](#).

Next steps

- To get started with upgrading your AKS cluster, see [Upgrade an AKS cluster](#)

Use Planned Maintenance window for scheduling exclusive Azure Kubernetes Service (AKS) weekly releases (Preview)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Planned Maintenance allows you to schedule weekly maintenance windows that will ensure the weekly releases [releases](#) are controlled. Maintenance Windows are configured using the Azure CLI, allowing you to select from a set of pre-available configurations.

Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

Limitations

When you use Planned Maintenance, the following restrictions apply:

- AKS reserves the right to break these windows for unplanned/reactive maintenance operations that are urgent or critical.
- Currently, performing maintenance operations are considered *best-effort only* and are not guaranteed to occur within a specified window.
- Updates cannot be blocked for more than seven days.

Available pre-created public maintenance configurations for you to pick

There are two general kinds of pre-created public maintenance configurations:

- For Weekday (Monday, Tuesday, Wednesday, Thursday), from 10 pm to 6 am next morning.
- For Weekend (Friday, Saturday, Sunday), from 10 pm to 6 am next morning.

For a list of pre-created public maintenance configurations on the weekday schedule, see below. For weekend schedules, replace `weekday` with `weekend`.

CONFIGURATION NAME	TIME ZONE
aks-mrp-cfg-weekday_utc12	UTC+12

CONFIGURATION NAME	TIME ZONE
...	...
aks-mrp-cfg-weekday_utc1	UTC+1
aks-mrp-cfg-weekday_utc	UTC+0
aks-mrp-cfg-weekday_utc-1	UTC-1
...	...
aks-mrp-cfg-weekday_utc-12	UTC-12

Assign a public maintenance configuration to an AKS Cluster

Find the public maintenance configuration ID by name:

```
az maintenance public-configuration show --resource-name "aks-mrp-cfg-weekday_utc8"
```

This call may prompt you to install the `maintenance` extension. Once done, you can proceed:

The output should look like the below example. Be sure to take note of the `id` field -

```
{
  "duration": "08:00",
  "expirationDateTime": null,
  "extensionProperties": {
    "maintenanceSubScope": "AKS"
  },
  "id": "/subscriptions/0159df5c-b605-45a9-9876-
36e17d5286e0/providers/Microsoft.Maintenance/publicMaintenanceConfigurations/aks-mrp-cfg-weekday_utc8",
  "installPatches": null,
  "location": "westus2",
  "maintenanceScope": "Resource",
  "name": "aks-mrp-cfg-weekday_utc8",
  "namespace": "Microsoft.Maintenance",
  "recurEvery": "Week Monday,Tuesday,Wednesday,Thursday",
  "startDateTime": "2022-08-01 22:00",
  "systemData": null,
  "tags": {},
  "timeZone": "China Standard Time",
  "type": "Microsoft.Maintenance/publicMaintenanceConfigurations",
  "visibility": "Public"
}
```

Next, assign the public maintenance configuration to your AKS cluster using the ID:

```
az maintenance assignment create --maintenance-configuration-id "/subscriptions/0159df5c-b605-45a9-9876-
36e17d5286e0/providers/Microsoft.Maintenance/publicMaintenanceConfigurations/aks-mrp-cfg-weekday_utc8" --
name assignmentName --provider-name "Microsoft.ContainerService" --resource-group myResourceGroup --
resource-name myAKSCluster --resource-type "managedClusters"
```

List all maintenance windows in an existing cluster

```
az maintenance assignment list --provider-name "Microsoft.ContainerService" --resource-group myResourceGroup  
--resource-name myAKScluster --resource-type "managedClusters"
```

Delete a public maintenance configuration of an AKS cluster

```
az maintenance assignment delete --name assignmentName --provider-name "Microsoft.ContainerService" --  
resource-group myResourceGroup --resource-name myAKScluster --resource-type "managedClusters"
```

Enable Cloud Controller Manager

10/27/2022 • 2 minutes to read • [Edit Online](#)

As a Cloud Provider, Microsoft Azure works closely with the Kubernetes community to support our infrastructure on behalf of users.

Previously, Cloud provider integration with Kubernetes was "in-tree", where any changes to Cloud specific features would follow the standard Kubernetes release cycle. When issues were fixed or enhancements were rolled out, they would need to be within the Kubernetes community's release cycle.

The Kubernetes community is now adopting an "out-of-tree" model where the Cloud providers will control their releases independently of the core Kubernetes release schedule through the [cloud-provider-azure](#) component. As part of this cloud-provider-azure component, we are also introducing a cloud-node-manager component, which is a component of the Kubernetes node lifecycle controller. This component is deployed by a DaemonSet in the *kube-system* namespace. To view this component, use

```
kubectl get po -n kube-system | grep cloud-node-manager
```

We recently rolled out the Cloud Storage Interface (CSI) drivers to be the default in Kubernetes version 1.21 and above.

NOTE

When enabling Cloud Controller Manager on your AKS cluster, this will also enable the out of tree CSI drivers.

The Cloud Controller Manager is the default controller from Kubernetes 1.22, supported by AKS. If running < v1.22, follow instructions below.

Prerequisites

You must have the following resource installed:

- The Azure CLI
- Kubernetes version 1.20.x or above
- The `aks-preview` extension version 0.5.5 or later

Register the `EnableCloudControllerManager` feature flag

To use the Cloud Controller Manager feature, you must enable the `EnableCloudControllerManager` feature flag on your subscription.

```
az feature register --name EnableCloudControllerManager --namespace Microsoft.ContainerService
```

You can check on the registration status by using the `az feature list` command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/EnableCloudControllerManager')].{Name:name, State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider by using the `az provider register` command:

```
az provider register --namespace Microsoft.ContainerService
```

Install the aks-preview CLI extension

```
# Install the aks-preview extension  
az extension add --name aks-preview  
  
# Update the extension to make sure you have the latest version installed  
az extension update --name aks-preview
```

Create a new AKS cluster with Cloud Controller Manager with version <1.22

To create a cluster using the Cloud Controller Manager, pass `EnableCloudControllerManager=True` as a customer header to the Azure API using the Azure CLI.

```
az group create --name myResourceGroup --location eastus  
az aks create -n aks -g myResourceGroup --aks-custom-headers EnableCloudControllerManager=True
```

Upgrade an AKS cluster to Cloud Controller Manager on an existing cluster with version <1.22

To upgrade a cluster to use the Cloud Controller Manager, pass `EnableCloudControllerManager=True` as a customer header to the Azure API using the Azure CLI.

```
az aks upgrade -n aks -g myResourceGroup -k <version> --aks-custom-headers EnableCloudControllerManager=True
```

Next steps

- For more information on CSI drivers, and the default behavior for Kubernetes versions above 1.21, please see our [documentation](#).
- You can find more information about the Kubernetes community direction regarding Out of Tree providers on the [community blog post](#).

Upgrade an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 11 minutes to read • [Edit Online](#)

Part of the AKS cluster lifecycle involves performing periodic upgrades to the latest Kubernetes version. It's important you apply the latest security releases, or upgrade to get the latest features. This article shows you how to check for, configure, and apply upgrades to your AKS cluster.

For AKS clusters that use multiple node pools or Windows Server nodes, see [Upgrade a node pool in AKS](#).

Before you begin

- [Azure CLI](#)
- [Azure PowerShell](#)

This article requires that you're running the Azure CLI version 2.34.1 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

WARNING

An AKS cluster upgrade triggers a cordon and drain of your nodes. If you have a low compute quota available, the upgrade may fail. For more information, see [increase quotas](#)

Check for available AKS cluster upgrades

- [Azure CLI](#)
- [Azure PowerShell](#)

To check which Kubernetes releases are available for your cluster, use the `az aks get-upgrades` command. The following example checks for available upgrades to *myAKSCluster* in *myResourceGroup*.

```
az aks get-upgrades --resource-group myResourceGroup --name myAKSCluster --output table
```

NOTE

When you upgrade a supported AKS cluster, Kubernetes minor versions can't be skipped. All upgrades must be performed sequentially by major version number. For example, upgrades between *1.14.x-> 1.15.x* or *1.15.x-> 1.16.x* are allowed, however *1.14.x-> 1.16.x* is not allowed.

Skipping multiple versions can only be done when upgrading from an *unsupported version* back to a *supported version*. For example, an upgrade from an unsupported *1.10.x-> 1.15.x* can be completed if available.

The following example output shows that the cluster can be upgraded to versions *1.19.1* and *1.19.3*:

Name	ResourceGroup	MasterVersion	Upgrades
default	myResourceGroup	1.18.10	1.19.1, 1.19.3

The following example output means that the appservice-kube extension isn't compatible with your Azure CLI version (a minimum of version 2.34.1 is required):

```
The 'appservice-kube' extension is not compatible with this version of the CLI.  
You have CLI core version 2.0.81 and this extension requires a min of 2.34.1.  
Table output unavailable. Use the --query option to specify an appropriate query. Use --debug for more info.
```

If you receive this output, you need to update your Azure CLI version. The `az upgrade` command was added in version 2.11.0 and doesn't work with versions prior to 2.11.0. Older versions can be updated by reinstalling Azure CLI as described in [Install the Azure CLI](#). If your Azure CLI version is 2.11.0 or later, you'll receive a message to run `az upgrade` to upgrade Azure CLI to the latest version.

If your Azure CLI is updated and you receive the following example output, it means that no upgrades are available:

```
ERROR: Table output unavailable. Use the --query option to specify an appropriate query. Use --debug for more info.
```

If no upgrades are available, create a new cluster with a supported version of Kubernetes and migrate your workloads from the existing cluster to the new cluster. It's not supported to upgrade a cluster to a newer Kubernetes version when `az aks get-upgrades` shows that no upgrades are available.

Customize node surge upgrade

IMPORTANT

Node surges require subscription quota for the requested max surge count for each upgrade operation. For example, a cluster that has 5 node pools, each with a count of 4 nodes, has a total of 20 nodes. If each node pool has a max surge value of 50%, additional compute and IP quota of 10 nodes (2 nodes * 5 pools) is required to complete the upgrade.

If using Azure CNI, validate there are available IPs in the subnet as well to [satisfy IP requirements of Azure CNI](#).

By default, AKS configures upgrades to surge with one extra node. A default value of one for the max surge settings will enable AKS to minimize workload disruption by creating an extra node before the cordon/drain of existing applications to replace an older versioned node. The max surge value may be customized per node pool to enable a trade-off between upgrade speed and upgrade disruption. By increasing the max surge value, the upgrade process completes faster, but setting a large value for max surge may cause disruptions during the upgrade process.

For example, a max surge value of 100% provides the fastest possible upgrade process (doubling the node count) but also causes all nodes in the node pool to be drained simultaneously. You may wish to use a higher value such as this for testing environments. For production node pools, we recommend a `max_surge` setting of 33%.

AKS accepts both integer values and a percentage value for max surge. An integer such as "5" indicates five extra nodes to surge. A value of "50%" indicates a surge value of half the current node count in the pool. Max surge percent values can be a minimum of 1% and a maximum of 100%. A percent value is rounded up to the nearest node count. If the max surge value is higher than the current node count at the time of upgrade, the current node count is used for the max surge value.

During an upgrade, the max surge value can be a minimum of 1 and a maximum value equal to the number of nodes in your node pool. You can set larger values, but the maximum number of nodes used for max surge won't be higher than the number of nodes in the pool at the time of upgrade.

IMPORTANT

The max surge setting on a node pool is persistent. Subsequent Kubernetes upgrades or node version upgrades will use this setting. You may change the max surge value for your node pools at any time. For production node pools, we recommend a max-surge setting of 33%.

Use the following commands to set max surge values for new or existing node pools.

```
# Set max surge for a new node pool
az aks nodepool add -n mynodepool -g MyResourceGroup --cluster-name MyManagedCluster --max-surge 33%
```

```
# Update max surge for an existing node pool
az aks nodepool update -n mynodepool -g MyResourceGroup --cluster-name MyManagedCluster --max-surge 5
```

Upgrade an AKS cluster

- [Azure CLI](#)
- [Azure PowerShell](#)

With a list of available versions for your AKS cluster, use the [az aks upgrade](#) command to upgrade. During the upgrade process, AKS will:

- Add a new buffer node (or as many nodes as configured in [max surge](#)) to the cluster that runs the specified Kubernetes version.
- [Cordon and drain](#) one of the old nodes to minimize disruption to running applications. If you're using max surge, it will [cordon and drain](#) as many nodes at the same time as the number of buffer nodes specified.
- When the old node is fully drained, it will be reimaged to receive the new version, and it will become the buffer node for the following node to be upgraded.
- This process repeats until all nodes in the cluster have been upgraded.
- At the end of the process, the last buffer node will be deleted, maintaining the existing agent node count and zone balance.

NOTE

If no patch is specified, the cluster will automatically be upgraded to the specified minor version's latest GA patch. For example, setting `--kubernetes-version` to `1.21` will result in the cluster upgrading to `1.21.9`.

When upgrading by alias minor version, only a higher minor version is supported. For example, upgrading from `1.20.x` to `1.20` will not trigger an upgrade to the latest GA `1.20` patch, but upgrading to `1.21` will trigger an upgrade to the latest GA `1.21` patch.

```
az aks upgrade \
--resource-group myResourceGroup \
--name myAKSCluster \
--kubernetes-version KUBERNETES_VERSION
```

It takes a few minutes to upgrade the cluster, depending on how many nodes you have.

IMPORTANT

Ensure that any `PodDisruptionBudgets` (PDBs) allow for at least 1 pod replica to be moved at a time otherwise the drain/evict operation will fail. If the drain operation fails, the upgrade operation will fail by design to ensure that the applications are not disrupted. Please correct what caused the operation to stop (incorrect PDBs, lack of quota, and so on) and re-try the operation.

To confirm that the upgrade was successful, use the `az aks show` command:

```
az aks show --resource-group myResourceGroup --name myAKSCluster --output table
```

The following example output shows that the cluster now runs `1.19.1`:

Name	Location	ResourceGroup	KubernetesVersion	ProvisioningState	Fqdn
myAKSCluster	eastus	myResourceGroup	1.19.1	Succeeded	myakscluster-dns-379cbbb9.hcp.eastus.azmk8s.io

View the upgrade events

When you upgrade your cluster, the following Kubernetes events may occur on each node:

- Surge – Create surge node.
- Drain – Pods are being evicted from the node. Each pod has a 30-minute timeout to complete the eviction.
- Update – Update of a node has succeeded or failed.
- Delete – Deleted a surge node.

Use `kubectl get events` to show events in the default namespaces while running an upgrade. For example:

```
kubectl get events
```

The following example output shows some of the above events listed during an upgrade.

```
...
default 2m1s Normal Drain node/aks-nodepool1-96663640-vmss000001 Draining node: [aks-nodepool1-96663640-vmss000001]
...
default 9m22s Normal Surge node/aks-nodepool1-96663640-vmss000002 Created a surge node [aks-nodepool1-96663640-vmss000002 nodepool1] for agentpool %!s(MISSING)
...
```

Set auto-upgrade channel

In addition to manually upgrading a cluster, you can set an auto-upgrade channel on your cluster. For more information, see [Auto-upgrading an AKS cluster](#).

Special considerations for node pools that span multiple Availability Zones

AKS uses best-effort zone balancing in node groups. During an Upgrade surge, zone(s) for the surge node(s) in virtual machine scale sets is unknown ahead of time. This can temporarily cause an unbalanced zone

configuration during an upgrade. However, AKS deletes the surge node(s) once the upgrade has been completed and preserves the original zone balance. If you desire to keep your zones balanced during upgrade, increase the surge to a multiple of three nodes. Virtual machine scale sets will then balance your nodes across Availability Zones with best-effort zone balancing.

If you have PVCs backed by Azure LRS Disks, they'll be bound to a particular zone, and they may fail to recover immediately if the surge node doesn't match the zone of the PVC. This could cause downtime on your application when the Upgrade operation continues to drain nodes but the PVs are bound to a zone. To handle this case and maintain high availability, configure a [Pod Disruption Budget](#) on your application. This allows Kubernetes to respect your availability requirements during Upgrade's drain operation.

Next steps

This article showed you how to upgrade an existing AKS cluster. To learn more about deploying and managing AKS clusters, see the set of tutorials.

[AKS tutorials](#)

Azure Kubernetes Service (AKS) Uptime SLA

10/27/2022 • 3 minutes to read • [Edit Online](#)

Uptime SLA is a tier to enable a financially backed, higher SLA for an AKS cluster. Clusters with Uptime SLA, also referred to as [Paid SKU tier](#) in AKS REST APIs, come with greater amount of control plane resources and automatically scale to meet the load of your cluster. Uptime SLA guarantees 99.95% availability of the Kubernetes API server endpoint for clusters that use [Availability Zones](#), and 99.9% of availability for clusters that don't use Availability Zones. AKS uses master node replicas across update and fault domains to ensure SLA requirements are met.

AKS recommends use of Uptime SLA in production workloads to ensure availability of control plane components. By contrast, clusters on the [Free SKU tier](#) support fewer replicas and limited resources for the control plane and are not suitable for production workloads.

You can still create unlimited number of free clusters with a service level objective (SLO) of 99.5% and opt for the preferred SLO.

IMPORTANT

For clusters with egress lockdown, see [limit egress traffic](#) to open appropriate ports.

Region availability

- Uptime SLA is available in public regions and Azure Government regions where [AKS is supported](#).
- Uptime SLA is available for [private AKS clusters](#) in all public regions where AKS is supported.

SLA terms and conditions

Uptime SLA is a paid feature and is enabled per cluster. Uptime SLA pricing is determined by the number of discrete clusters, and not by the size of the individual clusters. You can view [Uptime SLA pricing details](#) for more information.

Before you begin

Azure CLI version 2.8.0 or later and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Creating a new cluster with Uptime SLA

To create a new cluster with the Uptime SLA, you use the Azure CLI. Create a new cluster in an existing resource group or create a new one. To learn more about resource groups and working with them, see [managing resource groups using the Azure CLI](#).

Use the `az aks create` command to create an AKS cluster. The following example creates a cluster named `myAKSCluster` with one node enables the Uptime SLA. This operation takes several minutes to complete:

```
az aks create --resource-group myResourceGroup --name myAKSCluster --uptime-sla --node-count 1
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster. The

following example output of the JSON snippet shows the paid tier for the SKU, indicating your cluster is enabled with Uptime SLA:

```
},
"sku": {
    "name": "Basic",
    "tier": "Paid"
},
```

Modify an existing cluster to use Uptime SLA

You can update your existing clusters to use Uptime SLA.

NOTE

Updating your cluster to enable the Uptime SLA does not disrupt its normal operation or impact its availability.

The following command uses the [az aks update](#) command to update the existing cluster:

```
# Update an existing cluster to use Uptime SLA
az aks update --resource-group myResourceGroup --name myAKSCluster --uptime-sla
```

This process takes several minutes to complete. When finished, the following example JSON snippet shows the paid tier for the SKU, indicating your cluster is enabled with Uptime SLA:

```
},
"sku": {
    "name": "Basic",
    "tier": "Paid"
},
```

Opt out of Uptime SLA

At any time you can opt out of using the Uptime SLA by updating your cluster to change it back to the free tier.

NOTE

Updating your cluster to stop using the Uptime SLA does not disrupt its normal operation or impact its availability.

The following command uses the [az aks update](#) command to update the existing cluster:

```
az aks update --resource-group myResourceGroup --name myAKSCluster --no-uptime-sla
```

This process takes several minutes to complete.

Next steps

- Use [Availability Zones](#) to increase high availability with your AKS cluster workloads.
- Configure your cluster to [limit egress traffic](#).

Draft for Azure Kubernetes Service (AKS) (preview)

10/27/2022 • 3 minutes to read • [Edit Online](#)

Draft is an open-source project that streamlines Kubernetes development by taking a non-containerized application and generating the Dockerfiles, Kubernetes manifests, Helm charts, Kustomize configurations, and other artifacts associated with a containerized application. Draft can also create a GitHub Action workflow file to quickly build and deploy applications onto any Kubernetes cluster.

How it works

Draft has the following commands to help ease your development on Kubernetes:

- **draft create**: Creates the Dockerfile and the proper manifest files.
- **draft setup-gh**: Sets up your GitHub OIDC.
- **draft generate-workflow**: Generates the GitHub Action workflow file for deployment onto your cluster.
- **draft up**: Sets up your GitHub OIDC and generates a GitHub Action workflow file, combining the previous two commands.

Prerequisites

- If you don't have an Azure subscription, create a [free account](#) before you begin.
- Install the latest version of the [Azure CLI](#) and the *aks-preview* extension.
- If you don't have one already, you need to create an [AKS cluster](#) and an Azure Container Registry instance.

Install the `aks-preview` Azure CLI extension

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

```
# Install the aks-preview extension
az extension add --name aks-preview

# Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

Create artifacts using `draft create`

To create a Dockerfile, Helm chart, Kubernetes manifest, or Kustomize files needed to deploy your application onto an AKS cluster, use the `draft create` command:

```
az aks draft create
```

You can also run the command on a specific directory using the `--destination` flag:

```
az aks draft create --destination /Workspaces/ContosoAir
```

Set up GitHub OIDC using `draft setup-gh`

To use Draft, you have to register your application with GitHub using `draft setup-gh`. This step only needs to be done once per repository.

```
az aks draft setup-gh
```

Generate a GitHub Action workflow file for deployment using `draft generate-workflow`

After you create your artifacts and set up GitHub OIDC, you can generate a GitHub Action workflow file, creating an action that deploys your application onto your AKS cluster. Once your workflow file is generated, you must commit it into your repository in order to initiate the GitHub Action.

```
az aks draft generate-workflow
```

You can also run the command on a specific directory using the `--destination` flag:

```
az aks draft generate-workflow --destination /Workspaces/ContosoAir
```

Set up GitHub OpenID Connect (OIDC) and generate a GitHub Action workflow file using `draft up`

`draft up` is a single command to accomplish GitHub OIDC setup and generate a GitHub Action workflow file for deployment. It effectively combines the `draft setup-gh` and `draft generate-workflow` commands, meaning it's most commonly used when getting started in a new repository for the first time, and only needs to be run once. Subsequent updates to the GitHub Action workflow file can be made using `draft generate-workflow`.

```
az aks draft up
```

You can also run the command on a specific directory using the `--destination` flag:

```
az aks draft up --destination /Workspaces/ContosoAir
```

Use Web Application Routing with Draft to make your application accessible over the internet

[Web Application Routing](#) is the easiest way to get your web application up and running in Kubernetes securely, removing the complexity of ingress controllers and certificate and DNS management while offering configuration for enterprises looking to bring their own. Web Application Routing offers a managed ingress controller based on nginx that you can use without restrictions and integrates out of the box with Open Service Mesh to secure intra-cluster communications.

To set up Draft with Web Application Routing, use `az aks draft update` and pass in the DNS name and Azure Key Vault-stored certificate when prompted:

```
az aks draft update
```

You can also run the command on a specific directory using the `--destination` flag:

```
az aks draft update --destination /Workspaces/ContosoAir
```

Reduce latency with proximity placement groups

10/27/2022 • 4 minutes to read • [Edit Online](#)

NOTE

When using proximity placement groups on AKS, colocation only applies to the agent nodes. Node to node and the corresponding hosted pod to pod latency is improved. The colocation does not affect the placement of a cluster's control plane.

When deploying your application in Azure, spreading Virtual Machine (VM) instances across regions or availability zones creates network latency, which may impact the overall performance of your application. A proximity placement group is a logical grouping used to make sure Azure compute resources are physically located close to each other. Some applications like gaming, engineering simulations, and high-frequency trading (HFT) require low latency and tasks that complete quickly. For high-performance computing (HPC) scenarios such as these, consider using [proximity placement groups](#) (PPG) for your cluster's node pools.

Before you begin

This article requires that you are running the Azure CLI version 2.14 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Limitations

- A proximity placement group can map to at most one availability zone.
- A node pool must use Virtual Machine Scale Sets to associate a proximity placement group.
- A node pool can associate a proximity placement group at node pool create time only.

Node pools and proximity placement groups

The first resource you deploy with a proximity placement group attaches to a specific data center. Additional resources deployed with the same proximity placement group are colocated in the same data center. Once all resources using the proximity placement group have been stopped (deallocated) or deleted, it's no longer attached.

- Many node pools can be associated with a single proximity placement group.
- A node pool may only be associated with a single proximity placement group.

Configure proximity placement groups with availability zones

NOTE

While proximity placement groups require a node pool to use at most one availability zone, the [baseline Azure VM SLA of 99.9%](#) is still in effect for VMs in a single zone.

Proximity placement groups are a node pool concept and associated with each individual node pool. Using a PPG resource has no impact on AKS control plane availability. This can impact how a cluster should be designed with zones. To ensure a cluster is spread across multiple zones the following design is recommended.

- Provision a cluster with the first system pool using 3 zones and no proximity placement group associated. This ensures the system pods land in a dedicated node pool which will spread across multiple zones.
- Add additional user node pools with a unique zone and proximity placement group associated to each pool.

An example is nodepool1 in zone 1 and PPG1, nodepool2 in zone 2 and PPG2, nodepool3 in zone 3 with PPG3. This ensures at a cluster level, nodes are spread across multiple zones and each individual node pool is colocated in the designated zone with a dedicated PPG resource.

Create a new AKS cluster with a proximity placement group

The following example uses the `az group create` command to create a resource group named *myResourceGroup* in the *centralus* region. An AKS cluster named *myAKSCluster* is then created using the `az aks create` command.

Accelerated networking greatly improves networking performance of virtual machines. Ideally, use proximity placement groups in conjunction with accelerated networking. By default, AKS uses accelerated networking on [supported virtual machine instances](#), which include most Azure virtual machine with two or more vCPUs.

Create a new AKS cluster with a proximity placement group associated to the first system node pool:

```
# Create an Azure resource group
az group create --name myResourceGroup --location centralus
```

Run the following command, and store the ID that is returned:

```
# Create proximity placement group
az ppg create -n myPPG -g myResourceGroup -l centralus -t standard
```

The command produces output, which includes the *id* value you need for upcoming CLI commands:

```
{
  "availabilitySets": null,
  "colocationStatus": null,
  "id": "/subscriptions/yourSubscriptionID/resourceGroups/myResourceGroup/providers/Microsoft.Compute/proximityPlacementGroups/myPPG",
  "location": "centralus",
  "name": "myPPG",
  "proximityPlacementGroupType": "Standard",
  "resourceGroup": "myResourceGroup",
  "tags": {},
  "type": "Microsoft.Compute/proximityPlacementGroups",
  "virtualMachineScaleSets": null,
  "virtualMachines": null
}
```

Use the proximity placement group resource ID for the *myPPGResourceID* value in the below command:

```
# Create an AKS cluster that uses a proximity placement group for the initial system node pool only. The PPG has no effect on the cluster control plane.
az aks create \
  --resource-group myResourceGroup \
  --name myAKScluster \
  --ppg myPPGResourceID
```

Add a proximity placement group to an existing cluster

You can add a proximity placement group to an existing cluster by creating a new node pool. You can then optionally migrate existing workloads to the new node pool, and then delete the original node pool.

Use the same proximity placement group that you created earlier, and this will ensure agent nodes in both node pools in your AKS cluster are physically located in the same data center.

Use the resource ID from the proximity placement group you created earlier, and add a new node pool with the [az aks nodepool add](#) command:

```
# Add a new node pool that uses a proximity placement group, use a --node-count = 1 for testing
az aks nodepool add \
    --resource-group myResourceGroup \
    --cluster-name myAKSCluster \
    --name mynodepool \
    --node-count 1 \
    --ppg myPPGResourceID
```

Clean up

To delete the cluster, use the [az group delete](#) command to delete the AKS resource group:

```
az group delete --name myResourceGroup --yes --no-wait
```

Next steps

- Learn more about [proximity placement groups](#).

Azure Kubernetes Service (AKS) node image upgrade

10/27/2022 • 4 minutes to read • [Edit Online](#)

AKS supports upgrading the images on a node so you're up to date with the newest OS and runtime updates. AKS regularly provides new images with the latest updates, so it's beneficial to upgrade your node's images regularly for the latest AKS features. Linux node images are updated weekly, and Windows node images updated monthly. Although customers will be notified of image upgrades via the AKS release notes, it might take up to a week for updates to be rolled out in all regions. This article shows you how to upgrade AKS cluster node images and how to update node pool images without upgrading the version of Kubernetes.

For more information about the latest images provided by AKS, see the [AKS release notes](#).

For information on upgrading the Kubernetes version for your cluster, see [Upgrade an AKS cluster](#).

NOTE

The AKS cluster must use virtual machine scale sets for the nodes.

Check if your node pool is on the latest node image

You can see what is the latest node image version available for your node pool with the following command:

```
az aks nodepool get-upgrades \
--nodepool-name mynodepool \
--cluster-name myAKSCluster \
--resource-group myResourceGroup
```

In the output you can see the `latestNodeImageVersion` like on the example below:

```
{
  "id": "/subscriptions/XXXX-XXX-XXX-XXX-
XXXXXXXX/resourcegroups/myResourceGroup/providers/Microsoft.ContainerService/managedClusters/myAKSCluster/agent
Pools/nodepool1/upgradeProfiles/default",
  "kubernetesVersion": "1.17.11",
  "latestNodeImageVersion": "AKSUBuntu-1604-2020.10.28",
  "name": "default",
  "osType": "Linux",
  "resourceGroup": "myResourceGroup",
  "type": "Microsoft.ContainerService/managedClusters/agentPools/upgradeProfiles",
  "upgrades": null
}
```

So for `nodepool1` the latest node image available is `AKSUBuntu-1604-2020.10.28`. You can now compare it with the current node image version in use by your node pool by running:

```
az aks nodepool show \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name mynodepool \
--query nodeImageVersion
```

An example output would be:

```
"AKSUbuntu-1604-2020.10.08"
```

So in this example you could upgrade from the current `AKSUbuntu-1604-2020.10.08` image version to the latest version `AKSUbuntu-1604-2020.10.28`.

Upgrade all nodes in all node pools

Upgrading the node image is done with `az aks upgrade`. To upgrade the node image, use the following command:

```
az aks upgrade \
--resource-group myResourceGroup \
--name myAKSCluster \
--node-image-only
```

During the upgrade, check the status of the node images with the following `kubectl` command to get the labels and filter out the current node image information:

NOTE

This command may differ slightly depending on the shell you use. See the [Kubernetes JSONPath documentation](#) for more information on Windows/PowerShell environments.

```
kubectl get nodes -o jsonpath='{range .items[*]}{.metadata.name}{"\t"}{.metadata.labels.kubernetes\\.azure\\.com\\/node-image-version}{"\n"}{end}'
```

When the upgrade is complete, use `az aks show` to get the updated node pool details. The current node image is shown in the `nodeImageVersion` property.

```
az aks show \
--resource-group myResourceGroup \
--name myAKSCluster
```

Upgrade a specific node pool

Upgrading the image on a node pool is similar to upgrading the image on a cluster.

To update the OS image of the node pool without doing a Kubernetes cluster upgrade, use the `--node-image-only` option in the following example:

```
az aks nodepool upgrade \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name mynodepool \
--node-image-only
```

During the upgrade, check the status of the node images with the following `kubectl` command to get the labels and filter out the current node image information:

NOTE

This command may differ slightly depending on the shell you use. See the [Kubernetes JSONPath documentation](#) for more information on Windows/PowerShell environments.

```
kubectl get nodes -o jsonpath='{range .items[*]}{.metadata.name}{"\t"}{.metadata.labels.kubernetes\.azure\.com\/node-image-version}{"\n"}{end}'
```

When the upgrade is complete, use `az aks nodepool show` to get the updated node pool details. The current node image is shown in the `nodeImageVersion` property.

```
az aks nodepool show \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name mynodepool
```

Upgrade node images with node surge

To speed up the node image upgrade process, you can upgrade your node images using a customizable node surge value. By default, AKS uses one additional node to configure upgrades.

If you'd like to increase the speed of upgrades, use the `--max-surge` value to configure the number of nodes to be used for upgrades so they complete faster. To learn more about the trade-offs of various `--max-surge` settings, see [Customize node surge upgrade](#).

The following command sets the max surge value for performing a node image upgrade:

```
az aks nodepool upgrade \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name mynodepool \  
  --max-surge 33% \  
  --node-image-only \  
  --no-wait
```

During the upgrade, check the status of the node images with the following `kubectl` command to get the labels and filter out the current node image information:

```
kubectl get nodes -o jsonpath='{range .items[*]}{.metadata.name} {"\t"}{.metadata.labels.kubernetes\.azure\.com\/node-image-version}{"\n"}{end}'
```

Use `az aks nodepool show` to get the updated node pool details. The current node image is shown in the `nodeImageVersion` property.

```
az aks nodepool show \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name mynodepool
```

Next steps

- See the [AKS release notes](#) for information about the latest node images.

- Learn how to upgrade the Kubernetes version with [Upgrade an AKS cluster](#).
- [Automatically apply cluster and node pool upgrades with GitHub Actions](#)
- Learn more about multiple node pools and how to upgrade node pools with [Create and manage multiple node pools](#).

Apply security updates to Azure Kubernetes Service (AKS) nodes automatically using GitHub Actions

10/27/2022 • 6 minutes to read • [Edit Online](#)

Security updates are a key part of maintaining your AKS cluster's security and compliance with the latest fixes for the underlying OS. These updates include OS security fixes or kernel updates. Some updates require a node reboot to complete the process.

Running `az aks upgrade` gives you a zero downtime way to apply updates. The command handles applying the latest updates to all your cluster's nodes, cordoning and draining traffic to the nodes, and restarting the nodes, then allowing traffic to the updated nodes. If you update your nodes using a different method, AKS will not automatically restart your nodes.

NOTE

The main difference between `az aks upgrade` when used with the `--node-image-only` flag is that, when it's used, only the node images will be upgraded. If omitted, both the node images and the Kubernetes control plane version will be upgraded. You can check [the docs for managed upgrades on nodes](#) and [the docs for cluster upgrades](#) for more in-depth information.

All Kubernetes' nodes run in a standard Azure virtual machine (VM). These VMs can be Windows or Linux-based. The Linux-based VMs use an Ubuntu image, with the OS configured to automatically check for updates every night.

When you use the `az aks upgrade` command, Azure CLI creates a surge of new nodes with the latest security and kernel updates, these nodes are initially cordoned to prevent any apps from being scheduled to them until the update is finished. After completion, Azure cordons (makes the node unavailable for scheduling of new workloads) and drains (moves the existent workloads to other node) the older nodes and uncordon the new ones, effectively transferring all the scheduled applications to the new nodes.

This process is better than updating Linux-based kernels manually because Linux requires a reboot when a new kernel update is installed. If you update the OS manually, you also need to reboot the VM, manually cordoning and draining all the apps.

This article shows you how you can automate the update process of AKS nodes. You'll use GitHub Actions and Azure CLI to create an update task based on `cron` that runs automatically.

Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

You also need the Azure CLI version 2.0.59 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

This article also assumes you have a [GitHub](#) account to create your actions in.

Create a timed GitHub Action

`cron` is a utility that allows you to run a set of commands, or job, on an automated schedule. To create job to

update your AKS nodes on an automated schedule, you'll need a repository to host your actions. Usually, GitHub actions are configured in the same repository as your application, but you can use any repository. For this article we'll be using your [profile repository](#). If you don't have one, create a new repository with the same name as your GitHub username.

1. Navigate to your repository on GitHub
2. Click on the **Actions** tab at the top of the page.
3. If you already set up a workflow in this repository, you'll be directed to the list of completed runs, in this case, click on the **New Workflow** button. If this is your first workflow in the repository, GitHub will present you with some project templates, click on the **Set up a workflow yourself** link below the description text.
4. Change the workflow `name` and `on` tags similar to the below. GitHub Actions use the same [POSIX cron syntax](#) as any Linux-based system. In this schedule, we're telling the workflow to run every 15 days at 3am.

```
name: Upgrade cluster node images
on:
  schedule:
    - cron: '0 3 */15 * *'
```

5. Create a new job using the below. This job is named `upgrade-node`, runs on an Ubuntu agent, and will connect to your Azure CLI account to execute the needed steps to upgrade the nodes.

```
name: Upgrade cluster node images
on:
  schedule:
    - cron: '0 3 */15 * *'
jobs:
  upgrade-node:
    runs-on: ubuntu-latest
```

Set up the Azure CLI in the workflow

In the `steps` key, you'll define all the work the workflow will execute to upgrade the nodes.

Download and sign in to the Azure CLI.

1. On the right-hand side of the GitHub Actions screen, find the *marketplace search bar* and type "Azure Login".
2. You'll get as a result, an Action called **Azure Login** published by **Azure**:

The screenshot shows the GitHub Marketplace search results for 'Azure Login'. At the top, there's a search bar with 'Azure Login' typed in. Below it, the text 'Marketplace / Search results' is displayed. The first result is 'Azure Login' by Azure, which has a blue checkmark indicating it's a verified action. The description says: 'Authenticate to Azure and run your Az CLI or Az PowerShell based Actions or scripts. gith...'. To the right of the action card, there's a star icon followed by the number '66', indicating the number of reviews. Below this, another action is listed: 'Azure Container Registry Login' by Azure, also with a blue checkmark, and a description: 'Log in to Azure Container Registry (ACR) or any private container registry'.

3. Click on **Azure Login**. On the next screen, click the **copy icon** in the top right of the code sample.

[Marketplace / Search results / Azure Login](#)

 **Azure Login**
By Azure  v1.1  43

Authenticate to Azure and run your Az CLI or Az PowerShell based Actions or scripts. [github.com/Azure/Actions](#)

[View full Marketplace listing](#)

Installation

Copy and paste the following snippet into your `.yml` file.

Version: v1.1 ▾ 

```
- name: Azure Login
  uses: Azure/login@v1.1
  with:
    # Paste output of `az ad sp create-for-rbac` as value of secret variable
    creds:
    # Set this value to true to enable Azure PowerShell Login in addition to
    enable-AzPSSession: # optional
    # Set this value to true to enable support for accessing tenants without
    allow-no-subscriptions: # optional
```

4. Paste the following under the `steps` key:

```
name: Upgrade cluster node images

on:
  schedule:
    - cron: '0 3 */15 * *'

jobs:
  upgrade-node:
    runs-on: ubuntu-latest

  steps:
    - name: Azure Login
      uses: Azure/login@v1.1
      with:
        creds: ${{ secrets.AZURE_CREDENTIALS }}
```

5. From the Azure CLI, run the following command to generate a new username and password.

```
az ad sp create-for-rbac --role Contributor --scopes /subscriptions/{subscriptionID} -o json
```

The output should be similar to the following json:

```
{
  "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "displayName": "azure-cli-xxxx-xx-xx-xx-xx-xx",
  "name": "http://azure-cli-xxxx-xx-xx-xx-xx-xx",
  "password": "xXxXxXxXx",
  "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

6. In a new browser window navigate to your GitHub repository and open the **Settings** tab of the

repository. Click **Secrets** then, click on **New Repository Secret**.

7. For *Name*, use `AZURE_CREDENTIALS`.

8. For *Value*, add the entire contents from the output of the previous step where you created a new username and password.

Secrets / New secret

Name

`AZURE_CREDENTIALS`

Value

```
{  
  "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",  
  "displayName": "azure-cli-xxxx-xx-xx-xx-xx",  
  "name": "http://azure-cli-xxxx-xx-xx-xx-xx",  
  "password": "xXxXxXxX",  
  "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"  
}
```

Add secret

9. Click **Add Secret**.

The CLI used by your action will be logged to your Azure account and ready to run commands.

To create the steps to execute Azure CLI commands.

1. Navigate to the **search page** on *GitHub marketplace* on the right-hand side of the screen and search *Azure CLI Action*. Choose *Azure CLI Action by Azure*.

Azure CLI Action

[Marketplace / Search results](#)



Azure CLI Action

By Azure

☆ 24

Automate your GitHub workflows using Azure CLI scripts

2. Click the copy button on the *GitHub marketplace result* and paste the contents of the action in the main editor, below the *Azure Login* step, similar to the following:

```

name: Upgrade cluster node images

on:
  schedule:
    - cron: '0 3 */15 * *'

jobs:
  upgrade-node:
    runs-on: ubuntu-latest

    steps:
      - name: Azure Login
        uses: Azure/login@v1.1
        with:
          creds: ${{ secrets.AZURE_CREDENTIALS }}
      - name: Upgrade node images
        uses: Azure/cli@v1.0.0
        with:
          inlineScript: az aks upgrade -g {resourceGroupName} -n {aksClusterName} --node-image-only -
-yes

```

TIP

You can decouple the `-g` and `-n` parameters from the command by adding them to secrets similar to the previous steps. Replace the `{resourceGroupName}` and `{aksClusterName}` placeholders by their secret counterparts, for example `${{secrets.RESOURCE_GROUP_NAME}}` and `${{secrets.AKS_CLUSTER_NAME}}`

3. Rename the file to `upgrade-node-images`.

4. Click **Start Commit**, add a message title, and save the workflow.

Once you create the commit, the workflow will be saved and ready for execution.

NOTE

To upgrade a single node pool instead of all node pools on the cluster, add the `--name` parameter to the

`az aks nodepool upgrade` command to specify the node pool name. For example:

```
az aks nodepool upgrade -g {resourceGroupName} --cluster-name {aksClusterName} --name {{nodePoolName}} -
-node-image-only
```

Run the GitHub Action manually

You can run the workflow manually, in addition to the scheduled run, by adding a new `on` trigger called `workflow_dispatch`. The finished file should look like the YAML below:

```
name: Upgrade cluster node images

on:
  schedule:
    - cron: '0 3 */15 * *'
  workflow_dispatch:

jobs:
  upgrade-node:
    runs-on: ubuntu-latest

    steps:
      - name: Azure Login
        uses: Azure/login@v1.1
        with:
          creds: ${{ secrets.AZURE_CREDENTIALS }}

    # Code for upgrading one or more node pools
```

Next steps

- See the [AKS release notes](#) for information about the latest node images.
- Learn how to upgrade the Kubernetes version with [Upgrade an AKS cluster](#).
- Learn more about multiple node pools and how to upgrade node pools with [Create and manage multiple node pools](#).
- Learn more about [system node pools](#)
- To learn how to save costs using Spot instances, see [add a spot node pool to AKS](#)

Apply security and kernel updates to Linux nodes in Azure Kubernetes Service (AKS)

10/27/2022 • 5 minutes to read • [Edit Online](#)

To protect your clusters, security updates are automatically applied to Linux nodes in AKS. These updates include OS security fixes or kernel updates. Some of these updates require a node reboot to complete the process. AKS doesn't automatically reboot these Linux nodes to complete the update process.

The process to keep Windows Server nodes up to date is a little different. Windows Server nodes don't receive daily updates. Instead, you perform an AKS upgrade that deploys new nodes with the latest base Window Server image and patches. For AKS clusters that use Windows Server nodes, see [Upgrade a node pool in AKS](#).

This article shows you how to use the open-source [kured \(KUBernetes REboot Daemon\)](#) to watch for Linux nodes that require a reboot, then automatically handle the rescheduling of running pods and node reboot process.

NOTE

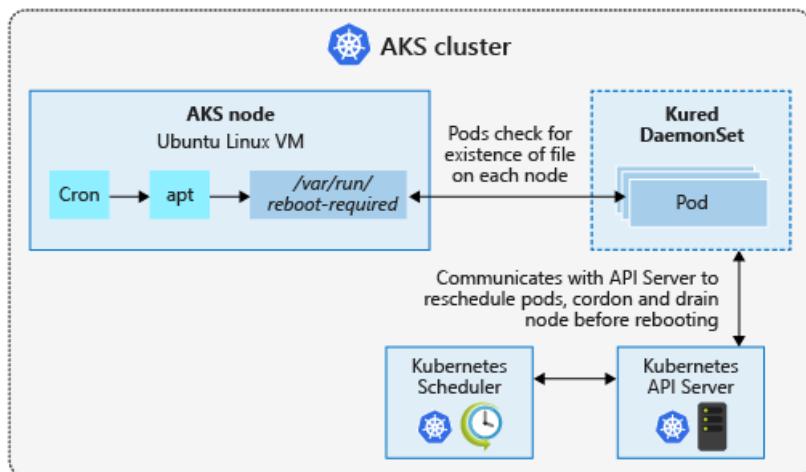
Kured is an open-source project by Weaveworks. Please direct issues to the [kured GitHub](#). Additional support can be found in the #weave-community Slack channel.

Before you begin

You need the Azure CLI version 2.0.59 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Understand the AKS node update experience

In an AKS cluster, your Kubernetes nodes run as Azure virtual machines (VMs). These Linux-based VMs use an Ubuntu image, with the OS configured to automatically check for updates every day. If security or kernel updates are available, they are automatically downloaded and installed.



Some security updates, such as kernel updates, require a node reboot to finalize the process. A Linux node that requires a reboot creates a file named `/var/run/reboot-required`. This reboot process doesn't happen automatically.

You can use your own workflows and processes to handle node reboots, or use [kured](#) to orchestrate the

process. With `kured`, a [DaemonSet](#) is deployed that runs a pod on each Linux node in the cluster. These pods in the DaemonSet watch for existence of the `/var/run/reboot-required` file, and then initiate a process to reboot the nodes.

Node image upgrades

Unattended upgrades apply updates to the Linux node OS, but the image used to create nodes for your cluster remains unchanged. If a new Linux node is added to your cluster, the original image is used to create the node. This new node will receive all the security and kernel updates available during the automatic check every day but will remain unpatched until all checks and restarts are complete.

Alternatively, you can use node image upgrade to check for and update node images used by your cluster. For more details on node image upgrade, see [Azure Kubernetes Service \(AKS\) node image upgrade](#).

Node upgrades

There is an additional process in AKS that lets you *upgrade* a cluster. An upgrade is typically to move to a newer version of Kubernetes, not just apply node security updates. An AKS upgrade performs the following actions:

- A new node is deployed with the latest security updates and Kubernetes version applied.
- An old node is cordoned and drained.
- Pods are scheduled on the new node.
- The old node is deleted.

You can't remain on the same Kubernetes version during an upgrade event. You must specify a newer version of Kubernetes. To upgrade to the latest version of Kubernetes, you can [upgrade your AKS cluster](#).

Deploy kured in an AKS cluster

To deploy the `kured` DaemonSet, install the following official Kured Helm chart. This creates a role and cluster role, bindings, and a service account, then deploys the DaemonSet using `kured`.

```
# Add the Kured Helm repository
helm repo add kubereboot https://kubereboot.github.io/charts/

# Update your local Helm chart repository cache
helm repo update

# Create a dedicated namespace where you would like to deploy kured into
kubectl create namespace kured

# Install kured in that namespace with Helm 3 (only on Linux nodes, kured is not working on Windows nodes)
helm install my-release kubereboot/kured --namespace kured --set nodeSelector."kubernetes.io/os"=linux
```

You can also configure additional parameters for `kured`, such as integration with Prometheus or Slack. For more information about additional configuration parameters, see the [kured Helm chart](#).

Update cluster nodes

By default, Linux nodes in AKS check for updates every evening. If you don't want to wait, you can manually perform an update to check that `kured` runs correctly. First, follow the steps to [SSH to one of your AKS nodes](#). Once you have an SSH connection to the Linux node, check for updates and apply them as follows:

```
sudo apt-get update && sudo apt-get upgrade -y
```

If updates were applied that require a node reboot, a file is written to `/var/run/reboot-required`. `Kured` checks for nodes that require a reboot every 60 minutes by default.

Monitor and review reboot process

When one of the replicas in the DaemonSet has detected that a node reboot is required, a lock is placed on the node through the Kubernetes API. This lock prevents additional pods being scheduled on the node. The lock also indicates that only one node should be rebooted at a time. With the node cordoned off, running pods are drained from the node, and the node is rebooted.

You can monitor the status of the nodes using the [kubectl get nodes](#) command. The following example output shows a node with a status of *SchedulingDisabled* as the node prepares for the reboot process:

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-28993262-0	Ready,SchedulingDisabled	agent	1h	v1.11.7

Once the update process is complete, you can view the status of the nodes using the [kubectl get nodes](#) command with the `--output wide` parameter. This additional output lets you see a difference in *KERNEL-VERSION* of the underlying nodes, as shown in the following example output. The *aks-nodepool1-28993262-0* was updated in a previous step and shows kernel version *4.15.0-1039-azure*. The node *aks-nodepool1-28993262-1* that hasn't been updated shows kernel version *4.15.0-1037-azure*.

NAME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE
AKS-NODEPOOL1-28993262-0	Ready	agent	1h	v1.11.7	10.240.0.4	<none>	Ubuntu
16.04.6 LTS	4.15.0-1039-azure	docker://3.0.4					
AKS-NODEPOOL1-28993262-1	Ready	agent	1h	v1.11.7	10.240.0.5	<none>	Ubuntu
16.04.6 LTS	4.15.0-1037-azure	docker://3.0.4					

Next steps

This article detailed how to use [kured](#) to reboot Linux nodes automatically as part of the security update process. To upgrade to the latest version of Kubernetes, you can [upgrade your AKS cluster](#).

For AKS clusters that use Windows Server nodes, see [Upgrade a node pool in AKS](#).

Connect to Azure Kubernetes Service (AKS) cluster nodes for maintenance or troubleshooting

10/27/2022 • 4 minutes to read • [Edit Online](#)

Throughout the lifecycle of your Azure Kubernetes Service (AKS) cluster, you may need to access an AKS node. This access could be for maintenance, log collection, or other troubleshooting operations. You can access AKS nodes using SSH, including Windows Server nodes. You can also [connect to Windows Server nodes using remote desktop protocol \(RDP\) connections](#). For security purposes, the AKS nodes aren't exposed to the internet. To connect to the AKS nodes, you use `kubectl debug` or the private IP address.

This article shows you how to create a connection to an AKS node.

Before you begin

This article assumes you have an SSH key. If not, you can create an SSH key using [macOS or Linux](#) or [Windows](#). If you use PuTTY Gen to create the key pair, save the key pair in an OpenSSH format rather than the default PuTTY private key format (.ppk file).

You also need the Azure CLI version 2.0.64 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create an interactive shell connection to a Linux node

To create an interactive shell connection to a Linux node, use the `kubectl debug` command to run a privileged container on your node. To list your nodes, use the `kubectl get nodes` command:

```
kubectl get nodes -o wide
```

The following example resembles output from the command:

NAME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE
KERNEL-VERSION	CONTAINER-RUNTIME						
aks-nodepool1-12345678-vmss000000	Ready	agent	13m	v1.19.9	10.240.0.4	<none>	Ubuntu
18.04.5 LTS	5.4.0-1046-azure	containerd://1.4.4+azure					
aks-nodepool1-12345678-vmss000001	Ready	agent	13m	v1.19.9	10.240.0.35	<none>	Ubuntu
18.04.5 LTS	5.4.0-1046-azure	containerd://1.4.4+azure					
aksnpnwin000000	Ready	agent	87s	v1.19.9	10.240.0.67	<none>	Windows
Server 2019 Datacenter	10.0.17763.1935	docker://19.3.1					

Use the `kubectl debug` command to run a container image on the node to connect to it.

```
kubectl debug node/aks-nodepool1-12345678-vmss000000 -it --image=mcr.microsoft.com/dotnet/runtime-deps:6.0
```

The following command starts a privileged container on your node and connects to it.

```
kubectl debug node/aks-nodepool1-12345678-vmss000000 -it --image=mcr.microsoft.com/dotnet/runtime-deps:6.0
```

The following example resembles output from the command:

```
Creating debugging pod node-debugger-aks-nodepool1-12345678-vmss000000-bkmmx with container debugger on node  
aks-nodepool1-12345678-vmss000000.
```

```
If you don't see a command prompt, try pressing enter.
```

```
root@aks-nodepool1-12345678-vmss000000:/#
```

This privileged container gives access to the node.

NOTE

You can interact with the node session by running `chroot /host` from the privileged container.

Remove Linux node access

When done, `exit` the interactive shell session. After the interactive container session closes, delete the pod used for access with `kubectl delete pod`.

```
kubectl delete pod node-debugger-aks-nodepool1-12345678-vmss000000-bkmmx
```

Create the SSH connection to a Windows node

At this time, you can't connect to a Windows Server node directly by using `kubectl debug`. Instead, you need to first connect to another node in the cluster, then connect to the Windows Server node from that node using SSH. Alternatively, you can [connect to Windows Server nodes using remote desktop protocol \(RDP\) connections](#) instead of using SSH.

To connect to another node in the cluster, use the `kubectl debug` command. For more information, see [Create an interactive shell connection to a Linux node](#).

To create the SSH connection to the Windows Server node from another node, use the SSH keys provided when you created the AKS cluster and the internal IP address of the Windows Server node.

Open a new terminal window and use the `kubectl get pods` command to get the name of the pod started by `kubectl debug`.

```
kubectl get pods
```

The following example resembles output from the command:

NAME	READY	STATUS	RESTARTS	AGE
node-debugger-aks-nodepool1-12345678-vmss000000-bkmmx	1/1	Running	0	21s

In the above example, `node-debugger-aks-nodepool1-12345678-vmss000000-bkmmx` is the name of the pod started by `kubectl debug`.

Use the `kubectl port-forward` command to open a connection to the deployed pod:

```
kubectl port-forward node-debugger-aks-nodepool1-12345678-vmss000000-bkmmx 2022:22
```

The following example resembles output from the command:

```
Forwarding from 127.0.0.1:2022 -> 22
Forwarding from [::1]:2022 -> 22
```

The above example begins forwarding network traffic from port 2022 on your development computer to port 22 on the deployed pod. When using `kubectl port-forward` to open a connection and forward network traffic, the connection remains open until you stop the `kubectl port-forward` command.

Open a new terminal and run the command `kubectl get nodes` to show the internal IP address of the Windows Server node:

```
kubectl get nodes -o wide
```

The following example resembles output from the command:

NAME	KERNEL-VERSION	CONTAINER-RUNTIME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE
aks-nodepool1-12345678-vmss00000	18.04.5 LTS	5.4.0-1046-azure	Ready	agent	13m	v1.19.9	10.240.0.4	<none>	Ubuntu
aks-nodepool1-12345678-vmss00001	18.04.5 LTS	5.4.0-1046-azure	Ready	agent	13m	v1.19.9	10.240.0.35	<none>	Ubuntu
aksnpwin00000	Server 2019 Datacenter	10.0.17763.1935	Ready	agent	87s	v1.19.9	10.240.0.67	<none>	Windows

In the above example, `10.240.0.67` is the internal IP address of the Windows Server node.

Create an SSH connection to the Windows Server node using the internal IP address, and connect to port 22 through port 2022 on your development computer. The default username for AKS nodes is `azureuser`. Accept the prompt to continue with the connection. You are then provided with the bash prompt of your Windows Server node:

```
ssh -o 'ProxyCommand ssh -p 2022 -W %h:%p azureuser@127.0.0.1' azureuser@10.240.0.67
```

The following example resembles output from the command:

```
The authenticity of host '10.240.0.67 (10.240.0.67)' can't be established.
ECDSA key fingerprint is SHA256:1234567890abcdefghijklmnopqrstuvwxyzABCDEF.
Are you sure you want to continue connecting (yes/no)? yes

[...]

Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

azureuser@aksnpwin00000 C:\Users\azureuser>
```

NOTE

If you prefer to use password authentication, include the parameter `-o PreferredAuthentications=password`. For example:

```
ssh -o 'ProxyCommand ssh -p 2022 -W %h:%p azureuser@127.0.0.1' -o PreferredAuthentications=password
azureuser@10.240.0.67
```

When done, `exit` the SSH session, stop any port forwarding, and then `exit` the interactive container session.

After the interactive container session closes, delete the pod used for SSH access using the `kubectl delete pod` command.

```
kubectl delete pod node-debugger-aks-nodepool1-12345678-vmss000000-bkmmx
```

Next steps

If you need more troubleshooting data, you can [view the kubelet logs](#) or [view the Kubernetes master node logs](#).

Create and configure an Azure Kubernetes Services (AKS) cluster to use virtual nodes

10/27/2022 • 2 minutes to read • [Edit Online](#)

To rapidly scale application workloads in an AKS cluster, you can use virtual nodes. With virtual nodes, you have quick provisioning of pods, and only pay per second for their execution time. You don't need to wait for Kubernetes cluster autoscaler to deploy VM compute nodes to run the additional pods. Virtual nodes are only supported with Linux pods and nodes.

The virtual nodes add-on for AKS, is based on the open source project [Virtual Kubelet](#).

This article gives you an overview of the region availability and networking requirements for using virtual nodes, as well as the known limitations.

Regional availability

All regions, where ACI supports VNET SKUs, are supported for virtual nodes deployments. For more details, see [Resource availability for Azure Container Instances in Azure regions](#).

For available CPU and memory SKUs in each region, please check the [Azure Container Instances Resource availability for Azure Container Instances in Azure regions - Linux container groups](#)

Network requirements

Virtual nodes enable network communication between pods that run in Azure Container Instances (ACI) and the AKS cluster. To provide this communication, a virtual network subnet is created and delegated permissions are assigned. Virtual nodes only work with AKS clusters created using *advanced* networking (Azure CNI). By default, AKS clusters are created with *basic* networking (kubenet).

Pods running in Azure Container Instances (ACI) need access to the AKS API server endpoint, in order to configure networking.

Known limitations

Virtual Nodes functionality is heavily dependent on ACI's feature set. In addition to the [quotas and limits for Azure Container Instances](#), the following scenarios are not yet supported with Virtual nodes:

- Using service principal to pull ACR images. [Workaround](#) is to use [Kubernetes secrets](#)
- [Virtual Network Limitations](#) including VNet peering, Kubernetes network policies, and outbound traffic to the internet with network security groups.
- Init containers
- [Host aliases](#)
- [Arguments](#) for exec in ACI
- [DaemonSets](#) will not deploy pods to the virtual nodes
- Virtual nodes support scheduling Linux pods. You can manually install the open source [Virtual Kubelet ACI](#) provider to schedule Windows Server containers to ACI.
- Virtual nodes require AKS clusters with Azure CNI networking.
- Using api server authorized ip ranges for AKS.
- Volume mounting Azure Files share support [General-purpose V2](#) and [General-purpose V1](#). Follow the

instructions for mounting a volume with Azure Files share.

- Using IPv6 is not supported.
- Virtual nodes don't support the [Container hooks](#) feature.

Next steps

Configure virtual nodes for your clusters:

- [Create virtual nodes using Azure CLI](#)
- [Create virtual nodes using the portal in Azure Kubernetes Services \(AKS\)](#)

Virtual nodes are often one component of a scaling solution in AKS. For more information on scaling solutions, see the following articles:

- [Use the Kubernetes horizontal pod autoscaler](#)
- [Use the Kubernetes cluster autoscaler](#)
- [Check out the Autoscale sample for Virtual Nodes](#)
- [Read more about the Virtual Kubelet open source library](#)

Create and configure an Azure Kubernetes Services (AKS) cluster to use virtual nodes using the Azure CLI

10/27/2022 • 7 minutes to read • [Edit Online](#)

This article shows you how to use the Azure CLI to create and configure the virtual network resources and AKS cluster, then enable virtual nodes.

Before you begin

Virtual nodes enable network communication between pods that run in Azure Container Instances (ACI) and the AKS cluster. To provide this communication, a virtual network subnet is created and delegated permissions are assigned. Virtual nodes only work with AKS clusters created using *advanced* networking (Azure CNI). By default, AKS clusters are created with *basic* networking (kubenet). This article shows you how to create a virtual network and subnets, then deploy an AKS cluster that uses advanced networking.

IMPORTANT

Before using virtual nodes with AKS, review both the [limitations of AKS virtual nodes](#) and the [virtual networking limitations of ACI](#). These limitations affect the location, networking configuration, and other configuration details of both your AKS cluster and the virtual nodes.

If you have not previously used ACI, register the service provider with your subscription. You can check the status of the ACI provider registration using the [az provider list](#) command, as shown in the following example:

```
az provider list --query "[?contains(namespace,'Microsoft.ContainerInstance')]" -o table
```

The *Microsoft.ContainerInstance* provider should report as *Registered*, as shown in the following example output:

Namespace	RegistrationState	RegistrationPolicy
Microsoft.ContainerInstance	Registered	RegistrationRequired

If the provider shows as *NotRegistered*, register the provider using the [az provider register](#) as shown in the following example:

```
az provider register --namespace Microsoft.ContainerInstance
```

Launch Azure Cloud Shell

The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

To open the Cloud Shell, select **Try it** from the upper right corner of a code block. You can also launch Cloud Shell in a separate browser tab by going to <https://shell.azure.com/bash>. Select **Copy** to copy the blocks of code,

paste it into the Cloud Shell, and press enter to run it.

If you prefer to install and use the CLI locally, this article requires Azure CLI version 2.0.49 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create a resource group

An Azure resource group is a logical group in which Azure resources are deployed and managed. Create a resource group with the `az group create` command. The following example creates a resource group named `myResourceGroup` in the `westus` location.

```
az group create --name myResourceGroup --location westus
```

Create a virtual network

Create a virtual network using the `az network vnet create` command. The following example creates a virtual network name `myVnet` with an address prefix of `10.0.0.0/8`, and a subnet named `myAKSSubnet`. The address prefix of this subnet defaults to `10.240.0.0/16`:

```
az network vnet create \
--resource-group myResourceGroup \
--name myVnet \
--address-prefixes 10.0.0.0/8 \
--subnet-name myAKSSubnet \
--subnet-prefix 10.240.0.0/16
```

Now create an additional subnet for virtual nodes using the `az network vnet subnet create` command. The following example creates a subnet named `myVirtualNodeSubnet` with the address prefix of `10.241.0.0/16`.

```
az network vnet subnet create \
--resource-group myResourceGroup \
--vnet-name myVnet \
--name myVirtualNodeSubnet \
--address-prefixes 10.241.0.0/16
```

Create an AKS cluster with managed identity

Instead of using a system-assigned identity, you can also use a user-assigned identity. For more information, see [Use managed identities](#).

You deploy an AKS cluster into the AKS subnet created in a previous step. Get the ID of this subnet using `az network vnet subnet show`:

```
az network vnet subnet show --resource-group myResourceGroup --vnet-name myVnet --name myAKSSubnet --query id -o tsv
```

Use the `az aks create` command to create an AKS cluster. The following example creates a cluster named `myAKSCluster` with one node. Replace `<subnetId>` with the ID obtained in the previous step.

```
az aks create \
--resource-group myResourceGroup \
--name myAKSCluster \
--node-count 1 \
--network-plugin azure \
--vnet-subnet-id <subnetId> \
```

After several minutes, the command completes and returns JSON-formatted information about the cluster.

Enable virtual nodes addon

To enable virtual nodes, now use the [az aks enable-addons](#) command. The following example uses the subnet named *myVirtualNodeSubnet* created in a previous step:

```
az aks enable-addons \
--resource-group myResourceGroup \
--name myAKSCluster \
--addons virtual-node \
--subnet-name myVirtualNodeSubnet
```

Connect to the cluster

To configure `kubectl` to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command. This step downloads credentials and configures the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

To verify the connection to your cluster, use the [kubectl get](#) command to return a list of the cluster nodes.

```
kubectl get nodes
```

The following example output shows the single VM node created and then the virtual node for Linux, *virtual-node-aci-linux*.

NAME	STATUS	ROLES	AGE	VERSION
virtual-node-aci-linux	Ready	agent	28m	v1.11.2
aks-agentpool-14693408-0	Ready	agent	32m	v1.11.2

Deploy a sample app

Create a file named `virtual-node.yaml` and copy in the following YAML. To schedule the container on the node, a `nodeSelector` and `toleration` are defined.

```

apiVersion: apps/v1
kind: Deployment
metadata:
  name: aci-helloworld
spec:
  replicas: 1
  selector:
    matchLabels:
      app: aci-helloworld
  template:
    metadata:
      labels:
        app: aci-helloworld
    spec:
      containers:
        - name: aci-helloworld
          image: mcr.microsoft.com/azuredocs/aci-helloworld
          ports:
            - containerPort: 80
      nodeSelector:
        kubernetes.io/role: agent
        beta.kubernetes.io/os: linux
        type: virtual-kubelet
      tolerations:
        - key: virtual-kubelet.io/provider
          operator: Exists
        - key: azure.com/aci
          effect: NoSchedule

```

Run the application with the [kubectl apply](#) command.

```
kubectl apply -f virtual-node.yaml
```

Use the [kubectl get pods](#) command with the `-o wide` argument to output a list of pods and the scheduled node. Notice that the `aci-helloworld` pod has been scheduled on the `virtual-node-aci-linux` node.

```
kubectl get pods -o wide
```

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE
aci-helloworld-9b55975f-bnmfl	1/1	Running	0	4m	10.241.0.4	virtual-node-aci-linux

The pod is assigned an internal IP address from the Azure virtual network subnet delegated for use with virtual nodes.

NOTE

If you use images stored in Azure Container Registry, [configure and use a Kubernetes secret](#). A current limitation of virtual nodes is that you can't use integrated Azure AD service principal authentication. If you don't use a secret, pods scheduled on virtual nodes fail to start and report the error `HTTP response status code 400 error code "InaccessibleImage"`.

Test the virtual node pod

To test the pod running on the virtual node, browse to the demo application with a web client. As the pod is assigned an internal IP address, you can quickly test this connectivity from another pod on the AKS cluster.

Create a test pod and attach a terminal session to it:

```
kubectl run -it --rm testvk --image=mcr.microsoft.com/dotnet/runtime-deps:6.0
```

Install `curl` in the pod using `apt-get`:

```
apt-get update && apt-get install -y curl
```

Now access the address of your pod using `curl`, such as <http://10.241.0.4>. Provide your own internal IP address shown in the previous `kubectl get pods` command:

```
curl -L http://10.241.0.4
```

The demo application is displayed, as shown in the following condensed example output:

```
<html>
<head>
  <title>Welcome to Azure Container Instances!</title>
</head>
[...]
```

Close the terminal session to your test pod with `exit`. When your session is ended, the pod is deleted.

Remove virtual nodes

If you no longer wish to use virtual nodes, you can disable them using the `az aks disable-addons` command.

If necessary, go to <https://shell.azure.com> to open Azure Cloud Shell in your browser.

First, delete the `aci-helloworld` pod running on the virtual node:

```
kubectl delete -f virtual-node.yaml
```

The following example command disables the Linux virtual nodes:

```
az aks disable-addons --resource-group myResourceGroup --name myAKSCluster --addons virtual-node
```

Now, remove the virtual network resources and resource group:

```

# Change the name of your resource group, cluster and network resources as needed
RES_GROUP=myResourceGroup
AKS_CLUSTER=myAKScluster
AKS_VNET=myVnet
AKS_SUBNET=myVirtualNodeSubnet

# Get AKS node resource group
NODE_RES_GROUP=$(az aks show --resource-group $RES_GROUP --name $AKS_CLUSTER --query nodeResourceGroup --
output tsv)

# Get network profile ID
NETWORK_PROFILE_ID=$(az network profile list --resource-group $NODE_RES_GROUP --query "[0].id" --output tsv)

# Delete the network profile
az network profile delete --id $NETWORK_PROFILE_ID -y

# Grab the service association link ID
SAL_ID=$(az network vnet subnet show --resource-group $RES_GROUP --vnet-name $AKS_VNET --name $AKS_SUBNET --
query id --output tsv)/providers/Microsoft.ContainerInstance/serviceAssociationLinks/default

# Delete the service association link for the subnet
az resource delete --ids $SAL_ID --api-version 2021-10-01

# Delete the subnet delegation to Azure Container Instances
az network vnet subnet update --resource-group $RES_GROUP --vnet-name $AKS_VNET --name $AKS_SUBNET --remove
delegations

```

Next steps

In this article, a pod was scheduled on the virtual node and assigned a private, internal IP address. You could instead create a service deployment and route traffic to your pod through a load balancer or ingress controller. For more information, see [Create a basic ingress controller in AKS](#).

Virtual nodes are often one component of a scaling solution in AKS. For more information on scaling solutions, see the following articles:

- [Use the Kubernetes horizontal pod autoscaler](#)
- [Use the Kubernetes cluster autoscaler](#)
- [Check out the Autoscale sample for Virtual Nodes](#)
- [Read more about the Virtual Kubelet open source library](#)

Create and configure an Azure Kubernetes Services (AKS) cluster to use virtual nodes in the Azure portal

10/27/2022 • 5 minutes to read • [Edit Online](#)

This article shows you how to use the Azure portal to create and configure the virtual network resources and an AKS cluster with virtual nodes enabled.

NOTE

This article gives you an overview of the region availability and limitations using virtual nodes.

Before you begin

Virtual nodes enable network communication between pods that run in Azure Container Instances (ACI) and the AKS cluster. To provide this communication, a virtual network subnet is created and delegated permissions are assigned. Virtual nodes only work with AKS clusters created using *advanced* networking (Azure CNI). By default, AKS clusters are created with *basic* networking (kubenet). This article shows you how to create a virtual network and subnets, then deploy an AKS cluster that uses advanced networking.

If you have not previously used ACI, register the service provider with your subscription. You can check the status of the ACI provider registration using the [az provider list](#) command, as shown in the following example:

```
az provider list --query "[?contains(namespace, 'Microsoft.ContainerInstance')]" -o table
```

The *Microsoft.ContainerInstance* provider should report as *Registered*, as shown in the following example output:

Namespace	RegistrationState	RegistrationPolicy
Microsoft.ContainerInstance	Registered	RegistrationRequired

If the provider shows as *NotRegistered*, register the provider using the [az provider register](#) as shown in the following example:

```
az provider register --namespace Microsoft.ContainerInstance
```

Sign in to Azure

Sign in to the Azure portal at <https://portal.azure.com>.

Create an AKS cluster

In the top left-hand corner of the Azure portal, select **Create a resource > Kubernetes Service**.

On the **Basics** page, configure the following options:

- **PROJECT DETAILS:** Select an Azure subscription, then select or create an Azure resource group, such as `myResourceGroup`. Enter a **Kubernetes cluster name**, such as `myAKSCluster`.
- **CLUSTER DETAILS:** Select a region and Kubernetes version for the AKS cluster.
- **PRIMARY NODE POOL:** Select a VM size for the AKS nodes. The VM size **cannot** be changed once an AKS cluster has been deployed.
 - Select the number of nodes to deploy into the cluster. For this article, set **Node count** to **1**. Node count **can** be adjusted after the cluster has been deployed.

Click **Next: Node Pools**.

On the **Node Pools** page, select *Enable virtual nodes*.

[Home](#) > [Kubernetes services](#) >

Create Kubernetes cluster ... X

[Basics](#) [**Node pools**](#) [Authentication](#) [Networking](#) [Integrations](#) [Tags](#) [Review + create](#)

Node pools

In addition to the required primary node pool configured on the Basics tab, you can also add optional node pools to handle a variety of workloads [Learn more about multiple node pools](#)

[+ Add node pool](#) [Delete](#)

Name	Mode	OS type	Node count	Node size
<input type="checkbox"/> <code>agentpool</code>	System	Linux	1	Standard_DS2_v2

Enable virtual nodes

Virtual nodes allow burstable scaling backed by serverless Azure Container Instances. [Learn more about virtual nodes](#)

`Enable virtual nodes` (i) ✓

Enable virtual machine scale sets

Enabling virtual machine scale sets will create a cluster that uses virtual machine scale sets instead of individual virtual machines for the cluster nodes. Virtual machine scale sets are required for scenarios including autoscaling, multiple node pools, and Windows support. [Learn more about virtual machine scale sets in AKS](#)

`Enable virtual machine scale sets` (i) ✓
 (i) Virtual machine scale sets are required for availability zones

[Review + create](#)

[< Previous](#)

[Next : Authentication >](#)

By default, a cluster identity is created. This cluster identity is used for cluster communication and integration with other Azure services. By default, this cluster identity is a managed identity. For more information, see [Use managed identities](#). You can also use a service principal as your cluster identity.

The cluster is also configured for advanced networking. The virtual nodes are configured to use their own Azure virtual network subnet. This subnet has delegated permissions to connect Azure resources between the AKS cluster. If you don't already have delegated subnet, the Azure portal creates and configures the Azure virtual network and subnet for use with the virtual nodes.

Select **Review + create**. After the validation is complete, select **Create**.

It takes a few minutes to create the AKS cluster and to be ready for use.

Connect to the cluster

The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account. To manage a Kubernetes cluster, use **kubectl**, the Kubernetes command-line client. The `kubectl` client is pre-installed in the Azure Cloud Shell.

To open the Cloud Shell, select Try it from the upper right corner of a code block. You can also launch Cloud Shell in a separate browser tab by going to <https://shell.azure.com/bash>. Select Copy to copy the blocks of code, paste it into the Cloud Shell, and press enter to run it.

Use the az aks get-credentials command to configure kubectl to connect to your Kubernetes cluster. The following example gets credentials for the cluster name *myAKSCluster* in the resource group named *myResourceGroup*.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

To verify the connection to your cluster, use the kubectl get command to return a list of the cluster nodes.

```
kubectl get nodes
```

The following example output shows the single VM node created and then the virtual node for Linux, *virtual-node-aci-linux*.

NAME	STATUS	ROLES	AGE	VERSION
virtual-node-aci-linux	Ready	agent	28m	v1.11.2
aks-agentpool-14693408-0	Ready	agent	32m	v1.11.2

Deploy a sample app

In the Azure Cloud Shell, create a file named `virtual-node.yaml` and copy in the following YAML. To schedule the container on the node, a `nodeSelector` and `toleration` are defined. These settings allow the pod to be scheduled on the virtual node and confirm that the feature is successfully enabled.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: aci-helloworld
spec:
  replicas: 1
  selector:
    matchLabels:
      app: aci-helloworld
  template:
    metadata:
      labels:
        app: aci-helloworld
    spec:
      containers:
        - name: aci-helloworld
          image: mcr.microsoft.com/azuredocs/aci-helloworld
          ports:
            - containerPort: 80
      nodeSelector:
        kubernetes.io/role: agent
        beta.kubernetes.io/os: linux
        type: virtual-kubelet
      tolerations:
        - key: virtual-kubelet.io/provider
          operator: Exists
```

Run the application with the kubectl apply command.

```
kubectl apply -f virtual-node.yaml
```

Use the `kubectl get pods` command with the `-o wide` argument to output a list of pods and the scheduled node.

Notice that the `virtual-node-helloworld` pod has been scheduled on the `virtual-node-linux` node.

```
kubectl get pods -o wide
```

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE
virtual-node-helloworld-9b55975f-bnmfl	1/1	Running	0	4m	10.241.0.4	virtual-node-aci-linux

The pod is assigned an internal IP address from the Azure virtual network subnet delegated for use with virtual nodes.

NOTE

If you use images stored in Azure Container Registry, [configure and use a Kubernetes secret](#). A current limitation of virtual nodes is that you can't use integrated Azure AD service principal authentication. If you don't use a secret, pods scheduled on virtual nodes fail to start and report the error `HTTP response status code 400 error code "InaccessibleImage"`.

Test the virtual node pod

To test the pod running on the virtual node, browse to the demo application with a web client. As the pod is assigned an internal IP address, you can quickly test this connectivity from another pod on the AKS cluster. Create a test pod and attach a terminal session to it:

```
kubectl run -it --rm virtual-node-test --image=mcr.microsoft.com/dotnet/runtime-deps:6.0
```

Install `curl` in the pod using `apt-get`:

```
apt-get update && apt-get install -y curl
```

Now access the address of your pod using `curl`, such as `http://10.241.0.4`. Provide your own internal IP address shown in the previous `kubectl get pods` command:

```
curl -L http://10.241.0.4
```

The demo application is displayed, as shown in the following condensed example output:

```
<html>
<head>
  <title>Welcome to Azure Container Instances!</title>
</head>
[...]
```

Close the terminal session to your test pod with `exit`. When your session is ended, the pod is deleted.

Next steps

In this article, a pod was scheduled on the virtual node and assigned a private, internal IP address. You could instead create a service deployment and route traffic to your pod through a load balancer or ingress controller. For more information, see [Create a basic ingress controller in AKS](#).

Virtual nodes are one component of a scaling solution in AKS. For more information on scaling solutions, see the following articles:

- [Use the Kubernetes horizontal pod autoscaler](#)
- [Use the Kubernetes cluster autoscaler](#)
- [Check out the Autoscale sample for Virtual Nodes](#)
- [Read more about the Virtual Kubelet open source library](#)

Automatically scale a cluster to meet application demands on Azure Kubernetes Service (AKS)

10/27/2022 • 12 minutes to read • [Edit Online](#)

To keep up with application demands in Azure Kubernetes Service (AKS), you may need to adjust the number of nodes that run your workloads. The cluster autoscaler component can watch for pods in your cluster that can't be scheduled because of resource constraints. When issues are detected, the number of nodes in a node pool is increased to meet the application demand. Nodes are also regularly checked for a lack of running pods, with the number of nodes then decreased as needed. This ability to automatically scale up or down the number of nodes in your AKS cluster lets you run an efficient, cost-effective cluster.

This article shows you how to enable and manage the cluster autoscaler in an AKS cluster.

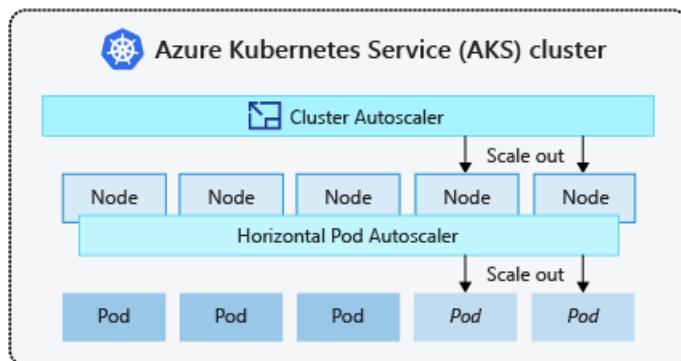
Before you begin

This article requires that you're running the Azure CLI version 2.0.76 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

About the cluster autoscaler

To adjust to changing application demands, such as between the workday and evening or on a weekend, clusters often need a way to automatically scale. AKS clusters can scale in one of two ways:

- The **cluster autoscaler** watches for pods that can't be scheduled on nodes because of resource constraints. The cluster then automatically increases the number of nodes.
- The **horizontal pod autoscaler** uses the Metrics Server in a Kubernetes cluster to monitor the resource demand of pods. If an application needs more resources, the number of pods is automatically increased to meet the demand.



Both the horizontal pod autoscaler and cluster autoscaler can also decrease the number of pods and nodes as needed. The cluster autoscaler decreases the number of nodes when there has been unused capacity for a period of time. Pods on a node to be removed by the cluster autoscaler are safely scheduled elsewhere in the cluster. The cluster autoscaler may be unable to scale down if pods can't move, such as in the following situations:

- A pod is directly created and isn't backed by a controller object, such as a deployment or replica set.
- A pod disruption budget (PDB) is too restrictive and doesn't allow the number of pods to be fall below a certain threshold.
- A pod uses node selectors or anti-affinity that can't be honored if scheduled on a different node.

For more information about how the cluster autoscaler may be unable to scale down, see [What types of pods can prevent the cluster autoscaler from removing a node?](#)

The cluster autoscaler uses startup parameters for things like time intervals between scale events and resource thresholds. For more information on what parameters the cluster autoscaler uses, see [Using the autoscaler profile](#).

The cluster and horizontal pod autoscalers can work together, and are often both deployed in a cluster. When combined, the horizontal pod autoscaler is focused on running the number of pods required to meet application demand. The cluster autoscaler is focused on running the number of nodes required to support the scheduled pods.

NOTE

Manual scaling is disabled when you use the cluster autoscaler. Let the cluster autoscaler determine the required number of nodes. If you want to manually scale your cluster, [disable the cluster autoscaler](#).

Create an AKS cluster and enable the cluster autoscaler

If you need to create an AKS cluster, use the `az aks create` command. To enable and configure the cluster autoscaler on the node pool for the cluster, use the `--enable-cluster-autoscaler` parameter, and specify a node `--min-count` and `--max-count`.

IMPORTANT

The cluster autoscaler is a Kubernetes component. Although the AKS cluster uses a virtual machine scale set for the nodes, don't manually enable or edit settings for scale set autoscale in the Azure portal or using the Azure CLI. Let the Kubernetes cluster autoscaler manage the required scale settings. For more information, see [Can I modify the AKS resources in the node resource group?](#)

The following example creates an AKS cluster with a single node pool backed by a virtual machine scale set. It also enables the cluster autoscaler on the node pool for the cluster and sets a minimum of 1 and maximum of 3 nodes:

```
# First create a resource group
az group create --name myResourceGroup --location eastus

# Now create the AKS cluster and enable the cluster autoscaler
az aks create \
  --resource-group myResourceGroup \
  --name myAKSCluster \
  --node-count 1 \
  --vm-set-type VirtualMachineScaleSets \
  --load-balancer-sku standard \
  --enable-cluster-autoscaler \
  --min-count 1 \
  --max-count 3
```

It takes a few minutes to create the cluster and configure the cluster autoscaler settings.

Update an existing AKS cluster to enable the cluster autoscaler

Use the `az aks update` command to enable and configure the cluster autoscaler on the node pool for the existing cluster. Use the `--enable-cluster-autoscaler` parameter, and specify a node `--min-count` and `--max-count`.

IMPORTANT

The cluster autoscaler is a Kubernetes component. Although the AKS cluster uses a virtual machine scale set for the nodes, don't manually enable or edit settings for scale set autoscale in the Azure portal or using the Azure CLI. Let the Kubernetes cluster autoscaler manage the required scale settings. For more information, see [Can I modify the AKS resources in the node resource group?](#)

The following example updates an existing AKS cluster to enable the cluster autoscaler on the node pool for the cluster and sets a minimum of 1 and maximum of 3 nodes:

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--enable-cluster-autoscaler \
--min-count 1 \
--max-count 3
```

It takes a few minutes to update the cluster and configure the cluster autoscaler settings.

Change the cluster autoscaler settings

IMPORTANT

If you have multiple node pools in your AKS cluster, skip to the [autoscale with multiple agent pools section](#). Clusters with multiple agent pools require use of the `az aks nodepool` command set to change node pool specific properties instead of `az aks`.

In the previous step to create an AKS cluster or update an existing node pool, the cluster autoscaler minimum node count was set to 1, and the maximum node count was set to 3. As your application demands change, you may need to adjust the cluster autoscaler node count.

To change the node count, use the `az aks update` command.

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--update-cluster-autoscaler \
--min-count 1 \
--max-count 5
```

The above example updates cluster autoscaler on the single node pool in *myAKSCluster* to a minimum of 1 and maximum of 5 nodes.

NOTE

The cluster autoscaler will enforce the minimum count in cases where the actual count drops below the minimum due to external factors, such as during a spot eviction or when changing the minimum count value from the AKS API.

Monitor the performance of your applications and services, and adjust the cluster autoscaler node counts to match the required performance.

Using the autoscaler profile

You can also configure more granular details of the cluster autoscaler by changing the default values in the cluster-wide autoscaler profile. For example, a scale down event happens after nodes are under-utilized after 10 minutes. If you had workloads that ran every 15 minutes, you may want to change the autoscaler profile to scale down under utilized nodes after 15 or 20 minutes. When you enable the cluster autoscaler, a default profile is used unless you specify different settings. The cluster autoscaler profile has the following settings that you can update:

SETTING	DESCRIPTION	DEFAULT VALUE
scan-interval	How often cluster is reevaluated for scale up or down	10 seconds
scale-down-delay-after-add	How long after scale up that scale down evaluation resumes	10 minutes
scale-down-delay-after-delete	How long after node deletion that scale down evaluation resumes	scan-interval
scale-down-delay-after-failure	How long after scale down failure that scale down evaluation resumes	3 minutes
scale-down-unneeded-time	How long a node should be unneeded before it is eligible for scale down	10 minutes
scale-down-unready-time	How long an unready node should be unneeded before it is eligible for scale down	20 minutes
scale-down-utilization-threshold	Node utilization level, defined as sum of requested resources divided by capacity, below which a node can be considered for scale down	0.5
max-graceful-termination-sec	Maximum number of seconds the cluster autoscaler waits for pod termination when trying to scale down a node	600 seconds
balance-similar-node-groups	Detects similar node pools and balances the number of nodes between them	false
expander	Type of node pool expander to be used in scale up. Possible values: <code>most-pods</code> , <code>random</code> , <code>least-waste</code> , <code>priority</code>	random
skip-nodes-with-local-storage	If true cluster autoscaler will never delete nodes with pods with local storage, for example, EmptyDir or HostPath	true
skip-nodes-with-system-pods	If true cluster autoscaler will never delete nodes with pods from kube-system (except for DaemonSet or mirror pods)	true

SETTING	DESCRIPTION	DEFAULT VALUE
max-empty-bulk-delete	Maximum number of empty nodes that can be deleted at the same time	10 nodes
new-pod-scale-up-delay	For scenarios like burst/batch scale where you don't want CA to act before the kubernetes scheduler could schedule all the pods, you can tell CA to ignore unscheduled pods before they're a certain age.	0 seconds
max-total-unready-percentage	Maximum percentage of unready nodes in the cluster. After this percentage is exceeded, CA halts operations	45%
max-node-provision-time	Maximum time the autoscaler waits for a node to be provisioned	15 minutes
ok-total-unready-count	Number of allowed unready nodes, irrespective of max-total-unready-percentage	3 nodes

IMPORTANT

The cluster autoscaler profile affects all node pools that use the cluster autoscaler. You can't set an autoscaler profile per node pool.

The cluster autoscaler profile requires version 2.11.1 or greater of the Azure CLI. If you need to install or upgrade, see [Install Azure CLI](#).

Set the cluster autoscaler profile on an existing AKS cluster

Use the `az aks update` command with the `cluster-autoscaler-profile` parameter to set the cluster autoscaler profile on your cluster. The following example configures the scan interval setting as 30s in the profile.

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--cluster-autoscaler-profile scan-interval=30s
```

When you enable the cluster autoscaler on node pools in the cluster, these node pools with CA enabled will also use the cluster autoscaler profile. For example:

```
az aks nodepool update \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name mynodepool \
--enable-cluster-autoscaler \
--min-count 1 \
--max-count 3
```

IMPORTANT

When you set the cluster autoscaler profile, any existing node pools with the cluster autoscaler enabled will start using the profile immediately.

Set the cluster autoscaler profile when creating an AKS cluster

You can also use the `cluster-autoscaler-profile` parameter when you create your cluster. For example:

```
az aks create \
--resource-group myResourceGroup \
--name myAKSCluster \
--node-count 1 \
--enable-cluster-autoscaler \
--min-count 1 \
--max-count 3 \
--cluster-autoscaler-profile scan-interval=30s
```

The above command creates an AKS cluster and defines the scan interval as 30 seconds for the cluster-wide autoscaler profile. The command also enables the cluster autoscaler on the initial node pool, sets the minimum node count to 1 and the maximum node count to 3.

Reset cluster autoscaler profile to default values

Use the `az aks update` command to reset the cluster autoscaler profile on your cluster.

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--cluster-autoscaler-profile ""
```

Disable the cluster autoscaler

If you no longer wish to use the cluster autoscaler, you can disable it using the `az aks update` command, specifying the `--disable-cluster-autoscaler` parameter. Nodes aren't removed when the cluster autoscaler is disabled.

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--disable-cluster-autoscaler
```

You can manually scale your cluster after disabling the cluster autoscaler by using the `az aks scale` command. If you use the horizontal pod autoscaler, that feature continues to run with the cluster autoscaler disabled, but pods may end up unable to be scheduled if all node resources are in use.

Re-enable a disabled cluster autoscaler

If you wish to re-enable the cluster autoscaler on an existing cluster, you can re-enable it using the `az aks update` command, specifying the `--enable-cluster-autoscaler`, `--min-count`, and `--max-count` parameters.

Retrieve cluster autoscaler logs and status

To diagnose and debug autoscaler events, logs and status can be retrieved from the cluster autoscaler.

AKS manages the cluster autoscaler on your behalf and runs it in the managed control plane. You can enable

control plane node to see the logs and operations from CA.

To configure logs to be pushed from the cluster autoscaler into Log Analytics, follow these steps.

1. Set up a rule for resource logs to push cluster-autoscaler logs to Log Analytics. [Instructions are detailed here](#), ensure you check the box for `cluster-autoscaler` when selecting options for "Logs".
 2. Select the "Logs" section on your cluster via the Azure portal.
 3. Input the following example query into Log Analytics:

```
AzureDiagnostics  
| where Category == "cluster-autoscaler"
```

You should see logs similar to the following example as long as there are logs to retrieve.

The screenshot shows the Azure Log Analytics workspace interface. On the left, there's a navigation sidebar with sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Node pools, Upgrade, Scale, Networking, Dev Spaces, Deployment center (preview), Policies (preview), Properties, Locks, Export template, Monitoring, Insights, Metrics (preview), and Logs. The main area has a search bar at the top left, followed by a 'New Query 1*' button and a 'Run' button. Below that is a 'Time range : Last 24 hours' dropdown. The central part of the screen shows a schema editor with 'Schema' and 'Filter' tabs, and a query editor with the following code:

```
AzureDiagnostics  
| where Category == "cluster-autoscaler"
```

Below the schema editor, there's a 'Completed. Showing results from the last 24 hours.' message and a timestamp of 00:00:00.286. At the bottom, there are tabs for 'Table' (selected) and 'Chart', and a 'Columns' dropdown. A table below shows the results of the query, with columns: TimeGenerated [UTC], OperationName, Category, and cpnNamespace_s. The table lists multiple entries for each second from 11/7/2019, 9:35:00.000 PM to 11/7/2019, 9:35:00.000 PM, all categorized under 'cluster-autoscaler'.

The cluster autoscaler will also write out health status to a `configmap` named `cluster-autoscaler-status`. To retrieve these logs, execute the following `kubectl` command. A health status will be reported for each node pool configured with the cluster autoscaler.

```
kubectl get configmap -n kube-system cluster-autoscaler-status -o yaml
```

To learn more about what is logged from the autoscaler, read the FAQ on the [Kubernetes/autoscaler GitHub project](#).

Use the cluster autoscaler with multiple node pools enabled

The cluster autoscaler can be used together with [multiple node pools](#) enabled. Follow that document to learn how to enable multiple node pools and add additional node pools to an existing cluster. When using both features together, you enable the cluster autoscaler on each individual node pool in the cluster and can pass unique autoscaling rules to each.

The below command assumes you followed the [initial instructions](#) earlier in this document and you want to update an existing node pool's max-count from 3 to 5. Use the [`az aks nodepool update`](#) command to update an existing node pool's settings.

```
az aks nodepool update \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name nodepool1 \  
  --update-cluster-autoscaler \  
  --min-count 1 \  
  --max-count 5
```

The cluster autoscaler can be disabled with `az aks nodepool update` and passing the

```
--disable-cluster-autoscaler
```

```
az aks nodepool update \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name nodepool1 \  
  --disable-cluster-autoscaler
```

If you wish to re-enable the cluster autoscaler on an existing cluster, you can re-enable it using the `az aks nodepool update` command, specifying the `--enable-cluster-autoscaler`, `--min-count`, and `--max-count` parameters.

NOTE

If you are planning on using the cluster autoscaler with nodepools that span multiple zones and leverage scheduling features related to zones such as volume topological scheduling, the recommendation is to have one nodepool per zone and enable the `--balance-similar-node-groups` through the autoscaler profile. This will ensure that the autoscaler will scale up successfully and try and keep the sizes of the nodepools balanced.

Configure the horizontal pod autoscaler

Kubernetes supports [horizontal pod autoscaling](#) to adjust the number of pods in a deployment depending on CPU utilization or other select metrics. The [Metrics Server](#) is used to provide resource utilization to Kubernetes. You can configure horizontal pod autoscaling through the `kubectl autoscale` command or through a manifest. For more details on using the horizontal pod autoscaler, see [HorizontalPodAutoscaler Walkthrough](#).

Next steps

This article showed you how to automatically scale the number of AKS nodes. You can also use the horizontal pod autoscaler to automatically adjust the number of pods that run your application. For steps on using the horizontal pod autoscaler, see [Scale applications in AKS](#).

To further help improve cluster resource utilization and free up CPU and memory for other pods, see [Vertical Pod Autoscaler](#).

Create an Azure Kubernetes Service (AKS) cluster that uses availability zones

10/27/2022 • 7 minutes to read • [Edit Online](#)

An Azure Kubernetes Service (AKS) cluster distributes resources such as nodes and storage across logical sections of underlying Azure infrastructure. This deployment model when using availability zones, ensures nodes in a given availability zone are physically separated from those defined in another availability zone. AKS clusters deployed with multiple availability zones configured across a cluster provide a higher level of availability to protect against a hardware failure or a planned maintenance event.

By defining node pools in a cluster to span multiple zones, nodes in a given node pool are able to continue operating even if a single zone has gone down. Your applications can continue to be available even if there is a physical failure in a single datacenter if orchestrated to tolerate failure of a subset of nodes.

This article shows you how to create an AKS cluster and distribute the node components across availability zones.

Before you begin

You need the Azure CLI version 2.0.76 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Limitations and region availability

AKS clusters can currently be created using availability zones in the following regions:

- Australia East
- Brazil South
- Canada Central
- Central India
- Central US
- East Asia
- East US
- East US 2
- France Central
- Germany West Central
- Japan East
- Korea Central
- North Europe
- Norway East
- Southeast Asia
- South Africa North
- South Central US
- Sweden Central
- Switzerland North
- UK South
- US Gov Virginia

- West Europe
- West US 2
- West US 3

The following limitations apply when you create an AKS cluster using availability zones:

- You can only define availability zones when the cluster or node pool is created.
- Availability zone settings can't be updated after the cluster is created. You also can't update an existing, non-availability zone cluster to use availability zones.
- The chosen node size (VM SKU) selected must be available across all availability zones selected.
- Clusters with availability zones enabled require use of Azure Standard Load Balancers for distribution across zones. This load balancer type can only be defined at cluster create time. For more information and the limitations of the standard load balancer, see [Azure load balancer standard SKU limitations](#).

Azure disk availability zone support

- Volumes that use Azure managed LRS disks are not zone-redundant resources, those volumes cannot be attached across zones and must be co-located in the same zone as a given node hosting the target pod.
- Volumes that use Azure managed ZRS disks(supported by Azure Disk CSI driver v1.5.0+) are zone-redundant resources, those volumes can be scheduled on all zone and non-zone agent nodes.

Kubernetes is aware of Azure availability zones since version 1.12. You can deploy a PersistentVolumeClaim object referencing an Azure Managed Disk in a multi-zone AKS cluster and [Kubernetes will take care of scheduling](#) any pod that claims this PVC in the correct availability zone.

Azure Resource Manager templates and availability zones

When *creating* an AKS cluster, if you explicitly define a [null value in a template](#) with syntax such as `"availabilityZones": null`, the Resource Manager template treats the property as if it doesn't exist, which means your cluster won't have availability zones enabled. Also, if you create a cluster with a Resource Manager template that omits the availability zones property, availability zones are disabled.

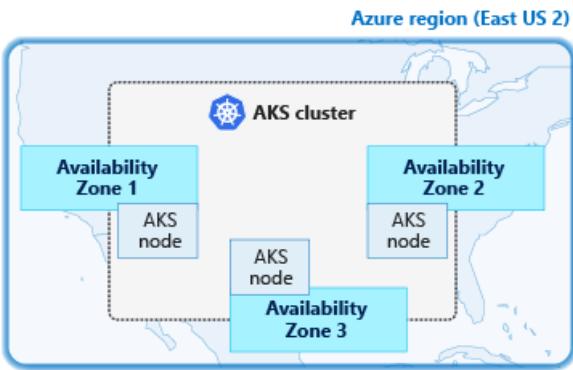
You can't update settings for availability zones on an existing cluster, so the behavior is different when updating an AKS cluster with Resource Manager templates. If you explicitly set a null value in your template for availability zones and *update* your cluster, there are no changes made to your cluster for availability zones. However, if you omit the availability zones property with syntax such as `"availabilityZones": []`, the deployment attempts to disable availability zones on your existing AKS cluster and **fails**.

Overview of availability zones for AKS clusters

Availability zones are a high-availability offering that protects your applications and data from datacenter failures. Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's always more than one zone in all zone enabled regions. The physical separation of availability zones within a region protects applications and data from datacenter failures.

For more information, see [What are availability zones in Azure?](#).

AKS clusters that are deployed using availability zones can distribute nodes across multiple zones within a single region. For example, a cluster in the *East US 2* region can create nodes in all three availability zones in *East US 2*. This distribution of AKS cluster resources improves cluster availability as they're resilient to failure of a specific zone.



If a single zone becomes unavailable, your applications continue to run if the cluster is spread across multiple zones.

Create an AKS cluster across availability zones

When you create a cluster using the `az aks create` command, the `--zones` parameter defines which zones agent nodes are deployed into. The control plane components such as etcd or the API are spread across the available zones in the region if you define the `--zones` parameter at cluster creation time. The specific zones which the control plane components are spread across are independent of what explicit zones are selected for the initial node pool.

If you don't define any zones for the default agent pool when you create an AKS cluster, control plane components are not guaranteed to spread across availability zones. You can add additional node pools using the `az aks nodepool add` command and specify `--zones` for new nodes, but it will not change how the control plane has been spread across zones. Availability zone settings can only be defined at cluster or node pool create-time.

The following example creates an AKS cluster named *myAKSCluster* in the resource group named *myResourceGroup*. A total of 3 nodes are created - one agent in zone 1, one in 2, and then one in 3.

```
az group create --name myResourceGroup --location eastus2

az aks create \
    --resource-group myResourceGroup \
    --name myAKSCluster \
    --generate-ssh-keys \
    --vm-set-type VirtualMachineScaleSets \
    --load-balancer-sku standard \
    --node-count 3 \
    --zones 1 2 3
```

It takes a few minutes to create the AKS cluster.

When deciding what zone a new node should belong to, a given AKS node pool will use a [best effort zone balancing offered by underlying Azure Virtual Machine Scale Sets](#). A given AKS node pool is considered "balanced" if each zone has the same number of VMs or +- 1 VM in all other zones for the scale set.

Verify node distribution across zones

When the cluster is ready, list the agent nodes in the scale set to see what availability zone they're deployed in.

First, get the AKS cluster credentials using the `az aks get-credentials` command:

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

Next, use the `kubectl describe` command to list the nodes in the cluster and filter on the

```
topology.kubernetes.io/zone
```

 value. The following example is for a Bash shell.

```
kubectl describe nodes | grep -e "Name:" -e "topology.kubernetes.io/zone"
```

The following example output shows the three nodes distributed across the specified region and availability zones, such as *eastus2-1* for the first availability zone and *eastus2-2* for the second availability zone:

```
Name: aks-nodepool1-28993262-vmss00000
topology.kubernetes.io/zone=eastus2-1
Name: aks-nodepool1-28993262-vmss00001
topology.kubernetes.io/zone=eastus2-2
Name: aks-nodepool1-28993262-vmss00002
topology.kubernetes.io/zone=eastus2-3
```

As you add additional nodes to an agent pool, the Azure platform automatically distributes the underlying VMs across the specified availability zones.

Note that in newer Kubernetes versions (1.17.0 and later), AKS is using the newer label `topology.kubernetes.io/zone` in addition to the deprecated `failure-domain.beta.kubernetes.io/zone`. You can get the same result as above with by running the following script:

```
kubectl get nodes -o custom-
columns=NAME:'{.metadata.name}',REGION:'{.metadata.labels.topology\\.kubernetes\\.io/region}',ZONE:'{metadata.labels.topology\\.kubernetes\\.io/zone}'
```

Which will give you a more succinct output:

NAME	REGION	ZONE
aks-nodepool1-34917322-vmss000000	eastus	eastus-1
aks-nodepool1-34917322-vmss000001	eastus	eastus-2
aks-nodepool1-34917322-vmss000002	eastus	eastus-3

Verify pod distribution across zones

As documented in [Well-Known Labels, Annotations and Taints](#), Kubernetes uses the `topology.kubernetes.io/zone` label to automatically distribute pods in a replication controller or service across the different zones available. In order to test this, you can scale up your cluster from 3 to 5 nodes, to verify correct pod spreading:

```
az aks scale \
--resource-group myResourceGroup \
--name myAKSCluster \
--node-count 5
```

When the scale operation completes after a few minutes, the command

```
kubectl describe nodes | grep -e "Name:" -e "topology.kubernetes.io/zone"
```

 in a Bash shell should give an output similar to this sample:

```
Name: aks-nodepool1-28993262-vmss00000  
topology.kubernetes.io/zone=eastus2-1  
Name: aks-nodepool1-28993262-vmss00001  
topology.kubernetes.io/zone=eastus2-2  
Name: aks-nodepool1-28993262-vmss00002  
topology.kubernetes.io/zone=eastus2-3  
Name: aks-nodepool1-28993262-vmss00003  
topology.kubernetes.io/zone=eastus2-1  
Name: aks-nodepool1-28993262-vmss00004  
topology.kubernetes.io/zone=eastus2-2
```

We now have two additional nodes in zones 1 and 2. You can deploy an application consisting of three replicas. We will use NGINX as an example:

```
kubectl create deployment nginx --image=mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine  
kubectl scale deployment nginx --replicas=3
```

By viewing nodes where your pods are running, you see pods are running on the nodes corresponding to three different availability zones. For example, with the command

```
kubectl describe pod | grep -e "^\w+Name:" -e "^\w+Node:"
```

 in a Bash shell you would get an output similar to this:

```
Name: nginx-6db489d4b7-ktdwg  
Node: aks-nodepool1-28993262-vmss00000/10.240.0.4  
Name: nginx-6db489d4b7-v7zvj  
Node: aks-nodepool1-28993262-vmss00002/10.240.0.6  
Name: nginx-6db489d4b7-xz6wj  
Node: aks-nodepool1-28993262-vmss00004/10.240.0.8
```

As you can see from the previous output, the first pod is running on node 0, which is located in the availability zone `eastus2-1`. The second pod is running on node 2, which corresponds to `eastus2-3`, and the third one in node 4, in `eastus2-2`. Without any additional configuration, Kubernetes is spreading the pods correctly across all three availability zones.

Next steps

This article detailed how to create an AKS cluster that uses availability zones. For more considerations on highly available clusters, see [Best practices for business continuity and disaster recovery in AKS](#).

Azure Kubernetes Service (AKS) node pool snapshot

10/27/2022 • 3 minutes to read • [Edit Online](#)

AKS releases a new node image weekly and every new cluster, new node pool, or upgrade cluster will always receive the latest image that can make it hard to maintain your environments consistent and to have repeatable environments.

Node pool snapshots allow you to take a configuration snapshot of your node pool and then create new node pools or new clusters based of that snapshot for as long as that configuration and kubernetes version is supported. For more information on the supportability windows, see [Supported Kubernetes versions in AKS](#).

The snapshot is an Azure resource that will contain the configuration information from the source node pool such as the node image version, kubernetes version, OS type, and OS SKU. You can then reference this snapshot resource and the respective values of its configuration to create any new node pool or cluster based off of it.

Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart using the [Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

Limitations

- Any node pool or cluster created from a snapshot must use a VM from the same virtual machine family as the snapshot, for example, you can't create a new N-Series node pool based of a snapshot captured from a D-Series node pool because the node images in those cases are structurally different.
- Snapshots must be created and used in the same region as the source node pool.

Take a node pool snapshot

In order to take a snapshot from a node pool first you'll need the node pool resource ID, which you can get from the command below:

```
NODEPOOL_ID=$(az aks nodepool show --name nodepool1 --cluster-name myAKSCluster --resource-group myResourceGroup --query id -o tsv)
```

IMPORTANT

Your AKS node pool must be created or upgraded after Nov 10th, 2021 in order for a snapshot to be taken from it. If you are using the `aks-preview` Azure CLI extension version `0.5.59` or newer, the commands for node pool snapshot have changed. For updated commands, see the [Node Pool Snapshot CLI reference](#).

Now, to take a snapshot from the previous node pool you'll use the `az aks snapshot` CLI command.

```
az aks nodepool snapshot create --name MySnapshot --resource-group MyResourceGroup --nodepool-id $NODEPOOL_ID --location eastus
```

Create a node pool from a snapshot

First you'll need the resource ID from the snapshot that was previously created, which you can get from the command below:

```
SNAPSHOT_ID=$(az aks nodepool snapshot show --name MySnapshot --resource-group myResourceGroup --query id -o tsv)
```

Now, we can use the command below to add a new node pool based off of this snapshot.

```
az aks nodepool add --name np2 --cluster-name myAKScluster --resource-group myResourceGroup --snapshot-id $SNAPSHOT_ID
```

Upgrading a node pool to a snapshot

You can upgrade a node pool to a snapshot configuration so long as the snapshot kubernetes version and node image version are more recent than the versions in the current node pool.

First you'll need the resource ID from the snapshot that was previously created, which you can get from the command below:

```
SNAPSHOT_ID=$(az aks nodepool snapshot show --name MySnapshot --resource-group myResourceGroup --query id -o tsv)
```

Now, we can use this command to upgrade this node pool to this snapshot configuration.

```
az aks nodepool upgrade --name nodepool1 --cluster-name myAKScluster --resource-group myResourceGroup --snapshot-id $SNAPSHOT_ID
```

NOTE

Your node pool image version will be the same contained in the snapshot and will remain the same throughout every scale operation. However, if this node pool is upgraded or a node image upgrade is performed without providing a snapshot-id the node image will be upgraded to latest.

Create a cluster from a snapshot

When you create a cluster from a snapshot, the cluster original system pool will be created from the snapshot configuration.

First you'll need the resource ID from the snapshot that was previously created, which you can get from the command below:

```
SNAPSHOT_ID=$(az aks nodepool snapshot show --name MySnapshot --resource-group myResourceGroup --query id -o tsv)
```

Now, we can use this command to create this cluster off of the snapshot configuration.

```
az aks create --name myAKScluster2 --resource-group myResourceGroup --snapshot-id $SNAPSHOT_ID
```

Next steps

- See the [AKS release notes](#) for information about the latest node images.
- Learn how to upgrade the Kubernetes version with [Upgrade an AKS cluster](#).
- Learn how to upgrade your node image version with [Node Image Upgrade](#)
- Learn more about multiple node pools and how to upgrade node pools with [Create and manage multiple node pools](#).

Add Azure Dedicated Host to an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 4 minutes to read • [Edit Online](#)

Azure Dedicated Host is a service that provides physical servers - able to host one or more virtual machines - dedicated to one Azure subscription. Dedicated hosts are the same physical servers used in our data centers, provided as a resource. You can provision dedicated hosts within a region, availability zone, and fault domain. Then, you can place VMs directly into your provisioned hosts, in whatever configuration best meets your needs.

Using Azure Dedicated Hosts for nodes with your AKS cluster has the following benefits:

- Hardware isolation at the physical server level. No other VMs will be placed on your hosts. Dedicated hosts are deployed in the same data centers and share the same network and underlying storage infrastructure as other, non-isolated hosts.
- Control over maintenance events initiated by the Azure platform. While most maintenance events have little to no impact on your virtual machines, there are some sensitive workloads where each second of pause can have an impact. With dedicated hosts, you can opt in to a maintenance window to reduce the impact to your service.

Before you begin

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- Before you start, ensure that your version of the Azure CLI is 2.39.0 or later. If it's an earlier version, [install the latest version](#).

Limitations

The following limitations apply when you integrate Azure Dedicated Host with Azure Kubernetes Service:

- An existing agent pool can't be converted from non-ADH to ADH or ADH to non-ADH.
- It isn't supported to update agent pool from host group A to host group B.
- Using ADH across subscriptions.

Add a Dedicated Host Group to an AKS cluster

A host group is a resource that represents a collection of dedicated hosts. You create a host group in a region and an availability zone, and add hosts to it. When planning for high availability, there are more options. You can use one or both of the following options with your dedicated hosts:

- Span across multiple availability zones. In this case, you're required to have a host group in each of the zones you wish to use.
- Span across multiple fault domains, which are mapped to physical racks.

In either case, you need to provide the fault domain count for your host group. If you don't want to span fault domains in your group, use a fault domain count of 1.

You can also decide to use both availability zones and fault domains.

Not all host SKUs are available in all regions, and availability zones. You can list host availability, and any offer restrictions before you start provisioning dedicated hosts.

```
az vm list-skus -l eastus -r hostGroups/hosts -o table
```

NOTE

First, when using host group, the nodepool fault domain count is always the same as the host group fault domain count. In order to use cluster auto-scaling to work with ADH and AKS, please make sure your host group fault domain count and capacity is enough. Secondly, only change fault domain count from the default of 1 to any other number if you know what they are doing as a misconfiguration could lead to a unscalable configuration.

Create a Host Group

Now create a dedicated host in the host group. In addition to a name for the host, you're required to provide the SKU for the host. Host SKU captures the supported VM series and the hardware generation for your dedicated host.

For more information about the host SKUs and pricing, see [Azure Dedicated Host pricing](#).

Use `az vm host create` to create a host. If you set a fault domain count for your host group, you'll be asked to specify the fault domain for your host.

In this example, we'll use `az vm host group create` to create a host group using both availability zones and fault domains.

```
az vm host group create \
--name myHostGroup \
-g myDHResourceGroup \
-z 1 \
--platform-fault-domain-count 1 \
--automatic-placement true
```

Create a Dedicated Host

Now create a dedicated host in the host group. In addition to a name for the host, you're required to provide the SKU for the host. Host SKU captures the supported VM series and the hardware generation for your dedicated host.

If you set a fault domain count for your host group, you'll need to specify the fault domain for your host.

```
az vm host create \
--host-group myHostGroup \
--name myHost \
--sku DSv3-Type1 \
--platform-fault-domain 1 \
-g myDHResourceGroup
```

Use a user-assigned Identity

IMPORTANT

A user-assigned Identity with "contributor" role on the Resource Group of the Host Group is required.

First, create a Managed Identity

```
az identity create -g <Resource Group> -n <Managed Identity name>
```

Assign Managed Identity

```
az role assignment create --assignee <id> --role "Contributor" --scope <Resource id>
```

Create an AKS cluster using the Host Group

Create an AKS cluster, and add the Host Group you just configured.

```
az aks create -g MyResourceGroup -n MyManagedCluster --location eastus --nodepool-name agentpool1 --node-count 1 --host-group-id <id> --node-vm-size Standard_D2s_v3 --enable-managed-identity --assign-identity <id>
```

Add a Dedicated Host Node Pool to an existing AKS cluster

Add a Host Group to an already existing AKS cluster.

```
az aks nodepool add --cluster-name MyManagedCluster --name agentpool3 --resource-group MyResourceGroup --node-count 1 --host-group-id <id> --node-vm-size Standard_D2s_v3
```

Remove a Dedicated Host Node Pool from an AKS cluster

```
az aks nodepool delete --cluster-name MyManagedCluster --name agentpool3 --resource-group MyResourceGroup
```

Next steps

In this article, you learned how to create an AKS cluster with a Dedicated host, and to add a dedicated host to an existing cluster. For more information about Dedicated Hosts, see [dedicated-hosts](#).

Create and manage multiple node pools for a cluster in Azure Kubernetes Service (AKS)

10/27/2022 • 24 minutes to read • [Edit Online](#)

In Azure Kubernetes Service (AKS), nodes of the same configuration are grouped together into *node pools*. These node pools contain the underlying VMs that run your applications. The initial number of nodes and their size (SKU) is defined when you create an AKS cluster, which creates a [system node pool](#). To support applications that have different compute or storage demands, you can create additional [user node pools](#). System node pools serve the primary purpose of hosting critical system pods such as CoreDNS and tunnelfront. User node pools serve the primary purpose of hosting your application pods. However, application pods can be scheduled on system node pools if you wish to only have one pool in your AKS cluster. User node pools are where you place your application-specific pods. For example, use these additional user node pools to provide GPUs for compute-intensive applications, or access to high-performance SSD storage.

NOTE

This feature enables higher control over how to create and manage multiple node pools. As a result, separate commands are required for create/update/delete. Previously cluster operations through `az aks create` or `az aks update` used the managedCluster API and were the only options to change your control plane and a single node pool. This feature exposes a separate operation set for agent pools through the agentPool API and require use of the `az aks nodepool` command set to execute operations on an individual node pool.

This article shows you how to create and manage multiple node pools in an AKS cluster.

Before you begin

You need the Azure CLI version 2.2.0 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Limitations

The following limitations apply when you create and manage AKS clusters that support multiple node pools:

- See [Quotas, virtual machine size restrictions, and region availability in Azure Kubernetes Service \(AKS\)](#).
- You can delete system node pools, provided you have another system node pool to take its place in the AKS cluster.
- System pools must contain at least one node, and user node pools may contain zero or more nodes.
- The AKS cluster must use the Standard SKU load balancer to use multiple node pools, the feature isn't supported with Basic SKU load balancers.
- The AKS cluster must use virtual machine scale sets for the nodes.
- You can't change the VM size of a node pool after you create it.
- The name of a node pool may only contain lowercase alphanumeric characters and must begin with a lowercase letter. For Linux node pools the length must be between 1 and 12 characters, for Windows node pools the length must be between 1 and 6 characters.
- All node pools must reside in the same virtual network.
- When creating multiple node pools at cluster create time, all Kubernetes versions used by node pools must match the version set for the control plane. This can be updated after the cluster has been provisioned by using per node pool operations.

Create an AKS cluster

IMPORTANT

If you run a single system node pool for your AKS cluster in a production environment, we recommend you use at least three nodes for the node pool.

To get started, create an AKS cluster with a single node pool. The following example uses the [az group create](#) command to create a resource group named *myResourceGroup* in the *eastus* region. An AKS cluster named *myAKSCluster* is then created using the [az aks create](#) command.

NOTE

The *Basic* load balancer SKU is **not supported** when using multiple node pools. By default, AKS clusters are created with the *Standard* load balancer SKU from the Azure CLI and Azure portal.

```
# Create a resource group in East US
az group create --name myResourceGroup --location eastus

# Create a basic single-node AKS cluster
az aks create \
  --resource-group myResourceGroup \
  --name myAKSCluster \
  --vm-set-type VirtualMachineScaleSets \
  --node-count 2 \
  --generate-ssh-keys \
  --load-balancer-sku standard
```

It takes a few minutes to create the cluster.

NOTE

To ensure your cluster operates reliably, you should run at least 2 (two) nodes in the default node pool, as essential system services are running across this node pool.

When the cluster is ready, use the [az aks get-credentials](#) command to get the cluster credentials for use with `kubectl`:

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

Add a node pool

The cluster created in the previous step has a single node pool. Let's add a second node pool using the [az aks nodepool add](#) command. The following example creates a node pool named *mynodepool* that runs 3 nodes:

```
az aks nodepool add \
  --resource-group myResourceGroup \
  --cluster-name myAKSCluster \
  --name mynodepool \
  --node-count 3
```

NOTE

The name of a node pool must start with a lowercase letter and can only contain alphanumeric characters. For Linux node pools the length must be between 1 and 12 characters, for Windows node pools the length must be between 1 and 6 characters.

To see the status of your node pools, use the [az aks node pool list](#) command and specify your resource group and cluster name:

```
az aks nodepool list --resource-group myResourceGroup --cluster-name myAKSCluster
```

The following example output shows that *mynodepool* has been successfully created with three nodes in the node pool. When the AKS cluster was created in the previous step, a default *nodepool1* was created with a node count of 2.

```
[  
 {  
   ...  
   "count": 3,  
   ...  
   "name": "mynodepool",  
   "orchestratorVersion": "1.15.7",  
   ...  
   "vmSize": "Standard_DS2_v2",  
   ...  
 },  
 {  
   ...  
   "count": 2,  
   ...  
   "name": "nodepool1",  
   "orchestratorVersion": "1.15.7",  
   ...  
   "vmSize": "Standard_DS2_v2",  
   ...  
 }  
 ]
```

TIP

If no *VmSize* is specified when you add a node pool, the default size is *Standard_D2s_v3* for Windows node pools and *Standard_DS2_v2* for Linux node pools. If no *OrchestratorVersion* is specified, it defaults to the same version as the control plane.

Add an ARM64 node pool

The ARM64 processor provides low power compute for your Kubernetes workloads. To create an ARM64 node pool, you will need to choose a [Dpsv5](#), [Dplsv5](#) or [Epsv5](#) series Virtual Machine.

Use `az aks nodepool add` command to add an ARM64 node pool.

```
az aks nodepool add \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name armpool \  
  --node-count 3 \  
  --node-vm-size Standard_Dpds_v5
```

Add a Mariner node pool

Mariner is an open-source Linux distribution available as an AKS container host. It provides high reliability, security, and consistency. Mariner only includes the minimal set of packages needed for running container workloads, which improves boot times and overall performance.

You can add a Mariner node pool into your existing cluster using the `az aks nodepool add` command and specifying `--os-sku mariner`.

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--os-sku mariner
```

Migrate Ubuntu nodes to Mariner

Use the following instructions to migrate your Ubuntu nodes to Mariner nodes.

1. Add a Mariner node pool into your existing cluster using the `az aks nodepool add` command and specifying `--os-sku mariner`.

NOTE

When adding a new Mariner node pool, you need to add at least one as `--mode System`. Otherwise, AKS won't allow you to delete your existing Ubuntu node pool.

2. [Cordon the existing Ubuntu nodes](#).
3. [Drain the existing Ubuntu nodes](#).
4. Remove the existing Ubuntu nodes using the `az aks delete` command.

```
az aks nodepool delete \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name myNodePool
```

Add a node pool with a unique subnet

A workload may require splitting a cluster's nodes into separate pools for logical isolation. This isolation can be supported with separate subnets dedicated to each node pool in the cluster. This can address requirements such as having non-contiguous virtual network address space to split across node pools.

NOTE

Make sure to use Azure CLI version `2.35.0` or later.

Limitations

- All subnets assigned to node pools must belong to the same virtual network.
- System pods must have access to all nodes/pods in the cluster to provide critical functionality such as DNS resolution and tunneling kubectl logs/exec/port-forward proxy.
- If you expand your VNET after creating the cluster you must update your cluster (perform any managed cluster operation but node pool operations don't count) before adding a subnet outside the original cidr. AKS will error-out on the agent pool add now though we originally allowed it. The `aks-preview` Azure CLI extension (version 0.5.66+) now supports running `az aks update -g <resourceGroup> -n <clusterName>` without any optional arguments. This command will perform an update operation without making any changes, which can recover a cluster stuck in a failed state.

- In clusters with Kubernetes version < 1.23.3, kube-proxy will SNAT traffic from new subnets, which can cause Azure Network Policy to drop the packets.
- Windows nodes will SNAT traffic to the new subnets until the node pool is reimaged.
- Internal load balancers default to one of the node pool subnets (usually the first subnet of the node pool at cluster creation). To override this behavior, you can [specify the load balancer's subnet explicitly using an annotation](#).

To create a node pool with a dedicated subnet, pass the subnet resource ID as an additional parameter when creating a node pool.

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name mynodepool \
--node-count 3 \
--vnet-subnet-id <YOUR_SUBNET_RESOURCE_ID>
```

Upgrade a node pool

NOTE

Upgrade and scale operations on a cluster or node pool cannot occur simultaneously, if attempted an error is returned. Instead, each operation type must complete on the target resource prior to the next request on that same resource. Read more about this on our [troubleshooting guide](#).

The commands in this section explain how to upgrade a single specific node pool. The relationship between upgrading the Kubernetes version of the control plane and the node pool are explained in the [section below](#).

NOTE

The node pool OS image version is tied to the Kubernetes version of the cluster. You will only get OS image upgrades, following a cluster upgrade.

Since there are two node pools in this example, we must use [az aks nodepool upgrade](#) to upgrade a node pool. To see the available upgrades use [az aks get-upgrades](#)

```
az aks get-upgrades --resource-group myResourceGroup --name myAKSCluster
```

Let's upgrade the *mynodepool*. Use the [az aks nodepool upgrade](#) command to upgrade the node pool, as shown in the following example:

```
az aks nodepool upgrade \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name mynodepool \
--kubernetes-version KUBERNETES_VERSION \
--no-wait
```

List the status of your node pools again using the [az aks node pool list](#) command. The following example shows that *mynodepool* is in the *Upgrading* state to *KUBERNETES_VERSION*:

```
az aks nodepool list -g myResourceGroup --cluster-name myAKSCluster
```

```
[  
 {  
 ...  
 "count": 3,  
 ...  
 "name": "mynodepool",  
 "orchestratorVersion": "KUBERNETES_VERSION",  
 ...  
 "provisioningState": "Upgrading",  
 ...  
 "vmSize": "Standard_DS2_v2",  
 ...  
 },  
 {  
 ...  
 "count": 2,  
 ...  
 "name": "nodepool1",  
 "orchestratorVersion": "1.15.7",  
 ...  
 "provisioningState": "Succeeded",  
 ...  
 "vmSize": "Standard_DS2_v2",  
 ...  
 }  
]
```

It takes a few minutes to upgrade the nodes to the specified version.

As a best practice, you should upgrade all node pools in an AKS cluster to the same Kubernetes version. The default behavior of `az aks upgrade` is to upgrade all node pools together with the control plane to achieve this alignment. The ability to upgrade individual node pools lets you perform a rolling upgrade and schedule pods between node pools to maintain application uptime within the above constraints mentioned.

Upgrade a cluster control plane with multiple node pools

NOTE

Kubernetes uses the standard [Semantic Versioning](#) versioning scheme. The version number is expressed as $x.y.z$ where x is the major version, y is the minor version, and z is the patch version. For example, in version `1.12.6`, 1 is the major version, 12 is the minor version, and 6 is the patch version. The Kubernetes version of the control plane and the initial node pool are set during cluster creation. All additional node pools have their Kubernetes version set when they are added to the cluster. The Kubernetes versions may differ between node pools as well as between a node pool and the control plane.

An AKS cluster has two cluster resource objects with Kubernetes versions associated.

1. A cluster control plane Kubernetes version.
2. A node pool with a Kubernetes version.

A control plane maps to one or many node pools. The behavior of an upgrade operation depends on which Azure CLI command is used.

Upgrading an AKS control plane requires using `az aks upgrade`. This command upgrades the control plane version and all node pools in the cluster.

Issuing the `az aks upgrade` command with the `--control-plane-only` flag upgrades only the cluster control

plane. None of the associated node pools in the cluster are changed.

Upgrading individual node pools requires using `az aks nodepool upgrade`. This command upgrades only the target node pool with the specified Kubernetes version

Validation rules for upgrades

The valid Kubernetes upgrades for a cluster's control plane and node pools are validated by the following sets of rules.

- Rules for valid versions to upgrade node pools:
 - The node pool version must have the same *major* version as the control plane.
 - The node pool *minor* version must be within two *minor* versions of the control plane version.
 - The node pool version can't be greater than the control `major.minor.patch` version.
- Rules for submitting an upgrade operation:
 - You can't downgrade the control plane or a node pool Kubernetes version.
 - If a node pool Kubernetes version isn't specified, behavior depends on the client being used.
Declaration in Resource Manager templates falls back to the existing version defined for the node pool if used, if none is set the control plane version is used to fall back on.
 - You can either upgrade or scale a control plane or a node pool at a given time, you can't submit multiple operations on a single control plane or node pool resource simultaneously.

Scale a node pool manually

As your application workload demands change, you may need to scale the number of nodes in a node pool. The number of nodes can be scaled up or down.

To scale the number of nodes in a node pool, use the `az aks node pool scale` command. The following example scales the number of nodes in *mynodepool* to 5:

```
az aks nodepool scale \
    --resource-group myResourceGroup \
    --cluster-name myAKSCluster \
    --name mynodepool \
    --node-count 5 \
    --no-wait
```

List the status of your node pools again using the `az aks node pool list` command. The following example shows that *mynodepool* is in the *Scaling* state with a new count of 5 nodes:

```
az aks nodepool list -g myResourceGroup --cluster-name myAKSCluster
```

```
[  
  {  
    ...  
    "count": 5,  
    ...  
    "name": "mynodepool",  
    "orchestratorVersion": "1.15.7",  
    ...  
    "provisioningState": "Scaling",  
    ...  
    "vmSize": "Standard_DS2_v2",  
    ...  
  },  
  {  
    ...  
    "count": 2,  
    ...  
    "name": "nodepool1",  
    "orchestratorVersion": "1.15.7",  
    ...  
    "provisioningState": "Succeeded",  
    ...  
    "vmSize": "Standard_DS2_v2",  
    ...  
  }  
]
```

It takes a few minutes for the scale operation to complete.

Scale a specific node pool automatically by enabling the cluster autoscaler

AKS offers a separate feature to automatically scale node pools with a feature called the [cluster autoscaler](#). This feature can be enabled per node pool with unique minimum and maximum scale counts per node pool. Learn how to [use the cluster autoscaler per node pool](#).

Delete a node pool

If you no longer need a pool, you can delete it and remove the underlying VM nodes. To delete a node pool, use the [az aks node pool delete](#) command and specify the node pool name. The following example deletes the *mynodepool* created in the previous steps:

Caution

When you delete a node pool, AKS doesn't perform cordon and drain, and there are no recovery options for data loss that may occur when you delete a node pool. If pods can't be scheduled on other node pools, those applications become unavailable. Make sure you don't delete a node pool when in-use applications don't have data backups or the ability to run on other node pools in your cluster. To minimize the disruption of rescheduling pods currently running on the node pool you are going to delete, perform a cordon and drain on all nodes in the node pool before deleting. For more information, see [cordon and drain node pools](#).

```
az aks nodepool delete -g myResourceGroup --cluster-name myAKSCluster --name mynodepool --no-wait
```

The following example output from the [az aks node pool list](#) command shows that *mynodepool* is in the *Deleting* state:

```
az aks nodepool list -g myResourceGroup --cluster-name myAKSCluster
```

```
[  
 {  
 ...  
 "count": 5,  
 ...  
 "name": "mynodepool",  
 "orchestratorVersion": "1.15.7",  
 ...  
 "provisioningState": "Deleting",  
 ...  
 "vmSize": "Standard_DS2_v2",  
 ...  
 },  
 {  
 ...  
 "count": 2,  
 ...  
 "name": "nodepool1",  
 "orchestratorVersion": "1.15.7",  
 ...  
 "provisioningState": "Succeeded",  
 ...  
 "vmSize": "Standard_DS2_v2",  
 ...  
 }  
 ]
```

It takes a few minutes to delete the nodes and the node pool.

Associate capacity reservation groups to node pools (preview)

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

As your application workloads demands, you may associate node pools to capacity reservation groups created prior. This ensures guaranteed capacity is allocated for your node pools.

For more information on the capacity reservation groups, please refer to [Capacity Reservation Groups](#).

Associating a node pool with an existing capacity reservation group can be done using `az aks nodepool add` command and specifying a capacity reservation group with the `--capacityReservationGroup` flag. The capacity reservation group should already exist, otherwise the node pool will be added to the cluster with a warning and no capacity reservation group gets associated.

```
az aks nodepool add -g MyRG --cluster-name MyMC -n myAP --capacityReservationGroup myCRG
```

Associating a system node pool with an existing capacity reservation group can be done using `az aks create` command. If the capacity reservation group specified doesn't exist, then a warning is issued and the cluster gets created without any capacity reservation group association.

```
az aks create -g MyRG --cluster-name MyMC --capacityReservationGroup myCRG
```

Deleting a node pool command will implicitly dissociate a node pool from any associated capacity reservation group, before that node pool is deleted.

```
az aks nodepool delete -g MyRG --cluster-name MyMC -n myAP
```

Deleting a cluster command implicitly dissociates all node pools in a cluster from their associated capacity reservation groups.

```
az aks delete -g MyRG --cluster-name MyMC
```

Specify a VM size for a node pool

In the previous examples to create a node pool, a default VM size was used for the nodes created in the cluster. A more common scenario is for you to create node pools with different VM sizes and capabilities. For example, you may create a node pool that contains nodes with large amounts of CPU or memory, or a node pool that provides GPU support. In the next step, you [use taints and tolerations](#) to tell the Kubernetes scheduler how to limit access to pods that can run on these nodes.

In the following example, create a GPU-based node pool that uses the *Standard_NC6* VM size. These VMs are powered by the NVIDIA Tesla K80 card. For information on available VM sizes, see [Sizes for Linux virtual machines in Azure](#).

Create a node pool using the [az aks node pool add](#) command again. This time, specify the name *gpunodepool*, and use the `--node-vm-size` parameter to specify the *Standard_NC6* size:

```
az aks nodepool add \
  --resource-group myResourceGroup \
  --cluster-name myAKSCluster \
  --name gpunodepool \
  --node-count 1 \
  --node-vm-size Standard_NC6 \
  --no-wait
```

The following example output from the [az aks node pool list](#) command shows that *gpunodepool* is *Creating* nodes with the specified *VmSize*.

```
az aks nodepool list -g myResourceGroup --cluster-name myAKSCluster
```

```
[  
 {  
 ...  
 "count": 1,  
 ...  
 "name": "gpunodepool",  
 "orchestratorVersion": "1.15.7",  
 ...  
 "provisioningState": "Creating",  
 ...  
 "vmSize": "Standard_NC6",  
 ...  
 },  
 {  
 ...  
 "count": 2,  
 ...  
 "name": "nodepool1",  
 "orchestratorVersion": "1.15.7",  
 ...  
 "provisioningState": "Succeeded",  
 ...  
 "vmSize": "Standard_DS2_v2",  
 ...  
 }  
 ]
```

It takes a few minutes for the *gpunodepool* to be successfully created.

Specify a taint, label, or tag for a node pool

When creating a node pool, you can add taints, labels, or tags to that node pool. When you add a taint, label, or tag, all nodes within that node pool also get that taint, label, or tag.

IMPORTANT

Adding taints, labels, or tags to nodes should be done for the entire node pool using `az aks nodepool`. Applying taints, labels, or tags to individual nodes in a node pool using `kubectl` is not recommended.

Setting nodepool taints

To create a node pool with a taint, use `az aks nodepool add`. Specify the name *taintnp* and use the `--node-taints` parameter to specify *sku=gpu:NoSchedule* for the taint.

```
az aks nodepool add \  
 --resource-group myResourceGroup \  
 --cluster-name myAKSCluster \  
 --name taintnp \  
 --node-count 1 \  
 --node-taints sku=gpu:NoSchedule \  
 --no-wait
```

The following example output from the `az aks nodepool list` command shows that *taintnp* is *Creating* nodes with the specified *nodeTaints*:

```
az aks nodepool list -g myResourceGroup --cluster-name myAKSCluster
```

```
[  
 {  
 ...  
 "count": 1,  
 ...  
 "name": "taintnp",  
 "orchestratorVersion": "1.15.7",  
 ...  
 "provisioningState": "Creating",  
 ...  
 "nodeTaints": [  
     "sku=gpu:NoSchedule"  
 ],  
 ...  
 },  
 ...  
 ]
```

The taint information is visible in Kubernetes for handling scheduling rules for nodes. The Kubernetes scheduler can use taints and tolerations to restrict what workloads can run on nodes.

- A **taint** is applied to a node that indicates only specific pods can be scheduled on them.
- A **toleration** is then applied to a pod that allows them to *tolerate* a node's taint.

For more information on how to use advanced Kubernetes scheduled features, see [Best practices for advanced scheduler features in AKS](#)

In the previous step, you applied the *sku=gpu:NoSchedule* taint when you created your node pool. The following basic example YAML manifest uses a toleration to allow the Kubernetes scheduler to run an NGINX pod on a node in that node pool.

Create a file named `nginx-toleration.yaml` and copy in the following example YAML:

```
apiVersion: v1  
kind: Pod  
metadata:  
  name: mypod  
spec:  
  containers:  
    - image: mcr.microsoft.com/oss/nginx/nginx:1.15.9-alpine  
      name: mypod  
      resources:  
        requests:  
          cpu: 100m  
          memory: 128Mi  
        limits:  
          cpu: 1  
          memory: 2G  
  tolerations:  
    - key: "sku"  
      operator: "Equal"  
      value: "gpu"  
      effect: "NoSchedule"
```

Schedule the pod using the `kubectl apply -f nginx-toleration.yaml` command:

```
kubectl apply -f nginx-toleration.yaml
```

It takes a few seconds to schedule the pod and pull the NGINX image. Use the `kubectl describe pod` command to view the pod status. The following condensed example output shows the *sku=gpu:NoSchedule* toleration is

applied. In the events section, the scheduler has assigned the pod to the `aks-taintnp-28993262-vmss000000` node:

```
kubectl describe pod mypod
```

```
[...]
Tolerations:    node.kubernetes.io/not-ready:NoExecute for 300s
                  node.kubernetes.io/unreachable:NoExecute for 300s
                  sku=gpu:NoSchedule
Events:
  Type      Reason     Age   From           Message
  ----      ----     --   --   -----
  Normal    Scheduled  4m48s  default-scheduler  Successfully assigned default/mypod to aks-taintnp-28993262-
  Normal    Pulling    4m47s  kubelet        pulling image "mcr.microsoft.com/oss/nginx/nginx:1.15.9-
  Normal    Pulled    4m43s  kubelet        Successfully pulled image
  "mcr.microsoft.com/oss/nginx/nginx:1.15.9-alpine"
  Normal    Created    4m40s  kubelet        Created container
  Normal    Started   4m40s  kubelet        Started container
```

Only pods that have this toleration applied can be scheduled on nodes in `taintnp`. Any other pod would be scheduled in the `nodepool1` node pool. If you create additional node pools, you can use additional taints and tolerations to limit what pods can be scheduled on those node resources.

Setting nodepool labels

For more information on using labels with node pools, see [Use labels in an Azure Kubernetes Service \(AKS\) cluster](#).

Setting nodepool Azure tags

For more information on using Azure tags with node pools, see [Use Azure tags in Azure Kubernetes Service \(AKS\)](#).

Add a FIPS-enabled node pool

For more information on enabling Federal Information Process Standard (FIPS) for your AKS cluster, see [Enable Federal Information Process Standard \(FIPS\) for Azure Kubernetes Service \(AKS\) node pools](#).

Manage node pools using a Resource Manager template

When you use an Azure Resource Manager template to create and managed resources, you can typically update the settings in your template and redeploy to update the resource. With node pools in AKS, the initial node pool profile can't be updated once the AKS cluster has been created. This behavior means that you can't update an existing Resource Manager template, make a change to the node pools, and redeploy. Instead, you must create a separate Resource Manager template that updates only the node pools for an existing AKS cluster.

Create a template such as `aks-agentpools.json` and paste the following example manifest. This example template configures the following settings:

- Updates the `Linux` node pool named `myagentpool` to run three nodes.
- Sets the nodes in the node pool to run Kubernetes version `1.15.7`.
- Defines the node size as `Standard_DS2_v2`.

Edit these values as need to update, add, or delete node pools as needed:

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "clusterName": {
            "type": "string",
            "metadata": {
                "description": "The name of your existing AKS cluster."
            }
        },
        "location": {
            "type": "string",
            "metadata": {
                "description": "The location of your existing AKS cluster."
            }
        },
        "agentPoolName": {
            "type": "string",
            "defaultValue": "myagentpool",
            "metadata": {
                "description": "The name of the agent pool to create or update."
            }
        },
        "vnetSubnetId": {
            "type": "string",
            "defaultValue": "",
            "metadata": {
                "description": "The Vnet subnet resource ID for your existing AKS cluster."
            }
        }
    },
    "variables": {
        "apiVersion": {
            "aks": "2020-01-01"
        },
        "agentPoolProfiles": {
            "maxPods": 30,
            "osDiskSizeGB": 0,
            "agentCount": 3,
            "agentVmSize": "Standard_DS2_v2",
            "osType": "Linux",
            "vnetSubnetId": "[parameters('vnetSubnetId')]"
        }
    },
    "resources": [
        {
            "apiVersion": "2020-01-01",
            "type": "Microsoft.ContainerService/managedClusters/agentPools",
            "name": "[concat(parameters('clusterName'), '/', parameters('agentPoolName'))]",
            "location": "[parameters('location')]",
            "properties": {
                "maxPods": "[variables('agentPoolProfiles').maxPods]",
                "osDiskSizeGB": "[variables('agentPoolProfiles').osDiskSizeGB]",
                "count": "[variables('agentPoolProfiles').agentCount]",
                "vmSize": "[variables('agentPoolProfiles').agentVmSize]",
                "osType": "[variables('agentPoolProfiles').osType]",
                "storageProfile": "ManagedDisks",
                "type": "VirtualMachineScaleSets",
                "vnetSubnetID": "[variables('agentPoolProfiles').vnetSubnetId]",
                "orchestratorVersion": "1.15.7"
            }
        }
    ]
}
```

Deploy this template using the [az deployment group create](#) command, as shown in the following example.

You're prompted for the existing AKS cluster name and location:

```
az deployment group create \
--resource-group myResourceGroup \
--template-file aks-agentpools.json
```

TIP

You can add a tag to your node pool by adding the *tag* property in the template, as shown in the following example.

```
...
"resources": [
{
  ...
  "properties": {
    ...
    "tags": {
      "name1": "val1"
    },
    ...
  }
}
...
}
```

It may take a few minutes to update your AKS cluster depending on the node pool settings and operations you define in your Resource Manager template.

Assign a public IP per node for your node pools

AKS nodes don't require their own public IP addresses for communication. However, scenarios may require nodes in a node pool to receive their own dedicated public IP addresses. A common scenario is for gaming workloads, where a console needs to make a direct connection to a cloud virtual machine to minimize hops. This scenario can be achieved on AKS by using Node Public IP.

First, create a new resource group.

```
az group create --name myResourceGroup2 --location eastus
```

Create a new AKS cluster and attach a public IP for your nodes. Each of the nodes in the node pool receives a unique public IP. You can verify this by looking at the Virtual Machine Scale Set instances.

```
az aks create -g MyResourceGroup2 -n MyManagedCluster -l eastus --enable-node-public-ip
```

For existing AKS clusters, you can also add a new node pool, and attach a public IP for your nodes.

```
az aks nodepool add -g MyResourceGroup2 --cluster-name MyManagedCluster -n nodepool2 --enable-node-public-ip
```

Use a public IP prefix

There are a number of [benefits to using a public IP prefix](#). AKS supports using addresses from an existing public IP prefix for your nodes by passing the resource ID with the flag `node-public-ip-prefix` when creating a new cluster or adding a node pool.

First, create a public IP prefix using [az network public-ip prefix create](#):

```
az network public-ip prefix create --length 28 --location eastus --name MyPublicIPPrefix --resource-group MyResourceGroup3
```

View the output, and take note of the `id` for the prefix:

```
{  
  ...  
  "id": "/subscriptions/<subscription-id>/resourceGroups/myResourceGroup3/providers/Microsoft.Network/publicIPPrefixes/MyPublicIPPrefix",  
  ...  
}
```

Finally, when creating a new cluster or adding a new node pool, use the flag `--node-public-ip-prefix` and pass in the prefix's resource ID:

```
az aks create -g MyResourceGroup3 -n MyManagedCluster -l eastus --enable-node-public-ip --node-public-ip-prefix /subscriptions/<subscription-id>/resourcegroups/MyResourceGroup3/providers/Microsoft.Network/publicIPPrefixes/MyPublicIPPrefix
```

Locate public IPs for nodes

You can locate the public IPs for your nodes in various ways:

- Use the Azure CLI command [az vmss list-instance-public-ips](#).
- Use [PowerShell or Bash commands](#).
- You can also view the public IPs in the Azure portal by viewing the instances in the Virtual Machine Scale Set.

IMPORTANT

The [node resource group](#) contains the nodes and their public IPs. Use the node resource group when executing commands to find the public IPs for your nodes.

```
az vmss list-instance-public-ips -g MC_MyResourceGroup2_MyManagedCluster_eastus -n YourVirtualMachineScaleSetName
```

Clean up resources

In this article, you created an AKS cluster that includes GPU-based nodes. To reduce unnecessary cost, you may want to delete the `gpunodepool`, or the whole AKS cluster.

To delete the GPU-based node pool, use the [az aks nodepool delete](#) command as shown in following example:

```
az aks nodepool delete -g myResourceGroup --cluster-name myAKScluster --name gpunodepool
```

To delete the cluster itself, use the [az group delete](#) command to delete the AKS resource group:

```
az group delete --name myResourceGroup --yes --no-wait
```

You can also delete the additional cluster you created for the public IP for node pools scenario.

```
az group delete --name myResourceGroup2 --yes --no-wait
```

Next steps

- Learn more about [system node pools](#).
- In this article, you learned how to create and manage multiple node pools in an AKS cluster. For more information about how to control pods across node pools, see [Best practices for advanced scheduler features in AKS](#).
- To create and use Windows Server container node pools, see [Create a Windows Server container in AKS](#).
- Use [proximity placement groups](#) to reduce latency for your AKS applications.

Add an Azure Spot node pool to an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 6 minutes to read • [Edit Online](#)

A Spot node pool is a node pool backed by an [Azure Spot Virtual machine scale set](#). Using Spot VMs for nodes with your AKS cluster allows you to take advantage of unutilized capacity in Azure at a significant cost savings. The amount of available unutilized capacity will vary based on many factors, including node size, region, and time of day.

When you deploy a Spot node pool, Azure will allocate the Spot nodes if there's capacity available. There's no SLA for the Spot nodes. A Spot scale set that backs the Spot node pool is deployed in a single fault domain and offers no high availability guarantees. At any time when Azure needs the capacity back, the Azure infrastructure will evict Spot nodes.

Spot nodes are great for workloads that can handle interruptions, early terminations, or evictions. For example, workloads such as batch processing jobs, development and testing environments, and large compute workloads may be good candidates to schedule on a Spot node pool.

In this article, you add a secondary Spot node pool to an existing Azure Kubernetes Service (AKS) cluster.

This article assumes a basic understanding of Kubernetes and Azure Load Balancer concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#).

If you don't have an Azure subscription, create a [free account](#) before you begin.

Before you begin

When you create a cluster to use a Spot node pool, that cluster must use Virtual Machine Scale Sets for node pools and the *Standard* SKU load balancer. You must also add another node pool after you create your cluster, which is covered in a later step.

This article requires that you're running the Azure CLI version 2.14 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Limitations

The following limitations apply when you create and manage AKS clusters with a Spot node pool:

- A Spot node pool can't be the cluster's default node pool. A Spot node pool can only be used for a secondary pool.
- The control plane and node pools can't be upgraded at the same time. You must upgrade them separately or remove the Spot node pool to upgrade the control plane and remaining node pools at the same time.
- A Spot node pool must use Virtual Machine Scale Sets.
- You can't change `ScaleSetPriority` or `SpotMaxPrice` after creation.
- When setting `SpotMaxPrice`, the value must be -1 or a positive value with up to five decimal places.
- A Spot node pool will have the label `kubernetes.azure.com/scalesetpriority:spot`, the taint `kubernetes.azure.com/scalesetpriority=spot:NoSchedule`, and system pods will have anti-affinity.
- You must add a [corresponding toleration](#) and affinity to schedule workloads on a Spot node pool.

Add a Spot node pool to an AKS cluster

You must add a Spot node pool to an existing cluster that has multiple node pools enabled. For more details on

creating an AKS cluster with multiple node pools, see [use multiple node pools](#).

Create a node pool using the `az aks nodepool add` command:

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name spotnodepool \
--priority Spot \
--eviction-policy Delete \
--spot-max-price -1 \
--enable-cluster-autoscaler \
--min-count 1 \
--max-count 3 \
--no-wait
```

By default, you create a node pool with a *priority* of *Regular* in your AKS cluster when you create a cluster with multiple node pools. The above command adds an auxiliary node pool to an existing AKS cluster with a *priority* of *Spot*. The *priority* of *Spot* makes the node pool a Spot node pool. The *eviction-policy* parameter is set to *Delete* in the above example, which is the default value. When you set the *eviction policy* to *Delete*, nodes in the underlying scale set of the node pool are deleted when they're evicted. You can also set the eviction policy to *Deallocate*. When you set the eviction policy to *Deallocate*, nodes in the underlying scale set are set to the stopped-deallocated state upon eviction. Nodes in the stopped-deallocated state count against your compute quota and can cause issues with cluster scaling or upgrading. The *priority* and *eviction-policy* values can only be set during node pool creation. Those values can't be updated later.

The command also enables the [cluster autoscaler](#), which is recommended to use with Spot node pools. Based on the workloads running in your cluster, the cluster autoscaler scales up and scales down the number of nodes in the node pool. For Spot node pools, the cluster autoscaler will scale up the number of nodes after an eviction if more nodes are still needed. If you change the maximum number of nodes a node pool can have, you also need to adjust the `maxCount` value associated with the cluster autoscaler. If you don't use a cluster autoscaler, upon eviction, the Spot pool will eventually decrease to zero and require a manual operation to receive any additional Spot nodes.

IMPORTANT

Only schedule workloads on Spot node pools that can handle interruptions, such as batch processing jobs and testing environments. It is recommended that you set up [taints and tolerations](#) on your Spot node pool to ensure that only workloads that can handle node evictions are scheduled on a Spot node pool. For example, the above command by default adds a taint of `kubernetes.azure.com/scalesetpriority=spot:NoSchedule` so only pods with a corresponding toleration are scheduled on this node.

Verify the Spot node pool

To verify your node pool has been added as a Spot node pool:

```
az aks nodepool show --resource-group myResourceGroup --cluster-name myAKSCluster --name spotnodepool
```

Confirm `scaleSetPriority` is *Spot*.

To schedule a pod to run on a Spot node, add a toleration and node affinity that corresponds to the taint applied to your Spot node. The following example shows a portion of a yaml file that defines a toleration that corresponds to the `kubernetes.azure.com/scalesetpriority=spot:NoSchedule` taint and a node affinity that corresponds to the `kubernetes.azure.com/scalesetpriority=spot` label used in the previous step.

```
spec:  
  containers:  
    - name: spot-example  
  tolerations:  
    - key: "kubernetes.azure.com/scalesetpriority"  
      operator: "Equal"  
      value: "spot"  
      effect: "NoSchedule"  
  affinity:  
    nodeAffinity:  
      requiredDuringSchedulingIgnoredDuringExecution:  
        nodeSelectorTerms:  
          - matchExpressions:  
            - key: "kubernetes.azure.com/scalesetpriority"  
              operator: In  
              values:  
                - "spot"  
...  
...
```

When a pod with this toleration and node affinity is deployed, Kubernetes will successfully schedule the pod on the nodes with the taint and label applied.

Upgrade a Spot node pool

Upgrading Spot node pools was previously unsupported, but is now an available operation. When Upgrading a Spot node pool, AKS will internally issue a cordon and an eviction notice, but no drain is applied. There are no surge nodes available for Spot node pool upgrades. Outside of these changes, behavior when upgrading Spot node pools is consistent with other node pool types.

For more information on upgrading, see [Upgrade an AKS cluster](#) and the Azure CLI command `az aks upgrade`.

Max price for a Spot pool

Pricing for Spot instances is variable, based on region and SKU. For more information, see pricing for [Linux](#) and [Windows](#).

With variable pricing, you have option to set a max price, in US dollars (USD), using up to five decimal places. For example, the value *0.98765* would be a max price of \$0.98765 USD per hour. If you set the max price to *-1*, the instance won't be evicted based on price. The price for the instance will be the current price for Spot or the price for a standard instance, whichever is less, as long as there's capacity and quota available.

Next steps

In this article, you learned how to add a Spot node pool to an AKS cluster. For more information about how to control pods across node pools, see [Best practices for advanced scheduler features in AKS](#).

Use Confidential Virtual Machines (CVM) in Azure Kubernetes Service (AKS) cluster

10/27/2022 • 2 minutes to read • [Edit Online](#)

You can use the generally available [confidential VM sizes \(DCav5/ECav5\)](#) to add a node pool to your AKS cluster with CVM. Confidential VMs with AMD SEV-SNP support bring a new set of security features to protect data-in-use with full VM memory encryption. These features enable node pools with CVM to target the migration of highly sensitive container workloads to AKS without any code refactoring while benefiting from the features of AKS. The nodes in a node pool created with CVM use a customized Ubuntu 20.04 image specially configured for CVM. For more details on CVM, see [Confidential VM node pools support on AKS with AMD SEV-SNP confidential VMs](#).

Adding a node pool with CVM to your AKS cluster is currently in preview.

Before you begin

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI installed](#).
- An existing AKS cluster in the *westus*, *eastus*, *westeurope*, or *northeurope* region.
- The [DCav5](#) and [DCadsv5-series](#) or [ECav5](#) and [ECadsv5-series](#) SKUs available for your subscription.

Limitations

The following limitations apply when adding a node pool with CVM to AKS:

- You can't use `--enable-fips-image`, ARM64, or Mariner.
- You can't upgrade an existing node pool to use CVM.
- The [DCav5](#) and [DCadsv5-series](#) or [ECav5](#) and [ECadsv5-series](#) SKUs must be available for your subscription in the region where the cluster is created.

Add a node pool with the CVM to AKS

To add a node pool with the CVM to AKS, use `az aks nodepool add` and set `node-vm-size` to `Standard_DCa4_v5`.

For example:

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name cvmnodepool \
--node-count 3 \
--node-vm-size Standard_DCa4_v5
```

Verify the node pool uses CVM

To verify a node pool uses CVM, use `az aks nodepool show` and verify the `vmSize` is `Standard_DCa4_v5`. For example:

```
az aks nodepool show \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name cvmnodepool \  
  --query 'vmSize'
```

The following example command and output shows the node pool uses CVM:

```
az aks nodepool show \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name cvmnodepool \  
  --query 'vmSize'  
  
"Standard_DC4as_v5"
```

Remove a node pool with CVM from an AKS cluster

To remove a node pool with CVM from an AKS cluster, use `az aks nodepool delete`. For example:

```
az aks nodepool delete \  
  --resource-group myResourceGroup \  
  --cluster-name myAKSCluster \  
  --name cvmnodepool
```

Next steps

In this article, you learned how to add a node pool with CVM to an AKS cluster. For more information about CVM, see [Confidential VM node pools support on AKS with AMD SEV-SNP confidential VMs](#).

Manage system node pools in Azure Kubernetes Service (AKS)

10/27/2022 • 10 minutes to read • [Edit Online](#)

In Azure Kubernetes Service (AKS), nodes of the same configuration are grouped together into *node pools*. Node pools contain the underlying VMs that run your applications. System node pools and user node pools are two different node pool modes for your AKS clusters. System node pools serve the primary purpose of hosting critical system pods such as `CoreDNS` and `metrics-server`. User node pools serve the primary purpose of hosting your application pods. However, application pods can be scheduled on system node pools if you wish to only have one pool in your AKS cluster. Every AKS cluster must contain at least one system node pool with at least one node.

IMPORTANT

If you run a single system node pool for your AKS cluster in a production environment, we recommend you use at least three nodes for the node pool.

Before you begin

- [Azure CLI](#)
- [Azure PowerShell](#)

You need the Azure CLI version 2.3.1 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Limitations

The following limitations apply when you create and manage AKS clusters that support system node pools.

- See [Quotas, virtual machine size restrictions, and region availability in Azure Kubernetes Service \(AKS\)](#).
- The AKS cluster must be built with virtual machine scale sets as the VM type and the *Standard* SKU load balancer.
- The name of a node pool may only contain lowercase alphanumeric characters and must begin with a lowercase letter. For Linux node pools, the length must be between 1 and 12 characters. For Windows node pools, the length must be between 1 and 6 characters.
- An API version of 2020-03-01 or greater must be used to set a node pool mode. Clusters created on API versions older than 2020-03-01 contain only user node pools, but can be migrated to contain system node pools by following [update pool mode steps](#).
- The mode of a node pool is a required property and must be explicitly set when using ARM templates or direct API calls.

System and user node pools

For a system node pool, AKS automatically assigns the label `kubernetes.azure.com/mode: system` to its nodes. This causes AKS to prefer scheduling system pods on node pools that contain this label. This label does not prevent you from scheduling application pods on system node pools. However, we recommend you isolate critical system pods from your application pods to prevent misconfigured or rogue application pods from accidentally killing system pods. You can enforce this behavior by creating a dedicated system node pool. Use

the `CriticalAddonsOnly=true:NoSchedule` taint to prevent application pods from being scheduled on system node pools.

System node pools have the following restrictions:

- System pools osType must be Linux.
- User node pools osType may be Linux or Windows.
- System pools must contain at least one node, and user node pools may contain zero or more nodes.
- System node pools require a VM SKU of at least 2 vCPUs and 4GB memory. But burstable-VM(B series) is not recommended.
- A minimum of two nodes 4 vCPUs is recommended(e.g. Standard_DS4_v2), especially for large clusters (Multiple CoreDNS Pod replicas, 3-4+ add-ons, etc.).
- System node pools must support at least 30 pods as described by the [minimum and maximum value formula for pods](#).
- Spot node pools require user node pools.
- Adding an additional system node pool or changing which node pool is a system node pool will *NOT* automatically move system pods. System pods can continue to run on the same node pool even if you change it to a user node pool. If you delete or scale down a node pool running system pods that was previously a system node pool, those system pods are redeployed with preferred scheduling to the new system node pool.

You can do the following operations with node pools:

- Create a dedicated system node pool (prefer scheduling of system pods to node pools of `mode:system`)
- Change a system node pool to be a user node pool, provided you have another system node pool to take its place in the AKS cluster.
- Change a user node pool to be a system node pool.
- Delete user node pools.
- You can delete system node pools, provided you have another system node pool to take its place in the AKS cluster.
- An AKS cluster may have multiple system node pools and requires at least one system node pool.
- If you want to change various immutable settings on existing node pools, you can create new node pools to replace them. One example is to add a new node pool with a new maxPods setting and delete the old node pool.

Create a new AKS cluster with a system node pool

- [Azure CLI](#)
- [Azure PowerShell](#)

When you create a new AKS cluster, you automatically create a system node pool with a single node. The initial node pool defaults to a mode of type system. When you create new node pools with `az aks nodepool add`, those node pools are user node pools unless you explicitly specify the mode parameter.

The following example creates a resource group named *myResourceGroup* in the *eastus* region.

```
az group create --name myResourceGroup --location eastus
```

Use the `az aks create` command to create an AKS cluster. The following example creates a cluster named *myAKSCluster* with one dedicated system pool containing one node. For your production workloads, ensure you are using system node pools with at least three nodes. This operation may take several minutes to complete.

```
# Create a new AKS cluster with a single system pool
az aks create -g myResourceGroup --name myAKSCluster --node-count 1 --generate-ssh-keys
```

Add a dedicated system node pool to an existing AKS cluster

- [Azure CLI](#)
- [Azure PowerShell](#)

You can add one or more system node pools to existing AKS clusters. It's recommended to schedule your application pods on user node pools, and dedicate system node pools to only critical system pods. This prevents rogue application pods from accidentally killing system pods. Enforce this behavior with the

`CriticalAddonsOnly=true:NoSchedule` taint for your system node pools.

The following command adds a dedicated node pool of mode type system with a default count of three nodes.

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name systempool \
--node-count 3 \
--node-taints CriticalAddonsOnly=true:NoSchedule \
--mode System
```

Show details for your node pool

You can check the details of your node pool with the following command.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
az aks nodepool show -g myResourceGroup --cluster-name myAKSCluster -n systempool
```

A mode of type **System** is defined for system node pools, and a mode of type **User** is defined for user node pools. For a system pool, verify the taint is set to `CriticalAddonsOnly=true:NoSchedule`, which will prevent application pods from being scheduled on this node pool.

```
{  
    "agentPoolType": "VirtualMachineScaleSets",  
    "availabilityZones": null,  
    "count": 3,  
    "enableAutoScaling": null,  
    "enableNodePublicIp": false,  
    "id":  
        "/subscriptions/yourSubscriptionId/resourcegroups/myResourceGroup/providers/Microsoft.ContainerService/managedClusters/myAKSCluster/agentPools/systempool",  
        "maxCount": null,  
        "maxPods": 110,  
        "minCount": null,  
        "mode": "System",  
        "name": "systempool",  
        "nodeImageVersion": "AKSUbuntu-1604-2020.06.30",  
        "nodeLabels": {},  
        "nodeTaints": [  
            "CriticalAddonsOnly=true:NoSchedule"  
        ],  
        "orchestratorVersion": "1.16.10",  
        "osDiskSizeGb": 128,  
        "osType": "Linux",  
        "provisioningState": "Succeeded",  
        "proximityPlacementGroupId": null,  
        "resourceGroup": "myResourceGroup",  
        "scaleSetEvictionPolicy": null,  
        "scaleSetPriority": null,  
        "spotMaxPrice": null,  
        "tags": null,  
        "type": "Microsoft.ContainerService/managedClusters/agentPools",  
        "upgradeSettings": {  
            "maxSurge": null  
        },  
        "vmSize": "Standard_DS2_v2",  
        "vnetSubnetId": null  
}  
}
```

Update existing cluster system and user node pools

- [Azure CLI](#)
- [Azure PowerShell](#)

NOTE

An API version of 2020-03-01 or greater must be used to set a system node pool mode. Clusters created on API versions older than 2020-03-01 contain only user node pools as a result. To receive system node pool functionality and benefits on older clusters, update the mode of existing node pools with the following commands on the latest Azure CLI version.

You can change modes for both system and user node pools. You can change a system node pool to a user pool only if another system node pool already exists on the AKS cluster.

This command changes a system node pool to a user node pool.

```
az aks nodepool update -g myResourceGroup --cluster-name myAKSCluster -n mynodepool --mode user
```

This command changes a user node pool to a system node pool.

```
az aks nodepool update -g myResourceGroup --cluster-name myAKSCluster -n mynodepool --mode system
```

Delete a system node pool

NOTE

To use system node pools on AKS clusters before API version 2020-03-02, add a new system node pool, then delete the original default node pool.

You must have at least two system node pools on your AKS cluster before you can delete one of them.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
az aks nodepool delete -g myResourceGroup --cluster-name myAKSCluster -n mynodepool
```

Clean up resources

- [Azure CLI](#)
- [Azure PowerShell](#)

To delete the cluster, use the [az group delete](#) command to delete the AKS resource group:

```
az group delete --name myResourceGroup --yes --no-wait
```

Next steps

In this article, you learned how to create and manage system node pools in an AKS cluster. For more information about how to use multiple node pools, see [use multiple node pools](#).

Create WebAssembly System Interface (WASI) node pools in Azure Kubernetes Service (AKS) to run your WebAssembly (WASM) workload (preview)

10/27/2022 • 5 minutes to read • [Edit Online](#)

[WebAssembly \(WASM\)](#) is a binary format that is optimized for fast download and maximum execution speed in a WASM runtime. A WASM runtime is designed to run on a target architecture and execute WebAssemblies in a sandbox, isolated from the host computer, at near-native performance. By default, WebAssemblies can't access resources on the host outside of the sandbox unless it is explicitly allowed, and they can't communicate over sockets to access things environment variables or HTTP traffic. The [WebAssembly System Interface \(WASI\)](#) standard defines an API for WASM runtimes to provide access to WebAssemblies to the environment and resources outside the host using a capabilities model.

IMPORTANT

WASI nodepools now use [containerd shims](#) to run WASM workloads. Previously, AKS used [Krustlet](#) to allow WASM modules to be run on Kubernetes. If you are still using Krustlet-based WASI nodepools, you can migrate to containerd shims by creating a new WASI nodepool and migrating your workloads to the new nodepool.

Before you begin

WASM/WASI node pools are currently in preview.

IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

You must also have the latest version of the Azure CLI and `aks-preview` extension installed.

Register the `WasmNodePoolPreview` preview feature

To use the feature, you must also enable the `WasmNodePoolPreview` feature flag on your subscription.

Register the `WasmNodePoolPreview` feature flag by using the `az feature register` command, as shown in the following example:

```
az feature register --namespace "Microsoft.ContainerService" --name "WasmNodePoolPreview"
```

It takes a few minutes for the status to show *Registered*. Verify the registration status by using the `az feature list` command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/WasmNodePoolPreview')].{Name:name, State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider by using the [az provider register](#) command:

```
az provider register --namespace Microsoft.ContainerService
```

Install the `aks-preview` Azure CLI

You also need the *aks-preview* Azure CLI extension version 0.5.34 or later. Install the *aks-preview* Azure CLI extension by using the [az extension add](#) command. Or install any available updates by using the [az extension update](#) command.

```
# Install the aks-preview extension
az extension add --name aks-preview

# Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

Limitations

- Currently, there are only containerd shims available for [spin](#) and [slight](#) applications, which use the [wasmtime](#) runtime. In addition to wasmtime runtime applications, you can also run containers on WASM/WASI node pools.
- You can run containers and wasm modules on the same node, but you can't run containers and wasm modules on the same pod.
- The WASM/WASI node pools can't be used for system node pool.
- The *os-type* for WASM/WASI node pools must be Linux.
- You can't use the Azure portal to create WASM/WASI node pools.

Add a WASM/WASI node pool to an existing AKS Cluster

To add a WASM/WASI node pool, use the [az aks nodepool add](#) command. The following example creates a WASI node pool named *mywasipool* with one node.

```
az aks nodepool add \
  --resource-group myResourceGroup \
  --cluster-name myAKSCluster \
  --name mywasipool \
  --node-count 1 \
  --workload-runtime WasmWasi
```

NOTE

The default value for the *workload-runtime* parameter is *ocicontainer*. To create a node pool that runs container workloads, omit the *workload-runtime* parameter or set the value to *ocicontainer*.

Verify the *workloadRuntime* value using [az aks nodepool show](#). For example:

```
az aks nodepool show -g myResourceGroup --cluster-name myAKSCluster -n mywasipool --query workloadRuntime
```

The following example output shows the `mywasipool` has the `workloadRuntime` type of `WasmWasi`.

```
$ az aks nodepool show -g myResourceGroup --cluster-name myAKSCluster -n mywasipool --query workloadRuntime  
"WasmWasi"
```

Configure `kubectl` to connect to your Kubernetes cluster using the [az aks get-credentials](#) command. The following command:

```
az aks get-credentials -n myakscluster -g myresourcegroup
```

Use `kubectl get nodes` to display the nodes in your cluster.

```
$ kubectl get nodes -o wide  
NAME                  STATUS   ROLES   AGE      VERSION   INTERNAL-IP   EXTERNAL-IP   OS-IMAGE  
KERNEL-VERSION        CONTAINER-RUNTIME  
aks-mywasipool-12456878-vmss000000   Ready    agent    123m    v1.23.12   <WASINODE_IP>   <none>       Ubuntu  
22.04.1 LTS   5.15.0-1020-azure   containerd://1.5.11+azure-2  
aks-nodepool1-12456878-vmss000000   Ready    agent    133m    v1.23.12   <NODE_IP>     <none>       Ubuntu  
22.04.1 LTS   5.15.0-1020-azure   containerd://1.5.11+azure-2
```

Use `kubectl describe node` to show the labels on a node in the WASI node pool. The following example shows the details of `aks-mywasipool-12456878-vmss000000`.

```
$ kubectl describe node aks-mywasipool-12456878-vmss000000  
  
Name:           aks-mywasipool-12456878-vmss000000  
Roles:          agent  
Labels:         agentpool=mywasipool  
...  
               kubernetes.azure.com/wasmtime-slight-v1=true  
               kubernetes.azure.com/wasmtime-spin-v1=true  
...
```

Add a `RuntimeClass` for running `spin` and `slight` applications. Create a file named `wasm-runtimeclass.yaml` with the following content:

```
apiVersion: node.k8s.io/v1  
kind: RuntimeClass  
metadata:  
  name: "wasmtime-slight-v1"  
handler: "slight"  
scheduling:  
  nodeSelector:  
    "kubernetes.azure.com/wasmtime-slight-v1": "true"  
---  
apiVersion: node.k8s.io/v1  
kind: RuntimeClass  
metadata:  
  name: "wasmtime-spin-v1"  
handler: "spin"  
scheduling:  
  nodeSelector:  
    "kubernetes.azure.com/wasmtime-spin-v1": "true"
```

Use `kubectl` to create the `RuntimeClass` objects.

```
kubectl apply -f wasm-runtimeclass.yaml
```

Running WASM/WASI Workload

Create a file named `slight.yaml` with the following content:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: wasm-slight
spec:
  replicas: 1
  selector:
    matchLabels:
      app: wasm-slight
  template:
    metadata:
      labels:
        app: wasm-slight
    spec:
      runtimeClassName: wasmtime-slight-v1
      containers:
        - name: testwasm
          image: ghcr.io/deislabs/containerd-wasm-shims/examples/slight-rust-hello:latest
          command: ["/"]
---
apiVersion: v1
kind: Service
metadata:
  name: wasm-slight
spec:
  type: LoadBalancer
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
  selector:
    app: wasm-slight
```

NOTE

When developing applications, modules should be build against the `wasm32-wasi` target. For more details, see the [spin](#) and [slight](#) documentation.

Use `kubectl` to run your example deployment:

```
kubectl apply -f slight.yaml
```

Use `kubectl get svc` to get the external IP address of the service.

```
$ kubectl get svc
NAME      TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE
kubernetes  ClusterIP  10.0.0.1      <none>        443/TCP      10m
wasm-slight  LoadBalancer  10.0.133.247  <EXTERNAL-IP>  80:30725/TCP  2m47s
```

Access the example application at `http://EXTERNAL-IP/hello`. The following example uses `curl`.

```
$ curl http://EXTERNAL-IP/hello
hello
```

NOTE

If your request times out, use `kubectl get pods` and `kubectl describe pod <POD_NAME>` to check the status of the pod. If the pod is not running, use `kubectl get rs` and `kubectl describe rs <REPLICA_SET_NAME>` to see if the replica set is having issues creating a new pod.

Clean up

To remove the example deployment, use `kubectl delete`.

```
kubectl delete -f slight.yaml
```

To remove the WASM/WASI node pool, use `az aks nodepool delete`.

```
az aks nodepool delete --name mywasipool -g myresourcegroup --cluster-name myakscluster
```

Start and stop an Azure Kubernetes Service (AKS) node pool

10/27/2022 • 2 minutes to read • [Edit Online](#)

Your AKS workloads may not need to run continuously, for example a development cluster that has node pools running specific workloads. To optimize your costs, you can completely turn off (stop) your node pools in your AKS cluster, allowing you to save on compute costs.

Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart using the [Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

Stop an AKS node pool

IMPORTANT

When using node pool start/stop, the following is expected behavior:

- You can't stop system pools.
- Spot node pools are supported.
- Stopped node pools can be upgraded.
- The cluster and node pool must be running.

Use `az aks nodepool stop` to stop a running AKS node pool. The following example stops the *testnodepool* node pool:

```
az aks nodepool stop --nodepool-name testnodepool --resource-group myResourceGroup --cluster-name myAKSCluster
```

You can verify when your node pool is stopped by using the `az aks show` command and confirming the `powerState` shows as `Stopped` as on the below output:

```
{  
[...]  
  "osType": "Linux",  
  "podSubnetId": null,  
  "powerState": {  
    "code": "Stopped"  
  },  
  "provisioningState": "Succeeded",  
  "proximityPlacementGroupId": null,  
[...]  
}
```

NOTE

If the `provisioningState` shows `Stopping`, your node pool hasn't fully stopped yet.

Start a stopped AKS node pool

Use `az aks nodepool start` to start a stopped AKS node pool. The following example starts the stopped node pool named `testnodepool`.

```
az aks nodepool start --nodepool-name testnodepool --resource-group myResourceGroup --cluster-name myAKScluster
```

You can verify your node pool has started using `az aks show` and confirming the `powerState` shows `Running`. For example:

```
{
[...]
"osType": "Linux",
"podSubnetId": null,
"powerState": {
    "code": "Running"
},
"provisioningState": "Succeeded",
"proximityPlacementGroupId": null,
[...]
}
```

NOTE

If the `provisioningState` shows `Starting`, your node pool hasn't fully started yet.

Next steps

- To learn how to scale `User` pools to 0, see [Scale `User` pools to 0](#).
- To learn how to stop your cluster, see [Cluster start/stop](#).
- To learn how to save costs using Spot instances, see [Add a spot node pool to AKS](#).
- To learn more about the AKS support policies, see [AKS support policies](#).

Resize node pools in Azure Kubernetes Service (AKS)

10/27/2022 • 9 minutes to read • [Edit Online](#)

Due to an increasing number of deployments or to run a larger workload, you may want to change the virtual machine scale set plan or resize AKS instances. However, as per [support policies for AKS](#):

AKS agent nodes appear in the Azure portal as regular Azure IaaS resources. But these virtual machines are deployed into a custom Azure resource group (usually prefixed with MC_*) . You cannot do any direct customizations to these nodes using the IaaS APIs or resources. Any custom changes that are not done via the AKS API will not persist through an upgrade, scale, update or reboot.

This lack of persistence also applies to the resize operation, thus, resizing AKS instances in this manner isn't supported. In this how-to guide, you'll learn the recommended method to address this scenario.

IMPORTANT

This method is specific to virtual machine scale set-based AKS clusters. When using virtual machine availability sets, you are limited to only one node pool per cluster.

Example resources

Suppose you want to resize an existing node pool, called `nodepool1`, from SKU size Standard_DS2_v2 to Standard_DS3_v2. To accomplish this task, you'll need to create a new node pool using Standard_DS3_v2, move workloads from `nodepool1` to the new node pool, and remove `nodepool1`. In this example, we'll call this new node pool `mynodepool`.

Node pool	Provisioning state ⓘ	Power state ⓘ	Node count	Mode	Kubernetes version	Node size	Operating system
nodepool1	Succeeded	Running	✓ 3/3 ready	System	1.21.9	Standard_DS2_v2	Linux

```
kubectl get nodes

NAME                      STATUS    ROLES   AGE     VERSION
aks-nodepool1-31721111-vmss000000  Ready    agent   10d    v1.21.9
aks-nodepool1-31721111-vmss000001  Ready    agent   10d    v1.21.9
aks-nodepool1-31721111-vmss000002  Ready    agent   10d    v1.21.9
```

```
kubectl get pods -o wide -A
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	IP	NODE
NOMINATED NODE	READINESS GATES						
default	sampleapp2-74b4b974ff-676sz	1/1	Running	0	93m	10.244.1.6	aks-
nodepool1-31721111-vmss000002	<none>	<none>					
default	sampleapp2-76b6c4c59b-pfgbh	1/1	Running	0	94m	10.244.1.5	aks-
nodepool1-31721111-vmss000002	<none>	<none>					
kube-system	azure-ip-masq-agent-4n66k	1/1	Running	0	10d	10.240.0.6	aks-
nodepool1-31721111-vmss000002	<none>	<none>					
kube-system	azure-ip-masq-agent-9p4c8	1/1	Running	0	10d	10.240.0.4	aks-
nodepool1-31721111-vmss000000	<none>	<none>					
kube-system	azure-ip-masq-agent-nb7mx	1/1	Running	0	10d	10.240.0.5	aks-
nodepool1-31721111-vmss000001	<none>	<none>					
kube-system	coredns-845757d86-dtvvs	1/1	Running	0	10d	10.244.0.2	aks-
nodepool1-31721111-vmss000000	<none>	<none>					
kube-system	coredns-845757d86-x27pp	1/1	Running	0	10d	10.244.2.3	aks-
nodepool1-31721111-vmss000001	<none>	<none>					
kube-system	coredns-autoscaler-5f85dc856b-nfrmh	1/1	Running	0	10d	10.244.2.4	aks-
nodepool1-31721111-vmss000001	<none>	<none>					
kube-system	csi-azuredisk-node-9nfzt	3/3	Running	0	10d	10.240.0.4	aks-
nodepool1-31721111-vmss000000	<none>	<none>					
kube-system	csi-azuredisk-node-bb1sb	3/3	Running	0	10d	10.240.0.5	aks-
nodepool1-31721111-vmss000001	<none>	<none>					
kube-system	csi-azuredisk-node-tjhj4	3/3	Running	0	10d	10.240.0.6	aks-
nodepool1-31721111-vmss000002	<none>	<none>					
kube-system	csi-azurefile-node-9pcr8	3/3	Running	0	3d10h	10.240.0.6	aks-
nodepool1-31721111-vmss000002	<none>	<none>					
kube-system	csi-azurefile-node-bh2pc	3/3	Running	0	3d10h	10.240.0.5	aks-
nodepool1-31721111-vmss000001	<none>	<none>					
kube-system	csi-azurefile-node-h75gq	3/3	Running	0	3d10h	10.240.0.4	aks-
nodepool1-31721111-vmss000000	<none>	<none>					
kube-system	konnectivity-agent-6cd55c69cf-ngdlb	1/1	Running	0	10d	10.240.0.6	aks-
nodepool1-31721111-vmss000002	<none>	<none>					
kube-system	konnectivity-agent-6cd55c69cf-rvvqt	1/1	Running	0	10d	10.240.0.4	aks-
nodepool1-31721111-vmss000000	<none>	<none>					
kube-system	kube-proxy-4wzx7	1/1	Running	0	10d	10.240.0.4	aks-
nodepool1-31721111-vmss000000	<none>	<none>					
kube-system	kube-proxy-g5tvr	1/1	Running	0	10d	10.240.0.6	aks-
nodepool1-31721111-vmss000002	<none>	<none>					
kube-system	kube-proxy-mrv54	1/1	Running	0	10d	10.240.0.5	aks-
nodepool1-31721111-vmss000001	<none>	<none>					
kube-system	metrics-server-774f99dbf4-h52hn	1/1	Running	1	3d10h	10.244.1.3	aks-
nodepool1-31721111-vmss000002	<none>	<none>					

Create a new node pool with the desired SKU

- [Azure CLI](#)
- [Azure PowerShell](#)

Use the `az aks nodepool add` command to create a new node pool called `mynodepool` with three nodes using the `Standard_DS3_v2` VM SKU:

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name mynodepool \
--node-count 3 \
--node-vm-size Standard_DS3_v2 \
--mode System \
--no-wait
```

NOTE

Every AKS cluster must contain at least one system node pool with at least one node. In the example above, we are using a `--mode` of `System`, as the cluster is assumed to have only one node pool, necessitating a `System` node pool to replace it. A node pool's mode can be [updated at any time](#).

When resizing, be sure to consider other requirements and configure your node pool accordingly. You may need to modify the above command. For a full list of the configuration options, see the [az aks nodepool add](#) reference page.

After a few minutes, the new node pool has been created:

Node pool	Provisioning state ⓘ	Power state ⓘ	Node count	Mode	Kubernetes version	Node size	Operating system
mynodepool	Succeeded	Running	3/3 ready	System	1.21.9	Standard_DS3_v2	Linux
nodepool1	Succeeded	Running	3/3 ready	System	1.21.9	Standard_DS2_v2	Linux

```
kubectl get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
aks-mynodepool-20823458-vmss000000	Ready	agent	23m	v1.21.9
aks-mynodepool-20823458-vmss000001	Ready	agent	23m	v1.21.9
aks-mynodepool-20823458-vmss000002	Ready	agent	23m	v1.21.9
aks-nodepool1-31721111-vmss000000	Ready	agent	10d	v1.21.9
aks-nodepool1-31721111-vmss000001	Ready	agent	10d	v1.21.9
aks-nodepool1-31721111-vmss000002	Ready	agent	10d	v1.21.9

Cordon the existing nodes

Cordoning marks specified nodes as unschedulable and prevents any more pods from being added to the nodes.

First, obtain the names of the nodes you'd like to cordon with `kubectl get nodes`. Your output should look similar to the following:

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-31721111-vmss000000	Ready	agent	7d21h	v1.21.9
aks-nodepool1-31721111-vmss000001	Ready	agent	7d21h	v1.21.9
aks-nodepool1-31721111-vmss000002	Ready	agent	7d21h	v1.21.9

Next, using `kubectl cordon <node-names>`, specify the desired nodes in a space-separated list:

```
kubectl cordon aks-nodepool1-31721111-vmss000000 aks-nodepool1-31721111-vmss000001 aks-nodepool1-31721111-vmss000002
```

```
node/aks-nodepool1-31721111-vmss000000 cordoned
node/aks-nodepool1-31721111-vmss000001 cordoned
node/aks-nodepool1-31721111-vmss000002 cordoned
```

Drain the existing nodes

IMPORTANT

To successfully drain nodes and evict running pods, ensure that any PodDisruptionBudgets (PDBs) allow for at least 1 pod replica to be moved at a time, otherwise the drain/evict operation will fail. To check this, you can run

```
kubectl get pdb -A
```

 and make sure `ALLOWED DISRUPTIONS` is at least 1 or higher.

Draining nodes will cause pods running on them to be evicted and recreated on the other, schedulable nodes.

To drain nodes, use `kubectl drain <node-names> --ignore-daemonsets --delete-emptydir-data`, again using a space-separated list of node names:

IMPORTANT

Using `--delete-emptydir-data` is required to evict the AKS-created `coredns` and `metrics-server` pods. If this flag isn't used, an error is expected. For more information, see the [documentation on emptydir](#).

```
kubectl drain aks-nodepool1-31721111-vmss000000 aks-nodepool1-31721111-vmss000001 aks-nodepool1-31721111-vmss000002 --ignore-daemonsets --delete-emptydir-data
```

After the drain operation finishes, all pods other than those controlled by daemon sets are running on the new node pool:

kubectl get pods -o wide -A							
NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	IP	NODE
NOMINATED NODE	READINESS GATES						
default	sampleapp2-74b4b974ff-676sz	1/1	Running	0	15m	10.244.4.5	aks-
mynodepool-20823458-vmss000002	<none>	<none>					
default	sampleapp2-76b6c4c59b-rhmzq	1/1	Running	0	16m	10.244.4.3	aks-
mynodepool-20823458-vmss000002	<none>	<none>					
kube-system	azure-ip-masq-agent-4n66k	1/1	Running	0	10d	10.240.0.6	aks-
nodepool1-31721111-vmss000002	<none>	<none>					
kube-system	azure-ip-masq-agent-9p4c8	1/1	Running	0	10d	10.240.0.4	aks-
nodepool1-31721111-vmss000000	<none>	<none>					
kube-system	azure-ip-masq-agent-nb7mx	1/1	Running	0	10d	10.240.0.5	aks-
nodepool1-31721111-vmss000001	<none>	<none>					
kube-system	azure-ip-masq-agent-sxn96	1/1	Running	0	49m	10.240.0.9	aks-
mynodepool-20823458-vmss000002	<none>	<none>					
kube-system	azure-ip-masq-agent-tsq98	1/1	Running	0	49m	10.240.0.8	aks-
mynodepool-20823458-vmss000001	<none>	<none>					
kube-system	azure-ip-masq-agent-xzrdl	1/1	Running	0	49m	10.240.0.7	aks-
mynodepool-20823458-vmss000000	<none>	<none>					
kube-system	coredns-845757d86-d2pkc	1/1	Running	0	17m	10.244.3.2	aks-
mynodepool-20823458-vmss000000	<none>	<none>					
kube-system	coredns-845757d86-f8g9s	1/1	Running	0	17m	10.244.5.2	aks-
mynodepool-20823458-vmss000001	<none>	<none>					
kube-system	coredns-autoscaler-5f85dc856b-f8xh2	1/1	Running	0	17m	10.244.4.2	aks-
mynodepool-20823458-vmss000002	<none>	<none>					
kube-system	csi-azuredisk-node-7md2w	3/3	Running	0	49m	10.240.0.7	aks-
mynodepool-20823458-vmss000000	<none>	<none>					
kube-system	csi-azuredisk-node-9nfzt	3/3	Running	0	10d	10.240.0.4	aks-
nodepool1-31721111-vmss000000	<none>	<none>					
kube-system	csi-azuredisk-node-bblsb	3/3	Running	0	10d	10.240.0.5	aks-
nodepool1-31721111-vmss000001	<none>	<none>					
kube-system	csi-azuredisk-node-lcmtz	3/3	Running	0	49m	10.240.0.9	aks-
mynodepool-20823458-vmss000002	<none>	<none>					
kube-system	csi-azuredisk-node-mmncr	3/3	Running	0	49m	10.240.0.8	aks-
mynodepool-20823458-vmss000001	<none>	<none>					
kube-system	csi-azuredisk-node-tjhj4	3/3	Running	0	10d	10.240.0.6	aks-
nodepool1-31721111-vmss000002	<none>	<none>					

kube-system	csi-azurefile-node-29w6z	3/3	Running	0	49m	10.240.0.9	aks-
mynodepool-20823458-vms00002	<none>	<none>					
kube-system	csi-azurefile-node-4nrx7	3/3	Running	0	49m	10.240.0.7	aks-
mynodepool-20823458-vms00000	<none>	<none>					
kube-system	csi-azurefile-node-9pcr8	3/3	Running	0	3d11h	10.240.0.6	aks-
nodepool1-31721111-vms00002	<none>	<none>					
kube-system	csi-azurefile-node-bh2pc	3/3	Running	0	3d11h	10.240.0.5	aks-
nodepool1-31721111-vms00001	<none>	<none>					
kube-system	csi-azurefile-node-gqqnv	3/3	Running	0	49m	10.240.0.8	aks-
mynodepool-20823458-vms00001	<none>	<none>					
kube-system	csi-azurefile-node-h75gq	3/3	Running	0	3d11h	10.240.0.4	aks-
nodepool1-31721111-vms00000	<none>	<none>					
kube-system	konnectivity-agent-6cd55c69cf-2bbp5	1/1	Running	0	17m	10.240.0.7	aks-
mynodepool-20823458-vms00000	<none>	<none>					
kube-system	konnectivity-agent-6cd55c69cf-7zxzxj	1/1	Running	0	16m	10.240.0.8	aks-
mynodepool-20823458-vms00001	<none>	<none>					
kube-system	kube-proxy-4wzx7	1/1	Running	0	10d	10.240.0.4	aks-
nodepool1-31721111-vms00000	<none>	<none>					
kube-system	kube-proxy-7h8r5	1/1	Running	0	49m	10.240.0.7	aks-
mynodepool-20823458-vms00000	<none>	<none>					
kube-system	kube-proxy-g5tvr	1/1	Running	0	10d	10.240.0.6	aks-
nodepool1-31721111-vms00002	<none>	<none>					
kube-system	kube-proxy-mrv54	1/1	Running	0	10d	10.240.0.5	aks-
nodepool1-31721111-vms00001	<none>	<none>					
kube-system	kube-proxy-nqmnj	1/1	Running	0	49m	10.240.0.9	aks-
mynodepool-20823458-vms00002	<none>	<none>					
kube-system	kube-proxy-zn77s	1/1	Running	0	49m	10.240.0.8	aks-
mynodepool-20823458-vms00001	<none>	<none>					
kube-system	metrics-server-774f99dbf4-2x6x8	1/1	Running	0	16m	10.244.4.4	aks-
mynodepool-20823458-vms00002	<none>	<none>					

Troubleshooting

You may see an error like the following:

Error when evicting pods/[podname] -n [namespace] (will retry after 5s): Cannot evict pod as it would violate the pod's disruption budget.

By default, your cluster has AKS_managed pod disruption budgets (such as `coredns-pdb` or `konnectivity-agent`) with a `MinAvailable` of 1. If, for example, there are two `coredns` pods running, while one of them is getting recreated and is unavailable, the other is unable to be affected due to the pod disruption budget. This resolves itself after the initial `coredns` pod is scheduled and running, allowing the second pod to be properly evicted and recreated.

TIP

Consider draining nodes one-by-one for a smoother eviction experience and to avoid throttling. For more information, see:

- [Plan for availability using a pod disruption budget](#)
- [Specifying a Disruption Budget for your Application](#)
- [Disruptions](#)

Remove the existing node pool

- [Azure CLI](#)
- [Azure PowerShell](#)

To delete the existing node pool, use the Azure portal or the `az aks nodepool delete` command:

IMPORTANT

When you delete a node pool, AKS doesn't perform cordon and drain. To minimize the disruption of rescheduling pods currently running on the node pool you are going to delete, perform a cordon and drain on all nodes in the node pool before deleting.

```
az aks nodepool delete \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name nodepool1
```

After completion, the final result is the AKS cluster having a single, new node pool with the new, desired SKU size and all the applications and pods properly running:

Node pool	Provisioning state ⓘ	Power state ⓘ	Node count	Mode	Kubernetes version	Node size	Operating system
mynodepool	Succeeded	Running	3/3 ready	System	1.21.9	Standard_DS3_v2	Linux

```
kubectl get nodes

NAME                      STATUS   ROLES   AGE    VERSION
aks-mynodepool-20823458-vmss000000  Ready   agent   63m   v1.21.9
aks-mynodepool-20823458-vmss000001  Ready   agent   63m   v1.21.9
aks-mynodepool-20823458-vmss000002  Ready   agent   63m   v1.21.9
```

Next steps

After resizing a node pool by cordoning and draining, learn more about [using multiple node pools](#).

Use the Mariner container host on Azure Kubernetes Service (AKS)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Mariner is an open-source Linux distribution created by Microsoft, and it's now available for preview as a container host on Azure Kubernetes Service (AKS). The Mariner container host provides reliability and consistency from cloud to edge across the AKS, AKS-HCI, and Arc products. You can deploy Mariner node pools in a new cluster, add Mariner node pools to your existing Ubuntu clusters, or migrate your Ubuntu nodes to Mariner nodes. To learn more about Mariner, see the [Mariner documentation](#).

Why use Mariner

The Mariner container host on AKS uses a native AKS image that provides one place to do all Linux development. Every package is built from source and validated, ensuring your services run on proven components. Mariner is lightweight, only including the necessary set of packages needed to run container workloads. It provides a reduced attack surface and eliminates patching and maintenance of unnecessary packages. At Mariner's base layer, it has a Microsoft hardened kernel tuned for Azure. Learn more about the [key capabilities of Mariner](#).

How to use Mariner on AKS

To get started using Mariner on AKS, see:

- [Creating a cluster with Mariner](#)
- [Add a Mariner node pool to your existing cluster](#)
- [Ubuntu to Mariner migration](#)

How to upgrade Mariner nodes

We recommend keeping your clusters up to date and secured by enabling automatic upgrades for your cluster.

To enable automatic upgrades, see:

- [Automatically upgrade an Azure Kubernetes Service \(AKS\) cluster](#)
- [Deploy kured in an AKS cluster](#)

To manually upgrade the node-image on a cluster, you can run `az aks nodepool upgrade`:

```
az aks nodepool upgrade \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name myNodePool \
--node-image-only
```

Regional availability

Mariner is available for use in the same regions as AKS.

Limitations

Mariner currently has the following limitations:

- Mariner does not yet have image SKUs for GPU, ARM64, SGX, or FIPS.
- Mariner does not yet have FedRAMP, FIPS, or CIS certification.
- Mariner cannot yet be deployed through Azure portal or Terraform.
- Qualys and Trivy are the only vulnerability scanning tools that support Mariner today.
- The Mariner container host is a Gen 2 image. Mariner does not plan to offer a Gen 1 SKU.
- Node configurations are not yet supported.
- Mariner is not yet supported in GitHub actions.
- Mariner does not support AppArmor. Support for SELinux can be manually configured.
- Some addons, extensions, and open-source integrations may not be supported yet on Mariner. Azure Monitor, Grafana, Helm, Key Vault, and Container Insights are confirmed to be supported.
- AKS diagnostics does not yet support Mariner.

Access Kubernetes resources from the Azure portal

10/27/2022 • 4 minutes to read • [Edit Online](#)

The Azure portal includes a Kubernetes resource view for easy access to the Kubernetes resources in your Azure Kubernetes Service (AKS) cluster. Viewing Kubernetes resources from the Azure portal reduces context switching between the Azure portal and the `kubectl` command-line tool, streamlining the experience for viewing and editing your Kubernetes resources. The resource viewer currently includes multiple resource types, such as deployments, pods, and replica sets.

The Kubernetes resource view from the Azure portal replaces the AKS dashboard add-on, which is deprecated.

Prerequisites

To view Kubernetes resources in the Azure portal, you need an AKS cluster. Any cluster is supported, but if using Azure Active Directory (Azure AD) integration, your cluster must use [AKS-managed Azure AD integration](#). If your cluster uses legacy Azure AD, you can upgrade your cluster in the portal or with the [Azure CLI](#). You can also [use the Azure portal](#) to create a new AKS cluster.

View Kubernetes resources

To see the Kubernetes resources, navigate to your AKS cluster in the Azure portal. The navigation pane on the left is used to access your resources. The resources include:

- **Namespaces** displays the namespaces of your cluster. The filter at the top of the namespace list provides a quick way to filter and display your namespace resources.
- **Workloads** shows information about deployments, pods, replica sets, stateful sets, daemon sets, jobs, and cron jobs deployed to your cluster. The screenshot below shows the default system pods in an example AKS cluster.
- **Services and ingresses** shows all of your cluster's service and ingress resources.
- **Storage** shows your Azure storage classes and persistent volume information.
- **Configuration** shows your cluster's config maps and secrets.

The screenshot shows the Azure portal interface for managing an AKS cluster named 'aks-portal-docs'. The left sidebar contains navigation links for Home, AKS clusters, and various management sections like Overview, Activity log, Access control (IAM), Tags, and Security. Under 'Kubernetes resources', the 'Workloads' section is selected, showing a list of Deployments. The 'Deployments' tab is active, with other tabs for Pods, Replica sets, Stateful sets, Daemon sets, Jobs, and Cron jobs. A search bar at the top allows filtering by deployment name, label selector, or namespace. The main table lists the following pods:

Name	Namespace	Ready	Up-to-date	Available	Age
coredns-autoscaler	kube-system	✓ 1/1	1	1	49 minutes
coredns	kube-system	✓ 2/2	2	2	49 minutes
metrics-server	kube-system	✓ 1/1	1	1	49 minutes
omsagent-ss	kube-system	✓ 1/1	1	1	49 minutes
tunnelfront	kube-system	✓ 1/1	1	1	49 minutes

Deploy an application

In this example, we'll use our sample AKS cluster to deploy the Azure Vote application from the [AKS quickstart](#).

1. Select **Add** from any of the resource views (Namespace, Workloads, Services and ingresses, Storage, or Configuration).
2. Paste the YAML for the Azure Vote application from the [AKS quickstart](#).
3. Select **Add** at the bottom of the YAML editor to deploy the application.

Once the YAML file is added, the resource viewer shows both Kubernetes services that were created: the internal service (azure-vote-back), and the external service (azure-vote-front) to access the Azure Vote application. The external service includes a linked external IP address so you can easily view the application in your browser.

Name	Namespace	Status	Type	Cluster IP	External IP	Ports	Age
kubernetes	default	Ok	ClusterIP	10.0.0.1		443/TCP	55 minutes
healthmodel-replicaset-service	kube-system	Ok	ClusterIP	10.0.226.252		25227/TCP	55 minutes
kube-dns	kube-system	Ok	ClusterIP	10.0.0.10		53/UDP,53/TCP	55 minutes
metrics-server	kube-system	Ok	ClusterIP	10.0.75.143		443/TCP	55 minutes
azure-vote-back	default	Ok	ClusterIP	10.0.223.33		6379/TCP	8 seconds
azure-vote-front	default	Ok	LoadBalancer	10.0.57.52	52.154.169.60	80:30864/TCP	7 seconds

Monitor deployment insights

AKS clusters with [Container insights](#) enabled can quickly view deployment and other insights. From the Kubernetes resources view, users can see the live status of individual deployments, including CPU and memory usage, as well as transition to Azure monitor for more in-depth information about specific nodes and containers. Here's an example of deployment insights from a sample AKS cluster:

Name	Namespace	Ready	Up-To-Date	Available	Age
azure-vote-back	default	1/1	1	1	12 minutes
azure-vote-front	default	1/1	1	1	12 minutes
coredns	kube-system	2/2	2	2	an hour
coredns-autoscaler	kube-system	1/1	1	1	an hour
metrics-server	kube-system	1/1	1	1	an hour
omsagent-rs	kube-system	1/1	1	1	an hour
tunneelfront	kube-system	1/1	1	1	an hour

Edit YAML

The Kubernetes resource view also includes a YAML editor. A built-in YAML editor means you can update or create services and deployments from within the portal and apply changes immediately.

azure-vote-front | YAML

Service

The screenshot shows the Azure Portal interface for managing a Kubernetes service named 'azure-vote-front'. The 'YAML' tab is selected, displaying the following YAML code:

```
1 kind: Service
2 apiVersion: v1
3 metadata:
4   name: azure-vote-front
5   namespace: default
6   selfLink: /api/v1/namespaces/default/services/azure-vote-front
7   uid:
8   resourceVersion: '857494'
9   creationTimestamp: '2020-08-04T21:27:12Z'
10  finalizers:
11    - service.kubernetes.io/load-balancer-cleanup
12  managedFields:
13    - manager: Mozilla
14      operation: Update
15      apiVersion: v1
16      time: '2020-08-04T21:27:12Z'
17      fieldsType: FieldsV1
18      fieldsV1:
19        'f:spec':
20          'f:externalTrafficPolicy': {}
21        'f:ports':
22          .: {}
23          'k:{"port":80,"protocol":"TCP"}':
24            .: {}
25            'f:port': {}
26            'f:protocol': {}
```

Below the code editor are two buttons: 'Review + save' and 'Discard'.

After editing the YAML, changes are applied by selecting **Review + save**, confirming the changes, and then saving again.

WARNING

Performing direct production changes via UI or CLI is not recommended, you should leverage [continuous integration \(CI\) and continuous deployment \(CD\) best practices](#). The Azure Portal Kubernetes management capabilities and the YAML editor are built for learning and flighting new deployments in a development and testing setting.

Troubleshooting

This section addresses common problems and troubleshooting steps.

Unauthorized access

To access the Kubernetes resources, you must have access to the AKS cluster, the Kubernetes API, and the Kubernetes objects. Ensure that you're either a cluster administrator or a user with the appropriate permissions to access the AKS cluster. For more information on cluster security, see [Access and identity options for AKS](#).

NOTE

The kubernetes resource view in the Azure Portal is only supported by [managed-AAD enabled clusters](#) or non-AAD enabled clusters. If you are using a managed-AAD enabled cluster, your AAD user or identity needs to have the respective roles/role bindings to access the kubernetes API, in addition to the permission to pull the user `kubeconfig`.

Enable resource view

For existing clusters, you may need to enable the Kubernetes resource view. To enable the resource view, follow the prompts in the portal for your cluster.

- [Azure CLI](#)
- [Azure PowerShell](#)

TIP

The AKS feature for [API server authorized IP ranges](#) can be added to limit API server access to only the firewall's public endpoint. Another option for such clusters is updating `--api-server-authorized-ip-ranges` to include access for a local client computer or IP address range (from which portal is being browsed). To allow this access, you need the computer's public IPv4 address. You can find this address with below command or by searching "what is my IP address" in an internet browser.

```
# Retrieve your IP address
CURRENT_IP=$(dig +short myip.opendns.com @resolver1.opendns.com)
```

```
# Add to AKS approved list
az aks update -g $RG -n $AKSNAME --api-server-authorized-ip-ranges $CURRENT_IP/32
```

Next steps

This article showed you how to access Kubernetes resources for your AKS cluster. See [Deployments and YAML manifests](#) for a deeper understanding of cluster resources and the YAML files that are accessed with the Kubernetes resource viewer.

Use Azure tags in Azure Kubernetes Service (AKS)

10/27/2022 • 6 minutes to read • [Edit Online](#)

With Azure Kubernetes Service (AKS), you can set Azure tags on an AKS cluster and its related resources by using Azure Resource Manager, through the Azure CLI. For some resources, you can also use Kubernetes manifests to set Azure tags. Azure tags are a useful tracking resource for certain business processes, such as *chargeback*.

This article explains how to set Azure tags for AKS clusters and related resources.

Before you begin

It's a good idea to understand what happens when you set and update Azure tags with AKS clusters and their related resources. For example:

- Tags set on an AKS cluster apply to all resources that are related to the cluster, but not the node pools. This operation overwrites the values of existing keys.
- Tags set on a node pool apply only to resources related to that node pool. This operation overwrites the values of existing keys. Resources outside that node pool, including resources for the rest of the cluster and other node pools, are unaffected.
- Public IPs, files, and disks can have tags set by Kubernetes through a Kubernetes manifest. Tags set in this way will maintain the Kubernetes values, even if you update them later by using another method. When public IPs, files, or disks are removed through Kubernetes, any tags that are set by Kubernetes are removed. Tags on those resources that aren't tracked by Kubernetes remain unaffected.

Prerequisites

- The Azure CLI version 2.0.59 or later, installed and configured.

To find your version, run `az --version`. If you need to install it or update your version, see [Install Azure CLI](#).

- Kubernetes version 1.20 or later, installed.

Limitations

- Azure tags have keys that are case-insensitive for operations, such as when you're retrieving a tag by searching the key. In this case, a tag with the specified key will be updated or retrieved regardless of casing. Tag values are case-sensitive.
- In AKS, if multiple tags are set with identical keys but different casing, the tags are used in alphabetical order. For example, `{"Key1": "val1", "kEy1": "val2", "key1": "val3"}` results in `Key1` and `val1` being set.
- For shared resources, tags aren't able to determine the split in resource usage on their own.

Add tags to the cluster

When you create or update an AKS cluster with the `--tags` parameter, the following are assigned the Azure tags that you've specified:

- The AKS cluster
- The route table that's associated with the cluster
- The public IP that's associated with the cluster
- The load balancer that's associated with the cluster

- The network security group that's associated with the cluster
- The virtual network that's associated with the cluster
- The AKS managed kubelet msi associated with the cluster
- The AKS managed addon msi associated with the cluster
- The private DNS zone associated with the private cluster
- The private endpoint associated with the private cluster

NOTE

Azure Private DNS only supports 15 tags. [tag resources](#).

To create a cluster and assign Azure tags, run `az aks create` with the `--tags` parameter, as shown in the following command. Running the command creates a *myAKSCluster* in the *myResourceGroup* with the tags *dept=IT* and *costcenter=9999*.

NOTE

To set tags on the initial node pool, the node resource group, the virtual machine scale set, and each virtual machine scale set instance that's associated with the initial node pool, also set the `--nodepool-tags` parameter.

```
az aks create \
  --resource-group myResourceGroup \
  --name myAKSCluster \
  --tags dept=IT costcenter=9999 \
  --generate-ssh-keys
```

IMPORTANT

If you're using existing resources when you're creating a new cluster, such as an IP address or route table,

`az aks create` overwrites the set of tags. If you delete that cluster later, any tags set by the cluster will be removed.

Verify that the tags have been applied to the cluster and related resources. The cluster tags for *myAKSCluster* are shown in the following example:

```
$ az aks show -g myResourceGroup -n myAKSCluster --query '[tags]'
{
  "clusterTags": {
    "costcenter": "9999",
    "dept": "IT"
  }
}
```

To update the tags on an existing cluster, run `az aks update` with the `--tags` parameter. Running the command updates the *myAKSCluster* with the tags *team=alpha* and *costcenter=1234*.

```
az aks update \
  --resource-group myResourceGroup \
  --name myAKSCluster \
  --tags team=alpha costcenter=1234
```

Verify that the tags have been applied to the cluster. For example:

```
$ az aks show -g myResourceGroup -n myAKScluster --query '[tags]'  
{  
  "clusterTags": {  
    "costcenter": "1234",  
    "team": "alpha"  
  }  
}
```

IMPORTANT

Setting tags on a cluster by using `az aks update` overwrites the set of tags. For example, if your cluster has the tags `dept=IT` and `costcenter=9999` and you use `az aks update` with the tags `team=alpha` and `costcenter=1234`, the new list of tags would be `team=alpha` and `costcenter=1234`.

Adding tags to node pools

You can apply an Azure tag to a new or existing node pool in your AKS cluster. Tags applied to a node pool are applied to each node within the node pool and are persisted through upgrades. Tags are also applied to new nodes that are added to a node pool during scale-out operations. Adding a tag can help with tasks such as policy tracking or cost estimation.

When you create or update a node pool with the `--tags` parameter, the tags that you specify are assigned to the following resources:

- The node pool
- The node resource group
- The virtual machine scale set and each virtual machine scale set instance that's associated with the node pool

To create a node pool with an Azure tag, run `az aks nodepool add` with the `--tags` parameter. Running the following command creates a `tagnodepool` node pool with the tags `abtest=a` and `costcenter=5555` in the `myAKScluster`.

```
az aks nodepool add \  
  --resource-group myResourceGroup \  
  --cluster-name myAKScluster \  
  --name tagnodepool \  
  --node-count 1 \  
  --tags abtest=a costcenter=5555 \  
  --no-wait
```

Verify that the tags have been applied to the `tagnodepool` node pool.

```
$ az aks show -g myResourceGroup -n myAKScluster --query 'agentPoolProfiles[].{nodepoolName:name,tags:tags}'  
[  
  {  
    "nodepoolName": "nodepool1",  
    "tags": null  
  },  
  {  
    "nodepoolName": "tagnodepool",  
    "tags": {  
      "abtest": "a",  
      "costcenter": "5555"  
    }  
  }  
]
```

To update a node pool with an Azure tag, run `az aks nodepool update` with the `--tags` parameter. Running the following command updates the `tagnodepool` node pool with the tags `appversion=0.0.2` and `costcenter=4444` in the `myAKSCluster`, which already has the tags `abtest=a` and `costcenter=5555`.

```
az aks nodepool update \
    --resource-group myResourceGroup \
    --cluster-name myAKSCluster \
    --name tagnodepool \
    --tags appversion=0.0.2 costcenter=4444 \
    --no-wait
```

IMPORTANT

Setting tags on a node pool by using `az aks nodepool update` overwrites the set of tags. For example, if your node pool has the tags `abtest=a` and `costcenter=5555`, and you use `az aks nodepool update` with the tags `appversion=0.0.2` and `costcenter=4444`, the new list of tags would be `appversion=0.0.2` and `costcenter=4444`.

Verify that the tags have been updated on the nodepool.

```
$ az aks show -g myResourceGroup -n myAKSCluster --query 'agentPoolProfiles[].{nodepoolName:name,tags:tags}'  
[  
  {  
    "nodepoolName": "nodepool1",  
    "tags": null  
  },  
  {  
    "nodepoolName": "tagnodepool",  
    "tags": {  
      "appversion": "0.0.2",  
      "costcenter": "4444"  
    }  
  }  
]
```

Add tags by using Kubernetes

You can apply Azure tags to public IPs, disks, and files by using a Kubernetes manifest.

For public IPs, use `service.beta.kubernetes.io/azure-pip-tags` under `annotations`. For example:

```
apiVersion: v1
kind: Service
metadata:
  annotations:
    service.beta.kubernetes.io/azure-pip-tags: costcenter=3333,team=beta
spec:
  ...

```

For files and disks, use *tags* under *parameters*. For example:

```
---  
apiVersion: storage.k8s.io/v1  
...  
parameters:  
...  
tags: costcenter=3333,team=beta  
...
```

IMPORTANT

Setting tags on files, disks, and public IPs by using Kubernetes updates the set of tags. For example, if your disk has the tags *dept=IT* and *costcenter=5555*, and you use Kubernetes to set the tags *team=beta* and *costcenter=3333*, the new list of tags would be *dept=IT*, *team=beta*, and *costcenter=3333*.

Any updates that you make to tags through Kubernetes will retain the value that's set through Kubernetes. For example, if your disk has tags *dept=IT* and *costcenter=5555* set by Kubernetes, and you use the portal to set the tags *team=beta* and *costcenter=3333*, the new list of tags would be *dept=IT*, *team=beta*, and *costcenter=5555*. If you then remove the disk through Kubernetes, the disk would have the tag *team=beta*.

Use labels in an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 4 minutes to read • [Edit Online](#)

If you have multiple node pools, you may want to add a label during node pool creation. [These labels](#) are visible in Kubernetes for handling scheduling rules for nodes. You can add labels to a node pool anytime, and they'll be set on all nodes in the node pool.

In this how-to guide, you'll learn how to use labels in an AKS cluster.

Prerequisites

You need the Azure CLI version 2.2.0 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Create an AKS cluster with a label

To create an AKS cluster with a label, use `az aks create`. Specify the `--node-labels` parameter to set your labels. Labels must be a key/value pair and have a [valid syntax](#).

```
az aks create \
  --resource-group myResourceGroup \
  --name myAKSCluster \
  --node-count 2 \
  --nodepool-labels dept=IT costcenter=9000
```

Verify the labels were set by running `kubectl get nodes --show-labels`.

```
kubectl get nodes --show-labels | grep -e "costcenter=9000" -e "dept=IT"
```

Create a node pool with a label

To create a node pool with a label, use `az aks nodepool add`. Specify the name *labelnp* and use the `--labels` parameter to specify *dept=HR* and *costcenter=5000* for labels. Labels must be a key/value pair and have a [valid syntax](#)

```
az aks nodepool add \
  --resource-group myResourceGroup \
  --cluster-name myAKSCluster \
  --name labelnp \
  --node-count 1 \
  --labels dept=HR costcenter=5000 \
  --no-wait
```

The following example output from the `az aks nodepool list` command shows that *labelnp* is *Creating* nodes with the specified *nodeLabels*:

```
az aks nodepool list -g myResourceGroup --cluster-name myAKSCluster

```output
[
 {
 ...
 "count": 1,
 ...
 "name": "labelnp",
 "orchestratorVersion": "1.15.7",
 ...
 "provisioningState": "Creating",
 ...
 "nodeLabels": {
 "costcenter": "5000",
 "dept": "HR"
 },
 ...
 },
 ...
]
```

Verify the labels were set by running `kubectl get nodes --show-labels`.

```
kubectl get nodes --show-labels | grep -e "costcenter=5000" -e "dept=HR"
```

## Updating labels on existing node pools

To update a label on existing node pools, use [az aks nodepool update](#). Updating labels on existing node pools will overwrite the old labels with the new labels. Labels must be a key/value pair and have a [valid syntax](#).

```
az aks nodepool update \
 --resource-group myResourceGroup \
 --cluster-name myAKSCluster \
 --name labelnp \
 --labels dept=ACCT costcenter=6000 \
 --no-wait
```

Verify the labels were set by running `kubectl get nodes --show-labels`.

```
kubectl get nodes --show-labels | grep -e "costcenter=6000" -e "dept=ACCT"
```

## Unavailable labels

### Reserved system labels

Since the [2021-08-19 AKS release](#), Azure Kubernetes Service (AKS) has stopped the ability to make changes to AKS reserved labels. Attempting to change these labels will result in an error message.

The following labels are reserved for use by AKS. *Virtual node usage* specifies if these labels could be a supported system feature on virtual nodes.

Some properties that these system features change aren't available on the virtual nodes, because they require modifying the host.

Label	Value	Example/Options	Virtual Node Usage
kubernetes.azure.com/agentpool	<agent pool name>	nodepool1	Same
kubernetes.io/arch	amd64	runtime.GOARCH	N/A
kubernetes.io/os	<OS Type>	Linux/Windows	Same
node.kubernetes.io/instance-type	<VM size>	Standard_NC6	Virtual
topology.kubernetes.io/region	<Azure region>	westus2	Same
topology.kubernetes.io/zone	<Azure zone>	0	Same
kubernetes.azure.com/cluster	<MC_RgName>	MC_aks_myAKSCluster_westus2	Same
kubernetes.azure.com/module	<mode>	User or system	User
kubernetes.azure.com/role	agent	Agent	Same
kubernetes.azure.com/scale-setpriority	<VMSS priority>	Spot or regular	N/A
kubernetes.io/hostname	<hostname>	aks-nodepool-00000000-vmss000000	Same
kubernetes.azure.com/storageprofile	<OS disk storage profile>	Managed	N/A
kubernetes.azure.com/storage-tier	<OS disk storage tier>	Premium_LRS	N/A
kubernetes.azure.com/instance-sku	<SKU family>	Standard_N	Virtual
kubernetes.azure.com/node-image-version	<VHD version>	AKSUbuntu-1804-2020.03.05	Virtual node version
kubernetes.azure.com/subnet	<nodepool subnet name>	subnetName	Virtual node subnet name
kubernetes.azure.com/vnet	<nodepool vnet name>	vnetName	Virtual node virtual network
kubernetes.azure.com/ppg	<nodepool ppg name>	ppgName	N/A
kubernetes.azure.com/encrypted-set	<nodepool encrypted-set name>	encrypted-set-name	N/A

Label	Value	Example/Options	Virtual Node Usage
kubernetes.azure.com/accelerator	<accelerator>	nvidia	N/A
kubernetes.azure.com/fips_enabled	<is fips enabled?>	true	N/A
kubernetes.azure.com/os-sku	<os/sku>	Create or update OS SKU	Linux

- *Same* is included in places where the expected values for the labels don't differ between a standard node pool and a virtual node pool. As virtual node pods don't expose any underlying virtual machine (VM), the VM SKU values are replaced with the SKU *Virtual*.
- *Virtual node version* refers to the current version of the [virtual Kubelet-ACI connector release](#).
- *Virtual node subnet name* is the name of the subnet where virtual node pods are deployed into Azure Container Instance (ACI).
- *Virtual node virtual network* is the name of the virtual network, which contains the subnet where virtual node pods are deployed on ACI.

## Reserved prefixes

The following list of prefixes are reserved for usage by AKS and can't be used for any node.

- kubernetes.azure.com/
- kubernetes.io/

For additional reserved prefixes, see [Kubernetes well-known labels, annotations, and taints](#).

## Deprecated labels

The following labels are planned for deprecation with the release of [Kubernetes v1.24](#). Customers should change any label references to the recommended substitute.

Label	Recommended Substitute	Maintainer
failure-domain.beta.kubernetes.io/region	topology.kubernetes.io/region	<a href="#">Kubernetes</a>
failure-domain.beta.kubernetes.io/zone	topology.kubernetes.io/zone	<a href="#">Kubernetes</a>
beta.kubernetes.io/arch	kubernetes.io/arch	<a href="#">Kubernetes</a>
beta.kubernetes.io/instance-type	node.kubernetes.io/instance-type	<a href="#">Kubernetes</a>
beta.kubernetes.io/os	kubernetes.io/os	<a href="#">Kubernetes</a>
node-role.kubernetes.io/agent*	kubernetes.azure.com/role=agent	Azure Kubernetes Service
kubernetes.io/role*	kubernetes.azure.com/role=agent	Azure Kubernetes Service
Agentpool*	kubernetes.azure.com/agentpool	Azure Kubernetes Service
Storageprofile*	kubernetes.azure.com/storageprofile	Azure Kubernetes Service

LABEL	RECOMMENDED SUBSTITUTE	MAINTAINER
StorageTier*	kubernetes.azure.com/storageTier	Azure Kubernetes Service
Accelerator*	kubernetes.azure.com/accelerator	Azure Kubernetes Service

\*Newly deprecated. For more information, see [Release Notes](#) on when these labels will no longer be maintained.

## Next steps

Learn more about Kubernetes labels at the [Kubernetes labels documentation](#).

# Overview of Microsoft Defender for Containers

10/27/2022 • 6 minutes to read • [Edit Online](#)

Microsoft Defender for Containers is the cloud-native solution that is used to secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications.

Defender for Containers assists you with the three core aspects of container security:

- **Environment hardening** - Defender for Containers protects your Kubernetes clusters whether they're running on Azure Kubernetes Service, Kubernetes on-premises/IaaS, or Amazon EKS. Defender for Containers continuously assesses clusters to provide visibility into misconfigurations and guidelines to help mitigate identified threats.
- **Vulnerability assessment** - Vulnerability assessment and management tools for images stored in ACR registries and running in Azure Kubernetes Service.
- **Run-time threat protection for nodes and clusters** - Threat protection for clusters and Linux nodes generates security alerts for suspicious activities.

You can learn more by watching this video from the Defender for Cloud in the Field video series: [Microsoft Defender for Containers](#).

## Microsoft Defender for Containers plan availability

ASPECT	DETAILS
Release state:	General availability (GA) Certain features are in preview, for a full list see the <a href="#">availability</a> section.
Feature availability	Refer to the <a href="#">availability</a> section for additional information on feature release state and availability.
Pricing:	<b>Microsoft Defender for Containers</b> is billed as shown on the <a href="#">pricing page</a>
Required roles and permissions:	<ul style="list-style-type: none"><li>• To deploy the required components, see the <a href="#">permissions for each of the components</a></li><li>• <b>Security admin</b> can dismiss alerts</li><li>• <b>Security reader</b> can view vulnerability assessment findings</li></ul> <p>See also <a href="#">Azure Container Registry roles and permissions</a></p>

ASPECT	DETAILS
Clouds:	<p><b>Azure:</b></p> <ul style="list-style-type: none"> <li>✓ Commercial clouds</li> <li>✓ National clouds (Azure Government, Azure China 21Vianet) (Except for preview features))</li> </ul> <p><b>Non-Azure:</b></p> <ul style="list-style-type: none"> <li>✓ Connected AWS accounts (Preview)</li> <li>✓ Connected GCP projects (Preview)</li> <li>✓ On-prem/IaaS supported via Arc enabled Kubernetes (Preview).</li> </ul> <p>For more information about, see the <a href="#">availability section</a>.</p>

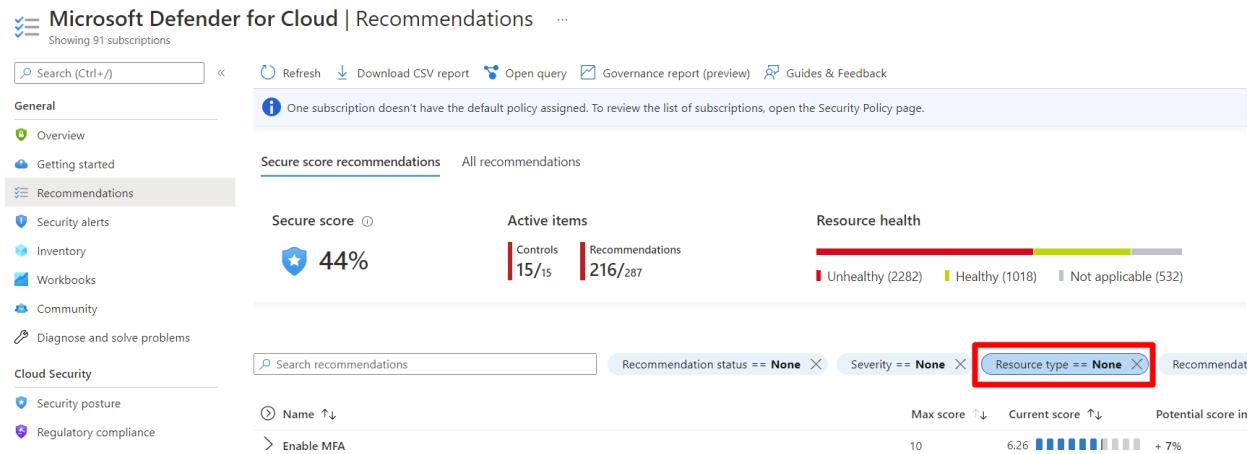
## Hardening

### Continuous monitoring of your Kubernetes clusters - wherever they're hosted

Defender for Cloud continuously assesses the configurations of your clusters and compares them with the initiatives applied to your subscriptions. When it finds misconfigurations, Defender for Cloud generates security recommendations that are available on Defender for Cloud's Recommendations page. The recommendations allow you to investigate and remediate issues. For details on the recommendations that might appear for this feature, check out the [compute section](#) of the recommendations reference table.

For Kubernetes clusters on EKS, you'll need to [connect your AWS account to Microsoft Defender for Cloud](#) and ensure you've enabled the CSPM plan.

You can use the resource filter to review the outstanding recommendations for your container-related resources, whether in asset inventory or the recommendations page:



The screenshot shows the Microsoft Defender for Cloud Recommendations page. The left sidebar includes sections for General, Recommendations (which is selected), Security alerts, Inventory, Workbooks, Community, and Diagnose and solve problems. Under Cloud Security, there are links for Security posture and Regulatory compliance. The main content area displays a secure score of 44%, 15/1s controls, 216/287 recommendations, and a resource health bar showing 2282 unhealthy, 1018 healthy, and 532 not applicable items. A search bar at the top allows filtering by recommendation status, severity, and resource type. The resource type filter is highlighted with a red box.

### Kubernetes data plane hardening

To protect the workloads of your Kubernetes containers with tailored recommendations, you can install the [Azure Policy for Kubernetes](#). Learn more about [monitoring components](#) for Defender for Cloud.

With the add-on on your AKS cluster, every request to the Kubernetes API server will be monitored against the predefined set of best practices before being persisted to the cluster. You can then configure it to enforce the best practices and mandate them for future workloads.

For example, you can mandate that privileged containers shouldn't be created, and any future requests to do so will be blocked.

You can learn more about [Kubernetes data plane hardening](#).

# Vulnerability assessment

## Scanning images in container registries

Defender for Containers scans the containers in Azure Container Registry (ACR) and Amazon AWS Elastic Container Registry (ECR) to notify you if there are known vulnerabilities in your images.

When you push an image to a container registry and while the image is stored in the container registry, Defender for Containers automatically scans it. Defender for Containers checks for known vulnerabilities in packages or dependencies defined in the image file.

When the scan completes, Defender for Containers provides details for each vulnerability detected, a security classification for each vulnerability detected, and guidance on how to remediate issues and protect vulnerable attack surfaces.

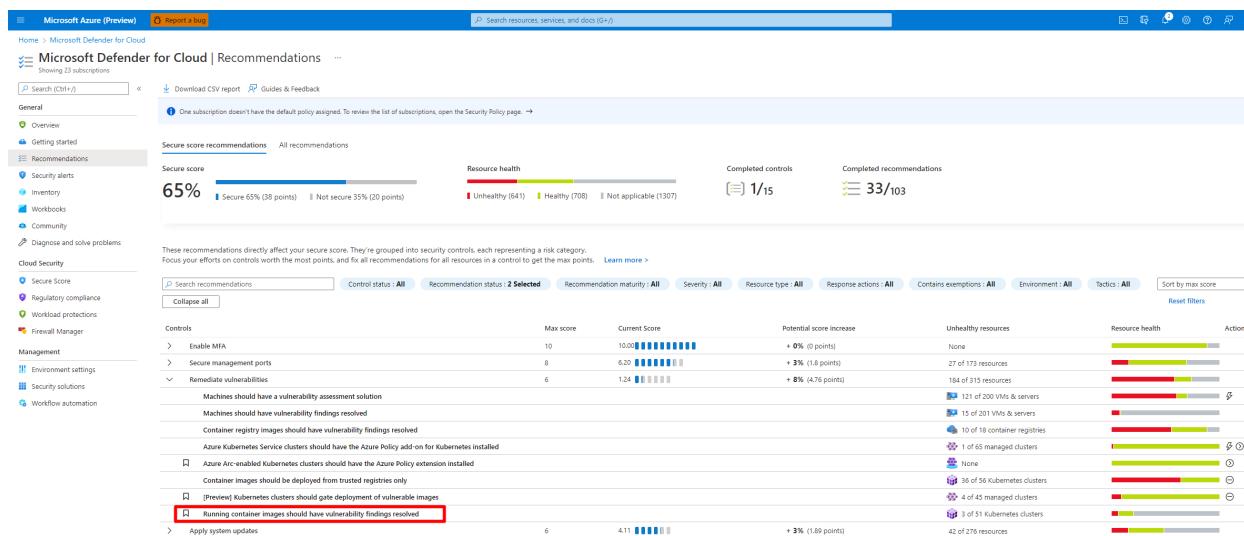
Learn more about:

- [Vulnerability assessment for Azure Container Registry \(ACR\)](#)
- [Vulnerability assessment for Amazon AWS Elastic Container Registry \(ECR\)](#)

## View vulnerabilities for running images in Azure Container Registry (ACR)

Defender for Cloud gives its customers the ability to prioritize the remediation of vulnerabilities in images that are currently being used within their environment using the [Running container images should have vulnerability findings resolved](#) recommendation.

To provide findings for the recommendation, Defender for Cloud collects the inventory of your running containers that are collected by the Defender agent installed on your AKS clusters. Defender for Cloud correlates that inventory with the vulnerability assessment scan of images that are stored in ACR. The recommendation shows your running containers with the vulnerabilities associated with the images that are used by each container and provides vulnerability reports and remediation steps.



Learn more about [viewing vulnerabilities for running images in \(ACR\)](#).

## Run-time protection for Kubernetes nodes and clusters

Defender for Containers provides real-time threat protection for your containerized environments and generates alerts for suspicious activities. You can use this information to quickly remediate security issues and improve the security of your containers. Threat protection at the cluster level is provided by the Defender agent and analysis of the Kubernetes audit logs. Examples of events at this level include exposed Kubernetes dashboards, creation of high-privileged roles, and the creation of sensitive mounts.

Defender for Containers also includes host-level threat detection with over 60 Kubernetes-aware analytics, AI,

and anomaly detections based on your runtime workload.

Defender for Cloud monitors the attack surface of multicloud Kubernetes deployments based on the [MITRE ATT&CK® matrix for Containers](#), a framework developed by the [Center for Threat-Informed Defense](#) in close partnership with Microsoft.

## FAQ - Defender for Containers

- [What are the options to enable the new plan at scale?](#)
- [Does Microsoft Defender for Containers support AKS clusters with virtual machines scale sets?](#)
- [Does Microsoft Defender for Containers support AKS without scale set \(default\)?](#)
- [Do I need to install the Log Analytics VM extension on my AKS nodes for security protection?](#)

### **What are the options to enable the new plan at scale?**

You can use the Azure Policy [Configure Microsoft Defender for Containers to be enabled](#), to enable Defender for Containers at scale. You can also see all of the options that are available to [enable Microsoft Defender for Containers](#).

### **Does Microsoft Defender for Containers support AKS clusters with virtual machines scale sets?**

Yes.

### **Does Microsoft Defender for Containers support AKS without scale set (default)?**

No. Only Azure Kubernetes Service (AKS) clusters that use virtual machine scale sets for the nodes is supported.

### **Do I need to install the Log Analytics VM extension on my AKS nodes for security protection?**

No, AKS is a managed service, and manipulation of the IaaS resources isn't supported. The Log Analytics VM extension isn't needed and may result in extra charges.

## Learn More

Learn more about Defender for Containers in the following blogs:

- [Introducing Microsoft Defender for Containers](#)
- [Demonstrating Microsoft Defender for Cloud](#)

The release state of Defender for Containers is broken down by two dimensions: environment and feature. So, for example:

- **Kubernetes data plane recommendations** for AKS clusters are GA
- **Kubernetes data plane recommendations** for EKS clusters are preview

To view the status of the full matrix of features and environments, see [Microsoft Defender for Containers feature availability](#).

## Next steps

In this overview, you learned about the core elements of container security in Microsoft Defender for Cloud. To enable the plan, see:

[Enable Defender for Containers](#)

# Enable Microsoft Defender for Containers

10/27/2022 • 27 minutes to read • [Edit Online](#)

Microsoft Defender for Containers is the cloud-native solution for securing your containers.

Defender for Containers protects your clusters whether they're running in:

- **Azure Kubernetes Service (AKS)** - Microsoft's managed service for developing, deploying, and managing containerized applications.
- **Amazon Elastic Kubernetes Service (EKS) in a connected Amazon Web Services (AWS) account** - Amazon's managed service for running Kubernetes on AWS without needing to install, operate, and maintain your own Kubernetes control plane or nodes.
- **Google Kubernetes Engine (GKE) in a connected Google Cloud Platform (GCP) project** - Google's managed environment for deploying, managing, and scaling applications using GCP infrastructure.
- **Other Kubernetes distributions** (using Azure Arc-enabled Kubernetes) - Cloud Native Computing Foundation (CNCF) certified Kubernetes clusters hosted on-premises or on IaaS. For more information, see the [On-prem/IaaS \(Arc\)](#) section of [Supported features by environment](#).

Learn about this plan in [Overview of Microsoft Defender for Containers](#).

You can learn more by watching these videos from the Defender for Cloud in the Field video series:

- [Microsoft Defender for Containers in a multi-cloud environment](#)
- [Protect Containers in GCP with Defender for Containers](#)

## NOTE

Defender for Containers' support for Arc-enabled Kubernetes clusters, AWS EKS, and GCP GKE. This is a preview feature.

To learn more about the supported operating systems, feature availability, outbound proxy and more see the [Defender for Containers feature availability](#).

## Network requirements - AKS

Validate the following endpoints are configured for outbound access so that the Defender profile can connect to Microsoft Defender for Cloud to send security data and events:

See the [required FQDN/application rules for Microsoft Defender for Containers](#).

By default, AKS clusters have unrestricted outbound (egress) internet access.

## Network requirements

Validate the following endpoints are configured for outbound access so that the Defender extension can connect to Microsoft Defender for Cloud to send security data and events:

For Azure public cloud deployments:

DOMAIN	PORT
*.ods.opinsights.azure.com	443
*.oms.opinsights.azure.com	443
login.microsoftonline.com	443

The following domains are only necessary if you're using a relevant OS. For example, if you have EKS clusters running in AWS, then you would only need to apply the

Amazon Linux 2 (Eks): Domain: "amazonlinux.\*.amazonaws.com/2/extras/\*" domain.

DOMAIN	PORT	HOST OPERATING SYSTEMS
amazonlinux.*.amazonaws.com/2/extras/*	443	Amazon Linux 2
yum default repositories	-	RHEL / Centos
apt default repositories	-	Debian

You'll also need to validate the [Azure Arc-enabled Kubernetes network requirements](#).

#### TIP

When using this extension with [AKS hybrid clusters provisioned from Azure](#) you must set `--cluster-type` to use `provisionedClusters` and also add `--cluster-resource-provider microsoft.hybridcontainerservice` to the command. Installing Azure Arc extensions on AKS hybrid clusters provisioned from Azure is currently in preview.

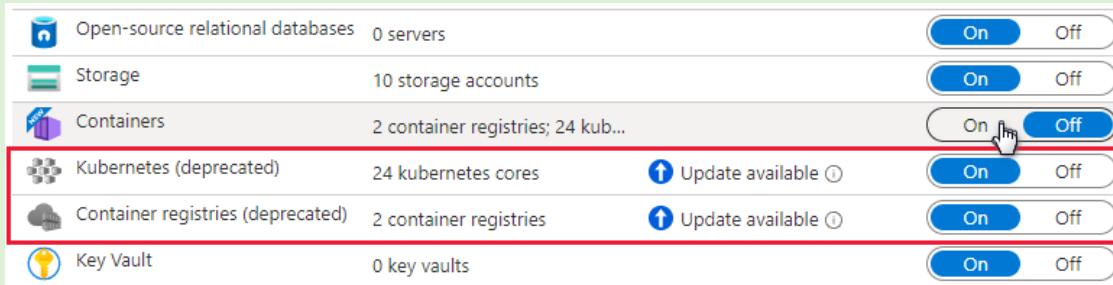
## Enable the plan

To enable the plan:

- From Defender for Cloud's menu, open the [Environment settings page](#) and select the relevant subscription.
- In the [Defender plans page](#), enable **Defender for Containers**

#### TIP

If the subscription already has Defender for Kubernetes and/or Defender for container registries enabled, an update notice is shown. Otherwise, the only option will be **Defender for Containers**.



- By default, when enabling the plan through the Azure portal, [Microsoft Defender for Containers](#) is configured to auto provision (automatically install) required components to provide the protections

offered by plan, including the assignment of a default workspace.

If you want to disable auto provisioning during the onboarding process, select **Edit configuration** for the **Containers** plan. This opens the Advanced options, where you can disable auto provisioning for each component.

In addition, you can modify this configuration from the [Defender plans page](#) or from the [Auto provisioning page](#) on the **Microsoft Defender for Containers** components row:

The screenshot shows the 'Settings | Auto provisioning' page for the 'Contoso' plan. On the left, there's a sidebar with 'Defender plans' (selected), 'Auto provisioning' (highlighted in red), 'Email notifications', 'Integrations', 'Workflow automation', 'Continuous export', 'Policy settings', and 'Security policy'. The main area is titled 'Auto provisioning - Extensions'. It lists several extensions with their status, resource count, and description. One extension, 'Microsoft Defender for Containers components (preview)', is highlighted with a red box. Its status is 'Off', it monitors '2 of 2 Kubernetes clusters', and its description says it 'Deploys Defender for Kubernetes components for environment hardening and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes workloads'. There are also 'Edit configuration' and 'Learn more' links.

#### NOTE

If you choose to **disable the plan** at any time after enabling it through the portal as shown above, you'll need to manually remove Defender for Containers components deployed on your clusters.

You can [assign a custom workspace](#) through Azure Policy.

4. If you disable the auto provisioning of any component, you can easily deploy the component to one or more clusters using the appropriate recommendation:

- Policy Add-on for Kubernetes - [Azure Kubernetes Service clusters should have the Azure Policy Add-on for Kubernetes installed](#)
- Azure Kubernetes Service profile - [Azure Kubernetes Service clusters should have Defender profile enabled](#)
- Azure Arc-enabled Kubernetes Defender extension - [Azure Arc-enabled Kubernetes clusters should have the Defender extension installed](#)
- Azure Arc-enabled Kubernetes Policy extension - [Azure Arc-enabled Kubernetes clusters should have the Azure Policy extension installed](#)

#### NOTE

Microsoft Defender for Containers is configured to defend all of your clouds automatically. When you install all of the required prerequisites and enable all of the auto provisioning capabilities.

If you choose to disable all of the auto provision configuration options, no agents, or components will be deployed to your clusters. Protection will be limited to the Agentless features only. Learn which features are Agentless in the [availability section](#) for Defender for Containers.

# Deploy the Defender profile

You can enable the Defender for Containers plan and deploy all of the relevant components from the Azure portal, the REST API, or with a Resource Manager template. For detailed steps, select the relevant tab.

Once the Defender profile has been deployed, a default workspace will be automatically assigned. You can [assign a custom workspace](#) in place of the default workspace through Azure Policy.

## NOTE

The Defender profile is deployed to each node to provide the runtime protections and collect signals from those nodes using [eBPF technology](#).

- [Azure portal](#)
- [REST API](#)
- [Azure CLI](#)
- [Resource Manager](#)

## Use the fix button from the Defender for Cloud recommendation

A streamlined, frictionless, process lets you use the Azure portal pages to enable the Defender for Cloud plan and setup auto provisioning of all the necessary components for defending your Kubernetes clusters at scale.

A dedicated Defender for Cloud recommendation provides:

- **Visibility** about which of your clusters has the Defender profile deployed
  - Fix button to deploy it to those clusters without the extension
1. From Microsoft Defender for Cloud's recommendations page, open the **Enable enhanced security** security control.
  2. Use the filter to find the recommendation named **Azure Kubernetes Service clusters should have Defender profile enabled**.

## TIP

Notice the Fix icon in the actions column

3. Select the clusters to see the details of the healthy and unhealthy resources - clusters with and without the profile.
4. From the unhealthy resources list, select a cluster and select **Remediate** to open the pane with the remediation confirmation.
5. Select **Fix X resources**.

## Enable the plan

To enable the plan:

1. From Defender for Cloud's menu, open the [Environment settings page](#) and select the relevant subscription.
2. In the [Defender plans page](#), enable **Defender for Containers**.

#### TIP

If the subscription already has Defender for Kubernetes or Defender for container registries enabled, an update notice is shown. Otherwise, the only option will be **Defender for Containers**.

	Open-source relational databases	0 servers	<button>On</button> <button>Off</button>
	Storage	10 storage accounts	<button>On</button> <button>Off</button>
	Containers	2 container registries; 24 kub...	<button>On</button> <span style="background-color: #e0e0e0;">Off</span>
	Kubernetes (deprecated)	24 kubernetes cores	<span style="background-color: #e0e0e0;">On</span> <button>Off</button> Update available ⓘ
	Container registries (deprecated)	2 container registries	<span style="background-color: #e0e0e0;">On</span> <button>Off</button> Update available ⓘ
	Key Vault	0 key vaults	<span style="background-color: #e0e0e0;">On</span> <button>Off</button>

3. By default, when enabling the plan through the Azure portal, **Microsoft Defender for Containers** is configured to auto provision (automatically install) required components to provide the protections offered by plan, including the assignment of a default workspace.

If you want to disable auto provisioning during the onboarding process, select **Edit configuration** for the **Containers** plan. The Advanced options will appear, and you can disable auto provisioning for each component.

In addition, you can modify this configuration from the **Defender plans page** or from the **Auto provisioning page** on the **Microsoft Defender for Containers components** row:

Settings | Auto provisioning ...

Contoso

Search (Ctrl+ /) Save

Auto provisioning - Extensions

Defender for Cloud collects security data and events from your resources and services to help you prevent, detect, and respond to threats. When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy. [Learn more](#)

Enable all extensions

Extension	Status	Resources missing extension	Description	Configuration
Log Analytics agent for Azure VMs	On	9 of 34 virtual machines	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. <a href="#">Learn more</a>	Selected workspace: ns Security events: Common <a href="#">Edit configuration</a>
Log Analytics agent for Azure Arc Machines (preview)	On	23 of 27 Azure Arc machines	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. <a href="#">Learn more</a>	Selected workspace: defaultwork <a href="#">Edit configuration</a>
Vulnerability assessment for machines	Off	40 of 57 VMs & servers	Enables vulnerability assessment on your Azure and hybrid machines. <a href="#">Learn more</a>	-
Guest Configuration agent (preview)	Off	3 of 34 virtual machines	Checks machines running in Azure and Arc Connected Machines for security misconfigurations. Settings such as configuration of the operating system, application configurations, and environment settings are all validated. To learn more, see <a href="#">Understand Azure Policy's Guest Configuration</a> .	-
Microsoft Dependency agent (preview)	On	10 of 33 virtual machines	You can collect and store network traffic data by onboarding to the VM Insights service. <a href="#">Learn more</a>	-
Microsoft Defender for Containers components (preview)	Off	2 of 2 Kubernetes clusters	Deploys Defender for Kubernetes components for environment hardening and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes workloads. <a href="#">Learn more</a>	-

#### NOTE

If you choose to **disable the plan** at any time after enabling it through the portal as shown above, you'll need to manually remove Defender for Containers components deployed on your clusters.

You can **assign a custom workspace** through Azure Policy.

4. If you disable the auto provisioning of any component, you can easily deploy the component to one or more clusters using the appropriate recommendation:
  - Policy Add-on for Kubernetes - **Azure Kubernetes Service clusters should have the Azure Policy Add-**

on for Kubernetes installed

- Azure Kubernetes Service profile - [Azure Kubernetes Service clusters should have Defender profile enabled](#)
- Azure Arc-enabled Kubernetes extension - [Azure Arc-enabled Kubernetes clusters should have the Defender extension installed](#)
- Azure Arc-enabled Kubernetes Policy extension - [Azure Arc-enabled Kubernetes clusters should have the Azure Policy extension installed](#)

## Prerequisites

Before deploying the extension, ensure you:

- [Connect the Kubernetes cluster to Azure Arc](#)
- Complete the [pre-requisites listed under the generic cluster extensions documentation](#).

## Deploy the Defender extension

You can deploy the Defender extension using a range of methods. For detailed steps, select the relevant tab.

- [Azure portal](#)
- [Azure CLI](#)
- [Resource Manager](#)
- [REST API](#)

### Use the fix button from the Defender for Cloud recommendation

A dedicated Defender for Cloud recommendation provides:

- **Visibility** about which of your clusters has the Defender for Kubernetes extension deployed
- Fix button to deploy it to those clusters without the extension

1. From Microsoft Defender for Cloud's recommendations page, open the **Enable enhanced security** security control.
2. Use the filter to find the recommendation named **Azure Arc-enabled Kubernetes clusters should have Defender for Cloud's extension installed**.

The screenshot shows the Microsoft Defender for Cloud Recommendations page. The left sidebar has a 'Recommendations' section with various categories like Overview, Getting started, and Workbooks. The main area displays a recommendation titled 'Enable Azure Defender'. A red box highlights the 'Actions' column for this recommendation, specifically the 'Quick fix' button. The status bar at the bottom indicates '2 Selected' recommendations.

#### TIP

Notice the Fix icon in the actions column

3. Select the extension to see the details of the healthy and unhealthy resources - clusters with and without the extension.

4. From the unhealthy resources list, select a cluster and select **Remediate** to open the pane with the remediation options.

5. Select the relevant Log Analytics workspace and select **Remediate x resource**.

The screenshot shows the Azure Security Center remediation pane. At the top, it displays a navigation bar with 'Dashboard > Security Center >' followed by the title 'Azure Arc enabled Kubernetes clusters should have Azure Defender's extension ins...'. Below the title are three buttons: 'Exempt', 'View policy definition', and 'Open query'. The pane is divided into sections: 'Severity' (High), 'Freshness interval' (30 Min), 'Description' (explaining the extension's threat protection), 'Remediation steps' (collapsed), 'Affected resources' (listing 'Unhealthy resources (2)', 'Healthy resources (2)', and 'Not applicable resources (0)'). A table lists two clusters: 'k8s\_arc\_demo' (Subscription: ASC DEMO) and 'asc-arc-k8s-demo' (Subscription: ProdTest2). At the bottom, there are buttons for 'Remediate' (which is highlighted in blue), 'Trigger logic app', and 'Exempt'. A feedback section asks 'Was this recommendation useful?' with 'Yes' and 'No' radio buttons.

## Verify the deployment

To verify that your cluster has the Defender extension installed on it, follow the steps in one of the tabs below:

- [Azure portal - Defender for Cloud](#)
- [Azure portal - Azure Arc](#)
- [Azure CLI](#)
- [REST API](#)

### Use Defender for Cloud recommendation to verify the status of your extension

1. From Microsoft Defender for Cloud's recommendations page, open the **Enable Microsoft Defender for Cloud** security control.
2. Select the recommendation named **Azure Arc-enabled Kubernetes clusters should have Microsoft Defender for Cloud's extension installed**.

The screenshot shows the Microsoft Defender for Cloud Recommendations page. On the left, there's a navigation sidebar with links like General, Overview, Getting started, Recommendations (which is selected), Security alerts, Inventory, Workbooks, Community, and Cloud Security. The main area has a search bar, a download CSV report button, and a guides & feedback link. A message says: "Each security control below represents a security risk you should mitigate. Address the recommendations in each control, focusing on the controls worth the most points. To get the max score, fix all recommendations for all resources in a control." Below this is a table with columns: Controls, Unhealthy resources, Resource health, and Actions. One row is highlighted with a red box: "Enable Azure Defender" with the sub-note "Azure Arc enabled Kubernetes clusters should have Microsoft Defender's extension enabled". The "Resource health" column shows a progress bar for 8 of 25 resources, and the "Actions" column has a "Quick fix" button.

- Check that the cluster on which you deployed the extension is listed as **Healthy**.

## Protect Amazon Elastic Kubernetes Service clusters

### IMPORTANT

If you haven't already connected an AWS account, [connect your AWS accounts to Microsoft Defender for Cloud](#).

To protect your EKS clusters, enable the Containers plan on the relevant account connector:

- From Defender for Cloud's menu, open **Environment settings**.
- Select the AWS connector.

The screenshot shows the Microsoft Defender for Cloud Environment settings page. The left sidebar includes General, Overview, Getting started, Recommendations (selected), Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems, Cloud Security (Secure Score, Regulatory compliance, Workload protections, Firewall Manager), Management, and Environment settings (which is selected and highlighted with a red box). The main area displays Azure subscriptions (74) and AWS accounts (7). Below is a table with columns: Name, Total resources, Defender coverage, and Standards. It lists Azure subscriptions (22) and AWS accounts (2). An AWS account named "ContosoConnector" is selected and highlighted with a red box. The table also shows "2/3 plans" and "AWS CIS 1.2.0 (preview)".

- Set the toggle for the **Containers** plan to **On**.

The screenshot shows the configuration page for the Containers plan. It includes a description: "Provides real-time threat protection for the EKS clusters and generates alerts for suspicious activity." There are two checkboxes: "Audit logs enabled" (checked) and "Will incur additional AWS costs" (unchecked). Below these are "Free (preview)" and "Configure" buttons. To the right is a toggle switch with "On" and "Off" options, where "On" is highlighted with a red box.

- (Optional) To change the retention period for your audit logs, select **Configure**, enter the required timeframe, and select **Save**.

Kubernetes audit logs to Microsoft Defender  On

Control plane audit logs will be sent from the EKS control plane to your account's CloudWatch logs. S3, Kinesis, and SQS resources will also be created.

Audit logs enabled  Will incur additional AWS costs  Configure >

Retention period (days) \*

For details of the costs involved, see the pricing pages for CloudWatch, S3, Kinesis, and SQS.

#### NOTE

If you disable this configuration, then the Threat detection (control plane) feature will be disabled. Learn more about [features availability](#).

5. (Optional) Enable vulnerability scanning of your ECR images. Learn more about [vulnerability assessment for ECR images](#).

6. Continue through the remaining pages of the connector wizard.

7. Azure Arc-enabled Kubernetes, the Defender extension, and the Azure Policy extension should be installed and running on your EKS clusters. There is a dedicated Defender for Cloud recommendations to install these extensions (and Azure Arc if necessary):

- EKS clusters should have Microsoft Defender's extension for Azure Arc installed

For each of the recommendations, follow the steps below to install the required extensions.

#### To install the required extensions:

a. From Defender for Cloud's [Recommendations](#) page, search for one of the recommendations by name.

b. Select an unhealthy cluster.

#### IMPORTANT

You must select the clusters one at a time.

Don't select the clusters by their hyperlinked names: select anywhere else in the relevant row.

c. Select Fix.

d. Defender for Cloud generates a script in the language of your choice: select Bash (for Linux) or PowerShell (for Windows).

e. Select [Download remediation logic](#).

f. Run the generated script on your cluster.

g. Repeat steps "a" through "f" for the second recommendation.

## EKS clusters should have Azure Defender's extension for Azure Arc installed

[Open query](#)

Severity: **High** Freshness interval: **6 Hours**

**Select the row; not the resource's name**

**Affected resources**

Unhealthy resources (7) Healthy resources (4) Not applicable resources (0)

Name	AWS Account	Connector name	Region	Resource type	Subscription
policy-addon-cluster-us-w	102614528198	securityConnector	us-west-2	AWS EKS Cluster	ASC DEMO

[Fix](#) [Trigger logic app](#)

Was this recommendation useful?  Yes  No

### View recommendations and alerts for your EKS clusters

**TIP**

You can simulate container alerts by following the instructions in [this blog post](#).

To view the alerts and recommendations for your EKS clusters, use the filters on the alerts, recommendations, and inventory pages to filter by resource type **AWS EKS cluster**.

Dashboard > Microsoft Defender for Cloud

**Microsoft Defender for Cloud | Security alerts** Showing 74 subscriptions

1. **Security alerts**

2. **Active alerts by severity**

3. **Filter**: Resource type = AWS EKS Cluster

4. **AWS EKS Cluster** selected

5. **OK**

Alert details:

Severity	Alert title	Affected resource
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	E2EClusterARC-Stable
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	E2EClusterARC-Stable
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	E2EClusterARC-Stable
High	Malicious credential theft tool execution detected	CH1-VictimVM00
High	Malicious credential theft tool execution detected	CH1-VICTIMVM-Dev
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	E2EClusterARC-Stable
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	E2EClusterARC-Stable
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	E2EClusterARC-Stable
High	Malicious credential theft tool execution detected	CH1-VictimVM00
High	Malicious credential theft tool execution detected	CH1-VICTIMVM-Dev
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	E2EClusterARC-Stable
High	Microsoft Defender for Cloud test alert for K8S (not a threat) (Preview)	E2EClusterARC-Stable

# Protect Google Kubernetes Engine (GKE) clusters

## IMPORTANT

If you haven't already connected a GCP project, [connect your GCP projects to Microsoft Defender for Cloud](#).

To protect your GKE clusters, you'll need to enable the Containers plan on the relevant GCP project.

**To protect Google Kubernetes Engine (GKE) clusters:**

1. Sign in to the [Azure portal](#).
2. Navigate to Microsoft Defender for Cloud > Environment settings.
3. Select the relevant GCP connector

The screenshot shows the Microsoft Defender for Cloud interface. At the top, there's a navigation bar with 'Microsoft Azure (Preview)' and a 'Report a bug' button. Below it, a breadcrumb trail shows 'Home > Microsoft Defender for Cloud'. The main area has a title 'Microsoft Defender for Cloud | Environment' and a subtitle 'Showing subscription'. On the left, a sidebar lists various sections like General, Overview, Getting started, Recommendations, Security alerts, Inventory, Workbooks, Community, and Diagnose and solve problems. In the center, there's a summary section with a cloud icon and the number '1' labeled 'Azure subscriptions'. A message box says 'Welcome to the new multi-cloud'. Below this, there's a search bar and a 'Expand all' button. The main list shows 'Name ↑' followed by 'Azure', 'AWS (preview)', and 'GCP (preview)'. Under 'GCP (preview)', the item 'Containers-GCP' is highlighted with a red box around it.

4. Select the **Next: Select plans >** button.
  5. Ensure that the Containers plan is toggled to **On**.
- 
- The screenshot shows the 'Containers' plan configuration page. It includes a description of what the plan does, a status indicator 'Partially configured: 2 / 3 Configure >', and a toggle switch labeled 'On' which is highlighted with a red box. There are also 'Free (preview)' and 'Will incur GCP costs.' links.
6. (Optional) [Configure the containers plan](#).
  7. Select the **Copy** button.

### Copy script to GCP Cloud Shell

A Cloud Shell template to configure access on GCP side has been created according to the plans selected in the previous tab.

```
Enable APIs
gcloud services enable iam.googleapis.com sts.googleapis.com clouresourcemanager.googleapis.com iamcredentials.googleapis.com
Create CSPM service account reader role
gcloud iam service-accounts create microsoft-defender-cspm \
--display-name="Microsoft Defender CSPM"
gcloud projects add-iam-policy-binding 332211654987 \
--member="serviceAccount:microsoft-defender-cspm@332211654987.iam.gserviceaccount.com" \
--role="roles/viewer"
Create MDPC identity federation
gcloud iam workload-identity-pools create microsoft-defender-for-cloud \
--location="global" --display-name="microsoft defender for cloud" \
--description="MicrosoftDefenderForCloud"
gcloud iam service-accounts add-iam-policy-binding microsoft-defender-cspm@332211654987.iam.gserviceaccount.com \
--role=roles/iam.workloadIdentityUser \
--member="principalSet://iam.googleapis.com/projects/112233456789/locations/global/workloadIdentityPools/microsoft-defender-for-cloud/*"
Create CSPM identity pool
gcloud iam workload-identity-pools providers create-oidc cspm \
--location="global" --workload-identity-pool="microsoft-defender-for-cloud" \
--issuer-uri="https://sts.windows.net/33e01921-4d64-4f8c-a055-5bdaffd5e33d" \
--allowed-audiences="api://6e81e733-9e7f-474a-85f0-385c097ff1f2" \
--attribute-mapping="google.subject=assertion.sub"
```

Copy

[GCP Cloud Shell >](#)

8. Select the **GCP Cloud Shell >** button.

9. Paste the script into the Cloud Shell terminal, and run it.

The connector will update after the script executes. This process can take up to 6-8 hours up to complete.

### Deploy the solution to specific clusters

If you disabled any of the default auto provisioning configurations to Off, during the [GCP connector onboarding process](#), or afterwards. You'll need to manually install Azure Arc-enabled Kubernetes, the Defender extension, and the Azure Policy extensions to each of your GKE clusters to get the full security value out of Defender for Containers.

There are 2 dedicated Defender for Cloud recommendations you can use to install the extensions (and Arc if necessary):

- GKE clusters should have Microsoft Defender's extension for Azure Arc installed
- GKE clusters should have the Azure Policy extension installed

### To deploy the solution to specific clusters:

1. Sign in to the [Azure portal](#).
2. Navigate to **Microsoft Defender for Cloud > Recommendations**.
3. From Defender for Cloud's **Recommendations** page, search for one of the recommendations by name.

The screenshot shows the Microsoft Defender for Cloud Recommendations page. On the left, a sidebar menu includes General, Recommendations (selected), Security alerts, Inventory, Workbooks, Community, and Diagnose and solve problems. Under Cloud Security, it lists Secure Score, Regulatory compliance, Workload protections, and Firewall Manager. Under Management, it lists Environment settings, Security solutions, and Workflow automation. The main content area displays a Secure score of 69% (Secure 69% (40 points) / Not secure 31% (18 points)), Resource health (Unhealthy (677) / Healthy (538) / Not applicable (839)), and Completed controls (1/15). Below these are sections for Secure score recommendations and Completed recommendations (38/116). A detailed table follows, showing recommendations for GKE clusters, filtered by Control status: All, Recommendation status: 2 Selected, and Resource type: All. The table columns include Controls, Max score, Current Score, Potential score increase, Unhealthy resources, Resource health, and Actions. One row is expanded to show 'Enable enhanced security features' and 'GKE clusters should have Microsoft Defender's extens...'.

4. Select an unhealthy GKE cluster.

**IMPORTANT**

You must select the clusters one at a time.

Don't select the clusters by their hyperlinked names: select anywhere else in the relevant row.

5. Select the name of the unhealthy resource.

6. Select Fix.

## GKE clusters should have Microsoft Defender protection

 Open query

Severity

High

Freshness interval



6 Hours

### Description

Microsoft Defender's [cluster extension](#) provides security capabilities for your GKE clusters. The extension works with Azure Arc-enabled Kubernetes. Learn more about [Microsoft Defender for Cloud's security features](#).

### Remediation steps

### Affected resources

[Unhealthy resources \(4\)](#)    [Healthy resources \(5\)](#)

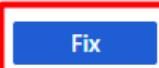
 [Search GCP resources](#)

Name

 [protected-demo](#)

 [gke-vanilla](#)

 [gke-protected](#)

 [Fix](#)

[Trigger logic app](#)

7. Defender for Cloud will generate a script in the language of your choice:

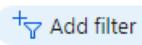
- For Linux, select **Bash**.
- For Windows, select **PowerShell**.

8. Select **Download remediation logic**.

9. Run the generated script on your cluster.

10. Repeat steps *3 through 8* for the second recommendation.

## View your GKE cluster alerts

1. Sign in to the [Azure portal](#).
2. Navigate to **Microsoft Defender for Cloud > Security alerts**.
3. Select the  [button](#).
4. In the Filter dropdown menu, select **Resource type**.
5. In the Value dropdown menu, select **GCP GKE Cluster**.
6. Select **Ok**.

# Simulate security alerts from Microsoft Defender for Containers

A full list of supported alerts is available in the [reference table of all Defender for Cloud security alerts](#).

1. To simulate a security alert, run the following command from the cluster:

```
kubectl get pods --namespace=asc-alerttest-662jfi039n
```

The expected response is "No resource found".

Within 30 minutes, Defender for Cloud will detect this activity and trigger a security alert.

2. In the Azure portal, open Microsoft Defender for Cloud's security alerts page and look for the alert on the relevant resource:

The screenshot shows the Microsoft Defender for Cloud Security alerts page. The left sidebar has a 'Security alerts' section selected. The main area displays a summary of 687 active alerts and 39 affected resources. A chart titled 'Active alerts by severity' shows the distribution of alerts across High (54), Medium (528), and Low (105) severity levels. Below the summary, a table lists individual alerts with columns for Severity, Alert title, Affected resource, Activity start time, and MITRE ATT&CK tactics. One specific alert is highlighted: 'New container in the kube-system namespace detected'. The details pane on the right provides a detailed description of this alert, stating it was detected via Kubernetes audit log analysis. It notes that a new container was found in the kube-system namespace, which typically contains system components like kubelet and kube-proxy. Attackers can use this namespace for hiding malicious components. The affected resource is listed as 'ASC-Arc-K8S-demo' under 'Affected resource'.

## Remove the Defender extension

To remove this - or any - Defender for Cloud extension, it's not enough to turn off auto provisioning:

- Enabling auto provisioning, potentially impacts *existing* and *future* machines.
- Disabling auto provisioning for an extension, only affects the *future* machines - nothing is uninstalled by disabling auto provisioning.

Nevertheless, to ensure the Defender for Containers components aren't automatically provisioned to your resources from now on, disable auto provisioning of the extensions as explained in [Configure auto provisioning for agents and extensions from Microsoft Defender for Cloud](#).

You can remove the extension using Azure portal, Azure CLI, or REST API as explained in the tabs below.

- [Azure portal - Arc](#)
- [Azure CLI](#)
- [REST API](#)

### Use Azure portal to remove the extension

1. From the Azure portal, open Azure Arc.
2. From the infrastructure list, select **Kubernetes clusters** and then select the specific cluster.

3. Open the extensions page. The extensions on the cluster are listed.

4. Select the cluster and select **Uninstall**.

The screenshot shows the 'Extensions (preview)' page for a cluster named 'ASC-Arc-K8S-Demo'. The 'Uninstall' button is highlighted with a red box. Below it, a note says: 'To view the list of available extensions and to install new extensions on your cluster, visit [Extensions for Azure Arc enabled Kubernetes](#).<sup>1</sup>'

Name	Type	Version	Install status	Auto upgrade minor version
microsoft.azuredefender.kubernetes	microsoft.azuredefender.kubernetes	0.4.61	Installed	Enabled

## Default Log Analytics workspace for AKS

The Log Analytics workspace is used by the Defender profile as a data pipeline to send data from the cluster to Defender for Cloud without retaining any data in the Log Analytics workspace itself. As a result, users won't be billed in this use case.

The Defender profile uses a default Log Analytics workspace. If you don't already have a default Log Analytics workspace, Defender for Cloud will create a new resource group and default workspace when the Defender profile is installed. The default workspace is created based on your [region](#).

The naming convention for the default Log Analytics workspace and resource group is:

- **Workspace:** DefaultWorkspace-[subscription-ID]-[geo]
- **Resource Group:** DefaultResourceGroup-[geo]

### Assign a custom workspace

When you enable the auto-provision option, a default workspace will be automatically assigned. You can assign a custom workspace through Azure Policy.

#### To check if you have a workspace assigned:

1. Sign in to the [Azure portal](#).

2. Search for and select **Policy**.

The screenshot shows the Azure portal search results for 'policy'. The 'Policy' item is highlighted with a red box. Other items shown include 'Time Series Insights access policies' and 'Application security groups'.

3. Select **Definitions**.

4. Search for policy ID `64def556-fbad-4622-930e-72d1d5589bf5`.

The screenshot shows the 'Policy | Definitions' page. The search bar contains the policy ID `64def556-fbad-4622-930e-72d1d5589bf5`. The 'Definitions' link in the left sidebar is highlighted with a red box.

5. Select **Configure Azure Kubernetes Service clusters to enable Defender profile**.

6. Select **Assignment**.

Home > Policy >

### Configure Azure Kubernetes Service clusters to enable Defender profile

Policy definition

Assign Edit definition Duplicate definition Delete definition Export definition

Essentials

Name : Configure Azure Kubernetes Service clusters to enable Defender profile  
Description : Microsoft Defender for Containers provides cloud-native Kubernetes security capabilities including environment hardening, workload protection, ...  
Available Effects : DeployIfNotExists, Disabled  
Category : Kubernetes

Definition Assignments (2) Parameters

Only 10 scopes are pre-selected.

Scope 10 selected Search Filter by name or ID...

name	Scope
Defender for Containers provisioning AKS Security Profile	DEMO
Defender for Containers provisioning AKS Security Profile	Sample

7. Follow the [Create a new assignment with custom workspace](#) steps if the policy hasn't yet been assigned to the relevant scope. Or, follow the [Update assignment with custom workspace](#) steps if the policy is already assigned and you want to change it to use a custom workspace.

#### Create a new assignment with custom workspace

If the policy hasn't been assigned, you'll see **Assignments (0)**.

Home > Policy >

### [Preview]: Configure Azure Kubernetes Service clusters to enable Defender profile

Policy definition

Assign Edit definition Duplicate definition Delete definition Export definition

Essentials

Name : [Preview]: Configure Azure Kubernetes Service clusters to enable Defender profile  
Description : Microsoft Defender for Containers provides cloud-native Kubernetes security capabilities including environment hardening, workload protection, ...  
Available Effects : DeployIfNotExists, Disabled  
Category : Kubernetes

Definition Assignments (0) Parameters

To assign custom workspace:

1. Select **Assign**.
2. In the **Parameters** tab, deselect the **Only show parameters that need input or review** option.
3. Select a LogAnalyticsWorkspaceResource ID from the dropdown menu.

Home > Policy > [Preview]: Configure Azure Kubernetes Service clusters to enable Defender profile > Defender for Containers provisioning AKS Security Profile >

### Defender for Containers provisioning AKS Security Profile

Basics Parameters Remediation Non-compliance messages Review + save

LogAnalyticsWorkspaceResource  Only show parameters that need input or review

LogAnalyticsWorkspaceResourceId

4. Select **Review + create**.

## 5. Select **Create**.

### Update assignment with custom workspace

If the policy has already been assigned to a workspace, you'll see **Assignments (1)**.

Home > Policy >

## [Preview]: Configure Azure Kubernetes Service clusters to enable Defender profile

Policy definition

Assign Edit definition Duplicate definition Delete definition Export definition

Essentials

Name : [Preview]: Configure Azure Kubernetes Service clusters to enable Defender profile

Description : Microsoft Defender for Containers provides cloud-native Kubernetes security capabilities including environment hardening, workload protection, and threat detection.

Available Effects : DeployIfNotExists, Disabled

Category : Kubernetes

Microsoft Defender run-time protection cluster to collect security data from your Kubernetes environment.

Definition Assignments (1) Parameters

1 { "protection": { "type": "Container", "logAnalyticsWorkspaceResource": "ASC DEMO" } }

**NOTE**

If you have more than one subscription the number may be higher.

### To assign custom workspace:

#### 1. Select the relevant assignment.

Home > Policy > [Preview]: Configure Azure Kubernetes Service clusters to enable Defender profile

Only 10 scopes are pre-selected.

Definition Assignments (1) Parameters

Scope	Search	Assigned by
10 selected	Filter by name or ID...	ASC DEMO
name		
* Defender for Containers provisioning AKS Security Profile		

#### 2. Select **Edit assignment**.

#### 3. In the **Parameters** tab, deselect the **Only show parameters that need input or review** option.

#### 4. Select a LogAnalyticsWorkspaceResource ID from the dropdown menu.

Home > Policy > [Preview]: Configure Azure Kubernetes Service clusters to enable Defender profile > Defender for Containers provisioning AKS Security Profile

LogAnalyticsWorkspaceResource

LogAnalyticsWorkspaceResourceId

#### 5. Select **Review + create**.

#### 6. Select **Create**.

# Default Log Analytics workspace for Arc

The Log Analytics workspace is used by the Defender extension as a data pipeline to send data from the cluster to Defender for Cloud without retaining any data in the Log Analytics workspace itself. As a result, users won't be billed in this use case.

The Defender extension uses a default Log Analytics workspace. If you don't already have a default Log Analytics workspace, Defender for Cloud will create a new resource group and default workspace when the Defender extension is installed. The default workspace is created based on your [region](#).

The naming convention for the default Log Analytics workspace and resource group is:

- **Workspace:** DefaultWorkspace-[subscription-ID]-[geo]
- **Resource Group:** DefaultResourceGroup-[geo]

## Assign a custom workspace

When you enable the auto-provision option, a default workspace will be automatically assigned. You can assign a custom workspace through Azure Policy.

### To check if you have a workspace assigned:

1. Sign in to the [Azure portal](#).
2. Search for, and select Policy.

A screenshot of the Microsoft Azure (Preview) portal. The top navigation bar shows 'Microsoft Azure (Preview)' and a search bar with 'policy'. Below the navigation is the 'Azure services' blade, which includes a 'Create a resource' button and a 'Policy' item highlighted with a red box. Other items in the blade include 'Services' (with a red box around it), 'Azure Active Directory (39)', 'Firewall Policies', and 'Time Series Insights access policies' and 'Application security groups'.

3. Select Definitions.

4. Search for policy ID `708b60a6-d253-4fe0-9114-4be4c00f012c`.

A screenshot of the 'Policy | Definitions' page in the Azure portal. The left sidebar shows 'Overview', 'Getting started', 'Compliance', 'Remediation', 'Events', 'Authoring' (with 'Definitions' selected and highlighted with a red box), 'Assignments', and 'Exemptions'. The main area has a search bar with '708b60a6-d253-4fe0-9114-4be4...' and a table with columns 'Name ↑', 'Definition location ↑', and 'Policies ↑'. One row in the table is visible, titled 'Configure Azure Arc enabled Kubernetes clusters to install M...'. The table also includes a 'Scope' dropdown set to '53 selected'.

5. Select **Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension..**

6. Select **Assignments**.

Home > Policy >

## Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension

Policy definition

[Assign](#) [Edit definition](#) [Duplicate definition](#) [Delete definition](#) [Export definition](#)

[Essentials](#)

Name	: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension	Definition location	: --
Description	: Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects ...	Definition ID	: /providers
Available Effects	: DeployIfExists, Disabled	Type	: Built-in
Category	: Kubernetes	Mode	: Indexed

Definition [Assignments \(2\)](#) Parameters

**Only 10 scopes are pre-selected.**

Scope  [...](#) Search

name	Scope
Defender for Containers provisioning ARC k8s Enabled	DEMO
Defender for Containers provisioning ARC k8s Enabled	Sample

- Follow the [Create a new assignment with custom workspace](#) steps if the policy hasn't yet been assigned to the relevant scope. Or, follow the [Update assignment with custom workspace](#) steps if the policy is already assigned and you want to change it to use a custom workspace.

#### Create a new assignment with custom workspace

If the policy hasn't been assigned, you'll see [Assignments \(0\)](#).

Home > Policy >

## [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension

Policy definition

[Assign](#) [Edit definition](#) [Duplicate definition](#) [Delete definition](#) [Export definition](#)

[Essentials](#)

Name	: [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension
Description	: Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects ...
Available Effects	: DeployIfExists, Disabled
Category	: Kubernetes

Definition [Assignments \(0\)](#) Parameters

#### To assign custom workspace:

- Select **Assign**.
- In the **Parameters** tab, deselect the **Only show parameters that need input or review** option.
- Select a LogAnalyticsWorkspaceResource ID from the dropdown menu.

Home > Policy > [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension >

## [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension

Basics [Parameters](#) Remediation Non-compliance messages Review + create

Search by parameter name   Only show parameters that need input or review

Effect **\***  DeployIfExists  LogAnalyticsWorkspaceResourceId  ExcludedDistributions  [ "aks", "aks\_management", "eks", "gke" ]

- Select **Review + create**.
- Select **Create**.

## Update assignment with custom workspace

If the policy has already been assigned to a workspace, you'll see [Assignments \(1\)](#).

### NOTE

If you have more than one subscription the number may be higher. If you have a number 1 or higher, the assignment may still not be on the relevant scope. If this is the case, you will want to follow the [Create a new assignment with custom workspace](#) steps.

## [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension

Policy definition

[Assign](#) [Edit definition](#) [Duplicate definition](#) [Delete definition](#) [Export definition](#)

^ Essentials

Name	: [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension	Definition location	: --
Description	: Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects ...	Definition ID	: /providers/
Available Effects	: DeployIfNotExists, Disabled	Type	: Built-in
Category	: Kubernetes	Mode	: Indexed

Definition [Assignments \(1\)](#) Parameters

### To assign custom workspace:

1. Select the relevant assignment.

Home > Policy >

## [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension

Policy definition

[Assign](#) [Edit definition](#) [Duplicate definition](#) [Delete definition](#) [Export definition](#)

^ Essentials

Name	: [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension	Definition location	: --
Description	: Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects ...	Definition ID	: /provider
Available Effects	: DeployIfNotExists, Disabled	Type	: Built-in
Category	: Kubernetes	Mode	: Indexed

Definition [Assignments \(1\)](#) Parameters

i Only 10 scopes are pre-selected.

Scope	Search
10 selected	Filter by name or ID...

name Scope

<a href="#">Defender for Containers provisioning ARC k8s Enabled</a>	DEMO
----------------------------------------------------------------------	------

2. Select Edit assignment.

3. In the Parameters tab, deselect the **Only show parameters that need input or review** option.

4. Select a LogAnalyticsWorkspaceResource ID from the dropdown menu.

Home > Policy > [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension >

## [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension

... [Edit](#) [Delete](#) [View history](#) [View details](#)

Basics [Parameters](#) Remediation Non-compliance messages Review + create

Search by parameter name  Only show parameters that need input or review

Effect \* [DeployIfNotExists](#)

LogAnalyticsWorkspaceResourceId [Select](#)

ExcludedDistributions \* [aks, aks\\_management, eks, gke](#) [Select](#)

5. Select **Review + create**.

6. Select **Create**.

## Remove the Defender profile

To remove this - or any - Defender for Cloud extension, it's not enough to turn off auto provisioning:

- **Enabling** auto provisioning, potentially impacts *existing* and *future* machines.
- **Disabling** auto provisioning for an extension, only affects the *future* machines - nothing is uninstalled by disabling auto provisioning.

Nevertheless, to ensure the Defender for Containers components aren't automatically provisioned to your resources from now on, disable auto provisioning of the extensions as explained in [Configure auto provisioning for agents and extensions from Microsoft Defender for Cloud](#).

You can remove the profile using the REST API or a Resource Manager template as explained in the tabs below.

- [REST API](#)
- [Azure CLI](#)
- [Resource Manager](#)

### Use REST API to remove the Defender profile from AKS

To remove the profile using the REST API, run the following PUT command:

```
https://management.azure.com/subscriptions/{{SubscriptionId}}/resourcegroups/{{ResourceGroup}}/providers/Microsoft.ContainerService/managedClusters/{{ClusterName}}?api-version={{ApiVersion}}
```

NAME	DESCRIPTION	MANDATORY
SubscriptionId	Cluster's subscription ID	Yes
ResourceGroup	Cluster's resource group	Yes
ClusterName	Cluster's name	Yes
ApiVersion	API version, must be >= 2022-06-01	Yes

Request body:

```
{
 "location": "{{Location}}",
 "properties": {
 "securityProfile": {
 "defender": {
 "securityMonitoring": {
 "enabled": false
 }
 }
 }
 }
}
```

Request body parameters:

Name	Description	Mandatory
location	Cluster's location	Yes
properties.securityProfile.defender.securityMonitoring.enabled	Determines whether to enable or disable Microsoft Defender for Containers on the cluster	Yes

## FAQ

- [How can I use my existing Log Analytics workspace?](#)
- [Can I delete the default workspaces created by Defender for Cloud?](#)
- [I deleted my default workspace, how can I get it back?](#)
- [Where is the default Log Analytics workspace located?](#)
- [My organization requires me to tag my resources, and required extension didn't get installed, what went wrong?](#)

### How can I use my existing Log Analytics workspace?

You can use your existing Log Analytics workspace by following the steps in the [Assign a custom workspace](#) workspace section of this article.

### Can I delete the default workspaces created by Defender for Cloud?

We don't recommend deleting the default workspace. Defender for Containers uses the default workspaces to collect security data from your clusters. Defender for Containers will be unable to collect data, and some security recommendations and alerts, will become unavailable if you delete the default workspace.

### I deleted my default workspace, how can I get it back?

To recover your default workspace, you need to remove the Defender profile/extension, and reinstall the agent. Reinstalling the Defender profile/extension creates a new default workspace.

### Where is the default Log Analytics workspace located?

Depending on your region, the default Log Analytics workspace located will be located in various locations. To check your region see [Where is the default Log Analytics workspace created?](#)

### My organization requires me to tag my resources, and required extension didn't get installed, what went wrong?

The Defender agent uses the Log analytics workspace to send data from your Kubernetes clusters to Defender for Cloud. The Defender for Cloud adds the Log analytic workspace and the resource group as a parameter for the agent to use.

However, if your organization has a policy that requires a specific tag on your resources, it may cause the extension installation to fail during the resource group or the default workspace creation stage. If it fails, you can either:

- [Assign a custom workspace](#) and add any tag your organization requires.  
or  
• If your company requires you to tag your resource, you should navigate to that policy and exclude the following resources:
  1. The resource group `DefaultResourceGroup-<RegionShortCode>`
  2. The Workspace `DefaultWorkspace-<sub-id>-<RegionShortCode>`

RegionShortCode is a 2-4 letters string.

## Learn More

You can check out the following blogs:

- [Protect your Google Cloud workloads with Microsoft Defender for Cloud](#)
- [Introducing Microsoft Defender for Containers](#)
- [A new name for multicloud security: Microsoft Defender for Cloud](#)

## Next steps

Now that you enabled Defender for Containers, you can:

- [Scan your ACR images for vulnerabilities](#)
- [Scan your Amazon AWS ECR images for vulnerabilities](#)

# Overview of Microsoft Defender for Containers

10/27/2022 • 6 minutes to read • [Edit Online](#)

Microsoft Defender for Containers is the cloud-native solution that is used to secure your containers so you can improve, monitor, and maintain the security of your clusters, containers, and their applications.

Defender for Containers assists you with the three core aspects of container security:

- **Environment hardening** - Defender for Containers protects your Kubernetes clusters whether they're running on Azure Kubernetes Service, Kubernetes on-premises/IaaS, or Amazon EKS. Defender for Containers continuously assesses clusters to provide visibility into misconfigurations and guidelines to help mitigate identified threats.
- **Vulnerability assessment** - Vulnerability assessment and management tools for images stored in ACR registries and running in Azure Kubernetes Service.
- **Run-time threat protection for nodes and clusters** - Threat protection for clusters and Linux nodes generates security alerts for suspicious activities.

You can learn more by watching this video from the Defender for Cloud in the Field video series: [Microsoft Defender for Containers](#).

## Microsoft Defender for Containers plan availability

ASPECT	DETAILS
Release state:	General availability (GA) Certain features are in preview, for a full list see the <a href="#">availability</a> section.
Feature availability	Refer to the <a href="#">availability</a> section for additional information on feature release state and availability.
Pricing:	<b>Microsoft Defender for Containers</b> is billed as shown on the <a href="#">pricing page</a>
Required roles and permissions:	<ul style="list-style-type: none"><li>• To deploy the required components, see the <a href="#">permissions for each of the components</a></li><li>• <b>Security admin</b> can dismiss alerts</li><li>• <b>Security reader</b> can view vulnerability assessment findings</li></ul> <p>See also <a href="#">Azure Container Registry roles and permissions</a></p>

ASPECT	DETAILS
Clouds:	<p><b>Azure:</b></p> <ul style="list-style-type: none"> <li>✓ Commercial clouds</li> <li>✓ National clouds (Azure Government, Azure China 21Vianet) (Except for preview features))</li> </ul> <p><b>Non-Azure:</b></p> <ul style="list-style-type: none"> <li>✓ Connected AWS accounts (Preview)</li> <li>✓ Connected GCP projects (Preview)</li> <li>✓ On-prem/IaaS supported via Arc enabled Kubernetes (Preview).</li> </ul> <p>For more information about, see the <a href="#">availability section</a>.</p>

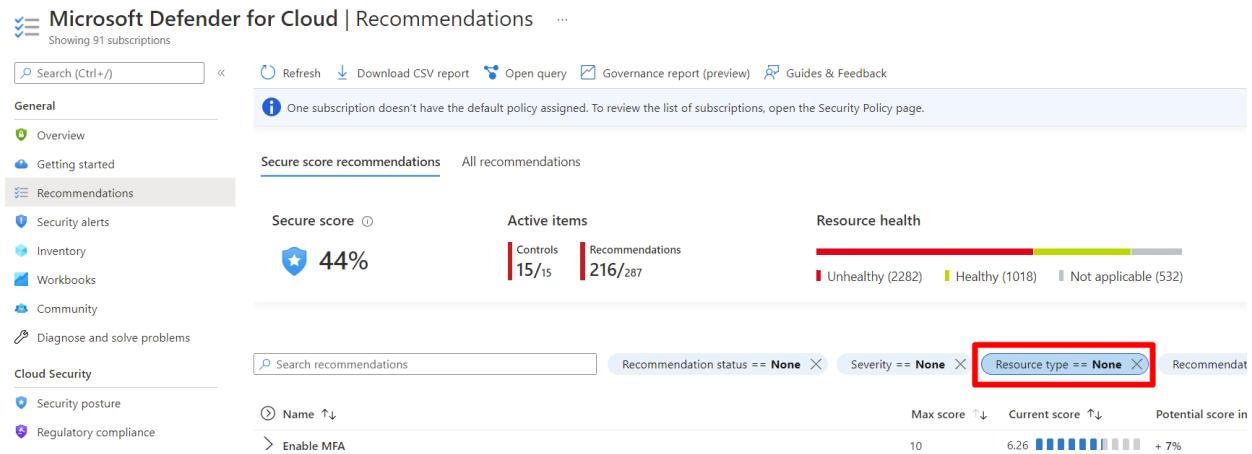
## Hardening

### Continuous monitoring of your Kubernetes clusters - wherever they're hosted

Defender for Cloud continuously assesses the configurations of your clusters and compares them with the initiatives applied to your subscriptions. When it finds misconfigurations, Defender for Cloud generates security recommendations that are available on Defender for Cloud's Recommendations page. The recommendations allow you to investigate and remediate issues. For details on the recommendations that might appear for this feature, check out the [compute section](#) of the recommendations reference table.

For Kubernetes clusters on EKS, you'll need to [connect your AWS account to Microsoft Defender for Cloud](#) and ensure you've enabled the CSPM plan.

You can use the resource filter to review the outstanding recommendations for your container-related resources, whether in asset inventory or the recommendations page:



The screenshot shows the Microsoft Defender for Cloud Recommendations page. The left sidebar includes sections for General, Recommendations (which is selected), Security alerts, Inventory, Workbooks, Community, and Diagnose and solve problems. Under Cloud Security, there are links for Security posture and Regulatory compliance. The main content area displays a secure score of 44%, 15/15 controls, and 216/287 recommendations. A resource health bar shows 2282 unhealthy items, 1018 healthy items, and 532 not applicable items. A search bar at the bottom allows filtering by recommendation status, severity, and resource type, with the 'Resource type = None' filter highlighted by a red box.

### Kubernetes data plane hardening

To protect the workloads of your Kubernetes containers with tailored recommendations, you can install the [Azure Policy for Kubernetes](#). Learn more about [monitoring components](#) for Defender for Cloud.

With the add-on on your AKS cluster, every request to the Kubernetes API server will be monitored against the predefined set of best practices before being persisted to the cluster. You can then configure it to enforce the best practices and mandate them for future workloads.

For example, you can mandate that privileged containers shouldn't be created, and any future requests to do so will be blocked.

You can learn more about [Kubernetes data plane hardening](#).

# Vulnerability assessment

## Scanning images in container registries

Defender for Containers scans the containers in Azure Container Registry (ACR) and Amazon AWS Elastic Container Registry (ECR) to notify you if there are known vulnerabilities in your images.

When you push an image to a container registry and while the image is stored in the container registry, Defender for Containers automatically scans it. Defender for Containers checks for known vulnerabilities in packages or dependencies defined in the image file.

When the scan completes, Defender for Containers provides details for each vulnerability detected, a security classification for each vulnerability detected, and guidance on how to remediate issues and protect vulnerable attack surfaces.

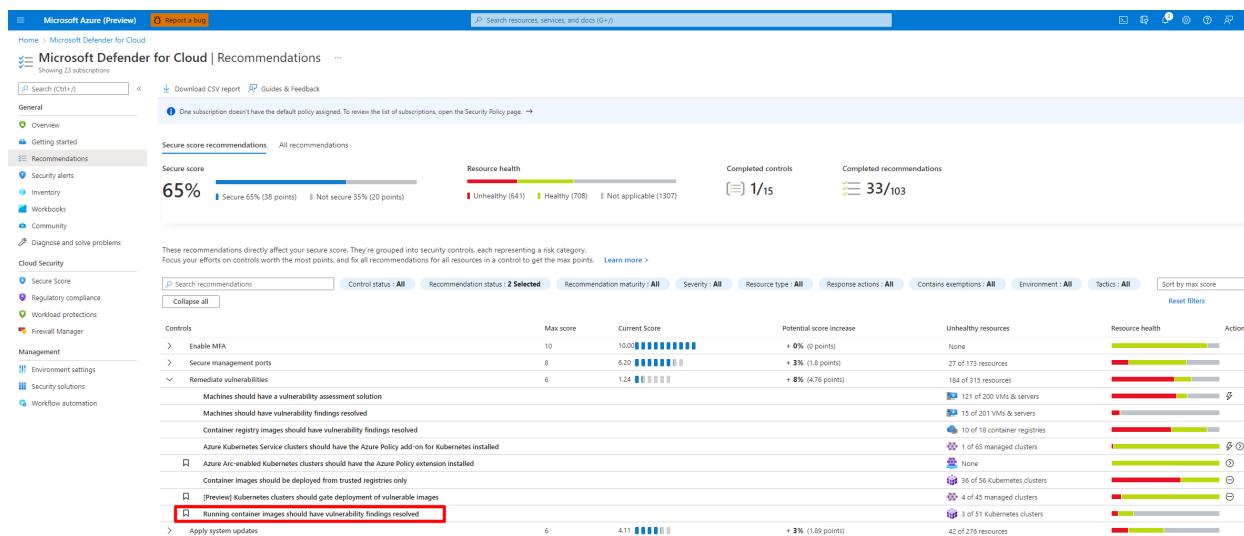
Learn more about:

- [Vulnerability assessment for Azure Container Registry \(ACR\)](#)
- [Vulnerability assessment for Amazon AWS Elastic Container Registry \(ECR\)](#)

## View vulnerabilities for running images in Azure Container Registry (ACR)

Defender for Cloud gives its customers the ability to prioritize the remediation of vulnerabilities in images that are currently being used within their environment using the [Running container images should have vulnerability findings resolved](#) recommendation.

To provide findings for the recommendation, Defender for Cloud collects the inventory of your running containers that are collected by the Defender agent installed on your AKS clusters. Defender for Cloud correlates that inventory with the vulnerability assessment scan of images that are stored in ACR. The recommendation shows your running containers with the vulnerabilities associated with the images that are used by each container and provides vulnerability reports and remediation steps.



Learn more about [viewing vulnerabilities for running images in \(ACR\)](#).

## Run-time protection for Kubernetes nodes and clusters

Defender for Containers provides real-time threat protection for your containerized environments and generates alerts for suspicious activities. You can use this information to quickly remediate security issues and improve the security of your containers. Threat protection at the cluster level is provided by the Defender agent and analysis of the Kubernetes audit logs. Examples of events at this level include exposed Kubernetes dashboards, creation of high-privileged roles, and the creation of sensitive mounts.

Defender for Containers also includes host-level threat detection with over 60 Kubernetes-aware analytics, AI,

and anomaly detections based on your runtime workload.

Defender for Cloud monitors the attack surface of multicloud Kubernetes deployments based on the [MITRE ATT&CK® matrix for Containers](#), a framework developed by the [Center for Threat-Informed Defense](#) in close partnership with Microsoft.

## FAQ - Defender for Containers

- [What are the options to enable the new plan at scale?](#)
- [Does Microsoft Defender for Containers support AKS clusters with virtual machines scale sets?](#)
- [Does Microsoft Defender for Containers support AKS without scale set \(default\)?](#)
- [Do I need to install the Log Analytics VM extension on my AKS nodes for security protection?](#)

### **What are the options to enable the new plan at scale?**

You can use the Azure Policy [Configure Microsoft Defender for Containers to be enabled](#), to enable Defender for Containers at scale. You can also see all of the options that are available to [enable Microsoft Defender for Containers](#).

### **Does Microsoft Defender for Containers support AKS clusters with virtual machines scale sets?**

Yes.

### **Does Microsoft Defender for Containers support AKS without scale set (default)?**

No. Only Azure Kubernetes Service (AKS) clusters that use virtual machine scale sets for the nodes is supported.

### **Do I need to install the Log Analytics VM extension on my AKS nodes for security protection?**

No, AKS is a managed service, and manipulation of the IaaS resources isn't supported. The Log Analytics VM extension isn't needed and may result in extra charges.

## Learn More

Learn more about Defender for Containers in the following blogs:

- [Introducing Microsoft Defender for Containers](#)
- [Demonstrating Microsoft Defender for Cloud](#)

The release state of Defender for Containers is broken down by two dimensions: environment and feature. So, for example:

- **Kubernetes data plane recommendations** for AKS clusters are GA
- **Kubernetes data plane recommendations** for EKS clusters are preview

To view the status of the full matrix of features and environments, see [Microsoft Defender for Containers feature availability](#).

## Next steps

In this overview, you learned about the core elements of container security in Microsoft Defender for Cloud. To enable the plan, see:

[Enable Defender for Containers](#)

# Use a service principal with Azure Kubernetes Service (AKS)

10/27/2022 • 10 minutes to read • [Edit Online](#)

To access other Azure Active Directory (Azure AD) resources, an AKS cluster requires either an [Azure Active Directory \(AD\) service principal](#) or a [managed identity](#). A service principal or managed identity is needed to dynamically create and manage other Azure resources such as an Azure load balancer or container registry (ACR).

Managed identities are the recommended way to authenticate with other resources in Azure, and is the default authentication method for your AKS cluster. For more information about using a managed identity with your cluster, see [Use a system-assigned managed identity](#).

This article shows how to create and use a service principal for your AKS clusters.

## Before you begin

To create an Azure AD service principal, you must have permissions to register an application with your Azure AD tenant, and to assign the application to a role in your subscription. If you don't have the necessary permissions, you need to ask your Azure AD or subscription administrator to assign the necessary permissions, or pre-create a service principal for you to use with the AKS cluster.

If you're using a service principal from a different Azure AD tenant, there are other considerations around the permissions available when you deploy the cluster. You may not have the appropriate permissions to read and write directory information. For more information, see [What are the default user permissions in Azure Active Directory?](#)

## Prerequisites

Azure CLI version 2.0.59 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Azure PowerShell version 5.0.0 or later. Run `Get-InstalledModule -Name Az` to find the version. If you need to install or upgrade, see [Install the Azure Az PowerShell module](#).

## Manually create a service principal

- [Azure CLI](#)
- [Azure PowerShell](#)

To manually create a service principal with the Azure CLI, use the `az ad sp create-for-rbac` command.

```
az ad sp create-for-rbac --name myAKSClusterServicePrincipal
```

The output is similar to the following example. Copy the values for `appId` and `password`. These values are used when you create an AKS cluster in the next section.

```
{
 "appId": "559513bd-0c19-4c1a-87cd-851a26af5fc",
 "displayName": "myAKSClusterServicePrincipal",
 "name": "http://myAKSClusterServicePrincipal",
 "password": "e763725a-5eee-40e8-a466-dc88d980f415",
 "tenant": "72f988bf-86f1-41af-91ab-2d7cd011db48"
}
```

## Specify a service principal for an AKS cluster

- [Azure CLI](#)
- [Azure PowerShell](#)

To use an existing service principal when you create an AKS cluster using the `az aks create` command, use the `--service-principal` and `--client-secret` parameters to specify the `appId` and `password` from the output of the `az ad sp create-for-rbac` command:

```
az aks create \
 --resource-group myResourceGroup \
 --name myAKScluster \
 --service-principal <appId> \
 --client-secret <password>
```

### NOTE

If you're using an existing service principal with customized secret, ensure the secret is not longer than 190 bytes.

## Delegate access to other Azure resources

The service principal for the AKS cluster can be used to access other resources. For example, if you want to deploy your AKS cluster into an existing Azure virtual network subnet or connect to Azure Container Registry (ACR), you need to delegate access to those resources to the service principal.

- [Azure CLI](#)
- [Azure PowerShell](#)

To delegate permissions, create a role assignment using the `az role assignment create` command. Assign the `appId` to a particular scope, such as a resource group or virtual network resource. A role then defines what permissions the service principal has on the resource, as shown in the following example:

```
az role assignment create --assignee <appId> --scope <resourceScope> --role Contributor
```

The `--scope` for a resource needs to be a full resource ID, such as `/subscriptions/<guid>/resourceGroups/myResourceGroup` or `/subscriptions/<guid>/resourceGroups/myResourceGroupVnet/providers/Microsoft.Network/virtualNetworks/myVnet`

### NOTE

If you have removed the Contributor role assignment from the node resource group, the operations below may fail. Permission granted to a cluster using a system-assigned managed identity may take up 60 minutes to populate.

The following sections detail common delegations that you may need to assign.

## Azure Container Registry

- [Azure CLI](#)
- [Azure PowerShell](#)

If you use Azure Container Registry (ACR) as your container image store, you need to grant permissions to the service principal for your AKS cluster to read and pull images. Currently, the recommended configuration is to use the `az aks create` or `az aks update` command to integrate with a registry and assign the appropriate role for the service principal. For detailed steps, see [Authenticate with Azure Container Registry from Azure Kubernetes Service](#).

## Networking

You may use advanced networking where the virtual network and subnet or public IP addresses are in another resource group. Assign the [Network Contributor](#) built-in role on the subnet within the virtual network.

Alternatively, you can create a [custom role](#) with permissions to access the network resources in that resource group. For more information, see [AKS service permissions](#).

## Storage

If you need to access existing disk resources in another resource group, assign one of the following set of role permissions:

- Create a [custom role](#) and define the following role permissions:
  - `Microsoft.Compute/disks/read`
  - `Microsoft.Compute/disks/write`
- Or, assign the [Storage Account Contributor](#) built-in role on the resource group

## Azure Container Instances

If you use Virtual Kubelet to integrate with AKS and choose to run Azure Container Instances (ACI) in resource group separate from the AKS cluster, the AKS cluster service principal must be granted *Contributor* permissions on the ACI resource group.

## Other considerations

- [Azure CLI](#)
- [Azure PowerShell](#)

When using AKS and an Azure AD service principal, consider the following:

- The service principal for Kubernetes is a part of the cluster configuration. However, don't use this identity to deploy the cluster.
- By default, the service principal credentials are valid for one year. You can [update or rotate the service principal credentials](#) at any time.
- Every service principal is associated with an Azure AD application. The service principal for a Kubernetes cluster can be associated with any valid Azure AD application name (for example: <https://www.contoso.org/example>). The URL for the application doesn't have to be a real endpoint.
- When you specify the service principal **Client ID**, use the value of the `appId`.
- On the agent node VMs in the Kubernetes cluster, the service principal credentials are stored in the file `/etc/kubernetes/azure.json`
- When you use the `az aks create` command to generate the service principal automatically, the service principal credentials are written to the file `~/.azure/aksServicePrincipal.json` on the machine used to run the command.
- If you don't specify a service principal with AKS CLI commands, the default service principal located at

`~/.azure/aksServicePrincipal.json` is used.

- You can optionally remove the `aksServicePrincipal.json` file, and AKS creates a new service principal.
- When you delete an AKS cluster that was created by [az aks create](#), the service principal created automatically isn't deleted.
  - To delete the service principal, query for your clusters `servicePrincipalProfile.clientId` and then delete it using the [az ad sp delete](#) command. Replace the values for the `-g` parameter for the resource group name, and `-n` parameter for the cluster name:

```
az ad sp delete --id $(az aks show -g myResourceGroup -n myAKSCluster --query servicePrincipalProfile.clientId -o tsv)
```

## Troubleshoot

- [Azure CLI](#)
- [Azure PowerShell](#)

The service principal credentials for an AKS cluster are cached by the Azure CLI. If these credentials have expired, you encounter errors during deployment of the AKS cluster. The following error message when running [az aks create](#) may indicate a problem with the cached service principal credentials:

```
Operation failed with status: 'Bad Request'.
Details: The credentials in ServicePrincipalProfile were invalid. Please see https://aka.ms/aks-sp-help for more details.
(Details: adal: Refresh request failed. Status Code = '401').
```

Check the age of the credentials file by running the following command:

```
ls -la $HOME/.azure/aksServicePrincipal.json
```

The default expiration time for the service principal credentials is one year. If your `aksServicePrincipal.json` file is older than one year, delete the file and retry deploying the AKS cluster.

### General Azure CLI troubleshooting

The Azure CLI can run in several shell environments, but with slight format variations. If you have unexpected results with Azure CLI commands, see [How to use the Azure CLI successfully](#).

## Next steps

For more information about Azure Active Directory service principals, see [Application and service principal objects](#).

For information on how to update the credentials, see [Update or rotate the credentials for a service principal in AKS](#).

# Use a managed identity in Azure Kubernetes Service

10/27/2022 • 11 minutes to read • [Edit Online](#)

An Azure Kubernetes Service (AKS) cluster requires an identity to access Azure resources like load balancers and managed disks. This identity can be either a managed identity or a service principal. By default, when you create an AKS cluster a system-assigned managed identity is automatically created. The identity is managed by the Azure platform and doesn't require you to provision or rotate any secrets. For more information about managed identities in Azure AD, see [Managed identities for Azure resources](#).

To use a [service principal](#), you have to create one, as AKS does not create one automatically. Clusters using a service principal eventually expire and the service principal must be renewed to keep the cluster working. Managing service principals adds complexity, thus it's easier to use managed identities instead. The same permission requirements apply for both service principals and managed identities.

Managed identities are essentially a wrapper around service principals, and make their management simpler. Managed identities use certificate-based authentication, and each managed identities credential has an expiration of 90 days and it's rolled after 45 days. AKS uses both system-assigned and user-assigned managed identity types, and these identities are immutable.

## Prerequisites

Azure CLI version 2.23.0 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Limitations

- Tenants move or migrate a managed identity-enabled cluster isn't supported.
- If the cluster has Azure AD pod-managed identity (`aad-pod-identity`) enabled, Node-Managed Identity (NMI) pods modify the nodes' iptables to intercept calls to the Azure Instance Metadata (IMDS) endpoint. This configuration means any request made to the Metadata endpoint is intercepted by NMI even if the pod doesn't use `aad-pod-identity`. `AzurePodIdentityException` CRD can be configured to inform `aad-pod-identity` that any requests to the Metadata endpoint originating from a pod that matches labels defined in CRD should be proxied without any processing in NMI. The system pods with `kubernetes.azure.com/managedby: aks` label in `kube-system` namespace should be excluded in `aad-pod-identity` by configuring the `AzurePodIdentityException` CRD. For more information, see [Disable aad-pod-identity for a specific pod or application](#). To configure an exception, install the [mic-exception YAML](#).

### NOTE

If you are considering implementing [Azure AD pod-managed identity](#) on your AKS cluster, we recommend you first review the [workload identity overview](#) article to understand our recommendations and options to set up your cluster to use an Azure AD workload identity (preview). This authentication method replaces pod-managed identity (preview), which integrates with the Kubernetes native capabilities to federate with any external identity providers.

## Summary of managed identities

AKS uses several managed identities for built-in services and add-ons.

IDENTITY	NAME	USE CASE	DEFAULT PERMISSIONS	BRING YOUR OWN IDENTITY
Control plane	AKS Cluster Name	Used by AKS control plane components to manage cluster resources including ingress load balancers and AKS managed public IPs, Cluster Autoscaler, Azure Disk & File CSI drivers	Contributor role for Node resource group	Supported
Kubelet	AKS Cluster Name-agentpool	Authentication with Azure Container Registry (ACR)	NA (for kubernetes v1.15+)	Supported
Add-on	AzureNPM	No identity required	NA	No
Add-on	AzureCNI network monitoring	No identity required	NA	No
Add-on	azure-policy (gatekeeper)	No identity required	NA	No
Add-on	azure-policy	No identity required	NA	No
Add-on	Calico	No identity required	NA	No
Add-on	Dashboard	No identity required	NA	No
Add-on	HTTPApplicationRouting	Manages required network resources	Reader role for node resource group, contributor role for DNS zone	No
Add-on	Ingress application gateway	Manages required network resources	Contributor role for node resource group	No
Add-on	omsagent	Used to send AKS metrics to Azure Monitor	Monitoring Metrics Publisher role	No
Add-on	Virtual-Node (ACIConnector)	Manages required network resources for Azure Container Instances (ACI)	Contributor role for node resource group	No
OSS project	aad-pod-identity	Enables applications to access cloud resources securely with Microsoft Azure Active Directory (Azure AD)	NA	Steps to grant permission at <a href="https://github.com/Azure/aad-pod-identity#role-assignment">https://github.com/Azure/aad-pod-identity#role-assignment</a> .

## Create an AKS cluster using a managed identity

#### NOTE

AKS will create a system-assigned kubelet identity in the Node resource group if you do not [specify your own kubelet managed identity](#).

You can create an AKS cluster using a system-assigned managed identity by running the following CLI command.

First, create an Azure resource group:

```
Create an Azure resource group
az group create --name myResourceGroup --location westus2
```

Then, create an AKS cluster:

```
az aks create -g myResourceGroup -n myManagedCluster --enable-managed-identity
```

Once the cluster is created, you can then deploy your application workloads to the new cluster and interact with it just as you've done with service-principal-based AKS clusters.

Finally, get credentials to access the cluster:

```
az aks get-credentials --resource-group myResourceGroup --name myManagedCluster
```

## Update an AKS cluster to use a managed identity

To update an AKS cluster currently using a service principal to work with a system-assigned managed identity, run the following CLI command.

```
az aks update -g <RGName> -n <AKSName> --enable-managed-identity
```

#### NOTE

An update will only work if there is an actual VHD update to consume. If you are running the latest VHD, you'll need to wait until the next VHD is available in order to perform the update.

#### NOTE

After updating, your cluster's control plane and addon pods, they use the managed identity, but kubelet will continue using a service principal until you upgrade your agentpool. Perform an `az aks nodepool upgrade --node-image-only` on your nodes to complete the update to a managed identity.

If your cluster was using `--attach-acr` to pull from image from Azure Container Registry, after updating your cluster to a managed identity, you need to rerun `az aks update --attach-acr <ACR Resource ID>` to let the newly created kubelet used for managed identity get the permission to pull from ACR. Otherwise, you won't be able to pull from ACR after the upgrade.

The Azure CLI will ensure your addon's permission is correctly set after migrating, if you're not using the Azure CLI to perform the migrating operation, you'll need to handle the addon identity's permission by yourself. Here is one example using an [Azure Resource Manager](#) template.

## WARNING

A nodepool upgrade will cause downtime for your AKS cluster as the nodes in the nodepools will be cordoned/drained and then reimaged.

## Add role assignment for control plane identity

When creating and using your own VNet, attached Azure disk, static IP address, route table or user-assigned kubelet identity where the resources are outside of the worker node resource group, the Azure CLI adds the role assignment automatically. If you are using an ARM template or other method, you need to use the Principal ID of the cluster managed identity to perform a role assignment.

### NOTE

If you are not using the Azure CLI but using your own VNet, attached Azure disk, static IP address, route table or user-assigned kubelet identity that are outside of the worker node resource group, it's recommended to use [user-assigned control plane identity](#). For system-assigned control plane identity, we cannot get the identity ID before creating cluster, which delays role assignment from taking effect.

### Get the Principal ID of control plane identity

You can find existing identity's Principal ID by running the following command:

```
az identity show --ids <identity-resource-id>
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "id": "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myIdentity",
 "location": "eastus",
 "name": "myIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
```

### Add role assignment

For Vnet, attached Azure disk, static IP address, route table which are outside the default worker node resource group, you need to assign the `Contributor` role on custom resource group.

```
az role assignment create --assignee <control-plane-identity-principal-id> --role "Contributor" --scope "<custom-resource-group-resource-id>"
```

Example:

```
az role assignment create --assignee 22222222-2222-2222-2222-222222222222 --role "Contributor" --scope "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/custom-resource-group"
```

For user-assigned kubelet identity which is outside the default worker node resource group, you need to assign

the [Managed Identity Operator](#) on kubelet identity.

```
az role assignment create --assignee <control-plane-identity-principal-id> --role "Managed Identity Operator" --scope "<kubelet-identity-resource-id>"
```

Example:

```
az role assignment create --assignee 22222222-2222-2222-2222-222222222222 --role "Managed Identity Operator" --scope "/subscriptions/00000000-0000-0000-0000-000000000000/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myKubeletIdentity"
```

#### NOTE

Permission granted to your cluster's managed identity used by Azure may take up 60 minutes to populate.

## Bring your own control plane managed identity

A custom control plane managed identity enables access to be granted to the existing identity prior to cluster creation. This feature enables scenarios such as using a custom VNET or outboundType of UDR with a pre-created managed identity.

#### NOTE

USDoD Central, USDoD East, USGov Iowa regions in Azure US Government cloud aren't currently supported.

AKS will create a system-assigned kubelet identity in the Node resource group if you do not [specify your own kubelet managed identity](#).

If you don't have a managed identity, you should create one by running the [az identity](#) command.

```
az identity create --name myIdentity --resource-group myResourceGroup
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "clientSecretUrl": "<clientSecretUrl>",
 "id": "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myIdentity",
 "location": "westus2",
 "name": "myIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
```

Run the following command to create a cluster with your existing identity:

```
az aks create \
--resource-group myResourceGroup \
--name myManagedCluster \
--network-plugin azure \
--vnet-subnet-id <subnet-id> \
--docker-bridge-address 172.17.0.1/16 \
--dns-service-ip 10.2.0.10 \
--service-cidr 10.2.0.0/24 \
--enable-managed-identity \
--assign-identity <identity-resource-id>
```

A successful cluster creation using your own managed identity should resemble the following **userAssignedIdentities** profile information:

```
"identity": {
 "principalId": null,
 "tenantId": null,
 "type": "UserAssigned",
 "userAssignedIdentities": {

 "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myIdentity": {
 "clientId": "<client-id>",
 "principalId": "<principal-id>"
 }
 }
},
```

## Use a pre-created kubelet managed identity

A Kubelet identity enables access granted to the existing identity prior to cluster creation. This feature enables scenarios such as connection to ACR with a pre-created managed identity.

### Prerequisites

Azure CLI version 2.26.0 or later installed. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

### Limitations

- Only works with a user-assigned managed cluster.
- China East and China North regions in Azure China 21Vianet aren't currently supported.

### Create user-assigned managed identities

If you don't have a control plane managed identity, you can create by running the following `az identity create` command:

```
az identity create --name myIdentity --resource-group myResourceGroup
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "clientSecretUrl": "<clientSecretUrl>",
 "id":
 "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myIdentity",
 "location": "westus2",
 "name": "myIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
}
```

If you don't have a kubelet managed identity, you can create one by running the following [az identity create](#) command:

```
az identity create --name myKubeletIdentity --resource-group myResourceGroup
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "clientSecretUrl": "<clientSecretUrl>",
 "id":
 "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myKubeletIdentity",
 "location": "westus2",
 "name": "myKubeletIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
```

### Create a cluster using user-assigned kubelet identity

Now you can use the following command to create your AKS cluster with your existing identities. Provide the control plane identity resource ID via `assign-identity` and the kubelet managed identity via

```
assign-kubelet-identity :
```

```
az aks create \
 --resource-group myResourceGroup \
 --name myManagedCluster \
 --network-plugin azure \
 --vnet-subnet-id <subnet-id> \
 --docker-bridge-address 172.17.0.1/16 \
 --dns-service-ip 10.2.0.10 \
 --service-cidr 10.2.0.0/24 \
 --enable-managed-identity \
 --assign-identity <identity-resource-id> \
 --assign-kubelet-identity <kubelet-identity-resource-id>
```

A successful AKS cluster creation using your own kubelet managed identity should resemble the following output:

```
"identity": {
 "principalId": null,
 "tenantId": null,
 "type": "UserAssigned",
 "userAssignedIdentities": {

 "/subscriptions/<subscriptionid>/resourcegroups/resourcegroups/providers/Microsoft.ManagedIdentity/userAssig
 nedIdentities/myIdentity": {
 "clientId": "<client-id>",
 "principalId": "<principal-id>"
 }
 }
},
"identityProfile": {
 "kubeletidentity": {
 "clientId": "<client-id>",
 "objectId": "<object-id>",
 "resourceId": "<resource-id>"
 }
},
"/subscriptions/<subscriptionid>/resourcegroups/resourcegroups/providers/Microsoft.ManagedIdentity/userAssig
nedIdentities/myKubeletIdentity"
}
```

## Update an existing cluster using kubelet identity

Update kubelet identity on an existing AKS cluster with your existing identities.

### WARNING

Updating kubelet managed identity upgrades Nodepool, which causes downtime for your AKS cluster as the nodes in the nodepools will be cordoned/drained and then reimaged.

### NOTE

If your cluster was using `--attach-acr` to pull from image from Azure Container Registry, after updating your cluster kubelet identity, you need to rerun `az aks update --attach-acr <ACR Resource ID>` to let the newly created kubelet used for managed identity get the permission to pull from ACR. Otherwise, you won't be able to pull from ACR after the upgrade.

## Make sure the CLI version is 2.37.0 or later

```
Check the version of Azure CLI modules
az version

Upgrade the version to make sure it is 2.37.0 or later
az upgrade
```

## Get the current control plane identity for your AKS cluster

Confirm your AKS cluster is using user-assigned control plane identity with the following CLI command:

```
az aks show -g <RGName> -n <ClusterName> --query "servicePrincipalProfile"
```

If the cluster is using a managed identity, the output shows `clientId` with a value of `msi`. A cluster using a service principal shows an object ID. For example:

```
{
 "clientId": "msi"
}
```

After verifying the cluster is using a managed identity, you can find the control plane identity's resource ID by running the following command:

```
az aks show -g <RGName> -n <ClusterName> --query "identity"
```

For user-assigned control plane identity, the output should look like:

```
{
 "principalId": null,
 "tenantId": null,
 "type": "UserAssigned",
 "userAssignedIdentities": <identity-resource-id>
 "clientId": "<client-id>",
 "principalId": "<principal-id>"
},
```

#### Updating your cluster with kubelet identity

If you don't have a kubelet managed identity, you can create one by running the following [az identity create](#) command:

```
az identity create --name myKubeletIdentity --resource-group myResourceGroup
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "clientSecretUrl": "<clientSecretUrl>",
 "id":
 "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myKubeletIdentity",
 "location": "westus2",
 "name": "myKubeletIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
```

Now you can use the following command to update your cluster with your existing identities. Provide the control plane identity resource ID via `assign-identity` and the kubelet managed identity via

```
assign-kubelet-identity :
```

```
az aks update \
 --resource-group myResourceGroup \
 --name myManagedCluster \
 --enable-managed-identity \
 --assign-identity <identity-resource-id> \

```

A successful cluster update using your own kubelet managed identity contains the following output:

```
"identity": {
 "principalId": null,
 "tenantId": null,
 "type": "UserAssigned",
 "userAssignedIdentities": {

 "/subscriptions/<subscriptionid>/resourcegroups/resourcegroups/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myIdentity": {
 "clientId": "<client-id>",
 "principalId": "<principal-id>"
 }
 },
 "identityProfile": {
 "kubeletidentity": {
 "clientId": "<client-id>",
 "objectId": "<object-id>",
 "resourceId": ""
 }
 }
},
```

## Next steps

Use [Azure Resource Manager templates](#) to create a managed identity-enabled cluster.

# Use ImageCleaner to clean up stale images on your Azure Kubernetes Service cluster (preview)

10/27/2022 • 4 minutes to read • [Edit Online](#)

It's common to use pipelines to build and deploy images on Azure Kubernetes Service (AKS) clusters. While great for image creation, this process often doesn't account for the stale images left behind and can lead to image bloat on cluster nodes. These images can present security issues as they may contain vulnerabilities. By cleaning these unreferenced images, you can remove an area of risk in your clusters. When done manually, this process can be time intensive, which ImageCleaner can mitigate via automatic image identification and removal.

## NOTE

ImageCleaner is a feature based on [Eraser](#). On an AKS cluster, the feature name and property name is `ImageCleaner` while the relevant ImageCleaner pods' names contain `Eraser`.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI](#) or [Azure PowerShell](#) and the `aks-preview` 0.5.96 or later CLI extension installed.
- The `EnableImageCleanerPreview` feature flag registered on your subscription:
  - [Azure CLI](#)
  - [Azure PowerShell](#)

Register the `EnableImageCleanerPreview` feature flag by using the [az feature register](#) command, as shown in the following example:

```
az feature register --namespace "Microsoft.ContainerService" --name "EnableImageCleanerPreview"
```

It takes a few minutes for the status to show *Registered*. Verify the registration status by using the [az feature list](#) command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/EnableImageCleanerPreview')].{Name:name,State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider by using the [az provider register](#) command:

```
az provider register --namespace Microsoft.ContainerService
```

## Limitations

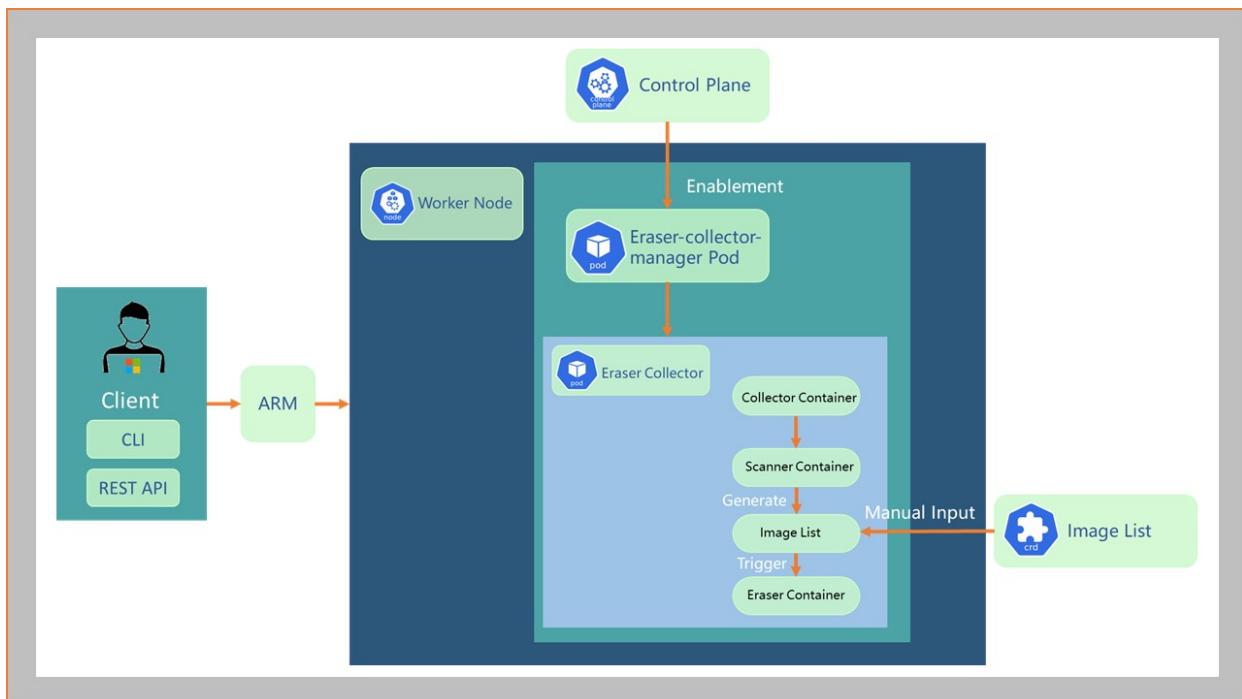
ImageCleaner does not support the following:

- ARM64 node pools. For more information, see [Azure Virtual Machines with ARM-based processors](#).
- Windows node pools.

## How ImageCleaner works

When enabled, an `eraser-controller-manager` pod is deployed on each agent node, which will use an `ImageList` CRD to determine unreferenced and vulnerable images. Vulnerability is determined based on a `trivy` scan, after which images with a `LOW`, `MEDIUM`, `HIGH`, or `CRITICAL` classification are flagged. An updated `ImageList` will be automatically generated by ImageCleaner based on a set time interval, and can also be supplied manually.

Once an `ImageList` is generated, ImageCleaner will remove all the images in the list from node VMs.



## Configuration options

In addition to choosing between manual and automatic mode, there are several options for ImageCleaner:

NAME	DESCRIPTION	REQUIRED
--enable-image-cleaner	Enable the ImageCleaner feature for an AKS cluster	Yes, unless disable is specified
--disable-image-cleaner	Disable the ImageCleaner feature for an AKS cluster	Yes, unless enable is specified
--image-cleaner-interval-hours	This parameter determines the interval time (in hours) ImageCleaner will use to run. The default value is one week, the minimum value is 24 hours and the maximum is three months.	No

NAME	DESCRIPTION	REQUIRED
------	-------------	----------

#### NOTE

After disabling ImageCleaner, the old configuration still exists. This means that if you enable the feature again without explicitly passing configuration, the existing value will be used rather than the default.

## Enable ImageCleaner on your AKS cluster

To create a new AKS cluster using the default interval, use [az aks create](#):

```
az aks create -g MyResourceGroup -n MyManagedCluster \
--enable-image-cleaner
```

To enable on an existing AKS cluster, use [az aks update](#):

```
az aks update -g MyResourceGroup -n MyManagedCluster \
--enable-image-cleaner
```

The `--image-cleaner-interval-hours` parameter can be specified at creation time or for an existing cluster. For example, the following command updates the interval for a cluster with ImageCleaner already enabled:

```
az aks update -g MyResourceGroup -n MyManagedCluster \
--image-cleaner-interval-hours 48
```

After the feature is enabled, the `eraser-controller-manager-xxx` pod and `collector-aks-xxx` pod will be deployed. Based on your configuration, ImageCleaner will generate an `ImageList` containing non-running and vulnerable images at the desired interval. ImageCleaner will automatically remove these images from cluster nodes.

## Manually remove images

To manually remove images from your cluster using ImageCleaner, first create an `ImageList`. For example, save the following as `image-list.yml`:

```
apiVersion: eraser.sh/v1alpha1
kind: ImageList
metadata:
 name: imagelist
spec:
 images:
 - docker.io/library/alpine:3.7.3 # You can also use "*" to specify all non-running images
```

And apply it to the cluster:

```
kubectl apply -f image-list.yml
```

A job named `eraser-aks-xxx` will be triggered which causes ImageCleaner to remove the desired images from all nodes.

## Disable ImageCleaner

To stop using ImageCleaner, you can disable it via the `--disable-image-cleaner` flag:

```
az aks update -g MyResourceGroup -n MyManagedCluster
--disable-image-cleaner
```

## Logging

The deletion logs are stored in the `image-cleaner-kind-worker` pods. You can check these via `kubectl logs` or via the Container Insights pod log table if the [Azure Monitor add-on](#) is enabled.

# Use Azure role-based access control to define access to the Kubernetes configuration file in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

You can interact with Kubernetes clusters using the `kubectl` tool. The Azure CLI provides an easy way to get the access credentials and configuration information to connect to your AKS clusters using `kubectl`. To limit who can get that Kubernetes configuration (*kubeconfig*) information and to limit the permissions they then have, you can use Azure role-based access control (Azure RBAC).

This article shows you how to assign Azure roles that limit who can get the configuration information for an AKS cluster.

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

This article also requires that you are running the Azure CLI version 2.0.65 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Available cluster roles permissions

When you interact with an AKS cluster using the `kubectl` tool, a configuration file is used that defines cluster connection information. This configuration file is typically stored in `~/.kube/config`. Multiple clusters can be defined in this *kubeconfig* file. You switch between clusters using the `kubectl config use-context` command.

The `az aks get-credentials` command lets you get the access credentials for an AKS cluster and merges them into the *kubeconfig* file. You can use Azure role-based access control (Azure RBAC) to control access to these credentials. These Azure roles let you define who can retrieve the *kubeconfig* file, and what permissions they then have within the cluster.

The two built-in roles are:

- **Azure Kubernetes Service Cluster Admin Role**
  - Allows access to `Microsoft.ContainerService/managedClusters/listClusterAdminCredential/action` API call. This API call [lists the cluster admin credentials](#).
  - Downloads *kubeconfig* for the *clusterAdmin* role.
- **Azure Kubernetes Service Cluster User Role**
  - Allows access to `Microsoft.ContainerService/managedClusters/listClusterUserCredential/action` API call. This API call [lists the cluster user credentials](#).
  - Downloads *kubeconfig* for *clusterUser* role.

These Azure roles can be applied to an Azure Active Directory (AD) user or group.

#### NOTE

On clusters that use Azure AD, users with the *clusterUser* role have an empty *kubeconfig* file that prompts a log in. Once logged in, users have access based on their Azure AD user or group settings. Users with the *clusterAdmin* role have admin access.

On clusters that do not use Azure AD, the *clusterUser* role has same effect of *clusterAdmin* role.

## Assign role permissions to a user or group

To assign one of the available roles, you need to get the resource ID of the AKS cluster and the ID of the Azure AD user account or group. The following example commands:

- Get the cluster resource ID using the `az aks show` command for the cluster named *myAKSCluster* in the *myResourceGroup* resource group. Provide your own cluster and resource group name as needed.
- Use the `az account show` and `az ad user show` commands to get your user ID.
- Finally, assign a role using the `az role assignment create` command.

The following example assigns the *Azure Kubernetes Service Cluster Admin Role* to an individual user account:

```
Get the resource ID of your AKS cluster
$AKS_CLUSTER=$(az aks show --resource-group myResourceGroup --name myAKSCluster --query id -o tsv)

Get the account credentials for the logged in user
$ACCOUNT_UPN=$(az account show --query user.name -o tsv)
$ACCOUNT_ID=$(az ad user show --id $ACCOUNT_UPN --query objectId -o tsv)

Assign the 'Cluster Admin' role to the user
az role assignment create \
 --assignee $ACCOUNT_ID \
 --scope $AKS_CLUSTER \
 --role "Azure Kubernetes Service Cluster Admin Role"
```

#### IMPORTANT

In some cases, the *user.name* in the account is different than the *userPrincipalName*, such as with Azure AD guest users:

```
$ az account show --query user.name -o tsv
user@contoso.com
$ az ad user list --query "[?contains(otherMails,'user@contoso.com')].{UPN:userPrincipalName}" -o tsv
user_contoso.com#EXT#@contoso.onmicrosoft.com
```

In this case, set the value of *ACCOUNT\_UPN* to the *userPrincipalName* from the Azure AD user. For example, if your account *user.name* is *user@contoso.com*.

```
ACCOUNT_UPN=$(az ad user list --query "[?contains(otherMails,'user@contoso.com')].{UPN:userPrincipalName}" -o tsv)
```

#### TIP

If you want to assign permissions to an Azure AD group, update the `--assignee` parameter shown in the previous example with the object ID for the *group* rather than a *user*. To obtain the object ID for a group, use the `az ad group show` command. The following example gets the object ID for the Azure AD group named *appdev*.

```
az ad group show --group appdev --query objectId -o tsv
```

You can change the previous assignment to the *Cluster User Role* as needed.

The following example output shows the role assignment has been successfully created:

```
{
 "canDelegate": null,
 "id":
 "/subscriptions/<guid>/resourcegroups/myResourceGroup/providers/Microsoft.ContainerService/managedClusters/m
yAKScluster/providers/Microsoft.Authorization/roleAssignments/b2712174-5a41-4ecb-82c5-12b8ad43d4fb",
 "name": "b2712174-5a41-4ecb-82c5-12b8ad43d4fb",
 "principalId": "946016dd-9362-4183-b17d-4c416d1f8f61",
 "resourceGroup": "myResourceGroup",
 "roleDefinitionId": "/subscriptions/<guid>/providers/Microsoft.Authorization/roleDefinitions/0ab01a8-8aac-
4efd-b8c2-3ee1fb270be8",
 "scope":
 "/subscriptions/<guid>/resourcegroups/myResourceGroup/providers/Microsoft.ContainerService/managedClusters/m
yAKScluster",
 "type": "Microsoft.Authorization/roleAssignments"
}
```

## Get and verify the configuration information

With Azure roles assigned, use the [az aks get-credentials](#) command to get the *kubeconfig* definition for your AKS cluster. The following example gets the *--admin* credentials, which work correctly if the user has been granted the *Cluster Admin Role*.

```
az aks get-credentials --resource-group myResourceGroup --name myAKScluster --admin
```

You can then use the [kubectl config view](#) command to verify that the *context* for the cluster shows that the admin configuration information has been applied:

```
$ kubectl config view

apiVersion: v1
clusters:
- cluster:
 certificate-authority-data: DATA+OMITTED
 server: https://myaksclust-myresourcegroup-19da35-4839be06.hcp.eastus.azmk8s.io:443
 name: myAKScluster
contexts:
- context:
 cluster: myAKScluster
 user: clusterAdmin_myResourceGroup_myAKScluster
 name: myAKScluster-admin
current-context: myAKScluster-admin
kind: Config
preferences: {}
users:
- name: clusterAdmin_myResourceGroup_myAKScluster
 user:
 client-certificate-data: REDACTED
 client-key-data: REDACTED
 token: e9f2f819a4496538b02cefff94e61d35
```

## Remove role permissions

To remove role assignments, use the [az role assignment delete](#) command. Specify the account ID and cluster resource ID, as obtained in the previous commands. If you assigned the role to a group rather than a user, specify the appropriate group object ID rather than account object ID for the `--assignee` parameter:

```
az role assignment delete --assignee $ACCOUNT_ID --scope $AKS_CLUSTER
```

## Next steps

For enhanced security on access to AKS clusters, [integrate Azure Active Directory authentication](#).

# Secure access to the API server using authorized IP address ranges in Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

In Kubernetes, the API server receives requests to perform actions in the cluster such as to create resources or scale the number of nodes. The API server is the central way to interact with and manage a cluster. To improve cluster security and minimize attacks, the API server should only be accessible from a limited set of IP address ranges.

This article shows you how to use API server authorized IP address ranges, using the Azure CLI, to limit which IP addresses and CIDRs can access control plane.

## Before you begin

- You need the Azure CLI version 2.0.76 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).
- To learn what IP addresses to include when integrating your AKS cluster with Azure DevOps, see the Azure DevOps [Allowed IP addresses and domain URLs](#) article.

### Limitations

The API server Authorized IP ranges feature has the following limitations:

- On clusters created after API server authorized IP address ranges moved out of preview in October 2019, API server authorized IP address ranges are only supported on the *Standard* SKU load balancer. Existing clusters with the *Basic* SKU load balancer and API server authorized IP address ranges configured will continue work as is, but they can't be migrated to a *Standard* SKU load balancer. Existing clusters will also continue to work if their Kubernetes version or control plane are upgraded.
- API server authorized IP address ranges aren't supported with private clusters.
- When using this feature with clusters that use [Public IP per Node](#), those node pools with public IP per node enabled must use public IP prefixes, and those prefixes must be added as authorized ranges.

## Overview of API server authorized IP ranges

The Kubernetes API server is how the underlying Kubernetes APIs are exposed. This component provides the interaction for management tools, such as `kubectl` or the Kubernetes dashboard. AKS provides a single-tenant cluster control plane, with a dedicated API server. By default, the API server is assigned a public IP address, and you should control access using Kubernetes role-based access control (Kubernetes RBAC) or Azure RBAC.

To secure access to the otherwise publicly accessible AKS control plane / API server, you can enable and use authorized IP ranges. These authorized IP ranges only allow defined IP address ranges to communicate with the API server. A request made to the API server from an IP address that isn't part of these authorized IP ranges is blocked. Continue to use Kubernetes RBAC or Azure RBAC to authorize users and the actions they request.

For more information about the API server and other cluster components, see [Kubernetes core concepts for AKS](#).

## Create an AKS cluster with API server authorized IP ranges enabled

Create a cluster using the `az aks create` and specify the `--api-server-authorized-ip-ranges` parameter to provide

a list of authorized IP address ranges. These IP address ranges are usually address ranges used by your on-premises networks or public IPs. When you specify a CIDR range, start with the first IP address in the range. For example, `137.117.106.90/29` is a valid range, but make sure you specify the first IP address in the range, such as `137.117.106.88/29`.

#### IMPORTANT

By default, your cluster uses the [Standard SKU load balancer](#) which you can use to configure the outbound gateway. When you enable API server authorized IP ranges during cluster creation, the public IP for your cluster is also allowed by default in addition to the ranges you specify. If you specify "" or no value for `--api-server-authorized-ip-ranges`, API server authorized IP ranges will be disabled. Note that if you're using PowerShell, use `--api-server-authorized-ip-ranges=""` (with equals sign) to avoid any parsing issues.

The following example creates a single-node cluster named `myAKSCluster` in the resource group named `myResourceGroup` with API server authorized IP ranges enabled. The IP address ranges allowed are `73.140.245.0/24`:

```
az aks create \
 --resource-group myResourceGroup \
 --name myAKSCluster \
 --node-count 1 \
 --vm-set-type VirtualMachineScaleSets \
 --load-balancer-sku standard \
 --api-server-authorized-ip-ranges 73.140.245.0/24 \
 --generate-ssh-keys
```

#### NOTE

You should add these ranges to an allow list:

- The firewall public IP address
- Any range that represents networks that you'll administer the cluster from

The upper limit for the number of IP ranges you can specify is 200.

The rules can take up to two minutes to propagate. Please allow up to that time when testing the connection.

## Specify the outbound IPs for the Standard SKU load balancer

While creating an AKS cluster, if you specify the outbound IP addresses or prefixes for the cluster, they are allowed as well. For example:

```
az aks create \
 --resource-group myResourceGroup \
 --name myAKSCluster \
 --node-count 1 \
 --vm-set-type VirtualMachineScaleSets \
 --load-balancer-sku standard \
 --api-server-authorized-ip-ranges 73.140.245.0/24 \
 --load-balancer-outbound-ips <publicIpId1>,<publicIpId2> \
 --generate-ssh-keys
```

In the above example, all IPs provided in the parameter `--Load-balancer-outbound-ip-prefixes` are allowed along with the IPs in the `--api-server-authorized-ip-ranges` parameter.

Instead, you can specify the `--Load-balancer-outbound-ip-prefixes` parameter to allow outbound load balancer IP prefixes.

## Allow only the outbound public IP of the Standard SKU load balancer

When you enable API server authorized IP ranges during cluster creation, the outbound public IP for the Standard SKU load balancer for your cluster is also allowed by default in addition to the ranges you specify. To allow only the outbound public IP of the Standard SKU load balancer, use `0.0.0.0/32` when specifying the `--api-server-authorized-ip-ranges` parameter.

In the following example, only the outbound public IP of the Standard SKU load balancer is allowed, and you can only access the API server from the nodes within the cluster.

```
az aks create \
 --resource-group myResourceGroup \
 --name myAKScluster \
 --node-count 1 \
 --vm-set-type VirtualMachineScaleSets \
 --load-balancer-sku standard \
 --api-server-authorized-ip-ranges 0.0.0.0/32 \
 --generate-ssh-keys
```

## Update a cluster's API server authorized IP ranges

To update the API server authorized IP ranges on an existing cluster, use `az aks update` command and use the `--api-server-authorized-ip-ranges`, `--Load-balancer-outbound-ip-prefixes`, `--Load-balancer-outbound-ips`, or `--Load-balancer-outbound-ip-prefixes` parameters.

The following example updates API server authorized IP ranges on the cluster named `myAKScluster` in the resource group named `myResourceGroup`. The IP address range to authorize is `73.140.245.0/24`:

```
az aks update \
 --resource-group myResourceGroup \
 --name myAKScluster \
 --api-server-authorized-ip-ranges 73.140.245.0/24
```

You can also use `0.0.0.0/32` when specifying the `--api-server-authorized-ip-ranges` parameter to allow only the public IP of the Standard SKU load balancer.

## Disable authorized IP ranges

To disable authorized IP ranges, use `az aks update` and specify an empty range to disable API server authorized IP ranges. For example:

```
az aks update \
 --resource-group myResourceGroup \
 --name myAKScluster \
 --api-server-authorized-ip-ranges ""
```

### IMPORTANT

When running this command using the PowerShell in Azure Cloud Shell or from your local computer, the double-quote string value for the `--api-server-authorized-ip-rangers` argument needs to be [enclosed in single quotes](#). Otherwise, an error message is returned indicating an expected argument is missing.

## Find existing authorized IP ranges

To find IP ranges that have been authorized, use `az aks show` and specify the cluster's name and resource group.

For example:

```
az aks show \
--resource-group myResourceGroup \
--name myAKScluster \
--query apiServerAccessProfile.authorizedIpRanges
```

## Update, disable, and find authorized IP ranges using Azure portal

The above operations of adding, updating, finding, and disabling authorized IP ranges can also be performed in the Azure portal. To access, navigate to **Networking** under **Settings** in the menu blade of your cluster resource.

The screenshot shows the Azure portal interface for managing a Kubernetes service. The left sidebar lists various settings like Overview, Activity log, and Networking. The Networking section is currently selected. On the right, there's a detailed view of the cluster's networking profile, including its type (Kubenet), CIDR ranges, and DNS service IP. Under the Traffic routing section, the 'Enable HTTP application routing' checkbox is unchecked. In the Security section, it's noted that the cluster is private and not enabled for HTTP application routing. The 'Set authorized IP ranges' checkbox is checked, and the IP range '73.140.245.0/24' is listed in the input field, which is highlighted with a red border.

## How to find my IP to include in `--api-server-authorized-ip-ranges` ?

You must add your development machines, tooling, or automation IP addresses to the AKS cluster list of approved IP ranges to access the API server from there.

Another option is to configure a jumpbox with the necessary tooling inside a separate subnet in the firewall's virtual network. This assumes your environment has a firewall with the respective network, and you've added the firewall IPs to authorized ranges. Similarly, if you've forced tunneling from the AKS subnet to the firewall subnet, having the jumpbox in the cluster subnet is also okay.

To add another IP address to the approved ranges, use the following commands.

```
Retrieve your IP address
CURRENT_IP=$(dig +short "myip.opendns.com" "@resolver1.opendns.com")
```

```
Add to AKS approved list
az aks update -g $RG -n $AKSNAME --api-server-authorized-ip-ranges $CURRENT_IP/32
```

#### NOTE

The above example appends the API server authorized IP ranges on the cluster. To disable authorized IP ranges, use

```
az aks update
```

Another option is to use the following command on Windows systems to get the public IPv4 address, or you can follow the steps in [Find your IP address](#).

```
Invoke-RestMethod http://ipinfo.io/json | Select -exp ip
```

You can also find this address by searching on *what is my IP address* in an internet browser.

## Next steps

In this article, you enabled API server authorized IP ranges. This approach is one part of how you can securely run an AKS cluster. For more information, see [Security concepts for applications and clusters in AKS](#) and [Best practices for cluster security and upgrades in AKS](#).

# Add Key Management Service (KMS) etcd encryption to an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 9 minutes to read • [Edit Online](#)

This article shows you how to enable encryption at rest for your Kubernetes data in etcd using Azure Key Vault with the Key Management Service (KMS) plugin. The KMS plugin allows you to:

- Use a key in Key Vault for etcd encryption.
- Bring your own keys.
- Provide encryption at rest for secrets stored in etcd.
- Rotate the keys in Key Vault.

For more information on using the KMS plugin, see [Encrypting Secret Data at Rest](#).

## Prerequisites

- An Azure account with an active subscription. [Create an account for free](#).
- Azure CLI version 2.39.0 or later. Run `az --version` to find your version. If you need to install or upgrade, see [Install Azure CLI](#).

### WARNING

KMS only supports Konnectivity and Vnet Integration. You can use `kubectl get po -n kube-system` to verify the results show that a konnectivity-agent-xxx pod is running. If there is, it means the AKS cluster is using Konnectivity. When using VNet integration, you can run the command `az aks cluster show -g -n` to verify the setting `enableVnetIntegration` is set to `true`.

## Limitations

The following limitations apply when you integrate KMS etcd encryption with AKS:

- Deletion of the key, Key Vault, or the associated identity.
- KMS etcd encryption doesn't work with system-assigned managed identity. The key vault access policy is required to be set before the feature is enabled. In addition, system-assigned managed identity isn't available until cluster creation, thus there's a cycle dependency.
- Using more than 2000 secrets in a cluster.
- Bring your own (BYO) Azure Key Vault from another tenant.
- Change associated Azure Key Vault model (public, private) if KMS is enabled. For [changing associated key vault mode](#), you need to disable and enable KMS again.
- Stop/start cluster which is enabled KMS with private key vault.

KMS supports [public key vault](#) and [private key vault](#).

## Enable KMS with public key vault

[Create a key vault and key](#)

## WARNING

Deleting the key or the Azure Key Vault is not supported and will cause the secrets to be unrecoverable in the cluster.

If you need to recover your Key Vault or key, see [Azure Key Vault recovery management with soft delete and purge protection](#).

### For non-RBAC key vault

Use `az keyvault create` to create a key vault.

```
az keyvault create --name MyKeyVault --resource-group MyResourceGroup
```

Use `az keyvault key create` to create a key.

```
az keyvault key create --name MyKeyName --vault-name MyKeyVault
```

Use `az keyvault key show` to export the key ID.

```
export KEY_ID=$(az keyvault key show --name MyKeyName --vault-name MyKeyVault --query 'key.kid' -o tsv)
echo $KEY_ID
```

The above example stores the key ID in *KEY\_ID*.

### For RBAC key vault

Use `az keyvault create` to create a key vault using Azure Role Based Access Control.

```
export KEYVAULT_RESOURCE_ID=$(az keyvault create --name MyKeyVault --resource-group MyResourceGroup --enable-rbac-authorization true --query id -o tsv)
```

Assign yourself permission to create a key.

```
az role assignment create --role "Key Vault Crypto Officer" --assignee-object-id $($az ad signed-in-user show --query id --out tsv) --assignee-principal-type "User" --scope $KEYVAULT_RESOURCE_ID
```

Use `az keyvault key create` to create a key.

```
az keyvault key create --name MyKeyName --vault-name MyKeyVault
```

Use `az keyvault key show` to export the key ID.

```
export KEY_ID=$(az keyvault key show --name MyKeyName --vault-name MyKeyVault --query 'key.kid' -o tsv)
echo $KEY_ID
```

The above example stores the key ID in *KEY\_ID*.

### Create a user-assigned managed identity

Use `az identity create` to create a user-assigned managed identity.

```
az identity create --name MyIdentity --resource-group MyResourceGroup
```

Use `az identity show` to get the identity object ID.

```
IDENTITY_OBJECT_ID=$(az identity show --name MyIdentity --resource-group MyResourceGroup --query 'principalId' -o tsv)
echo $IDENTITY_OBJECT_ID
```

The above example stores the value of the identity object ID in *IDENTITY\_OBJECT\_ID*.

Use `az identity show` to get the identity resource ID.

```
IDENTITY_RESOURCE_ID=$(az identity show --name MyIdentity --resource-group MyResourceGroup --query 'id' -o tsv)
echo $IDENTITY_RESOURCE_ID
```

The above example stores the value of the identity resource ID in *IDENTITY\_RESOURCE\_ID*.

### Assign permissions (decrypt and encrypt) to access key vault

#### For non-RBAC key vault

If your key vault is not enabled with `--enable-rbac-authorization`, you can use `az keyvault set-policy` to create an Azure key vault policy.

```
az keyvault set-policy -n MyKeyVault --key-permissions decrypt encrypt --object-id $IDENTITY_OBJECT_ID
```

#### For RBAC key vault

If your key vault is enabled with `--enable-rbac-authorization`, you need to assign the "Key Vault Crypto User" RBAC role which has decrypt, encrypt permission.

```
az role assignment create --role "Key Vault Crypto User" --assignee-object-id $IDENTITY_OBJECT_ID --assignee-principal-type "ServicePrincipal" --scope $KEYVAULT_RESOURCE_ID
```

### Create an AKS cluster with KMS etcd encryption enabled

Create an AKS cluster using the `az aks create` command with the `--enable-azure-keyvault-kms`, `--azure-keyvault-kms-key-vault-network-access` and `--azure-keyvault-kms-key-id` parameters to enable KMS etcd encryption.

```
az aks create --name myAKSCluster --resource-group MyResourceGroup --assign-identity $IDENTITY_RESOURCE_ID --enable-azure-keyvault-kms --azure-keyvault-kms-key-vault-network-access "Public" --azure-keyvault-kms-key-id $KEY_ID
```

### Update an existing AKS cluster to enable KMS etcd encryption

Use `az aks update` with the `--enable-azure-keyvault-kms`, `--azure-keyvault-kms-key-vault-network-access` and `--azure-keyvault-kms-key-id` parameters to enable KMS etcd encryption on an existing cluster.

```
az aks update --name myAKSCluster --resource-group MyResourceGroup --enable-azure-keyvault-kms --azure-keyvault-kms-key-vault-network-access "Public" --azure-keyvault-kms-key-id $KEY_ID
```

Use the following command to update all secrets. Otherwise, old secrets won't be encrypted. For larger clusters, you may want to subdivide the secrets by namespace or script an update.

```
kubectl get secrets --all-namespaces -o json | kubectl replace -f -
```

## Rotate the existing keys

After changing the key ID (including key name and key version), you can use `az aks update` with the `--enable-azure-keyvault-kms`, `--azure-keyvault-kms-key-vault-network-access` and `--azure-keyvault-kms-key-id` parameters to rotate the existing keys of KMS.

### WARNING

Remember to update all secrets after key rotation. Otherwise, the secrets will be inaccessible if the old keys don't exist or aren't working.

```
az aks update --name myAKSCluster --resource-group MyResourceGroup --enable-azure-keyvault-kms --azure-keyvault-kms-key-vault-network-access "Public" --azure-keyvault-kms-key-id $NEW_KEY_ID
```

Use the following command to update all secrets. Otherwise, old secrets will still be encrypted with the previous key. For larger clusters, you may want to subdivide the secrets by namespace or script an update.

```
kubectl get secrets --all-namespaces -o json | kubectl replace -f -
```

## Enable KMS with private key vault

If you enable KMS with private key vault, AKS will create a private endpoint and private link in the node resource group automatically. The key vault will be added a private endpoint connection with the AKS cluster.

### Create a private key vault and key

#### WARNING

Deleting the key or the Azure Key Vault isn't supported and will cause the secrets to be unrecoverable in the cluster.

If you need to recover your key vault or key, see [Azure Key Vault recovery management with soft delete and purge protection](#).

Use `az keyvault create` to create a private key vault.

```
az keyvault create --name MyKeyVault --resource-group MyResourceGroup --public-network-access Disabled
```

It's not supported to create or update keys in private key vault without private endpoint. To manage private key vaults, you can refer to [Integrate Key Vault with Azure Private Link](#).

### Create a user-assigned managed identity

Use `az identity create` to create a user-assigned managed identity.

```
az identity create --name MyIdentity --resource-group MyResourceGroup
```

Use `az identity show` to get the identity object ID.

```
IDENTITY_OBJECT_ID=$(az identity show --name MyIdentity --resource-group MyResourceGroup --query 'principalId' -o tsv)
echo $IDENTITY_OBJECT_ID
```

The above example stores the value of the identity object ID in `IDENTITY_OBJECT_ID`.

Use `az identity show` to get identity resource ID.

```
IDENTITY_RESOURCE_ID=$(az identity show --name MyIdentity --resource-group MyResourceGroup --query 'id' -o tsv)
echo $IDENTITY_RESOURCE_ID
```

The above example stores the value of the identity resource ID in `$IDENTITY_RESOURCE_ID`.

### Assign permissions (decrypt and encrypt) to access key vault

#### For non-RBAC key vault

If your key vault is not enabled with `--enable-rbac-authorization`, you can use `az keyvault set-policy` to create an Azure key vault policy.

```
az keyvault set-policy -n MyKeyVault --key-permissions decrypt encrypt --object-id $IDENTITY_OBJECT_ID
```

#### For RBAC key vault

If your key vault is enabled with `--enable-rbac-authorization`, you need to assign a RBAC role that contains decrypt, encrypt permission.

```
az role assignment create --role "Key Vault Crypto User" --assignee-object-id $IDENTITY_OBJECT_ID --
assignee-principal-type "ServicePrincipal" --scope $KEYVAULT_RESOURCE_ID
```

### Assign permission for creating private link

For private key vaults, you need the *Key Vault Contributor* role to create a private link between the private key vault and the cluster.

```
az role assignment create --role "Key Vault Contributor" --assignee-object-id $IDENTITY_OBJECT_ID --
assignee-principal-type "ServicePrincipal" --scope $KEYVAULT_RESOURCE_ID
```

### Create an AKS cluster with private key vault and enable KMS etcd encryption

Create an AKS cluster using the `az aks create` command with the `--enable-azure-keyvault-kms`, `--azure-keyvault-kms-key-id`, `--azure-keyvault-kms-key-vault-network-access` and `--azure-keyvault-kms-key-vault-resource-id` parameters to enable KMS etcd encryption with private key vault.

```
az aks create --name myAKSCluster --resource-group MyResourceGroup --assign-identity $IDENTITY_RESOURCE_ID -
--enable-azure-keyvault-kms --azure-keyvault-kms-key-id $KEY_ID --azure-keyvault-kms-key-vault-network-access
"Private" --azure-keyvault-kms-key-vault-resource-id $KEYVAULT_RESOURCE_ID
```

### Update an existing AKS cluster to enable KMS etcd encryption with private key vault

Use `az aks update` with the `--enable-azure-keyvault-kms`, `--azure-keyvault-kms-key-id`, `--azure-keyvault-kms-key-vault-network-access` and `--azure-keyvault-kms-key-vault-resource-id` parameters to enable KMS etcd encryption on an existing cluster with private key vault.

```
az aks update --name myAKSCluster --resource-group MyResourceGroup --enable-azure-keyvault-kms --azure-
keyvault-kms-key-id $KEY_ID --azure-keyvault-kms-key-vault-network-access "Private" --azure-keyvault-kms-
key-vault-resource-id $KEYVAULT_RESOURCE_ID
```

Use the following command to update all secrets. Otherwise, old secrets won't be encrypted. For larger clusters, you may want to subdivide the secrets by namespace or script an update.

```
kubectl get secrets --all-namespaces -o json | kubectl replace -f -
```

## Rotate the existing keys

After changing the key ID (including key name and key version), you can use `az aks update` with the `--enable-azure-keyvault-kms`, `--azure-keyvault-kms-key-id`, `--azure-keyvault-kms-key-vault-network-access` and `--azure-keyvault-kms-key-vault-resource-id` parameters to rotate the existing keys of KMS.

### WARNING

Remember to update all secrets after key rotation. Otherwise, the secrets will be inaccessible if the old keys are not existing or working.

```
az aks update --name myAKSCluster --resource-group MyResourceGroup --enable-azure-keyvault-kms --azure-keyvault-kms-key-id $NewKEY_ID --azure-keyvault-kms-key-vault-network-access "Private" --azure-keyvault-kms-key-vault-resource-id $KEYVAULT_RESOURCE_ID
```

Use the following command to update all secrets. Otherwise, old secrets will still be encrypted with the previous key. For larger clusters, you may want to subdivide the secrets by namespace or script an update.

```
kubectl get secrets --all-namespaces -o json | kubectl replace -f -
```

## Update key vault mode

### NOTE

To change a different key vault with a different mode (public, private), you can run `az aks update` directly. To change the mode of attached key vault, you need to disable KMS and re-enable it with the new key vault IDs.

Below are the steps about how to migrate the attached public key vault to private mode.

### Disable KMS on the cluster

Disable the KMS on existing cluster and release the key vault.

```
az aks update --name myAKSCluster --resource-group MyResourceGroup --disable-azure-keyvault-kms
```

### Change key vault mode

Update the key vault from public to private.

```
az keyvault update --name MyKeyVault --resource-group MyResourceGroup --public-network-access Disabled
```

### Enable KMS on the cluster with updated key vault

Re-enable the KMS with updated private key vault.

```
az aks update --name myAKSCluster --resource-group MyResourceGroup --enable-azure-keyvault-kms --azure-keyvault-kms-key-id $NewKEY_ID --azure-keyvault-kms-key-vault-network-access "Private" --azure-keyvault-kms-key-vault-resource-id $KEYVAULT_RESOURCE_ID
```

After configuring KMS, you can enable [diagnostic-settings for key vault to check the encryption logs](#).

## Disable KMS

Use the following command to disable KMS on existing cluster.

```
az aks update --name myAKSCluster --resource-group MyResourceGroup --disable-azure-keyvault-kms
```

Use the following command to update all secrets. Otherwise, the old secrets will still be encrypted with the previous key. For larger clusters, you may want to subdivide the secrets by namespace or script an update.

```
kubectl get secrets --all-namespaces -o json | kubectl replace -f -
```

# Update or rotate the credentials for Azure Kubernetes Service (AKS)

10/27/2022 • 5 minutes to read • [Edit Online](#)

AKS clusters created with a service principal have a one-year expiration time. As you near the expiration date, you can reset the credentials to extend the service principal for an additional period of time. You may also want to update, or rotate, the credentials as part of a defined security policy. This article details how to update these credentials for an AKS cluster.

You may also have [integrated your AKS cluster with Azure Active Directory \(Azure AD\)](#), and use it as an authentication provider for your cluster. In that case you will have 2 more identities created for your cluster, the Azure AD Server App and the Azure AD Client App, you may also reset those credentials.

Alternatively, you can use a managed identity for permissions instead of a service principal. Managed identities are easier to manage than service principals and do not require updates or rotations. For more information, see [Use managed identities](#).

## Before you begin

You need the Azure CLI version 2.0.65 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Update or create a new service principal for your AKS cluster

When you want to update the credentials for an AKS cluster, you can choose to either:

- Update the credentials for the existing service principal.
- Create a new service principal and update the cluster to use these new credentials.

### WARNING

If you choose to create a *new* service principal, wait around 30 minutes for the service principal permission to propagate across all regions. Updating a large AKS cluster to use these credentials may take a long time to complete.

## Check the expiration date of your service principal

To check the expiration date of your service principal, use the `az ad sp credential list` command. The following example gets the service principal ID for the cluster named *myAKSCluster* in the *myResourceGroup* resource group using the `az aks show` command. The service principal ID is set as a variable named *SP\_ID* for use with the `az ad sp credential list` command.

```
SP_ID=$(az aks show --resource-group myResourceGroup --name myAKSCluster \
 --query servicePrincipalProfile.clientId -o tsv)
az ad sp credential list --id "$SP_ID" --query "[].endDateTime" -o tsv
```

## Reset the existing service principal credential

To update the credentials for the existing service principal, get the service principal ID of your cluster using the `az aks show` command. The following example gets the ID for the cluster named *myAKSCluster* in the *myResourceGroup* resource group. The service principal ID is set as a variable named *SP\_ID* for use in additional command. These commands use Bash syntax.

## WARNING

When you reset your cluster credentials on an AKS cluster that uses Azure Virtual Machine Scale Sets, a [node image upgrade](#) is performed to update your nodes with the new credential information.

```
SP_ID=$(az aks show --resource-group myResourceGroup --name myAKSCluster \
--query servicePrincipalProfile.clientId -o tsv)
```

With a variable set that contains the service principal ID, now reset the credentials using [az ad sp credential reset](#). The following example lets the Azure platform generate a new secure secret for the service principal. This new secure secret is also stored as a variable.

```
SP_SECRET=$(az ad sp credential reset --id "$SP_ID" --query password -o tsv)
```

Now continue on to [update AKS cluster with new service principal credentials](#). This step is necessary for the Service Principal changes to reflect on the AKS cluster.

### Create a new service principal

If you chose to update the existing service principal credentials in the previous section, skip this step. Continue to [update AKS cluster with new service principal credentials](#).

To create a service principal and then update the AKS cluster to use these new credentials, use the [az ad sp create-for-rbac](#) command.

```
az ad sp create-for-rbac --role Contributor --scopes /subscriptions/mySubscriptionID
```

The output is similar to the following example. Make a note of your own `appId` and `password`. These values are used in the next step.

```
{
 "appId": "7d837646-b1f3-443d-874c-fd83c7c739c5",
 "name": "7d837646-b1f3-443d-874c-fd83c7c739c",
 "password": "a5ce83c9-9186-426d-9183-614597c7f2f7",
 "tenant": "a4342dc8-cd0e-4742-a467-3129c469d0e5"
}
```

Now define variables for the service principal ID and client secret using the output from your own [az ad sp create-for-rbac](#) command, as shown in the following example. The `SP_ID` is your `appId`, and the `SP_SECRET` is your `password`.

```
SP_ID=7d837646-b1f3-443d-874c-fd83c7c739c5
SP_SECRET=a5ce83c9-9186-426d-9183-614597c7f2f7
```

Now continue on to [update AKS cluster with new service principal credentials](#). This step is necessary for the Service Principal changes to reflect on the AKS cluster.

## Update AKS cluster with new service principal credentials

## IMPORTANT

For large clusters, updating the AKS cluster with a new service principal may take a long time to complete. Consider reviewing and customizing the [node surge upgrade settings](#) to minimize disruption during cluster updates and upgrades.

Regardless of whether you chose to update the credentials for the existing service principal or create a service principal, you now update the AKS cluster with your new credentials using the [az aks update-credentials](#) command. The variables for the `--service-principal` and `--client-secret` are used:

```
az aks update-credentials \
--resource-group myResourceGroup \
--name myAKScluster \
--reset-service-principal \
--service-principal "$SP_ID" \
--client-secret "${SP_SECRET:Q}"
```

## NOTE

`${SP_SECRET:Q}` escapes any special characters in `SP_SECRET`, which can cause the command to fail. The above example works for Azure Cloud Shell and zsh terminals. For BASH terminals, use  `${SP_SECRET@Q}` .

For small and midsize clusters, it takes a few moments for the service principal credentials to be updated in the AKS.

## Update AKS Cluster with new Azure AD Application credentials

You may create new Azure AD Server and Client applications by following the [Azure AD integration steps](#). Or reset your existing Azure AD Applications following the [same method as for service principal reset](#). After that you just need to update your cluster Azure AD Application credentials using the same [az aks update-credentials](#) command but using the `--reset-aad` variables.

```
az aks update-credentials \
--resource-group myResourceGroup \
--name myAKScluster \
--reset-aad \
--aad-server-app-id <SERVER APPLICATION ID> \
--aad-server-app-secret <SERVER APPLICATION SECRET> \
--aad-client-app-id <CLIENT APPLICATION ID>
```

## Next steps

In this article, the service principal for the AKS cluster itself and the Azure AD Integration Applications were updated. For more information on how to manage identity for workloads within a cluster, see [Best practices for authentication and authorization in AKS](#).

# AKS-managed Azure Active Directory integration

10/27/2022 • 11 minutes to read • [Edit Online](#)

AKS-managed Azure AD integration simplifies the Azure AD integration process. Previously, users were required to create a client and server app, and required the Azure AD tenant to grant Directory Read permissions. In the new version, the AKS resource provider manages the client and server apps for you.

## Azure AD authentication overview

Cluster administrators can configure Kubernetes role-based access control (Kubernetes RBAC) based on a user's identity or directory group membership. Azure AD authentication is provided to AKS clusters with OpenID Connect. OpenID Connect is an identity layer built on top of the OAuth 2.0 protocol. For more information on OpenID Connect, see the [Open ID connect documentation](#).

Learn more about the Azure AD integration flow on the [Azure Active Directory integration concepts documentation](#).

## Limitations

- AKS-managed Azure AD integration can't be disabled
- Changing a AKS-managed Azure AD integrated cluster to legacy AAD is not supported
- Clusters without Kubernetes RBAC enabled aren't supported for AKS-managed Azure AD integration

## Prerequisites

- The Azure CLI version 2.29.0 or later
- Kubectl with a minimum version of [1.18.1](#) or [kubelogin](#)
- If you are using [helm](#), minimum version of helm 3.3.

### IMPORTANT

You must use Kubectl with a minimum version of 1.18.1 or kubelogin. The difference between the minor versions of Kubernetes and kubectl should not be more than 1 version. If you don't use the correct version, you will notice authentication issues.

To install kubectl and kubelogin, use the following commands:

```
sudo az aks install-cli
kubectl version --client
kubelogin --version
```

Use [these instructions](#) for other operating systems.

## Before you begin

For your cluster, you need an Azure AD group. This group will be registered as an admin group on the cluster to grant cluster admin permissions. You can use an existing Azure AD group, or create a new one. Record the object ID of your Azure AD group.

```
List existing groups in the directory
az ad group list --filter "displayname eq '<group-name>'" -o table
```

To create a new Azure AD group for your cluster administrators, use the following command:

```
Create an Azure AD group
az ad group create --display-name myAKSAdminGroup --mail-nickname myAKSAdminGroup
```

## Create an AKS cluster with Azure AD enabled

Create an AKS cluster by using the following CLI commands.

Create an Azure resource group:

```
Create an Azure resource group
az group create --name myResourceGroup --location centralus
```

Create an AKS cluster, and enable administration access for your Azure AD group

```
Create an AKS-managed Azure AD cluster
az aks create -g myResourceGroup -n myManagedCluster --enable-aad --aad-admin-group-object-ids <id> [--aad-tenant-id <id>]
```

A successful creation of an AKS-managed Azure AD cluster has the following section in the response body

```
"AADProfile": {
 "adminGroupObjectIds": [
 "5d24****-****-****-****-****afa27aed"
],
 "clientAppId": null,
 "managed": true,
 "serverAppId": null,
 "serverAppSecret": null,
 "tenantId": "72f9****-****-****-****-****d011db47"
}
```

Once the cluster is created, you can start accessing it.

## Access an Azure AD enabled cluster

Before you access the cluster using an Azure AD defined group, you'll need the [Azure Kubernetes Service Cluster User](#) built-in role.

Get the user credentials to access the cluster:

```
az aks get-credentials --resource-group myResourceGroup --name myManagedCluster
```

Follow the instructions to sign in.

Use the kubectl get nodes command to view nodes in the cluster:

```
kubectl get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-15306047-0	Ready	agent	102m	v1.15.10
aks-nodepool1-15306047-1	Ready	agent	102m	v1.15.10
aks-nodepool1-15306047-2	Ready	agent	102m	v1.15.10

Configure [Azure role-based access control \(Azure RBAC\)](#) to configure additional security groups for your clusters.

## Troubleshooting access issues with Azure AD

### IMPORTANT

The steps described below are bypassing the normal Azure AD group authentication. Use them only in an emergency.

If you're permanently blocked by not having access to a valid Azure AD group with access to your cluster, you can still obtain the admin credentials to access the cluster directly.

To do these steps, you'll need to have access to the [Azure Kubernetes Service Cluster Admin](#) built-in role.

```
az aks get-credentials --resource-group myResourceGroup --name myManagedCluster --admin
```

## Enable AKS-managed Azure AD Integration on your existing cluster

You can enable AKS-managed Azure AD Integration on your existing Kubernetes RBAC enabled cluster. Ensure to set your admin group to keep access on your cluster.

```
az aks update -g MyResourceGroup -n MyManagedCluster --enable-aad --aad-admin-group-object-ids <id-1> [--aad-tenant-id <id>]
```

A successful activation of an AKS-managed Azure AD cluster has the following section in the response body

```
"AADProfile": {
 "adminGroupObjectIds": [
 "5d24****-****-****-****-****afa27aed"
],
 "clientAppId": null,
 "managed": true,
 "serverAppId": null,
 "serverAppSecret": null,
 "tenantId": "72f9****-****-****-****-****d011db47"
}
```

Download user credentials again to access your cluster by following the steps [here](#).

## Upgrading to AKS-managed Azure AD Integration

If your cluster uses legacy Azure AD integration, you can upgrade to AKS-managed Azure AD Integration.

```
az aks update -g myResourceGroup -n myManagedCluster --enable-aad --aad-admin-group-object-ids <id> [--aad-tenant-id <id>]
```

A successful migration of an AKS-managed Azure AD cluster has the following section in the response body

```
"AADProfile": {
 "adminGroupObjectIds": [
 "5d24****-****-****-****-****afa27aed"
],
 "clientAppId": null,
 "managed": true,
 "serverAppId": null,
 "serverAppSecret": null,
 "tenantId": "72f9****-****-****-****-****d011db47"
}
```

Update kubeconfig in order to access the cluster, follow the steps [here](#).

## Non-interactive sign in with kubelogin

There are some non-interactive scenarios, such as continuous integration pipelines, that aren't currently available with kubectl. You can use [kubelogin](#) to access the cluster with non-interactive service principal sign-in.

## Disable local accounts

When deploying an AKS Cluster, local accounts are enabled by default. Even when enabling RBAC or Azure Active Directory integration, `--admin` access still exists, essentially as a non-auditable backdoor option. With this in mind, AKS offers users the ability to disable local accounts via a flag, `disable-local-accounts`. A field, `properties.disableLocalAccounts`, has also been added to the managed cluster API to indicate whether the feature has been enabled on the cluster.

### NOTE

On clusters with Azure AD integration enabled, users belonging to a group specified by `aad-admin-group-object-ids` will still be able to gain access via non-admin credentials. On clusters without Azure AD integration enabled and `properties.disableLocalAccounts` set to true, obtaining both user and admin credentials will fail.

### NOTE

After disabling local accounts users on an already existing AKS cluster where users might have used local account/s, admin must [rotate the cluster certificates](#), in order to revoke the certificates those users might have access to. If this is a new cluster then no action is required.

## Create a new cluster without local accounts

To create a new AKS cluster without any local accounts, use the `az aks create` command with the `disable-local-accounts` flag:

```
az aks create -g <resource-group> -n <cluster-name> --enable-aad --aad-admin-group-object-ids <aad-group-id>
--disable-local-accounts
```

In the output, confirm local accounts have been disabled by checking the field `properties.disableLocalAccounts` is set to true:

```
"properties": {
 ...
 "disableLocalAccounts": true,
 ...
}
```

Attempting to get admin credentials will fail with an error message indicating the feature is preventing access:

```
az aks get-credentials --resource-group <resource-group> --name <cluster-name> --admin

Operation failed with status: 'Bad Request'. Details: Getting static credential is not allowed because this
cluster is set to disable local accounts.
```

### Disable local accounts on an existing cluster

To disable local accounts on an existing AKS cluster, use the [az aks update](#) command with the `disable-local-accounts` flag:

```
az aks update -g <resource-group> -n <cluster-name> --enable-aad --aad-admin-group-object-ids <aad-group-id>
--disable-local-accounts
```

In the output, confirm local accounts have been disabled by checking the field `properties.disableLocalAccounts` is set to true:

```
"properties": {
 ...
 "disableLocalAccounts": true,
 ...
}
```

Attempting to get admin credentials will fail with an error message indicating the feature is preventing access:

```
az aks get-credentials --resource-group <resource-group> --name <cluster-name> --admin

Operation failed with status: 'Bad Request'. Details: Getting static credential is not allowed because this
cluster is set to disable local accounts.
```

### Re-enable local accounts on an existing cluster

AKS also offers the ability to re-enable local accounts on an existing cluster with the `enable-local` flag:

```
az aks update -g <resource-group> -n <cluster-name> --enable-aad --aad-admin-group-object-ids <aad-group-id>
--enable-local
```

In the output, confirm local accounts have been re-enabled by checking the field `properties.disableLocalAccounts` is set to false:

```
"properties": {
 ...
 "disableLocalAccounts": false,
 ...
}
```

Attempting to get admin credentials will succeed:

```
az aks get-credentials --resource-group <resource-group> --name <cluster-name> --admin
```

```
Merged "<cluster-name>-admin" as current context in C:\Users\<username>\.kube\config
```

## Use Conditional Access with Azure AD and AKS

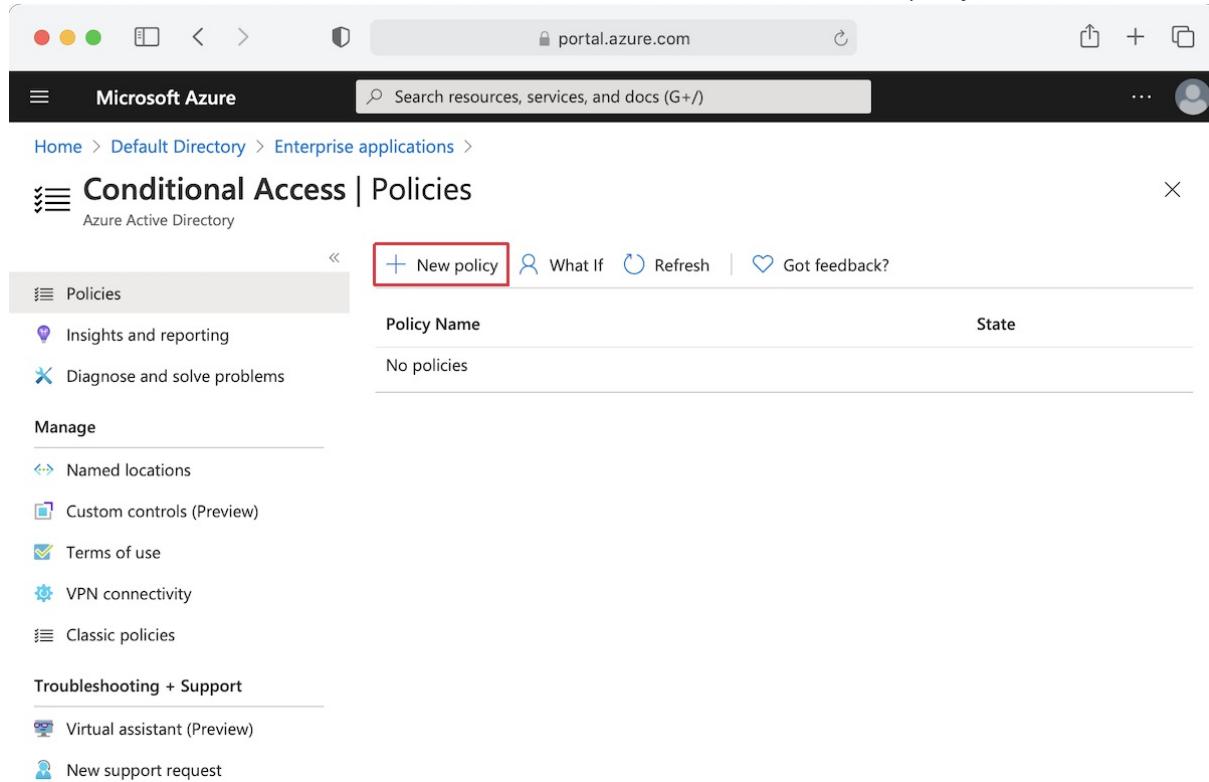
When integrating Azure AD with your AKS cluster, you can also use [Conditional Access](#) to control access to your cluster.

### NOTE

Azure AD Conditional Access is an Azure AD Premium capability.

To create an example Conditional Access policy to use with AKS, complete the following steps:

1. At the top of the Azure portal, search for and select Azure Active Directory.
2. In the menu for Azure Active Directory on the left-hand side, select *Enterprise applications*.
3. In the menu for Enterprise applications on the left-hand side, select *Conditional Access*.
4. In the menu for Conditional Access on the left-hand side, select *Policies* then *New policy*.



The screenshot shows the Microsoft Azure Conditional Access Policies page. The URL in the browser is portal.azure.com. The main heading is "Conditional Access | Policies". On the left, there's a sidebar with sections like "Policies", "Insights and reporting", "Diagnose and solve problems", "Manage", "Named locations", "Custom controls (Preview)", "Terms of use", "VPN connectivity", and "Classic policies". Below the sidebar, there's a "Troubleshooting + Support" section with "Virtual assistant (Preview)" and "New support request". At the top right, there are buttons for "New policy" (which is highlighted with a red box), "What If", "Refresh", and "Got feedback?". The main table area shows one row: "Policy Name" is "No policies" and "State" is "None".

5. Enter a name for the policy such as *aks-policy*.
6. Select *Users and groups*, then under *Include* select *Select users and groups*. Choose the users and groups where you want to apply the policy. For this example, choose the same Azure AD group that has administration access to your cluster.

## New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Example: 'Device compliance app policy'

### Assignments

Users and groups ⓘ



Specific users included

Cloud apps or actions ⓘ



No cloud apps or actions selected

Conditions ⓘ



0 conditions selected

### Access controls

Grant ⓘ



0 controls selected

Session ⓘ



0 controls selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users

[Learn more](#)

**Include**    **Exclude**

None

All users

Select users and groups

All guest and external users ⓘ

Directory roles ⓘ

Users and groups

Select



1 group

MY

myAKSAdminGroup

...

7. Select *Cloud apps or actions*, then under *Include* select *Select apps*. Search for *Azure Kubernetes Service* and select *Azure Kubernetes Service AAD Server*.

# New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Example: 'Device compliance app policy'

## Assignments

Users and groups ⓘ



Specific users included

Cloud apps or actions ⓘ



1 app included

Conditions ⓘ



0 conditions selected

## Access controls

Grant ⓘ



0 controls selected

Session ⓘ



0 controls selected

Control user access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

[Cloud apps](#)[User actions](#)
[Include](#)   [Exclude](#)
 None All cloud apps Select apps

Select



Azure Kubernetes Service AAD S...

AK

Azure Kubernetes Service AAD ! ...  
6dae42f8-4368-4678-94ff-3960e28e36...

8. Under *Access controls*, select *Grant*. Select *Grant access* then *Require device to be marked as compliant*.

# New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Example: 'Device compliance app policy'

## Assignments

Users and groups ⓘ



Specific users included

Cloud apps or actions ⓘ



1 app included

Conditions ⓘ



0 conditions selected

## Access controls

Grant ⓘ



0 controls selected

Session ⓘ



0 controls selected

## Grant



Control user access enforcement to block or grant access. [Learn more](#)

 Block access Grant access Require multi-factor authentication ⓘ Require device to be marked as compliant ⓘ Require Hybrid Azure AD joined device ⓘ Require approved client app ⓘ  
[See list of approved client apps](#) Require app protection policy ⓘ  
[See list of policy protected client apps](#) Require password change ⓘ

For multiple controls

 Require all the selected controls Require one of the selected controls
 Don't lock yourself out! Make sure that your device is compliant.

9. Under *Enable policy*, select *On* then *Create*.

Home > Default Directory > Enterprise applications > Conditional Access >

## New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Example: 'Device compliance app policy'

### Assignments

Users and groups ⓘ >

Specific users included

Cloud apps or actions ⓘ >

1 app included

Conditions ⓘ >

0 conditions selected

### Access controls

Grant ⓘ >

1 control selected

Session ⓘ >

0 controls selected

### Enable policy

Report-only  On  Off

**Create**

Get the user credentials to access the cluster, for example:

```
az aks get-credentials --resource-group myResourceGroup --name myManagedCluster
```

Follow the instructions to sign in.

Use the `kubectl get nodes` command to view nodes in the cluster:

```
kubectl get nodes
```

Follow the instructions to sign in again. Notice there is an error message stating you are successfully logged in, but your admin requires the device requesting access to be managed by your Azure AD to access the resource.

In the Azure portal, navigate to Azure Active Directory, select *Enterprise applications* then under *Activity* select *Sign-ins*. Notice an entry at the top with a *Status* of *Failed* and a *Conditional Access* of *Success*. Select the entry then select *Conditional Access* in *Details*. Notice your Conditional Access policy is listed.

Details							
Basic info	Location	Device info	Authentication Details	Conditional Access	Report-only	Additional Details	Troubleshooting and support
Policy Name ↑↓	Grant Controls ↑↓		Session Controls ↑↓		Result ↑↓		
<a href="#">aks-policy</a>	require compliant device				Failure		
A sign-in can also be interrupted (e.g. blocked, MFA challenged) because of a user risk policy or sign-in risk policy. Currently, this tab only lists Conditional Access policies.							

## Configure just-in-time cluster access with Azure AD and AKS

Another option for cluster access control is to use Privileged Identity Management (PIM) for just-in-time requests.

### NOTE

PIM is an Azure AD Premium capability requiring a Premium P2 SKU. For more on Azure AD SKUs, see the [pricing guide](#).

To integrate just-in-time access requests with an AKS cluster using AKS-managed Azure AD integration, complete the following steps:

1. At the top of the Azure portal, search for and select Azure Active Directory.
2. Take note of the Tenant ID, referred to for the rest of these instructions as `<tenant-id>`

The screenshot shows the Azure Active Directory Overview page. On the left, there's a navigation menu with sections like Overview, Getting started, Preview hub, and Diagnose and solve problems. Under Manage, there are links for Users, Groups, External Identities, Roles and administrators, Administrative units, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Licenses, Azure AD Connect, Custom domain names, and Mobility (MDM and MAM). The main content area has a section titled 'Default Directory' with a search bar. Below it are two boxes: 'Tenant information' (containing Your role: Global administrator, License: Azure AD Premium P2, Tenant ID: 4ee91c09-89de-4e00-8214-515f..., Primary domain: user.contoso.com) and 'Azure AD Connect' (Status: Not enabled, Last sync: Sync has never run). A red box highlights the Tenant ID field.

3. In the menu for Azure Active Directory on the left-hand side, under *Manage* select *Groups* then *New Group*.

The screenshot shows the 'Groups | All groups (Preview)' page. The left sidebar includes links for All groups (Preview), Deleted groups, and Diagnose and solve problems. Under Settings, there are General, Expiration, and Naming policy options. Activity links include Privileged access groups (Preview), Access reviews, Audit logs, and Bulk operation results. Troubleshooting + Support includes a New support request link. At the top, there's a toolbar with 'New group' (highlighted with a red box), Download groups, Delete, Refresh, Columns, Preview features, and more. Below the toolbar, a message says 'This page includes previews available for your evaluation. View previews →'. A search bar and filter options are also present. The main area shows a table with columns: Name, Object Id, Group Type, Membership Ty..., Email, and Source. The table displays 'No groups found'.

4. Make sure a Group Type of *Security* is selected and enter a group name, such as *myJITGroup*. Under *Azure AD Roles can be assigned to this group (Preview)*, select *Yes*. Finally, select *Create*.

Microsoft Azure Search resources, services, and docs (G+)

Home > Default Directory > Groups > New Group

Group type \* ①  
Security

Group name \* ①  
myJITGroup

Group description ①  
Enter a description for the group

Azure AD roles can be assigned to the group (Preview) ①  
 Yes  No

Membership type ①  
Assigned

Owners  
No owners selected

Members  
No members selected

Roles  
No roles selected

**Create**

5. You will be brought back to the *Groups* page. Select your newly created group and take note of the Object ID, referred to for the rest of these instructions as `<object-id>`.

Microsoft Azure Search resources, services, and docs (G+)

Home > myJITGroup

**myJITGroup** Group

**Overview (Preview)**

**Diagnose and solve problems**

**Manage**

- Properties
- Members (Preview)
- Owners (Preview)
- Administrative units
- Group memberships (Preview)
- Assigned roles (Preview)
- Applications
- Licenses
- Azure role assignments

**Activity**

- Privileged access (Preview)
- Access reviews
- Audit logs
- Bulk operation results

**Troubleshooting + Support**

New support request

**MY** myJITGroup

**Membership type**: Assigned

**Source**: Cloud

**Type**: Security

**Object Id**: b91afa54-4717-41ef-912a-a0ace8e42e76

**Creation date**: 2/17/2021, 2:10:34 PM

**Direct members**: 0 Total, 0 User(s), 0 Group(s), 0 Device(s), 0 Other(s)

**Group memberships**: 0

**Owners**: 0

**Total members**: 0

6. Deploy an AKS cluster with AKS-managed Azure AD integration by using the `<tenant-id>` and `<object-id>` values from earlier:

```
az aks create -g myResourceGroup -n myManagedCluster --enable-aad --aad-admin-group-object-ids
<object-id> --aad-tenant-id <tenant-id>
```

7. Back in the Azure portal, in the menu for *Activity* on the left-hand side, select *Privileged Access (Preview)* and

select *Enable Privileged Access*.

The screenshot shows the Microsoft Azure Groups page for a group named "myJITGroup". On the left, there's a sidebar with sections like "Manage", "Activity", and "Troubleshooting + Support". Under "Activity", "Privileged access (Preview)" is selected. In the main content area, there's a large "Enable Privileged Access" button with a blue border. Below it, there's a section titled "Privileged Access Groups enable just-in-time (JIT) access to the Owner or Member role of this group. JIT access by Azure AD PIM provides enhanced security for owners with delegated administrative tasks." To the right of this text are two cards: "Learn more about Privileged Access Groups" (with a people icon) and "Activate more in less time" (with a gear icon). At the bottom of the main content area is a "Feedback" card.

8. Select *Add Assignments* to begin granting access.

The screenshot shows the Microsoft Azure Groups page for "myJITGroup". The "Activity" sidebar is open, showing "Privileged access (Preview)" is selected. In the main content area, there's a header with "Add assignments" highlighted with a red box. Below the header, there are tabs for "Eligible assignments", "Active assignments" (which is selected), and "Expired assignments". A search bar allows searching by member name or principal name. A table below shows "No results".

9. Select a role of *member*, and select the users and groups to whom you wish to grant cluster access. These assignments can be modified at any time by a group admin. When you're ready to move on, select *Next*.

Microsoft Azure Search resources, services, and docs (G+) Home > Default Directory > Groups > myJITGroup >

## Add assignments

Privileged Identity Management | Privileged access groups (Preview)

**Membership** **Setting**

Resource  
myJITGroup

Resource type  
Security

Select role ⓘ  
Member

Select member(s) \* ⓘ  
1 Member(s) selected

Selected member(s) ⓘ

 Test User  
user\_contoso.com#EXT#@user.contoso.com Remove

---

**Next >** **Cancel**

10. Choose an assignment type of *Active*, the desired duration, and provide a justification. When you're ready to proceed, select *Assign*. For more on assignment types, see [Assign eligibility for a privileged access group \(preview\)](#) in Privileged Identity Management.

Microsoft Azure Search resources, services, and docs (G+) Home > Default Directory > Groups > myJITGroup >

## Add assignments

Privileged Identity Management | Privileged access groups (Preview)

**Membership** **Setting**

Assignment type ⓘ  
 Eligible  
 Active

Maximum allowed assignment duration is 6 month(s).

Assignment starts \*  
02/17/2021 3:34:59 PM

Assignment ends \*  
08/16/2021 4:34:59 PM

Enter justification \*  
AKS cluster access

---

**Assign** **< Prev** **Cancel**

Once the assignments have been made, verify just-in-time access is working by accessing the cluster. For example:

```
az aks get-credentials --resource-group myResourceGroup --name myManagedCluster
```

Follow the steps to sign in.

Use the `kubectl get nodes` command to view nodes in the cluster:

```
kubectl get nodes
```

Note the authentication requirement and follow the steps to authenticate. If successful, you should see output similar to the following:

```
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
AAAAAAA to authenticate.
```

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-61156405-vmss000000	Ready	agent	6m36s	v1.18.14
aks-nodepool1-61156405-vmss000001	Ready	agent	6m42s	v1.18.14
aks-nodepool1-61156405-vmss000002	Ready	agent	6m33s	v1.18.14

## Apply Just-in-Time access at the namespace level

1. Integrate your AKS cluster with [Azure RBAC](#).
2. Associate the group you want to integrate with Just-in-Time access with a namespace in the cluster through role assignment.

```
az role assignment create --role "Azure Kubernetes Service RBAC Reader" --assignee <AAD-ENTITY-ID> --scope
$AKS_ID/namespaces/<namespace-name>
```

3. Associate the group you just configured at the namespace level with PIM to complete the configuration.

## Troubleshooting

If `kubectl get nodes` returns an error similar to the following:

```
Error from server (Forbidden): nodes is forbidden: User "aaaa1111-11aa-aa11-a1a1-111111aaaa" cannot list
resource "nodes" in API group "" at the cluster scope
```

Make sure the admin of the security group has given your account an *Active* assignment.

## Next steps

- Learn about [Azure RBAC integration for Kubernetes Authorization](#)
- Learn about [Azure AD integration with Kubernetes RBAC](#).
- Use [kubelogin](#) to access features for Azure authentication that aren't available in kubectl.
- Learn more about [AKS and Kubernetes identity concepts](#).
- Use [Azure Resource Manager \(ARM\) templates](#) to create AKS-managed Azure AD enabled clusters.

# Integrate Azure Active Directory with Azure Kubernetes Service using the Azure CLI (legacy)

10/27/2022 • 8 minutes to read • [Edit Online](#)

## WARNING

\*\*The feature described in this document, Azure AD Integration (legacy), will be deprecated on February 29th 2024.

AKS has a new improved [AKS-managed Azure AD](#) experience that doesn't require you to manage server or client application. If you want to migrate follow the instructions [here](#).

Azure Kubernetes Service (AKS) can be configured to use Azure Active Directory (AD) for user authentication. In this configuration, you can log into an AKS cluster using an Azure AD authentication token. Cluster operators can also configure Kubernetes role-based access control (Kubernetes RBAC) based on a user's identity or directory group membership.

This article shows you how to create the required Azure AD components, then deploy an Azure AD-enabled cluster and create a basic Kubernetes role in the AKS cluster.

For the complete sample script used in this article, see [Azure CLI samples - AKS integration with Azure AD] [complete-script].

## The following limitations apply:

- Azure AD can only be enabled on Kubernetes RBAC-enabled cluster.
- Azure AD legacy integration can only be enabled during cluster creation.

## Before you begin

You need the Azure CLI version 2.0.61 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

Go to <https://shell.azure.com> to open Cloud Shell in your browser.

For consistency and to help run the commands in this article, create a variable for your desired AKS cluster name. The following example uses the name *myakscluster*.

```
aksname="myakscluster"
```

## Azure AD authentication overview

Azure AD authentication is provided to AKS clusters with OpenID Connect. OpenID Connect is an identity layer built on top of the OAuth 2.0 protocol. For more information on OpenID Connect, see the [Open ID connect documentation](#).

From inside of the Kubernetes cluster, Webhook Token Authentication is used to verify authentication tokens. Webhook token authentication is configured and managed as part of the AKS cluster. For more information on Webhook token authentication, see the [webhook authentication documentation](#).

#### NOTE

When configuring Azure AD for AKS authentication, two Azure AD applications are configured. This operation must be completed by an Azure tenant administrator.

## Create Azure AD server component

To integrate with AKS, you create and use an Azure AD application that acts as an endpoint for the identity requests. The first Azure AD application you need gets Azure AD group membership for a user.

Create the server application component using the [az ad app create](#) command, then update the group membership claims using the [az ad app update](#) command. The following example uses the *aksname* variable defined in the [Before you begin](#) section, and creates a variable

```
Create the Azure AD application
serverApplicationId=$(az ad app create \
 --display-name "${aksname}Server" \
 --identifier-uris "https://${aksname}Server" \
 --query appId -o tsv)

Update the application group membership claims
az ad app update --id $serverApplicationId --set groupMembershipClaims=All
```

Now create a service principal for the server app using the [az ad sp create](#) command. This service principal is used to authenticate itself within the Azure platform. Then, get the service principal secret using the [az ad sp credential reset](#) command and assign to the variable named *serverApplicationSecret* for use in one of the following steps:

```
Create a service principal for the Azure AD application
az ad sp create --id $serverApplicationId

Get the service principal secret
serverApplicationSecret=$(az ad sp credential reset \
 --name $serverApplicationId \
 --credential-description "AKSPassword" \
 --query password -o tsv)
```

The Azure AD service principal needs permissions to perform the following actions:

- Read directory data
- Sign in and read user profile

Assign these permissions using the [az ad app permission add](#) command:

```
az ad app permission add \
 --id $serverApplicationId \
 --api 00000003-0000-0000-000000000000 \
 --api-permissions e1fe6dd8-ba31-4d61-89e7-88639da4683d=Scope 06da0dbc-49e2-44d2-8312-53f166ab848a=Scope
7ab1d382-f21e-4acd-a863-ba3e13f7da61=Role
```

Finally, grant the permissions assigned in the previous step for the server application using the [az ad app permission grant](#) command. This step fails if the current account is not a tenant admin. You also need to add permissions for Azure AD application to request information that may otherwise require administrative consent using the [az ad app permission admin-consent](#):

```
az ad app permission grant --id $serverApplicationId --api 00000003-0000-0000-c000-000000000000
az ad app permission admin-consent --id $serverApplicationId
```

## Create Azure AD client component

The second Azure AD application is used when a user logs to the AKS cluster with the Kubernetes CLI (`kubectl`). This client application takes the authentication request from the user and verifies their credentials and permissions. Create the Azure AD app for the client component using the [az ad app create](#) command:

```
clientApplicationId=$(az ad app create \
--display-name "${aksname}Client" \
--native-app \
--reply-urls "https://${aksname}Client" \
--query appId -o tsv)
```

Create a service principal for the client application using the [az ad sp create](#) command:

```
az ad sp create --id $clientApplicationId
```

Get the oAuth2 ID for the server app to allow the authentication flow between the two app components using the [az ad app show](#) command. This oAuth2 ID is used in the next step.

```
oAuthPermissionId=$(az ad app show --id $serverApplicationId --query "oauth2Permissions[0].id" -o tsv)
```

Add the permissions for the client application and server application components to use the oAuth2 communication flow using the [az ad app permission add](#) command. Then, grant permissions for the client application to communicate with the server application using the [az ad app permission grant](#) command:

```
az ad app permission add --id $clientApplicationId --api $serverApplicationId --api-permissions
${oAuthPermissionId}=Scope
az ad app permission grant --id $clientApplicationId --api $serverApplicationId
```

## Deploy the cluster

With the two Azure AD applications created, now create the AKS cluster itself. First, create a resource group using the [az group create](#) command. The following example creates the resource group in the *EastUS* region:

Create a resource group for the cluster:

```
az group create --name myResourceGroup --location EastUS
```

Get the tenant ID of your Azure subscription using the [az account show](#) command. Then, create the AKS cluster using the [az aks create](#) command. The command to create the AKS cluster provides the server and client application IDs, the server application service principal secret, and your tenant ID:

```
tenantId=$(az account show --query tenantId -o tsv)

az aks create \
 --resource-group myResourceGroup \
 --name $aksname \
 --node-count 1 \
 --generate-ssh-keys \
 --aad-server-app-id $serverApplicationId \
 --aad-server-app-secret $serverApplicationSecret \
 --aad-client-app-id $clientApplicationId \
 --aad-tenant-id $tenantId
```

Finally, get the cluster admin credentials using the [az aks get-credentials](#) command. In one of the following steps, you get the regular *user* cluster credentials to see the Azure AD authentication flow in action.

```
az aks get-credentials --resource-group myResourceGroup --name $aksname --admin
```

## Create Kubernetes RBAC binding

Before an Azure Active Directory account can be used with the AKS cluster, a role binding or cluster role binding needs to be created. *Roles* define the permissions to grant, and *bindings* apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster. For more information, see [Using Kubernetes RBAC authorization](#).

Get the user principal name (UPN) for the user currently logged in using the [az ad signed-in-user show](#) command. This user account is enabled for Azure AD integration in the next step.

```
az ad signed-in-user show --query userPrincipalName -o tsv
```

### IMPORTANT

If the user you grant the Kubernetes RBAC binding for is in the same Azure AD tenant, assign permissions based on the *userPrincipalName*. If the user is in a different Azure AD tenant, query for and use the *objectId* property instead.

Create a YAML manifest named `basic-azure-ad-binding.yaml` and paste the following contents. On the last line, replace *userPrincipalName\_or\_objectId* with the UPN or object ID output from the previous command:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
 name: contoso-cluster-admins
roleRef:
 apiGroup: rbac.authorization.k8s.io
 kind: ClusterRole
 name: cluster-admin
subjects:
- apiGroup: rbac.authorization.k8s.io
 kind: User
 name: userPrincipalName_or_objectId
```

Create the ClusterRoleBinding using the [kubectl apply](#) command and specify the filename of your YAML manifest:

```
kubectl apply -f basic-azure-ad-binding.yaml
```

## Access cluster with Azure AD

Now let's test the integration of Azure AD authentication for the AKS cluster. Set the `kubectl` config context to use regular user credentials. This context passes all authentication requests back through Azure AD.

```
az aks get-credentials --resource-group myResourceGroup --name $aksname --overwrite-existing
```

Now use the `kubectl get pods` command to view pods across all namespaces:

```
kubectl get pods --all-namespaces
```

You receive a sign in prompt to authenticate using Azure AD credentials using a web browser. After you've successfully authenticated, the `kubectl` command displays the pods in the AKS cluster, as shown in the following example output:

```
kubectl get pods --all-namespaces
```

```
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code BYMK7UXVD to authenticate.
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
kube-system	coredns-754f947b4-2v75r	1/1	Running	0	23h
kube-system	coredns-754f947b4-tghwh	1/1	Running	0	23h
kube-system	coredns-autoscaler-6fcdb7d64-4wkvp	1/1	Running	0	23h
kube-system	heapster-5fb7488d97-t5wzk	2/2	Running	0	23h
kube-system	kube-proxy-2nd5m	1/1	Running	0	23h
kube-system	kube-svc-redirect-swp9r	2/2	Running	0	23h
kube-system	kubernetes-dashboard-847bb4ddc6-trt7m	1/1	Running	0	23h
kube-system	metrics-server-7b97f9cd9-btxzz	1/1	Running	0	23h
kube-system	tunnelfront-6ff887cffb-xkfmq	1/1	Running	0	23h

The authentication token received for `kubectl` is cached. You are only repromted to sign in when the token has expired or the Kubernetes config file is re-created.

If you see an authorization error message after you've successfully signed in using a web browser as in the following example output, check the following possible issues:

```
error: You must be logged in to the server (Unauthorized)
```

- You defined the appropriate object ID or UPN, depending on if the user account is in the same Azure AD tenant or not.
- The user is not a member of more than 200 groups.
- Secret defined in the application registration for server matches the value configured using `--aad-server-app-secret`
- Be sure that only one version of kubectl is installed on your machine at a time. Conflicting versions can cause issues during authorization. To install the latest version, use `az aks install-cli`.

## Next steps

For the complete script that contains the commands shown in this article, see the [Azure AD integration script in the AKS samples repo][complete-script].

To use Azure AD users and groups to control access to cluster resources, see [Control access to cluster resources using Kubernetes role-based access control and Azure AD identities in AKS](#).

For more information about how to secure Kubernetes clusters, see [Access and identity options for AKS](#).

For best practices on identity and resource control, see [Best practices for authentication and authorization in AKS](#).

# Enable Group Managed Service Accounts (GMSA) for your Windows Server nodes on your Azure Kubernetes Service (AKS) cluster

10/27/2022 • 8 minutes to read • [Edit Online](#)

**Group Managed Service Accounts (GMSA)** is a managed domain account for multiple servers that provides automatic password management, simplified service principal name (SPN) management and the ability to delegate the management to other administrators. AKS provides the ability to enable GMSA on your Windows Server nodes, which allows containers running on Windows Server nodes to integrate with and be managed by GMSA.

## Pre-requisites

Enabling GMSA with Windows Server nodes on AKS requires:

- Kubernetes 1.19 or greater.
- Azure CLI version 2.35.0 or greater
- [Managed identities](#) with your AKS cluster.
- Permissions to create or update an Azure Key Vault.
- Permissions to configure GMSA on Active Directory Domain Service or on-prem Active Directory.
- The domain controller must have Active Directory Web Services enabled and must be reachable on port 9389 by the AKS cluster.

## Configure GMSA on Active Directory domain controller

To use GMSA with AKS, you need both GMSA and a standard domain user credential to access the GMSA credential configured on your domain controller. To configure GMSA on your domain controller, see [Getting Started with Group Managed Service Accounts](#). For the standard domain user credential, you can use an existing user or create a new one, as long as it has access to the GMSA credential.

### IMPORTANT

You must use either Active Directory Domain Service or on-prem Active Directory. At this time, you can't use Azure Active Directory to configure GMSA with an AKS cluster.

## Store the standard domain user credentials in Azure Key Vault

Your AKS cluster uses the standard domain user credentials to access the GMSA credentials from the domain controller. To provide secure access to those credentials for the AKS cluster, those credentials should be stored in Azure Key Vault. You can create a new key vault or use an existing key vault.

Use `az keyvault secret set` to store the standard domain user credential as a secret in your key vault. The following example stores the domain user credential with the key *GMSADomainUserCred* in the *MyAKSGMSAVault* key vault. You should replace the parameters with your own key vault, key, and domain user credential.

```
az keyvault secret set --vault-name MyAKSGMSAVault --name "GMSADomainUserCred" --value
"$Domain\\$DomainUsername:$DomainUserPassword"
```

#### NOTE

Use the Fully Qualified Domain Name for the Domain rather than the Partially Qualified Domain Name that may be used on internal networks.

The above command escapes the `value` parameter for running the Azure CLI on a Linux shell. When running the Azure CLI command on Windows PowerShell, you don't need to escape characters in the `value` parameter.

## Optional: Use a custom VNET with custom DNS

Your domain controller needs to be configured through DNS so it is reachable by the AKS cluster. You can configure your network and DNS outside of your AKS cluster to allow your cluster to access the domain controller. Alternatively, you can configure a custom VNET with a custom DNS using Azure CNI with your AKS cluster to provide access to your domain controller. For more details, see [Configure Azure CNI networking in Azure Kubernetes Service \(AKS\)](#).

## Optional: Use your own kubelet identity for your cluster

To provide the AKS cluster access to your key vault, the cluster kubelet identity needs access to your key vault. By default, when you create a cluster with managed identity enabled, a kubelet identity is automatically created. You can grant access to your key vault for this identity after cluster creation, which is done in a later step.

Alternatively, you can create your own identity and use this identity during cluster creation in a later step. For more details on the provided managed identities, see [Summary of managed identities](#).

To create your own identity, use `az identity create` to create an identity. The following example creates a *myIdentity* identity in the *myResourceGroup* resource group.

```
az identity create --name myIdentity --resource-group myResourceGroup
```

You can grant your kubelet identity access to your key vault before or after you create your cluster. The following example uses `az identity list` to get the id of the identity and set it to *MANAGED\_ID* then uses `az keyvault set-policy` to grant the identity access to the *MyAKSGMSAVault* key vault.

```
MANAGED_ID=$(az identity list --query "[].id" -o tsv)
az keyvault set-policy --name "MyAKSGMSAVault" --object-id $MANAGED_ID --secret-permissions get
```

## Create AKS cluster

To use GMSA with your AKS cluster, use the *enable-windows-gmsa*, *gmsa-dns-server*, *gmsa-root-domain-name*, and *enable-managed-identity* parameters.

#### NOTE

When creating a cluster with Windows Server node pools, you need to specify the administrator credentials when creating the cluster. The following commands prompt you for a username and set it `WINDOWS_USERNAME` for use in a later command (remember that the commands in this article are entered into a BASH shell).

```
echo "Please enter the username to use as administrator credentials for Windows Server nodes on your cluster: " && read WINDOWS_USERNAME
```

Use `az aks create` to create an AKS cluster then `az aks nodepool add` to add a Windows Server node pool. The following example creates a *MyAKS* cluster in the *MyResourceGroup* resource group, enables GMSA, and then adds a new node pool named *npwin*.

#### NOTE

If you are using a custom vnet, you also need to specify the id of the vnet using `vnet-subnet-id` and may need to also add `docker-bridge-address`, `dns-service-ip`, and `service-cidr` depending on your configuration.

If you created your own identity for the kubelet identity, use the `assign-kubelet-identity` parameter to specify your identity.

```
DNS_SERVER=<IP address of DNS server>
ROOT_DOMAIN_NAME="contoso.com"

az aks create \
 --resource-group MyResourceGroup \
 --name MyAKS \
 --vm-set-type VirtualMachineScaleSets \
 --network-plugin azure \
 --load-balancer-sku standard \
 --windows-admin-username $WINDOWS_USERNAME \
 --enable-managed-identity \
 --enable-windows-gmsa \
 --gmsa-dns-server $DNS_SERVER \
 --gmsa-root-domain-name $ROOT_DOMAIN_NAME

az aks nodepool add \
 --resource-group myResourceGroup \
 --cluster-name myAKS \
 --os-type Windows \
 --name npwin \
 --node-count 1
```

You can also enable GMSA on existing clusters that already have Windows Server nodes and managed identities enabled using `az aks update`. For example:

```
az aks update \
 --resource-group MyResourceGroup \
 --name MyAKS \
 --enable-windows-gmsa \
 --gmsa-dns-server $DNS_SERVER \
 --gmsa-root-domain-name $ROOT_DOMAIN_NAME
```

After creating your cluster or updating your cluster, use `az keyvault set-policy` to grant the identity access to your key vault. The following example grants the kubelet identity created by the cluster access to the *MyAKSGMSAVault* key vault.

#### NOTE

If you provided your own identity for the kubelet identity, skip this step.

```
MANAGED_ID=$(az aks show -g MyResourceGroup -n MyAKS --query "identityProfile.kubeletIdentity.objectId" -o tsv)

az keyvault set-policy --name "MyAKSGMSAVault" --object-id $MANAGED_ID --secret-permissions get
```

## Install GMSA cred spec

To configure `kubectl` to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command. The following example gets credentials for the AKS cluster named *MyAKS* in the *MyResourceGroup*.

```
az aks get-credentials --resource-group MyResourceGroup --name MyAKS
```

Create a *gmsa-spec.yaml* with the following, replacing the placeholders with your own values.

```
apiVersion: windows.k8s.io/v1alpha1
kind: GMSACredentialSpec
metadata:
 name: aks-gmsa-spec # This name can be changed, but it will be used as a reference in the pod spec
credspec:
 ActiveDirectoryConfig:
 GroupManagedServiceAccounts:
 - Name: $GMSA_ACCOUNT_USERNAME
 Scope: $NETBIOS_DOMAIN_NAME
 - Name: $GMSA_ACCOUNT_USERNAME
 Scope: $DNS_DOMAIN_NAME
 HostAccountConfig:
 PluginGUID: '{CCC2A336-D7F3-4818-A213-272B7924213E}'
 PortableCcgVersion: "1"
 PluginInput: ObjectId=$MANAGED_ID;SecretUri=$SECRET_URI # SECRET_URI takes the form
https://$akvName.vault.azure.net/secrets/$akvSecretName
 CmsPlugins:
 - ActiveDirectory
 DomainJoinConfig:
 DnsName: $DNS_DOMAIN_NAME
 DnsTreeName: $DNS_ROOT_DOMAIN_NAME
 Guid: $AD_DOMAIN_OBJECT_GUID
 MachineAccountName: $GMSA_ACCOUNT_USERNAME
 NetBiosName: $NETBIOS_DOMAIN_NAME
 Sid: $GMSA_SID
```

Create a *gmsa-role.yaml* with the following.

```
#Create the Role to read the credspec
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
 name: aks-gmsa-role
rules:
 - apiGroups: ["windows.k8s.io"]
 resources: ["gmsacredentialspecs"]
 verbs: ["use"]
 resourceNames: ["aks-gmsa-spec"]
```

Create a *gmsa-role-binding.yaml* with the following.

```

apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
 name: allow-default-svc-account-read-on-aks-gmsa-spec
 namespace: default
subjects:
- kind: ServiceAccount
 name: default
 namespace: default
roleRef:
 kind: ClusterRole
 name: aks-gmsa-role
 apiGroup: rbac.authorization.k8s.io

```

Use `kubectl apply` to apply the changes from `gmsa-spec.yaml`, `gmsa-role.yaml`, and `gmsa-role-binding.yaml`.

```

kubectl apply -f gmsa-spec.yaml
kubectl apply -f gmsa-role.yaml
kubectl apply -f gmsa-role-binding.yaml

```

## Verify GMSA is installed and working

Create a `gmsa-demo.yaml` with the following.

```

kind: ConfigMap
apiVersion: v1
metadata:
 labels:
 app: gmsa-demo
 name: gmsa-demo
 namespace: default
data:
 run.ps1: |
 $ErrorActionPreference = "Stop"

 Write-Output "Configuring IIS with authentication."

 # Add required Windows features, since they are not installed by default.
 Install-WindowsFeature "Web-Windows-Auth", "Web-Asp-Net45"

 # Create simple ASP.Net page.
 New-Item -Force -ItemType Directory -Path 'C:\inetpub\wwwroot\app'
 Set-Content -Path 'C:\inetpub\wwwroot\app\default.aspx' -Value 'Authenticated as
<%=User.Identity.Name%>, Type of Authentication: <%=User.Identity.AuthenticationType%>'

 # Configure IIS with authentication.
 Import-Module IISAdministration
 Start-IISCommitDelay
 (Get-IISConfigSection -SectionPath
 'system.webServer/security/authentication/windowsAuthentication').Attributes['enabled'].value = $true
 (Get-IISConfigSection -SectionPath
 'system.webServer/security/authentication/anonymousAuthentication').Attributes['enabled'].value = $false
 (Get-IIServerManager).Sites[0].Applications[0].VirtualDirectories[0].PhysicalPath =
 'C:\inetpub\wwwroot\app'
 Stop-IISCommitDelay

 Write-Output "IIS with authentication is ready."

 C:\ServiceMonitor.exe w3svc

apiVersion: apps/v1

```

```

kind: Deployment
metadata:
 labels:
 app: gmsa-demo
 name: gmsa-demo
 namespace: default
spec:
 replicas: 1
 selector:
 matchLabels:
 app: gmsa-demo
 template:
 metadata:
 labels:
 app: gmsa-demo
 spec:
 securityContext:
 windowsOptions:
 gmsaCredentialSpecName: aks-gmsa-spec
 containers:
 - name: iis
 image: mcr.microsoft.com/windows/servercore/iis:windowsservercore-ltsc2019
 imagePullPolicy: IfNotPresent
 command:
 - powershell
 args:
 - -File
 - /gmsa-demo/run.ps1
 volumeMounts:
 - name: gmsa-demo
 mountPath: /gmsa-demo
 volumes:
 - configMap:
 defaultMode: 420
 name: gmsa-demo
 name: gmsa-demo
 nodeSelector:
 kubernetes.io/os: windows

apiVersion: v1
kind: Service
metadata:
 labels:
 app: gmsa-demo
 name: gmsa-demo
 namespace: default
spec:
 ports:
 - port: 80
 targetPort: 80
 selector:
 app: gmsa-demo
 type: LoadBalancer

```

Use `kubectl apply` to apply the changes from `gmsa-demo.yaml`

```
kubectl apply -f gmsa-demo.yaml
```

Use `kubectl get service` to display the IP address of the example application.

```
kubectl get service gmsa-demo --watch
```

Initially the *EXTERNAL-IP* for the `gmsa-demo` service is shown as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
gmsa-demo	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

When the *EXTERNAL-IP* address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
gmsa-demo LoadBalancer 10.0.37.27 EXTERNAL-IP 80:30572/TCP 2m
```

To verify GMSA is working and configured correctly, open a web browser to the external IP address of *gmsa-demo* service. Authenticate with `$NETBIOS_DOMAIN_NAME\$AD_USERNAME` and password and confirm you see `Authenticated as $NETBIOS_DOMAIN_NAME\$AD_USERNAME, Type of Authentication: Negotiate`.

## Troubleshooting

### No authentication is prompted when loading the page

If the page loads, but you are not prompted to authenticate, use `kubelet logs POD_NAME` to display the logs of your pod and verify you see *IIS with authentication is ready*.

### Connection timeout when trying to load the page

If you receive a connection timeout when trying to load the page, verify the sample app is running with `kubectl get pods --watch`. Sometimes the external IP address for the sample app service is available before the sample app pod is running.

### Pod fails to start and an *winapi* error shows in the pod events

After running `kubectl get pods --watch` and waiting several minutes, if your pod does not start, run `kubectl describe pod POD_NAME`. If you see a *winapi* error in the pod events, this is likely an error in your GMSA cred spec configuration. Verify all the replacement values in *gmsa-spec.yaml* are correct, rerun `kubectl apply -f gmsa-spec.yaml`, and redeploy the sample application.

# Use Azure RBAC for Kubernetes Authorization

10/27/2022 • 6 minutes to read • [Edit Online](#)

Today you can already leverage [integrated authentication between Azure Active Directory \(Azure AD\) and AKS](#). When enabled, this integration allows customers to use Azure AD users, groups, or service principals as subjects in Kubernetes RBAC, see more [here](#). This feature frees you from having to separately manage user identities and credentials for Kubernetes. However, you still have to set up and manage Azure RBAC and Kubernetes RBAC separately. For more details on authentication and authorization with RBAC on AKS, see [here](#).

This document covers a new approach that allows for the unified management and access control across Azure Resources, AKS, and Kubernetes resources.

## Before you begin

The ability to manage RBAC for Kubernetes resources from Azure gives you the choice to manage RBAC for the cluster resources either using Azure or native Kubernetes mechanisms. When enabled, Azure AD principals will be validated exclusively by Azure RBAC while regular Kubernetes users and service accounts are exclusively validated by Kubernetes RBAC. For more details on authentication and authorization with RBAC on AKS, see [here](#).

### Prerequisites

- Ensure you have the Azure CLI version 2.24.0 or later
- Ensure you have installed [kubectl v1.18.3+](#).

### Limitations

- Requires [Managed Azure AD integration](#).
- Use [kubectl v1.18.3+](#).
- If you have CRDs and are making custom role definitions, the only way to cover CRDs today is to provide `Microsoft.ContainerService/managedClusters/*/read`. AKS is working on providing more granular permissions for CRDs. For the remaining objects you can use the specific API Groups, for example:  
`Microsoft.ContainerService/apps/deployments/read`.
- New role assignments can take up to 5min to propagate and be updated by the authorization server.
- Requires the Azure AD tenant configured for authentication to be the same as the tenant for the subscription that holds the AKS cluster.

## Create a new cluster using Azure RBAC and managed Azure AD integration

Create an AKS cluster by using the following CLI commands.

Create an Azure resource group:

```
Create an Azure resource group
az group create --name myResourceGroup --location westus2
```

Create the AKS cluster with managed Azure AD integration and Azure RBAC for Kubernetes Authorization.

```
Create an AKS-managed Azure AD cluster
az aks create -g MyResourceGroup -n MyManagedCluster --enable-aad --enable-azure-rbac
```

A successful creation of a cluster with Azure AD integration and Azure RBAC for Kubernetes Authorization has the following section in the response body:

```
"AADProfile": {
 "adminGroupObjectIds": null,
 "clientAppId": null,
 "enableAzureRbac": true,
 "managed": true,
 "serverAppId": null,
 "serverAppSecret": null,
 "tenantId": "*****-****-****-****-*****"
}
```

## Integrate Azure RBAC into an existing cluster

### NOTE

To use Azure RBAC for Kubernetes Authorization, Azure Active Directory integration must be enabled on your cluster. For more, see [Azure Active Directory integration](#).

To add Azure RBAC for Kubernetes Authorization into an existing AKS cluster, use the `az aks update` command with the flag `enable-azure-rbac`.

```
az aks update -g myResourceGroup -n myAKScluster --enable-azure-rbac
```

To remove Azure RBAC for Kubernetes Authorization from an existing AKS cluster, use the `az aks update` command with the flag `disable-azure-rbac`.

```
az aks update -g myResourceGroup -n myAKScluster --disable-azure-rbac
```

## Create role assignments for users to access cluster

AKS provides the following four built-in roles:

ROLE	DESCRIPTION
Azure Kubernetes Service RBAC Reader	Allows read-only access to see most objects in a namespace. It doesn't allow viewing roles or role bindings. This role doesn't allow viewing <code>Secrets</code> , since reading the contents of Secrets enables access to ServiceAccount credentials in the namespace, which would allow API access as any ServiceAccount in the namespace (a form of privilege escalation)
Azure Kubernetes Service RBAC Writer	Allows read/write access to most objects in a namespace. This role doesn't allow viewing or modifying roles or role bindings. However, this role allows accessing <code>Secrets</code> 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.

ROLE	DESCRIPTION
Azure Kubernetes Service RBAC Admin	Allows admin access, intended to be granted within a namespace. Allows read/write access to most resources in a namespace (or cluster scope), including the ability to create roles and role bindings within the namespace. This role doesn't allow write access to resource quota or to the namespace itself.
Azure Kubernetes Service RBAC Cluster Admin	Allows super-user access to perform any action on any resource. It gives full control over every resource in the cluster and in all namespaces.

Roles assignments scoped to the **entire AKS cluster** can be done either on the Access Control (IAM) blade of the cluster resource on Azure portal or by using Azure CLI commands as shown below:

```
Get your AKS Resource ID
AKS_ID=$(az aks show -g MyResourceGroup -n MyManagedCluster --query id -o tsv)
```

```
az role assignment create --role "Azure Kubernetes Service RBAC Admin" --assignee <AAD-ENTITY-ID> --scope $AKS_ID
```

where `<AAD-ENTITY-ID>` could be a username (for example, user@contoso.com) or even the ClientID of a service principal.

You can also create role assignments scoped to a specific **namespace** within the cluster:

```
az role assignment create --role "Azure Kubernetes Service RBAC Reader" --assignee <AAD-ENTITY-ID> --scope $AKS_ID/namespaces/<namespace-name>
```

Today, role assignments scoped to namespaces need to be configured via Azure CLI.

### Create custom roles definitions

Optionally you may choose to create your own role definition and then assign as above.

Below is an example of a role definition that allows a user to only read deployments and nothing else. You can check the full list of possible actions [here](#).

Copy the below json into a file called `deploy-view.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/<YOUR SUBSCRIPTION ID>"
]
}
```

Replace `<YOUR SUBSCRIPTION ID>` by the ID from your subscription, which you can get by running:

```
az account show --query id -o tsv
```

Now we can create the role definition by running the below command from the folder where you saved

`deploy-view.json`:

```
az role definition create --role-definition @deploy-view.json
```

Now that you have your role definition, you can assign it to a user or other identity by running:

```
az role assignment create --role "AKS Deployment Reader" --assignee <AAD-ENTITY-ID> --scope $AKS_ID
```

## Use Azure RBAC for Kubernetes Authorization with `kubectl`

### NOTE

Ensure you have the latest `kubectl` by running the below command:

```
az aks install-cli
```

You might need to run it with `sudo` privileges.

Now that you have assigned your desired role and permissions. You can start calling the Kubernetes API, for example, from `kubectl`.

For this purpose, let's first get the cluster's kubeconfig using the below command:

```
az aks get-credentials -g MyResourceGroup -n MyManagedCluster
```

### IMPORTANT

You'll need the [Azure Kubernetes Service Cluster User](#) built-in role to perform the step above.

Now, you can use `kubectl` to, for example, list the nodes in the cluster. The first time you run it you'll need to sign in, and subsequent commands will use the respective access token.

```
kubectl get nodes
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
AAAAAAA to authenticate.
```

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-93451573-vmss000000	Ready	agent	3h6m	v1.15.11
aks-nodepool1-93451573-vmss000001	Ready	agent	3h6m	v1.15.11
aks-nodepool1-93451573-vmss000002	Ready	agent	3h6m	v1.15.11

## Use Azure RBAC for Kubernetes Authorization with `kubelogin`

To unblock additional scenarios like non-interactive logins, older `kubectl` versions or leveraging SSO across multiple clusters without the need to sign in to new cluster, granted that your token is still valid, AKS created an exec plugin called `kubelogin`.

You can use it by running:

```
export KUBECONFIG=/path/to/kubeconfig
kubelogin convert-kubeconfig
```

The first time, you'll have to sign in interactively like with regular `kubectl`, but afterwards you'll no longer need to, even for new Azure AD clusters (as long as your token is still valid).

```
kubectl get nodes
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
AAAAAAA to authenticate.
```

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-93451573-vmss000000	Ready	agent	3h6m	v1.15.11
aks-nodepool1-93451573-vmss000001	Ready	agent	3h6m	v1.15.11
aks-nodepool1-93451573-vmss000002	Ready	agent	3h6m	v1.15.11

## Clean up

### Clean Role assignment

```
az role assignment list --scope $AKS_ID --query [].id -o tsv
```

Copy the ID or IDs from all the assignments you did and then.

```
az role assignment delete --ids <LIST OF ASSIGNMENT IDS>
```

### Clean up role definition

```
az role definition delete -n "AKS Deployment Reader"
```

### Delete cluster and resource group

```
az group delete -n MyResourceGroup
```

## Next steps

- Read more about AKS Authentication, Authorization, Kubernetes RBAC, and Azure RBAC [here](#).
- Read more about Azure RBAC [here](#).
- Read more about the all the actions you can use to granularly define custom Azure roles for Kubernetes authorization [here](#).

# Control access to cluster resources using Kubernetes role-based access control and Azure Active Directory identities in Azure Kubernetes Service

10/27/2022 • 11 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) can be configured to use Azure Active Directory (AD) for user authentication. In this configuration, you sign in to an AKS cluster using an Azure AD authentication token. Once authenticated, you can use the built-in Kubernetes role-based access control (Kubernetes RBAC) to manage access to namespaces and cluster resources based on a user's identity or group membership.

This article shows you how to control access using Kubernetes RBAC in an AKS cluster based on Azure AD group membership. Example groups and users are created in Azure AD, then Roles and RoleBindings are created in the AKS cluster to grant the appropriate permissions to create and view resources.

## Before you begin

This article assumes that you have an existing AKS cluster enabled with Azure AD integration. If you need an AKS cluster, see [Integrate Azure Active Directory with AKS](#).

You need the Azure CLI version 2.0.61 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Create demo groups in Azure AD

In this article, let's create two user roles that can be used to show how Kubernetes RBAC and Azure AD control access to cluster resources. The following two example roles are used:

- **Application developer**
  - A user named *aksdev* that is part of the *appdev* group.
- **Site reliability engineer**
  - A user named *akssre* that is part of the *opssre* group.

In production environments, you can use existing users and groups within an Azure AD tenant.

First, get the resource ID of your AKS cluster using the `az aks show` command. Assign the resource ID to a variable named *AKS\_ID* so that it can be referenced in additional commands.

```
AKS_ID=$(az aks show \
--resource-group myResourceGroup \
--name myAKScluster \
--query id -o tsv)
```

Create the first example group in Azure AD for the application developers using the `az ad group create` command. The following example creates a group named *appdev*.

```
APPDEV_ID=$(az ad group create --display-name appdev --mail-nickname appdev --query objectId -o tsv)
```

Now, create an Azure role assignment for the *appdev* group using the `az role assignment create` command. This assignment lets any member of the group use `kubectl` to interact with an AKS cluster by granting them the

## Azure Kubernetes Service Cluster User Role.

```
az role assignment create \
--assignee $APPDEV_ID \
--role "Azure Kubernetes Service Cluster User Role" \
--scope $AKS_ID
```

### TIP

If you receive an error such as

```
Principal 35bfec9328bd4d8d9b54dea6dac57b82 does not exist in the directory a5443dcd-cd0e-494d-a387-3039b419f0d5.
```

, wait a few seconds for the Azure AD group object ID to propagate through the directory then try the

```
az role assignment create
```

Create a second example group, this one for SREs named *opssre*.

```
OPSSRE_ID=$(az ad group create --display-name opssre --mail-nickname opssre --query objectId -o tsv)
```

Again, create an Azure role assignment to grant members of the group the *Azure Kubernetes Service Cluster User Role*.

```
az role assignment create \
--assignee $OPSSRE_ID \
--role "Azure Kubernetes Service Cluster User Role" \
--scope $AKS_ID
```

## Create demo users in Azure AD

With two example groups created in Azure AD for our application developers and SREs, now lets create two example users. To test the Kubernetes RBAC integration at the end of the article, you sign in to the AKS cluster with these accounts.

Set the user principal name (UPN) and password for the application developers. The following command prompts you for the UPN and sets it to *AAD\_DEV\_UPN* for use in a later command (remember that the commands in this article are entered into a BASH shell). The UPN must include the verified domain name of your tenant, for example `aksdev@contoso.com`.

```
echo "Please enter the UPN for application developers: " && read AAD_DEV_UPN
```

The following command prompts you for the password and sets it to *AAD\_DEV\_PW* for use in a later command.

```
echo "Please enter the secure password for application developers: " && read AAD_DEV_PW
```

Create the first user account in Azure AD using the [az ad user create](#) command.

The following example creates a user with the display name *AKS Dev* and the UPN and secure password using the values in *AAD\_DEV\_UPN* and *AAD\_DEV\_PW*.

```
AKSDEV_ID=$(az ad user create \
--display-name "AKS Dev" \
--user-principal-name $AAD_DEV_UPN \
--password $AAD_DEV_PW \
--query objectId -o tsv)
```

Now add the user to the *appdev* group created in the previous section using the [az ad group member add](#) command:

```
az ad group member add --group appdev --member-id $AKSDEV_ID
```

Set the UPN and password for SREs. The following command prompts you for the UPN and sets it to *AAD\_SRE\_UPN* for use in a later command (remember that the commands in this article are entered into a BASH shell). The UPN must include the verified domain name of your tenant, for example `akssre@contoso.com`.

```
echo "Please enter the UPN for SREs: " && read AAD_SRE_UPN
```

The following command prompts you for the password and sets it to *AAD\_SRE\_PW* for use in a later command.

```
echo "Please enter the secure password for SREs: " && read AAD_SRE_PW
```

Create a second user account. The following example creates a user with the display name *AKS SRE* and the UPN and secure password using the values in *AAD\_SRE\_UPN* and *AAD\_SRE\_PW*.

```
Create a user for the SRE role
AKSSRE_ID=$(az ad user create \
--display-name "AKS SRE" \
--user-principal-name $AAD_SRE_UPN \
--password $AAD_SRE_PW \
--query objectId -o tsv)

Add the user to the opssre Azure AD group
az ad group member add --group opssre --member-id $AKSSRE_ID
```

## Create the AKS cluster resources for app devs

The Azure AD groups and users are now created. Azure role assignments were created for the group members to connect to an AKS cluster as a regular user. Now, let's configure the AKS cluster to allow these different groups access to specific resources.

First, get the cluster admin credentials using the [az aks get-credentials](#) command. In one of the following sections, you get the regular *user* cluster credentials to see the Azure AD authentication flow in action.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster --admin
```

Create a namespace in the AKS cluster using the [kubectl create namespace](#) command. The following example creates a namespace name *dev*.

```
kubectl create namespace dev
```

In Kubernetes, *Roles* define the permissions to grant, and *RoleBindings* apply them to desired users or groups. These assignments can be applied to a given namespace, or across the entire cluster. For more information, see

## Using Kubernetes RBAC authorization.

First, create a Role for the *dev* namespace. This role grants full permissions to the namespace. In production environments, you can specify more granular permissions for different users or groups.

Create a file named `role-dev-namespace.yaml` and paste the following YAML manifest:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
 name: dev-user-full-access
 namespace: dev
rules:
- apiGroups: ["", "extensions", "apps"]
 resources: ["*"]
 verbs: ["*"]
- apiGroups: ["batch"]
 resources:
 - jobs
 - cronjobs
 verbs: ["*"]
```

Create the Role using the [kubectl apply](#) command and specify the filename of your YAML manifest:

```
kubectl apply -f role-dev-namespace.yaml
```

Next, get the resource ID for the *appdev* group using the [az ad group show](#) command. This group is set as the subject of a RoleBinding in the next step.

```
az ad group show --group appdev --query id -o tsv
```

Now, create a RoleBinding for the *appdev* group to use the previously created Role for namespace access. Create a file named `rolebinding-dev-namespace.yaml` and paste the following YAML manifest. On the last line, replace `groupId` with the group object ID output from the previous command:

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
 name: dev-user-access
 namespace: dev
roleRef:
 apiGroup: rbac.authorization.k8s.io
 kind: Role
 name: dev-user-full-access
subjects:
- kind: Group
 namespace: dev
 name: groupId
```

### TIP

If you want to create the RoleBinding for a single user, specify `kind: User` and replace `groupId` with the user principal name (UPN) in the above sample.

Create the RoleBinding using the [kubectl apply](#) command and specify the filename of your YAML manifest:

```
kubectl apply -f rolebinding-dev-namespace.yaml
```

## Create the AKS cluster resources for SREs

Now, repeat the previous steps to create a namespace, Role, and RoleBinding for the SREs.

First, create a namespace for *sre* using the [kubectl create namespace](#) command:

```
kubectl create namespace sre
```

Create a file named [role-sre-namespace.yaml](#) and paste the following YAML manifest:

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
 name: sre-user-full-access
 namespace: sre
rules:
- apiGroups: ["", "extensions", "apps"]
 resources: ["*"]
 verbs: ["*"]
- apiGroups: ["batch"]
 resources:
 - jobs
 - cronjobs
 verbs: ["*"]
```

Create the Role using the [kubectl apply](#) command and specify the filename of your YAML manifest:

```
kubectl apply -f role-sre-namespace.yaml
```

Get the resource ID for the *opssre* group using the [az ad group show](#) command:

```
az ad group show --group opssre --query id -o tsv
```

Create a RoleBinding for the *opssre* group to use the previously created Role for namespace access. Create a file named [rolebinding-sre-namespace.yaml](#) and paste the following YAML manifest. On the last line, replace *groupObjectId* with the group object ID output from the previous command:

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
 name: sre-user-access
 namespace: sre
roleRef:
 apiGroup: rbac.authorization.k8s.io
 kind: Role
 name: sre-user-full-access
subjects:
- kind: Group
 namespace: sre
 name: groupObjectId
```

Create the RoleBinding using the [kubectl apply](#) command and specify the filename of your YAML manifest:

```
kubectl apply -f rolebinding-sre-namespace.yaml
```

## Interact with cluster resources using Azure AD identities

Now, let's test the expected permissions work when you create and manage resources in an AKS cluster. In these examples, you schedule and view pods in the user's assigned namespace. Then, you try to schedule and view pods outside of the assigned namespace.

First, reset the *kubeconfig* context using the `az aks get-credentials` command. In a previous section, you set the context using the cluster admin credentials. The admin user bypasses Azure AD sign in prompts. Without the `--admin` parameter, the user context is applied that requires all requests to be authenticated using Azure AD.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster --overwrite-existing
```

Schedule a basic NGINX pod using the `kubectl run` command in the *dev* namespace:

```
kubectl run nginx-dev --image=mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine --namespace dev
```

As the sign in prompt, enter the credentials for your own `appdev@contoso.com` account created at the start of the article. Once you are successfully signed in, the account token is cached for future `kubectl` commands. The NGINX is successfully scheduled, as shown in the following example output:

```
$ kubectl run nginx-dev --image=mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine --namespace dev
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
B24ZD6FP8 to authenticate.
pod/nginx-dev created
```

Now use the `kubectl get pods` command to view pods in the *dev* namespace.

```
kubectl get pods --namespace dev
```

As shown in the following example output, the NGINX pod is successfully *Running*.

```
$ kubectl get pods --namespace dev
NAME READY STATUS RESTARTS AGE
nginx-dev 1/1 Running 0 4m
```

### Create and view cluster resources outside of the assigned namespace

Now try to view pods outside of the *dev* namespace. Use the `kubectl get pods` command again, this time to see `--all-namespaces` as follows:

```
kubectl get pods --all-namespaces
```

The user's group membership does not have a Kubernetes Role that allows this action, as shown in the following example output:

```
$ kubectl get pods --all-namespaces

Error from server (Forbidden): pods is forbidden: User "aksdev@contoso.com" cannot list resource "pods" in
API group "" at the cluster scope
```

In the same way, try to schedule a pod in different namespace, such as the *sre* namespace. The user's group membership does not align with a Kubernetes Role and RoleBinding to grant these permissions, as shown in the following example output:

```
$ kubectl run nginx-dev --image=mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine --namespace sre

Error from server (Forbidden): pods is forbidden: User "aksdev@contoso.com" cannot create resource "pods" in
API group "" in the namespace "sre"
```

### Test the SRE access to the AKS cluster resources

To confirm that our Azure AD group membership and Kubernetes RBAC work correctly between different users and groups, try the previous commands when signed in as the *opssre* user.

Reset the *kubeconfig* context using the [az aks get-credentials](#) command that clears the previously cached authentication token for the *aksdev* user:

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster --overwrite-existing
```

Try to schedule and view pods in the assigned *sre* namespace. When prompted, sign in with your own [opssre@contoso.com](#) credentials created at the start of the article:

```
kubectl run nginx-sre --image=mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine --namespace sre
kubectl get pods --namespace sre
```

As shown in the following example output, you can successfully create and view the pods:

```
$ kubectl run nginx-sre --image=mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine --namespace sre

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
BM4RHP3FD to authenticate.

pod/nginx-sre created

$ kubectl get pods --namespace sre

NAME READY STATUS RESTARTS AGE
nginx-sre 1/1 Running 0 1m
```

Now, try to view or schedule pods outside of assigned SRE namespace:

```
kubectl get pods --all-namespaces
kubectl run nginx-sre --image=mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine --namespace dev
```

These `kubectl` commands fail, as shown in the following example output. The user's group membership and Kubernetes Role and RoleBindings don't grant permissions to create or manager resources in other namespaces:

```
$ kubectl get pods --all-namespaces
Error from server (Forbidden): pods is forbidden: User "akssre@contoso.com" cannot list pods at the cluster
scope

$ kubectl run nginx-sre --image=mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine --namespace dev
Error from server (Forbidden): pods is forbidden: User "akssre@contoso.com" cannot create pods in the
namespace "dev"
```

## Clean up resources

In this article, you created resources in the AKS cluster and users and groups in Azure AD. To clean up all these resources, run the following commands:

```
Get the admin kubeconfig context to delete the necessary cluster resources
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster --admin

Delete the dev and sre namespaces. This also deletes the pods, Roles, and RoleBindings
kubectl delete namespace dev
kubectl delete namespace sre

Delete the Azure AD user accounts for aksdev and akssre
az ad user delete --upn-or-object-id $AKSDEV_ID
az ad user delete --upn-or-object-id $AKSSRE_ID

Delete the Azure AD groups for appdev and opssre. This also deletes the Azure role assignments.
az ad group delete --group appdev
az ad group delete --group opssre
```

## Next steps

For more information about how to secure Kubernetes clusters, see [Access and identity options for AKS](#).

For best practices on identity and resource control, see [Best practices for authentication and authorization in AKS](#).

# Custom certificate authority (CA) in Azure Kubernetes Service (AKS) (preview)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Custom certificate authorities (CAs) allow you to establish trust between your Azure Kubernetes Service (AKS) cluster and your workloads, such as private registries, proxies, and firewalls. A Kubernetes secret is used to store the certificate authority's information, then it's passed to all nodes in the cluster.

This feature is applied per nodepool, so new and existing nodepools must be configured to enable this feature.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI installed](#).
- A base64 encoded certificate string.

## Limitations

This feature isn't currently supported for Windows nodepools.

### Install the `aks-preview` extension

You also need the `aks-preview` Azure CLI extensions version 0.5.72 or later. Install the `aks-preview` extension by using the [az extension add](#) command, or install any available updates by using the [az extension update](#) command.

```
Install the aks-preview extension
az extension add --name aks-preview

Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

### Register the `CustomCATrustPreview` preview feature

Register the `CustomCATrustPreview` feature flag by using the [az feature register](#) command:

```
az feature register --namespace "Microsoft.ContainerService" --name "CustomCATrustPreview"
```

It takes a few minutes for the status to show *Registered*. Verify the registration status by using the [az feature list](#) command:

```
az feature list --query "[?contains(name, 'Microsoft.ContainerService/CustomCATrustPreview')].{Name:name,State:properties.state}" -o table
```

Refresh the registration of the *Microsoft.ContainerService* resource provider by using the [az provider register](#) command:

```
az provider register --namespace Microsoft.ContainerService
```

## Configure a new AKS cluster to use a custom CA

To configure a new AKS cluster to use a custom CA, run the [az aks create](#) command with the `--enable-custom-ca-trust` parameter.

```
az aks create \
--resource-group myResourceGroup \
--name myAKScluster \
--node-count 2 \
--enable-custom-ca-trust
```

## Configure a new nodepool to use a custom CA

To configure a new nodepool to use a custom CA, run the [az aks nodepool add](#) command with the `--enable-custom-ca-trust` parameter.

```
az aks nodepool add \
--cluster-name myAKScluster \
--resource-group myResourceGroup \
--name myNodepool \
--enable-custom-ca-trust \
--os-type Linux
```

## Configure an existing nodepool to use a custom CA

To configure an existing nodepool to use a custom CA, run the [az aks nodepool update](#) command with the `--enable-custom-trust-ca` parameter.

```
az aks nodepool update \
--resource-group myResourceGroup \
--cluster-name myAKScluster \
--name myNodepool \
--enable-custom-ca-trust
```

## Create a Kubernetes secret with your CA information

Create a [Kubernetes secret](#) YAML manifest with your base64 encoded certificate string in the `data` field. Data from this secret is used to update CAs on all nodes.

You must ensure that:

- The secret is named `custom-ca-trust-secret`.
- The secret is created in the `kube-system` namespace.

```
apiVersion: v1
kind: Secret
metadata:
 name: custom-ca-trust-secret
 namespace: kube-system
type: Opaque
data:
 ca1.crt: |
 {base64EncodedCertStringHere}
 ca2.crt: |
 {anotherBase64EncodedCertStringHere}
```

To update or remove a CA, edit and apply the YAML manifest. The cluster will poll for changes and update the nodes accordingly. This process may take a couple of minutes before changes are applied.

## Next steps

For more information on AKS security best practices, see [Best practices for cluster security and upgrades in Azure Kubernetes Service \(AKS\)](#).

# Certificate rotation in Azure Kubernetes Service (AKS)

10/27/2022 • 5 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) uses certificates for authentication with many of its components. If you have a RBAC-enabled cluster built after March 2022, it's enabled with certificate auto-rotation. Periodically, you may need to rotate those certificates for security or policy reasons. For example, you may have a policy to rotate all your certificates every 90 days.

## NOTE

Certificate auto-rotation will *only* be enabled by default for RBAC enabled AKS clusters.

This article shows you how certificate rotation works in your AKS cluster.

## Before you begin

This article requires that you are running the Azure CLI version 2.0.77 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## AKS certificates, Certificate Authorities, and Service Accounts

AKS generates and uses the following certificates, Certificate Authorities, and Service Accounts:

- The AKS API server creates a Certificate Authority (CA) called the Cluster CA.
- The API server has a Cluster CA, which signs certificates for one-way communication from the API server to kubelets.
- Each kubelet also creates a Certificate Signing Request (CSR), which is signed by the Cluster CA, for communication from the kubelet to the API server.
- The API aggregator uses the Cluster CA to issue certificates for communication with other APIs. The API aggregator can also have its own CA for issuing those certificates, but it currently uses the Cluster CA.
- Each node uses a Service Account (SA) token, which is signed by the Cluster CA.
- The `kubectl` client has a certificate for communicating with the AKS cluster.

Certificates mentioned above are maintained by Microsoft, except the cluster certificate, which you have to maintain.

#### NOTE

AKS clusters created prior to May 2019 have certificates that expire after two years. Any cluster created after May 2019 or any cluster that has its certificates rotated have Cluster CA certificates that expire after 30 years. All other AKS certificates, which use the Cluster CA for signing, will expire after two years and are automatically rotated during an AKS version upgrade which happened after 8/1/2021. To verify when your cluster was created, use `kubectl get nodes` to see the *Age* of your node pools.

Additionally, you can check the expiration date of your cluster's certificate. For example, the following bash command displays the client certificate details for the *myAKSCluster* cluster in resource group *rg*.

```
kubectl config view --raw -o jsonpath=".users[?(.name == 'clusterUser_rg_myAKSCluster')].user.client-certificate-data" | base64 -d | openssl x509 -text | grep -A2 Validity
```

To check expiration date of apiserver certificate, run the following command:

```
curl https://{{apiserver-fqdn}} -k -v 2>&1 |grep expire
```

To check the expiration date of certificate on VMAS agent node, run the following command:

```
az vm run-command invoke -g MC_rg_myAKSCluster_region -n vm-name --command-id RunShellScript --query 'value[0].message' -otsv --scripts "openssl x509 -in /etc/kubernetes/certs/apiserver.crt -noout -enddate"
```

To check expiration date of certificate on one virtual machine scale set agent node, run the following command:

```
az vmss run-command invoke -g MC_rg_myAKSCluster_region -n vmss-name --instance-id 0 --command-id RunShellScript --query 'value[0].message' -otsv --scripts "openssl x509 -in /etc/kubernetes/certs/apiserver.crt -noout -enddate"
```

## Certificate Auto Rotation

For AKS to automatically rotate non-CA certificates, the cluster must have [TLS Bootstrapping](#) which has been enabled by default in all Azure regions.

#### NOTE

If you have an existing cluster you have to upgrade that cluster to enable Certificate Auto-Rotation. Do not disable bootstrap to keep your auto-rotation enabled.

#### NOTE

If the cluster is in a stopped state during the auto certificate rotation only the control plane certificates are rotated. In this case the nodepool should be recreated, after certificate rotation, in order to initiate the nodepool certificate rotation.

For any AKS clusters created or upgraded after March 2022 Azure Kubernetes Service will automatically rotate non-CA certificates on both the control plane and agent nodes within 80% of the client certificate valid time, before they expire with no downtime for the cluster.

### How to check whether current agent node pool is TLS Bootstrapping enabled?

To verify if TLS Bootstrapping is enabled on your cluster browse to the following paths:

- On a Linux node: `/var/lib/kubelet/bootstrap-kubeconfig`
- On a Windows node: `C:\k\bootstrap-config`

To access agent nodes, see [Connect to Azure Kubernetes Service cluster nodes for maintenance or troubleshooting](#) for more information.

#### NOTE

The file path may change as Kubernetes version evolves in the future.

Once a region is configured, create a new cluster or upgrade an existing cluster with `az aks upgrade` to set that cluster for auto-certificate rotation. A control plane and node pool upgrade is needed to enable this feature.

```
az aks upgrade -g $RESOURCE_GROUP_NAME -n $CLUSTER_NAME
```

#### Limitation

Certificate auto-rotation will only be enabled by default for RBAC enabled AKS clusters.

## Manually rotate your cluster certificates

#### WARNING

Rotating your certificates using `az aks rotate-certs` will recreate all of your nodes, VM scale set and their Disks and can cause up to 30 minutes of downtime for your AKS cluster.

Use `az aks get-credentials` to sign in to your AKS cluster. This command also downloads and configures the `kubectl` client certificate on your local machine.

```
az aks get-credentials -g $RESOURCE_GROUP_NAME -n $CLUSTER_NAME
```

Use `az aks rotate-certs` to rotate all certificates, CAs, and SAs on your cluster.

```
az aks rotate-certs -g $RESOURCE_GROUP_NAME -n $CLUSTER_NAME
```

#### IMPORTANT

It may take up to 30 minutes for `az aks rotate-certs` to complete. If the command fails before completing, use `az aks show` to verify the status of the cluster is *Certificate Rotating*. If the cluster is in a failed state, rerun `az aks rotate-certs` to rotate your certificates again.

Verify that the old certificates aren't valid by running any `kubectl` command. If you haven't updated the certificates used by `kubectl`, you'll see an error similar to the following example:

```
kubectl get nodes
Unable to connect to the server: x509: certificate signed by unknown authority (possibly because of
"crypto/rsa: verification error" while trying to verify candidate authority certificate "ca")
```

To update the certificate used by `kubectl`, run the `az aks get-credentials` command:

```
az aks get-credentials -g $RESOURCE_GROUP_NAME -n $CLUSTER_NAME --overwrite-existing
```

To verify the certificates have been updated, run the following [kubectl get][kubectl-get] command:

```
kubectl get nodes
```

**NOTE**

If you have any services that run on top of AKS, you might need to update their certificates.

## Next steps

This article showed you how to automatically rotate your cluster's certificates, CAs, and SAs. You can see [Best practices for cluster security and upgrades in Azure Kubernetes Service \(AKS\)](#) for more information on AKS security best practices.

# Secure your cluster with Azure Policy

10/27/2022 • 4 minutes to read • [Edit Online](#)

To improve the security of your Azure Kubernetes Service (AKS) cluster, you can apply and enforce built-in security policies on your cluster using Azure Policy. [Azure Policy](#) helps to enforce organizational standards and to assess compliance at-scale. After installing the [Azure Policy Add-on for AKS](#), you can apply individual policy definitions or groups of policy definitions called initiatives (sometimes called policysets) to your cluster. See [Azure Policy built-in definitions for AKS](#) for a complete list of AKS policy and initiative definitions.

This article shows you how to apply policy definitions to your cluster and verify those assignments are being enforced.

## Prerequisites

- This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).
- The Azure Policy Add-on for AKS installed on an AKS cluster. Follow these [steps to install the Azure Policy Add-on](#).

## Assign a built-in policy definition or initiative

To apply a policy definition or initiative, use the Azure portal.

1. Navigate to the Azure Policy service in Azure portal.
2. In the left pane of the Azure Policy page, select **Definitions**.
3. Under **Categories** select `Kubernetes`.
4. Choose the policy definition or initiative you want to apply. For this example, select the `Kubernetes cluster pod security baseline standards for Linux-based workloads` initiative.
5. Select **Assign**.
6. Set the **Scope** to the resource group of the AKS cluster with the Azure Policy Add-on enabled.
7. Select the **Parameters** page and update the **Effect** from `audit` to `deny` to block new deployments violating the baseline initiative. You can also add additional namespaces to exclude from evaluation. For this example, keep the default values.
8. Select **Review + create** then **Create** to submit the policy assignment.

## Create and assign a custom policy definition

Custom policies allow you to define rules for using Azure. For example, you can enforce:

- Security practices
- Cost management
- Organization-specific rules (like naming or locations)

Before creating a custom policy, check the [list of common patterns and samples](#) to see if your case is already covered.

Custom policy definitions are written in JSON. To learn more about creating a custom policy, see [Azure Policy definition structure](#) and [Create a custom policy definition](#).

#### NOTE

Azure Policy now utilizes a new property known as `templateInfo` that allows users to define the source type for the constraint template. By defining `templateInfo` in policy definitions, users don't have to define `constraintTemplate` or `constraint` properties. Users still need to define `apiGroups` and `kinds`. For more information on this, see [Understanding Azure Policy effects](#).

Once your custom policy definition has been created, see [Assign a policy definition](#) for a step-by-step walkthrough of assigning the policy to your Kubernetes cluster.

## Validate a Azure Policy is running

Confirm the policy assignments are applied to your cluster by running the following:

```
kubectl get constrainttemplates
```

#### NOTE

Policy assignments can take up to 20 minutes to sync into each cluster.

The output should be similar to:

```
$ kubectl get constrainttemplate
NAME AGE
k8sazureallowedcapabilities 23m
k8sazureallowedusersgroups 23m
k8sazureblockhostnamespace 23m
k8sazurecontainerallowedimages 23m
k8sazurecontainerallowedports 23m
k8sazurecontainerlimits 23m
k8sazurecontainernoprivilege 23m
k8sazurecontainernoprivilegeescalation 23m
k8sazureenforceapparmor 23m
k8sazurehostfilesystem 23m
k8sazurehostnetworkingports 23m
k8sazurereadonlyrootfilesystem 23m
k8sazureserviceallowedports 23m
```

## Validate rejection of a privileged pod

Let's first test what happens when you schedule a pod with the security context of `privileged: true`. This security context escalates the pod's privileges. The initiative disallows privileged pods, so the request will be denied resulting in the deployment being rejected.

Create a file named `nginx-privileged.yaml` and paste the following YAML manifest:

```
apiVersion: v1
kind: Pod
metadata:
 name: nginx-privileged
spec:
 containers:
 - name: nginx-privileged
 image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 securityContext:
 privileged: true
```

Create the pod with [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f nginx-privileged.yaml
```

As expected the pod fails to be scheduled, as shown in the following example output:

```
$ kubectl apply -f nginx-privileged.yaml

Error from server ([denied by azurepolicy-container-no-privilege-00edd87bf80f443fa51d10910255adbc4013d590bec3d290b4f48725d4dfbdf9] Privileged container is not allowed: nginx-privileged, securityContext: {"privileged": true}): error when creating "privileged.yaml": admission webhook "validation.gatekeeper.sh" denied the request: [denied by azurepolicy-container-no-privilege-00edd87bf80f443fa51d10910255adbc4013d590bec3d290b4f48725d4dfbdf9] Privileged container is not allowed: nginx-privileged, securityContext: {"privileged": true}
```

The pod doesn't reach the scheduling stage, so there are no resources to delete before you move on.

### Test creation of an unprivileged pod

In the previous example, the container image automatically tried to use root to bind NGINX to port 80. This request was denied by the policy initiative, so the pod fails to start. Let's try now running that same NGINX pod without privileged access.

Create a file named `nginx-unprivileged.yaml` and paste the following YAML manifest:

```
apiVersion: v1
kind: Pod
metadata:
 name: nginx-unprivileged
spec:
 containers:
 - name: nginx-unprivileged
 image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
```

Create the pod using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f nginx-unprivileged.yaml
```

The pod is successfully scheduled. When you check the status of the pod using the [kubectl get pods](#) command, the pod is *Running*.

```
$ kubectl get pods

NAME READY STATUS RESTARTS AGE
nginx-unprivileged 1/1 Running 0 18s
```

This example shows the baseline initiative affecting only deployments which violate policies in the collection. Allowed deployments continue to function.

Delete the NGINX unprivileged pod using the [kubectl delete](#) command and specify the name of your YAML manifest:

```
kubectl delete -f nginx-unprivileged.yaml
```

## Disable a policy or initiative

To remove the baseline initiative:

1. Navigate to the Policy pane on the Azure portal.
2. Select **Assignments** from the left pane.
3. Click the ... button next to the `Kubernetes cluster pod security baseline standards for Linux-based workloads` initiative.
4. Select **Delete assignment**.

## Next steps

For more information about how Azure Policy works:

- [Azure Policy Overview](#)
- [Azure Policy initiatives and polices for AKS](#)
- Remove the [Azure Policy Add-on](#).

# Understand Azure Policy for Kubernetes clusters

10/27/2022 • 18 minutes to read • [Edit Online](#)

Azure Policy extends [Gatekeeper](#) v3, an *admission controller webhook* for [Open Policy Agent](#) (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner. Azure Policy makes it possible to manage and report on the compliance state of your Kubernetes clusters from one place. The add-on enacts the following functions:

- Checks with Azure Policy service for policy assignments to the cluster.
- Deploys policy definitions into the cluster as [constraint template](#) and [constraint](#) custom resources.
- Reports auditing and compliance details back to Azure Policy service.

Azure Policy for Kubernetes supports the following cluster environments:

- [Azure Kubernetes Service \(AKS\)](#)
- [Azure Arc enabled Kubernetes](#)

## IMPORTANT

The Azure Policy Add-on Helm model and the add-on for AKS Engine have been *deprecated*. Instructions can be found below for [removal of those add-ons](#).

## Overview

To enable and use Azure Policy with your Kubernetes cluster, take the following actions:

1. Configure your Kubernetes cluster and install the [Azure Kubernetes Service \(AKS\)](#) add-on

### NOTE

For common issues with installation, see [Troubleshoot - Azure Policy Add-on](#).

2. [Understand the Azure Policy language for Kubernetes](#)
3. [Assign a definition to your Kubernetes cluster](#)
4. [Wait for validation](#)

## Limitations

The following general limitations apply to the Azure Policy Add-on for Kubernetes clusters:

- Azure Policy Add-on for Kubernetes is supported on Kubernetes version 1.14 or higher.
- Azure Policy Add-on for Kubernetes can only be deployed to Linux node pools.
- Only built-in policy definitions are supported. Custom policy definitions are a *public preview* feature.
- Maximum number of pods supported by the Azure Policy Add-on: **10,000**
- Maximum number of Non-compliant records per policy per cluster: **500**
- Maximum number of Non-compliant records per subscription: **1 million**
- Installations of Gatekeeper outside of the Azure Policy Add-on aren't supported. Uninstall any components installed by a previous Gatekeeper installation before enabling the Azure Policy Add-on.

- Reasons for non-compliance aren't available for the `Microsoft.Kubernetes.Data` Resource Provider mode. Use Component details.
- Component-level exemptions aren't supported for Resource Provider modes.

The following limitations apply only to the Azure Policy Add-on for AKS:

- AKS Pod security policy and the Azure Policy Add-on for AKS can't both be enabled. For more information, see [AKS pod security limitation](#).
- Namespaces automatically excluded by Azure Policy Add-on for evaluation: *kube-system*, *gatekeeper-system*, and *aks-periscope*.

## Recommendations

The following are general recommendations for using the Azure Policy Add-on:

- The Azure Policy Add-on requires three Gatekeeper components to run: One audit pod and two webhook pod replicas. These components consume more resources as the count of Kubernetes resources and policy assignments increases in the cluster, which requires audit and enforcement operations.
  - For fewer than 500 pods in a single cluster with a max of 20 constraints: two vCPUs and 350 MB memory per component.
  - For more than 500 pods in a single cluster with a max of 40 constraints: three vCPUs and 600 MB memory per component.
- Windows pods [don't support security contexts](#). Thus, some of the Azure Policy definitions, such as disallowing root privileges, can't be escalated in Windows pods and only apply to Linux pods.

The following recommendation applies only to AKS and the Azure Policy Add-on:

- Use system node pool with `CriticalAddonsOnly` taint to schedule Gatekeeper pods. For more information, see [Using system node pools](#).
- Secure outbound traffic from your AKS clusters. For more information, see [Control egress traffic for cluster nodes](#).
- If the cluster has `aad-pod-identity` enabled, Node Managed Identity (NMI) pods modify the nodes' iptables to intercept calls to the Azure Instance Metadata endpoint. This configuration means any request made to the Metadata endpoint is intercepted by NMI even if the pod doesn't use `aad-pod-identity`.

AzurePodIdentityException CRD can be configured to inform `aad-pod-identity` that any requests to the Metadata endpoint originating from a pod that matches labels defined in CRD should be proxied without any processing in NMI. The system pods with `kubernetes.azure.com/managedby: aks` label in *kube-system* namespace should be excluded in `aad-pod-identity` by configuring the AzurePodIdentityException CRD. For more information, see [Disable aad-pod-identity for a specific pod or application](#). To configure an exception, install the [mic-exception YAML](#).

## Install Azure Policy Add-on for AKS

Before installing the Azure Policy Add-on or enabling any of the service features, your subscription must enable the **Microsoft.PolicyInsights** resource providers.

1. You need the Azure CLI version 2.12.0 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install the Azure CLI](#).
2. Register the resource providers and preview features.
  - Azure portal:  
Register the **Microsoft.PolicyInsights** resource providers. For steps, see [Resource providers and](#)

types.

- Azure CLI:

```
Log in first with az login if you're not using Cloud Shell

Provider register: Register the Azure Policy provider
az provider register --namespace Microsoft.PolicyInsights
```

3. If limited preview policy definitions were installed, remove the add-on with the **Disable** button on your AKS cluster under the **Policies** page.

4. The AKS cluster must be version **1.14** or higher. Use the following script to validate your AKS cluster version:

```
Log in first with az login if you're not using Cloud Shell

Look for the value in kubernetesVersion
az aks list
```

5. Install version **2.12.0** or higher of the Azure CLI. For more information, see [Install the Azure CLI](#).

Once the above prerequisite steps are completed, install the Azure Policy Add-on in the AKS cluster you want to manage.

- Azure portal

1. Launch the AKS service in the Azure portal by selecting **All services**, then searching for and selecting **Kubernetes services**.
2. Select one of your AKS clusters.
3. Select **Policies** on the left side of the Kubernetes service page.
4. In the main page, select the **Enable add-on** button.

- Azure CLI

```
Log in first with az login if you're not using Cloud Shell

az aks enable-addons --addons azure-policy --name MyAKSCluster --resource-group MyResourceGroup
```

To validate that the add-on installation was successful and that the *azure-policy* and *gatekeeper* pods are running, run the following command:

```
azure-policy pod is installed in kube-system namespace
kubectl get pods -n kube-system

gatekeeper pod is installed in gatekeeper-system namespace
kubectl get pods -n gatekeeper-system
```

Lastly, verify that the latest add-on is installed by running this Azure CLI command, replacing `<rg>` with your resource group name and `<cluster-name>` with the name of your AKS cluster:

`az aks show --query addonProfiles.azurepolicy -g <rg> -n <cluster-name>`. The result should look similar to the following output:

```
{
 "config": null,
 "enabled": true,
 "identity": null
}
```

## Install Azure Policy Extension for Azure Arc enabled Kubernetes

Azure Policy for Kubernetes makes it possible to manage and report on the compliance state of your Kubernetes clusters from one place.

This article describes how to [create](#), [show extension status](#), and [delete](#) the Azure Policy for Kubernetes extension.

For an overview of the extensions platform, see [Azure Arc cluster extensions](#).

### Prerequisites

Note: If you have already deployed Azure Policy for Kubernetes on an Azure Arc cluster using Helm directly without extensions, follow the instructions listed to [delete the Helm chart](#). Once the deletion is done, you can then proceed.

1. Ensure your Kubernetes cluster is a supported distribution.

Note: Azure Policy for Arc extension is supported on [the following Kubernetes distributions](#).

2. Ensure you have met all the common prerequisites for Kubernetes extensions listed [here](#) including [connecting your cluster to Azure Arc](#).

Note: Azure Policy extension is supported for Arc enabled Kubernetes clusters [in these regions](#).

3. Open ports for the Azure Policy extension. The Azure Policy extension uses these domains and ports to fetch policy definitions and assignments and report compliance of the cluster back to Azure Policy.

DOMAIN	PORT
data.policy.core.windows.net	443
store.policy.core.windows.net	443
login.windows.net	443
dc.services.visualstudio.com	443

4. Before installing the Azure Policy extension or enabling any of the service features, your subscription must enable the **Microsoft.PolicyInsights** resource providers.

Note: To enable the resource provider, follow the steps in [Resource providers and types](#) or run either the Azure CLI or Azure PowerShell command:

- Azure CLI

```
Log in first with az login if you're not using Cloud Shell
Provider register: Register the Azure Policy provider
az provider register --namespace 'Microsoft.PolicyInsights'
```

- Azure PowerShell

```
Log in first with Connect-AzAccount if you're not using Cloud Shell

Provider register: Register the Azure Policy provider
Register-AzResourceProvider -ProviderNamespace 'Microsoft.PolicyInsights'
```

## Create Azure Policy extension

Note the following for Azure Policy extension creation:

- Auto-upgrade is enabled by default which will update Azure Policy extension minor version if any new changes are deployed.
- Any proxy variables passed as parameters to `connectedk8s` will be propagated to the Azure Policy extension to support outbound proxy.

To create an extension instance, for your Arc enabled cluster, run the following command substituting `<>` with your values:

```
az k8s-extension create --cluster-type connectedClusters --cluster-name <CLUSTER_NAME> --resource-group
<RESOURCE_GROUP> --extension-type Microsoft.PolicyInsights --name <EXTENSION_INSTANCE_NAME>
```

**Example:**

```
az k8s-extension create --cluster-type connectedClusters --cluster-name my-test-cluster --resource-group my-
test-rg --extension-type Microsoft.PolicyInsights --name azurepolicy
```

**Example Output:**

```
{
 "aksAssignedIdentity": null,
 "autoUpgradeMinorVersion": true,
 "configurationProtectedSettings": {},
 "configurationSettings": {},
 "customLocationSettings": null,
 "errorInfo": null,
 "extensionType": "microsoft.policyinsights",
 "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/my-test-rg/providers/Microsoft.Kubernetes/connectedClusters/my-test-cluster/providers/Microsoft.KubernetesConfiguration/extensions/azurepolicy",
 "identity": {
 "principalId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
 "tenantId": null,
 "type": "SystemAssigned"
 },
 "location": null,
 "name": "azurepolicy",
 "packageUri": null,
 "provisioningState": "Succeeded",
 "releaseTrain": "Stable",
 "resourceGroup": "my-test-rg",
 "scope": {
 "cluster": {
 "releaseNamespace": "kube-system"
 },
 "namespace": null
 },
 "statuses": [],
 "systemData": {
 "createdAt": "2021-10-27T01:20:06.834236+00:00",
 "createdBy": null,
 "createdByType": null,
 "lastModifiedAt": "2021-10-27T01:20:06.834236+00:00",
 "lastModifiedBy": null,
 "lastModifiedByType": null
 },
 "type": "Microsoft.KubernetesConfiguration/extensions",
 "version": "1.1.0"
}
```

## Show Azure Policy extension

To check the extension instance creation was successful, and inspect extension metadata, run the following command substituting `<>` with your values:

```
az k8s-extension show --cluster-type connectedClusters --cluster-name <CLUSTER_NAME> --resource-group <RESOURCE_GROUP> --name <EXTENSION_INSTANCE_NAME>
```

### Example:

```
az k8s-extension show --cluster-type connectedClusters --cluster-name my-test-cluster --resource-group my-test-rg --name azurepolicy
```

To validate that the extension installation was successful and that the azure-policy and gatekeeper pods are running, run the following command:

```
azure-policy pod is installed in kube-system namespace
kubectl get pods -n kube-system

gatekeeper pod is installed in gatekeeper-system namespace
kubectl get pods -n gatekeeper-system
```

## Delete Azure Policy extension

To delete the extension instance, run the following command substituting <> with your values:

```
az k8s-extension delete --cluster-type connectedClusters --cluster-name <CLUSTER_NAME> --resource-group
<RESOURCE_GROUP> --name <EXTENSION_INSTANCE_NAME>
```

## Policy language

The Azure Policy language structure for managing Kubernetes follows that of existing policy definitions. With a [Resource Provider mode](#) of `Microsoft.Kubernetes.Data`, the effects `audit` and `deny` are used to manage your Kubernetes clusters. `Audit` and `deny` must provide `details` properties specific to working with [OPA Constraint Framework](#) and Gatekeeper v3.

As part of the `details.templateInfo`, `details.constraint`, or `details.constraintTemplate` properties in the policy definition, Azure Policy passes the URI or Base64Encoded value of these [CustomResourceDefinitions](#) (CRD) to the add-on. Rego is the language that OPA and Gatekeeper support to validate a request to the Kubernetes cluster. By supporting an existing standard for Kubernetes management, Azure Policy makes it possible to reuse existing rules and pair them with Azure Policy for a unified cloud compliance reporting experience. For more information, see [What is Rego?](#).

## Assign a policy definition

To assign a policy definition to your Kubernetes cluster, you must be assigned the appropriate Azure role-based access control (Azure RBAC) policy assignment operations. The Azure built-in roles [Resource Policy Contributor](#) and [Owner](#) have these operations. To learn more, see [Azure RBAC permissions in Azure Policy](#).

Find the built-in policy definitions for managing your cluster using the Azure portal with the following steps. If using a custom policy definition, search for it by name or the category that you created it with.

1. Start the Azure Policy service in the Azure portal. Select **All services** in the left pane and then search for and select **Policy**.
2. In the left pane of the Azure Policy page, select **Definitions**.
3. From the Category dropdown list box, use **Select all** to clear the filter and then select **Kubernetes**.
4. Select the policy definition, then select the **Assign** button.
5. Set the **Scope** to the management group, subscription, or resource group of the Kubernetes cluster where the policy assignment will apply.

### NOTE

When assigning the Azure Policy for Kubernetes definition, the **Scope** must include the cluster resource.

6. Give the policy assignment a **Name** and **Description** that you can use to identify it easily.
7. Set the **Policy enforcement** to one of the values below.

- **Enabled** - Enforce the policy on the cluster. Kubernetes admission requests with violations are denied.
- **Disabled** - Don't enforce the policy on the cluster. Kubernetes admission requests with violations aren't denied. Compliance assessment results are still available. When rolling out new policy definitions to running clusters, *Disabled* option is helpful for testing the policy definition as admission requests with violations aren't denied.

8. Select **Next**.

9. Set **parameter values**

- To exclude Kubernetes namespaces from policy evaluation, specify the list of namespaces in parameter **Namespace exclusions**. It's recommended to exclude: *kube-system*, *gatekeeper-system*, and *azure-arc*.

10. Select **Review + create**.

Alternately, use the [Assign a policy - Portal](#) quickstart to find and assign a Kubernetes policy. Search for a Kubernetes policy definition instead of the sample 'audit vms'.

#### IMPORTANT

Built-in policy definitions are available for Kubernetes clusters in category **Kubernetes**. For a list of built-in policy definitions, see [Kubernetes samples](#).

## Policy evaluation

The add-on checks in with Azure Policy service for changes in policy assignments every 15 minutes. During this refresh cycle, the add-on checks for changes. These changes trigger creates, updates, or deletes of the constraint templates and constraints.

In a Kubernetes cluster, if a namespace has the cluster-appropriate label, the admission requests with violations aren't denied. Compliance assessment results are still available.

- Azure Arc-enabled Kubernetes cluster: `admission.policy.azure.com/ignore`
- Azure Kubernetes Service cluster: `control-plane`

#### NOTE

While a cluster admin may have permission to create and update constraint templates and constraints resources install by the Azure Policy Add-on, these aren't supported scenarios as manual updates are overwritten. Gatekeeper continues to evaluate policies that existed prior to installing the add-on and assigning Azure Policy policy definitions.

Every 15 minutes, the add-on calls for a full scan of the cluster. After gathering details of the full scan and any real-time evaluations by Gatekeeper of attempted changes to the cluster, the add-on reports the results back to Azure Policy for inclusion in [compliance details](#) like any Azure Policy assignment. Only results for active policy assignments are returned during the audit cycle. Audit results can also be seen as [violations](#) listed in the status field of the failed constraint. For details on *Non-compliant* resources, see [Component details for Resource Provider modes](#).

#### NOTE

Each compliance report in Azure Policy for your Kubernetes clusters include all violations within the last 45 minutes. The timestamp indicates when a violation occurred.

Some other considerations:

- If the cluster subscription is registered with Microsoft Defender for Cloud, then Microsoft Defender for Cloud Kubernetes policies are applied on the cluster automatically.
- When a deny policy is applied on cluster with existing Kubernetes resources, any pre-existing resource that is not compliant with the new policy continues to run. When the non-compliant resource gets rescheduled on a different node the Gatekeeper blocks the resource creation.
- When a cluster has a deny policy that validates resources, the user will not see a rejection message when creating a deployment. For example, consider a Kubernetes deployment that contains replicasets and pods. When a user executes `kubectl describe deployment $MY_DEPLOYMENT`, it does not return a rejection message as part of events. However, `kubectl describe replicsets.apps $MY_DEPLOYMENT` returns the events associated with rejection.

#### NOTE

Init containers may be included during policy evaluation. To see if init containers are included, review the CRD for the following or a similar declaration:

```
input_containers[c] {
 c := input.review.object.spec.initContainers[_]
}
```

#### Constraint template conflicts

If constraint templates have the same resource metadata name, but the policy definition references the source at different locations, the policy definitions are considered to be in conflict. Example: Two policy definitions reference the same `template.yaml` file stored at different source locations such as the Azure Policy template store (`store.policy.core.windows.net`) and GitHub.

When policy definitions and their constraint templates are assigned but aren't already installed on the cluster and are in conflict, they are reported as a conflict and won't be installed into the cluster until the conflict is resolved. Likewise, any existing policy definitions and their constraint templates that are already on the cluster that conflict with newly assigned policy definitions continue to function normally. If an existing assignment is updated and there is a failure to sync the constraint template, the cluster is also marked as a conflict. For all conflict messages, see [AKS Resource Provider mode compliance reasons](#)

## Logging

As a Kubernetes controller/container, both the `azure-policy` and `gatekeeper` pods keep logs in the Kubernetes cluster. The logs can be exposed in the [Insights](#) page of the Kubernetes cluster. For more information, see [Monitor your Kubernetes cluster performance with Azure Monitor for containers](#).

To view the add-on logs, use `kubectl`:

```
Get the azure-policy pod name installed in kube-system namespace
kubectl logs <azure-policy pod name> -n kube-system

Get the gatekeeper pod name installed in gatekeeper-system namespace
kubectl logs <gatekeeper pod name> -n gatekeeper-system
```

For more information, see [Debugging Gatekeeper](#) in the Gatekeeper documentation.

## View Gatekeeper artifacts

After the add-on downloads the policy assignments and installs the constraint templates and constraints on the cluster, it annotates both with Azure Policy information like the policy assignment ID and the policy definition ID. To configure your client to view the add-on related artifacts, use the following steps:

1. Setup `kubeconfig` for the cluster.

For an Azure Kubernetes Service cluster, use the following Azure CLI:

```
Set context to the subscription
az account set --subscription <YOUR-SUBSCRIPTION>

Save credentials for kubeconfig into .kube in your home folder
az aks get-credentials --resource-group <RESOURCE-GROUP> --name <CLUSTER-NAME>
```

2. Test the cluster connection.

Run the `kubectl cluster-info` command. A successful run has each service responding with a URL of where it's running.

### View the add-on constraint templates

To view constraint templates downloaded by the add-on, run `kubectl get constrainttemplates`. Constraint templates that start with `k8sazure` are the ones installed by the add-on.

### Get Azure Policy mappings

To identify the mapping between a constraint template downloaded to the cluster and the policy definition, use `kubectl get constrainttemplates <TEMPLATE> -o yaml`. The results look similar to the following output:

```
apiVersion: templates.gatekeeper.sh/v1beta1
kind: ConstraintTemplate
metadata:
 annotations:
 azure-policy-definition-id:
 /subscriptions/<SUBID>/providers/Microsoft.Authorization/policyDefinitions/<GUID>
 constraint-template-installed-by: azure-policy-addon
 constraint-template: <URL-OF-YAML>
 creationTimestamp: "2021-09-01T13:20:55Z"
 generation: 1
 managedFields:
 - apiVersion: templates.gatekeeper.sh/v1beta1
 fieldsType: FieldsV1
...
...
```

`<SUBID>` is the subscription ID and `<GUID>` is the ID of the mapped policy definition. `<URL-OF-YAML>` is the source location of the constraint template that the add-on downloaded to install on the cluster.

### View constraints related to a constraint template

Once you have the names of the [add-on downloaded constraint templates](#), you can use the name to see the related constraints. Use `kubectl get <constraintTemplateName>` to get the list. Constraints installed by the add-on start with `azurepolicy-`.

### View constraint details

The constraint has details about violations and mappings to the policy definition and assignment. To see the details, use `kubectl get <CONSTRAINT-TEMPLATE> <CONSTRAINT> -o yaml`. The results look similar to the following output:

```

apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sAzureContainerAllowedImages
metadata:
 annotations:
 azure-policy-assignment-id: /subscriptions/<SUB-ID>/resourceGroups/<RG-NAME>/providers/Microsoft.Authorization/policyAssignments/<ASSIGNMENT-GUID>
 azure-policy-definition-id: /providers/Microsoft.Authorization/policyDefinitions/<DEFINITION-GUID>
 azure-policy-definition-reference-id: ""
 azure-policy-setdefinition-id: ""
 constraint-installed-by: azure-policy-addon
 constraint-url: <URL-OF-YAML>
 creationTimestamp: "2021-09-01T13:20:55Z"
spec:
 enforcementAction: deny
 match:
 excludedNamespaces:
 - kube-system
 - gatekeeper-system
 - azure-arc
 parameters:
 imageRegex: ^.+azurecr.io/.+$
status:
 auditTimestamp: "2021-09-01T13:48:16Z"
 totalViolations: 32
 violations:
 - enforcementAction: deny
 kind: Pod
 message: Container image nginx for container hello-world has not been allowed.
 name: hello-world-78f7bfd5b8-lmc5b
 namespace: default
 - enforcementAction: deny
 kind: Pod
 message: Container image nginx for container hello-world has not been allowed.
 name: hellow-world-89f8bfd6b9-zkggg

```

## Troubleshooting the add-on

For more information about troubleshooting the Add-on for Kubernetes, see the [Kubernetes section](#) of the Azure Policy troubleshooting article.

For Azure Policy extension for Arc extension related issues, please see:

- [Azure Arc enabled Kubernetes troubleshooting](#)

For Azure Policy related issues, please see:

- [Inspect Azure Policy logs](#)
- [General troubleshooting for Azure Policy on Kubernetes](#)

## Remove the add-on

### Remove the add-on from AKS

To remove the Azure Policy Add-on from your AKS cluster, use either the Azure portal or Azure CLI:

- Azure portal

1. Launch the AKS service in the Azure portal by selecting **All services**, then searching for and selecting **Kubernetes services**.
2. Select your AKS cluster where you want to disable the Azure Policy Add-on.
3. Select **Policies** on the left side of the Kubernetes service page.

4. In the main page, select the **Disable add-on** button.

- Azure CLI

```
Log in first with az login if you're not using Cloud Shell

az aks disable-addons --addons azure-policy --name MyAKSCluster --resource-group MyResourceGroup
```

## Remove the add-on from Azure Arc enabled Kubernetes

### NOTE

Azure Policy Add-on Helm model is now deprecated. Please opt for the [Azure Policy Extension for Azure Arc enabled Kubernetes](#) instead.

To remove the Azure Policy Add-on and Gatekeeper from your Azure Arc enabled Kubernetes cluster, run the following Helm command:

```
helm uninstall azure-policy-addon
```

## Remove the add-on from AKS Engine

### NOTE

The AKS Engine product is now deprecated for Azure public cloud customers. Please consider using [Azure Kubernetes Service \(AKS\)](#) for managed Kubernetes or [Cluster API Provider Azure](#) for self-managed Kubernetes. There are no new features planned; this project will only be updated for CVEs & similar, with Kubernetes 1.24 as the final version to receive updates.

To remove the Azure Policy Add-on and Gatekeeper from your AKS Engine cluster, use the method that aligns with how the add-on was installed:

- If installed by setting the **addons** property in the cluster definition for AKS Engine:

Redeploy the cluster definition to AKS Engine after changing the **addons** property for *azure-policy* to false:

```
"addons": [{}
 "name": "azure-policy",
 "enabled": false
]
```

For more information, see [AKS Engine - Disable Azure Policy Add-on](#).

- If installed with Helm Charts, run the following Helm command:

```
helm uninstall azure-policy-addon
```

## Diagnostic data collected by Azure Policy Add-on

The Azure Policy Add-on for Kubernetes collects limited cluster diagnostic data. This diagnostic data is vital technical data related to software and performance. It's used in the following ways:

- Keep Azure Policy Add-on up to date

- Keep Azure Policy Add-on secure, reliable, performant
- Improve Azure Policy Add-on - through the aggregate analysis of the use of the add-on

The information collected by the add-on isn't personal data. The following details are currently collected:

- Azure Policy Add-on agent version
- Cluster type
- Cluster region
- Cluster resource group
- Cluster resource ID
- Cluster subscription ID
- Cluster OS (Example: Linux)
- Cluster city (Example: Seattle)
- Cluster state or province (Example: Washington)
- Cluster country or region (Example: United States)
- Exceptions/errors encountered by Azure Policy Add-on during agent installation on policy evaluation
- Number of Gatekeeper policy definitions not installed by Azure Policy Add-on

## Next steps

- Review examples at [Azure Policy samples](#).
- Review the [Policy definition structure](#).
- Review [Understanding policy effects](#).
- Understand how to [programmatically create policies](#).
- Learn how to [get compliance data](#).
- Learn how to [remediate non-compliant resources](#).
- Review what a management group is with [Organize your resources with Azure management groups](#).

# Bring your own keys (BYOK) with Azure disks in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

Azure Storage encrypts all data in a storage account at rest. By default, data is encrypted with Microsoft-managed keys. For more control over encryption keys, you can supply customer-managed keys to use for encryption at rest for both the OS and data disks for your AKS clusters.

Learn more about customer-managed keys on [Linux](#) and [Windows](#).

## Limitations

- Data disk encryption support is limited to AKS clusters running Kubernetes version 1.17 and above.
- Encryption of OS disk with customer-managed keys can only be enabled when creating an AKS cluster.

## Prerequisites

- You must enable soft delete and purge protection for *Azure Key Vault* when using Key Vault to encrypt managed disks.
- You need the Azure CLI version 2.11.1 or later.
- Customer-managed keys are only supported in Kubernetes versions 1.17 and higher.
- If you choose to rotate (change) your keys periodically, for more information see [Customer-managed keys and encryption of Azure managed disk](#).

## Create an Azure Key Vault instance

Use an Azure Key Vault instance to store your keys. You can optionally use the Azure portal to [Configure customer-managed keys with Azure Key Vault](#)

Create a new *resource group*, then create a new *Key Vault* instance and enable soft delete and purge protection. Ensure you use the same region and resource group names for each command.

```
Optionally retrieve Azure region short names for use on upcoming commands
az account list-locations
```

```
Create new resource group in a supported Azure region
az group create -l myAzureRegionName -n myResourceGroup

Create an Azure Key Vault resource in a supported Azure region
az keyvault create -n myKeyVaultName -g myResourceGroup -l myAzureRegionName --enable-purge-protection true
--enable-soft-delete true
```

## Create an instance of a DiskEncryptionSet

Replace *myKeyVaultName* with the name of your key vault. You will also need a *key* stored in Azure Key Vault to complete the following steps. Either store your existing Key in the Key Vault you created on the previous steps, or [generate a new key](#) and replace *myKeyName* below with the name of your key.

```

Retrieve the Key Vault Id and store it in a variable
$keyVaultId=az keyvault show --name myKeyVaultName --query "[id]" -o tsv

Retrieve the Key Vault key URL and store it in a variable
$keyVaultKeyUrl=az keyvault key show --vault-name myKeyVaultName --name myKeyName --query "[key.kid]" -o tsv

Create a DiskEncryptionSet
az disk-encryption-set create -n myDiskEncryptionSetName -l myAzureRegionName -g myResourceGroup --source-vault $keyVaultId --key-url $keyVaultKeyUrl

```

#### **IMPORTANT**

Ensure your AKS cluster identity has **read** permission of DiskEncryptionSet

## Grant the DiskEncryptionSet access to key vault

Use the DiskEncryptionSet and resource groups you created on the prior steps, and grant the DiskEncryptionSet resource access to the Azure Key Vault.

```

Retrieve the DiskEncryptionSet value and set a variable
$desIdentity=az disk-encryption-set show -n myDiskEncryptionSetName -g myResourceGroup --query "[identity.principalId]" -o tsv

Update security policy settings
az keyvault set-policy -n myKeyVaultName -g myResourceGroup --object-id $desIdentity --key-permissions wrapkey unwrapkey get

```

## Create a new AKS cluster and encrypt the OS disk

Create a new **resource group** and AKS cluster, then use your key to encrypt the OS disk.

#### **IMPORTANT**

Ensure you create a new resorce group for your AKS cluster

```

Retrieve the DiskEncryptionSet value and set a variable
$diskEncryptionSetId=az disk-encryption-set show -n mydiskEncryptionSetName -g myResourceGroup --query "[id]" -o tsv

Create a resource group for the AKS cluster
az group create -n myResourceGroup -l myAzureRegionName

Create the AKS cluster
az aks create -n myAKScluster -g myResourceGroup --node-osdisk-diskencryptionset-id $diskEncryptionSetId --kubernetes-version KUBERNETES_VERSION --generate-ssh-keys

```

When new node pools are added to the cluster created above, the customer-managed key provided during the create process is used to encrypt the OS disk.

## Encrypt your AKS cluster data disk(optional)

OS disk encryption key is used to encrypt the data disk if the key isn't provided for data disk from AKS version 1.17.2. You can also encrypt AKS data disks with your other keys.

## IMPORTANT

Ensure you have the proper AKS credentials. The managed identity needs to have contributor access to the resource group where the diskencryptionset is deployed. Otherwise, you'll get an error suggesting that the managed identity does not have permissions.

```
Retrieve your Azure Subscription Id from id property as shown below
az account list
```

The following example resembles output from the command:

```
someuser@Azure:~$ az account list
[
 {
 "cloudName": "AzureCloud",
 "id": "666e66d8-1e43-4136-be25-f25bb5de5893",
 "isDefault": true,
 "name": "MyAzureSubscription",
 "state": "Enabled",
 "tenantId": "3ebcdf90-2069-4529-a1ab-7bdcb24df7cd",
 "user": {
 "cloudShellID": true,
 "name": "someuser@azure.com",
 "type": "user"
 }
 }
]
```

Create a file called **byok-azure-disk.yaml** that contains the following information. Replace myAzureSubscriptionId, myResourceGroup, and myDiskEncryptionSetName with your values, and apply the yaml. Make sure to use the resource group where your DiskEncryptionSet is deployed. If you use the Azure Cloud Shell, this file can be created using vi or nano as if working on a virtual or physical system:

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
 name: byok
provisioner: disk.csi.azure.com # replace with "kubernetes.io/azure-disk" if aks version is less than 1.21
parameters:
 skuName: StandardSSD_LRS
 kind: managed
 diskEncryptionSetID:
 "/subscriptions/{myAzureSubscriptionId}/resourceGroups/{myResourceGroup}/providers/Microsoft.Compute/diskEncryptionSets/{myDiskEncryptionSetName}"
```

Next, run the following commands to update your AKS cluster:

```
Get credentials
az aks get-credentials --name myAksCluster --resource-group myResourceGroup --output table

Update cluster
kubectl apply -f byok-azure-disk.yaml
```

## Using Azure tags

For more information on using Azure tags, see [Use Azure tags in Azure Kubernetes Service \(AKS\)](#).

## Next steps

Review [best practices for AKS cluster security](#)

# Host-based encryption on Azure Kubernetes Service (AKS)

10/27/2022 • 2 minutes to read • [Edit Online](#)

With host-based encryption, the data stored on the VM host of your AKS agent nodes' VMs is encrypted at rest and flows encrypted to the Storage service. This means the temp disks are encrypted at rest with platform-managed keys. The cache of OS and data disks is encrypted at rest with either platform-managed keys or customer-managed keys depending on the encryption type set on those disks.

By default, when using AKS, OS and data disks use server-side encryption with platform-managed keys. The caches for these disks are also encrypted at rest with platform-managed keys. You can specify your own managed keys following [Bring your own keys \(BYOK\) with Azure disks in Azure Kubernetes Service](#). The cache for these disks will then also be encrypted using the key that you specify in this step.

Host-based encryption is different than server-side encryption (SSE), which is used by Azure Storage. Azure-managed disks use Azure Storage to automatically encrypt data at rest when saving data. Host-based encryption uses the host of the VM to handle encryption before the data flows through Azure Storage.

## Before you begin

This feature can only be set at cluster creation or node pool creation time.

### NOTE

Host-based encryption is available in [Azure regions](#) that support server side encryption of Azure managed disks and only with specific [supported VM sizes](#).

### Prerequisites

- Ensure you have the CLI extension v2.23 or higher version installed.
- Ensure you have the `EncryptionAtHost` feature flag under `Microsoft.Compute` enabled.

### Register `EncryptionAtHost` feature

To create an AKS cluster that uses host-based encryption, you must enable the `EncryptionAtHost` feature flags on your subscription.

Register the `EncryptionAtHost` feature flag using the [az feature register](#) command as shown in the following example:

```
az feature register --namespace "Microsoft.Compute" --name "EncryptionAtHost"
```

It takes a few minutes for the status to show *Registered*. You can check on the registration status using the [az feature list](#) command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.Compute/EncryptionAtHost')].{Name:name, State:properties.state}"
```

When ready, refresh the registration of the `Microsoft.Compute` resource providers using the [az provider register](#) command:

```
az provider register --namespace Microsoft.Compute
```

## Limitations

- Can only be enabled on new node pools.
- Can only be enabled in [Azure regions](#) that support server-side encryption of Azure managed disks and only with specific [supported VM sizes](#).
- Requires an AKS cluster and node pool based on Virtual Machine Scale Sets(VMSS) as *VM set type*.

## Use host-based encryption on new clusters

Configure the cluster agent nodes to use host-based encryption when the cluster is created.

```
az aks create --name myAKSCluster --resource-group myResourceGroup -s Standard_DS2_v2 -l westus2 --enable-encryption-at-host
```

If you want to create clusters without host-based encryption, you can do so by omitting the `--enable-encryption-at-host` parameter.

## Use host-based encryption on existing clusters

You can enable host-based encryption on existing clusters by adding a new node pool to your cluster. Configure a new node pool to use host-based encryption by using the `--enable-encryption-at-host` parameter.

```
az aks nodepool add --name hostencrypt --cluster-name myAKSCluster --resource-group myResourceGroup -s Standard_DS2_v2 -l westus2 --enable-encryption-at-host
```

If you want to create new node pools without the host-based encryption feature, you can do so by omitting the `--enable-encryption-at-host` parameter.

## Next steps

Review [best practices for AKS cluster security](#) Read more about [host-based encryption](#).

# Enable Federal Information Process Standard (FIPS) for Azure Kubernetes Service (AKS) node pools

10/27/2022 • 3 minutes to read • [Edit Online](#)

The Federal Information Processing Standard (FIPS) 140-2 is a US government standard that defines minimum security requirements for cryptographic modules in information technology products and systems. Azure Kubernetes Service (AKS) allows you to create Linux and Windows node pools with FIPS 140-2 enabled. Deployments running on FIPS-enabled node pools can use those cryptographic modules to provide increased security and help meet security controls as part of FedRAMP compliance. For more information on FIPS 140-2, see [Federal Information Processing Standard \(FIPS\) 140](#).

## Prerequisites

You need the Azure CLI version 2.32.0 or later installed and configured. Run `az --version` to find the version. For more information about installing or upgrading the Azure CLI, see [Install Azure CLI](#).

FIPS-enabled node pools have the following limitations:

- FIPS-enabled node pools require Kubernetes version 1.19 and greater.
- To update the underlying packages or modules used for FIPS, you must use [Node Image Upgrade](#).
- Container images on the FIPS nodes haven't been assessed for FIPS compliance.

### IMPORTANT

The FIPS-enabled Linux image is a different image than the default Linux image used for Linux-based node pools. To enable FIPS on a node pool, you must create a new Linux-based node pool. You can't enable FIPS on existing node pools.

FIPS-enabled node images may have different version numbers, such as kernel version, than images that are not FIPS-enabled. Also, the update cycle for FIPS-enabled node pools and node images may differ from node pools and images that are not FIPS-enabled.

## Create a FIPS-enabled Linux node pool

To create a FIPS-enabled Linux node pool, use the `az aks nodepool add` command with the `--enable-fips-image` parameter when creating a node pool.

```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name fipsnp \
--enable-fips-image
```

### NOTE

You can also use the `--enable-fips-image` parameter with `[az aks create][az-aks-create]` when creating a cluster to enable FIPS on the default node pool. When adding node pools to a cluster created in this way, you still must use the `--enable-fips-image` parameter when adding node pools to create a FIPS-enabled node pool.

To verify your node pool is FIPS-enabled, use `az aks show` to check the `enableFIPS` value in `agentPoolProfiles`.

```
az aks show \
--resource-group myResourceGroup \
--name myAKSCluster \
--query="agentPoolProfiles[].{Name:name enableFips:enableFips}" \
-o table
```

The following example output shows the *fipsnsp* node pool is FIPS-enabled and *nodepool1* isn't.

Name	enableFips
-----	-----
fipsnsp	True
nodepool1	False

You can also verify deployments have access to the FIPS cryptographic libraries using `kubectl debug` on a node in the FIPS-enabled node pool. Use `kubectl get nodes` to list the nodes:

```
$ kubectl get nodes
NAME STATUS ROLES AGE VERSION
aks-fipsnsp-12345678-vmss000000 Ready agent 6m4s v1.19.9
aks-fipsnsp-12345678-vmss000001 Ready agent 5m21s v1.19.9
aks-fipsnsp-12345678-vmss000002 Ready agent 6m8s v1.19.9
aks-nodepool1-12345678-vmss000000 Ready agent 34m v1.19.9
```

In the above example, the nodes starting with `aks-fipsnsp` are part of the FIPS-enabled node pool. Use `kubectl debug` to run a deployment with an interactive session on one of those nodes in the FIPS-enabled node pool.

```
kubectl debug node/aks-fipsnsp-12345678-vmss000000 -it --image=mcr.microsoft.com/dotnet/runtime-deps:6.0
```

From the interactive session, you can verify the FIPS cryptographic libraries are enabled:

```
root@aks-fipsnsp-12345678-vmss000000:/# cat /proc/sys/crypto/fips_enabled
1
```

FIPS-enabled node pools also have a `kubernetes.azure.com/fips_enabled=true` label, which can be used by deployments to target those node pools.

## Create a FIPS-enabled Windows node pool

To create a FIPS-enabled Windows node pool, use the `az aks nodepool add` command with the `--enable-fips-image` parameter when creating a node pool. Unlike Linux-based node pools, Windows node pools share the same image set.

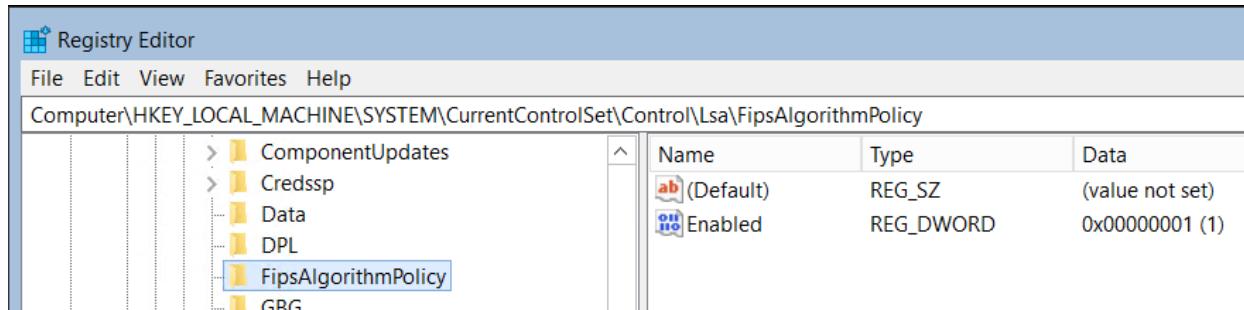
```
az aks nodepool add \
--resource-group myResourceGroup \
--cluster-name myAKSCluster \
--name fipsnsp \
--enable-fips-image \
--os-type Windows
```

To verify your node pool is FIPS-enabled, use `az aks show` to check the `enableFIPS` value in `agentPoolProfiles`.

```
az aks show \
--resource-group myResourceGroup \
--name myAKScluster \
--query="agentPoolProfiles[].{Name:name enableFips:enableFips}" \
-o table
```

To verify Windows node pools have access to the FIPS cryptographic libraries, [create an RDP connection to a Windows node](#) in a FIPS-enabled node pool and check the registry.

1. From the Run application, enter `regedit`.
2. Look for `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy` in the registry.
3. If `Enabled` is set to 1, then FIPS is enabled.



FIPS-enabled node pools also have a `kubernetes.azure.com/fips_enabled=true` label, which can be used by deployments to target those node pools.

## Next steps

To learn more about AKS security, see [Best practices for cluster security and upgrades in Azure Kubernetes Service \(AKS\)](#).

# Use an Azure AD workload identity (preview) on Azure Kubernetes Service (AKS)

10/27/2022 • 6 minutes to read • [Edit Online](#)

Today with Azure Kubernetes Service (AKS), you can assign [managed identities at the pod-level](#), which has been a preview feature. This pod-managed identity allows the hosted workload or application access to resources through Azure Active Directory (Azure AD). For example, a workload stores files in Azure Storage, and when it needs to access those files, the pod authenticates itself against the resource as an Azure managed identity. This authentication method has been replaced with [Azure Active Directory \(Azure AD\) workload identities](#) (preview), which integrate with the Kubernetes native capabilities to federate with any external identity providers. This approach is simpler to use and deploy, and overcomes several limitations in Azure AD pod-managed identity:

- Removes the scale and performance issues that existed for identity assignment
- Supports Kubernetes clusters hosted in any cloud or on-premises
- Supports both Linux and Windows workloads
- Removes the need for Custom Resource Definitions and pods that intercept [Azure Instance Metadata Service \(IMDS\)](#) traffic
- Avoids the complicated and error-prone installation steps such as cluster role assignment from the previous iteration

Azure AD workload identity works especially well with the Azure Identity client library using the [Azure SDK](#) and the [Microsoft Authentication Library](#) (MSAL) if you're using [application registration](#). Your workload can use any of these libraries to seamlessly authenticate and access Azure cloud resources.

This article helps you understand this new authentication feature, and reviews the options available to plan your migration phases and project strategy.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Dependencies

- AKS supports Azure AD workload identities on version 1.22 and higher.
- The Azure CLI version 2.40.0 or later. Run `az --version` to find the version, and run `az upgrade` to upgrade the version. If you need to install or upgrade, see [Install Azure CLI](#).
- The `aks-preview` extension version 0.5.102 or later.
- The following are the minimum versions of the [Azure Identity](#) client library supported:
  - [.NET](#) 1.5.0
  - [Java](#) 1.4.0

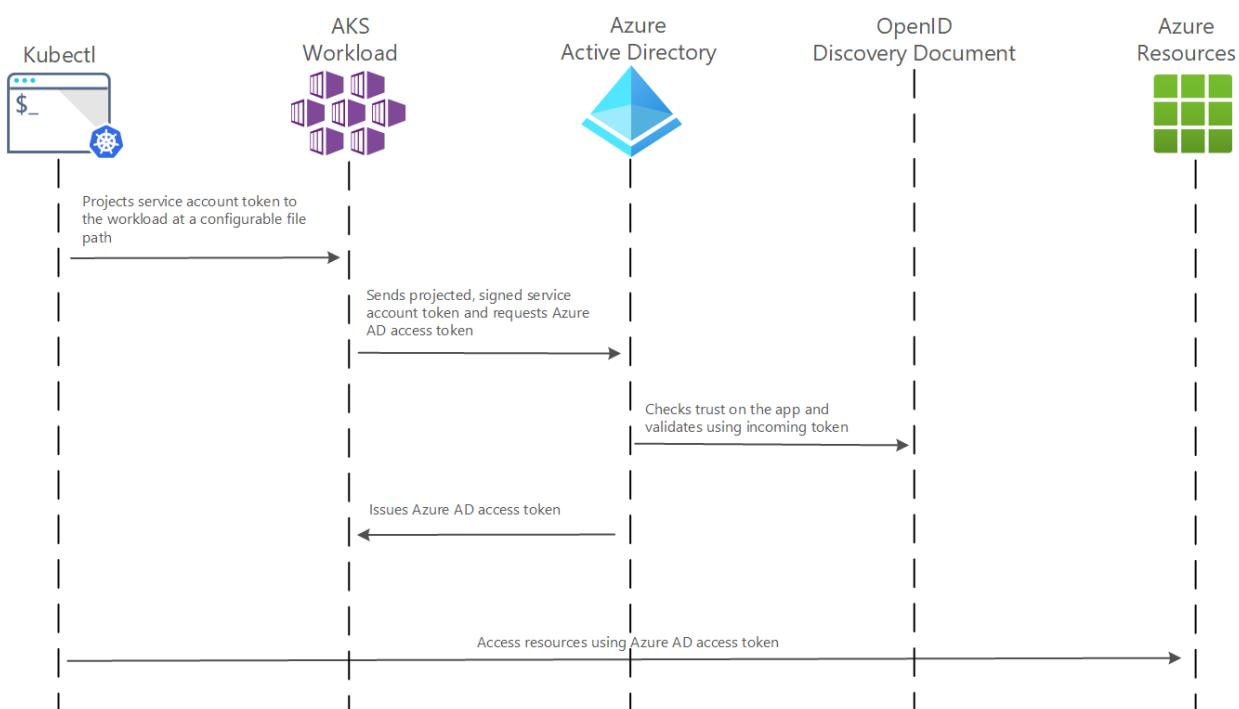
- JavaScript 2.0.0
- Python 1.7.0

## Limitations

- You can only have 20 federated identity credentials per managed identity.
- It takes a few seconds for the federated identity credential to be propagated after being initially added.

## How it works

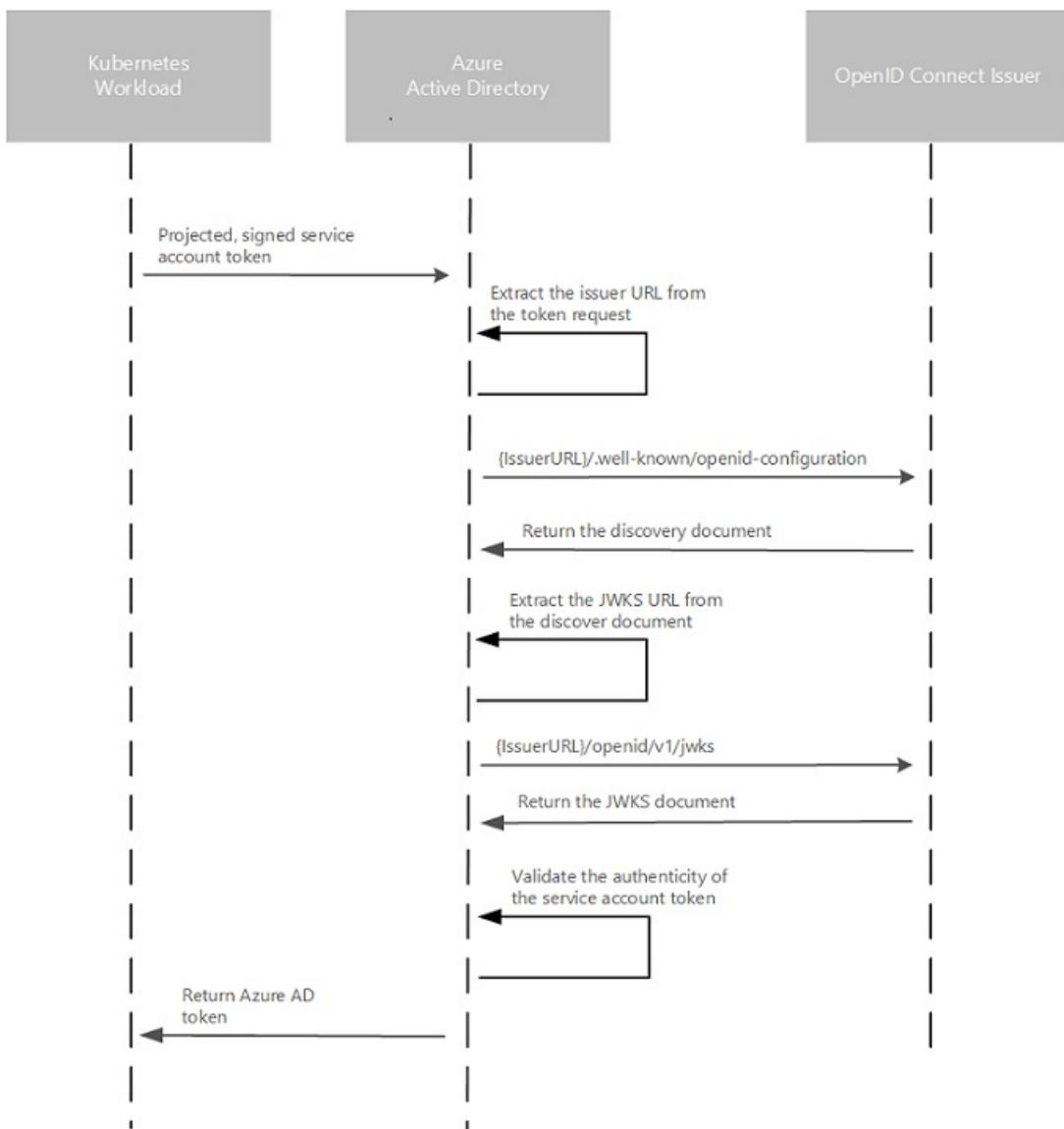
In this security model, the AKS cluster acts as token issuer, Azure Active Directory uses OpenID Connect to discover public signing keys and verify the authenticity of the service account token before exchanging it for an Azure AD token. Your workload can exchange a service account token projected to its volume for an Azure AD token using the Azure Identity client library or the Microsoft Authentication Library.



The following table describes the required OIDC issuer endpoints for Azure AD workload identity:

ENDPOINT	DESCRIPTION
{IssuerURL}/.well-known/openid-configuration	Also known as the OIDC discovery document. This contains the metadata about the issuer's configurations.
{IssuerURL}/openid/v1/jwks	This contains the public signing key(s) that Azure AD uses to verify the authenticity of the service account token.

The following diagram summarizes the authentication sequence using OpenID Connect.



## Service account labels and annotations

Azure AD workload identity supports the following mappings related to a service account:

- One-to-one where a service account references an Azure AD object.
- Many-to-one where multiple service accounts references the same Azure AD object.
- One-to-many where a service account references multiple Azure AD objects by changing the client ID annotation.

### NOTE

If the service account annotations are updated, you need to restart the pod for the changes to take effect.

If you've used [Azure AD pod-managed identity](#), think of a service account as an Azure Identity, except a service account is part of the core Kubernetes API, rather than a [Custom Resource Definition](#) (CRD). The following describes a list of available labels and annotations that can be used to configure the behavior when exchanging the service account token for an Azure AD access token.

### Service account labels

LABEL	DESCRIPTION	RECOMMENDED VALUE	REQUIRED
<code>azure.workload.identity/use</code>	Represents the service account is to be used for workload identity.	true	Yes

## Service account annotations

ANNOTATION	DESCRIPTION	DEFAULT
<code>azure.workload.identity/client-id</code>	Represents the Azure AD application client ID to be used with the pod.	
<code>azure.workload.identity/tenant-id</code>	Represents the Azure tenant ID where the Azure AD application is registered.	AZURE_TENANT_ID environment variable extracted from <code>azure-wi-webhook-config</code> ConfigMap.
<code>azure.workload.identity/service-account-token-expiration</code>	Represents the <code>expirationSeconds</code> field for the projected service account token. It's an optional field that you configure to prevent downtime caused by errors during service account token refresh. Kubernetes service account token expiry isn't correlated with Azure AD tokens. Azure AD tokens expire in 24 hours after they're issued.	3600 Supported range is 3600-86400.

## Pod annotations

ANNOTATION	DESCRIPTION	DEFAULT
<code>azure.workload.identity/service-account-token-expiration</code>	Represents the <code>expirationSeconds</code> field for the projected service account token. It's an optional field that you configure to prevent any downtime caused by errors during service account token refresh. Kubernetes service account token expiry isn't correlated with Azure AD tokens. Azure AD tokens expire in 24 hours after they're issued. <sup>1</sup>	3600 Supported range is 3600-86400.
<code>azure.workload.identity/skip-containers</code>	Represents a semi-colon-separated list of containers to skip adding projected service account token volume. For example <code>container1;container2</code> .	By default, the projected service account token volume is added to all containers if the service account is labeled with <code>azure.workload.identity/use: true</code> .

ANNOTATION	DESCRIPTION	DEFAULT
<code>azure.workload.identity/inject-proxy-sidecar</code>	Injects a proxy init container and proxy sidecar into the pod. The proxy sidecar is used to intercept token requests to IMDS and acquire an Azure AD token on behalf of the user with federated identity credential.	true
<code>azure.workload.identity/proxy-sidecar-port</code>	Represents the port of the proxy sidecar.	8080

<sup>1</sup> Takes precedence if the service account is also annotated.

## How to migrate to workload identity

On a cluster that is already running a pod-managed identity, you can configure it to use workload identity one of two ways. The first option allows you to use the same configuration you've implemented for pod-managed identity today. You just need to annotate the service account within the namespace with the identity, and it enables workload identity to inject the annotations into the pods.

The second option is to rewrite your application to use the latest version of the Azure Identity client library.

To help streamline and ease the migration process, we've developed a migration sidecar that converts the IMDS transactions your application makes over to [OpenID Connect](#) (OIDC). The migration sidecar isn't intended to be a long-term solution, but a way to get up and running quickly on workload identity. Running the migration sidecar within your application proxies the application IMDS transactions over to OIDC. The alternative approach is to upgrade to a supported version of the [Azure Identity](#) client library, which supports OIDC authentication.

The following table summarizes our migration or deployment recommendations for workload identity.

SCENARIO	DESCRIPTION
New or existing cluster deployment <a href="#">runs a supported version</a> of Azure Identity client library	No migration steps are required. Sample deployment resources: - <a href="#">Deploy and configure workload identity on a new cluster</a> - <a href="#">Tutorial: Use a workload identity with an application on AKS</a>
New or existing cluster deployment <a href="#">runs an unsupported version</a> of Azure Identity client library	Update container image to use a supported version of the Azure Identity SDK, or use the <a href="#">migration sidecar</a> .

## Next steps

- To learn how to set up your pod to authenticate using a workload identity as a migration option, see [Modernize application authentication with workload identity](#).
- See the tutorial [Use a workload identity with an application on Azure Kubernetes Service \(AKS\)](#), which helps you deploy an Azure Kubernetes Service cluster and configure a sample application to use a workload identity.

# Deploy and configure workload identity (preview) on an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 5 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is a managed Kubernetes service that lets you quickly deploy and manage Kubernetes clusters. In this article, you will:

- Deploy an AKS cluster using the Azure CLI that includes the OpenID Connect Issuer and an Azure AD workload identity (preview)
- Grant access to your Azure Key Vault
- Create an Azure Active Directory (Azure AD) workload identity and Kubernetes service account
- Configure the managed identity for token federation.

This article assumes you have a basic understanding of Kubernetes concepts. For more information, see [Kubernetes core concepts for Azure Kubernetes Service \(AKS\)](#). If you aren't familiar with Azure AD workload identity (preview), see the following [Overview](#) article.

- This article requires version 2.40.0 or later of the Azure CLI. If using Azure Cloud Shell, the latest version is already installed.
- You've installed the latest version of the `aks-preview` extension, version 0.5.102 or later.
- The identity you're using to create your cluster has the appropriate minimum permissions. For more details on access and identity for AKS, see [Access and identity options for Azure Kubernetes Service \(AKS\)](#).
- If you have multiple Azure subscriptions, select the appropriate subscription ID in which the resources should be billed using the `az account` command.

## Install the `aks-preview` Azure CLI extension

### IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

To install the `aks-preview` extension, run the following command:

```
az extension add --name aks-preview
```

Run the following command to update to the latest version of the extension released:

```
az extension update --name aks-preview
```

## Register the 'EnableWorkloadIdentityPreview' feature flag

Register the `EnableWorkloadIdentityPreview` feature flag by using the [az feature register](#) command, as shown in the following example:

```
az feature register --namespace "Microsoft.ContainerService" --name "EnableWorkloadIdentityPreview"
```

It takes a few minutes for the status to show *Registered*. Verify the registration status by using the [az feature list](#) command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/EnableWorkloadIdentityPreview')].{Name:name, State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider by using the [az provider register](#) command:

```
az provider register --namespace Microsoft.ContainerService
```

## Create AKS cluster

Create an AKS cluster using the [az aks create](#) command with the `--enable-oidc-issuer` parameter to use the OIDC Issuer. The following example creates a cluster named *myAKSCluster* with one node in the *myResourceGroup*:

```
az aks create -g myResourceGroup -n myAKSCluster --node-count 1 --enable-oidc-issuer --enable-workload-identity --generate-ssh-keys
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

### NOTE

When you create an AKS cluster, a second resource group is automatically created to store the AKS resources. For more information, see [Why are two resource groups created with AKS?](#).

To get the OIDC Issuer URL and save it to an environmental variable, run the following command. Replace the default values for the cluster name and the resource group name.

```
export AKS_OIDC_ISSUER=$(az aks show -n myAKSCluster -g myResourceGroup --query "oidcIssuerProfile.issuerUrl" -otsv)"
```

## Create a managed identity and grant permissions to access Azure Key Vault

This step is necessary if you need to access secrets, keys, and certificates that are mounted in Azure Key Vault from a pod. Perform the following steps to configure access with a managed identity. These steps assume you have an Azure Key Vault already created and configured in your subscription. If you don't have one, see [Create an Azure Key Vault using the Azure CLI](#).

Before proceeding, you need the following information:

- Name of the Key Vault

- Resource group holding the Key Vault

You can retrieve this information using the Azure CLI command: [az keyvault list](#).

1. Use the Azure CLI [az account set](#) command to set a specific subscription to be the current active subscription. Then use the [az identity create](#) command to create a managed identity.

```
az account set --subscription "subscriptionID"
```

```
az identity create --name "userAssignedIdentityName" --resource-group "resourceGroupName" --location "location" --subscription "subscriptionID"
```

2. Set an access policy for the managed identity to access secrets in your Key Vault by running the following commands:

```
export USER_ASSIGNED_CLIENT_ID=$(az identity show --resource-group "resourceGroupName" --name "userAssignedIdentityName" --query 'clientId' -otsv)"
```

```
az keyvault set-policy --name "keyVaultName" --secret-permissions get --spn "${USER_ASSIGNED_CLIENT_ID}"
```

## Create Kubernetes service account

Create a Kubernetes service account and annotate it with the client ID of the managed identity created in the previous step. Use the [az aks get-credentials](#) command and replace the values for the cluster name and the resource group name.

```
az aks get-credentials -n myAKScluster -g MyResourceGroup
```

Copy and paste the following multi-line input in the Azure CLI, and update the values for `serviceAccountName` and `serviceAccountNamespace` with the Kubernetes service account name and its namespace.

```
cat <<EOF | kubectl apply -f -
apiVersion: v1
kind: ServiceAccount
metadata:
 annotations:
 azure.workload.identity/client-id: ${USER_ASSIGNED_CLIENT_ID}
 labels:
 azure.workload.identity/use: "true"
 name: serviceAccountName
 namespace: serviceAccountNamespace
EOF
```

The following output resembles successful creation of the identity:

```
Serviceaccount/workload-identity-sa created
```

## Establish federated identity credential

Use the [az identity federated-credential create](#) command to create the federated identity credential between the

managed identity, the service account issuer, and the subject. Replace the values `resourceGroupName`, `userAssignedIdentityName`, `federatedIdentityName`, `serviceAccountNamespace`, and `serviceAccountName`.

```
az identity federated-credential create --name federatedIdentityName --identity-name userAssignedIdentityName --resource-group resourceGroupName --issuer ${AKS_OIDC_ISSUER} --subject system:serviceaccount:serviceAccountNamespace:serviceAccountName
```

#### NOTE

It takes a few seconds for the federated identity credential to be propagated after being initially added. If a token request is made immediately after adding the federated identity credential, it might lead to failure for a couple of minutes as the cache is populated in the directory with old data. To avoid this issue, you can add a slight delay after adding the federated identity credential.

## Next steps

In this article, you deployed a Kubernetes cluster and configured it to use a workload identity in preparation for application workloads to authenticate with that credential. Now you're ready to deploy your application and configure it to use the workload identity with the latest version of the [Azure Identity](#) client library. If you can't rewrite your application to use the latest client library version, you can [set up your application pod](#) to authenticate using managed identity with workload identity as a short-term migration solution.

# Modernize application authentication with workload identity sidecar

10/27/2022 • 5 minutes to read • [Edit Online](#)

If your Kubernetes application runs on Azure Kubernetes Service (AKS) and is using a managed identity to securely access resources in Azure, you can set up a migration sidecar ensuring a smooth transition using the new Azure Identity SDK and minimize downtime. This sidecar intercepts Instance Metadata Service (IMDS) traffic and routes them to Azure Active Directory (Azure AD) using OpenID Connect (OIDC). This enables you to migrate from using managed identity with pod identity to workload identity, until you can migrate your applications to use the latest version of Azure Identity SDK.

This article shows you how to set up your application pod to authenticate using managed identity with workload identity as a short-term migration solution.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Before you begin

- The Azure CLI version 2.40.0 or later. Run `az --version` to find the version, and run `az upgrade` to upgrade the version. If you need to install or upgrade, see [Install Azure CLI][install-azure-cli].

## Create a managed identity

If you don't have a managed identity created and assigned to your pod, perform the following steps to create and grant the necessary permissions to storage, Key Vault, or whatever resources your application needs to authenticate with in Azure.

1. Use the Azure CLI `az account set` command to set a specific subscription to be the current active subscription. Then use the `az identity create` command to create a managed identity.

```
az account set --subscription "subscriptionID"
```

```
az identity create --name "userAssignedIdentityName" --resource-group "resourceGroupName" --location "location" --subscription "subscriptionID"
```

```
export USER_ASSIGNED_CLIENT_ID=$(az identity show --resource-group "resourceGroupName" --name "userAssignedIdentityName" --query 'clientId' -otsv)"
```

2. Grant the managed identity the permissions required to access the resources in Azure it requires.

- To get the OIDC Issuer URL and save it to an environmental variable, run the following command. Replace the default values for the cluster name and the resource group name.

```
export AKS_OIDC_ISSUER=$(az aks show -n myAKScluster -g myResourceGroup --query "oidcIssuerProfile.issuerUrl" -otsv)"
```

## Create Kubernetes service account

If you don't have a dedicated Kubernetes service account created for this application, perform the following steps to create and then annotate it with the client ID of the managed identity created in the previous step. Use the [az aks get-credentials](#) command and replace the values for the cluster name and the resource group name.

```
az aks get-credentials -n myAKScluster -g "${RESOURCE_GROUP}"
```

Copy and paste the following multi-line input in the Azure CLI.

```
cat <<EOF | kubectl apply -f -
apiVersion: v1
kind: ServiceAccount
metadata:
 annotations:
 azure.workload.identity/client-id: ${USER_ASSIGNED_CLIENT_ID}
 labels:
 azure.workload.identity/use: "true"
 name: ${SERVICE_ACCOUNT_NAME}
 namespace: ${SERVICE_ACCOUNT_NAMESPACE}
EOF
```

The following output resembles successful creation of the identity:

```
Serviceaccount/workload-identity-sa created
```

## Establish federated identity credential

Use the [az identity federated-credential create](#) command to create the federated identity credential between the managed identity, the service account issuer, and the subject. Replace the values `resourceGroupName`, `userAssignedIdentityName`, `federatedIdentityName`, `serviceAccountNamespace`, and `serviceAccountName`.

```
az identity federated-credential create --name federatedIdentityName --identity-name userAssignedIdentityName --resource-group resourceGroupName --issuer ${AKS_OIDC_ISSUER} --subject system:serviceaccount:${SERVICE_ACCOUNT_NAMESPACE}:${SERVICE_ACCOUNT_NAME}
```

### NOTE

It takes a few seconds for the federated identity credential to be propagated after being initially added. If a token request is made immediately after adding the federated identity credential, it might lead to failure for a couple of minutes as the cache is populated in the directory with old data. To avoid this issue, you can add a slight delay after adding the federated identity credential.

## Deploy the workload

If your application is using managed identity and still relies on IMDS to get an access token, you can use the

workload identity migration sidecar to start migrating to workload identity. This sidecar is a migration solution and in the long-term applications, you should modify their code to use the latest Azure Identity SDKs that support client assertion.

To update or deploy the workload, add these pod annotations only if you want to use the migration sidecar. You inject the following [annotation](#) values to use the sidecar in your pod specification:

- `azure.workload.identity/inject-proxy-sidecar` - value is `true` or `false`
- `azure.workload.identity/proxy-sidecar-port` - value is the desired port for the proxy sidecar. The default value is `8080`.

When a pod with the above annotations is created, the Azure Workload Identity mutating webhook automatically injects the init-container and proxy sidecar to the pod spec.

The webhook that is already running adds the following YAML snippets to the pod deployment. The following is an example of the mutated pod spec:

```
apiVersion: v1
kind: Pod
metadata:
 name: httpbin-pod
 labels:
 app: httpbin
spec:
 serviceAccountName: workload-identity-sa
 initContainers:
 - name: init-networking
 image: mcr.microsoft.com/oss/azure/workload-identity/proxy-init:v0.13.0
 securityContext:
 capabilities:
 add:
 - NET_ADMIN
 drop:
 - ALL
 privileged: true
 runAsUser: 0
 env:
 - name: PROXY_PORT
 value: "8080"
 containers:
 - name: nginx
 image: nginx:alpine
 ports:
 - containerPort: 80
 - name: proxy
 image: mcr.microsoft.com/oss/azure/workload-identity/proxy:v0.13.0
 ports:
 - containerPort: 8080
```

This configuration applies to any configuration where a pod is being created. After updating or deploying your application, you can verify the pod is in a running state using the [kubectl describe pod](#) command. Replace the value `podName` with the image name of your deployed pod.

```
kubectl describe pods podName -c azwi-proxy
```

To verify that pod is passing IMDS transactions, use the [\[kubectl logs\]\[kubelet-logs\]](#) command. Replace the value `podName` with the image name of your deployed pod:

```
kubectl logs podName
```

The following log output resembles successful communication through the proxy sidecar. Verify that the logs show a token is successfully acquired and the GET operation is successful.

```
I0926 00:29:29.968723 1 proxy.go:97] proxy "msg"="starting the proxy server" "port"=8080
"userAgent"="azure-workload-identity/proxy/v0.13.0-12-gc8527f3 (linux/amd64) c8527f3/2022-09-26-00:19"
I0926 00:29:29.972496 1 proxy.go:173] proxy "msg"="received readyz request" "method"="GET"
"uri"="/readyz"
I0926 00:29:30.936769 1 proxy.go:107] proxy "msg"="received token request" "method"="GET"
"uri"="/metadata/identity/oauth2/token?resource=https://management.core.windows.net/api-version=2018-02-
01&client_id=<client_id>"
I0926 00:29:31.101998 1 proxy.go:129] proxy "msg"="successfully acquired token" "method"="GET"
"uri"="/metadata/identity/oauth2/token?resource=https://management.core.windows.net/api-version=2018-02-
01&client_id=<client_id>"
```

## Remove pod-managed identity

After you've completed your testing and the application is successfully able to get a token using the proxy sidecar, you can remove the Azure AD pod-managed identity mapping for the pod from your cluster, and then remove the identity.

1. Run the [az aks pod-identity delete](#) command to remove the identity from your pod. This should only be done after all pods in the namespace using the pod-managed identity mapping have migrated to use the sidecar.

```
az aks pod-identity delete --name podIdentityName --namespace podIdentityNamespace --resource-group
myResourceGroup --cluster-name myAKSCluster
```

## Next steps

This article showed you how to set up your pod to authenticate using a workload identity as a migration option. For more information about Azure AD workload identity (preview), see the following [Overview](#) article.

# Use Azure Active Directory pod-managed identities in Azure Kubernetes Service (Preview)

10/27/2022 • 9 minutes to read • [Edit Online](#)

Azure Active Directory (Azure AD) pod-managed identities use Kubernetes primitives to associate [managed identities for Azure resources](#) and identities in Azure AD with pods. Administrators create identities and bindings as Kubernetes primitives that allow pods to access Azure resources that rely on Azure AD as an identity provider.

## NOTE

We recommend you review [Azure AD workload identity](#) (preview). This authentication method replaces pod-managed identity (preview), which integrates with the Kubernetes native capabilities to federate with any external identity providers on behalf of the application.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Before you begin

You must have the following resource installed:

- The Azure CLI, version 2.20.0 or later
- The `aks-preview` extension version 0.5.5 or later

## Limitations

- A maximum of 200 pod identities are allowed for a cluster.
- A maximum of 200 pod identity exceptions are allowed for a cluster.
- Pod-managed identities are available on Linux node pools only.
- This feature is only supported for Virtual Machine Scale Sets backed clusters.

Register the `EnablePodIdentityPreview`

Register the `EnablePodIdentityPreview` feature:

```
az feature register --name EnablePodIdentityPreview --namespace Microsoft.ContainerService
```

Install the `aks-preview` Azure CLI

You also need the `aks-preview` Azure CLI extension version 0.5.5 or later. Install the `aks-preview` Azure CLI extension by using the [az extension add](#) command. Or install any available updates by using the [az extension update](#) command.

```
Install the aks-preview extension
az extension add --name aks-preview

Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

## Operation mode options

Azure AD pod identity supports two modes of operation:

- **Standard Mode:** In this mode, the following two components are deployed to the AKS cluster:
  - **Managed Identity Controller (MIC):** An MIC is a Kubernetes controller that watches for changes to pods, [AzureIdentity](#) and [AzureIdentityBinding](#) through the Kubernetes API Server. When it detects a relevant change, the MIC adds or deletes [AzureAssignedIdentity](#) as needed. Specifically, when a pod is scheduled, the MIC assigns the managed identity on Azure to the underlying virtual machine scale set used by the node pool during the creation phase. When all pods using the identity are deleted, it removes the identity from the virtual machine scale set of the node pool, unless the same managed identity is used by other pods. The MIC takes similar actions when [AzureIdentity](#) or [AzureIdentityBinding](#) are created or deleted.
  - **Node Managed Identity (NMI):** NMI is a pod that runs as a DaemonSet on each node in the AKS cluster. NMI intercepts security token requests to the [Azure Instance Metadata Service](#) on each node, redirect them to itself and validates if the pod has access to the identity it's requesting a token for and fetch the token from the Azure AD tenant on behalf of the application.
- **Managed Mode:** This mode offers only NMI. When installed via the AKS cluster add-on, Azure manages creation of Kubernetes primitives ([AzureIdentity](#) and [AzureIdentityBinding](#)) and identity assignment in response to CLI commands by the user. Otherwise, if installed via Helm chart, the identity needs to be manually assigned and managed by the user. For more information, see [Pod identity in managed mode](#).

When you install the Azure AD pod identity via Helm chart or YAML manifest as shown in the [Installation Guide](#), you can choose between the `standard` and `managed` mode. If you instead decide to install the Azure AD pod identity using the AKS cluster add-on as shown in this article, the setup will use the `managed` mode.

## Create an AKS cluster with Azure Container Networking Interface (CNI)

### NOTE

This is the default recommended configuration

Create an AKS cluster with Azure CNI and pod-managed identity enabled. The following commands use [az group create](#) to create a resource group named *myResourceGroup* and the [az aks create](#) command to create an AKS cluster named *myAKSCluster* in the *myResourceGroup* resource group.

```
az group create --name myResourceGroup --location eastus
az aks create -g myResourceGroup -n myAKSCluster --enable-pod-identity --network-plugin azure
```

Use [az aks get-credentials](#) to sign in to your AKS cluster. This command also downloads and configures the `kubectl` client certificate on your development computer.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

#### NOTE

When you enable pod-managed identity on your AKS cluster, an AzurePodIdentityException named `aks-addon-exception` is added to the `kube-system` namespace. An AzurePodIdentityException allows pods with certain labels to access the Azure Instance Metadata Service (IMDS) endpoint without being intercepted by the NMI server. The `aks-addon-exception` allows AKS first-party addons, such as Azure AD pod-managed identity, to operate without having to manually configure an AzurePodIdentityException. Optionally, you can add, remove, and update an AzurePodIdentityException using

```
az aks pod-identity exception add , az aks pod-identity exception delete ,
az aks pod-identity exception update , or kubectl .
```

## Update an existing AKS cluster with Azure CNI

Update an existing AKS cluster with Azure CNI to include pod-managed identity.

```
az aks update -g $MY_RESOURCE_GROUP -n $MY_CLUSTER --enable-pod-identity
```

## Using Kubenet network plugin with Azure Active Directory pod-managed identities

#### IMPORTANT

Running `aad-pod-identity` in a cluster with Kubenet is not a recommended configuration due to security concerns. Default Kubenet configuration fails to prevent ARP spoofing, which could be utilized by a pod to act as another pod and gain access to an identity it's not intended to have. Please follow the mitigation steps and configure policies before enabling `aad-pod-identity` in a cluster with Kubenet.

### Mitigation

To mitigate the vulnerability at the cluster level, you can use the Azure built-in policy "Kubernetes cluster containers should only use allowed capabilities" to limit the `CAP_NET_RAW` attack.

Add `NET_RAW` to "Required drop capabilities"

Assign policy ...

The screenshot shows the 'Parameters' tab of an Azure Policy assignment. The 'Required drop capabilities' field is highlighted with a red box. Other fields shown include 'Effect' (audit), 'Namespace exclusions' (containing 'kube-system', 'gatekeeper-system', 'azure-arc'), 'Namespace inclusions' (empty), 'Kubernetes label selector' (empty), and 'Allowed capabilities' (empty).

If you are not using Azure Policy, you can use OpenPolicyAgent admission controller together with Gatekeeper validating webhook. Provided you have Gatekeeper already installed in your cluster, add the ConstraintTemplate of type K8sPSPCapabilities:

```
kubectl apply -f https://raw.githubusercontent.com/open-policy-agent/gatekeeper-library/master/library/pod-security-policy/capabilities/template.yaml
```

Add a template to limit the spawning of Pods with the NET\_RAW capability:

```
apiVersion: constraints.gatekeeper.sh/v1beta1
kind: K8sPSPCapabilities
metadata:
 name: prevent-net-raw
spec:
 match:
 kinds:
 - apiGroups: [""]
 kinds: ["Pod"]
 excludedNamespaces:
 - "kube-system"
 parameters:
 requiredDropCapabilities: ["NET_RAW"]
```

## Create an AKS cluster with Kubenet network plugin

Create an AKS cluster with Kubenet network plugin and pod-managed identity enabled.

```
az aks create -g $MY_RESOURCE_GROUP -n $MY_CLUSTER --enable-pod-identity --enable-pod-identity-with-kubenet
```

## Update an existing AKS cluster with Kubenet network plugin

Update an existing AKS cluster with Kubenet network plugin to include pod-managed identity.

```
az aks update -g $MY_RESOURCE_GROUP -n $MY_CLUSTER --enable-pod-identity --enable-pod-identity-with-kubenet
```

## Create an identity

### IMPORTANT

You must have the relevant permissions (for example, Owner) on your subscription to create the identity.

Create an identity which will be used by the demo pod with [az identity create](#) and set the *IDENTITY\_CLIENT\_ID* and *IDENTITY\_RESOURCE\_ID* variables.

```
az group create --name myIdentityResourceGroup --location eastus
export IDENTITY_RESOURCE_GROUP="myIdentityResourceGroup"
export IDENTITY_NAME="application-identity"
az identity create --resource-group ${IDENTITY_RESOURCE_GROUP} --name ${IDENTITY_NAME}
export IDENTITY_CLIENT_ID=$(az identity show -g ${IDENTITY_RESOURCE_GROUP} -n ${IDENTITY_NAME} --query clientId -otsv)
export IDENTITY_RESOURCE_ID=$(az identity show -g ${IDENTITY_RESOURCE_GROUP} -n ${IDENTITY_NAME} --query id -otsv)"
```

## Assign permissions for the managed identity

The managed identity that will be assigned to the pod needs to be granted permissions that align with the

actions it will be taking.

To run the demo, the *IDENTITY\_CLIENT\_ID* managed identity must have Virtual Machine Contributor permissions in the resource group that contains the virtual machine scale set of your AKS cluster.

```
NODE_GROUP=$(az aks show -g myResourceGroup -n myAKSCluster --query nodeResourceGroup -o tsv)
NODES_RESOURCE_ID=$(az group show -n $NODE_GROUP -o tsv --query "id")
az role assignment create --role "Virtual Machine Contributor" --assignee "$IDENTITY_CLIENT_ID" --scope
$NODES_RESOURCE_ID
```

## Create a pod identity

Create a pod identity for the cluster using `az aks pod-identity add`.

```
export POD_IDENTITY_NAME="my-pod-identity"
export POD_IDENTITY_NAMESPACE="my-app"
az aks pod-identity add --resource-group myResourceGroup --cluster-name myAKSCluster --namespace
${POD_IDENTITY_NAMESPACE} --name ${POD_IDENTITY_NAME} --identity-resource-id ${IDENTITY_RESOURCE_ID}
```

### NOTE

The "POD\_IDENTITY\_NAME" has to be a valid [DNS subdomain name](#) as defined in [RFC 1123](#).

### NOTE

When you assign the pod identity by using `pod-identity add`, the Azure CLI attempts to grant the Managed Identity Operator role over the pod identity (*IDENTITY\_RESOURCE\_ID*) to the cluster identity.

Azure will create an `AzureIdentity` resource in your cluster representing the identity in Azure, and an `AzureIdentityBinding` resource which connects the `AzureIdentity` to a selector. You can view these resources with

```
kubectl get azureidentity -n $POD_IDENTITY_NAMESPACE
kubectl get azureidentitybinding -n $POD_IDENTITY_NAMESPACE
```

## Run a sample application

For a pod to use AAD pod-managed identity, the pod needs an `aadpodidbinding` label with a value that matches a selector from a `AzureIdentityBinding`. By default, the selector will match the name of the pod identity, but it can also be set using the `--binding-selector` option when calling `az aks pod-identity add`.

To run a sample application using AAD pod-managed identity, create a `demo.yaml` file with the following contents. Replace *POD\_IDENTITY\_NAME*, *IDENTITY\_CLIENT\_ID*, and *IDENTITY\_RESOURCE\_GROUP* with the values from the previous steps. Replace *SUBSCRIPTION\_ID* with your subscription ID.

### NOTE

In the previous steps, you created the *POD\_IDENTITY\_NAME*, *IDENTITY\_CLIENT\_ID*, and *IDENTITY\_RESOURCE\_GROUP* variables. You can use a command such as `echo` to display the value you set for variables, for example

```
echo $POD_IDENTITY_NAME
```

```

apiVersion: v1
kind: Pod
metadata:
 name: demo
 labels:
 aadpodidbinding: $POD_IDENTITY_NAME
spec:
 containers:
 - name: demo
 image: mcr.microsoft.com/oss/azure/aad-pod-identity/demo:v1.6.3
 args:
 - --subscriptionid=$SUBSCRIPTION_ID
 - --clientid=$IDENTITY_CLIENT_ID
 - --resourcegroup=$IDENTITY_RESOURCE_GROUP
 env:
 - name: MY_POD_NAME
 valueFrom:
 fieldRef:
 fieldPath: metadata.name
 - name: MY_POD_NAMESPACE
 valueFrom:
 fieldRef:
 fieldPath: metadata.namespace
 - name: MY_POD_IP
 valueFrom:
 fieldRef:
 fieldPath: status.podIP
 nodeSelector:
 kubernetes.io/os: linux

```

Notice the pod definition has an *aadpodidbinding* label with a value that matches the name of the pod identity you ran `az aks pod-identity add` in the previous step.

Deploy `demo.yaml` to the same namespace as your pod identity using `kubectl apply`:

```
kubectl apply -f demo.yaml --namespace $POD_IDENTITY_NAMESPACE
```

Verify the sample application successfully runs using `kubectl logs`.

```
kubectl logs demo --follow --namespace $POD_IDENTITY_NAMESPACE
```

Verify that the logs show a token is successfully acquired and the *GET* operation is successful.

```

...
successfully doARMOperations vm count 0
successfully acquired a token using the MSI,
msiEndpoint(http://169.254.169.254/metadata/identity/oauth2/token)
successfully acquired a token, userAssignedID MSI,
msiEndpoint(http://169.254.169.254/metadata/identity/oauth2/token) clientID(xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxx)
successfully made GET on instance metadata
...

```

## Run an application with multiple identities

To enable an application to use multiple identities, set the `--binding-selector` to the same selector when creating pod identities.

```
az aks pod-identity add --resource-group myResourceGroup --cluster-name myAKSCluster --namespace ${POD_IDENTITY_NAMESPACE} --name ${POD_IDENTITY_NAME_1} --identity-resource-id ${IDENTITY_RESOURCE_ID_1} --binding-selector myMultiIdentitySelector
az aks pod-identity add --resource-group myResourceGroup --cluster-name myAKSCluster --namespace ${POD_IDENTITY_NAMESPACE} --name ${POD_IDENTITY_NAME_2} --identity-resource-id ${IDENTITY_RESOURCE_ID_2} --binding-selector myMultiIdentitySelector
```

Then set the `aadpodidbinding` field in your pod YAML to the binding selector you specified.

```
apiVersion: v1
kind: Pod
metadata:
 name: demo
 labels:
 aadpodidbinding: myMultiIdentitySelector
...
```

## Clean up

To remove an Azure AD pod-managed identity from your cluster, remove the sample application and the pod identity from the cluster. Then remove the identity.

```
kubectl delete pod demo --namespace ${POD_IDENTITY_NAMESPACE}
az aks pod-identity delete --name ${POD_IDENTITY_NAME} --namespace ${POD_IDENTITY_NAMESPACE} --resource-group myResourceGroup --cluster-name myAKSCluster
az identity delete -g ${IDENTITY_RESOURCE_GROUP} -n ${IDENTITY_NAME}
```

## Next steps

For more information on managed identities, see [Managed identities for Azure resources](#).

# Secure traffic between pods using network policies in Azure Kubernetes Service (AKS)

10/27/2022 • 9 minutes to read • [Edit Online](#)

When you run modern, microservices-based applications in Kubernetes, you often want to control which components can communicate with each other. The principle of least privilege should be applied to how traffic can flow between pods in an Azure Kubernetes Service (AKS) cluster. Let's say you likely want to block traffic directly to back-end applications. The *Network Policy* feature in Kubernetes lets you define rules for ingress and egress traffic between pods in a cluster.

This article shows you how to install the Network Policy engine and create Kubernetes network policies to control the flow of traffic between pods in AKS. Network Policy could be used for Linux-based or Windows-based nodes and pods in AKS.

## Before you begin

You need the Azure CLI version 2.0.61 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Overview of Network Policy

All pods in an AKS cluster can send and receive traffic without limitations, by default. To improve security, you can define rules that control the flow of traffic. Back-end applications are often only exposed to required front-end services, for example. Or, database components are only accessible to the application tiers that connect to them.

Network Policy is a Kubernetes specification that defines access policies for communication between Pods. Using network policies, you define an ordered set of rules to send and receive traffic and apply them to a collection of pods that match one or more label selectors.

These Network Policy rules are defined as YAML manifests. Network policies can be included as part of a wider manifest that also creates a deployment or service.

## Network policy options in AKS

Azure provides two ways to implement Network Policy. You choose a Network Policy option when you create an AKS cluster. The policy option can't be changed after the cluster is created:

- Azure's own implementation, called *Azure Network Policy Manager (NPM)*.
- *Calico Network Policies*, an open-source network and network security solution founded by [Tigera](#).

Azure NPM for Linux uses Linux *IPTables* and Azure NPM for Windows uses *Host Network Service (HNS) ACL Policies* to enforce the specified policies. Policies are translated into sets of allowed and disallowed IP pairs. These pairs are then programmed as IPTable/HNS ACLPolicy filter rules.

## Differences between Azure NPM and Calico Network Policy and their capabilities

CAPABILITY	AZURE NPM	CALICO NETWORK POLICY
Supported platforms	Linux, Windows Server 2022	Linux, Windows Server 2019 and 2022
Supported networking options	Azure CNI	Azure CNI (Linux, Windows Server 2019 and 2022) and kubenet (Linux)
Compliance with Kubernetes specification	All policy types supported	All policy types supported
Additional features	None	Extended policy model consisting of Global Network Policy, Global Network Set, and Host Endpoint. For more information on using the <code>calicoctl</code> CLI to manage these extended features, see <a href="#">calicoctl user reference</a> .
Support	Supported by Azure support and Engineering team	Calico community support. For more information on additional paid support, see <a href="#">Project Calico support options</a> .
Logging	Logs available with <code>kubectl log -n kube-system</code> command	For more information, see <a href="#">Calico component logs</a>

## Limitations:

Azure Network Policy Manager(NPM) doesn't support IPv6. Otherwise, Azure NPM fully supports the network policy spec in Linux.

- In Windows, Azure NPM doesn't support the following:
  - named ports
  - SCTP protocol
  - negative match label or namespace selectors (e.g. all labels except "debug=true")
  - "except" CIDR blocks (a CIDR with exceptions)

### NOTE

- Azure NPM pod logs will record an error if an unsupported policy is created.

## Create an AKS cluster and enable Network Policy

To see network policies in action, let's create an AKS cluster that supports network policy and then work on adding policies.

### IMPORTANT

The network policy feature can only be enabled when the cluster is created. You can't enable network policy on an existing AKS cluster.

To use Azure NPM, you must use the [Azure CNI plug-in](#). Calico Network Policy could be used with either this same Azure CNI plug-in or with the Kubenet CNI plug-in.

The following example script:

- Creates an AKS cluster with system-assigned identity and enables Network Policy.
  - The *Azure NPM* option is used. To use Calico as the Network Policy option instead, use the `--network-policy calico` parameter. Note: Calico could be used with either `--network-plugin azure` or `--network-plugin kubenet`.

Instead of using a system-assigned identity, you can also use a user-assigned identity. For more information, see [Use managed identities](#).

### Create an AKS cluster with Azure NPM enabled - Linux only

In this section, we'll work on creating a cluster with Linux node pools and Azure NPM enabled.

To begin, you should replace the values for `$RESOURCE_GROUP_NAME` and `$CLUSTER_NAME` variables.

```
$RESOURCE_GROUP_NAME=myResourceGroup-NP
$CLUSTER_NAME=myAKSCluster
$LOCATION=canadaeast
```

Create the AKS cluster and specify *azure* for the `network-plugin` and `network-policy`.

Use the following command to create a cluster:

```
az aks create \
 --resource-group $RESOURCE_GROUP_NAME \
 --name $CLUSTER_NAME \
 --node-count 1 \
 --network-plugin azure \
 --network-policy azure
```

### Create an AKS cluster with Azure NPM enabled - Windows Server 2022 (Preview)

In this section, we'll work on creating a cluster with Windows node pools and Azure NPM enabled.

Please execute the following commands prior to creating a cluster:

```
az extension add --name aks-preview
az extension update --name aks-preview
az feature register --namespace Microsoft.ContainerService --name AKSWindows2022Preview
az feature register --namespace Microsoft.ContainerService --name WindowsNetworkPolicyPreview
az provider register -n Microsoft.ContainerService
```

#### NOTE

At this time, Azure NPM with Windows nodes is available on Windows Server 2022 only

Now, you should replace the values for `$RESOURCE_GROUP_NAME`, `$CLUSTER_NAME` and `$WINDOWS_USERNAME` variables.

```
$RESOURCE_GROUP_NAME=myResourceGroup-NP
$CLUSTER_NAME=myAKSCluster
$WINDOWS_USERNAME=myWindowsUserName
$LOCATION=canadaeast
```

Create a username to use as administrator credentials for your Windows Server containers on your cluster. The following command prompts you for a username. Set it to `$WINDOWS_USERNAME` (remember that the commands in this article are entered into a BASH shell).

```
echo "Please enter the username to use as administrator credentials for Windows Server containers on your cluster: " && read WINDOWS_USERNAME
```

Use the following command to create a cluster:

```
az aks create \
--resource-group $RESOURCE_GROUP_NAME \
--name $CLUSTER_NAME \
--node-count 1 \
--windows-admin-username $WINDOWS_USERNAME \
--network-plugin azure \
--network-policy azure
```

It takes a few minutes to create the cluster. By default, your cluster is created with only a Linux node pool. If you would like to use Windows node pools, you can add one. For example:

```
az aks nodepool add \
--resource-group $RESOURCE_GROUP_NAME \
--cluster-name $CLUSTER_NAME \
--os-type Windows \
--name npwin \
--node-count 1
```

#### IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

### Create an AKS cluster for Calico network policies

Create the AKS cluster and specify *azure* for the network plugin, and *calico* for the Network Policy. Using *calico* as the Network Policy enables Calico networking on both Linux and Windows node pools.

If you plan on adding Windows node pools to your cluster, include the `windows-admin-username` and `windows-admin-password` parameters with that meet the [Windows Server password requirements](#).

#### IMPORTANT

At this time, using Calico network policies with Windows nodes is available on new clusters using Kubernetes version 1.20 or later with Calico 3.17.2 and requires using Azure CNI networking. Windows nodes on AKS clusters with Calico enabled also have [Direct Server Return \(DSR\)](#) enabled by default.

For clusters with only Linux node pools running Kubernetes 1.20 with earlier versions of Calico, the Calico version will automatically be upgraded to 3.17.2.

Create a username to use as administrator credentials for your Windows Server containers on your cluster. The following command prompts you for a username. Set it to `$WINDOWS_USERNAME` (remember that the commands in this article are entered into a BASH shell).

```
echo "Please enter the username to use as administrator credentials for Windows Server containers on your cluster: " && read WINDOWS_USERNAME
```

```
az aks create \
--resource-group $RESOURCE_GROUP_NAME \
--name $CLUSTER_NAME \
--node-count 1 \
--windows-admin-username $WINDOWS_USERNAME \
--network-plugin azure \
--network-policy calico
```

It takes a few minutes to create the cluster. By default, your cluster is created with only a Linux node pool. If you would like to use Windows node pools, you can add one. For example:

```
az aks nodepool add \
--resource-group $RESOURCE_GROUP_NAME \
--cluster-name $CLUSTER_NAME \
--os-type Windows \
--name npwin \
--node-count 1
```

## Verify Network Policy setup

When the cluster is ready, configure `kubectl` to connect to your Kubernetes cluster by using the [az aks get-credentials](#) command. This command downloads credentials and configures the Kubernetes CLI to use them:

```
az aks get-credentials --resource-group $RESOURCE_GROUP_NAME --name $CLUSTER_NAME
```

To begin verification of Network Policy, we'll create a sample application and set traffic rules.

Firstly, let's create a namespace called *demo* to run the example pods:

```
kubectl create namespace demo
```

We'll now create two pods in the cluster named *client* and *server*.

### NOTE

If you want to schedule the *client* or *server* on a particular node, add the following bit before the `--command` argument in the pod creation `kubectl run` command:

```
--overrides='{"spec": { "nodeSelector": {"kubernetes.io/os": "linux|windows"}}}
```

Create a *server* pod. This pod will serve on TCP port 80:

```
kubectl run server -n demo --image=k8s.gcr.io/e2e-test-images/agnhost:2.33 --labels="app=server" --port=80 --command -- /agnhost serve-hostname --tcp --http=false --port "80"
```

Create a *client* pod. The below command will run bash on the client pod:

```
kubectl run -it client -n demo --image=k8s.gcr.io/e2e-test-images/agnhost:2.33 --command -- bash
```

Now, in a separate window, run the following command to get the server IP:

```
kubectl get pod --output=wide
```

The output should look like:

NAME	READY	STATUS	RESTARTS	AGE	IP	NODE	NOMINATED NODE	READINESS GATES
server	1/1	Running	0	30s	10.224.0.72	akswin22000001	<none>	<none>

### Test Connectivity without Network Policy

In the client's shell, verify connectivity with the server by executing the following command. Replace *server-ip* by IP found in the output from executing previous command. There will be no output if the connection is successful:

```
/agnhost connect <server-ip>:80 --timeout=3s --protocol=tcp
```

### Test Connectivity with Network Policy

Create a file named demo-policy.yaml and paste the following YAML manifest to add network policies:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
 name: demo-policy
 namespace: demo
spec:
 podSelector:
 matchLabels:
 app: server
 ingress:
 - from:
 - podSelector:
 matchLabels:
 app: client
 ports:
 - port: 80
 protocol: TCP
```

Specify the name of your YAML manifest and apply it using [kubectl apply](#):

```
kubectl apply -f demo-policy.yaml
```

Now, in the client's shell, verify connectivity with the server by executing the following `/agnhost` command:

```
/agnhost connect <server-ip>:80 --timeout=3s --protocol=tcp
```

Connectivity with traffic will be blocked since the server is labeled with `app=server`, but the client isn't labeled.

The connect command above will yield this output:

```
TIMEOUT
```

Run the following command to label the *client* and verify connectivity with the server (output should return

nothing).

```
kubectl label pod client -n demo app=client
```

## Clean up resources

In this article, we created a namespace and two pods and applied a Network Policy. To clean up these resources, use the [kubectl delete](#) command and specify the resource name:

```
kubectl delete namespace demo
```

## Next steps

For more about network resources, see [Network concepts for applications in Azure Kubernetes Service \(AKS\)](#).

To learn more about policies, see [Kubernetes network policies](#).

# Preview - Secure your cluster using pod security policies in Azure Kubernetes Service (AKS)

10/27/2022 • 14 minutes to read • [Edit Online](#)

## WARNING

The feature described in this document, pod security policy (preview), will begin deprecation with Kubernetes version 1.21, with its removal in version 1.25. You can now [Migrate Pod Security Policy to Pod Security Admission Controller](#) ahead of the deprecation.

After pod security policy (preview) is deprecated, you must have already migrated to Pod Security Admission controller or disabled the feature on any existing clusters using the deprecated feature to perform future cluster upgrades and stay within Azure support.

To improve the security of your AKS cluster, you can limit what pods can be scheduled. Pods that request resources you don't allow can't run in the AKS cluster. You define this access using pod security policies. This article shows you how to use pod security policies to limit the deployment of pods in AKS.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

You need the Azure CLI version 2.0.61 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

### Install aks-preview CLI extension

To use pod security policies, you need the *aks-preview* CLI extension version 0.4.1 or higher. Install the *aks-preview* Azure CLI extension using the `az extension add` command, then check for any available updates using the `az extension update` command:

```
Install the aks-preview extension
az extension add --name aks-preview

Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

### Register pod security policy feature provider

To create or update an AKS cluster to use pod security policies, first enable a feature flag on your subscription. To

register the *PodSecurityPolicyPreview* feature flag, use the [az feature register](#) command as shown in the following example:

```
az feature register --name PodSecurityPolicyPreview --namespace Microsoft.ContainerService
```

It takes a few minutes for the status to show *Registered*. You can check on the registration status using the [az feature list](#) command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/PodSecurityPolicyPreview')].{Name:name,State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider using the [az provider register](#) command:

```
az provider register --namespace Microsoft.ContainerService
```

## Overview of pod security policies

In a Kubernetes cluster, an admission controller is used to intercept requests to the API server when a resource is to be created. The admission controller can then *validate* the resource request against a set of rules, or *mutate* the resource to change deployment parameters.

*PodSecurityPolicy* is an admission controller that validates a pod specification meets your defined requirements. These requirements may limit the use of privileged containers, access to certain types of storage, or the user or group the container can run as. When you try to deploy a resource where the pod specifications don't meet the requirements outlined in the pod security policy, the request is denied. This ability to control what pods can be scheduled in the AKS cluster prevents some possible security vulnerabilities or privilege escalations.

When you enable pod security policy in an AKS cluster, some default policies are applied. These default policies provide an out-of-the-box experience to define what pods can be scheduled. However, cluster users may run into problems deploying pods until you define your own policies. The recommended approach is to:

- Create an AKS cluster
- Define your own pod security policies
- Enable the pod security policy feature

To show how the default policies limit pod deployments, in this article we first enable the pod security policies feature, then create a custom policy.

### Behavior changes between pod security policy and Azure Policy

Below is a summary of behavior changes between pod security policy and Azure Policy.

SCENARIO	POD SECURITY POLICY	AZURE POLICY
Installation	Enable pod security policy feature	Enable Azure Policy Add-on
Deploy policies	Deploy pod security policy resource	Assign Azure policies to the subscription or resource group scope. The Azure Policy Add-on is required for Kubernetes resource applications.

SCENARIO	POD SECURITY POLICY	AZURE POLICY
Default policies	When pod security policy is enabled in AKS, default Privileged and Unrestricted policies are applied.	No default policies are applied by enabling the Azure Policy Add-on. You must explicitly enable policies in Azure Policy.
Who can create and assign policies	Cluster admin creates a pod security policy resource	Users must have a minimum role of 'owner' or 'Resource Policy Contributor' permissions on the AKS cluster resource group. - Through API, users can assign policies at the AKS cluster resource scope. The user should have minimum of 'owner' or 'Resource Policy Contributor' permissions on AKS cluster resource. - In the Azure portal, policies can be assigned at the Management group/subscription/resource group level.
Authorizing policies	Users and Service Accounts require explicit permissions to use pod security policies.	No additional assignment is required to authorize policies. Once policies are assigned in Azure, all cluster users can use these policies.
Policy applicability	The admin user bypasses the enforcement of pod security policies.	All users (admin & non-admin) sees the same policies. There is no special casing based on users. Policy application can be excluded at the namespace level.
Policy scope	Pod security policies are not namespaced	Constraint templates used by Azure Policy are not namespaced.
Deny/Audit/Mutation action	Pod security policies support only deny actions. Mutation can be done with default values on create requests. Validation can be done during update requests.	Azure Policy supports both audit & deny actions. Mutation is not supported yet, but planned.
Pod security policy compliance	There is no visibility on compliance of pods that existed before enabling pod security policy. Non-compliant pods created after enabling pod security policies are denied.	Non-compliant pods that existed before applying Azure policies would show up in policy violations. Non-compliant pods created after enabling Azure policies are denied if policies are set with a deny effect.
How to view policies on the cluster	<code>kubectl get psp</code>	<code>kubectl get constrainttemplate</code> - All policies are returned.
Pod security policy standard - Privileged	A privileged pod security policy resource is created by default when enabling the feature.	Privileged mode implies no restriction, as a result it is equivalent to not having any Azure Policy assignment.
Pod security policy standard - Baseline/default	User installs a pod security policy baseline resource.	Azure Policy provides a <a href="#">built-in baseline initiative</a> which maps to the baseline pod security policy.

SCENARIO	POD SECURITY POLICY	AZURE POLICY
Pod security policy standard - Restricted	User installs a pod security policy restricted resource.	Azure Policy provides a <a href="#">built-in restricted initiative</a> which maps to the restricted pod security policy.

## Enable pod security policy on an AKS cluster

You can enable or disable pod security policy using the [az aks update](#) command. The following example enables pod security policy on the cluster name *myAKSCluster* in the resource group named *myResourceGroup*.

### NOTE

For real-world use, don't enable the pod security policy until you have defined your own custom policies. In this article, you enable pod security policy as the first step to see how the default policies limit pod deployments.

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--enable-pod-security-policy
```

## Default AKS policies

When you enable pod security policy, AKS creates one default policy named *privileged*. Don't edit or remove the default policy. Instead, create your own policies that define the settings you want to control. Let's first look at what these default policies are and how they impact pod deployments.

To view the policies available, use the [kubectl get psp](#) command, as shown in the following example

```
$ kubectl get psp

NAME PRIV CAPS SELINUX RUNASUSER FSGROUP SUPGROUP READONLYROOTFS VOLUMES
privileged true * RunAsAny RunAsAny RunAsAny RunAsAny false *
configMap,emptyDir,projected,secret,downwardAPI,persistentVolumeClaim
```

The *privileged* pod security policy is applied to any authenticated user in the AKS cluster. This assignment is controlled by ClusterRoles and ClusterRoleBindings. Use the [kubectl get rolebindings](#) command and search for the *default:privileged*:binding in the *kube-system* namespace:

```
kubectl get rolebindings default:privileged -n kube-system -o yaml
```

As shown in the following condensed output, the *psp:privileged* ClusterRole is assigned to any *system:authenticated* users. This ability provides a basic level of privilege without your own policies being defined.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
 [...]
 name: default:privileged
 [...]
roleRef:
 apiGroup: rbac.authorization.k8s.io
 kind: ClusterRole
 name: psp:privileged
subjects:
- apiGroup: rbac.authorization.k8s.io
 kind: Group
 name: system:masters
```

It's important to understand how these default policies interact with user requests to schedule pods before you start to create your own pod security policies. In the next few sections, let's schedule some pods to see these default policies in action.

## Create a test user in an AKS cluster

By default, when you use the [az aks get-credentials](#) command, the *admin* credentials for the AKS cluster are added to your `kubectl` config. The admin user bypasses the enforcement of pod security policies. If you use Azure Active Directory integration for your AKS clusters, you could sign in with the credentials of a non-admin user to see the enforcement of policies in action. In this article, let's create a test user account in the AKS cluster that you can use.

Create a sample namespace named *psp-aks* for test resources using the [kubectl create namespace](#) command. Then, create a service account named *nonadmin-user* using the [kubectl create serviceaccount](#) command:

```
kubectl create namespace psp-aks
kubectl create serviceaccount --namespace psp-aks nonadmin-user
```

Next, create a RoleBinding for the *nonadmin-user* to perform basic actions in the namespace using the [kubectl create rolebinding](#) command:

```
kubectl create rolebinding \
--namespace psp-aks \
psp-aks-editor \
--clusterrole=edit \
--serviceaccount=psp-aks:nonadmin-user
```

### Create alias commands for admin and non-admin user

To highlight the difference between the regular admin user when using `kubectl` and the non-admin user created in the previous steps, create two command-line aliases:

- The `kubectl-admin` alias is for the regular admin user, and is scoped to the *psp-aks* namespace.
- The `kubectl-nonadminuser` alias is for the *nonadmin-user* created in the previous step, and is scoped to the *psp-aks* namespace.

Create these two aliases as shown in the following commands:

```
alias kubectl-admin='kubectl --namespace psp-aks'
alias kubectl-nonadminuser='kubectl --as=system:serviceaccount:psp-aks:nonadmin-user --namespace psp-aks'
```

## Test the creation of a privileged pod

Let's first test what happens when you schedule a pod with the security context of `privileged: true`. This security context escalates the pod's privileges. In the previous section that showed the default AKS pod security policies, the *privilege* policy should deny this request.

Create a file named `nginx-privileged.yaml` and paste the following YAML manifest:

```
apiVersion: v1
kind: Pod
metadata:
 name: nginx-privileged
spec:
 containers:
 - name: nginx-privileged
 image: mcr.microsoft.com/oss/nginx/nginx:1.14.2-alpine
 securityContext:
 privileged: true
```

Create the pod using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl-nonadminuser apply -f nginx-privileged.yaml
```

The pod fails to be scheduled, as shown in the following example output:

```
$ kubectl-nonadminuser apply -f nginx-privileged.yaml

Error from server (Forbidden): error when creating "nginx-privileged.yaml": pods "nginx-privileged" is
forbidden: unable to validate against any pod security policy: []
```

The pod doesn't reach the scheduling stage, so there are no resources to delete before you move on.

## Test creation of an unprivileged pod

In the previous example, the pod specification requested privileged escalation. This request is denied by the default *privilege* pod security policy, so the pod fails to be scheduled. Let's try now running that same NGINX pod without the privilege escalation request.

Create a file named `nginx-unprivileged.yaml` and paste the following YAML manifest:

```
apiVersion: v1
kind: Pod
metadata:
 name: nginx-unprivileged
spec:
 containers:
 - name: nginx-unprivileged
 image: mcr.microsoft.com/oss/nginx/nginx:1.14.2-alpine
```

Create the pod using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl-nonadminuser apply -f nginx-unprivileged.yaml
```

The pod fails to be scheduled, as shown in the following example output:

```
$ kubectl-nonadminuser apply -f nginx-unprivileged.yaml

Error from server (Forbidden): error when creating "nginx-unprivileged.yaml": pods "nginx-unprivileged" is
forbidden: unable to validate against any pod security policy: []
```

The pod doesn't reach the scheduling stage, so there are no resources to delete before you move on.

## Test creation of a pod with a specific user context

In the previous example, the container image automatically tried to use root to bind NGINX to port 80. This request was denied by the default *privilege* pod security policy, so the pod fails to start. Let's try now running that same NGINX pod with a specific user context, such as `runAsUser: 2000`.

Create a file named `nginx-unprivileged-nonroot.yaml` and paste the following YAML manifest:

```
apiVersion: v1
kind: Pod
metadata:
 name: nginx-unprivileged-nonroot
spec:
 containers:
 - name: nginx-unprivileged
 image: mcr.microsoft.com/oss/nginx/nginx:1.14.2-alpine
 securityContext:
 runAsUser: 2000
```

Create the pod using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl-nonadminuser apply -f nginx-unprivileged-nonroot.yaml
```

The pod fails to be scheduled, as shown in the following example output:

```
$ kubectl-nonadminuser apply -f nginx-unprivileged-nonroot.yaml

Error from server (Forbidden): error when creating "nginx-unprivileged-nonroot.yaml": pods "nginx-
unprivileged-nonroot" is forbidden: unable to validate against any pod security policy: []
```

The pod doesn't reach the scheduling stage, so there are no resources to delete before you move on.

## Create a custom pod security policy

Now that you've seen the behavior of the default pod security policies, let's provide a way for the *nonadmin-user* to successfully schedule pods.

Let's create a policy to reject pods that request privileged access. Other options, such as `runAsUser` or allowed `volumes`, aren't explicitly restricted. This type of policy denies a request for privileged access, but otherwise lets the cluster run the requested pods.

Create a file named `psp-deny-privileged.yaml` and paste the following YAML manifest:

```

apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
 name: psp-deny-privileged
spec:
 privileged: false
 seLinux:
 rule: RunAsAny
 supplementalGroups:
 rule: RunAsAny
 runAsUser:
 rule: RunAsAny
 fsGroup:
 rule: RunAsAny
 volumes:
 - '*'

```

Create the policy using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f psp-deny-privileged.yaml
```

To view the policies available, use the [kubectl get psp](#) command, as shown in the following example. Compare the *psp-deny-privileged* policy with the default *privilege* policy that was enforced in the previous examples to create a pod. Only the use of *PRIV* escalation is denied by your policy. There are no restrictions on the user or group for the *psp-deny-privileged* policy.

\$ kubectl get psp							
NAME	PRIV	CAPS	SELINUX	RUNASUSER	FSGROUP	SUPGROUP	READONLYROOTFS
VOLUMES							
privileged	true	*	RunAsAny	RunAsAny	RunAsAny	RunAsAny	false
*							
psp-deny-privileged	false		RunAsAny	RunAsAny	RunAsAny	RunAsAny	false
*							

## Allow user account to use the custom pod security policy

In the previous step, you created a pod security policy to reject pods that request privileged access. To allow the policy to be used, you create a *Role* or a *ClusterRole*. Then, you associate one of these roles using a *RoleBinding* or *ClusterRoleBinding*.

For this example, create a ClusterRole that allows you to *use* the *psp-deny-privileged* policy created in the previous step. Create a file named `psp-deny-privileged-clusterrole.yaml` and paste the following YAML manifest:

```

kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
 name: psp-deny-privileged-clusterrole
rules:
- apiGroups:
 - extensions
 resources:
 - podsecuritypolicies
 resourceNames:
 - psp-deny-privileged
 verbs:
 - use

```

Create the ClusterRole using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f psp-deny-privileged-clusterrole.yaml
```

Now create a ClusterRoleBinding to use the ClusterRole created in the previous step. Create a file named [psp-deny-privileged-clusterrolebinding.yaml](#) and paste the following YAML manifest:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
 name: psp-deny-privileged-clusterrolebinding
roleRef:
 apiGroup: rbac.authorization.k8s.io
 kind: ClusterRole
 name: psp-deny-privileged-clusterrole
subjects:
- apiGroup: rbac.authorization.k8s.io
 kind: Group
 name: system:serviceaccounts
```

Create a ClusterRoleBinding using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f psp-deny-privileged-clusterrolebinding.yaml
```

#### NOTE

In the first step of this article, the pod security policy feature was enabled on the AKS cluster. The recommended practice was to only enable the pod security policy feature after you've defined your own policies. This is the stage where you would enable the pod security policy feature. One or more custom policies have been defined, and user accounts have been associated with those policies. Now you can safely enable the pod security policy feature and minimize problems caused by the default policies.

## Test the creation of an unprivileged pod again

With your custom pod security policy applied and a binding for the user account to use the policy, let's try to create an unprivileged pod again. Use the same [nginx-privileged.yaml](#) manifest to create the pod using the [kubectl apply](#) command:

```
kubectl-nonadminuser apply -f nginx-unprivileged.yaml
```

The pod is successfully scheduled. When you check the status of the pod using the [kubectl get pods](#) command, the pod is *Running*.

```
$ kubectl-nonadminuser get pods
NAME READY STATUS RESTARTS AGE
nginx-unprivileged 1/1 Running 0 7m14s
```

This example shows how you can create custom pod security policies to define access to the AKS cluster for different users or groups. The default AKS policies provide tight controls on what pods can run, so create your own custom policies to then correctly define the restrictions you need.

Delete the NGINX unprivileged pod using the [kubectl delete](#) command and specify the name of your YAML

manifest:

```
kubectl-nonadminuser delete -f nginx-unprivileged.yaml
```

## Clean up resources

To disable pod security policy, use the [az aks update](#) command again. The following example disables pod security policy on the cluster name *myAKSCluster* in the resource group named *myResourceGroup*.

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--disable-pod-security-policy
```

Next, delete the ClusterRole and ClusterRoleBinding:

```
kubectl delete -f psp-deny-privileged-clusterrolebinding.yaml
kubectl delete -f psp-deny-privileged-clusterrole.yaml
```

Delete the security policy using [kubectl delete](#) command and specify the name of your YAML manifest:

```
kubectl delete -f psp-deny-privileged.yaml
```

Finally, delete the *psp-aks* namespace:

```
kubectl delete namespace psp-aks
```

## Next steps

This article showed you how to create a pod security policy to prevent the use of privileged access. There are lots of features that a policy can enforce, such as type of volume or the RunAs user. For more information on the available options, see the [Kubernetes pod security policy reference docs](#).

For more information about limiting pod network traffic, see [Secure traffic between pods using network policies in AKS](#).

# Use Pod Security Admission in Azure Kubernetes Service (AKS)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Pod Security Admission enforces Pod Security Standards policies on pods running in a namespace. Pod Security Admission is enabled by default in AKS and is controlled by adding labels to a namespace. For more information about Pod Security Admission, see [Enforce Pod Security Standards with Namespace Labels](#). For more information about the Pod Security Standards used by Pod Security Admission, see [Pod Security Standards](#).

Pod Security Admission is a built-in policy solution for single cluster implementations. If you are looking for enterprise-grade policy, then [Azure policy](#) is a better choice.

## Before you begin

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI installed](#).
- An existing AKS cluster running Kubernetes version 1.23 or higher.

## Enable Pod Security Admission for a namespace in your cluster

To enable PSA for a namespace in your cluster, set the `pod-security.kubernetes.io/enforce` label with the policy value you want to enforce. For example:

```
kubectl label --overwrite ns NAMESPACE pod-security.kubernetes.io/enforce=restricted
```

The above command enforces the `restricted` policy for the `NAMESPACE` namespace.

You can also enable Pod Security Admission for all your namespaces. For example:

```
kubectl label --overwrite ns --all pod-security.kubernetes.io/warn=baseline
```

The above example will generate a user-facing warning if any pods are deployed to any namespace that does not meet the `baseline` policy.

## Example of enforcing a Pod Security Admission policy with a deployment

Create two namespaces, one with the `restricted` policy and one with the `baseline` policy.

```
kubectl create namespace test-restricted
kubectl create namespace test-privileged
kubectl label --overwrite ns test-restricted pod-security.kubernetes.io/enforce=restricted pod-security.kubernetes.io/warn=restricted
kubectl label --overwrite ns test-privileged pod-security.kubernetes.io/enforce=privileged pod-security.kubernetes.io/warn=privileged
```

Both the `test-restricted` and `test-privileged` namespaces will block running pods as well as generate a user-facing warning if any pods attempt to run that do not meet the configured policy.

Attempt to deploy pods to the `test-restricted` namespace.

```
kubectl apply --namespace test-restricted -f https://raw.githubusercontent.com/Azure-Samples/azure-voting-app-redis/master/azure-vote-all-in-one-redis.yaml
```

Notice you get a warning that the pods violate the configured policy.

```
...
Warning: would violate PodSecurity "restricted:latest": allowPrivilegeEscalation != false (container "azure-vote-back" must set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "azure-vote-back" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "azure-vote-back" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "azure-vote-back" must set securityContext.seccompProfile.type to "RuntimeDefault" or "Localhost")
deployment.apps/azure-vote-back created
service/azure-vote-back created
Warning: would violate PodSecurity "restricted:latest": allowPrivilegeEscalation != false (container "azure-vote-front" must set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "azure-vote-front" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "azure-vote-front" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "azure-vote-front" must set securityContext.seccompProfile.type to "RuntimeDefault" or "Localhost")
deployment.apps/azure-vote-front created
service/azure-vote-front created
```

Confirm there are no pods running in the `test-restricted` namespace.

```
kubectl get pods --namespace test-restricted
```

```
$ kubectl get pods --namespace test-restricted
No resources found in test-restricted namespace.
```

Attempt to deploy pods to the `test-privileged` namespace.

```
kubectl apply --namespace test-privileged -f https://raw.githubusercontent.com/Azure-Samples/azure-voting-app-redis/master/azure-vote-all-in-one-redis.yaml
```

Notice there are no warnings about pods not meeting the configured policy.

Confirm you have pods running in the `test-privileged` namespace.

```
kubectl get pods --namespace test-privileged
```

```
$ kubectl get pods --namespace test-privileged
NAME READY STATUS RESTARTS AGE
azure-vote-back-6fcdc5cbd5-svbd5 1/1 Running 0 2m29s
azure-vote-front-5f4b8d498-tqzwv 1/1 Running 0 2m28s
```

Delete both the `test-restricted` and `test-privileged` namespaces.

```
kubectl delete namespace test-restricted test-privileged
```

## Next steps

In this article, you learned how to enable Pod Security Admission an AKS cluster. For more information about

Pod Security Admission, see [Enforce Pod Security Standards with Namespace Labels](#). For more information about the Pod Security Standards used by Pod Security Admission, see [Pod Security Standards](#).

# Use the Azure Key Vault Provider for Secrets Store CSI Driver in an AKS cluster

10/27/2022 • 10 minutes to read • [Edit Online](#)

The Azure Key Vault Provider for Secrets Store CSI Driver allows for the integration of an Azure key vault as a secret store with an Azure Kubernetes Service (AKS) cluster via a [CSI volume](#).

## Limitations

- A container using subPath volume mount will not receive secret updates when it is rotated. See [See](#)

## Prerequisites

- If you don't have an Azure subscription, create a [free account](#) before you begin.
- Before you start, ensure that your version of the Azure CLI is 2.30.0 or later. If it's an earlier version, [install the latest version](#).
- If restricting Ingress to the cluster, ensure Ports 9808 and 8095 are open.

## Supported Kubernetes versions

The minimum recommended Kubernetes version is based on the [rolling Kubernetes version support window](#). Ensure that you're running version N-2 or later.

## Features

- Mounts secrets, keys, and certificates to a pod by using a CSI volume
- Supports CSI inline volumes
- Supports mounting multiple secrets store objects as a single volume
- Supports pod portability with the [SecretProviderClass](#) CRD
- Supports Windows containers
- Syncs with Kubernetes secrets
- Supports auto rotation of mounted contents and synced Kubernetes secrets

## Create an AKS cluster with Azure Key Vault Provider for Secrets Store CSI Driver support

First, create an Azure resource group:

```
az group create -n myResourceGroup -l eastus2
```

To create an AKS cluster with Azure Key Vault Provider for Secrets Store CSI Driver capability, use the [az aks create](#) command with the [azure-keyvault-secrets-provider](#) add-on.

```
az aks create -n myAKScluster -g myResourceGroup --enable-addons azure-keyvault-secrets-provider --enable-managed-identity
```

A user-assigned managed identity, named [azurekeyvaultsecretsprovider-\\*](#), is created by the add-on for the purpose of accessing Azure resources. The following example uses this identity to connect to the Azure key vault

where the secrets will be stored, but you can also use other [identity access methods](#). Take note of the identity's `clientId` in the output:

```
....
"addonProfiles": {
 "azureKeyvaultSecretsProvider": {
 ...
 "identity": {
 "clientId": "<client-id>",
 ...
 }
 }
}
```

## Upgrade an existing AKS cluster with Azure Key Vault Provider for Secrets Store CSI Driver support

To upgrade an existing AKS cluster with Azure Key Vault Provider for Secrets Store CSI Driver capability, use the `az aks enable-addons` command with the `azure-keyvault-secrets-provider` add-on:

```
az aks enable-addons --addons azure-keyvault-secrets-provider --name myAKSCluster --resource-group
myResourceGroup
```

As mentioned in the preceding section, the add-on creates a user-assigned managed identity that you can use to authenticate to your Azure key vault.

## Verify the Azure Key Vault Provider for Secrets Store CSI Driver installation

The preceding command installs the Secrets Store CSI Driver and the Azure Key Vault Provider on your nodes. Verify that the installation is finished by listing all pods that have the `secrets-store-csi-driver` and `secrets-store-provider-azure` labels in the kube-system namespace, and ensure that your output looks similar to the output shown here:

```
kubectl get pods -n kube-system -l 'app in (secrets-store-csi-driver, secrets-store-provider-azure)'

NAME READY STATUS RESTARTS AGE
aks-secrets-store-csi-driver-4vpkj 3/3 Running 2 4m25s
aks-secrets-store-csi-driver-ctjq6 3/3 Running 2 4m21s
aks-secrets-store-csi-driver-tlvlq 3/3 Running 2 4m24s
aks-secrets-store-provider-azure-5p4nb 1/1 Running 0 4m21s
aks-secrets-store-provider-azure-6pqmv 1/1 Running 0 4m24s
aks-secrets-store-provider-azure-f5qlm 1/1 Running 0 4m25s
```

Be sure that a Secrets Store CSI Driver pod and a Secrets Store Provider Azure pod are running on each node in your cluster's node pools.

## Create or use an existing Azure key vault

In addition to an AKS cluster, you'll need an Azure key vault resource that stores the secret content. Keep in mind that the key vault's name must be globally unique.

```
az keyvault create -n <keyvault-name> -g myResourceGroup -l eastus2
```

Your Azure key vault can store keys, secrets, and certificates. In this example, you'll set a plain-text secret called

```
ExampleSecret :
```

```
az keyvault secret set --vault-name <keyvault-name> -n ExampleSecret --value MyAKSEExampleSecret
```

Take note of the following properties for use in the next section:

- The name of the secret object in the key vault
- The object type (secret, key, or certificate)
- The name of your Azure key vault resource
- The Azure tenant ID that the subscription belongs to

## Provide an identity to access the Azure key vault

The Secrets Store CSI Driver allows for the following methods to access an Azure key vault:

- An [Azure Active Directory pod identity](#) (preview)
- An [Azure Active Directory workload identity](#) (preview)
- A user-assigned or system-assigned managed identity

Follow the instructions in [Provide an identity to access the Azure Key Vault Provider for Secrets Store CSI Driver](#) for your chosen method.

### NOTE

The rest of the examples on this page require that you've followed the instructions in [Provide an identity to access the Azure Key Vault Provider for Secrets Store CSI Driver](#), chosen one of the identity methods, and configured a SecretProviderClass. Come back to this page after completed those steps.

## Validate the secrets

After the pod starts, the mounted content at the volume path that you specified in your deployment YAML is available.

```
show secrets held in secrets-store
kubectl exec busybox-secrets-store-inline -- ls /mnt/secrets-store/
print a test secret 'ExampleSecret' held in secrets-store
kubectl exec busybox-secrets-store-inline -- cat /mnt/secrets-store/ExampleSecret
```

## Obtain certificates and keys

The Azure Key Vault design makes sharp distinctions between keys, secrets, and certificates. The Key Vault service's certificates features were designed to make use of its key and secret capabilities. When a key vault certificate is created, an addressable key and secret are also created with the same name. The key allows key operations, and the secret allows the retrieval of the certificate value as a secret.

A key vault certificate also contains public x509 certificate metadata. The key vault stores both the public and private components of your certificate in a secret. You can obtain each individual component by specifying the `objectType` in `SecretProviderClass`. The following table shows which objects map to the various resources associated with your certificate:

OBJECT	RETURN VALUE	RETURNS ENTIRE CERTIFICATE CHAIN
key	The public key, in Privacy Enhanced Mail (PEM) format	N/A
cert	The certificate, in PEM format	No
secret	The private key and certificate, in PEM format	Yes

## Disable the Azure Key Vault Provider for Secrets Store CSI Driver on an existing AKS cluster

### NOTE

Before you disable the add-on, ensure that no `SecretProviderClass` is in use. Trying to disable the add-on while `SecretProviderClass` exists will result in an error.

To disable the Azure Key Vault Provider for Secrets Store CSI Driver capability in an existing cluster, use the `az aks disable-addons` command with the `azure-keyvault-secrets-provider` flag:

```
az aks disable-addons --addons azure-keyvault-secrets-provider -g myResourceGroup -n myAKSCluster
```

### NOTE

If the add-on is disabled, existing workloads will have no issues and will not see any updates in the mounted secrets. If the pod restarts or a new pod is created as part of scale-up event, the pod will fail to start because the driver is no longer running.

## Additional configuration options

### Enable and disable autorotation

### NOTE

When the Azure Key Vault Provider for Secrets Store CSI Driver is enabled, it updates the pod mount and the Kubernetes secret that's defined in the `secretObjects` field of `SecretProviderClass`. It does so by polling for changes periodically, based on the rotation poll interval you've defined. The default rotation poll interval is 2 minutes.

#### NOTE

When a secret is updated in an external secrets store after initial pod deployment, the Kubernetes Secret and the pod mount will be periodically updated depending on how the application consumes the secret data.

**Mount the Kubernetes Secret as a volume:** Use the auto rotation and Sync K8s secrets features of Secrets Store CSI Driver. The application will need to watch for changes from the mounted Kubernetes Secret volume. When the Kubernetes Secret is updated by the CSI Driver, the corresponding volume contents are automatically updated.

**Application reads the data from the container's filesystem:** Use the rotation feature of Secrets Store CSI Driver. The application will need to watch for the file change from the volume mounted by the CSI driver.

**Use the Kubernetes Secret for an environment variable:** Restart the pod to get the latest secret as an environment variable. Use a tool such as [Reloader](#) to watch for changes on the synced Kubernetes Secret and perform rolling upgrades on pods.

To enable autorotation of secrets, use the `enable-secret-rotation` flag when you create your cluster:

```
az aks create -n myAKSCluster2 -g myResourceGroup --enable-addons azure-keyvault-secrets-provider --enable-secret-rotation
```

Or update an existing cluster with the add-on enabled:

```
az aks addon update -g myResourceGroup -n myAKSCluster2 -a azure-keyvault-secrets-provider --enable-secret-rotation
```

To specify a custom rotation interval, use the `rotation-poll-interval` flag:

```
az aks addon update -g myResourceGroup -n myAKSCluster2 -a azure-keyvault-secrets-provider --enable-secret-rotation --rotation-poll-interval 5m
```

To disable autorotation, first disable the addon. Then, re-enable the addon without the `enable-secret-rotation` flag.

#### Sync mounted content with a Kubernetes secret

You might sometimes want to create a Kubernetes secret to mirror the mounted content.

When you create a `SecretProviderClass`, use the `secretObjects` field to define the desired state of the Kubernetes secret, as shown in the following example.

#### NOTE

The YAML examples here are incomplete. You'll need to modify them to support your chosen method of access to your key vault identity. For details, see [Provide an identity to access the Azure Key Vault Provider for Secrets Store CSI Driver](#).

The secrets will sync only after you start a pod to mount them. To rely solely on syncing with the Kubernetes secrets feature doesn't work. When all the pods that consume the secret are deleted, the Kubernetes secret is also deleted.

```

apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: azure-sync
spec:
 provider: azure
 secretObjects: # [OPTIONAL] SecretObjects defines the desired state of synced
 Kubernetes secret objects
 - data:
 - key: username # data field to populate
 objectName: foo1 # name of the mounted content to sync; this could be the
 # name or the object alias
 secretName: foosecret # name of the Kubernetes secret object
 type: Opaque # type of Kubernetes secret object (for example, Opaque,
 kubernetes.io/tls)

```

#### NOTE

Make sure that the `objectName` in the `secretObjects` field matches the file name of the mounted content. If you use `objectAlias` instead, it should match the object alias.

#### Set an environment variable to reference Kubernetes secrets

After you've created the Kubernetes secret, you can reference it by setting an environment variable in your pod, as shown in the following example code:

#### NOTE

The example here demonstrates access to a secret through env variables and through volume/volumeMount. This is for illustrative purposes; a typical application would use one method or the other. However, be aware that in order for a secret to be available through env variables, it first must be mounted by at least one pod.

```

kind: Pod
apiVersion: v1
metadata:
 name: busybox-secrets-store-inline
spec:
 containers:
 - name: busybox
 image: k8s.gcr.io/e2e-test-images/busybox:1.29-1
 command:
 - "/bin/sleep"
 - "10000"
 volumeMounts:
 - name: secrets-store01-inline
 mountPath: "/mnt/secrets-store"
 readOnly: true
 env:
 - name: SECRET_USERNAME
 valueFrom:
 secretKeyRef:
 name: foosecret
 key: username
 volumes:
 - name: secrets-store01-inline
 csi:
 driver: secrets-store.csi.k8s.io
 readOnly: true
 volumeAttributes:
 secretProviderClass: "azure-sync"

```

# Metrics

## The Azure Key Vault Provider

Metrics are served via Prometheus from port 8898, but this port isn't exposed outside the pod by default.

Access the metrics over localhost by using `kubectl port-forward`:

```
kubectl port-forward -n kube-system ds/aks-secrets-store-provider-azure 8898:8898 &
curl localhost:8898/metrics
```

The following table lists the metrics that are provided by the Azure Key Vault Provider for Secrets Store CSI Driver:

METRIC	DESCRIPTION	TAGS
keyvault_request	The distribution of how long it took to get from the key vault	<code>os_type=&lt;runtime os&gt;, provider=azure, object_name=&lt;keyvault object name&gt;</code> <code>,</code> <code>object_type=&lt;keyvault object type&gt;</code> <code>, error=&lt;error if failed&gt;</code>
grpc_request	The distribution of how long it took for the gRPC requests	<code>os_type=&lt;runtime os&gt;, provider=azure, grpc_method=&lt;rpc full method&gt;, grpc_code=&lt;grpc status code&gt;, grpc_message=&lt;grpc status message&gt;</code>

## The Secrets Store CSI Driver

Metrics are served from port 8095, but this port is not exposed outside the pod by default. Access the metrics over localhost by using `kubectl port-forward`:

```
kubectl port-forward -n kube-system ds/aks-secrets-store-csi-driver 8095:8095 &
curl localhost:8095/metrics
```

The following table lists the metrics provided by the Secrets Store CSI Driver:

METRIC	DESCRIPTION	TAGS
total_node_publish	The total number of successful volume mount requests	<code>os_type=&lt;runtime os&gt;, provider=&lt;provider name&gt;</code>
total_node_unpublish	The total number of successful volume unmount requests	<code>os_type=&lt;runtime os&gt;</code>
total_node_publish_error	The total number of errors with volume mount requests	<code>os_type=&lt;runtime os&gt;, provider=&lt;provider name&gt;, error_type=&lt;error code&gt;</code>
total_node_unpublish_error	The total number of errors with volume unmount requests	<code>os_type=&lt;runtime os&gt;</code>

METRIC	DESCRIPTION	TAGS
total_sync_k8s_secret	The total number of Kubernetes secrets synced	<code>os_type=&lt;runtime os&gt;</code> , <code>provider=&lt;provider name&gt;</code>
sync_k8s_secret_duration_sec	The distribution of how long it took to sync the Kubernetes secret	<code>os_type=&lt;runtime os&gt;</code>
total_rotation_reconcile	The total number of rotation reconciles	<code>os_type=&lt;runtime os&gt;</code> , <code>rotated=&lt;true or false&gt;</code>
total_rotation_reconcile_error	The total number of rotation reconciles with error	<code>os_type=&lt;runtime os&gt;</code> , <code>rotated=&lt;true or false&gt;</code> , <code>error_type=&lt;error code&gt;</code>
total_rotation_reconcile_error	The distribution of how long it took to rotate secrets-store content for pods	<code>os_type=&lt;runtime os&gt;</code>

## Next steps

Now that you've learned how to use the Azure Key Vault Provider for Secrets Store CSI Driver with an AKS cluster, see [Enable CSI drivers for Azure Disks and Azure Files on AKS](#).

# Provide an identity to access the Azure Key Vault Provider for Secrets Store CSI Driver

10/27/2022 • 10 minutes to read • [Edit Online](#)

The Secrets Store CSI Driver on Azure Kubernetes Service (AKS) provides a variety of methods of identity-based access to your Azure key vault. This article outlines these methods and how to use them to access your key vault and its contents from your AKS cluster. For more information, see [Use the Secrets Store CSI Driver](#).

## Use Azure AD workload identity (preview)

An [Azure AD workload identity](#) is an identity used by an application running on a pod that can authenticate itself against other Azure services that support it, such as Storage or SQL. It integrates with the capabilities native to Kubernetes to federate with external identity providers. In this security model, the AKS cluster acts as token issuer where Azure Active Directory uses OpenID Connect to discover public signing keys and verify the authenticity of the service account token before exchanging it for an Azure AD token. Your workload can exchange a service account token projected to its volume for an Azure AD token using the Azure Identity client library using the Azure SDK or the Microsoft Authentication Library (MSAL).

### NOTE

This authentication method replaces pod-managed identity (preview).

### Prerequisites

- Installed the latest version of the `aks-preview` extension, version 0.5.102 or later. To learn more, see [How to install extensions](#).
- Existing KeyVault
- Existing Azure Subscription with `EnableWorkloadIdentityPreview` feature enabled
- Existing AKS cluster with `enable-oidc-issuer` and `enable-workload-identity` enabled

Azure AD workload identity (preview) is supported on both Windows and Linux clusters.

### Configure workload identity

1. Use the Azure CLI `az account set` command to set a specific subscription to be the current active subscription. Then use the `az identity create` command to create a managed identity.

```
export subscriptionID=<subscription id>
export resourceGroupName=<resource group name>
export UAMI=<name for user assigned identity>
export KEYVAULT_NAME=<existing keyvault name>
export clusterName=<aks cluster name>

az account set --subscription $subscriptionID
az identity create --name $UAMI --resource-group $resourceGroupName
export USER_ASSIGNED_CLIENT_ID="$(az identity show -g $resourceGroupName --name $UAMI --query
'clientId' -o tsv)"
export IDENTITY_TENANT=$(az aks show --name $clusterName --resource-group $resourceGroupName --query
aadProfile.tenantId -o tsv)
```

2. You need to set an access policy that grants the workload identity permission to access the Key Vault secrets, access keys, and certificates. The rights are assigned using the `az keyvault set-policy` command

shown below.

```
az keyvault set-policy -n $KEYVAULT_NAME --key-permissions get --spn $USER_ASSIGNED_CLIENT_ID
az keyvault set-policy -n $KEYVAULT_NAME --secret-permissions get --spn $USER_ASSIGNED_CLIENT_ID
az keyvault set-policy -n $KEYVAULT_NAME --certificate-permissions get --spn $USER_ASSIGNED_CLIENT_ID
```

- Run the `az aks show` command to get the AKS cluster OIDC issuer URL.

```
export AKS_OIDC_ISSUER=$(az aks show --resource-group $resourceGroupName --name $clusterName --query
"oidcIssuerProfile.issuerUrl" -o tsv)
echo $AKS_OIDC_ISSUER
```

**NOTE**

If the URL is empty, verify you have installed the latest version of the `aks-preview` extension, version 0.5.102 or later. Also verify you've [enabled the OIDC issuer](#) (preview).

- Establish a federated identity credential between the Azure AD application and the service account issuer and subject. Get the object ID of the Azure AD application. Update the values for `serviceAccountName` and `serviceAccountNamespace` with the Kubernetes service account name and its namespace.

```
export serviceAccountName="workload-identity-sa" # sample name; can be changed
export serviceAccountNamespace="default" # can be changed to namespace of your workload

cat <<EOF | kubectl apply -f -
apiVersion: v1
kind: ServiceAccount
metadata:
 annotations:
 azure.workload.identity/client-id: ${USER_ASSIGNED_CLIENT_ID}
 labels:
 azure.workload.identity/use: "true"
 name: ${serviceAccountName}
 namespace: ${serviceAccountNamespace}
EOF
```

Next, use the `az identity federated-credential create` command to create the federated identity credential between the Managed Identity, the service account issuer, and the subject.

```
export federatedIdentityName="aksfederatedidentity" # can be changed as needed
az identity federated-credential create --name $federatedIdentityName --identity-name $UAMI --
resource-group $resourceGroupName --issuer ${AKS_OIDC_ISSUER} --subject
system:serviceaccount:${serviceAccountNamespace}:${serviceAccountName}
```

- Deploy a `SecretProviderClass` by using the following YAML script, noticing that the variables will be interpolated:

```

cat <<EOF | kubectl apply -f -
This is a SecretProviderClass example using workload identity to access your key vault
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: azure-kvname-workload-identity # needs to be unique per namespace
spec:
 provider: azure
 parameters:
 usePodIdentity: "false"
 useVMManagedIdentity: "false"
 clientId: "${USER_ASSIGNED_CLIENT_ID}" # Setting this to use workload identity
 keyvaultName: ${KEYVAULT_NAME} # Set to the name of your key vault
 cloudName: "" # [OPTIONAL for Azure] if not provided, the Azure
environment defaults to AzurePublicCloud
 objects: |
 array:
 - |
 objectName: secret1
 objectType: secret # object types: secret, key, or cert
 objectVersion: "" # [OPTIONAL] object versions, default to latest if empty
 - |
 objectName: key1
 objectType: key
 objectVersion: ""
 tenantId: "${IDENTITY_TENANT}" # The tenant ID of the key vault
EOF

```

## 6. Deploy a sample pod. Notice the service account reference in the pod definition:

```

cat <<EOF | kubectl -n $serviceAccountNamespace -f -
This is a sample pod definition for using SecretProviderClass and the user-assigned identity to
access your key vault
kind: Pod
apiVersion: v1
metadata:
 name: busybox-secrets-store-inline-user-msi
spec:
 serviceAccountName: ${serviceAccountName}
 containers:
 - name: busybox
 image: k8s.gcr.io/e2e-test-images/busybox:1.29-1
 command:
 - "/bin/sleep"
 - "10000"
 volumeMounts:
 - name: secrets-store01-inline
 mountPath: "/mnt/secrets-store"
 readOnly: true
 volumes:
 - name: secrets-store01-inline
 csi:
 driver: secrets-store.csi.k8s.io
 readOnly: true
 volumeAttributes:
 secretProviderClass: "azure-kvname-workload-identity"
EOF

```

## Use pod-managed identities

Azure Active Directory (Azure AD) pod-managed identities (preview) use AKS primitives to associate managed identities for Azure resources and identities in Azure AD with pods. You can use these identities to grant access to the Azure Key Vault Secrets Provider for Secrets Store CSI driver.

## Prerequisites

- Ensure that the [Azure AD pod identity add-on](#) has been enabled on your cluster.
- You must be using a Linux-based cluster.

## Use an Azure AD pod-managed identity

1. Follow the instructions in [Use Azure Active Directory pod-managed identities in Azure Kubernetes Service \(Preview\)](#) to create a cluster identity, assign it permissions, and create a pod identity. Take note of the newly created identity's `clientId` and `name`.
2. Assign permissions to the new identity to enable it to read your key vault and view its contents by running the following commands:

```
set policy to access keys in your key vault
az keyvault set-policy -n <keyvault-name> --key-permissions get --spn <pod-identity-client-id>
set policy to access secrets in your key vault
az keyvault set-policy -n <keyvault-name> --secret-permissions get --spn <pod-identity-client-id>
set policy to access certs in your key vault
az keyvault set-policy -n <keyvault-name> --certificate-permissions get --spn <pod-identity-client-id>
```

3. Create a `SecretProviderClass` by using the following YAML, using your own values for `aadpodidbinding`, `tenantId`, and the objects to retrieve from your key vault:

```
This is a SecretProviderClass example using aad-pod-identity to access the key vault
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: azure-kvname-podid
spec:
 provider: azure
 parameters:
 usePodIdentity: "true" # Set to true for using aad-pod-identity to access your key
 vault
 keyvaultName: <key-vault-name> # Set to the name of your key vault
 cloudName: "" # [OPTIONAL for Azure] if not provided, the Azure
 environment defaults to AzurePublicCloud
 objects: |
 array:
 - |
 objectName: secret1
 objectType: secret # object types: secret, key, or cert
 objectVersion: "" # [OPTIONAL] object versions, default to latest if empty
 - |
 objectName: key1
 objectType: key
 objectVersion: ""
 tenantId: <tenant-Id> # The tenant ID of the key vault
```

4. Apply the `SecretProviderClass` to your cluster:

```
kubectl apply -f secretproviderclass.yaml
```

5. Create a pod by using the following YAML, using the name of your identity:

```

This is a sample pod definition for using SecretProviderClass and aad-pod-identity to access the
key vault
kind: Pod
apiVersion: v1
metadata:
 name: busybox-secrets-store-inline-podid
 labels:
 aadpodidbinding: <name> # Set the label value to the name of your pod identity
spec:
 containers:
 - name: busybox
 image: k8s.gcr.io/e2e-test-images/busybox:1.29-1
 command:
 - "/bin/sleep"
 - "10000"
 volumeMounts:
 - name: secrets-store01-inline
 mountPath: "/mnt/secrets-store"
 readOnly: true
 volumes:
 - name: secrets-store01-inline
 csi:
 driver: secrets-store.csi.k8s.io
 readOnly: true
 volumeAttributes:
 secretProviderClass: "azure-kvname-podid"

```

## 6. Apply the pod to your cluster:

```
kubectl apply -f pod.yaml
```

## Use a user-assigned managed identity

- To access your key vault, you can use the user-assigned managed identity that you created when you [enabled a managed identity on your AKS cluster](#):

```
az aks show -g <resource-group> -n <cluster-name> --query
addonProfiles.azureKeyvaultSecretsProvider.identity.clientId -o tsv
```

Alternatively, you can create a new managed identity and assign it to your virtual machine (VM) scale set or to each VM instance in your availability set:

```
az identity create -g <resource-group> -n <identity-name>
az vmss identity assign -g <resource-group> -n <agent-pool-vmss> --identities <identity-resource-id>
az vm identity assign -g <resource-group> -n <agent-pool-vm> --identities <identity-resource-id>
```

- To grant your identity permissions that enable it to read your key vault and view its contents, run the following commands:

```
set policy to access keys in your key vault
az keyvault set-policy -n <keyvault-name> --key-permissions get --spn <identity-client-id>
set policy to access secrets in your key vault
az keyvault set-policy -n <keyvault-name> --secret-permissions get --spn <identity-client-id>
set policy to access certs in your key vault
az keyvault set-policy -n <keyvault-name> --certificate-permissions get --spn <identity-client-id>
```

- Create a `SecretProviderClass` by using the following YAML, using your own values for

`userAssignedIdentityID`, `keyvaultName`, `tenantId`, and the objects to retrieve from your key vault:

```
This is a SecretProviderClass example using user-assigned identity to access your key vault
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: azure-kvname-user-msi
spec:
 provider: azure
 parameters:
 usePodIdentity: "false"
 useVMManagedIdentity: "true" # Set to true for using managed identity
 userAssignedIdentityID: <client-id> # Set the clientID of the user-assigned managed identity to
use
 keyvaultName: <key-vault-name> # Set to the name of your key vault
 cloudName: "" # [OPTIONAL for Azure] if not provided, the Azure
environment defaults to AzurePublicCloud
 objects: |
 array:
 - |
 objectName: secret1
 objectType: secret # object types: secret, key, or cert
 objectVersion: "" # [OPTIONAL] object versions, default to latest if empty
 - |
 objectName: key1
 objectType: key
 objectVersion: ""
 tenantId: <tenant-id> # The tenant ID of the key vault
```

4. Apply the `SecretProviderClass` to your cluster:

```
kubectl apply -f secretproviderclass.yaml
```

5. Create a pod by using the following YAML:

```
This is a sample pod definition for using SecretProviderClass and the user-assigned identity to
access your key vault
kind: Pod
apiVersion: v1
metadata:
 name: busybox-secrets-store-inline-user-msi
spec:
 containers:
 - name: busybox
 image: k8s.gcr.io/e2e-test-images/busybox:1.29-1
 command:
 - "/bin/sleep"
 - "10000"
 volumeMounts:
 - name: secrets-store01-inline
 mountPath: "/mnt/secrets-store"
 readOnly: true
 volumes:
 - name: secrets-store01-inline
 csi:
 driver: secrets-store.csi.k8s.io
 readOnly: true
 volumeAttributes:
 secretProviderClass: "azure-kvname-user-msi"
```

6. Apply the pod to your cluster:

```
kubectl apply -f pod.yaml
```

## Use a system-assigned managed identity

### Prerequisites

#### IMPORTANT

Before you begin this step, [enable system-assigned managed identity](#) on your AKS cluster's VMs or scale sets.

### Usage

1. Verify that your Virtual Machine Scale Set or Availability Set nodes have their own system-assigned identity:

```
az vmss identity show -g <resource group> -n <vmss scalset name> -o yaml
az vm identity show -g <resource group> -n <vm name> -o yaml
```

#### NOTE

The output should contain `type: SystemAssigned`. Make a note of the `principalId`.

IMDS is looking for a System Assigned Identity on VMSS first, then it will look for a User Assigned Identity and pull that if there is only 1. If there are multiple User Assigned Identities IMDS will throw an error as it does not know which identity to pull.

2. To grant your identity permissions that enable it to read your key vault and view its contents, run the following commands:

```
set policy to access keys in your key vault
az keyvault set-policy -n <keyvault-name> --key-permissions get --spn <identity-principal-id>
set policy to access secrets in your key vault
az keyvault set-policy -n <keyvault-name> --secret-permissions get --spn <identity-principal-id>
set policy to access certs in your key vault
az keyvault set-policy -n <keyvault-name> --certificate-permissions get --spn <identity-principal-id>
```

3. Create a `SecretProviderClass` by using the following YAML, using your own values for `keyvaultName`, `tenantId`, and the objects to retrieve from your key vault:

```

This is a SecretProviderClass example using system-assigned identity to access your key vault
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: azure-kvname-system-msi
spec:
 provider: azure
 parameters:
 usePodIdentity: "false"
 useVMManagedIdentity: "true" # Set to true for using managed identity
 userAssignedIdentityID: "" # If empty, then defaults to use the system assigned identity on
 # the VM
 keyvaultName: <key-vault-name>
 cloudName: "" # [OPTIONAL for Azure] if not provided, the Azure environment
 # defaults to AzurePublicCloud
 objects: |
 array:
 - |
 objectName: secret1
 objectType: secret # object types: secret, key, or cert
 objectVersion: "" # [OPTIONAL] object versions, default to latest if empty
 - |
 objectName: key1
 objectType: key
 objectVersion: ""
 tenantId: <tenant-id> # The tenant ID of the key vault

```

4. Apply the `SecretProviderClass` to your cluster:

```
kubectl apply -f secretproviderclass.yaml
```

5. Create a pod by using the following YAML:

```

This is a sample pod definition for using SecretProviderClass and system-assigned identity to
access your key vault
kind: Pod
apiVersion: v1
metadata:
 name: busybox-secrets-store-inline-system-msi
spec:
 containers:
 - name: busybox
 image: k8s.gcr.io/e2e-test-images/busybox:1.29-1
 command:
 - "/bin/sleep"
 - "10000"
 volumeMounts:
 - name: secrets-store01-inline
 mountPath: "/mnt/secrets-store"
 readOnly: true
 volumes:
 - name: secrets-store01-inline
 csi:
 driver: secrets-store.csi.k8s.io
 readOnly: true
 volumeAttributes:
 secretProviderClass: "azure-kvname-system-msi"

```

## Next steps

To validate that the secrets are mounted at the volume path that's specified in your pod's YAML, see [Use the](#)

Azure Key Vault Provider for Secrets Store CSI Driver in an AKS cluster.

# Set up Secrets Store CSI Driver to enable NGINX Ingress Controller with TLS

10/27/2022 • 7 minutes to read • [Edit Online](#)

This article walks you through the process of securing an NGINX Ingress Controller with TLS with an Azure Kubernetes Service (AKS) cluster and an Azure Key Vault (AKV) instance. For more information, see [TLS in Kubernetes](#).

Importing the ingress TLS certificate to the cluster can be accomplished using one of two methods:

- **Application** - The application deployment manifest declares and mounts the provider volume. Only when the application is deployed, is the certificate made available in the cluster, and when the application is removed the secret is removed as well. This scenario fits development teams who are responsible for the application's security infrastructure and their integration with the cluster.
- **Ingress Controller** - The ingress deployment is modified to declare and mount the provider volume. The secret is imported when ingress pods are created. The application's pods have no access to the TLS certificate. This scenario fits scenarios where one team (for example, IT) manages and creates infrastructure and networking components (including HTTPS TLS certificates) and other teams manage application lifecycle. In this case, ingress is specific to a single namespace/workload and is deployed in the same namespace as the application.

## Prerequisites

- If you don't have an Azure subscription, create a [free account](#) before you begin.
- Before you start, ensure your Azure CLI version is >= `2.30.0`, or [install the latest version](#).
- An AKS cluster with the Secrets Store CSI Driver configured.
- An Azure Key Vault instance.

## Generate a TLS certificate

```
export CERT_NAME=aks-ingress-cert
openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
 -out aks-ingress-tls.crt \
 -keyout aks-ingress-tls.key \
 -subj "/CN=demo.azure.com/O=aks-ingress-tls"
```

## Import the certificate to AKV

```
export AKV_NAME="[YOUR AKV NAME]"
openssl pkcs12 -export -in aks-ingress-tls.crt -inkey aks-ingress-tls.key -out $CERT_NAME.pfx
skip Password prompt
```

```
az keyvault certificate import --vault-name $AKV_NAME -n $CERT_NAME -f $CERT_NAME.pfx
```

## Deploy a SecretProviderClass

First, create a new namespace:

```
export NAMESPACE=ingress-basic
```

```
kubectl create namespace $NAMESPACE
```

Select a [method to provide an access identity](#) and configure your SecretProviderClass YAML accordingly.

Additionally:

- Be sure to use `objectType=secret`, which is the only way to obtain the private key and the certificate from AKV.
- Set `kubernetes.io/tls` as the `type` in your `secretObjects` section.

See the following example of what your SecretProviderClass might look like:

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
 name: azure-tls
spec:
 provider: azure
 secretObjects: # secretObjects defines the desired state of synced K8s secret
 objects
 - secretName: ingress-tls-csi
 type: kubernetes.io/tls
 data:
 - objectName: $CERT_NAME
 key: tls.key
 - objectName: $CERT_NAME
 key: tls.crt
 parameters:
 usePodIdentity: "false"
 useVMManagedIdentity: "true"
 userAssignedIdentityID: <client id>
 keyvaultName: $AKV_NAME # the name of the AKV instance
 objects: |
 array:
 - |
 objectName: $CERT_NAME
 objectType: secret
 tenantId: $TENANT_ID # the tenant ID of the AKV instance
```

Apply the SecretProviderClass to your Kubernetes cluster:

```
kubectl apply -f secretProviderClass.yaml -n $NAMESPACE
```

## Deploy the ingress controller

### Add the official ingress chart repository

```
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx
helm repo update
```

### Configure and deploy the NGINX ingress

As mentioned above, depending on your scenario, you can choose to bind the certificate to either the application or to the ingress controller. Follow the below instructions according to your selection:

#### Bind certificate to application

The application's deployment will reference the Secrets Store CSI Driver's Azure Key Vault provider.

```
helm install ingress-nginx/ingress-nginx --generate-name \
--namespace $NAMESPACE \
--set controller.replicaCount=2 \
--set controller.nodeSelector."kubernetes\.io/os"=linux \
--set controller.service.annotations."service\.beta\.kubernetes\.io/azure-load-balancer-health-probe-
request-path"/=healthz \
--set defaultBackend.nodeSelector."kubernetes\.io/os"=linux
```

#### Bind certificate to ingress controller

The ingress controller's deployment will reference the Secrets Store CSI Driver's Azure Key Vault provider.

##### NOTE

If not using Azure Active Directory (AAD) pod identity as your method of access, remove the line with

```
--set controller.podLabels.aadpodidbinding=$AAD_POD_IDENTITY_NAME
```

```
helm install ingress-nginx/ingress-nginx --generate-name \
--namespace $NAMESPACE \
--set controller.replicaCount=2 \
--set controller.nodeSelector."kubernetes\.io/os"=linux \
--set defaultBackend.nodeSelector."kubernetes\.io/os"=linux \
--set controller.service.annotations."service\.beta\.kubernetes\.io/azure-load-balancer-health-probe-
request-path"/=healthz \
--set controller.podLabels.aadpodidbinding=$AAD_POD_IDENTITY_NAME \
-f - <<EOF
controller:
 extraVolumes:
 - name: secrets-store-inline
 csi:
 driver: secrets-store.csi.k8s.io
 readOnly: true
 volumeAttributes:
 secretProviderClass: "azure-tls"
 extraVolumeMounts:
 - name: secrets-store-inline
 mountPath: "/mnt/secrets-store"
 readOnly: true
EOF
```

Verify the Kubernetes secret has been created:

```
kubectl get secret -n $NAMESPACE
```

NAME	TYPE	DATA	AGE
ingress-tls-csi	kubernetes.io/tls	2	1m34s

## Deploy the application

Again, depending on your scenario, the instructions will change slightly. Follow the instructions corresponding to the scenario you've selected so far:

#### Deploy the application using an application reference

Create a file named `aks-helloworld-one.yaml` with the following content:

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: aks-helloworld-one
spec:
 replicas: 1
 selector:
 matchLabels:
 app: aks-helloworld-one
 template:
 metadata:
 labels:
 app: aks-helloworld-one
 spec:
 containers:
 - name: aks-helloworld-one
 image: mcr.microsoft.com/azuredocs/aks-helloworld:v1
 ports:
 - containerPort: 80
 env:
 - name: TITLE
 value: "Welcome to Azure Kubernetes Service (AKS)"
 volumeMounts:
 - name: secrets-store-inline
 mountPath: "/mnt/secrets-store"
 readOnly: true
 volumes:
 - name: secrets-store-inline
 csi:
 driver: secrets-store.csi.k8s.io
 readOnly: true
 volumeAttributes:
 secretProviderClass: "azure-tls"

apiVersion: v1
kind: Service
metadata:
 name: aks-helloworld-one
spec:
 type: ClusterIP
 ports:
 - port: 80
 selector:
 app: aks-helloworld-one
```

Create a file named `aks-helloworld-two.yaml` with the following content:

```

apiVersion: apps/v1
kind: Deployment
metadata:
 name: aks-helloworld-two
spec:
 replicas: 1
 selector:
 matchLabels:
 app: aks-helloworld-two
 template:
 metadata:
 labels:
 app: aks-helloworld-two
 spec:
 containers:
 - name: aks-helloworld-two
 image: mcr.microsoft.com/azuredocs/aks-helloworld:v1
 ports:
 - containerPort: 80
 env:
 - name: TITLE
 value: "AKS Ingress Demo"
 volumeMounts:
 - name: secrets-store-inline
 mountPath: "/mnt/secrets-store"
 readOnly: true
 volumes:
 - name: secrets-store-inline
 csi:
 driver: secrets-store.csi.k8s.io
 readOnly: true
 volumeAttributes:
 secretProviderClass: "azure-tls"

apiVersion: v1
kind: Service
metadata:
 name: aks-helloworld-two
spec:
 type: ClusterIP
 ports:
 - port: 80
 selector:
 app: aks-helloworld-two

```

And apply them to your cluster:

```

kubectl apply -f aks-helloworld-one.yaml -n $NAMESPACE
kubectl apply -f aks-helloworld-two.yaml -n $NAMESPACE

```

Verify the Kubernetes secret has been created:

NAME	TYPE	DATA	AGE
ingress-tls-csi	kubernetes.io/tls	2	1m34s

## Deploy the application using an ingress controller reference

Create a file named `aks-helloworld-one.yaml` with the following content:

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: aks-helloworld-one
spec:
 replicas: 1
 selector:
 matchLabels:
 app: aks-helloworld-one
 template:
 metadata:
 labels:
 app: aks-helloworld-one
 spec:
 containers:
 - name: aks-helloworld-one
 image: mcr.microsoft.com/azuredocs/aks-helloworld:v1
 ports:
 - containerPort: 80
 env:
 - name: TITLE
 value: "Welcome to Azure Kubernetes Service (AKS)"

apiVersion: v1
kind: Service
metadata:
 name: aks-helloworld-one
spec:
 type: ClusterIP
 ports:
 - port: 80
 selector:
 app: aks-helloworld-one
```

Create a file named `aks-helloworld-two.yaml` with the following content:

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: aks-helloworld-two
spec:
 replicas: 1
 selector:
 matchLabels:
 app: aks-helloworld-two
 template:
 metadata:
 labels:
 app: aks-helloworld-two
 spec:
 containers:
 - name: aks-helloworld-two
 image: mcr.microsoft.com/azuredocs/aks-helloworld:v1
 ports:
 - containerPort: 80
 env:
 - name: TITLE
 value: "AKS Ingress Demo"

apiVersion: v1
kind: Service
metadata:
 name: aks-helloworld-two
spec:
 type: ClusterIP
 ports:
 - port: 80
 selector:
 app: aks-helloworld-two
```

And apply them to your cluster:

```
kubectl apply -f aks-helloworld-one.yaml -n $NAMESPACE
kubectl apply -f aks-helloworld-two.yaml -n $NAMESPACE
```

## Deploy an ingress resource referencing the secret

Finally, we can deploy a Kubernetes ingress resource referencing our secret. Create a file name `hello-world-ingress.yaml` with the following content:

```

apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 name: ingress-tls
 annotations:
 nginx.ingress.kubernetes.io/rewrite-target: /$2
spec:
 ingressClassName: nginx
 tls:
 - hosts:
 - demo.azure.com
 secretName: ingress-tls-csi
 rules:
 - host: demo.azure.com
 http:
 paths:
 - path: /hello-world-one(/|$(.)*)
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-one
 port:
 number: 80
 - path: /hello-world-two(/|$(.)*)
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-two
 port:
 number: 80
 - path: /(.*)
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-one
 port:
 number: 80

```

Make note of the `tls` section referencing the secret we've created earlier, and apply the file to your cluster:

```
kubectl apply -f hello-world-ingress.yaml -n $NAMESPACE
```

## Obtain the external IP address of the ingress controller

Use `kubectl get service` to obtain the external IP address for the ingress controller.

```
kubectl get service --namespace $NAMESPACE --selector app.kubernetes.io/name=ingress-nginx
```

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)
AGE				
nginx-ingress-1588032400-controller	LoadBalancer	10.0.255.157	EXTERNAL_IP 80:31293/TCP,443:31265/TCP 19m	
nginx-ingress-1588032400-default-backend	ClusterIP	10.0.223.214	<none>	80/TCP 19m

## Test ingress secured with TLS

Use `curl` to verify your ingress has been properly configured with TLS. Be sure to use the external IP you've obtained from the previous step:

```
curl -v -k --resolve demo.azure.com:443:EXTERNAL_IP https://demo.azure.com
```

No additional path was provided with the address, so the ingress controller defaults to the /route. The first demo application is returned, as shown in the following condensed example output:

```
[...]
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
 <link rel="stylesheet" type="text/css" href="/static/default.css">
 <title>Welcome to Azure Kubernetes Service (AKS)</title>
[...]
```

The `-v` parameter in our `curl` command outputs verbose information, including the TLS certificate received. Half-way through your curl output, you can verify that your own TLS certificate was used. The `-k` parameter continues loading the page even though we're using a self-signed certificate. The following example shows that the `issuer: CN=demo.azure.com; O=aks-ingress-tls` certificate was used:

```
[...]
* Server certificate:
* subject: CN=demo.azure.com; O=aks-ingress-tls
* start date: Oct 22 22:13:54 2021 GMT
* expire date: Oct 22 22:13:54 2022 GMT
* issuer: CN=demo.azure.com; O=aks-ingress-tls
* SSL certificate verify result: self signed certificate (18), continuing anyway.
[...]
```

Now add `/hello-world-two` path to the address, such as `https://demo.azure.com/hello-world-two`. The second demo application with the custom title is returned, as shown in the following condensed example output:

```
curl -v -k --resolve demo.azure.com:443:EXTERNAL_IP https://demo.azure.com/hello-world-two

[...]
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
 <link rel="stylesheet" type="text/css" href="/static/default.css">
 <title>AKS Ingress Demo</title>
[...]
```

# Create a private Azure Kubernetes Service cluster

10/27/2022 • 11 minutes to read • [Edit Online](#)

In a private cluster, the control plane or API server has internal IP addresses that are defined in the [RFC1918 - Address Allocation for Private Internet](#) document. By using a private cluster, you can ensure network traffic between your API server and your node pools remains on the private network only.

The control plane or API server is in an Azure Kubernetes Service (AKS)-managed Azure subscription. A customer's cluster or node pool is in the customer's subscription. The server and the cluster or node pool can communicate with each other through the [Azure Private Link service](#) in the API server virtual network and a private endpoint that's exposed in the subnet of the customer's AKS cluster.

When you provision a private AKS cluster, AKS by default creates a private FQDN with a private DNS zone and an additional public FQDN with a corresponding A record in Azure public DNS. The agent nodes still use the A record in the private DNS zone to resolve the private IP address of the private endpoint for communication to the API server.

## Region availability

Private cluster is available in public regions, Azure Government, and Azure China 21Vianet regions where [AKS is supported](#).

## Prerequisites

- The Azure CLI version 2.28.0 and higher.
- The aks-preview extension 0.5.29 or higher.
- If using ARM or the Azure REST API, the AKS API version must be 2021-05-01 or higher.
- Azure Private Link service is supported on Standard Azure Load Balancer only. Basic Azure Load Balancer isn't supported.
- To use a custom DNS server, add the Azure public IP address 168.63.129.16 as the upstream DNS server in the custom DNS server. For more information about the Azure IP address, see [What is IP address 168.63.129.16?](#)

## Create a private AKS cluster

### Create a resource group

Create a resource group or use an existing resource group for your AKS cluster.

```
az group create -l westus -n MyResourceGroup
```

### Default basic networking

```
az aks create -n <private-cluster-name> -g <private-cluster-resource-group> --load-balancer-sku standard --enable-private-cluster
```

Where `--enable-private-cluster` is a mandatory flag for a private cluster.

### Advanced networking

```
az aks create \
 --resource-group <private-cluster-resource-group> \
 --name <private-cluster-name> \
 --load-balancer-sku standard \
 --enable-private-cluster \
 --network-plugin azure \
 --vnet-subnet-id <subnet-id> \
 --docker-bridge-address 172.17.0.1/16 \
 --dns-service-ip 10.2.0.10 \
 --service-cidr 10.2.0.0/24
```

Where `--enable-private-cluster` is a mandatory flag for a private cluster.

#### NOTE

If the Docker bridge address CIDR (172.17.0.1/16) clashes with the subnet CIDR, change the Docker bridge address appropriately.

## Use custom domains

If you want to configure custom domains that can only be resolved internally, see [Use custom domains](#) for more information.

## Disable Public FQDN

The following parameters can be leveraged to disable Public FQDN.

### Disable Public FQDN on a new AKS cluster

```
az aks create -n <private-cluster-name> -g <private-cluster-resource-group> --load-balancer-sku standard --enable-private-cluster --enable-managed-identity --assign-identity <ResourceId> --private-dns-zone <private-dns-zone-mode> --disable-public-fqdn
```

### Disable Public FQDN on an existing cluster

```
az aks update -n <private-cluster-name> -g <private-cluster-resource-group> --disable-public-fqdn
```

## Configure Private DNS Zone

The following parameters can be leveraged to configure Private DNS Zone.

- "system", which is also the default value. If the `--private-dns-zone` argument is omitted, AKS will create a Private DNS Zone in the Node Resource Group.
- "none", defaults to public DNS which means AKS will not create a Private DNS Zone.
- "CUSTOM\_PRIVATE\_DNS\_ZONE\_RESOURCE\_ID", which requires you to create a Private DNS Zone in this format for Azure global cloud: `privatelink.<region>.azmk8s.io` or `<subzone>.privatelink.<region>.azmk8s.io`. You will need the Resource ID of that Private DNS Zone going forward. Additionally, you will need a user assigned identity or service principal with at least the `private dns zone contributor` and `network contributor` roles.
  - If the Private DNS Zone is in a different subscription than the AKS cluster, you need to register Microsoft.ContainerServices in both the subscriptions.
  - "fqdn-subdomain" can be utilized with "CUSTOM\_PRIVATE\_DNS\_ZONE\_RESOURCE\_ID" only to provide subdomain capabilities to `privatelink.<region>.azmk8s.io`

## Create a private AKS cluster with Private DNS Zone

```
az aks create -n <private-cluster-name> -g <private-cluster-resource-group> --load-balancer-sku standard --enable-private-cluster --enable-managed-identity --assign-identity <ResourceId> --private-dns-zone [system|none]
```

## Create a private AKS cluster with Custom Private DNS Zone or Private DNS SubZone

```
Custom Private DNS Zone name should be in format "<subzone>.privatelink.<region>.azmk8s.io"
az aks create -n <private-cluster-name> -g <private-cluster-resource-group> --load-balancer-sku standard --enable-private-cluster --enable-managed-identity --assign-identity <ResourceId> --private-dns-zone <custom private dns zone or custom private dns subzone ResourceId>
```

## Create a private AKS cluster with Custom Private DNS Zone and Custom Subdomain

```
Custom Private DNS Zone name could be in formats "privatelink.<region>.azmk8s.io" or "<subzone>.privatelink.<region>.azmk8s.io"
az aks create -n <private-cluster-name> -g <private-cluster-resource-group> --load-balancer-sku standard --enable-private-cluster --enable-managed-identity --assign-identity <ResourceId> --private-dns-zone <custom private dns zone ResourceId> --fqdn-subdomain <subdomain>
```

## Options for connecting to the private cluster

The API server endpoint has no public IP address. To manage the API server, you'll need to use a VM that has access to the AKS cluster's Azure Virtual Network (VNet). There are several options for establishing network connectivity to the private cluster.

- Create a VM in the same Azure Virtual Network (VNet) as the AKS cluster.
- Use a VM in a separate network and set up [Virtual network peering](#). See the section below for more information on this option.
- Use an [Express Route or VPN](#) connection.
- Use the [AKS command invoke feature](#).
- Use a [private endpoint](#) connection.

Creating a VM in the same VNET as the AKS cluster is the easiest option. Express Route and VPNs add costs and require additional networking complexity. Virtual network peering requires you to plan your network CIDR ranges to ensure there are no overlapping ranges.

## Virtual network peering

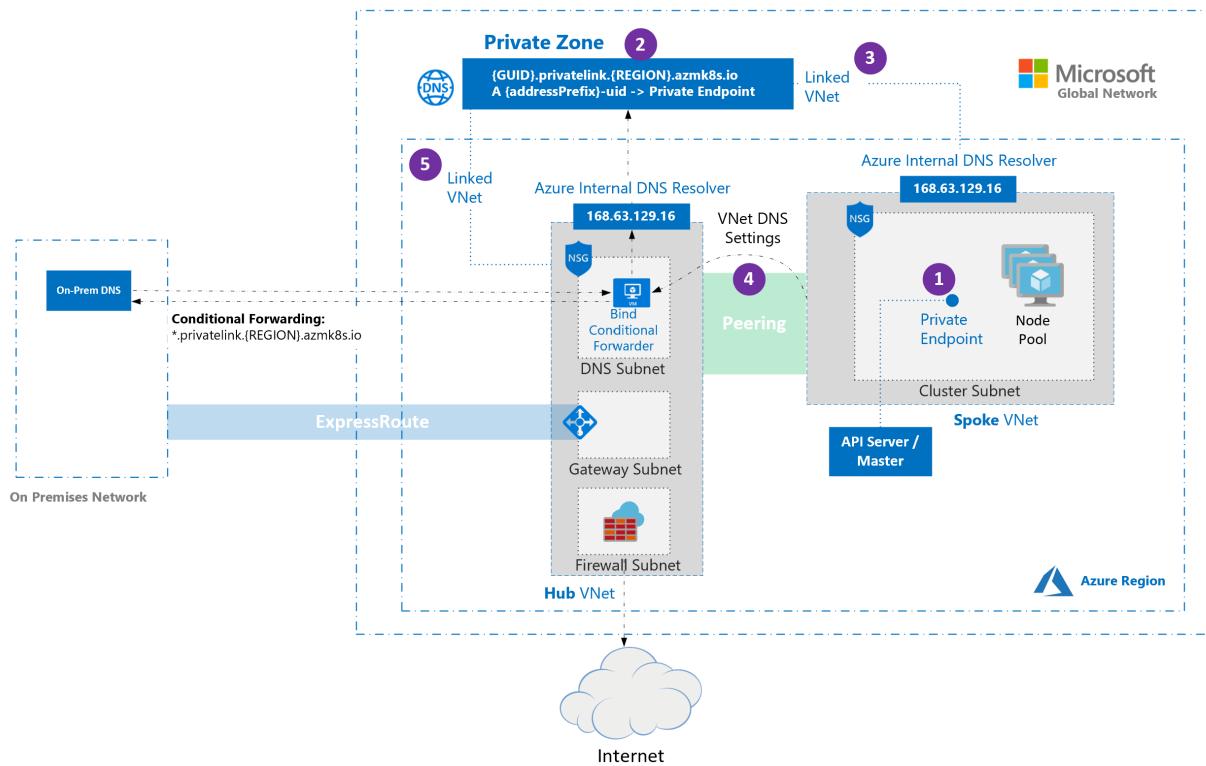
As mentioned, virtual network peering is one way to access your private cluster. To use virtual network peering, you need to set up a link between virtual network and the private DNS zone.

1. Go to the node resource group in the Azure portal.
2. Select the private DNS zone.
3. In the left pane, select the **Virtual network** link.
4. Create a new link to add the virtual network of the VM to the private DNS zone. It takes a few minutes for the DNS zone link to become available.
5. In the Azure portal, navigate to the resource group that contains your cluster's virtual network.
6. In the right pane, select the virtual network. The virtual network name is in the form *aks-vnet-\**.
7. In the left pane, select **Peerings**.
8. Select **Add**, add the virtual network of the VM, and then create the peering.
9. Go to the virtual network where you have the VM, select **Peerings**, select the AKS virtual network, and then

create the peering. If the address ranges on the AKS virtual network and the VM's virtual network clash, peering fails. For more information, see [Virtual network peering](#).

## Hub and spoke with custom DNS

[Hub and spoke architectures](#) are commonly used to deploy networks in Azure. In many of these deployments, DNS settings in the spoke VNets are configured to reference a central DNS forwarder to allow for on-premises and Azure-based DNS resolution. When deploying an AKS cluster into such a networking environment, there are some special considerations that must be taken into account.



1. By default, when a private cluster is provisioned, a private endpoint (1) and a private DNS zone (2) are created in the cluster-managed resource group. The cluster uses an A record in the private zone to resolve the IP of the private endpoint for communication to the API server.
2. The private DNS zone is linked only to the VNet that the cluster nodes are attached to (3). This means that the private endpoint can only be resolved by hosts in that linked VNet. In scenarios where no custom DNS is configured on the VNet (default), this works without issue as hosts point at 168.63.129.16 for DNS that can resolve records in the private DNS zone because of the link.
3. In scenarios where the VNet containing your cluster has custom DNS settings (4), cluster deployment fails unless the private DNS zone is linked to the VNet that contains the custom DNS resolvers (5). This link can be created manually after the private zone is created during cluster provisioning or via automation upon detection of creation of the zone using event-based deployment mechanisms (for example, Azure Event Grid and Azure Functions).

### NOTE

Conditional Forwarding doesn't support subdomains.

#### NOTE

If you are using [Bring Your Own Route Table with kubenet](#) and [Bring Your Own DNS with Private Cluster](#), the cluster creation will fail. You will need to associate the [RouteTable](#) in the node resource group to the subnet after the cluster creation failed, in order to make the creation successful.

## Use a private endpoint connection

A private endpoint can be set up so that an Azure Virtual Network doesn't need to be peered to communicate to the private cluster. To use a private endpoint, create a new private endpoint in your virtual network then create a link between your virtual network and a new private DNS zone.

#### IMPORTANT

If the virtual network is configured with custom DNS servers, private DNS will need to be set up appropriately for the environment. See the [virtual networks name resolution documentation](#) for more details.

1. On the Azure portal menu or from the Home page, select **Create a resource**.
2. Search for **Private Endpoint** and select **Create > Private Endpoint**.
3. Select **Create**.
4. On the **Basics** tab, set up the following options:
  - **Project details:**
    - Select an **Azure Subscription**.
    - Select the **Azure Resource group** where your virtual network is located.
  - **Instance details:**
    - Enter a **Name** for the private endpoint, such as *myPrivateEndpoint*.
    - Select a **Region** for the private endpoint.

#### IMPORTANT

Check that the region selected is the same as the virtual network where you want to connect from, otherwise you won't see your virtual network in the **Configuration** tab.

5. Select **Next: Resource** when complete.
6. On the **Resource** tab, set up the following options:
  - **Connection method:** *Connect to an Azure resource in my directory*
  - **Subscription:** Select your Azure Subscription where the private cluster is located
  - **Resource type:** *Microsoft.ContainerService/managedClusters*
  - **Resource:** *myPrivateAKSCluster*
  - **Target sub-resource:** *management*
7. Select **Next: Configuration** when complete.
8. On the **Configuration** tab, set up the following options:
  - **Networking:**
    - **Virtual network:** *myVirtualNetwork*
    - **Subnet:** *mySubnet*
9. Select **Next: Tags** when complete.
10. (Optional) On the **Tags** tab, set up key-values as needed.
11. Select **Next: Review + create**, and then select **Create** when validation completes.

Record the private IP address of the private endpoint. This private IP address is used in a later step.

After the private endpoint has been created, create a new private DNS zone with the same name as the private DNS zone that was created by the private cluster.

1. Go to the node resource group in the Azure portal.
2. Select the private DNS zone and record:
  - the name of the private DNS zone, which follows the pattern `*.privatelink.<region>.azmk8s.io`
  - the name of the A record (excluding the private DNS name)
  - the time-to-live (TTL)
3. On the Azure portal menu or from the Home page, select **Create a resource**.
4. Search for **Private DNS zone** and select **Create > Private DNS Zone**.
5. On the **Basics** tab, set up the following options:
  - **Project details:**
    - Select an Azure Subscription
    - Select the Azure Resource group where the private endpoint was created
  - **Instance details:**
    - Enter the **Name** of the DNS zone retrieved from previous steps
    - **Region** defaults to the Azure Resource group location
6. Select **Review + create** when complete and select **Create** when validation completes.

After the private DNS zone is created, create an A record. This record associates the private endpoint to the private cluster.

1. Go to the private DNS zone created in previous steps.
2. On the **Overview** page, select **+ Record set**.
3. On the **Add record set** tab, set up the following options:
  - **Name:** Input the name retrieved from the A record in the private cluster's DNS zone
  - **Type:** *A - Alias record to IPv4 address*
  - **TTL:** Input the number to match the record from the A record private cluster's DNS zone
  - **TTL Unit:** Change the dropdown value to match the A record from the private cluster's DNS zone
  - **IP address:** Input the IP address of the private endpoint that was created previously

#### IMPORTANT

When creating the A record, use only the name, and not the fully qualified domain name (FQDN).

Once the A record is created, link the private DNS zone to the virtual network that will access the private cluster.

1. Go to the private DNS zone created in previous steps.
2. In the left pane, select **Virtual network links**.
3. Create a new link to add the virtual network to the private DNS zone. It takes a few minutes for the DNS zone link to become available.

#### WARNING

If the private cluster is stopped and restarted, the private cluster's original private link service is removed and re-created, which breaks the connection between your private endpoint and the private cluster. To resolve this issue, delete and re-create any user created private endpoints linked to the private cluster. DNS records will also need to be updated if the re-created private endpoints have new IP addresses.

## Limitations

- IP authorized ranges can't be applied to the private API server endpoint, they only apply to the public API server
- [Azure Private Link service limitations](#) apply to private clusters.
- No support for Azure DevOps Microsoft-hosted Agents with private clusters. Consider using [Self-hosted Agents](#).
- If you need to enable Azure Container Registry to work with a private AKS cluster, [set up a private link for the container registry in the cluster virtual network](#) or set up peering between the Container Registry virtual network and the private cluster's virtual network.
- No support for converting existing AKS clusters into private clusters
- Deleting or modifying the private endpoint in the customer subnet will cause the cluster to stop functioning.

# Use `command invoke` to access a private Azure Kubernetes Service (AKS) cluster

10/27/2022 • 2 minutes to read • [Edit Online](#)

Accessing a private AKS cluster requires that you connect to that cluster either from the cluster virtual network, from a peered network, or via a configured private endpoint. These approaches require configuring a VPN, Express Route, deploying a *jumpbox* within the cluster virtual network, or creating a private endpoint inside of another virtual network. Alternatively, you can use `command invoke` to access private clusters without having to configure a VPN or Express Route. Using `command invoke` allows you to remotely invoke commands like `kubectl` and `helm` on your private cluster through the Azure API without directly connecting to the cluster. Permissions for using `command invoke` are controlled through the `Microsoft.ContainerService/managedClusters/runcommand/action` and `Microsoft.ContainerService/managedclusters/commandResults/read` roles.

## Prerequisites

- An existing private cluster.
- The Azure CLI version 2.24.0 or later.
- Access to the `Microsoft.ContainerService/managedClusters/runcommand/action` and `Microsoft.ContainerService/managedclusters/commandResults/read` roles on the cluster.

## Limitations

The pod created by the `run` command provides the following binaries:

- The latest compatible version of `kubectl` for your cluster with `kustomize`.
- `helm`

In addition, `command invoke` runs the commands from your cluster so any commands run in this manner are subject to networking and other restrictions you have configured on your cluster. Also make sure that there are enough nodes and resources in your cluster to schedule this command pod.

## Use `command invoke` to run a single command

Use `az aks command invoke --command` to run a command on your cluster. For example:

```
az aks command invoke \
--resource-group myResourceGroup \
--name myAKSCluster \
--command "kubectl get pods -n kube-system"
```

The above example runs the `kubectl get pods -n kube-system` command on the *myAKSCluster* cluster in *myResourceGroup*.

## Use `command invoke` to run multiple commands

Use `az aks command invoke --command` to run multiple commands on your cluster. For example:

```
az aks command invoke \
--resource-group myResourceGroup \
--name myAKSCluster \
--command "helm repo add bitnami https://charts.bitnami.com/bitnami && helm repo update && helm install my-release bitnami/nginx"
```

The above example runs three `helm` commands on the *myAKSCluster* cluster in *myResourceGroup*.

## Use `command invoke` to run commands with an attached file or directory

Use `az aks command invoke --command` to run commands on your cluster and `--file` to attach a file or directory for use by those commands. For example:

```
az aks command invoke \
--resource-group myResourceGroup \
--name myAKSCluster \
--command "kubectl apply -f deployment.yaml -n default" \
--file deployment.yaml
```

The above runs `kubectl apply -f deployment.yaml -n default` on the *myAKSCluster* cluster in *myResourceGroup*. The `deployment.yaml` file used by that command is attached from the current directory on the development computer where `az aks command invoke` was run.

You can also attach all files in the current directory. For example:

```
az aks command invoke \
--resource-group myResourceGroup \
--name myAKSCluster \
--command "kubectl apply -f deployment.yaml configmap.yaml -n default" \
--file .
```

The above runs `kubectl apply -f deployment.yaml configmap.yaml -n default` on the *myAKSCluster* cluster in *myResourceGroup*. The `deployment.yaml` and `configmap.yaml` files used by that command are part of the current directory on the development computer where `az aks command invoke` was run.

# Use kubenet networking with your own IP address ranges in Azure Kubernetes Service (AKS)

10/27/2022 • 13 minutes to read • [Edit Online](#)

By default, AKS clusters use [kubenet](#), and an Azure virtual network and subnet are created for you. With *kubenet*, nodes get an IP address from the Azure virtual network subnet. Pods receive an IP address from a logically different address space to the Azure virtual network subnet of the nodes. Network address translation (NAT) is then configured so that the pods can reach resources on the Azure virtual network. The source IP address of the traffic is NAT'd to the node's primary IP address. This approach greatly reduces the number of IP addresses that you need to reserve in your network space for pods to use.

With [Azure Container Networking Interface \(CNI\)](#), every pod gets an IP address from the subnet and can be accessed directly. These IP addresses must be unique across your network space, and must be planned in advance. Each node has a configuration parameter for the maximum number of pods that it supports. The equivalent number of IP addresses per node are then reserved up front for that node. This approach requires more planning, and often leads to IP address exhaustion or the need to rebuild clusters in a larger subnet as your application demands grow. You can configure the maximum pods deployable to a node at cluster create time or when creating new node pools. If you don't specify maxPods when creating new node pools, you receive a default value of 110 for kubenet.

This article shows you how to use *kubenet* networking to create and use a virtual network subnet for an AKS cluster. For more information on network options and considerations, see [Network concepts for Kubernetes and AKS](#).

## Prerequisites

- The virtual network for the AKS cluster must allow outbound internet connectivity.
- Don't create more than one AKS cluster in the same subnet.
- AKS clusters may not use `169.254.0.0/16`, `172.30.0.0/16`, `172.31.0.0/16`, or `192.0.2.0/24` for the Kubernetes service address range, pod address range or cluster virtual network address range.
- The cluster identity used by the AKS cluster must have at least [Network Contributor](#) role on the subnet within your virtual network. CLI helps do the role assignment automatically. If you are using ARM template or other clients, the role assignment needs to be done manually. You must also have the appropriate permissions, such as the subscription owner, to create a cluster identity and assign it permissions. If you wish to define a [custom role](#) instead of using the built-in Network Contributor role, the following permissions are required:
  - `Microsoft.Network/virtualNetworks/subnets/join/action`
  - `Microsoft.Network/virtualNetworks/subnets/read`

### WARNING

To use Windows Server node pools, you must use Azure CNI. The use of kubenet as the network model is not available for Windows Server containers.

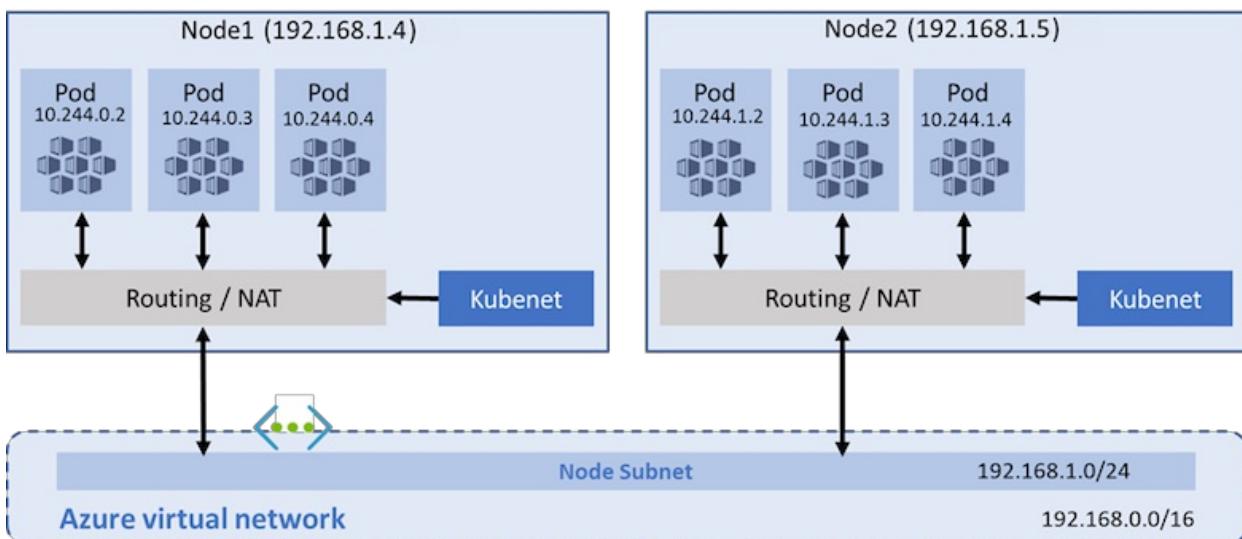
## Before you begin

You need the Azure CLI version 2.0.65 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

# Overview of kubenet networking with your own subnet

In many environments, you have defined virtual networks and subnets with allocated IP address ranges. These virtual network resources are used to support multiple services and applications. To provide network connectivity, AKS clusters can use *kubenet* (basic networking) or Azure CNI (advanced networking).

With *kubenet*, only the nodes receive an IP address in the virtual network subnet. Pods can't communicate directly with each other. Instead, User Defined Routing (UDR) and IP forwarding is used for connectivity between pods across nodes. By default, UDRs and IP forwarding configuration is created and maintained by the AKS service, but you have the option to [bring your own route table for custom route management](#). You could also deploy pods behind a service that receives an assigned IP address and load balances traffic for the application. The following diagram shows how the AKS nodes receive an IP address in the virtual network subnet, but not the pods:



Azure supports a maximum of 400 routes in a UDR, so you can't have an AKS cluster larger than 400 nodes. AKS [Virtual Nodes](#) and Azure Network Policies aren't supported with *kubenet*. You can use [Calico Network Policies](#), as they are supported with *kubenet*.

With *Azure CNI*, each pod receives an IP address in the IP subnet, and can directly communicate with other pods and services. Your clusters can be as large as the IP address range you specify. However, the IP address range must be planned in advance, and all of the IP addresses are consumed by the AKS nodes based on the maximum number of pods that they can support. Advanced network features and scenarios such as [Virtual Nodes](#) or Network Policies (either Azure or Calico) are supported with *Azure CNI*.

## Limitations & considerations for kubenet

- An additional hop is required in the design of *kubenet*, which adds minor latency to pod communication.
- Route tables and user-defined routes are required for using *kubenet*, which adds complexity to operations.
- Direct pod addressing isn't supported for *kubenet* due to *kubenet* design.
- Unlike *Azure CNI* clusters, multiple *kubenet* clusters can't share a subnet.
- AKS doesn't apply Network Security Groups (NSGs) to its subnet and will not modify any of the NSGs associated with that subnet. If you provide your own subnet and add NSGs associated with that subnet, you must ensure the security rules in the NSGs allow traffic between the node and pod CIDR. For more details, see [Network security groups](#).
- Features not supported on *kubenet* include:
  - [Azure network policies](#), but Calico network policies are supported on *kubenet*
  - [Windows node pools](#)
  - [Virtual nodes add-on](#)

## IP address availability and exhaustion

With *Azure CNI*, a common issue is the assigned IP address range is too small to then add additional nodes when you scale or upgrade a cluster. The network team may also not be able to issue a large enough IP address range to support your expected application demands.

As a compromise, you can create an AKS cluster that uses *kubenet* and connect to an existing virtual network subnet. This approach lets the nodes receive defined IP addresses, without the need to reserve a large number of IP addresses up front for all of the potential pods that could run in the cluster.

With *kubenet*, you can use a much smaller IP address range and be able to support large clusters and application demands. For example, even with a /27 IP address range on your subnet, you could run a 20-25 node cluster with enough room to scale or upgrade. This cluster size would support up to 2,200-2,750 pods (with a default maximum of 110 pods per node). The maximum number of pods per node that you can configure with *kubenet* in AKS is 110.

The following basic calculations compare the difference in network models:

- **kubenet** - a simple /24 IP address range can support up to 251 nodes in the cluster (each Azure virtual network subnet reserves the first three IP addresses for management operations)
  - This node count could support up to 27,610 pods (with a default maximum of 110 pods per node with *kubenet*)
- **Azure CNI** - that same basic /24 subnet range could only support a maximum of 8 nodes in the cluster
  - This node count could only support up to 240 pods (with a default maximum of 30 pods per node with *Azure CNI*)

### NOTE

These maximums don't take into account upgrade or scale operations. In practice, you can't run the maximum number of nodes that the subnet IP address range supports. You must leave some IP addresses available for use during scale or upgrade operations.

## Virtual network peering and ExpressRoute connections

To provide on-premises connectivity, both *kubenet* and *Azure-CNI* network approaches can use [Azure virtual network peering](#) or [ExpressRoute connections](#). Plan your IP address ranges carefully to prevent overlap and incorrect traffic routing. For example, many on-premises networks use a 10.0.0.0/8 address range that is advertised over the ExpressRoute connection. It's recommended to create your AKS clusters into Azure virtual network subnets outside of this address range, such as 172.16.0.0/16.

## Choose a network model to use

The choice of which network plugin to use for your AKS cluster is usually a balance between flexibility and advanced configuration needs. The following considerations help outline when each network model may be the most appropriate.

Use *kubenet* when:

- You have limited IP address space.
- Most of the pod communication is within the cluster.
- You don't need advanced AKS features such as virtual nodes or Azure Network Policy. Use [Calico network policies](#).

Use *Azure CNI* when:

- You have available IP address space.
- Most of the pod communication is to resources outside of the cluster.

- You don't want to manage user defined routes for pod connectivity.
- You need AKS advanced features such as virtual nodes or Azure Network Policy. Use [Calico network policies](#).

For more information to help you decide which network model to use, see [Compare network models and their support scope](#).

## Create a virtual network and subnet

To get started with using *kubenet* and your own virtual network subnet, first create a resource group using the [az group create](#) command. The following example creates a resource group named *myResourceGroup* in the *eastus* location:

```
az group create --name myResourceGroup --location eastus
```

If you don't have an existing virtual network and subnet to use, create these network resources using the [az network vnet create](#) command. In the following example, the virtual network is named *myAKSVnet* with the address prefix of *192.168.0.0/16*. A subnet is created named *myAKSSubnet* with the address prefix *192.168.1.0/24*.

```
az network vnet create \
--resource-group myResourceGroup \
--name myAKSVnet \
--address-prefixes 192.168.0.0/16 \
--subnet-name myAKSSubnet \
--subnet-prefix 192.168.1.0/24
```

Get the subnet resource ID and store as a variable:

```
SUBNET_ID=$(az network vnet subnet show --resource-group myResourceGroup --vnet-name myAKSVnet --name myAKSSubnet --query id -o tsv)
```

## Create an AKS cluster in the virtual network

Now create an AKS cluster in your virtual network and subnet using the [az aks create](#) command.

### Create an AKS cluster with system-assigned managed identities

You can create an AKS cluster using a system-assigned managed identity by running the following CLI command.

#### NOTE

When using system-assigned identity, azure-cli will grant Network Contributor role to the system-assigned identity after the cluster is created. If you are using an ARM template or other clients, you need to use the [user-assigned managed identity](#)

```
az aks create \
--resource-group myResourceGroup \
--name myAKScluster \
--node-count 3 \
--network-plugin kubenet \
--vnet-subnet-id $SUBNET_ID
```

## NOTE

If you wish to enable an AKS cluster to include a [Calico network policy](#) you can use the following command.

```
az aks create \
 --resource-group myResourceGroup \
 --name myAKSCluster \
 --node-count 3 \
 --network-plugin kubenet --network-policy calico \
 --vnet-subnet-id $SUBNET_ID
```

## Create an AKS cluster with user-assigned managed identities

### Create or obtain a managed identity

If you don't have a managed identity, you should create one by running the [az identity](#) command.

```
az identity create --name myIdentity --resource-group myResourceGroup
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "clientSecretUrl": "<clientSecretUrl>",
 "id": "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myIdentity",
 "location": "westus2",
 "name": "myIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
```

If you have an existing managed identity, you can find the Principal ID by running the following command:

```
az identity show --ids <identity-resource-id>
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "id": "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myIdentity",
 "location": "eastus",
 "name": "myIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
```

### Add role assignment for managed identity

If you are using Azure CLI, the role will be added automatically and you can skip this step. If you are using an

ARM template or other clients, you need to use the Principal ID of the cluster managed identity to perform a role assignment.

To assign the correct delegations in the remaining steps, use the [az network vnet show](#) and [az network vnet subnet show](#) commands to get the required resource IDs. These resource IDs are stored as variables and referenced in the remaining steps:

```
VNET_ID=$(az network vnet show --resource-group myResourceGroup --name myAKSVnet --query id -o tsv)
```

Now assign the managed identity for your AKS cluster *Network Contributor* permissions on the virtual network using the [az role assignment create](#) command. Provide the <principalId> as shown in the output from the previous command to create the identity:

```
az role assignment create --assignee <control-plane-identity-principal-id> --scope $VNET_ID --role "Network Contributor"
```

Example:

```
az role assignment create --assignee 22222222-2222-2222-2222-222222222222 --scope "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/myResourceGroup/providers/Microsoft.Network/virtualNetworks/myAKSVnet" --role "Network Contributor"
```

#### NOTE

Permission granted to your cluster's managed identity used by Azure may take up 60 minutes to populate.

#### Create an AKS cluster

Now you can create an AKS cluster using the user-assigned managed identity by running the following CLI command. Provide the control plane identity resource ID via `--assign-identity`

```
az aks create \
 --resource-group myResourceGroup \
 --name myAKScluster \
 --node-count 3 \
 --network-plugin kubenet \
 --vnet-subnet-id $SUBNET_ID \
 --enable-managed-identity \
 --assign-identity <identity-resource-id>
```

When you create an AKS cluster, a network security group and route table are automatically created. These network resources are managed by the AKS control plane. The network security group is automatically associated with the virtual NICs on your nodes. The route table is automatically associated with the virtual network subnet. Network security group rules and route tables are automatically updated as you create and expose services.

## Bring your own subnet and route table with kubenet

With kubenet, a route table must exist on your cluster subnet(s). AKS supports bringing your own existing subnet and route table.

If your custom subnet does not contain a route table, AKS creates one for you and adds rules to it throughout the cluster lifecycle. If your custom subnet contains a route table when you create your cluster, AKS acknowledges the existing route table during cluster operations and adds/updates rules accordingly for cloud

provider operations.

#### WARNING

Custom rules can be added to the custom route table and updated. However, rules are added by the Kubernetes cloud provider which must not be updated or removed. Rules such as 0.0.0.0/0 must always exist on a given route table and map to the target of your internet gateway, such as an NVA or other egress gateway. Take caution when updating rules that only your custom rules are being modified.

Learn more about setting up a [custom route table](#).

Kubenet networking requires organized route table rules to successfully route requests. Due to this design, route tables must be carefully maintained for each cluster which relies on it. Multiple clusters cannot share a route table because pod CIDRs from different clusters may overlap which causes unexpected and broken routing. When configuring multiple clusters on the same virtual network or dedicating a virtual network to each cluster, ensure the following limitations are considered.

Limitations:

- A custom route table must be associated to the subnet before you create the AKS cluster.
- The associated route table resource cannot be updated after cluster creation. While the route table resource cannot be updated, custom rules can be modified on the route table.
- Each AKS cluster must use a single, unique route table for all subnets associated with the cluster. You cannot reuse a route table with multiple clusters due to the potential for overlapping pod CIDRs and conflicting routing rules.
- For system-assigned managed identity, it's only supported to provide your own subnet and route table via Azure CLI. That's because CLI will add the role assignment automatically. If you are using an ARM template or other clients, you must use a [user-assigned managed identity](#), assign permissions before cluster creation, and ensure the user-assigned identity has write permissions to your custom subnet and custom route table.
- Using the same route table with multiple AKS clusters isn't supported.

#### NOTE

To create and use your own VNet and route table with `kubenet` network plugin, you need to use [user-assigned control plane identity](#). For system-assigned control plane identity, the identity ID cannot be retrieved before creating a cluster, which causes a delay during role assignment.

To create and use your own VNet and route table with `azure` network plugin, both system-assigned and user-assigned managed identities are supported. But user-assigned managed identity is more recommended for BYO scenarios.

After creating a custom route table and associating it with a subnet in your virtual network, you can create a new AKS cluster specifying your route table with a user-assigned managed identity. You need to use the subnet ID for where you plan to deploy your AKS cluster. This subnet also must be associated with your custom route table.

```
Find your subnet ID
az network vnet subnet list --resource-group
 --vnet-name
 [--subscription]
```

```
Create a kubernetes cluster with with a custom subnet preconfigured with a route table
az aks create -g myResourceGroup -n myManagedCluster --vnet-subnet-id mySubnetIDResourceID --enable-managed-
identity --assign-identity controlPlaneIdentityResourceID
```

## Next steps

With an AKS cluster deployed into your existing virtual network subnet, you can now use the cluster as normal. Get started with [creating new apps using Helm](#) or [deploy existing apps using Helm](#).

# Use dual-stack kubenet networking in Azure Kubernetes Service (AKS) (Preview)

10/27/2022 • 7 minutes to read • [Edit Online](#)

AKS clusters can now be deployed in a dual-stack (using both IPv4 and IPv6 addresses) mode when using [kubenet](#) networking and a dual-stack Azure virtual network. In this configuration, nodes receive both an IPv4 and IPv6 address from the Azure virtual network subnet. Pods receive both an IPv4 and IPv6 address from a logically different address space to the Azure virtual network subnet of the nodes. Network address translation (NAT) is then configured so that the pods can reach resources on the Azure virtual network. The source IP address of the traffic is NAT'd to the node's primary IP address of the same family (IPv4 to IPv4 and IPv6 to IPv6).

This article shows you how to use dual-stack networking with an AKS cluster. For more information on network options and considerations, see [Network concepts for Kubernetes and AKS](#).

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Limitations

### NOTE

Dual-stack kubenet networking is currently not available in sovereign clouds. This note will be removed when rollout is complete.

- Azure Route Tables have a hard limit of 400 routes per table. Because each node in a dual-stack cluster requires two routes, one for each IP address family, dual-stack clusters are limited to 200 nodes.
- During preview, service objects are only supported with `externalTrafficPolicy: Local`.
- Dual-stack networking is required for the Azure Virtual Network and the pod CIDR - single stack IPv6-only isn't supported for node or pod IP addresses. Services can be provisioned on IPv4 or IPv6.
- Features **not supported on dual-stack kubenet** include:
  - [Azure network policies](#)
  - [Calico network policies](#)
  - [NAT Gateway](#)
  - [Virtual nodes add-on](#)
  - [Windows node pools](#)

## Prerequisites

- All prerequisites from [configure kubenet networking](#) apply.

- AKS dual-stack clusters require Kubernetes version v1.21.2 or greater. v1.22.2 or greater is recommended to take advantage of the [out-of-tree cloud controller manager](#), which is the default on v1.22 and up.
- Azure CLI with the `aks-preview` extension 0.5.48 or newer.
- If using Azure Resource Manager templates, schema version 2021-10-01 is required.

### Register the `AKS-EnableDualStack` preview feature

To create an AKS dual-stack cluster, you must enable the `AKS-EnableDualStack` feature flag on your subscription.

Register the `AKS-EnableDualStack` feature flag by using the `az feature register` command, as shown in the following example:

```
az feature register --namespace "Microsoft.ContainerService" --name "AKS-EnableDualStack"
```

It takes a few minutes for the status to show *Registered*. Verify the registration status by using the

```
az feature list
```

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/AKS-EnableDualStack')].{Name:name, State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider by using the

```
az provider register
```

```
az provider register --namespace Microsoft.ContainerService
```

### Install the `aks-preview` CLI extension

```
Install the aks-preview extension
az extension add --name aks-preview

Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

## Overview of dual-stack networking in Kubernetes

Kubernetes v1.23 brings stable upstream support for [IPv4/IPv6 dual-stack](#) clusters, including pod and service networking. Nodes and pods are always assigned both an IPv4 and an IPv6 address, while services can be single-stack on either address family or dual-stack.

AKS configures the required supporting services for dual-stack networking. This configuration includes:

- Dual-stack virtual network configuration (if managed Virtual Network is used)
- IPv4 and IPv6 node and pod addresses
- Outbound rules for both IPv4 and IPv6 traffic
- Load balancer setup for IPv4 and IPv6 services

## Deploying a dual-stack cluster

Three new attributes are provided to support dual-stack clusters:

- `--ip-families` - takes a comma-separated list of IP families to enable on the cluster.
  - Currently only `ipv4` or `ipv4,ipv6` are supported.
- `--pod-cidrs` - takes a comma-separated list of CIDR notation IP ranges to assign pod IPs from.

- The count and order of ranges in this list must match the value provided to `--ip-families`.
- If no values are supplied, the default values of `10.244.0.0/16,fd12:3456:789a::/64` will be used.
- `--service-cidrs` - takes a comma-separated list of CIDR notation IP ranges to assign service IPs from.
  - The count and order of ranges in this list must match the value provided to `--ip-families`.
  - If no values are supplied, the default values of `10.0.0.0/16,fd12:3456:789a:1::/108` will be used.
  - The IPv6 subnet assigned to `--service-cidrs` can be no larger than a /108.

## Deploy the cluster

- [Azure CLI](#)
- [Azure Resource Manager](#)
- [Bicep](#)

Deploying a dual-stack cluster requires passing the `--ip-families` parameter with the parameter value of `ipv4,ipv6` to indicate that a dual-stack cluster should be created.

1. First, create a resource group to create the cluster in:

```
az group create -l <Region> -n <ResourceGroupName>
```

2. Then create the cluster itself:

```
az aks create -l <Region> -g <ResourceGroupName> -n <ClusterName> --ip-families ipv4,ipv6
```

Finally, after the cluster has been created, get the admin credentials:

```
az aks get-credentials -g <ResourceGroupName> -n <ClusterName> -a
```

## Inspect the nodes to see both IP families

Once the cluster is provisioned, confirm that the nodes are provisioned with dual-stack networking:

```
kubectl get nodes -o=custom-columns="NAME:.metadata.name,ADDRESSES:.status.addresses[?(@.type=='InternalIP')].address,PODCIDRS:.spec.podCIDRs[*]"
```

The output from the `kubectl get nodes` command will show that the nodes have addresses and pod IP assignment space from both IPv4 and IPv6.

NAME	ADDRESSES	PODCIDRS
aks-nodepool1-14508455-vmss000000	10.240.0.4,2001:1234:5678:9abc::4	10.244.0.0/24,fd12:3456:789a::/80
aks-nodepool1-14508455-vmss000001	10.240.0.5,2001:1234:5678:9abc::5	10.244.1.0/24,fd12:3456:789a:0:1::/80
aks-nodepool1-14508455-vmss000002	10.240.0.6,2001:1234:5678:9abc::6	10.244.2.0/24,fd12:3456:789a:0:2::/80

## Create an example workload

### Deploy an nginx web server

Once the cluster has been created, workloads can be deployed as usual. A simple example webserver can be created using the following command:

- [kubectl create](#)

- [YAML](#)

```
kubectl create deployment nginx --image=nginx:latest --replicas=3
```

Using the following `kubectl get pods` command will show that the pods have both IPv4 and IPv6 addresses (note that the pods will not show IP addresses until they are ready):

```
kubectl get pods -o custom-
columns="NAME:.metadata.name,IPs:.status.podIPs[*].ip,NODE:.spec.nodeName,READY:.status.conditions[?(@.type=='Ready')].status"
```

NAME	IPs	NODE	READY
nginx-55649fd747-9cr7h	10.244.2.2,fd12:3456:789a:0:2::2	aks-nodepool1-14508455-vmss000002	True
nginx-55649fd747-p5lr9	10.244.0.7,fd12:3456:789a::7	aks-nodepool1-14508455-vmss000000	True
nginx-55649fd747-r2rqh	10.244.1.2,fd12:3456:789a:0:1::2	aks-nodepool1-14508455-vmss000001	True

**Expose the workload via a `LoadBalancer`-type service**

**IMPORTANT**

There are currently two limitations pertaining to IPv6 services in AKS. These are both preview limitations and work is underway to remove them.

- Azure Load Balancer sends health probes to IPv6 destinations from a link-local address. This traffic cannot be routed to a pod and thus traffic flowing to IPv6 services deployed with `externalTrafficPolicy: Cluster` will fail. During preview, IPv6 services MUST be deployed with `externalTrafficPolicy: Local`, which causes `kube-proxy` to respond to the probe on the node, in order to function.
- Only the first IP address for a service will be provisioned to the load balancer, so a dual-stack service will only receive a public IP for its first listed IP family. In order to provide a dual-stack service for a single deployment, please create two services targeting the same selector, one for IPv4 and one for IPv6.

IPv6 services in Kubernetes can be exposed publicly similarly to an IPv4 service.

- [kubectl expose](#)
- [YAML](#)

```
kubectl expose deployment nginx --name=nginx-ipv4 --port=80 --type=LoadBalancer --overrides='{"spec": {"externalTrafficPolicy":"Local"}}'
kubectl expose deployment nginx --name=nginx-ipv6 --port=80 --type=LoadBalancer --overrides='{"spec": {"externalTrafficPolicy":"Local", "ipFamilies": ["IPv6"]}}'
```

```
service/nginx-ipv4 exposed
service/nginx-ipv6 exposed
```

Once the deployment has been exposed and the `LoadBalancer` services have been fully provisioned, `kubectl get services` will show the IP addresses of the services:

```
kubectl get services
```

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
nginx-ipv4	LoadBalancer	10.0.88.78	20.46.24.24	80:30652/TCP	97s
nginx-ipv6	LoadBalancer	fd12:3456:789a:1::981a	2603:1030:8:5::2d	80:32002/TCP	63s

Next, we can verify functionality via a command-line web request from an IPv6 capable host (note that Azure Cloud Shell is not IPv6 capable):

```
SERVICE_IP=$(kubectl get services nginx-ipv6 -o jsonpath='{.status.loadBalancer.ingress[0].ip}')
curl -s "http://[$SERVICE_IP]" | head -n5
```

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
```

# Configure Azure CNI networking in Azure Kubernetes Service (AKS)

10/27/2022 • 18 minutes to read • [Edit Online](#)

By default, AKS clusters use [kubenet](#), and a virtual network and subnet are created for you. With [kubenet](#), nodes get an IP address from a virtual network subnet. Network address translation (NAT) is then configured on the nodes, and pods receive an IP address "hidden" behind the node IP. This approach reduces the number of IP addresses that you need to reserve in your network space for pods to use.

With [Azure Container Networking Interface \(CNI\)](#), every pod gets an IP address from the subnet and can be accessed directly. These IP addresses must be unique across your network space, and must be planned in advance. Each node has a configuration parameter for the maximum number of pods that it supports. The equivalent number of IP addresses per node are then reserved up front for that node. This approach requires more planning, and often leads to IP address exhaustion or the need to rebuild clusters in a larger subnet as your application demands grow.

This article shows you how to use [Azure CNI](#) networking to create and use a virtual network subnet for an AKS cluster. For more information on network options and considerations, see [Network concepts for Kubernetes and AKS](#).

## Prerequisites

- The virtual network for the AKS cluster must allow outbound internet connectivity.
- AKS clusters may not use `169.254.0.0/16`, `172.30.0.0/16`, `172.31.0.0/16`, or `192.0.2.0/24` for the Kubernetes service address range, pod address range, or cluster virtual network address range.
- The cluster identity used by the AKS cluster must have at least [Network Contributor](#) permissions on the subnet within your virtual network. If you wish to define a [custom role](#) instead of using the built-in Network Contributor role, the following permissions are required:
  - `Microsoft.Network/virtualNetworks/subnets/join/action`
  - `Microsoft.Network/virtualNetworks/subnets/read`
- The subnet assigned to the AKS node pool cannot be a [delegated subnet](#).
- AKS doesn't apply Network Security Groups (NSGs) to its subnet and will not modify any of the NSGs associated with that subnet. If you provide your own subnet and add NSGs associated with that subnet, you must ensure the security rules in the NSGs allow traffic within the node CIDR range. For more details, see [Network security groups](#).

## Plan IP addressing for your cluster

Clusters configured with Azure CNI networking require additional planning. The size of your virtual network and its subnet must accommodate the number of pods you plan to run and the number of nodes for the cluster.

IP addresses for the pods and the cluster's nodes are assigned from the specified subnet within the virtual network. Each node is configured with a primary IP address. By default, 30 additional IP addresses are pre-configured by Azure CNI that are assigned to pods scheduled on the node. When you scale out your cluster, each node is similarly configured with IP addresses from the subnet. You can also view the [maximum pods per node](#).

## IMPORTANT

The number of IP addresses required should include considerations for upgrade and scaling operations. If you set the IP address range to only support a fixed number of nodes, you cannot upgrade or scale your cluster.

- When you **upgrade** your AKS cluster, a new node is deployed into the cluster. Services and workloads begin to run on the new node, and an older node is removed from the cluster. This rolling upgrade process requires a minimum of one additional block of IP addresses to be available. Your node count is then  $n + 1$ .
  - This consideration is particularly important when you use Windows Server node pools. Windows Server nodes in AKS do not automatically apply Windows Updates, instead you perform an upgrade on the node pool. This upgrade deploys new nodes with the latest Window Server 2019 base node image and security patches. For more information on upgrading a Windows Server node pool, see [Upgrade a node pool in AKS](#).
- When you **scale** an AKS cluster, a new node is deployed into the cluster. Services and workloads begin to run on the new node. Your IP address range needs to take into considerations how you may want to scale up the number of nodes and pods your cluster can support. One additional node for upgrade operations should also be included. Your node count is then  $n + \text{number-of-additional-scaled-nodes-you-anticipate} + 1$ .

If you expect your nodes to run the maximum number of pods, and regularly destroy and deploy pods, you should also factor in some additional IP addresses per node. These additional IP addresses take into consideration it may take a few seconds for a service to be deleted and the IP address released for a new service to be deployed and acquire the address.

The IP address plan for an AKS cluster consists of a virtual network, at least one subnet for nodes and pods, and a Kubernetes service address range.

ADDRESS RANGE / AZURE RESOURCE	LIMITS AND SIZING
Virtual network	The Azure virtual network can be as large as /8, but is limited to 65,536 configured IP addresses. Consider all your networking needs, including communicating with services in other virtual networks, before configuring your address space. For example, if you configure too large of an address space, you may run into issues with overlapping other address spaces within your network.

ADDRESS RANGE / AZURE RESOURCE	LIMITS AND SIZING
Subnet	<p>Must be large enough to accommodate the nodes, pods, and all Kubernetes and Azure resources that might be provisioned in your cluster. For example, if you deploy an internal Azure Load Balancer, its front-end IPs are allocated from the cluster subnet, not public IPs. The subnet size should also take into account upgrade operations or future scaling needs.</p> <p>To calculate the <i>minimum</i> subnet size including an additional node for upgrade operations:</p> <pre>(number of nodes + 1) + ((number of nodes + 1) * maximum pods per node that you configure)</pre> <p>Example for a 50 node cluster:</p> <pre>(51) + (51 * 30 (default)) = 1,581 (/21 or larger)</pre> <p>Example for a 50 node cluster that also includes provision to scale up an additional 10 nodes:</p> <pre>(61) + (61 * 30 (default)) = 1,891 (/21 or larger)</pre> <p>If you don't specify a maximum number of pods per node when you create your cluster, the maximum number of pods per node is set to 30. The minimum number of IP addresses required is based on that value. If you calculate your minimum IP address requirements on a different maximum value, see <a href="#">how to configure the maximum number of pods per node</a> to set this value when you deploy your cluster.</p>
Kubernetes service address range	This range should not be used by any network element on or connected to this virtual network. Service address CIDR must be smaller than /12. You can reuse this range across different AKS clusters.
Kubernetes DNS service IP address	IP address within the Kubernetes service address range that will be used by cluster service discovery. Don't use the first IP address in your address range. The first address in your subnet range is used for the <code>kubernetes.default.svc.cluster.local</code> address.
Docker bridge address	The Docker bridge network address represents the default <code>docker0</code> bridge network address present in all Docker installations. While <code>docker0</code> bridge is not used by AKS clusters or the pods themselves, you must set this address to continue to support scenarios such as <code>docker build</code> within the AKS cluster. It is required to select a CIDR for the Docker bridge network address because otherwise Docker will pick a subnet automatically, which could conflict with other CIDRs. You must pick an address space that does not collide with the rest of the CIDRs on your networks, including the cluster's service CIDR and pod CIDR. Default of 172.17.0.1/16. You can reuse this range across different AKS clusters.

## Maximum pods per node

The maximum number of pods per node in an AKS cluster is 250. The *default* maximum number of pods per node varies between *kubenet* and *Azure CNI* networking, and the method of cluster deployment.

DEPLOYMENT METHOD	KUBENET DEFAULT	AZURE CNI DEFAULT	CONFIGURABLE AT DEPLOYMENT
Azure CLI	110	30	Yes (up to 250)
Resource Manager template	110	30	Yes (up to 250)
Portal	110	110 (configurable in the Node Pools tab)	Yes (up to 250)

## Configure maximum - new clusters

You're able to configure the maximum number of pods per node at cluster deployment time or as you add new node pools. You can set the maximum pods per node value as high as 250.

If you don't specify maxPods when creating new node pools, you receive a default value of 30 for Azure CNI.

A minimum value for maximum pods per node is enforced to guarantee space for system pods critical to cluster health. The minimum value that can be set for maximum pods per node is 10 if and only if the configuration of each node pool has space for a minimum of 30 pods. For example, setting the maximum pods per node to the minimum of 10 requires each individual node pool to have a minimum of 3 nodes. This requirement applies for each new node pool created as well, so if 10 is defined as maximum pods per node each subsequent node pool added must have at least 3 nodes.

NETWORKING	MINIMUM	MAXIMUM
Azure CNI	10	250
Kubenet	10	250

### NOTE

The minimum value in the table above is strictly enforced by the AKS service. You can not set a maxPods value lower than the minimum shown as doing so can prevent the cluster from starting.

- **Azure CLI:** Specify the `--max-pods` argument when you deploy a cluster with the [az aks create](#) command. The maximum value is 250.
- **Resource Manager template:** Specify the `maxPods` property in the [ManagedClusterAgentPoolProfile](#) object when you deploy a cluster with a Resource Manager template. The maximum value is 250.
- **Azure portal:** Change the `Max pods per node` field in the node pool settings when creating a cluster or adding a new node pool.

## Configure maximum - existing clusters

The maxPod per node setting can be defined when you create a new node pool. If you need to increase the maxPod per node setting on an existing cluster, add a new node pool with the new desired maxPod count. After migrating your pods to the new pool, delete the older pool. To delete any older pool in a cluster, ensure you are setting node pool modes as defined in the [system node pools document](#).

## Deployment parameters

When you create an AKS cluster, the following parameters are configurable for Azure CNI networking:

**Virtual network:** The virtual network into which you want to deploy the Kubernetes cluster. If you want to create a new virtual network for your cluster, select *Create new* and follow the steps in the *Create virtual*

*network* section. If you want to select an existing virtual network, make sure it is in the same location and Azure subscription as your Kubernetes cluster. For information about the limits and quotas for an Azure virtual network, see [Azure subscription and service limits, quotas, and constraints](#).

**Subnet:** The subnet within the virtual network where you want to deploy the cluster. If you want to create a new subnet in the virtual network for your cluster, select *Create new* and follow the steps in the *Create subnet* section. For hybrid connectivity, the address range shouldn't overlap with any other virtual networks in your environment.

**Azure Network Plugin:** When Azure network plugin is used, the internal LoadBalancer service with "externalTrafficPolicy=Local" can't be accessed from VMs with an IP in clusterCIDR that does not belong to AKS cluster.

**Kubernetes service address range:** This parameter is the set of virtual IPs that Kubernetes assigns to internal [services](#) in your cluster. You can use any private address range that satisfies the following requirements:

- Must not be within the virtual network IP address range of your cluster
- Must not overlap with any other virtual networks with which the cluster virtual network peers
- Must not overlap with any on-premises IPs
- Must not be within the ranges `169.254.0.0/16`, `172.30.0.0/16`, `172.31.0.0/16`, or `192.0.2.0/24`

Although it's technically possible to specify a service address range within the same virtual network as your cluster, doing so is not recommended. Unpredictable behavior can result if overlapping IP ranges are used. For more information, see the [FAQ](#) section of this article. For more information on Kubernetes services, see [Services](#) in the Kubernetes documentation.

**Kubernetes DNS service IP address:** The IP address for the cluster's DNS service. This address must be within the *Kubernetes service address range*. Don't use the first IP address in your address range. The first address in your subnet range is used for the `kubernetes.default.svc.cluster.local` address.

**Docker Bridge address:** The Docker bridge network address represents the default `docker0` bridge network address present in all Docker installations. While `docker0` bridge is not used by AKS clusters or the pods themselves, you must set this address to continue to support scenarios such as `docker build` within the AKS cluster. It is required to select a CIDR for the Docker bridge network address because otherwise Docker will pick a subnet automatically which could conflict with other CIDRs. You must pick an address space that does not collide with the rest of the CIDRs on your networks, including the cluster's service CIDR and pod CIDR.

## Configure networking - CLI

When you create an AKS cluster with the Azure CLI, you can also configure Azure CNI networking. Use the following commands to create a new AKS cluster with Azure CNI networking enabled.

First, get the subnet resource ID for the existing subnet into which the AKS cluster will be joined:

```
$ az network vnet subnet list \
 --resource-group myVnet \
 --vnet-name myVnet \
 --query "[0].id" --output tsv

/subscriptions/<guid>/resourceGroups/myVnet/providers/Microsoft.Network/virtualNetworks/myVnet/subnets/defau
lt
```

Use the `az aks create` command with the `--network-plugin azure` argument to create a cluster with advanced networking. Update the `--vnet-subnet-id` value with the subnet ID collected in the previous step:

```
az aks create \
--resource-group myResourceGroup \
--name myAKSCluster \
--network-plugin azure \
--vnet-subnet-id <subnet-id> \
--docker-bridge-address 172.17.0.1/16 \
--dns-service-ip 10.2.0.10 \
--service-cidr 10.2.0.0/24 \
--generate-ssh-keys
```

## Configure networking - portal

The following screenshot from the Azure portal shows an example of configuring these settings during AKS cluster creation:

The screenshot shows the 'Networking' tab of the 'Create Kubernetes cluster' wizard. It includes the following sections:

- Network configuration:** A radio button group where 'Azure CNI' is selected. A note below explains that the Azure CNI plugin requires an IP address from the subnet for each pod, which can exhaust available IP addresses if a high value is set for pods per node.
- Virtual network:** A dropdown menu showing '(New) myResourceGroup-vnet' with a 'Create new' link.
- Cluster subnet:** A dropdown menu showing '(new) default (10.240.0.0/16)'.
- Kubernetes service address range:** A dropdown menu showing '10.0.0/16'.
- Kubernetes DNS service IP address:** A dropdown menu showing '10.0.0.10'.
- Docker Bridge address:** A dropdown menu showing '172.17.0.1/16'.

## Dynamic allocation of IPs and enhanced subnet support

A drawback with the traditional CNI is the exhaustion of pod IP addresses as the AKS cluster grows, resulting in the need to rebuild the entire cluster in a bigger subnet. The new dynamic IP allocation capability in Azure CNI solves this problem by allocating pod IPs from a subnet separate from the subnet hosting the AKS cluster. It offers the following benefits:

- Better IP utilization:** IPs are dynamically allocated to cluster Pods from the Pod subnet. This leads to better utilization of IPs in the cluster compared to the traditional CNI solution, which does static allocation of IPs for every node.
- Scalable and flexible:** Node and pod subnets can be scaled independently. A single pod subnet can be shared across multiple node pools of a cluster or across multiple AKS clusters deployed in the same VNet.

You can also configure a separate pod subnet for a node pool.

- **High performance:** Since pods are assigned VNet IPs, they have direct connectivity to other cluster pods and resources in the VNet. The solution supports very large clusters without any degradation in performance.
- **Separate VNet policies for pods:** Since pods have a separate subnet, you can configure separate VNet policies for them that are different from node policies. This enables many useful scenarios such as allowing internet connectivity only for pods and not for nodes, fixing the source IP for pod in a node pool using a VNet Network NAT, and using NSGs to filter traffic between node pools.
- **Kubernetes network policies:** Both the Azure Network Policies and Calico work with this new solution.

## Additional prerequisites

### NOTE

When using dynamic allocation of IPs, exposing an application as a Private Link Service using a Kubernetes Load Balancer Service is not supported.

The [prerequisites](#) already listed for Azure CNI still apply, but there are a few additional limitations:

- Only Linux node clusters and node pools are supported.
- AKS Engine and DIY clusters are not supported.
- Azure CLI version `2.37.0` or later.

## Planning IP addressing

When using this feature, planning is much simpler. Since the nodes and pods scale independently, their address spaces can also be planned separately. Since pod subnets can be configured to the granularity of a node pool, customers can always add a new subnet when they add a node pool. The system pods in a cluster/node pool also receive IPs from the pod subnet, so this behavior needs to be accounted for.

IPs are allocated to nodes in batches of 16. Pod subnet IP allocation should be planned with a minimum of 16 IPs per node in the cluster; nodes will request 16 IPs on startup and will request another batch of 16 any time there are <8 IPs unallocated in their allotment.

The planning of IPs for Kubernetes services and Docker bridge remain unchanged.

## Maximum pods per node in a cluster with dynamic allocation of IPs and enhanced subnet support

The pods per node values when using Azure CNI with dynamic allocation of IPs have changed slightly from the traditional CNI behavior:

CNI	DEFAULT	CONFIGURABLE AT DEPLOYMENT
Traditional Azure CNI	30	Yes (up to 250)
Azure CNI with dynamic allocation of IPs	250	Yes (up to 250)

All other guidance related to configuring the maximum nodes per pod remains the same.

## Additional deployment parameters

The deployment parameters described above are all still valid, with one exception:

- The **subnet** parameter now refers to the subnet related to the cluster's nodes.
- An additional parameter **pod subnet** is used to specify the subnet whose IP addresses will be dynamically allocated to pods.

## Configure networking - CLI with dynamic allocation of IPs and enhanced subnet support

Using dynamic allocation of IPs and enhanced subnet support in your cluster is similar to the default method for configuring a cluster Azure CNI. The following example walks through creating a new virtual network with a subnet for nodes and a subnet for pods, and creating a cluster that uses Azure CNI with dynamic allocation of IPs and enhanced subnet support. Be sure to replace variables such as `$subscription` with your own values:

First, create the virtual network with two subnets:

```
resourceGroup="myResourceGroup"
vnet="myVirtualNetwork"
location="westcentralus"

Create the resource group
az group create --name $resourceGroup --location $location

Create our two subnet network
az network vnet create -g $resourceGroup --location $location --name $vnet --address-prefixes 10.0.0.0/8 -o none
az network vnet subnet create -g $resourceGroup --vnet-name $vnet --name nodesubnet --address-prefixes 10.240.0.0/16 -o none
az network vnet subnet create -g $resourceGroup --vnet-name $vnet --name podsubnet --address-prefixes 10.241.0.0/16 -o none
```

Then, create the cluster, referencing the node subnet using `--vnet-subnet-id` and the pod subnet using `--pod-subnet-id`:

```
clusterName="myAKSCluster"
subscription="aaaaaaaa-aaaaa-aaaaaa-aaaa"

az aks create -n $clusterName -g $resourceGroup -l $location \
--max-pods 250 \
--node-count 2 \
--network-plugin azure \
--vnet-subnet-id
/subscriptions/$subscription/resourceGroups/$resourceGroup/providers/Microsoft.Network/virtualNetworks/$vnet
/subnets/nodesubnet \
--pod-subnet-id
/subscriptions/$subscription/resourceGroups/$resourceGroup/providers/Microsoft.Network/virtualNetworks/$vnet
/subnets/podsubnet
```

### Adding node pool

When adding node pool, reference the node subnet using `--vnet-subnet-id` and the pod subnet using `--pod-subnet-id`. The following example creates two new subnets that are then referenced in the creation of a new node pool:

```
az network vnet subnet create -g $resourceGroup --vnet-name $vnet --name node2subnet --address-prefixes 10.242.0.0/16 -o none
az network vnet subnet create -g $resourceGroup --vnet-name $vnet --name pod2subnet --address-prefixes 10.243.0.0/16 -o none

az aks nodepool add --cluster-name $clusterName -g $resourceGroup -n newnodepool \
--max-pods 250 \
--node-count 2 \
--vnet-subnet-id
/subscriptions/$subscription/resourceGroups/$resourceGroup/providers/Microsoft.Network/virtualNetworks/$vnet
/subnets/node2subnet \
--pod-subnet-id
/subscriptions/$subscription/resourceGroups/$resourceGroup/providers/Microsoft.Network/virtualNetworks/$vnet
/subnets/pod2subnet \
--no-wait
```

# Frequently asked questions

The following questions and answers apply to the Azure CNI networking configuration.

- *Can I deploy VMs in my cluster subnet?*

Yes.

- *What source IP do external systems see for traffic that originates in an Azure CNI-enabled pod?*

Systems in the same virtual network as the AKS cluster see the pod IP as the source address for any traffic from the pod. Systems outside the AKS cluster virtual network see the node IP as the source address for any traffic from the pod.

- *Can I configure per-pod network policies?*

Yes, Kubernetes network policy is available in AKS. To get started, see [Secure traffic between pods by using network policies in AKS](#).

- *Is the maximum number of pods deployable to a node configurable?*

Yes, when you deploy a cluster with the Azure CLI or a Resource Manager template. See [Maximum pods per node](#).

You can't change the maximum number of pods per node on an existing cluster.

- *How do I configure additional properties for the subnet that I created during AKS cluster creation? For example, service endpoints.*

The complete list of properties for the virtual network and subnets that you create during AKS cluster creation can be configured in the standard virtual network configuration page in the Azure portal.

- *Can I use a different subnet within my cluster virtual network for the Kubernetes service address range?*

It's not recommended, but this configuration is possible. The service address range is a set of virtual IPs (VIPs) that Kubernetes assigns to internal services in your cluster. Azure Networking has no visibility into the service IP range of the Kubernetes cluster. Because of the lack of visibility into the cluster's service address range, it's possible to later create a new subnet in the cluster virtual network that overlaps with the service address range. If such an overlap occurs, Kubernetes could assign a service an IP that's already in use by another resource in the subnet, causing unpredictable behavior or failures. By ensuring you use an address range outside the cluster's virtual network, you can avoid this overlap risk.

## Dynamic allocation of IP addresses and enhanced subnet support FAQs

The following questions and answers apply to the Azure CNI network configuration when using [Dynamic allocation of IP addresses and enhanced subnet support](#).

- *Can I assign multiple pod subnets to a cluster/node pool?*

Only one subnet can be assigned to a cluster or node pool. However, multiple clusters or node pools can share a single subnet.

- *Can I assign Pod subnets from a different VNet altogether?*

No, the pod subnet should be from the same VNet as the cluster.

- *Can some node pools in a cluster use the traditional CNI while others use the new CNI?*

The entire cluster should use only one type of CNI.

## Next steps

Learn more about networking in AKS in the following articles:

- [Use a static IP address with the Azure Kubernetes Service \(AKS\) load balancer](#)
- [Use an internal load balancer with Azure Container Service \(AKS\)](#)
- [Create a basic ingress controller with external network connectivity](#)
- [Enable the HTTP application routing add-on](#)
- [Create an ingress controller that uses an internal, private network and IP address](#)
- [Create an ingress controller with a dynamic public IP and configure Let's Encrypt to automatically generate TLS certificates](#)
- [Create an ingress controller with a static public IP and configure Let's Encrypt to automatically generate TLS certificates](#)

# Configure Azure CNI Overlay networking in Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

The traditional [Azure Container Networking Interface \(CNI\)](#) assigns a VNet IP address to every Pod either from a pre-reserved set of IPs on every node or from a separate subnet reserved for pods. This approach requires IP address planning and could lead to address exhaustion and difficulties in scaling your clusters as your application demands grow.

With Azure CNI Overlay, the cluster nodes are deployed into an Azure Virtual Network subnet, whereas pods are assigned IP addresses from a private CIDR logically different from the VNet hosting the nodes. Pod and node traffic within the cluster use an overlay network, and Network Address Translation (via the node's IP address) is used to reach resources outside the cluster. This solution saves a significant amount of VNet IP addresses and enables you to seamlessly scale your cluster to very large sizes. An added advantage is that the private CIDR can be reused in different AKS clusters, truly extending the IP space available for containerized applications in AKS.

## NOTE

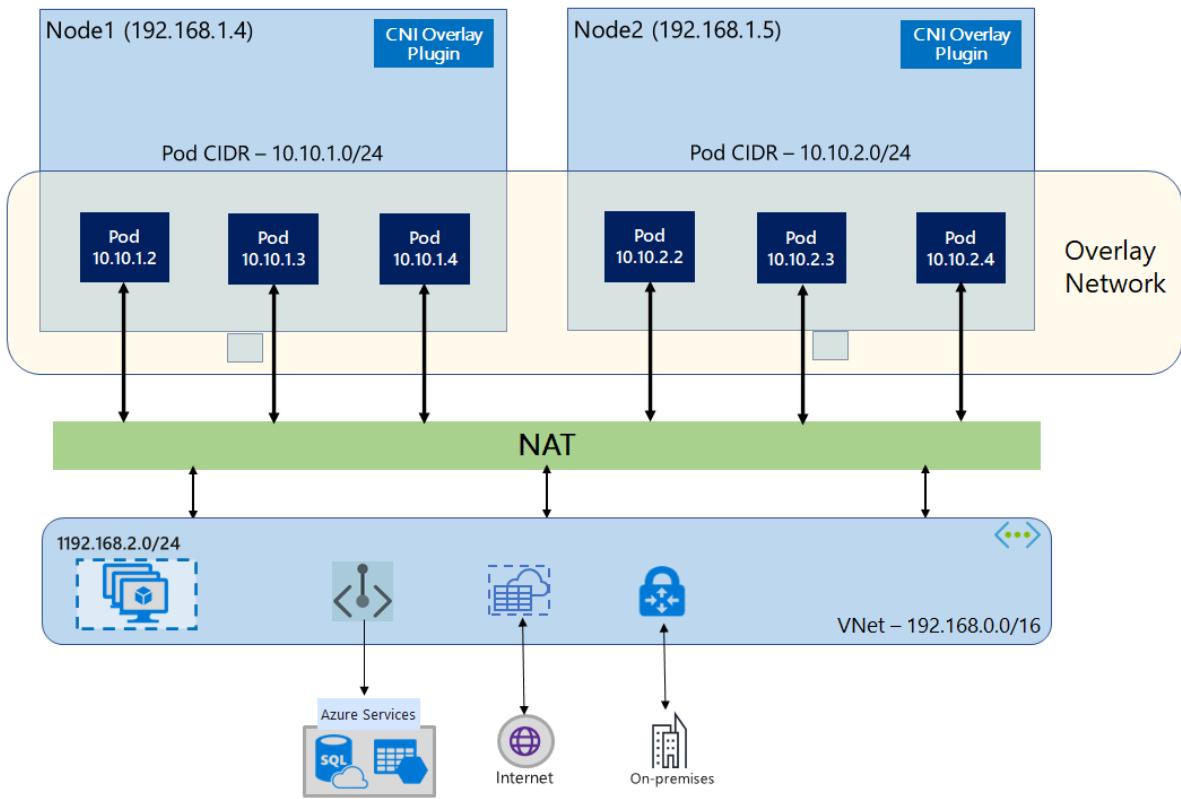
Azure CNI Overlay is currently available in the following regions:

- North Central US
- West Central US

## Overview of overlay networking

In overlay networking, only the Kubernetes cluster nodes are assigned IPs from a subnet. Pods receive IPs from a private CIDR that is provided at the time of cluster creation. Each node is assigned a /24 address space carved out from the same CIDR. Additional nodes that are created when you scale out a cluster automatically receive /24 address spaces from the same CIDR. Azure CNI assigns IPs to pods from this /24 space.

A separate routing domain is created in the Azure Networking stack for the pod's private CIDR space, which creates an overlay network for direct communication between pods. There is no need to provision custom routes on the cluster subnet or use an encapsulation method to tunnel traffic between pods. This provides connectivity performance between pods on par with VMs in a VNet.



Communication with endpoints outside the cluster, such as on-premises and peered VNets, happens using the node IP through Network Address Translation. Azure CNI translates the source IP (overlay IP of the pod) of the traffic to the primary IP address of the VM, which enables the Azure Networking stack to route the traffic to the destination. Endpoints outside the cluster can't connect to a pod directly. You will have to publish the pod's application as a Kubernetes Load Balancer service to make it reachable on the VNet.

Outbound (egress) connectivity to the internet for overlay pods can be provided using a [Standard SKU Load Balancer](#) or [Managed NAT Gateway](#). You can also control egress traffic by directing it to a firewall using [User Defined Routes on the cluster subnet](#).

Ingress connectivity to the cluster can be achieved using an ingress controller such as Nginx or [HTTP application routing](#).

## Difference between Kubenet and Azure CNI Overlay

Like Azure CNI Overlay, Kubenet assigns IP addresses to pods from an address space logically different from the VNet but has scaling and other limitations. The below table provides a detailed comparison between Kubenet and Azure CNI Overlay. If you do not want to assign VNet IP addresses to pods due to IP shortage, then Azure CNI Overlay is the recommended solution.

AREA	AZURE CNI OVERLAY	KUBENET
Cluster scale	1000 nodes and 250 pods/node	400 nodes and 250 pods/node
Network configuration	Simple - no additional configuration required for pod networking	Complex - requires route tables and UDRs on cluster subnet for pod networking
Pod connectivity performance	Performance on par with VMs in a VNet	Additional hop adds minor latency
Kubernetes Network Policies	Azure Network Policies, Calico	Calico

AREA	AZURE CNI OVERLAY	KUBENET
OS platforms supported	Linux only	Linux only

## IP address planning

- **Cluster Nodes:** Cluster nodes go into a subnet in your VNet, so ensure that you have a subnet big enough to account for future scale. A simple `/24` subnet can host up to 251 nodes (the first three IP addresses in a subnet are reserved for management operations).
- **Pods:** The overlay solution assigns a `/24` address space for pods on every node from the private CIDR that you specify during cluster creation. The `/24` size is fixed and can't be increased or decreased. You can run up to 250 pods on a node. When planning the pod address space, ensure that the private CIDR is large enough to provide `/24` address spaces for new nodes to support future cluster expansion. The following are additional factors to consider when planning pod address space:
  - Pod CIDR space must not overlap with the cluster subnet range.
  - Pod CIDR space must not overlap with IP ranges used in on-premises networks and peered networks.
  - The same pod CIDR space can be used on multiple independent AKS clusters in the same VNet.
- **Kubernetes service address range:** The size of the service address CIDR depends on the number of cluster services you plan to create. It must be smaller than `/12`. This range should also not overlap with the pod CIDR range, cluster subnet range, and IP range used in peered VNets and on-premises networks.
- **Kubernetes DNS service IP address:** This is an IP address within the Kubernetes service address range that will be used by cluster service discovery. Don't use the first IP address in your address range. The first address in your subnet range is used for the `kubernetes.default.svc.cluster.local` address.

## Maximum pods per node

You can configure the maximum number of pods per node at the time of cluster creation or when you add a new node pool. The default for Azure CNI Overlay is 30. The maximum value that you can specify in Azure CNI Overlay is 250, and the minimum value is 10. The maximum pods per node value configured during creation of a node pool applies to the nodes in that node pool only.

## Choosing a network model to use

Azure CNI offers two IP addressing options for pods- the traditional configuration that assigns VNet IPs to pods, and overlay networking. The choice of which option to use for your AKS cluster is a balance between flexibility and advanced configuration needs. The following considerations help outline when each network model may be the most appropriate.

Use overlay networking when:

- You would like to scale to a large number of Pods but have limited IP address space in your VNet.
- Most of the pod communication is within the cluster.
- You don't need advanced AKS features, such as virtual nodes.

Use the traditional VNet option when:

- You have available IP address space.
- Most of the pod communication is to resources outside of the cluster.
- Resources outside the cluster need to reach pods directly.

- You need AKS advanced features, such as virtual nodes.

## Limitations with Azure CNI Overlay

The overlay solution has the following limitations today

- Only available for Linux and not for Windows.
- You can't deploy multiple overlay clusters in the same subnet.
- Overlay can be enabled only for new clusters. Existing (already deployed) clusters can't be configured to use overlay.
- You can't use Application Gateway as an Ingress Controller (AGIC) for an overlay cluster.
- v5 VM SKUs are not currently supported.

## Steps to set up overlay clusters

### IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

The following example walks through the steps to create a new virtual network with a subnet for the cluster nodes and an AKS cluster that uses Azure CNI Overlay. Be sure to replace the variables with your own values.

First, opt into the feature by running the following command:

```
az feature register --namespace Microsoft.ContainerService --name AzureOverlayPreview
```

Create a virtual network with a subnet for the cluster nodes.

```
resourceGroup="myResourceGroup"
vnet="myVirtualNetwork"
location="westcentralus"

Create the resource group
az group create --name $resourceGroup --location $location

Create a VNet and a subnet for the cluster nodes
az network vnet create -g $resourceGroup --location $location --name $vnet --address-prefixes 10.0.0.0/8 -o none
az network vnet subnet create -g $resourceGroup --vnet-name $vnet --name nodesubnet --address-prefix 10.10.0.0/16 -o none
```

Create a cluster with Azure CNI Overlay. Use `--network-plugin-mode` to specify that this is an overlay cluster. If the pod CIDR is not specified then AKS assigns a default space, viz. 10.244.0.0/16.

```
clusterName="myOverlayCluster"
subscription="aaaaaaaa-aaaaa-aaaaaa-aaaa"

az aks create -n $clusterName -g $resourceGroup --location $location --network-plugin azure --network-
plugin-mode overlay --pod-cidr 192.168.0.0/16 --vnet-subnet-id
/subscriptions/$subscription/resourceGroups/$resourceGroup/providers/Microsoft.Network/virtualNetworks/$vnet
/subnets/nodesubnet
```

## Frequently asked questions

- *How do pods and cluster nodes communicate with each other?*

Pods and nodes talk to each other directly without any SNAT requirements.

- *Can I configure the size of the address space assigned to each space?*

No, this is fixed at `/24` today and can't be changed.

- *Can I add more private pod CIDRs to a cluster after the cluster has been created?*

No, a private pod CIDR can only be specified at the time of cluster creation.

- *What are the max nodes and pods per cluster supported by Azure CNI Overlay?*

The max scale in terms of nodes and pods per cluster is the same as the max limits supported by AKS today.

# Create an Azure Kubernetes Service cluster with API Server VNet Integration (PREVIEW)

10/27/2022 • 6 minutes to read • [Edit Online](#)

An Azure Kubernetes Service (AKS) cluster with API Server VNet Integration configured projects the API server endpoint directly into a delegated subnet in the VNet where AKS is deployed. This enables network communication between the API server and the cluster nodes without any required private link or tunnel. The API server will be available behind an Internal Load Balancer VIP in the delegated subnet, which the nodes will be configured to utilize. By using API Server VNet Integration, you can ensure network traffic between your API server and your node pools remains on the private network only.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## API server connectivity

The control plane or API server is in an Azure Kubernetes Service (AKS)-managed Azure subscription. A customer's cluster or node pool is in the customer's subscription. The server and the virtual machines that make up the cluster nodes can communicate with each other through the API server VIP and pod IPs that are projected into the delegated subnet.

API Server VNet Integration is supported for public or private clusters, and public access can be added or removed after cluster provisioning. Unlike non-VNet integrated clusters, the agent nodes always communicate directly with the private IP address of the API Server Internal Load Balancer (ILB) IP without using DNS. All node to API server traffic is kept on private networking and no tunnel is required for API server to node connectivity. Out-of-cluster clients needing to communicate with the API server can do so normally if public network access is enabled. If public network access is disabled, they should follow the same private DNS setup methodology as standard [private clusters](#).

## Region availability

API Server VNet Integration is available in the following regions at this time:

- eastus2
- northcentralus
- westcentralus
- westus2

## Prerequisites

- Azure CLI with aks-preview extension 0.5.97 or later.
- If using ARM or the REST API, the AKS API version must be 2022-04-02-preview or later.

## Install the aks-preview CLI extension

```
Install the aks-preview extension
az extension add --name aks-preview

Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

### Register the `EnableAPIServerVnetIntegrationPreview` preview feature

To create an AKS cluster with API Server VNet Integration, you must enable the `EnableAPIServerVnetIntegrationPreview` feature flag on your subscription.

Register the `EnableAPIServerVnetIntegrationPreview` feature flag by using the `az feature register` command, as shown in the following example:

```
az feature register --namespace "Microsoft.ContainerService" --name "EnableAPIServerVnetIntegrationPreview"
```

It takes a few minutes for the status to show *Registered*. Verify the registration status by using the `az feature list` command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/EnableAPIServerVnetIntegrationPreview')].{Name:name, State:properties.state}"
```

When the feature has been registered, refresh the registration of the *Microsoft.ContainerService* resource provider by using the `az provider register` command:

```
az provider register --namespace Microsoft.ContainerService
```

## Create an AKS cluster with API Server VNet Integration using Managed VNet

AKS clusters with API Server VNet Integration can be configured in either managed VNet or bring-your-own VNet mode. They can be created as either public clusters (with API server access available via a public IP) or private clusters (where the API server is only accessible via private VNet connectivity), and can be toggled between these two states without redeploying.

### Create a resource group

Create a resource group or use an existing resource group for your AKS cluster.

```
az group create -l westus2 -n <resource-group>
```

### Deploy a public cluster

```
az aks create -n <cluster-name> \
-g <resource-group> \
-l <location> \
--network-plugin azure \
--enable-apiserver-vnet-integration
```

The `--enable-apiserver-vnet-integration` flag configures API Server VNet integration for Managed VNet mode.

### Deploy a private cluster

```
az aks create -n <cluster-name> \
-g <resource-group> \
-l <location> \
--network-plugin azure \
--enable-private-cluster \
--enable-apiserver-vnet-integration
```

The `--enable-private-cluster` flag is mandatory for a private cluster, and `--enable-apiserver-vnet-integration` configures API Server VNet integration for Managed VNet mode.

## Create an AKS Private cluster with API Server VNet Integration using bring-your-own VNet

When using bring-your-own VNet, an API server subnet must be created and delegated to `Microsoft.ContainerService/managedClusters`. This grants the AKS service permissions to inject the API server pods and internal load balancer into that subnet. The subnet may not be used for any other workloads, but may be used for multiple AKS clusters located in the same virtual network. An AKS cluster will require from 2-7 IP addresses depending on cluster scale. The minimum supported API server subnet size is a /28.

Note that the cluster identity needs permissions to both the API server subnet and the node subnet. Lack of permissions at the API server subnet will cause a provisioning failure.

### WARNING

Running out of IP addresses may prevent API server scaling and cause an API server outage.

### Create a resource group

Create a resource group or use an existing resource group for your AKS cluster.

```
az group create -l <location> -n <resource-group>
```

### Create a virtual network

```
Create the virtual network
az network vnet create -n <vnet-name> \
-l <location> \
--address-prefixes 172.19.0.0/16

Create an API server subnet
az network vnet subnet create --vnet-name <vnet-name> \
--name <apiserver-subnet-name> \
--delegations Microsoft.ContainerService/managedClusters \
--address-prefixes 172.19.0.0/28

Create a cluster subnet
az network vnet subnet create --vnet-name <vnet-name> \
--name <cluster-subnet-name> \
--address-prefixes 172.19.1.0/24
```

### Create a managed identity and give it permissions on the virtual network

```
Create the identity
az identity create -n <managed-identity-name> -l <location>

Assign Network Contributor to the API server subnet
az role assignment create --scope <apiserver-subnet-resource-id> \
 --role "Network Contributor" \
 --assignee <managed-identity-client-id>

Assign Network Contributor to the cluster subnet
az role assignment create --scope <cluster-subnet-resource-id> \
 --role "Network Contributor" \
 --assignee <managed-identity-client-id>
```

## Deploy a public cluster

```
az aks create -n <cluster-name> \
 -g <resource-group> \
 -l <location> \
 --network-plugin azure \
 --enable-apiserver-vnet-integration \
 --vnet-subnet-id <cluster-subnet-resource-id> \
 --apiserver-subnet-id <apiserver-subnet-resource-id> \
 --assign-identity <managed-identity-resource-id>
```

## Deploy a private cluster

```
az aks create -n <cluster-name> \
 -g <resource-group> \
 -l <location> \
 --network-plugin azure \
 --enable-private-cluster \
 --enable-apiserver-vnet-integration \
 --vnet-subnet-id <cluster-subnet-resource-id> \
 --apiserver-subnet-id <apiserver-subnet-resource-id> \
 --assign-identity <managed-identity-resource-id>
```

## Convert an existing AKS cluster to API Server VNet Integration

Existing AKS public clusters can be converted to API Server VNet Integration clusters by supplying an API server subnet that meets the requirements above (in the same VNet as the cluster nodes, permissions granted for the AKS cluster identity, and size of at least /28). This is a one-way migration; clusters cannot have API Server VNet Integration disabled after it has been enabled.

This upgrade will perform a node-image version upgrade on all node pools - all workloads will be restarted as all nodes will undergo a rolling image upgrade.

### WARNING

Converting a cluster to API Server VNet Integration will result in a change of the API Server IP address, though the hostname will remain the same. If the IP address of the API server has been configured in any firewalls or network security group rules, those rules may need to be updated.

```
az aks update -n <cluster-name> \
 -g <resource-group> \
 --enable-apiserver-vnet-integration \
 --apiserver-subnet-id <apiserver-subnet-resource-id>
```

# Enable or disable private cluster mode on an existing cluster with API Server VNet Integration

AKS clusters configured with API Server VNet Integration can have public network access/private cluster mode enabled or disabled without redeploying the cluster. The API server hostname will not change, but public DNS entries will be modified or removed as appropriate.

## Enable private cluster mode

```
az aks update -n <cluster-name> \
 -g <resource-group> \
 --enable-private-cluster
```

## Disable private cluster mode

```
az aks update -n <cluster-name> \
 -g <resource-group> \
 --disable-private-cluster
```

## Limitations

- Existing AKS private clusters cannot be converted to API Server VNet Integration clusters at this time.
- [Private Link Service](#) will not work if deployed against the API Server injected addresses at this time, so the API server cannot be exposed to other virtual networks via private link. To access the API server from outside the cluster network, utilize either [VNet peering](#) or [AKS run command](#).

# Bring your own Container Network Interface (CNI) plugin with Azure Kubernetes Service (AKS)

10/27/2022 • 3 minutes to read • [Edit Online](#)

Kubernetes does not provide a network interface system by default; this functionality is provided by [network plugins](#). Azure Kubernetes Service provides several supported CNI plugins. Documentation for supported plugins can be found from the [networking concepts page](#).

While the supported plugins meet most networking needs in Kubernetes, advanced users of AKS may desire to utilize the same CNI plugin used in on-premises Kubernetes environments or to make use of specific advanced functionality available in other CNI plugins.

This article shows how to deploy an AKS cluster with no CNI plugin pre-installed, which allows for installation of any third-party CNI plugin that works in Azure.

## Support

BYOCNI has support implications - Microsoft support will not be able to assist with CNI-related issues in clusters deployed with BYOCNI. For example, CNI-related issues would cover most east/west (pod to pod) traffic, along with `kubectl proxy` and similar commands. If CNI-related support is desired, a supported AKS network plugin can be used or support could be procured for the BYOCNI plugin from a third-party vendor.

Support will still be provided for non-CNI-related issues.

## Prerequisites

- For ARM/Bicep, use at least template version 2022-01-02-preview or 2022-06-01
- For Azure CLI, use at least version 2.39.0
- The virtual network for the AKS cluster must allow outbound internet connectivity.
- AKS clusters may not use `169.254.0.0/16`, `172.30.0.0/16`, `172.31.0.0/16`, or `192.0.2.0/24` for the Kubernetes service address range, pod address range, or cluster virtual network address range.
- The cluster identity used by the AKS cluster must have at least [Network Contributor](#) permissions on the subnet within your virtual network. If you wish to define a [custom role](#) instead of using the built-in Network Contributor role, the following permissions are required:
  - `Microsoft.Network/virtualNetworks/subnets/join/action`
  - `Microsoft.Network/virtualNetworks/subnets/read`
- The subnet assigned to the AKS node pool cannot be a [delegated subnet](#).
- AKS doesn't apply Network Security Groups (NSGs) to its subnet and will not modify any of the NSGs associated with that subnet. If you provide your own subnet and add NSGs associated with that subnet, you must ensure the security rules in the NSGs allow traffic within the node CIDR range. For more details, see [Network security groups](#).

## Cluster creation steps

### Deploy a cluster

- [Azure CLI](#)
- [Azure Resource Manager](#)
- [Bicep](#)

Deploying a BYOCNI cluster requires passing the `--network-plugin` parameter with the parameter value of `none`.

1. First, create a resource group to create the cluster in:

```
az group create -l <Region> -n <ResourceGroupName>
```

2. Then create the cluster itself:

```
az aks create -l <Region> -g <ResourceGroupName> -n <ClusterName> --network-plugin none
```

## Deploy a CNI plugin

When AKS provisioning completes, the cluster will be online, but all of the nodes will be in a `NotReady` state:

```
$ kubectl get nodes
NAME STATUS ROLES AGE VERSION
aks-nodepool1-23902496-vmss000000 NotReady agent 6m9s v1.21.9

$ kubectl get node -o custom-columns='NAME:.metadata.name,STATUS:.status.conditions[?(@.type=="Ready")].message'
NAME STATUS
aks-nodepool1-23902496-vmss000000 container runtime network not ready: NetworkReady=false
reason:NetworkPluginNotReady message:Network plugin returns error: cni plugin not initialized
```

At this point, the cluster is ready for installation of a CNI plugin.

## Next steps

Learn more about networking in AKS in the following articles:

- [Use a static IP address with the Azure Kubernetes Service \(AKS\) load balancer](#)
- [Use an internal load balancer with Azure Container Service \(AKS\)](#)
- [Create a basic ingress controller with external network connectivity](#)
- [Enable the HTTP application routing add-on](#)
- [Create an ingress controller that uses an internal, private network and IP address](#)
- [Create an ingress controller with a dynamic public IP and configure Let's Encrypt to automatically generate TLS certificates](#)
- [Create an ingress controller with a static public IP and configure Let's Encrypt to automatically generate TLS certificates](#)

# Configure Azure CNI Powered by Cilium in Azure Kubernetes Service (AKS) (Preview)

10/27/2022 • 4 minutes to read • [Edit Online](#)

Azure CNI Powered by Cilium combines the robust control plane of Azure CNI with the dataplane of [Cilium](#) to provide high-performance networking and security.

By making use of eBPF programs loaded into the Linux kernel and a more efficient API object structure, Azure CNI Powered by Cilium provides the following benefits:

- Functionality equivalent to existing Azure CNI and Azure CNI Overlay plugins
- Faster service routing
- More efficient network policy enforcement
- Better observability of cluster traffic
- Support for larger clusters (more nodes, pods, and services)

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## IP Address Management (IPAM) with Azure CNI Powered by Cilium

Azure CNI Powered by Cilium can be deployed using two different methods for assigning pod IPs:

- assign IP addresses from a VNet (similar to existing Azure CNI with Dynamic Pod IP Assignment)
- assign IP addresses from an overlay network (similar to Azure CNI Overlay mode)

## NOTE

Azure CNI Overlay networking currently requires the `Microsoft.ContainerService/AzureOverlayPreview` feature and may be available only in certain regions. For more information, see [Azure CNI Overlay networking](#).

If you aren't sure which option to select, read "[Choosing a network model to use](#)".

## Network Policy Enforcement

Cilium enforces [network policies to allow or deny traffic between pods](#). With Cilium, you don't need to install a separate network policy engine such as Azure Network Policy Manager or Calico.

## Limitations

Azure CNI powered by Cilium currently has the following limitations:

- Available only for new clusters.
- Available only for Linux and not for Windows.
- Cilium L7 policy enforcement is disabled.
- Hubble is disabled.
- Kubernetes services with `internalTrafficPolicy=Local` aren't supported ([Cilium issue #17796](#)).
- Multiple Kubernetes services can't use the same host port with different protocols (for example, TCP or UDP) ([Cilium issue #14287](#)).
- Network policies may be enforced on reply packets when a pod connects to itself via service cluster IP ([Cilium issue #19406](#)).

## Prerequisites

- Azure CLI version 2.41.0 or later. Run `az --version` to see the currently installed version. If you need to install or upgrade, see [Install Azure CLI][/cli/azure/install-azure-cli].
- Azure CLI with aks-preview extension 0.5.109 or later.
- If using ARM templates or the REST API, the AKS API version must be 2022-09-02-preview or later.

### Install the aks-preview CLI extension

```
Install the aks-preview extension
az extension add --name aks-preview

Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

### Register the `CiliumDataPlanePreview` preview feature

To create an AKS cluster with Azure CNI powered by Cilium, you must enable the `CiliumDataPlanePreview` feature flag on your subscription.

Register the `CiliumDataPlanePreview` feature flag by using the `az feature register` command, as shown in the following example:

```
az feature register --namespace "Microsoft.ContainerService" --name "CiliumDataPlanePreview"
```

It takes a few minutes for the status to show *Registered*. Verify the registration status by using the `az feature list` command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/CiliumDataPlanePreview')].{Name:name, State:properties.state}"
```

When the feature has been registered, refresh the registration of the *Microsoft.ContainerService* resource provider by using the `az provider register` command:

```
az provider register --namespace Microsoft.ContainerService
```

## Create a new AKS Cluster with Azure CNI Powered by Cilium

### Option 1: Assign IP addresses from a VNet

Run the following commands to create a resource group and VNet with a subnet for nodes and a subnet for pods.

```
Create the resource group
az group create --name <resourceGroupName> --location <location>
```

```
Create a VNet with a subnet for nodes and a subnet for pods
az network vnet create -g <resourceGroupName> --location <location> --name <vnetName> --address-prefixes
<address prefix, example: 10.0.0.0/8> -o none
az network vnet subnet create -g <resourceGroupName> --vnet-name <vnetName> --name nodesubnet --address-
prefixes <address prefix, example: 10.240.0.0/16> -o none
az network vnet subnet create -g <resourceGroupName> --vnet-name <vnetName> --name podsubnet --address-
prefixes <address prefix, example: 10.241.0.0/16> -o none
```

Create the cluster using `--enable-cilium-dataplane`:

```
az aks create -n <clusterName> -g <resourceGroupName> -l <location> \
--max-pods 250 \
--node-count 2 \
--network-plugin azure \
--vnet-subnet-id
/subscriptions/<subscriptionId>/resourceGroups/<resourceGroupName>/providers/Microsoft.Network/virtualNetwor
ks/<vnetName>/subnets/nodesubnet \
--pod-subnet-id
/subscriptions/<subscriptionId>/resourceGroups/<resourceGroupName>/providers/Microsoft.Network/virtualNetwor
ks/<vnetName>/subnets/podsubnet \
--enable-cilium-dataplane
```

## Option 2: Assign IP addresses from an overlay network

Run these commands to create a resource group and VNet with a single subnet:

```
Create the resource group
az group create --name <resourceGroupName> --location <location>
```

```
Create a VNet with a subnet for nodes and a subnet for pods
az network vnet create -g <resourceGroupName> --location <location> --name <vnetName> --address-prefixes
<address prefix, example: 10.0.0.0/8> -o none
az network vnet subnet create -g <resourceGroupName> --vnet-name <vnetName> --name nodesubnet --address-
prefixes <address prefix, example: 10.240.0.0/16> -o none
```

Then create the cluster using `--enable-cilium-dataplane`:

```
az aks create -n <clusterName> -g <resourceGroupName> -l <location> \
--max-pods 250 \
--node-count 2 \
--network-plugin azure \
--network-plugin-mode overlay \
--pod-cidr 192.168.0.0/16 \
--vnet-subnet-id
/subscriptions/<subscriptionId>/resourceGroups/<resourceGroupName>/providers/Microsoft.Network/virtualNetwor
ks/<vnetName>/subnets/nodesubnet \
--enable-cilium-dataplane
```

## Frequently asked questions

- *Can I customize Cilium configuration?*

No, the Cilium configuration is managed by AKS and can't be modified. We recommend that customers

who require more control use AKS BYO CNI and install Cilium manually.

- *Can I use `ciliumNetworkPolicy` custom resources instead of Kubernetes `NetworkPolicy` resources?*

`ciliumNetworkPolicy` custom resources aren't officially supported. We recommend that customers use Kubernetes `NetworkPolicy` resources to configure network policies.

## Next steps

Learn more about networking in AKS in the following articles:

- [Use a static IP address with the Azure Kubernetes Service \(AKS\) load balancer](#)
- [Use an internal load balancer with Azure Container Service \(AKS\)](#)
- [Create a basic ingress controller with external network connectivity](#)
- [Enable the HTTP application routing add-on](#)
- [Create an ingress controller that uses an internal, private network and IP address](#)
- [Create an ingress controller with a dynamic public IP and configure Let's Encrypt to automatically generate TLS certificates](#)
- [Create an ingress controller with a static public IP and configure Let's Encrypt to automatically generate TLS certificates](#)

# Use an internal load balancer with Azure Kubernetes Service (AKS)

10/27/2022 • 6 minutes to read • [Edit Online](#)

To restrict access to your applications in Azure Kubernetes Service (AKS), you can create and use an internal load balancer. An internal load balancer makes a Kubernetes service accessible only to applications running in the same virtual network as the Kubernetes cluster. This article shows you how to create and use an internal load balancer with Azure Kubernetes Service (AKS).

## NOTE

Azure Load Balancer is available in two SKUs - *Basic* and *Standard*. By default, the Standard SKU is used when you create an AKS cluster. When creating a Service with type as LoadBalancer, you will get the same LB type as when you provision the cluster. For more information, see [Azure load balancer SKU comparison](#).

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart using the [Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

You also need the Azure CLI version 2.0.59 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

The AKS cluster identity needs permission to manage network resources if you use an existing subnet or resource group. For information, see [Use kubenet networking with your own IP address ranges in Azure Kubernetes Service \(AKS\)](#) or [Configure Azure CNI networking in Azure Kubernetes Service \(AKS\)](#). If you are configuring your load balancer to use an [IP address in a different subnet](#), ensure the AKS cluster identity also has read access to that subnet.

For more information on permissions, see [Delegate AKS access to other Azure resources](#).

## Create an internal load balancer

To create an internal load balancer, create a service manifest named `internal-lb.yaml` with the service type *LoadBalancer* and the *azure-load-balancer-internal* annotation as shown in the following example:

```
apiVersion: v1
kind: Service
metadata:
 name: internal-app
 annotations:
 service.beta.kubernetes.io/azure-load-balancer-internal: "true"
spec:
 type: LoadBalancer
 ports:
 - port: 80
 selector:
 app: internal-app
```

Deploy the internal load balancer using the [kubectl apply](#) and specify the name of your YAML manifest:

```
kubectl apply -f internal-lb.yaml
```

An Azure load balancer is created in the node resource group and connected to the same virtual network as the AKS cluster.

When you view the service details, the IP address of the internal load balancer is shown in the *EXTERNAL-IP* column. In this context, *External*/is in relation to the external interface of the load balancer, not that it receives a public, external IP address. It may take a minute or two for the IP address to change from *<pending>* to an actual internal IP address, as shown in the following example:

```
$ kubectl get service internal-app

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
internal-app LoadBalancer 10.0.248.59 10.240.0.7 80:30555/TCP 2m
```

## Specify an IP address

If you would like to use a specific IP address with the internal load balancer, add the *loadBalancerIP* property to the load balancer YAML manifest. In this scenario, the specified IP address must reside in the same subnet as the AKS cluster but can't already be assigned to a resource. For example, an IP address in the range designated for the Kubernetes subnet within the AKS cluster shouldn't be used.

```
apiVersion: v1
kind: Service
metadata:
 name: internal-app
 annotations:
 service.beta.kubernetes.io/azure-load-balancer-internal: "true"
spec:
 type: LoadBalancer
 loadBalancerIP: 10.240.0.25
 ports:
 - port: 80
 selector:
 app: internal-app
```

When deployed and you view the service details, the IP address in the *EXTERNAL-IP* column reflects your specified IP address:

```
$ kubectl get service internal-app

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
internal-app LoadBalancer 10.0.184.168 10.240.0.25 80:30225/TCP 4m
```

For more information on configuring your load balancer in a different subnet, see [Specify a different subnet](#)

## Connect Azure Private Link service to internal load balancer (Preview)

### Before you begin

You must have the following resource installed:

- The Azure CLI
- Kubernetes version 1.22.x or above

### Create a Private Link service connection

To attach an Azure Private Link service to an internal load balancer, create a service manifest named `internal-lb-pls.yaml` with the service type *LoadBalancer* and the `azure-load-balancer-internal` and `azure-pls-create` annotation as shown in the example below. For more options, refer to the [Azure Private Link Service Integration](#) design document

```
apiVersion: v1
kind: Service
metadata:
 name: internal-app
 annotations:
 service.beta.kubernetes.io/azure-load-balancer-internal: "true"
 service.beta.kubernetes.io/azure-pls-create: "true"
spec:
 type: LoadBalancer
 ports:
 - port: 80
 selector:
 app: internal-app
```

Deploy the internal load balancer using the `kubectl apply` and specify the name of your YAML manifest:

```
kubectl apply -f internal-lb-pls.yaml
```

An Azure load balancer is created in the node resource group and connected to the same virtual network as the AKS cluster.

When you view the service details, the IP address of the internal load balancer is shown in the *EXTERNAL-IP* column. In this context, *External* is in relation to the external interface of the load balancer, not that it receives a public, external IP address. It may take a minute or two for the IP address to change from *<pending>* to an actual internal IP address, as shown in the following example:

```
$ kubectl get service internal-app
NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
internal-app LoadBalancer 10.125.17.53 10.125.0.66 80:30430/TCP 64m
```

Additionally, a Private Link Service object will also be created that connects to the Frontend IP configuration of the Load Balancer associated with the Kubernetes service. Details of the Private Link Service object can be retrieved as shown in the following example:

```
$ AKS_MC_RG=$(az aks show -g myResourceGroup --name myAKSCluster --query nodeResourceGroup -o tsv)
$ az network private-link-service list -g ${AKS_MC_RG} --query "[].{Name:name,Alias:alias}" -o table
Name Alias

pls-xyz pls-xyz.abc123-defg-4hij-56kl-789mnop.eastus2.azure.privatelinkservice
```

## Create a Private Endpoint to the Private Link service

A Private Endpoint allows you to privately connect to your Kubernetes service object via the Private Link Service created above. To do so, follow the example shown below:

```
$ AKS_PLS_ID=$(az network private-link-service list -g ${AKS_MC_RG} --query "[].id" -o tsv)
$ az network private-endpoint create \
 -g myOtherResourceGroup \
 --name myAKSServicePE \
 --vnet-name myOtherVNET \
 --subnet pe-subnet \
 --private-connection-resource-id ${AKS_PLS_ID} \
 --connection-name connectToMyK8sService
```

## Use private networks

When you create your AKS cluster, you can specify advanced networking settings. This approach lets you deploy the cluster into an existing Azure virtual network and subnets. One scenario is to deploy your AKS cluster into a private network connected to your on-premises environment and run services only accessible internally. For more information, see [configure your own virtual network subnets with Kubenet or Azure CNI](#).

No changes to the previous steps are needed to deploy an internal load balancer in an AKS cluster that uses a private network. The load balancer is created in the same resource group as your AKS cluster but connected to your private virtual network and subnet, as shown in the following example:

```
$ kubectl get service internal-app

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
internal-app LoadBalancer 10.1.15.188 10.0.0.35 80:31669/TCP 1m
```

### NOTE

You may need to grant the cluster identity for your AKS cluster the *Network Contributor* role to the resource group where your Azure virtual network resources are deployed. View the cluster identity with [az aks show](#), such as `az aks show --resource-group myResourceGroup --name myAKSCluster --query "identity"`. To create a role assignment, use the [az role assignment create](#) command.

## Specify a different subnet

To specify a subnet for your load balancer, add the *azure-load-balancer-internal-subnet* annotation to your service. The subnet specified must be in the same virtual network as your AKS cluster. When deployed, the load balancer *EXTERNAL-IP* address is part of the specified subnet.

```
apiVersion: v1
kind: Service
metadata:
 name: internal-app
 annotations:
 service.beta.kubernetes.io/azure-load-balancer-internal: "true"
 service.beta.kubernetes.io/azure-load-balancer-internal-subnet: "apps-subnet"
spec:
 type: LoadBalancer
 ports:
 - port: 80
 selector:
 app: internal-app
```

## Delete the load balancer

When all services that use the internal load balancer are deleted, the load balancer itself is also deleted.

You can also directly delete a service as with any Kubernetes resource, such as

```
kubectl delete service internal-app
```

, which also then deletes the underlying Azure load balancer.

## Next steps

Learn more about Kubernetes services at the [Kubernetes services documentation](#).

# Use a public Standard Load Balancer in Azure Kubernetes Service (AKS)

10/27/2022 • 21 minutes to read • [Edit Online](#)

The Azure Load Balancer is on L4 of the Open Systems Interconnection (OSI) model that supports both inbound and outbound scenarios. It distributes inbound flows that arrive at the load balancer's front end to the backend pool instances.

A **public** Load Balancer when integrated with AKS serves two purposes:

1. To provide outbound connections to the cluster nodes inside the AKS virtual network. It achieves this objective by translating the nodes private IP address to a public IP address that is part of its *Outbound Pool*.
2. To provide access to applications via Kubernetes services of type `LoadBalancer`. With it, you can easily scale your applications and create highly available services.

An **internal (or private)** load balancer is used where only private IPs are allowed as frontend. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can also be accessed from an on-premises network in a hybrid scenario.

This document covers the integration with Public Load balancer. For internal Load Balancer integration, see the [AKS Internal Load balancer documentation](#).

## Before you begin

Azure Load Balancer is available in two SKUs - *Basic* and *Standard*. By default, *Standard* SKU is used when you create an AKS cluster. The *Standard* SKU gives you access to added functionality, such as a larger backend pool, [multiple node pools](#), [Availability Zones](#), and is [secure by default](#). It's the recommended Load Balancer SKU for AKS.

For more information on the *Basic* and *Standard* SKUs, see [Azure load balancer SKU comparison](#).

This article assumes you have an AKS cluster with the *Standard* SKU Azure Load Balancer and walks through how to use and configure some of the capabilities and features of the load balancer. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

### IMPORTANT

If you prefer not to leverage the Azure Load Balancer to provide outbound connection and instead have your own gateway, firewall or proxy for that purpose you can skip the creation of the load balancer outbound pool and respective frontend IP by using [Outbound type as UserDefinedRouting \(UDR\)](#). The Outbound type defines the egress method for a cluster and it defaults to type: load balancer.

## Use the public standard load balancer

After creating an AKS cluster with Outbound Type: Load Balancer (default), the cluster is ready to use the load balancer to expose services as well.

For that you can create a public Service of type `LoadBalancer` as shown in the following example. Start by creating a service manifest named `public-svc.yaml`:

```
apiVersion: v1
kind: Service
metadata:
 name: public-svc
spec:
 type: LoadBalancer
 ports:
 - port: 80
 selector:
 app: public-app
```

Deploy the public service manifest by using [kubectl apply](#) and specify the name of your YAML manifest:

```
kubectl apply -f public-svc.yaml
```

The Azure Load Balancer will be configured with a new public IP that will front this new service. Since the Azure Load Balancer can have multiple Frontend IPs, each new service deployed will get a new dedicated frontend IP to be uniquely accessed.

You can confirm your service is created and the load balancer is configured by running for example:

```
kubectl get service public-svc
```

NAMESPACE	NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
default	public-svc	LoadBalancer	10.0.39.110	52.156.88.187	80:32068/TCP	52s

When you view the service details, the public IP address created for this service on the load balancer is shown in the *EXTERNAL-IP* column. It may take a minute or two for the IP address to change from *<pending>* to an actual public IP address, as shown in the above example.

## Configure the public standard load balancer

When using the Standard SKU public load balancer, there's a set of options that can be customized at creation time or by updating the cluster. These options allow you to customize the Load Balancer to meet your workloads needs and should be reviewed accordingly. With the Standard load balancer you can:

- Set or scale the number of Managed Outbound IPs
- Bring your own custom [Outbound IPs or Outbound IP Prefix](#)
- Customize the number of allocated outbound ports to each node of the cluster
- Configure the timeout setting for idle connections

### IMPORTANT

Only one outbound IP option (managed IPs, bring your own IP, or IP Prefix) can be used at a given time.

### Scale the number of managed outbound public IPs

Azure Load Balancer provides outbound connectivity from a virtual network in addition to inbound. Outbound rules make it simple to configure public Standard Load Balancer's outbound network address translation.

Like all Load Balancer rules, outbound rules follow the same familiar syntax as load balancing and inbound NAT rules:

*frontend IPs + parameters + backend pool*

An outbound rule configures outbound NAT for all virtual machines identified by the backend pool to be translated to the frontend. And parameters provide additional fine grained control over the outbound NAT algorithm.

While an outbound rule can be used with just a single public IP address, outbound rules ease the configuration burden for scaling outbound NAT. You can use multiple IP addresses to plan for large-scale scenarios and you can use outbound rules to mitigate SNAT exhaustion prone patterns. Each additional IP address provided by a frontend provides 64k ephemeral ports for Load Balancer to use as SNAT ports.

When using a *Standard* SKU load balancer with managed outbound public IPs, which are created by default, you can scale the number of managed outbound public IPs using the `load-balancer-managed-ip-count` parameter.

To update an existing cluster, run the following command. This parameter can also be set at cluster create-time to have multiple managed outbound public IPs.

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--load-balancer-managed-outbound-ip-count 2
```

The above example sets the number of managed outbound public IPs to 2 for the *myAKSCluster* cluster in *myResourceGroup*.

You can also use the `load-balancer-managed-ip-count` parameter to set the initial number of managed outbound public IPs when creating your cluster by appending the `--load-balancer-managed-outbound-ip-count` parameter and setting it to your desired value. The default number of managed outbound public IPs is 1.

### Provide your own outbound public IPs or prefixes

When you use a *Standard* SKU load balancer, by default the AKS cluster automatically creates a public IP in the AKS-managed infrastructure resource group and assigns it to the load balancer outbound pool.

A public IP created by AKS is considered an AKS managed resource. This means the lifecycle of that public IP is intended to be managed by AKS and requires no user action directly on the public IP resource. Alternatively, you can assign your own custom public IP or public IP prefix at cluster creation time. Your custom IPs can also be updated on an existing cluster's load balancer properties.

Requirements for using your own public IP or prefix:

- Custom public IP addresses must be created and owned by the user. Managed public IP addresses created by AKS cannot be reused as bringing your own custom IP as it can cause management conflicts.
- You must ensure the AKS cluster identity (Service Principal or Managed Identity) has permissions to access the outbound IP. As per the [required public IP permissions list](#).
- Make sure you meet the [pre-requisites and constraints](#) necessary to configure Outbound IPs or Outbound IP prefixes.

### Update the cluster with your own outbound public IP

Use the `az network public-ip show` command to list the IDs of your public IPs.

```
az network public-ip show --resource-group myResourceGroup --name myPublicIP --query id -o tsv
```

The above command shows the ID for the *myPublicIP* public IP in the *myResourceGroup* resource group.

Use the `az aks update` command with the `load-balancer-outbound-ips` parameter to update your cluster with your public IPs.

The following example uses the `load-balancer-outbound-ips` parameter with the IDs from the previous

command.

```
az aks update \
--resource-group myResourceGroup \
--name myAKScluster \
--load-balancer-outbound-ips <publicIpId1>,<publicIpId2>
```

#### Update the cluster with your own outbound public IP prefix

You can also use public IP prefixes for egress with your *Standard* SKU load balancer. The following example uses the [az network public-ip prefix show](#) command to list the IDs of your public IP prefixes:

```
az network public-ip prefix show --resource-group myResourceGroup --name myPublicIPPrefix --query id -o tsv
```

The above command shows the ID for the *myPublicIPPrefix* public IP prefix in the *myResourceGroup* resource group.

The following example uses the *load-balancer-outbound-ip-prefixes* parameter with the IDs from the previous command.

```
az aks update \
--resource-group myResourceGroup \
--name myAKScluster \
--load-balancer-outbound-ip-prefixes <publicIpPrefixId1>,<publicIpPrefixId2>
```

#### Create the cluster with your own public IP or prefixes

You may wish to bring your own IP addresses or IP prefixes for egress at cluster creation time to support scenarios like adding egress endpoints to an allowlist. Append the same parameters shown above to your cluster creation step to define your own public IPs and IP prefixes at the start of a cluster's lifecycle.

Use the [az aks create](#) command with the *load-balancer-outbound-ips* parameter to create a new cluster with your public IPs at the start.

```
az aks create \
--resource-group myResourceGroup \
--name myAKScluster \
--load-balancer-outbound-ips <publicIpId1>,<publicIpId2>
```

Use the [az aks create](#) command with the *load-balancer-outbound-ip-prefixes* parameter to create a new cluster with your public IP prefixes at the start.

```
az aks create \
--resource-group myResourceGroup \
--load-balancer-outbound-ip-prefixes <publicIpPrefixId1>,<publicIpPrefixId2>
```

#### Configure the allocated outbound ports

## IMPORTANT

If you have applications on your cluster which can establish a large number of connections to small set of destinations, for example many instances of a frontend application connecting to a database, you may have a scenario very susceptible to encounter SNAT port exhaustion. SNAT port exhaustion happens when an application runs out of outbound ports to use to establish a connection to another application or host. If you have a scenario where you may encounter SNAT port exhaustion, it is highly recommended that you increase the allocated outbound ports and outbound frontend IPs on the load balancer to prevent SNAT port exhaustion. See below for information on how to properly calculate outbound ports and outbound frontend IP values.

By default, AKS sets *AllocatedOutboundPorts* on its load balancer to `0`, which enables [automatic outbound port assignment based on backend pool size](#) when creating a cluster. For example, if a cluster has 50 or fewer nodes, 1024 ports are allocated to each node. As the number of nodes in the cluster is increased, fewer ports will be available per node. To show the *AllocatedOutboundPorts* value for the AKS cluster load balancer, use

```
az network lb outbound-rule list
```

```
NODE_RG=$(az aks show --resource-group myResourceGroup --name myAKSCluster --query nodeResourceGroup -o tsv)
az network lb outbound-rule list --resource-group $NODE_RG --lb-name kubernetes -o table
```

The following example output shows that automatic outbound port assignment based on backend pool size is enabled for the cluster:

AllocatedOutboundPorts	EnableTcpReset	IdleTimeoutInMinutes	Name	Protocol	
ProvisioningState	ResourceGroup				
0	True	30	aksOutboundRule	All	Succeeded
MC_myResourceGroup_myAKSCluster_eastus					

To configure a specific value for *AllocatedOutboundPorts* and outbound IP address when creating or updating a cluster, use `load-balancer-outbound-ports` and either `load-balancer-managed-outbound-ip-count`, `load-balancer-outbound-ips`, or `load-balancer-outbound-ip-prefixes`. Before setting a specific value or increasing an existing value for either for outbound ports and outbound IP address, you must calculate the appropriate number of outbound ports and IP address. Use the following equation for this calculation rounded to the nearest integer:

```
64,000 ports per IP / <outbound ports per node> * <number of outbound IPs> = <maximum number of nodes in the cluster>
```

When calculating the number of outbound ports and IPs and setting the values, remember:

- The number of outbound ports is fixed per node based on the value you set.
- The value for outbound ports must be a multiple of 8.
- Adding more IPs does not add more ports to any node. It provides capacity for more nodes in the cluster.
- You must account for nodes that may be added as part of upgrades, including the count of nodes specified via [maxSurge values](#).

The following examples show how the number of outbound ports and IP addresses are affected by the values you set:

- If the default values are used and the cluster has 48 nodes, each node will have 1024 ports available.
- If the default values are used and the cluster scales from 48 to 52 nodes, each node will be updated from 1024 ports available to 512 ports available.
- If outbound ports is set to 1,000 and outbound IP count is set to 2, then the cluster can support a maximum

of 128 nodes:  $64,000 \text{ ports per IP} / 1,000 \text{ ports per node} * 2 \text{ IPs} = 128 \text{ nodes}$ .

- If outbound ports is set to 1,000 and outbound IP count is set to 7, then the cluster can support a maximum of 448 nodes:  $64,000 \text{ ports per IP} / 1,000 \text{ ports per node} * 7 \text{ IPs} = 448 \text{ nodes}$ .
- If outbound ports is set to 4,000 and outbound IP count is set to 2, then the cluster can support a maximum of 32 nodes:  $64,000 \text{ ports per IP} / 4,000 \text{ ports per node} * 2 \text{ IPs} = 32 \text{ nodes}$ .
- If outbound ports is set to 4,000 and outbound IP count is set to 7, then the cluster can support a maximum of 112 nodes:  $64,000 \text{ ports per IP} / 4,000 \text{ ports per node} * 7 \text{ IPs} = 112 \text{ nodes}$ .

### IMPORTANT

After calculating the number outbound ports and IPs, verify you have additional outbound port capacity to handle node surge during upgrades. It is critical to allocate sufficient excess ports for additional nodes needed for upgrade and other operations. AKS defaults to one buffer node for upgrade operations. If using [maxSurge values](#), multiply the outbound ports per node by your maxSurge value to determine the number of ports required. For example if you calculated you needed 4000 ports per node with 7 IP address on a cluster with a maximum of 100 nodes and a max surge of 2:

- 2 surge nodes \* 4000 ports per node = 8000 ports needed for node surge during upgrades.
- 100 nodes \* 4000 ports per node = 400,000 ports required for your cluster.
- 7 IPs \* 64000 ports per IP = 448,000 ports available for your cluster.

The above example shows the cluster has an excess capacity of 48,000 ports, which is sufficient to handle the 8000 ports needed for node surge during upgrades.

Once the values have been calculated and verified, you can apply those values using

`load-balancer-outbound-ports` and either `load-balancer-managed-outbound-ip-count`, `load-balancer-outbound-ips`, or `load-balancer-outbound-ip-prefixes` when creating or updating a cluster. For example:

```
az aks update \
 --resource-group myResourceGroup \
 --name myAKScluster \
 --load-balancer-managed-outbound-ip-count 7 \
 --load-balancer-outbound-ports 4000
```

### Configure the load balancer idle timeout

When SNAT port resources are exhausted, outbound flows fail until existing flows release SNAT ports. Load Balancer reclaims SNAT ports when the flow closes and the AKS-configured load balancer uses a 30-minute idle timeout for reclaiming SNAT ports from idle flows. You can also use transport (for example, [TCP keepalives](#)) or [application-layer keepalives](#) to refresh an idle flow and reset this idle timeout if necessary. You can configure this timeout following the below example:

```
az aks update \
 --resource-group myResourceGroup \
 --name myAKScluster \
 --load-balancer-idle-timeout 4
```

If you expect to have numerous short lived connections, and no connections that are long lived and might have long times of idle, like leveraging `kubectl proxy` or `kubectl port-forward` consider using a low timeout value such as 4 minutes. Also, when using TCP keepalives, it's sufficient to enable them on one side of the connection. For example, it's sufficient to enable them on the server side only to reset the idle timer of the flow and it's not necessary for both sides to start TCP keepalives. Similar concepts exist for application layer, including database client-server configurations. Check the server side for what options exist for application-specific keepalives.

## IMPORTANT

AKS enables TCP Reset on idle by default and recommends you keep this configuration on and leverage it for more predictable application behavior on your scenarios. TCP RST is only sent during TCP connection in ESTABLISHED state. Read more about it [here](#).

When setting *IdleTimeoutInMinutes* to a different value than the default of 30 minutes, consider how long your workloads will need an outbound connection. Also consider the default timeout value for a *Standard* SKU load balancer used outside of AKS is 4 minutes. An *IdleTimeoutInMinutes* value that more accurately reflects your specific AKS workload can help decrease SNAT exhaustion caused by tying up connections no longer being used.

## WARNING

Altering the values for *AllocatedOutboundPorts* and *IdleTimeoutInMinutes* may significantly change the behavior of the outbound rule for your load balancer and should not be done lightly, without understanding the tradeoffs and your application's connection patterns, check the [SNAT Troubleshooting section below](#) and review the [Load Balancer outbound rules](#) and [outbound connections in Azure](#) before updating these values to fully understand the impact of your changes.

## Restrict inbound traffic to specific IP ranges

The following manifest uses *loadBalancerSourceRanges* to specify a new IP range for inbound external traffic:

```
apiVersion: v1
kind: Service
metadata:
 name: azure-vote-front
spec:
 type: LoadBalancer
 ports:
 - port: 80
 selector:
 app: azure-vote-front
 loadBalancerSourceRanges:
 - MY_EXTERNAL_IP_RANGE
```

This example updates the rule to allow inbound external traffic only from the `MY_EXTERNAL_IP_RANGE` range. If you replace `MY_EXTERNAL_IP_RANGE` with the internal subnet IP address, traffic is restricted to only cluster internal IPs. If traffic is restricted to cluster internal IPs, clients outside your Kubernetes cluster won't be able to access the load balancer.

## NOTE

Inbound, external traffic flows from the load balancer to the virtual network for your AKS cluster. The virtual network has a Network Security Group (NSG) which allows all inbound traffic from the load balancer. This NSG uses a [service tag](#) of type *LoadBalancer* to allow traffic from the load balancer.

## Maintain the client's IP on inbound connections

By default, a service of type `LoadBalancer` in [Kubernetes](#) and in AKS won't persist the client's IP address on the connection to the pod. The source IP on the packet that's delivered to the pod will be the private IP of the node. To maintain the client's IP address, you must set `service.spec.externalTrafficPolicy` to `local` in the service definition. The following manifest shows an example:

```

apiVersion: v1
kind: Service
metadata:
 name: azure-vote-front
spec:
 type: LoadBalancer
 externalTrafficPolicy: Local
 ports:
 - port: 80
 selector:
 app: azure-vote-front

```

## Additional customizations via Kubernetes Annotations

Below is a list of annotations supported for Kubernetes services with type `LoadBalancer`, these annotations only apply to **INBOUND** flows:

ANNOTATION	VALUE	DESCRIPTION
<code>service.beta.kubernetes.io/azure-load-balancer-internal</code>	<code>true</code> or <code>false</code>	Specify whether the load balancer should be internal. It's defaulting to public if not set.
<code>service.beta.kubernetes.io/azure-load-balancer-internal-subnet</code>	Name of the subnet	Specify which subnet the internal load balancer should be bound to. It's defaulting to the subnet configured in cloud config file if not set.
<code>service.beta.kubernetes.io/azure-dns-label-name</code>	Name of the DNS label on Public IPs	Specify the DNS label name for the <b>public</b> service. If it is set to empty string, the DNS entry in the Public IP will not be used.
<code>service.beta.kubernetes.io/azure-shared-securityrule</code>	<code>true</code> or <code>false</code>	Specify that the service should be exposed using an Azure security rule that may be shared with another service, trading specificity of rules for an increase in the number of services that can be exposed. This annotation relies on the Azure <a href="#">Augmented Security Rules</a> feature of Network Security groups.
<code>service.beta.kubernetes.io/azure-load-balancer-resource-group</code>	Name of the resource group	Specify the resource group of load balancer public IPs that aren't in the same resource group as the cluster infrastructure (node resource group).
<code>service.beta.kubernetes.io/azure-allowed-service-tags</code>	List of allowed service tags	Specify a list of allowed <a href="#">service tags</a> separated by comma.
<code>service.beta.kubernetes.io/azure-load-balancer-tcp-idle-timeout</code>	TCP idle timeouts in minutes	Specify the time, in minutes, for TCP connection idle timeouts to occur on the load balancer. Default and minimum value is 4. Maximum value is 30. Must be an integer.

ANNOTATION	VALUE	DESCRIPTION
<code>service.beta.kubernetes.io/azure-load-balancer-disable-tcp-reset</code>	true	Disable <code>enableTcpReset</code> for SLB. Deprecated in Kubernetes 1.18 and removed in 1.20.

## Troubleshooting SNAT

If you know that you're starting many outbound TCP or UDP connections to the same destination IP address and port, and you observe failing outbound connections or are advised by support that you're exhausting SNAT ports (preallocated ephemeral ports used by PAT), you have several general mitigation options. Review these options and decide what is available and best for your scenario. It's possible that one or more can help manage this scenario. For detailed information, review the [Outbound Connections Troubleshooting Guide](#).

Frequently the root cause of SNAT exhaustion is an anti-pattern for how outbound connectivity is established, managed, or configurable timers changed from their default values. Review this section carefully.

### Steps

1. Check if your connections remain idle for a long time and rely on the default idle timeout for releasing that port. If so the default timeout of 30 min might need to be reduced for your scenario.
2. Investigate how your application is creating outbound connectivity (for example, code review or packet capture).
3. Determine if this activity is expected behavior or whether the application is misbehaving. Use [metrics](#) and [logs](#) in Azure Monitor to substantiate your findings. Use "Failed" category for SNAT Connections metric for example.
4. Evaluate if appropriate [patterns](#) are followed.
5. Evaluate if SNAT port exhaustion should be mitigated with [additional Outbound IP addresses + additional Allocated Outbound Ports](#) .

### Design patterns

Always take advantage of connection reuse and connection pooling whenever possible. These patterns will avoid resource exhaustion problems and result in predictable behavior. Primitives for these patterns can be found in many development libraries and frameworks.

- Atomic requests (one request per connection) are generally not a good design choice. Such anti-pattern limits scale, reduces performance, and decreases reliability. Instead, reuse HTTP/S connections to reduce the numbers of connections and associated SNAT ports. The application scale will increase and performance improve because of reduced handshakes, overhead, and cryptographic operation cost when using TLS.
- If you're using out of cluster/custom DNS, or custom upstream servers on coreDNS have in mind that DNS can introduce many individual flows at volume when the client isn't caching the DNS resolvers result. Make sure to customize coreDNS first instead of using custom DNS servers, and define a good caching value.
- UDP flows (for example DNS lookups) allocate SNAT ports for the duration of the idle timeout. The longer the idle timeout, the higher the pressure on SNAT ports. Use short idle timeout (for example 4 minutes). Use connection pools to shape your connection volume.
- Never silently abandon a TCP flow and rely on TCP timers to clean up flow. If you don't let TCP explicitly close the connection, state remains allocated at intermediate systems and endpoints and makes SNAT ports unavailable for other connections. This pattern can trigger application failures and SNAT exhaustion.
- Don't change OS-level TCP close related timer values without expert knowledge of impact. While the TCP stack will recover, your application performance can be negatively affected when the endpoints of a connection have mismatched expectations. Wishing to change timers is usually a sign of an underlying design problem. Review following recommendations.

# Moving from a basic SKU load balancer to standard SKU

If you have an existing cluster with the Basic SKU Load Balancer, there are important behavioral differences to note when migrating to use a cluster with the Standard SKU Load Balancer.

For example, making blue/green deployments to migrate clusters is a common practice given the `load-balancer-sku` type of a cluster can only be defined at cluster create time. However, *Basic SKU* Load Balancers use *Basic SKU* IP Addresses, which aren't compatible with *Standard SKU* Load Balancers as they require *Standard SKU* IP Addresses. When migrating clusters to upgrade Load Balancer SKUs, a new IP address with a compatible IP Address SKU will be required.

For more considerations on how to migrate clusters, visit [our documentation on migration considerations](#) to view a list of important topics to consider when migrating. The below limitations are also important behavioral differences to note when using Standard SKU Load Balancers in AKS.

## Limitations

The following limitations apply when you create and manage AKS clusters that support a load balancer with the *StandardSKU*:

- At least one public IP or IP prefix is required for allowing egress traffic from the AKS cluster. The public IP or IP prefix is also required to maintain connectivity between the control plane and agent nodes and to maintain compatibility with previous versions of AKS. You have the following options for specifying public IPs or IP prefixes with a *StandardSKU* load balancer:
  - Provide your own public IPs.
  - Provide your own public IP prefixes.
  - Specify a number up to 100 to allow the AKS cluster to create that many *StandardSKU* public IPs in the same resource group created as the AKS cluster, which is usually named with *MC\_* at the beginning. AKS assigns the public IP to the *StandardSKU* load balancer. By default, one public IP will automatically be created in the same resource group as the AKS cluster, if no public IP, public IP prefix, or number of IPs is specified. You also must allow public addresses and avoid creating any Azure Policy that bans IP creation.
- A public IP created by AKS cannot be reused as a custom bring your own public IP address. All custom IP addresses must be created and managed by the user.
- Defining the load balancer SKU can only be done when you create an AKS cluster. You can't change the load balancer SKU after an AKS cluster has been created.
- You can only use one type of load balancer SKU (Basic or Standard) in a single cluster.
- *StandardSKU* Load Balancers only support *StandardSKU* IP Addresses.

## Next steps

Learn more about Kubernetes services at the [Kubernetes services documentation](#).

Learn more about using Internal Load Balancer for Inbound traffic at the [AKS Internal Load Balancer documentation](#).

# Configure `kube-proxy` in Azure Kubernetes Service (AKS) (preview)

10/27/2022 • 3 minutes to read • [Edit Online](#)

`kube-proxy` is a component of Kubernetes that handles routing traffic for services within the cluster. There are two backends available for Layer 3/4 load balancing in upstream `kube-proxy` - iptables and IPVS.

- iptables is the default backend utilized in the majority of Kubernetes clusters. It is simple and well supported, but is not as efficient or intelligent as IPVS.
- IPVS utilizes the Linux Virtual Server, a layer 3/4 load balancer built into the Linux kernel. IPVS provides a number of advantages over the default iptables configuration, including state awareness, connection tracking, and more intelligent load balancing.

The AKS managed `kube-proxy` DaemonSet can also be disabled entirely if that is desired to support [bring-your-own CNI](#).

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Prerequisites

- Azure CLI with aks-preview extension 0.5.105 or later.
- If using ARM or the REST API, the AKS API version must be 2022-08-02-preview or later.

### Install the aks-preview CLI extension

```
Install the aks-preview extension
az extension add --name aks-preview

Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

### Register the `KubeProxyConfigurationPreview` preview feature

To create an AKS cluster with custom `kube-proxy` configuration, you must enable the `KubeProxyConfigurationPreview` feature flag on your subscription.

Register the `KubeProxyConfigurationPreview` feature flag by using the `az feature register` command, as shown in the following example:

```
az feature register --namespace "Microsoft.ContainerService" --name "KubeProxyConfigurationPreview"
```

It takes a few minutes for the status to show *Registered*. Verify the registration status by using the

```
az feature list command:
```

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/KubeProxyConfigurationPreview')].{Name:name, State:properties.state}"
```

When the feature has been registered, refresh the registration of the *Microsoft.ContainerService* resource provider by using the `az provider register` command:

```
az provider register --namespace Microsoft.ContainerService
```

## Configurable options

The full `kube-proxy` configuration structure can be found in the [AKS Cluster Schema](#).

- `enabled` - whether or not to deploy the `kube-proxy` DaemonSet. Defaults to true.
- `mode` - can be set to `IPTABLES` or `IPVS`. Defaults to `IPTABLES`.
- `ipvsConfig` - if `mode` is `IPVS`, this object contains IPVS-specific configuration properties.
  - `scheduler` - which connection scheduler to utilize. Supported values:
    - `LeastConnections` - sends connections to the backend pod with the fewest connections
    - `RoundRobin` - distributes connections evenly between backend pods
    - `tcpFinTimeoutSeconds` - the value used for timeout after a FIN has been received in a TCP session
    - `tcpTimeoutSeconds` - the value used for timeout length for idle TCP sessions
    - `udpTimeoutSeconds` - the value used for timeout length for idle UDP sessions

### NOTE

IPVS load balancing operates in each node independently and is still only aware of connections flowing through the local node. This means that while `LeastConnections` results in more even load under higher number of connections, when low numbers of connections (# connects < 2 \* node count) occur traffic may still be relatively unbalanced.

## Utilize `kube-proxy` configuration in a new or existing AKS cluster using Azure CLI

`kube-proxy` configuration is a cluster-wide setting. No action is needed to update your services.

### WARNING

Changing the `kube-proxy` configuration may cause a slight interruption in cluster service traffic flow.

To begin, create a JSON configuration file with the desired settings:

### Create a configuration file

```
{
 "enabled": true,
 "mode": "IPVS",
 "ipvsConfig": {
 "scheduler": "LeastConnection",
 "TCPTimeoutSeconds": 900,
 "TCPFINTTimeoutSeconds": 120,
 "UDPTimeoutSeconds": 300
 }
}
```

## Deploy a new cluster

Deploy your cluster using `az aks create` and pass in the configuration file:

```
az aks create -g <resourceGroup> -n <clusterName> --kube-proxy-config kube-proxy.json
```

## Update an existing cluster

Configure your cluster using `az aks update` and pass in the configuration file:

```
az aks update -g <resourceGroup> -n <clusterName> --kube-proxy-config kube-proxy.json
```

## Next steps

Learn more about utilizing the Standard Load Balancer for inbound traffic at the [AKS Standard Load Balancer documentation][load-balancer-standard.md].

Learn more about using Internal Load Balancer for Inbound traffic at the [AKS Internal Load Balancer documentation](#).

Learn more about Kubernetes services at the [Kubernetes services documentation](#).

# Use a static public IP address and DNS label with the Azure Kubernetes Service (AKS) load balancer

10/27/2022 • 4 minutes to read • [Edit Online](#)

By default, the public IP address assigned to a load balancer resource created by an AKS cluster is only valid for the lifespan of that resource. If you delete the Kubernetes service, the associated load balancer and IP address are also deleted. If you want to assign a specific IP address or retain an IP address for redeployed Kubernetes services, you can create and use a static public IP address.

This article shows you how to create a static public IP address and assign it to your Kubernetes service.

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart using the [Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

You also need the Azure CLI version 2.0.59 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

This article covers using a *Standard* SKU IP with a *Standard* SKU load balancer. For more information, see [IP address types and allocation methods in Azure](#).

## Create a static IP address

Create a static public IP address with the `az network public-ip create` command. The following creates a static IP resource named *myAKSPublicIP* in the *myResourceGroup* resource group:

```
az network public-ip create \
 --resource-group myResourceGroup \
 --name myAKSPublicIP \
 --sku Standard \
 --allocation-method static
```

### NOTE

If you are using a *Basic* SKU load balancer in your AKS cluster, use *Basic* for the *sku* parameter when defining a public IP. Only *Basic* SKU IPs work with the *Basic* SKU load balancer and only *Standard* SKU IPs work with *Standard* SKU load balancers.

The IP address is displayed, as shown in the following condensed example output:

```
{
 "publicIp": {
 ...
 "ipAddress": "40.121.183.52",
 ...
 }
}
```

You can later get the public IP address using the `az network public-ip list` command. Specify the name of the

node resource group and public IP address you created, and query for the *ipAddress* as shown in the following example:

```
$ az network public-ip show --resource-group myResourceGroup --name myAKSPublicIP --query ipAddress --output tsv
40.121.183.52
```

## Create a service using the static IP address

Before creating a service, ensure the cluster identity used by the AKS cluster has delegated permissions to the other resource group. For example:

```
az role assignment create \
 --assignee <Client ID> \
 --role "Network Contributor" \
 --scope /subscriptions/<subscription id>/resourceGroups/<resource group name>
```

### IMPORTANT

If you customized your outbound IP make sure your cluster identity has permissions to both the outbound public IP and this inbound public IP.

To create a *LoadBalancer* service with the static public IP address, add the `loadBalancerIP` property and the value of the static public IP address to the YAML manifest. Create a file named `load-balancer-service.yaml` and copy in the following YAML. Provide your own public IP address created in the previous step. The following example also sets the annotation to the resource group named *myResourceGroup*. Provide your own resource group name.

```
apiVersion: v1
kind: Service
metadata:
 annotations:
 service.beta.kubernetes.io/azure-load-balancer-resource-group: myResourceGroup
 name: azure-load-balancer
spec:
 loadBalancerIP: 40.121.183.52
 type: LoadBalancer
 ports:
 - port: 80
 selector:
 app: azure-load-balancer
```

Create the service and deployment with the `kubectl apply` command.

```
kubectl apply -f load-balancer-service.yaml
```

## Apply a DNS label to the service

If your service is using a dynamic or static public IP address, you can use the service annotation `service.beta.kubernetes.io/azure-dns-label-name` to set a public-facing DNS label. This publishes a fully qualified domain name for your service using Azure's public DNS servers and top-level domain. The annotation value must be unique within the Azure location, so it's recommended to use a sufficiently qualified label.

Azure will then automatically append a default suffix, such as <location>.cloudapp.azure.com (where location is the region you selected), to the name you provide, to create the fully qualified DNS name. For example:

```
apiVersion: v1
kind: Service
metadata:
 annotations:
 service.beta.kubernetes.io/azure-dns-label-name: myserviceuniquelabel
 name: azure-load-balancer
spec:
 type: LoadBalancer
 ports:
 - port: 80
 selector:
 app: azure-load-balancer
```

#### NOTE

To publish the service on your own domain, see [Azure DNS](#) and the [external-dns](#) project.

## Troubleshoot

If the static IP address defined in the *loadBalancerIP* property of the Kubernetes service manifest does not exist, or has not been created in the node resource group and no additional delegations configured, the load balancer service creation fails. To troubleshoot, review the service creation events with the `kubectl describe` command. Provide the name of the service as specified in the YAML manifest, as shown in the following example:

```
kubectl describe service azure-load-balancer
```

Information about the Kubernetes service resource is displayed. The *Events* at the end of the following example output indicate that the *user supplied IP Address was not found*. In these scenarios, verify that you have created the static public IP address in the node resource group and that the IP address specified in the Kubernetes service manifest is correct.

```
Name: azure-load-balancer
Namespace: default
Labels: <none>
Annotations: <none>
Selector: app=azure-load-balancer
Type: LoadBalancer
IP: 10.0.18.125
IP: 40.121.183.52
Port: <unset> 80/TCP
TargetPort: 80/TCP
NodePort: <unset> 32582/TCP
Endpoints: <none>
Session Affinity: None
External Traffic Policy: Cluster
Events:
 Type Reason Age From Message
 ---- ---- ---- ---- -----
 Normal CreatingLoadBalancer 7s (x2 over 22s) service-controller Creating load balancer
 Warning CreatingLoadBalancerFailed 6s (x2 over 12s) service-controller Error creating load balancer
(will retry): Failed to create load balancer for service default/azure-load-balancer: user supplied IP
Address 40.121.183.52 was not found
```

## Next steps

For additional control over the network traffic to your applications, you may want to instead [create an ingress controller](#). You can also [create an ingress controller with a static public IP address](#).

# HTTP proxy support in Azure Kubernetes Service

10/27/2022 • 3 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) clusters, whether deployed into a managed or custom virtual network, have certain outbound dependencies necessary to function properly. Previously, in environments requiring internet access to be routed through HTTP proxies, this was a problem. Nodes had no way of bootstrapping the configuration, environment variables, and certificates necessary to access internet services.

This feature adds HTTP proxy support to AKS clusters, exposing a straightforward interface that cluster operators can use to secure AKS-required network traffic in proxy-dependent environments.

Some more complex solutions may require creating a chain of trust to establish secure communications across the network. The feature also enables installation of a trusted certificate authority onto the nodes as part of bootstrapping a cluster.

## Limitations and other details

The following scenarios are **not** supported:

- Different proxy configurations per node pool
- Updating proxy settings post cluster creation
- User/Password authentication
- Custom CAs for API server communication
- Windows-based clusters
- Node pools using Virtual Machine Availability Sets (VMAS)

By default, `httpProxy`, `httpsProxy`, and `trustedCa` have no value.

## Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- Latest version of [Azure CLI installed](#).

## Configuring an HTTP proxy using Azure CLI

Using AKS with an HTTP proxy is done at cluster creation, using the `az aks create` command and passing in configuration as a JSON file.

The schema for the config file looks like this:

```
{
 "httpProxy": "string",
 "httpsProxy": "string",
 "noProxy": [
 "string"
],
 "trustedCa": "string"
}
```

`httpProxy` : A proxy URL to use for creating HTTP connections outside the cluster. The URL scheme must be

`http` . `httpsProxy` : A proxy URL to use for creating HTTPS connections outside the cluster. If this is not specified,

then `httpProxy` is used for both HTTP and HTTPS connections. `noProxy`: A list of destination domain names, domains, IP addresses or other network CIDRs to exclude proxying. `trustedCa`: A string containing the `base64 encoded` alternative CA certificate content. For now we only support `PEM` format. Another thing to note is that, for compatibility with Go-based components that are part of the Kubernetes system, the certificate MUST support `Subject Alternative Names(SANs)` instead of the deprecated Common Name certs.

Example input: Note the CA cert should be the base64 encoded string of the PEM format cert content.

```
{
 "httpProxy": "http://myproxy.server.com:8080/",
 "httpsProxy": "https://myproxy.server.com:8080/",
 "noProxy": [
 "localhost",
 "127.0.0.1"
],
 "trustedCA":
 "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUgvVENDQmVXZ0F3SUJB...b3Rpbk15RGszaWfyCkYxMF1scWNPbWVYMXVGbUtizGkv
 WG9yR2xrQ29NRjNURhg4cm1wOURCaUIvCi0tLS0tRU5EIENFU1RJRK1DQVRFLS0tLS0="
}
```

Create a file and provide values for `httpProxy`, `httpsProxy`, and `noProxy`. If your environment requires it, also provide a `trustedCa` value. Next, deploy a cluster, passing in your filename via the `http-proxy-config` flag.

```
az aks create -n $clusterName -g $resourceGroup --http-proxy-config aks-proxy-config.json
```

Your cluster will initialize with the HTTP proxy configured on the nodes.

## Configuring an HTTP proxy using Azure Resource Manager (ARM) templates

Deploying an AKS cluster with an HTTP proxy configured via ARM template is straightforward. The same schema used for CLI deployment exists in the `Microsoft.ContainerService/managedClusters` definition under properties:

```
"properties": {
 ...,
 "httpProxyConfig": {
 "httpProxy": "string",
 "httpsProxy": "string",
 "noProxy": [
 "string"
],
 "trustedCa": "string"
 }
}
```

In your template, provide values for `httpProxy`, `httpsProxy`, and `noProxy`. If necessary, also provide a value for `trustedCa`. Deploy the template, and your cluster should initialize with your HTTP proxy configured on the nodes.

## Handling CA rollover

Values for `httpProxy`, `httpsProxy`, and `noProxy` cannot be changed after cluster creation. However, to support rolling CA certs, the value for `trustedCa` can be changed and applied to the cluster with the [az aks update](#) command.

For example, assuming a new file has been created with the base64 encoded string of the new CA cert called *aks-proxy-config-2.json*, the following action will update the cluster:

```
az aks update -n $clusterName -g $resourceGroup --http-proxy-config aks-proxy-config-2.json
```

## Monitoring add-on configuration

When using the HTTP proxy with the Monitoring add-on, the following configurations are supported:

- Outbound proxy without authentication
- Outbound proxy with username & password authentication
- Outbound proxy with trusted cert for Log Analytics endpoint

The following configurations are not supported:

- The Custom Metrics and Recommended Alerts features are not supported when using proxy with trusted cert
- Outbound proxy is not supported with Azure Monitor Private Link Scope (AMPLS)

## Next steps

- For more on the network requirements of AKS clusters, see [control egress traffic for cluster nodes in AKS](#).

# Create an ingress controller in Azure Kubernetes Service (AKS)

10/27/2022 • 12 minutes to read • [Edit Online](#)

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services. Kubernetes ingress resources are used to configure the ingress rules and routes for individual Kubernetes services. When you use an ingress controller and ingress rules, a single IP address can be used to route traffic to multiple services in a Kubernetes cluster.

This article shows you how to deploy the [NGINX ingress controller](#) in an Azure Kubernetes Service (AKS) cluster. Two applications are then run in the AKS cluster, each of which is accessible over the single IP address.

## NOTE

There are two open source ingress controllers for Kubernetes based on Nginx: one is maintained by the Kubernetes community ([kubernetes/ingress-nginx](#)), and one is maintained by NGINX, Inc. ([nginxinc/kubernetes-ingress](#)). This article will be using the Kubernetes community ingress controller.

## Before you begin

This article uses [Helm 3](#) to install the NGINX ingress controller on a [supported version of Kubernetes](#). Make sure that you're using the latest release of Helm and have access to the *ingress-nginx* Helm repository. The steps outlined in this article may not be compatible with previous versions of the Helm chart, NGINX ingress controller, or Kubernetes.

- [Azure CLI](#)
- [Azure PowerShell](#)

This article also requires that you're running the Azure CLI version 2.0.64 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

In addition, this article assumes you have an existing AKS cluster with an integrated Azure Container Registry (ACR). For more information on creating an AKS cluster with an integrated ACR, see [Authenticate with Azure Container Registry from Azure Kubernetes Service](#).

## Basic configuration

To create a basic NGINX ingress controller without customizing the defaults, you'll use Helm.

- [Azure CLI](#)
- [Azure PowerShell](#)

```

NAMESPACE=ingress-basic

helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx
helm repo update

helm install ingress-nginx ingress-nginx/ingress-nginx \
--create-namespace \
--namespace $NAMESPACE \
--set controller.service.annotations."service\\.beta\\.kubernetes\\.io/azure-load-balancer-health-probe-
request-path"/=healthz

```

The above configuration uses the default configuration for simplicity. You can add parameters for customizing the deployment, for example, `--set controller.replicaCount=3`. The next section will show a highly customized example of the ingress controller.

## Customized configuration

As an alternative to the basic configuration presented in the above section, the next set of steps will show how to deploy a customized ingress controller. You'll have the option of using an internal static IP address, or using a dynamic public IP address.

### Import the images used by the Helm chart into your ACR

- [Azure CLI](#)
- [Azure PowerShell](#)

To control image versions, you'll want to import them into your own Azure Container Registry. The [NGINX ingress controller Helm chart](#) relies on three container images. Use `az acr import` to import those images into your ACR.

```

REGISTRY_NAME=<REGISTRY_NAME>
SOURCE_REGISTRY=k8s.gcr.io
CONTROLLER_IMAGE=ingress-nginx/controller
CONTROLLER_TAG=v1.2.1
PATCH_IMAGE=ingress-nginx/kube-webhook-certgen
PATCH_TAG=v1.1.1
DEFAULTBACKEND_IMAGE=defaultbackend-amd64
DEFAULTBACKEND_TAG=1.5

az acr import --name $REGISTRY_NAME --source $SOURCE_REGISTRY/$CONTROLLER_IMAGE:$CONTROLLER_TAG --image
$CONTROLLER_IMAGE:$CONTROLLER_TAG
az acr import --name $REGISTRY_NAME --source $SOURCE_REGISTRY/$PATCH_IMAGE:$PATCH_TAG --image
$PATCH_IMAGE:$PATCH_TAG
az acr import --name $REGISTRY_NAME --source $SOURCE_REGISTRY/$DEFAULTBACKEND_IMAGE:$DEFAULTBACKEND_TAG --
image $DEFAULTBACKEND_IMAGE:$DEFAULTBACKEND_TAG

```

#### NOTE

In addition to importing container images into your ACR, you can also import Helm charts into your ACR. For more information, see [Push and pull Helm charts to an Azure Container Registry](#).

### Use an internal IP address

By default, an NGINX ingress controller is created with a dynamic public IP address assignment. A common configuration requirement is to use an internal, private network and IP address. This approach allows you to restrict access to your services to internal users, with no external access.

Create a file named `internal-ingress.yaml` using the following example manifest:

```
controller:
 service:
 loadBalancerIP: 10.224.0.42
 annotations:
 service.beta.kubernetes.io/azure-load-balancer-internal: "true"
```

This example assigns `10.224.0.42` to the `loadBalancerIP` resource. Provide your own internal IP address for use with the ingress controller. Make sure that this IP address isn't already in use within your virtual network. Also, if you're using an existing virtual network and subnet, you must configure your AKS cluster with the correct permissions to manage the virtual network and subnet. For more information, see [Use kubenet networking with your own IP address ranges in Azure Kubernetes Service \(AKS\)](#) or [Configure Azure CNI networking in Azure Kubernetes Service \(AKS\)](#).

When you deploy the `nginx-ingress` chart with Helm, add the `-f internal-ingress.yaml` parameter.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
Add the ingress-nginx repository
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx

Set variable for ACR location to use for pulling images
ACR_URL=<REGISTRY_URL>

Use Helm to deploy an NGINX ingress controller
helm install ingress-nginx ingress-nginx/ingress-nginx \
 --version 4.1.3 \
 --namespace ingress-basic \
 --create-namespace \
 --set controller.replicaCount=2 \
 --set controller.nodeSelector."kubernetes\.io/os"=linux \
 --set controller.image.registry=$ACR_URL \
 --set controller.image.image=$CONTROLLER_IMAGE \
 --set controller.image.tag=$CONTROLLER_TAG \
 --set controller.image.digest="" \
 --set controller.admissionWebhooks.patch.nodeSelector."kubernetes\.io/os"=linux \
 --set controller.service.annotations."service\.beta\.kubernetes\.io/azure-load-balancer-health-probe-
request-path"/=healthz \
 --set controller.admissionWebhooks.patch.image.registry=$ACR_URL \
 --set controller.admissionWebhooks.patch.image.image=$PATCH_IMAGE \
 --set controller.admissionWebhooks.patch.image.tag=$PATCH_TAG \
 --set controller.admissionWebhooks.patch.image.digest="" \
 --set defaultBackend.nodeSelector."kubernetes\.io/os"=linux \
 --set defaultBackend.image.registry=$ACR_URL \
 --set defaultBackend.image.image=$DEFAULTBACKEND_IMAGE \
 --set defaultBackend.image.tag=$DEFAULTBACKEND_TAG \
 --set defaultBackend.image.digest="" \
 -f internal-ingress.yaml
```

## Create an ingress controller

To create the ingress controller, use Helm to install `nginx-ingress`. The ingress controller needs to be scheduled on a Linux node. Windows Server nodes shouldn't run the ingress controller. A node selector is specified using the `--set nodeSelector` parameter to tell the Kubernetes scheduler to run the NGINX ingress controller on a Linux-based node.

For added redundancy, two replicas of the NGINX ingress controllers are deployed with the `--set controller.replicaCount` parameter. To fully benefit from running replicas of the ingress controller, make sure there's more than one node in your AKS cluster.

The following example creates a Kubernetes namespace for the ingress resources named *ingress-basic* and is intended to work within that namespace. Specify a namespace for your own environment as needed. If your AKS cluster isn't Kubernetes role-based access control enabled, add `--set rbac.create=false` to the Helm commands.

#### NOTE

If you would like to enable [client source IP preservation](#) for requests to containers in your cluster, add

```
--set controller.service.externalTrafficPolicy=Local
```

to the Helm install command. The client source IP is stored in the request header under *X-Forwarded-For*. When you're using an ingress controller with client source IP preservation enabled, TLS pass-through won't work.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
Add the ingress-nginx repository
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx

Set variable for ACR location to use for pulling images
ACR_URL=<REGISTRY_URL>

Use Helm to deploy an NGINX ingress controller
helm install nginx-ingress ingress-nginx/ingress-nginx \
 --version 4.1.3 \
 --namespace ingress-basic \
 --create-namespace \
 --set controller.replicaCount=2 \
 --set controller.nodeSelector."kubernetes\.io/os"=linux \
 --set controller.image.registry=$ACR_URL \
 --set controller.image.image=$CONTROLLER_IMAGE \
 --set controller.image.tag=$CONTROLLER_TAG \
 --set controller.image.digest="" \
 --set controller.admissionWebhooks.patch.nodeSelector."kubernetes\.io/os"=linux \
 --set controller.service.annotations."service\.beta\.kubernetes\.io/azure-load-balancer-health-probe-
request-path"/=healthz \
 --set controller.admissionWebhooks.patch.image.registry=$ACR_URL \
 --set controller.admissionWebhooks.patch.image.image=$PATCH_IMAGE \
 --set controller.admissionWebhooks.patch.image.tag=$PATCH_TAG \
 --set controller.admissionWebhooks.patch.image.digest="" \
 --set defaultBackend.nodeSelector."kubernetes\.io/os"=linux \
 --set defaultBackend.image.registry=$ACR_URL \
 --set defaultBackend.image.image=$DEFAULTBACKEND_IMAGE \
 --set defaultBackend.image.tag=$DEFAULTBACKEND_TAG \
 --set defaultBackend.image.digest=""
```

## Check the load balancer service

Check the load balancer service by using `kubectl get services`.

```
kubectl get services --namespace ingress-basic -o wide -w ingress-nginx-controller
```

When the Kubernetes load balancer service is created for the NGINX ingress controller, an IP address is assigned under *EXTERNAL-IP*, as shown in the following example output:

NAME AGE	SELECTOR	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
NAME SELECTOR		TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	
ingress-nginx-controller	app.kubernetes.io/component=controller,app.kubernetes.io/instance=ingress-nginx,app.kubernetes.io/name=ingress-nginx	LoadBalancer	10.0.65.205	EXTERNAL-IP	80:30957/TCP,443:32414/TCP	1m

No ingress rules have been created yet, so the NGINX ingress controller's default 404 page is displayed if you browse to the external IP address. Ingress rules are configured in the following steps.

## Run demo applications

To see the ingress controller in action, run two demo applications in your AKS cluster. In this example, you use `kubectl apply` to deploy two instances of a simple *Hello world* application.

Create an `aks-helloworld-one.yaml` file and copy in the following example YAML:

```

apiVersion: apps/v1
kind: Deployment
metadata:
 name: aks-helloworld-one
spec:
 replicas: 1
 selector:
 matchLabels:
 app: aks-helloworld-one
 template:
 metadata:
 labels:
 app: aks-helloworld-one
 spec:
 containers:
 - name: aks-helloworld-one
 image: mcr.microsoft.com/azuredocs/aks-helloworld:v1
 ports:
 - containerPort: 80
 env:
 - name: TITLE
 value: "Welcome to Azure Kubernetes Service (AKS)"

apiVersion: v1
kind: Service
metadata:
 name: aks-helloworld-one
spec:
 type: ClusterIP
 ports:
 - port: 80
 selector:
 app: aks-helloworld-one

```

Create an `aks-helloworld-two.yaml` file and copy in the following example YAML:

```

apiVersion: apps/v1
kind: Deployment
metadata:
 name: aks-helloworld-two
spec:
 replicas: 1
 selector:
 matchLabels:
 app: aks-helloworld-two
 template:
 metadata:
 labels:
 app: aks-helloworld-two
 spec:
 containers:
 - name: aks-helloworld-two
 image: mcr.microsoft.com/azuredocs/aks-helloworld:v1
 ports:
 - containerPort: 80
 env:
 - name: TITLE
 value: "AKS Ingress Demo"

apiVersion: v1
kind: Service
metadata:
 name: aks-helloworld-two
spec:
 type: ClusterIP
 ports:
 - port: 80
 selector:
 app: aks-helloworld-two

```

Run the two demo applications using `kubectl apply`:

```

kubectl apply -f aks-helloworld-one.yaml --namespace ingress-basic
kubectl apply -f aks-helloworld-two.yaml --namespace ingress-basic

```

## Create an ingress route

Both applications are now running on your Kubernetes cluster. To route traffic to each application, create a Kubernetes ingress resource. The ingress resource configures the rules that route traffic to one of the two applications.

In the following example, traffic to `EXTERNAL_IP/hello-world-one` is routed to the service named `aks-helloworld-one`. Traffic to `EXTERNAL_IP/hello-world-two` is routed to the `aks-helloworld-two` service. Traffic to `EXTERNAL_IP/static` is routed to the service named `aks-helloworld-one` for static assets.

Create a file named `hello-world-ingress.yaml` and copy in the following example YAML.

```

apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 name: hello-world-ingress
 annotations:
 nginx.ingress.kubernetes.io/ssl-redirect: "false"
 nginx.ingress.kubernetes.io/use-regex: "true"
 nginx.ingress.kubernetes.io/rewrite-target: /$2
spec:
 ingressClassName: nginx
 rules:
 - http:
 paths:
 - path: /hello-world-one(/|$(.))
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-one
 port:
 number: 80
 - path: /hello-world-two(/|$(.))
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-two
 port:
 number: 80
 - path: /(.*)
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-one
 port:
 number: 80

apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 name: hello-world-ingress-static
 annotations:
 nginx.ingress.kubernetes.io/ssl-redirect: "false"
 nginx.ingress.kubernetes.io/rewrite-target: /static/$2
spec:
 ingressClassName: nginx
 rules:
 - http:
 paths:
 - path: /static(/|$(.))
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-one
 port:
 number: 80

```

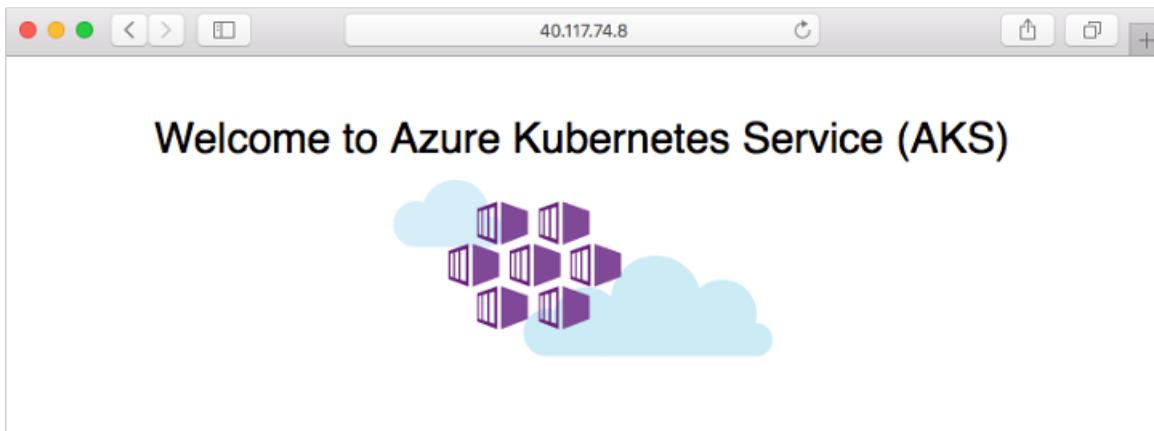
Create the ingress resource using the `kubectl apply` command.

```
kubectl apply -f hello-world-ingress.yaml --namespace ingress-basic
```

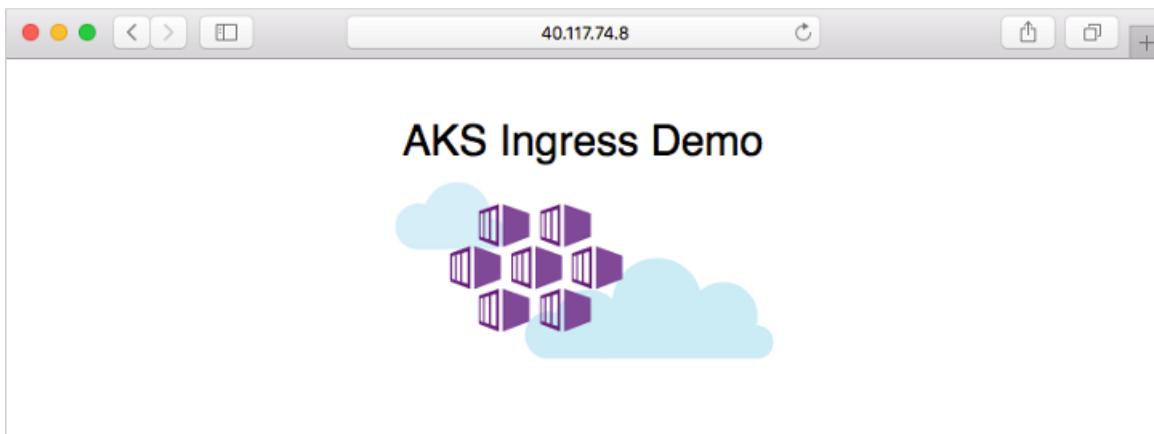
## Test the ingress controller

To test the routes for the ingress controller, browse to the two applications. Open a web browser to the IP address of your NGINX ingress controller, such as *EXTERNAL\_IP*. The first demo application is displayed in the

web browser, as shown in the following example:



Now add the `/hello-world-two` path to the IP address, such as `EXTERNAL_IP/hello-world-two`. The second demo application with the custom title is displayed:



### Test an internal IP address

To test the routes for the ingress controller using an internal IP, create a test pod and attach a terminal session to it:

```
kubectl run -it --rm aks-ingress-test --image=mcr.microsoft.com/dotnet/runtime-deps:6.0 --namespace ingress-basic
```

Install `curl` in the pod using `apt-get`:

```
apt-get update && apt-get install -y curl
```

Now access the address of your Kubernetes ingress controller using `curl`, such as <http://10.224.0.42>. Provide your own internal IP address specified when you deployed the ingress controller.

```
curl -L http://10.224.0.42
```

No path was provided with the address, so the ingress controller defaults to the `/route`. The first demo application is returned, as shown in the following condensed example output:

```
$ curl -L http://10.224.0.42

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
 <link rel="stylesheet" type="text/css" href="/static/default.css">
 <title>Welcome to Azure Kubernetes Service (AKS)</title>
[...]
```

Now add `/hello-world-two` path to the address, such as <http://10.224.0.42/hello-world-two>. The second demo application with the custom title is returned, as shown in the following condensed example output:

```
$ curl -L -k http://10.224.0.42/hello-world-two

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
 <link rel="stylesheet" type="text/css" href="/static/default.css">
 <title>AKS Ingress Demo</title>
[...]
```

## Clean up resources

This article used Helm to install the ingress components and sample apps. When you deploy a Helm chart, many Kubernetes resources are created. These resources include pods, deployments, and services. To clean up these resources, you can either delete the entire sample namespace, or the individual resources.

### Delete the sample namespace and all resources

To delete the entire sample namespace, use the `kubectl delete` command and specify your namespace name. All the resources in the namespace are deleted.

```
kubectl delete namespace ingress-basic
```

### Delete resources individually

Alternatively, a more granular approach is to delete the individual resources created. List the Helm releases with the `helm list` command. Look for charts named `nginx-ingress` and `aks-helloworld`, as shown in the following example output:

```
$ helm list --namespace ingress-basic

NAME NAMESPACE REVISION UPDATED STATUS
CHART
nginx-ingress ingress-basic 1 2020-01-06 19:55:46.358275 -0600 CST deployed
nginx-ingress-1.27.1 0.26.1
```

Uninstall the releases with the `helm uninstall` command. The following example uninstalls the NGINX ingress deployment.

```
$ helm uninstall ingress-nginx --namespace ingress-basic

release "ingress-nginx" uninstalled
```

Next, remove the two sample applications:

```
kubectl delete -f aks-helloworld-one.yaml --namespace ingress-basic
kubectl delete -f aks-helloworld-two.yaml --namespace ingress-basic
```

Remove the ingress route that directed traffic to the sample apps:

```
kubectl delete -f hello-world-ingress.yaml
```

Finally, you can delete the itself namespace. Use the `kubectl delete` command and specify your namespace name:

```
kubectl delete namespace ingress-basic
```

## Next steps

To configure TLS with your existing ingress components, see [Use TLS with an ingress controller](#).

To configure your AKS cluster to use HTTP application routing, see [Enable the HTTP application routing add-on](#).

This article included some external components to AKS. To learn more about these components, see the following project pages:

- [Helm CLI](#)
- [NGINX ingress controller](#)

# Use TLS with an ingress controller on Azure Kubernetes Service (AKS)

10/27/2022 • 13 minutes to read • [Edit Online](#)

The transport layer security (TLS) protocol uses certificates to provide security for communication, encryption, authentication, and integrity. Using TLS with an ingress controller on AKS allows you to secure communication between your applications and experience the benefits of an ingress controller.

You can bring your own certificates and integrate them with the Secrets Store CSI driver. Alternatively, you can use [cert-manager](#), which automatically generates and configures [Let's Encrypt](#) certificates. Two applications run in the AKS cluster, each of which is accessible over a single IP address.

## NOTE

There are two open source ingress controllers for Kubernetes based on Nginx: one is maintained by the Kubernetes community ([kubernetes/ingress-nginx](#)), and one is maintained by NGINX, Inc. ([nginxinc/kubernetes-ingress](#)). This article uses the Kubernetes community ingress controller.

## Before you begin

- This article assumes you have an ingress controller and applications set up. If you need an ingress controller or example applications, see [Create an ingress controller](#).
- This article uses [Helm 3](#) to install the NGINX ingress controller on a [supported version of Kubernetes](#). Make sure you're using the latest release of Helm and have access to the `ingress-nginx` and `jetstack` Helm repositories. The steps outlined in this article may not be compatible with previous versions of the Helm chart, NGINX ingress controller, or Kubernetes.
  - For more information on configuring and using Helm, see [Install applications with Helm in Azure Kubernetes Service \(AKS\)](#). For upgrade instructions, see the [Helm install docs](#).
- This article assumes you have an existing AKS cluster with an integrated Azure Container Registry (ACR). For more information on creating an AKS cluster with an integrated ACR, see [Authenticate with Azure Container Registry from Azure Kubernetes Service](#).
- If you're using Azure CLI, this article requires that you're running the Azure CLI version 2.0.64 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).
- If you're using Azure PowerShell, this article requires that you're running Azure PowerShell version 5.9.0 or later. Run `Get-InstalledModule -Name Az` to find the version. If you need to install or upgrade, see [Install Azure PowerShell](#).

## Use TLS with your own certificates with Secrets Store CSI Driver

To use TLS with your own certificates with Secrets Store CSI Driver, you need an AKS cluster with the Secrets Store CSI Driver configured and an Azure Key Vault instance. For more information, see [Set up Secrets Store CSI Driver to enable NGINX Ingress Controller with TLS](#).

## Use TLS with Let's Encrypt certificates

To use TLS with [Let's Encrypt](#) certificates, you'll deploy [cert-manager](#), which automatically generates and

configures Let's Encrypt certificates.

## Import the cert-manager images used by the Helm chart into your ACR

- [Azure CLI](#)
- [Azure PowerShell](#)

Use `az acr import` to import the following images into your ACR.

```
REGISTRY_NAME=<REGISTRY_NAME>
CERT_MANAGER_REGISTRY=quay.io
CERT_MANAGER_TAG=v1.8.0
CERT_MANAGER_IMAGE_CONTROLLER=jetstack/cert-manager-controller
CERT_MANAGER_IMAGE_WEBHOOK=jetstack/cert-manager-webhook
CERT_MANAGER_IMAGE_CAINJECTOR=jetstack/cert-manager-cainjector

az acr import --name $REGISTRY_NAME --source
$CERT_MANAGER_REGISTRY/$CERT_MANAGER_IMAGE_CONTROLLER:$CERT_MANAGER_TAG --image
$CERT_MANAGER_IMAGE_CONTROLLER:$CERT_MANAGER_TAG
az acr import --name $REGISTRY_NAME --source
$CERT_MANAGER_REGISTRY/$CERT_MANAGER_IMAGE_WEBHOOK:$CERT_MANAGER_TAG --image
$CERT_MANAGER_IMAGE_WEBHOOK:$CERT_MANAGER_TAG
az acr import --name $REGISTRY_NAME --source
$CERT_MANAGER_REGISTRY/$CERT_MANAGER_IMAGE_CAINJECTOR:$CERT_MANAGER_TAG --image
$CERT_MANAGER_IMAGE_CAINJECTOR:$CERT_MANAGER_TAG
```

### NOTE

In addition to importing container images into your ACR, you can import Helm charts into your ACR. For more information, see [Push and pull Helm charts to an Azure Container Registry](#).

## Ingress controller configuration options

An NGINX ingress controller is created with a new public IP address assignment by default. This public IP address is only static for the lifespan of the ingress controller. If you delete the ingress controller, the public IP address assignment will be lost. If you create another ingress controller, a new public IP address will be assigned.

You can configure your ingress controller using one of the following methods:

- Using a dynamic public IP address.
- Using a static public IP address.

## Use a static public IP address

A common configuration requirement is to provide the NGINX ingress controller an existing static public IP address. The static public IP address remains if the ingress controller is deleted.

Follow the commands below to create an IP address that will be deleted if you delete your AKS cluster.

- [Azure CLI](#)
- [Azure PowerShell](#)

Get the resource group name of the AKS cluster with the `az aks show` command.

```
az aks show --resource-group myResourceGroup --name myAKSCluster --query nodeResourceGroup -o tsv
```

Next, create a public IP address with the *static* allocation method using the `az network public-ip create`

command. The following example creates a public IP address named *myAKSPublicIP* in the AKS cluster resource group obtained in the previous step.

```
az network public-ip create --resource-group MC_myResourceGroup_myAKSCluster_eastus --name myAKSPublicIP --sku Standard --allocation-method static --query publicIp.ipAddress -o tsv
```

#### NOTE

Alternatively, you can create an IP address in a different resource group, which can be managed separately from your AKS cluster. If you create an IP address in a different resource group, ensure the following are true:

- The cluster identity used by the AKS cluster has delegated permissions to the resource group, such as *Network Contributor*.
- Add the

```
--set controller.service.annotations."service\.beta\.kubernetes\.io/azure-load-balancer-resource-group"="<RESOURCE_GROUP>"
```

parameter. Replace *<RESOURCE\_GROUP>* with the name of the resource group where the IP address resides.

You must pass a parameter to the Helm release when you upgrade the ingress controller. This ensures that the ingress controller service is made aware of the load balancer that will be allocated to it. For the HTTPS certificates to work correctly, a DNS name label is used to configure a fully qualified domain name (FQDN) for the ingress controller IP address.

1. Add the

```
--set controller.service.annotations."service\.beta\.kubernetes\.io/azure-dns-label-name"="<DNS_LABEL>"
```

parameter. The DNS label can be set either when the ingress controller is first deployed, or it can be configured later.

2. Add the `--set controller.service.loadBalancerIP="<STATIC_IP>"` parameter. Specify your own public IP address that was created in the previous step.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
DNS_LABEL="demo-aks-ingress"
NAMESPACE="ingress-basic"
STATIC_IP=<STATIC_IP>

helm upgrade nginx-ingress ingress-nginx/ingress-nginx \
--namespace $NAMESPACE \
--set controller.service.annotations."service\.beta\.kubernetes\.io/azure-dns-label-name"=$DNS_LABEL \
--set controller.service.loadBalancerIP=$STATIC_IP
```

For more information, see [Use a static public IP address and DNS label with the AKS load balancer](#).

## Use a dynamic IP address

An Azure public IP address is created for the ingress controller upon creation. This public IP address is static for the lifespan of the ingress controller. If you delete the ingress controller, the public IP address assignment will be lost. If you create another ingress controller, a new public IP address will be assigned.

To get the public IP address, use the `kubectl get service` command.

```
kubectl --namespace ingress-basic get services -o wide -w nginx-ingress-ingress-nginx-controller
```

The example output shows the details about the ingress controller.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)
AGE	SELECTOR			
nginx-ingress-ingress-nginx-controller	LoadBalancer	10.0.74.133	EXTERNAL_IP	
80:32486/TCP, 443:30953/TCP	44s	app.kubernetes.io/component=controller,app.kubernetes.io/instance=nginx-ingress,app.kubernetes.io/name=ingress-nginx		

## Add an A record to your DNS zone

If you're using a custom domain, you need to add an A record to your DNS zone. Otherwise, you need to configure the public IP address with an FQDN.

- [Azure CLI](#)
- [Azure PowerShell](#)

Add an *A* record to your DNS zone with the external IP address of the NGINX service using [az network dns record-set a add-record](#).

```
az network dns record-set a add-record \
--resource-group myResourceGroup \
--zone-name MY_CUSTOM_DOMAIN \
--record-set-name "*" \
--ipv4-address MY_EXTERNAL_IP
```

## Configure an FQDN for the ingress controller

Optionally, you can configure an FQDN for the ingress controller IP address instead of a custom domain. Your FQDN will be of the form <CUSTOM LABEL>. <AZURE REGION NAME>.cloudapp.azure.com . You can configure it using one of the following methods:

- Setting the DNS label using the Azure CLI or Azure PowerShell
- Setting the DNS label using Helm chart settings

### Method 1: Set the DNS label using the Azure CLI or Azure PowerShell

- [Azure CLI](#)
- [Azure PowerShell](#)

```
Public IP address of your ingress controller
IP="MY_EXTERNAL_IP"

Name to associate with public IP address
DNSNAME="demo-aks-ingress"

Get the resource-id of the public IP
PUBLICIPID=$(az network public-ip list --query "[?ipAddress!=null][?contains(ipAddress, '$IP')].[id]" --output tsv)

Update public IP address with DNS name
az network public-ip update --ids $PUBLICIPID --dns-name $DNSNAME

Display the FQDN
az network public-ip show --ids $PUBLICIPID --query "[dnsSettings.fqdn]" --output tsv
```

### Method 2: Set the DNS label using Helm chart settings

You can pass an annotation setting to your Helm chart configuration by using the

--set controller.service.annotations."service\\.beta\\.kubernetes\\.io/azure-dns-label-name" parameter. This parameter can be set either when the ingress controller is first deployed, or it can be configured later.

The following example shows how to update this setting after the controller has been deployed.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
DNS_LABEL="demo-aks-ingress"
NAMESPACE="ingress-basic"

helm upgrade nginx-ingress ingress-nginx/ingress-nginx \
--namespace $NAMESPACE \
--set controller.service.annotations."service\\.beta\\.kubernetes\\.io/azure-dns-label-name"=$DNS_LABEL
```

## Install cert-manager

The NGINX ingress controller supports TLS termination. There are several ways to retrieve and configure certificates for HTTPS. This article uses [cert-manager](#), which provides automatic [Lets Encrypt](#) certificate generation and management functionality.

To install the cert-manager controller, use the following commands.

- [Azure CLI](#)
- [Azure PowerShell](#)

```
Set variable for ACR location to use for pulling images
ACR_URL=<REGISTRY_URL>

Label the ingress-basic namespace to disable resource validation
kubectl label namespace ingress-basic cert-manager.io/disable-validation=true

Add the Jetstack Helm repository
helm repo add jetstack https://charts.jetstack.io

Update your local Helm chart repository cache
helm repo update

Install the cert-manager Helm chart
helm install cert-manager jetstack/cert-manager \
--namespace ingress-basic \
--version $CERT_MANAGER_TAG \
--set installCRDs=true \
--set nodeSelector."kubernetes\\.io/os"=linux \
--set image.repository=$ACR_URL/$CERT_MANAGER_IMAGE_CONTROLLER \
--set image.tag=$CERT_MANAGER_TAG \
--set webhook.image.repository=$ACR_URL/$CERT_MANAGER_IMAGE_WEBHOOK \
--set webhook.image.tag=$CERT_MANAGER_TAG \
--set cainjector.image.repository=$ACR_URL/$CERT_MANAGER_IMAGE_CAINJECTOR \
--set cainjector.image.tag=$CERT_MANAGER_TAG
```

For more information on cert-manager configuration, see the [cert-manager project](#).

## Create a CA cluster issuer

Before certificates can be issued, cert-manager requires one of the following:

- An [Issuer](#), which works in a single namespace.
- A [ClusterIssuer](#) resource, which works across all namespaces.

For more information, see the [cert-manager issuer](#) documentation.

Create a cluster issuer, such as `cluster-issuer.yaml`, using the following example manifest. Replace `MY_EMAIL_ADDRESS` with a valid address from your organization.

```
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
 name: letsencrypt
spec:
 acme:
 server: https://acme-v02.api.letsencrypt.org/directory
 email: MY_EMAIL_ADDRESS
 privateKeySecretRef:
 name: letsencrypt
 solvers:
 - http01:
 ingress:
 class: nginx
 podTemplate:
 spec:
 nodeSelector:
 "kubernetes.io/os": linux
```

To create the issuer, use the `kubectl apply` command.

```
kubectl apply -f cluster-issuer.yaml
```

## Update your ingress routes

You need to update your ingress routes to handle traffic to your FQDN or custom domain.

In the following example, traffic is routed as such:

- Traffic to `hello-world-ingress.MY_CUSTOM_DOMAIN` is routed to the `aks-helloworld-one` service.
- Traffic to `hello-world-ingress.MY_CUSTOM_DOMAIN/hello-world-two` is routed to the `aks-helloworld-two` service.
- Traffic to `hello-world-ingress.MY_CUSTOM_DOMAIN/static` is routed to the service named `aks-helloworld-one` for static assets.

### NOTE

If you configured an FQDN for the ingress controller IP address instead of a custom domain, use the FQDN instead of `hello-world-ingress.MY_CUSTOM_DOMAIN`.

For example, if your FQDN is `demo-aks-ingress.eastus.cloudapp.azure.com`, replace `hello-world-ingress.MY_CUSTOM_DOMAIN` with `demo-aks-ingress.eastus.cloudapp.azure.com` in `hello-world-ingress.yaml`.

Create or update the `hello-world-ingress.yaml` file using the following example YAML file. Update the `spec.tls.hosts` and `spec.rules.host` to the DNS name you created in a previous step.

```

apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 name: hello-world-ingress
 annotations:
 nginx.ingress.kubernetes.io/rewrite-target: /$2
 nginx.ingress.kubernetes.io/use-regex: "true"
 cert-manager.io/cluster-issuer: letsencrypt
spec:
 ingressClassName: nginx
 tls:
 - hosts:
 - hello-world-ingress.MY_CUSTOM_DOMAIN
 secretName: tls-secret
 rules:
 - host: hello-world-ingress.MY_CUSTOM_DOMAIN
 http:
 paths:
 - path: /hello-world-one(/|$(.)*)
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-one
 port:
 number: 80
 - path: /hello-world-two(/|$(.)*)
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-two
 port:
 number: 80
 - path: /(.*)
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-one
 port:
 number: 80

apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 name: hello-world-ingress-static
 annotations:
 nginx.ingress.kubernetes.io/ssl-redirect: "false"
 nginx.ingress.kubernetes.io/rewrite-target: /static/$2
spec:
 ingressClassName: nginx
 tls:
 - hosts:
 - hello-world-ingress.MY_CUSTOM_DOMAIN
 secretName: tls-secret
 rules:
 - host: hello-world-ingress.MY_CUSTOM_DOMAIN
 http:
 paths:
 - path: /static(/|$(.)*)
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld-one
 port:
 number: 80

```

Update the ingress resource using the `kubectl apply` command.

```
kubectl apply -f hello-world-ingress.yaml --namespace ingress-basic
```

## Verify a certificate object has been created

Next, a certificate resource must be created. The certificate resource defines the desired X.509 certificate. For more information, see [cert-manager certificates](#). Cert-manager automatically creates a certificate object for you using ingress-shim, which is automatically deployed with cert-manager since v0.2.2. For more information, see the [ingress-shim documentation](#).

To verify that the certificate was created successfully, use the `kubectl get certificate --namespace ingress-basic` command and verify *READY* is *True*. This may take several minutes.

```
kubectl get certificate --namespace ingress-basic
```

The following output shows the certificate's status.

NAME	READY	SECRET	AGE
tls-secret	True	tls-secret	11m

## Test the ingress configuration

Open a web browser to *hello-world-ingress.MY\_CUSTOM\_DOMAIN* or the FQDN of your Kubernetes ingress controller. Ensure the following are true:

- You're redirected to use HTTPS.
- The certificate is *trusted*.
- The demo application is shown in the web browser.
- Add `/hello-world-two` to the end of the domain and ensure the second demo application with the custom title is shown.

## Clean up resources

This article used Helm to install the ingress components, certificates, and sample apps. When you deploy a Helm chart, many Kubernetes resources are created. These resources include pods, deployments, and services. To clean up these resources, you can either delete the entire sample namespace or the individual resources.

### Delete the sample namespace and all resources

To delete the entire sample namespace, use the `kubectl delete` command and specify your namespace name. All the resources in the namespace are deleted.

```
kubectl delete namespace ingress-basic
```

### Delete resources individually

Alternatively, you can delete the resource individually. First, remove the cluster issuer resources.

```
kubectl delete -f cluster-issuer.yaml --namespace ingress-basic
```

List the Helm releases with the `helm list` command. Look for charts named *nginx* and *cert-manager*, as shown in the following example output.

```
$ helm list --namespace ingress-basic
```

NAME	NAMESPACE	REVISION	UPDATED	STATUS
CHART	APP VERSION			
cert-manager	ingress-basic	1	2020-01-15 10:23:36.515514 -0600 CST	deployed
cert-manager-v0.13.0	v0.13.0			
nginx	ingress-basic	1	2020-01-15 10:09:45.982693 -0600 CST	deployed
nginx-ingress-1.29.1	0.27.0			

Uninstall the releases with the `helm uninstall` command. The following example uninstalls the NGINX ingress and cert-manager deployments.

```
$ helm uninstall cert-manager nginx --namespace ingress-basic
```

```
release "cert-manager" uninstalled
release "nginx" uninstalled
```

Next, remove the two sample applications.

```
kubectl delete -f aks-helloworld-one.yaml --namespace ingress-basic
kubectl delete -f aks-helloworld-two.yaml --namespace ingress-basic
```

Remove the ingress route that directed traffic to the sample apps.

```
kubectl delete -f hello-world-ingress.yaml --namespace ingress-basic
```

Finally, you can delete the itself namespace. Use the `kubectl delete` command and specify your namespace name.

```
kubectl delete namespace ingress-basic
```

## Next steps

This article included some external components to AKS. To learn more about these components, see the following project pages:

- [Helm CLI](#)
- [NGINX ingress controller](#)
- [cert-manager](#)

You can also:

- [Enable the HTTP application routing add-on](#)

# HTTP application routing

10/27/2022 • 7 minutes to read • [Edit Online](#)

The HTTP application routing solution makes it easy to access applications that are deployed to your Azure Kubernetes Service (AKS) cluster. When the solution's enabled, it configures an [Ingress controller](#) in your AKS cluster. As applications are deployed, the solution also creates publicly accessible DNS names for application endpoints.

When the add-on is enabled, it creates a DNS Zone in your subscription. For more information about DNS cost, see [DNS pricing](#).

**Caution**

The HTTP application routing add-on is designed to let you quickly create an ingress controller and access your applications. This add-on is not currently designed for use in a production environment and is not recommended for production use. For production-ready ingress deployments that include multiple replicas and TLS support, see [Create an HTTPS ingress controller](#).

## Limitations

- HTTP application routing doesn't currently work with AKS versions 1.22.6+

## HTTP routing solution overview

The add-on deploys two components: a [Kubernetes Ingress controller](#) and an [External-DNS](#) controller.

- **Ingress controller:** The Ingress controller is exposed to the internet by using a Kubernetes service of type LoadBalancer. The Ingress controller watches and implements [Kubernetes Ingress resources](#), which creates routes to application endpoints.
- **External-DNS controller:** Watches for Kubernetes Ingress resources and creates DNS A records in the cluster-specific DNS zone.

## Deploy HTTP routing: CLI

The HTTP application routing add-on can be enabled with the Azure CLI when deploying an AKS cluster. To do so, use the `az aks create` command with the `--enable-addons` argument.

```
az aks create --resource-group myResourceGroup --name myAKSCluster --enable-addons http_application_routing
```

**TIP**

If you want to enable multiple add-ons, provide them as a comma-separated list. For example, to enable HTTP application routing and monitoring, use the format `--enable-addons http_application_routing,monitoring`.

You can also enable HTTP routing on an existing AKS cluster using the `az aks enable-addons` command. To enable HTTP routing on an existing cluster, add the `--addons` parameter and specify `http_application_routing` as shown in the following example:

```
az aks enable-addons --resource-group myResourceGroup --name myAKSCluster --addons http_application_routing
```

After the cluster is deployed or updated, use the `az aks show` command to retrieve the DNS zone name.

```
az aks show --resource-group myResourceGroup --name myAKSCluster --query
addonProfiles.httpApplicationRouting.config.HTTPApplicationRoutingZoneName -o table
```

This name is needed to deploy applications to the AKS cluster and is shown in the following example output:

```
9f9c1fe7-21a1-416d-99cd-3543bb92e4c3.eastus.aksapp.io
```

## Deploy HTTP routing: Portal

The HTTP application routing add-on can be enabled through the Azure portal when deploying an AKS cluster.

Home > Kubernetes services > Create Kubernetes cluster

### Create Kubernetes cluster

X

Basics Scale Authentication Networking Monitoring Tags Review + create

You can change networking settings for your cluster, including enabling HTTP application routing and configuring your network using either the 'Basic' or 'Advanced' options:

- 'Basic' networking creates a new VNet for your cluster using default values.
- 'Advanced' networking allows clusters to use a new or existing VNet with customizable addresses. Application pods are connected directly to the VNet, which allows for native integration with VNet features.

Learn more about networking in Azure Kubernetes Service

HTTP application routing ⓘ  Yes  No

Load balancer ⓘ Standard

Network configuration ⓘ  Basic  Advanced

Review + create  < Previous  Next : Monitoring >

After the cluster is deployed, browse to the auto-created AKS resource group and select the DNS zone. Take note of the DNS zone name. This name is needed to deploy applications to the AKS cluster.

Home > Resource groups > MC\_myAKSCluster\_myAKSCluster\_westeurope > 8d61f730-e2a7-4e57-93ab-48a331a3ee54.westeurope.aksapp.io

DNS zone

8d61f730-e2a7-4e57-93ab-48a331a3ee54.westeurope.aksapp.io

Search (Ctrl+ /) Record set Move Delete zone Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Properties Locks Automation script

Tags (change) Click here to add tags

Search record sets

NAME	TYPE	TTL	VALUE
@	NS	172800	ns1-01.azure-dns.com. ns2-01.azure-dns.net. ns3-01.azure-dns.org. ns4-01.azure-dns.info.
@	SOA	3600	Email: azuredns-hostmaster.microsoft.com Host: ns1-01.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1

## Connect to your AKS cluster

To connect to the Kubernetes cluster from your local computer, you use [kubectl](#), the Kubernetes command-line client.

If you use the Azure Cloud Shell, `kubectl` is already installed. You can also install it locally using the [az aks install-cli](#) command:

```
az aks install-cli
```

To configure `kubectl` to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command. The following example gets credentials for the AKS cluster named *MyAKSCluster* in the *MyResourceGroup*.

```
az aks get-credentials --resource-group MyResourceGroup --name MyAKSCluster
```

## Use HTTP routing

The HTTP application routing solution may only be triggered on Ingress resources that are annotated as follows:

```
annotations:
 kubernetes.io/ingress.class: addon-http-application-routing
```

Create a file named **samples-http-application-routing.yaml** and copy in the following YAML. On line 43, update `<CLUSTER_SPECIFIC_DNS_ZONE>` with the DNS zone name collected in the previous step of this article.

```

apiVersion: apps/v1
kind: Deployment
metadata:
 name: aks-helloworld
spec:
 replicas: 1
 selector:
 matchLabels:
 app: aks-helloworld
 template:
 metadata:
 labels:
 app: aks-helloworld
 spec:
 containers:
 - name: aks-helloworld
 image: mcr.microsoft.com/azuredocs/aks-helloworld:v1
 ports:
 - containerPort: 80
 env:
 - name: TITLE
 value: "Welcome to Azure Kubernetes Service (AKS)"

apiVersion: v1
kind: Service
metadata:
 name: aks-helloworld
spec:
 type: ClusterIP
 ports:
 - port: 80
 selector:
 app: aks-helloworld

apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 name: aks-helloworld
 annotations:
 kubernetes.io/ingress.class: addon-http-application-routing
spec:
 rules:
 - host: aks-helloworld.<CLUSTER_SPECIFIC_DNS_ZONE>
 http:
 paths:
 - path: /
 pathType: Prefix
 backend:
 service:
 name: aks-helloworld
 port:
 number: 80

```

Use the [kubectl apply](#) command to create the resources.

```
kubectl apply -f samples-http-application-routing.yaml
```

The following example shows the created resources:

```
$ kubectl apply -f samples-http-application-routing.yaml

deployment.apps/aks-helloworld created
service/aks-helloworld created
ingress.networking.k8s.io/aks-helloworld created
```

Open a web browser to *aks-helloworld.<CLUSTER\_SPECIFIC\_DNS\_ZONE>*, for example *aks-helloworld.9f9c1fe7-21a1-416d-99cd-3543bb92e4c3.eastus.aksapp.io* and verify you see the demo application. The application may take a few minutes to appear.

## Remove HTTP routing

The HTTP routing solution can be removed using the Azure CLI. To do so run the following command, substituting your AKS cluster and resource group name.

```
az aks disable-addons --addons http_application_routing --name myAKSCluster --resource-group myResourceGroup
--no-wait
```

When the HTTP application routing add-on is disabled, some Kubernetes resources may remain in the cluster. These resources include *configMaps* and *secrets*, and are created in the *kube-system* namespace. To maintain a clean cluster, you may want to remove these resources.

Look for *addon-http-application-routing* resources using the following [kubectl get](#) commands:

```
kubectl get deployments --namespace kube-system
kubectl get services --namespace kube-system
kubectl get configmaps --namespace kube-system
kubectl get secrets --namespace kube-system
```

The following example output shows configMaps that should be deleted:

```
$ kubectl get configmaps --namespace kube-system

NAMESPACE NAME DATA AGE
kube-system addon-http-application-routing-nginx-configuration 0 9m7s
kube-system addon-http-application-routing-tcp-services 0 9m7s
kube-system addon-http-application-routing-udp-services 0 9m7s
```

To delete resources, use the [kubectl delete](#) command. Specify the resource type, resource name, and namespace. The following example deletes one of the previous configmaps:

```
kubectl delete configmaps addon-http-application-routing-nginx-configuration --namespace kube-system
```

Repeat the previous [kubectl delete](#) step for all *addon-http-application-routing* resources that remained in your cluster.

## Troubleshoot

Use the [kubectl logs](#) command to view the application logs for the External-DNS application. The logs should confirm that an A and TXT DNS record were created successfully.

```
$ kubectl logs -f deploy/addon-http-application-routing-external-dns -n kube-system

time="2018-04-26T20:36:19Z" level=info msg="Updating A record named 'aks-helloworld' to '52.242.28.189' for
Azure DNS zone '471756a6-e744-4aa0-aa01-89c4d162a7a7.canadaeast.aksapp.io'."
time="2018-04-26T20:36:21Z" level=info msg="Updating TXT record named 'aks-helloworld' to
'"heritage=external-dns,external-dns/owner=default"' for Azure DNS zone '471756a6-e744-4aa0-aa01-
89c4d162a7a7.canadaeast.aksapp.io'."
```

These records can also be seen on the DNS zone resource in the Azure portal.

NAME	TYPE	TTL	VALUE
@	NS	172800	ns1-01.azure-dns.com. ns2-01.azure-dns.net. ns3-01.azure-dns.org. ns4-01.azure-dns.info.
@	SOA	3600	Email: azuredns-hostmaster.microsoft.com Host: ns1-01.azure-dns.com. Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 300 Serial number: 1
party-clippy	A	300	40.91.216.190
party-clippy	TXT	300	"heritage=external-dns,external-dns/owner=default"

Use the `kubectl logs` command to view the application logs for the Nginx Ingress controller. The logs should confirm the `CREATE` of an Ingress resource and the reload of the controller. All HTTP activity is logged.

```
$ kubectl logs -f deploy/addon-http-application-routing-nginx-ingress-controller -n kube-system

NGINX Ingress controller
 Release: 0.13.0
 Build: git-4bc943a
 Repository: https://github.com/kubernetes/ingress-nginx

I0426 20:30:12.212936 9 flags.go:162] Watching for ingress class: addon-http-application-routing
W0426 20:30:12.213041 9 flags.go:165] only Ingress with class "addon-http-application-routing" will be
processed by this ingress controller
W0426 20:30:12.213505 9 client_config.go:533] Neither --kubeconfig nor --master was specified. Using
the inClusterConfig. This might not work.
I0426 20:30:12.213752 9 main.go:181] Creating API client for https://10.0.0.1:443
I0426 20:30:12.287928 9 main.go:225] Running in Kubernetes Cluster version v1.8 (v1.8.11) - git
(clean) commit 1df6a8381669a6c753f79cb31ca2e3d57ee7c8a3 - platform linux/amd64
I0426 20:30:12.290988 9 main.go:84] validated kube-system/addon-http-application-routing-default-http-
backend as the default backend
I0426 20:30:12.294314 9 main.go:105] service kube-system/addon-http-application-routing-nginx-ingress
validated as source of Ingress status
I0426 20:30:12.426443 9 stat_collector.go:77] starting new nginx stats collector for Ingress
controller running in namespace (class addon-http-application-routing)
I0426 20:30:12.426509 9 stat_collector.go:78] collector extracting information from port 18080
I0426 20:30:12.448779 9 nginx.go:281] starting Ingress controller
I0426 20:30:12.463585 9 event.go:218] Event(v1.ObjectReference{Kind:"ConfigMap", Namespace:"kube-
system", Name:"addon-http-application-routing-nginx-configuration", UID:"2588536c-4990-11e8-a5e1-
0a58ac1f0ef2", APIVersion:"v1", ResourceVersion:"559", FieldPath:""}): type: 'Normal' reason: 'CREATE'
ConfigMap kube-system/addon-http-application-routing-nginx-configuration
I0426 20:30:12.466945 9 event.go:218] Event(v1.ObjectReference{Kind:"ConfigMap", Namespace:"kube-
system", Name:"addon-http-application-routing-tcp-services", UID:"258ca065-4990-11e8-a5e1-0a58ac1f0ef2",
APIVersion:"v1", ResourceVersion:"561", FieldPath:""}): type: 'Normal' reason: 'CREATE' ConfigMap kube-
system/addon-http-application-routing-tcp-services
I0426 20:30:12.467053 9 event.go:218] Event(v1.ObjectReference{Kind:"ConfigMap", Namespace:"kube-
system", Name:"addon-http-application-routing-udp-services", UID:"259023bc-4990-11e8-a5e1-0a58ac1f0ef2",
APIVersion:"v1", ResourceVersion:"562", FieldPath:""}): type: 'Normal' reason: 'CREATE' ConfigMap kube-
system/addon-http-application-routing-udp-services
I0426 20:30:13.649195 9 nginx.go:302] starting NGINX process...
I0426 20:30:13.649347 9 leaderelection.go:175] attempting to acquire leader lease kube-
system/ingress-controller-leader-addon-http-application-routing...
I0426 20:30:13.649776 9 controller.go:170] backend reload required
I0426 20:30:13.649800 9 stat_collector.go:34] changing prometheus collector from to default
I0426 20:30:13.662191 9 leaderelection.go:184] successfully acquired lease kube-system/ingress-
controller-leader-addon-http-application-routing
I0426 20:30:13.662292 9 status.go:196] new leader elected: addon-http-application-routing-nginx-
ingress-controller-5cxntd6
I0426 20:30:13.763362 9 controller.go:179] ingress backend successfully reloaded...
I0426 21:51:55.249327 9 event.go:218] Event(v1.ObjectReference{Kind:"Ingress", Namespace:"default",
Name:"aks-helloworld", UID:"092c9599-499c-11e8-a5e1-0a58ac1f0ef2", APIVersion:"extensions",
ResourceVersion:"7346", FieldPath:""}): type: 'Normal' reason: 'CREATE' Ingress default/aks-helloworld
W0426 21:51:57.908771 9 controller.go:775] service default/aks-helloworld does not have any active
endpoints
I0426 21:51:57.908951 9 controller.go:170] backend reload required
I0426 21:51:58.042932 9 controller.go:179] ingress backend successfully reloaded...
167.220.24.46 - [167.220.24.46] - - [26/Apr/2018:21:53:20 +0000] "GET / HTTP/1.1" 200 234 "" "Mozilla/5.0
(compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" 197 0.001 [default-aks-helloworld-80] 10.244.0.13:8080
234 0.004 200
```

## Clean up

Remove the associated Kubernetes objects created in this article using `kubectl delete`.

```
kubectl delete -f samples-http-application-routing.yaml
```

The example output shows Kubernetes objects have been removed.

```
$ kubectl delete -f samples-http-application-routing.yaml

deployment "aks-helloworld" deleted
service "aks-helloworld" deleted
ingress "aks-helloworld" deleted
```

## Next steps

For information on how to install an HTTPS-secured Ingress controller in AKS, see [HTTPS Ingress on Azure Kubernetes Service \(AKS\)](#).

# Tutorial: Enable application gateway ingress controller add-on for an existing AKS cluster with an existing application gateway

10/27/2022 • 6 minutes to read • [Edit Online](#)

You can use Azure CLI or portal to enable the [application gateway ingress controller \(AGIC\)](#) add-on for an existing [Azure Kubernetes Services \(AKS\)](#) cluster. In this tutorial, you'll learn how to use AGIC add-on to expose your Kubernetes application in an existing AKS cluster through an existing application gateway deployed in separate virtual networks. You'll start by creating an AKS cluster in one virtual network and an application gateway in a separate virtual network to simulate existing resources. You'll then enable the AGIC add-on, peer the two virtual networks together, and deploy a sample application that will be exposed through the application gateway using the AGIC add-on. If you're enabling the AGIC add-on for an existing application gateway and existing AKS cluster in the same virtual network, then you can skip the peering step below. The add-on provides a much faster way of deploying AGIC for your AKS cluster than [through Helm](#) and also offers a fully managed experience.

In this tutorial, you learn how to:

- Create a resource group
- Create a new AKS cluster
- Create a new application gateway
- Enable the AGIC add-on in the existing AKS cluster through Azure CLI
- Enable the AGIC add-on in the existing AKS cluster through Azure portal
- Peer the application gateway virtual network with the AKS cluster virtual network
- Deploy a sample application using AGIC for ingress on the AKS cluster
- Check that the application is reachable through application gateway

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

## Prerequisites

- Use the Bash environment in [Azure Cloud Shell](#). For more information, see [Azure Cloud Shell Quickstart - Bash](#).  
[Launch Cloud Shell](#)
- If you prefer to run CLI reference commands locally, [install](#) the Azure CLI. If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a Docker container](#).
  - If you're using a local installation, sign in to the Azure CLI by using the [az login](#) command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).
  - When you're prompted, install the Azure CLI extension on first use. For more information about extensions, see [Use extensions with the Azure CLI](#).
  - Run [az version](#) to find the version and dependent libraries that are installed. To upgrade to the latest version, run [az upgrade](#).

## Create a resource group

In Azure, you allocate related resources to a resource group. Create a resource group by using [az group create](#). The following example creates a resource group named **myResourceGroup** in the **East US** location (region):

```
az group create --name myResourceGroup --location eastus
```

## Deploy a new AKS cluster

You'll now deploy a new AKS cluster, to simulate having an existing AKS cluster that you want to enable the AGIC add-on for.

In the following example, you'll be deploying a new AKS cluster named **myCluster** using [Azure CNI](#) and [Managed Identities](#) in the resource group you created, **myResourceGroup**.

```
az aks create -n myCluster -g myResourceGroup --network-plugin azure --enable-managed-identity --generate-ssh-keys
```

To configure more parameters for the above command, see [az aks create](#).

### NOTE

A node resource group will be created with the name **MC\_resource-group-name\_cluster-name\_location**.

## Deploy a new application gateway

You'll now deploy a new application gateway, to simulate having an existing application gateway that you want to use to load balance traffic to your AKS cluster, **myCluster**. The name of the application gateway will be **myApplicationGateway**, but you'll need to first create a public IP resource, named **myPublicIp**, and a new virtual network called **myVnet** with address space 10.0.0.0/16, and a subnet with address space 10.0.0.0/24 called **mySubnet**, and deploy your application gateway in **mySubnet** using **myPublicIp**.

### Caution

When you use an AKS cluster and application gateway in separate virtual networks, the address spaces of the two virtual networks must not overlap. The default address space that an AKS cluster deploys in is 10.224.0.0/12.

```
az network public-ip create -n myPublicIp -g myResourceGroup --allocation-method Static --sku Standard
az network vnet create -n myVnet -g myResourceGroup --address-prefix 10.0.0.0/16 --subnet-name mySubnet --subnet-prefix 10.0.0.0/24
az network application-gateway create -n myApplicationGateway -l eastus -g myResourceGroup --sku Standard_v2 --public-ip-address myPublicIp --vnet-name myVnet --subnet mySubnet --priority 100
```

### NOTE

application gateway ingress controller (AGIC) add-on **only** supports application gateway v2 SKUs (Standard and WAF), and **not** the application gateway v1 SKUs.

## Enable the AGIC add-on in existing AKS cluster through Azure CLI

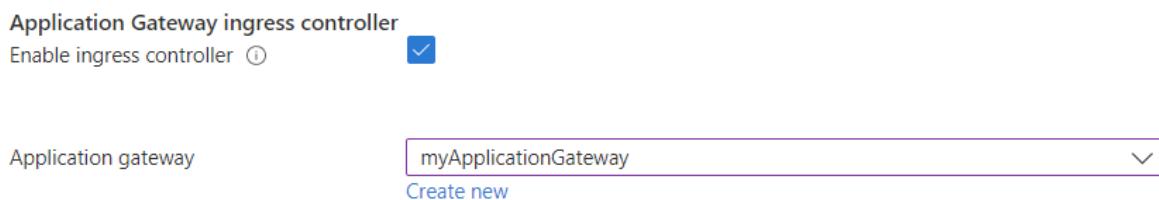
If you'd like to continue using Azure CLI, you can continue to enable the AGIC add-on in the AKS cluster you created, **myCluster**, and specify the AGIC add-on to use the existing application gateway you created,

myApplicationGateway.

```
appgwId=$(az network application-gateway show -n myApplicationGateway -g myResourceGroup -o tsv --query "id")
az aks enable-addons -n myCluster -g myResourceGroup -a ingress-appgw --appgw-id $appgwId
```

## Enable the AGIC add-on in existing AKS cluster through Azure portal

If you'd like to use Azure portal to enable AGIC add-on, go to (<https://aka.ms/azure/portal/aks/agic>) and navigate to your AKS cluster through the portal link. From there, go to the Networking tab within your AKS cluster. You'll see an application gateway ingress controller section, which allows you to enable/disable the ingress controller add-on using the Azure portal. Select the box next to **Enable ingress controller**, and then select the application gateway you created, **myApplicationGateway** from the dropdown menu. Select **Save**.



## Peer the two virtual networks together

Since you deployed the AKS cluster in its own virtual network and the Application gateway in another virtual network, you'll need to peer the two virtual networks together in order for traffic to flow from the Application gateway to the pods in the cluster. Peering the two virtual networks requires running the Azure CLI command two separate times, to ensure that the connection is bi-directional. The first command will create a peering connection from the Application gateway virtual network to the AKS virtual network; the second command will create a peering connection in the other direction.

```
nodeResourceGroup=$(az aks show -n myCluster -g myResourceGroup -o tsv --query "nodeResourceGroup")
aksVnetName=$(az network vnet list -g $nodeResourceGroup -o tsv --query "[0].name")

aksVnetId=$(az network vnet show -n $aksVnetName -g $nodeResourceGroup -o tsv --query "id")
az network vnet peering create -n AppGWtoAKSVnetPeering -g myResourceGroup --vnet-name myVnet --remote-vnet $aksVnetId --allow-vnet-access

appGVnetId=$(az network vnet show -n myVnet -g myResourceGroup -o tsv --query "id")
az network vnet peering create -n AKSToAppGVnetPeering -g $nodeResourceGroup --vnet-name $aksVnetName --remote-vnet $appGVnetId --allow-vnet-access
```

### NOTE

In the "Deploy a new AKS cluster" step above we created AKS with Azure CNI, in case you have an existing AKS cluster using [Kubenet mode](#) you need to update the route table to help the packets destined for a POD IP reach the node which is hosting the pod. A simple way to achieve this is by associating the same route table created by AKS to the Application Gateway's subnet.

## Deploy a sample application using AGIC

You'll now deploy a sample application to the AKS cluster you created that will use the AGIC add-on for Ingress and connect the application gateway to the AKS cluster. First, you'll get credentials to the AKS cluster you deployed by running the `az aks get-credentials` command.

```
az aks get-credentials -n myCluster -g myResourceGroup
```

Once you have the credentials to the cluster you created, run the following command to set up a sample application that uses AGIC for Ingress to the cluster. AGIC will update the application gateway you set up earlier with corresponding routing rules to the new sample application you deployed.

```
kubectl apply -f https://raw.githubusercontent.com/Azure/application-gateway-kubernetes-ingress/master/docs/examples/aspnetapp.yaml
```

## Check that the application is reachable

Now that the application gateway is set up to serve traffic to the AKS cluster, let's verify that your application is reachable. You'll first get the IP address of the Ingress.

```
kubectl get ingress
```

Check that the sample application you created is up and running by either visiting the IP address of the application gateway that you got from running the above command or check with `curl`. It may take application gateway a minute to get the update, so if the application gateway is still in an "Updating" state on Azure portal, then let it finish before trying to reach the IP address.

## Clean up resources

When no longer needed, delete all resources created in this tutorial by deleting `myResourceGroup` and `MC_myResourceGroup_myCluster_eastus` resource groups:

```
az group delete --name myResourceGroup
az group delete --name MC_myResourceGroup_myCluster_eastus
```

## Next steps

[Learn more about disabling the AGIC add-on](#)

# Control egress traffic for cluster nodes in Azure Kubernetes Service (AKS)

10/27/2022 • 26 minutes to read • [Edit Online](#)

This article provides the necessary details that allow you to secure outbound traffic from your Azure Kubernetes Service (AKS). It contains the cluster requirements for a base AKS deployment, and additional requirements for optional addons and features. [An example will be provided at the end on how to configure these requirements with Azure Firewall](#). However, you can apply this information to any outbound restriction method or appliance.

## Background

AKS clusters are deployed on a virtual network. This network can be managed (created by AKS) or custom (pre-configured by the user beforehand). In either case, the cluster has **outbound** dependencies on services outside of that virtual network (the service has no inbound dependencies).

For management and operational purposes, nodes in an AKS cluster need to access certain ports and fully qualified domain names (FQDNs). These endpoints are required for the nodes to communicate with the API server, or to download and install core Kubernetes cluster components and node security updates. For example, the cluster needs to pull base system container images from Microsoft Container Registry (MCR).

The AKS outbound dependencies are almost entirely defined with FQDNs, which don't have static addresses behind them. The lack of static addresses means that Network Security Groups can't be used to lock down the outbound traffic from an AKS cluster.

By default, AKS clusters have unrestricted outbound (egress) internet access. This level of network access allows nodes and services you run to access external resources as needed. If you wish to restrict egress traffic, a limited number of ports and addresses must be accessible to maintain healthy cluster maintenance tasks. The simplest solution to securing outbound addresses lies in use of a firewall device that can control outbound traffic based on domain names. Azure Firewall, for example, can restrict outbound HTTP and HTTPS traffic based on the FQDN of the destination. You can also configure your preferred firewall and security rules to allow these required ports and addresses.

### IMPORTANT

This document covers only how to lock down the traffic leaving the AKS subnet. AKS has no ingress requirements by default. Blocking **internal subnet traffic** using network security groups (NSGs) and firewalls is not supported. To control and block the traffic within the cluster, use [Network Policies](#).

## Required outbound network rules and FQDNs for AKS clusters

The following network and FQDN/application rules are required for an AKS cluster, you can use them if you wish to configure a solution other than Azure Firewall.

- IP Address dependencies are for non-HTTP/S traffic (both TCP and UDP traffic)
- FQDN HTTP/HTTPS endpoints can be placed in your firewall device.
- Wildcard HTTP/HTTPS endpoints are dependencies that can vary with your AKS cluster based on a number of qualifiers.
- AKS uses an admission controller to inject the FQDN as an environment variable to all deployments under kube-system and gatekeeper-system, that ensures all system communication between nodes and API server

uses the API server FQDN and not the API server IP.

- If you have an app or solution that needs to talk to the API server, you must add an **additional** network rule to allow *TCP communication to port 443 of your API server's IP*.
- On rare occasions, if there's a maintenance operation your API server IP might change. Planned maintenance operations that can change the API server IP are always communicated in advance.

### Azure Global required network rules

The required network rules and IP address dependencies are:

DESTINATION ENDPOINT	PROTOCOL	PORT	USE
<code>*:1194</code> <i>Or</i> <code>ServiceTag -</code> <code>AzureCloud.&lt;Region&gt;:1194</code> <i>Or</i> <code>Regional CIDRs -</code> <code>RegionCIDRs:1194</code> <i>Or</i> <code>APIServerPublicIP:1194</code> <code>(only known after cluster creation)</code>	UDP	1194	For tunneled secure communication between the nodes and the control plane. This is not required for <a href="#">private clusters</a> , or for clusters with the <i>knettivity-agent</i> enabled.
<code>*:9000</code> <i>Or</i> <code>ServiceTag -</code> <code>AzureCloud.&lt;Region&gt;:9000</code> <i>Or</i> <code>Regional CIDRs -</code> <code>RegionCIDRs:9000</code> <i>Or</i> <code>APIServerPublicIP:9000</code> <code>(only known after cluster creation)</code>	TCP	9000	For tunneled secure communication between the nodes and the control plane. This is not required for <a href="#">private clusters</a> , or for clusters with the <i>knettivity-agent</i> enabled.
<code>*:123</code> or <code>ntp.ubuntu.com:123</code> (if using Azure Firewall network rules)	UDP	123	Required for Network Time Protocol (NTP) time synchronization on Linux nodes. This is not required for nodes provisioned after March 2021.
<code>CustomDNSIP:53</code> <code>(if using custom DNS servers)</code>	UDP	53	If you're using custom DNS servers, you must ensure they're accessible by the cluster nodes.
<code>APIServerPublicIP:443</code> <code>(if running pods/deployments that access the API Server)</code>	TCP	443	Required if running pods/deployments that access the API Server, those pods/deployments would use the API IP. This port is not required for <a href="#">private clusters</a> .

### Azure Global required FQDN / application rules

The following FQDN / application rules are required:

DESTINATION FQDN	PORT	USE
*.hcp.<location>.azmk8s.io	HTTPS:443	Required for Node <-> API server communication. Replace <location> with the region where your AKS cluster is deployed. This is required for clusters with <i>konnectivity-agent</i> enabled. Konnectivity also uses Application-Layer Protocol Negotiation (ALPN) to communicate between agent and server. Blocking or rewriting the ALPN extension will cause a failure. This is not required for <a href="#">private clusters</a> .
mcr.microsoft.com	HTTPS:443	Required to access images in Microsoft Container Registry (MCR). This registry contains first-party images/charts (for example, coreDNS, etc.). These images are required for the correct creation and functioning of the cluster, including scale and upgrade operations.
*.data.mcr.microsoft.com	HTTPS:443	Required for MCR storage backed by the Azure content delivery network (CDN).
management.azure.com	HTTPS:443	Required for Kubernetes operations against the Azure API.
login.microsoftonline.com	HTTPS:443	Required for Azure Active Directory authentication.
packages.microsoft.com	HTTPS:443	This address is the Microsoft packages repository used for cached <i>apt-get</i> operations. Example packages include Moby, PowerShell, and Azure CLI.
acs-mirror.azureedge.net	HTTPS:443	This address is for the repository required to download and install required binaries like kubenet and Azure CNI.

## Azure China 21Vianet required network rules

The required network rules and IP address dependencies are:

DESTINATION ENDPOINT	PROTOCOL	PORT	USE
*:1194 <i>Or</i> ServiceTag - AzureCloud.Region:1194 <i>Or</i> Regional CIDRs - RegionCIDRs:1194 <i>Or</i> APIServerPublicIP:1194 (only known after cluster creation)	UDP	1194	For tunneled secure communication between the nodes and the control plane.

DESTINATION ENDPOINT	PROTOCOL	PORT	USE
<pre>*:9000 Or ServiceTag - AzureCloud.&lt;Region&gt;:9000</pre> <p>Or</p> <pre>Regional CIDRs - RegionCIDRs:9000 Or APIServerPublicIP:9000 (only known after cluster creation)</pre>	TCP	9000	For tunneled secure communication between the nodes and the control plane.
<pre>*:22 Or ServiceTag - AzureCloud.&lt;Region&gt;:22 Or Regional CIDRs - RegionCIDRs:22 Or APIServerPublicIP:22 (only known after cluster creation)</pre>	TCP	22	For tunneled secure communication between the nodes and the control plane.
<pre>*:123 or ntp.ubuntu.com:123 (if using Azure Firewall network rules)</pre>	UDP	123	Required for Network Time Protocol (NTP) time synchronization on Linux nodes.
<pre>CustomDNSIP:53 (if using custom DNS servers)</pre>	UDP	53	If you're using custom DNS servers, you must ensure they're accessible by the cluster nodes.
<pre>APIServerPublicIP:443 (if running pods/deployments that access the API Server)</pre>	TCP	443	Required if running pods/deployments that access the API Server, those pod/deployments would use the API IP.

#### Azure China 21Vianet required FQDN / application rules

The following FQDN / application rules are required:

DESTINATION FQDN	PORT	USE
*.hcp. <location>.cx.prod.service.azk8s.cn	HTTPS:443	Required for Node <-> API server communication. Replace <location> with the region where your AKS cluster is deployed.
*.tun. <location>.cx.prod.service.azk8s.cn	HTTPS:443	Required for Node <-> API server communication. Replace <location> with the region where your AKS cluster is deployed.
mcr.microsoft.com	HTTPS:443	Required to access images in Microsoft Container Registry (MCR). This registry contains first-party images/charts (for example, coreDNS, etc.). These images are required for the correct creation and functioning of the cluster, including scale and upgrade operations.
.data.mcr.microsoft.com	HTTPS:443	Required for MCR storage backed by the Azure Content Delivery Network (CDN).
management.chinacloudapi.cn	HTTPS:443	Required for Kubernetes operations against the Azure API.
login.chinacloudapi.cn	HTTPS:443	Required for Azure Active Directory authentication.
packages.microsoft.com	HTTPS:443	This address is the Microsoft packages repository used for cached <i>apt-get</i> operations. Example packages include Moby, PowerShell, and Azure CLI.
*.azk8s.cn	HTTPS:443	This address is for the repository required to download and install required binaries like kubenet and Azure CNI.

## Azure US Government required network rules

The required network rules and IP address dependencies are:

DESTINATION ENDPOINT	PROTOCOL	PORT	USE
*:1194 <i>Or</i> ServiceTag - AzureCloud. <Region>:1194 <i>Or</i> Regional CIDRs - RegionCIDRs:1194 <i>Or</i> APIServerPublicIP:1194 (only known after cluster creation)	UDP	1194	For tunneled secure communication between the nodes and the control plane.

DESTINATION ENDPOINT	PROTOCOL	PORT	USE
<p>*:9000</p> <p>Or</p> <p>ServiceTag -</p> <p>AzureCloud. &lt;Region&gt;:9000</p> <p>Or</p> <p>Regional CIDRs -</p> <p>RegionCIDRs:9000</p> <p>Or</p> <p>APIServerPublicIP:9000</p> <p>(only known after cluster creation)</p>	TCP	9000	For tunneled secure communication between the nodes and the control plane.
<p>*:123 or</p> <p>ntp.ubuntu.com:123 (if using Azure Firewall network rules)</p>	UDP	123	Required for Network Time Protocol (NTP) time synchronization on Linux nodes.
<p>CustomDNSIP:53</p> <p>(if using custom DNS servers)</p>	UDP	53	If you're using custom DNS servers, you must ensure they're accessible by the cluster nodes.
<p>APIServerPublicIP:443</p> <p>(if running pods/deployments that access the API Server)</p>	TCP	443	Required if running pods/deployments that access the API Server, those pods/deployments would use the API IP.

### Azure US Government required FQDN / application rules

The following FQDN / application rules are required:

DESTINATION FQDN	PORT	USE
<p>*.hcp. &lt;location&gt;.cx.aks.containerservice.azure.us</p>	HTTPS:443	Required for Node <-> API server communication. Replace <location> with the region where your AKS cluster is deployed.
mcr.microsoft.com	HTTPS:443	Required to access images in Microsoft Container Registry (MCR). This registry contains first-party images/charts (for example, coreDNS, etc.). These images are required for the correct creation and functioning of the cluster, including scale and upgrade operations.
*.data.mcr.microsoft.com	HTTPS:443	Required for MCR storage backed by the Azure content delivery network (CDN).
management.usgovcloudapi.net	HTTPS:443	Required for Kubernetes operations against the Azure API.

DESTINATION FQDN	PORT	USE
login.microsoftonline.us	HTTPS:443	Required for Azure Active Directory authentication.
packages.microsoft.com	HTTPS:443	This address is the Microsoft packages repository used for cached <i>apt-get</i> operations. Example packages include Moby, PowerShell, and Azure CLI.
acs-mirror.azureedge.net	HTTPS:443	This address is for the repository required to install required binaries like kubenet and Azure CNI.

## Optional recommended FQDN / application rules for AKS clusters

The following FQDN / application rules are optional but recommended for AKS clusters:

DESTINATION FQDN	PORT	USE
security.ubuntu.com , azure.archive.ubuntu.com , changelogs.ubuntu.com	HTTP:80	This address lets the Linux cluster nodes download the required security patches and updates.

If you choose to block/not allow these FQDNs, the nodes will only receive OS updates when you do a [node image upgrade](#) or [cluster upgrade](#).

## GPU enabled AKS clusters

### Required FQDN / application rules

The following FQDN / application rules are required for AKS clusters that have GPU enabled:

DESTINATION FQDN	PORT	USE
nvidia.github.io	HTTPS:443	This address is used for correct driver installation and operation on GPU-based nodes.
us.download.nvidia.com	HTTPS:443	This address is used for correct driver installation and operation on GPU-based nodes.
download.docker.com	HTTPS:443	This address is used for correct driver installation and operation on GPU-based nodes.

## Windows Server based node pools

### Required FQDN / application rules

The following FQDN / application rules are required for using Windows Server based node pools:

DESTINATION FQDN	PORT	USE
onegetcdn.azureedge.net, go.microsoft.com	HTTPS:443	To install windows-related binaries
*.mp.microsoft.com, www.msftconnecttest.com, ctldl.windowsupdate.com	HTTP:80	To install windows-related binaries

## AKS addons and integrations

### Microsoft Defender for Containers

#### Required FQDN / application rules

The following FQDN / application rules are required for AKS clusters that have Microsoft Defender for Containers enabled.

FQDN	PORT	USE
login.microsoftonline.com	HTTPS:443	Required for Active Directory Authentication.
*.ods.opinsights.azure.com	HTTPS:443	Required for Microsoft Defender to upload security events to the cloud.
*.oms.opinsights.azure.com	HTTPS:443	Required to Authenticate with LogAnalytics workspaces.

### CSI Secret Store

#### Required FQDN / application rules

The following FQDN / application rules are required for AKS clusters that have CSI Secret Store enabled.

FQDN	PORT	USE
vault.azure.net	HTTPS:443	Required for CSI Secret Store addon pods to talk to Azure KeyVault server.

### Azure Monitor for containers

There are two options to provide access to Azure Monitor for containers, you may allow the Azure Monitor [ServiceTag](#) or provide access to the required FQDN/Application Rules.

#### Required network rules

The following FQDN / application rules are required:

DESTINATION ENDPOINT	PROTOCOL	PORT	USE
ServiceTag - AzureMonitor:443	TCP	443	This endpoint is used to send metrics data and logs to Azure Monitor and Log Analytics.

#### Required FQDN / application rules

The following FQDN / application rules are required for AKS clusters that have the Azure Monitor for containers enabled:

FQDN	PORT	USE
dc.services.visualstudio.com	HTTPS:443	This endpoint is used for metrics and monitoring telemetry using Azure Monitor.
*.ods.opinsights.azure.com	HTTPS:443	This endpoint is used by Azure Monitor for ingesting log analytics data.
*.oms.opinsights.azure.com	HTTPS:443	This endpoint is used by omsagent, which is used to authenticate the log analytics service.
*.monitoring.azure.com	HTTPS:443	This endpoint is used to send metrics data to Azure Monitor.

## Azure Policy

### Required FQDN / application rules

The following FQDN / application rules are required for AKS clusters that have the Azure Policy enabled.

FQDN	PORT	USE
data.policy.core.windows.net	HTTPS:443	This address is used to pull the Kubernetes policies and to report cluster compliance status to policy service.
store.policy.core.windows.net	HTTPS:443	This address is used to pull the Gatekeeper artifacts of built-in policies.
dc.services.visualstudio.com	HTTPS:443	Azure Policy add-on that sends telemetry data to applications insights endpoint.

### Azure China 21Vianet Required FQDN / application rules

The following FQDN / application rules are required for AKS clusters that have the Azure Policy enabled.

FQDN	PORT	USE
data.policy.azure.cn	HTTPS:443	This address is used to pull the Kubernetes policies and to report cluster compliance status to policy service.
store.policy.azure.cn	HTTPS:443	This address is used to pull the Gatekeeper artifacts of built-in policies.

### Azure US Government Required FQDN / application rules

The following FQDN / application rules are required for AKS clusters that have the Azure Policy enabled.

FQDN	PORT	USE

FQDN	PORT	USE
data.policy.azure.us	HTTPS:443	This address is used to pull the Kubernetes policies and to report cluster compliance status to policy service.
store.policy.azure.us	HTTPS:443	This address is used to pull the Gatekeeper artifacts of built-in policies.

## Cluster extensions

### Required FQDN / application rules

The following FQDN / application rules are required for using cluster extensions on AKS clusters.

FQDN	PORT	USE
<region>.dp.kubernetesconfiguration.a	HTTPS:443	This address is used to fetch configuration information from the Cluster Extensions service and report extension status to the service.
mcr.microsoft.com, *.data.mcr.microsoft.com	HTTPS:443	This address is required to pull container images for installing cluster extension agents on AKS cluster.

### Azure US Government Required FQDN / application rules

The following FQDN / application rules are required for using cluster extensions on AKS clusters.

FQDN	PORT	USE
<region>.dp.kubernetesconfiguration.a	HTTPS:443	This address is used to fetch configuration information from the Cluster Extensions service and report extension status to the service.
mcr.microsoft.com, *.data.mcr.microsoft.com	HTTPS:443	This address is required to pull container images for installing cluster extension agents on AKS cluster.

#### NOTE

If any addon does not explicitly stated here, that means the core requirements are covering it.

## Restrict egress traffic using Azure firewall

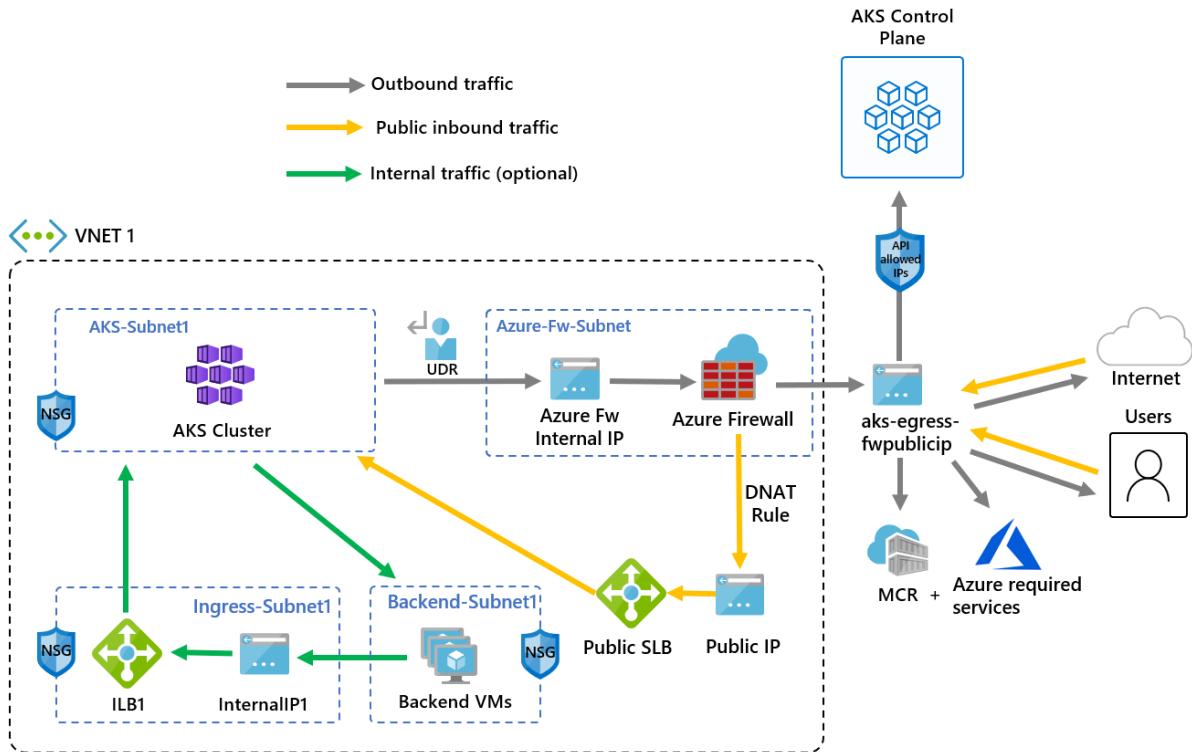
Azure Firewall provides an Azure Kubernetes Service ( AzureKubernetesService ) FQDN Tag to simplify this configuration.

## NOTE

The FQDN tag contains all the FQDNs listed above and is kept automatically up to date.

We recommend having a minimum of 20 Frontend IPs on the Azure Firewall for production scenarios to avoid incurring in SNAT port exhaustion issues.

Below is an example architecture of the deployment:



- Public Ingress is forced to flow through firewall filters
  - AKS agent nodes are isolated in a dedicated subnet.
  - Azure Firewall is deployed in its own subnet.
  - A DNAT rule translates the FW public IP into the LB frontend IP.
- Outbound requests start from agent nodes to the Azure Firewall internal IP using a user-defined route
  - Requests from AKS agent nodes follow a UDR that has been placed on the subnet the AKS cluster was deployed into.
  - Azure Firewall egresses out of the virtual network from a public IP frontend
  - Access to the public internet or other Azure services flows to and from the firewall frontend IP address
  - Optionally, access to the AKS control plane is protected by API server Authorized IP ranges, which includes the firewall public frontend IP address.
- Internal Traffic
  - Optionally, instead or in addition to a Public Load Balancer you can use an Internal Load Balancer for internal traffic, which you could isolate on its own subnet as well.

The below steps make use of Azure Firewall's `AzureKubernetesService` FQDN tag to restrict the outbound traffic from the AKS cluster and provide an example how to configure public inbound traffic via the firewall.

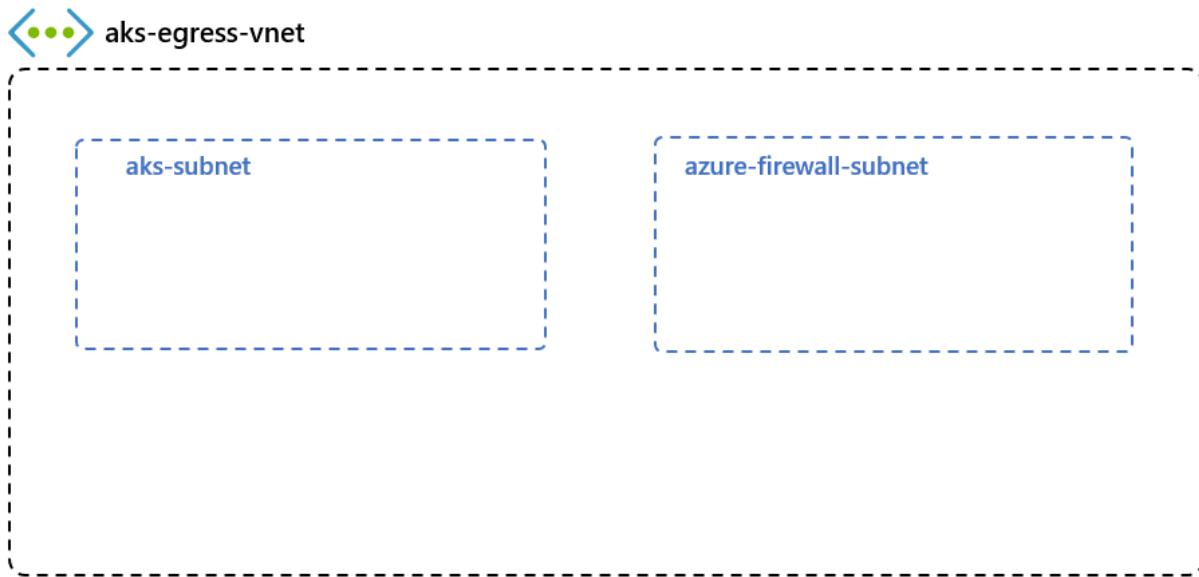
### Set configuration via environment variables

Define a set of environment variables to be used in resource creations.

```
PREFIX="aks-egress"
RG="${PREFIX}-rg"
LOC="eastus"
PLUGIN=azure
AKSNAME="${PREFIX}"
VNET_NAME="${PREFIX}-vnet"
AKSSUBNET_NAME="aks-subnet"
DO NOT CHANGE FWSUBNET_NAME - This is currently a requirement for Azure Firewall.
FWSUBNET_NAME="AzureFirewallSubnet"
FWNAME="${PREFIX}-fw"
FWPUBLICIP_NAME="${PREFIX}-fwpublicip"
FWIPCONFIG_NAME="${PREFIX}-fwconfig"
FWROUTE_TABLE_NAME="${PREFIX}-fwrt"
FWROUTE_NAME="${PREFIX}-fwrn"
FWROUTE_NAME_INTERNET="${PREFIX}-fwinternet"
```

### Create a virtual network with multiple subnets

Provision a virtual network with two separate subnets, one for the cluster, one for the firewall. Optionally you could also create one for internal service ingress.



Create a resource group to hold all of the resources.

```
Create Resource Group

az group create --name $RG --location $LOC
```

Create a virtual network with two subnets to host the AKS cluster and the Azure Firewall. Each will have their own subnet. Let's start with the AKS network.

```

Dedicated virtual network with AKS subnet

az network vnet create \
--resource-group $RG \
--name $VNET_NAME \
--location $LOC \
--address-prefixes 10.42.0.0/16 \
--subnet-name $AKSSUBNET_NAME \
--subnet-prefix 10.42.1.0/24

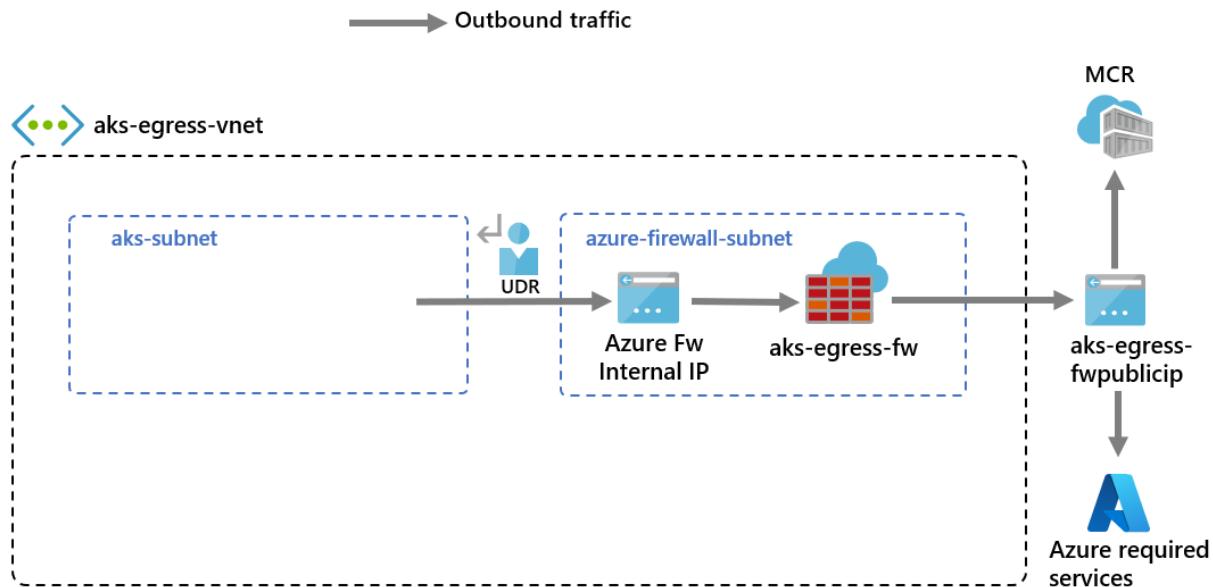
Dedicated subnet for Azure Firewall (Firewall name cannot be changed)

az network vnet subnet create \
--resource-group $RG \
--vnet-name $VNET_NAME \
--name $FWSUBNET_NAME \
--address-prefix 10.42.2.0/24

```

## Create and set up an Azure Firewall with a UDR

Azure Firewall inbound and outbound rules must be configured. The main purpose of the firewall is to enable organizations to configure granular ingress and egress traffic rules into and out of the AKS Cluster.



### IMPORTANT

If your cluster or application creates a large number of outbound connections directed to the same or small subset of destinations, you might require more firewall frontend IPs to avoid maxing out the ports per frontend IP. For more information on how to create an Azure firewall with multiple IPs, see [here](#)

Create a standard SKU public IP resource that will be used as the Azure Firewall frontend address.

```
az network public-ip create -g $RG -n $FWPUBLICIP_NAME -l $LOC --sku "Standard"
```

Register the preview cli-extension to create an Azure Firewall.

```
Install Azure Firewall preview CLI extension

az extension add --name azure-firewall

Deploy Azure Firewall

az network firewall create -g $RG -n $FWNAME -l $LOC --enable-dns-proxy true
```

The IP address created earlier can now be assigned to the firewall frontend.

#### NOTE

Set up of the public IP address to the Azure Firewall may take a few minutes. To leverage FQDN on network rules we need DNS proxy enabled, when enabled the firewall will listen on port 53 and will forward DNS requests to the DNS server specified above. This will allow the firewall to translate that FQDN automatically.

```
Configure Firewall IP Config

az network firewall ip-config create -g $RG -f $FWNAME -n $FWIPCONFIG_NAME --public-ip-address
$FWPUBLICIP_NAME --vnet-name $VNET_NAME
```

When the previous command has succeeded, save the firewall frontend IP address for configuration later.

```
Capture Firewall IP Address for Later Use

FWPUBLIC_IP=$(az network public-ip show -g $RG -n $FWPUBLICIP_NAME --query "ipAddress" -o tsv)
FWPRIVATE_IP=$(az network firewall show -g $RG -n $FWNAME --query "ipConfigurations[0].privateIpAddress" -o tsv)
```

#### NOTE

If you use secure access to the AKS API server with [authorized IP address ranges](#), you need to add the firewall public IP into the authorized IP range.

## Create a UDR with a hop to Azure Firewall

Azure automatically routes traffic between Azure subnets, virtual networks, and on-premises networks. If you want to change any of Azure's default routing, you do so by creating a route table.

Create an empty route table to be associated with a given subnet. The route table will define the next hop as the Azure Firewall created above. Each subnet can have zero or one route table associated to it.

```
Create UDR and add a route for Azure Firewall

az network route-table create -g $RG -l $LOC --name $FWRROUTE_TABLE_NAME
az network route-table route create -g $RG --name $FWRROUTE_NAME --route-table-name $FWRROUTE_TABLE_NAME --
address-prefix 0.0.0.0/0 --next-hop-type VirtualAppliance --next-hop-ip-address $FWPRIVATE_IP
az network route-table route create -g $RG --name $FWRROUTE_NAME_INTERNET --route-table-name
$FWRROUTE_TABLE_NAME --address-prefix $FWPUBLIC_IP/32 --next-hop-type Internet
```

See [virtual network route table documentation](#) about how you can override Azure's default system routes or add additional routes to a subnet's route table.

## Adding firewall rules

#### NOTE

For applications outside of the kube-system or gatekeeper-system namespaces that needs to talk to the API server, an additional network rule to allow TCP communication to port 443 for the API server IP in addition to adding application rule for fqdn-tag AzureKubernetesService is required.

Below are three network rules you can use to configure on your firewall, you may need to adapt these rules based on your deployment. The first rule allows access to port 9000 via TCP. The second rule allows access to port 1194 and 123 via UDP (if you're deploying to Azure China 21Vianet, you might require [more](#)). Both these rules will only allow traffic destined to the Azure Region CIDR that we're using, in this case East US. Finally, we'll add a third network rule opening port 123 to `ntp.ubuntu.com` FQDN via UDP (adding an FQDN as a network rule is one of the specific features of Azure Firewall, and you'll need to adapt it when using your own options).

After setting the network rules, we'll also add an application rule using the `AzureKubernetesService` that covers all needed FQDNs accessible through TCP port 443 and port 80.

```
Add FW Network Rules

az network firewall network-rule create -g $RG -f $FWNAME --collection-name 'aksfwnr' -n 'apiudp' --
protocols 'UDP' --source-addresses '*' --destination-addresses "AzureCloud.$LOC" --destination-ports 1194 --
action allow --priority 100
az network firewall network-rule create -g $RG -f $FWNAME --collection-name 'aksfwnr' -n 'apitcp' --
protocols 'TCP' --source-addresses '*' --destination-addresses "AzureCloud.$LOC" --destination-ports 9000
az network firewall network-rule create -g $RG -f $FWNAME --collection-name 'aksfwnr' -n 'time' --protocols
'UDP' --source-addresses '*' --destination-fqdns 'ntp.ubuntu.com' --destination-ports 123

Add FW Application Rules

az network firewall application-rule create -g $RG -f $FWNAME --collection-name 'aksfwar' -n 'fqdn' --
source-addresses '*' --protocols 'http=80' 'https=443' --fqdn-tags "AzureKubernetesService" --action allow -
-priority 100
```

See [Azure Firewall documentation](#) to learn more about the Azure Firewall service.

#### Associate the route table to AKS

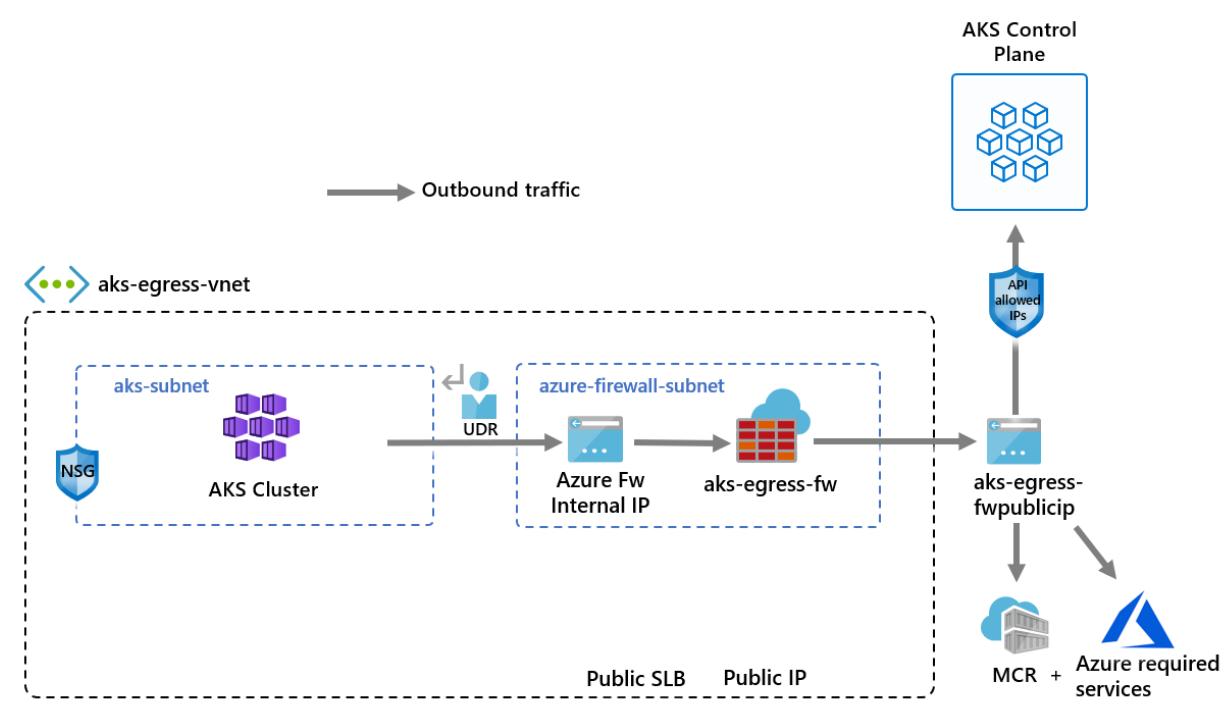
To associate the cluster with the firewall, the dedicated subnet for the cluster's subnet must reference the route table created above. Association can be done by issuing a command to the virtual network holding both the cluster and firewall to update the route table of the cluster's subnet.

```
Associate route table with next hop to Firewall to the AKS subnet

az network vnet subnet update -g $RG --vnet-name $VNET_NAME --name $AKSSUBNET_NAME --route-table
$FWROUTE_TABLE_NAME
```

#### Deploy AKS with outbound type of UDR to the existing network

Now an AKS cluster can be deployed into the existing virtual network. We'll also use [outbound type userDefinedRouting](#), this feature ensures any outbound traffic will be forced through the firewall and no other egress paths will exist (by default the Load Balancer outbound type could be used).



The target subnet to be deployed into is defined with the environment variable, `$SUBNETID`. We didn't define the `$SUBNETID` variable in the previous steps. To set the value for the subnet ID, you can use the following command:

```
SUBNETID=$(az network vnet subnet show -g $RG --vnet-name $VNET_NAME --name $AKSSUBNET_NAME --query id -o tsv)
```

You'll define the outbound type to use the UDR that already exists on the subnet. This configuration will enable AKS to skip the setup and IP provisioning for the load balancer.

#### IMPORTANT

For more information on outbound type UDR including limitations, see [egress outbound type UDR](#).

#### TIP

Additional features can be added to the cluster deployment such as [Private Cluster](#).

The AKS feature for [API server authorized IP ranges](#) can be added to limit API server access to only the firewall's public endpoint. The authorized IP ranges feature is denoted in the diagram as optional. When enabling the authorized IP range feature to limit API server access, your developer tools must use a jumpbox from the firewall's virtual network or you must add all developer endpoints to the authorized IP range.

#### Create an AKS cluster with system-assigned identities

#### NOTE

AKS will create a system-assigned kubelet identity in the Node resource group if you do not [specify your own kubelet managed identity](#).

For user defined routing (UDR), system-assigned identity only supports CNI network plugin. Because for kubelet network plugin, AKS cluster needs permission on route table as kubernetes cloud-provider manages rules.

You can create an AKS cluster using a system-assigned managed identity with CNI network plugin by running the following CLI command.

```
az aks create -g $RG -n $AKSNAME -l $LOC \
--node-count 3 \
--network-plugin azure \
--outbound-type userDefinedRouting \
--vnet-subnet-id $SUBNETID \
--api-server-authorized-ip-ranges $FWPUBLIC_IP
```

#### Create an AKS cluster with user-assigned identities

Create user-assigned managed identities

If you don't have a control plane managed identity, you can create by running the following [az identity create](#) command:

```
az identity create --name myIdentity --resource-group myResourceGroup
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "clientSecretUrl": "<clientSecretUrl>",
 "id": "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myIdentity",
 "location": "westus2",
 "name": "myIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
```

If you don't have a kubelet managed identity, you can create one by running the following [az identity create](#) command:

```
az identity create --name myKubeletIdentity --resource-group myResourceGroup
```

The output should resemble the following:

```
{
 "clientId": "<client-id>",
 "clientSecretUrl": "<clientSecretUrl>",
 "id": "/subscriptions/<subscriptionid>/resourcegroups/myResourceGroup/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myKubeletIdentity",
 "location": "westus2",
 "name": "myKubeletIdentity",
 "principalId": "<principal-id>",
 "resourceGroup": "myResourceGroup",
 "tags": {},
 "tenantId": "<tenant-id>",
 "type": "Microsoft.ManagedIdentity/userAssignedIdentities"
}
```

## NOTE

For creating and using your own VNet and route table where the resources are outside of the worker node resource group, the CLI will add the role assignment automatically. If you are using an ARM template or other client, you need to use the Principal ID of the cluster managed identity to perform a [role assignment](#).

### Create an AKS cluster with user-assigned identities

Now you can use the following command to create your AKS cluster with your existing identities in the subnet.

Provide the control plane identity resource ID via `assign-identity` and the kubelet managed identity via

`assign-kubelet-identity` :

```
az aks create -g $RG -n $AKSNAME -l $LOC \
--node-count 3 \
--network-plugin kubenet \
--outbound-type userDefinedRouting \
--vnet-subnet-id $SUBNETID \
--api-server-authorized-ip-ranges $FWPUBLIC_IP \
--enable-managed-identity \
--assign-identity <identity-resource-id> \
--assign-kubelet-identity <kubelet-identity-resource-id>
```

## Enable developer access to the API server

If you used authorized IP ranges for the cluster on the previous step, you must add your developer tooling IP addresses to the AKS cluster list of approved IP ranges in order to access the API server from there. Another option is to configure a jumpbox with the needed tooling inside a separate subnet in the Firewall's virtual network.

Add another IP address to the approved ranges with the following command

```
Retrieve your IP address
CURRENT_IP=$(dig @resolver1.opendns.com ANY myip.opendns.com +short)

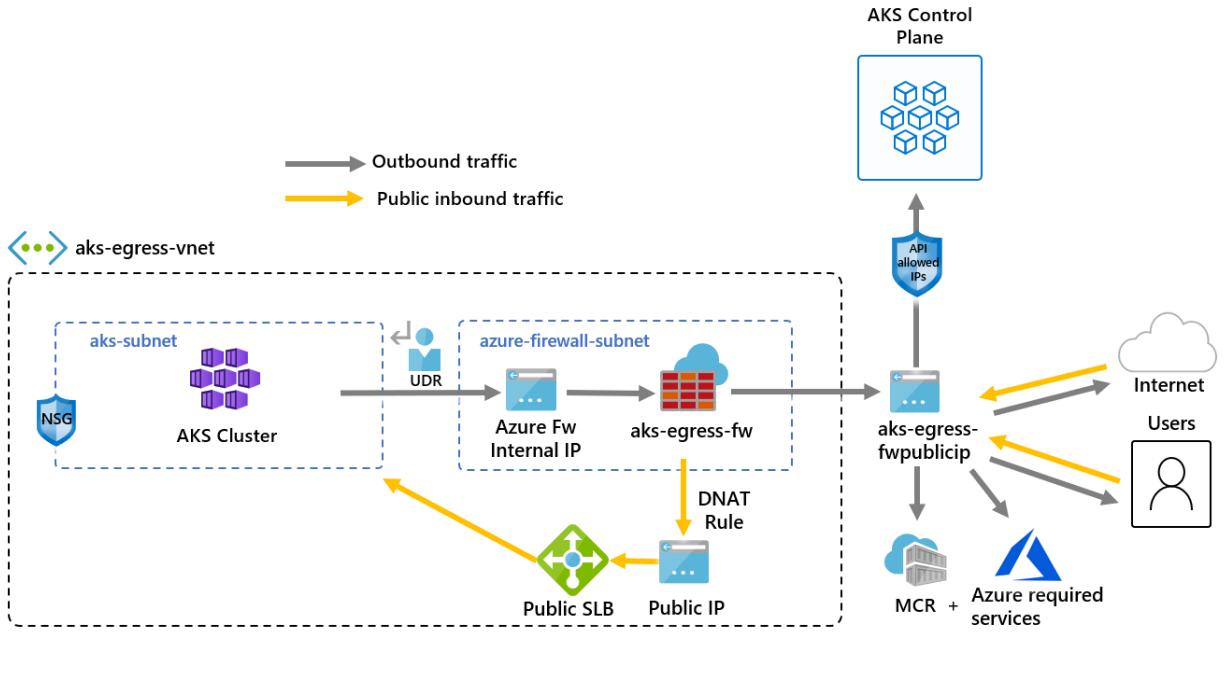
Add to AKS approved list
az aks update -g $RG -n $AKSNAME --api-server-authorized-ip-ranges $CURRENT_IP/32
```

Use the `az aks get-credentials` command to configure `kubectl` to connect to your newly created Kubernetes cluster.

```
az aks get-credentials -g $RG -n $AKSNAME
```

## Deploy a public service

You can now start exposing services and deploying applications to this cluster. In this example, we'll expose a public service, but you may also choose to expose an internal service via [internal load balancer](#).



Deploy the Azure voting app application by copying the yaml below to a file named `example.yaml`.

```
voting-storage-deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: voting-storage
spec:
 replicas: 1
 selector:
 matchLabels:
 app: voting-storage
 template:
 metadata:
 labels:
 app: voting-storage
 spec:
 containers:
 - name: voting-storage
 image: mcr.microsoft.com/aks/samples/voting/storage:2.0
 args: ["--ignore-db-dir=lost+found"]
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 ports:
 - containerPort: 3306
 name: mysql
 volumeMounts:
 - name: mysql-persistent-storage
 mountPath: /var/lib/mysql
 env:
 - name: MYSQL_ROOT_PASSWORD
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_ROOT_PASSWORD
 - name: MYSQL_USER
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
```

```

 key: MYSQL_USER
 - name: MYSQL_PASSWORD
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_PASSWORD
 - name: MYSQL_DATABASE
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_DATABASE
 volumes:
 - name: mysql-persistent-storage
 persistentVolumeClaim:
 claimName: mysql-pv-claim

voting-storage-secret.yaml
apiVersion: v1
kind: Secret
metadata:
 name: voting-storage-secret
type: Opaque
data:
 MYSQL_USER: ZGJ1c2Vy
 MYSQL_PASSWORD: UGFzc3dvcmQxMg==
 MYSQL_DATABASE: YXp1cmV2b3Rl
 MYSQL_ROOT_PASSWORD: UGFzc3dvcmQxMg==

voting-storage-pv-claim.yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: mysql-pv-claim
spec:
 accessModes:
 - ReadWriteOnce
 resources:
 requests:
 storage: 1Gi

voting-storage-service.yaml
apiVersion: v1
kind: Service
metadata:
 name: voting-storage
 labels:
 app: voting-storage
spec:
 ports:
 - port: 3306
 name: mysql
 selector:
 app: voting-storage

voting-app-deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: voting-app
spec:
 replicas: 1
 selector:
 matchLabels:
 app: voting-app
 template:
 metadata:
 labels:
 app: voting-app
 spec:

```

```

containers:
 - name: voting-app
 image: mcr.microsoft.com/aks/samples/voting/app:2.0
 imagePullPolicy: Always
 ports:
 - containerPort: 8080
 name: http
 env:
 - name: MYSQL_HOST
 value: "voting-storage"
 - name: MYSQL_USER
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_USER
 - name: MYSQL_PASSWORD
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_PASSWORD
 - name: MYSQL_DATABASE
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_DATABASE
 - name: ANALYTICS_HOST
 value: "voting-analytics"

voting-app-service.yaml
apiVersion: v1
kind: Service
metadata:
 name: voting-app
 labels:
 app: voting-app
spec:
 type: LoadBalancer
 ports:
 - port: 80
 targetPort: 8080
 name: http
 selector:
 app: voting-app

voting-analytics-deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
 name: voting-analytics
spec:
 replicas: 1
 selector:
 matchLabels:
 app: voting-analytics
 version: "2.0"
 template:
 metadata:
 labels:
 app: voting-analytics
 version: "2.0"
 spec:
 containers:
 - name: voting-analytics
 image: mcr.microsoft.com/aks/samples/voting/analytics:2.0
 imagePullPolicy: Always
 ports:
 - containerPort: 8080
 name: http
 env:

```

```

- name: MYSQL_HOST
 value: "voting-storage"
- name: MYSQL_USER
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_USER
- name: MYSQL_PASSWORD
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_PASSWORD
- name: MYSQL_DATABASE
 valueFrom:
 secretKeyRef:
 name: voting-storage-secret
 key: MYSQL_DATABASE

voting-analytics-service.yaml
apiVersion: v1
kind: Service
metadata:
 name: voting-analytics
 labels:
 app: voting-analytics
spec:
 ports:
 - port: 8080
 name: http
 selector:
 app: voting-analytics

```

Deploy the service by running:

```
kubectl apply -f example.yaml
```

## Add a DNAT rule to Azure Firewall

### IMPORTANT

When you use Azure Firewall to restrict egress traffic and create a user-defined route (UDR) to force all egress traffic, make sure you create an appropriate DNAT rule in Firewall to correctly allow ingress traffic. Using Azure Firewall with a UDR breaks the ingress setup due to asymmetric routing. (The issue occurs if the AKS subnet has a default route that goes to the firewall's private IP address, but you're using a public load balancer - ingress or Kubernetes service of type: LoadBalancer). In this case, the incoming load balancer traffic is received via its public IP address, but the return path goes through the firewall's private IP address. Because the firewall is stateful, it drops the returning packet because the firewall isn't aware of an established session. To learn how to integrate Azure Firewall with your ingress or service load balancer, see [Integrate Azure Firewall with Azure Standard Load Balancer](#).

To configure inbound connectivity, a DNAT rule must be written to the Azure Firewall. To test connectivity to your cluster, a rule is defined for the firewall frontend public IP address to route to the internal IP exposed by the internal service.

The destination address can be customized as it's the port on the firewall to be accessed. The translated address must be the IP address of the internal load balancer. The translated port must be the exposed port for your Kubernetes service.

You'll need to specify the internal IP address assigned to the load balancer created by the Kubernetes service. Retrieve the address by running:

```
kubectl get services
```

The IP address needed will be listed in the EXTERNAL-IP column, similar to the following.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
kubernetes	ClusterIP	10.41.0.1	<none>	443/TCP	10h
voting-analytics	ClusterIP	10.41.88.129	<none>	8080/TCP	9m
voting-app	LoadBalancer	10.41.185.82	20.39.18.6	80:32718/TCP	9m
voting-storage	ClusterIP	10.41.221.201	<none>	3306/TCP	9m

Get the service IP by running:

```
SERVICE_IP=$(kubectl get svc voting-app -o jsonpath='{.status.loadBalancer.ingress[*].ip}')
```

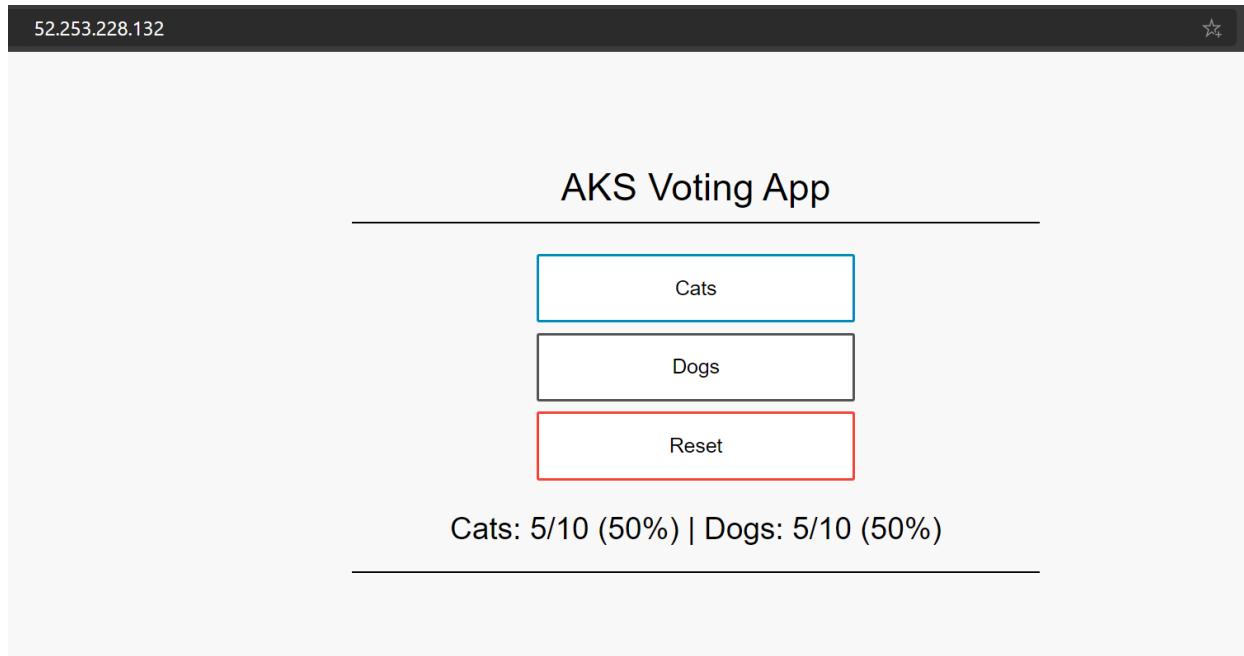
Add the NAT rule by running:

```
az network firewall nat-rule create --collection-name exampleset --destination-addresses $FWPUBLIC_IP --destination-ports 80 --firewall-name $FWNAME --name inboundrule --protocols Any --resource-group $RG --source-addresses '*' --translated-port 80 --action Dnat --priority 100 --translated-address $SERVICE_IP
```

## Validate connectivity

Navigate to the Azure Firewall frontend IP address in a browser to validate connectivity.

You should see the AKS voting app. In this example, the Firewall public IP was [52.253.228.132](http://52.253.228.132).



## Clean up resources

To clean up Azure resources, delete the AKS resource group.

```
az group delete -g $RG
```

## Next steps

In this article, you learned what ports and addresses to allow if you want to restrict egress traffic for the cluster. You also saw how to secure your outbound traffic using Azure Firewall.

If needed, you can generalize the steps above to forward the traffic to your preferred egress solution, following the [Outbound Type `userDefinedRoute` documentation](#).

If you want to restrict how pods communicate between themselves and East-West traffic restrictions within cluster see [Secure traffic between pods using network policies in AKS](#).

# Customize cluster egress with a User-Defined Route

10/27/2022 • 3 minutes to read • [Edit Online](#)

Egress from an AKS cluster can be customized to fit specific scenarios. By default, AKS will provision a Standard SKU Load Balancer to be set up and used for egress. However, the default setup may not meet the requirements of all scenarios if public IPs are disallowed or additional hops are required for egress.

This article walks through how to customize a cluster's egress route to support custom network scenarios, such as those which disallows public IPs and requires the cluster to sit behind a network virtual appliance (NVA).

## Prerequisites

- Azure CLI version 2.0.81 or greater
- API version of `2020-01-01` or greater

## Limitations

- `OutboundType` can only be defined at cluster create time and can't be updated afterwards.
- Setting `outboundType` requires AKS clusters with a `vm-set-type` of `VirtualMachineScaleSets` and `load-balancer-sku` of `Standard`.
- Setting `outboundType` to a value of `UDR` requires a user-defined route with valid outbound connectivity for the cluster.
- Setting `outboundType` to a value of `UDR` implies the ingress source IP routed to the load-balancer may **not match** the cluster's outgoing egress destination address.

## Overview of outbound types in AKS

An AKS cluster can be customized with a unique `outboundType` of type `loadBalancer` or `userDefinedRouting`.

### IMPORTANT

Outbound type impacts only the egress traffic of your cluster. For more information, see [setting up ingress controllers](#).

### NOTE

You can use your own [route table](#) with UDR and kubenet networking. Make sure your cluster identity (service principal or managed identity) has Contributor permissions to the custom route table.

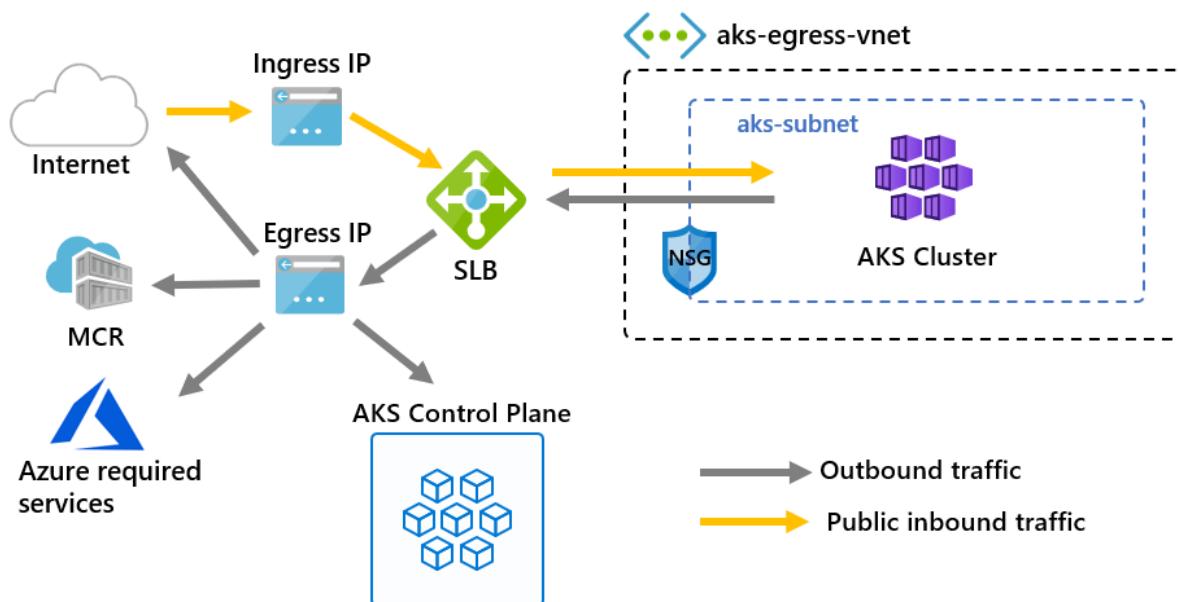
### Outbound type of `loadBalancer`

If `loadBalancer` is set, AKS completes the following configuration automatically. The load balancer is used for egress through an AKS assigned public IP. An outbound type of `loadBalancer` supports Kubernetes services of type `loadBalancer`, which expect egress out of the load balancer created by the AKS resource provider.

The following configuration is done by AKS.

- A public IP address is provisioned for cluster egress.
- The public IP address is assigned to the load balancer resource.
- Backend pools for the load balancer are set up for agent nodes in the cluster.

Below is a network topology deployed in AKS clusters by default, which use an `outboundType` of `loadBalancer`.



### Outbound type of userDefinedRouting

#### NOTE

Using outbound type is an advanced networking scenario and requires proper network configuration.

If `userDefinedRouting` is set, AKS won't automatically configure egress paths. The egress setup must be done by you.

The AKS cluster must be deployed into an existing virtual network with a subnet that has been previously configured because when not using standard load balancer (SLB) architecture, you must establish explicit egress. As such, this architecture requires explicitly sending egress traffic to an appliance like a firewall, gateway, proxy or to allow the Network Address Translation (NAT) to be done by a public IP assigned to the standard load balancer or appliance.

#### Load balancer creation with userDefinedRouting

AKS clusters with an outbound type of UDR receive a standard load balancer (SLB) only when the first Kubernetes service of type 'loadBalancer' is deployed. The load balancer is configured with a public IP address for *inbound* requests and a backend pool for *inbound* requests. Inbound rules are configured by the Azure cloud provider, but no **outbound public IP address or outbound rules** are configured as a result of having an outbound type of UDR. Your UDR will still be the only source for egress traffic.

Azure load balancers [don't incur a charge until a rule is placed](#).

## Deploy a cluster with outbound type of UDR and Azure Firewall

To illustrate the application of a cluster with outbound type using a user-defined route, a cluster can be configured on a virtual network with an Azure Firewall on its own subnet. See this example on the [restrict egress traffic with Azure firewall example](#).

## IMPORTANT

Outbound type of UDR requires there is a route for 0.0.0.0/0 and next hop destination of NVA (Network Virtual Appliance) in the route table. The route table already has a default 0.0.0.0/0 to Internet, without a Public IP to SNAT just adding this route will not provide you egress. AKS will validate that you don't create a 0.0.0.0/0 route pointing to the Internet but instead to NVA or gateway, etc. When using an outbound type of UDR, a load balancer public IP address for **inbound requests** is not created unless a service of type *loadbalancer* is configured. A public IP address for **outbound requests** is never created by AKS if an outbound type of UDR is set.

## Next steps

See [Azure networking UDR overview](#).

See [how to create, change, or delete a route table](#).

# Managed NAT Gateway

10/27/2022 • 2 minutes to read • [Edit Online](#)

Whilst AKS customers are able to route egress traffic through an Azure Load Balancer, there are limitations on the amount of outbound flows of traffic that is possible.

Azure NAT Gateway allows up to 64,512 outbound UDP and TCP traffic flows per IP address with a maximum of 16 IP addresses.

This article will show you how to create an AKS cluster with a Managed NAT Gateway for egress traffic.

## Before you begin

To use Managed NAT gateway, you must have the following:

- The latest version of the Azure CLI
- Kubernetes version 1.20.x or above

## Create an AKS cluster with a Managed NAT Gateway

To create an AKS cluster with a new Managed NAT Gateway, use `--outbound-type managedNATGateway` as well as `--nat-gateway-managed-outbound-ip-count` and `--nat-gateway-idle-timeout` when running `az aks create`. The following example creates a *myresourcegroup* resource group, then creates a *natcluster* AKS cluster in *myresourcegroup* with a Managed NAT Gateway, two outbound IPs, and an idle timeout of 30 seconds.

```
az group create --name myresourcegroup --location southcentralus
```

```
az aks create \
 --resource-group myResourceGroup \
 --name natcluster \
 --node-count 3 \
 --outbound-type managedNATGateway \
 --nat-gateway-managed-outbound-ip-count 2 \
 --nat-gateway-idle-timeout 30
```

### IMPORTANT

If no value the outbound IP address is specified, the default value is one.

## Update the number of outbound IP addresses

To update the outbound IP address or idle timeout, use `--nat-gateway-managed-outbound-ip-count` or `--nat-gateway-idle-timeout` when running `az aks update`. For example:

```
az aks update \
 --resource-group myresourcegroup \
 --name natcluster \
 --nat-gateway-managed-outbound-ip-count 5
```

## Create an AKS cluster with a user-assigned NAT Gateway

To create an AKS cluster with a user-assigned NAT Gateway, use `--outbound-type userAssignedNATGateway` when running `az aks create`. This configuration requires bring-your-own networking (via [Kubenet](#) or [Azure CNI](#)) and that the NAT Gateway is preconfigured on the subnet. The following commands create the required resources for this scenario. Make sure to run them all in the same session so that the values stored to variables are still available for the `az aks create` command.

1. Create the resource group:

```
az group create --name myresourcegroup \
--location southcentralus
```

2. Create a managed identity for network permissions and store the ID to `$IDENTITY_ID` for later use:

```
IDENTITY_ID=$(az identity create \
--resource-group myresourcegroup \
--name natclusterid \
--location southcentralus \
--query id \
--output tsv)
```

3. Create a public IP for the NAT gateway:

```
az network public-ip create \
--resource-group myresourcegroup \
--name mynatgatewaypip \
--location southcentralus \
--sku standard
```

4. Create the NAT gateway:

```
az network nat gateway create \
--resource-group myresourcegroup \
--name mynatgateway \
--location southcentralus \
--public-ip-addresses mynatgatewaypip
```

5. Create a virtual network:

```
az network vnet create \
--resource-group myresourcegroup \
--name myvnet \
--location southcentralus \
--address-prefixes 172.16.0.0/20
```

6. Create a subnet in the virtual network using the NAT gateway and store the ID to `$SUBNET_ID` for later use:

```
SUBNET_ID=$(az network vnet subnet create \
--resource-group myresourcegroup \
--vnet-name myvnet \
--name natcluster \
--address-prefixes 172.16.0.0/22 \
--nat-gateway mynatgateway \
--query id \
--output tsv)
```

7. Create an AKS cluster using the subnet with the NAT gateway and the managed identity:

```
az aks create \
--resource-group myresourcegroup \
--name natcluster \
--location southcentralus \
--network-plugin azure \
--vnet-subnet-id $SUBNET_ID \
--outbound-type userAssignedNATGateway \
--enable-managed-identity \
--assign-identity $IDENTITY_ID
```

## Next Steps

- For more information on Azure NAT Gateway, see [Azure NAT Gateway](#).

# Customize CoreDNS with Azure Kubernetes Service

10/27/2022 • 5 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) uses the [CoreDNS](#) project for cluster DNS management and resolution with all 1.12.x and higher clusters. Previously, the kube-dns project was used. This kube-dns project is now deprecated. For more information about CoreDNS customization and Kubernetes, see the [official upstream documentation](#).

As AKS is a managed service, you cannot modify the main configuration for CoreDNS (a *CoreFile*). Instead, you use a Kubernetes *ConfigMap* to override the default settings. To see the default AKS CoreDNS ConfigMaps, use the `kubectl get configmaps --namespace=kube-system coredns -o yaml` command.

This article shows you how to use ConfigMaps for basic customization options of CoreDNS in AKS. This approach differs from configuring CoreDNS in other contexts such as using the CoreFile. Verify the version of CoreDNS you are running as the configuration values may change between versions.

## NOTE

`kube-dns` offered different [customization options](#) via a Kubernetes config map. CoreDNS is **not** backwards compatible with kube-dns. Any customizations you previously used must be updated for use with CoreDNS.

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

When creating a configuration like the examples below, your names in the *data* section must end in either `.server` or `.override`. This naming convention is defined in the default AKS CoreDNS Configmap which you can view using the `kubectl get configmaps --namespace=kube-system coredns -o yaml` command.

## What is supported/unsupported

All built-in CoreDNS plugins are supported. No add-on/third party plugins are supported.

## Rewrite DNS

One scenario you have is to perform on-the-fly DNS name rewrites. In the following example, replace `<domain to be written>` with your own fully qualified domain name. Create a file named `corednsms.yaml` and paste the following example configuration:

```
apiVersion: v1
kind: ConfigMap
metadata:
 name: coredns-custom
 namespace: kube-system
data:
 test.server: | # you may select any name here, but it must end with the .server file extension
 <domain to be rewritten>.com:53 {
 log
 errors
 rewrite stop {
 name regex (.*).<domain to be rewritten>.com {1}.default.svc.cluster.local
 answer name (.*).default.svc.cluster.local {1}.<domain to be rewritten>.com
 }
 forward . /etc/resolv.conf # you can redirect this to a specific DNS server such as 10.0.0.10, but that
 server must be able to resolve the rewritten domain name
 }
```

#### IMPORTANT

If you redirect to a DNS server, such as the CoreDNS service IP, that DNS server must be able to resolve the rewritten domain name.

Create the ConfigMap using the [kubectl apply configmap](#) command and specify the name of your YAML manifest:

```
kubectl apply -f corednsm.yaml
```

To verify the customizations have been applied, use the [kubectl get configmaps](#) and specify your *coredns-custom* ConfigMap:

```
kubectl get configmaps --namespace=kube-system coredns-custom -o yaml
```

Now force CoreDNS to reload the ConfigMap. The [kubectl delete pod](#) command isn't destructive and doesn't cause down time. The `kube-dns` pods are deleted, and the Kubernetes Scheduler then recreates them. These new pods contain the change in TTL value.

```
kubectl delete pod --namespace kube-system -l k8s-app=kube-dns
```

#### NOTE

The command above is correct. While we're changing `coredns`, the deployment is under the `kube-dns` label.

## Custom forward server

If you need to specify a forward server for your network traffic, you can create a ConfigMap to customize DNS. In the following example, update the `forward` name and address with the values for your own environment.

Create a file named `corednsm.yaml` and paste the following example configuration:

```
apiVersion: v1
kind: ConfigMap
metadata:
 name: coredns-custom
 namespace: kube-system
data:
 test.server: | # you may select any name here, but it must end with the .server file extension
 <domain to be rewritten>.com:53 {
 forward foo.com 1.1.1.1
 }
```

As in the previous examples, create the ConfigMap using the [kubectl apply configmap](#) command and specify the name of your YAML manifest. Then, force CoreDNS to reload the ConfigMap using the [kubectl delete pod](#) for the Kubernetes Scheduler to recreate them:

```
kubectl apply -f corednsms.yaml
kubectl delete pod --namespace kube-system --selector k8s-app=kube-dns
```

## Use custom domains

You may want to configure custom domains that can only be resolved internally. For example, you may want to resolve the custom domain *puglife.local*, which isn't a valid top-level domain. Without a custom domain ConfigMap, the AKS cluster can't resolve the address.

In the following example, update the custom domain and IP address to direct traffic to with the values for your own environment. Create a file named `corednsms.yaml` and paste the following example configuration:

```
apiVersion: v1
kind: ConfigMap
metadata:
 name: coredns-custom
 namespace: kube-system
data:
 puglife.server: | # you may select any name here, but it must end with the .server file extension
 puglife.local:53 {
 errors
 cache 30
 forward . 192.11.0.1 # this is my test/dev DNS server
 }
```

As in the previous examples, create the ConfigMap using the [kubectl apply configmap](#) command and specify the name of your YAML manifest. Then, force CoreDNS to reload the ConfigMap using the [kubectl delete pod](#) for the Kubernetes Scheduler to recreate them:

```
kubectl apply -f corednsms.yaml
kubectl delete pod --namespace kube-system --selector k8s-app=kube-dns
```

## Stub domains

CoreDNS can also be used to configure stub domains. In the following example, update the custom domains and IP addresses with the values for your own environment. Create a file named `corednsms.yaml` and paste the following example configuration:

```
apiVersion: v1
kind: ConfigMap
metadata:
 name: coredns-custom
 namespace: kube-system
data:
 test.server: | # you may select any name here, but it must end with the .server file extension
 abc.com:53 {
 errors
 cache 30
 forward . 1.2.3.4
 }
 my.cluster.local:53 {
 errors
 cache 30
 forward . 2.3.4.5
 }
```

As in the previous examples, create the ConfigMap using the [kubectl apply configmap](#) command and specify the name of your YAML manifest. Then, force CoreDNS to reload the ConfigMap using the [kubectl delete pod](#) for the Kubernetes Scheduler to recreate them:

```
kubectl apply -f corednsm.yaml
kubectl delete pod --namespace kube-system --selector k8s-app=kube-dns
```

## Hosts plugin

As all built-in plugins are supported this means that the CoreDNS [Hosts](#) plugin is available to customize as well:

```
apiVersion: v1
kind: ConfigMap
metadata:
 name: coredns-custom # this is the name of the configmap you can overwrite with your changes
 namespace: kube-system
data:
 test.override: | # you may select any name here, but it must end with the .override file extension
 hosts {
 10.0.0.1 example1.org
 10.0.0.2 example2.org
 10.0.0.3 example3.org
 fallthrough
 }
```

## Troubleshooting

For general CoreDNS troubleshooting steps, such as checking the endpoints or resolution, see [Debugging DNS Resolution](#).

To enable DNS query logging, apply the following configuration in your coredns-custom ConfigMap:

```
apiVersion: v1
kind: ConfigMap
metadata:
 name: coredns-custom
 namespace: kube-system
data:
 log.override: | # you may select any name here, but it must end with the .override file extension
 log
```

After you apply the configuration changes, use the `kubectl logs` command to view the CoreDNS debug logging. For example:

```
kubectl logs --namespace kube-system --selector k8s-app=kube-dns
```

## Next steps

This article showed some example scenarios for CoreDNS customization. For information on the CoreDNS project, see [the CoreDNS upstream project page](#).

To learn more about core network concepts, see [Network concepts for applications in AKS](#).

# Container Storage Interface (CSI) drivers on Azure Kubernetes Service (AKS)

10/27/2022 • 5 minutes to read • [Edit Online](#)

The Container Storage Interface (CSI) is a standard for exposing arbitrary block and file storage systems to containerized workloads on Kubernetes. By adopting and using CSI, Azure Kubernetes Service (AKS) can write, deploy, and iterate plug-ins to expose new or improve existing storage systems in Kubernetes without having to touch the core Kubernetes code and wait for its release cycles.

The CSI storage driver support on AKS allows you to natively use:

- **Azure Disks** can be used to create a Kubernetes *DataDisk* resource. Disks can use Azure Premium Storage, backed by high-performance SSDs, or Azure Standard Storage, backed by regular HDDs or Standard SSDs. For most production and development workloads, use Premium Storage. Azure Disks are mounted as *ReadWriteOnce* and are only available to one node in AKS. For storage volumes that can be accessed by multiple pods simultaneously, use Azure Files.
- **Azure Files** can be used to mount an SMB 3.0/3.1 share backed by an Azure storage account to pods. With Azure Files, you can share data across multiple nodes and pods. Azure Files can use Azure Standard storage backed by regular HDDs or Azure Premium storage backed by high-performance SSDs.
- **Azure Blob storage** can be used to mount Blob storage (or object storage) as a file system into a container or pod. Using Blob storage enables your cluster to support applications that work with large unstructured datasets like log file data, images or documents, HPC, and others. Additionally, if you ingest data into [Azure Data Lake storage](#), you can directly mount and use it in AKS without configuring another interim filesystem.

## IMPORTANT

Starting with Kubernetes version 1.21, AKS only uses CSI drivers by default and CSI migration is enabled. Existing in-tree persistent volumes will continue to function. However, internally Kubernetes hands control of all storage management operations (previously targeting in-tree drivers) to CSI drivers.

*In-tree drivers* refers to the storage drivers that are part of the core Kubernetes code opposed to the CSI drivers, which are plug-ins.

## NOTE

Azure Disks CSI driver v2 (preview) improves scalability and reduces pod failover latency. It uses shared disks to provision attachment replicas on multiple cluster nodes and integrates with the pod scheduler to ensure a node with an attachment replica is chosen on pod failover. Azure Disks CSI driver v2 (preview) also provides the ability to fine tune performance. If you're interested in participating in the preview, submit a request: <https://aka.ms/DiskCSIV2Preview>. This preview version is provided without a service level agreement, and you can occasionally expect breaking changes while in preview. The preview version isn't recommended for production workloads. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

## Prerequisites

You need the Azure CLI version 2.40 installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Disable CSI storage drivers on a new cluster

--disable-disk-driver allows you to disable the [Azure Disks CSI driver](#). --disable-file-driver allows you to disable the [Azure Files CSI driver](#). --disable-snapshot-controller allows you to disable the [snapshot controller](#).

To disable CSI storage drivers on a new cluster, use --disable-disk-driver, --disable-file-driver, and --disable-snapshot-controller.

```
az aks create -n myAKSCluster -g myResourceGroup --disable-disk-driver --disable-file-driver --disable-snapshot-controller
```

## Disable CSI storage drivers on an existing cluster

To disable CSI storage drivers on an existing cluster, use --disable-disk-driver, --disable-file-driver, and --disable-snapshot-controller.

```
az aks update -n myAKSCluster -g myResourceGroup --disable-disk-driver --disable-file-driver --disable-snapshot-controller
```

## Enable CSI storage drivers on an existing cluster

--enable-disk-driver allows you enable the [Azure Disks CSI driver](#). --enable-file-driver allows you to enable the [Azure Files CSI driver](#). --enable-snapshot-controller allows you to enable the [snapshot controller](#).

To enable CSI storage drivers on an existing cluster with CSI storage drivers disabled, use --enable-disk-driver, --enable-file-driver, and --enable-snapshot-controller.

```
az aks update -n myAKSCluster -g myResourceGroup --enable-disk-driver --enable-file-driver --enable-snapshot-controller
```

## Migrate custom in-tree storage classes to CSI

If you've created in-tree driver storage classes, those storage classes continue to work since CSI migration is turned on after upgrading your cluster to 1.21.x. If you want to use CSI features you'll need to perform the migration.

Migrating these storage classes involves deleting the existing ones, and re-creating them with the provisioner set to `disk.csi.azure.com` if using Azure Disks, and `files.csi.azure.com` if using Azure Files.

### Migrate storage class provisioner

The following example YAML manifest shows the difference between the in-tree storage class definition configured to use Azure Disks, and the equivalent using a CSI storage class definition. The CSI storage system supports the same features as the in-tree drivers, so the only change needed would be the value for provisioner.

#### Original in-tree storage class definition

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
 name: custom-managed-premium
provisioner: kubernetes.io/azure-disk
reclaimPolicy: Delete
parameters:
 storageAccountType: Premium_LRS
```

#### CSI storage class definition

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
 name: custom-managed-premium
provisioner: disk.csi.azure.com
reclaimPolicy: Delete
parameters:
 storageAccountType: Premium_LRS
```

The CSI storage system supports the same features as the In-tree drivers, so the only change needed would be the provisioner.

## Migrate in-tree persistent volumes

### IMPORTANT

If your in-tree persistent volume `reclaimPolicy` is set to **Delete**, you need to change its policy to **Retain** to persist your data. This can be achieved using a [patch operation on the PV](#). For example:

```
kubectl patch pv pv-azuredisk --type merge --patch '{"spec": {"persistentVolumeReclaimPolicy": "Retain"}}'
```

### Migrate in-tree Azure Disks persistent volumes

If you have in-tree Azure Disks persistent volumes, get `diskURI` from in-tree persistent volumes and then follow this [guide](#) to set up CSI driver persistent volumes.

### Migrate in-tree Azure File persistent volumes

If you have in-tree Azure File persistent volumes, get `secretName`, `shareName` from in-tree persistent volumes and then follow this [guide](#) to set up CSI driver persistent volumes

## Next steps

- To use the CSI driver for Azure Disks, see [Use Azure Disks with CSI drivers](#).
- To use the CSI driver for Azure Files, see [Use Azure Files with CSI drivers](#).
- To use the CSI driver for Azure Blob storage, see [Use Azure Blob storage with CSI drivers](#)
- For more about storage best practices, see [Best practices for storage and backups in Azure Kubernetes Service](#).
- For more information on CSI migration, see [Kubernetes In-Tree to CSI Volume Migration](#).

# Use the Azure Disks Container Storage Interface (CSI) driver in Azure Kubernetes Service (AKS)

10/27/2022 • 13 minutes to read • [Edit Online](#)

The Azure Disks Container Storage Interface (CSI) driver is a [CSI specification](#)-compliant driver used by Azure Kubernetes Service (AKS) to manage the lifecycle of Azure Disks.

The CSI is a standard for exposing arbitrary block and file storage systems to containerized workloads on Kubernetes. By adopting and using CSI, AKS now can write, deploy, and iterate plug-ins to expose new or improve existing storage systems in Kubernetes. Using CSI drivers in AKS avoids having to touch the core Kubernetes code and wait for its release cycles.

To create an AKS cluster with CSI driver support, see [Enable CSI driver on AKS](#). This article describes how to use the Azure Disks CSI driver version 1.

## NOTE

Azure Disks CSI driver v2 (preview) improves scalability and reduces pod failover latency. It uses shared disks to provision attachment replicas on multiple cluster nodes and integrates with the pod scheduler to ensure a node with an attachment replica is chosen on pod failover. Azure Disks CSI driver v2 (preview) also provides the ability to fine tune performance. If you're interested in participating in the preview, submit a request: <https://aka.ms/DiskCSIV2Preview>. This preview version is provided without a service level agreement, and you can occasionally expect breaking changes while in preview. The preview version isn't recommended for production workloads. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

## NOTE

*In-tree drivers* refers to the current storage drivers that are part of the core Kubernetes code versus the new CSI drivers, which are plug-ins.

## Azure Disks CSI driver features

In addition to in-tree driver features, Azure Disks CSI driver supports the following features:

- Performance improvements during concurrent disk attach and detach
  - In-tree drivers attach or detach disks in serial, while CSI drivers attach or detach disks in batch. There's significant improvement when there are multiple disks attaching to one node.
- Premium SSD v1 and v2 are supported.
- Zone-redundant storage (ZRS) disk support
  - `Premium_ZRS`, `StandardSSD_ZRS` disk types are supported. ZRS disk could be scheduled on the zone or non-zone node, without the restriction that disk volume should be co-located in the same zone as a given node. For more information, including which regions are supported, see [Zone-redundant storage for managed disks](#).
- [Snapshot](#)
- [Volume clone](#)
- [Resize disk PV without downtime\(Preview\)](#)

## Storage class driver dynamic disks parameters

NAME	MEANING	AVAILABLE VALUE	MANDATORY	DEFAULT VALUE
skuName	Azure Disks storage account type (alias: storageAccountType )	Standard_LRS , Premium_LRS , StandardSSD_LRS , PremiumV2_LRS , UltraSSD_LRS , Premium_ZRS , StandardSSD_ZRS	No	StandardSSD_LRS
fsType	File System Type	ext4 , ext3 , ext2 , xfs , btrfs for Linux, ntfs for Windows	No	ext4 for Linux, ntfs for Windows
cachingMode	Azure Data Disk Host Cache Setting	None , ReadOnly , ReadWrite	No	ReadOnly
location	Specify Azure region where Azure Disks will be created	eastus , westus , etc.	No	If empty, driver will use the same location name as current AKS cluster
resourceGroup	Specify the resource group where the Azure Disks will be created	Existing resource group name	No	If empty, driver will use the same resource group name as current AKS cluster
DiskIOPSReadWrite	UltraSSD disk IOPS Capability (minimum: 2 IOPS/GiB )	100~160000	No	500
DiskMBpsReadWrite	UltraSSD disk Throughput Capability(minimum: 0.032/GiB)	1~2000	No	100
LogicalSectorSize	Logical sector size in bytes for Ultra disk. Supported values are 512 ad 4096. 4096 is the default.	512 , 4096	No	4096
tags	Azure Disk tags	Tag format: key1=val1,key2=val2	No	""
diskEncryptionSetID	ResourceID of the disk encryption set to use for <a href="#">enabling encryption at rest</a>	format:  /subscriptions/{subs-id}/resourceGroups/{rg-name}/providers/Microsoft.Compute/diskEncryptionSets/{diskEncryptionSetName}	No	""
diskEncryptionType	Encryption type of the disk encryption set	EncryptionAtRestWithCustomerKey (by default), EncryptionAtRestWithPlatformAndCustomerKeys	No	""

Name	Meaning	Available Value	Mandatory	Default Value
writeAcceleratorEnabled	Write Accelerator on Azure Disks	true , false	No	""
networkAccessPolicy	NetworkAccessPolicy property to prevent generation of the SAS URI for a disk or a snapshot	AllowAll , DenyAll , AllowPrivate	No	AllowAll
diskAccessID	ARM ID of the DiskAccess resource to use private endpoints on disks		No	''
enableBursting	Enable on-demand bursting beyond the provisioned performance target of the disk. On-demand bursting should only be applied to Premium disk and when the disk size > 512 GB. Ultra and shared disk isn't supported. Bursting is disabled by default.	true , false	No	false
useragent	User agent used for customer usage attribution		No	Generated Useragent formatted driverName/driverVersion compiler/version (OS-ARCH)
enableAsyncAttach	Allow multiple disk attach operations (in batch) on one node in parallel. While this parameter can speed up disk attachment, you may encounter Azure API throttling limit when there are large number of volume attachments.	true , false	No	false
subscriptionID	Specify Azure subscription ID where the Azure Disks will be created	Azure subscription ID	No	If not empty, resourceGroup must be provided.

## Use CSI persistent volumes with Azure Disks

A [persistent volume](#) (PV) represents a piece of storage that's provisioned for use with Kubernetes pods. A PV can be used by one or many pods and can be dynamically or statically provisioned. This article shows you how to dynamically create PVs with Azure disk for use by a single pod in an AKS cluster. For static provisioning, see

Create a static volume with Azure Disks.

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Dynamically create Azure Disks PVs by using the built-in storage classes

A storage class is used to define how a unit of storage is dynamically created with a persistent volume. For more information on Kubernetes storage classes, see [Kubernetes storage classes](#).

When you use the Azure Disks CSI driver on AKS, there are two more built-in `StorageClasses` that use the Azure Disks CSI storage driver. The other CSI storage classes are created with the cluster alongside the in-tree default storage classes.

- `managed-csi` : Uses Azure Standard SSD locally redundant storage (LRS) to create a managed disk.
- `managed-csi-premium` : Uses Azure Premium LRS to create a managed disk.

The reclaim policy in both storage classes ensures that the underlying Azure Disks are deleted when the respective PV is deleted. The storage classes also configure the PVs to be expandable. You just need to edit the persistent volume claim (PVC) with the new size.

To use these storage classes, create a [PVC](#) and respective pod that references and uses them. A PVC is used to automatically provision storage based on a storage class. A PVC can use one of the pre-created storage classes or a user-defined storage class to create an Azure-managed disk for the desired SKU and size. When you create a pod definition, the PVC is specified to request the desired storage.

Create an example pod and respective PVC by running the `kubectl apply` command:

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-driver/master/deploy/example/pvc-azuredisk-csi.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-driver/master/deploy/example/nginx-pod-azuredisk.yaml
```

The output of the command resembles the following example:

```
persistentvolumeclaim/pvc-azuredisk created
pod/nginx-azuredisk created
```

After the pod is in the running state, run the following command to create a new file called `test.txt`.

```
kubectl exec nginx-azuredisk -- touch /mnt/azuredisk/test.txt
```

To validate the disk is correctly mounted, run the following command and verify you see the `test.txt` file in the output:

```
kubectl exec nginx-azuredisk -- ls /mnt/azuredisk
lost+found
outfile
test.txt
```

## Create a custom storage class

The default storage classes are suitable for most common scenarios. For some cases, you might want to have

your own storage class customized with your own parameters. For example, you might want to change the `volumeBindingMode` class.

You can use a `volumeBindingMode: Immediate` class that guarantees it occurs immediately once the PVC is created. When your node pools are topology constrained, for example when using availability zones, PVs would be bound or provisioned without knowledge of the pod's scheduling requirements.

To address this scenario, you can use `volumeBindingMode: WaitForFirstConsumer`, which delays the binding and provisioning of a PV until a pod that uses the PVC is created. This way, the PV conforms and is provisioned in the availability zone (or other topology) that's specified by the pod's scheduling constraints. The default storage classes use `volumeBindingMode: WaitForFirstConsumer` class.

Create a file named `sc-azuredisk-csi-waitforfirstconsumer.yaml`, and then paste the following manifest. The storage class is the same as our `managed-csi` storage class, but with a different `volumeBindingMode` class.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
 name: azuredisk-csi-waitforfirstconsumer
provisioner: disk.csi.azure.com
parameters:
 skuname: StandardSSD_LRS
allowVolumeExpansion: true
reclaimPolicy: Delete
volumeBindingMode: WaitForFirstConsumer
```

Create the storage class by running the `kubectl apply` command and specify your `sc-azuredisk-csi-waitforfirstconsumer.yaml` file:

```
kubectl apply -f sc-azuredisk-csi-waitforfirstconsumer.yaml
```

The output of the command resembles the following example:

```
storageclass.storage.k8s.io/azuredisk-csi-waitforfirstconsumer created
```

## Volume snapshots

The Azure Disks CSI driver supports creating [snapshots of persistent volumes](#). As part of this capability, the driver can perform either *full* or *incremental* snapshots depending on the value set in the `incremental` parameter (by default, it's true).

The following table provides details for all of the parameters.

NAME	MEANING	AVAILABLE VALUE	MANDATORY	DEFAULT VALUE
resourceGroup	Resource group for storing snapshot shots	EXISTING RESOURCE GROUP	No	If not specified, snapshot will be stored in the same resource group as source Azure Disks
incremental	Take full or incremental snapshot	true , false	No	true

Name	Meaning	Available Value	Mandatory	Default Value
tags	Azure Disks <a href="#">tags</a>	Tag format: 'key1=val1,key2=val2'	No	""
userAgent	User agent used for <a href="#">customer usage attribution</a>		No	Generated Useragent formatted <code>driverName/driverVersion compiler/version (OS-ARCH)</code>
subscriptionID	Specify Azure subscription ID where Azure Disks will be created	Azure subscription ID	No	If not empty, <code>resourceGroup</code> must be provided, <code>incremental</code> must set as <code>false</code>

## Create a volume snapshot

For an example of this capability, create a [volume snapshot class](#) with the `kubectl apply` command:

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-driver/master/deploy/example/snapshot/storageclass-azuredisk-snapshot.yaml
```

The output of the command resembles the following example:

```
volumesnapshotclass.snapshot.storage.k8s.io/csi-azuredisk-vsc created
```

Now let's create a [volume snapshot](#) from the PVC that [we dynamically created at the beginning of this tutorial](#), `pvc-azuredisk`.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-driver/master/deploy/example/snapshot/azuredisk-volume-snapshot.yaml
```

The output of the command resembles the following example:

```
volumesnapshot.snapshot.storage.k8s.io/azuredisk-volume-snapshot created
```

To verify that the snapshot was created correctly, run the following command:

```
kubectl describe volumesnapshot azuredisk-volume-snapshot
```

The output of the command resembles the following example:

```

Name: azuredisk-volume-snapshot
Namespace: default
Labels: <none>
Annotations: API Version: snapshot.storage.k8s.io/v1
Kind: VolumeSnapshot
Metadata:
 Creation Timestamp: 2020-08-27T05:27:58Z
 Finalizers:
 snapshot.storage.kubernetes.io/volumesnapshot-as-source-protection
 snapshot.storage.kubernetes.io/volumesnapshot-bound-protection
 Generation: 1
 Resource Version: 714582
 Self Link: /apis/snapshot.storage.k8s.io/v1/namespaces/default/volumesnapshots/azuredisk-volume-
snapshot
 UID: dd953ab5-6c24-42d4-ad4a-f33180e0ef87
Spec:
 Source:
 Persistent Volume Claim Name: pvc-azuredisk
 Volume Snapshot Class Name: csi-azuredisk-vsc
Status:
 Bound Volume Snapshot Content Name: snapcontent-dd953ab5-6c24-42d4-ad4a-f33180e0ef87
 Creation Time: 2020-08-31T05:27:59Z
 Ready To Use: true
 Restore Size: 10Gi
Events: <none>

```

### Create a new PVC based on a volume snapshot

You can create a new PVC based on a volume snapshot. Use the snapshot created in the previous step, and create a [new PVC](#) and a [new pod](#) to consume it.

```

kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-
driver/master/deploy/example/snapshot/pvc-azuredisk-snapshot-restored.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-
driver/master/deploy/example/snapshot/nginx-pod-restored-snapshot.yaml

```

The output of the command resembles the following example:

```

persistentvolumeclaim/pvc-azuredisk-snapshot-restored created
pod/nginx-restored created

```

Finally, let's make sure it's the same PVC created before by checking the contents by running the following command:

```

kubectl exec nginx-restored -- ls /mnt/azuredisk

```

The output of the command resembles the following example:

```

lost+found
outfile
test.txt

```

As expected, we can still see our previously created `test.txt` file.

## Clone volumes

A cloned volume is defined as a duplicate of an existing Kubernetes volume. For more information on cloning volumes in Kubernetes, see the conceptual documentation for [volume cloning](#).

The CSI driver for Azure Disks supports volume cloning. To demonstrate, create a [cloned volume](#) of the previously created `azuredisk-pvc` and a new pod to consume it.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-driver/master/deploy/example/cloning/pvc-azuredisk-cloning.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-driver/master/deploy/example/cloning/nginx-pod-restored-cloning.yaml
```

The output of the command resembles the following example:

```
persistentvolumeclaim/pvc-azuredisk-cloning created
pod/nginx-restored-cloning created
```

You can verify the content of the cloned volume by running the following command and confirming the file `test.txt` is created:

```
kubectl exec nginx-restored-cloning -- ls /mnt/azuredisk
```

The output of the command resembles the following example:

```
lost+found
outfile
test.txt
```

## Resize a persistent volume without downtime (Preview)

### IMPORTANT

Azure Disks CSI driver supports expanding PVCs without downtime (Preview). Follow this [link](#) to register the disk online resize feature.

```
az feature register --namespace Microsoft.Compute --name LiveResize
```

```
az feature show --namespace Microsoft.Compute --name LiveResize
```

Follow this [link](#) to expand PVCs **with** downtime if you cannot try preview feature.

You can request a larger volume for a PVC. Edit the PVC object, and specify a larger size. This change triggers the expansion of the underlying volume that backs the PV.

### NOTE

A new PV is never created to satisfy the claim. Instead, an existing volume is resized.

In AKS, the built-in `managed-csi` storage class already supports expansion, so use the [PVC created earlier with this storage class](#). The PVC requested a 10-Gi persistent volume. You can confirm by running the following command:

```
kubectl exec -it nginx-azuredisk -- df -h /mnt/azuredisk
```

The output of the command resembles the following example:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sdc	9.8G	42M	9.8G	1%	/mnt/azuredisk

Expand the PVC by increasing the `spec.resources.requests.storage` field running the following command:

```
kubectl patch pvc pvc-azuredisk --type merge --patch '{"spec": {"resources": {"requests": {"storage": "15Gi"}}}}'
```

The output of the command resembles the following example:

```
persistentvolumeclaim/pvc-azuredisk patched
```

Run the following command to confirm the volume size has increased:

```
kubectl get pv
```

The output of the command resembles the following example:

NAME	CAPACITY	ACCESS MODES	RECLAIM POLICY	STATUS	CLAIM
STORAGECLASS	REASON AGE				
pvc-391ea1a6-0191-4022-b915-c8dc4216174a	15Gi	RWO	Delete	Bound	default/pvc-azuredisk
(...)	managed-csi	2d2h			

And after a few minutes, run the following commands to confirm the size of the PVC:

```
kubectl get pvc pvc-azuredisk
```

The output of the command resembles the following example:

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS
AGE					
pvc-azuredisk	Bound	pvc-391ea1a6-0191-4022-b915-c8dc4216174a	15Gi	RWO	managed-csi
2d2h					

Run the following command to confirm the size of the disk inside the pod:

```
kubectl exec -it nginx-azuredisk -- df -h /mnt/azuredisk
```

The output of the command resembles the following example:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sdc	15G	46M	15G	1%	/mnt/azuredisk

## On-demand bursting

On-demand disk bursting model allows disk bursts whenever its needs exceed its current capacity. This model generates extra charges anytime the disk bursts. On-demand bursting is only available for premium SSDs larger than 512 GiB. For more information on premium SSDs provisioned IOPS and throughput per disk, see [Premium SSD size](#). Alternatively, credit-based bursting is where the disk will burst only if it has burst credits accumulated

in its credit bucket. Credit-based bursting doesn't generate extra charges when the disk bursts. Credit-based bursting is only available for premium SSDs 512 GiB and smaller, and standard SSDs 1024 GiB and smaller. For more information on on-demand bursting, see [On-demand bursting](#).

#### IMPORTANT

The default `managed-csi-premium` storage class has on-demand bursting disabled and uses credit-based bursting. Any premium SSD dynamically created by a persistent volume claim based on the default `managed-csi-premium` storage class also has on-demand bursting disabled.

To create a premium SSD persistent volume with [on-demand bursting](#) enabled, you can create a new storage class with the `enableBursting` parameter set to `true` as shown in the following YAML template. For more information on enabling on-demand bursting, see [On-demand bursting](#). For more information on building your own storage class with on-demand bursting enabled, see [Create a Burstable Managed CSI Premium Storage Class](#).

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
 name: burstable-managed-csi-premium
provisioner: disk.csi.azure.com
parameters:
 skuname: Premium_LRS
 enableBursting: "true"
reclaimPolicy: Delete
volumeBindingMode: WaitForFirstConsumer
allowVolumeExpansion: true
```

## Windows containers

The Azure Disks CSI driver supports Windows nodes and containers. If you want to use Windows containers, follow the [Windows containers quickstart](#) to add a Windows node pool.

After you have a Windows node pool, you can now use the built-in storage classes like `managed-csi`. You can deploy an example [Windows-based stateful set](#) that saves timestamps into the file `data.txt` by running the following `kubectl apply` command:

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azuredisk-csi-
driver/master/deploy/example/windows/statefulset.yaml
```

The output of the command resembles the following example:

```
statefulset.apps/busybox-azuredisk created
```

To validate the content of the volume, run the following command:

```
kubectl exec -it busybox-azuredisk-0 -- cat c:\\\\mnt\\\\azuredisk\\\\data.txt # on Linux/MacOS Bash
kubectl exec -it busybox-azuredisk-0 -- cat c:\\\\mnt\\\\azuredisk\\\\data.txt # on Windows Powershell/CMD
```

The output of the command resembles the following example:

2020-08-27 08:13:41Z

2020-08-27 08:13:42Z

2020-08-27 08:13:44Z

(...)

## Next steps

- To learn how to use CSI driver for Azure Files, see [Use Azure Files with CSI driver](#).
- To learn how to use CSI driver for Azure Blob storage (preview), see [Use Azure Blob storage with CSI driver \(preview\)](#).
- For more information about storage best practices, see [Best practices for storage and backups in Azure Kubernetes Service](#).

# Use Azure Files Container Storage Interface (CSI) driver in Azure Kubernetes Service (AKS)

10/27/2022 • 9 minutes to read • [Edit Online](#)

The Azure Files Container Storage Interface (CSI) driver is a [CSI specification](#)-compliant driver used by Azure Kubernetes Service (AKS) to manage the lifecycle of Azure Files shares. The CSI is a standard for exposing arbitrary block and file storage systems to containerized workloads on Kubernetes.

By adopting and using CSI, AKS now can write, deploy, and iterate plug-ins to expose new or improve existing storage systems in Kubernetes. Using CSI drivers in AKS avoids having to touch the core Kubernetes code and wait for its release cycles.

To create an AKS cluster with CSI drivers support, see [Enable CSI drivers on AKS](#).

## NOTE

*In-tree drivers* refers to the current storage drivers that are part of the core Kubernetes code versus the new CSI drivers, which are plug-ins.

## Azure Files CSI driver new features

In addition to the original in-tree driver features, Azure Files CSI driver supports the following new features:

- Network File System (NFS) version 4.1
- [Private endpoint](#)
- Creating large mount of file shares in parallel

## Use a persistent volume with Azure Files

A [persistent volume \(PV\)](#) represents a piece of storage that's provisioned for use with Kubernetes pods. A PV can be used by one or many pods and can be dynamically or statically provisioned. If multiple pods need concurrent access to the same storage volume, you can use Azure Files to connect by using the [Server Message Block \(SMB\)](#) or [NFS protocol](#). This article shows you how to dynamically create an Azure Files share for use by multiple pods in an AKS cluster. For static provisioning, see [Manually create and use a volume with an Azure Files share](#).

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Dynamically create Azure Files PVs by using the built-in storage classes

A storage class is used to define how an Azure Files share is created. A storage account is automatically created in the [node resource group](#) for use with the storage class to hold the Azure Files shares. Choose one of the following [Azure storage redundancy SKUs](#) for *skuName*:

- **Standard\_LRS**: Standard locally redundant storage
- **Standard\_GRS**: Standard geo-redundant storage
- **Standard\_ZRS**: Standard zone-redundant storage
- **Standard\_RAGRS**: Standard read-access geo-redundant storage

- **Standard\_RAGZRS**: Standard read-access geo-zone-redundant storage
- **Premium\_LRS**: Premium locally redundant storage
- **Premium\_ZRS**: Premium zone-redundant storage

#### NOTE

Azure Files supports Azure Premium Storage. The minimum premium file share is 100 GB.

When you use storage CSI drivers on AKS, there are two more built-in `StorageClasses` that use the Azure Files CSI storage drivers. The other CSI storage classes are created with the cluster alongside the in-tree default storage classes.

- `azurefile-csi` : Uses Azure Standard Storage to create an Azure Files share.
- `azurefile-csi-premium` : Uses Azure Premium Storage to create an Azure Files share.

The reclaim policy on both storage classes ensures that the underlying Azure Files share is deleted when the respective PV is deleted. The storage classes also configure the file shares to be expandable, you just need to edit the [persistent volume claim](#) (PVC) with the new size.

To use these storage classes, create a PVC and respective pod that references and uses them. A PVC is used to automatically provision storage based on a storage class. A PVC can use one of the pre-created storage classes or a user-defined storage class to create an Azure Files share for the desired SKU and size. When you create a pod definition, the PVC is specified to request the desired storage.

Create an [example PVC and pod that prints the current date into an `outfile`](#) by running the `kubectl apply` commands:

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azurefile-csi-driver/master/deploy/example/pvc-azurefile-csi.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azurefile-csi-driver/master/deploy/example/nginx-pod-azurefile.yaml
```

The output of the command resembles the following example:

```
persistentvolumeclaim/pvc-azurefile created
pod/nginx-azurefile created
```

After the pod is in the running state, you can validate that the file share is correctly mounted by running the following command and verifying the output contains the `outfile`:

```
kubectl exec nginx-azurefile -- ls -l /mnt/azurefile
```

The output of the command resembles the following example:

```
total 29
-rwxrwxrwx 1 root root 29348 Aug 31 21:59 outfile
```

## Create a custom storage class

The default storage classes suit the most common scenarios, but not all. For some cases, you might want to have your own storage class customized with your own parameters. For example, use the following manifest to configure the `mountOptions` of the file share.

The default value for `fileMode` and `dirMode` is `0777` for Kubernetes mounted file shares. You can specify the different mount options on the storage class object.

Create a file named `azure-file-sc.yaml`, and paste the following example manifest:

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
 name: my-azurefile
provisioner: file.csi.azure.com
reclaimPolicy: Delete
volumeBindingMode: Immediate
allowVolumeExpansion: true
mountOptions:
 - dir_mode=0640
 - file_mode=0640
 - uid=0
 - gid=0
 - mfsymlinks
 - cache=strict # https://linux.die.net/man/8/mount.cifs
 - nosharesock
parameters:
 skuName: Standard_LRS
```

Create the storage class by running the `kubectl apply` command:

```
kubectl apply -f azure-file-sc.yaml
```

The output of the command resembles the following example:

```
storageclass.storage.k8s.io/my-azurefile created
```

The Azure Files CSI driver supports creating [snapshots of persistent volumes](#) and the underlying file shares.

#### NOTE

This driver only supports snapshot creation, restore from snapshot is not supported by this driver. Snapshots can be restored from Azure portal or CLI. For more information about creating and restoring a snapshot, see [Overview of share snapshots for Azure Files](#).

Create a [volume snapshot class](#) with the `kubectl apply` command:

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azurefile-csi-driver/master/deploy/example/snapshot/volumesnapshotclass-azurefile.yaml
```

The output of the command resembles the following example:

```
volumesnapshotclass.snapshot.storage.k8s.io/csi-azurefile-vsc created
```

Create a [volume snapshot](#) from the PVC we dynamically created at the beginning of this tutorial, `pvc-azurefile`.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azurefile-csi-driver/master/deploy/example/snapshot/volumesnapshot-azurefile.yaml
```

The output of the command resembles the following example:

```
volumesnapshot.snapshot.storage.k8s.io/azurefile-volume-snapshot created
```

Verify the snapshot was created correctly by running the following command:

```
kubectl describe volumesnapshot azurefile-volume-snapshot
```

The output of the command resembles the following example:

```
Name: azurefile-volume-snapshot
Namespace: default
Labels: <none>
Annotations: API Version: snapshot.storage.k8s.io/v1beta1
Kind: VolumeSnapshot
Metadata:
 Creation Timestamp: 2020-08-27T22:37:41Z
 Finalizers:
 snapshot.storage.kubernetes.io/volumesnapshot-as-source-protection
 snapshot.storage.kubernetes.io/volumesnapshot-bound-protection
 Generation: 1
 Resource Version: 955091
 Self Link: /apis/snapshot.storage.k8s.io/v1beta1/namespaces/default/volumesnapshots/azurefile-
volume-snapshot
 UID: c359a38f-35c1-4fb1-9da9-2c06d35ca0f4
Spec:
 Source:
 Persistent Volume Claim Name: pvc-azurefile
 Volume Snapshot Class Name: csi-azurefile-vsc
Status:
 Bound Volume Snapshot Content Name: snapcontent-c359a38f-35c1-4fb1-9da9-2c06d35ca0f4
 Ready To Use: false
 Events: <none>
```

## Resize a persistent volume

You can request a larger volume for a PVC. Edit the PVC object, and specify a larger size. This change triggers the expansion of the underlying volume that backs the PV.

### NOTE

A new PV is never created to satisfy the claim. Instead, an existing volume is resized.

In AKS, the built-in `azurefile-csi` storage class already supports expansion, so use the [PVC created earlier with this storage class](#). The PVC requested a 100Gi file share. We can confirm that by running:

```
kubectl exec -it nginx-azurefile -- df -h /mnt/azurefile
```

The output of the command resembles the following example:

Filesystem	Size	Used	Avail
Use% Mounted on			
//f149b5a219bd34caeb07de9.file.core.windows.net/pvc-5e5d9980-da38-492b-8581-17e3cad01770	100G	128K	100G
1% /mnt/azurefile			

Expand the PVC by increasing the `spec.resources.requests.storage` field:

```
kubectl patch pvc pvc-azurefile --type merge --patch '{"spec": {"resources": {"requests": {"storage": "200Gi"}}}}'
```

The output of the command resembles the following example:

```
persistentvolumeclaim/pvc-azurefile patched
```

Verify that both the PVC and the file system inside the pod show the new size:

```
kubectl get pvc pvc-azurefile
NAME STATUS VOLUME CAPACITY ACCESS MODES STORAGECLASS
AGE
pvc-azurefile Bound pvc-5e5d9980-da38-492b-8581-17e3cad01770 200Gi RWX azurefile-csi
64m

kubectl exec -it nginx-azurefile -- df -h /mnt/azurefile
Filesystem Size Used Avail
Use% Mounted on
//f149b5a219bd34caeb07de9.file.core.windows.net/pvc-5e5d9980-da38-492b-8581-17e3cad01770 200G 128K 200G
1% /mnt/azurefile
```

## Use a persistent volume with private Azure Files storage (private endpoint)

If your Azure Files resources are protected with a private endpoint, you must create your own storage class that's customized with the following parameters:

- `resourceGroup` : The resource group where the storage account is deployed.
- `storageAccount` : The storage account name.
- `server` : The FQDN of the storage account's private endpoint (for example, `<storage account name>.privatelink.file.core.windows.net` ).

Create a file named `private-azure-file-sc.yaml`, and then paste the following example manifest in the file. Replace the values for `<resourceGroup>` and `<storageAccountName>`.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
 name: private-azurefile-csi
provisioner: file.csi.azure.com
allowVolumeExpansion: true
parameters:
 resourceGroup: <resourceGroup>
 storageAccount: <storageAccountName>
 server: <storageAccountName>.privatelink.file.core.windows.net
reclaimPolicy: Delete
volumeBindingMode: Immediate
mountOptions:
 - dir_mode=0777
 - file_mode=0777
 - uid=0
 - gid=0
 - mfsymlinks
 - cache=strict # https://linux.die.net/man/8/mount.cifs
 - nosharesock # reduce probability of reconnect race
 - actimeo=30 # reduce latency for metadata-heavy workload
```

Create the storage class by using the [kubectl apply](#) command:

```
kubectl apply -f private-azure-file-sc.yaml
```

The output of the command resembles the following example:

```
storageclass.storage.k8s.io/private-azurefile-csi created
```

Create a file named *private-pvc.yaml*, and then paste the following example manifest in the file:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: private-azurefile-pvc
spec:
 accessModes:
 - ReadWriteMany
 storageClassName: private-azurefile-csi
 resources:
 requests:
 storage: 100Gi
```

Create the PVC by using the [kubectl apply](#) command:

```
kubectl apply -f private-pvc.yaml
```

## NFS file shares

Azure Files supports the NFS v4.1 protocol. NFS version 4.1 support for Azure Files provides you with a fully managed NFS file system as a service built on a highly available and highly durable distributed resilient storage platform.

This option is optimized for random access workloads with in-place data updates and provides full POSIX file system support. This section shows you how to use NFS shares with the Azure File CSI driver on an AKS cluster.

## Prerequisites

- Your AKS clusters service principal or managed identity must be added to the Contributor role to the storage account.
- Your AKS cluster *Control plane* identity (that is, your AKS cluster name) is added to the [Contributor](#) role in the resource group hosting the VNet.

## Create NFS file share storage class

Create a file named `nfs-sc.yaml` and copy the manifest below.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
 name: azurefile-csi-nfs
provisioner: file.csi.azure.com
allowVolumeExpansion: true
parameters:
 protocol: nfs
mountOptions:
 - nconnect=8
```

After editing and saving the file, create the storage class with the [kubectl apply](#) command:

```
kubectl apply -f nfs-sc.yaml
```

The output of the command resembles the following example:

```
storageclass.storage.k8s.io/azurefile-csi-nfs created
```

## Create a deployment with an NFS-backed file share

You can deploy an example [stateful set](#) that saves timestamps into a file `data.txt` by deploying the following command with the [kubectl apply](#) command:

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azurefile-csi-
driver/master/deploy/example/nfs/statefulset.yaml
```

The output of the command resembles the following example:

```
statefulset.apps/statefulset-azurefile created
```

Validate the contents of the volume by running the following command:

```
kubectl exec -it statefulset-azurefile-0 -- df -h
```

The output of the command resembles the following example:

Filesystem	Size	Used	Avail	Use%	Mounted on
...					
/dev/sda1					29G 11G 19G
37% /etc/hosts					
accountname.file.core.windows.net:/accountname/pvc-fa72ec43-ae64-42e4-a8a2-556606f5da38	100G	0	100G	0%	/mnt/azurefile
...					

## NOTE

Note that since NFS file share is in Premium account, the minimum file share size is 100GB. If you create a PVC with a small storage size, you might encounter an error similar to the following: *failed to create file share ... size (5)....*

## Windows containers

The Azure Files CSI driver also supports Windows nodes and containers. To use Windows containers, follow the [Windows containers quickstart](#) to add a Windows node pool.

After you have a Windows node pool, use the built-in storage classes like `azurefile-csi` or create a custom one. You can deploy an example [Windows-based stateful set](#) that saves timestamps into a file `data.txt` by running the `kubectl apply` command:

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-sigs/azurefile-csi-driver/master/deploy/example/windows/statefulset.yaml
```

The output of the command resembles the following example:

```
statefulset.apps/busybox-azurefile created
```

Validate the contents of the volume by running the following `kubectl exec` command:

```
kubectl exec -it busybox-azurefile-0 -- cat c:\\mnt\\azurefile\\data.txt # on Linux/MacOS Bash
kubectl exec -it busybox-azurefile-0 -- cat c:\\mnt\\azurefile\\data.txt # on Windows Powershell/CMD
```

The output of the commands resembles the following example:

```
2020-08-27 22:11:01Z
2020-08-27 22:11:02Z
2020-08-27 22:11:04Z
(...)
```

## Next steps

- To learn how to use CSI driver for Azure Disks, see [Use Azure Disks with CSI driver](#).
- To learn how to use CSI driver for Azure Blob storage (preview), see [Use Azure Blob storage with CSI driver \(preview\)](#).
- For more about storage best practices, see [Best practices for storage and backups in Azure Kubernetes Service](#).

# Use Azure Blob storage Container Storage Interface (CSI) driver (preview)

10/27/2022 • 7 minutes to read • [Edit Online](#)

The Azure Blob storage Container Storage Interface (CSI) driver (preview) is a [CSI specification](#)-compliant driver used by Azure Kubernetes Service (AKS) to manage the lifecycle of Azure Blob storage. The CSI is a standard for exposing arbitrary block and file storage systems to containerized workloads on Kubernetes.

By adopting and using CSI, AKS now can write, deploy, and iterate plug-ins to expose new or improve existing storage systems in Kubernetes. Using CSI drivers in AKS avoids having to touch the core Kubernetes code and wait for its release cycles.

Mounting Azure Blob storage as a file system into a container or pod, enables you to use blob storage with a number of applications that work massive amounts of unstructured data. For example:

- Log file data
- Images, documents, and streaming video or audio
- Disaster recovery data

The data on the object storage can be accessed by applications using BlobFuse or Network File System (NFS) 3.0 protocol. Before the introduction of the Azure Blob storage CSI driver (preview), the only option was to manually install an unsupported driver to access Blob storage from your application running on AKS. When the Azure Blob storage CSI driver (preview) is enabled on AKS, there are two built-in storage classes: *azureblob-fuse-premium* and *azureblob-nfs-premium*.

To create an AKS cluster with CSI drivers support, see [CSI drivers on AKS](#). To learn more about the differences in access between each of the Azure storage types using the NFS protocol, see [Compare access to Azure Files, Blob Storage, and Azure NetApp Files with NFS](#).

## Azure Blob storage CSI driver (preview) features

Azure Blob storage CSI driver (preview) supports the following features:

- BlobFuse and Network File System (NFS) version 3.0 protocol

## Before you begin

- The Azure CLI version 2.37.0 or later. Run `az --version` to find the version, and run `az upgrade` to upgrade the version. If you need to install or upgrade, see [Install Azure CLI](#).
- Install the `aks-preview` Azure CLI extension version 0.5.85 or later.
- If the open-source CSI Blob storage driver is installed on your cluster, uninstall it before enabling the preview driver.

### Uninstall open-source driver

Perform the steps in this [link](#) if you previously installed the [CSI Blob Storage open-source driver](#) to access Azure Blob storage from your cluster.

## Install the Azure CLI `aks-preview` extension

The following steps are required to install and register the Azure CLI `aks-preview` extension and driver in your

subscription.

1. To use the Azure CLI aks-preview extension for enabling the Blob storage CSI driver (preview) on your AKS cluster, run the following command to install it:

```
az extension add --name aks-preview
```

2. Run the following command to register the CSI driver (preview):

```
az feature register --name EnableBlobCSIDriver --namespace Microsoft.ContainerService
```

3. To register the provider, run the following command:

```
az provider register -n Microsoft.ContainerService
```

When newer versions of the extension are released, run the following command to upgrade the extension to the latest release:

```
az extension update --name aks-preview
```

## Enable CSI driver on a new or existing AKS cluster

Using the Azure CLI, you can enable the Blob storage CSI driver (preview) on a new or existing AKS cluster before you configure a persistent volume for use by pods in the cluster.

To enable the driver on a new cluster, include the `--enable-blob-driver` parameter with the `az aks create` command as shown in the following example:

```
az aks create --enable-blob-driver -n myAKSCluster -g myResourceGroup
```

To enable the driver on an existing cluster, include the `--enable-blob-driver` parameter with the `az aks update` command as shown in the following example:

```
az aks update --enable-blob-driver -n myAKSCluster -g myResourceGroup
```

You're prompted to confirm there isn't an open-source Blob CSI driver installed. After confirming, it may take several minutes to complete this action. Once it's complete, you should see in the output the status of enabling the driver on your cluster. The following example is resembles the section indicating the results of the previous command:

```
"storageProfile": {
 "blobCsiDriver": {
 "enabled": true
 },
```

## Disable CSI driver on an existing AKS cluster

Using the Azure CLI, you can disable the Blob storage CSI driver on an existing AKS cluster after you remove the persistent volume from the cluster.

To disable the driver on an existing cluster, include the `--disable-blob-driver` parameter with the `az aks update` command as shown in the following example:

```
az aks update --disable-blob-driver -n myAKSCluster -g myResourceGroup
```

## Use a persistent volume with Azure Blob storage

A [persistent volume](#) (PV) represents a piece of storage that's provisioned for use with Kubernetes pods. A PV can be used by one or many pods and can be dynamically or statically provisioned. If multiple pods need concurrent access to the same storage volume, you can use Azure Blob storage to connect by using the Network File System (NFS) or blobfuse. This article shows you how to dynamically create an Azure Blob storage container for use by multiple pods in an AKS cluster.

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Dynamically create Azure Blob storage PVs by using the built-in storage classes

A storage class is used to define how an Azure Blob storage container is created. A storage account is automatically created in the node resource group for use with the storage class to hold the Azure Blob storage container. Choose one of the following Azure storage redundancy SKUs for skuName:

- **Standard\_LRS**: Standard locally redundant storage
- **Premium\_LRS**: Premium locally redundant storage
- **Standard\_GRS**: Standard geo-redundant storage
- **Standard\_RAGRS**: Standard read-access geo-redundant storage

When you use storage CSI drivers on AKS, there are two additional built-in StorageClasses that use the Azure Blob CSI storage driver (preview).

The reclaim policy on both storage classes ensures that the underlying Azure Blob storage is deleted when the respective PV is deleted. The storage classes also configure the container to be expandable by default, as the `set allowVolumeExpansion` parameter is set to **true**.

Use the `kubectl get sc` command to see the storage classes. The following example shows the `azureblob-fuse-premium` and `azureblob-nfs-premium` storage classes available within an AKS cluster:

NAME	PROVISIONER	RECLAIMPOLICY	VOLUMEBINDINGMODE
ALLOWVOLUMEEXPANSION	AGE		
azureblob-fuse-premium	blob.csi.azure.com	Delete	Immediate
23h			true
azureblob-nfs-premium	blob.csi.azure.com	Delete	Immediate
23h			true

To use these storage classes, create a PVC and respective pod that references and uses them. A PVC is used to automatically provision storage based on a storage class. A PVC can use one of the pre-created storage classes or a user-defined storage class to create an Azure Blob storage container for the desired SKU, size, and protocol to communicate with it. When you create a pod definition, the PVC is specified to request the desired storage.

## Using a StatefulSet

To have a storage volume persist for your workload, you can use a StatefulSet. This makes it easier to match existing volumes to new Pods that replace any that have failed. The following examples demonstrate how to set up a StatefulSet for Blob storage using either Blobfuse or the NFS protocol.

- [NFS](#)
- [Blobfuse](#)

1. Create a file named `azure-blob-nfs-ss.yaml` and copy in the following YAML.

```

apiVersion: apps/v1
kind: StatefulSet
metadata:
 name: statefulset-blob-nfs
 labels:
 app: nginx
spec:
 serviceName: statefulset-blob-nfs
 replicas: 1
 template:
 metadata:
 labels:
 app: nginx
 spec:
 nodeSelector:
 "kubernetes.io/os": linux
 containers:
 - name: statefulset-blob-nfs
 image: mcr.microsoft.com/oss/nginx/nginx:1.19.5
 volumeMounts:
 - name: persistent-storage
 mountPath: /mnt/blob
 updateStrategy:
 type: RollingUpdate
 selector:
 matchLabels:
 app: nginx
 volumeClaimTemplates:
 - metadata:
 name: persistent-storage
 annotations:
 volume.beta.kubernetes.io/storage-class: azureblob-nfs-premium
 spec:
 accessModes: ["ReadWriteMany"]
 resources:
 requests:
 storage: 100Gi

```

2. Create the StatefulSet with the `kubectl create` command:

```
kubectl create -f azure-blob-nfs-ss.yaml
```

## Next steps

- To learn how to manually set up a static persistent volume, see [Create and use a volume with Azure Blob storage](#).
- To learn how to dynamically set up a persistent volume, see [Create and use a dynamic persistent volume with Azure Blob storage](#).
- To learn how to use CSI driver for Azure Disks, see [Use Azure Disks with CSI driver](#).
- To learn how to use CSI driver for Azure Files, see [Use Azure Files with CSI driver](#).
- For more about storage best practices, see [Best practices for storage and backups in Azure Kubernetes Service](#).

# Integrate Azure NetApp Files with Azure Kubernetes Service

10/27/2022 • 10 minutes to read • [Edit Online](#)

A persistent volume represents a piece of storage that has been provisioned for use with Kubernetes pods. A persistent volume can be used by one or many pods and can be dynamically or statically provisioned. This article shows you how to create [Azure NetApp Files](#) volumes to be used by pods in an Azure Kubernetes Service (AKS) cluster.

[Azure NetApp Files](#) is an enterprise-class, high-performance, metered file storage service running on Azure. Kubernetes users have two options when it comes to using Azure NetApp Files volumes for Kubernetes workloads:

- Create Azure NetApp Files volumes **statically**: In this scenario, the creation of volumes is achieved external to AKS; volumes are created using `az` /Azure UI and are then exposed to Kubernetes by the creation of a `PersistentVolume`. Statically created Azure NetApp Files volumes have lots of limitations (for example, inability to be expanded, needing to be over-provisioned, and so on) and are not recommended for most use cases.
- Create Azure NetApp Files volumes **on-demand**, orchestrating through Kubernetes: This method is the **preferred** mode of operation for creating multiple volumes directly through Kubernetes and is achieved using [Astra Trident](#). Astra Trident is a CSI-compliant dynamic storage orchestrator that helps provision volumes natively through Kubernetes.

Using a CSI driver to directly consume Azure NetApp Files volumes from AKS workloads is **highly recommended** for most use cases. This requirement is fulfilled using Astra Trident, an open-source dynamic storage orchestrator for Kubernetes. Astra Trident is an enterprise-grade storage orchestrator purpose-built for Kubernetes, fully supported by NetApp. It simplifies access to storage from Kubernetes clusters by automating storage provisioning. You can take advantage of Astra Trident's Container Storage Interface (CSI) driver for Azure NetApp Files to abstract underlying details and create, expand, and snapshot volumes on-demand. Also, using Astra Trident enables you to use [Astra Control Service](#) built on top of Astra Trident to backup, recover, move, and manage the application-data lifecycle of your AKS workloads across clusters within and across Azure regions to meet your business and service continuity needs.

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

### IMPORTANT

Your AKS cluster must also be [in a region that supports Azure NetApp Files](#).

You also need the Azure CLI version 2.0.59 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

### Prerequisites

The following considerations apply when you use Azure NetApp Files:

- Azure NetApp Files is only available [in selected Azure regions](#).

- After the initial deployment of an AKS cluster, you can choose to provision Azure NetApp Files volumes statically or dynamically.
- To use dynamic provisioning with Azure NetApp Files, install and configure [Astra Trident](#) version 19.07 or later.

## Configure Azure NetApp Files

Register the *Microsoft.NetApp* resource provider:

```
az provider register --namespace Microsoft.NetApp --wait
```

### NOTE

This can take some time to complete.

When you create an Azure NetApp account for use with AKS, you can create the account in an existing resource group or create a new one in the same region as the AKS cluster. The following example creates an account named *myaccount1* in the *myResourceGroup* resource group and *eastus* region:

```
az netappfiles account create \
--resource-group myResourceGroup \
--location eastus \
--account-name myaccount1
```

Create a new capacity pool by using [az netappfiles pool create](#). The following example creates a new capacity pool named *mypool1* with 4 TB in size and *Premium* service level:

```
az netappfiles pool create \
--resource-group myResourceGroup \
--location eastus \
--account-name myaccount1 \
--pool-name mypool1 \
--size 4 \
--service-level Premium
```

Create a subnet to [delegate to Azure NetApp Files](#) using [az network vnet subnet create](#). *This subnet must be in the same virtual network as your AKS cluster.*

```
RESOURCE_GROUP=myResourceGroup
VNET_NAME=$(az network vnet list --resource-group $RESOURCE_GROUP --query [].name -o tsv)
VNET_ID=$(az network vnet show --resource-group $RESOURCE_GROUP --name $VNET_NAME --query "id" -o tsv)
SUBNET_NAME=MyNetAppSubnet
az network vnet subnet create \
--resource-group $RESOURCE_GROUP \
--vnet-name $VNET_NAME \
--name $SUBNET_NAME \
--delegations "Microsoft.NetApp/volumes" \
--address-prefixes 10.0.0.0/28
```

Volumes can either be provisioned statically or dynamically. Both options are covered in detail below.

## Provision Azure NetApp Files volumes statically

Create a volume by using [az netappfiles volume create](#).

```

RESOURCE_GROUP=myResourceGroup
LOCATION=eastus
ANF_ACCOUNT_NAME=myaccount1
POOL_NAME=mypool1
SERVICE_LEVEL=Premium
VNET_NAME=$(az network vnet list --resource-group $RESOURCE_GROUP --query [].name -o tsv)
VNET_ID=$(az network vnet show --resource-group $RESOURCE_GROUP --name $VNET_NAME --query "id" -o tsv)
SUBNET_NAME=MyNetAppSubnet
SUBNET_ID=$(az network vnet subnet show --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --name $SUBNET_NAME --query "id" -o tsv)
VOLUME_SIZE_GiB=100 # 100 GiB
UNIQUE_FILE_PATH="myfilepath2" # Note that file path needs to be unique within all ANF Accounts

az netappfiles volume create \
 --resource-group $RESOURCE_GROUP \
 --location $LOCATION \
 --account-name $ANF_ACCOUNT_NAME \
 --pool-name $POOL_NAME \
 --name "myvol1" \
 --service-level $SERVICE_LEVEL \
 --vnet $VNET_ID \
 --subnet $SUBNET_ID \
 --usage-threshold $VOLUME_SIZE_GiB \
 --file-path $UNIQUE_FILE_PATH \
 --protocol-types "NFSv3"

```

## Create the PersistentVolume

List the details of your volume using [az netappfiles volume show](#)

```

az netappfiles volume show \
 --resource-group $RESOURCE_GROUP \
 --account-name $ANF_ACCOUNT_NAME \
 --pool-name $POOL_NAME \
 --volume-name "myvol1" -o JSON

```

```
{
 ...
 "creationToken": "myfilepath2",
 ...
 "mountTargets": [
 {
 ...
 "ipAddress": "10.0.0.4",
 ...
 }
],
 ...
}
```

Create a `pv-nfs.yaml` defining a PersistentVolume. Replace `path` with the *creationToken* and `server` with *ipAddress* from the previous command. For example:

```

apiVersion: v1
kind: PersistentVolume
metadata:
 name: pv-nfs
spec:
 capacity:
 storage: 100Gi
 accessModes:
 - ReadWriteMany
 mountOptions:
 - vers=3
 nfs:
 server: 10.0.0.4
 path: /myfilepath2
```

Update the *server* and *path* to the values of your NFS (Network File System) volume you created in the previous step. Create the PersistentVolume with the [kubectl apply](#) command:

```
kubectl apply -f pv-nfs.yaml
```

Verify the *Status* of the PersistentVolume is *Available* using the [kubectl describe](#) command:

```
kubectl describe pv pv-nfs
```

### Create the PersistentVolumeClaim

Create a [pvc-nfs.yaml](#) defining a PersistentVolume. For example:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: pvc-nfs
spec:
 accessModes:
 - ReadWriteMany
 storageClassName: ""
 resources:
 requests:
 storage: 1Gi
```

Create the PersistentVolumeClaim with the [kubectl apply](#) command:

```
kubectl apply -f pvc-nfs.yaml
```

Verify the *Status* of the PersistentVolumeClaim is *Bound* using the [kubectl describe](#) command:

```
kubectl describe pvc pvc-nfs
```

### Mount with a pod

Create a [nginx-nfs.yaml](#) defining a pod that uses the PersistentVolumeClaim. For example:

```

kind: Pod
apiVersion: v1
metadata:
 name: nginx-nfs
spec:
 containers:
 - image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 name: nginx-nfs
 command:
 - "/bin/sh"
 - "-c"
 - "while true; do echo $(date) >> /mnt/azure/outfile; sleep 1; done"
 volumeMounts:
 - name: disk01
 mountPath: /mnt/azure
 volumes:
 - name: disk01
 persistentVolumeClaim:
 claimName: pvc-nfs

```

Create the pod with the [kubectl apply](#) command:

```
kubectl apply -f nginx-nfs.yaml
```

Verify the pod is *Running* using the [kubectl describe](#) command:

```
kubectl describe pod nginx-nfs
```

Verify your volume has been mounted in the pod by using [kubectl exec](#) to connect to the pod then `df -h` to check if the volume is mounted.

```
$ kubectl exec -it nginx-nfs -- sh
```

```
/ # df -h
Filesystem Size Used Avail Use% Mounted on
...
10.0.0.4:/myfilepath2 100T 384K 100T 1% /mnt/azure
...
```

## Provision Azure NetApp Files volumes dynamically

### Install and configure Astra Trident

To dynamically provision volumes, you need to install Astra Trident. Astra Trident is NetApp's dynamic storage provisioner that is purpose-built for Kubernetes. Simplify the consumption of storage for Kubernetes applications using Astra Trident's industry-standard [Container Storage Interface \(CSI\)](#) drivers. Astra Trident deploys in Kubernetes clusters as pods and provides dynamic storage orchestration services for your Kubernetes workloads.

You can learn more from the [documentation]<https://docs.netapp.com/us-en/trident/index.html>.

Before proceeding to the next step, you will need to:

1. **Install Astra Trident.** Trident can be installed using the operator/Helm chart/`tridentctl`. The instructions provided below explain how Astra Trident can be installed using the operator. To learn how the other install methods work, see the [Install Guide](#).

2. **Create a backend.** To instruct Astra Trident about the Azure NetApp Files subscription and where it needs to create volumes, a backend is created. This step requires details about the account that was created in the previous step.

#### Install Astra Trident using the operator

This section walks you through the installation of Astra Trident using the operator. You can also choose to install using one of its other methods:

- [Helm chart](#).
- [tridentctl](#).

See to [Deploying Trident](#) to understand how each option works and identify the one that works best for you.

Download Astra Trident from its [GitHub repository](#). Choose from the desired version and download the installer bundle.

```
#Download Astra Trident

$ wget https://github.com/NetApp/trident/releases/download/v21.07.1/trident-installer-21.07.1.tar.gz
$ tar xzvf trident-installer-21.07.1.tar.gz
```

Deploy the operator using `deploy/bundle.yaml`.

```
$ kubectl create ns trident

namespace/trident created

$ kubectl apply -f trident-installer/deploy/bundle.yaml -n trident

serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created
```

Create a `TridentOrchestrator` to install Astra Trident.

```
$ kubectl apply -f trident-installer/deploy/crds/tridentorchestrator_cr.yaml

tridentorchestrator.trident.netapp.io/trident created
```

The operator installs by using the parameters provided in the `TridentOrchestrator` spec. You can learn about the configuration parameters and example backends from the extensive [installation](#) and [backend guides](#).

Confirm Astra Trident was installed.

```
$ kubectl describe trc trident
Name: trident
Namespace:
Labels: <none>
Annotations: <none>
API Version: trident.netapp.io/v1
Kind: TridentOrchestrator
...
Spec:
 Debug: true
 Namespace: trident
Status:
 Current Installation Params:
 IPv6: false
 Autosupport Hostname:
 Autosupport Image: netapp/trident-autosupport:21.01
 Autosupport Proxy:
 Autosupport Serial Number:
 Debug: true
 Enable Node Prep: false
 Image Pull Secrets:
 Image Registry:
 k8sTimeout: 30
 Kubelet Dir: /var/lib/kubelet
 Log Format: text
 Silence Autosupport: false
 Trident Image: netapp/trident:21.07.1
 Message: Trident installed
 Namespace: trident
 Status: Installed
 Version: v21.07.1
 Events:
 Type Reason Age From Message
 ---- ----- ---- -- -----
 Normal Installing 74s trident-operator.netapp.io Installing Trident
 Normal Installed 67s trident-operator.netapp.io Trident installed
```

## Create a backend

After Astra Trident is installed, create a backend that points to your Azure NetApp Files subscription.

```
$ kubectl apply -f trident-installer/sample-input/backends-samples/azure-netapp-files/backend-anf.yaml -n
trident

secret/backend-tbc-anf-secret created
tridentbackendconfig.trident.netapp.io/backend-tbc-anf created
```

Before running the command, you need to update `backend-anf.yaml` to include details about the Azure NetApp Files subscription, such as:

- `subscriptionID` for the Azure subscription with Azure NetApp Files enabled. The
- `tenantID`, `clientID`, and `clientSecret` from an [App Registration](#) in Azure Active Directory (AD) with sufficient permissions for the Azure NetApp Files service. The App Registration must carry the `Owner` or `Contributor` role that's predefined by Azure.
- Azure location that contains at least one delegated subnet.

In addition, you can choose to provide a different service level. Azure NetApp Files provides three [service levels](#): Standard, Premium, and Ultra.

## Create a StorageClass

A storage class is used to define how a unit of storage is dynamically created with a persistent volume. To

consume Azure NetApp Files volumes, a storage class must be created. Create a file named `anf-storageclass.yaml` and copy in the manifest provided below.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
 name: azure-netapp-files
provisioner: csi.trident.netapp.io
parameters:
 backendType: "azure-netapp-files"
 fsType: "nfs"
```

Create the storage class using `kubectl apply` command:

```
$ kubectl apply -f anf-storageclass.yaml

storageclass/azure-netapp-files created

$ kubectl get sc
NAME PROVISIONER RECLAIMPOLICY VOLUMEBINDINGMODE ALLOWVOLUMEEXPANSION AGE
azure-netapp-files csi.trident.netapp.io Delete Immediate false 3s
```

### Create a PersistentVolumeClaim

A PersistentVolumeClaim (PVC) is a request for storage by a user. Upon the creation of a PersistentVolumeClaim, Astra Trident automatically creates an Azure NetApp Files volume and makes it available for Kubernetes workloads to consume.

Create a file named `anf-pvc.yaml` and provide the following manifest. In this example, a 1-TiB volume is created that is *ReadWriteMany*.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
 name: anf-pvc
spec:
 accessModes:
 - ReadWriteMany
 resources:
 requests:
 storage: 1Ti
 storageClassName: azure-netapp-files
```

Create the persistent volume claim with the `kubectl apply` command:

```
$ kubectl apply -f anf-pvc.yaml

persistentvolumeclaim/anf-pvc created

$ kubectl get pvc
kubectl get pvc -n trident
NAME STATUS VOLUME CAPACITY ACCESS MODES STORAGECLASS
AGE
anf-pvc Bound pvc-bffa315d-3f44-4770-86eb-c922f567a075 1Ti RWO azure-netapp-files
62s
```

### Use the persistent volume

After the PVC is created, a pod can be spun up to access the Azure NetApp Files volume. The manifest below can be used to define an NGINX pod that mounts the Azure NetApp Files volume that was created in the previous

step. In this example, the volume is mounted at `/mnt/data`.

Create a file named `anf-nginx-pod.yaml`, which contains the following manifest:

```
kind: Pod
apiVersion: v1
metadata:
 name: nginx-pod
spec:
 containers:
 - name: nginx
 image: mcr.microsoft.com/oss/nginx/nginx:latest1.15.5-alpine
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 volumeMounts:
 - mountPath: "/mnt/data"
 name: volume
 volumes:
 - name: volume
 persistentVolumeClaim:
 claimName: anf-pvc
```

Create the pod with the `kubectl apply` command:

```
$ kubectl apply -f anf-nginx-pod.yaml
pod/nginx-pod created
```

Kubernetes has now created a pod with the volume mounted and accessible within the `nginx` container at `/mnt/data`. Confirm by checking the event logs for the pod using `kubectl describe`:

```
$ kubectl describe pod nginx-pod
[...]
Volumes:
volume:
 Type: PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
 ClaimName: anf-pvc
 ReadOnly: false
default-token-k7952:
 Type: Secret (a volume populated by a Secret)
 SecretName: default-token-k7952
 Optional: false
[...]
Events:
 Type Reason Age From Message
 ---- ----- ---- --- -----
 Normal Scheduled 15s default-scheduler Successfully assigned trident/nginx-pod to brameshb-non-root-test
 Normal SuccessfulAttachVolume 15s attachdetach-controller AttachVolume.Attach succeeded for volume "pvc-bffa315d-3f44-4770-86eb-c922f567a075"
 Normal Pulled 12s kubelet Container image "mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine" already present on machine
 Normal Created 11s kubelet Created container nginx
 Normal Started 10s kubelet Started container nginx
```

Astra Trident supports many features with Azure NetApp Files, such as:

- Expanding volumes
- On-demand volume snapshots
- Importing volumes

## Using Azure tags

For more details on using Azure tags, see [Use Azure tags in Azure Kubernetes Service \(AKS\)](#).

## Next steps

- For more information on Azure NetApp Files, see [What is Azure NetApp Files](#).

# Use Azure ultra disks on Azure Kubernetes Service

10/27/2022 • 4 minutes to read • [Edit Online](#)

Azure ultra disks offer high throughput, high IOPS, and consistent low latency disk storage for your stateful applications. One major benefit of ultra disks is the ability to dynamically change the performance of the SSD along with your workloads without the need to restart your agent nodes. Ultra disks are suited for data-intensive workloads.

## Before you begin

This feature can only be set at cluster creation or node pool creation time.

### IMPORTANT

Azure ultra disks require nodepools deployed in availability zones and regions that support these disks as well as only specific VM series. See the [Ultra disks GA scope and limitations](#).

### Limitations

- See the [Ultra disks GA scope and limitations](#)
- The supported size range for a Ultra disks is between 100 and 1500

## Create a new cluster that can use Ultra disks

Create an AKS cluster that is able to leverage Ultra Disks by using the following CLI commands. Use the

```
--enable-ultra-ssd
```

flag to set the `EnableUltrassd` feature.

Create an Azure resource group:

```
Create an Azure resource group
az group create --name myResourceGroup --location westus2
```

Create the AKS cluster with support for Ultra Disks.

```
Create an AKS-managed Azure AD cluster
az aks create -g MyResourceGroup -n MyManagedCluster -l westus2 --node-vm-size Standard_D2s_v3 --zones 1 2 -
--node-count 2 --enable-ultra-ssd
```

If you want to create clusters without ultra disk support, you can do so by omitting the `--enable-ultra-ssd` parameter.

## Enable Ultra disks on an existing cluster

You can enable ultra disks on existing clusters by adding a new node pool to your cluster that support ultra disks. Configure a new node pool to use ultra disks by using the `--enable-ultra-ssd` flag.

```
az aks nodepool add --name ultradisk --cluster-name myAKScluster --resource-group myResourceGroup --node-vm-
size Standard_D2s_v3 --zones 1 2 --node-count 2 --enable-ultra-ssd
```

If you want to create new node pools without support for ultra disks, you can do so by omitting the

```
--enable-ultra-ssd
```

parameter.

## Use ultra disks dynamically with a storage class

To use ultra disks in our deployments or stateful sets you can use a [storage class for dynamic provisioning](#).

### Create the storage class

A storage class is used to define how a unit of storage is dynamically created with a persistent volume. For more information on Kubernetes storage classes, see [Kubernetes Storage Classes](#).

In this case, we'll create a storage class that references ultra disks. Create a file named `azure-ultra-disk-sc.yaml`, and copy in the following manifest.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
 name: ultra-disk-sc
provisioner: disk.csi.azure.com # replace with "kubernetes.io/azure-disk" if aks version is less than 1.21
volumeBindingMode: WaitForFirstConsumer # optional, but recommended if you want to wait until the pod that
will use this disk is created
parameters:
 skuname: UltraSSD_LRS
 kind: managed
 cachingMode: None
 diskIopsReadWrite: "2000" # minimum value: 2 IOPS/GiB
 diskMbpsReadWrite: "320" # minimum value: 0.032/GiB
```

Create the storage class with the `kubectl apply` command and specify your `azure-ultra-disk-sc.yaml` file:

```
$ kubectl apply -f azure-ultra-disk-sc.yaml

storageclass.storage.k8s.io/ultra-disk-sc created
```

## Create a persistent volume claim

A persistent volume claim (PVC) is used to automatically provision storage based on a storage class. In this case, a PVC can use the previously created storage class to create an ultra disk.

Create a file named `azure-ultra-disk-pvc.yaml`, and copy in the following manifest. The claim requests a disk named `ultra-disk` that is `1000 GB` in size with `ReadWriteOnce` access. The `ultra-disk-sc` storage class is specified as the storage class.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: ultra-disk
spec:
 accessModes:
 - ReadWriteOnce
 storageClassName: ultra-disk-sc
 resources:
 requests:
 storage: 1000Gi
```

Create the persistent volume claim with the `kubectl apply` command and specify your `azure-ultra-disk-pvc.yaml` file:

```
$ kubectl apply -f azure-ultra-disk-pvc.yaml
```

```
persistentvolumeclaim/ultra-disk created
```

## Use the persistent volume

Once the persistent volume claim has been created and the disk successfully provisioned, a pod can be created with access to the disk. The following manifest creates a basic NGINX pod that uses the persistent volume claim named *ultra-disk* to mount the Azure disk at the path `/mnt/azure`.

Create a file named `nginx-ultra.yaml`, and copy in the following manifest.

```
kind: Pod
apiVersion: v1
metadata:
 name: nginx-ultra
spec:
 containers:
 - name: nginx-ultra
 image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 volumeMounts:
 - mountPath: "/mnt/azure"
 name: volume
 volumes:
 - name: volume
 persistentVolumeClaim:
 claimName: ultra-disk
```

Create the pod with the `kubectl apply` command, as shown in the following example:

```
$ kubectl apply -f nginx-ultra.yaml
```

```
pod/nginx-ultra created
```

You now have a running pod with your Azure disk mounted in the `/mnt/azure` directory. This configuration can be seen when inspecting your pod via `kubectl describe pod nginx-ultra`, as shown in the following condensed example:

```
$ kubectl describe pod nginx-ultra

[...]
Volumes:
volume:
 Type: PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
 ClaimName: azure-managed-disk
 ReadOnly: false
default-token-smm2n:
 Type: Secret (a volume populated by a Secret)
 SecretName: default-token-smm2n
 Optional: false
[...]
Events:
 Type Reason Age From Message
 ---- ----- -- -- -----
 Normal Scheduled 2m default-scheduler Successfully assigned mypod to
 aks-nodepool1-79590246-0
 Normal SuccessfulMountVolume 2m kubelet, aks-nodepool1-79590246-0 MountVolume.SetUp succeeded for
 volume "default-token-smm2n"
 Normal SuccessfulMountVolume 1m kubelet, aks-nodepool1-79590246-0 MountVolume.SetUp succeeded for
 volume "pvc-faf0f176-8b8d-11e8-923b-deb28c58d242"
[...]
```

## Using Azure tags

For more details on using Azure tags, see [Use Azure tags in Azure Kubernetes Service \(AKS\)](#).

## Next steps

- For more about ultra disks, see [Using Azure ultra disks](#).
- For more about storage best practices, see [Best practices for storage and backups in Azure Kubernetes Service \(AKS\)](#)

# Dynamically create and use a persistent volume with Azure Blob storage in Azure Kubernetes Service (AKS)

10/27/2022 • 6 minutes to read • [Edit Online](#)

Container-based applications often need to access and persist data in an external data volume. If multiple pods need concurrent access to the same storage volume, you can use Azure Blob storage to connect using [blobfuse](#) or [Network File System](#) (NFS).

This article shows you how to install the Container Storage Interface (CSI) driver and dynamically create an Azure Blob storage container to attach to a pod in AKS.

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Before you begin

- This article assumes that you have an existing AKS cluster running version 1.21 or higher. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).
- If you don't have a storage account that supports the NFS v3 protocol, review [NFS v3 support with Azure Blob storage](#).
- [Enable the Blob storage CSI driver](#) (preview) on your AKS cluster.

## Dynamic provisioning parameters

NAME	DESCRIPTION	EXAMPLE	MANDATORY	DEFAULT VALUE
skuName	Specify an Azure storage account type (alias: <code>storageAccountType</code> ).	<code>Standard_LRS</code> , <code>Premium_LRS</code> , <code>Standard_GRS</code> , <code>Standard_RAGRS</code>	No	<code>Standard_LRS</code>
location	Specify an Azure location.	<code>eastus</code>	No	If empty, driver will use the same location name as current cluster.
resourceGroup	Specify an Azure resource group name.	myResourceGroup	No	If empty, driver will use the same resource group name as current cluster.

NAME	DESCRIPTION	EXAMPLE	MANDATORY	DEFAULT VALUE
storageAccount	Specify an Azure storage account name.	storageAccountName	- No for blobfuse mount - Yes for NFSv3 mount.	- For blobfuse mount: if empty, driver finds a suitable storage account that matches <code>skuName</code> in the same resource group. If a storage account name is provided, storage account must exist. - For NFSv3 mount, storage account name must be provided.
protocol	Specify blobfuse mount or NFSv3 mount.	<code>fuse</code> , <code>nfs</code>	No	<code>fuse</code>
containerName	Specify the existing container (directory) name.	container	No	If empty, driver creates a new container name, starting with <code>pvc-fuse</code> for blobfuse or <code>pvc-nfs</code> for NFS v3.
containerNamePrefix	Specify Azure storage directory prefix created by driver.	my	Can only contain lowercase letters, numbers, hyphens, and length should be fewer than 21 characters.	No
server	Specify Azure storage account domain name.	Existing storage account DNS domain name, for example <code>&lt;storage-account&gt;.privatelink.blob.core.windows.net</code>	No	If empty, driver uses default <code>&lt;storage-account&gt;.blob.core.windows.net</code> or other sovereign cloud storage account DNS domain name.
allowBlobPublicAccess	Allow or disallow public access to all blobs or containers for storage account created by driver.	<code>true</code> , <code>false</code>	No	<code>false</code>
storageEndpointSuffix	Specify Azure storage endpoint suffix.	<code>core.windows.net</code>	No	If empty, driver will use default storage endpoint suffix according to cloud environment.
tags	[tags][az-tags] would be created in new storage account.	Tag format: 'foo=aaa,bar=bbb'	No	""

NAME	DESCRIPTION	EXAMPLE	MANDATORY	DEFAULT VALUE
matchTags	Match tags when driver tries to find a suitable storage account.	true , false	No	false
---	<b>Following parameters are only for blobfuse</b>	---	---	---
subscriptionID	Specify Azure subscription ID where blob storage directory will be created.	Azure subscription ID	No	If not empty, resourceGroup must be provided.
storeAccountKey	Specify store account key to Kubernetes secret.  Note: false means driver uses kubelet identity to get account key.	true , false	No	true
secretName	Specify secret name to store account key.		No	
secretNamespace	Specify the namespace of secret to store account key.	default , kube-system , etc.	No	pvc namespace
isHnsEnabled	Enable Hierarchical namespace for Azure DataLake storage account.	true , false	No	false
---	<b>Following parameters are only for NFS protocol</b>	---	---	---
mountPermissions	Specify mounted folder permissions.	The default is 0777 . If set to 0 , driver won't perform chmod after mount.	0777	No

## Create a persistent volume claim using built-in storage class

A persistent volume claim (PVC) uses the storage class object to dynamically provision an Azure Blob storage container. The following YAML can be used to create a persistent volume claim 5 GB in size with *ReadWriteMany* access, using the built-in storage class. For more information on access modes, see the [Kubernetes persistent volume](#) documentation.

1. Create a file named `blob-nfs-pvc.yaml` and copy in the following YAML.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: azure-blob-storage
 annotations:
 volume.beta.kubernetes.io/storage-class: azureblob-nfs-premium
spec:
 accessModes:
 - ReadWriteMany
 storageClassName: my-blobstorage
 resources:
 requests:
 storage: 5Gi
```

2. Create the persistent volume claim with the `kubectl create` command:

```
kubectl create -f blob-nfs-pvc.yaml
```

Once completed, the Blob storage container will be created. You can use the `kubectl get` command to view the status of the PVC:

```
kubectl get pvc azure-blob-storage
```

The output of the command resembles the following example:

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES
STORAGECLASS	AGE			
azure-blob-storage	Bound	pvc-b88e36c5-c518-4d38-a5ee-337a7dda0a68	5Gi	RWX
azureblob-nfs-premium	92m			

## Use the persistent volume claim

The following YAML creates a pod that uses the persistent volume claim **azure-blob-storage** to mount the Azure Blob storage at the `'/mnt/blob'` path.

1. Create a file named `blob-nfs-pv`, and copy in the following YAML. Make sure that the `claimName` matches the PVC created in the previous step.

```
kind: Pod
apiVersion: v1
metadata:
 name: mypod
spec:
 containers:
 - name: mypod
 image: mcr.microsoft.com/oss/nginx/nginx:1.17.3-alpine
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 volumeMounts:
 - mountPath: "/mnt/blob"
 name: volume
 volumes:
 - name: volume
 persistentVolumeClaim:
 claimName: azure-blob-storage
```

2. Create the pod with the [kubectl apply](#) command:

```
kubectl apply -f blob-nfs-pv.yaml
```

3. After the pod is in the running state, run the following command to create a new file called `test.txt`.

```
kubectl exec mypod -- touch /mnt/blob/test.txt
```

4. To validate the disk is correctly mounted, run the following command, and verify you see the `test.txt` file in the output:

```
kubectl exec mypod -- ls /mnt/blob
```

The output of the command resembles the following example:

```
test.txt
```

## Create a custom storage class

The default storage classes suit the most common scenarios, but not all. For some cases, you might want to have your own storage class customized with your own parameters. To demonstrate, two examples are shown. One based on using the NFS protocol, and the other using blobfuse.

### Storage class using NFS protocol

In this example, the following manifest configures mounting a Blob storage container using the NFS protocol. Use it to add the `tags` parameter.

1. Create a file named `blob-nfs-sc.yaml`, and paste the following example manifest:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
 name: azureblob-nfs-premium
provisioner: blob.csi.azure.com
parameters:
 protocol: nfs
 tags: environment=Development
volumeBindingMode: Immediate
```

2. Create the storage class with the [kubectl apply](#) command:

```
kubectl apply -f blob-nfs-sc.yaml
```

The output of the command resembles the following example:

```
storageclass.storage.k8s.io/blob-nfs-premium created
```

### Storage class using blobfuse

In this example, the following manifest configures using blobfuse and mount a Blob storage container. Use it to update the *skuName* parameter.

1. Create a file named `blobfuse-sc.yaml`, and paste the following example manifest:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
 name: azureblob-fuse-premium
provisioner: blob.csi.azure.com
parameters:
 skuName: Standard_GRS # available values: Standard_LRS, Premium_LRS, Standard_GRS, Standard_RAGRS
 reclaimPolicy: Delete
 volumeBindingMode: Immediate
 allowVolumeExpansion: true
 mountOptions:
 - -o allow_other
 - --file-cache-timeout-in-seconds=120
 - --use-attr-cache=true
 - --cancel-list-on-mount-seconds=10 # prevent billing charges on mounting
 - -o attr_timeout=120
 - -o entry_timeout=120
 - -o negative_timeout=120
 - --log-level=LOG_WARNING # LOG_WARNING, LOG_INFO, LOG_DEBUG
 - --cache-size-mb=1000 # Default will be 80% of available memory, eviction will happen beyond that.
```

2. Create the storage class with the [kubectl apply](#) command:

```
kubectl apply -f blobfuse-sc.yaml
```

The output of the command resembles the following example:

```
storageclass.storage.k8s.io/blob-fuse-premium created
```

## Next steps

- To learn how to use CSI driver for Azure Blob storage, see [Use Azure Blob storage with CSI driver][azure-csi]

`blob-storage-csi`].

- To learn how to manually set up a static persistent volume, see [Create and use a volume with Azure Blob storage](#).
- For associated best practices, see [Best practices for storage and backups in AKS](#).

# Create and use a static volume with Azure Blob storage in Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

Container-based applications often need to access and persist data in an external data volume. If multiple pods need concurrent access to the same storage volume, you can use Azure Blob storage to connect using [blobfuse](#) or [Network File System](#) (NFS).

This article shows you how to create an Azure Blob storage container or use an existing one and attach it to a pod in AKS.

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Before you begin

- This article assumes that you have an existing AKS cluster running version 1.21 or higher. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).
- If you don't have a storage account that supports the NFS v3 protocol, review [NFS v3 support with Azure Blob storage](#).
- [Enable the Blob storage CSI driver](#) (preview) on your AKS cluster.

## Static provisioning parameters

NAME	DESCRIPTION	EXAMPLE	MANDATORY	DEFAULT VALUE
volumeAttributes.resourceGroup	Specify Azure resource group name.	myResourceGroup	No	If empty, driver will use the same resource group name as current cluster.
volumeAttributes.storageAccount	Specify existing Azure storage account name.	storageAccountName	Yes	
volumeAttributes.containerName	Specify existing container name.	container	Yes	
volumeAttributes.protocol	Specify blobfuse mount or NFS v3 mount.	<code>fuse</code> , <code>nfs</code>	No	<code>fuse</code>
---	Following parameters are only for blobfuse	---	---	---
volumeAttributes.secretName	Secret name that stores storage account name and key (only applies for SMB).		No	

NAME	DESCRIPTION	EXAMPLE	MANDATORY	DEFAULT VALUE
volumeAttributes.secretNamespace	Specify namespace of secret to store account key.	default	No	Pvc namespace
nodeStageSecretRef.name	Specify secret name that stores (see examples below):  azurestorageaccountkey azurestorageaccountsastoken msisecret azureraigespnclientsecret  .		Existing Kubernetes secret name	No
nodeStageSecretRef.namespace	Specify the namespace of secret.	k8s namespace	Yes	
---	<b>Following parameters are only for NFS protocol</b>	---	---	---
volumeAttributes.mountPermissions	Specify mounted folder permissions.	0777	No	
---	<b>Following parameters are only for NFS VNet setting</b>	---	---	---
vnetResourceGroup	Specify VNet resource group hosting virtual network.	myResourceGroup	No	If empty, driver uses the vnetResourceGroup value specified in the Azure cloud config file.
vnetName	Specify the virtual network name.	aksVNet	No	If empty, driver uses the vnetName value specified in the Azure cloud config file.
subnetName	Specify the existing subnet name of the agent node.	aksSubnet	No	If empty, driver uses the subnetName value in Azure cloud config file.
---	<b>Following parameters are only for feature: blobfuse</b> <b>Managed Identity and Service Principal Name authentication</b>	---	---	---

Name	Description	Example	Mandatory	Default Value
volumeAttributes.AzureStorageAuthType	Specify the authentication type.	Key , SAS , MSI , SPN	No	Key
volumeAttributes.AzureStorageIdentityClientID	Specify the Identity Client ID.		No	
volumeAttributes.AzureStorageIdentityObjectID	Specify the Identity Object ID.		No	
volumeAttributes.AzureStorageIdentityResourceID	Specify the Identity Resource ID.		No	
volumeAttributes.MSIEndpoint	Specify the MSI endpoint.		No	
volumeAttributes.AzureStorageSPNClientID	Specify the Azure Service Principal Name (SPN) Client ID.		No	
volumeAttributes.AzureStorageSPNTenantID	Specify the Azure SPN Tenant ID.		No	
volumeAttributes.AzureStorageAADEndpoint	Specify the Azure Active Directory (Azure AD) endpoint.		No	
---	<b>Following parameters are only for feature: blobfuse read account key or SAS token from key vault</b>	---	---	---
volumeAttributes.keyVaultURL	Specify Azure Key Vault DNS name.	{vault-name}.vault.azure.net	No	
volumeAttributes.keyVaultSecretName	Specify Azure Key Vault secret name.	Existing Azure Key Vault secret name.	No	
volumeAttributes.keyVaultSecretVersion	Azure Key Vault secret version.	Existing version	No	If empty, driver uses current version.

## Create a Blob storage container

When you create an Azure Blob storage resource for use with AKS, you can create the resource in the node resource group. This approach allows the AKS cluster to access and manage the blob storage resource. If instead you create the blob storage resource in a separate resource group, you must grant the Azure Kubernetes Service managed identity for your cluster the [Contributor](#) role to the blob storage resource group.

For this article, create the container in the node resource group. First, get the resource group name with the `az`

`aks show` command and add the `--query nodeResourceGroup` query parameter. The following example gets the node resource group for the AKS cluster named **myAKSCluster** in the resource group named **myResourceGroup**:

```
az aks show --resource-group myResourceGroup --name myAKSCluster --query nodeResourceGroup -o tsv
```

The output of the command resembles the following example:

```
MC_myResourceGroup_myAKSCluster_eastus
```

Next, create a container for storing blobs following the steps in the [Manage blob storage](#) to authorize access and then create the container.

## Mount Blob storage as a volume using NFS

Mounting Blob storage using the NFS v3 protocol doesn't authenticate using an account key. Your AKS cluster needs to reside in the same or peered virtual network as the agent node. The only way to secure the data in your storage account is by using a virtual network and other network security settings. For more information on how to set up NFS access to your storage account, see [Mount Blob Storage by using the Network File System \(NFS\) 3.0 protocol](#).

The following example demonstrates how to mount a Blob storage container as a persistent volume using the NFS protocol.

1. Create a file named `pv-blob-nfs.yaml` and copy in the following YAML. Under `storageClass`, update `resourceGroup`, `storageAccount`, and `containerName`.

```
apiVersion: v1
kind: PersistentVolume
metadata:
 name: pv-blob
spec:
 capacity:
 storage: 10Gi
 accessModes:
 - ReadWriteMany
 persistentVolumeReclaimPolicy: Retain # If set as "Delete" container would be removed after pvc deletion
 storageClassName: azureblob-nfs-premium
 csi:
 driver: blob.csi.azure.com
 readOnly: false
 # make sure this volumeid is unique in the cluster
 # `#` is not allowed in self defined volumeHandle
 volumeHandle: unique-volumeid
 volumeAttributes:
 resourceGroup: resourceName
 storageAccount: storageAccountName
 containerName: containerName
 protocol: nfs
```

2. Run the following command to create the persistent volume using the `kubectl create` command referencing the YAML file created earlier:

```
kubectl create -f pv-blob-nfs.yaml
```

3. Create a `pvc-blob-nfs.yaml` file with a *PersistentVolume*. For example:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
 name: pvc-blob
spec:
 accessModes:
 - ReadWriteMany
 resources:
 requests:
 storage: 10Gi
 volumeName: pv-blob
 storageClassName: azureblob-nfs-premium
```

4. Run the following command to create the persistent volume claim using the `kubectl create` command referencing the YAML file created earlier:

```
kubectl create -f pvc-blob-nfs.yaml
```

## Mount Blob storage as a volume using Blobfuse

Kubernetes needs credentials to access the Blob storage container created earlier, which is either an Azure access key or SAS tokens. These credentials are stored in a Kubernetes secret, which is referenced when you create a Kubernetes pod.

1. Use the `kubectl create secret` command to create the secret. You can authenticate using a [Kubernetes secret](#) or [shared access signature \(SAS\) tokens](#).

- [Secret](#)
- [SAS tokens](#)

The following example creates a [Secret object](#) named *azure-secret* and populates the *azurestorageaccountname* and *azurestorageaccountkey*. You need to provide the account name and key from an existing Azure storage account.

```
kubectl create secret generic azure-secret --from-literal azurestorageaccountname=NAME --from-literal
azurestorageaccountkey="KEY" --type=Opaque
```

2. Create a `pv-blobfuse.yaml` file. Under `volumeAttributes`, update `containerName`. Under `nodeStateSecretRef`, update `name` with the name of the Secret object created earlier. For example:

```

apiVersion: v1
kind: PersistentVolume
metadata:
 name: pv-blob
spec:
 capacity:
 storage: 10Gi
 accessModes:
 - ReadWriteMany
 persistentVolumeReclaimPolicy: Retain # If set as "Delete" container would be removed after pvc deletion
 storageClassName: azureblob-fuse-premium
 mountOptions:
 - -o allow_other
 - --file-cache-timeout-in-seconds=120
 csi:
 driver: blob.csi.azure.com
 readOnly: false
 # make sure this volumeid is unique in the cluster
 # `#` is not allowed in self defined volumeHandle
 volumeHandle: unique-volumeid
 volumeAttributes:
 containerName: containerName
 nodeStageSecretRef:
 name: azure-secret
 namespace: default

```

3. Run the following command to create the persistent volume using the `kubectl create` command referencing the YAML file created earlier:

```
kubectl create -f pv-blobfuse.yaml
```

4. Create a `pvc-blobfuse.yaml` file with a *PersistentVolume*. For example:

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: pvc-blob
spec:
 accessModes:
 - ReadWriteMany
 resources:
 requests:
 storage: 10Gi
 volumeName: pv-blob
 storageClassName: azureblob-fuse-premium

```

5. Run the following command to create the persistent volume claim using the `kubectl create` command referencing the YAML file created earlier:

```
kubectl create -f pvc-blobfuse.yaml
```

## Use the persistence volume

The following YAML creates a pod that uses the persistent volume or persistent volume claim named **pvc-blob** created earlier, to mount the Azure Blob storage at the `'/mnt/blob'` path.

1. Create a file named `nginx-pod-blob.yaml`, and copy in the following YAML. Make sure that the

`claimName` matches the PVC created in the previous step when creating a persistent volume for NFS or Blobfuse.

```
kind: Pod
apiVersion: v1
metadata:
 name: nginx-blob
spec:
 nodeSelector:
 "kubernetes.io/os": linux
 containers:
 - image: mcr.microsoft.com/oss/nginx/nginx:1.17.3-alpine
 name: nginx-blob
 volumeMounts:
 - name: blob01
 mountPath: "/mnt/blob"
 volumes:
 - name: blob01
 persistentVolumeClaim:
 claimName: pvc-blob
```

- Run the following command to create the pod and mount the PVC using the `kubectl create` command referencing the YAML file created earlier:

```
kubectl create -f nginx-pod-blob.yaml
```

- Run the following command to create an interactive shell session with the pod to verify the Blob storage mounted:

```
kubectl exec -it nginx-blob -- df -h
```

The output from the command resembles the following example:

Filesystem	Size	Used	Avail	Use%	Mounted on
...					
blobfuse	14G	41M	13G	1%	/mnt/blob
...					

## Next steps

- To learn how to use CSI driver for Azure Blob storage, see [Use Azure Blob storage with CSI driver](#).
- To learn how to manually set up a dynamic persistent volume, see [Create and use a dynamic volume with Azure Blob storage](#).
- For associated best practices, see [Best practices for storage and backups in AKS](#).

# Dynamically create and use a persistent volume with Azure Disks in Azure Kubernetes Service (AKS)

10/27/2022 • 7 minutes to read • [Edit Online](#)

A persistent volume represents a piece of storage that has been provisioned for use with Kubernetes pods. A persistent volume can be used by one or many pods, and can be dynamically or statically provisioned. This article shows you how to dynamically create persistent volumes with Azure Disks for use by a single pod in an Azure Kubernetes Service (AKS) cluster.

## NOTE

An Azure Disk can only be mounted with *Access mode* type *ReadWriteOnce*, which makes it available to one node in AKS. If you need to share a persistent volume across multiple nodes, use [Azure Files](#).

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Before you begin

This article assumes that you have an existing AKS cluster with 1.21 or later version. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

You also need the Azure CLI version 2.0.59 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Built-in storage classes

A storage class is used to define how a unit of storage is dynamically created with a persistent volume. For more information on Kubernetes storage classes, see [Kubernetes Storage Classes](#).

Each AKS cluster includes four pre-created storage classes, two of them configured to work with Azure Disks:

- The *default* storage class provisions a standard SSD Azure Disk.
  - Standard storage is backed by Standard SSDs and delivers cost-effective storage while still delivering reliable performance.
- The *managed-csi-premium* storage class provisions a premium Azure Disk.
  - Premium disks are backed by SSD-based high-performance, low-latency disk. Perfect for VMs running production workload. If the AKS nodes in your cluster use premium storage, select the *managed-premium* class.

If you use one of the default storage classes, you can't update the volume size after the storage class is created. To be able to update the volume size after a storage class is created, add the line `allowVolumeExpansion: true` to one of the default storage classes, or you can create your own custom storage class. It's not supported to reduce the size of a PVC (to prevent data loss). You can edit an existing storage class by using the `kubectl edit sc` command.

For example, if you want to use a disk of size 4 TiB, you must create a storage class that defines `cachingmode: None` because [disk caching isn't supported for disks 4 TiB and larger](#).

For more information about storage classes and creating your own storage class, see [Storage options for applications in AKS](#).

Use the `kubectl get sc` command to see the pre-created storage classes. The following example shows the pre-create storage classes available within an AKS cluster:

```
kubectl get sc
```

The output of the command resembles the following example:

NAME	PROVISIONER	AGE
default (default)	disk.csi.azure.com	1h
managed-csi	disk.csi.azure.com	1h

#### NOTE

Persistent volume claims are specified in GiB but Azure managed disks are billed by SKU for a specific size. These SKUs range from 32GiB for S4 or P4 disks to 32TiB for S80 or P80 disks (in preview). The throughput and IOPS performance of a Premium managed disk depends on the both the SKU and the instance size of the nodes in the AKS cluster. For more information, see [Pricing and performance of managed disks](#).

## Create a persistent volume claim

A persistent volume claim (PVC) is used to automatically provision storage based on a storage class. In this case, a PVC can use one of the pre-created storage classes to create a standard or premium Azure managed disk.

Create a file named `azure-pvc.yaml`, and copy in the following manifest. The claim requests a disk named `azure-managed-disk` that is 5 GB in size with *ReadWriteOnce* access. The `managed-csi` storage class is specified as the storage class.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: azure-managed-disk
spec:
 accessModes:
 - ReadWriteOnce
 storageClassName: managed-csi
 resources:
 requests:
 storage: 5Gi
```

#### TIP

To create a disk that uses premium storage, use `storageClassName: managed-csi-premium` rather than `managed-csi`.

Create the persistent volume claim with the `kubectl apply` command and specify your `azure-pvc.yaml` file:

```
kubectl apply -f azure-pvc.yaml
```

The output of the command resembles the following example:

```
persistentvolumeclaim/azure-managed-disk created
```

## Use the persistent volume

Once the persistent volume claim has been created and the disk successfully provisioned, a pod can be created with access to the disk. The following manifest creates a basic NGINX pod that uses the persistent volume claim named *azure-managed-disk* to mount the Azure Disk at the path `/mnt/azure`. For Windows Server containers, specify a *mountPath* using the Windows path convention, such as '*D:*'.

Create a file named `azure-pvc-disk.yaml`, and copy in the following manifest.

```
kind: Pod
apiVersion: v1
metadata:
 name: mypod
spec:
 containers:
 - name: mypod
 image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 volumeMounts:
 - mountPath: "/mnt/azure"
 name: volume
 volumes:
 - name: volume
 persistentVolumeClaim:
 claimName: azure-managed-disk
```

Create the pod with the [kubectl apply](#) command, as shown in the following example:

```
kubectl apply -f azure-pvc-disk.yaml

pod/mypod created
```

You now have a running pod with your Azure Disk mounted in the `/mnt/azure` directory. This configuration can be seen when inspecting your pod via `kubectl describe pod mypod`, as shown in the following condensed example:

```
kubectl describe pod mypod
```

The output of the command resembles the following example:

```
[...]
Volumes:
volume:
 Type: PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
 ClaimName: azure-managed-disk
 ReadOnly: false
default-token-smm2n:
 Type: Secret (a volume populated by a Secret)
 SecretName: default-token-smm2n
 Optional: false
[...]
Events:
 Type Reason Age From Message
 ---- ----- ---- -- -----
 Normal Scheduled 2m default-scheduler Successfully assigned mypod to aks-nodepool1-79590246-0
 Normal SuccessfulMountVolume 2m kubelet, aks-nodepool1-79590246-0 MountVolume.SetUp succeeded for volume "default-token-smm2n"
 Normal SuccessfulMountVolume 1m kubelet, aks-nodepool1-79590246-0 MountVolume.SetUp succeeded for volume "pvc-faf0f176-8b8d-11e8-923b-deb28c58d242"
[...]
```

## Use Ultra Disks

To use ultra disk, see [Use Ultra Disks on Azure Kubernetes Service \(AKS\)](#).

## Back up a persistent volume

To back up the data in your persistent volume, take a snapshot of the managed disk for the volume. You can then use this snapshot to create a restored disk and attach to pods as a means of restoring the data.

First, get the volume name with the `kubectl get pvc` command, such as for the PVC named *azure-managed-disk*:

```
$ kubectl get pvc azure-managed-disk

NAME STATUS VOLUME CAPACITY ACCESS MODES
STORAGECLASS AGE pvc-faf0f176-8b8d-11e8-923b-deb28c58d242 5Gi RWO
premium 3m
```

This volume name forms the underlying Azure Disk name. Query for the disk ID with [az disk list](#) and provide your PVC volume name, as shown in the following example:

```
az disk list --query '[].id | [?contains(@,`pvc-faf0f176-8b8d-11e8-923b-deb28c58d242`)]' -o tsv
/subscriptions/<guid>/resourceGroups/MC_MYRESOURCEGROUP_MYAKSCLUSTER_EASTUS/providers/MicrosoftCompute/disks
/kubernetes-dynamic-pvc-faf0f176-8b8d-11e8-923b-deb28c58d242
```

Use the disk ID to create a snapshot disk with [az snapshot create](#). The following example creates a snapshot named *pvcSnapshot* in the same resource group as the AKS cluster (*MC\_myResourceGroup\_myAKSCluster\_eastus*). You may encounter permission issues if you create snapshots and restore disks in resource groups that the AKS cluster doesn't have access to.

```
az snapshot create \
 --resource-group MC_myResourceGroup_myAKSCluster_eastus \
 --name pvcSnapshot \
 --source
/subscriptions/<guid>/resourceGroups/MC_myResourceGroup_myAKSCluster_eastus/providers/MicrosoftCompute/disks
/kubernetes-dynamic-pvc-faf0f176-8b8d-11e8-923b-deb28c58d242
```

Depending on the amount of data on your disk, it may take a few minutes to create the snapshot.

## Restore and use a snapshot

To restore the disk and use it with a Kubernetes pod, use the snapshot as a source when you create a disk with [az disk create](#). This operation preserves the original resource if you then need to access the original data snapshot. The following example creates a disk named *pvcRestored* from the snapshot named *pvcSnapshot*.

```
az disk create --resource-group MC_myResourceGroup_myAKSCluster_eastus --name pvcRestored --source
pvcSnapshot
```

To use the restored disk with a pod, specify the ID of the disk in the manifest. Get the disk ID with the [az disk show](#) command. The following example gets the disk ID for *pvcRestored* created in the previous step:

```
az disk show --resource-group MC_myResourceGroup_myAKSCluster_eastus --name pvcRestored --query id -o tsv
```

Create a pod manifest named `azure-restored.yaml` and specify the disk URI obtained in the previous step. The following example creates a basic NGINX web server, with the restored disk mounted as a volume at `/mnt/azure`.

```
kind: Pod
apiVersion: v1
metadata:
 name: mypodrestored
spec:
 containers:
 - name: mypodrestored
 image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 volumeMounts:
 - mountPath: "/mnt/azure"
 name: volume
 volumes:
 - name: volume
 azureDisk:
 kind: Managed
 diskName: pvcRestored
 diskURI:
/subscriptions/<guid>/resourceGroups/MC_myResourceGroupAKS_myAKSCluster_eastus/providers/Microsoft.Compute/disks/pvcRestored
```

Create the pod with the [kubectl apply](#) command, as shown in the following example:

```
$ kubectl apply -f azure-restored.yaml
```

The output of the command resembles the following example:

```
pod/mypodrestored created
```

You can use `kubectl describe pod mypodrestored` to view details of the pod, such as the following condensed example that shows the volume information:

```
kubectl describe pod mypodrestored
```

The output of the command resembles the following example:

```
[...]
Volumes:
volume:
 Type: AzureDisk (an Azure Data Disk mount on the host and bind mount to the pod)
 DiskName: pvcRestored
 DiskURI: /subscriptions/19da35d3-9a1a-4f3b-9b9c-
 3c56ef409565/resourceGroups/MC_myResourceGroupAKS_myAKSCluster_eastus/providers/Microsoft.Compute/disks/pvcR
 estored
 Kind: Managed
 FSType: ext4
 CachingMode: ReadWrite
 ReadOnly: false
[...]
```

## Using Azure tags

For more information on using Azure tags, see [Use Azure tags in Azure Kubernetes Service \(AKS\)](#).

## Next steps

For associated best practices, see [Best practices for storage and backups in AKS](#).

Learn more about Kubernetes persistent volumes using Azure Disks.

[Kubernetes plugin for Azure Disks](#)

# Create a static volume with Azure disks in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

Container-based applications often need to access and persist data in an external data volume. If a single pod needs access to storage, you can use Azure disks to present a native volume for application use. This article shows you how to manually create an Azure disk and attach it to a pod in AKS.

## NOTE

An Azure disk can only be mounted to a single pod at a time. If you need to share a persistent volume across multiple pods, use [Azure Files](#).

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Before you begin

This article assumes that you have an existing AKS cluster with 1.21 or later version. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

If you want to interact with Azure disks on an AKS cluster with 1.20 or previous version, see the [Kubernetes plugin for Azure disks](#).

## Storage class static provisioning

The following table describes the Storage Class parameters for the Azure disk CSI driver static provisioning:

NAME	MEANING	AVAILABLE VALUE	MANDATORY	DEFAULT VALUE
volumeHandle	Azure disk URI	/subscriptions/{sub-id}resourcegroups/{groupname}/providers/microsoft.compute/disks/{disk-id}	Yes	N/A
volumeAttributes.fsType	File system type	ext4 , ext3 , ext2 , xfs , btrfs for Linux, ntfs for Windows	No	ext4 for Linux, ntfs for Windows
volumeAttributes.partition	Partition number of the existing disk (only supported on Linux)	1 , 2 , 3	No	Empty (no partition) - Make sure partition format is like -part1
volumeAttributes.cachingMode	Disk host cache setting	None , ReadOnly , ReadWrite	No	ReadOnly

## Create an Azure disk

When you create an Azure disk for use with AKS, you can create the disk resource in the **node** resource group. This approach allows the AKS cluster to access and manage the disk resource. If instead you created the disk in a

separate resource group, you must grant the Azure Kubernetes Service (AKS) managed identity for your cluster the `contributor` role to the disk's resource group. In this exercise, you're going to create the disk in the same resource group as your cluster.

1. Identify the resource group name using the `az aks show` command and add the

`--query nodeResourceGroup` parameter. The following example gets the node resource group for the AKS cluster name *myAKSCluster* in the resource group name *myResourceGroup*.

```
$ az aks show --resource-group myResourceGroup --name myAKSCluster --query nodeResourceGroup -o tsv
MC_myResourceGroup_myAKSCluster_eastus
```

2. Create a disk using the `az disk create` command. Specify the node resource group name obtained in the previous command, and then a name for the disk resource, such as *myAKSDisk*. The following example creates a 20GiB disk, and outputs the ID of the disk after it's created. If you need to create a disk for use with Windows Server containers, add the `--os-type windows` parameter to correctly format the disk.

```
az disk create \
--resource-group MC_myResourceGroup_myAKSCluster_eastus \
--name myAKSDisk \
--size-gb 20 \
--query id --output tsv
```

#### NOTE

Azure disks are billed by SKU for a specific size. These SKUs range from 32GiB for S4 or P4 disks to 32TiB for S80 or P80 disks (in preview). The throughput and IOPS performance of a Premium managed disk depends on both the SKU and the instance size of the nodes in the AKS cluster. See [Pricing and Performance of Managed Disks](#).

The disk resource ID is displayed once the command has successfully completed, as shown in the following example output. This disk ID is used to mount the disk in the next section.

```
/subscriptions/<subscriptionID>/resourceGroups/MC_myAKSCluster_myAKSCluster_eastus/providers/Microsoft.Compute/disks/myAKSDisk
```

## Mount disk as a volume

1. Create a `pv-azuredisk.yaml` file with a *PersistentVolume*. Update `volumeHandle` with disk resource ID from the previous step. For example:

```

apiVersion: v1
kind: PersistentVolume
metadata:
 name: pv-azuredisk
spec:
 capacity:
 storage: 20Gi
 accessModes:
 - ReadWriteOnce
 persistentVolumeReclaimPolicy: Retain
 storageClassName: managed-csi
 csi:
 driver: disk.csi.azure.com
 readOnly: false
 volumeHandle:
 /subscriptions/<subscriptionID>/resourceGroups/MC_myAKSCluster_myAKSCluster_eastus/providers/Microsoft.Compute/disks/myAKSDisk
 volumeAttributes:
 fsType: ext4

```

2. Create a *pvc-azuredisk.yaml* file with a *PersistentVolumeClaim* that uses the *PersistentVolume*. For example:

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: pvc-azuredisk
spec:
 accessModes:
 - ReadWriteOnce
 resources:
 requests:
 storage: 20Gi
 volumeName: pv-azuredisk
 storageClassName: managed-csi

```

3. Use the `kubectl` commands to create the *PersistentVolume* and *PersistentVolumeClaim*, referencing the two YAML files created earlier:

```

kubectl apply -f pv-azuredisk.yaml
kubectl apply -f pvc-azuredisk.yaml

```

4. To verify your *PersistentVolumeClaim* is created and bound to the *PersistentVolume*, run the following command:

```

$ kubectl get pvc pvc-azuredisk

NAME STATUS VOLUME CAPACITY ACCESS MODES STORAGECLASS AGE
pvc-azuredisk Bound pv-azuredisk 20Gi RWO managed-csi 5s

```

5. Create a *azure-disk-pod.yaml* file to reference your *PersistentVolumeClaim*. For example:

```
apiVersion: v1
kind: Pod
metadata:
 name: mypod
spec:
 nodeSelector:
 kubernetes.io/os: linux
 containers:
 - image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 name: mypod
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 volumeMounts:
 - name: azure
 mountPath: /mnt/azure
 volumes:
 - name: azure
 persistentVolumeClaim:
 claimName: pvc-azuredisk
```

- Run the following command to apply the configuration and mount the volume, referencing the YAML configuration file created in the previous steps:

```
kubectl apply -f azure-disk-pod.yaml
```

## Next steps

To learn about our recommended storage and backup practices, see [Best practices for storage and backups in AKS](#).

# Dynamically create and use a persistent volume with Azure Files in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

A persistent volume represents a piece of storage that has been provisioned for use with Kubernetes pods. A persistent volume can be used by one or many pods, and can be dynamically or statically provisioned. If multiple pods need concurrent access to the same storage volume, you can use Azure Files to connect using the [Server Message Block \(SMB\) protocol](#). This article shows you how to dynamically create an Azure Files share for use by multiple pods in an Azure Kubernetes Service (AKS) cluster.

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Before you begin

This article assumes that you have an existing AKS cluster with 1.21 or later version. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

You also need the Azure CLI version 2.0.59 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Create a storage class

A storage class is used to define how an Azure file share is created. A storage account is automatically created in the [node resource group](#) for use with the storage class to hold the Azure file shares. Choose of the following [Azure storage redundancy](#) for *skuName*:

- *Standard\_LRS* - standard locally redundant storage (LRS)
- *Standard\_GRS* - standard geo-redundant storage (GRS)
- *Standard\_ZRS* - standard zone redundant storage (ZRS)
- *Standard\_RAGRS* - standard read-access geo-redundant storage (RA-GRS)
- *Premium\_LRS* - premium locally redundant storage (LRS)
- *Premium\_ZRS* - premium zone redundant storage (ZRS)

### NOTE

Minimum premium file share is 100GB.

For more information on Kubernetes storage classes for Azure Files, see [Kubernetes Storage Classes](#).

Create a file named `azure-file-sc.yaml` and copy in the following example manifest. For more information on *mountOptions*, see the [Mount options](#) section.

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
 name: my-azurefile
provisioner: file.csi.azure.com # replace with "kubernetes.io/azure-file" if aks version is less than 1.21
allowVolumeExpansion: true
mountOptions:
 - dir_mode=0777
 - file_mode=0777
 - uid=0
 - gid=0
 - mfsymlinks
 - cache=strict
 - actimeo=30
parameters:
 skuName: Premium_LRS
```

Create the storage class with the [kubectl apply](#) command:

```
kubectl apply -f azure-file-sc.yaml
```

## Create a persistent volume claim

A persistent volume claim (PVC) uses the storage class object to dynamically provision an Azure file share. The following YAML can be used to create a persistent volume claim *100 GB* in size with *ReadWriteMany* access. For more information on access modes, see the [Kubernetes persistent volume](#) documentation.

Now create a file named `azure-file-pvc.yaml` and copy in the following YAML. Make sure that the *storageClassName* matches the storage class created in the last step:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: my-azurefile
spec:
 accessModes:
 - ReadWriteMany
 storageClassName: my-azurefile
 resources:
 requests:
 storage: 100Gi
```

### NOTE

If using the *Premium\_LRS* sku for your storage class, the minimum value for *storage* must be *100Gi*.

Create the persistent volume claim with the [kubectl apply](#) command:

```
kubectl apply -f azure-file-pvc.yaml
```

Once completed, the file share will be created. A Kubernetes secret is also created that includes connection information and credentials. You can use the [kubectl get](#) command to view the status of the PVC:

```
$ kubectl get pvc my-azurefile

NAME STATUS VOLUME CAPACITY ACCESS MODES STORAGECLASS
AGE
my-azurefile Bound pvc-8436e62e-a0d9-11e5-8521-5a8664dc0477 10Gi RWX my-azurefile
5m
```

## Use the persistent volume

The following YAML creates a pod that uses the persistent volume claim *my-azurefile* to mount the Azure file share at the */mnt/azure* path. For Windows Server containers, specify a *mountPath* using the Windows path convention, such as '*D:*'.

Create a file named `azure-pvc-files.yaml`, and copy in the following YAML. Make sure that the *claimName* matches the PVC created in the last step.

```
kind: Pod
apiVersion: v1
metadata:
 name: mypod
spec:
 containers:
 - name: mypod
 image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 volumeMounts:
 - mountPath: "/mnt/azure"
 name: volume
 volumes:
 - name: volume
 persistentVolumeClaim:
 claimName: my-azurefile
```

Create the pod with the [kubectl apply](#) command.

```
kubectl apply -f azure-pvc-files.yaml
```

You now have a running pod with your Azure Files share mounted in the */mnt/azure* directory. This configuration can be seen when inspecting your pod via `kubectl describe pod mypod`. The following condensed example output shows the volume mounted in the container:

```
Containers:
 mypod:
 Container ID: docker://053bc9c0df72232d755aa040bfba8b533fa696b123876108dec400e364d2523e
 Image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 Image ID: docker-
 pullable://nginx@sha256:d85914d547a6c92faa39ce7058bd7529baacab7e0cd4255442b04577c4d1f424
 State: Running
 Started: Fri, 01 Mar 2019 23:56:16 +0000
 Ready: True
 Mounts:
 /mnt/azure from volume (rw)
 /var/run/secrets/kubernetes.io/serviceaccount from default-token-8rv4z (ro)
 [...]
Volumes:
 volume:
 Type: PersistentVolumeClaim (a reference to a PersistentVolumeClaim in the same namespace)
 ClaimName: my-azurefile
 ReadOnly: false
 [...]
```

## Mount options

The default value for `fileMode` and `dirMode` is `0777` for Kubernetes version 1.13.0 and above. If dynamically creating the persistent volume with a storage class, mount options can be specified on the storage class object. The following example sets `0777`:

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
 name: my-azurefile
provisioner: file.csi.azure.com # replace with "kubernetes.io/azure-file" if aks version is less than 1.21
allowVolumeExpansion: true
mountOptions:
 - dir_mode=0777
 - file_mode=0777
 - uid=0
 - gid=0
 - mfsymlinks
 - cache=strict
 - actimeo=30
parameters:
 skuName: Premium_LRS
```

## Using Azure tags

For more details on using Azure tags, see [Use Azure tags in Azure Kubernetes Service \(AKS\)](#).

## Next steps

For associated best practices, see [Best practices for storage and backups in AKS](#).

For storage class parameters, see [Dynamic Provision](#).

Learn more about Kubernetes persistent volumes using Azure Files.

[Kubernetes plugin for Azure Files](#)

# Manually create and use a volume with Azure Files share in Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

Container-based applications often need to access and persist data in an external data volume. If multiple pods need concurrent access to the same storage volume, you can use Azure Files to connect using the [Server Message Block \(SMB\) protocol](#). This article shows you how to manually create an Azure Files share and attach it to a pod in AKS.

For more information on Kubernetes volumes, see [Storage options for applications in AKS](#).

## Before you begin

This article assumes that you have an existing AKS cluster with 1.21 or later version. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

If you want to interact with Azure Files on an AKS cluster with 1.20 or previous version, see the [Kubernetes plugin for Azure Files](#).

## Create an Azure file share

Before you can use Azure Files as a Kubernetes volume, you must create an Azure Storage account and the file share. The following commands create a resource group named *myAKSShare*, a storage account, and a Files share named *aksshare*:

```
Change these four parameters as needed for your own environment
$AKS_PERS_STORAGE_ACCOUNT_NAME=mystorageaccount$RANDOM
$AKS_PERS_RESOURCE_GROUP=myAKSShare
$AKS_PERS_LOCATION=eastus
$AKS_PERS_SHARE_NAME=aksshare

Create a resource group
az group create --name $AKS_PERS_RESOURCE_GROUP --location $AKS_PERS_LOCATION

Create a storage account
az storage account create -n $AKS_PERS_STORAGE_ACCOUNT_NAME -g $AKS_PERS_RESOURCE_GROUP -l $AKS_PERS_LOCATION --sku Standard_LRS

Export the connection string as an environment variable, this is used when creating the Azure file share
export AZURE_STORAGE_CONNECTION_STRING=$(az storage account show-connection-string -n $AKS_PERS_STORAGE_ACCOUNT_NAME -g $AKS_PERS_RESOURCE_GROUP -o tsv)

Create the file share
az storage share create -n $AKS_PERS_SHARE_NAME --connection-string $AZURE_STORAGE_CONNECTION_STRING

Get storage account key
$STORAGE_KEY=$(az storage account keys list --resource-group $AKS_PERS_RESOURCE_GROUP --account-name $AKS_PERS_STORAGE_ACCOUNT_NAME --query "[0].value" -o tsv)

Echo storage account name and key
echo Storage account name: $AKS_PERS_STORAGE_ACCOUNT_NAME
echo Storage account key: $STORAGE_KEY
```

Make a note of the storage account name and key shown at the end of the script output. These values are needed when you create the Kubernetes volume in one of the following steps.

## Create a Kubernetes secret

Kubernetes needs credentials to access the file share created in the previous step. These credentials are stored in a [Kubernetes secret](#), which is referenced when you create a Kubernetes pod.

Use the `kubectl create secret` command to create the secret. The following example creates a secret named `azure-secret` and populates the `azurerestorageaccountname` and `azurerestorageaccountkey` from the previous step. To use an existing Azure storage account, provide the account name and key.

```
kubectl create secret generic azure-secret --from-literal=azurerestorageaccountname=$AKS_PERS_STORAGE_ACCOUNT_NAME --from-literal=azurerestorageaccountkey=$STORAGE_KEY
```

## Mount file share as an inline volume

### NOTE

Inline volume can only access secrets in the same namespace as the pod. To specify a different secret namespace, [please use the persistent volume example](#) below instead.

To mount the Azure Files share into your pod, configure the volume in the container spec. Create a new file named `azure-files-pod.yaml` with the following contents. If you changed the name of the Files share or secret name, update the `shareName` and `secretName`. If desired, update the `mountPath`, which is the path where the Files share is mounted in the pod. For Windows Server containers, specify a `mountPath` using the Windows path convention, such as '`D:`'.

```
apiVersion: v1
kind: Pod
metadata:
 name: mypod
spec:
 nodeSelector:
 kubernetes.io/os: linux
 containers:
 - image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 name: mypod
 resources:
 requests:
 cpu: 100m
 memory: 128Mi
 limits:
 cpu: 250m
 memory: 256Mi
 volumeMounts:
 - name: azure
 mountPath: /mnt/azure
 volumes:
 - name: azure
 csi:
 driver: file.csi.azure.com
 readOnly: false
 volumeAttributes:
 secretName: azure-secret # required
 shareName: aksshare # required
 mountOptions: "dir_mode=0777,file_mode=0777,cache=strict,actimeo=30" # optional
```

Use the `kubectl` command to create the pod.

```
kubectl apply -f azure-files-pod.yaml
```

You now have a running pod with an Azure Files share mounted at `/mnt/azure`. You can use `kubectl describe pod mypod` to verify the share is mounted successfully.

## Mount file share as a persistent volume

- Mount options

The default value for `fileMode` and `dirMode` is `0777`.

```
apiVersion: v1
kind: PersistentVolume
metadata:
 name: azurefile
spec:
 capacity:
 storage: 5Gi
 accessModes:
 - ReadWriteMany
 persistentVolumeReclaimPolicy: Retain
 storageClassName: azurefile-csi
 csi:
 driver: file.csi.azure.com
 readOnly: false
 volumeHandle: unique-volumeid # make sure this volumeid is unique in the cluster
 volumeAttributes:
 resourceGroup: EXISTING_RESOURCE_GROUP_NAME # optional, only set this when storage account is not in
the same resource group as agent node
 shareName: aksshare
 nodeStageSecretRef:
 name: azure-secret
 namespace: default
 mountOptions:
 - dir_mode=0777
 - file_mode=0777
 - uid=0
 - gid=0
 - mfsymlinks
 - cache=strict
 - nosharesock
 - nobrl
```

Create a `azurefile-mount-options-pvc.yaml` file with a `PersistentVolumeClaim` that uses the `PersistentVolume`. For example:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: azurefile
spec:
 accessModes:
 - ReadWriteMany
 storageClassName: azurefile-csi
 volumeName: azurefile
 resources:
 requests:
 storage: 5Gi
```

Use the `kubectl` commands to create the `PersistentVolume` and `PersistentVolumeClaim`.

```
kubectl apply -f azurefile-mount-options-pv.yaml
kubectl apply -f azurefile-mount-options-pvc.yaml
```

Verify your *PersistentVolumeClaim* is created and bound to the *PersistentVolume*.

```
$ kubectl get pvc azurefile

NAME STATUS VOLUME CAPACITY ACCESS MODES STORAGECLASS AGE
azurefile Bound azurefile 5Gi RWX azurefile 5s
```

Update your container spec to reference your *PersistentVolumeClaim* and update your pod. For example:

```
...
volumes:
- name: azure
 persistentVolumeClaim:
 claimName: azurefile
```

As the pod spec can't be updated in place, use `kubectl` commands to delete, and then re-create the pod:

```
kubectl delete pod mypod
kubectl apply -f azure-files-pod.yaml
```

## Next steps

For Azure File CSI driver parameters, see [CSI driver parameters](#).

For associated best practices, see [Best practices for storage and backups in AKS](#).

# Integrate Azure HPC Cache with Azure Kubernetes Service

10/27/2022 • 6 minutes to read • [Edit Online](#)

Azure HPC Cache speeds access to your data for high-performance computing (HPC) tasks. By caching files in Azure, Azure HPC Cache brings the scalability of cloud computing to your existing workflow. This article shows you how to integrate Azure HPC Cache with Azure Kubernetes Service (AKS).

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart using the [Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

### IMPORTANT

Your AKS cluster must be [in a region that supports Azure HPC Cache](#).

You also need to install and configure Azure CLI version 2.7 or later. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#). See [hpc-cache-cli-prerequisites](#) for more information about using Azure CLI with HPC Cache.

You will also need to install the hpc-cache Azure CLI extension. Please do the following:

```
az extension add --upgrade -n hpc-cache
```

## Set up Azure HPC Cache

This section explains the steps to create and configure your HPC Cache.

### 1. Find the AKS node resource group

First, get the resource group name with the `az aks show` command and add the `--query nodeResourceGroup` query parameter. You will create your HPC Cache in the same resource group.

The following example gets the node resource group name for the AKS cluster named `myAKSCluster` in the resource group name `myResourceGroup`:

```
az aks show --resource-group myResourceGroup --name myAKSCluster --query nodeResourceGroup -o tsv
```

```
MC_myResourceGroup_myAKSCluster_eastus
```

### 2. Create the cache subnet

There are a number of [prerequisites](#) that must be satisfied before running an HPC Cache. Most importantly, the cache requires a *dedicated* subnet with at least 64 IP addresses available. This subnet must not host other VMs or containers. This subnet must be accessible from the AKS nodes.

Create the dedicated HPC Cache subnet:

```
RESOURCE_GROUP=MC_myResourceGroup_myAKSCluster_eastus
VNET_NAME=$(az network vnet list --resource-group $RESOURCE_GROUP --query [].name -o tsv)
VNET_ID=$(az network vnet show --resource-group $RESOURCE_GROUP --name $VNET_NAME --query "id" -o tsv)
SUBNET_NAME=MyHpcCacheSubnet
az network vnet subnet create \
 --resource-group $RESOURCE_GROUP \
 --vnet-name $VNET_NAME \
 --name $SUBNET_NAME \
 --address-prefixes 10.0.0.0/26
```

Register the *Microsoft.StorageCache* resource provider:

```
az provider register --namespace Microsoft.StorageCache --wait
```

**NOTE**

The resource provider registration can take some time to complete.

### 3. Create the HPC Cache

Create an HPC Cache in the node resource group from step 1 and in the same region as your AKS cluster. Use [az hpc-cache create](#).

**NOTE**

The HPC Cache takes approximately 20 minutes to be created.

```
RESOURCE_GROUP=MC_myResourceGroup_myAKSCluster_eastus
VNET_NAME=$(az network vnet list --resource-group $RESOURCE_GROUP --query [].name -o tsv)
VNET_ID=$(az network vnet show --resource-group $RESOURCE_GROUP --name $VNET_NAME --query "id" -o tsv)
SUBNET_NAME=MyHpcCacheSubnet
SUBNET_ID=$(az network vnet subnet show --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --name $SUBNET_NAME --query "id" -o tsv)
az hpc-cache create \
 --resource-group $RESOURCE_GROUP \
 --cache-size-gb "3072" \
 --location eastus \
 --subnet $SUBNET_ID \
 --sku-name "Standard_2G" \
 --name MyHpcCache
```

### 4. Create a storage account and new container

Create the Azure Storage account for the Blob storage container. The HPC Cache will cache content that is stored in this Blob storage container.

**IMPORTANT**

You need to select a unique storage account name. Replace 'uniquestorageaccount' with something that will be unique for you.

Check that the storage account name that you have selected is available.

```
STORAGE_ACCOUNT_NAME=uniquestorageaccount
az storage account check-name --name $STORAGE_ACCOUNT_NAME
```

```
RESOURCE_GROUP=MC_myResourceGroup_myAKSCluster_eastus
STORAGE_ACCOUNT_NAME=uniquestorageaccount
az storage account create \
-n $STORAGE_ACCOUNT_NAME \
-g $RESOURCE_GROUP \
-l eastus \
--sku Standard_LRS
```

Create the Blob container within the storage account.

```
STORAGE_ACCOUNT_NAME=uniquestorageaccount
STORAGE_ACCOUNT_ID=$(az storage account show --name $STORAGE_ACCOUNT_NAME --query "id" -o tsv)
AD_USER=$(az ad signed-in-user show --query objectId -o tsv)
CONTAINER_NAME=mystoragecontainer
az role assignment create --role "Storage Blob Data Contributor" --assignee $AD_USER --scope
$STORAGE_ACCOUNT_ID
az storage container create --name $CONTAINER_NAME --account-name $STORAGE_ACCOUNT_NAME --auth-mode login
```

Provide permissions to the Azure HPC Cache service account to access your storage account and Blob container.

```
HPC_CACHE_USER="StorageCache Resource Provider"
STORAGE_ACCOUNT_NAME=uniquestorageaccount
STORAGE_ACCOUNT_ID=$(az storage account show --name $STORAGE_ACCOUNT_NAME --query "id" -o tsv)
$HPC_CACHE_ID=$(az ad sp list --display-name "${HPC_CACHE_USER}" --query "[].objectId" -o tsv)
az role assignment create --role "Storage Account Contributor" --assignee $HPC_CACHE_ID --scope
$STORAGE_ACCOUNT_ID
az role assignment create --role "Storage Blob Data Contributor" --assignee $HPC_CACHE_ID --scope
$STORAGE_ACCOUNT_ID
```

## 5. Configure the storage target

Add the blob container to your HPC Cache as a storage target.

```
RESOURCE_GROUP=MC_myResourceGroup_myAKSCluster_eastus
STORAGE_ACCOUNT_NAME=uniquestorageaccount
STORAGE_ACCOUNT_ID=$(az storage account show --name $STORAGE_ACCOUNT_NAME --query "id" -o tsv)
CONTAINER_NAME=mystoragecontainer
az hpc-cache blob-storage-target add \
--resource-group $RESOURCE_GROUP \
--cache-name MyHpcCache \
--name MyStorageTarget \
--storage-account $STORAGE_ACCOUNT_ID \
--container-name $CONTAINER_NAME \
--virtual-namespace-path "/myfilepath"
```

## 6. Set up client load balancing

Create a Azure Private DNS Zone for the client-facing IP addresses.

```

RESOURCE_GROUP=MC_myResourceGroup_myAKSCluster_eastus
VNET_NAME=$(az network vnet list --resource-group $RESOURCE_GROUP --query [].name -o tsv)
VNET_ID=$(az network vnet show --resource-group $RESOURCE_GROUP --name $VNET_NAME --query "id" -o tsv)
PRIVATE_DNS_ZONE="myhpccache.local"
az network private-dns zone create \
 -g $RESOURCE_GROUP \
 -n $PRIVATE_DNS_ZONE
az network private-dns link vnet create \
 -g $RESOURCE_GROUP \
 -n MyDNSLink \
 -z $PRIVATE_DNS_ZONE \
 -v $VNET_NAME \
 -e true

```

Create the round-robin DNS name.

```

DNS_NAME="server"
PRIVATE_DNS_ZONE="myhpccache.local"
RESOURCE_GROUP=MC_myResourceGroup_myAKSCluster_eastus
HPC_MOUNTS0=$(az hpc-cache show --name "MyHpcCache" --resource-group $RESOURCE_GROUP --query
"mountAddresses[0]" -o tsv | tr --delete '\r')
HPC_MOUNTS1=$(az hpc-cache show --name "MyHpcCache" --resource-group $RESOURCE_GROUP --query
"mountAddresses[1]" -o tsv | tr --delete '\r')
HPC_MOUNTS2=$(az hpc-cache show --name "MyHpcCache" --resource-group $RESOURCE_GROUP --query
"mountAddresses[2]" -o tsv | tr --delete '\r')
az network private-dns record-set a add-record -g $RESOURCE_GROUP -z $PRIVATE_DNS_ZONE -n $DNS_NAME -a
$HPC_MOUNTS0
az network private-dns record-set a add-record -g $RESOURCE_GROUP -z $PRIVATE_DNS_ZONE -n $DNS_NAME -a
$HPC_MOUNTS1
az network private-dns record-set a add-record -g $RESOURCE_GROUP -z $PRIVATE_DNS_ZONE -n $DNS_NAME -a
$HPC_MOUNTS2

```

## Create the AKS persistent volume

Create a `pv-nfs.yaml` file to define a [persistent volume](#).

```

apiVersion: v1
kind: PersistentVolume
metadata:
 name: pv-nfs
spec:
 capacity:
 storage: 10000Gi
 accessModes:
 - ReadWriteMany
 mountOptions:
 - vers=3
 nfs:
 server: server.myhpccache.local
 path: /

```

First, ensure that you have credentials for your Kubernetes cluster.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

Update the *server* and *path* to the values of your NFS (Network File System) volume you created in the previous step. Create the persistent volume with the [kubectl apply](#) command:

```
kubectl apply -f pv-nfs.yaml
```

Verify that status of the persistent volume is **Available** using the [kubectl describe](#) command:

```
kubectl describe pv pv-nfs
```

## Create the persistent volume claim

Create a [pvc-nfs.yaml](#) defining a [persistent volume claim](#). For example:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: pvc-nfs
spec:
 accessModes:
 - ReadWriteMany
 storageClassName: ""
 resources:
 requests:
 storage: 100Gi
```

Use the [kubectl apply](#) command to create the persistent volume claim:

```
kubectl apply -f pvc-nfs.yaml
```

Verify that the status of the persistent volume claim is **Bound** using the [kubectl describe](#) command:

```
kubectl describe pvc pvc-nfs
```

## Mount the HPC Cache with a pod

Create a [nginx-nfs.yaml](#) file to define a pod that uses the persistent volume claim. For example:

```
kind: Pod
apiVersion: v1
metadata:
 name: nginx-nfs
spec:
 containers:
 - image: mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine
 name: nginx-nfs
 command:
 - "/bin/sh"
 - "-c"
 - "while true; do echo $(date) >> /mnt/azure/myfilepath/outfile; sleep 1; done"
 volumeMounts:
 - name: disk01
 mountPath: /mnt/azure
 volumes:
 - name: disk01
 persistentVolumeClaim:
 claimName: pvc-nfs
```

Create the pod with the [kubectl apply](#) command:

```
kubectl apply -f nginx-nfs.yaml
```

Verify that the pod is running by using the [kubectl describe](#) command:

```
kubectl describe pod nginx-nfs
```

Verify your volume has been mounted in the pod by using [kubectl exec](#) to connect to the pod then `df -h` to check if the volume is mounted.

```
kubectl exec -it nginx-nfs -- sh
```

```
/ # df -h
Filesystem Size Used Avail Use% Mounted on
...
server.myhpccache.local:/myfilepath 8.0E 0 8.0E 0% /mnt/azure/myfilepath
...
```

## Frequently asked questions (FAQ)

### **Running applications as non-root**

If you need to run an application as a non-root user, you may need to disable root squashing to chown a directory to another user. The non-root user will need to own a directory to access the file system. For the user to own a directory, the root user must chown a directory to that user, but if the HPC Cache is squashing root, this operation will be denied because the root user (UID 0) is being mapped to the anonymous user. More information about root squashing and client access policies is found [here](#).

### **Sending feedback**

We'd love to hear from you! Please send any feedback or questions to [aks-hpccache-feed@microsoft.com](mailto:aks-hpccache-feed@microsoft.com).

## Next steps

- For more information on Azure HPC Cache, see [HPC Cache Overview](#).
- For more information on using NFS with AKS, see [Manually create and use an NFS \(Network File System\) Linux Server volume with Azure Kubernetes Service \(AKS\)](#).

# Manually create and use a Linux NFS (Network File System) Server with Azure Kubernetes Service (AKS)

10/27/2022 • 4 minutes to read • [Edit Online](#)

Sharing data between containers is often a necessary component of container-based services and applications. You usually have various pods that need access to the same information on an external persistent volume. While Azure Files is an option, creating an NFS Server on an Azure VM is another form of persistent shared storage.

This article will show you how to create an NFS Server on an Azure Ubuntu virtual machine, and set up your AKS cluster with access to this shared file system as a persistent volume.

## Before you begin

This article assumes that you have the following components and configuration to support this configuration:

- An existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).
- Your AKS cluster needs to be on the same or peered Azure virtual network (VNet) as the NFS Server. The cluster must be created on an existing VNet, which can be the same VNet as your NFS Server VM. The steps for configuring with an existing VNet are described in the following articles: [creating AKS Cluster in existing VNET](#) and [connecting virtual networks with VNET peering](#).
- An Azure Ubuntu [Linux virtual machine](#) running version 18.04 or later. To deploy a Linux VM on Azure, see [Create and manage Linux VMs](#).

If you deploy your AKS cluster first, Azure automatically populates the virtual network settings when deploying your Azure Ubuntu VM, associating the Ubuntu VM on the same VNet. But if you want to work with peered networks instead, consult the documentation above.

## Deploying the NFS Server onto a virtual machine

1. To deploy an NFS Server on the Azure Ubuntu virtual machine, copy the following Bash script and save it to your local machine. Replace the value for the variable **AKS\_SUBNET** with the correct one from your AKS cluster or else the default value specified opens your NFS Server to all ports and connections. In this article, the file is named `nfs-server-setup.sh`.

```

#!/bin/bash

This script should be executed on Linux Ubuntu Virtual Machine

EXPORT_DIRECTORY=${1:-/export/data}
DATA_DIRECTORY=${2:-/data}
AKS_SUBNET=${3:-*}

echo "Updating packages"
apt-get -y update

echo "Installing NFS kernel server"

apt-get -y install nfs-kernel-server

echo "Making data directory ${DATA_DIRECTORY}"
mkdir -p ${DATA_DIRECTORY}

echo "Making new directory to be exported and linked to data directory: ${EXPORT_DIRECTORY}"
mkdir -p ${EXPORT_DIRECTORY}

echo "Mount binding ${DATA_DIRECTORY} to ${EXPORT_DIRECTORY}"
mount --bind ${DATA_DIRECTORY} ${EXPORT_DIRECTORY}

echo "Giving 777 permissions to ${EXPORT_DIRECTORY} directory"
chmod 777 ${EXPORT_DIRECTORY}

parentdir=$(dirname "${EXPORT_DIRECTORY}")
echo "Giving 777 permissions to parent: ${parentdir} directory"
chmod 777 $parentdir

echo "Appending bound directories into fstab"
echo "${DATA_DIRECTORY} ${EXPORT_DIRECTORY} none bind 0 0" >> /etc/fstab

echo "Appending localhost and Kubernetes subnet address ${AKS_SUBNET} to exports configuration file"
echo "/export ${AKS_SUBNET}(rw,async,insecure,fsid=0,crossmnt,no_subtree_check)" >>
/etc/exports
echo "/export localhost(rw,async,insecure,fsid=0,crossmnt,no_subtree_check)" >> /etc/exports

nohup service nfs-kernel-server restart

```

The script initiates a restart of the NFS Server, and afterwards you can proceed with connecting to the NFS Server from your AKS cluster.

- After creating your Linux VM, copy the file created in the previous step from your local machine to the VM using the following command:

```
scp /path/to/nfs-server-setup.sh username@vm-ip-address:/home/{username}
```

- After the file is copied over, open a secure shell (SSH) connection to the VM and execute the following command:

```
sudo ./nfs-server-setup.sh
```

If execution fails because of a permission denied error, set execution permission for all by running the following command:

```
chmod +x ~/nfs-server-setup.sh
```

# Connecting AKS cluster to NFS Server

You can connect the NFS Server to your AKS cluster by provisioning a persistent volume and persistent volume claim that specifies how to access the volume. Connecting the two resources in the same or peered virtual networks is necessary. To learn how to set up the cluster in the same VNet, see: [Creating AKS Cluster in existing VNet](#).

Once both resources are on the same virtual or peered VNet, next provision a persistent volume and a persistent volume claim in your AKS Cluster. The containers can then mount the NFS drive to their local directory.

1. Create a `pv-azurefilesnfs.yaml` file with a *PersistentVolume*. For example:

```
apiVersion: v1
kind: PersistentVolume
metadata:
 name: NFS_NAME
 labels:
 type: nfs
spec:
 capacity:
 storage: 1Gi
 accessModes:
 - ReadWriteMany
 nfs:
 server: NFS_INTERNAL_IP
 path: NFS_EXPORT_FILE_PATH
```

Replace the values for `NFS_INTERNAL_IP`, `NFS_NAME` and `NFS_EXPORT_FILE_PATH` with the actual settings from your NFS Server.

2. Create a `pvc-azurefilesnfs.yaml` file with a *PersistentVolumeClaim* that uses the *PersistentVolume*. For example:

#### IMPORTANT

`storageClassName` value needs to remain an empty string or the claim won't work.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
 name: NFS_NAME
spec:
 accessModes:
 - ReadWriteMany
 storageClassName: ""
 resources:
 requests:
 storage: 1Gi
 selector:
 matchLabels:
 type: nfs
```

Replace the value for `NFS_NAME` with the actual setting from your NFS Server.

## Troubleshooting

If you can't connect to the server from your AKS cluster, the issue might be the exported directory or its parent,

doesn't have sufficient permissions to access the NFS Server VM.

Check that both your export directory and its parent directory have 777 permissions.

You can check permissions by running the following command and the directories should have '*drwxrwxrwx*' permissions:

```
ls -l
```

## Next steps

- For associated best practices, see [Best practices for storage and backups in AKS](#).
- To learn more on setting up your NFS Server or to help debug issues, see the following tutorial from the Ubuntu community [NFS Tutorial](#)

# Monitoring Azure Kubernetes Service (AKS) with Azure Monitor

10/27/2022 • 15 minutes to read • [Edit Online](#)

This scenario describes how to use Azure Monitor to monitor the health and performance of Azure Kubernetes Service (AKS). It includes collection of telemetry critical for monitoring, analysis and visualization of collected data to identify trends, and how to configure alerting to be proactively notified of critical issues.

The [Cloud Monitoring Guide](#) defines the [primary monitoring objectives](#) you should focus on for your Azure resources. This scenario focuses on Health and Status monitoring using Azure Monitor.

## Scope of the scenario

This scenario is intended for customers using Azure Monitor to monitor AKS. It does not include the following, although this content may be added in subsequent updates to the scenario.

- Monitoring of Kubernetes clusters outside of Azure except for referring to existing content for Azure Arc-enabled Kubernetes.
- Monitoring of AKS with tools other than Azure Monitor except to fill gaps in Azure Monitor and Container Insights.

### NOTE

Azure Monitor was designed to monitor the availability and performance of cloud resources. While the operational data stored in Azure Monitor may be useful for investigating security incidents, other services in Azure were designed to monitor security. Security monitoring for AKS is done with [Microsoft Sentinel](#) and [Microsoft Defender for Cloud](#). See [Monitor virtual machines with Azure Monitor - Security monitoring](#) for a description of the security monitoring tools in Azure and their relationship to Azure Monitor.

For information on using the security services to monitor AKS, see [Microsoft Defender for Kubernetes - the benefits and features](#) and [Connect Azure Kubernetes Service \(AKS\) diagnostics logs to Microsoft Sentinel](#).

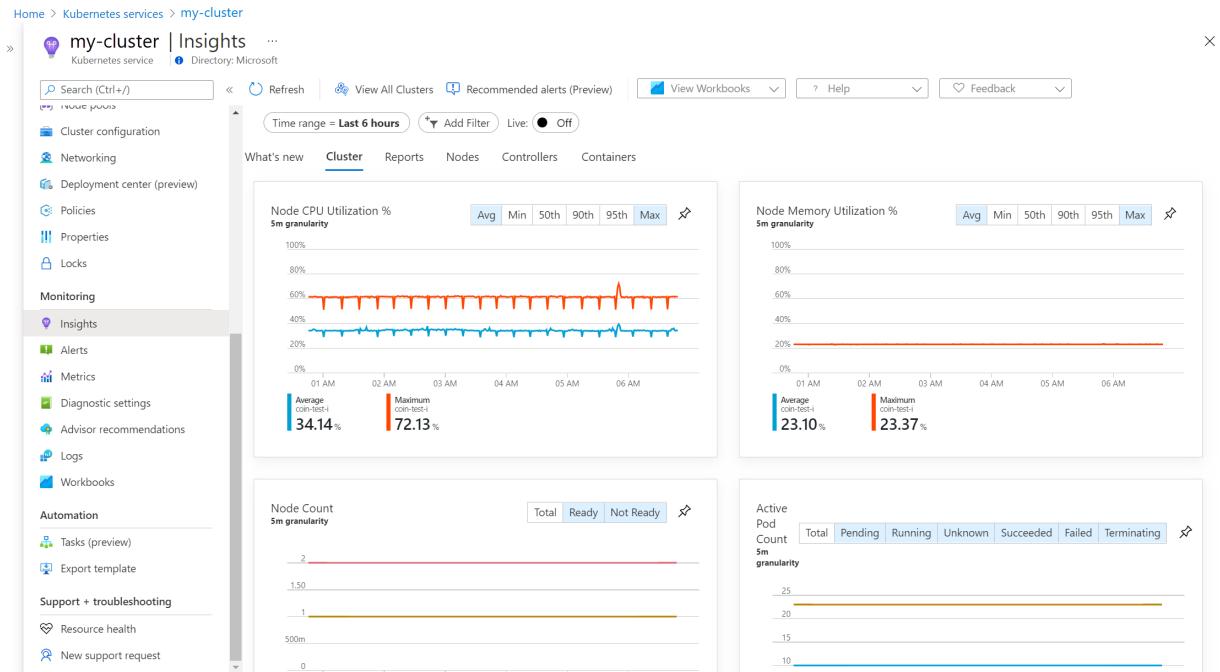
## Container insights

AKS generates [platform metrics and resource logs](#), like any other Azure resource, that you can use to monitor its basic health and performance. Enable [Container insights](#) to expand on this monitoring. Container insights is a feature in Azure Monitor that monitors the health and performance of managed Kubernetes clusters hosted on AKS in addition to other cluster configurations. Container insights provides interactive views and workbooks that analyze collected data for a variety of monitoring scenarios.

[Prometheus](#) and [Grafana](#) are CNCF backed widely popular open source tools for kubernetes monitoring. AKS exposes many metrics in Prometheus format which makes Prometheus a popular choice for monitoring.

[Container insights](#) has native integration with AKS, collecting critical metrics and logs, alerting on identified issues, and providing visualization with workbooks. It also collects certain Prometheus metrics, and many native Azure Monitor Insights are built-up on top of Prometheus metrics. Container insights complements and completes E2E monitoring of AKS including log collection which Prometheus as stand-alone tool doesn't provide. Many customers use Prometheus integration and Azure Monitor together for E2E monitoring.

Learn more about using Container insights at [Container insights overview](#). [Monitor layers of AKS with Container insights](#) below introduces various features of Container insights and the monitoring scenarios that they support.



## Configure monitoring

The following sections describe the steps required to configure full monitoring of your AKS cluster using Azure Monitor.

### Create Log Analytics workspace

You require at least one Log Analytics workspace to support Container insights and to collect and analyze other telemetry about your AKS cluster. There is no cost for the workspace, but you do incur ingestion and retention costs when you collect data. See [Azure Monitor Logs pricing details](#) for details.

If you're just getting started with Azure Monitor, then start with a single workspace and consider creating additional workspaces as your requirements evolve. Many environments will use a single workspace for all the Azure resources they monitor. You can even share a workspace used by [Microsoft Defender for Cloud](#) and [Microsoft Sentinel](#), although many customers choose to segregate their availability and performance telemetry from security data.

See [Designing your Azure Monitor Logs deployment](#) for details on logic that you should consider for designing a workspace configuration.

### Enable container insights

When you enable Container insights for your AKS cluster, it deploys a containerized version of the [Log Analytics agent](#) that sends data to Azure Monitor. There are multiple methods to enable it depending whether you're working with a new or existing AKS cluster. See [Enable Container insights](#) for prerequisites and configuration options.

### Configure collection from Prometheus

Container insights allows you to send Prometheus metrics to [Azure Monitor managed service for Prometheus](#) or to your Log Analytics workspace without requiring a local Prometheus server. You can analyze this data using Azure Monitor features along with other data collected by Container insights. See [Collect Prometheus metrics with Container insights](#) for details on this configuration.

### Collect resource logs

The logs for AKS control plane components are implemented in Azure as [resource logs](#). Container insights doesn't currently use these logs, so you do need to create your own log queries to view and analyze them. See [How to query logs from Container insights](#) for details on the structure of these logs and how to write queries for them.

You need to create a diagnostic setting to collect resource logs. Create multiple diagnostic settings to send different sets of logs to different locations. See [Create diagnostic settings to send platform logs and metrics to different destinations](#) to create diagnostic settings for your AKS cluster.

There is a cost for sending resource logs to a workspace, so you should only collect those log categories that you intend to use. Send logs to an Azure storage account to reduce costs if you need to retain the information but don't require it to be readily available for analysis. See [Resource logs](#) for a description of the categories that are available for AKS and See [Azure Monitor Logs pricing details](#) for details on the cost of ingesting and retaining log data. Start by collecting a minimal number of categories and then modify the diagnostic setting to collect additional categories as your needs increase and as you understand your associated costs.

If you're unsure about which resource logs to initially enable, use the recommendations in the following table which are based on the most common customer requirements. Enable the other categories if you later find that you require this information.

CATEGORY	ENABLE?	DESTINATION
cluster-autoscaler	Enable if autoscale is enabled	Log Analytics workspace
guard	Enable if Azure Active Directory is enabled	Log Analytics workspace
kube-apiserver	Enable	Log Analytics workspace
kube-audit	Enable	Azure storage. This keeps costs to a minimum yet retains the audit logs if they're required by an auditor.
kube-audit-admin	Enable	Log Analytics workspace
kube-controller-manager	Enable	Log Analytics workspace
kube-scheduler	Disable	
AllMetrics	Enable	Log Analytics workspace

## Access Azure Monitor features

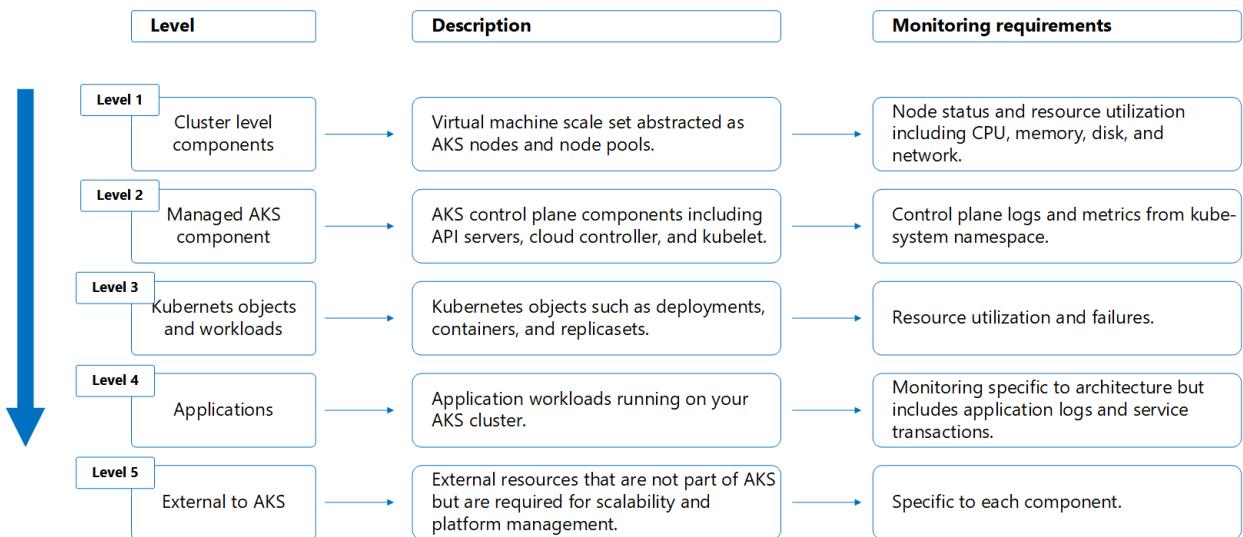
Access Azure Monitor features for all AKS clusters in your subscription from the **Monitoring** menu in the Azure portal or for a single AKS cluster from the **Monitor** section of the **Kubernetes services** menu. The screenshot below shows the cluster's **Monitor** menu.

Name	Status	95th %	95th	Containers	Restarts	UpTime	Node	Trend 95th % (1 bar = 15m)
cpu-stre...	1 ⚠️ 1 ✅	26%	980 mc	2	0	355 days	-	<div style="width: 26%;">███████████</div>
cpu...	Ok	52%	980 mc	1	0	355 days	aks-agentpool...	<div style="width: 52%;">███████████</div>
cpu...	⚠️ Warn	-	-	1	0	356 days	aks-agentpool...	<div style="width: 0%;">██████████</div>
tunnelef...	1 ✅	5%	97 mc	1	0	3 days	-	<div style="width: 5%;">██████████</div>
omsage...	1 ✅	5%	10 mc	1	0	1 day	-	<div style="width: 5%;">██████████</div>
omsage...	1 ✅	2%	20 mc	1	0	3 days	-	<div style="width: 2%;">██████████</div>
omsgage...	1 ⚠️ 1 ✅	2%	9 mc	2	0	144 days	-	<div style="width: 2%;">██████████</div>
kuberne...	1 ✅	2%	2 mc	1	7	52 days	-	<div style="width: 2%;">██████████</div>
dashboa...	1 ✅	0.3%	0.3 mc	1	0	244 days	-	<div style="width: 0.3%;">██████████</div>
coredns...	2 ✅	0.2%	6 mc	2	0	66 days	-	<div style="width: 0.2%;">██████████</div>

MENU OPTION	DESCRIPTION
Insights	Opens container insights for the current cluster. Select <b>Containers</b> from the <b>Monitor</b> menu to open container insights for all clusters.
Alerts	Views alerts for the current cluster.
Metrics	Open metrics explorer with the scope set to the current cluster.
Diagnostic settings	Create diagnostic settings for the cluster to collect resource logs.
Advisor	Recommendations for the current cluster from Azure Advisor.
Logs	Open Log Analytics with the scope set to the current cluster to analyze log data and access prebuilt queries.
Workbooks	Open workbook gallery for Kubernetes service.

## Monitor layers of AKS with Container insights

Because of the wide variance in Kubernetes implementations, each customer will have unique requirements for AKS monitoring. The approach you take should be based on factors including scale, topology, organizational roles, and multi-cluster tenancy. This section presents a common strategy that is a bottoms-up approach starting from infrastructure up through applications. Each layer has distinct monitoring requirements. These layers are illustrated in the following diagram and discussed in more detail in the following sections.

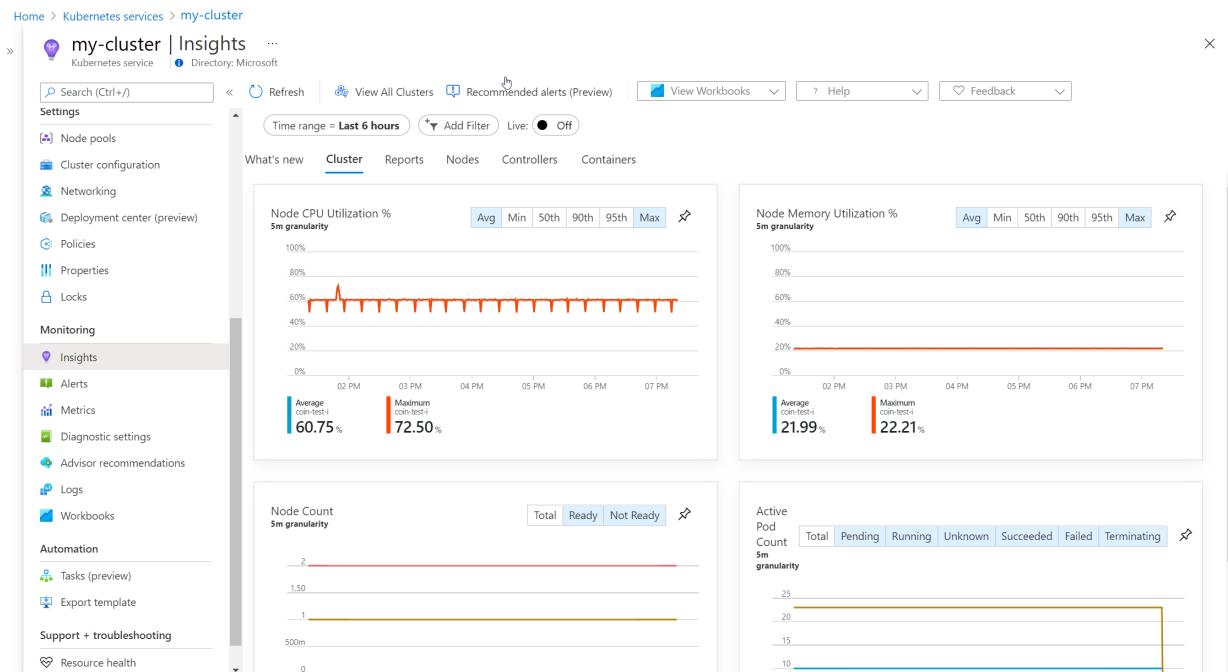


## Level 1 - Cluster level components

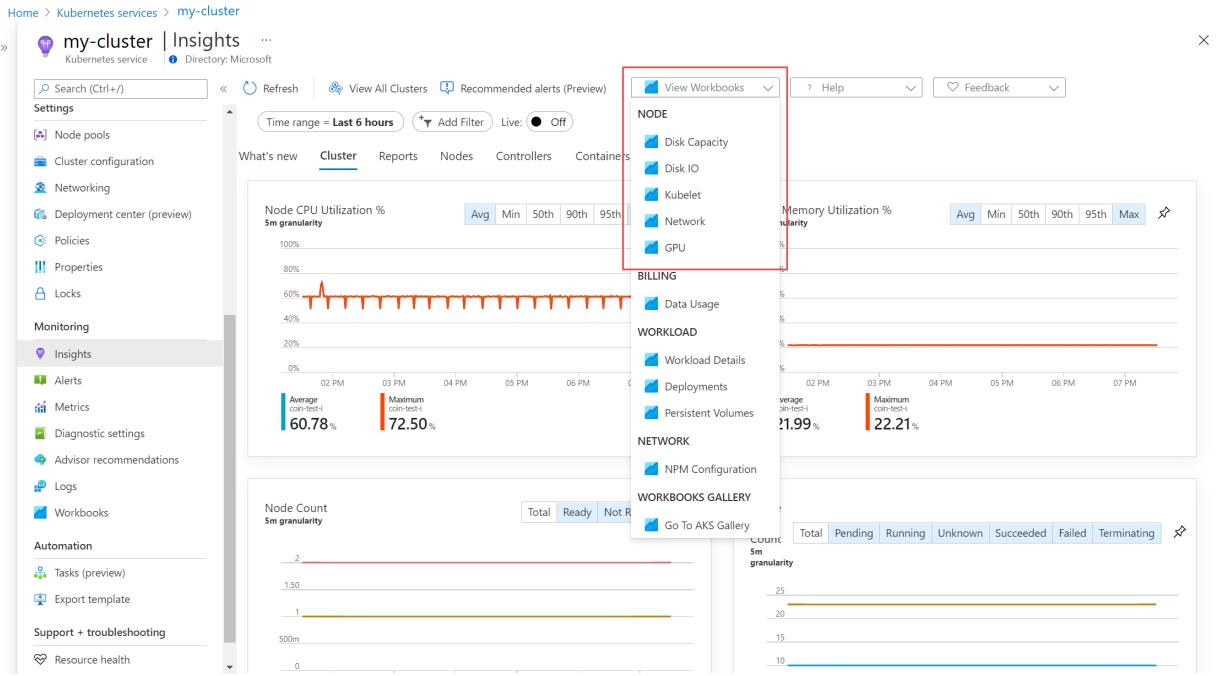
Cluster level includes the following components.

COMPONENT	MONITORING REQUIREMENTS
Node	Understand the readiness status and performance of CPU, memory, and disk for each node and proactively monitor their usage trends before deploying any workloads.

Use existing views and reports in Container Insights to monitor cluster level components. The **Cluster** view gives you a quick view of the performance of the nodes in your cluster including their CPU and memory utilization. Use the **Nodes** view to view the health of each node in addition to the health and performance of the pods running on each. See [Monitor your Kubernetes cluster performance with Container insights](#) for details on using this view and analyzing node health and performance.



Use **Node** workbooks in Container Insights to analyze disk capacity and IO in addition to GPU usage. See [Node workbooks](#) for a description of these workbooks.



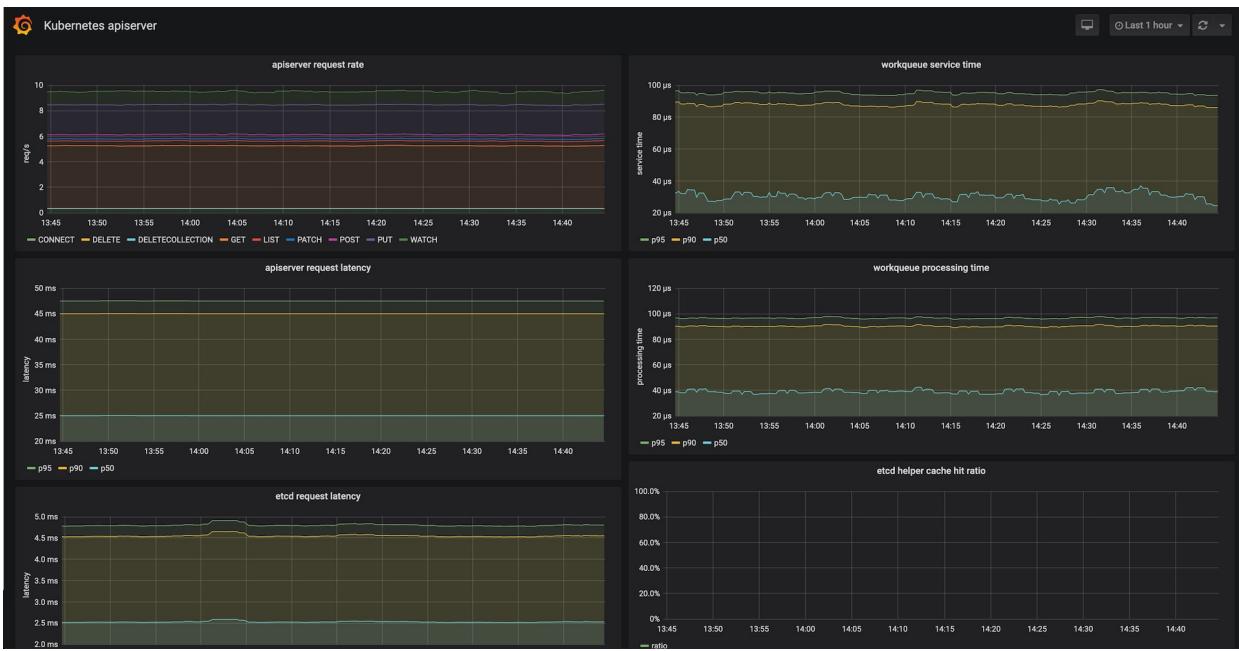
For troubleshooting scenarios, you may need to access the AKS nodes directly for maintenance or immediate log collection. For security purposes, the AKS nodes aren't exposed to the internet but you can `kubectl debug` to SSH to the AKS nodes. See [Connect with SSH to Azure Kubernetes Service \(AKS\) cluster nodes for maintenance or troubleshooting](#) for details on this process.

## Level 2 - Managed AKS components

Managed AKS level includes the following components.

COMPONENT	MONITORING
API Server	Monitor the status of API server, identifying any increase in request load and bottlenecks if the service is down.
Kubelet	Monitoring Kubelet helps in troubleshooting of pod management issues, pods not starting, nodes not ready or pods getting killed.

Azure Monitor and container insights don't yet provide full monitoring for the API server. You can use metrics explorer to view the **Inflight Requests** counter, but you should refer to metrics in Prometheus for a complete view of API Server performance. This includes such values as request latency and workqueue processing time. A Grafana dashboard that provides views of the critical metrics for the API server is available at [Grafana Labs](#). Use this dashboard on your existing Grafana server or setup a new Grafana server in Azure using [Monitor your Azure services in Grafana](#)



Use the Kubelet workbook to view the health and performance of each kubelet. See [Resource Monitoring workbooks](#) for details on this workbook. For troubleshooting scenarios, you can access kubelet logs using the process described at [Get kubelet logs from Azure Kubernetes Service \(AKS\) cluster nodes](#).

## Resource logs

Use [log queries with resource logs](#) to analyze control plane logs generated by AKS components.

## Level 3 - Kubernetes objects and workloads

Kubernetes objects and workloads level include the following components.

COMPONENT	MONITORING REQUIREMENTS
Deployments	Monitor actual vs desired state of the deployment and the status and resource utilization of the pods running on them.
Pods	Monitor status and resource utilization, including CPU and memory, of the pods running on your AKS cluster.

COMPONENT	MONITORING REQUIREMENTS
Containers	Monitor the resource utilization, including CPU and memory, of the containers running on your AKS cluster.

Use existing views and reports in Container Insights to monitor containers and pods. Use the **Nodes** and **Controllers** views to view the health and performance of the pods running on them and drill down to the health and performance of their containers. View the health and performance for containers directly from the **Containers** view. See [Monitor your Kubernetes cluster performance with Container insights](#) for details on using this view and analyzing container health and performance.

Name	Status	95th %	Pod	Node	Restarts	UpTime	Trend 95th % (1 bar = 15m)
cpu-stress	Ok	52%	982 mc	cpu-stress-558...	aks-agentpool-...	0	353 days
tunnel-front	Ok	5%	95 mc	tunnelfront-78...	aks-agentpool-...	0	1 day
omsagent-...	Ok	4%	8 mc	omsagent-win-...	aksakswin00000	0	1 day
omsagent	Ok	2%	18 mc	omsagent-rs-5...	aks-agentpool-...	0	1 day
omsagent	Ok	2%	9 mc	omsagent-55tg...	aks-agentpool-...	0	142 days
kubernetes-...	Ok	1%	1 mc	kubernetes-das...	aks-agentpool-...	0	50 days
dashboard-...	Ok	0.4%	0.4 mc	dashboard-met...	aks-agentpool-...	0	242 days
mongo	Ok	0.2%	5 mc	mongo	aks-agentpool-...	0	143 days
kube-proxy	Ok	0.2%	3 mc	kube-proxy-bkj...	aks-agentpool-...	0	355 days
coredns	Ok	0.2%	3 mc	coredns-5f77fc...	aks-agentpool-...	0	64 days

Use the **Deployment** workbook in Container insights to view metrics collected for deployments. See [Deployment & HPA metrics with Container insights](#) for details.

#### NOTE

Deployments view in Container insights is currently in public preview.

**Deployments** ⚡ ...

coin-test-i

Workbooks Edit 🖥️ 🗑️ 🛡️ 🤖 ? Help Auto refresh: Off

Time Range Namespace Deployment HPA

Last 6 hours All All All

Deployment HPA

Deployment Status

Warning Healthy

2 10

...

Deployment	↑↓	Namespace	↑↓	Age↑↓	Ready	↑↓	ReadyTrend	Up-to-date	↑↓	Up-to-dateTrend	Available	↑↓	AvailableTrend
tunnelfront		kube-system		355.7 days	✓ 100%			✓ 100%			✓ 100%		
sixty-second-log-app		windows-log		354.9 days	✓ 100%			✓ 100%			✓ 100%		
omsagent-rs		kube-system		142.6 days	✓ 100%			✓ 100%			✓ 100%		
metrics-server		kube-system		355.7 days	✓ 100%			✓ 100%			✓ 100%		
kubernetes-dashboard		kube-system		355.7 days	✓ 100%			✓ 100%			✓ 100%		
hello-world-logger-app		default		354.8 days	✓ 100%			✓ 100%			✓ 100%		
dashboard-metrics-scraper		kube-system		355.7 days	✓ 100%			✓ 100%			✓ 100%		
cpu-stress		default		354.8 days	✓ 100%			✓ 100%			✓ 100%		

## Live data

In troubleshooting scenarios, Container insights provides access to live AKS container logs (stdout/stderror), events, and pod metrics. See [How to view Kubernetes logs, events, and pod metrics in real-time](#) for details on using this feature.

Home > my-cluster

my-cluster | Insights ...

Kubernetes service Directory: Microsoft

Refresh View All Clusters Recommended alerts (Preview) View Workbooks ? Help

Time range = Last 6 hours Add Filter

What's new Cluster Reports Nodes Controllers Containers

Search by name... Metric: CPU Usage (millicores) (computed from Capacity) Min Avg 50th 90th 95th Max

**kube-proxy | Live Logs**

Container View in Log Analytics

Overview Live Logs Live Events

Search...

II Pause 🔍 Scroll

42 secs ago 10/27/2018:44:403324 1 proxier.go:708] Syncing iptables rules  
 42 secs ago 10/27/2018:44:45132 1 proxier.go:793] Not using "-random-fully" in the MASQUERADE rule for iptables because the local version of iptables does not support it  
 42 secs ago 10/27/2018:44:451095 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/metrics-server"  
 42 secs ago 10/27/2018:44:451118 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/healthmodel-replicaset-service"  
 42 secs ago 10/27/2018:44:451124 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/kube-dns"  
 42 secs ago 10/27/2018:44:451129 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/dashboard-metrics-scraper"  
 42 secs ago 10/27/2018:44:451134 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/kubernetes-dashboard"  
 42 secs ago 10/27/2018:44:451146 1 bounded\_frequency\_runner.go:221] sync-runner: ran, next possible in 0s, periodic in 30s  
 42 secs ago 10/27/2019:14:451394 1 proxier.go:708] Syncing iptables rules  
 42 secs ago 10/27/2019:14:451130 1 proxier.go:793] Not using "-random-fully" in the MASQUERADE rule for iptables because the local version of iptables does not support it  
 42 secs ago 10/27/2019:14:451130 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/metrics-server"  
 42 secs ago 10/27/2019:14:451134 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/healthmodel-replicaset-service"  
 42 secs ago 10/27/2019:14:500901 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/kube-dns"  
 42 secs ago 10/27/2019:14:500905 1 healthcheck.go:235] Not saving endpoints for unknown healthcheck "kube-system/dashboard-metrics-scraper"  
 42 secs ago 10/27/2019:14:500918 1 bounded\_frequency\_runner.go:221] sync-runner: ran, next possible in 0s, periodic in 30s

Name	Status	95th % ↓	95th	Containers	UpTime
aks-agentpool-93403730-vmss000000	✓ Ok	62%	1244 mc	25	369 days
Other Processes	-	0%	121 mc	-	-
cpu-stress-558997d548-nzcvw	✓ Ok	52%	980 mc	1	367 days
tunnelfront-67866cd94f-8l2qf	✓ Ok	5%	99 mc	1	11 hours
omsagent-5s5tg	✓ Ok	2%	9 mc	1	156 days
omsagent-rs-c56964c89-82r59	✓ Ok	1%	13 mc	1	11 hours
kubernetes-dashboard-64ccc85575-hz...	✓ Ok	1%	1 mc	1	64 days
dashboard-metrics-scraper-6587ff9d84...	✓ Ok	0.4%	0.4 mc	1	256 days
mongo	✓ Ok	0.3%	5 mc	1	157 days
kube-proxy-bkjqmq	✓ Ok	0.2%	4 mc	1	369 days
kube-proxy	✓ Ok	0.2%	4 mc	1	369 days
coredns-5f77fc5965-f55f	✓ Ok	0.2%	3 mc	1	78 days

## Level 4- Applications

The application level includes the application workloads running in the AKS cluster.

COMPONENT	MONITORING REQUIREMENTS
Applications	Monitor microservice application deployments to identify application failures and latency issues. Includes such information as request rates, response times, and exceptions.

Application Insights provides complete monitoring of applications running on AKS and other environments. If you have a Java application, you can provide monitoring without instrumenting your code following [Zero instrumentation application monitoring for Kubernetes - Azure Monitor Application Insights](#). For complete monitoring though, you should configure code-based monitoring depending on your application.

- [ASP.NET Applications](#)
- [ASP.NET Core Applications](#)
- [.NET Console Applications](#)
- [Java](#)
- [Node.js](#)
- [Python](#)
- [Other platforms](#)

See [What is Application Insights?](#)

## Level 5- External components

Components external to AKS include the following.

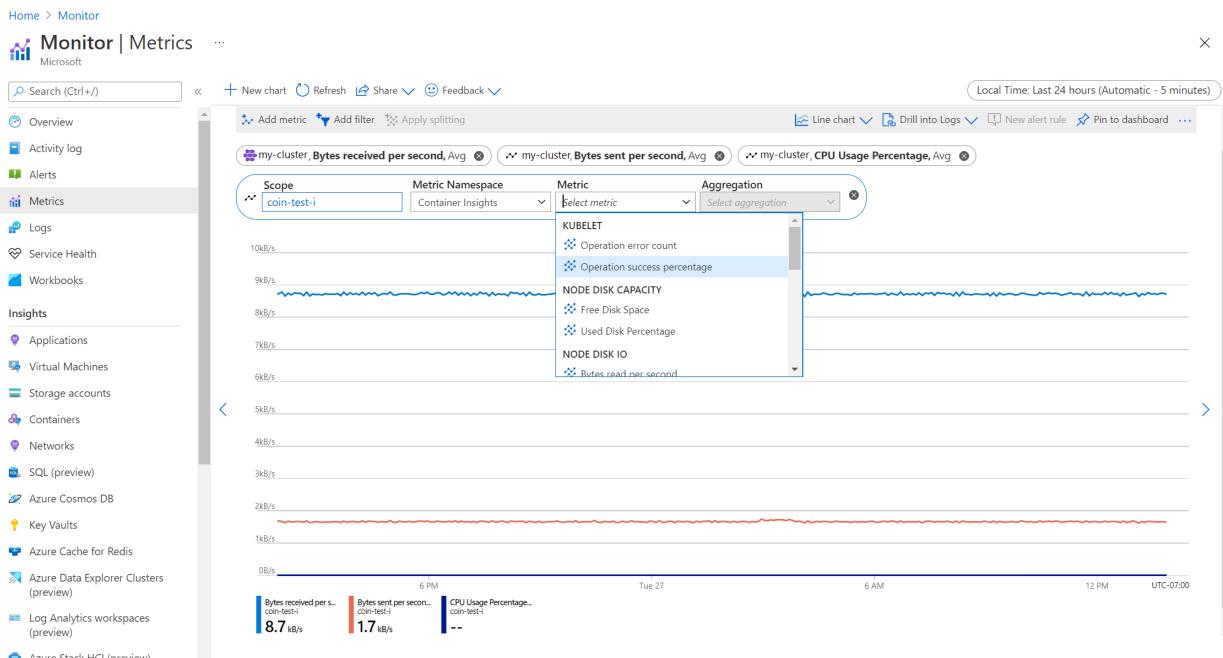
COMPONENT	MONITORING REQUIREMENTS
Service Mesh, Ingress, Egress	Metrics based on component.
Database and work queues	Metrics based on component.

Monitor external components such as Service Mesh, Ingress, Egress with Prometheus and Grafana or other proprietary tools. Monitor databases and other Azure resources using other features of Azure Monitor.

## Analyze metric data with metrics explorer

Use metrics explorer when you want to perform custom analysis of metric data collected for your containers. Metrics explorer allows you plot charts, visually correlate trends, and investigate spikes and dips in metrics' values. Create a metrics alert to proactively notify you when a metric value crosses a threshold, and pin charts to dashboards for use by different members of your organization.

See [Getting started with Azure Metrics Explorer](#) for details on using this feature. For a list of the platform metrics collected for AKS, see [Monitoring AKS data reference metrics](#). When Container insights is enabled for a cluster, [additional metric values](#) are available.



## Analyze log data with Log Analytics

Use Log Analytics when you want to analyze resource logs or dig deeper into the data used to create the views in Container insights. Log Analytics allows you to perform custom analysis of your log data.

See [How to query logs from Container insights](#) for details on using log queries to analyze data collected by Container insights. See [Using queries in Azure Monitor Log Analytics](#) for information on using these queries and [Log Analytics tutorial](#) for a complete tutorial on using Log Analytics to run queries and work with their results.

For a list of the tables collected for AKS that you can analyze in metrics explorer, see [Monitoring AKS data reference logs](#).

The screenshot shows the Azure Monitor Logs interface. On the left, there's a navigation sidebar with links like Home, Monitor, Overview, Activity log, Alerts, Metrics, Logs, Service Health, Workbooks, Insights, Applications, Virtual Machines, Storage accounts, Containers, Networks, SQL (preview), Azure Cosmos DB, Key Vaults, Azure Cache for Redis, Azure Data Explorer Clusters (preview), Log Analytics workspaces (preview), and Azure Stack HCI (preview). The 'Logs' link is highlighted. The main area is titled 'New Query 1\*' and shows a 'Queries' section. A dropdown menu 'Query packs: Select query packs' is open, showing 'Kubernetes Services' as the selected option. Below this, there are several query cards: 'Container Lifecycle Information' (Run, Example query), 'Kubernetes events' (Run, Example query), 'Image inventory' (Run, Example query), 'Container CPU' (Run, Example query), and 'Container memory' (Run, Example query). At the top right of the main area, there are buttons for Feedback, Queries, Query explorer, Documentation, and a close button.

In addition to Container insights data, you can use log queries to analyze resource logs from AKS. For a list of the log categories available, see [AKS data reference resource logs](#). You must create a diagnostic setting to collect each category as described in [Configure monitoring](#) before that data will be collected.

## Alerts

[Alerts in Azure Monitor](#) proactively notify you of interesting data and patterns in your monitoring data. They allow you to identify and address issues in your system before your customers notice them. There are no preconfigured alert rules for AKS clusters, but you can create your own based on data collected by Container insights.

### IMPORTANT

Most alert rules have a cost that's dependent on the type of rule, how many dimensions it includes, and how frequently it's run. Refer to [Alert rules in Azure Monitor pricing](#) before you create any alert rules.

### Choosing the alert type

The most common types of alert rules in Azure Monitor are [metric alerts](#) and [log query alerts](#). The type of alert rule that you create for a particular scenario will depend on where the data is located that you're alerting on. You may have cases though where data for a particular alerting scenario is available in both Metrics and Logs, and you need to determine which rule type to use.

It's typically the best strategy to use metric alerts instead of log alerts when possible since they're more responsive and stateful. You can create a metric alert on any values you can analyze in metrics explorer. If the logic for your alert rule requires data in Logs, or if it requires more complex logic, then you can use a log query alert rule.

For example, if you want to alert when an application workload is consuming excessive CPU then you can create a metric alert using the CPU metric. If you need an alert when a particular message is found in a control plane log, then you'll require a log alert.

### **Metric alert rules**

Metric alert rules use the same metric values as metrics explorer. In fact, you can create an alert rule directly from metrics explorer with the data you're currently analyzing. You can use any of the values in [AKS data reference metrics](#) for metric alert rules.

Container insights includes a feature in public preview that creates a recommended set of metric alert rules for your AKS cluster. This feature creates new metric values (also in preview) used by the alert rules that you can also use in metrics explorer. See [Recommended metric alerts \(preview\) from Container insights](#) for details on this feature and on creating metric alerts for AKS.

### **Log alerts rules**

Use log alert rules to generate an alert from the results of a log query. This may be data collected by Container insights or from AKS resource logs. See [How to create log alerts from Container insights](#) for details on log alert rules for AKS and a set of sample queries designed for alert rules. You can also refer to [How to query logs from Container insights](#) for details on log queries that could be modified for alert rules.

### **Virtual machine alerts**

AKS relies on a virtual machine scale set that must be healthy to run AKS workloads. You can alert on critical metrics such as CPU, memory, and storage for the virtual machines using the guidance at [Monitor virtual machines with Azure Monitor: Alerts](#).

### **Prometheus alerts**

For those conditions where Azure Monitor either doesn't have the data required for an alerting condition, or where the alerting may not be responsive enough, you should configure alerts in Prometheus. One example is alerting for the API server. Azure Monitor doesn't collect critical information for the API server including whether it's available or experiencing a bottleneck. You can create a log query alert using the data from the kube-apiserver resource log category, but this can take up to several minutes before you receive an alert which may not be sufficient for your requirements.

## **Next steps**

- See [Monitoring AKS data reference](#) for a reference of the metrics, logs, and other important values created by AKS.

# Monitoring AKS data reference

10/27/2022 • 3 minutes to read • [Edit Online](#)

See [Monitoring AKS](#) for details on collecting and analyzing monitoring data for AKS.

## Metrics

The following table lists the platform metrics collected for AKS. Follow each link for a detailed list of the metrics for each particular type.

METRIC TYPE	RESOURCE PROVIDER / TYPE NAMESPACE AND LINK TO INDIVIDUAL METRICS
Managed clusters	<a href="#">Microsoft.ContainerService/managedClusters</a>
Connected clusters	<a href="#">microsoft.kubernetes/connectedClusters</a>
Virtual machines	<a href="#">Microsoft.Compute/virtualMachines</a>
Virtual machine scale sets	<a href="#">Microsoft.Compute/virtualMachineScaleSets</a>
Virtual machine scale sets virtual machines	<a href="#">Microsoft.Compute/virtualMachineScaleSets/virtualMachines</a>

For more information, see a list of [all platform metrics supported in Azure Monitor](#).

In addition to the above platform metrics, Azure Monitor container insights collects [these custom metrics](#) for nodes, pods, containers, and persistent volumes.

## Metric dimensions

The following table lists [dimensions](#) for AKS metrics.

DIMENSION NAME	DESCRIPTION
requestKind	Used by metrics such as <i>Inflight Requests</i> to split by type of request.
condition	Used by metrics such as <i>Statuses for various node conditions</i> , <i>Number of pods in Ready state</i> to split by condition type.
status	Used by metrics such as <i>Statuses for various node conditions</i> to split by status of the condition.
status2	Used by metrics such as <i>Statuses for various node conditions</i> to split by status of the condition.
node	Used by metrics such as <i>CPU Usage Millicores</i> to split by the name of the node.

DIMENSION NAME	DESCRIPTION
phase	Used by metrics such as <i>Number of pods by phase</i> to split by the phase of the pod.
namespace	Used by metrics such as <i>Number of pods by phase</i> to split by the namespace of the pod.
pod	Used by metrics such as <i>Number of pods by phase</i> to split by the name of the pod.
nodepool	Used by metrics such as <i>Disk Used Bytes</i> to split by the name of the nodepool.
device	Used by metrics such as <i>Disk Used Bytes</i> to split by the name of the device.

## Resource logs

The following table lists the resource log categories you can collect for AKS. These are the logs for AKS control plane components. See [Configure monitoring](#) for information on creating a diagnostic setting to collect these logs and recommendations on which to enable. See [How to query logs from Container insights](#) for query examples.

For reference, see a list of [all resource logs category types supported in Azure Monitor](#).

CATEGORY	DESCRIPTION
kube-apiserver	Logs from the API server.
kube-audit	Audit log data for every audit event including get, list, create, update, delete, patch, and post.
kube-audit-admin	Subset of the kube-audit log category. Significantly reduces the number of logs by excluding the get and list audit events from the log.
kube-controller-manager	Gain deeper visibility of issues that may arise between Kubernetes and the Azure control plane. A typical example is the AKS cluster having a lack of permissions to interact with Azure.
kube-scheduler	Logs from the scheduler.
cluster-autoscaler	Understand why the AKS cluster is scaling up or down, which may not be expected. This information is also useful to correlate time intervals where something interesting may have happened in the cluster.
cloud-controller-manager	Logs from the cloud-node-manager component of the Kubernetes cloud controller manager.
guard	Managed Azure Active Directory and Azure RBAC audits. For managed Azure AD, this includes token in and user info out. For Azure RBAC, this includes access reviews in and out.

CATEGORY	DESCRIPTION
csi-azuredisk-controller	Logs from the Azure Disk CSI storage driver.
csi-azurefile-controller	Logs from the Azure Files CSI storage driver.
csi-snapshot-controller	Logs from the Azure CSI driver snapshot controller.
AllMetrics	Includes all platform metrics. Sends these values to Log Analytics workspace where it can be evaluated with other data using log queries.

## Azure Monitor Logs tables

This section refers to all of the Azure Monitor Logs tables relevant to AKS and available for query by Log Analytics.

RESOURCE TYPE	NOTES
Kubernetes services	Follow this link for a list of all tables used by AKS and a description of their structure.

For a reference of all Azure Monitor Logs / Log Analytics tables, see the [Azure Monitor Log Table Reference](#).

## Activity log

The following table lists a few example operations related to AKS that may be created in the [Activity log](#). Use the Activity log to track information such as when a cluster is created or had its configuration change. You can either view this information in the portal or create an Activity log alert to be proactively notified when an event occurs.

OPERATION	DESCRIPTION
Microsoft.ContainerService/managedClusters/write	Create or update managed cluster
Microsoft.ContainerService/managedClusters/delete	Delete Managed Cluster
Microsoft.ContainerService/managedClusters/listClusterMonitoringUserCredential/action	List clusterMonitoringUser credential
Microsoft.ContainerService/managedClusters/listClusterAdminCredential/action	List clusterAdmin credential
Microsoft.ContainerService/managedClusters/agentpools/write	Create or Update Agent Pool

For a complete list of possible log entries, see [Microsoft.ContainerService Resource Provider options](#).

For more information on the schema of Activity Log entries, see [Activity Log schema](#).

## See also

- See [Monitoring Azure AKS](#) for a description of monitoring Azure AKS.
- See [Monitoring Azure resources with Azure Monitor](#) for details on monitoring Azure resources.

# Get kubelet logs from Azure Kubernetes Service (AKS) cluster nodes

10/27/2022 • 2 minutes to read • [Edit Online](#)

As part of operating an AKS cluster, you may need to review logs to troubleshoot a problem. Built-in to the Azure portal is the ability to view logs for the [AKS master components](#) or [containers in an AKS cluster](#). Occasionally, you may need to get *kubelet* logs from an AKS node for troubleshooting purposes.

This article shows you how you can use `journalctl` to view the *kubelet* logs on an AKS node.

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart [using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

## Create an SSH connection

First, create an SSH connection with the node on which you need to view *kubelet* logs. This operation is detailed in the [SSH into Azure Kubernetes Service \(AKS\) cluster nodes](#) document.

## Get kubelet logs

Once you have connected to the node via `kubectl debug`, run the following command to pull the *kubelet* logs:

```
chroot /host
journalctl -u kubelet -o cat
```

### NOTE

You don't need to use `sudo journalctl` since you are already `root` on the node.

### NOTE

For Windows nodes, the log data is in `C:\k` and can be viewed using the `more` command:

```
more C:\k\kubelet.log
```

The following sample output shows the *kubelet* log data:

```
I0508 12:26:17.905042 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:26:27.943494 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:26:28.920125 8672 server.go:796] GET /stats/summary: (10.370874ms) 200 [[Ruby] 10.244.0.2:52292]
I0508 12:26:37.964650 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:26:47.996449 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:26:58.019746 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:27:05.107680 8672 server.go:796] GET /stats/summary/: (24.853838ms) 200 [[Go-http-client/1.1]
10.244.0.3:44660]
I0508 12:27:08.041736 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:27:18.068505 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:27:28.094889 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:27:38.121346 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:27:44.015205 8672 server.go:796] GET /stats/summary: (30.236824ms) 200 [[Ruby] 10.244.0.2:52588]
I0508 12:27:48.145640 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:27:58.178534 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:28:05.040375 8672 server.go:796] GET /stats/summary/: (27.78503ms) 200 [[Go-http-client/1.1]
10.244.0.3:44660]
I0508 12:28:08.214158 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:28:18.242160 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:28:28.274408 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:28:38.296074 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:28:48.321952 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
I0508 12:28:58.344656 8672 kubelet_node_status.go:497] Using Node Hostname from cloudprovider: "aks-
agentpool-11482510-0"
```

## Next steps

If you need additional troubleshooting information from the Kubernetes master, see [view Kubernetes master node logs in AKS](#).

View Kubernetes logs, events, and pod metrics in real time

10/27/2022 • 6 minutes to read • [Edit Online](#)

Container insights includes the Live Data feature. You can use this advanced diagnostic feature for direct access to your Azure Kubernetes Service (AKS) container logs (stdout/stderror), events, and pod metrics. It exposes direct access to `kubectl logs -c`, `kubectl get` events, and `kubectl top pods`. A console pane shows the logs, events, and metrics generated by the container engine to help with troubleshooting issues in real time.

This article provides an overview of this feature and helps you understand how to use it.

For help with setting up or troubleshooting the Live Data feature, see the [Setup guide](#). This feature directly accesses the Kubernetes API. For more information about the authentication model, see [The Kubernetes API](#).

## View AKS resource live logs

To view the live logs for pods, deployments, and replica sets with or without Container insights from the AKS resource view:

1. In the Azure portal, browse to the AKS cluster resource group and select your AKS resource.
  2. Select **Workloads** in the **Kubernetes resources** section of the menu.
  3. Select a pod, deployment, or replica set from the respective tab.
  4. Select **Live Logs** from the resource's menu.
  5. Select a pod to start collecting the live data.

## View logs

You can view real-time log data as it's generated by the container engine on the **Nodes**, **Controllers**, or **Containers** view. To view log data:

1. In the Azure portal, browse to the AKS cluster resource group and select your AKS resource.

- On the AKS cluster dashboard, under **Monitoring** on the left side, select **Insights**.
- Select the **Nodes, Controllers, or Containers** tab.
- Select an object from the performance grid. In the **Properties** pane on the right side, select **View live data**. If the AKS cluster is configured with single sign-on by using Azure Active Directory (Azure AD), you're prompted to authenticate on first use during that browser session. Select your account and finish authentication with Azure.

#### NOTE

To view the data from your Log Analytics workspace, select **View in analytics** in the **Properties** pane. The log search results potentially show **Nodes**, **Daemon Sets**, **Replica Sets**, **Jobs**, **Cron Jobs**, **Pods**, and **Containers**. These logs might no longer exist. Attempting to search logs for a container that isn't available in `kubectl` will also fail here. To learn more about viewing historical logs, events, and metrics, see [How to query logs from Container insights](#).

After successful authentication, the Live Data console pane appears below the performance data grid. You can view log data here in a continuous stream. If the fetch status indicator shows a green check mark at the far right, it means data can be retrieved, and it begins streaming to your console.

The screenshot shows the AKS Live Data console pane. At the top, there are filter options for 'Time range = Last 6 hours' and 'Add Filter'. Below this, a navigation bar includes 'Cluster', 'Nodes' (which is selected), 'Controllers', 'Containers', and 'Deployments (Preview)'. A search bar labeled 'Search by name...' and a metric selector 'Metric: CPU Usage (millicores)' are also present. The main area displays a table of pod and container status. A specific container named 'redirector' is highlighted. On the right, a properties pane for 'redirector' shows details like 'Container Name: redirector', 'Container ID: f857fa0a05369e1aaef9b8609d8226c68dfc9960625c3215d4e6dbaec492b433', 'Container Status: running', and a log stream window showing recent log entries. The log entries include messages related to Kubernetes service ports and Docker rules.

The pane title shows the name of the pod the container is grouped with.

## View events

You can view real-time event data as it's generated by the container engine on the **Nodes**, **Controllers**, **Containers**, or **Deployments** view when a container, pod, node, ReplicaSet, DaemonSet, job, CronJob, or Deployment is selected. To view events:

- In the Azure portal, browse to the AKS cluster resource group and select your AKS resource.
- On the AKS cluster dashboard, under **Monitoring** on the left side, select **Insights**.
- Select the **Nodes, Controllers, Containers**, or **Deployments** tab.
- Select an object from the performance grid. In the **Properties** pane on the right side, select **View live**

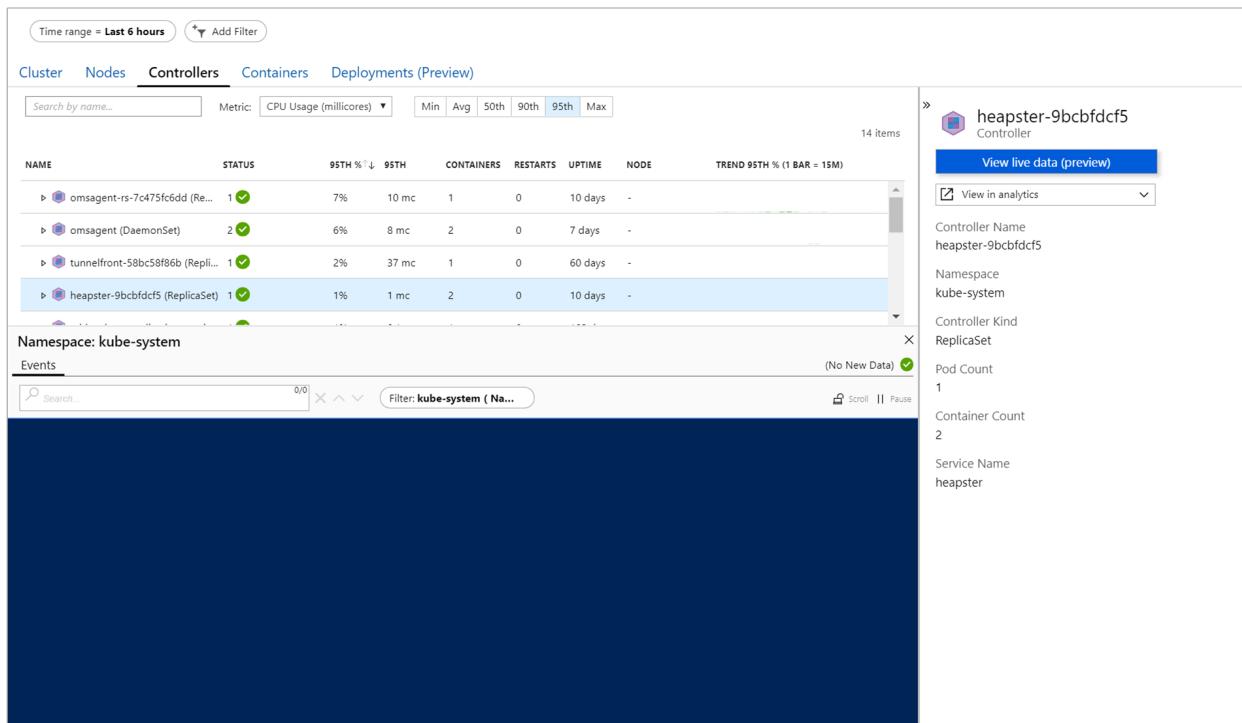
**data.** If the AKS cluster is configured with single sign-on by using Azure AD, you're prompted to authenticate on first use during that browser session. Select your account and finish authentication with Azure.

#### NOTE

To view the data from your Log Analytics workspace, select **View in analytics** in the **Properties** pane. The log search results potentially show **Nodes**, **Daemon Sets**, **Replica Sets**, **Jobs**, **Cron Jobs**, **Pods**, and **Containers**. These logs might no longer exist. Attempting to search logs for a container that isn't available in `kubectl` will also fail here. To learn more about viewing historical logs, events, and metrics, see [How to query logs from Container insights](#).

After successful authentication, the Live Data console pane appears below the performance data grid. If the fetch status indicator shows a green check mark at the far right, it means data can be retrieved, and it begins streaming to your console.

If the object you selected was a container, select the **Events** option in the pane. If you selected a node, pod, or controller, viewing events is automatically selected.



The pane title shows the name of the Pod the container is grouped with.

#### Filter events

While you view events, you can also limit the results by using the **Filter** pill found to the right of the search bar. Depending on the resource you select, the pill lists a pod, namespace, or cluster to choose from.

## View metrics

You can view real-time metric data as it's generated by the container engine from the **Nodes** or **Controllers** view only when a **Pod** is selected. To view metrics:

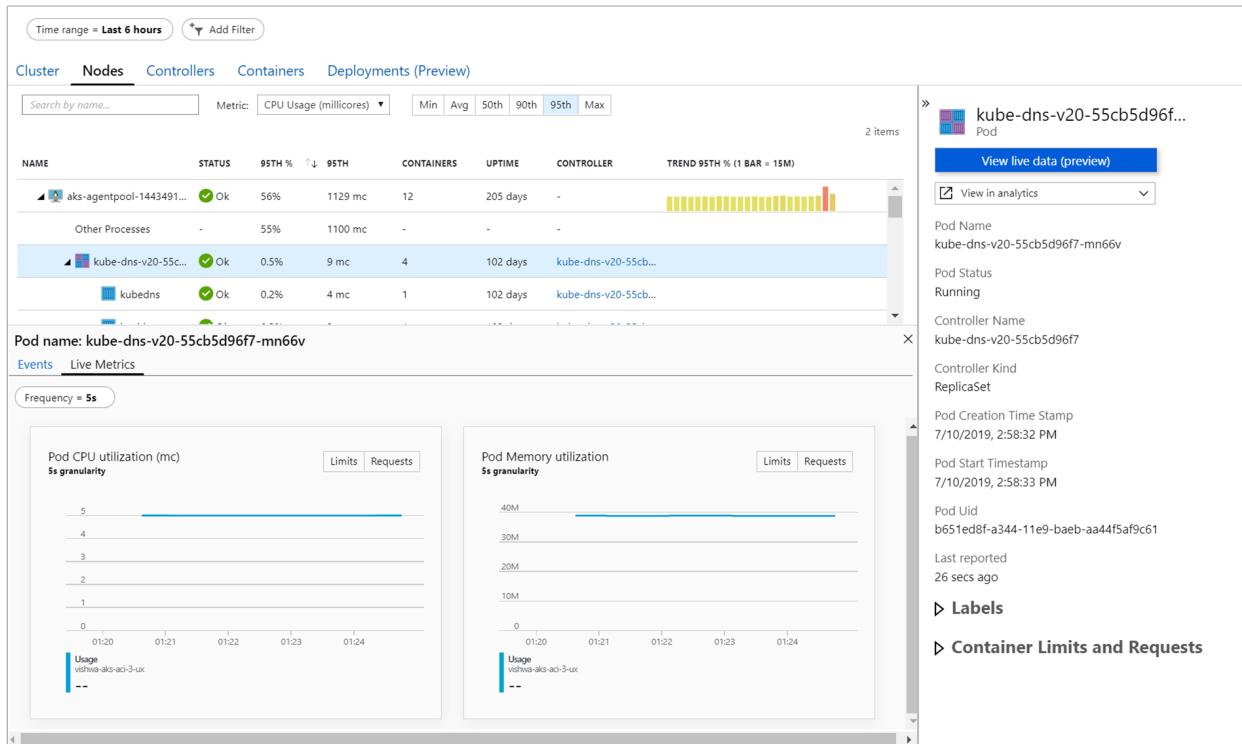
1. In the Azure portal, browse to the AKS cluster resource group and select your AKS resource.
2. On the AKS cluster dashboard, under **Monitoring** on the left side, select **Insights**.
3. Select either the **Nodes** or **Controllers** tab.

4. Select a **Pod** object from the performance grid. In the **Properties** pane on the right side, select **View live data**. If the AKS cluster is configured with single sign-on by using Azure AD, you're prompted to authenticate on first use during that browser session. Select your account and finish authentication with Azure.

#### NOTE

To view the data from your Log Analytics workspace, select the **View in analytics** option in the **Properties** pane. The log search results potentially show **Nodes**, **Daemon Sets**, **Replica Sets**, **Jobs**, **Cron Jobs**, **Pods**, and **Containers**. These logs might no longer exist. Attempting to search logs for a container that isn't available in `kubectl` will also fail here. To learn more about viewing historical logs, events, and metrics, see [How to query logs from Container insights](#).

After successful authentication, the Live Data console pane appears below the performance data grid. Metric data is retrieved and begins streaming to your console for presentation in the two charts. The pane title shows the name of the pod the container is grouped with.



## Use live data views

The following sections describe functionality that you can use in the different live data views.

### Search

The Live Data feature includes search functionality. In the **Search** box, you can filter results by entering a keyword or term. Any matching results are highlighted to allow quick review. While you view the events, you can also limit the results by using the **Filter** feature to the right of the search bar. Depending on what resource you've selected, you can choose from a pod, namespace, or cluster.

Pod name: kube-svc-redirect-t8b9l (redirector)

Logs Events

destination 1/16 X ^ v

(No New Data) ✓

2019-10-21T16:54:06.137209651Z target prot opt source destination

2019-10-21T16:54:06.137214751Z DNAT tcp -- anywhere 10.0.0.1 to:127.0.0.1:14612

2019-10-21T16:54:06.137218452Z RETURN all -- anywhere anywhere

2019-10-21T16:54:06.141669266Z [ Mon Oct 21 16:54:06 UTC 2019 ] INF: found expected rule count in chain:aks-hcp-custom-svc

2019-10-21T16:54:06.141682766Z [ Mon Oct 21 16:54:06 UTC 2019 ] INF: Will validate the following rules:

2019-10-21T16:54:06.141687066Z ++++++  
2019-10-21T16:54:06.14534646Z Chain aks-hcp-custom-svc (2 references)  
2019-10-21T16:54:06.14535986Z num target prot opt source destination  
2019-10-21T16:54:06.14536416Z 1 DNAT tcp -- anywhere 10.0.0.1 to:127.0.0.1:14612  
2019-10-21T16:54:06.14536776Z 2 RETURN all -- anywhere anywhere  
2019-10-21T16:54:06.14537116Z ++++++  
2019-10-21T16:54:06.150201984Z [ Mon Oct 21 16:54:06 UTC 2019 ] INF: Rule #1 match expectation with [1 DNAT tcp -- anywhere 10.0.0.1 to:127.0.0.1:14612]  
2019-10-21T16:54:06.156271639Z [ Mon Oct 21 16:54:06 UTC 2019 ] INF: Rule #2 match expectation with [2 RETURN all -- anywhere anywhere]  
2019-10-21T16:54:06.157287965Z [ Mon Oct 21 16:54:06 UTC 2019 ] INF: chain aks-hcp-custom-svc is valid  
2019-10-21T16:54:06.16411234Z [ Mon Oct 21 16:54:06 UTC 2019 ] INF: Jump rule aks-hcp-custom-svc was found at position #1 in OUTPUT  
2019-10-21T16:54:06.16511376Z [ Mon Oct 21 16:54:06 UTC 2019 ] INF: Rules in OUTPUT are:  
2019-10-21T16:54:06.16526637Z ++++++  
2019-10-21T16:54:06.16817184Z Chain OUTPUT (policy ACCEPT)  
2019-10-21T16:54:06.16818334Z num target prot opt source destination  
2019-10-21T16:54:06.168187145Z 1 aks-hcp-custom-svc all -- anywhere anywhere

## Scroll lock and pause

To suspend autoscroll and control the behavior of the pane so that you can manually scroll through the new data read, select the **Scroll** option. To re-enable autoscroll, select **Scroll** again. You can also pause retrieval of log or event data by selecting the **Pause** option. When you're ready to resume, select **Play**.

Pod name: kube-svc-redirect-4w7qq (redirector)

Logs Events (Paused)

Search... 0/0

Scro Play

```
2019-10-21T17:09:27.328073512Z [Mon Oct 21 17:09:27 UTC 2019] INFO: Rule #2: match expectation with [z RETURN all -- anywhere anywhere]
2019-10-21T17:09:27.328073512Z [Mon Oct 21 17:09:27 UTC 2019] INFO: chain aks-hcp-custom-svc is valid
2019-10-21T17:09:27.335665584Z [Mon Oct 21 17:09:27 UTC 2019] INFO: Jump rule aks-hcp-custom-svc was found at position #1 in OUTPUT
2019-10-21T17:09:27.33693453Z [Mon Oct 21 17:09:27 UTC 2019] INFO: Rules in OUTPUT are:
2019-10-21T17:09:27.33694353Z ++++++
2019-10-21T17:09:27.342360624Z Chain OUTPUT (policy ACCEPT)
2019-10-21T17:09:27.342371725Z num target prot opt source destination
2019-10-21T17:09:27.342375125Z 1 aks-hcp-custom-svc all -- anywhere anywhere
2019-10-21T17:09:27.342377925Z 2 KUBE-SERVICES all -- anywhere anywhere /* kubernetes service portals */
2019-10-21T17:09:27.342380825Z 3 DOCKER all -- anywhere 127.0.0.0/8 ADDRTYPE match dst-type LOCAL
2019-10-21T17:09:27.34251453Z ++++++
2019-10-21T17:09:27.350940932Z [Mon Oct 21 17:09:27 UTC 2019] INFO: Jump rule aks-hcp-custom-svc was found at position #1 in PREROUTING
2019-10-21T17:09:27.3522168276Z [Mon Oct 21 17:09:27 UTC 2019] INFO: Rules in PREROUTING are:
2019-10-21T17:09:27.352211677Z ++++++
2019-10-21T17:09:27.353607627Z Chain PREROUTING (policy ACCEPT)
2019-10-21T17:09:27.353618727Z num target prot opt source destination
2019-10-21T17:09:27.353622128Z 1 aks-hcp-custom-svc all -- anywhere anywhere
2019-10-21T17:09:27.353625428Z 2 KUBE-SERVICES all -- anywhere anywhere /* kubernetes service portals */
2019-10-21T17:09:27.353628828Z 3 DOCKER all -- anywhere anywhere ADDRTYPE match dst-type LOCAL
2019-10-21T17:09:27.353742332Z ++++++
2019-10-21T17:09:27.354929974Z [Mon Oct 21 17:09:27 UTC 2019] INFO: Done - going to sleep for 10
```

The screenshot shows the 'Live Logs (preview)' page for a deployment named 'my-deployment'. The top navigation bar includes 'Home > my-service > my-deployment'. The main title is 'my-deployment | Live Logs (preview)'. On the left, there's a sidebar with 'Overview', 'YAML', 'Events', 'Insights', and 'Live Logs (preview)' (which is highlighted). A search bar at the top has 'Search (Ctrl+I)' and a 'Refresh' button. Below the search bar is a 'Filter grid data' section with a 'Search...' input field and a dropdown menu set to 'my-pod-0000000000-00000'. The main content area displays the message 'Looking for historical logs? View in Log Analytics'. It shows '12 item(s). Streaming is paused' and features a red box around the 'Play' button, which is part of a larger 'Play/Stop' button. There's also a 'Scroll' button next to it.

Suspend or pause autoscroll for only a short period of time while you're troubleshooting an issue. These

requests might affect the availability and throttling of the Kubernetes API on your cluster.

**IMPORTANT**

No data is stored permanently during the operation of this feature. All information captured during the session is deleted when you close your browser or navigate away from it. Data only remains present for visualization inside the five-minute window of the metrics feature. Any metrics older than five minutes are also deleted. The Live Data buffer queries within reasonable memory usage limits.

## Next steps

- To continue learning how to use Azure Monitor and monitor other aspects of your AKS cluster, see [View Azure Kubernetes Service health](#).
- To see predefined queries and examples to create alerts and visualizations or perform further analysis of your clusters, see [How to query logs from Container insights](#).

# Connect with RDP to Azure Kubernetes Service (AKS) cluster Windows Server nodes for maintenance or troubleshooting

10/27/2022 • 10 minutes to read • [Edit Online](#)

Throughout the lifecycle of your Azure Kubernetes Service (AKS) cluster, you may need to access an AKS Windows Server node. This access could be for maintenance, log collection, or other troubleshooting operations. You can access the AKS Windows Server nodes using RDP. For security purposes, the AKS nodes aren't exposed to the internet.

Alternatively, if you want to SSH to your AKS Windows Server nodes, you'll need access to the same key-pair that was used during cluster creation. Follow the steps in [SSH into Azure Kubernetes Service \(AKS\) cluster nodes](#).

This article shows you how to create an RDP connection with an AKS node using their private IP addresses.

## Before you begin

- [Azure CLI](#)
- [Azure PowerShell](#)

This article assumes that you have an existing AKS cluster with a Windows Server node. If you need an AKS cluster, see the article on [creating an AKS cluster with a Windows container using the Azure CLI](#). You need the Windows administrator username and password for the Windows Server node you want to troubleshoot. You also need an RDP client such as [Microsoft Remote Desktop](#).

If you need to reset the password, use `az aks update` to change the password.

```
az aks update -g myResourceGroup -n myAKScluster --windows-admin-password $WINDOWS_ADMIN_PASSWORD
```

If you need to reset the username and password, see [Reset Remote Desktop Services or its administrator password in a Windows VM](#).

You also need the Azure CLI version 2.0.61 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Deploy a virtual machine to the same subnet as your cluster

The Windows Server nodes of your AKS cluster don't have externally accessible IP addresses. To make an RDP connection, you can deploy a virtual machine with a publicly accessible IP address to the same subnet as your Windows Server nodes.

The following example creates a virtual machine named *myVM* in the *myResourceGroup* resource group.

- [Azure CLI](#)
- [Azure PowerShell](#)

You'll need to get the subnet ID used by your Windows Server node pool. The commands below will query for the following information:

- The cluster's node resource group
- The virtual network
- The subnet's name
- The subnet ID

```
CLUSTER_RG=$(az aks show -g myResourceGroup -n myAKSCluster --query nodeResourceGroup -o tsv)
VNET_NAME=$(az network vnet list -g $CLUSTER_RG --query [0].name -o tsv)
SUBNET_NAME=$(az network vnet subnet list -g $CLUSTER_RG --vnet-name $VNET_NAME --query [0].name -o tsv)
SUBNET_ID=$(az network vnet subnet show -g $CLUSTER_RG --vnet-name $VNET_NAME --name $SUBNET_NAME --query id -o tsv)
```

Now that you've the SUBNET\_ID, run the following command in the same Azure Cloud Shell window to create the VM:

```
PUBLIC_IP_ADDRESS="myVMPublicIP"

az vm create \
--resource-group myResourceGroup \
--name myVM \
--image win2019datacenter \
--admin-username azureuser \
--admin-password {admin-password} \
--subnet $SUBNET_ID \
--nic-delete-option delete \
--os-disk-delete-option delete \
--nsg "" \
--public-ip-address $PUBLIC_IP_ADDRESS \
--query publicIpAddress -o tsv
```

The following example output shows the VM has been successfully created and displays the public IP address of the virtual machine.

```
13.62.204.18
```

Record the public IP address of the virtual machine. You'll use this address in a later step.

## Allow access to the virtual machine

AKS node pool subnets are protected with NSGs (Network Security Groups) by default. To get access to the virtual machine, you'll have to enable access in the NSG.

### NOTE

The NSGs are controlled by the AKS service. Any change you make to the NSG will be overwritten at any time by the control plane.

- [Azure CLI](#)
- [Azure PowerShell](#)

First, get the resource group and name of the NSG to add the rule to:

```
CLUSTER_RG=$(az aks show -g myResourceGroup -n myAKSCluster --query nodeResourceGroup -o tsv)
NSG_NAME=$(az network nsg list -g $CLUSTER_RG --query [].name -o tsv)
```

Then, create the NSG rule:

```
az network nsg rule create \
--name tempRDPAccess \
--resource-group $CLUSTER_RG \
--nsg-name $NSG_NAME \
--priority 100 \
--destination-port-range 3389 \
--protocol Tcp \
--description "Temporary RDP access to Windows nodes"
```

## Get the node address

- [Azure CLI](#)
- [Azure PowerShell](#)

To manage a Kubernetes cluster, you use [kubectl](#), the Kubernetes command-line client. If you use Azure Cloud Shell, `kubectl` is already installed. To install `kubectl` locally, use the [az aks install-cli](#) command:

```
az aks install-cli
```

To configure `kubectl` to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command. This command downloads credentials and configures the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

List the internal IP address of the Windows Server nodes using the [kubectl get](#) command:

```
kubectl get nodes -o wide
```

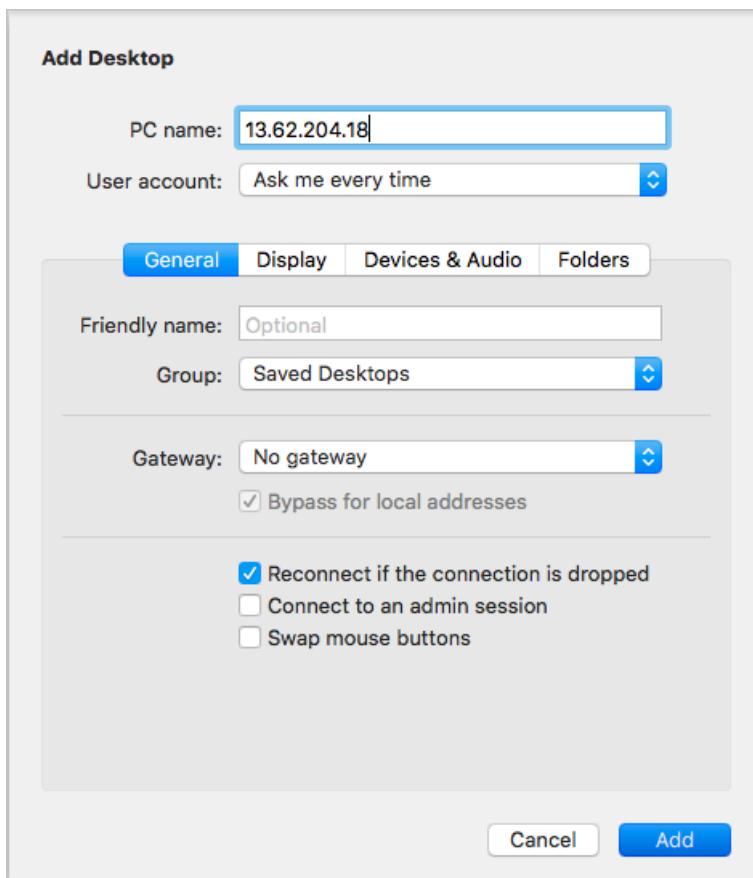
The following example output shows the internal IP addresses of all the nodes in the cluster, including the Windows Server nodes.

```
$ kubectl get nodes -o wide
NAME STATUS ROLES AGE VERSION INTERNAL-IP EXTERNAL-IP OS-IMAGE
KERNEL-VERSION CONTAINER-RUNTIME
aks-nodepool1-42485177-vmss000000 Ready agent 18h v1.12.7 10.240.0.4 <none> Ubuntu
16.04.6 LTS 4.15.0-1040-azure docker://3.0.4
aksnpwin000000 Ready agent 13h v1.12.7 10.240.0.67 <none> Windows
Server Datacenter 10.0.17763.437
```

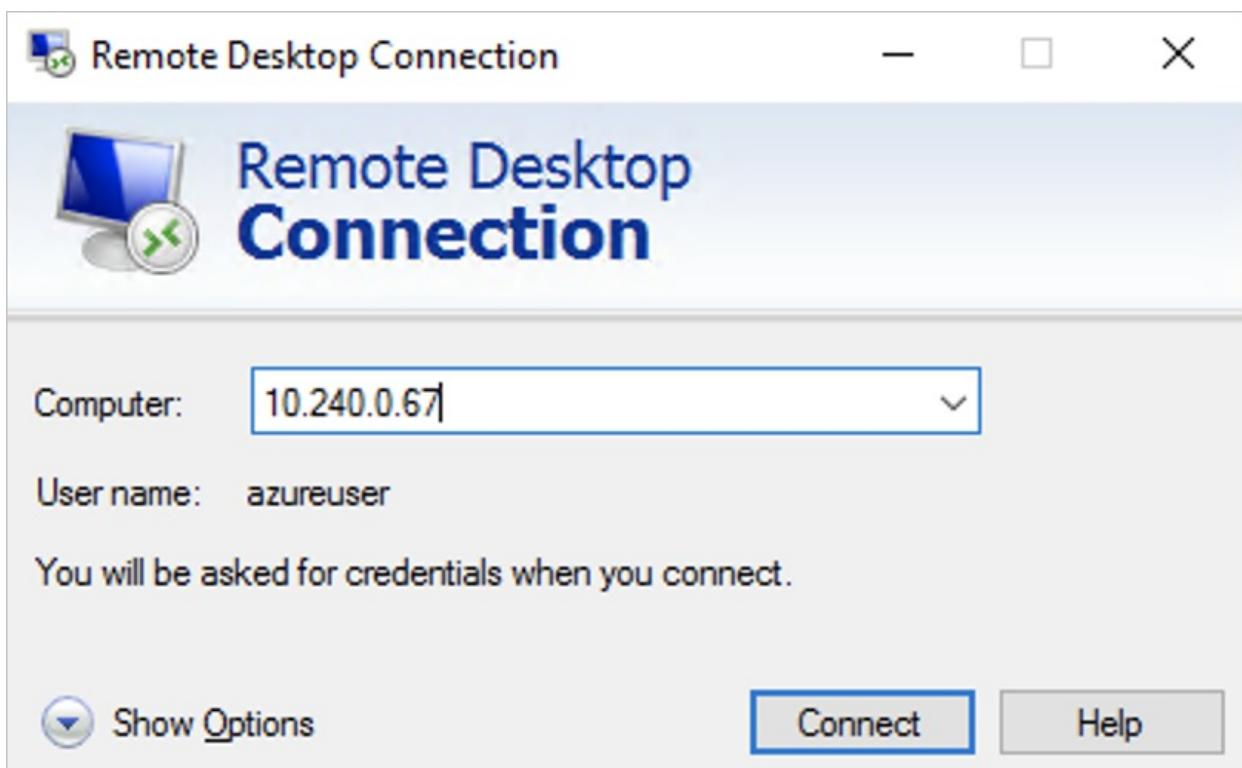
Record the internal IP address of the Windows Server node you wish to troubleshoot. You'll use this address in a later step.

## Connect to the virtual machine and node

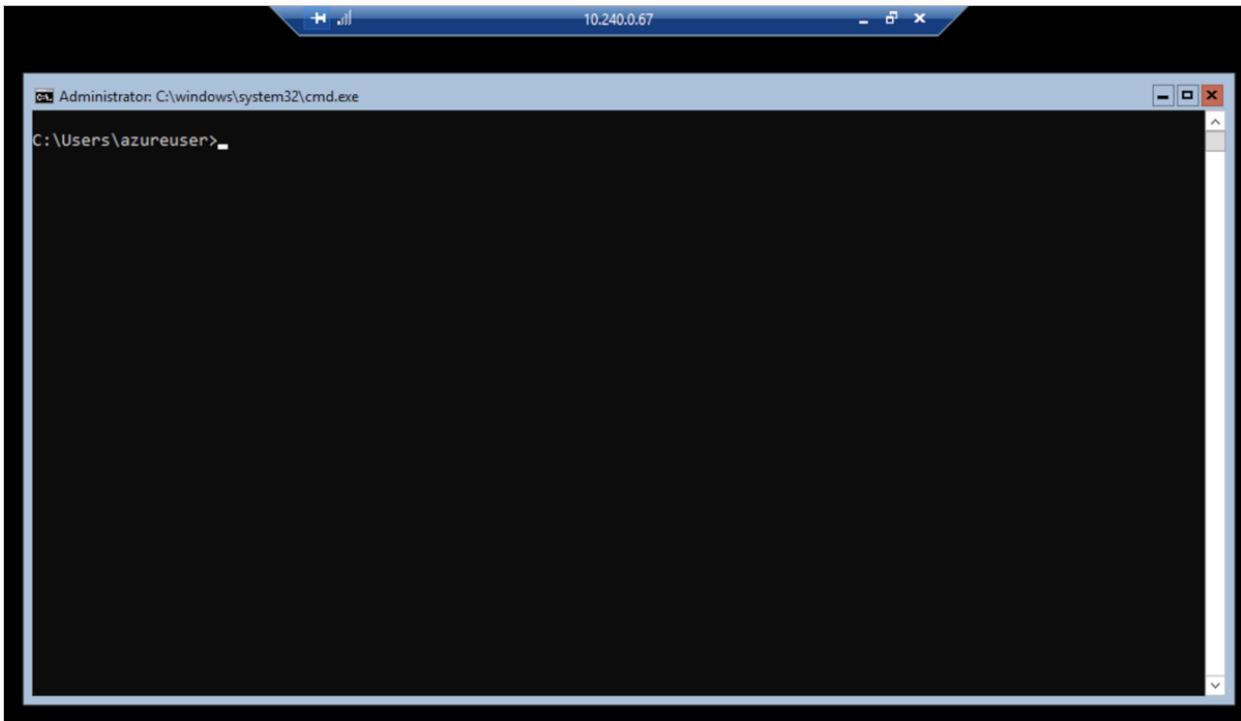
Connect to the public IP address of the virtual machine you created earlier using an RDP client such as [Microsoft Remote Desktop](#).



After you've connected to your virtual machine, connect to the *internal IP address* of the Windows Server node you want to troubleshoot using an RDP client from within your virtual machine.



You're now connected to your Windows Server node.



You can now run any troubleshooting commands in the *cmd* window. Since Windows Server nodes use Windows Server Core, there's not a full GUI or other GUI tools when you connect to a Windows Server node over RDP.

## Remove RDP access

- [Azure CLI](#)
- [Azure PowerShell](#)

When done, exit the RDP connection to the Windows Server node then exit the RDP session to the virtual machine. After you exit both RDP sessions, delete the virtual machine with the `az vm delete` command:

```
Delete the virtual machine
az vm delete \
--resource-group myResourceGroup \
--name myVM
```

Delete the public IP associated with the virtual machine:

```
az network public-ip delete \
--resource-group myResourceGroup \
--name $PUBLIC_IP_ADDRESS
```

Delete the NSG rule:

```
CLUSTER_RG=$(az aks show -g myResourceGroup -n myAKSCluster --query nodeResourceGroup -o tsv)
NSG_NAME=$(az network nsg list -g $CLUSTER_RG --query [].name -o tsv)
az network nsg rule delete \
--resource-group $CLUSTER_RG \
--nsg-name $NSG_NAME \
--name tempRDPAccess
```

## Connect with Azure Bastion

Alternatively, you can use [Azure Bastion](#) to connect to your Windows Server node.

## Deploy Azure Bastion

To deploy Azure Bastion, you'll need to find the virtual network your AKS cluster is connected to.

1. In the Azure portal, go to **Virtual networks**. Select the virtual network your AKS cluster is connected to.
2. Under **Settings**, select **Bastion**, then select **Deploy Bastion**. Wait until the process is finished before going to the next step.

## Connect to your Windows Server nodes using Azure Bastion

Go to the node resource group of the AKS cluster. Run the command below in the Azure Cloud Shell to get the name of your node resource group:

- [Azure CLI](#)
- [Azure PowerShell](#)

```
az aks show -n myAKSCluster -g myResourceGroup --query 'nodeResourceGroup' -o tsv
```

1. Select **Overview**, and select your Windows node pool virtual machine scale set.
2. Under **Settings**, select **Instances**. Select a Windows server node that you'd like to connect to.
3. Under **Support + troubleshooting**, select **Bastion**.
4. Enter the credentials you set up when the AKS cluster was created. Select **Connect**.

You can now run any troubleshooting commands in the *cmd* window. Since Windows Server nodes use Windows Server Core, there's not a full GUI or other GUI tools when you connect to a Windows Server node over RDP.

### NOTE

If you close out of the terminal window, press **CTRL + ALT + End**, select **Task Manager**, select **More details**, select **File**, select **Run new task**, and enter **cmd.exe** to open another terminal. You can also logout and re-connect with Bastion.

## Remove Bastion access

When you're finished, exit the Bastion session and remove the Bastion resource.

1. In the Azure portal, go to **Bastion** and select the Bastion resource you created.
2. At the top of the page, select **Delete**. Wait until the process is complete before proceeding to the next step.
3. In the Azure portal, go to **Virtual networks**. Select the virtual network that your AKS cluster is connected to.
4. Under **Settings**, select **Subnet**, and delete the **AzureBastionSubnet** subnet that was created for the Bastion resource.

## Next steps

If you need more troubleshooting data, you can [view the Kubernetes primary node logs](#) or [Azure Monitor](#).

# Use Windows HostProcess containers

10/27/2022 • 2 minutes to read • [Edit Online](#)

HostProcess / Privileged containers extend the Windows container model to enable a wider range of Kubernetes cluster management scenarios. HostProcess containers run directly on the host and maintain behavior and access similar to that of a regular process. HostProcess containers allow users to package and distribute management operations and functionalities that require host access while retaining versioning and deployment methods provided by containers.

A privileged DaemonSet can carry out changes or monitor a Linux host on Kubernetes but not Windows hosts. HostProcess containers are the Windows equivalent of host elevation.

## Limitations

- HostProcess containers require Kubernetes 1.23 or greater.
- HostProcess containers require `containerd` 1.6 or higher container runtime.
- HostProcess pods can only contain HostProcess containers. This is a current limitation of the Windows operating system. Non-privileged Windows containers can't share a vNIC with the host IP namespace.
- HostProcess containers run as a process on the host. The only isolation those containers have from the host is the resource constraints imposed on the HostProcess user account.
- Filesystem isolation and Hyper-V isolation aren't supported for HostProcess containers.
- Volume mounts are supported and are mounted under the container volume. See Volume Mounts.
- A limited set of host user accounts are available for Host Process containers by default. See Choosing a User Account.
- Resource limits such as disk, memory, and cpu count, work the same way as fashion as processes on the host.
- Named pipe mounts and Unix domain sockets are not directly supported, but can be accessed on their host path, for example `\.\.\pipe\*`.

## Run a HostProcess workload

To use HostProcess features with your deployment, set `privileged: true`, `hostProcess: true`, and `hostNetwork: true`.

```
spec:
 ...
 containers:
 ...
 securityContext:
 privileged: true
 windowsOptions:
 hostProcess: true
 ...
 hostNetwork: true
 ...
```

To run an example workload that uses HostProcess features on an existing AKS cluster with Windows nodes, create `hostprocess.yaml` with the following:

```

apiVersion: apps/v1
kind: DaemonSet
metadata:
 name: privileged-daemonset
 namespace: kube-system
 labels:
 app: privileged-daemonset
spec:
 selector:
 matchLabels:
 app: privileged-daemonset
 template:
 metadata:
 labels:
 app: privileged-daemonset
 spec:
 nodeSelector:
 kubernetes.io/os: windows
 containers:
 - name: powershell
 image: mcr.microsoft.com/powershell:lts-nanoserver-1809
 securityContext:
 privileged: true
 windowsOptions:
 hostProcess: true
 runAsUserName: "NT AUTHORITY\\SYSTEM"
 command:
 - pwsh.exe
 - -command
 - |
 $AdminRights = ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]"Administrator")
 Write-Host "Process has admin rights: $AdminRights"
 while ($true) { Start-Sleep -Seconds 2147483 }
 hostNetwork: true
 terminationGracePeriodSeconds: 0

```

Use `kubectl` to run the example workload:

```
kubectl apply -f hostprocess.yaml
```

You should see the following output:

```
$ kubectl apply -f hostprocess.yaml
daemonset.apps/privileged-daemonset created
```

You can verify your workload use the features of HostProcess by view the pod's logs.

Use `kubectl` to find the name of the pod in the `kube-system` namespace.

```
$ kubectl get pods --namespace kube-system
NAME READY STATUS RESTARTS AGE
...
privileged-daemonset-12345 1/1 Running 0 2m13s
```

Use `kubectl log` to view the logs of the pod and verify the pod has administrator rights:

```
$ kubectl logs privileged-daemonset-12345 --namespace kube-system
InvalidOperation: Unable to find type [Security.Principal.WindowsPrincipal].
Process has admin rights:
```

## Next steps

For more details on HostProcess containers and Microsoft's contribution to Kubernetes upstream, see the [Alpha in v1.22: Windows HostProcess Containers](#).

# Frequently asked questions for Windows Server node pools in AKS

10/27/2022 • 10 minutes to read • [Edit Online](#)

In Azure Kubernetes Service (AKS), you can create a node pool that runs Windows Server as the guest OS on the nodes. These nodes can run native Windows container applications, such as those built on the .NET Framework. There are differences in how the Linux and Windows OS provides container support. Some common Linux Kubernetes and pod-related features are not currently available for Windows node pools.

This article outlines some of the frequently asked questions and OS concepts for Windows Server nodes in AKS.

## Which Windows operating systems are supported?

AKS uses Windows Server 2019 and Windows Server 2022 as the host OS version and only supports process isolation. Container images built by using other Windows Server versions are not supported. For more information, see [Windows container version compatibility](#).

## Is Kubernetes different on Windows and Linux?

Windows Server node pool support includes some limitations that are part of the upstream Windows Server in Kubernetes project. These limitations are not specific to AKS. For more information on the upstream support from the Kubernetes project, see the [Supported functionality and limitations](#) section of the [Intro to Windows support in Kubernetes](#) document.

Historically, Kubernetes is Linux-focused. Many examples used in the upstream [Kubernetes.io](#) website are intended for use on Linux nodes. When you create deployments that use Windows Server containers, the following considerations at the OS level apply:

- **Identity:** Linux identifies a user by an integer user identifier (UID). A user also has an alphanumeric user name for logging on, which Linux translates to the user's UID. Similarly, Linux identifies a user group by an integer group identifier (GID) and translates a group name to its corresponding GID. Windows Server uses a larger binary security identifier (SID) that's stored in the Windows Security Access Manager (SAM) database. This database is not shared between the host and containers, or between containers.
- **File permissions:** Windows Server uses an access control list based on SIDs, rather than a bitmask of permissions and UID+GID.
- **File paths:** The convention on Windows Server is to use \ instead of /. In pod specs that mount volumes, specify the path correctly for Windows Server containers. For example, rather than a mount point of `/mnt/volume` in a Linux container, specify a drive letter and location such as `/K/Volume` to mount as the `K:` drive.

## What kind of disks are supported for Windows?

Azure Disks and Azure Files are the supported volume types, and are accessed as NTFS volumes in the Windows Server container.

## Can I run Windows only clusters in AKS?

The master nodes (the control plane) in an AKS cluster are hosted by the AKS service. You won't be exposed to the operating system of the nodes hosting the master components. All AKS clusters are created with a default

first node pool, which is Linux-based. This node pool contains system services that are needed for the cluster to function. We recommend that you run at least two nodes in the first node pool to ensure the reliability of your cluster and the ability to do cluster operations. The first Linux-based node pool can't be deleted unless the AKS cluster itself is deleted.

## How do I patch my Windows nodes?

To get the latest patches for Windows nodes, you can either [upgrade the node pool](#) or [upgrade the node image](#). Windows Updates are not enabled on nodes in AKS. AKS releases new node pool images as soon as patches are available, and it's the user's responsibility to upgrade node pools to stay current on patches and hotfixes. This patch process is also true for the Kubernetes version being used. [AKS release notes](#) indicate when new versions are available. For more information on upgrading the Windows Server node pool, see [Upgrade a node pool in AKS](#). If you're only interested in updating the node image, see [AKS node image upgrades](#).

### NOTE

The updated Windows Server image will only be used if a cluster upgrade (control plane upgrade) has been performed prior to upgrading the node pool.

## What network plug-ins are supported?

AKS clusters with Windows node pools must use the Azure Container Networking Interface (Azure CNI) (advanced) networking model. Kubenet (basic) networking is not supported. For more information on the differences in network models, see [Network concepts for applications in AKS](#). The Azure CNI network model requires extra planning and consideration for IP address management. For more information on how to plan and implement Azure CNI, see [Configure Azure CNI networking in AKS](#).

Windows nodes on AKS clusters also have [Direct Server Return \(DSR\)](#) enabled by default when Calico is enabled.

## Is preserving the client source IP supported?

At this time, [client source IP preservation](#) is not supported with Windows nodes.

## Can I change the maximum number of pods per node?

Yes. For the implications of making a change and the options that are available, see [Maximum number of pods](#).

## Why am I seeing an error when I try to create a new Windows agent pool?

If you created your cluster before February 2020 and have never done any cluster upgrade operations, the cluster still uses an old Windows image. You may have seen an error that resembles:

"The following list of images referenced from the deployment template is not found: Publisher: MicrosoftWindowsServer, Offer: WindowsServer, Sku: 2019-datacenter-core-smalldisk-2004, Version: latest. Please refer to [Find and use Azure Marketplace VM images with Azure PowerShell](#) for instructions on finding available images."

To fix this error:

1. Upgrade the [cluster control plane](#) to update the image offer and publisher.
2. Create new Windows agent pools.
3. Move Windows pods from existing Windows agent pools to new Windows agent pools.

4. Delete old Windows agent pools.

## How do I rotate the service principal for my Windows node pool?

Windows node pools do not support service principal rotation. To update the service principal, create a new Windows node pool and migrate your pods from the older pool to the new one. After your pods are migrated to the new pool, delete the older node pool.

Instead of service principals, use managed identities, which are essentially wrappers around service principals. For more information, see [Use managed identities in Azure Kubernetes Service](#).

## How do I change the administrator password for Windows Server nodes on my cluster?

- [Azure CLI](#)
- [Azure PowerShell](#)

When you create your AKS cluster, you specify the `--windows-admin-password` and `--windows-admin-username` parameters to set the administrator credentials for any Windows Server nodes on the cluster. If you didn't specify administrator credentials when you created a cluster by using the Azure portal or when setting `--vm-set-type VirtualMachineScaleSets` and `--network-plugin azure` by using the Azure CLI, the username defaults to *azureuser* and a randomized password.

To change the administrator password, use the `az aks update` command:

```
az aks update \
 --resource-group $RESOURCE_GROUP \
 --name $CLUSTER_NAME \
 --windows-admin-password $NEW_PW
```

### IMPORTANT

Performing the `az aks update` operation upgrades only Windows Server node pools. Linux node pools are not affected.

When you're changing `--windows-admin-password`, the new password must be at least 14 characters and meet [Windows Server password requirements](#).

## How many node pools can I create?

The AKS cluster can have a maximum of 100 node pools. You can have a maximum of 1,000 nodes across those node pools. For more information, see [Node pool limitations](#).

## What can I name my Windows node pools?

A Windows node pool can have a six-character name.

## Are all features supported with Windows nodes?

Kubenet is currently not supported with Windows nodes.

## Can I run ingress controllers on Windows nodes?

Yes, an ingress controller that supports Windows Server containers can run on Windows nodes in AKS.

## Can my Windows Server containers use gMSA?

Group-managed service account (gMSA) support is generally available for Windows on AKS. See [Enable Group Managed Service Accounts \(GMSA\) for your Windows Server nodes on your Azure Kubernetes Service \(AKS\) cluster](#)

## Can I use Azure Monitor for containers with Windows nodes and containers?

Yes, you can. However, Azure Monitor is in public preview for gathering logs (stdout, stderr) and metrics from Windows containers. You can also attach to the live stream of stdout logs from a Windows container.

## Are there any limitations on the number of services on a cluster with Windows nodes?

A cluster with Windows nodes can have approximately 500 services before it encounters port exhaustion.

## Can I use Azure Hybrid Benefit with Windows nodes?

Yes. Azure Hybrid Benefit for Windows Server reduces operating costs by letting you bring your on-premises Windows Server license to AKS Windows nodes.

Azure Hybrid Benefit can be used on your entire AKS cluster or on individual nodes. For individual nodes, you need to browse to the [node resource group](#) and apply the Azure Hybrid Benefit to the nodes directly. For more information on applying Azure Hybrid Benefit to individual nodes, see [Azure Hybrid Benefit for Windows Server](#).

To use Azure Hybrid Benefit on a new AKS cluster, run the `az aks create` command and use the `--enable-ahub` argument.

```
az aks create \
 --resource-group myResourceGroup \
 --name myAKScluster \
 --load-balancer-sku Standard \
 --windows-admin-password 'Password1234$' \
 --windows-admin-username azure \
 --network-plugin azure
 --enable-ahub
```

To use Azure Hybrid Benefit on an existing AKS cluster, run the `az aks update` command and use the update the cluster by using the `--enable-ahub` argument.

```
az aks update \
 --resource-group myResourceGroup
 --name myAKScluster
 --enable-ahub
```

To check if Azure Hybrid Benefit is set on the Windows nodes in the cluster, run the `az vmss show` command with the `--name` and `--resource-group` arguments to query the virtual machine scale set. To identify the resource group the scale set for the Windows node pool is created in, you can run the `az vmss list -o table` command.

```
az vmss show --name myScaleSet --resource-group MC_<resourceGroup>_<clusterName>_<region>
```

If the Windows nodes in the scale set have Azure Hybrid Benefit enabled, the output of `az vmss show` will be

similar to the following:

```
""hardwareProfile": null,
 "licenseType": "Windows_Server",
 "networkProfile": {
 "healthProbe": null,
 "networkApiVersion": null,
```

## How do I change the time zone of a running container?

To change the time zone of a running Windows Server container, connect to the running container with a PowerShell session. For example:

```
kubectl exec -it CONTAINER-NAME -- powershell
```

In the running container, use [Set-TimeZone](#) to set the time zone of the running container. For example:

```
Set-TimeZone -Id "Russian Standard Time"
```

To see the current time zone of the running container or an available list of time zones, use [Get-TimeZone](#).

## Can I maintain session affinity from client connections to pods with Windows containers?

Although maintaining session affinity from client connections to pods with Windows containers will be supported in the Windows Server 2022 OS version, you achieve session affinity by client IP currently by limiting your desired pod to run a single instance per node and configuring your Kubernetes service to direct traffic to the pod on the local node.

Use the following configuration:

1. Use an AKS cluster running a minimum version of 1.20.
2. Constrain your pod to allow only one instance per Windows node. You can achieve this by using anti-affinity in your deployment configuration.
3. In your Kubernetes service configuration, set `externalTrafficPolicy=Local`. This ensures that the Kubernetes service directs traffic only to pods within the local node.
4. In your Kubernetes service configuration, set `sessionAffinity: ClientIP`. This ensures that the Azure Load Balancer gets configured with session affinity.

## Next steps

To get started with Windows Server containers in AKS, see [Create a node pool that runs Windows Server in AKS](#).

# Upgrade Kubernetes workloads from Windows Server 2019 to 2022

10/27/2022 • 4 minutes to read • [Edit Online](#)

Upgrading the OS version of a running Windows workload on Azure Kubernetes Service (AKS) requires you to deploy a new node pool as Windows versions must match on each node pool. This article describes the steps to upgrade the OS version for Windows workloads as well as other important aspects.

## Limitations

Windows Server 2019 and Windows Server 2022 cannot co-exist on the same node pool on AKS. A new node pool must be created to host the new OS version. It's important that you match the permissions and access of the previous node pool to the new one.

## Before you begin

- Update the FROM statement on your dockerfile to the new OS version.
- Check your application and verify that the container app works on the new OS version.
- Deploy the verified container app on AKS to a development or testing environment.
- Take note of the new image name or tag. This will be used below to replace the 2019 version of the image on the YAML file to be deployed to AKS.

### NOTE

Check out [Dockerfile on Windows](#) and [Optimize Windows Dockerfiles](#) to learn more about how to build a dockerfile for Windows workloads.

## Add a Windows Server 2022 node pool to the existing cluster

Windows Server 2019 and 2022 cannot co-exist on the same node pool on AKS. To upgrade your application, you need a separate node pool for Windows Server 2022. For more information on how to add a new Windows Server 2022 node pool to an existing AKS cluster, see [Add a Windows Server 2022 node pool](#).

## Update your YAML file

Node Selector is the most common and recommended option for placement of Windows pods on Windows nodes. To use Node Selector, make the following annotation to your YAML files:

```
nodeSelector:
 "kubernetes.io/os": windows
```

The above annotation will find *any* Windows node available and place the pod on that node (of course, following all other scheduling rules). When upgrading from Windows Server 2019 to Windows Server 2022, you need to enforce not only the placement on a Windows node, but also on a node that is running the latest OS version. To accomplish this, one option is to use a different annotation:

```
nodeSelector:
 "kubernetes.azure.com/os-sku": Windows2022
```

Once you update the nodeSelector on the YAML file, you should also update the container image to be used. You can get this information from the previous step on which you created a new version of the containerized application by changing the FROM statement on your dockerfile.

**NOTE**

You should leverage the same YAML file you used to deploy the application in the first place - this will ensure no other configuration is changed, only the nodeSelector and the image to be used.

## Apply the new YAML file to the existing workload

If you have an application deployed already, ensure you follow the steps recommended above to deploy a new node pool with Windows Server 2022 nodes. Once deployed, your environment will show Windows Server 2019 and 2022 nodes, with the workloads running on the 2019 nodes:

```
kubectl get nodes -o wide
```

The command above will show all nodes on your AKS cluster with additional details on the output:

NAME	KERNEL-VERSION	CONTAINER-RUNTIME	STATUS	ROLES	AGE	VERSION	INTERNAL-IP	EXTERNAL-IP	OS-IMAGE
aks-agentpool-18877473-vmss000000	18.04.6 LTS	5.4.0-1085-azure	Ready	agent	5h40m	v1.23.8	10.240.0.4	<none>	Ubuntu
akspoolws000000	Server 2022 Datacenter	10.0.20348.825	Ready	agent	3h15m	v1.23.8	10.240.0.208	<none>	Windows
akspoolws000001	Server 2022 Datacenter	10.0.20348.825	Ready	agent	3h17m	v1.23.8	10.240.0.239	<none>	Windows
akspoolws000002	Server 2022 Datacenter	10.0.20348.825	Ready	agent	3h17m	v1.23.8	10.240.1.14	<none>	Windows
akswspool000000	Server 2019 Datacenter	10.0.17763.3165	Ready	agent	5h37m	v1.23.8	10.240.0.115	<none>	Windows
akswspool000001	Server 2019 Datacenter	10.0.17763.3165	Ready	agent	5h37m	v1.23.8	10.240.0.146	<none>	Windows
akswspool000002	Server 2019 Datacenter	10.0.17763.3165	Ready	agent	5h37m	v1.23.8	10.240.0.177	<none>	Windows

With the Windows Server 2022 node pool deployed and the YAML file configured, you can now deploy the new version of the YAML:

```
kubectl apply -f <filename>
```

The command above should return a "configured" status for the deployment:

```
deployment.apps/sample configured
service/sample unchanged
```

At this point, AKS will start the process of terminating the existing pods and deploying new pods to the Windows Server 2022 nodes. You can check the status of your deployment by running:

```
kubectl get pods -o wide
```

The command above return the status of the pods on the default namespace. You might need to change the command above to list the pods on specific namespaces.

NAME NODE	READY READINESS GATES	STATUS	RESTARTS	AGE	IP	NODE	NOMINATED
sample-7794bfcc4c-k62cq <none>	1/1	Running	0	2m49s	10.240.0.238	akspoolws000000	<none>
sample-7794bfcc4c-rswq9 <none>	1/1	Running	0	2m49s	10.240.1.10	akspoolws000001	<none>
sample-7794bfcc4c-sh78c <none>	1/1	Running	0	2m49s	10.240.0.228	akspoolws000000	<none>

## Active Directory, gMSA and Managed Identity implications

If you are leveraging Group Managed Service Accounts (gMSA) you will need to update the Managed Identity configuration for the new node pool. gMSA uses a secret (user account and password) so the node on which the Windows pod is running can authenticate the container against Active Directory. To access that secret on Azure Key Vault, the node uses a Managed Identity that allows the node to access the resource. Since Managed Identities are configured per node pool, and the pod now resides on a new node pool, you need to update that configuration. Check out [Enable Group Managed Service Accounts \(GMSA\) for your Windows Server nodes on your Azure Kubernetes Service \(AKS\) cluster](#) for more information.

The same principle applies to Managed Identities used for any other pod/node pool when accessing other Azure resources. Any access provided via Managed Identity needs to be updated to reflect the new node pool. To view update and sign-in activities, see [How to view Managed Identity activity](#).

# Install existing applications with Helm in Azure Kubernetes Service (AKS)

10/27/2022 • 5 minutes to read • [Edit Online](#)

[Helm](#) is an open-source packaging tool that helps you install and manage the lifecycle of Kubernetes applications. Similar to Linux package managers such as *APT* and *Yum*, Helm is used to manage Kubernetes charts, which are packages of preconfigured Kubernetes resources.

This article shows you how to configure and use Helm in a Kubernetes cluster on AKS.

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the [AKS quickstart using the Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

In addition, this article assumes you have an existing AKS cluster with an integrated ACR. For more details on creating an AKS cluster with an integrated ACR, see [Authenticate with Azure Container Registry from Azure Kubernetes Service](#).

You also need the Helm CLI installed, which is the client that runs on your development system. It allows you to start, stop, and manage applications with Helm. If you use the Azure Cloud Shell, the Helm CLI is already installed. For installation instructions on your local platform, see [Installing Helm](#).

### IMPORTANT

Helm is intended to run on Linux nodes. If you have Windows Server nodes in your cluster, you must ensure that Helm pods are only scheduled to run on Linux nodes. You also need to ensure that any Helm charts you install are also scheduled to run on the correct nodes. The commands in this article use `[node-selectors][k8s-node-selector]` to make sure pods are scheduled to the correct nodes, but not all Helm charts may expose a node selector. You can also consider using other options on your cluster, such as [taints](#).

## Verify your version of Helm

Use the `helm version` command to verify you have Helm 3 installed:

```
helm version
```

The following example shows Helm version 3.0.0 installed:

```
$ helm version

version.BuildInfo{Version:"v3.0.0", GitCommit:"e29ce2a54e96cd02ccfce88bee4f58bb6e2a28b6",
GitTreeState:"clean", GoVersion:"go1.13.4"}
```

## Install an application with Helm v3

### Add Helm repositories

Use the `helm repo` command to add the *ingress-nginx* repository.

```
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx
```

## Find Helm charts

Helm charts are used to deploy applications into a Kubernetes cluster. To search for pre-created Helm charts, use the [helm search](#) command:

```
helm search repo ingress-nginx
```

The following condensed example output shows some of the Helm charts available for use:

```
$ helm search repo ingress-nginx

NAME CHART VERSION APP VERSION DESCRIPTION
ingress-nginx/ingress-nginx 2.12.0 0.34.1 Ingress controller for Kubernetes using
NGINX a...
```

To update the list of charts, use the [helm repo update](#) command.

```
helm repo update
```

The following example shows a successful repo update:

```
$ helm repo update

Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "ingress-nginx" chart repository
Update Complete. ✨ Happy Helming! ✨
```

## Import the images used by the Helm chart into your ACR

This article uses the [NGINX ingress controller Helm chart](#), which relies on three container images. Use [az acr import](#) to import those images into your ACR.

```
REGISTRY_NAME=<REGISTRY_NAME>
CONTROLLER_REGISTRY=k8s.gcr.io
CONTROLLER_IMAGE=ingress-nginx/controller
CONTROLLER_TAG=v0.48.1
PATCH_REGISTRY=docker.io
PATCH_IMAGE=jettech/kube-webhook-certgen
PATCH_TAG=v1.5.1
DEFAULTBACKEND_REGISTRY=k8s.gcr.io
DEFAULTBACKEND_IMAGE=defaultbackend-amd64
DEFAULTBACKEND_TAG=1.5

az acr import --name $REGISTRY_NAME --source $CONTROLLER_REGISTRY/$CONTROLLER_IMAGE:$CONTROLLER_TAG --image
$CONTROLLER_IMAGE:$CONTROLLER_TAG
az acr import --name $REGISTRY_NAME --source $PATCH_REGISTRY/$PATCH_IMAGE:$PATCH_TAG --image
$PATCH_IMAGE:$PATCH_TAG
az acr import --name $REGISTRY_NAME --source
$DEFAULTBACKEND_REGISTRY/$DEFAULTBACKEND_IMAGE:$DEFAULTBACKEND_TAG --image
$DEFAULTBACKEND_IMAGE:$DEFAULTBACKEND_TAG
```

#### NOTE

In addition to importing container images into your ACR, you can also import Helm charts into your ACR. For more information, see [Push and pull Helm charts to an Azure container registry](#).

## Run Helm charts

To install charts with Helm, use the [helm install](#) command and specify a release name and the name of the chart to install. To see installing a Helm chart in action, let's install a basic nginx deployment using a Helm chart.

#### TIP

The following example creates a Kubernetes namespace for the ingress resources named *ingress-basic* and is intended to work within that namespace. Specify a namespace for your own environment as needed.

```
ACR_URL=<REGISTRY_URL>

Create a namespace for your ingress resources
kubectl create namespace ingress-basic

Use Helm to deploy an NGINX ingress controller
helm install nginx-ingress ingress-nginx/ingress-nginx \
--version 4.0.13 \
--namespace ingress-basic \
--set controller.replicaCount=2 \
--set controller.nodeSelector."kubernetes\.io/os"=linux \
--set controller.image.registry=$ACR_URL \
--set controller.image.image=$CONTROLLER_IMAGE \
--set controller.image.tag=$CONTROLLER_TAG \
--set controller.image.digest="" \
--set controller.admissionWebhooks.patch.nodeSelector."kubernetes\.io/os"=linux \
--set controller.service.annotations."service\.beta\.kubernetes\.io/azure-load-balancer-health-probe-
request-path"/=healthz \
--set controller.admissionWebhooks.patch.image.registry=$ACR_URL \
--set controller.admissionWebhooks.patch.image.image=$PATCH_IMAGE \
--set controller.admissionWebhooks.patch.image.tag=$PATCH_TAG \
--set defaultBackend.nodeSelector."kubernetes\.io/os"=linux \
--set defaultBackend.image.registry=$ACR_URL \
--set defaultBackend.image.image=$DEFAULTBACKEND_IMAGE \
--set defaultBackend.image.tag=$DEFAULTBACKEND_TAG \
--set defaultBackend.image.digest=""
```

The following condensed example output shows the deployment status of the Kubernetes resources created by the Helm chart:

```
NAME: nginx-ingress
LAST DEPLOYED: Wed Jul 28 11:35:29 2021
NAMESPACE: ingress-basic
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
The ingress-nginx controller has been installed.
It may take a few minutes for the LoadBalancer IP to be available.
You can watch the status by running 'kubectl --namespace ingress-basic get services -o wide -w nginx-
ingress-ingress-nginx-controller'
...

```

Use the `kubectl get services` command to get the *EXTERNAL-IP* of your service.

```
kubectl --namespace ingress-basic get services -o wide -w nginx-ingress-ingress-nginx-controller
```

For example, the below command shows the *EXTERNAL-IP* for the *nginx-ingress-ingress-nginx-controller* service:

```
$ kubectl --namespace ingress-basic get services -o wide -w nginx-ingress-ingress-nginx-controller
NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S)
AGE SELECTOR
nginx-ingress-ingress-nginx-controller LoadBalancer 10.0.254.93 <EXTERNAL_IP>
80:30004/TCP,443:30348/TCP 61s app.kubernetes.io/component=controller,app.kubernetes.io/instance=nginx-ingress,app.kubernetes.io/name=ingress-nginx
```

## List releases

To see a list of releases installed on your cluster, use the `helm list` command.

```
helm list --namespace ingress-basic
```

The following example shows the *my-nginx-ingress* release deployed in the previous step:

```
$ helm list --namespace ingress-basic
NAME NAMESPACE REVISION UPDATED STATUS
CHART APP VERSION
nginx-ingress ingress-basic 1 2021-07-28 11:35:29.9623734 -0500 CDT deployed
ingress-nginx-3.34.0 0.47.0
```

## Clean up resources

When you deploy a Helm chart, a number of Kubernetes resources are created. These resources include pods, deployments, and services. To clean up these resources, use the `helm uninstall` command and specify your release name, as found in the previous `helm list` command.

```
helm uninstall --namespace ingress-basic nginx-ingress
```

The following example shows the release named *my-nginx-ingress* has been uninstalled:

```
$ helm uninstall --namespace ingress-basic nginx-ingress
release "nginx-ingress" uninstalled
```

To delete the entire sample namespace, use the `kubectl delete` command and specify your namespace name. All the resources in the namespace are deleted.

```
kubectl delete namespace ingress-basic
```

## Next steps

For more information about managing Kubernetes application deployments with Helm, see the Helm documentation.

[Helm documentation](#)

# Using OpenFaaS on AKS

10/27/2022 • 4 minutes to read • [Edit Online](#)

[OpenFaaS](#) is a framework for building serverless functions through the use of containers. As an open source project, it has gained large-scale adoption within the community. This document details installing and using OpenFaaS on an Azure Kubernetes Service (AKS) cluster.

## Prerequisites

In order to complete the steps within this article, you need the following.

- Basic understanding of Kubernetes.
- An Azure Kubernetes Service (AKS) cluster and AKS credentials configured on your development system.
- Azure CLI installed on your development system.
- Git command-line tools installed on your system.

## Add the OpenFaaS helm chart repo

Go to <https://shell.azure.com> to open Azure Cloud Shell in your browser.

OpenFaaS maintains its own helm charts to keep up to date with all the latest changes.

```
helm repo add openfaas https://openfaas.github.io/faas-netes/
helm repo update
```

## Deploy OpenFaaS

As a good practice, OpenFaaS and OpenFaaS functions should be stored in their own Kubernetes namespace.

Create a namespace for the OpenFaaS system and functions:

```
kubectl apply -f https://raw.githubusercontent.com/openfaas/faas-netes/master/namespaces.yml
```

Generate a password for the OpenFaaS UI Portal and REST API:

```
generate a random password
PASSWORD=$(head -c 12 /dev/urandom | shasum| cut -d' ' -f1)

kubectl -n openfaas create secret generic basic-auth \
--from-literal=basic-auth-user=admin \
--from-literal=basic-auth-password="$PASSWORD"
```

You can get the value of the secret with `echo $PASSWORD`.

The password we create here will be used by the helm chart to enable basic authentication on the OpenFaaS Gateway, which is exposed to the Internet through a cloud LoadBalancer.

A Helm chart for OpenFaaS is included in the cloned repository. Use this chart to deploy OpenFaaS into your AKS cluster.

```
helm upgrade openfaas --install openfaas/openfaas \
--namespace openfaas \
--set basic_auth=true \
--set functionNamespace=openfaas-fn \
--set serviceType=LoadBalancer
```

Output:

```
NAME: openfaas
LAST DEPLOYED: Wed Feb 28 08:26:11 2018
NAMESPACE: openfaas
STATUS: DEPLOYED

RESOURCES:
==> v1/ConfigMap
NAME DATA AGE
prometheus-config 2 20s
alertmanager-config 1 20s

{snip}

NOTES:
To verify that openfaas has started, run:

kubectl --namespace=openfaas get deployments -l "release=openfaas, app=openfaas"
```

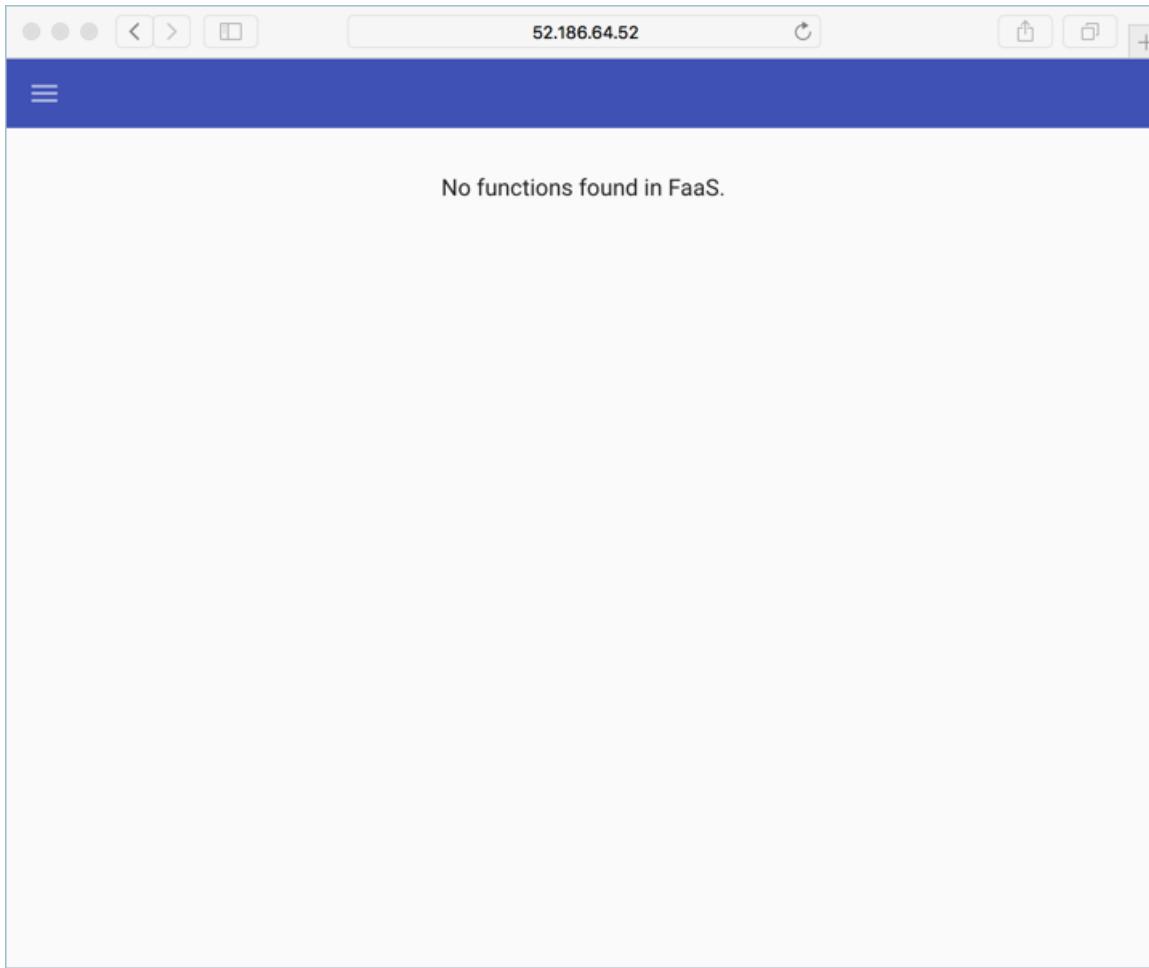
A public IP address is created for accessing the OpenFaaS gateway. To retrieve this IP address, use the [kubectl get service](#) command. It may take a minute for the IP address to be assigned to the service.

```
kubectl get service -l component=gateway --namespace openfaas
```

Output.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
gateway	ClusterIP	10.0.156.194	<none>	8080/TCP	7m
gateway-external	LoadBalancer	10.0.28.18	52.186.64.52	8080:30800/TCP	7m

To test the OpenFaaS system, browse to the external IP address on port 8080, <http://52.186.64.52:8080> in this example. You will be prompted to log in. The default user is `admin` and your password can be retrieved by using `echo $PASSWORD`.



Finally, install the OpenFaaS CLI. This example used brew, see the [OpenFaaS CLI documentation](#) for more options.

```
brew install faas-cli
```

Set `$OPENFAAS_URL` to the public IP found above.

Log in with the Azure CLI:

```
export OPENFAAS_URL=http://52.186.64.52:8080
echo -n $PASSWORD | ./faas-cli login -g $OPENFAAS_URL -u admin --password-stdin
```

## Create first function

Now that OpenFaaS is operational, create a function using the OpenFaaS portal.

Click on **Deploy New Function** and search for **Figlet**. Select the Figlet function, and click **Deploy**.

## Deploy A New Function

X

FROM STORE      MANUALLY

---

Search for Function

 figlet

---

**Figlet**

F OpenFaaS Figlet image. This repository comes with the blog post <http://jmkhael.io/create-a-serverless-ascii-banner-with-faas/>



---

CLOSE DIALOG      DEPLOY

Use curl to invoke the function. Replace the IP address in the following example with that of your OpenFaas gateway.

```
curl -X POST http://52.186.64.52:8080/function/figlet -d "Hello Azure"
```

## Output:

A musical score page showing measures 1-10 of a piece for two voices. The top staff uses soprano C-clef, common time, and a key signature of one sharp. The bottom staff uses alto F-clef, common time, and a key signature of one sharp. The music consists of eighth and sixteenth note patterns, with some rests and measure repeat signs.

## Create second function

Now create a second function. This example will be deployed using the OpenFaaS CLI and includes a custom container image and retrieving data from an Azure Cosmos DB instance. Several items need to be configured before creating the function.

First, create a new resource group for the Azure Cosmos DB instance.

```
az group create --name serverless-backing --location eastus
```

Deploy an Azure Cosmos DB instance of kind `MongoDB`. The instance needs a unique name, update `openfaas-cosmos` to something unique to your environment.

```
az cosmosdb create --resource-group serverless-backing --name openfaas-cosmos --kind MongoDB
```

Get the Azure Cosmos DB database connection string and store it in a variable.

Update the value for the `--resource-group` argument to the name of your resource group, and the `--name` argument to the name of your Azure Cosmos DB instance.

```
COSMOS=$(az cosmosdb list-connection-strings \
--resource-group serverless-backing \
--name openfaas-cosmos \
--query connectionStrings[0].connectionString \
--output tsv)
```

Now populate the Azure Cosmos DB with test data. Create a file named `plans.json` and copy in the following json.

```
{
 "name" : "two_person",
 "friendlyName" : "Two Person Plan",
 "portionSize" : "1-2 Person",
 "mealsPerWeek" : "3 Unique meals per week",
 "price" : 72,
 "description" : "Our basic plan, delivering 3 meals per week, which will feed 1-2 people.",
 "__v" : 0
}
```

Use the `mongoimport` tool to load the Azure Cosmos DB instance with data.

If needed, install the MongoDB tools. The following example installs these tools using brew, see the [MongoDB documentation](#) for other options.

```
brew install mongodb
```

Load the data into the database.

```
mongoimport --uri=$COSMOS -c plans < plans.json
```

Output:

```
2018-02-19T14:42:14.313+0000 connected to: localhost
2018-02-19T14:42:14.918+0000 imported 1 document
```

Run the following command to create the function. Update the value of the `-g` argument with your OpenFaaS gateway address.

```
faas-cli deploy -g http://52.186.64.52:8080 --image=shanepeckham/openfaascosmos --name=cosmos-query --
env=NODE_ENV=$COSMOS
```

Once deployed, you should see your newly created OpenFaaS endpoint for the function.

```
Deployed. 202 Accepted.
URL: http://52.186.64.52:8080/function/cosmos-query
```

Test the function using curl. Update the IP address with the OpenFaaS gateway address.

```
curl -s http://52.186.64.52:8080/function/cosmos-query
```

Output:

```
[{"ID": "", "Name": "two_person", "FriendlyName": "", "PortionSize": "", "MealsPerWeek": "", "Price": 72, "Description": "Our basic plan, delivering 3 meals per week, which will feed 1-2 people."}]
```

You can also test the function within the OpenFaaS UI.

The screenshot shows a browser window with the URL `52.186.64.52`. The title bar says "Invoke function". Below it is a button labeled "INVOKE". Underneath are three radio buttons: "Text" (selected), "JSON", and "Download". A "Request body" input field is empty. The "Response status" section shows "200". The "Round-trip (s)" section shows "0.721". The "Response body" section displays the JSON output from the previous code block.

```
[{"ID": "", "Name": "two_person", "FriendlyName": "", "PortionSize": "", "MealsPerWeek": "", "Price": 72, "Description": "Our basic plan, delivering 3 meals per week, which will feed 1-2 people."}]
```

## Next Steps

You can continue to learn with the [OpenFaaS workshop](#) through a set of hands-on labs that cover topics such as how to create your own GitHub bot, consuming secrets, viewing metrics, and auto-scaling.

# Use GPUs for compute-intensive workloads on Azure Kubernetes Service (AKS)

10/27/2022 • 10 minutes to read • [Edit Online](#)

Graphical processing units (GPUs) are often used for compute-intensive workloads such as graphics and visualization workloads. AKS supports the creation of GPU-enabled node pools to run these compute-intensive workloads in Kubernetes. For more information on available GPU-enabled VMs, see [GPU optimized VM sizes in Azure](#). For AKS node pools, we recommend a minimum size of *Standard\_NC6*. Note that the NVv4 series (based on AMD GPUs) are not yet supported with AKS.

## NOTE

GPU-enabled VMs contain specialized hardware that is subject to higher pricing and region availability. For more information, see the [pricing](#) tool and [region availability](#).

Currently, using GPU-enabled node pools is only available for Linux node pools.

## Before you begin

This article assumes that you have an existing AKS cluster. If you need an AKS cluster, see the AKS quickstart using the [Azure CLI](#), [using Azure PowerShell](#), or [using the Azure portal](#).

You also need the Azure CLI version 2.0.64 or later installed and configured. Run `az --version` to find the version. If you need to install or upgrade, see [Install Azure CLI](#).

## Get the credentials for your cluster

Get the credentials for your AKS cluster using the `az aks get-credentials` command. The following example command gets the credentials for the *myAKSCluster* in the *myResourceGroup* resource group.

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

## Add the NVIDIA device plugin

There are two options for adding the NVIDIA device plugin:

- Use the AKS GPU image
- Manually install the NVIDIA device plugin

## WARNING

You can use either of the above options, but you shouldn't manually install the NVIDIA device plugin daemon set with clusters that use the AKS GPU image.

## Update your cluster to use the AKS GPU image (preview)

AKS provides a fully configured AKS image that already contains the [NVIDIA device plugin for Kubernetes](#).

Register the `GPUDEDICATEDVHDPREVIEW` feature:

```
az feature register --name GPUDEDICATEDVHDPREVIEW --namespace Microsoft.ContainerService
```

It might take several minutes for the status to show as **Registered**. You can check the registration status by using the [az feature list](#) command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/GPUDedicatedVHDPreview')].{Name:name,State:properties.state}"
```

When the status shows as registered, refresh the registration of the `Microsoft.ContainerService` resource provider by using the [az provider register](#) command:

```
az provider register --namespace Microsoft.ContainerService
```

To install the aks-preview CLI extension, use the following Azure CLI commands:

```
az extension add --name aks-preview
```

To update the aks-preview CLI extension, use the following Azure CLI commands:

```
az extension update --name aks-preview
```

## Add a node pool for GPU nodes

To add a node pool with to your cluster, use [az aks nodepool add][az-aks-nodepool-add].

```
az aks nodepool add \
 --resource-group myResourceGroup \
 --cluster-name myAKSCluster \
 --name gpunp \
 --node-count 1 \
 --node-vm-size Standard_NC6 \
 --node-taints sku=gpu:NoSchedule \
 --aks-custom-headers UseGPUDEDICATEDVHD=true \
 --enable-cluster-autoscaler \
 --min-count 1 \
 --max-count 3
```

The above command adds a node pool named *gpunp* to the *myAKSCluster* in the *myResourceGroup* resource group. The command also sets the VM size for the node in the node pool to *Standard\_NC6*, enables the cluster autoscaler, configures the cluster autoscaler to maintain a minimum of one node and a maximum of three nodes in the node pool, specifies a specialized AKS GPU image nodes on your new node pool, and specifies a *sku=gpu:NoSchedule* taint for the node pool.

### NOTE

A taint and VM size can only be set for node pools during node pool creation, but the autoscaler settings can be updated at any time.

#### NOTE

If your GPU sku requires generation two VMs use `--aks-custom-headers UseGPUDedicatedVHD=true,usegen2vm=true`.

For example:

```
az aks nodepool add \
 --resource-group myResourceGroup \
 --cluster-name myAKSCluster \
 --name gpunp \
 --node-count 1 \
 --node-vm-size Standard_NC6 \
 --node-taints sku=gpu:NoSchedule \
 --aks-custom-headers UseGPUDedicatedVHD=true,usegen2vm=true \
 --enable-cluster-autoscaler \
 --min-count 1 \
 --max-count 3
```

#### Manually install the NVIDIA device plugin

Alternatively, you can deploy a DaemonSet for the NVIDIA device plugin. This DaemonSet runs a pod on each node to provide the required drivers for the GPUs.

Add a node pool with to your cluster using [az aks nodepool add][az-aks-nodepool-add].

```
az aks nodepool add \
 --resource-group myResourceGroup \
 --cluster-name myAKSCluster \
 --name gpunp \
 --node-count 1 \
 --node-vm-size Standard_NC6 \
 --node-taints sku=gpu:NoSchedule \
 --enable-cluster-autoscaler \
 --min-count 1 \
 --max-count 3
```

The above command adds a node pool named *gpunp* to the *myAKSCluster* in the *myResourceGroup* resource group. The command also sets the VM size for the nodes in the node pool to *Standard\_NC6*, enables the cluster autoscaler, configures the cluster autoscaler to maintain a minimum of one node and a maximum of three nodes in the node pool, and specifies a *sku=gpu:NoSchedule* taint for the node pool.

#### NOTE

A taint and VM size can only be set for node pools during node pool creation, but the autoscaler settings can be updated at any time.

Create a namespace using the [kubectl create namespace](#) command, such as *gpu-resources*.

```
kubectl create namespace gpu-resources
```

Create a file named *nvidia-device-plugin-ds.yaml* and paste the following YAML manifest. This manifest is provided as part of the [NVIDIA device plugin for Kubernetes project](#).

```

apiVersion: apps/v1
kind: DaemonSet
metadata:
 name: nvidia-device-plugin-daemonset
 namespace: gpu-resources
spec:
 selector:
 matchLabels:
 name: nvidia-device-plugin-ds
 updateStrategy:
 type: RollingUpdate
 template:
 metadata:
 # Mark this pod as a critical add-on; when enabled, the critical add-on scheduler
 # reserves resources for critical add-on pods so that they can be rescheduled after
 # a failure. This annotation works in tandem with the toleration below.
 annotations:
 scheduler.alpha.kubernetes.io/critical-pod: ""
 labels:
 name: nvidia-device-plugin-ds
 spec:
 tolerations:
 # Allow this pod to be rescheduled while the node is in "critical add-ons only" mode.
 # This, along with the annotation above marks this pod as a critical add-on.
 - key: CriticalAddonsOnly
 operator: Exists
 - key: nvidia.com/gpu
 operator: Exists
 effect: NoSchedule
 - key: "sku"
 operator: "Equal"
 value: "gpu"
 effect: "NoSchedule"
 containers:
 - image: mcr.microsoft.com/oss/nvidia/k8s-device-plugin:1.11
 name: nvidia-device-plugin-ctr
 securityContext:
 allowPrivilegeEscalation: false
 capabilities:
 drop: ["ALL"]
 volumeMounts:
 - name: device-plugin
 mountPath: /var/lib/kubelet/device-plugins
 volumes:
 - name: device-plugin
 hostPath:
 path: /var/lib/kubelet/device-plugins

```

Use [kubectl apply](#) to create the DaemonSet and confirm the NVIDIA device plugin is created successfully, as shown in the following example output:

```

$ kubectl apply -f nvidia-device-plugin-ds.yaml

daemonset "nvidia-device-plugin" created

```

## Confirm that GPUs are schedulable

With your AKS cluster created, confirm that GPUs are schedulable in Kubernetes. First, list the nodes in your cluster using the [kubectl get nodes](#) command:

```
$ kubectl get nodes

NAME STATUS ROLES AGE VERSION
aks-gpump-28993262-0 Ready agent 13m v1.20.7
```

Now use the [kubectl describe node](#) command to confirm that the GPUs are schedulable. Under the *Capacity* section, the GPU should list as `nvidia.com/gpu: 1`.

The following condensed example shows that a GPU is available on the node named *aks-nodepool1-18821093-0*.

```
$ kubectl describe node aks-gpump-28993262-0

Name: aks-gpump-28993262-0
Roles: agent
Labels: accelerator=nvidia
[...]
Capacity:
[...]
nvidia.com/gpu: 1
[...]
```

## Run a GPU-enabled workload

To see the GPU in action, schedule a GPU-enabled workload with the appropriate resource request. In this example, let's run a [Tensorflow](#) job against the [MNIST dataset](#).

Create a file named *samples-tf-mnist-demo.yaml* and paste the following YAML manifest. The following job manifest includes a resource limit of `nvidia.com/gpu: 1`:

### NOTE

If you receive a version mismatch error when calling into drivers, such as, CUDA driver version is insufficient for CUDA runtime version, review the NVIDIA driver matrix compatibility chart - <https://docs.nvidia.com/Deploy/CUDA-Compatibility/index.html>

```
apiVersion: batch/v1
kind: Job
metadata:
 labels:
 app: samples-tf-mnist-demo
 name: samples-tf-mnist-demo
spec:
 template:
 metadata:
 labels:
 app: samples-tf-mnist-demo
 spec:
 containers:
 - name: samples-tf-mnist-demo
 image: mcr.microsoft.com/azuredocs/samples-tf-mnist-demo:gpu
 args: ["--max_steps", "500"]
 imagePullPolicy: IfNotPresent
 resources:
 limits:
 nvidia.com/gpu: 1
 restartPolicy: OnFailure
 tolerations:
 - key: "sku"
 operator: "Equal"
 value: "gpu"
 effect: "NoSchedule"
```

Use the [kubectl apply](#) command to run the job. This command parses the manifest file and creates the defined Kubernetes objects:

```
kubectl apply -f samples-tf-mnist-demo.yaml
```

## View the status and output of the GPU-enabled workload

Monitor the progress of the job using the [kubectl get jobs](#) command with the `--watch` argument. It may take a few minutes to first pull the image and process the dataset. When the *COMPLETIONS* column shows *1/1*, the job has successfully finished. Exit the `kubectl --watch` command with *Ctrl-C*:

```
$ kubectl get jobs samples-tf-mnist-demo --watch
NAME COMPLETIONS DURATION AGE
samples-tf-mnist-demo 0/1 3m29s 3m29s
samples-tf-mnist-demo 1/1 3m10s 3m36s
```

To look at the output of the GPU-enabled workload, first get the name of the pod with the [kubectl get pods](#) command:

```
$ kubectl get pods --selector app=samples-tf-mnist-demo
NAME READY STATUS RESTARTS AGE
samples-tf-mnist-demo-mtd44 0/1 Completed 0 4m39s
```

Now use the [kubectl logs](#) command to view the pod logs. The following example pod logs confirm that the appropriate GPU device has been discovered, `Tesla K80`. Provide the name for your own pod:

```
$ kubectl logs samples-tf-mnist-demo-smnr6
```

```
2019-05-16 16:08:31.258328: I tensorflow/core/platform/cpu_feature_guard.cc:137] Your CPU supports
instructions that this TensorFlow binary was not compiled to use: SSE4.1 SSE4.2 AVX AVX2 FMA
2019-05-16 16:08:31.396846: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1030] Found device 0 with
properties:
name: Tesla K80 major: 3 minor: 7 memoryClockRate(GHz): 0.8235
pciBusID: 2fd7:00:00.0
totalMemory: 11.17GiB freeMemory: 11.10GiB
2019-05-16 16:08:31.396886: I tensorflow/core/common_runtime/gpu/gpu_device.cc:1120] Creating TensorFlow
device (/device:GPU:0) -> (device: 0, name: Tesla K80, pci bus id: 2fd7:00:00.0, compute capability: 3.7)
2019-05-16 16:08:36.076962: I tensorflow/stream_executor/dso_loader.cc:139] successfully opened CUDA library
libcupti.so.8.0 locally
Successfully downloaded train-images-idx3-ubyte.gz 9912422 bytes.
Extracting /tmp/tensorflow/input_data/train-images-idx3-ubyte.gz
Successfully downloaded train-labels-idx1-ubyte.gz 28881 bytes.
Extracting /tmp/tensorflow/input_data/train-labels-idx1-ubyte.gz
Successfully downloaded t10k-images-idx3-ubyte.gz 1648877 bytes.
Extracting /tmp/tensorflow/input_data/t10k-images-idx3-ubyte.gz
Successfully downloaded t10k-labels-idx1-ubyte.gz 4542 bytes.
Extracting /tmp/tensorflow/input_data/t10k-labels-idx1-ubyte.gz
Accuracy at step 0: 0.1081
Accuracy at step 10: 0.7457
Accuracy at step 20: 0.8233
Accuracy at step 30: 0.8644
Accuracy at step 40: 0.8848
Accuracy at step 50: 0.8889
Accuracy at step 60: 0.8898
Accuracy at step 70: 0.8979
Accuracy at step 80: 0.9087
Accuracy at step 90: 0.9099
Adding run metadata for 99
Accuracy at step 100: 0.9125
Accuracy at step 110: 0.9184
Accuracy at step 120: 0.922
Accuracy at step 130: 0.9161
Accuracy at step 140: 0.9219
Accuracy at step 150: 0.9151
Accuracy at step 160: 0.9199
Accuracy at step 170: 0.9305
Accuracy at step 180: 0.9251
Accuracy at step 190: 0.9258
Adding run metadata for 199
Accuracy at step 200: 0.9315
Accuracy at step 210: 0.9361
Accuracy at step 220: 0.9357
Accuracy at step 230: 0.9392
Accuracy at step 240: 0.9387
Accuracy at step 250: 0.9401
Accuracy at step 260: 0.9398
Accuracy at step 270: 0.9407
Accuracy at step 280: 0.9434
Accuracy at step 290: 0.9447
Adding run metadata for 299
Accuracy at step 300: 0.9463
Accuracy at step 310: 0.943
Accuracy at step 320: 0.9439
Accuracy at step 330: 0.943
Accuracy at step 340: 0.9457
Accuracy at step 350: 0.9497
Accuracy at step 360: 0.9481
Accuracy at step 370: 0.9466
Accuracy at step 380: 0.9514
Accuracy at step 390: 0.948
Adding run metadata for 399
Accuracy at step 400: 0.9469
Accuracy at step 410: 0.9489
Accuracy at step 420: 0.9529
Accuracy at step 430: 0.9507
Accuracy at step 440: 0.9504
Accuracy at step 450: 0.951
```

```
Accuracy at step 460: 0.9512
Accuracy at step 470: 0.9539
Accuracy at step 480: 0.9533
Accuracy at step 490: 0.9494
Adding run metadata for 499
```

## Use Container Insights to monitor GPU usage

The following metrics are available for [Container Insights with AKS](#) to monitor GPU usage.

METRIC NAME	METRIC DIMENSION (TAGS)	DESCRIPTION
containerGpuDutyCycle	<code>container.azm.ms/clusterId</code> , <code>container.azm.ms/clusterName</code> , <code>containerName</code> , <code>gpuId</code> , <code>gpuModel</code> , <code>gpuVendor</code>	Percentage of time over the past sample period (60 seconds) during which GPU was busy/actively processing for a container. Duty cycle is a number between 1 and 100.
containerGpuLimits	<code>container.azm.ms/clusterId</code> , <code>container.azm.ms/clusterName</code> , <code>containerName</code>	Each container can specify limits as one or more GPUs. It is not possible to request or limit a fraction of a GPU.
containerGpuRequests	<code>container.azm.ms/clusterId</code> , <code>container.azm.ms/clusterName</code> , <code>containerName</code>	Each container can request one or more GPUs. It is not possible to request or limit a fraction of a GPU.
containerGpumemoryTotalBytes	<code>container.azm.ms/clusterId</code> , <code>container.azm.ms/clusterName</code> , <code>containerName</code> , <code>gpuId</code> , <code>gpuModel</code> , <code>gpuVendor</code>	Amount of GPU Memory in bytes available to use for a specific container.
containerGpumemoryUsedBytes	<code>container.azm.ms/clusterId</code> , <code>container.azm.ms/clusterName</code> , <code>containerName</code> , <code>gpuId</code> , <code>gpuModel</code> , <code>gpuVendor</code>	Amount of GPU Memory in bytes used by a specific container.
nodeGpuAllocatable	<code>container.azm.ms/clusterId</code> , <code>container.azm.ms/clusterName</code> , <code>gpuVendor</code>	Number of GPUs in a node that can be used by Kubernetes.
nodeGpuCapacity	<code>container.azm.ms/clusterId</code> , <code>container.azm.ms/clusterName</code> , <code>gpuVendor</code>	Total Number of GPUs in a node.

## Clean up resources

To remove the associated Kubernetes objects created in this article, use the `kubectl delete job` command as follows:

```
kubectl delete jobs samples-tf-mnist-demo
```

## Next steps

To run Apache Spark jobs, see [Run Apache Spark jobs on AKS](#).

For more information about running machine learning (ML) workloads on Kubernetes, see [Kubeflow Labs](#).

For information on using Azure Kubernetes Service with Azure Machine Learning, see the following articles:

- [Configure a Kubernetes cluster for ML model training or deployment](#).
- [Deploy a model with an online endpoint](#).
- [High-performance serving with Triton Inference Server](#).

# Tutorial: Deploy Django app on AKS with Azure Database for PostgreSQL - Flexible Server

10/27/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO:  Azure Database for PostgreSQL - Flexible Server

In this quickstart, you deploy a Django application on Azure Kubernetes Service (AKS) cluster with Azure Database for PostgreSQL - Flexible Server using the Azure CLI.

**AKS** is a managed Kubernetes service that lets you quickly deploy and manage clusters. [Azure Database for PostgreSQL - Flexible Server](#) is a fully managed database service designed to provide more granular control and flexibility over database management functions and configuration settings.

## NOTE

This quickstart assumes a basic understanding of Kubernetes concepts, Django and PostgreSQL.

## Pre-requisites

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

- Launch [Azure Cloud Shell](#) in new browser window. You can [install Azure CLI](#) on your local machine too. If you're using a local install, login with Azure CLI by using the `az login` command. To finish the authentication process, follow the steps displayed in your terminal.
- Run `az version` to find the version and dependent libraries that are installed. To upgrade to the latest version, run [az upgrade](#). This article requires the latest version of Azure CLI. If you're using Azure Cloud Shell, the latest version is already installed.

## Create a resource group

An Azure resource group is a logical group in which Azure resources are deployed and managed. Let's create a resource group, *django-project* using the `az-group-create` command in the *eastus* location.

```
az group create --name django-project --location eastus
```

## NOTE

The location for the resource group is where resource group metadata is stored. It is also where your resources run in Azure if you don't specify another region during resource creation.

The following example output shows the resource group created successfully:

```
{
 "id": "/subscriptions/<guid>/resourceGroups/django-project",
 "location": "eastus",
 "managedBy": null,

 "name": "django-project",
 "properties": {
 "provisioningState": "Succeeded"
 },
 "tags": null
}
```

## Create AKS cluster

Use the [az aks create](#) command to create an AKS cluster. The following example creates a cluster named *djangoadappcluster* with one node. This will take several minutes to complete.

```
az aks create --resource-group django-project --name djangoadappcluster --node-count 1 --generate-ssh-keys
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

### NOTE

When creating an AKS cluster a second resource group is automatically created to store the AKS resources. See [Why are two resource groups created with AKS?](#)

## Connect to the cluster

To manage a Kubernetes cluster, you use [kubectl](#), the Kubernetes command-line client. If you use Azure Cloud Shell, `kubectl` is already installed.

### NOTE

If running Azure CLI locally, please run the [az aks install-cli](#) command to install `kubectl`.

To configure `kubectl` to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command. This command downloads credentials and configures the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group django-project --name djangoadappcluster
```

To verify the connection to your cluster, use the [kubectl get](#) command to return a list of the cluster nodes.

```
kubectl get nodes
```

The following example output shows the single node created in the previous steps. Make sure that the status of the node is *Ready*.

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-31718369-0	Ready	agent	6m44s	v1.12.8

# Create an Azure Database for PostgreSQL - Flexible Server

Create a flexible server with the [az postgres flexible-server create](#) command. The following command creates a server using service defaults and values from your Azure CLI's local context:

```
az postgres flexible-server create --public-access all
```

The server created has the below attributes:

- A new empty database, `postgres` is created when the server is first provisioned. In this quickstart we will use this database.
- Autogenerated server name, admin username, admin password, resource group name (if not already specified in local context), and in the same location as your resource group
- Using public-access argument allow you to create a server with public access to any client with correct username and password.
- Since the command is using local context it will create the server in the resource group `django-project` and in the region `eastus`.

## Build your Django docker image

Create a new [Django application](#) or use your existing Django project. Make sure your code is in this folder structure.

```
└── my-djangoapp
 ├── views.py
 ├── models.py
 ├── forms.py
 └── templates
 ...
 └── static
 ...
 └── ...
 └── my-django-project
 ├── settings.py
 ├── urls.py
 └── wsgi.py
 ...
 └── Dockerfile
 └── requirements.txt
 └── manage.py
```

Update `ALLOWED_HOSTS` in `settings.py` to make sure the Django application uses the external IP that gets assigned to kubernetes app.

```
ALLOWED_HOSTS = ['*']
```

Update `DATABASES={ }` section in the `settings.py` file. The code snippet below is reading the database host username and password from the Kubernetes manifest file.

```
DATABASES={
 'default':{
 'ENGINE':'django.db.backends.postgresql_psycopg2',
 'NAME':os.getenv('DATABASE_NAME'),
 'USER':os.getenv('DATABASE_USER'),
 'PASSWORD':os.getenv('DATABASE_PASSWORD'),
 'HOST':os.getenv('DATABASE_HOST'),
 'PORT':'5432',
 'OPTIONS': {'sslmode': 'require'}
 }
}
```

## Generate a requirements.txt file

Create a `requirements.txt` file to list out the dependencies for the Django Application. Here is an example `requirements.txt` file. You can use `pip freeze > requirements.txt` to generate a requirements.txt file for your existing application.

```
Django==2.2.17
postgres==3.0.0
psycopg2-binary==2.8.6
psycopg2-pool==1.1
pytz==2020.4
```

## Create a Dockerfile

Create a new file named `Dockerfile` and copy the code snippet below. This Dockerfile is setting up Python 3.8 and installing all the requirements listed in requirements.txt file.

```
Use the official Python image from the Docker Hub

FROM python:3.8.2

Make a new directory to put our code in.

RUN mkdir /code

Change the working directory.

WORKDIR /code

Copy to code folder

COPY . /code/

Install the requirements.

RUN pip install -r requirements.txt

Run the application:

CMD python manage.py runserver 0.0.0.0:8000
```

## Build your image

Make sure you're in the directory `my-django-app` in a terminal using the `cd` command. Run the following command to build your bulletin board image:

```
docker build --tag myblog:latest .
```

Deploy your image to [Docker hub](#) or [Azure Container registry](#).

#### IMPORTANT

If you are using Azure container registry (ACR), then run the `az aks update` command to attach ACR account with the AKS cluster.

```
az aks update -n djangoappcluster -g django-project --attach-acr <your-acr-name>
```

## Create Kubernetes manifest file

A Kubernetes manifest file defines a desired state for the cluster, such as what container images to run. Let's create a manifest file named `djangoapp.yaml` and copy in the following YAML definition.

#### IMPORTANT

Update `env` section below with your `SERVERNAME`, `YOUR-DATABASE-USERNAME`, `YOUR-DATABASE-PASSWORD` of your postgres flexible server.

```

apiVersion: apps/v1
kind: Deployment
metadata:
 name: django-app
spec:
 replicas: 1
 selector:
 matchLabels:
 app: django-app
 template:
 metadata:
 labels:
 app: django-app
 spec:
 containers:
 - name: django-app
 image: [DOCKER-HUB-USER-OR-ACR-ACCOUNT]/[YOUR-IMAGE-NAME]:[TAG]
 ports:
 - containerPort: 8000
 env:
 - name: DATABASE_HOST
 value: "SERVERNAME.postgres.database.azure.com"
 - name: DATABASE_USER
 value: "YOUR-DATABASE-USERNAME"
 - name: DATABASE_PASSWORD
 value: "YOUR-DATABASE-PASSWORD"
 - name: DATABASE_NAME
 value: "postgres"
 affinity:
 podAntiAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 - labelSelector:
 matchExpressions:
 - key: "app"
 operator: In
 values:
 - django-app
 topologyKey: "kubernetes.io/hostname"

apiVersion: v1
kind: Service
metadata:
 name: python-svc
spec:
 type: LoadBalancer
 ports:
 - protocol: TCP
 port: 80
 targetPort: 8000
 selector:
 app: django-app

```

## Deploy Django to AKS cluster

Deploy the application using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f djangoapp.yaml
```

The following example output shows the Deployments and Services created successfully:

```
deployment "django-app" created
service "python-svc" created
```

A deployment `django-app` allows you to describes details on of your deployment such as which images to use for the app, the number of pods and pod configuration. A service `python-svc` is created to expose the application through an external IP.

## Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete.

To monitor progress, use the `kubectl get service` command with the `--watch` argument.

```
kubectl get service python-svc --watch
```

Initially the *EXTERNAL-IP* for the *django-app* service is shown as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
django-app	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

When the *EXTERNAL-IP* address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
django-app LoadBalancer 10.0.37.27 52.179.23.131 80:30572/TCP 2m
```

Now open a web browser to the external IP address of your service (`http://<service-external-ip-address>`) and view the Django application.

### NOTE

- Currently the Django site is not using HTTPS. It is recommended to [ENABLE TLS with your own certificates](#).
- You can enable [HTTP routing](#) for your cluster. When http routing is enabled, it configures an Ingress controller in your AKS cluster. As > > applications are deployed, the solution also creates publicly accessible DNS names for application endpoints.

## Run database migrations

For any django application, you would need to run database migration or collect static files. You can run these django shell commands using `$ kubectl exec <pod-name> -- [COMMAND]`. Before running the command you need to find the pod name using `kubectl get pods`.

```
$ kubectl get pods
```

You will see an output like this:

NAME	READY	STATUS	RESTARTS	AGE
django-app-5d9cd6cd8-16x4b	1/1	Running	0	2m

Once the pod name has been found you can run django database migrations with the command

```
$ kubectl exec <pod-name> -- [COMMAND]. Note /code/ is the working directory for the project define in Dockerfile above.
```

```
$ kubectl exec django-app-5d9cd6cd8-16x4b -- python /code/manage.py migrate
```

The output would look like

```
Operations to perform:
 Apply all migrations: admin, auth, contenttypes, sessions
Running migrations:
 Applying contenttypes.0001_initial... OK
 Applying auth.0001_initial... OK
 Applying admin.0001_initial... OK
 Applying admin.0002_logentry_remove_auto_add... OK
 Applying admin.0003_logentry_add_action_flag_choices... OK

```

If you run into issues, please run `kubectl logs <pod-name>` to see what exception is thrown by your application. If the application is working successfully you would see an output like this when running `kubectl logs`.

```
Watching for file changes with StatReloader
Performing system checks...

System check identified no issues (0 silenced).

You have 17 unapplied migration(s). Your project may not work properly until you apply the migrations for
app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
December 08, 2020 - 23:24:14
Django version 2.2.17, using settings 'django_postgres_app.settings'
Starting development server at http://0.0.0.0:8000/
Quit the server with CONTROL-C.
```

## Clean up the resources

To avoid Azure charges, you should clean up unneeded resources. When the cluster is no longer needed, use the [az group delete](#) command to remove the resource group, container service, and all related resources.

```
az group delete --name django-project --yes --no-wait
```

### NOTE

When you delete the cluster, the Azure Active Directory service principal used by the AKS cluster is not removed. For steps on how to remove the service principal, see [AKS service principal considerations and deletion](#). If you used a managed identity, the identity is managed by the platform and does not require removal.

## Next steps

- Learn how to [access the Kubernetes web dashboard](#) for your AKS cluster
- Learn how to [enable continuous deployment](#)
- Learn how to [scale your cluster](#)
- Learn how to manage your [postgres flexible server](#)
- Learn how to [configure server parameters](#) for your database server.

# Deploy a Java application with Open Liberty or WebSphere Liberty on an Azure Kubernetes Service (AKS) cluster

10/27/2022 • 11 minutes to read • [Edit Online](#)

This article demonstrates how to:

- Run your Java, Java EE, Jakarta EE, or MicroProfile application on the Open Liberty or WebSphere Liberty runtime.
- Build the application Docker image using Open Liberty or WebSphere Liberty container images.
- Deploy the containerized application to an AKS cluster using the Open Liberty Operator.

The Open Liberty Operator simplifies the deployment and management of applications running on Kubernetes clusters. With the Open Liberty Operator, you can also perform more advanced operations, such as gathering traces and dumps.

For more information on Open Liberty, see [the Open Liberty project page](#). For more information on IBM WebSphere Liberty, see [the WebSphere Liberty product page](#).

This article uses the Azure Marketplace offer for Open/WebSphere Liberty to accelerate your journey to AKS. The offer automatically provisions a number of Azure resources including an Azure Container Registry (ACR) instance, an AKS cluster, an Azure App Gateway Ingress Controller (AGIC) instance, the Liberty Operator, and optionally a container image including Liberty and your application. To see the offer, visit the [Azure portal](#). If you prefer manual step-by-step guidance for running Liberty on AKS that doesn't utilize the automation enabled by the offer, see [Manually deploy a Java application with Open Liberty or WebSphere Liberty on an Azure Kubernetes Service \(AKS\) cluster](#).

If you don't have an [Azure subscription](#), create an [Azure free account](#) before you begin.

## Prerequisites

- Use the Bash environment in [Azure Cloud Shell](#). For more information, see [Azure Cloud Shell Quickstart - Bash](#).  
[Launch Cloud Shell](#)
- If you prefer to run CLI reference commands locally, [install](#) the Azure CLI. If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a Docker container](#).
  - If you're using a local installation, sign in to the Azure CLI by using the [az login](#) command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).
  - When you're prompted, install the Azure CLI extension on first use. For more information about extensions, see [Use extensions with the Azure CLI](#).
  - Run [az version](#) to find the version and dependent libraries that are installed. To upgrade to the latest version, run [az upgrade](#).
- This article requires at least version 2.31.0 of Azure CLI. If using Azure Cloud Shell, the latest version is already installed.
- If running the commands in this guide locally (instead of Azure Cloud Shell):

- Prepare a local machine with Unix-like operating system installed (for example, Ubuntu, macOS, Windows Subsystem for Linux).
- Install a Java SE implementation (for example, [Eclipse Open J9](#)).
- Install [Maven](#) 3.5.0 or higher.
- Install [Docker](#) for your OS.
- Make sure you have been assigned either the [Owner](#) role or the [Contributor](#) and [User Access Administrator](#) roles in the subscription. You can verify it by following steps in [List role assignments for a user or group](#).

## Create a Liberty on AKS deployment using the portal

The following steps guide you to create a Liberty runtime on AKS. After completing these steps, you'll have an Azure Container Registry and an Azure Kubernetes Service cluster for the sample application.

1. Visit the [Azure portal](#). In the search box at the top of the page, type *IBM WebSphere Liberty and Open Liberty on Azure Kubernetes Service*. When the suggestions start appearing, select the one and only match that appears in the **Marketplace** section. If you prefer, you can go directly to the offer with this shortcut link: <https://aka.ms/liberty-aks>.
2. Select **Create**.
3. In the **Basics** pane, create a new resource group. Because resource groups must be unique within a subscription, pick a unique name. An easy way to have unique names is to use a combination of your initials, today's date, and some identifier. For example, `ejb0913-java-liberty-project-rg`.
4. Select **East US** as **Region**.
5. Select **Next: Configure cluster**.
6. This section allows you to select an existing AKS cluster and Azure Container Registry (ACR), instead of causing the deployment to create a new one, if desired. This capability enables you to leverage the sidecar pattern, as shown in the [Azure architecture center](#). You can also adjust the settings for the size and number of the virtual machines in the AKS node pool. Leave all other values at the defaults and select **Next: Networking**.
7. Next to **Connect to Azure Application Gateway?** select **Yes**. This pane lets you customize the following deployment options.
  - a. You can customize the virtual network and subnet into which the deployment will place the resources. Leave these values at their defaults.
  - b. You can provide the TLS/SSL certificate presented by the Azure Application Gateway. Leave the values at the default to cause the offer to generate a self-signed certificate. Do not go to production using a self-certificate. For more information about self-signed certificates, see [Create a self-signed public certificate to authenticate your application](#).
  - c. You can enable cookie based affinity, also known as sticky sessions. We want this enabled for this article, so ensure this option is selected.



Enable cookie based affinity

8. Select **Review + create** to validate your selected options.
9. When you see the message **Validation Passed**, select **Create**. The deployment may take up to 20 minutes.

## Capture selected information from the deployment

If you navigated away from the **Deployment is in progress** page, the following steps will show you how to get back to that page. If you're still on the page that shows **Your deployment is complete**, you can skip to the third step.

1. In the upper left of any portal page, select the hamburger menu and select **Resource groups**.
2. In the box with the text **Filter for any field**, enter the first few characters of the resource group you created previously. If you followed the recommended convention, enter your initials, then select the appropriate resource group.
3. In the list of resources in the resource group, select the resource with **Type of Container registry**.
4. In the navigation pane, under **Settings** select **Access keys**.
5. Save aside the values for **Login server**, **Registry name**, **Username**, and **password**. You may use the copy icon at the right of each field to copy the value of that field to the system clipboard.
6. Navigate again to the resource group into which you deployed the resources.
7. In the **Settings** section, select **Deployments**.
8. Select the bottom-most deployment in the list. The **Deployment name** will match the publisher ID of the offer. It will contain the string **ibm**.
9. In the left pane, select **Outputs**.
10. Using the same copy technique as with the preceding values, save aside the values for the following outputs:
  - **appDeploymentTemplateYamlEncoded**
  - **cmdToConnectToCluster**

These values will be used later in this article. Note that several other useful commands are listed in the outputs.

## Create an Azure SQL Database

The following steps guide you through creating an Azure SQL Database single database for use with your app.

1. Create a single database in Azure SQL Database by following the steps in [Quickstart: Create an Azure SQL Database single database](#), carefully noting the differences in the box below. Return to this article after creating and configuring the database server.

## NOTE

At the Basics step, write down **Resource group**, **Database name**, <*server-name*>.database.windows.net, **Server admin login**, and **Password**. The database **Resource group** will be referred to as `<db-resource-group>` later in this article.

At the Networking step, set **Connectivity method** to **Public endpoint**, **Allow Azure services and resources to access this server** to **Yes**, and **Add current client IP address** to **Yes**.

Home > New > Azure SQL > Select SQL deployment option >

## Create SQL Database

Microsoft

Basics Networking Additional settings Tags Review + create

Configure network access and connectivity for your server. The configuration selected below will apply to the selected server 'jiangmasql' and all databases it manages. [Learn more](#)

**Network connectivity**

Choose an option for configuring connectivity to your server via public endpoint or private endpoint. Choosing no access creates with defaults and you can configure connection method after server creation. [Learn more](#)

Connectivity method \* ⓘ  No access  Public endpoint  Private endpoint

**Firewall rules**

Setting 'Allow Azure services and resources to access this server' to Yes allows communications from all resources inside the Azure boundary, that may or may not be part of your subscription. [Learn more](#)

Setting 'Add current client IP address' to Yes will add an entry for your client IP address to the server firewall.

Allow Azure services and resources to access this server \*  No  Yes

Add current client IP address \*  No  Yes

Also at the Networking step, under **Encrypted connections**, set the **Minimum TLS version** to **TLS 1.0**.

Encrypted connections

This server supports encrypted connections using Transport Layer Security (TLS). For information on TLS version and certificates, refer to connecting with TLS/SSL. [Learn more](#)

Minimum TLS version ⓘ

Now that the database and AKS cluster have been created, we can proceed to preparing AKS to host your Open Liberty application.

## Configure and deploy the sample application

Follow the steps in this section to deploy the sample application on the Liberty runtime. These steps use Maven and the `liberty-maven-plugin`. To learn more about the `liberty-maven-plugin` see [Building a web application with Maven](#).

### Check out the application

Clone the sample code for this guide. The sample is on [GitHub](#).

There are a few samples in the repository. We'll use `java-app/`. Here's the file structure of the application.

```
java-app
├─ src/main/
│ ├─ aks/
│ | ├─ db-secret.yaml
│ | ├─ openlibertyapplication.yaml
│ ├─ docker/
│ | ├─ Dockerfile
│ | ├─ Dockerfile-local
│ | ├─ Dockerfile-wlp
│ | └─ Dockerfile-wlp-local
│ ├─ liberty/config/
│ | ├─ server.xml
│ ├─ java/
│ ├─ resources/
│ └─ webapp/
└─ pom.xml
```

The directories *java*, *resources*, and *webapp* contain the source code of the sample application. The code declares and uses a data source named `jdbc/JavaEECafeDB`.

In the *aks* directory, we placed two deployment files. *db-secret.yaml* is used to create [Kubernetes Secrets](#) with DB connection credentials. The file *openlibertyapplication.yaml* is used to deploy the application image.

In the *docker* directory, we placed four Dockerfiles. *Dockerfile-local* is used for local debugging, and *Dockerfile* is used to build the image for an AKS deployment. These two files work with Open Liberty. *Dockerfile-wlp-local* and *Dockerfile-wlp* are also used for local debugging and to build the image for an AKS deployment respectively, but instead work with WebSphere Liberty.

In directory *liberty/config*, the *server.xml* FILE is used to configure the DB connection for the Open Liberty and WebSphere Liberty cluster.

### Acquire necessary variables from AKS deployment

After the offer is successfully deployed, an AKS cluster will be generated automatically. The AKS cluster is configured to connect to a generated ACR instance. Before we get started with the application, we need to extract the namespace configured for AKS.

1. Run the following command to print the current deployment file, using the

`appDeploymentTemplateYamlEncoded` you saved above. The output contains all the variables we need.

```
echo <appDeploymentTemplateYamlEncoded> | base64 -d
```

2. Save aside the `metadata.namespace` from this yaml output for later use in this article.

### Build the project

Now that you've gathered the necessary properties, you can build the application. The POM file for the project reads many properties from the environment.

Now that you've gathered the necessary properties, you can build the application. The POM file for the project reads many properties from the environment. The reason for this parameterization is to avoid having to hard-code values such as database server names, passwords, and other identifiers into the example source code. This allows the sample source code to be easier to use in a wider variety of contexts.

```
cd <path-to-your-repo>/java-app

The following variables will be used for deployment file generation
export LOGIN_SERVER=<Azure_Container_Registery_Login_Server_URL>
export REGISTRY_NAME=<Azure_Container_Registery_Name>
export USER_NAME=<Azure_Container_Registery_Username>
export PASSWORD=<Azure_Container_Registery_Password>
export DB_SERVER_NAME=<Server name>.database.windows.net
export DB_PORT_NUMBER=1433
export DB_NAME=<Database name>
export DB_USER=<Server admin login>@<Server name>
export DB_PASSWORD=<Server admin password>
export NAMESPACE=<metadata.namespace>

mvn clean install
```

## Test your project locally

Use the `liberty:devc` command to run and test the project locally before deploying to Azure. For more information on `liberty:devc`, see the [Liberty Plugin documentation](#). In the sample application, we've prepared `Dockerfile-local` and `Dockerfile-wlp-local` for use with `liberty:devc`.

1. Start your local docker environment if you haven't done so already. The instructions for doing this vary depending on the host operating system.
2. Start the application in `liberty:devc` mode

```
cd <path-to-your-repo>/java-app

If you're running with Open Liberty
mvn liberty:devc -Ddb.server.name=${DB_SERVER_NAME} -Ddb.port.number=${DB_PORT_NUMBER} -
Ddb.name=${DB_NAME} -Ddb.user=${DB_USER} -Ddb.password=${DB_PASSWORD} -Ddockerfile=target/Dockerfile-
local

If you're running with WebSphere Liberty
mvn liberty:devc -Ddb.server.name=${DB_SERVER_NAME} -Ddb.port.number=${DB_PORT_NUMBER} -
Ddb.name=${DB_NAME} -Ddb.user=${DB_USER} -Ddb.password=${DB_PASSWORD} -Ddockerfile=target/Dockerfile-
wlp-local
```

3. Verify the application works as expected. You should see a message similar to  
`[INFO] [AUDIT] CWWKZ0003I: The application javaee-cafe updated in 1.930 seconds.` in the command output if successful. Go to `http://localhost:9080/` in your browser and verify the application is accessible and all functions are working.
4. Press `Ctrl+C` to stop `liberty:devc` mode.

## Build image for AKS deployment

After successfully running the app in the Liberty Docker container, you can run the `docker build` command to build the image.

```

cd <path-to-your-repo>/java-app

Fetch maven artifactId as image name, maven build version as image version
export IMAGE_NAME=$(mvn -q -Dexec.executable=echo -Dexec.args='${project.artifactId}' --non-recursive
exec:exec)
export IMAGE_VERSION=$(mvn -q -Dexec.executable=echo -Dexec.args='${project.version}' --non-recursive
exec:exec)

cd <path-to-your-repo>/java-app/target

If you are running with Open Liberty
docker build -t ${IMAGE_NAME}:${IMAGE_VERSION} --pull --file=Dockerfile .

If you are running with WebSphere Liberty
docker build -t ${IMAGE_NAME}:${IMAGE_VERSION} --pull --file=Dockerfile-wlp .

```

## Upload image to ACR

Now, we upload the built image to the ACR created in the offer.

```

docker tag ${IMAGE_NAME}:${IMAGE_VERSION} ${LOGIN_SERVER}/${IMAGE_NAME}:${IMAGE_VERSION}
docker login -u ${USER_NAME} -p ${PASSWORD} ${LOGIN_SERVER}
docker push ${LOGIN_SERVER}/${IMAGE_NAME}:${IMAGE_VERSION}

```

## Deploy and test the application

The following steps deploy and test the application.

1. Connect to the AKS cluster.

Paste the value of **cmdToConnectToCluster** into a bash shell.

2. Apply the DB secret.

```

cd <path-to-your-repo>/java-app/target
kubectl apply -f db-secret.yaml

```

You'll see the output `secret/db-secret-postgres created`.

3. Apply the deployment file.

```

kubectl apply -f openlibertyapplication.yaml

```

4. Wait for the pods to be restarted.

Wait until all pods are restarted successfully using the following command.

```

kubectl get pods -n $NAMESPACE --watch

```

You should see output similar to the following to indicate that all the pods are running.

NAME	READY	STATUS	RESTARTS	AGE
javaee-cafe-cluster-67cdc95bc-2j2gr	1/1	Running	0	29s
javaee-cafe-cluster-67cdc95bc-fggtt8	1/1	Running	0	29s
javaee-cafe-cluster-67cdc95bc-h47qm	1/1	Running	0	29s

5. Verify the results.

- a. Get endpoint of the deployed service

```
kubectl get service -n $NAMESPACE
```

- b. Go to `http://EXTERNAL-IP` to test the application.

## Clean up resources

To avoid Azure charges, you should clean up unnecessary resources. When the cluster is no longer needed, use the [az group delete](#) command to remove the resource group, container service, container registry, and all related resources.

```
az group delete --name $RESOURCE_GROUP_NAME --yes --no-wait
az group delete --name <db-resource-group> --yes --no-wait
```

## Next steps

- [Azure Kubernetes Service](#)
- [Open Liberty](#)
- [Open Liberty Operator](#)
- [Open Liberty Server Configuration](#)

# Tutorial: Deploy WordPress app on AKS with Azure Database for MySQL - Flexible Server

10/27/2022 • 8 minutes to read • [Edit Online](#)

APPLIES TO:  Azure Database for MySQL - Flexible Server

In this quickstart, you deploy a WordPress application on Azure Kubernetes Service (AKS) cluster with Azure Database for MySQL - Flexible Server using the Azure CLI. [AKS](#) is a managed Kubernetes service that lets you quickly deploy and manage clusters. [Azure Database for MySQL - Flexible Server](#) is a fully managed database service designed to provide more granular control and flexibility over database management functions and configuration settings.

## NOTE

This quickstart assumes a basic understanding of Kubernetes concepts, WordPress and MySQL.

If you don't have an Azure subscription, create an [Azure free account](#) before you begin. With an Azure free account, you can now try Azure Database for MySQL - Flexible Server for free for 12 months. For more information, see [Try Flexible Server for free](#).

## Prerequisites

- Use the Bash environment in [Azure Cloud Shell](#). For more information, see [Azure Cloud Shell Quickstart - Bash](#). 
- If you prefer to run CLI reference commands locally, [install](#) the Azure CLI. If you're running on Windows or macOS, consider running Azure CLI in a Docker container. For more information, see [How to run the Azure CLI in a Docker container](#).
  - If you're using a local installation, sign in to the Azure CLI by using the [az login](#) command. To finish the authentication process, follow the steps displayed in your terminal. For other sign-in options, see [Sign in with the Azure CLI](#).
  - When you're prompted, install the Azure CLI extension on first use. For more information about extensions, see [Use extensions with the Azure CLI](#).
  - Run [az version](#) to find the version and dependent libraries that are installed. To upgrade to the latest version, run [az upgrade](#).
- This article requires the latest version of Azure CLI. If using Azure Cloud Shell, the latest version is already installed.

## NOTE

If running the commands in this quickstart locally (instead of Azure Cloud Shell), ensure you run the commands as administrator.

## Create a resource group

An Azure resource group is a logical group in which Azure resources are deployed and managed. Let's create a

resource group, *wordpress-project* using the `az group create`[`az-group-create`] command in the *eastus* location.

```
az group create --name wordpress-project --location eastus
```

#### NOTE

The location for the resource group is where resource group metadata is stored. It is also where your resources run in Azure if you don't specify another region during resource creation.

The following example output shows the resource group created successfully:

```
{
 "id": "/subscriptions/<guid>/resourceGroups/wordpress-project",
 "location": "eastus",
 "managedBy": null,
 "name": "wordpress-project",
 "properties": {
 "provisioningState": "Succeeded"
 },
 "tags": null
}
```

## Create AKS cluster

Use the `az aks create` command to create an AKS cluster. The following example creates a cluster named *myAKSCluster* with one node. This will take several minutes to complete.

```
az aks create --resource-group wordpress-project --name myAKScluster --node-count 1 --generate-ssh-keys
```

After a few minutes, the command completes and returns JSON-formatted information about the cluster.

#### NOTE

When creating an AKS cluster a second resource group is automatically created to store the AKS resources. See [Why are two resource groups created with AKS?](#)

## Connect to the cluster

To manage a Kubernetes cluster, you use `kubectl`, the Kubernetes command-line client. If you use Azure Cloud Shell, `kubectl` is already installed. To install `kubectl` locally, use the `az aks install-cli` command:

```
az aks install-cli
```

To configure `kubectl` to connect to your Kubernetes cluster, use the `az aks get-credentials` command. This command downloads credentials and configures the Kubernetes CLI to use them.

```
az aks get-credentials --resource-group wordpress-project --name myAKScluster
```

#### NOTE

The above command uses the default location for the [Kubernetes configuration file](#), which is `~/.kube/config`. You can specify a different location for your Kubernetes configuration file using `--file`.

To verify the connection to your cluster, use the [kubectl get](#) command to return a list of the cluster nodes.

```
kubectl get nodes
```

The following example output shows the single node created in the previous steps. Make sure that the status of the node is *Ready*:

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-31718369-0	Ready	agent	6m44s	v1.12.8

## Create an Azure Database for MySQL - Flexible Server

Create a flexible server with the [az mysql flexible-server create](#) command. The following command creates a server using service defaults and values from your Azure CLI's local context:

```
az mysql flexible-server create --public-access <YOUR-IP-ADDRESS>
```

The server created has the below attributes:

- A new empty database, `flexibleserverdb` is created when the server is first provisioned. In this quickstart we will use this database.
- Autogenerated server name, admin username, admin password, resource group name (if not already specified in local context), and in the same location as your resource group
- Service defaults for remaining server configurations: compute tier (Burstable), compute size/SKU (B1MS), backup retention period (7 days), and MySQL version (5.7)
- Using public-access argument allow you to create a server with public access protected by firewall rules. By providing your IP address to add the firewall rule to allow access from your client machine.
- Since the command is using Local context it will create the server in the resource group `wordpress-project` and in the region `eastus`.

## Build your WordPress docker image

Download the [latest WordPress](#) version. Create new directory `my-wordpress-app` for your project and use this simple folder structure

```

└──my-wordpress-app
 └──public
 ├──wp-admin
 | └──css
 . . .
 ├──wp-content
 | └──plugins
 . . .
 └──wp-includes
 . . .
 ├──wp-config-sample.php
 └──index.php
 . . .
 └──Dockerfile

```

Rename `wp-config-sample.php` to `wp-config.php` and replace lines from beginingin of

```
// ** MySQL settings - You can get this info from your web host ** // until the line
define('DB_COLLATE', '');
```

with the code snippet below. The code below is reading the database host, username and password from the Kubernetes manifest file.

```

//Using environment variables for DB connection information

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */

$connectstr_dbhost = getenv('DATABASE_HOST');
$connectstr_dbusername = getenv('DATABASE_USERNAME');
$connectstr_dbpassword = getenv('DATABASE_PASSWORD');
$connectst_dbname = getenv('DATABASE_NAME');

/** MySQL database name */
define('DB_NAME', $connectst_dbname);

/** MySQL database username */
define('DB_USER', $connectstr_dbusername);

/** MySQL database password */
define('DB_PASSWORD',$connectstr_dbpassword);

/** MySQL hostname */
define('DB_HOST', $connectstr_dbhost);

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/** SSL*/
define('MYSQL_CLIENT_FLAGS', MYSQLI_CLIENT_SSL);

```

## Create a Dockerfile

Create a new Dockerfile and copy this code snippet. This Dockerfile in setting up Apache web server with PHP and enabling mysqli extension.

```

FROM php:7.2-apache
COPY public/ /var/www/html/
RUN docker-php-ext-install mysqli
RUN docker-php-ext-enable mysqli

```

## Build your docker image

Make sure you're in the directory `my-wordpress-app` in a terminal using the `cd` command. Run the following command to build the image:

```
docker build --tag myblog:latest .
```

Deploy your image to [Docker hub](#) or [Azure Container registry](#).

### IMPORTANT

If you are using Azure container regdistry (ACR), then run the `az aks update` command to attach ACR account with the AKS cluster.

```
az aks update -n myAKSCluster -g wordpress-project --attach-acr <your-acr-name>
```

## Create Kubernetes manifest file

A Kubernetes manifest file defines a desired state for the cluster, such as what container images to run. Let's create a manifest file named `mywordpress.yaml` and copy in the following YAML definition.

### IMPORTANT

- Replace `[DOCKER-HUB-USER/ACR ACCOUNT]/[YOUR-IMAGE-NAME]:[TAG]` with your actual WordPress docker image name and tag, for example `docker-hub-user/myblog:latest`.
- Update `env` section below with your `SERVERNAME`, `YOUR-DATABASE-USERNAME`, `YOUR-DATABASE-PASSWORD` of your MySQL flexible server.

```

apiVersion: apps/v1
kind: Deployment
metadata:
 name: wordpress-blog
spec:
 replicas: 1
 selector:
 matchLabels:
 app: wordpress-blog
 template:
 metadata:
 labels:
 app: wordpress-blog
 spec:
 containers:
 - name: wordpress-blog
 image: [DOCKER-HUB-USER-OR-ACR-ACCOUNT]/[YOUR-IMAGE-NAME]:[TAG]
 ports:
 - containerPort: 80
 env:
 - name: DATABASE_HOST
 value: "SERVERNAME.mysql.database.azure.com" #Update here
 - name: DATABASE_USERNAME
 value: "YOUR-DATABASE-USERNAME" #Update here
 - name: DATABASE_PASSWORD
 value: "YOUR-DATABASE-PASSWORD" #Update here
 - name: DATABASE_NAME
 value: "flexibleserverdb"
 affinity:
 podAntiAffinity:
 requiredDuringSchedulingIgnoredDuringExecution:
 - labelSelector:
 matchExpressions:
 - key: "app"
 operator: In
 values:
 - wordpress-blog
 topologyKey: "kubernetes.io/hostname"

apiVersion: v1
kind: Service
metadata:
 name: php-svc
spec:
 type: LoadBalancer
 ports:
 - port: 80
 selector:
 app: wordpress-blog

```

## Deploy WordPress to AKS cluster

Deploy the application using the [kubectl apply](#) command and specify the name of your YAML manifest:

```
kubectl apply -f mywordpress.yaml
```

The following example output shows the Deployments and Services created successfully:

```
deployment "wordpress-blog" created
service "php-svc" created
```

## Test the application

When the application runs, a Kubernetes service exposes the application front end to the internet. This process can take a few minutes to complete.

To monitor progress, use the `kubectl get service` command with the `--watch` argument.

```
kubectl get service php-svc --watch
```

Initially the *EXTERNAL-IP* for the *wordpress-blog* service is shown as *pending*.

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
php-svc	LoadBalancer	10.0.37.27	<pending>	80:30572/TCP	6s

When the *EXTERNAL-IP* address changes from *pending* to an actual public IP address, use `CTRL-C` to stop the `kubectl` watch process. The following example output shows a valid public IP address assigned to the service:

```
php-svc LoadBalancer 10.0.37.27 52.179.23.131 80:30572/TCP 2m
```

## Browse WordPress

Open a web browser to the external IP address of your service to see your WordPress installation page.



## Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

### Information needed

Please provide the following information. Don't worry, you can always change these settings later.

**Site Title**

**Username**

Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

**Password**

  
Strong

Hide

**Important:** You will need this password to log in. Please store it in a secure location.

**Your Email**

Double-check your email address before continuing.

**Search Engine Visibility**

Discourage search engines from indexing this site  
It is up to search engines to honor this request.

[Install WordPress](#)

#### NOTE

- Currently the WordPress site is not using HTTPS. It is recommended to [ENABLE TLS with your own certificates](#).
- You can enable [HTTP routing](#) for your cluster.

## Clean up the resources

To avoid Azure charges, you should clean up unneeded resources. When the cluster is no longer needed, use the [az group delete](#) command to remove the resource group, container service, and all related resources.

```
az group delete --name wordpress-project --yes --no-wait
```

**NOTE**

When you delete the cluster, the Azure Active Directory service principal used by the AKS cluster is not removed. For steps on how to remove the service principal, see [AKS service principal considerations and deletion](#). If you used a managed identity, the identity is managed by the platform and does not require removal.

## Next steps

- Learn how to [access the Kubernetes web dashboard](#) for your AKS cluster
- Learn how to [scale your cluster](#)
- Learn how to manage your [MySQL flexible server](#)
- Learn how to [configure server parameters](#) for your database server.

# Use Azure API Management with microservices deployed in Azure Kubernetes Service

10/27/2022 • 7 minutes to read • [Edit Online](#)

Microservices are perfect for building APIs. With [Azure Kubernetes Service](#) (AKS), you can quickly deploy and operate a [microservices-based architecture](#) in the cloud. You can then leverage [Azure API Management](#) (API Management) to publish your microservices as APIs for internal and external consumption. This article describes the options of deploying API Management with AKS. It assumes basic knowledge of Kubernetes, API Management, and Azure networking.

## Background

When publishing microservices as APIs for consumption, it can be challenging to manage the communication between the microservices and the clients that consume them. There is a multitude of cross-cutting concerns such as authentication, authorization, throttling, caching, transformation, and monitoring. These concerns are valid regardless of whether the microservices are exposed to internal or external clients.

The [API Gateway](#) pattern addresses these concerns. An API gateway serves as a front door to the microservices, decouples clients from your microservices, adds an additional layer of security, and decreases the complexity of your microservices by removing the burden of handling cross cutting concerns.

[Azure API Management](#) is a turnkey solution to solve your API gateway needs. You can quickly create a consistent and modern gateway for your microservices and publish them as APIs. As a full-lifecycle API management solution, it also provides additional capabilities including a self-service developer portal for API discovery, API lifecycle management, and API analytics.

When used together, AKS and API Management provide a platform for deploying, publishing, securing, monitoring, and managing your microservices-based APIs. In this article, we will go through a few options of deploying AKS in conjunction with API Management.

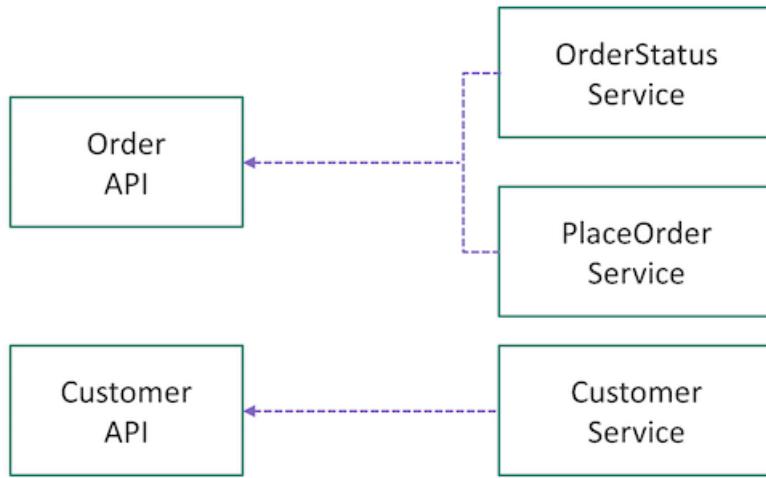
## Kubernetes Services and APIs

In a Kubernetes cluster, containers are deployed in [Pods](#), which are ephemeral and have a lifecycle. When a worker node dies, the Pods running on the node are lost. Therefore, the IP address of a Pod can change anytime. We cannot rely on it to communicate with the pod.

To solve this problem, Kubernetes introduced the concept of [Services](#). A Kubernetes Service is an abstraction layer which defines a logic group of Pods and enables external traffic exposure, load balancing and service discovery for those Pods.

When we are ready to publish our microservices as APIs through API Management, we need to think about how to map our Services in Kubernetes to APIs in API Management. There are no set rules. It depends on how you designed and partitioned your business capabilities or domains into microservices at the beginning. For instance, if the pods behind a Service are responsible for all operations on a given resource (e.g., Customer), the Service may be mapped to one API. If operations on a resource are partitioned into multiple microservices (e.g., GetOrder, PlaceOrder), then multiple Services may be logically aggregated into one single API in API management (See Fig. 1).

The mappings can also evolve. Since API Management creates a façade in front of the microservices, it allows us to refactor and right-size our microservices over time.



## Deploy API Management in front of AKS

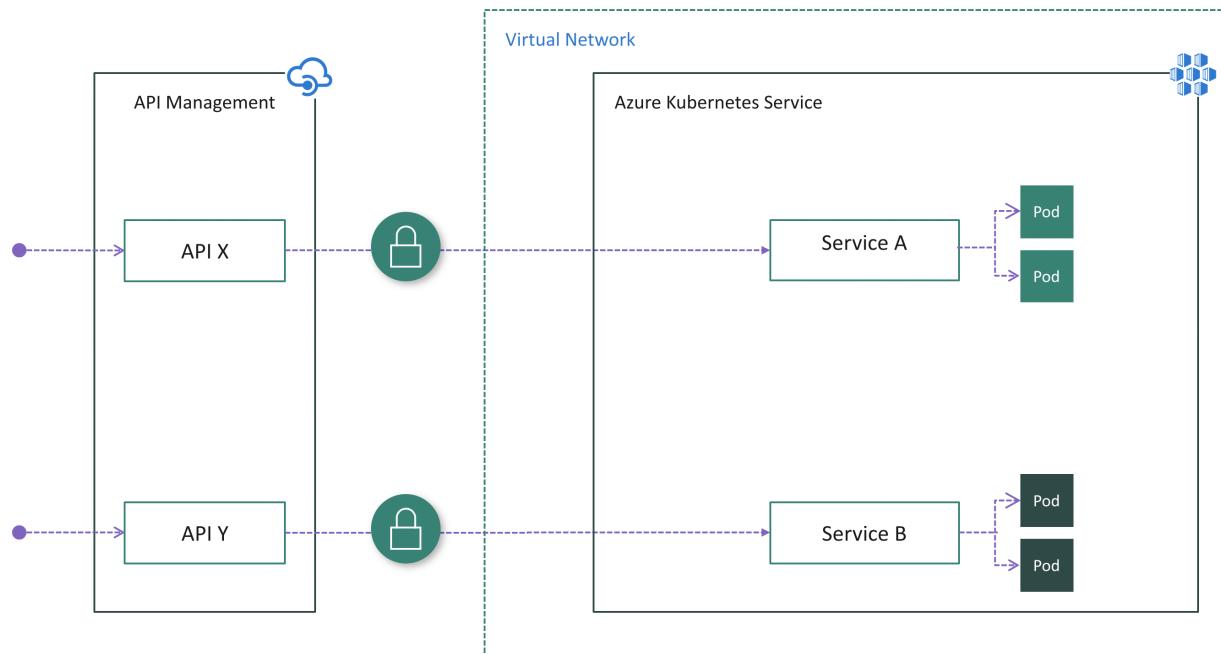
There are a few options of deploying API Management in front of an AKS cluster.

While an AKS cluster is always deployed in a virtual network (VNet), an API Management instance is not required to be deployed in a VNet. When API Management does not reside within the cluster VNet, the AKS cluster has to publish public endpoints for API Management to connect to. In that case, there is a need to secure the connection between API Management and AKS. In other words, we need to ensure the cluster can only be accessed exclusively through API Management. Let's go through the options.

### Option 1: Expose Services publicly

Services in an AKS cluster can be exposed publicly using [Service types](#) of NodePort, LoadBalancer, or ExternalName. In this case, Services are accessible directly from public internet. After deploying API Management in front of the cluster, we need to ensure all inbound traffic goes through API Management by applying authentication in the microservices. For instance, API Management can include an access token in each request made to the cluster. Each microservice is responsible for validating the token before processing the request.

This might be the easiest option to deploy API Management in front of AKS, especially if you already have authentication logic implemented in your microservices.



Pros:

- Easy configuration on the API Management side because it does not need to be injected into the cluster VNet
- No change on the AKS side if Services are already exposed publicly and authentication logic already exists in microservices

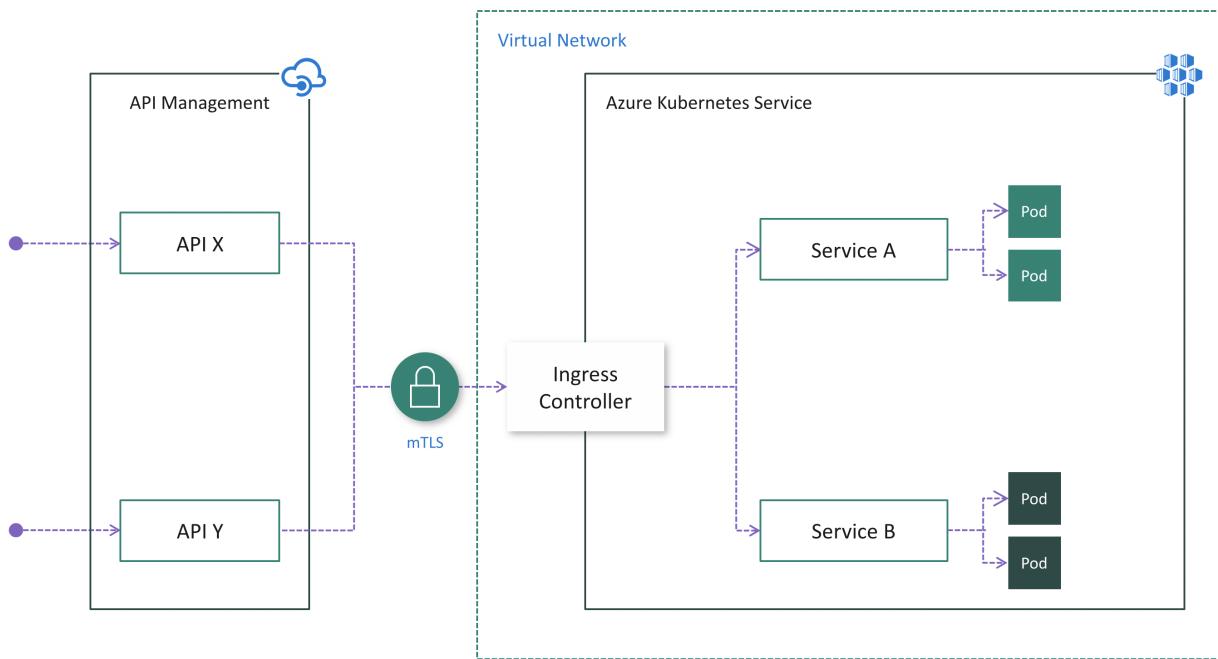
Cons:

- Potential security risk due to public visibility of endpoints
- No single-entry point for inbound cluster traffic
- Complicates microservices with duplicate authentication logic

### Option 2: Install an Ingress Controller

Although Option 1 might be easier, it has notable drawbacks as mentioned above. If an API Management instance does not reside in the cluster VNet, Mutual TLS authentication (mTLS) is a robust way of ensuring the traffic is secure and trusted in both directions between an API Management instance and an AKS cluster.

Mutual TLS authentication is [natively supported](#) by API Management and can be enabled in Kubernetes by [installing an Ingress Controller](#) (Fig. 3). As a result, authentication will be performed in the Ingress Controller, which simplifies the microservices. Additionally, you can add the IP addresses of API Management to the allowed list by Ingress to make sure only API Management has access to the cluster.



Pros:

- Easy configuration on the API Management side because it does not need to be injected into the cluster VNet and mTLS is natively supported
- Centralizes protection for inbound cluster traffic at the Ingress Controller layer
- Reduces security risk by minimizing publicly visible cluster endpoints

Cons:

- Increases complexity of cluster configuration due to extra work to install, configure and maintain the Ingress Controller and manage certificates used for mTLS
- Security risk due to public visibility of Ingress Controller endpoint(s)

When you publish APIs through API Management, it's easy and common to secure access to those APIs by using subscription keys. Developers who need to consume the published APIs must include a valid subscription key in HTTP requests when they make calls to those APIs. Otherwise, the calls are rejected immediately by the API

Management gateway. They aren't forwarded to the back-end services.

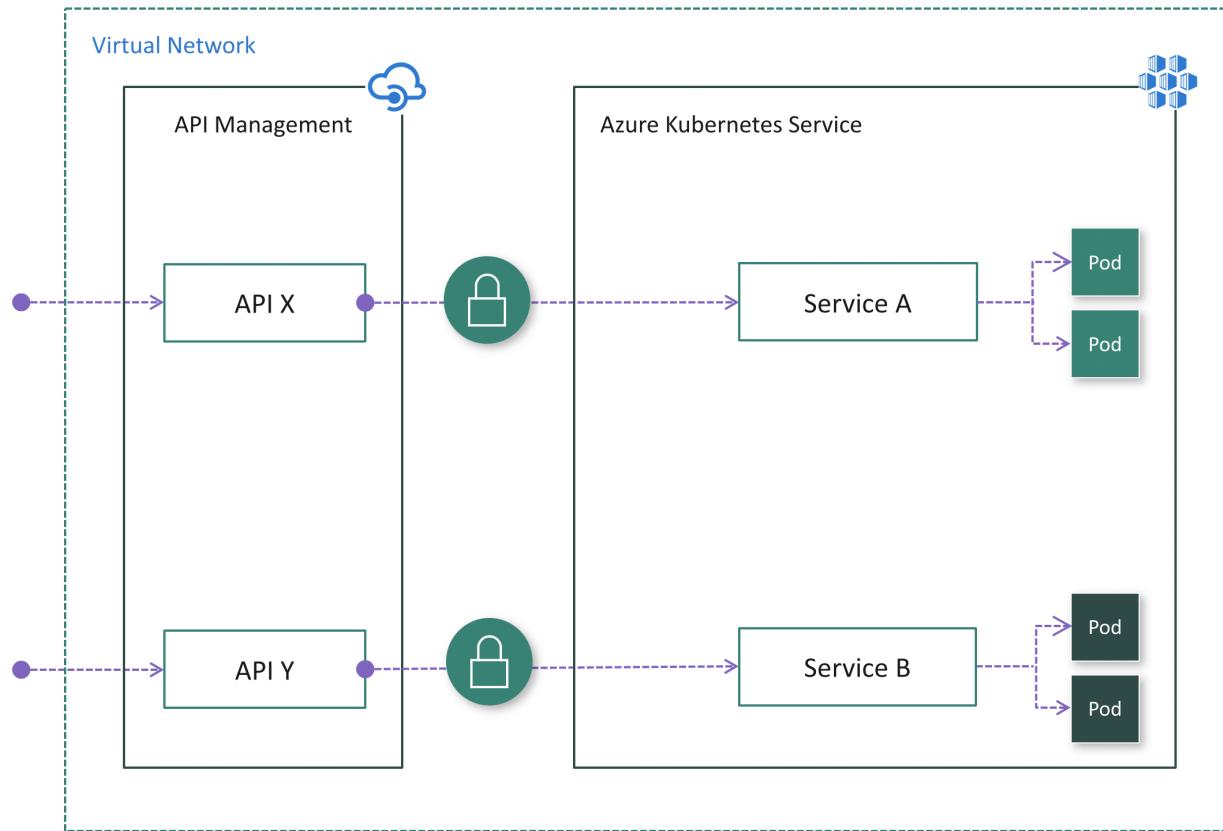
To get a subscription key for accessing APIs, a subscription is required. A subscription is essentially a named container for a pair of subscription keys. Developers who need to consume the published APIs can get subscriptions. And they don't need approval from API publishers. API publishers can also create subscriptions directly for API consumers.

### Option 3: Deploy APIM inside the cluster VNet

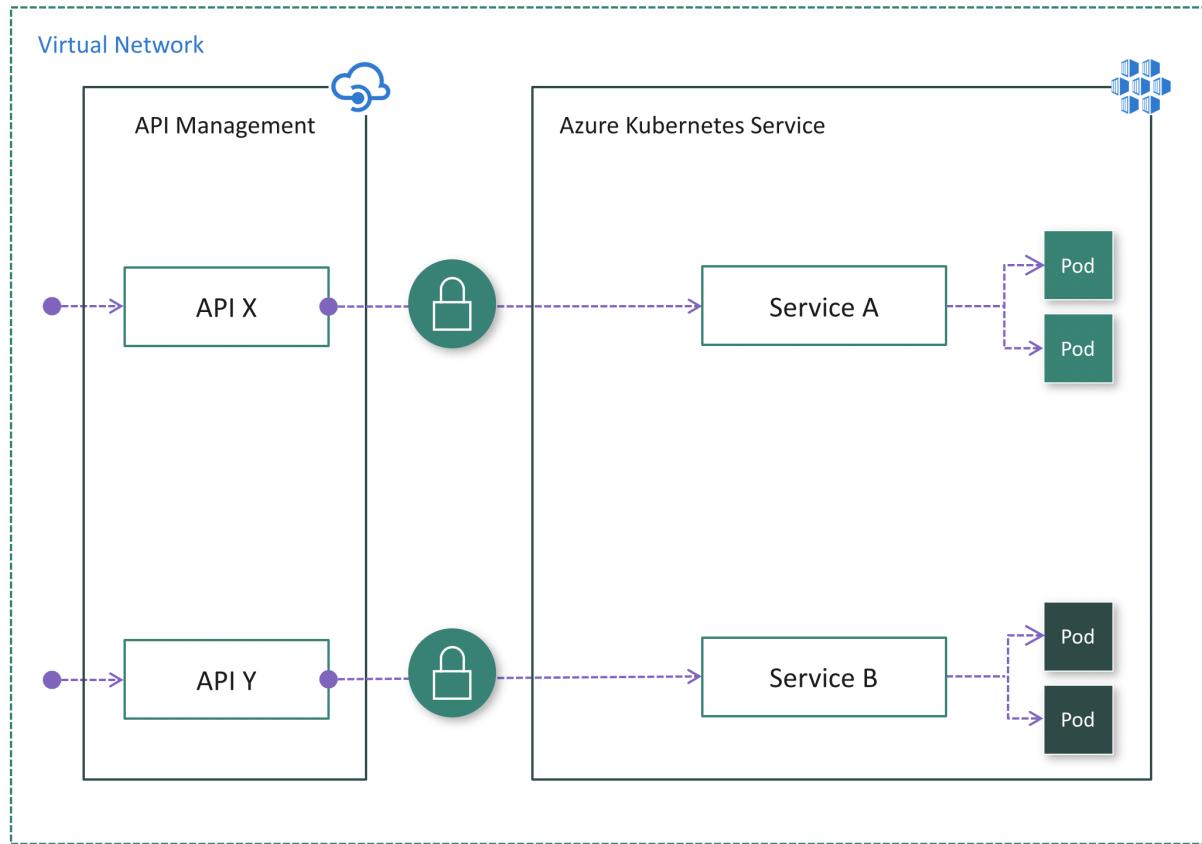
In some cases, customers with regulatory constraints or strict security requirements may find Option 1 and 2 not viable solutions due to publicly exposed endpoints. In others, the AKS cluster and the applications that consume the microservices might reside within the same VNet, hence there is no reason to expose the cluster publicly as all API traffic will remain within the VNet. For these scenarios, you can deploy API Management into the cluster VNet. [API Management Developer and Premium tiers](#) support VNet deployment.

There are two modes of [deploying API Management into a VNet](#) – External and Internal.

If API consumers do not reside in the cluster VNet, the External mode (Fig. 4) should be used. In this mode, the API Management gateway is injected into the cluster VNet but accessible from public internet via an external load balancer. It helps to hide the cluster completely while still allowing external clients to consume the microservices. Additionally, you can use Azure networking capabilities such as Network Security Groups (NSG) to restrict network traffic.



If all API consumers reside within the cluster VNet, then the Internal mode (Fig. 5) could be used. In this mode, the API Management gateway is injected into the cluster VNET and accessible only from within this VNet via an internal load balancer. There is no way to reach the API Management gateway or the AKS cluster from public internet.



In both cases, the AKS cluster is not publicly visible. Compared to Option 2, the Ingress Controller may not be necessary. Depending on your scenario and configuration, authentication might still be required between API Management and your microservices. For instance, if a Service Mesh is adopted, it always requires mutual TLS authentication.

Pros:

- The most secure option because the AKS cluster has no public endpoint
- Simplifies cluster configuration since it has no public endpoint
- Ability to hide both API Management and AKS inside the VNet using the Internal mode
- Ability to control network traffic using Azure networking capabilities such as Network Security Groups (NSG)

Cons:

- Increases complexity of deploying and configuring API Management to work inside the VNet

## Next steps

- Learn more about [Network concepts for applications in AKS](#)
- Learn more about [How to use API Management with virtual networks](#)

# Dapr extension for Azure Kubernetes Service (AKS) and Arc-enabled Kubernetes

10/27/2022 • 8 minutes to read • [Edit Online](#)

Dapr is a portable, event-driven runtime that simplifies building resilient, stateless, and stateful applications that run on the cloud and edge and embrace the diversity of languages and developer frameworks. Applying the benefits of a sidecar architecture, Dapr helps you tackle the challenges that come with building microservices and keeps your code platform agnostic. In particular, it helps solve problems around services:

- Calling other services reliably and securely
- Building event-driven apps with pub-sub
- Building applications that are portable across multiple cloud services and hosts (for example, Kubernetes vs. a VM)

By using the [Dapr extension to provision Dapr on your AKS or Arc-enabled Kubernetes cluster](#), you eliminate the overhead of downloading Dapr tooling and manually installing and managing the runtime on your AKS cluster. Additionally, the extension offers support for all [native Dapr configuration capabilities](#) through simple command-line arguments.

## NOTE

If you plan on installing Dapr in a Kubernetes production environment, see the [Dapr guidelines for production usage](#) documentation page.

## How it works

The Dapr extension uses the Azure CLI to provision the Dapr control plane on your AKS or Arc-enabled Kubernetes cluster. This will create:

- **dapr-operator**: Manages component updates and Kubernetes services endpoints for Dapr (state stores, pub/subs, etc.)
- **dapr-sidecar-injector**: Injects Dapr into annotated deployment pods and adds the environment variables `DAPR_HTTP_PORT` and `DAPR_GRPC_PORT` to enable user-defined applications to easily communicate with Dapr without hard-coding Dapr port values.
- **dapr-placement**: Used for actors only. Creates mapping tables that map actor instances to pods
- **dapr-sentry**: Manages mTLS between services and acts as a certificate authority. For more information, read the [security overview](#).

Once Dapr is installed on your cluster, you can begin to develop using the Dapr building block APIs by [adding a few annotations](#) to your deployments. For a more in-depth overview of the building block APIs and how to best use them, see the [Dapr building blocks overview](#).

## WARNING

If you install Dapr through the AKS or Arc-enabled Kubernetes extension, our recommendation is to continue using the extension for future management of Dapr instead of the Dapr CLI. Combining the two tools can cause conflicts and result in undesired behavior.

# Currently supported

## Dapr versions

The Dapr extension support varies depending on how you manage the runtime.

### Self-managed

For self-managed runtime, the Dapr extension supports:

- [The latest version of Dapr and two previous versions \(N-2\)](#)
- Upgrading minor version incrementally (for example, 1.5 -> 1.6 -> 1.7)

Self-managed runtime requires manual upgrade to remain in the support window. To upgrade Dapr via the extension, follow the [Update extension instance instructions](#).

### Auto-upgrade

Enabling auto-upgrade keeps your Dapr extension updated to the latest minor version. You may experience breaking changes between updates.

## Components

Azure + open source components are supported. Alpha and beta components are supported via best effort.

## Clouds/regions

Global Azure cloud is supported with Arc support on the following regions:

REGION	AKS SUPPORT	ARC FOR KUBERNETES SUPPORT
australiaeast	✓	✓
australiasoutheast	✓	✗
canadacentral	✓	✓
canadaeast	✓	✓
centralindia	✓	✓
centralus	✓	✓
eastasia	✓	✓
eastus	✓	✓
eastus2	✓	✓
eastus2euap	✗	✓
francecentral	✓	✓
germanywestcentral	✓	✓
japaneast	✓	✓
koreacentral	✓	✓

REGION	AKS SUPPORT	ARC FOR KUBERNETES SUPPORT
northcentralus	✓	✓
northeurope	✓	✓
norwayeast	✓	✗
southafricanorth	✓	✗
southcentralus	✓	✓
southeastasia	✓	✓
swedencentral	✓	✓
switzerlandnorth	✓	✓
uksouth	✓	✓
westcentralus	✓	✓
westeurope	✓	✓
westus	✓	✓
westus2	✓	✓
westus3	✓	✓

## Prerequisites

- If you don't have an Azure subscription, create a [free account](#) before you begin.
- Install the latest version of the [Azure CLI](#).
- If you don't have one already, you need to create an [AKS cluster](#) or connect an [Arc-enabled Kubernetes cluster](#).

### Set up the Azure CLI extension for cluster extensions

You'll need the `k8s-extension` Azure CLI extension. Install by running the following commands:

```
az extension add --name k8s-extension
```

If the `k8s-extension` extension is already installed, you can update it to the latest version using the following command:

```
az extension update --name k8s-extension
```

### Register the `KubernetesConfiguration` service provider

If you have not previously used cluster extensions, you may need to register the service provider with your

subscription. You can check the status of the provider registration using the [az provider list][az-provider-list] command, as shown in the following example:

```
az provider list --query "[?contains(namespace,'Microsoft.KubernetesConfiguration')]" -o table
```

The *Microsoft.KubernetesConfiguration* provider should report as *Registered*, as shown in the following example output:

Namespace	RegistrationState	RegistrationPolicy
Microsoft.KubernetesConfiguration	Registered	RegistrationRequired

If the provider shows as *NotRegistered*, register the provider using the [az provider register](#) as shown in the following example:

```
az provider register --namespace Microsoft.KubernetesConfiguration
```

## Create the extension and install Dapr on your AKS or Arc-enabled Kubernetes cluster

When installing the Dapr extension, use the flag value that corresponds to your cluster type:

- **AKS cluster:** `--cluster-type managedClusters`.
- **Arc-enabled Kubernetes cluster:** `--cluster-type connectedClusters`.

### NOTE

If you're using Dapr OSS on your AKS cluster and would like to install the Dapr extension for AKS, read more about [how to successfully migrate to the Dapr extension](#).

Create the Dapr extension, which installs Dapr on your AKS or Arc-enabled Kubernetes cluster. For example, for an AKS cluster:

```
az k8s-extension create --cluster-type managedClusters \
--cluster-name myAKSCluster \
--resource-group myResourceGroup \
--name myDaprExtension \
--extension-type Microsoft.Dapr
```

You have the option of allowing Dapr to auto-update its minor version by specifying the `--auto-upgrade-minor-version` parameter and setting the value to `true`:

```
--auto-upgrade-minor-version true
```

## Configuration settings

The extension enables you to set Dapr configuration options by using the `--configuration-settings` parameter. For example, to provision Dapr with high availability (HA) enabled, set the `global.ha.enabled` parameter to `true`:

```
az k8s-extension create --cluster-type managedClusters \
--cluster-name myAKSCluster \
--resource-group myResourceGroup \
--name myDaprExtension \
--extension-type Microsoft.Dapr \
--auto-upgrade-minor-version true \
--configuration-settings "global.ha.enabled=true" \
--configuration-settings "dapr_operator.replicaCount=2"
```

#### NOTE

If configuration settings are sensitive and need to be protected, for example cert related information, pass the `--configuration-protected-settings` parameter and the value will be protected from being read.

If no configuration-settings are passed, the Dapr configuration defaults to:

```
ha:
 enabled: true
 replicaCount: 3
 disruption:
 minimumAvailable: ""
 maximumUnavailable: "25%"
 prometheus:
 enabled: true
 port: 9090
 mTLS:
 enabled: true
 workloadCertTTL: 24h
 allowedClockSkew: 15m
```

For a list of available options, see [Dapr configuration](#).

## Targeting a specific Dapr version

#### NOTE

Dapr is supported with a rolling window, including only the current and previous versions. It is your operational responsibility to remain up to date with these supported versions. If you have an older version of Dapr, you may have to do intermediate upgrades to get to a supported version.

The same command-line argument is used for installing a specific version of Dapr or rolling back to a previous version. Set `--auto-upgrade-minor-version` to `false` and `--version` to the version of Dapr you wish to install. If the `version` parameter is omitted, the extension will install the latest version of Dapr. For example, to use Dapr X.X.X:

```
az k8s-extension create --cluster-type managedClusters \
--cluster-name myAKSCluster \
--resource-group myResourceGroup \
--name myDaprExtension \
--extension-type Microsoft.Dapr \
--auto-upgrade-minor-version false \
--version X.X.X
```

## Limiting the extension to certain nodes

In some configurations, you may only want to run Dapr on certain nodes. You can limit the extension by passing a `nodeSelector` in the extension configuration. If the desired `nodeSelector` contains `.`, you must escape them from the shell and the extension. For example, the following configuration will install Dapr to only nodes with `topology.kubernetes.io/zone: "us-east-1c"`:

```
az k8s-extension create --cluster-type managedClusters \
--cluster-name myAKSCluster \
--resource-group myResourceGroup \
--name myDaprExtension \
--extension-type Microsoft.Dapr \
--auto-upgrade-minor-version true \
--configuration-settings "global.ha.enabled=true" \
--configuration-settings "dapr_operator.replicaCount=2" \
--configuration-settings "global.nodeSelector.kubernetes\\.io/zone: us-east-1c"
```

For managing OS and architecture, use the [supported versions](#) of the `global.daprControlPlaneOs` and `global.daprControlPlaneArch` configuration:

```
az k8s-extension create --cluster-type managedClusters \
--cluster-name myAKSCluster \
--resource-group myResourceGroup \
--name myDaprExtension \
--extension-type Microsoft.Dapr \
--auto-upgrade-minor-version true \
--configuration-settings "global.ha.enabled=true" \
--configuration-settings "dapr_operator.replicaCount=2" \
--configuration-settings "global.daprControlPlaneOs=linux" \
--configuration-settings "global.daprControlPlaneArch=amd64"
```

## Show current configuration settings

Use the `az k8s-extension show` command to show the current Dapr configuration settings:

```
az k8s-extension show --cluster-type managedClusters \
--cluster-name myAKSCluster \
--resource-group myResourceGroup \
--name myDaprExtension
```

## Update configuration settings

### IMPORTANT

Some configuration options cannot be modified post-creation. Adjustments to these options require deletion and recreation of the extension, applicable to the following settings:

- `global.ha.*`
- `dapr_placement.*`

### NOTE

High availability (HA) can be enabled at any time. However, once enabled, disabling it requires deletion and recreation of the extension. If you aren't sure if high availability is necessary for your use case, we recommend starting with it disabled to minimize disruption.

To update your Dapr configuration settings, recreate the extension with the desired state. For example, assume we've previously created and installed the extension using the following configuration:

```
az k8s-extension create --cluster-type managedClusters \
--cluster-name myAKSCluster \
--resource-group myResourceGroup \
--name myDaprExtension \
--extension-type Microsoft.Dapr \
--auto-upgrade-minor-version true \
--configuration-settings "global.ha.enabled=true" \
--configuration-settings "dapr_operator.replicaCount=2"
```

To update the `dapr_operator.replicaCount` from two to three, use the following command:

```
az k8s-extension create --cluster-type managedClusters \
--cluster-name myAKSCluster \
--resource-group myResourceGroup \
--name myDaprExtension \
--extension-type Microsoft.Dapr \
--auto-upgrade-minor-version true \
--configuration-settings "global.ha.enabled=true" \
--configuration-settings "dapr_operator.replicaCount=3"
```

## Set the outbound proxy for Dapr extension for Azure Arc on-prem

If you want to use an outbound proxy with the Dapr extension for AKS, you can do so by:

1. Setting the proxy environment variables using the [dapr.io/env](#) annotations:
  - `HTTP_PROXY`
  - `HTTPS_PROXY`
  - `NO_PROXY`
2. [Installing the proxy certificate in the sidecar](#).

## Meet network requirements

The Dapr extension for AKS and Arc for Kubernetes requires outbound URLs on <https://:443> to function. In addition to the <https://mcr.microsoft.com/daprio> URL for pulling Dapr artifacts, verify you've included the [outbound URLs required for AKS or Arc for Kubernetes](#).

## Troubleshooting extension errors

If the extension fails to create or update, try suggestions and solutions in the [Dapr extension troubleshooting guide](#).

### Troubleshooting Dapr

Troubleshoot Dapr errors via the [common Dapr issues and solutions guide](#).

## Delete the extension

If you need to delete the extension and remove Dapr from your AKS cluster, you can use the following command:

```
az k8s-extension delete --resource-group myResourceGroup --cluster-name myAKSCluster --cluster-type \
managedClusters --name myDaprExtension
```

## Next Steps

- Once you have successfully provisioned Dapr in your AKS cluster, try deploying a [sample application](#).

# Migrate from Dapr OSS to the Dapr extension for Azure Kubernetes Service (AKS)

10/27/2022 • 2 minutes to read • [Edit Online](#)

You've installed and configured Dapr OSS on your Kubernetes cluster and want to migrate to the Dapr extension on AKS. Before you can successfully migrate to the Dapr extension, you need to fully remove Dapr OSS from your AKS cluster. In this guide, you will migrate from Dapr OSS by:

- Uninstalling Dapr, including CRDs and the `dapr-system` namespace
- Installing Dapr via the Dapr extension for AKS
- Applying your components
- Restarting your applications that use Dapr

## NOTE

Expect downtime of approximately 10 minutes while migrating to Dapr extension for AKS. Downtime may take longer depending on varying factors. During this downtime, no Dapr functionality should be expected to run.

## Uninstall Dapr

- [Dapr CLI](#)
- [Helm](#)

1. Run the following command to uninstall Dapr and all CRDs:

```
dapr uninstall -k --all
```

1. Uninstall the Dapr namespace:

```
kubectl delete namespace dapr-system
```

## NOTE

`dapr-system` is the default namespace installed with `dapr init -k`. If you created a custom namespace, replace `dapr-system` with your namespace.

## Register the `KubernetesConfiguration` service provider

If you have not previously used cluster extensions, you may need to register the service provider with your subscription. You can check the status of the provider registration using the `[az provider list][az-provider-list]` command, as shown in the following example:

```
az provider list --query "[?contains(namespace,'Microsoft.KubernetesConfiguration')]" -o table
```

The `Microsoft.KubernetesConfiguration` provider should report as *Registered*, as shown in the following

example output:

Namespace	RegistrationState	RegistrationPolicy
Microsoft.KubernetesConfiguration	Registered	RegistrationRequired

If the provider shows as *NotRegistered*, register the provider using the [az provider register][az-provider-register] as shown in the following example:

```
az provider register --namespace Microsoft.KubernetesConfiguration
```

## Install Dapr via the AKS extension

Once you've uninstalled Dapr from your system, install the [Dapr extension for AKS and Arc-enabled Kubernetes](#).

```
az k8s-extension create --cluster-type managedClusters \
--cluster-name <dapr-cluster-name> \
--resource-group <dapr-resource-group> \
--name <dapr-ext> \
--extension-type Microsoft.Dapr
```

## Apply your components

```
kubectl apply -f <component.yaml>
```

## Restart your applications that use Dapr

Restarting the deployment will create a new sidecar from the new Dapr installation.

```
kubectl rollout restart <deployment-name>
```

## Next steps

Learn more about [the cluster extension](#) and [how to use it](#).

# Troubleshoot Dapr extension installation errors

10/27/2022 • 2 minutes to read • [Edit Online](#)

This article details some common error messages you may encounter while installing the Dapr extension for Azure Kubernetes Service (AKS) or Arc for Kubernetes.

## Installation failure without an error message

If the extension fails to create or update without an error message, you can inspect where the creation of the extension failed by running the `az k8s-extension list` command. For example, if a wrong key is used in the configuration-settings, such as `global.ha=false` instead of `global.ha.enabled=false`:

```
az k8s-extension list --cluster-type managedClusters --cluster-name myCluster --resource-group
myResourceGroup
```

The below JSON is returned, and the error message is captured in the `message` property.

```
"statuses": [
 {
 "code": "InstallationFailed",
 "displayStatus": null,
 "level": null,
 "message": "Error: {failed to install chart from path [] for release [dapr-1]: err [template:
dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_poddisruptionbudget.yaml:1:17: executing
\\"dapr/charts/dapr_sidecar_injector/templates/dapr_sidecar_injector_poddisruptionbudget.yaml\\\" at
<.Values.global.ha.enabled>: can't evaluate field enabled in type interface {}]} occurred while doing the
operation : {Installing the extension} on the config",
 "time": null
 }
,
```

Another example:

```
az k8s-extension list --cluster-type managedClusters --cluster-name myCluster --resource-group
myResourceGroup
```

```
"statuses": [
 {
 "code": "InstallationFailed",
 "displayStatus": null,
 "level": null,
 "message": "The extension operation failed with the following error: unable to add the configuration
with configId {extension:microsoft-dapr} due to error: {error while adding the CRD configuration: error
{failed to get the immutable configMap from the elevated namespace with err: configmaps 'extension-
immutable-values' not found }}. (Code: ExtensionOperationFailed)",
 "time": null
 }
,
```

For these cases, possible remediation actions are to:

- [Restart your AKS or Arc for Kubernetes cluster.](#)
- Make sure you've [registered the KubernetesConfiguration service provider](#).

- Force delete and [reinstall the Dapr extension](#).

See below for examples of error messages you may encounter during Dapr extension install or update.

## Error: Dapr version doesn't exist

You're installing the Dapr extension and [targeting a specific version](#), but run into an error message saying the Dapr version doesn't exist.

```
(ExtensionOperationFailed) The extension operation failed with the following error: Failed to resolve the extension version from the given values.
Code: ExtensionOperationFailed
Message: The extension operation failed with the following error: Failed to resolve the extension version from the given values.
```

Try installing again, making sure to use a [supported version of Dapr](#).

## Error: Dapr version exists, but not in the mentioned region

Some versions of Dapr aren't available in all regions. If you receive an error message like the following, try installing in an [available region](#) where your Dapr version is supported.

```
(ExtensionTypeRegistrationGetFailed) Extension type microsoft.dapr is not registered in region <regionname>.
Code: ExtensionTypeRegistrationGetFailed
Message: Extension type microsoft.dapr is not registered in region <regionname>
```

## Error: `dapr-system` already exists

You're installing the Dapr extension for AKS or Arc for Kubernetes, but receive an error message indicating that Dapr already exists. This error message may look like:

```
(ExtensionOperationFailed) The extension operation failed with the following error: Error: {failed to install chart from path [] for release [dapr-ext]: err [rendered manifests contain a resource that already exists. Unable to continue with install: ServiceAccount "dapr-operator" in namespace "dapr-system" exists and cannot be imported into the current release: invalid ownership metadata; annotation validation error: key "meta.helm.sh/release-name" must equal "dapr-ext": current value is "dapr"]}} occurred while doing the operation : {Installing the extension} on the config
```

You need to uninstall Dapr OSS before installing the Dapr extension. For more information, read [Migrate from Dapr OSS](#).

## Next steps

If you're still running into issues, explore the [AKS troubleshooting guide](#) and the [Dapr OSS troubleshooting guide](#).

# Tutorial: Use GitOps with Flux v2 in Azure Arc-enabled Kubernetes or AKS clusters

10/27/2022 • 31 minutes to read • [Edit Online](#)

GitOps with Flux v2 can be enabled in Azure Kubernetes Service (AKS) managed clusters or Azure Arc-enabled Kubernetes connected clusters as a cluster extension. After the `microsoft.flux` cluster extension is installed, you can create one or more `fluxConfigurations` resources that sync your Git repository sources to the cluster and reconcile the cluster to the desired state. With GitOps, you can use your Git repository as the source of truth for cluster configuration and application deployment.

## NOTE

Eventually Azure will stop supporting GitOps with Flux v1, so begin using Flux v2 as soon as possible.

This tutorial describes how to use GitOps in a Kubernetes cluster. Before you dive in, take a moment to [learn how GitOps with Flux works conceptually](#).

## IMPORTANT

The `microsoft.flux` extension released major version 1.0.0. This includes the [multi-tenancy feature](#). If you have existing GitOps Flux v2 configurations that use a previous version of the `microsoft.flux` extension you can upgrade to the latest extension manually using the Azure CLI: "az k8s-extension create -g <RESOURCE\_GROUP> -c <CLUSTER\_NAME> -n flux --extension-type microsoft.flux -t <CLUSTER\_TYPE>" (use "-t connectedClusters" for Arc clusters and "-t managedClusters" for AKS clusters).

## TIP

When using this extension with [AKS hybrid clusters provisioned from Azure](#) you must set `--cluster-type` to use `provisionedClusters` and also add `--cluster-resource-provider microsoft.hybridcontainerservice` to the command. Installing Azure Arc extensions on AKS hybrid clusters provisioned from Azure is currently in preview.

## Prerequisites

To manage GitOps through the Azure CLI or the Azure portal, you need the following:

### For Azure Arc-enabled Kubernetes clusters

- An Azure Arc-enabled Kubernetes connected cluster that's up and running.

[Learn how to connect a Kubernetes cluster to Azure Arc](#). If you need to connect through an outbound proxy, then assure you [install the Arc agents with proxy settings](#).

- Read and write permissions on the `Microsoft.Kubernetes/connectedClusters` resource type.

### For Azure Kubernetes Service clusters

- An MSI-based AKS cluster that's up and running.

## IMPORTANT

Ensure that the AKS cluster is created with MSI (not SPN), because the `microsoft.flux` extension won't work with SPN-based AKS clusters. For new AKS clusters created with "az aks create", the cluster will be MSI-based by default. For already created SPN-based clusters that need to be converted to MSI run "az aks update -g \$RESOURCE\_GROUP -n \$CLUSTER\_NAME --enable-managed-identity". For more information, refer to [managed identity docs](#).

- Read and write permissions on the `Microsoft.ContainerService/managedClusters` resource type.
- Registration of your subscription with the `AKS-ExtensionManager` feature flag. Use the following command:

```
az feature register --namespace Microsoft.ContainerService --name AKS-ExtensionManager
```

## Common to both cluster types

- Read and write permissions on these resource types:
  - `Microsoft.KubernetesConfiguration/extensions`
  - `Microsoft.KubernetesConfiguration/fluxConfigurations`
- Azure CLI version 2.15 or later. [Install the Azure CLI](#) or use the following commands to update to the latest version:

```
az version
az upgrade
```

- Registration of the following Azure service providers. (It's OK to re-register an existing provider.)

```
az provider register --namespace Microsoft.Kubernetes
az provider register --namespace Microsoft.ContainerService
az provider register --namespace Microsoft.KubernetesConfiguration
```

Registration is an asynchronous process and should finish within 10 minutes. Use the following code to monitor the registration process:

```
az provider show -n Microsoft.KubernetesConfiguration -o table

Namespace RegistrationPolicy RegistrationState

Microsoft.KubernetesConfiguration RegistrationRequired Registered
```

## Version and region support

GitOps is currently supported in [all regions that Azure Arc-enabled Kubernetes supports](#). GitOps is currently supported in a subset of the regions that AKS supports. The GitOps service is adding new supported regions on a regular cadence.

The most recent version of the Flux v2 extension and the two previous versions (N-2) are supported. We generally recommend that you use the most recent version of the extension.

## Network requirements

The GitOps agents require outbound (egress) TCP to the repo source on either port 22 (SSH) or port 443 (HTTPS) to function. The agents also require the following outbound URLs:

ENDPOINT (DNS)	DESCRIPTION
<code>https://management.azure.com</code>	Required for the agent to communicate with the Kubernetes Configuration service.
<code>https://&lt;region&gt;.dp.kubernetesconfiguration.azure.com</code>	Data plane endpoint for the agent to push status and fetch configuration information. Depends on <code>&lt;region&gt;</code> (the supported regions mentioned earlier).
<code>https://login.microsoftonline.com</code>	Required to fetch and update Azure Resource Manager tokens.
<code>https://mcr.microsoft.com</code>	Required to pull container images for Flux controllers.

## Enable CLI extensions

### NOTE

The `k8s-configuration` CLI extension manages either Flux v2 or Flux v1 configurations. Eventually Azure will stop supporting GitOps with Flux v1, so begin using Flux v2 as soon as possible.

Install the latest `k8s-configuration` and `k8s-extension` CLI extension packages:

```
az extension add -n k8s-configuration
az extension add -n k8s-extension
```

To update these packages, use the following commands:

```
az extension update -n k8s-configuration
az extension update -n k8s-extension
```

To see the list of az CLI extensions installed and their versions, use the following command:

```
az extension list -o table

 Experimental ExtensionType Name Path
 Preview Version
 ----- -----
 False whl connectedk8s C:\Users\somename\.azure\cliextensions\connectedk8s
 False 1.2.7
 False whl k8s-configuration C:\Users\somename\.azure\cliextensions\k8s-
 configuration False 1.5.0
 False whl k8s-extension C:\Users\somename\.azure\cliextensions\k8s-extension
 False 1.1.0
```

### TIP

For help resolving any errors, see the Flux v2 suggestions in [Azure Arc-enabled Kubernetes and GitOps troubleshooting](#).

## Apply a Flux configuration by using the Azure CLI

Use the `k8s-configuration` Azure CLI extension (or the Azure portal) to enable GitOps in an AKS or Arc-enabled Kubernetes cluster. For a demonstration, use the public [gitops-flux2-kustomize-helm-mt](#) repository.

## IMPORTANT

The demonstration repo is designed to simplify your use of this tutorial and illustrate some key principles. To keep up to date, the repo can get breaking changes occasionally from version upgrades. These changes won't affect your new application of this tutorial, only previous tutorial applications that have not been deleted. To learn how to handle these changes please see the [breaking change disclaimer](#).

In the following example:

- The resource group that contains the cluster is `flux-demo-rg`.
- The name of the Azure Arc cluster is `flux-demo-arc`.
- The cluster type is Azure Arc (`-t connectedClusters`), but this example also works with AKS (`-t managedClusters`).
- The name of the Flux configuration is `cluster-config`.
- The namespace for configuration installation is `cluster-config`.
- The URL for the public Git repository is `https://github.com/Azure/gitops-flux2-kustomize-helm-mt`.
- The Git repository branch is `main`.
- The scope of the configuration is `cluster`. This gives the operators permissions to make changes throughout cluster. To use `namespace` scope with this tutorial, [see the changes needed](#).
- Two kustomizations are specified with names `infra` and `apps`. Each is associated with a path in the repository.
- The `apps` kustomization depends on the `infra` kustomization. (The `infra` kustomization must finish before the `apps` kustomization runs.)
- Set `prune=true` on both kustomizations. This setting assures that the objects that Flux deployed to the cluster will be cleaned up if they're removed from the repository or if the Flux configuration or kustomizations are deleted.

If the `microsoft.flux` extension isn't already installed in the cluster, it'll be installed. When the flux configuration is installed, the initial compliance state may be "Pending" or "Non-compliant" because reconciliation is still on-going. After a minute, you can query the configuration again and see the final compliance state.

```
az k8s-configuration flux create -g flux-demo-rg \
-c flux-demo-arc \
-n cluster-config \
--namespace cluster-config \
-t connectedClusters \
--scope cluster \
-u https://github.com/Azure/gitops-flux2-kustomize-helm-mt \
--branch main \
--kustomization name=infra path=./infrastructure prune=true \
--kustomization name=apps path=./apps/staging prune=true dependsOn\["infra"\]

'Microsoft.Flux' extension not found on the cluster, installing it now. This may take a few minutes...
'Microsoft.Flux' extension was successfully installed on the cluster
Creating the flux configuration 'cluster-config' in the cluster. This may take a few minutes...
{
 "complianceState": "Pending",
 ... (not shown because of pending status)
}
```

Show the configuration after allowing time to finish reconciliations.

```
az k8s-configuration flux show -g flux-demo-rg -c flux-demo-arc -n cluster-config -t connectedClusters \
{
 "bucket": null,
 "complianceState": "Compliant",
 "configurationProtectedSettings": {},
 "errorMessage": ""
}
```

```
"gitRepository": {
 "httpsCaCert": null,
 "httpsUser": null,
 "localAuthRef": null,
 "repositoryRef": {
 "branch": "main",
 "commit": null,
 "semver": null,
 "tag": null
 },
 "sshKnownHosts": null,
 "syncIntervalInSeconds": 600,
 "timeoutInSeconds": 600,
 "url": "https://github.com/Azure/gitops-flux2-kustomize-helm-mt"
},
"id": "/subscriptions/REDACTED/resourceGroups/flux-demo-
rg/providers/Microsoft.Kubernetes/connectedClusters/flux-demo-
arc/providers/Microsoft.KubernetesConfiguration/fluxConfigurations/cluster-config",
"kustomizations": {
 "apps": {
 "dependsOn": [
 "infra"
],
 "force": false,
 "name": "apps",
 "path": "./apps/staging",
 "prune": true,
 "retryIntervalInSeconds": null,
 "syncIntervalInSeconds": 600,
 "timeoutInSeconds": 600
 },
 "infra": {
 "dependsOn": null,
 "force": false,
 "name": "infra",
 "path": "./infrastructure",
 "prune": true,
 "retryIntervalInSeconds": null,
 "syncIntervalInSeconds": 600,
 "timeoutInSeconds": 600
 }
},
"name": "cluster-config",
"namespace": "cluster-config",
"provisioningState": "Succeeded",
"repositoryPublicKey": "",
"resourceGroup": "Flux2-Test-RG-EUS",
"scope": "cluster",
"sourceKind": "GitRepository",
"sourceSyncedCommitId": "main/4f1bdad4d0a54b939a5e3d52c51464f67e474fcf",
"sourceUpdatedAt": "2022-04-06T17:34:03+00:00",
"statusUpdatedAt": "2022-04-06T17:44:56.417000+00:00",
"statuses": [
{
 "appliedBy": null,
 "complianceState": "Compliant",
 "helmReleaseProperties": null,
 "kind": "GitRepository",
 "name": "cluster-config",
 "namespace": "cluster-config",
 "statusConditions": [
 {
 "lastTransitionTime": "2022-04-06T17:33:32+00:00",
 "message": "Fetched revision: main/4f1bdad4d0a54b939a5e3d52c51464f67e474fcf",
 "reason": "GitOperationSucceed",
 "status": "True",
 "type": "Ready"
 }
]
},
{
 "appliedBy": null,
```

```
"complianceState": "Compliant",
"helmReleaseProperties": null,
"kind": "Kustomization",
"name": "cluster-config-apps",
"namespace": "cluster-config",
"statusConditions": [
{
 "lastTransitionTime": "2022-04-06T17:44:04+00:00",
 "message": "Applied revision: main/4f1bdad4d0a54b939a5e3d52c51464f67e474fcf",
 "reason": "ReconciliationSucceeded",
 "status": "True",
 "type": "Ready"
}
],
},
{
 "appliedBy": {
 "name": "cluster-config-apps",
 "namespace": "cluster-config"
 },
 "complianceState": "Compliant",
 "helmReleaseProperties": {
 "failureCount": 0,
 "helmChartRef": {
 "name": "cluster-config-podinfo",
 "namespace": "cluster-config"
 },
 "installFailureCount": 0,
 "lastRevisionApplied": 1,
 "upgradeFailureCount": 0
 },
 "kind": "HelmRelease",
 "name": "podinfo",
 "namespace": "cluster-config",
 "statusConditions": [
 {
 "lastTransitionTime": "2022-04-06T17:33:43+00:00",
 "message": "Release reconciliation succeeded",
 "reason": "ReconciliationSucceeded",
 "status": "True",
 "type": "Ready"
 },
 {
 "lastTransitionTime": "2022-04-06T17:33:43+00:00",
 "message": "Helm install succeeded",
 "reason": "InstallSucceeded",
 "status": "True",
 "type": "Released"
 }
]
},
{
 "appliedBy": null,
 "complianceState": "Compliant",
 "helmReleaseProperties": null,
 "kind": "Kustomization",
 "name": "cluster-config-infra",
 "namespace": "cluster-config",
 "statusConditions": [
 {
 "lastTransitionTime": "2022-04-06T17:43:33+00:00",
 "message": "Applied revision: main/4f1bdad4d0a54b939a5e3d52c51464f67e474fcf",
 "reason": "ReconciliationSucceeded",
 "status": "True",
 "type": "Ready"
 }
]
},
{
 "appliedBy": {
 "name": "cluster-config-infra",
 "namespace": "cluster-config"
 }
```

```
 },
 "complianceState": "Compliant",
 "helmReleaseProperties": null,
 "kind": "HelmRepository",
 "name": "bitnami",
 "namespace": "cluster-config",
 "statusConditions": [
 {
 "lastTransitionTime": "2022-04-06T17:33:36+00:00",
 "message": "Fetched revision: 46a41610ea410558eb485bcb673fd01c4d1f47b86ad292160b256555b01cce81",
 "reason": "IndexationSucceed",
 "status": "True",
 "type": "Ready"
 }
]
 },
 {
 "appliedBy": {
 "name": "cluster-config-infra",
 "namespace": "cluster-config"
 },
 "complianceState": "Compliant",
 "helmReleaseProperties": null,
 "kind": "HelmRepository",
 "name": "podinfo",
 "namespace": "cluster-config",
 "statusConditions": [
 {
 "lastTransitionTime": "2022-04-06T17:33:33+00:00",
 "message": "Fetched revision: 421665ba04fab9b275b9830947417b2cebf67764eee46d568c94cf2a95a6341d",
 "reason": "IndexationSucceed",
 "status": "True",
 "type": "Ready"
 }
]
 },
 {
 "appliedBy": {
 "name": "cluster-config-infra",
 "namespace": "cluster-config"
 },
 "complianceState": "Compliant",
 "helmReleaseProperties": {
 "failureCount": 0,
 "helmChartRef": {
 "name": "cluster-config-nginx",
 "namespace": "cluster-config"
 },
 "installFailureCount": 0,
 "lastRevisionApplied": 1,
 "upgradeFailureCount": 0
 },
 "kind": "HelmRelease",
 "name": "nginx",
 "namespace": "cluster-config",
 "statusConditions": [
 {
 "lastTransitionTime": "2022-04-06T17:34:13+00:00",
 "message": "Release reconciliation succeeded",
 "reason": "ReconciliationSucceeded",
 "status": "True",
 "type": "Ready"
 },
 {
 "lastTransitionTime": "2022-04-06T17:34:13+00:00",
 "message": "Helm install succeeded",
 "reason": "InstallSucceeded",
 "status": "True",
 "type": "Released"
 }
]
 },
}
```

```

{
 "appliedBy": {
 "name": "cluster-config-infra",
 "namespace": "cluster-config"
 },
 "complianceState": "Compliant",
 "helmReleaseProperties": {
 "failureCount": 0,
 "helmChartRef": {
 "name": "cluster-config-redis",
 "namespace": "cluster-config"
 },
 "installFailureCount": 0,
 "lastRevisionApplied": 1,
 "upgradeFailureCount": 0
 },
 "kind": "HelmRelease",
 "name": "redis",
 "namespace": "cluster-config",
 "statusConditions": [
 {
 "lastTransitionTime": "2022-04-06T17:33:57+00:00",
 "message": "Release reconciliation succeeded",
 "reason": "ReconciliationSucceeded",
 "status": "True",
 "type": "Ready"
 },
 {
 "lastTransitionTime": "2022-04-06T17:33:57+00:00",
 "message": "Helm install succeeded",
 "reason": "InstallSucceeded",
 "status": "True",
 "type": "Released"
 }
]
},
{
 "appliedBy": {
 "name": "cluster-config-infra",
 "namespace": "cluster-config"
 },
 "complianceState": "Compliant",
 "helmReleaseProperties": null,
 "kind": "HelmChart",
 "name": "test-chart",
 "namespace": "cluster-config",
 "statusConditions": [
 {
 "lastTransitionTime": "2022-04-06T17:33:40+00:00",
 "message": "Pulled 'redis' chart with version '11.3.4'.",
 "reason": "ChartPullSucceeded",
 "status": "True",
 "type": "Ready"
 }
]
},
{
 "suspend": false,
 "systemData": {
 "createdAt": "2022-04-06T17:32:44.646629+00:00",
 "createdBy": null,
 "createdByType": null,
 "lastModifiedAt": "2022-04-06T17:32:44.646629+00:00",
 "lastModifiedBy": null,
 "lastModifiedByType": null
 },
 "type": "Microsoft.KubernetesConfiguration/fluxConfigurations"
}

```

These namespaces were created:

- `flux-system` : Holds the Flux extension controllers.
- `cluster-config` : Holds the Flux configuration objects.
- `nginx` , `podinfo` , `redis` : Namespaces for workloads described in manifests in the Git repository.

```
kubectl get namespaces
```

The `flux-system` namespace contains the Flux extension objects:

- Azure Flux controllers: `fluxconfig-agent` , `fluxconfig-controller`
- OSS Flux controllers: `source-controller` , `kustomize-controller` , `helm-controller` , `notification-controller`

The Flux agent and controller pods should be in a running state.

```
kubectl get pods -n flux-system
```

NAME	READY	STATUS	RESTARTS	AGE
fluxconfig-agent-9554ffb65-jqm8g	2/2	Running	0	21m
fluxconfig-controller-9d99c54c8-nztg8	2/2	Running	0	21m
helm-controller-59cc74dbc5-77772	1/1	Running	0	21m
kustomize-controller-5fb7d7b9d5-cjdhx	1/1	Running	0	21m
notification-controller-7d45678bc-fvlvr	1/1	Running	0	21m
source-controller-df7dc97cd-4drh2	1/1	Running	0	21m

The namespace `cluster-config` has the Flux configuration objects.

```
kubectl get crds
```

NAME	CREATED AT
alerts.notification.toolkit.fluxcd.io	2022-04-06T17:15:48Z
arccertificates.clusterconfig.azure.com	2022-03-28T21:45:19Z
azureclusteridentityrequests.clusterconfig.azure.com	2022-03-28T21:45:19Z
azureextensionidentities.clusterconfig.azure.com	2022-03-28T21:45:19Z
buckets.source.toolkit.fluxcd.io	2022-04-06T17:15:48Z
connectedclusters.arc.azure.com	2022-03-28T21:45:19Z
customlocationsettings.clusterconfig.azure.com	2022-03-28T21:45:19Z
extensionconfigs.clusterconfig.azure.com	2022-03-28T21:45:19Z
fluxconfigs.clusterconfig.azure.com	2022-04-06T17:15:48Z
gitconfigs.clusterconfig.azure.com	2022-03-28T21:45:19Z
gitrepositories.source.toolkit.fluxcd.io	2022-04-06T17:15:48Z
helmcharts.source.toolkit.fluxcd.io	2022-04-06T17:15:48Z
helmreleases.helm.toolkit.fluxcd.io	2022-04-06T17:15:48Z
helmrerepositories.source.toolkit.fluxcd.io	2022-04-06T17:15:48Z
imagepolicies.image.toolkit.fluxcd.io	2022-04-06T17:15:48Z
imagerepositories.image.toolkit.fluxcd.io	2022-04-06T17:15:48Z
imageupdateautomations.image.toolkit.fluxcd.io	2022-04-06T17:15:48Z
kustomizations.kustomize.toolkit.fluxcd.io	2022-04-06T17:15:48Z
providers.notification.toolkit.fluxcd.io	2022-04-06T17:15:48Z
receivers.notification.toolkit.fluxcd.io	2022-04-06T17:15:48Z
volumesnapshotclasses.snapshot.storage.k8s.io	2022-03-28T21:06:12Z
volumesnapshotcontents.snapshot.storage.k8s.io	2022-03-28T21:06:12Z
volumesnapshots.snapshot.storage.k8s.io	2022-03-28T21:06:12Z
websites.extensions.example.com	2022-03-30T23:42:32Z

```
kubectl get fluxconfigs -A
```

NAMESPACE	NAME	SCOPE	URL
PROVISION AGE			
cluster-config Succeeded 44m	cluster-config	cluster	<a href="https://github.com/Azure/gitops-flux2-kustomize-helm-mt">https://github.com/Azure/gitops-flux2-kustomize-helm-mt</a>

```
kubectl get gitrepositories -A
```

NAMESPACE	NAME	URL	READY	STATUS
AGE				
cluster-config	cluster-config	https://github.com/Azure/gitops-flux2-kustomize-helm-mt	True	Fetched revision: main/4f1bdad4d0a54b939a5e3d52c51464f67e474fcf 45m

```
kubectl get helmreleases -A
```

NAMESPACE	NAME	READY	STATUS	AGE
cluster-config	nginx	True	Release reconciliation succeeded	66m
cluster-config	podinfo	True	Release reconciliation succeeded	66m
cluster-config	redis	True	Release reconciliation succeeded	66m

```
kubectl get kustomizations -A
```

NAMESPACE	NAME	READY	STATUS	AGE
AGE				
cluster-config	cluster-config-apps	True	Applied revision: main/4f1bdad4d0a54b939a5e3d52c51464f67e474fcf 65m	
cluster-config	cluster-config-infra	True	Applied revision: main/4f1bdad4d0a54b939a5e3d52c51464f67e474fcf 65m	

Workloads are deployed from manifests in the Git repository.

```
kubectl get deploy -n nginx
```

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
nginx-ingress-controller	1/1	1	1	67m
nginx-ingress-controller-default-backend	1/1	1	1	67m

```
kubectl get deploy -n podinfo
```

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
podinfo	1/1	1	1	68m

```
kubectl get all -n redis
```

NAME	READY	STATUS	RESTARTS	AGE
pod/redis-master-0	1/1	Running	0	68m

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
service/redis-headless	ClusterIP	None	<none>	6379/TCP	68m
service/redis-master	ClusterIP	10.0.13.182	<none>	6379/TCP	68m

NAME	READY	AGE
statefulset.apps/redis-master	1/1	68m

## Delete the Flux configuration

You can delete the Flux configuration by using the following command. This action deletes both the `fluxConfigurations` resource in Azure and the Flux configuration objects in the cluster. Because the Flux configuration was originally created with the `prune=true` parameter for the kustomization, all of the objects created in the cluster based on manifests in the Git repository will be removed when the Flux configuration is removed.

```
az k8s-configuration flux delete -g flux-demo-rg -c flux-demo-arc -n cluster-config -t connectedClusters --yes
```

For an AKS cluster, use the same command but with `-t managedClusters` replacing `-t connectedClusters`.

Note that this action does *not* remove the Flux extension.

## Delete the Flux cluster extension

You can delete the Flux extension by using either the CLI or the portal. The delete action removes both the `microsoft.flux` extension resource in Azure and the Flux extension objects in the cluster.

If the Flux extension was created automatically when the Flux configuration was first created, the extension name will be `flux`.

For an Azure Arc-enabled Kubernetes cluster, use this command:

```
az k8s-extension delete -g flux-demo-rg -c flux-demo-arc -n flux -t connectedClusters --yes
```

For an AKS cluster, use the same command but with `-t managedClusters` replacing `-t connectedClusters`.

## Control which controllers are deployed with the Flux cluster extension

The `source`, `helm`, `kustomize`, and `notification` Flux controllers are installed by default. The `image-automation` and `image-reflector` controllers must be enabled explicitly. You can use the `k8s-extension` CLI to make those choices:

- `--config source-controller.enabled=<true/false>` (default `true`)
- `--config helm-controller.enabled=<true/false>` (default `true`)
- `--config kustomize-controller.enabled=<true/false>` (default `true`)
- `--config notification-controller.enabled=<true/false>` (default `true`)
- `--config image-automation-controller.enabled=<true/false>` (default `false`)
- `--config image-reflector-controller.enabled=<true/false>` (default `false`)

Here's an example for including the [Flux image-reflector and image-automation controllers](#). If the Flux extension was created automatically when a Flux configuration was first created, the extension name will be `flux`.

```
az k8s-extension create -g <cluster_resource_group> -c <cluster_name> -t <connectedClusters or
managedClusters> --name flux --extension-type microsoft.flux --config image-automation-
controller.enabled=true image-reflector-controller.enabled=true
```

## Using Kubelet identity as authentication method for Azure Kubernetes Clusters

When working with Azure Kubernetes clusters, one of the authentication options to use is kubelet identity. In order to let Flux use this, add a parameter `--config useKubeletIdentity=true` at the time of Flux extension installation.

```
az k8s-extension create --resource-group <resource-group> --cluster-name <cluster-name> --cluster-type
managedClusters --name flux --extension-type microsoft.flux --config useKubeletIdentity=true
```

## Red Hat OpenShift onboarding guidance

Flux controllers require a nonroot [Security Context Constraint](#) to properly provision pods on the cluster. These constraints must be added to the cluster prior to onboarding of the `microsoft.flux` extension.

```
NS="flux-system"
oc adm policy add-scc-to-user nonroot system:serviceaccount:$NS:kustomize-controller
oc adm policy add-scc-to-user nonroot system:serviceaccount:$NS:helm-controller
oc adm policy add-scc-to-user nonroot system:serviceaccount:$NS:source-controller
oc adm policy add-scc-to-user nonroot system:serviceaccount:$NS:notification-controller
oc adm policy add-scc-to-user nonroot system:serviceaccount:$NS:image-automation-controller
oc adm policy add-scc-to-user nonroot system:serviceaccount:$NS:image-reflector-controller
```

For more information on OpenShift guidance for onboarding Flux, refer to the [Flux documentation](#).

# Work with parameters

For a description of all parameters that Flux supports, see the [official Flux documentation](#). Flux in Azure doesn't support all parameters yet. Let us know if a parameter you need is missing from the Azure implementation.

You can see the full list of parameters that the `k8s-configuration flux` CLI command supports by using the `-h` parameter:

```
az k8s-configuration flux -h

Group
 az k8s-configuration flux : Commands to manage Flux v2 Kubernetes configurations.

Subgroups:
 deployed-object : Commands to see deployed objects associated with Flux v2 Kubernetes
 configurations.
 kustomization : Commands to manage Kustomizations associated with Flux v2 Kubernetes
 configurations.

Commands:
 create : Create a Flux v2 Kubernetes configuration.
 delete : Delete a Flux v2 Kubernetes configuration.
 list : List all Flux v2 Kubernetes configurations.
 show : Show a Flux v2 Kubernetes configuration.
 update : Update a Flux v2 Kubernetes configuration.
```

Here are the parameters for the `k8s-configuration flux create` CLI command:

```
az k8s-configuration flux create -h

This command is from the following extension: k8s-configuration

Command
 az k8s-configuration flux create : Create a Flux v2 Kubernetes configuration.

Arguments
 --cluster-name -c [Required] : Name of the Kubernetes cluster.
 --cluster-type -t [Required] : Specify Arc connected clusters or AKS managed clusters.
 Allowed values: connectedClusters, managedClusters.
 --name -n [Required] : Name of the flux configuration.
 --resource-group -g [Required] : Name of resource group. You can configure the default group
 using `az configure --defaults group=<name>`.
 --url -u [Required] : URL of the source to reconcile.
 --bucket-insecure : Communicate with a bucket without TLS. Allowed values: false,
 true.
 --bucket-name : Name of the S3 bucket to sync.
 --container-name : Name of the Azure Blob Storage container to sync
 --interval --sync-interval : Time between reconciliations of the source on the cluster.
 --kind : Source kind to reconcile. Allowed values: bucket, git, azblob.
 Default: git.
 --kustomization -k : Define kustomizations to sync sources with parameters ['name',
 'path', 'depends_on', 'timeout', 'sync_interval',
 'retry_interval', 'prune', 'force'].
 --namespace --ns : Namespace to deploy the configuration. Default: default.
 --no-wait : Do not wait for the long-running operation to finish.
 --scope -s : Specify scope of the operator to be 'namespace' or 'cluster'.
 Allowed values: cluster, namespace. Default: cluster.
 --suspend : Suspend the reconciliation of the source and kustomizations
 associated with this configuration. Allowed values: false,
 true.
 --timeout : Maximum time to reconcile the source before timing out.

Auth Arguments
 --local-auth-ref --local-ref : Local reference to a kubernetes secret in the configuration
 namespace to use for communication to the source.

Bucket Auth Arguments
 --bucket-access-key : Access Key ID used to authenticate with the bucket.
```

--bucket-secret-key	: Secret Key used to authenticate with the bucket.
<b>Git Auth Arguments</b>	
--https-ca-cert	: Base64-encoded HTTPS CA certificate for TLS communication with private repository sync.
--https-ca-cert-file	: File path to HTTPS CA certificate file for TLS communication with private repository sync.
--https-key	: HTTPS token/password for private repository sync.
--https-user	: HTTPS username for private repository sync.
--known-hosts	: Base64-encoded known_hosts data containing public SSH keys required to access private Git instances.
--known-hosts-file	: File path to known_hosts contents containing public SSH keys required to access private Git instances.
--ssh-private-key	: Base64-encoded private ssh key for private repository sync.
--ssh-private-key-file	: File path to private ssh key for private repository sync.
<b>Git Repo Ref Arguments</b>	
--branch	: Branch within the git source to reconcile with the cluster.
--commit	: Commit within the git source to reconcile with the cluster.
--semver	: Semver range within the git source to reconcile with the cluster.
--tag	: Tag within the git source to reconcile with the cluster.
<b>Global Arguments</b>	
--debug	: Increase logging verbosity to show all debug logs.
--help -h	: Show this help message and exit.
--only-show-errors	: Only show errors, suppressing warnings.
--output -o	: Output format. Allowed values: json, jsonc, none, table, tsv, yaml, yamlc. Default: json.
--query	: JMESPath query string. See <a href="http://jmespath.org/">http://jmespath.org/</a> for more information and examples.
--subscription	: Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.
--verbose	: Increase logging verbosity. Use --debug for full debug logs.
<b>Azure Blob Storage Account Auth Arguments</b>	
--sp_client_id	: The client ID for authenticating a service principal with Azure Blob, required for this authentication method
--sp_tenant_id	: The tenant ID for authenticating a service principal with Azure Blob, required for this authentication method
--sp_client_secret	: The client secret for authenticating a service principal with Azure Blob
--sp_client_cert	: The Base64 encoded client certificate for authenticating a service principal with Azure Blob
--sp_client_cert_password	: The password for the client certificate used to authenticate a service principal with Azure Blob
--sp_client_cert_send_chain	: Specifies whether to include x5c header in client claims when acquiring a token to enable subject name / issuer based authentication for the client certificate
--account_key	: The Azure Blob Shared Key for authentication
--sas_token	: The Azure Blob SAS Token for authentication
--mi_client_id	: The client ID of the managed identity for authentication with Azure Blob
<b>Examples</b>	
Create a Flux v2 Kubernetes configuration	
az k8s-configuration flux create --resource-group my-resource-group \ --cluster-name mycluster --cluster-type connectedClusters \ --name myconfig --scope cluster --namespace my-namespace \ --kind git --url https://github.com/Azure/arc-k8s-demo \ --branch main --kustomization name=my-kustomization	
Create a Kubernetes v2 Flux Configuration with Bucket Source Kind	
az k8s-configuration flux create --resource-group my-resource-group \ --cluster-name mycluster --cluster-type connectedClusters \ --name myconfig --scope cluster --namespace my-namespace \ --kind bucket --url https://bucket-provider.minio.io \ --bucket-name my-bucket --kustomization name=my-kustomization \ --bucket-access-key my-access-key --bucket-secret-key my-secret-key	
Create a Kubernetes v2 Flux Configuration with Azure Blob Storage Source Kind	
az k8s-configuration flux create --resource-group my-resource-group \ --cluster-name mvcluster --cluster-type connectedClusters \ --name myconfig --scope cluster --namespace my-namespace \ --kind blobstorage --url https://my-blobstorage.blob.core.windows.net \ --blobstorage-name my-blobstorage --kustomization name=my-kustomization	

```
--cluster-name my-cluster --cluster-type connectedClusters \
--name myconfig --scope cluster --namespace my-namespace \
--kind azblob --url https://mystorageaccount.blob.core.windows.net \
--container-name my-container --kustomization name=my-kustomization \
--account-key my-account-key
```

## Configuration general arguments

PARAMETER	FORMAT	NOTES
<code>--cluster-name</code> <code>-c</code>	String	Name of the cluster resource in Azure.
<code>--cluster-type</code> <code>-t</code>	<code>connectedClusters</code> , <code>managedClusters</code>	Use <code>connectedClusters</code> for Azure Arc-enabled Kubernetes clusters and <code>managedClusters</code> for AKS clusters.
<code>--resource-group</code> <code>-g</code>	String	Name of the Azure resource group that holds the Azure Arc or AKS cluster resource.
<code>--name</code> <code>-n</code>	String	Name of the Flux configuration in Azure.
<code>--namespace</code> <code>--ns</code>	String	Name of the namespace to deploy the configuration. Default: <code>default</code> .
<code>--scope</code> <code>-s</code>	String	Permission scope for the operators. Possible values are <code>cluster</code> (full access) or <code>namespace</code> (restricted access). Default: <code>cluster</code> .
<code>--suspend</code>	flag	Suspends all source and kustomize reconciliations defined in this Flux configuration. Reconciliations active at the time of suspension will continue.

## Source general arguments

PARAMETER	FORMAT	NOTES
<code>--kind</code>	String	Source kind to reconcile. Allowed values: <code>bucket</code> , <code>git</code> , <code>azblob</code> . Default: <code>git</code> .
<code>--timeout</code>	golang duration format	Maximum time to attempt to reconcile the source before timing out. Default: <code>10m</code> .
<code>--sync-interval</code> <code>--interval</code>	golang duration format	Time between reconciliations of the source on the cluster. Default: <code>10m</code> .

## Git repository source reference arguments

PARAMETER	FORMAT	NOTES
<code>--branch</code>	String	Branch within the Git source to sync to the cluster. Default: <code>master</code> . Newer repositories might have a root branch named <code>main</code> , in which case you need to set <code>--branch=main</code> .

PARAMETER	FORMAT	NOTES
--tag	String	Tag within the Git source to sync to the cluster. Example: <code>--tag=3.2.0</code> .
--semver	String	Git tag <code>semver</code> range within the Git source to sync to the cluster. Example: <code>--semver="&gt;=3.1.0-rc.1 &lt;3.2.0"</code> .
--commit	String	Git commit SHA within the Git source to sync to the cluster. Example: <code>--commit=363a6a8fe6a7f13e05d34c163b0ef02a777da2</code> .

For more information, see the [Flux documentation on Git repository checkout strategies](#).

### Public Git repository

PARAMETER	FORMAT	NOTES
--url -u	<code>http[s]://server/repo[.git]</code>	URL of the Git repository source to reconcile with the cluster.

### Private Git repository with SSH and Flux-created keys

Add the public key generated by Flux to the user account in your Git service provider.

PARAMETER	FORMAT	NOTES
--url -u	<code>ssh://user@server/repo[.git]</code>	<code>git@</code> should replace <code>user@</code> if the public key is associated with the repository instead of the user account.

### Private Git repository with SSH and user-provided keys

Use your own private key directly or from a file. The key must be in [PEM format](#) and end with a newline (`\n`).

Add the associated public key to the user account in your Git service provider.

PARAMETER	FORMAT	NOTES
--url -u	<code>ssh://user@server/repo[.git]</code>	<code>git@</code> should replace <code>user@</code> if the public key is associated with the repository instead of the user account.
--ssh-private-key	Base64 key in <a href="#">PEM format</a>	Provide the key directly.
--ssh-private-key-file	Full path to local file	Provide the full path to the local file that contains the PEM-format key.

### Private Git host with SSH and user-provided known hosts

The Flux operator maintains a list of common Git hosts in its `known_hosts` file. Flux uses this information to authenticate the Git repository before establishing the SSH connection. If you're using an uncommon Git repository or your own Git host, you can supply the host key so that Flux can identify your repository.

Just like private keys, you can provide your `known_hosts` content directly or in a file. When you're providing your own content, use the [known\\_hosts content format specifications](#), along with either of the preceding SSH key scenarios.

PARAMETER	FORMAT	NOTES
--url   -u	ssh://user@server/repo[.git]	git@ can replace user@.
--known-hosts	Base64 string	Provide known_hosts content directly.
--known-hosts-file	Full path to local file	Provide known_hosts content in a local file.

### Private Git repository with an HTTPS user and key

PARAMETER	FORMAT	NOTES
--url   -u	https://server/repo[.git]	HTTPS with Basic Authentication.
--https-user	Raw string	HTTPS username.
--https-key	Raw string	HTTPS personal access token or password.

### Private Git repository with an HTTPS CA certificate

PARAMETER	FORMAT	NOTES
--url   -u	https://server/repo[.git]	HTTPS with Basic Authentication.
--https-ca-cert	Base64 string	CA certificate for TLS communication.
--https-ca-cert-file	Full path to local file	Provide CA certificate content in a local file.

### Bucket source arguments

If you use a `bucket` source instead of a `git` source, here are the bucket-specific command arguments.

PARAMETER	FORMAT	NOTES
--url   -u	URL String	The URL for the <code>bucket</code> . Formats supported: http://, https://.
--bucket-name	String	Name of the <code>bucket</code> to sync.
--bucket-access-key	String	Access Key ID used to authenticate with the <code>bucket</code> .
--bucket-secret-key	String	Secret Key used to authenticate with the <code>bucket</code> .
--bucket-insecure	Boolean	Communicate with a <code>bucket</code> without TLS. If not provided, assumed false; if provided, assumed true.

### Azure Blob Storage Account source arguments

If you use a `azblob` source, here are the blob-specific command arguments.

PARAMETER	FORMAT	NOTES
--url <code>-u</code>	URL String	The URL for the <code>azblob</code> .
--container-name	String	Name of the Azure Blob Storage container to sync
--sp_client_id	String	The client ID for authenticating a service principal with Azure Blob, required for this authentication method
--sp_tenant_id	String	The tenant ID for authenticating a service principal with Azure Blob, required for this authentication method
--sp_client_secret	String	The client secret for authenticating a service principal with Azure Blob
--sp_client_cert	String	The Base64 encoded client certificate for authenticating a service principal with Azure Blob
--sp_client_cert_password	String	The password for the client certificate used to authenticate a service principal with Azure Blob
--sp_client_cert_send_chain	String	Specifies whether to include x5c header in client claims when acquiring a token to enable subject name / issuer based authentication for the client certificate
--account_key	String	The Azure Blob Shared Key for authentication
--sas_token	String	The Azure Blob SAS Token for authentication
--mi_client_id	String	The client ID of the managed identity for authentication with Azure Blob

#### Local secret for authentication with source

You can use a local Kubernetes secret for authentication with a `git`, `bucket` or `azBlob` source. The local secret must contain all of the authentication parameters needed for the source and must be created in the same namespace as the Flux configuration.

PARAMETER	FORMAT	NOTES
--local-auth-ref <code>--local-ref</code>	String	Local reference to a Kubernetes secret in the Flux configuration namespace to use for authentication with the source.

For HTTPS authentication, you create a secret with the `username` and `password`:

```
kubectl create ns flux-config
kubectl create secret generic -n flux-config my-custom-secret --from-literal=username=<my-username> --from-literal=password=<my-password-or-key>
```

For SSH authentication, you create a secret with the `identity` and `known_hosts` fields:

```
kubectl create ns flux-config
kubectl create secret generic -n flux-config my-custom-secret --from-file=identity=./id_rsa --from-file=known_hosts=./known_hosts
```

For both cases, when you create the Flux configuration, use `--local-auth-ref my-custom-secret` in place of the other authentication parameters:

```
az k8s-configuration flux create -g <cluster_resource_group> -c <cluster_name> -n <config_name> -t connectedClusters --scope cluster --namespace flux-config -u <git-repo-url> --kustomization name=kustomization1 --local-auth-ref my-custom-secret
```

Learn more about using a local Kubernetes secret with these authentication methods:

- [Git repository HTTPS authentication](#)
- [Git repository HTTPS self-signed certificates](#)
- [Git repository SSH authentication](#)
- [Bucket static authentication](#)

#### NOTE

If you need Flux to access the source through your proxy, you'll need to update the Azure Arc agents with the proxy settings. For more information, see [Connect using an outbound proxy server](#).

## Git implementation

To support various repository providers that implement Git, Flux can be configured to use one of two Git libraries: `go-git` or `libgit2`. See the [Flux documentation](#) for details.

The GitOps implementation of Flux v2 automatically determines which library to use for public cloud repositories:

- For GitHub, GitLab, and BitBucket repositories, Flux uses `go-git`.
- For Azure DevOps and all other repositories, Flux uses `libgit2`.

For on-premises repositories, Flux uses `libgit2`.

## Kustomization

By using `az k8s-configuration flux create`, you can create one or more kustomizations during the configuration.

PARAMETER	FORMAT	NOTES
<code>--kustomization</code>	No value	Start of a string of parameters that configure a kustomization. You can use it multiple times to create multiple kustomizations.
<code>name</code>	String	Unique name for this kustomization.
<code>path</code>	String	Path within the Git repository to reconcile with the cluster. Default is the top level of the branch.

PARAMETER	FORMAT	NOTES
<code>prune</code>	Boolean	Default is <code>false</code> . Set <code>prune=true</code> to assure that the objects that Flux deployed to the cluster will be cleaned up if they're removed from the repository or if the Flux configuration or kustomizations are deleted. Using <code>prune=true</code> is important for environments where users don't have access to the clusters and can make changes only through the Git repository.
<code>depends_on</code>	String	Name of one or more kustomizations (within this configuration) that must reconcile before this kustomization can reconcile. For example: <code>depends_on = ["kustomization1", "kustomization2"]</code> . Note that if you remove a kustomization that has dependent kustomizations, the dependent kustomizations will get a <code>DependencyNotReady</code> state and reconciliation will halt.
<code>timeout</code>	golang duration format	Default: <code>10m</code> .
<code>sync_interval</code>	golang duration format	Default: <code>10m</code> .
<code>retry_interval</code>	golang duration format	Default: <code>10m</code> .
<code>validation</code>	String	Values: <code>none</code> , <code>client</code> , <code>server</code> . Default: <code>none</code> . See <a href="#">Flux documentation</a> for details.
<code>force</code>	Boolean	Default: <code>false</code> . Set <code>force=true</code> to instruct the kustomize controller to re-create resources when patching fails because of an immutable field change.

You can also use `az k8s-configuration flux kustomization` to create, update, list, show, and delete kustomizations in a Flux configuration:

```
az k8s-configuration flux kustomization -h

Group
 az k8s-configuration flux kustomization : Commands to manage Kustomizations associated with Flux v2 Kubernetes configurations.

Commands:
 create : Create a Kustomization associated with a Flux v2 Kubernetes configuration.
 delete : Delete a Kustomization associated with a Flux v2 Kubernetes configuration.
 list : List Kustomizations associated with a Flux v2 Kubernetes configuration.
 show : Show a Kustomization associated with a Flux v2 Kubernetes configuration.
 update : Update a Kustomization associated with a Flux v2 Kubernetes configuration.
```

Here are the kustomization creation options:

```

az k8s-configuration flux kustomization create -h

This command is from the following extension: k8s-configuration

Command
az k8s-configuration flux kustomization create : Create a Kustomization associated with a
Kubernetes Flux v2 Configuration.

Arguments
--cluster-name -c [Required] : Name of the Kubernetes cluster.
--cluster-type -t [Required] : Specify Arc connected clusters or AKS managed clusters.
 Allowed values: connectedClusters, managedClusters.
--kustomization-name -k [Required] : Specify the name of the kustomization to target.
--name -n [Required] : Name of the flux configuration.
--resource-group -g [Required] : Name of resource group. You can configure the default
 group using `az configure --defaults group=<name>`.
--dependencies --depends --depends-on : Comma-separated list of kustomization dependencies.
--force : Re-create resources that cannot be updated on the
 cluster (i.e. jobs). Allowed values: false, true.
--interval --sync-interval : Time between reconciliations of the kustomization on the
 cluster.
--no-wait : Do not wait for the long-running operation to finish.
--path : Specify the path in the source that the kustomization
 should apply.
--prune : Garbage collect resources deployed by the kustomization
 on the cluster. Allowed values: false, true.
--retry-interval : Time between reconciliations of the kustomization on the
 cluster on failures, defaults to --sync-interval.
--timeout : Maximum time to reconcile the kustomization before
 timing out.

Global Arguments
--debug : Increase logging verbosity to show all debug logs.
--help -h : Show this help message and exit.
--only-show-errors : Only show errors, suppressing warnings.
--output -o : Output format. Allowed values: json, jsonc, none,
 table, tsv, yaml, yamlc. Default: json.
--query : JMESPath query string. See http://jmespath.org/ for more
 information and examples.
--subscription : Name or ID of subscription. You can configure the
 default subscription using `az account set -s
 NAME_OR_ID`.
--verbose : Increase logging verbosity. Use --debug for full debug
 logs.

Examples
Create a Kustomization associated with a Kubernetes v2 Flux Configuration
az k8s-configuration flux kustomization create --resource-group my-resource-group \
--cluster-name mycluster --cluster-type connectedClusters --name myconfig \
--kustomization-name my-kustomization-2 --path ./my/path --prune --force

```

## Manage GitOps configurations by using the Azure portal

The Azure portal is useful for managing GitOps configurations and the Flux extension in Azure Arc-enabled Kubernetes or AKS clusters. The portal displays all Flux configurations associated with each cluster and enables drilling in to each.

The portal provides the overall compliance state of the cluster. The Flux objects that have been deployed to the cluster are also shown, along with their installation parameters, compliance state, and any errors.

You can also use the portal to create, update, and delete GitOps configurations.

## Manage cluster configuration by using the Flux Kustomize controller

The Flux Kustomize controller is installed as part of the `microsoft.flux` cluster extension. It allows the declarative management of cluster configuration and application deployment by using Kubernetes manifests

synced from a Git repository. These Kubernetes manifests can include a *kustomize.yaml* file, but it isn't required.

For usage details, see the following:

- [Flux Kustomize controller](#)
- [Kustomize reference documents](#)
- [The kustomization file](#)
- [Kustomize project](#)
- [Kustomize guides](#)

## Manage Helm chart releases by using the Flux Helm controller

The Flux Helm controller is installed as part of the `microsoft.flux` cluster extension. It allows you to declaratively manage Helm chart releases with Kubernetes manifests that you maintain in your Git repository.

For usage details, see the following:

- [Flux for Helm users](#)
- [Manage Helm releases](#)
- [Migrate to Flux v2 Helm from Flux v1 Helm](#)
- [Flux Helm controller](#)

### TIP

Because of how Helm handles index files, processing helm charts is an expensive operation and can have very high memory footprint. As a result, helm chart reconciliation, when occurring in parallel, can cause memory spikes and OOMKilled if you are reconciling a large number of helm charts at a given time. By default, the source-controller sets its memory limit at 1Gi and its memory requests at 64Mi. If you need to increase this limit and requests due to a high number of large helm chart reconciliations, run the following command after installing the `microsoft.flux` extension:

```
az k8s-extension update -g <resource-group> -c <cluster-name> -n flux -t connectedClusters --config source-controller.resources.limits.memory=2Gi source-controller.resources.requests.memory=300Mi
```

## Use the `GitRepository` source for Helm charts

If your Helm charts are stored in the `GitRepository` source that you configure as part of the `fluxConfigurations` resource, you can indicate that the configured source should be used as the source of the Helm charts by adding `clusterconfig.azure.com/use-managed-source: "true"` to your `HelmRelease.yaml`, as shown in the following example:

```

apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
 name: somename
 namespace: somenamespace
 annotations:
 clusterconfig.azure.com/use-managed-source: "true"
spec:
 ...
```

By using this annotation, the `HelmRelease` that is deployed will be patched with the reference to the configured source. Currently, only `GitRepository` source is supported.

## Multi-tenancy

Flux v2 supports [multi-tenancy](#) in [version 0.26](#). This capability has been integrated into Azure GitOps with Flux v2.

[ !NOTE] For the multi-tenancy feature, you need to know if your manifests contain any cross-namespace sourceRef for HelmRelease, Kustomization, ImagePolicy, or other objects, or if you use a Kubernetes version less than 1.20.6. To prepare, take these actions:

- Upgrade to Kubernetes version 1.20.6 or greater.
- In your Kubernetes manifests, assure that all `sourceRef` are to objects within the same namespace as the GitOps configuration.
  - If you need time to update your manifests, you can [opt out of multi-tenancy](#). However, you still need to upgrade your Kubernetes version.

## Update manifests for multi-tenancy

Let's say you deploy a `fluxConfiguration` to one of our Kubernetes clusters in the `cluster-config` namespace with cluster scope. You configure the source to sync the <https://github.com/fluxcd/flux2-kustomize-helm-example> repo. This is the same sample Git repo used in the tutorial earlier in this doc. After Flux syncs the repo, it will deploy the resources described in the manifests (YAML files). Two of the manifests describe HelmRelease and HelmRepository objects.

```
apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
 name: nginx
 namespace: nginx
spec:
 releaseName: nginx-ingress-controller
 chart:
 spec:
 chart: nginx-ingress-controller
 sourceRef:
 kind: HelmRepository
 name: bitnami
 namespace: flux-system
 version: "5.6.14"
 interval: 1h0m0s
 install:
 remediation:
 retries: 3
 # Default values
 # https://github.com/bitnami/charts/blob/master/bitnami/nginx-ingress-controller/values.yaml
 values:
 service:
 type: NodePort
```

```
apiVersion: source.toolkit.fluxcd.io/v1beta1
kind: HelmRepository
metadata:
 name: bitnami
 namespace: flux-system
spec:
 interval: 30m
 url: https://charts.bitnami.com/bitnami
```

By default, the Flux extension will deploy the `fluxConfigurations` by impersonating the `flux-applier` service account that is deployed only in the `cluster-config` namespace. Using the above manifests, when multi-tenancy is enabled the HelmRelease would be blocked. This is because the HelmRelease is in the `nginx` namespace and is referencing a HelmRepository in the `flux-system` namespace. Also, the Flux helm-controller cannot apply the HelmRelease, because there is no `flux-applier` service account in the `nginx` namespace.

To work with multi-tenancy, the correct approach is to deploy all Flux objects into the same namespace as the `fluxConfigurations`. This avoids the cross-namespace reference issue, and allows the Flux controllers to get the permissions to apply the objects. Thus, for a GitOps configuration created in the `cluster-config` namespace, the

above manifests would change to these:

```
apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
 name: nginx
 namespace: cluster-config
spec:
 releaseName: nginx-ingress-controller
 targetNamespace: nginx
 chart:
 spec:
 chart: nginx-ingress-controller
 sourceRef:
 kind: HelmRepository
 name: bitnami
 namespace: cluster-config
 version: "5.6.14"
 interval: 1h0m0s
 install:
 remediation:
 retries: 3
 # Default values
 # https://github.com/bitnami/charts/blob/master/bitnami/nginx-ingress-controller/values.yaml
 values:
 service:
 type: NodePort
```

```
apiVersion: source.toolkit.fluxcd.io/v1beta1
kind: HelmRepository
metadata:
 name: bitnami
 namespace: cluster-config
spec:
 interval: 30m
 url: https://charts.bitnami.com/bitnami
```

## Opt out of multi-tenancy

When the `microsoft.flux` extension is installed, multi-tenancy is enabled by default to assure security by default in your clusters. However, if you need to disable multi-tenancy, you can opt out by creating or updating the `microsoft.flux` extension in your clusters with "`--configuration-settings multiTenancy.enforce=false`".

```
az k8s-extension create --extension-type microsoft.flux --configuration-settings multiTenancy.enforce=false
-c CLUSTER_NAME -g RESOURCE_GROUP -n flux -t <managedClusters or connectedClusters>

or

az k8s-extension update --configuration-settings multiTenancy.enforce=false -c CLUSTER_NAME -g
RESOURCE_GROUP -n flux -t <managedClusters or connectedClusters>
```

## Migrate from Flux v1

If you've been using Flux v1 in Azure Arc-enabled Kubernetes or AKS clusters and want to migrate to using Flux v2 in the same clusters, you first need to delete the Flux v1 `sourceControlConfigurations` from the clusters. The `microsoft.flux` cluster extension won't install if there are Flux v1 `sourceControlConfigurations` resources in the cluster.

Use these Azure CLI commands to find and then delete existing `sourceControlConfigurations` in a cluster:

```
az k8s-configuration list --cluster-name <Arc or AKS cluster name> --cluster-type <connectedClusters OR managedClusters> --resource-group <resource group name>
az k8s-configuration delete --name <configuration name> --cluster-name <Arc or AKS cluster name> --cluster-type <connectedClusters OR managedClusters> --resource-group <resource group name>
```

You can also use the Azure portal to view and delete GitOps configurations in Azure Arc-enabled Kubernetes or AKS clusters.

General information about migration from Flux v1 to Flux v2 is available in the fluxed project: [Migrate from Flux v1 to v2](#).

## Next steps

Advance to the next tutorial to learn how to apply configuration at scale with Azure Policy.

[Use Azure Policy to enforce GitOps at scale.](#)

# How to deploy a Container offer from Azure Marketplace (preview)

10/27/2022 • 3 minutes to read • [Edit Online](#)

Azure Marketplace is an online store that contains thousands of IT software applications and services built by industry-leading technology companies. In Azure Marketplace you can find, try, buy, and deploy the software and services you need to build new solutions and manage your cloud infrastructure. The catalog includes solutions for different industries and technical areas, free trials, and also consulting services from Microsoft partners.

Included among these solutions are Kubernetes application-based Container offers, which contain applications meant to run on Kubernetes clusters such as Azure Kubernetes Service (AKS). In this article, you will learn how to:

- Browse offers in Azure Marketplace
- Purchase an application
- Deploy the application on your AKS cluster
- Monitor usage and billing information

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## NOTE

This feature is currently only supported in the following regions:

- West Central US
- West Europe
- East US.

## Register resource providers

You must have registered the `Microsoft.ContainerService` and `Microsoft.KubernetesConfiguration` providers on your subscription using the `az provider register` command:

```
az provider register --namespace Microsoft.ContainerService --wait
az provider register --namespace Microsoft.KubernetesConfiguration --wait
```

## Browse offers

- Begin by visiting the Azure portal and searching for "*Marketplace*" in the top search bar.

- You can search for an offer or publisher directly by name or browse all offers. To find Kubernetes application offers, use the *Product type* filter for *Azure Containers*.

- **IMPORTANT**

The *Azure Containers* category includes both Kubernetes applications and standalone container images. This walkthrough is Kubernetes application-specific. If you find the steps to deploy an offer differ in some way, you are most likely trying to deploy a container image-based offer instead of a Kubernetes-application based offer.

To ensure you're searching for Kubernetes applications, include the term `KubernetesApps` in your search.

- Once you've decided on an application, click on the offer.

The screenshot shows the Azure Marketplace interface. On the left, there's a sidebar with navigation links like 'Home', 'Marketplace', 'Get Started', 'Service Providers', 'Management', 'Private Marketplace', 'Private Offer Management', 'My Marketplace' (which is selected), 'Favorites', 'Recently created', and 'Private products'. The main area has a search bar at the top with filters: 'Category : All', 'Pricing : All', 'Operating System : All', 'Publisher Type : All', and 'Product Type : Azure Containers' (which is highlighted with a red box). Below the search bar, there are additional filters: 'Azure benefit eligible only' and 'Publisher name : All'. A note says 'Showing 1 to 20 of 297 results with 1 selected filters. Clear Filters'. The main content area displays a grid of 12 offer cards. Each card contains the offer name, publisher, type, a brief description, and a 'Create' button. The offers include: MariaDB 10.2 Container for Ubuntu 18.04 (Tidal Media Inc, Container, Enhanced, hardened, and secured container solution with MariaDB Server), Trusted Certificate Service (Intel, Container, Kubernetes certificate signing solution using Intel® SGX), Cert Manager Webhook packaged by Bitnami (Bitnami, Container, Up-to-date, customizable, and secure container image), Apache Airflow packaged by Bitnami (Bitnami, Container, Up-to-date, customizable, and secure container image), Azure CLI packaged by Bitnami (Bitnami, Container, Up-to-date, customizable, and secure container image), OAuth2 Proxy packaged by Bitnami (Bitnami, Container, Up-to-date, customizable, and secure container image), Excel Writer for Azure Data Factory (Tidal Media Inc, Container, Create excel files using datasets for integration services and data factory. Simple api...), Jupyter Base Notebook packaged by Bitnami (Bitnami, Container, Up-to-date, customizable, and secure container image), Fluent Bit packaged by Bitnami (Bitnami, Container, Up-to-date, customizable, and secure container image), RabbitMQ Default User Credential Updater (Bitnami, Container, Up-to-date, customizable, and secure container image), Drupal packaged by Bitnami (Bitnami, Container, Up-to-date, customizable, and secure container image), and Airsonic 10.6.2 Alpine 3.9 Container Image (Tidal Media Inc, Container, Ready-to-run Container Image with Airsonic - flawless streaming media server solution).

## Purchasing a Kubernetes offer

- Review the plan and prices tab, select an option, and ensure the terms are acceptable before proceeding.

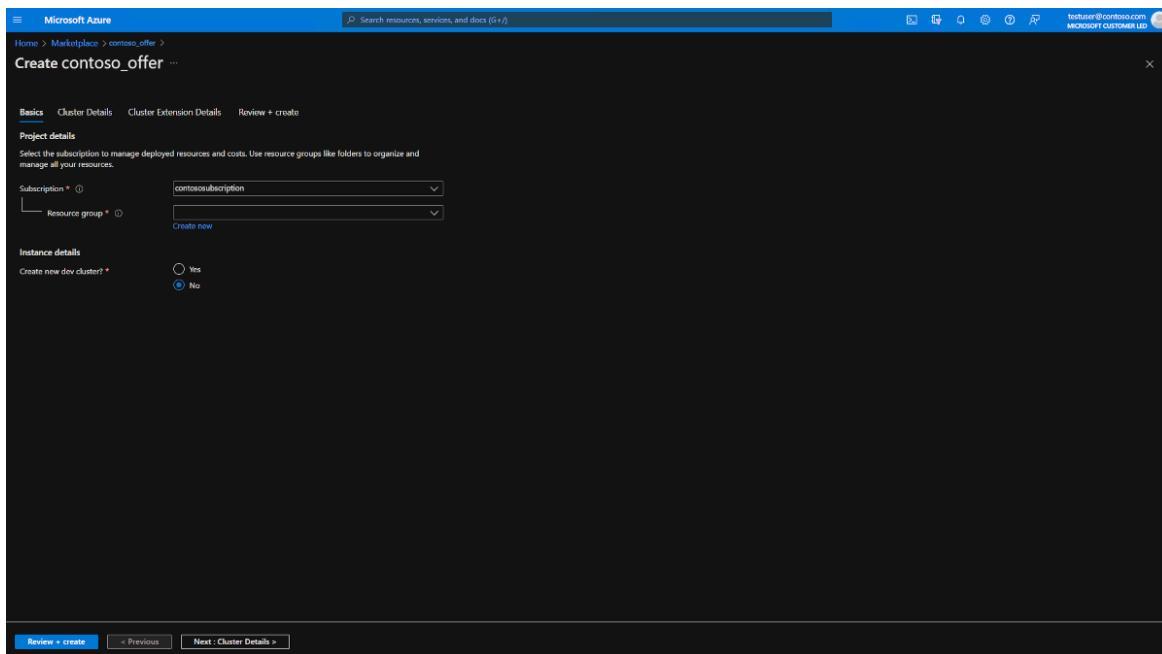
The screenshot shows the 'contoso\_offer' details page in the Azure Marketplace. At the top, it says 'Home > Marketplace > contoso\_offer > ... Test PMC 2 PC'. It indicates that the offer was shared privately with the user by the publisher. Below this, there's a 'Plans + Pricing' section with tabs for 'Overview', 'Plans + Pricing' (which is selected), 'Usage Information + Support', and 'Reviews'. A note states: 'The cost of running this product is a combination of the selected software plan plus the Azure infrastructure costs of the virtual machines on which you will be running this software. Your Azure infrastructure price might vary if you have enterprise agreements or other discounts. Costs might vary by deployment region.' The 'Plans + Pricing' table lists three plans:

Software plan	Price	Description
Private testplanpercorefree	Starting at \$0/hour (+ Azure Infrastructure costs)	test plan do not use
Private testbyplan	Bring your own license (BYOL) (+ Azure Infrastructure costs)	test plan do not use
Private testpercoreycoreplan	Starting at \$1/hour/pc/evcorecluster (+ Azure Infrastructure costs)	test plan do not use
Private testpercoreycoreplanfree	Starting at \$0/hour (+ Azure Infrastructure costs)	test plan do not use

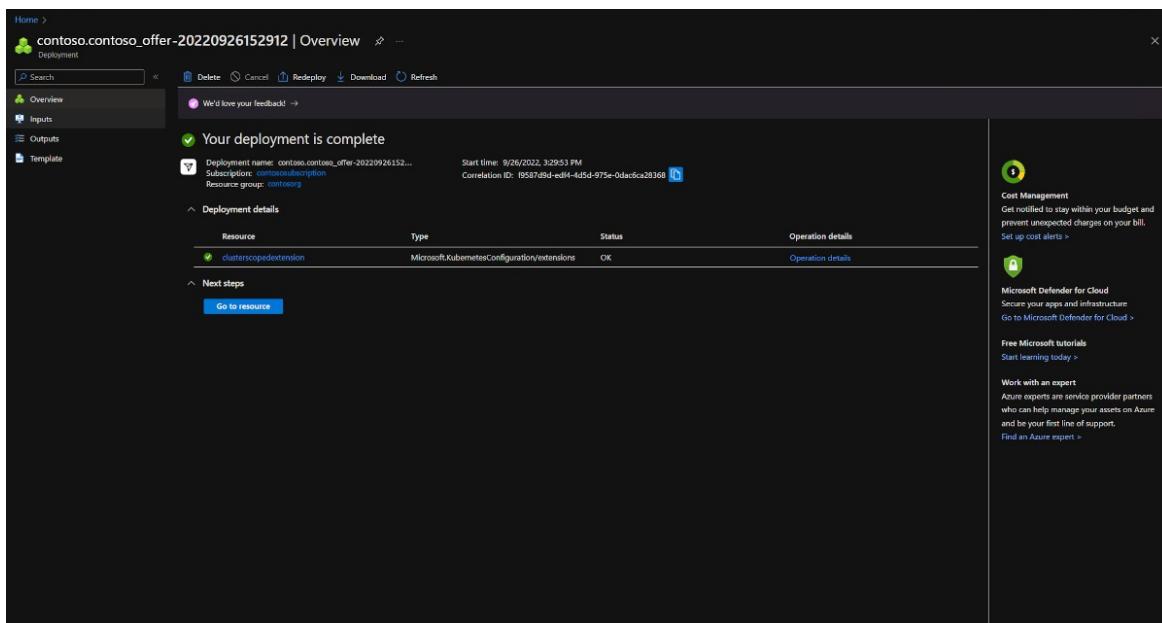
- Click "Create".

## Deploy a Kubernetes offer

- Follow the form, filling in information for your resource group, cluster, and any configuration options required by the application. You can decide to deploy on a new AKS cluster or use an existing cluster.



- After some time, the application will be deployed, as indicated by the Portal screen.



- You can also verify by listing the extensions running on your cluster:

```
az k8s-extension list --cluster-name <clusterName> --resource-group <resourceGroupName> --cluster-type managedClusters
```

## Manage offer lifecycle

For lifecycle management, an Azure Kubernetes offer is represented as a cluster extension for Azure Kubernetes service(AKS). For more details, see[cluster extensions for AKS](#).

Purchasing an offer from the Azure Marketplace creates a new instance of the extension on your AKS cluster. The extension instance can be viewed from the cluster using the following command:

```
az k8s-extension show --name <extension-name> --cluster-name <clusterName> --resource-group
<resourceGroupName> --cluster-type managedClusters
```

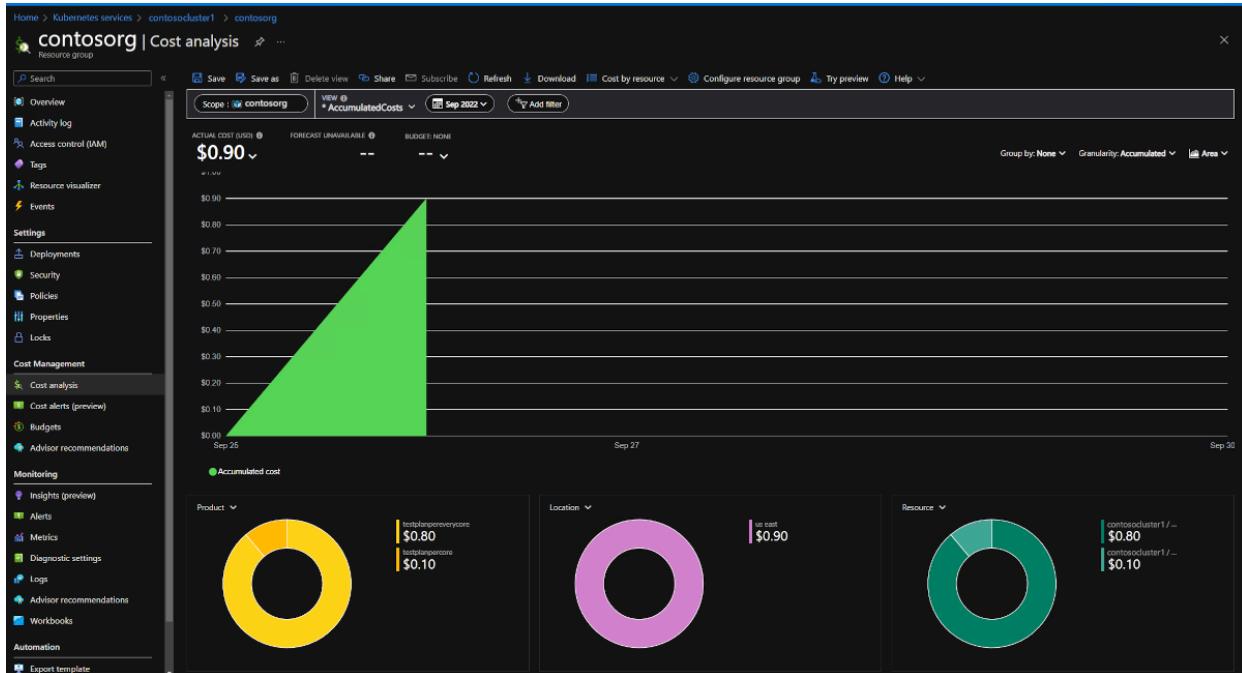
## Removing an offer

A purchased Azure Container offer plan can be deleted by deleting the extension instance on the cluster. For example:

```
az k8s-extension delete --name <extension-name> --cluster-name <clusterName> --resource-group
<resourceGroupName> --cluster-type managedClusters
```

## Monitor billing and usage information

To monitor billing and usage information for the offer you've deployed, visit Cost Management > Cost Analysis in your cluster's resource group's page in the Azure portal. You can see a breakdown of cost for the plan you've selected under "Product".



## Next Steps

- Learn more about [exploring and analyzing costs](#).

# Open Service Mesh AKS add-on

10/27/2022 • 2 minutes to read • [Edit Online](#)

**Open Service Mesh (OSM)** is a lightweight, extensible, cloud native service mesh that allows users to uniformly manage, secure, and get out-of-the-box observability features for highly dynamic microservice environments.

OSM runs an Envoy-based control plane on Kubernetes and can be configured with [SMI APIs](#). OSM works by injecting an Envoy proxy as a sidecar container with each instance of your application. The Envoy proxy contains and executes rules around access control policies, implements routing configuration, and captures metrics. The control plane continually configures the Envoy proxies to ensure policies and routing rules are up to date and ensures proxies are healthy.

The OSM project was originated by Microsoft and has since been donated and is governed by the [Cloud Native Computing Foundation \(CNCF\)](#).

## Installation and version

OSM can be added to your Azure Kubernetes Service (AKS) cluster by enabling the OSM add-on using the [Azure CLI](#) or a [Bicep template](#). The OSM add-on provides a fully supported installation of OSM that is integrated with AKS.

### IMPORTANT

Based on the version of Kubernetes your cluster is running, the OSM add-on installs a different version of OSM:

- If your cluster is running Kubernetes version 1.24.0 or greater, the OSM add-on installs version [1.2.0](#) of OSM.
- If your cluster is running a version of Kubernetes between 1.23.5 and 1.24.0, the OSM add-on installs version [1.1.1](#) of OSM.
- If your cluster is running a version of Kubernetes below 1.23.5, the OSM add-on installs version [1.0.0](#) of OSM.

## Capabilities and features

OSM provides the following capabilities and features:

- Secure service to service communication by enabling mutual TLS (mTLS).
- Onboard applications onto the OSM mesh using automatic sidecar injection of Envoy proxy.
- Transparently configure traffic shifting on deployments.
- Define and execute fine grained access control policies for services.
- Monitor and debug services using observability and insights into application metrics.
- Integrate with external certificate management.
- Integrates with existing ingress solutions such as [NGINX](#), [Contour](#), and [Web Application Routing](#). For more details on how ingress works with OSM, see [Using Ingress to manage external access to services within the cluster](#). For an example on integrating OSM with Contour for ingress, see [Ingress with Contour](#). For an example on integrating OSM with ingress controllers that use the `networking.k8s.io/v1` API, such as NGINX, see [Ingress with Kubernetes Nginx Ingress Controller](#). For more details on using Web Application Routing, which automatically integrates with OSM, see [Web Application Routing](#).

## Example scenarios

OSM can be used to help your AKS deployments in many different ways. For example:

- Encrypt communications between service endpoints deployed in the cluster.
- Enable traffic authorization of both HTTP/HTTPS and TCP traffic.
- Configure weighted traffic controls between two or more services for A/B testing or canary deployments.
- Collect and view KPIs from application traffic.

## Add-on limitations

The OSM AKS add-on has the following limitations:

- [Iptables redirection](#) for port IP address and port range exclusion must be enabled using `kubectl patch` after installation. For more details, see [iptables redirection](#).
- Pods that are onboarded to the mesh that need access to IMDS, Azure DNS, or the Kubernetes API server must have their IP addresses to the global list of excluded outbound IP ranges using [Global outbound IP range exclusions](#).
- At this time, OSM does not support Windows Server containers.

## Next steps

After enabling the OSM add-on using the [Azure CLI](#) or a [Bicep template](#), you can:

- [Deploy a sample application](#)
- [Onboard an existing application](#)

# Install the Open Service Mesh add-on by using the Azure CLI

10/27/2022 • 3 minutes to read • [Edit Online](#)

This article shows you how to install the Open Service Mesh (OSM) add-on on an Azure Kubernetes Service (AKS) cluster and verify that it's installed and running.

## IMPORTANT

Based on the version of Kubernetes your cluster is running, the OSM add-on installs a different version of OSM:

- If your cluster is running Kubernetes version 1.24.0 or greater, the OSM add-on installs version [1.2.0](#) of OSM.
- If your cluster is running a version of Kubernetes between 1.23.5 and 1.24.0, the OSM add-on installs version [1.1.1](#) of OSM.
- If your cluster is running a version of Kubernetes below 1.23.5, the OSM add-on installs version [1.0.0](#) of OSM.

## Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI installed](#).

## Install the OSM add-on on your cluster

To install the OSM add-on, use `--enable-addons open-service-mesh` when creating or updating a cluster.

The following example creates a *myResourceGroup* resource group. Then it creates a *myAKSCluster* cluster with three nodes and the OSM add-on.

```
az group create --name myResourceGroup --location eastus

az aks create \
 --resource-group myResourceGroup \
 --name myAKSCluster \
 --enable-addons open-service-mesh
```

For existing clusters, use `az aks enable-addons`. The following code shows an example.

## IMPORTANT

You can't enable the OSM add-on on an existing cluster if an OSM mesh is already on your cluster. Uninstall any existing OSM meshes on your cluster before enabling the OSM add-on.

```
az aks enable-addons \
 --resource-group myResourceGroup \
 --name myAKSCluster \
 --addons open-service-mesh
```

## Get the credentials for your cluster

Get the credentials for your AKS cluster by using the `az aks get-credentials` command. The following example command gets the credentials for *myAKSCluster* in the *myResourceGroup* resource group:

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

## Verify that the OSM add-on is installed on your cluster

To see if the OSM add-on is installed on your cluster, verify that the `enabled` value is `true` for `openServiceMesh` under `addonProfiles`. The following example shows the status of the OSM add-on for *myAKSCluster* in *myResourceGroup*:

```
az aks show --resource-group myResourceGroup --name myAKSCluster --query
'addonProfiles.openServiceMesh.enabled'
```

## Verify that the OSM mesh is running on your cluster

You can verify the version, status, and configuration of the OSM mesh that's running on your cluster. Use `kubectl` to display the image version of the *osm-controller* deployment. For example:

```
kubectl get deployment -n kube-system osm-controller -
o=jsonpath='{$.spec.template.spec.containers[:1].image}'
```

The following example output shows version *0.11.1* of the OSM mesh:

```
$ kubectl get deployment -n kube-system osm-controller -
o=jsonpath='{$.spec.template.spec.containers[:1].image}'
mcr.microsoft.com/ossopenservicemesh/osm-controller:v0.11.1
```

To verify the status of the OSM components running on your cluster, use `kubectl` to show the status of the `app.kubernetes.io/name=openservicemesh.io` deployments, pods, and services. For example:

```
kubectl get deployments -n kube-system --selector app.kubernetes.io/name=openservicemesh.io
kubectl get pods -n kube-system --selector app.kubernetes.io/name=openservicemesh.io
kubectl get services -n kube-system --selector app.kubernetes.io/name=openservicemesh.io
```

### IMPORTANT

If any pods have a status other than `Running`, such as `Pending`, your cluster might not have enough resources to run OSM. Review the sizing for your cluster, such as the number of nodes and the virtual machine's SKU, before continuing to use OSM on your cluster.

To verify the configuration of your OSM mesh, use `kubectl get meshconfig`. For example:

```
kubectl get meshconfig osm-mesh-config -n kube-system -o yaml
```

The following example output shows the configuration of an OSM mesh:

```

apiVersion: config.openservicemesh.io/v1alpha1
kind: MeshConfig
metadata:
 creationTimestamp: "0000-00-00A00:00:00A"
 generation: 1
 name: osm-mesh-config
 namespace: kube-system
 resourceVersion: "2494"
 uid: 6c4d67f3-c241-4aeb-bf4f-b029b08faa31
spec:
 certificate:
 serviceCertValidityDuration: 24h
 featureFlags:
 enableEgressPolicy: true
 enableMulticlusterMode: false
 enableWASMStats: true
 observability:
 enableDebugServer: true
 osmLogLevel: info
 tracing:
 address: jaeger.osm-system.svc.cluster.local
 enable: false
 endpoint: /api/v2/spans
 port: 9411
 sidecar:
 configResyncInterval: 0s
 enablePrivilegedInitContainer: false
 envoyImage: mcr.microsoft.com/oss/envoyproxy/envoy:v1.18.3
 initContainerImage: mcr.microsoft.com/oss/openservicemesh/init:v0.9.1
 logLevel: error
 maxDataPlaneConnections: 0
 resources: {}
 traffic:
 enableEgress: true
 enablePermissiveTrafficPolicyMode: true
 inboundExternalAuthorization:
 enable: false
 failureModeAllow: false
 statPrefix: inboundExtAuthz
 timeout: 1s
 useHTTPSIIngress: false

```

The preceding example shows `enablePermissiveTrafficPolicyMode: true`, which means OSM has permissive traffic policy mode enabled. With this mode enabled in your OSM mesh:

- The [SMI](#) traffic policy enforcement is bypassed.
- OSM automatically discovers services that are a part of the service mesh.
- OSM creates traffic policy rules on each Envoy proxy sidecar to be able to communicate with these services.

## Delete your cluster

When you no longer need the cluster, use the `az group delete` command to remove the resource group, the cluster, and all related resources:

```
az group delete --name myResourceGroup --yes --no-wait
```

Alternatively, you can uninstall the OSM add-on and the related resources from your cluster. For more information, see [Uninstall the Open Service Mesh add-on from your AKS cluster](#).

## Next steps

This article showed you how to install the OSM add-on on an AKS cluster, and then verify that it's installed and running. With the OSM add-on installed on your cluster, you can [deploy a sample application](#) or [onboard an existing application](#) to work with your OSM mesh.

# Deploy the Open Service Mesh add-on by using Bicep

10/27/2022 • 5 minutes to read • [Edit Online](#)

This article shows you how to deploy the Open Service Mesh (OSM) add-on to Azure Kubernetes Service (AKS) by using a [Bicep](#) template.

## IMPORTANT

Based on the version of Kubernetes your cluster is running, the OSM add-on installs a different version of OSM:

- If your cluster is running Kubernetes version 1.24.0 or greater, the OSM add-on installs version [1.2.0](#) of OSM.
- If your cluster is running a version of Kubernetes between 1.23.5 and 1.24.0, the OSM add-on installs version [1.1.1](#) of OSM.
- If your cluster is running a version of Kubernetes below 1.23.5, the OSM add-on installs version [1.0.0](#) of OSM.

[Bicep](#) is a domain-specific language that uses declarative syntax to deploy Azure resources. You can use Bicep in place of creating [Azure Resource Manager templates](#) to deploy your infrastructure-as-code Azure resources.

## Prerequisites

- Azure CLI version 2.20.0 or later
- An SSH public key used for deploying AKS
- [Visual Studio Code](#) with a Bash terminal
- The Visual Studio Code [Bicep extension](#)

## Install the OSM add-on for a new AKS cluster by using Bicep

For deployment of a new AKS cluster, you enable the OSM add-on at cluster creation. The following instructions use a generic Bicep template that deploys an AKS cluster by using ephemeral disks and the [kubenet](#) container network interface, and then enables the OSM add-on. For more advanced deployment scenarios, see [What is Bicep?](#).

### Create a resource group

In Azure, you can associate related resources by using a resource group. Create a resource group by using [az group create](#). The following example creates a resource group named *my-osm-bicep-aks-cluster-rg* in a specified Azure location (region):

```
az group create --name <my-osm-bicep-aks-cluster-rg> --location <azure-region>
```

### Create the main and parameters Bicep files

By using Visual Studio Code with a Bash terminal open, create a directory to store the necessary Bicep deployment files. The following example creates a directory named *bicep-osm-aks-addon* and changes to the directory:

```
mkdir bicep-osm-aks-addon
cd bicep-osm-aks-addon
```

Next, create both the main file and the parameters file, as shown in the following example:

```
touch osm.aks.bicep && touch osm.aks.parameters.json
```

Open the *osm.aks.bicep* file and copy the following example content to it. Then save the file.

```
// https://learn.microsoft.com/azure/aks/troubleshooting#what-naming-restrictions-are-enforced-for-aks-
resources-and-parameters
@minLength(3)
@maxLength(63)
@description('Provide a name for the AKS cluster. The only allowed characters are letters, numbers, dashes,
and underscore. The first and last character must be a letter or a number.')
param clusterName string
@minLength(3)
@maxLength(54)
@description('Provide a name for the AKS dnsPrefix. Valid characters include alphanumeric values and hyphens
(-). The dnsPrefix can\'t include special characters such as a period (.)')
param clusterDNSPrefix string
param k8Version string
param sshPubKey string

resource aksCluster 'Microsoft.ContainerService/managedClusters@2021-03-01' = {
 name: clusterName
 location: resourceGroup().location
 identity: {
 type: 'SystemAssigned'
 }
 properties: {
 kubernetesVersion: k8Version
 dnsPrefix: clusterDNSPrefix
 enableRBAC: true
 agentPoolProfiles: [
 {
 name: 'agentpool'
 count: 3
 vmSize: 'Standard_DS2_v2'
 osDiskSizeGB: 30
 osDiskType: 'Ephemeral'
 osType: 'Linux'
 mode: 'System'
 }
]
 linuxProfile: {
 adminUsername: 'adminUserName'
 ssh: {
 publicKeys: [
 {
 keyData: sshPubKey
 }
]
 }
 }
 addonProfiles: {
 openServiceMesh: {
 enabled: true
 config: {}
 }
 }
 }
}
```

Open the *osm.aks.parameters.json* file and copy the following example content to it. Add the deployment-specific parameters, and then save the file.

#### NOTE

The `osm.aks.parameters.json` file is an example template parameters file needed for the Bicep deployment. Update the parameters specifically for your deployment environment. The specific parameter values in this example need the following parameters to be updated: `clusterName`, `clusterDNSPrefix`, `k8Version`, and `sshPubKey`. To find a list of supported Kubernetes versions in your region, use the `az aks get-versions --location <region>` command.

```
{
 "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentParameters.json#",
 "contentVersion": "1.0.0.0",
 "parameters": {
 "clusterName": {
 "value": "<YOUR CLUSTER NAME HERE>"
 },
 "clusterDNSPrefix": {
 "value": "<YOUR CLUSTER DNS PREFIX HERE>"
 },
 "k8Version": {
 "value": "<YOUR SUPPORTED KUBERNETES VERSION HERE>"
 },
 "sshPubKey": {
 "value": "<YOUR SSH KEY HERE>"
 }
 }
}
```

## Deploy the Bicep files

To deploy the previously created Bicep files, open the terminal and authenticate to your Azure account for the Azure CLI by using the `az login` command. After you're authenticated to your Azure subscription, run the following commands for deployment:

```
az group create --name osm-bicep-test --location eastus2

az deployment group create \
 --name OSMBicepDeployment \
 --resource-group osm-bicep-test \
 --template-file osm.aks.bicep \
 --parameters @osm.aks.parameters.json
```

When the deployment finishes, you should see a message that says the deployment succeeded.

## Validate installation of the OSM add-on

You use several commands to check that all of the components of the OSM add-on are enabled and running.

First, query the add-on profiles of the cluster to check the enabled state of the installed add-ons. The following command should return `true`:

```
az aks list -g <my-osm-aks-cluster-rg> -o json | jq -r '.[].addonProfiles.openServiceMesh.enabled'
```

The following `kubectl` commands will report the status of `osm-controller`.

```
kubectl get deployments -n kube-system --selector app=osm-controller
kubectl get pods -n kube-system --selector app=osm-controller
kubectl get services -n kube-system --selector app=osm-controller
```

## Access the OSM add-on configuration

You can configure the OSM controller via the OSM MeshConfig resource, and you can view the OSM controller's configuration settings via the Azure CLI. Use the `kubectl get` command as shown in the following example:

```
kubectl get meshconfig osm-mesh-config -n kube-system -o yaml
```

Here's an example output of MeshConfig:

```
apiVersion: config.openservicemesh.io/v1alpha1
kind: MeshConfig
metadata:
 creationTimestamp: "0000-00-00A00:00:00A"
 generation: 1
 name: osm-mesh-config
 namespace: kube-system
 resourceVersion: "2494"
 uid: 6c4d67f3-c241-4aeb-bf4f-b029b08faa31
spec:
 certificate:
 serviceCertValidityDuration: 24h
 featureFlags:
 enableEgressPolicy: true
 enableMulticlusterMode: false
 enableWASMStats: true
 observability:
 enableDebugServer: true
 osmLogLevel: info
 tracing:
 address: jaeger.osm-system.svc.cluster.local
 enable: false
 endpoint: /api/v2/spans
 port: 9411
 sidecar:
 configResyncInterval: 0s
 enablePrivilegedInitContainer: false
 envoyImage: mcr.microsoft.com/oss/envoyproxy/envoy:v1.18.3
 initContainerImage: mcr.microsoft.com/oss/openservicemesh/init:v0.9.1
 logLevel: error
 maxDataPlaneConnections: 0
 resources: {}
 traffic:
 enableEgress: true
 enablePermissiveTrafficPolicyMode: true
 inboundExternalAuthorization:
 enable: false
 failureModeAllow: false
 statPrefix: inboundExtAuthz
 timeout: 1s
 useHTTPSGress: false
```

Notice that `enablePermissiveTrafficPolicyMode` is configured to `true`. In OSM, permissive traffic policy mode bypasses [SMI](#) traffic policy enforcement. In this mode, OSM automatically discovers services that are a part of the service mesh. The discovered services will have traffic policy rules programmed on each Envoy proxy sidecar to allow communications between these services.

## WARNING

Before you proceed, verify that your permissive traffic policy mode is set to `true`. If it isn't, change it to `true` by using the following command:

```
kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"traffic":{"enablePermissiveTrafficPolicyMode":true}}}' --type=merge
```

## Clean up resources

When you no longer need the Azure resources, use the Azure CLI to delete the deployment's test resource group:

```
az group delete --name osm-bicep-test
```

Alternatively, you can uninstall the OSM add-on and the related resources from your cluster. For more information, see [Uninstall the Open Service Mesh add-on from your AKS cluster](#).

## Next steps

This article showed you how to install the OSM add-on on an AKS cluster and verify that it's installed and running. With the OSM add-on installed on your cluster, you can [deploy a sample application](#) or [onboard an existing application](#) to work with your OSM mesh.

# Download and configure the Open Service Mesh (OSM) client library

10/27/2022 • 3 minutes to read • [Edit Online](#)

This article will discuss how to download the OSM client library to be used to operate and configure the OSM add-on for AKS, and how to configure the binary for your environment.

## IMPORTANT

Based on the version of Kubernetes your cluster is running, the OSM add-on installs a different version of OSM:

- If your cluster is running Kubernetes version 1.24.0 or greater, the OSM add-on installs version *1.2.0* of OSM.
- If your cluster is running a version of Kubernetes between 1.23.5 and 1.24.0, the OSM add-on installs version *1.1.1* of OSM.
- If your cluster is running a version of Kubernetes below 1.23.5, the OSM add-on installs version *1.0.0* of OSM.

## Download and install the Open Service Mesh (OSM) client binary

In a bash-based shell on Linux or [Windows Subsystem for Linux](#), use `curl` to download the OSM release and then extract with `tar` as follows:

```
Specify the OSM version that will be leveraged throughout these instructions
OSM_VERSION=v1.2.0

curl -sL "https://github.com/openservicemesh/osm/releases/download/$OSM_VERSION/osm-$OSM_VERSION-linux-
amd64.tar.gz" | tar -vxzf -
```

The `osm` client binary runs on your client machine and allows you to manage OSM in your AKS cluster. Use the following commands to install the OSM `osm` client binary in a bash-based shell on Linux or [Windows Subsystem for Linux](#). These commands copy the `osm` client binary to the standard user program location in your `PATH`.

```
sudo mv ./linux-amd64/osm /usr/local/bin/osm
sudo chmod +x /usr/local/bin/osm
```

You can verify the `osm` client library has been correctly added to your path and its version number with the following command.

```
osm version
```

## Download and install the Open Service Mesh (OSM) client binary

In a bash-based shell, use `curl` to download the OSM release and then extract with `tar` as follows:

```
Specify the OSM version that will be leveraged throughout these instructions
OSM_VERSION=v1.2.0

curl -sL "https://github.com/openservicemesh/osm/releases/download/$OSM_VERSION/osm-$OSM_VERSION-darwin-amd64.tar.gz" | tar -vxzf -
```

The `osm` client binary runs on your client machine and allows you to manage OSM in your AKS cluster. Use the following commands to install the OSM `osm` client binary in a bash-based shell. These commands copy the `osm` client binary to the standard user program location in your `PATH`.

```
sudo mv ./darwin-amd64/osm /usr/local/bin/osm
sudo chmod +x /usr/local/bin/osm
```

You can verify the `osm` client library has been correctly added to your path and its version number with the following command.

```
osm version
```

## Download and install the Open Service Mesh (OSM) client binary

In a PowerShell-based shell on Windows, use `Invoke-WebRequest` to download the OSM release and then extract with `Expand-Archive` as follows:

```
Specify the OSM version that will be leveraged throughout these instructions
$OSM_VERSION="v1.2=0"

[Net.ServicePointManager]::SecurityProtocol = "tls12"
$ProgressPreference = 'SilentlyContinue'; Invoke-WebRequest -URI
"https://github.com/openservicemesh/osm/releases/download/$OSM_VERSION/osm-$OSM_VERSION-windows-amd64.zip" -
OutFile "osm-$OSM_VERSION.zip"
Expand-Archive -Path "osm-$OSM_VERSION.zip" -DestinationPath .
```

The `osm` client binary runs on your client machine and allows you to manage the OSM controller in your AKS cluster. Use the following commands to install the OSM `osm` client binary in a PowerShell-based shell on Windows. These commands copy the `osm` client binary to an OSM folder and then make it available both immediately (in current shell) and permanently (across shell restarts) via your `PATH`. You don't need elevated (Admin) privileges to run these commands and you don't need to restart your shell.

```
Copy osm.exe to C:\OSM
New-Item -ItemType Directory -Force -Path "C:\OSM"
Move-Item -Path .\windows-amd64\osm.exe -Destination "C:\OSM\"

Add C:\OSM to PATH.
Make the new PATH permanently available for the current User
$USER_PATH = [environment]::GetEnvironmentVariable("PATH", "User") + ";C:\OSM\"
[environment]::SetEnvironmentVariable("PATH", $USER_PATH, "User")
Make the new PATH immediately available in the current shell
$env:PATH += ";C:\OSM\"
```

### WARNING

Do not attempt to install OSM from the binary using `osm install`. This will result in a installation of OSM that is not integrated as an add-on for AKS.

## Configure OSM CLI variables with an OSM\_CONFIG file

Users can override the default OSM CLI configuration to enhance the add-on experience. This can be done by creating a config file, similar to `kubeconfig`. The config file can be either created at `$HOME/.osm/config.yaml`, or at a different path that is exported using the `OSM_CONFIG` environment variable.

The file must contain the following YAML formatted content:

```
install:
 kind: managed
 distribution: AKS
 namespace: kube-system
```

If the file is not created at `$HOME/.osm/config.yaml`, remember to set the `OSM_CONFIG` environment variable to point to the path where the config file is created.

After setting OSM\_CONFIG, the output of the `osm env` command should be the following:

```
$ osm env

install:
 kind: managed
 distribution: AKS
 namespace: kube-system
```

# Integrations with Open Service Mesh on Azure Kubernetes Service (AKS)

10/27/2022 • 3 minutes to read • [Edit Online](#)

The Open Service Mesh (OSM) add-on integrates with features provided by Azure as well as open source projects.

## IMPORTANT

Integrations with open source projects aren't covered by the [AKS support policy](#).

## Ingress

Ingress allows for traffic external to the mesh to be routed to services within the mesh. With OSM, you can configure most ingress solutions to work with your mesh, but OSM works best with [Web Application Routing](#), [NGINX ingress](#), or [Contour ingress](#). Open source projects integrating with OSM are not covered by the [AKS support policy](#).

At this time, [Azure Gateway Ingress Controller \(AGIC\)](#) only works for HTTP backends. If you configure OSM to use AGIC, AGIC will not be used for other backends such as HTTPS and mTLS.

### Using the Azure Gateway Ingress Controller (AGIC) with the OSM add-on for HTTP ingress

## IMPORTANT

You can't configure [Azure Gateway Ingress Controller \(AGIC\)](#) for HTTPS ingress.

After installing the AGIC ingress controller, create a namespace for the application service, add it to the mesh using the OSM CLI, and deploy the application service to that namespace:

```
Create a namespace
kubectl create ns httpbin

Add the namespace to the mesh
osm namespace add httpbin

Deploy the application

export RELEASE_BRANCH=release-v1.2
kubectl apply -f https://raw.githubusercontent.com/openservicemesh/osm-
docs/$RELEASE_BRANCH/manifests/samples/httpbin/httpbin.yaml -n httpbin
```

Verify that the pods are up and running, and have the envoy sidecar injected:

```
kubectl get pods -n httpbin
```

Example output:

NAME	READY	STATUS	RESTARTS	AGE
httpbin-7c6464475-9wrr8	2/2	Running	0	6d20h

```
kubectl get svc -n httpbin
```

Example output:

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
httpbin	ClusterIP	10.0.92.135	<none>	14001/TCP	6d20h

Next, deploy the following `Ingress` and `IngressBackend` configurations to allow external clients to access the `httpbin` service on port `14001`.

```
kubectl apply -f <<EOF
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 name: httpbin
 namespace: httpbin
 annotations:
 kubernetes.io/ingress.class: azure/application-gateway
spec:
 rules:
 - http:
 paths:
 - path: /
 pathType: Prefix
 backend:
 service:
 name: httpbin
 port:
 number: 14001

kind: IngressBackend
apiVersion: policy.openservicemesh.io/v1alpha1
metadata:
 name: httpbin
 namespace: httpbin
spec:
 backends:
 - name: httpbin
 port:
 number: 14001 # targetPort of httpbin service
 protocol: http
 sources:
 - kind: IPRange
 name: 10.0.0.0/8
EOF
```

Ensure that both the `Ingress` and `IngressBackend` objects have been successfully deployed:

```
kubectl get ingress -n httpbin
```

Example output:

NAME	CLASS	HOSTS	ADDRESS	PORTS	AGE
httpbin	<none>	*	20.85.173.179	80	6d20h

```
kubectl get ingressbackend -n httpbin
```

Example output:

NAME	STATUS
httpbin	committed

Use `kubectl` to display the external IP address of the ingress service.

```
kubectl get ingress -n httpbin
```

Use `curl` to verify you can access the `httpbin` service using the external IP address of the ingress service.

```
curl -sI http://<external-ip>/get
```

Confirm you receive a response with `status 200`.

## Metrics observability

Observability of metrics allows you to view the metrics of your mesh and the deployments in your mesh. With OSM, you can use [Prometheus](#) and [Grafana](#) for metrics observability, but those integrations aren't covered by the [AKS support policy](#).

You can also integrate OSM with [Azure Monitor](#).

Before you can enable metrics on your mesh to integrate with Azure Monitor:

- Enable Azure Monitor on your cluster
- Enable the OSM add-on for your AKS cluster
- Onboard your application namespaces to the mesh

To enable metrics for a namespace in the mesh use `osm metrics enable`. For example:

```
osm metrics enable --namespace myappnamespace
```

Create a Configmap in the `kube-system` namespace that enables Azure Monitor to monitor your namespaces.

For example, create a `monitor-configmap.yaml` with the following to monitor the `myappnamespace`:

```
kind: ConfigMap
apiVersion: v1
data:
 schema-version: v1
 config-version: ver1
 osm-metric-collection-configuration: |-
 # OSM metric collection settings
 [osm_metric_collection_configuration]
 [osm_metric_collection_configuration.settings]
 # Namespaces to monitor
 monitor_namespaces = ["myappnamespace"]
metadata:
 name: container-azm-ms-osmconfig
 namespace: kube-system
```

Apply that ConfigMap using `kubectl apply`.

```
kubectl apply -f monitor-configmap.yaml
```

To access your metrics from the Azure portal, select your AKS cluster, then select *Logs* under *Monitoring*. From the *Monitoring* section, query the `InsightsMetrics` table to view metrics in the enabled namespaces. For example, the following query shows the *envoy* metrics for the *myappnamespace* namespace.

```
InsightsMetrics
| where Name contains "envoy"
| extend t=parse_json(Tags)
| where t.app == "myappnamespace"
```

## Automation and developer tools

OSM can integrate with certain automation projects and developer tooling to help operators and developers build and release applications. For example, OSM integrates with [Flagger](#) for progressive delivery and [Dapr](#) for building applications. OSM's integration with Flagger and Dapr aren't covered by the [AKS support policy](#).

## External authorization

External authorization allows you to offload authorization of HTTP requests to an external service. OSM can use external authorization by integrating with [Open Policy Agent \(OPA\)](#), but that integration isn't covered by the [AKS support policy](#).

## Certificate management

OSM has several types of certificates it uses to operate on your AKS cluster. OSM includes its own certificate manager called [Tresor](#), which is used by default. Alternatively, OSM allows you to integrate with [Hashicorp Vault](#) and [cert-manager](#), but those integrations aren't covered by the [AKS support policy](#).

# Open Service Mesh (OSM) AKS add-on Troubleshooting Guides

10/27/2022 • 5 minutes to read • [Edit Online](#)

When you deploy the OSM AKS add-on, you could possibly experience problems associated with configuration of the service mesh. The following guide will assist you on how to troubleshoot errors and resolve common problems.

## Verifying and Troubleshooting OSM components

### Check OSM Controller Deployment, Pod, and Service

```
kubectl get deployment,pod,service -n kube-system --selector app=osm-controller
```

A healthy OSM Controller would look like this:

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/osm-controller	2/2	2	2	3m4s
NAME	READY	STATUS	RESTARTS	AGE
pod/osm-controller-65bd8c445c-zsp4	1/1	Running	0	2m
pod/osm-controller-65bd8c445c-xqhmk	1/1	Running	0	16s
NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)
service/osm-controller	ClusterIP	10.96.185.178	<none>	15128/TCP,9092/TCP,9091/TCP
service/osm-validator	ClusterIP	10.96.11.78	<none>	9093/TCP

#### NOTE

For the osm-controller services the CLUSTER-IP would be different. The service NAME and PORT(S) must be the same as the example above.

### Check OSM Injector Deployment, Pod, and Service

```
kubectl get deployment,pod,service -n kube-system --selector app=osm-injector
```

A healthy OSM Injector would look like this:

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/osm-injector	2/2	2	2	4m37s
NAME	READY	STATUS	RESTARTS	AGE
pod/osm-injector-5c49bd8d7c-b6cx6	1/1	Running	0	4m21s
pod/osm-injector-5c49bd8d7c-dx587	1/1	Running	0	4m37s
NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)
service/osm-injector	ClusterIP	10.96.236.108	<none>	9090/TCP

### Check OSM Bootstrap Deployment, Pod, and Service

```
kubectl get deployment,pod,service -n kube-system --selector app=osm-bootstrap
```

A healthy OSM Bootstrap would look like this:

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/osm-bootstrap	1/1	1	1	5m25s
NAME	READY	STATUS	RESTARTS	AGE
pod/osm-bootstrap-594fffc6cb7-jc7bs	1/1	Running	0	5m25s
NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)
service/osm-bootstrap	ClusterIP	10.96.250.208	<none>	9443/TCP,9095/TCP

### Check Validating and Mutating webhooks

```
kubectl get ValidatingWebhookConfiguration --selector app=osm-controller
```

A healthy OSM Validating Webhook would look like this:

```
NAME WEBHOOKS AGE
aks-osm-validator-mesh-osm 1 81m
```

```
kubectl get MutatingWebhookConfiguration --selector app=osm-injector
```

A healthy OSM Mutating Webhook would look like this:

```
NAME WEBHOOKS AGE
aks-osm-webhook-osm 1 102m
```

#### Check for the service and the CA bundle of the Validating webhook

```
kubectl get ValidatingWebhookConfiguration aks-osm-validator-mesh-osm -o json | jq
'.webhooks[0].clientConfig.service'
```

A well configured Validating Webhook Configuration would look exactly like this:

```
{
 "name": "osm-config-validator",
 "namespace": "kube-system",
 "path": "/validate-webhook",
 "port": 9093
}
```

#### Check for the service and the CA bundle of the Mutating webhook

```
kubectl get MutatingWebhookConfiguration aks-osm-webhook-osm -o json | jq
'.webhooks[0].clientConfig.service'
```

A well configured Mutating Webhook Configuration would look exactly like this:

```
{
 "name": "osm-injector",
 "namespace": "kube-system",
 "path": "/mutate-pod-creation",
 "port": 9090
}
```

#### Check the `osm-mesh-config` resource

Check for the existence:

```
kubectl get meshconfig osm-mesh-config -n kube-system
```

Check the content of the OSM MeshConfig

```
kubectl get meshconfig osm-mesh-config -n kube-system -o yaml
```

```

apiVersion: config.openservicemesh.io/v1alpha1
kind: MeshConfig
metadata:
 creationTimestamp: "0000-00-00A00:00:00A"
 generation: 1
 name: osm-mesh-config
 namespace: kube-system
 resourceVersion: "2494"
 uid: 6c4d67f3-c241-4aeb-bf4f-b029b08faa31
spec:
 certificate:
 serviceCertValidityDuration: 24h
 featureFlags:
 enableEgressPolicy: true
 enableMultiClusterMode: false
 enableWASMStats: true
 observability:
 enableDebugServer: true
 osmLogLevel: info
 tracing:
 address: jaeger.kube-system.svc.cluster.local
 enable: false
 endpoint: /api/v2/spans
 port: 9411
 sidecar:
 configResyncInterval: 0s
 enablePrivilegedInitContainer: false
 envoyImage: mcr.microsoft.com/oss/envoyproxy/envoy:v1.18.3
 initContainerImage: mcr.microsoft.com/oss/openservicemesh/init:v0.9.1
 logLevel: error
 maxDataPlaneConnections: 0
 resources: {}
 traffic:
 enableEgress: true
 enablePermissiveTrafficPolicyMode: true
 inboundExternalAuthorization:
 enable: false
 failureModeAllow: false
 statPrefix: inboundExtAuthz
 timeout: 1s
 useHTTPSI ingress: false

```

`osm-mesh-config` resource values:

KEY	TYPE	DEFAULT VALUE	KUBECTL PATCH COMMAND EXAMPLES
spec.traffic.enableEgress	bool	true	<code>kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"traffic": {"enableEgress":true}}}' --type=merge</code>
spec.traffic.enablePermissiveTrafficPolicyMode	bool	true	<code>kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"traffic":{"enablePermissiveTrafficPolicyMode":true}}}' --type=merge</code>
spec.traffic.useHTTPSI ngress	bool	false	<code>kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"traffic": {"useHTTPSI ngress":true}}}' --type=merge</code>
spec.traffic.outboundPortExclusionList	array	[]	<code>kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"traffic": {"outboundPortExclusionList": [6379,8080]}}}' --type=merge</code>
spec.traffic.outboundIPRangeExclusionList	array	[]	<code>kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"traffic": {"outboundIPRangeExclusionList": ["10.0.0.0/32","1.1.1.1/24"]}}}' --type=merge</code>
spec.traffic.inboundPortExclusionList	array	[]	<code>kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"traffic": {"inboundPortExclusionList": [6379,8080]}}}' --type=merge</code>
spec.certificate.serviceCertValidityDuration	string	"24h"	<code>kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"certificate": {"serviceCertValidityDuration":"24h"}}}' --type=merge</code>

KEY	TYPE	DEFAULT VALUE	KUBECTL PATCH COMMAND EXAMPLES
spec.observability.enableDebugServer	bool	true	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"observability":{"enableDebugServer":true}}}' --type=merge
spec.observability.tracing.enabled	bool	false	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"observability":{"tracing":{"enabled":true}}}}' --type=merge
spec.observability.tracing.address	string	"jaeger.kube-system.svc.cluster.local"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"observability":{"tracing":{"address":"jaeger.kube-system.svc.cluster.local"}}}}' --type=merge
spec.observability.tracing.endpoint	string	"/api/v2/spans"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"observability":{"tracing":{"endpoint":"/api/v2/spans"}}}}' --type=merge
spec.observability.tracing.port	int	9411	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"observability":{"tracing":{"port":9411}}}}' --type=merge
spec.observability.tracing.osmLogLevel	string	"info"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"observability":{"tracing":{"osmLogLevel":"info"}}}}' --type=merge
spec.sidecar.enablePrivilegedInitContainer	bool	false	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"sidecar":{"enablePrivilegedInitContainer":true}}}' --type=merge
spec.sidecar.logLevel	string	"error"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"sidecar":{"logLevel":"error"}}}' --type=merge
spec.sidecar.maxDataPlaneConnections	int	0	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"sidecar":{"maxDataPlaneConnections":"error"}}}' --type=merge
spec.sidecar.envoyImage	string	"mcr.microsoft.com/oss/envoy"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"sidecar":{"envoyImage":"mcr.microsoft.com/oss/envoyproxy/envoy:v1"}}}' --type=merge
spec.sidecar.initContainerImage	string	"mcr.microsoft.com/oss/open-service-init:v1"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"sidecar":{"initContainerImage":"mcr.microsoft.com/oss/open-service-init:v1"}}}' --type=merge
spec.sidecar.configResyncInterval	string	"30s"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"sidecar":{"configResyncInterval":"30s"}}}' --type=merge
spec.featureFlags.enableWASMStats	bool	true	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"featureFlags":{"enableWASMStats":true}}}' --type=merge
spec.featureFlags.enableEgressPolicy	bool	true	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec":{"featureFlags":{"enableEgressPolicy":true}}}' --type=merge

KEY	TYPE	DEFAULT VALUE	KUBECTL PATCH COMMAND EXAMPLES
spec.featureFlags.enableMultiClusterMode	bool	"false"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"featureFlags": {"enableMultiClusterMode": "false"}}}' --type=merge
spec.featureFlags.enableSnapshotCacheMode	bool	"false"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"featureFlags": {"enableSnapshotCacheMode": "false"}}}' --type=merge
spec.featureFlags.enableAsyncProxyServiceMapping	bool	"false"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"featureFlags": {"enableAsyncProxyServiceMapping": "false"}}}' --type=merge
spec.featureFlags.enableIngressBackendPolicy	bool	"true"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"featureFlags": {"enableIngressBackendPolicy": "true"}}}' --type=merge
spec.featureFlags.enableEnvoyActiveHealthChecks	bool	"false"	kubectl patch meshconfig osm-mesh-config -n kube-system -p '{"spec": {"featureFlags": {"enableEnvoyActiveHealthChecks": "false"}}}' --type=merge

## Check Namespaces

### NOTE

The kube-system namespace will never participate in a service mesh and will never be labeled and/or annotated with the key/values below.

We use the `osm namespace add` command to join namespaces to a given service mesh. When a k8s namespace is part of the mesh (or for it to be part of the mesh) the following must be true:

View the annotations with

```
kubectl get namespace bookbuyer -o json | jq '.metadata.annotations'
```

The following annotation must be present:

```
{
 "openservicemesh.io/sidecar-injection": "enabled"
}
```

View the labels with

```
kubectl get namespace bookbuyer -o json | jq '.metadata.labels'
```

The following label must be present:

```
{
 "openservicemesh.io/monitored-by": "osm"
}
```

If a namespace is not annotated with `"openservicemesh.io/sidecar-injection": "enabled"` or not labeled with `"openservicemesh.io/monitored-by": "osm"` the OSM Injector will not add Envoy sidecars.

### NOTE

After `osm namespace add` is called only new pods will be injected with an Envoy sidecar. Existing pods must be restarted with `kubectl rollout restart deployment ...`

## Verify OSM CRDs:

Check whether the cluster has the required CRDs:

```
kubectl get crds
```

We must have the following installed on the cluster:

- `egresses.policy.openservicemesh.io`

- httproutegroups.specs.smi-spec.io
- ingressbackends.policy.openservicemesh.io
- meshconfigs.config.openservicemesh.io
- multiclusterservices.config.openservicemesh.io
- tcproutes.specs.smi-spec.io
- trafficsplits.split.smi-spec.io
- traffictargets.access.smi-spec.io

Get the versions of the SMI CRDs installed with this command:

```
osm mesh list
```

Expected output:

```
MESH NAME MESH NAMESPACE VERSION ADDED NAMESPACES
osm kube-system v0.11.1

MESH NAME MESH NAMESPACE SMI SUPPORTED
osm kube-system

HTTPRouteGroup:v1alpha4, TCPRoute:v1alpha4, TrafficSplit:v1alpha2, TrafficTarget:v1alpha3

To list the OSM controller pods for a mesh, please run the following command passing in the mesh's namespace
kubectl get pods -n <osm-mesh-namespace> -l app=osm-controller
```

OSM Controller v0.11.1 requires the following versions:

- traffictargets.access.smi-spec.io - [v1alpha3](#)
- httproutegroups.specs.smi-spec.io - [v1alpha4](#)
- tcproutes.specs.smi-spec.io - [v1alpha4](#)
- udproutes.specs.smi-spec.io - Not supported
- trafficsplits.split.smi-spec.io - [v1alpha2](#)
- \*.metrics.smi-spec.io - [v1alpha1](#)

#### Certificate management

Information on how OSM issues and manages certificates to Envoy proxies running on application pods can be found on the [OpenServiceMesh docs site](#).

#### Upgrading Envoy

When a new pod is created in a namespace monitored by the add-on, OSM will inject an [envoy proxy sidecar](#) in that pod. Information regarding how to update the envoy version can be found in the [Upgrade Guide](#) on the OpenServiceMesh docs site.

# Uninstall the Open Service Mesh (OSM) add-on from your Azure Kubernetes Service (AKS) cluster

10/27/2022 • 2 minutes to read • [Edit Online](#)

This article shows you how to uninstall the OMS add-on and related resources from your AKS cluster.

## Disable the OSM add-on from your cluster

Disable the OSM add-on in your cluster using `az aks disable-addon`. For example:

```
az aks disable-addons \
--resource-group myResourceGroup \
--name myAKSCluster \
--addons open-service-mesh
```

The above example removes the OSM add-on from the *myAKSCluster* in *myResourceGroup*.

## Remove additional OSM resources

After the OSM add-on is disabled, use `osm uninstall cluster-wide-resources` to uninstall the remaining resource on the cluster. For example:

```
osm uninstall cluster-wide-resources
```

### IMPORTANT

You must remove these additional resources after you disable the OSM add-on. Leaving these resources on your cluster may cause issues if you enable the OSM add-on again in the future.

# AKS release tracker

10/27/2022 • 2 minutes to read • [Edit Online](#)

AKS releases weekly rounds of fixes and feature and component updates that affect all clusters and customers. However, these releases can take up to two weeks to roll out to all regions from the initial time of shipping due to Azure Safe Deployment Practices (SDP). It is important for customers to know when a particular AKS release is hitting their region, and the AKS release tracker provides these details in real time by versions and regions.

## Why release tracker?

With AKS release tracker, customers can follow specific component updates present in an AKS version release, such as fixes shipped to a core add-on. In addition to providing real-time updates of region release status, the tracker also links to the specific version of the AKS [release notes](#) to help customers identify which instance of the release is relevant to them. As the data is updated in real time, customers can track the entire SDP process with a single tool.

## How to use the release tracker

To view the release tracker, visit the [AKS release status webpage](#).

The top half of the tracker shows the latest and 3 previously available release versions for each region, and links to the corresponding release notes entry. This view is helpful when you want to track the available versions by region.

### AKS Release Status

Last Update Time: 2022-04-03 01:02:03

#### Regional Status

Region	Currently in Operation	Last Three Versions
West Central US	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
East US	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
Brazil South	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
Canada Central	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
East US2	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
North Central US	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
West US2	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
Brazil Southeast	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
Canada East	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
Central US	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
South Central US	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
West US	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>
West US3	<a href="#">V20220403</a>	<a href="#">V20220327</a> , <a href="#">V20220320</a> , <a href="#">V20220313</a>

The bottom half of the tracker shows the SDP process. The table has two views: one shows the latest version and status update for each grouping of regions and the other shows the status and region availability of each currently supported version.

## SDP Process

Order	Regions	Version	Status
1	Canary	V20220403	In-progress
2	West Central US	V20220403	Finished
3	UK South	V20220403	Finished
4	East US	V20220327	Finished
5	Australia Central, Australia East	V20220403	Finished
6	Brazil South, Canada Central, Central India, East Asia	V20220403	Finished
7	East US2, France Central, Germany West Central, Japan East, Jioindia West, Korea Central, North Central US, North Europe, Norway East, Qatar Central, South Africa North, Sweden Central, Switzerland North, UAE North, UK West, West US2	V20220320	In-progress
8	Australia Central2, Australia Southeast, Brazil Southeast, Canada East, Central US, France South, Germany North, Japan West, Jioindia Central, Korea South, Norway West, South Africa West, South Central US, South East Asia, South India, Sweden South, Switzerland West, UAE Central, West Europe, West US, West US3	V20220403	Finished

# Simplified application autoscaling with Kubernetes Event-driven Autoscaling (KEDA) add-on (Preview)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Kubernetes Event-driven Autoscaling (KEDA) is a single-purpose and lightweight component that strives to make application autoscaling simple and is a CNCF Incubation project.

It applies event-driven autoscaling to scale your application to meet demand in a sustainable and cost-efficient manner with scale-to-zero.

The KEDA add-on makes it even easier by deploying a managed KEDA installation, providing you with a rich catalog of 50+ KEDA scalers that you can scale your applications with on your Azure Kubernetes Services (AKS) cluster.

## IMPORTANT

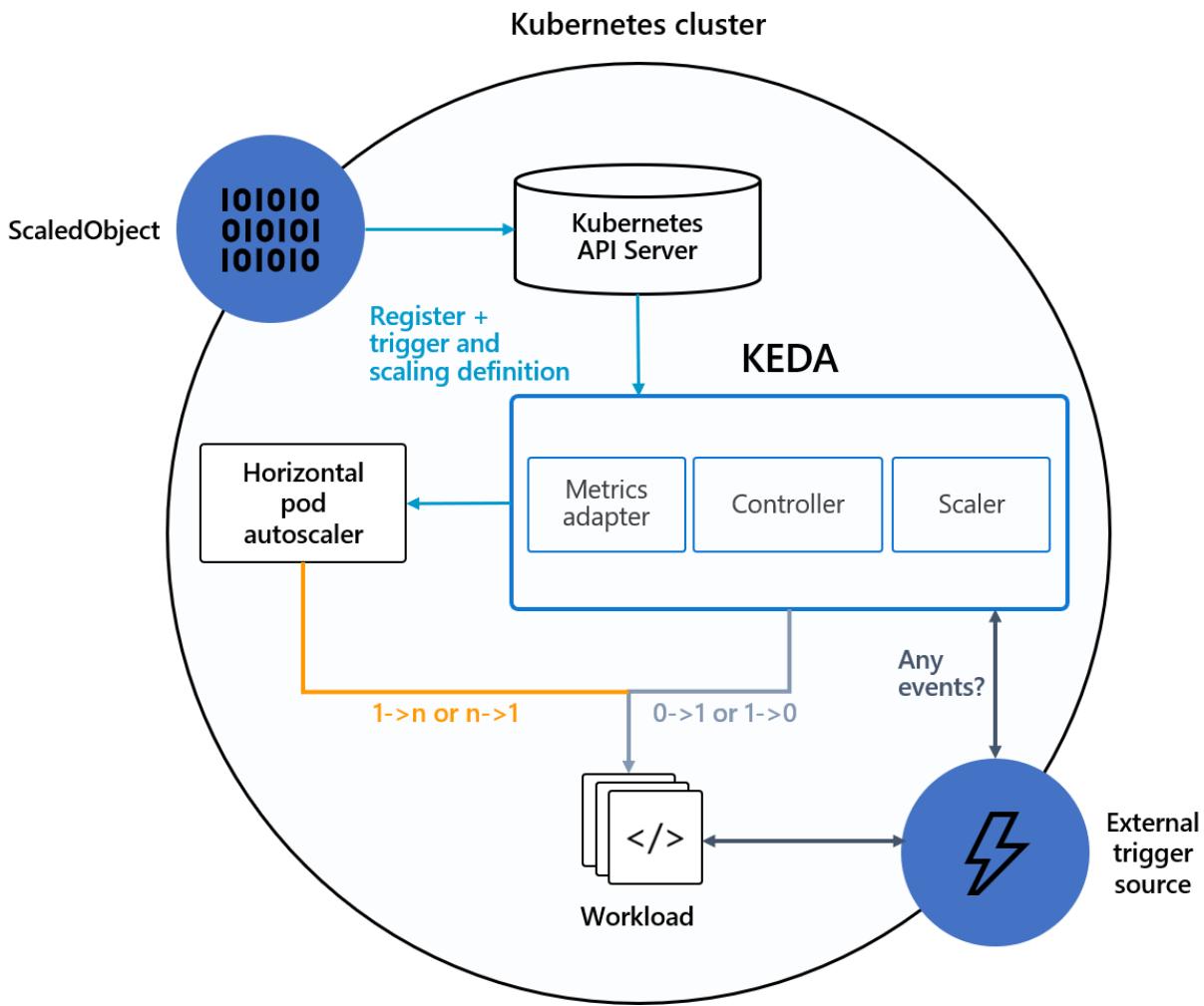
AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Architecture

[KEDA](#) provides two main components:

- **KEDA operator** allows end-users to scale workloads in/out from 0 to N instances with support for Kubernetes Deployments, Jobs, StatefulSets or any custom resource that defines `/scale` subresource.
- **Metrics server** exposes external metrics to Horizontal Pod Autoscaler (HPA) in Kubernetes for autoscaling purposes such as messages in a Kafka topic, or number of events in an Azure event hub. Due to upstream limitations, KEDA must be the only installed metric adapter.



Learn more about how KEDA works in the [official KEDA documentation](#).

## Installation and version

KEDA can be added to your Azure Kubernetes Service (AKS) cluster by enabling the KEDA add-on using an [ARM template](#) or [Azure CLI](#).

The KEDA add-on provides a fully supported installation of KEDA that is integrated with AKS.

### IMPORTANT

The KEDA add-on installs version 2.7.0 of KEDA on your cluster.

## Capabilities and features

KEDA provides the following capabilities and features:

- Build sustainable and cost-efficient applications with scale-to-zero
- Scale application workloads to meet demand using [a rich catalog of 50+ KEDA scalers](#)
- Autoscale applications with `ScaledObjects`, such as Deployments, StatefulSets or any custom resource that defines `/scale` subresource
- Autoscale job-like workloads with `ScaledJobs`
- Use production-grade security by decoupling autoscaling authentication from workloads
- Bring-your-own external scaler to use tailor-made autoscaling decisions

## Add-on limitations

The KEDA AKS add-on has the following limitations:

- KEDA's [HTTP add-on \(preview\)](#) to scale HTTP workloads isn't installed with the extension, but can be deployed separately.
- KEDA's [external scaler for Azure Cosmos DB](#) to scale based on Azure Cosmos DB change feed isn't installed with the extension, but can be deployed separately.
- Only one metric server is allowed in the Kubernetes cluster. Because of that the KEDA add-on should be the only metrics server inside the cluster.
  - Multiple KEDA installations aren't supported
- Managed identity isn't supported.

For general KEDA questions, we recommend [visiting the FAQ overview](#).

## Next steps

- [Enable the KEDA add-on with an ARM template](#)
- [Enable the KEDA add-on with the Azure CLI](#)
- [Troubleshoot KEDA add-on problems](#)
- [Autoscale a .NET Core worker processing Azure Service Bus Queue messages](#)

# Install the Kubernetes Event-driven Autoscaling (KEDA) add-on by using ARM template

10/27/2022 • 2 minutes to read • [Edit Online](#)

This article shows you how to deploy the Kubernetes Event-driven Autoscaling (KEDA) add-on to Azure Kubernetes Service (AKS) by using an [ARM](#) template.

## IMPORTANT

The KEDA add-on installs version *2.7.0* of KEDA on your cluster.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI installed](#).
- Firewall rules are configured to allow access to the Kubernetes API server. ([learn more](#))

### Register the `AKS-KedaPreview` feature flag

To use the KEDA, you must enable the `AKS-KedaPreview` feature flag on your subscription.

```
az feature register --name AKS-KedaPreview --namespace Microsoft.ContainerService
```

You can check on the registration status by using the `az feature list` command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/AKS-KedaPreview')].{Name:name,State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider by using the `az provider register` command:

```
az provider register --namespace Microsoft.ContainerService
```

## Install the KEDA add-on with Azure Resource Manager (ARM) templates

The KEDA add-on can be enabled by deploying an AKS cluster with an Azure Resource Manager template and

specifying the `workloadAutoScalerProfile` field:

```
"workloadAutoScalerProfile": {
 "keda": {
 "enabled": true
 }
}
```

## Connect to your AKS cluster

To connect to the Kubernetes cluster from your local computer, you use [kubectl](#), the Kubernetes command-line client.

If you use the Azure Cloud Shell, `kubectl` is already installed. You can also install it locally using the [az aks install-cli](#) command:

```
az aks install-cli
```

To configure `kubectl` to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command. The following example gets credentials for the AKS cluster named *MyAKSCluster* in the *MyResourceGroup*.

```
az aks get-credentials --resource-group MyResourceGroup --name MyAKSCluster
```

## Example deployment

The following snippet is a sample deployment that creates a cluster with KEDA enabled with a single node pool comprised of three `DS2_v5` nodes.

```
{
 "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
 "contentVersion": "1.0.0.0",
 "resources": [
 {
 "apiVersion": "2022-05-02-preview",
 "dependsOn": [],
 "type": "Microsoft.ContainerService/managedClusters",
 "location": "westcentralus",
 "name": "myAKSCluster",
 "properties": {
 "kubernetesVersion": "1.23.5",
 "enableRBAC": true,
 "dnsPrefix": "myAKSCluster",
 "agentPoolProfiles": [
 {
 "name": "agentpool",
 "osDiskSizeGB": 200,
 "count": 3,
 "enableAutoScaling": false,
 "vmSize": "Standard_D2S_v5",
 "osType": "Linux",
 "storageProfile": "ManagedDisks",
 "type": "VirtualMachineScaleSets",
 "mode": "System",
 "maxPods": 110,
 "availabilityZones": [],
 "nodeTaints": [],
 "enableNodePublicIP": false
 }
],
 "networkProfile": {
 "loadBalancerSku": "standard",
 "networkPlugin": "kubenet"
 },
 "workloadAutoScalerProfile": {
 "keda": {
 "enabled": true
 }
 },
 "identity": {
 "type": "SystemAssigned"
 }
 }
]
 }
}
```

## Start scaling apps with KEDA

Now that KEDA is installed, you can start autoscaling your apps with KEDA by using its custom resource definition has been defined (CRD).

To learn more about KEDA CRDs, follow the official [KEDA documentation](#) to define your scaler.

## Clean Up

To remove the resource group, and all related resources, use the [Az PowerShell module group delete](#) command:

```
az group delete --name MyResourceGroup
```

## Next steps

This article showed you how to install the KEDA add-on on an AKS cluster, and then verify that it's installed and running. With the KEDA add-on installed on your cluster, you can [deploy a sample application](#) to start scaling apps.

You can troubleshoot KEDA add-on problems in [this article](#).

# Install the Kubernetes Event-driven Autoscaling (KEDA) add-on by using Azure CLI

10/27/2022 • 3 minutes to read • [Edit Online](#)

This article shows you how to install the Kubernetes Event-driven Autoscaling (KEDA) add-on to Azure Kubernetes Service (AKS) by using Azure CLI. The article includes steps to verify that it's installed and running.

## IMPORTANT

The KEDA add-on installs version *2.7.0* of KEDA on your cluster.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI installed](#).
- Firewall rules are configured to allow access to the Kubernetes API server. ([learn more](#))

### Install the extension `aks-preview`

Install the `aks-preview` extension in the AKS cluster to make sure you have the latest version of AKS extension before installing KEDA add-on.

```
az extension add --upgrade --name aks-preview
```

### Register the `AKS-KedaPreview` feature flag

To use the KEDA, you must enable the `AKS-KedaPreview` feature flag on your subscription.

```
az feature register --name AKS-KedaPreview --namespace Microsoft.ContainerService
```

You can check on the registration status by using the `az feature list` command:

```
az feature list -o table --query "[?contains(name, 'Microsoft.ContainerService/AKS-KedaPreview')].{Name:name,State:properties.state}"
```

When ready, refresh the registration of the *Microsoft.ContainerService* resource provider by using the `az provider register` command:

```
az provider register --namespace Microsoft.ContainerService
```

## Install the KEDA add-on with Azure CLI

To install the KEDA add-on, use `--enable-keda` when creating or updating a cluster.

The following example creates a *myResourceGroup* resource group. Then it creates a *myAKSCluster* cluster with the KEDA add-on.

```
az group create --name myResourceGroup --location eastus

az aks create \
--resource-group myResourceGroup \
--name myAKSCluster \
--enable-keda
```

For existing clusters, use `az aks update` with `--enable-keda` option. The following code shows an example.

```
az aks update \
--resource-group myResourceGroup \
--name myAKSCluster \
--enable-keda
```

## Get the credentials for your cluster

Get the credentials for your AKS cluster by using the `az aks get-credentials` command. The following example command gets the credentials for *myAKSCluster* in the *myResourceGroup* resource group:

```
az aks get-credentials --resource-group myResourceGroup --name myAKSCluster
```

## Verify that the KEDA add-on is installed on your cluster

To see if the KEDA add-on is installed on your cluster, verify that the `enabled` value is `true` for `keda` under `workloadAutoScalerProfile`.

The following example shows the status of the KEDA add-on for *myAKSCluster* in *myResourceGroup*.

```
az aks show -g "myResourceGroup" --name myAKSCluster --query "workloadAutoScalerProfile.keda.enabled"
```

## Verify that KEDA is running on your cluster

You can verify KEDA that's running on your cluster. Use `kubectl` to display the operator and metrics server installed in the AKS cluster under `kube-system` namespace. For example:

```
kubectl get pods -n kube-system
```

The following example output shows that the KEDA operator and metrics API server are installed in the AKS cluster along with its status.

```
kubectl get pods -n kube-system

keda-operator-*****-k5rfv 1/1 Running 0 43m
keda-operator-metrics-apiserver-*****-sj857 1/1 Running 0 43m
```

To verify the version of your KEDA, use `kubectl get crd/scaledobjects.keda.sh -o yaml`. For example:

```
kubectl get crd/scaledobjects.keda.sh -o yaml
```

The following example output shows the configuration of KEDA in the `app.kubernetes.io/version` label:

```
kind: CustomResourceDefinition
metadata:
 annotations:
 controller-gen.kubebuilder.io/version: v0.8.0
 creationTimestamp: "2022-06-08T10:31:06Z"
 generation: 1
 labels:
 addonmanager.kubernetes.io/mode: Reconcile
 app.kubernetes.io/component: operator
 app.kubernetes.io/name: keda-operator
 app.kubernetes.io/part-of: keda-operator
 app.kubernetes.io/version: 2.7.0
 name: scaledobjects.keda.sh
 resourceVersion: "2899"
 uid: 85b8dec7-c3da-4059-8031-5954dc888a0b
spec:
 conversion:
 strategy: None
 group: keda.sh
 names:
 kind: ScaledObject
 listKind: ScaledObjectList
 plural: scaledobjects
 shortNames:
 - so
 singular: scaledobject
 scope: Namespaced
 # Redacted for simplicity
```

While KEDA provides various customization options, the KEDA add-on currently provides basic common configuration.

If you have requirement to run with another custom configurations, such as namespaces that should be watched or tweaking the log level, then you may edit the KEDA YAML manually and deploy it.

However, when the installation is customized there will no support offered for custom configurations.

## Disable KEDA add-on from your AKS cluster

When you no longer need KEDA add-on in the cluster, use the `az aks update` command with `--disable-keda` option. This execution will disable KEDA workload auto-scaler.

```
az aks update \
 --resource-group myResourceGroup \
 --name myAKSCluster \
 --disable-keda
```

## Next steps

This article showed you how to install the KEDA add-on on an AKS cluster using Azure CLI. The steps to verify that KEDA add-on is installed and running are included. With the KEDA add-on installed on your cluster, you can [deploy a sample application](#) to start scaling apps.

You can troubleshoot KEDA add-on problems in [this article](#).

# Integrations with Kubernetes Event-driven Autoscaling (KEDA) on Azure Kubernetes Service (AKS) (Preview)

10/27/2022 • 2 minutes to read • [Edit Online](#)

The Kubernetes Event-driven Autoscaling (KEDA) add-on integrates with features provided by Azure and open source projects.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## IMPORTANT

Integrations with open source projects are not covered by the [AKS support policy](#).

## Observe your autoscaling with Kubernetes events

KEDA automatically emits Kubernetes events allowing customers to operate their application autoscaling.

To learn about the available metrics, we recommend reading the [KEDA documentation](#).

## Scalers for Azure services

KEDA can integrate with various tools and services through [a rich catalog of 50+ KEDA scalers](#). It supports leading cloud platforms (such as Azure) and open-source technologies such as Redis and Kafka.

It leverages the following scalers for Azure services:

- [Azure Application Insights](#)
- [Azure Blob Storage](#)
- [Azure Data Explorer](#)
- [Azure Event Hubs](#)
- [Azure Log Analytics](#)
- [Azure Monitor](#)
- [Azure Pipelines](#)
- [Azure Service Bus](#)
- [Azure Storage Queue](#)

Next to the built-in scalers, you can install external scalers yourself to autoscale on other Azure services:

- [Azure Cosmos DB \(Change feed\)](#)

However, these external scalers aren't supported as part of the add-on and rely on community support.

## Next steps

- [Enable the KEDA add-on with an ARM template](#)
- [Enable the KEDA add-on with the Azure CLI](#)
- [Troubleshoot KEDA add-on problems](#)
- [Autoscale a .NET Core worker processing Azure Service Bus Queue message](#)

# Web Application Routing (Preview)

10/27/2022 • 11 minutes to read • [Edit Online](#)

The Web Application Routing add-on configures an [Ingress controller](#) in your Azure Kubernetes Service (AKS) cluster with SSL termination through certificates stored in Azure Key Vault. Optionally, it also integrates with Open Service Mesh (OSM) for end-to-end encryption of inter cluster communication using mutual TLS (mTLS). As applications are deployed, the add-on creates publicly accessible DNS names for endpoints.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## Limitations

- Web Application Routing currently doesn't support named ports in ingress backend.

## Web Application Routing add-on overview

The add-on deploys the following components:

- [nginx ingress controller](#): The ingress controller exposed to the internet.
- [external-dns controller](#): Watches for Kubernetes Ingress resources and creates DNS A records in the cluster-specific DNS zone. Note that this is only deployed when you pass in the `--dns-zone-resource-id` argument.

## Prerequisites

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI installed](#).
- An Azure Key Vault to store certificates.
- A DNS solution, such as [Azure DNS](#).

### Install the `aks-preview` Azure CLI extension

You also need the `aks-preview` Azure CLI extension version `0.5.75` or later. Install the `aks-preview` Azure CLI extension by using the [az extension add](#) command. Or install any available updates by using the [az extension update](#) command.

```
Install the aks-preview extension
az extension add --name aks-preview

Update the extension to make sure you have the latest version installed
az extension update --name aks-preview
```

### Create and export a self-signed SSL certificate (if you don't already own one)

If you already have an SSL certificate, you can skip this step, otherwise you can use these commands to create a self-signed SSL certificate to use with the Ingress. You will need to replace <Hostname> with the DNS name that you will be using.

```
Create a self-signed SSL certificate
openssl req -new -x509 -nodes -out aks-ingress-tls.crt -keyout aks-ingress-tls.key -subj "/CN=<Hostname>" -
addext "subjectAltName=DNS:<Hostname>"

Export the SSL certificate, skipping the password prompt
openssl pkcs12 -export -in aks-ingress-tls.crt -inkey aks-ingress-tls.key -out aks-ingress-tls.pfx
```

### Create an Azure Key Vault to store the certificate

If you don't already have an Azure Key Vault, use this command to create one. Azure Key Vault is used to securely store the SSL certificates that will be loaded into the Ingress.

```
az keyvault create -g <ResourceGroupName> -l <Location> -n <KeyVaultName>
```

### Import certificate to Azure Key Vault

Import the SSL certificate into Azure Key Vault.

```
az keyvault certificate import --vault-name <KeyVaultName> -n <KeyVaultCertificateName> -f aks-ingress-
tls.pfx
```

### Create an Azure DNS zone

If you want the add-on to automatically manage creating hostnames via Azure DNS, you need to [create an Azure DNS zone](#) if you don't have one already.

```
Create a DNS zone
az network dns zone create -g <ResourceGroupName> -n <ZoneName>
```

## Enable Web Application Routing via the Azure CLI

The Web Application Routing routing add-on can be enabled with the Azure CLI when deploying an AKS cluster. To do so, use the `az aks create` command with the `--enable-addons` argument. You can also enable Web Application Routing on an existing AKS cluster using the `az aks enable-addons` command.

- [With Open Service Mesh \(OSM\)](#)
- [Without Open Service Mesh \(OSM\)](#)

The following additional add-ons are required:

- **azure-keyvault-secrets-provider**: The Secret Store CSI provider for Azure Key Vault is required to retrieve the certificates from Azure Key Vault.
- **open-service-mesh**: If you require encrypted intra cluster traffic (recommended) between the nginx ingress and your services, the Open Service Mesh add-on is required which provides mutual TLS (mTLS).

## IMPORTANT

To enable the add-on to reload certificates from Azure Key Vault when they change, you should enable the [secret autorotation feature](#) of the Secret Store CSI driver with the `--enable-secret-rotation` argument. When the autorotation is enabled, the driver updates the pod mount and the Kubernetes secret by polling for changes periodically, based on the rotation poll interval you can define. The default rotation poll interval is 2 minutes.

```
az aks create -g <ResourceGroupName> -n <ClusterName> -l <Location> --enable-addons azure-keyvault-secrets-provider,open-service-mesh,web_application_routing --generate-ssh-keys --enable-secret-rotation
```

To enable Web Application Routing on an existing cluster, add the `--addons` parameter and specify `web_application_routing` as shown in the following example:

```
az aks enable-addons -g <ResourceGroupName> -n <ClusterName> --addons azure-keyvault-secrets-provider,open-service-mesh,web_application_routing --enable-secret-rotation
```

## NOTE

To use the add-on with Open Service Mesh, you should install the `osm` command-line tool. This command-line tool contains everything needed to configure and manage Open Service Mesh. The latest binaries are available on the [OSM GitHub releases page](#).

## Retrieve the add-on's managed identity object ID

Retrieve user managed identity object ID for the add-on. This will be used in the next steps to grant permissions against the Azure DNS zone and the Azure Key Vault. Provide your `<ResourceGroupName>`, `<ClusterName>`, and `<Location>` in the script below which will retrieve the managed identity's object ID.

```
Provide values for your environment
RGNAME=<ResourceGroupName>
CLUSTERNAME=<ClusterName>
LOCATION=<Location>

Retrieve user managed identity object ID for the add-on
SUBSCRIPTION_ID=$(az account show --query id --output tsv)
MANAGEDIDENTITYNAME="webapprouting-${CLUSTERNAME}"
MCRGNAME=$(az aks show -g ${RGNAME} -n ${CLUSTERNAME} --query nodeResourceGroup -o tsv)
USERMANAGEDIDENTITY_RESOURCEID="/subscriptions/${SUBSCRIPTION_ID}/resourceGroups/${MCRGNAME}/providers/Microsoft.ManagedIdentity/userAssignedIdentities/${MANAGEDIDENTITYNAME}"
MANAGEDIDENTITY_OBJECTID=$(az resource show --id $USERMANAGEDIDENTITY_RESOURCEID --query "properties.principalId" -o tsv | tr -d '[:space:]')
```

## Configure the add-on to use Azure DNS to manage creating DNS zones

If you are going to use Azure DNS, update the add-on to pass in the `--dns-zone-resource-id`.

Retrieve the resource ID for the DNS zone.

```
ZONEID=$(az network dns zone show -g <ResourceGroupName> -n <ZoneName> --query "id" --output tsv)
```

Grant **DNS Zone Contributor** permissions on the DNS zone to the add-on's managed identity.

```
az role assignment create --role "DNS Zone Contributor" --assignee $MANAGEDIDENTITY_OBJECTID --scope $ZONEID
```

Update the add-on to enable the integration with Azure DNS. This will create the **external-dns** controller.

```
az aks addon update -g <ResourceGroupName> -n <ClusterName> --addon web_application_routing --dns-zone-resource-id=$ZONEID
```

## Grant the add-on permissions to retrieve certificates from Azure Key Vault

The Web Application Routing add-on creates a user created managed identity in the cluster resource group. This managed identity will need to be granted permissions to retrieve SSL certificates from the Azure Key Vault.

Grant **GET** permissions for the Web Application Routing add-on to retrieve certificates from Azure Key Vault:

```
az keyvault set-policy --name <KeyVaultName> --object-id $MANAGEDIDENTITY_OBJECTID --secret-permissions get --certificate-permissions get
```

## Connect to your AKS cluster

To connect to the Kubernetes cluster from your local computer, you use [kubectl](#), the Kubernetes command-line client.

If you use the Azure Cloud Shell, **kubectl** is already installed. You can also install it locally using the

```
az aks install-cli
```

```
az aks install-cli
```

To configure **kubectl** to connect to your Kubernetes cluster, use the [az aks get-credentials](#) command.

```
az aks get-credentials -g <ResourceGroupName> -n <ClusterName>
```

## Deploy an application

Web Application Routing uses annotations on Kubernetes Ingress objects to create the appropriate resources, create records on Azure DNS (when configured), and retrieve the SSL certificates from Azure Key Vault.

- [With Open Service Mesh \(OSM\)](#)
- [Without Open Service Mesh \(OSM\)](#)

### Create the application namespace

For the sample application environment, let's first create a namespace called **hello-web-app-routing** to run the example pods:

```
kubectl create namespace hello-web-app-routing
```

We also need to add the application namespace to the OSM control plane:

```
osm namespace add hello-web-app-routing
```

## Create the deployment

Create a file named **deployment.yaml** and copy in the following YAML.

```
apiVersion: apps/v1
kind: Deployment
metadata:
 name: aks-helloworld
spec:
 replicas: 1
 selector:
 matchLabels:
 app: aks-helloworld
 template:
 metadata:
 labels:
 app: aks-helloworld
 spec:
 containers:
 - name: aks-helloworld
 image: mcr.microsoft.com/azuredocs/aks-helloworld:v1
 ports:
 - containerPort: 80
 env:
 - name: TITLE
 value: "Welcome to Azure Kubernetes Service (AKS)"
```

## Create the service

Create a file named **service.yaml** and copy in the following YAML.

```
apiVersion: v1
kind: Service
metadata:
 name: aks-helloworld
spec:
 type: ClusterIP
 ports:
 - port: 80
 selector:
 app: aks-helloworld
```

## Create the ingress

The Web Application Routing add-on creates an Ingress class on the cluster called

[webapprouting.kubernetes.azure.com](#). When you create an ingress object with this class, this will activate the add-on. To obtain the certificate URI to use in the Ingress from Azure Key Vault, run the following command.

```
az keyvault certificate show --vault-name <KeyVaultName> -n <KeyVaultCertificateName> --query "id" --output tsv
```

Create a file named **ingress.yaml** and copy in the following YAML.

#### NOTE

Update `<Hostname>` with your DNS host name and `<KeyVaultCertificateUri>` with the ID returned from Azure Key Vault. `secretName` is the name of the secret that going to be generated to store the certificate. This is the certificate that's going to be presented in the browser.

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
 annotations:
 kubernetes.azure.com/tls-cert-keyvault-uri: <KeyVaultCertificateUri>
 kubernetes.azure.com/use-osm-mtls: "true"
 nginx.ingress.kubernetes.io/backend-protocol: HTTPS
 nginx.ingress.kubernetes.io/configuration-snippet: |2-
 proxy_ssl_name "default.hello-web-app-routing.cluster.local";
 nginx.ingress.kubernetes.io/proxy-ssl-secret: kube-system/osm-ingress-client-cert
 nginx.ingress.kubernetes.io/proxy-ssl-verify: "on"
 name: aks-helloworld
 namespace: hello-web-app-routing
spec:
 ingressClassName: webapprouting.kubernetes.azure.com
 rules:
 - host: <Hostname>
 http:
 paths:
 - backend:
 service:
 name: aks-helloworld
 port:
 number: 80
 path: /
 pathType: Prefix
 tls:
 - hosts:
 - <Hostname>
 secretName: keyvault-aks-helloworld
```

### Create the ingress backend

Open Service Mesh (OSM) leverages its [IngressBackend API](#) to configure a backend service to accept ingress traffic from trusted sources. To proxy connections to HTTPS backends, we will configure the Ingress and IngressBackend configurations to use https as the backend protocol, and have OSM issue a certificate that Nginx will use as the client certificate to proxy HTTPS connections to TLS backends. The client certificate and CA certificate will be stored in a Kubernetes secret that Nginx will use to authenticate service mesh backends. For more information, refer to [Open Service Mesh: Ingress with Kubernetes Nginx Ingress Controller](#).

Create a file named `ingressbackend.yaml` and copy in the following YAML.

```
apiVersion: policy.openservicemesh.io/v1alpha1
kind: IngressBackend
metadata:
 name: aks-helloworld
 namespace: hello-web-app-routing
spec:
 backends:
 - name: aks-helloworld
 port:
 number: 80
 protocol: https
 tls:
 skipClientCertValidation: false
 sources:
 - kind: Service
 name: nginx
 namespace: app-routing-system
 - kind: AuthenticatedPrincipal
 name: ingress-nginx.ingress.cluster.local
```

## Create the resources on the cluster

Use the [kubectl apply](#) command to create the resources.

```
kubectl apply -f deployment.yaml -n hello-web-app-routing
kubectl apply -f service.yaml -n hello-web-app-routing
kubectl apply -f ingress.yaml -n hello-web-app-routing
kubectl apply -f ingressbackend.yaml -n hello-web-app-routing
```

The following example output shows the created resources:

```
deployment.apps/aks-helloworld created
service/aks-helloworld created
ingress.networking.k8s.io/aks-helloworld created
ingressbackend.policy.openservicemesh.io/aks-helloworld created
```

## Verify the managed ingress was created

```
kubectl get ingress -n hello-web-app-routing
```

NAME	CLASS	HOSTS	ADDRESS	PORTS	AGE
aks-helloworld	webapprouting.kubernetes.azure.com	myapp.contoso.com	20.51.92.19	80, 443	4m

## Accessing the endpoint over a DNS hostname

If you have not configured Azure DNS integration, you will need to configure your own DNS provider with an **A record** pointing to the ingress IP address and the host name you configured for the ingress, for example *myapp.contoso.com*.

## Remove Web Application Routing

First, remove the associated namespace:

```
kubectl delete namespace hello-web-app-routing
```

The Web Application Routing add-on can be removed using the Azure CLI. To do so run the following command,

substituting your AKS cluster and resource group name. Be careful if you already have some of the other add-ons (open-service-mesh or azure-keyvault-secrets-provider) enabled on your cluster so that you don't accidentally disable them.

```
az aks disable-addons --addons web_application_routing --name myAKSCluster --resource-group myResourceGroup
```

When the Web Application Routing add-on is disabled, some Kubernetes resources may remain in the cluster. These resources include *configMaps* and *secrets*, and are created in the *app-routing-system* namespace. To maintain a clean cluster, you may want to remove these resources.

# Deploy and manage cluster extensions for Azure Kubernetes Service (AKS)

10/27/2022 • 8 minutes to read • [Edit Online](#)

Cluster extensions provide an Azure Resource Manager driven experience for installation and lifecycle management of services like Azure Machine Learning (ML) on an AKS cluster. This feature enables:

- Azure Resource Manager-based deployment of extensions, including at-scale deployments across AKS clusters.
- Lifecycle management of the extension (Update, Delete) from Azure Resource Manager.

In this article, you'll learn about:

- How to create an extension instance.
- Available cluster extensions on AKS.
- How to view, list, update, and delete extension instances.

A conceptual overview of this feature is available in [Cluster extensions - Azure Arc-enabled Kubernetes](#) article.

## Prerequisites

### IMPORTANT

Ensure that your AKS cluster is created with a managed identity, as cluster extensions won't work with service principal-based clusters.

For new clusters created with `az aks create`, managed identity is configured by default. For existing service principal-based clusters that need to be switched over to managed identity, it can be enabled by running `az aks update` with the `--enable-managed-identity` flag. For more information, see [Use managed identity](#).

- An Azure subscription. If you don't have an Azure subscription, you can create a [free account](#).
- [Azure CLI](#) version >= 2.16.0 installed.

### NOTE

If you have enabled [AAD-based pod identity][use-azure-ad-pod-identity] on your AKS cluster or are considering implementing it, we recommend you first review [Migrate to workload identity](#) to understand our recommendations and options to set up your cluster to use an Azure AD workload identity (preview). This authentication method replaces pod-managed identity (preview), which integrates with the Kubernetes native capabilities to federate with any external identity providers.

## Set up the Azure CLI extension for cluster extensions

### NOTE

The minimum supported version for the `k8s-extension` Azure CLI extension is `1.0.0`. If you are unsure what version you have installed, run `az extension show --name k8s-extension` and look for the `version` field.

You'll also need the `k8s-extension` Azure CLI extension. Install the extension by running the following command:

```
az extension add --name k8s-extension
```

If the `k8s-extension` extension is already installed, you can update it to the latest version using the following command:

```
az extension update --name k8s-extension
```

## Currently available extensions

### NOTE

Cluster extensions provides a platform for different extensions to be installed and managed on an AKS cluster. If you are facing issues while using any of these extensions, please open a support ticket with the respective service.

EXTENSION	DESCRIPTION
Dapr	Dapr is a portable, event-driven runtime that makes it easy for any developer to build resilient, stateless and stateful applications that run on cloud and edge.
Azure ML	Use Azure Kubernetes Service clusters to train, inference, and manage machine learning models in Azure Machine Learning.
Flux (GitOps)	Use GitOps with Flux to manage cluster configuration and application deployment.

## Supported regions and Kubernetes versions

Cluster extensions can be used on AKS clusters in the regions listed in [Azure Arc enabled Kubernetes region support](#).

For supported Kubernetes versions, refer to the corresponding documentation for each extension.

## Usage of cluster extensions

### NOTE

The samples provided in this article are not complete, and are only meant to showcase functionality. For a comprehensive list of commands and their parameters, please see the [az k8s-extension CLI reference](#).

### Create extensions instance

Create a new extension instance with `k8s-extension create`, passing in values for the mandatory parameters.

The below command creates an Azure Machine Learning extension instance on your AKS cluster:

```
az k8s-extension create --name aml-compute --extension-type Microsoft.AzureML.Kubernetes --scope cluster --cluster-name <clusterName> --resource-group <resourceGroupName> --cluster-type managedClusters --configuration-settings enableInference=True allowInsecureConnections=True
```

## NOTE

The Cluster Extensions service is unable to retain sensitive information for more than 48 hours. If the cluster extension agents don't have network connectivity for more than 48 hours and can't determine whether to create an extension on the cluster, then the extension transitions to `Failed` state. Once in `Failed` state, you will need to run `k8s-extension create` again to create a fresh extension instance.

### Required parameters

PARAMETER NAME	DESCRIPTION
<code>--name</code>	Name of the extension instance
<code>--extension-type</code>	The type of extension you want to install on the cluster. For example: Microsoft.AzureML.Kubernetes
<code>--cluster-name</code>	Name of the AKS cluster on which the extension instance has to be created
<code>--resource-group</code>	The resource group containing the AKS cluster
<code>--cluster-type</code>	The cluster type on which the extension instance has to be created. Specify <code>managedClusters</code> as it maps to AKS clusters

### Optional parameters

PARAMETER NAME	DESCRIPTION
<code>--auto-upgrade-minor-version</code>	Boolean property that specifies if the extension minor version will be upgraded automatically or not. Default: <code>true</code> . If this parameter is set to true, you can't set <code>version</code> parameter, as the version will be dynamically updated. If set to <code>false</code> , extension won't be auto-upgraded even for patch versions.
<code>--version</code>	Version of the extension to be installed (specific version to pin the extension instance to). Must not be supplied if auto-upgrade-minor-version is set to <code>true</code> .
<code>--configuration-settings</code>	Settings that can be passed into the extension to control its functionality. Pass values as space separated <code>key=value</code> pairs after the parameter name. If this parameter is used in the command, then <code>--configuration-settings-file</code> can't be used in the same command.
<code>--configuration-settings-file</code>	Path to the JSON file having key value pairs to be used for passing in configuration settings to the extension. If this parameter is used in the command, then <code>--configuration-settings</code> can't be used in the same command.

PARAMETER NAME	DESCRIPTION
--configuration-protected-settings	These settings are not retrievable using <code>GET</code> API calls or <code>az k8s-extension show</code> commands, and are thus used to pass in sensitive settings. Pass values as space separated <code>key=value</code> pairs after the parameter name. If this parameter is used in the command, then <code>--configuration-protected-settings-file</code> can't be used in the same command.
--configuration-protected-settings-file	Path to the JSON file having key value pairs to be used for passing in sensitive settings to the extension. If this parameter is used in the command, then <code>--configuration-protected-settings</code> can't be used in the same command.
--scope	Scope of installation for the extension - <code>cluster</code> or <code>namespace</code>
--release-namespace	This parameter indicates the namespace within which the release is to be created. This parameter is only relevant if <code>scope</code> parameter is set to <code>cluster</code> .
--release-train	Extension authors can publish versions in different release trains such as <code>Stable</code> , <code>Preview</code> , etc. If this parameter isn't set explicitly, <code>Stable</code> is used as default. This parameter can't be used when <code>autoUpgradeMinorVersion</code> parameter is set to <code>false</code> .
--target-namespace	This parameter indicates the namespace within which the release will be created. Permission of the system account created for this extension instance will be restricted to this namespace. This parameter is only relevant if the <code>scope</code> parameter is set to <code>namespace</code> .

## Show details of an extension instance

View details of a currently installed extension instance with `k8s-extension show`, passing in values for the mandatory parameters:

```
az k8s-extension show --name azureml --cluster-name <clusterName> --resource-group <resourceGroupName> --cluster-type managedClusters
```

## List all extensions installed on the cluster

List all extensions installed on a cluster with `k8s-extension list`, passing in values for the mandatory parameters.

```
az k8s-extension list --cluster-name <clusterName> --resource-group <resourceGroupName> --cluster-type managedClusters
```

## Update extension instance

#### NOTE

Refer to documentation of the extension type (Eg: Azure ML) to learn about the specific settings under ConfigurationSetting and ConfigurationProtectedSettings that are allowed to be updated. For ConfigurationProtectedSettings, all settings are expected to be provided during an update of a single setting. If some settings are omitted, those settings would be considered obsolete and deleted.

Update an existing extension instance with `k8s-extension update`, passing in values for the mandatory parameters. The below command updates the auto-upgrade setting for an Azure Machine Learning extension instance:

```
az k8s-extension update --name azureml --extension-type Microsoft.AzureML.Kubernetes --scope cluster --cluster-name <clusterName> --resource-group <resourceGroupName> --cluster-type managedClusters
```

#### Required parameters

PARAMETER NAME	DESCRIPTION
<code>--name</code>	Name of the extension instance
<code>--extension-type</code>	The type of extension you want to install on the cluster. For example: Microsoft.AzureML.Kubernetes
<code>--cluster-name</code>	Name of the AKS cluster on which the extension instance has to be created
<code>--resource-group</code>	The resource group containing the AKS cluster
<code>--cluster-type</code>	The cluster type on which the extension instance has to be created. Specify <code>managedClusters</code> as it maps to AKS clusters

#### Optional parameters

PARAMETER NAME	DESCRIPTION
<code>--auto-upgrade-minor-version</code>	Boolean property that specifies if the extension minor version will be upgraded automatically or not. Default: <code>true</code> . If this parameter is set to true, you cannot set <code>version</code> parameter, as the version will be dynamically updated. If set to <code>false</code> , extension won't be auto-upgraded even for patch versions.
<code>--version</code>	Version of the extension to be installed (specific version to pin the extension instance to). Must not be supplied if auto-upgrade-minor-version is set to <code>true</code> .

PARAMETER NAME	DESCRIPTION
--configuration-settings	Settings that can be passed into the extension to control its functionality. Only the settings that require an update need to be provided. The provided settings would be replaced with the provided values. Pass values as space separated <code>key=value</code> pairs after the parameter name. If this parameter is used in the command, then <code>--configuration-settings-file</code> can't be used in the same command.
--configuration-settings-file	Path to the JSON file having key value pairs to be used for passing in configuration settings to the extension. If this parameter is used in the command, then <code>--configuration-settings</code> can't be used in the same command.
--configuration-protected-settings	These settings are not retrievable using <code>GET</code> API calls or <code>az k8s-extension show</code> commands, and are thus used to pass in sensitive settings. When you update a setting, all settings are expected to be specified. If some settings are omitted, those settings would be considered obsolete and deleted. Pass values as space separated <code>key=value</code> pairs after the parameter name. If this parameter is used in the command, then <code>--configuration-protected-settings-file</code> can't be used in the same command.
--configuration-protected-settings-file	Path to the JSON file having key value pairs to be used for passing in sensitive settings to the extension. If this parameter is used in the command, then <code>--configuration-protected-settings</code> can't be used in the same command.
--scope	Scope of installation for the extension - <code>cluster</code> or <code>namespace</code>
--release-train	Extension authors can publish versions in different release trains such as <code>Stable</code> , <code>Preview</code> , etc. If this parameter isn't set explicitly, <code>stable</code> is used as default. This parameter can't be used when <code>autoUpgradeMinorVersion</code> parameter is set to <code>false</code> .

## Delete extension instance

### NOTE

The Azure resource representing this extension gets deleted immediately. The Helm release on the cluster associated with this extension is only deleted when the agents running on the Kubernetes cluster have network connectivity and can reach out to Azure services again to fetch the desired state.

Delete an extension instance on a cluster with `k8s-extension delete`, passing in values for the mandatory parameters.

```
az k8s-extension delete --name azurerm --cluster-name <clusterName> --resource-group <resourceGroupName> --cluster-type managedClusters
```

# Deploy ASP.NET Core apps to Azure Kubernetes Service with Azure DevOps Starter

10/27/2022 • 7 minutes to read • [Edit Online](#)

Azure DevOps Starter presents a simplified experience where you can bring your existing code and Git repo or choose a sample application to create a continuous integration (CI) and continuous delivery (CD) pipeline to Azure.

DevOps Starter also:

- Automatically creates Azure resources, such as Azure Kubernetes Service (AKS).
- Creates and configures a release pipeline in Azure DevOps that sets up a build and release pipeline for CI/CD.
- Creates an Azure Application Insights resource for monitoring.
- Enables [Azure Monitor for containers](#) to monitor performance for the container workloads on the AKS cluster

In this tutorial, you will:

- Use DevOps Starter to deploy an ASP.NET Core app to AKS
- Configure Azure DevOps and an Azure subscription
- Examine the AKS cluster
- Examine the CI pipeline
- Examine the CD pipeline
- Commit changes to Git and automatically deploy them to Azure
- Clean up resources

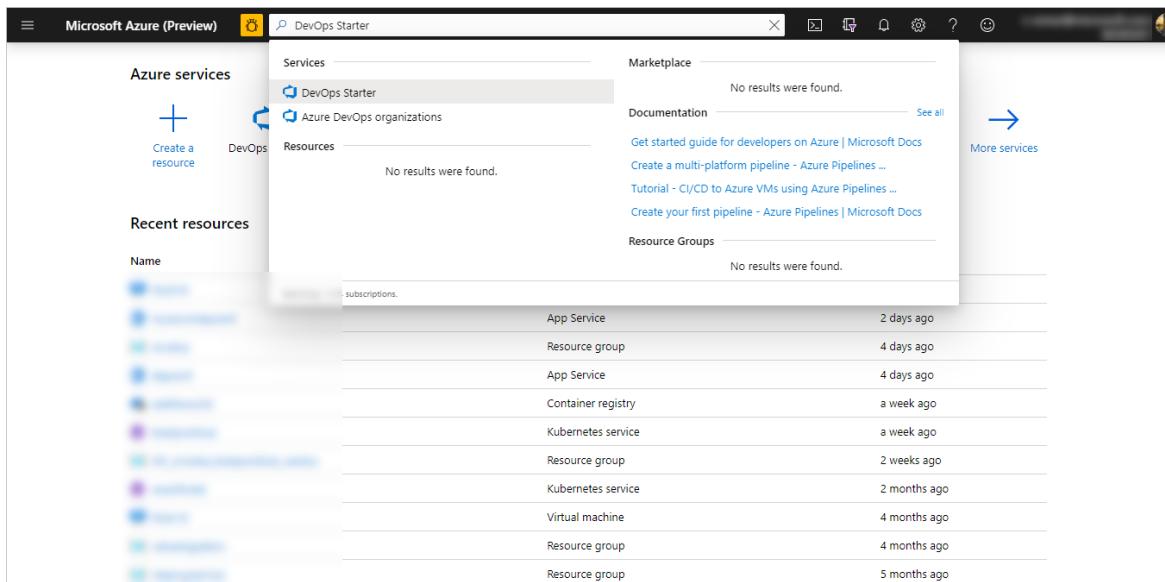
## Prerequisites

- An Azure subscription. You can get one free through [Visual Studio Dev Essentials](#).

## Use DevOps Starter to deploy an ASP.NET Core app to AKS

DevOps Starter creates a CI/CD pipeline in Azure Pipelines. You can create a new Azure DevOps organization or use an existing organization. DevOps Starter also creates Azure resources, such as an AKS cluster, in the Azure subscription of your choice.

1. Sign in to the [Azure portal](#).
2. In the search box, type **DevOps Starter**, and then select. Click on **Add** to create a new one.



3. Select .NET, and then select **Next**.
4. Under **Choose an application framework**, select **ASP.NET Core** and then select **Next**.
5. Select **Kubernetes Service**, and then select **Next**.

## Configure Azure DevOps and an Azure subscription

1. Create a new Azure DevOps organization, or select an existing organization.
2. Enter a name for your Azure DevOps project.
3. Select your Azure subscription.
4. To view additional Azure configuration settings and to identify the number of nodes for the AKS cluster, select **Change**. This pane displays various options for configuring the type and location of Azure services.
5. Exit the Azure configuration area, and then select **Done**. After a few minutes, the process is completed. A sample ASP.NET Core app is set up in a Git repo in your Azure DevOps organization, an AKS cluster is created, a CI/CD pipeline is executed, and your app is deployed to Azure.

After all this is completed, the Azure DevOps Starter dashboard is displayed in the Azure portal. You can also go to the DevOps Starter dashboard directly from **All resources** in the Azure portal.

This dashboard provides visibility into your Azure DevOps code repository, your CI/CD pipeline, and your AKS cluster. You can configure additional CI/CD options in your Azure DevOps pipeline. At the right, select **Browse** to view your running app.

## Examine the AKS cluster

DevOps Starter automatically configures an AKS cluster, which you can explore and customize. To familiarize yourself with the AKS cluster, do the following:

1. Go to the DevOps Starter dashboard.
2. At the right, select the AKS service. A pane opens for the AKS cluster. From this view you can perform various actions, such as monitoring container health, searching logs, and opening the Kubernetes dashboard.
3. At the right, select **View Kubernetes dashboard**. Optionally, follow the steps to open the Kubernetes dashboard.

## Examine the CI pipeline

DevOps Starter automatically configures a CI/CD pipeline in your Azure DevOps organization. You can explore and customize the pipeline. To familiarize yourself with it, do the following:

1. Go to the DevOps Starter dashboard.
2. At the top of the DevOps Starter dashboard, select **Build Pipelines**. A browser tab displays the build pipeline for your new project.
3. Point to the **Status** field, and then select the ellipsis (...). A menu displays several options, such as queueing a new build, pausing a build, and editing the build pipeline.
4. Select **Edit**.
5. In this pane, you can examine the various tasks for your build pipeline. The build performs various tasks, such as fetching sources from the Git repo, restoring dependencies, and publishing outputs used for deployments.
6. At the top of the build pipeline, select the build pipeline name.
7. Change the name of your build pipeline to something more descriptive, select **Save & queue**, and then select **Save**.
8. Under your build pipeline name, select **History**. This pane displays an audit trail of your recent changes for the build. Azure DevOps keeps track of any changes made to the build pipeline, and it allows you to compare versions.
9. Select **Triggers**. DevOps Starter automatically creates a CI trigger, and every commit to the repo starts a new build. Optionally, you can choose to include or exclude branches from the CI process.
10. Select **Retention**. Depending on your scenario, you can specify policies to keep or remove a certain number of builds.

## Examine the CD release pipeline

DevOps Starter automatically creates and configures the necessary steps to deploy from your Azure DevOps organization to your Azure subscription. These steps include configuring an Azure service connection to authenticate Azure DevOps to your Azure subscription. The automation also creates a release pipeline, which provides the CD to Azure. To learn more about the release pipeline, do the following:

1. Select **Build and Release**, and then select **Releases**. DevOps Starter creates a release pipeline to manage deployments to Azure.
2. Select the ellipsis (...) next to your release pipeline, and then select **Edit**. The release pipeline contains a *pipeline*, which defines the release process.
3. Under **Artifacts**, select **Drop**. The build pipeline you examined in the previous steps produces the output that's used for the artifact.
4. At the right of the **Drop** icon, select **Continuous deployment trigger**. This release pipeline has an enabled CD trigger, which executes a deployment every time a new build artifact is available. Optionally, you can disable the trigger so that your deployments require manual execution.
5. At the right, select **View releases** to display a history of releases.
6. Select the ellipsis (...) next to a release, and then select **Open**. You can explore several menus, such as a release summary, associated work items, and tests.
7. Select **Commits**. This view shows code commits that are associated with this deployment. Compare

releases to view the commit differences between deployments.

8. Select **Logs**. The logs contain useful information about the deployment process. You can view them both during and after deployments.

## Commit changes to Azure Repos and automatically deploy them to Azure

### NOTE

The following procedure tests the CI/CD pipeline by making a simple text change.

You're now ready to collaborate with a team on your app by using a CI/CD process that automatically deploys your latest work to your website. Each change to the Git repo starts a build in Azure DevOps, and a CD pipeline executes a deployment to Azure. Follow the procedure in this section, or use another technique to commit changes to your repo. For example, you can clone the Git repo in your favorite tool or IDE, and then push changes to this repo.

1. In the Azure DevOps menu, select **Code > Files**, and then go to your repo.
2. Go to the *Views\Home* directory, select the ellipsis (...) next to the *Index.cshtml* file, and then select **Edit**.
3. Make a change to the file, such as adding some text within one of the div tags.
4. At the top right, select **Commit**, and then select **Commit** again to push your change. After a few moments, a build starts in Azure DevOps and a release executes to deploy the changes. Monitor the build status on the DevOps Starter dashboard or in the browser with your Azure DevOps organization.
5. After the release is completed, refresh your app to verify your changes.

## Clean up resources

If you are testing, you can avoid accruing billing charges by cleaning up your resources. When they are no longer needed, you can delete the AKS cluster and related resources that you created in this tutorial. To do so, use the **Delete** functionality on the DevOps Starter dashboard.

### IMPORTANT

The following procedure permanently deletes resources. The **Delete** functionality destroys the data that's created by the project in DevOps Starter in both Azure and Azure DevOps, and you will be unable to retrieve it. Use this procedure only after you've carefully read the prompts.

1. In the Azure portal, go to the DevOps Starter dashboard.
2. At the top right, select **Delete**.
3. At the prompt, select **Yes** to *permanently delete* the resources.

## Next steps

You can optionally modify these build and release pipelines to meet the needs of your team. You can also use this CI/CD pattern as a template for your other pipelines. In this tutorial, you learned how to:

- Use DevOps Starter to deploy an ASP.NET Core app to AKS
- Configure Azure DevOps and an Azure subscription
- Examine the AKS cluster

- Examine the CI pipeline
- Examine the CD pipeline
- Commit changes to Git and automatically deploy them to Azure
- Clean up resources

To learn more about using the Kubernetes dashboard, see:

[Use the Kubernetes dashboard](#)

# Deployment Center for Azure Kubernetes

10/27/2022 • 6 minutes to read • [Edit Online](#)

## IMPORTANT

Deployment Center for Azure Kubernetes Service will be retired on March 31, 2023. [Learn more](#)

Deployment Center in Azure DevOps simplifies setting up a robust Azure DevOps pipeline for your application. By default, Deployment Center configures an Azure DevOps pipeline to deploy your application updates to the Kubernetes cluster. You can extend the default configured Azure DevOps pipeline and also add richer capabilities: the ability to gain approval before deploying, provision additional Azure resources, run scripts, upgrade your application, and even run more validation tests.

In this tutorial, you will:

- Configure an Azure DevOps pipeline to deploy your application updates to the Kubernetes cluster.
- Examine the continuous integration (CI) pipeline.
- Examine the continuous delivery (CD) pipeline.
- Clean up the resources.

## Prerequisites

- An Azure subscription. You can get one free through [Visual Studio Dev Essentials](#).
- An Azure Kubernetes Service (AKS) cluster.

## Create an AKS cluster

- Sign in to your [Azure portal](#).
- Select the [Cloud Shell](#) option on the right side of the menu bar in the Azure portal.
- To create the AKS cluster, run the following commands:

```
Create a resource group in the South India location:

az group create --name azooaks --location southindia

Create a cluster named azookubectl with one node.

az aks create --resource-group azooaks --name azookubectl --node-count 1 --enable-addons monitoring -
-generate-ssh-keys
```

## Deploy application updates to a Kubernetes cluster

- Go to the resource group that you created in the previous section.
- Select the AKS cluster, and then select **Deployment Center (preview)** on the left blade. Select **Get started**.

The screenshot shows the 'Deployment center' blade in the Azure portal. On the left, there's a sidebar with various options like Overview, Activity log, Access control (IAM), Tags, Settings, Upgrade, Scale, Dev Spaces, Deployment center (preview) (which has a red arrow pointing to it), Properties, Locks, Export template, Monitoring, and Insights. The main content area is titled 'Deployment Center' and contains a detailed description of what DevOps simplifies, mentioning Kubernetes, DevOps pipelines, approvals, and additional Azure resources.

3. Choose the location of the code and select **Next**. Then, select one of the currently supported repositories: [Azure Repos](#) or [GitHub](#).

Azure Repos is a set of version control tools that help you manage your code. Whether your software project is large or small, using version control as early as possible is a good idea.

- **Azure Repos:** Choose a repository from your existing project and organization.

The screenshot shows the 'Select the code location' step of a deployment wizard. At the top, there's a progress bar with four steps: 1. Source (highlighted in blue), 2. Repository, 3. Application, and 4. Resources. Below the progress bar, the title 'Select the code location' is centered. There are two options displayed: 'Azure Repos' (selected, indicated by a checked checkbox) and 'GitHub'. Both options have their respective logos and brief descriptions.

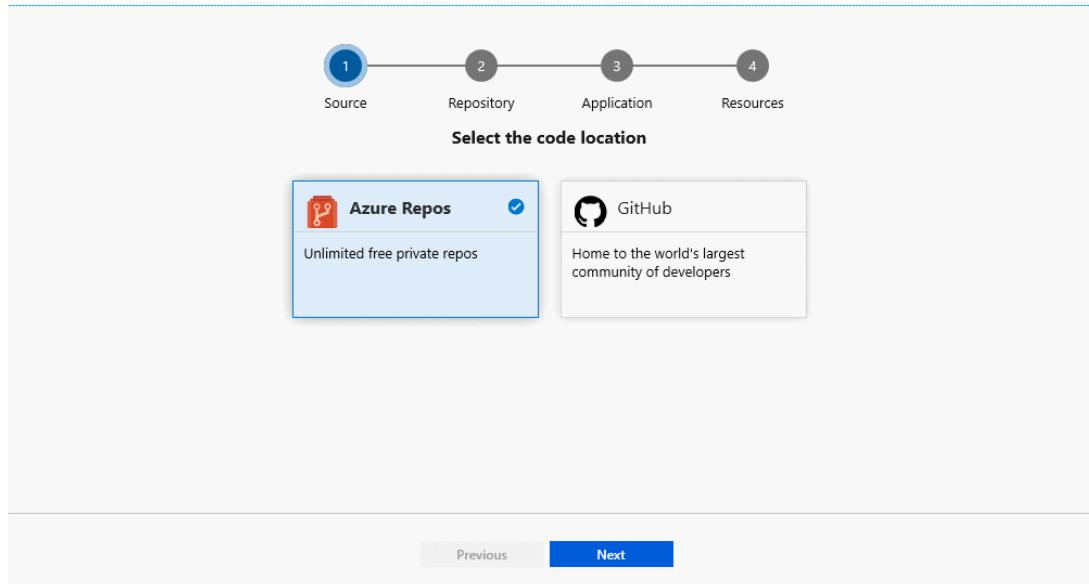
1 Source      2 Repository      3 Application      4 Resources

Select the code location

 <b>Azure Repos</b> <input checked="" type="checkbox"/>	 <b>GitHub</b>
Unlimited free private repos	Home to the world's largest community of developers

Previous      **Next**

- **GitHub:** Authorize and select the repository for your GitHub account.



4. Deployment Center analyzes the repository and detects your Dockerfile. If you want to update the Dockerfile, you can edit the identified port number.

Detected the following Dockerfile

```
src/MyHealth.Web/Dockerfile
1 FROM microsoft/aspnetcore:1.0
2 ARG source
3 WORKDIR /app
4 EXPOSE 80
5 COPY ${source:-obj}/Docker/publish .
6 ENTRYPOINT ["dotnet",
7 "MyHealth.Web.dll"]
```

We have detected the following values from your Dockerfile.  
Please update if required.

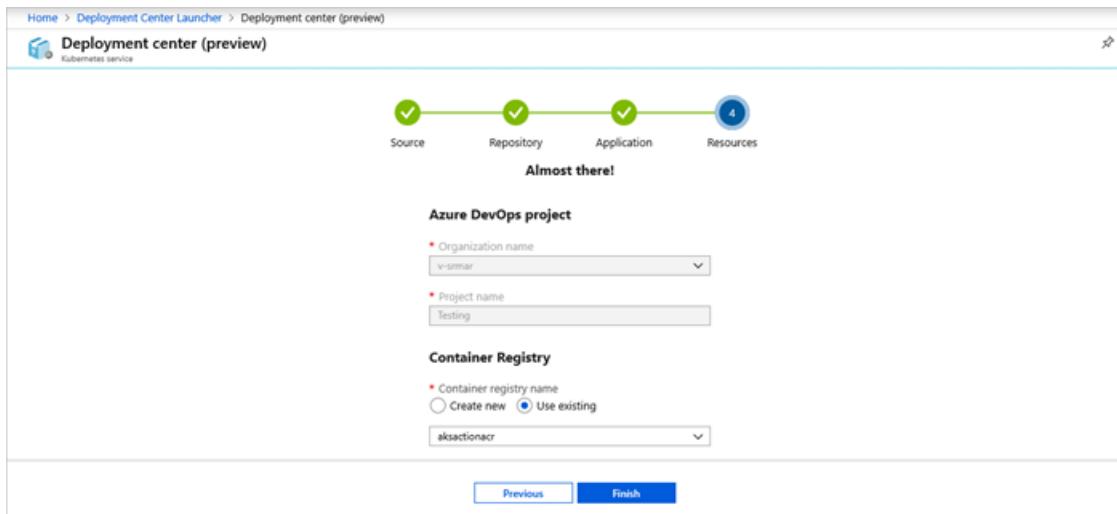
Port

If the repository doesn't contain the Dockerfile, the system displays a message to commit one.

Could not find a Dockerfile in the repository  
Please commit the Dockerfile to the repository to proceed further.

5. Select an existing container registry or create one, and then select **Finish**. The pipeline is created automatically and queues a build in [Azure Pipelines](#).

Azure Pipelines is a cloud service that you can use to automatically build and test your code project and make it available to other users. Azure Pipelines combines continuous integration and continuous delivery to constantly and consistently test and build your code and ship it to any target.



6. Select the link to see the ongoing pipeline.
7. You'll see the successful logs after deployment is complete.

BUILD/RELEASE	PROJECT NAME	UPDATED
Release-1 Build 20190409.1 playground-docs master	Testing	Just now

## Examine the CI pipeline

Deployment Center automatically configures your Azure DevOps organization's CI/CD pipeline. The pipeline can be explored and customized.

1. Go to the Deployment Center dashboard.
2. Select the build number from the list of successful logs to view the build pipeline for your project.
3. Select the ellipsis (...) in the upper-right corner. A menu shows several options, such as queuing a new build, retaining a build, and editing the build pipeline. Select **Edit pipeline**.
4. You can examine the different tasks for your build pipeline in this pane. The build performs various tasks, such as collecting sources from the Git repository, creating an image, pushing an image to the container registry, and publishing outputs that are used for deployments.
5. Select the name of the build pipeline at the top of the pipeline.
6. Change your build pipeline name to something more descriptive, select **Save & queue**, and then select **Save**.
7. Under your build pipeline, select **History**. This pane shows an audit trail of your recent build changes. Azure DevOps monitors any changes made to the build pipeline and allows you to compare versions.
8. Select **Triggers**. You can include or exclude branches from the CI process.

9. Select **Retention**. You can specify policies to keep or remove a number of builds, depending on your scenario.

## Examine the CD pipeline

Deployment Center automatically creates and configures the relationship between your Azure DevOps organization and your Azure subscription. The steps involved include setting up an Azure service connection to authenticate your Azure subscription with Azure DevOps. The automated process also creates a release pipeline, which provides continuous delivery to Azure.

1. Select **Pipelines**, and then select **Releases**.
2. To edit the release pipeline, select **Edit**.
3. Select **Drop** from the **Artifacts** list. In the previous steps, the construction pipeline you examined produces the output used for the artifact.
4. Select the **Continuous deployment** trigger on the right of the **Drop** option. This release pipeline has an enabled CD trigger that runs a deployment whenever a new build artifact is available. You can also disable the trigger to require manual execution for your deployments.
5. To examine all the tasks for your pipeline, select **Tasks**. The release sets the tiller environment, configures the `imagePullSecrets` parameter, installs Helm tools, and deploys the Helm charts to the Kubernetes cluster.
6. To view the release history, select **View releases**.
7. To see the summary, select **Release**. Select any of the stages to explore multiple menus, such as a release summary, associated work items, and tests.
8. Select **Commits**. This view shows code commits related to this deployment. Compare releases to see the commit differences between deployments.
9. Select **Logs**. The logs contain useful deployment information, which you can view during and after deployments.

## Clean up resources

You can delete the related resources that you created when you don't need them anymore. Use the delete functionality on the DevOps Projects dashboard.

## Next steps

You can modify these build and release pipelines to meet the needs of your team. Or, you can use this CI/CD model as a template for your other pipelines.

## Retirement

Deployment Center for Azure Kubernetes will be retired on March 31, 2023 in favor of [Automated deployments](#). We encourage you to switch for enjoy similar capabilities.

### Migration Steps

There is no migration required as AKS Deployment center experience does not store any information itself, it just helps users with their Day 0 getting started experience on Azure. Moving forward, the recommended way for users to get started on CI/CD for AKS will be using [Automated deployments](#) feature.

For existing pipelines, users will still be able to perform all operations from GitHub Actions or Azure DevOps after the retirement of this experience. Only the ability to create and view pipelines from Azure portal will be

removed. See [GitHub Actions](#) or [Azure DevOps](#) to learn how to get started.

For new application deployments to AKS, instead of using Deployment center users can get the same capabilities by using Automated deployments.

#### FAQ

1. Where can I manage my CD pipeline after this experience is deprecated?

Post retirement, you will not be able to view or create CD pipelines from Azure portal's AKS blade. However, as with the current experience, you can go to GitHub Actions or Azure DevOps portal and view or update the configured pipelines there.

2. Will I lose my earlier configured pipelines?

No. All the created pipelines will still be available and functional in GitHub or Azure DevOps. Only the experience of creating and viewing pipelines from Azure portal will be retired.

3. How can I still configure CD pipelines directly through Azure portal?

You can use Automated deployments available in the AKS blade in Azure portal.

# GitHub Actions for deploying to Kubernetes service

10/27/2022 • 5 minutes to read • [Edit Online](#)

[GitHub Actions](#) gives you the flexibility to build an automated software development lifecycle workflow. You can use multiple Kubernetes actions to deploy to containers from Azure Container Registry to Azure Kubernetes Service with GitHub Actions.

## Prerequisites

- An Azure account with an active subscription. [Create an account for free](#).
- A GitHub account. If you don't have one, sign up for [free](#).
- An existing AKS cluster with an attached Azure Container Registry (ACR).

## Configure integration between Azure and your GitHub repository

When using GitHub Actions, you need to configure the integration between Azure and your GitHub repository. For more details on connecting your GitHub repository to Azure, see [Use GitHub Actions to connect to Azure](#).

## Available actions

GitHub Actions helps you automate your software development workflows from within GitHub. For more details on using GitHub Actions with Azure, see [What is GitHub Actions for Azure](#).

The below table shows the available GitHub Actions that integrate specifically with AKS.

NAME	DESCRIPTION	MORE DETAILS
<a href="#">azure/aks-set-context</a>	Set the target AKS cluster context which will be used by other actions or run any kubectl commands.	<a href="#">azure/aks-set-context</a>
<a href="#">azure/k8s-set-context</a>	Set the target Kubernetes cluster context which will be used by other actions or run any kubectl commands.	<a href="#">azure/k8s-set-context</a>
<a href="#">azure/k8s-bake</a>	Bake manifest file to be used for deployments using Helm, kustomize or kompose.	<a href="#">azure/k8s-bake</a>
<a href="#">azure/k8s-create-secret</a>	Create a generic secret or docker-registry secret in the Kubernetes cluster.	<a href="#">azure/k8s-create-secret</a>
<a href="#">azure/k8s-deploy</a>	Deploy manifests to Kubernetes clusters.	<a href="#">azure/k8s-deploy</a>
<a href="#">azure/k8s-lint</a>	Validate/lint your manifest files.	<a href="#">azure/k8s-lint</a>
<a href="#">azure/setup-helm</a>	Install a specific version of Helm binary on the runner.	<a href="#">azure/setup-helm</a>

NAME	DESCRIPTION	MORE DETAILS
<code>azure/setup-kubectl</code>	Installs a specific version of kubectl on the runner.	<a href="#">azure/setup-kubectl</a>
<code>azure/k8s-artifact-substitute</code>	Update the tag or digest for container images.	<a href="#">azure/k8s-artifact-substitute</a>
<code>azure/aks-create-action</code>	Create an AKS cluster using Terraform.	<a href="#">azure/aks-create-action</a>
<code>azure/aks-github-runner</code>	Set up self-hosted agents for GitHub Actions.	<a href="#">azure/aks-github-runner</a>

In addition, the example in the next section uses the `azure/acr-build` action.

## Example of using GitHub Actions with AKS

As an example, you can use GitHub Actions to deploy an application to your AKS cluster every time a change is pushed to your GitHub repository. This example uses the [Azure Vote](#) application.

### NOTE

This example uses a service principal for authentication with your ACR and AKS cluster. Alternatively, you can configure Open ID Connect (OIDC) and update the `azure/login` action to use OIDC. For more details, see [Set up Azure Login with OpenID Connect authentication](#).

### Fork and update the repository

Navigate to the [Azure Vote](#) repository and click the **Fork** button.

Once the repository is forked, update `azure-vote-all-in-one-redis.yaml` to use your ACR for the `azure-vote-front` image

```
...
 containers:
 - name: azure-vote-front
 image: <registryName>.azurecr.io/azuredocs/azure-vote-front:v1
...

```

### IMPORTANT

The update to `azure-vote-all-in-one-redis.yaml` must be committed to your repository before you can complete the later steps.

### Create secrets

Create a service principal to access your resource group with the `Contributor` role using the following command, replacing:

- `<SUBSCRIPTION_ID>` with the subscription ID of your Azure account
- `<RESOURCE_GROUP>` with the name of the resource group where your ACR is located

```
az ad sp create-for-rbac \
--name "ghActionAzureVote" \
--scope /subscriptions/<SUBSCRIPTION_ID>/resourceGroups/<RESOURCE_GROUP> \
--role Contributor \
--sdk-auth
```

The following shows an example output from the above command.

```
{
 "clientId": <clientId>,
 "clientSecret": <clientSecret>,
 "subscriptionId": <subscriptionId>,
 "tenantId": <tenantId>,
 ...
}
```

In your GitHub repository, create the below secrets for your action to use. To create a secret:

1. Navigate to the repository's settings, and click *Secrets* then *Actions*.
2. For each secret, click *New Repository Secret* and enter the name and value of the secret.

For more details on creating secrets, see [Encrypted Secrets](#).

SECRET NAME	SECRET VALUE
AZURE_CREDENTIALS	The entire JSON output from the <code>az ad sp create-for-rbac</code> command
service_principal	The value of <code>&lt;clientId&gt;</code>
service_principal_password	The value of <code>&lt;clientSecret&gt;</code>
subscription	The value of <code>&lt;subscriptionId&gt;</code>
tenant	The value of <code>&lt;tenantId&gt;</code>
registry	The name of your registry
repository	azuredocs
resource_group	The name of your resource group
cluster_name	The name of your cluster

## Create actions file

Create a `.github/workflows/main.yml` in your repository with the following contents:

```

name: build_deploy_aks
on:
 push:
 paths:
 - "azure-vote/**"
jobs:
 build:
 runs-on: ubuntu-latest
 steps:
 - name: Checkout source code
 uses: actions/checkout@v3
 - name: ACR build
 id: build-push-acr
 uses: azure/acr-build@v1
 with:
 service_principal: ${{ secrets.service_principal }}
 service_principal_password: ${{ secrets.service_principal_password }}
 tenant: ${{ secrets.tenant }}
 registry: ${{ secrets.registry }}
 repository: ${{ secrets.repository }}
 image: azure-vote-front
 folder: azure-vote
 branch: master
 tag: ${{ github.sha }}
 - name: Azure login
 id: login
 uses: azure/login@v1.4.3
 with:
 creds: ${{ secrets.AZURE_CREDENTIALS }}
 - name: Set AKS context
 id: set-context
 uses: azure/aks-set-context@v3
 with:
 resource-group: '${{ secrets.resource_group }}'
 cluster-name: '${{ secrets.cluster_name }}'
 - name: Setup kubectl
 id: install-kubectl
 uses: azure/setup-kubectl@v3
 - name: Deploy to AKS
 id: deploy-aks
 uses: Azure/k8s-deploy@v4
 with:
 namespace: 'default'
 manifests: |
 azure-vote-all-in-one-redis.yaml
 images: '${{ secrets.registry }}.azuredcr.io/${{ secrets.repository }}/azure-vote-front:${{ github.sha }}"
 pull: false

```

## IMPORTANT

The `.github/workflows/main.yml` file must be committed to your repository before you can run the action.

The `on` section contains the event that triggers the action. In the above file, the action is triggered when a change is pushed to the `azure-vote` directory.

In the above file, the `steps` section contains each distinct action, which is executed in order:

1. *Checkout source code* uses the [GitHub Actions Checkout Action](#) to clone the repository.
2. *ACR build* uses the [Azure Container Registry Build Action](#) to build the image and upload it to your registry.
3. *Azure login* uses the [Azure Login Action](#) to sign in to your Azure account.
4. *Set AKS context* uses the [Azure AKS Set Context Action](#) to set the context for your AKS cluster.

5. *Setup kubectl* uses the [Azure AKS Setup Kubectl Action](#) to install kubectl on your runner.
6. *Deploy to AKS* uses the [Azure Kubernetes Deploy Action](#) to deploy the application to your Kuberentes cluster.

Confirm that the action is working by updating `azure-vote/azure-vote/config_file.cfg` to the following and pushing the changes to your repository:

```
UI Configurations
TITLE = 'Azure Voting App'
VOTE1VALUE = 'Fish'
VOTE2VALUE = 'Dogs'
SHOWHOST = 'false'
```

In your repository, click on *Actions* and confirm a workflow is running. Once complete, confirm the workflow has a green checkmark and the updated application is deployed to your cluster.

## Next steps

Review the following starter workflows for AKS. For more details on using starter workflows, see [Using starter workflows](#).

- [Azure Kubernetes Service \(Basic\)](#)
- [Azure Kubernetes Service Helm](#)
- [Azure Kubernetes Service Kustomize](#)
- [Azure Kubernetes Service Kompose](#)

[Learn how to create multiple pipelines on GitHub Actions with AKS](#)

[Learn about Azure Kubernetes Service](#)

# Automated Deployments for Azure Kubernetes Service (Preview)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Automated deployments simplify the process of setting up a GitHub Action and creating an automated pipeline for your code releases to your Azure Kubernetes Service (AKS) cluster. Once connected, every new commit will kick off the pipeline, resulting in your application being updated.

## IMPORTANT

AKS preview features are available on a self-service, opt-in basis. Previews are provided "as is" and "as available," and they're excluded from the service-level agreements and limited warranty. AKS previews are partially covered by customer support on a best-effort basis. As such, these features aren't meant for production use. For more information, see the following support articles:

- [AKS support policies](#)
- [Azure support FAQ](#)

## NOTE

This feature is not yet available in all regions.

## Prerequisites

- A GitHub account.
- An AKS cluster.
- An Azure Container Registry (ACR)

## Deploy an application to your AKS cluster

1. In the Azure portal, navigate to the resource group containing the AKS cluster you want to deploy the application to.
2. Select your AKS cluster, and then select **Automated deployments (preview)** on the left blade. Select **Create an automated deployment**.

3. Name your workflow and click **Authorize** to connect your Azure account with your GitHub account. After your accounts are linked, choose which repository and branch you would like to create the GitHub Action for.

- **GitHub:** Authorize and select the repository for your GitHub account.

Home > microsoft.aks-20220725082628 | Overview > myAKSCluster | Automated deployments (preview) > Create an automated deployment ...

**1 Repository** **2 Image** **3 Deployment details** **4 Review + deploy**

Select the repository where you've defined your application. We'll use the Docker files defined in the repository to set up the workflow. Azure will create a manifest file for you and store it in the same repository and branch as your application.

Workflow name

Repository location  GitHub  Authorized as 'testuser1'

Repository source  My repositories  All repositories

Repository \*

Branch \*

Previous **Next: Image**

4. Pick your dockerfile and your ACR and image.

**Create an automated deployment** ...

Repository     **Image**     Deployment details     Review + deploy

Review Dockerfile and provide below details

Dockerfile  \*  Dockerfile  
Switch | Preview

Dockerfile build context  \*  /

Azure Container Registry  \*  ContosoAirACR  
Create new

Azure Container Registry image  \*  (New) contosoair  
Create new

(Info) The selected image 'ContosoAirACR.azurecr.io/contosoair' should match the image defined in the deployment files. Any mismatch will result in a failure to deploy the image.

---

[Previous](#) **Next: Deployment details**

5. Determine whether you'll deploy with Helm or regular Kubernetes manifests. Once decided, pick the appropriate deployment files from your repository and decide which namespace you want to deploy into.

**Create an automated deployment** ...

Repository     **Image**     **Deployment details**     Review + deploy

Proceed to select your deployment details and assign the namespace. The Helm charts are a bundle of one or more Kubernetes manifest files grouped together. [Learn more](#) ⓘ  
The Kubernetes manifest files describe the resources you want to create (e.g. Deployment) and how to manage it in a cluster. [Learn more](#) ⓘ

Deployment options  \*  Helm charts  
 Kubernetes manifest files

Manifest files \*  2 files selected  
[Change](#)

Namespace  \*  (New) namespace-workflow-1658763941962  
[Create new](#)

---

[Previous](#) **Next: Review + create**

6. Review your deployment before creating the pull request.
7. Click **view pull request** to see your GitHub Action.

## Create an automated deployment

✓ Repository   ✓ Image   ✓ Deployment details   Review + deploy

### ✓ Pull request was successfully created

#### ✓ Azure Container Registry 'ContosoAirACR' was successfully created

Azure Container Registry is used to store newly built images from code changes that are later deployed to the AKS cluster.

#### ✓ Namespace 'namespace-workflow-1658763941962' was successfully created

Namespace is a logical grouping of resources in Kubernetes and AKS. The application delivered through automated deployment will be in this namespace.

#### ✓ Federated credentials for GitHub Actions was successfully created

The credentials used by GitHub Actions to authenticate to Azure Container Registry to push newly built images.

#### ✓ Azure Container Registry 'ContosoAirACR' was successfully connected

Connecting the Azure Container Registry to the AKS cluster allows the cluster to pull new images to deploy.

#### ✓ Successfully provisioned permissions for GitHub Actions on AKS and ACR

Provisioned minimal permissions used by GitHub Actions to push images to ACR and to deploy that image onto AKS cluster.

#### ✓ Next step: Approve pull request

A PR has been generated and must be merged before the automated deployment workflow is active.

[View pull request](#)

[Previous](#) [Close](#)

## 8. Merge the pull request to kick off the GitHub Action and deploy your application.

Add workflow to deploy to AKS #4

[Open](#) testuser1 wants to merge 1 commit into [main](#) from [aks-devhub-yesb1](#)

Conversation 0 Commits 1 Checks 0 Files changed 1

testuser1 commented 2 minutes ago Add workflow to deploy to AKS

Add more commits by pushing to the [aks-devhub-yesb1](#) branch on [testuser1/contosoAir](#)

This branch has no conflicts with the base branch Merging can be performed automatically.

[Merge pull request](#) You can also open this in GitHub Desktop or view command line instructions.

Write Preview Leave a comment

Attach files by dragging & dropping, selecting or pasting them.

[Close pull request](#) [Comment](#)

Remember, contributions to this repository should follow our [GitHub Community Guidelines](#).

Reviewers No reviews Still in progress? Convert to draft

Assignees No one—assign yourself

Labels None yet

Projects None yet

Milestone No milestone

Notifications Customize Unsubscribe You're receiving notifications because you authored the thread.

1 participant

## 9. Once your application is deployed, go back to automated deployments to see your history.

Workflow	Pull request	Last run status	Last run time	Workloads	Created on	Created by
ContosoAir	Merged	Succeeded	2022-07-23T16:15:40Z	namespace-workflow-1...	2022-07-23T16:08:55:41...	testuser1@contoso.com

## Clean up resources

You can remove any related resources that you created when you don't need them anymore individually or by deleting the resource group to which they belong. To delete your automated deployment, navigate to the automated deployment dashboard and select ..., then select **delete** and confirm your action.

## Next steps

You can modify these GitHub Actions to meet the needs of your team by opening them up in an editor like Visual Studio Code and changing them as you see fit.

Learn more about [GitHub Actions for Kubernetes](#).

# Build and deploy to Azure Kubernetes Service with Azure Pipelines

10/27/2022 • 12 minutes to read • [Edit Online](#)

## Azure DevOps Services

Use [Azure Pipelines](#) to automatically deploy to Azure Kubernetes Service (AKS). Azure Pipelines lets you build, test, and deploy with continuous integration (CI) and continuous delivery (CD) using [Azure DevOps](#).

In this article, you'll learn how to create a pipeline that continuously builds and deploys your app. Every time you change your code in a repository that contains a Dockerfile, the images are pushed to your Azure Container Registry, and the manifests are then deployed to your AKS cluster.

## Prerequisites

- An Azure account with an active subscription. [Create an account for free](#).
- An Azure Resource Manager service connection. [Create an Azure Resource Manager service connection](#).
- A GitHub account. Create a free [GitHub account](#) if you don't have one already.

## Get the code

Fork the following repository containing a sample application and a Dockerfile:

```
https://github.com/MicrosoftDocs/pipelines-javascript-docker
```

## Create the Azure resources

Sign in to the [Azure portal](#), and then select the [Cloud Shell](#) button in the upper-right corner.

### Create a container registry

```
Create a resource group
az group create --name myapp-rg --location eastus

Create a container registry
az acr create --resource-group myapp-rg --name myContainerRegistry --sku Basic

Create a Kubernetes cluster
az aks create \
 --resource-group myapp-rg \
 --name myapp \
 --node-count 1 \
 --enable-addons monitoring \
 --generate-ssh-keys
```

## Sign in to Azure Pipelines

Sign in to [Azure Pipelines](#). After you sign in, your browser goes to <https://dev.azure.com/my-organization-name> and displays your Azure DevOps dashboard.

Within your selected organization, create a *project*. If you don't have any projects in your organization, you see a

Create a project to get started screen. Otherwise, select the **Create Project** button in the upper-right corner of the dashboard.

## Create the pipeline

### Connect and select your repository

1. Sign in to your Azure DevOps organization and go to your project.
2. Go to **Pipelines**, and then select **New pipeline**.
3. Do the steps of the wizard by first selecting **GitHub** as the location of your source code.
4. You might be redirected to GitHub to sign in. If so, enter your GitHub credentials.
5. When you see the list of repositories, select your repository.
6. You might be redirected to GitHub to install the Azure Pipelines app. If so, select **Approve & install**.
7. Select **Deploy to Azure Kubernetes Service**.
8. If you're prompted, select the subscription in which you created your registry and cluster.
9. Select the `myapp` cluster.
10. For **Namespace**, select **Existing**, and then select **default**.
11. Select the name of your container registry.
12. You can leave the image name set to the default.
13. Set the service port to 8080.
14. Set the **Enable Review App for Pull Requests** checkbox for [review app](#) related configuration to be included in the pipeline YAML auto-generated in subsequent steps.
15. Select **Validate and configure**.

As Azure Pipelines creates your pipeline, the process will:

- Create a *Docker registry service connection* to enable your pipeline to push images into your container registry.
  - Create an *environment* and a Kubernetes resource within the environment. For an RBAC-enabled cluster, the created Kubernetes resource implicitly creates ServiceAccount and RoleBinding objects in the cluster so that the created ServiceAccount can't perform operations outside the chosen namespace.
  - Generate an `azure-pipelines.yml` file, which defines your pipeline.
  - Generate Kubernetes manifest files. These files are generated by hydrating the `deployment.yml` and `service.yml` templates based on selections you made. When you're ready, select **Save and run**.
16. Select **Save and run**.
  17. You can change the **Commit message** to something like *Add pipeline to our repository*. When you're ready, select **Save and run** to commit the new pipeline into your repo, and then begin the first run of your new pipeline!

## See your app deploy

As your pipeline runs, watch as your build stage, and then your deployment stage, go from blue (running) to green (completed). You can select the stages and jobs to watch your pipeline in action.

#### NOTE

If you're using a Microsoft-hosted agent, you must add the IP range of the Microsoft-hosted agent to your firewall. Get the weekly list of IP ranges from the [weekly JSON file](#), which is published every Wednesday. The new IP ranges become effective the following Monday. For more information, see [Microsoft-hosted agents](#). To find the IP ranges that are required for your Azure DevOps organization, learn how to [identify the possible IP ranges for Microsoft-hosted agents](#).

After the pipeline run is finished, explore what happened and then go see your app deployed. From the pipeline summary:

1. Select the **Environments** tab.
2. Select **View environment**.
3. Select the instance of your app for the namespace you deployed to. If you stuck to the defaults we mentioned above, then it will be the **myapp** app in the **default** namespace.
4. Select the **Services** tab.
5. Select and copy the external IP address to your clipboard.
6. Open a new browser tab or window and enter <IP address>:8080.

If you're building our sample app, then *Hello world* appears in your browser.

## How the pipeline builds

When you finished selecting options and then proceeded to validate and configure the pipeline Azure Pipelines created a pipeline for you, using the *Deploy to Azure Kubernetes Service* template.

The build stage uses the [Docker task](#) to build and push the image to the Azure Container Registry.

```
- stage: Build
 displayName: Build stage
 jobs:
 - job: Build
 displayName: Build job
 pool:
 vmImage: $(vmImageName)
 steps:
 - task: Docker@2
 displayName: Build and push an image to container registry
 inputs:
 command: buildAndPush
 repository: $(imageRepository)
 dockerfile: $(dockerfilePath)
 containerRegistry: $(dockerRegistryServiceConnection)
 tags: |
 $(tag)

 - task: PublishPipelineArtifact@1
 inputs:
 artifactName: 'manifests'
 path: 'manifests'
```

The deployment job uses the *Kubernetes manifest task* to create the `imagePullSecret` required by Kubernetes cluster nodes to pull from the Azure Container Registry resource. Manifest files are then used by the Kubernetes

manifest task to deploy to the Kubernetes cluster.

```
- stage: Deploy
displayName: Deploy stage
dependsOn: Build
jobs:
- deployment: Deploy
 displayName: Deploy job
 pool:
 vmImage: $(vmImageName)
 environment: 'myenv.aksnamespace' #customize with your environment
 strategy:
 runOnce:
 deploy:
 steps:
- task: DownloadPipelineArtifact@2
 inputs:
 artifactName: 'manifests'
 downloadPath: '$(System.ArtifactsDirectory)/manifests'

- task: KubernetesManifest@0
 displayName: Create imagePullSecret
 inputs:
 action: createSecret
 secretName: $(imagePullSecret)
 namespace: $(k8sNamespace)
 dockerRegistryEndpoint: $(dockerRegistryServiceConnection)

- task: KubernetesManifest@0
 displayName: Deploy to Kubernetes cluster
 inputs:
 action: deploy
 namespace: $(k8sNamespace)
 manifests: |
 $(System.ArtifactsDirectory)/manifests/deployment.yml
 $(System.ArtifactsDirectory)/manifests/service.yml
 imagePullSecrets: |
 $(imagePullSecret)
 containers: |
 $(containerRegistry)}/${imageRepository}:$(tag)
```

## Clean up resources

Whenever you're done with the resources you created, you can use the following command to delete them:

```
az group delete --name myapp-rg
```

Enter `y` when you're prompted.

Azure DevOps Services | Azure DevOps Server 2020 | Azure DevOps Server 2019

Use [Azure Pipelines](#) to automatically deploy to Azure Kubernetes Service (AKS). Azure Pipelines lets you build, test, and deploy with continuous integration (CI) and continuous delivery (CD) using [Azure DevOps](#).

In this article, you'll learn how to create a pipeline that continuously builds and deploys your app. Every time you change your code in a repository that contains a Dockerfile, the images are pushed to your Azure Container Registry, and the manifests are then deployed to your AKS cluster.

## Prerequisites

- An Azure account with an active subscription. [Create an account for free](#).

- An Azure Resource Manager service connection. [Create an Azure Resource Manager service connection](#).
- A GitHub account. Create a free [GitHub account](#) if you don't have one already.

## Get the code

Fork the following repository containing a sample application and a Dockerfile:

```
https://github.com/MicrosoftDocs/pipelines-javascript-docker
```

## Create the Azure resources

Sign in to the [Azure portal](#), and then select the [Cloud Shell](#) button in the upper-right corner.

### Create a container registry

```
Create a resource group
az group create --name myapp-rg --location eastus

Create a container registry
az acr create --resource-group myapp-rg --name myContainerRegistry --sku Basic

Create a Kubernetes cluster
az aks create \
 --resource-group myapp-rg \
 --name myapp \
 --node-count 1 \
 --enable-addons monitoring \
 --generate-ssh-keys
```

## Configure authentication

When you use Azure Container Registry (ACR) with Azure Kubernetes Service (AKS), you must establish an authentication mechanism. This can be achieved in two ways:

1. Grant AKS access to ACR. See [Authenticate with Azure Container Registry from Azure Kubernetes Service](#).
2. Use a [Kubernetes image pull secret](#). An image pull secret can be created by using the [Kubernetes deployment task](#).

## Create a release pipeline

The build pipeline used to set up CI has already built a Docker image and pushed it to an Azure Container Registry. It also packaged and published a Helm chart as an artifact. In the release pipeline, we'll deploy the container image as a Helm application to the AKS cluster.

1. In [Azure Pipelines](#) open the summary for your build.
2. In the build summary, choose the **Release** icon to start a new release pipeline.  
If you've previously created a release pipeline that uses these build artifacts, you'll be prompted to create a new release instead. In that case, go to the **Releases** page and start a new release pipeline from there by choosing the **+** icon.
3. Select the **Empty** job template.
4. Open the **Tasks** page and select **Agent job**.
5. Choose **+** to add a new task and add a **Helm tool installer** task. This ensures the agent that runs the

subsequent tasks has Helm and Kubectl installed on it.

6. Choose + again and add a **Package and deploy Helm charts** task. Configure the settings for this task as follows:

- **Connection Type:** Select **Azure Resource Manager** to connect to an AKS cluster by using an Azure service connection. Alternatively, if you want to connect to any Kubernetes cluster by using kubeconfig or a service account, you can select **Kubernetes Service Connection**. In this case, you'll need to create and select a Kubernetes service connection instead of an Azure subscription for the following setting.
- **Azure subscription:** Select a connection from the list under **Available Azure Service Connections** or create a more restricted permissions connection to your Azure subscription. If you see an **Authorize** button next to the input, use it to authorize the connection to your Azure subscription. If you don't see the required Azure subscription in the list of subscriptions, see [Create an Azure service connection](#) to manually set up the connection.
- **Resource group:** Enter or select the resource group containing your AKS cluster.
- **Kubernetes cluster:** Enter or select the AKS cluster you created.
- **Command:** Select **init** as the Helm command. This will install Tiller to your running Kubernetes cluster. It will also set up any necessary local configuration. Tick **Use canary image version** to install the latest pre-release version of Tiller. You could also choose to upgrade Tiller if it's pre-installed by ticking **Upgrade Tiller**. If these options are enabled, the task will run  
`helm init --canary-image --upgrade`

7. Choose + in the **Agent job** and add another **Package and deploy Helm charts** task. Configure the settings for this task as follows:

- **Kubernetes cluster:** Enter or select the AKS cluster you created.
- **Namespace:** Enter your Kubernetes cluster namespace where you want to deploy your application. Kubernetes supports multiple virtual clusters backed by the same physical cluster. These virtual clusters are called *namespaces*. You can use namespaces to create different environments such as dev, test, and staging in the same cluster.
- **Command:** Select **upgrade** as the Helm command. You can run any Helm command using this task and pass in command options as arguments. When you select the **upgrade**, the task shows some more fields:
  - **Chart Type:** Select **File Path**. Alternatively, you can specify **Chart Name** if you want to specify a URL or a chart name. For example, if the chart name is `stable/mysql`, the task will execute `helm upgrade stable/mysql`
  - **Chart Path:** This can be a path to a packaged chart or a path to an unpacked chart directory. In this example, you're publishing the chart using a CI build, so select the file package using file picker or enter `$(System.DefaultWorkingDirectory)/**/*.tgz`
  - **Release Name:** Enter a name for your release; for example, `azureddevops`
  - **Recreate Pods:** Tick this checkbox if there is a configuration change during the release and you want to replace a running pod with the new configuration.
  - **Reset Values:** Tick this checkbox if you want the values built into the chart to override all values provided by the task.
  - **Force:** Tick this checkbox if, should conflicts occur, you want to upgrade and rollback to delete, recreate the resource, and reinstall the full release. This is useful in scenarios where

applying patches can fail (for example, for services because the cluster IP address is immutable).

- **Arguments:** Enter the Helm command arguments and their values; for this example `--set image.repository=$(imageRepoName) --set image.tag=$(Build.BuildId)` See [this section](#) for a description of why we're using these arguments.
- **Enable TLS:** Tick this checkbox to enable strong TLS-based connections between Helm and Tiller.
- **CA certificate:** Specify a CA certificate to be uploaded and used to issue certificates for Tiller and Helm client.
- **Certificate:** Specify the Tiller certificate or Helm client certificate
- **Key:** Specify the Tiller Key or Helm client key

8. In the **Variables** page of the pipeline, add a variable named **imageRepoName** and set the value to the name of your Helm image repository. Typically, this is in the format `example.azurecr.io/coderepository`

9. Save the release pipeline.

### Arguments used in the Helm upgrade task

In the build pipeline, the container image is tagged with `$(Build.BuildId)` and this is pushed to an Azure Container Registry. In a Helm chart, you can parameterize the container image details such as the name and tag because the same chart can be used to deploy to different environments. These values can also be specified in the **values.yaml** file or be overridden by a user-supplied values file, which can in turn be overridden by `--set` parameters during the Helm install or upgrade.

In this example, we pass the following arguments:

```
--set image.repository=$(imageRepoName) --set image.tag=$(Build.BuildId)
```

The value of `$(imageRepoName)` was set in the **Variables** page (or the **variables** section of your YAML file). Alternatively, you can directly replace it with your image repository name in the `--set` arguments value or **values.yaml** file. For example:

```
image:
 repository: VALUE_TO_BE_OVERRIDDEN
 tag: latest
```

Another alternative is to set the **Set Values** option of the task to specify the argument values as comma-separated key-value pairs.

## Create a release to deploy your app

You're now ready to create a release, which means to start the process of running the release pipeline with the artifacts produced by a specific build. This will result in deploying the build:

1. Choose **+ Release** and select **Create a release**.
2. In the **Create a new release** panel, check that the artifact version you want to use is selected and choose **Create**.
3. Choose the release link in the information bar message. For example: "Release **Release-1** has been created".
4. In the pipeline view, choose the status link in the stages of the pipeline to see the logs and agent output.

# Azure Policy built-in definitions for Azure Kubernetes Service

10/27/2022 • 18 minutes to read • [Edit Online](#)

This page is an index of [Azure Policy built-in policy definitions](#) for Azure Kubernetes Service. For additional Azure Policy built-ins for other services, see [Azure Policy built-in definitions](#).

The name of each built-in policy definition links to the policy definition in the Azure portal. Use the link in the **Version** column to view the source on the [Azure Policy GitHub repo](#).

## Initiatives

NAME	DESCRIPTION	POLICIES	VERSION
<a href="#">Kubernetes cluster pod security baseline standards for Linux-based workloads</a>	This initiative includes the policies for the Kubernetes cluster pod security baseline standards. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For instructions on using this policy, visit <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	5	1.2.0
<a href="#">Kubernetes cluster pod security restricted standards for Linux-based workloads</a>	This initiative includes the policies for the Kubernetes cluster pod security restricted standards. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For instructions on using this policy, visit <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	8	2.3.0

## Policy definitions

### Microsoft.ContainerService

NAME (AZURE PORTAL)	DESCRIPTION	EFFECT(S)	VERSION (GITHUB)
------------------------	-------------	-----------	---------------------

NAME	DESCRIPTION	EFFECT(S)	VERSION
[Preview]: [Preview]: Kubernetes clusters should gate deployment of vulnerable images	Protect your Kubernetes clusters and container workloads from potential threats by restricting deployment of container images with vulnerable software components. Use Azure Defender CI/CD scanning ( <a href="https://aka.ms/AzureDefenderCICDscanning">https://aka.ms/AzureDefenderCICDscanning</a> ) and Azure defender for container registries ( <a href="https://aka.ms/AzureDefenderForContainerRegistries">https://aka.ms/AzureDefenderForContainerRegistries</a> ) to identify and patch vulnerabilities prior to deployment. Evaluation prerequisite: Policy Addon and Azure Defender Profile. Only applicable for private preview customers.	Audit, Deny, Disabled	2.0.0-preview
[Preview]: [Preview]: Kubernetes clusters should restrict creation of given resource type	Given Kubernetes resource type should not be deployed in certain namespace.	Audit, Deny, Disabled	1.1.0-preview
Authorized IP ranges should be defined on Kubernetes Services	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.	Audit, Disabled	2.0.1
Azure Kubernetes Clusters should use Azure CNI	Azure CNI is a prerequisite for some Azure Kubernetes Service features, including Azure network policies, Windows node pools and virtual nodes add-on. Learn more at: <a href="https://aka.ms/aks-azure-cni">https://aka.ms/aks-azure-cni</a>	Audit, Disabled	1.0.0
Azure Kubernetes Service Clusters should disable Command Invoke	Disabling command invoke can enhance the security by avoiding bypass of restricted network access or Kubernetes role-based access control	Audit, Disabled	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Azure Kubernetes Service Clusters should enable Azure Active Directory integration</a>	AKS-managed Azure Active Directory integration can manage the access to the clusters by configuring Kubernetes role-based access control (Kubernetes RBAC) based on a user's identity or directory group membership. Learn more at: <a href="https://aka.ms/aks-managed-aad">https://aka.ms/aks-managed-aad</a> .	Audit, Disabled	1.0.0
<a href="#">Azure Kubernetes Service clusters should have Defender profile enabled</a>	Microsoft Defender for Containers provides cloud-native Kubernetes security capabilities including environment hardening, workload protection, and run-time protection. When you enable the SecurityProfile.AzureDefender on your Azure Kubernetes Service cluster, an agent is deployed to your cluster to collect security event data. Learn more about Microsoft Defender for Containers in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-introduction?tabs=defender-for-container-arch-aks">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-introduction?tabs=defender-for-container-arch-aks</a>	Audit, Disabled	2.0.0
<a href="#">Azure Kubernetes Service Clusters should have local authentication methods disabled</a>	Disabling local authentication methods improves security by ensuring that Azure Kubernetes Service Clusters should exclusively require Azure Active Directory identities for authentication. Learn more at: <a href="https://aka.ms/aks-disable-local-accounts">https://aka.ms/aks-disable-local-accounts</a> .	Audit, Deny, Disabled	1.0.0
<a href="#">Azure Kubernetes Service Clusters should use managed identities</a>	Use managed identities to wrap around service principals, simplify cluster management and avoid the complexity required to managed service principals. Learn more at: <a href="https://aka.ms/aks-update-managed-identities">https://aka.ms/aks-update-managed-identities</a>	Audit, Disabled	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Azure Kubernetes Service Private Clusters should be enabled</a>	Enable the private cluster feature for your Azure Kubernetes Service cluster to ensure network traffic between your API server and your node pools remains on the private network only. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	1.0.0
<a href="#">Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters</a>	Azure Policy Add-on for Kubernetes service (AKS) extends Gatekeeper v3, an admission controller webhook for Open Policy Agent (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner.	Audit, Disabled	1.0.2
<a href="#">Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys</a>	Encrypting OS and data disks using customer-managed keys provides more control and greater flexibility in key management. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	1.0.0
<a href="#">Configure AAD integrated Azure Kubernetes Service Clusters with required Admin Group Access</a>	Ensure to improve cluster security by centrally govern Administrator access to Azure Active Directory integrated AKS clusters.	DeployIfNotExists, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
Configure Azure Kubernetes Service clusters to enable Defender profile	Microsoft Defender for Containers provides cloud-native Kubernetes security capabilities including environment hardening, workload protection, and run-time protection. When you enable the SecurityProfile.AzureDefender on your Azure Kubernetes Service cluster, an agent is deployed to your cluster to collect security event data. Learn more about Microsoft Defender for Containers: <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-introduction?tabs=defender-for-container-arch-aks">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-introduction?tabs=defender-for-container-arch-aks</a> .	DeployIfNotExists, Disabled	4.0.0
Configure installation of Flux extension on Kubernetes cluster	Install Flux extension on Kubernetes cluster to enable deployment of 'fluxconfigurations' in the cluster	DeployIfNotExists, Disabled	1.0.0
Configure Kubernetes clusters with Flux v2 configuration using Bucket source and secrets in KeyVault	Deploy a 'fluxConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined Bucket. This definition requires a Bucket SecretKey stored in Key Vault. For instructions, visit <a href="https://aka.ms/GitOpsFlux2Policy">https://aka.ms/GitOpsFlux2Policy</a> .	DeployIfNotExists, Disabled	1.0.0
Configure Kubernetes clusters with Flux v2 configuration using Git repository and HTTPS CA Certificate	Deploy a 'fluxConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined Git repository. This definition requires a HTTPS CA Certificate. For instructions, visit <a href="https://aka.ms/GitOpsFlux2Policy">https://aka.ms/GitOpsFlux2Policy</a> .	DeployIfNotExists, Disabled	1.0.1

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Configure Kubernetes clusters with Flux v2 configuration using Git repository and HTTPS secrets</a>	Deploy a 'fluxConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined Git repository. This definition requires a HTTPS key secret stored in Key Vault. For instructions, visit <a href="https://aka.ms/GitOpsFlux2Policy">https://aka.ms/GitOpsFlux2 Policy</a> .	DeployIfExists, Disabled	1.0.0
<a href="#">Configure Kubernetes clusters with Flux v2 configuration using Git repository and local secrets</a>	Deploy a 'fluxConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined Git repository. This definition requires local authentication secrets stored in the Kubernetes cluster. For instructions, visit <a href="https://aka.ms/GitOpsFlux2Policy">https://aka.ms/GitOpsFlux2 Policy</a> .	DeployIfExists, Disabled	1.0.0
<a href="#">Configure Kubernetes clusters with Flux v2 configuration using Git repository and SSH secrets</a>	Deploy a 'fluxConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined Git repository. This definition requires a SSH private key secret stored in Key Vault. For instructions, visit <a href="https://aka.ms/GitOpsFlux2Policy">https://aka.ms/GitOpsFlux2 Policy</a> .	DeployIfExists, Disabled	1.0.0
<a href="#">Configure Kubernetes clusters with Flux v2 configuration using public Git repository</a>	Deploy a 'fluxConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined Git repository. This definition requires no secrets. For instructions, visit <a href="https://aka.ms/GitOpsFlux2Policy">https://aka.ms/GitOpsFlux2 Policy</a> .	DeployIfExists, Disabled	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Configure Kubernetes clusters with specified Flux v2 Bucket source using local secrets</a>	Deploy a 'fluxConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined Bucket. This definition requires local authentication secrets stored in the Kubernetes cluster. For instructions, visit <a href="https://aka.ms/GitOpsFlux2Policy">https://aka.ms/GitOpsFlux2Policy</a> .	DeployIfExists, Disabled	1.0.0
<a href="#">Configure Kubernetes clusters with specified GitOps configuration using HTTPS secrets</a>	Deploy a 'sourceControlConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined git repo. This definition requires HTTPS user and key secrets stored in Key Vault. For instructions, visit <a href="https://aka.ms/K8sGitOpsPolicy">https://aka.ms/K8sGitOpsPolicy</a> .	auditIfExists, AuditIfExists, deployIfExists, DeployIfExists, disabled, Disabled	1.1.0
<a href="#">Configure Kubernetes clusters with specified GitOps configuration using no secrets</a>	Deploy a 'sourceControlConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined git repo. This definition requires no secrets. For instructions, visit <a href="https://aka.ms/K8sGitOpsPolicy">https://aka.ms/K8sGitOpsPolicy</a> .	auditIfExists, AuditIfExists, deployIfExists, DeployIfExists, disabled, Disabled	1.1.0
<a href="#">Configure Kubernetes clusters with specified GitOps configuration using SSH secrets</a>	Deploy a 'sourceControlConfiguration' to Kubernetes clusters to assure that the clusters get their source of truth for workloads and configurations from the defined git repo. This definition requires a SSH private key secret in Key Vault. For instructions, visit <a href="https://aka.ms/K8sGitOpsPolicy">https://aka.ms/K8sGitOpsPolicy</a> .	auditIfExists, AuditIfExists, deployIfExists, DeployIfExists, disabled, Disabled	1.1.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Deploy - Configure diagnostic settings for Azure Kubernetes Service to Log Analytics workspace</a>	Deploys the diagnostic settings for Azure Kubernetes Service to stream resource logs to a Log Analytics workspace.	DeployIfNotExists, Disabled	3.0.0
<a href="#">Deploy Azure Policy Add-on to Azure Kubernetes Service clusters</a>	Use Azure Policy Add-on to manage and report on the compliance state of your Azure Kubernetes Service (AKS) clusters. For more information, see <a href="https://aka.ms/akspolicydoc">https://aka.ms/akspolicydoc</a> .	DeployIfNotExists, Disabled	4.0.0
<a href="#">Disable Command Invoke on Azure Kubernetes Service clusters</a>	Disabling command invoke can enhance the security by rejecting invoke-command access to the cluster	DeployIfNotExists, Disabled	1.0.0
<a href="#">Ensure cluster containers have readiness or liveness probes configured</a>	This policy enforces that all pods have a readiness and/or liveness probes configured. Probe Types can be any of tcpSocket, httpGet and exec. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For instructions on using this policy, visit <a href="https://aka.ms/kubepolicydc">https://aka.ms/kubepolicydc</a> .	Audit, Deny, Disabled	2.0.0
<a href="#">Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits</a>	Enforce container CPU and memory resource limits to prevent resource exhaustion attacks in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydc">https://aka.ms/kubepolicydc</a> .	audit, Audit, deny, Deny, disabled, Disabled	8.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes cluster containers should not share host process ID or host IPC namespace</a>	<p>Block pod containers from sharing the host process ID namespace and host IPC namespace in a Kubernetes cluster. This recommendation is part of CIS 5.2.2 and CIS 5.2.3 which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	4.0.1
<a href="#">Kubernetes cluster containers should not use forbidden sysctl interfaces</a>	<p>Containers should not use forbidden sysctl interfaces in a Kubernetes cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	6.0.2
<a href="#">Kubernetes cluster containers should only use allowed AppArmor profiles</a>	<p>Containers should only use allowed AppArmor profiles in a Kubernetes cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	5.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes cluster containers should only use allowed capabilities</a>	Restrict the capabilities to reduce the attack surface of containers in a Kubernetes cluster. This recommendation is part of CIS 5.2.8 and CIS 5.2.9 which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	5.0.1
<a href="#">Kubernetes cluster containers should only use allowed images</a>	Use images from trusted registries to reduce the Kubernetes cluster's exposure risk to unknown vulnerabilities, security issues and malicious images. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	8.0.0
<a href="#">Kubernetes cluster containers should only use allowed ProcMountType</a>	Pod containers can only use allowed ProcMountTypes in a Kubernetes cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	7.0.1
<a href="#">Kubernetes cluster containers should only use allowed pull policy</a>	Restrict containers' pull policy to enforce containers to use only allowed images on deployments	Audit, Deny, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes cluster containers should only use allowed seccomp profiles</a>	<p>Pod containers can only use allowed seccomp profiles in a Kubernetes cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	5.0.1
<a href="#">Kubernetes cluster containers should run with a read only root file system</a>	<p>Run containers with a read only root file system to protect from changes at run-time with malicious binaries being added to PATH in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	5.0.0
<a href="#">Kubernetes cluster pod FlexVolume volumes should only use allowed drivers</a>	<p>Pod FlexVolume volumes should only use allowed drivers in a Kubernetes cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	4.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes cluster pod hostPath volumes should only use allowed host paths</a>	<p>Limit pod HostPath volume mounts to the allowed host paths in a Kubernetes Cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	5.0.1
<a href="#">Kubernetes cluster pods and containers should only run with approved user and group IDs</a>	<p>Control the user, primary group, supplemental group and file system group IDs that pods and containers can use to run in a Kubernetes Cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	5.0.2
<a href="#">Kubernetes cluster pods and containers should only use allowed SELinux options</a>	<p>Pods and containers should only use allowed SELinux options in a Kubernetes cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	6.0.2

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes cluster pods should only use allowed volume types</a>	<p>Pods can only use allowed volume types in a Kubernetes cluster. This recommendation is part of Pod Security Policies which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	4.0.1
<a href="#">Kubernetes cluster pods should only use approved host network and port range</a>	<p>Restrict pod access to the host network and the allowable host port range in a Kubernetes cluster. This recommendation is part of CIS 5.2.4 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	5.0.0
<a href="#">Kubernetes cluster pods should use specified labels</a>	<p>Use specified labels to identify the pods in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	6.2.1
<a href="#">Kubernetes cluster services should listen only on allowed ports</a>	<p>Restrict services to listen only on allowed ports to secure access to the Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	7.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes cluster services should only use allowed external IPs</a>	Use allowed external IPs to avoid the potential attack (CVE-2020-8554) in a Kubernetes cluster. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	4.0.1
<a href="#">Kubernetes cluster should not allow privileged containers</a>	Do not allow privileged containers creation in a Kubernetes cluster. This recommendation is part of CIS 5.2.1 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	8.0.0
<a href="#">Kubernetes cluster should not use naked pods</a>	Block usage of naked Pods. Naked Pods will not be rescheduled in the event of a node failure. Pods should be managed by Deployment, Replicset, Daemonset or Jobs	Audit, Deny, Disabled	1.0.0
<a href="#">Kubernetes cluster Windows containers should not overcommit cpu and memory</a>	Windows container resource requests should be less or equal to the resource limit or unspecified to avoid overcommit. If Windows memory is over-provisioned it will process pages in disk - which can slow down performance - instead of terminating the container with out-of-memory	Audit, Deny, Disabled	1.0.2
<a href="#">Kubernetes cluster Windows containers should only run with approved user and domain user group</a>	Control the user that Windows pods and containers can use to run in a Kubernetes Cluster. This recommendation is part of Pod Security Policies on Windows nodes which are intended to improve the security of your Kubernetes environments.	Audit, Deny, Disabled	1.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes clusters should be accessible only over HTTPS</a>	Use of HTTPS ensures authentication and protects data in transit from network layer eavesdropping attacks. This capability is currently generally available for Kubernetes Service (AKS), and in preview for AKS Engine and Azure Arc enabled Kubernetes. For more info, visit <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a>	audit, Audit, deny, Deny, disabled, Disabled	7.0.0
<a href="#">Kubernetes clusters should disable automounting API credentials</a>	Disable automounting API credentials to prevent a potentially compromised Pod resource to run API commands against Kubernetes clusters. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	3.0.1
<a href="#">Kubernetes clusters should not allow container privilege escalation</a>	Do not allow containers to run with privilege escalation to root in a Kubernetes cluster. This recommendation is part of CIS 5.2.5 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.0.1
<a href="#">Kubernetes clusters should not allow endpoint edit permissions of ClusterRole/system:aggregate-to-edit</a>	ClusterRole/system:aggregate-to-edit should not allow endpoint edit permissions due to CVE-2021-25740, Endpoint & EndpointSlice permissions allow cross-Namespace forwarding, <a href="https://github.com/kubernetes/kubernetes/issues/103675">https://github.com/kubernetes/kubernetes/issues/103675</a> . This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	Audit, Disabled	2.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes clusters should not grant CAP_SYS_ADMIN security capabilities</a>	To reduce the attack surface of your containers, restrict CAP_SYS_ADMIN Linux capabilities. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	4.0.0
<a href="#">Kubernetes clusters should not use specific security capabilities</a>	Prevent specific security capabilities in Kubernetes clusters to prevent ungranted privileges on the Pod resource. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	4.0.1
<a href="#">Kubernetes clusters should not use the default namespace</a>	Prevent usage of the default namespace in Kubernetes clusters to protect against unauthorized access for ConfigMap, Pod, Secret, Service, and ServiceAccount resource types. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	3.0.1
<a href="#">Kubernetes clusters should use Container Storage Interface(CSI) driver StorageClass</a>	The Container Storage Interface (CSI) is a standard for exposing arbitrary block and file storage systems to containerized workloads on Kubernetes. In-tree provisioner StorageClass should be deprecated since AKS version 1.21. To learn more, <a href="https://aka.ms/aks-csi-driver">https://aka.ms/aks-csi-driver</a>	Audit, Deny, Disabled	1.1.0
<a href="#">Kubernetes clusters should use internal load balancers</a>	Use internal load balancers to make a Kubernetes service accessible only to applications running in the same virtual network as the Kubernetes cluster. For more information, see <a href="https://aka.ms/kubepolicyd_oc">https://aka.ms/kubepolicyd_oc</a> .	audit, Audit, deny, Deny, disabled, Disabled	7.0.0

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Kubernetes resources should have required annotations</a>	Ensure that required annotations are attached on a given Kubernetes resource kind for improved resource management of your Kubernetes resources. This policy is generally available for Kubernetes Service (AKS), and preview for AKS Engine and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	Audit, Deny, Disabled	2.0.0
<a href="#">Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version</a>	Upgrade your Kubernetes service cluster to a later Kubernetes version to protect against known vulnerabilities in your current Kubernetes version. Vulnerability CVE-2019-9946 has been patched in Kubernetes versions 1.11.9+, 1.12.7+, 1.13.5+, and 1.14.0+	Audit, Disabled	1.0.2
<a href="#">Resource logs in Azure Kubernetes Service should be enabled</a>	Azure Kubernetes Service's resource logs can help recreate activity trails when investigating security incidents. Enable it to make sure the logs will exist when needed	AuditIfNotExists, Disabled	1.0.0
<a href="#">Role-Based Access Control (RBAC) should be used on Kubernetes Services</a>	To provide granular filtering on the actions that users can perform, use Role-Based Access Control (RBAC) to manage permissions in Kubernetes Service Clusters and configure relevant authorization policies.	Audit, Disabled	1.0.2
<a href="#">Running container images should have vulnerability findings resolved</a>	Container image vulnerability assessment scans container images running on your Kubernetes clusters for security vulnerabilities and exposes detailed findings for each image. Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks.	AuditIfNotExists, Disabled	1.0.1

NAME	DESCRIPTION	EFFECT(S)	VERSION
<a href="#">Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host</a>	To enhance data security, the data stored on the virtual machine (VM) host of your Azure Kubernetes Service nodes VMs should be encrypted at rest. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	1.0.0

## Next steps

- See the built-ins on the [Azure Policy GitHub repo](#).
- Review the [Azure Policy definition structure](#).
- Review [Understanding policy effects](#).

# Support policies for Azure Kubernetes Service

10/27/2022 • 9 minutes to read • [Edit Online](#)

This article provides details about technical support policies and limitations for Azure Kubernetes Service (AKS). The article also details agent node management, managed control plane components, third-party open-source components, and security or patch management.

## Service updates and releases

- For release information, see [AKS release notes](#).
- For information on features in preview, see the [AKS roadmap](#).

## Managed features in AKS

Base infrastructure as a service (IaaS) cloud components, such as compute or networking components, allow you access to low-level controls and customization options. By contrast, AKS provides a turnkey Kubernetes deployment that gives you the common set of configurations and capabilities you need for your cluster. As an AKS user, you have limited customization and deployment options. In exchange, you don't need to worry about or manage Kubernetes clusters directly.

With AKS, you get a fully managed *control plane*. The control plane contains all of the components and services you need to operate and provide Kubernetes clusters to end users. All Kubernetes components are maintained and operated by Microsoft.

Microsoft manages and monitors the following components through the control pane:

- Kubelet or Kubernetes API servers
- Etcd or a compatible key-value store, providing Quality of Service (QoS), scalability, and runtime
- DNS services (for example, kube-dns or CoreDNS)
- Kubernetes proxy or networking (except when [BYOCNI](#) is used)
- Any additional [add-ons](#) or system component running in the kube-system namespace

AKS isn't a Platform-as-a-Service (PaaS) solution. Some components, such as agent nodes, have *shared responsibility*, where users must help maintain the AKS cluster. User input is required, for example, to apply an agent node operating system (OS) security patch.

The services are *managed* in the sense that Microsoft and the AKS team deploys, operates, and is responsible for service availability and functionality. Customers can't alter these managed components. Microsoft limits customization to ensure a consistent and scalable user experience.

## Shared responsibility

When a cluster is created, you define the Kubernetes agent nodes that AKS creates. Your workloads are executed on these nodes.

Because your agent nodes execute private code and store sensitive data, Microsoft Support can access them only in a very limited way. Microsoft Support can't sign in to, execute commands in, or view logs for these nodes without your express permission or assistance.

Any modification done directly to the agent nodes using any of the IaaS APIs renders the cluster unsupportable. Any modification done to the agent nodes must be done using kubernetes-native mechanisms such as

Similarly, while you may add any metadata to the cluster and nodes, such as tags and labels, changing any of the system created metadata will render the cluster unsupported.

## AKS support coverage

Microsoft provides technical support for the following examples:

- Connectivity to all Kubernetes components that the Kubernetes service provides and supports, such as the API server.
- Management, uptime, QoS, and operations of Kubernetes control plane services (Kubernetes control plane, API server, etcd, and coreDNS, for example).
- Etcd data store. Support includes automated, transparent backups of all etcd data every 30 minutes for disaster planning and cluster state restoration. These backups aren't directly available to you or any users. They ensure data reliability and consistency. On-demand rollback or restore is not supported as a feature.
- Any integration points in the Azure cloud provider driver for Kubernetes. These include integrations into other Azure services such as load balancers, persistent volumes, or networking (Kubernetes and Azure CNI, except when [BYOCNI](#) is in use).
- Questions or issues about customization of control plane components such as the Kubernetes API server, etcd, and coreDNS.
- Issues about networking, such as Azure CNI, kubenet, or other network access and functionality issues, except when [BYOCNI](#) is in use. Issues could include DNS resolution, packet loss, routing, and so on. Microsoft supports various networking scenarios:
  - Kubenet and Azure CNI using managed VNETs or with custom (bring your own) subnets.
  - Connectivity to other Azure services and applications
  - Ingress controllers and ingress or load balancer configurations
  - Network performance and latency
  - [Network policies](#)

### NOTE

Any cluster actions taken by Microsoft/AKS are made with user consent under a built-in Kubernetes role `aks-service` and built-in role binding `aks-service-rolebinding`. This role enables AKS to troubleshoot and diagnose cluster issues, but can't modify permissions nor create roles or role bindings, or other high privilege actions. Role access is only enabled under active support tickets with just-in-time (JIT) access.

Microsoft doesn't provide technical support for the following examples:

- Questions about how to use Kubernetes. For example, Microsoft Support doesn't provide advice on how to create custom ingress controllers, use application workloads, or apply third-party or open-source software packages or tools.

### NOTE

Microsoft Support can advise on AKS cluster functionality, customization, and tuning (for example, Kubernetes operations issues and procedures).

- Third-party open-source projects that aren't provided as part of the Kubernetes control plane or deployed with AKS clusters. These projects might include Istio, Helm, Envoy, or others.

**NOTE**

Microsoft can provide best-effort support for third-party open-source projects such as Helm. Where the third-party open-source tool integrates with the Kubernetes Azure cloud provider or other AKS-specific bugs, Microsoft supports examples and applications from Microsoft documentation.

- Third-party closed-source software. This software can include security scanning tools and networking devices or software.
- Network customizations other than the ones listed in the [AKS documentation](#).
- Custom or 3rd-party CNI plugins used in [BYOCNI](#) mode.

## AKS support coverage for agent nodes

### Microsoft responsibilities for AKS agent nodes

Microsoft and users share responsibility for Kubernetes agent nodes where:

- The base OS image has required additions (such as monitoring and networking agents).
- The agent nodes receive OS patches automatically.
- Issues with the Kubernetes control plane components that run on the agent nodes are automatically remediated. These components include the below:
  - `Kube-proxy`
  - Networking tunnels that provide communication paths to the Kubernetes master components
  - `Kubelet`
  - Docker or `containerd`

**NOTE**

If an agent node is not operational, AKS might restart individual components or the entire agent node. These restart operations are automated and provide auto-remediation for common issues. If you want to know more about the auto-remediation mechanisms, see [Node Auto-Repair](#)

### Customer responsibilities for AKS agent nodes

Microsoft provides patches and new images for your image nodes weekly, but doesn't automatically patch them by default. To keep your agent node OS and runtime components patched, you should keep a regular [node image upgrade](#) schedule or automate it.

Similarly, AKS regularly releases new kubernetes patches and minor versions. These updates can contain security or functionality improvements to Kubernetes. You're responsible to keep your clusters' kubernetes version updated and according to the [AKS Kubernetes Support Version Policy](#).

### User customization of agent nodes

**NOTE**

AKS agent nodes appear in the Azure portal as regular Azure IaaS resources. But these virtual machines are deployed into a custom Azure resource group (usually prefixed with MC\_\*) . You cannot change the base OS image or do any direct customizations to these nodes using the IaaS APIs or resources. Any custom changes that are not done via the AKS API will not persist through an upgrade, scale, update or reboot. Also any change to the nodes' extensions like the CustomScriptExtension one can lead to unexpected behavior and should be prohibited. Avoid performing changes to the agent nodes unless Microsoft Support directs you to make changes.

AKS manages the lifecycle and operations of agent nodes on your behalf - modifying the IaaS resources

associated with the agent nodes is **not supported**. An example of an unsupported operation is customizing a node pool virtual machine scale set by manually changing configurations through the virtual machine scale set portal or API.

For workload-specific configurations or packages, AKS recommends using [Kubernetes daemon sets](#).

Using Kubernetes privileged [daemon sets](#) and init containers enables you to tune/modify or install 3rd party software on cluster agent nodes. Examples of such customizations include adding custom security scanning software or updating sysctl settings.

While this path is recommended if the above requirements apply, AKS engineering and support cannot assist in troubleshooting or diagnosing modifications that render the node unavailable due to a custom deployed [daemon set](#).

### Security issues and patching

If a security flaw is found in one or more of the managed components of AKS, the AKS team will patch all affected clusters to mitigate the issue. Alternatively, the team will give users upgrade guidance.

For agent nodes affected by a security flaw, Microsoft will notify you with details on the impact and the steps to fix or mitigate the security issue (normally a node image upgrade or a cluster patch upgrade).

### Node maintenance and access

Although you can sign in to and change agent nodes, doing this operation is discouraged because changes can make a cluster unsupportable.

## Network ports, access, and NSGs

You may only customize the NSGs on custom subnets. You may not customize NSGs on managed subnets or at the NIC level of the agent nodes. AKS has egress requirements to specific endpoints, to control egress and ensure the necessary connectivity, see [limit egress traffic](#). For ingress, the requirements are based on the applications you have deployed to cluster.

## Stopped or de-allocated clusters

As stated earlier, manually de-allocating all cluster nodes via the IaaS APIs/CLI/portal renders the cluster out of support. The only supported way to stop/de-allocate all nodes is to [stop the AKS cluster](#), which preserves the cluster state for up to 12 months.

Clusters that are stopped for more than 12 months will no longer preserve state.

Clusters that are de-allocated outside of the AKS APIs have no state preservation guarantees. The control planes for clusters in this state will be archived after 30 days, and deleted after 12 months.

AKS reserves the right to archive control planes that have been configured out of support guidelines for extended periods equal to and beyond 30 days. AKS maintains backups of cluster etcd metadata and can readily reallocate the cluster. This reallocation can be initiated by any PUT operation bringing the cluster back into support, such as an upgrade or scale to active agent nodes.

If your subscription is suspended or deleted, your cluster's control plane and state will be deleted after 90 days.

## Unsupported alpha and beta Kubernetes features

AKS only supports stable and beta features within the upstream Kubernetes project. Unless otherwise documented, AKS doesn't support any alpha feature that is available in the upstream Kubernetes project.

## Preview features or feature flags

For features and functionality that requires extended testing and user feedback, Microsoft releases new preview features or features behind a feature flag. Consider these features as prerelease or beta features.

Preview features or feature-flag features aren't meant for production. Ongoing changes in APIs and behavior, bug fixes, and other changes can result in unstable clusters and downtime.

Features in public preview are fall under 'best effort' support as these features are in preview and not meant for production and are supported by the AKS technical support teams during business hours only. For more information, see:

- [Azure Support FAQ](#)

## Upstream bugs and issues

Given the speed of development in the upstream Kubernetes project, bugs invariably arise. Some of these bugs can't be patched or worked around within the AKS system. Instead, bug fixes require larger patches to upstream projects (such as Kubernetes, node or agent operating systems, and kernel). For components that Microsoft owns (such as the Azure cloud provider), AKS and Azure personnel are committed to fixing issues upstream in the community.

When a technical support issue is root-caused by one or more upstream bugs, AKS support and engineering teams will:

- Identify and link the upstream bugs with any supporting details to help explain why this issue affects your cluster or workload. Customers receive links to the required repositories so they can watch the issues and see when a new release will provide fixes.
- Provide potential workarounds or mitigation. If the issue can be mitigated, a [known issue](#) will be filed in the AKS repository. The known-issue filing explains:
  - The issue, including links to upstream bugs.
  - The workaround and details about an upgrade or another persistence of the solution.
  - Rough timelines for the issue's inclusion, based on the upstream release cadence.

# Frequently asked questions about Azure Kubernetes Service (AKS)

10/27/2022 • 16 minutes to read • [Edit Online](#)

This article addresses frequent questions about Azure Kubernetes Service (AKS).

## Which Azure regions currently provide AKS?

For a complete list of available regions, see [AKS regions and availability](#).

## Can I spread an AKS cluster across regions?

No. AKS clusters are regional resources and can't span regions. See [best practices for business continuity and disaster recovery](#) for guidance on how to create an architecture that includes multiple regions.

## Can I spread an AKS cluster across availability zones?

Yes. You can deploy an AKS cluster across one or more [availability zones](#) in [regions that support them](#).

## Can I limit who has access to the Kubernetes API server?

Yes. There are two options for limiting access to the API server:

- Use [API Server Authorized IP Ranges](#) if you want to maintain a public endpoint for the API server but restrict access to a set of trusted IP ranges.
- Use a [private cluster](#) if you want to limit the API server to *only* be accessible from within your virtual network.

## Can I have different VM sizes in a single cluster?

Yes, you can use different virtual machine sizes in your AKS cluster by creating [multiple node pools](#).

## Are security updates applied to AKS agent nodes?

AKS patches CVE's that have a "vendor fix" every week. CVE's without a fix are waiting on a "vendor fix" before it can be remediated. The AKS images will get automatically updated inside of 30 days and it recommended that customer apply an updated Node Image on a regular cadence to ensure that latest patched images and OS patches are all applied and current:

- Manually, through the Azure portal or the Azure CLI.
- By upgrading your AKS cluster. The cluster upgrades [cordon and drain nodes](#) automatically and then bring a new node online with the latest Ubuntu image and a new patch version or a minor Kubernetes version. For more information, see [Upgrade an AKS cluster](#).
- By using [node image upgrade](#).

## What is the size limit on a container image in AKS?

AKS does not set a limit on the container image size. However, it is important to understand that the larger the image, the higher the memory demand. This could potentially exceed resource limits or the overall available memory of worker nodes. By default, memory for VM size Standard\_DS2\_v2 for an AKS cluster is set to 7 GiB.

When a container image is excessively large, as in the Terabyte (TBs) range, kubelet might not be able to pull it from your container registry to a node due to lack of disk space.

## Windows Server nodes

For Windows Server nodes, Windows Update does not automatically run and apply the latest updates. On a regular schedule around the Windows Update release cycle and your own validation process, you should perform an upgrade on the cluster and the Windows Server node pool(s) in your AKS cluster. This upgrade process creates nodes that run the latest Windows Server image and patches, then removes the older nodes. For more information on this process, see [Upgrade a node pool in AKS](#).

## Are there security threats targeting AKS that customers should be aware of?

Microsoft provides guidance for other actions you can take to secure your workloads through services like [Microsoft Defender for Containers](#). The following security threat is related to AKS and Kubernetes that customers should be aware of:

- [New large-scale campaign targets Kubeflow](#) - June 8, 2021

## How does the managed Control Plane communicate with my Nodes?

AKS uses a secure tunnel communication to allow the api-server and individual node kubelets to communicate even on separate virtual networks. The tunnel is secured through TLS encryption. The current main tunnel that is used by AKS is [Konnectivity, previously known as apiserver-network-proxy](#). Verify all network rules follow the [Azure required network rules and FQDNs](#).

## Why are two resource groups created with AKS?

AKS builds upon many Azure infrastructure resources, including virtual machine scale sets, virtual networks, and managed disks. This enables you to apply many of the core capabilities of the Azure platform within the managed Kubernetes environment provided by AKS. For example, most Azure virtual machine types can be used directly with AKS and Azure Reservations can be used to receive discounts on those resources automatically.

To enable this architecture, each AKS deployment spans two resource groups:

1. You create the first resource group. This group contains only the Kubernetes service resource. The AKS resource provider automatically creates the second resource group during deployment. An example of the second resource group is *MC\_myResourceGroup\_myAKSCluster\_eastus*. For information on how to specify the name of this second resource group, see the next section.
2. The second resource group, known as the *node resource group*, contains all of the infrastructure resources associated with the cluster. These resources include the Kubernetes node VMs, virtual networking, and storage. By default, the node resource group has a name like *MC\_myResourceGroup\_myAKSCluster\_eastus*. AKS automatically deletes the node resource group whenever the cluster is deleted, so it should only be used for resources that share the cluster's lifecycle.

## Can I provide my own name for the AKS node resource group?

Yes. By default, AKS will name the node resource group *MC\_resourcegroupname\_clusternamespace\_location*, but you can also provide your own name.

To specify your own resource group name, install the [aks-preview](#) Azure CLI extension version 0.3.2 or later. When you create an AKS cluster by using the [az aks create](#) command, use the `--node-resource-group` parameter and specify a name for the resource group. If you [use an Azure Resource Manager template](#) to deploy an AKS cluster, you can define the resource group name by using the *nodeResourceGroup* property.

- The secondary resource group is automatically created by the Azure resource provider in your own subscription.
- You can specify a custom resource group name only when you're creating the cluster.

As you work with the node resource group, keep in mind that you can't:

- Specify an existing resource group for the node resource group.
- Specify a different subscription for the node resource group.
- Change the node resource group name after the cluster has been created.
- Specify names for the managed resources within the node resource group.
- Modify or delete Azure-created tags of managed resources within the node resource group. (See additional information in the next section.)

## Can I modify tags and other properties of the AKS resources in the node resource group?

If you modify or delete Azure-created tags and other resource properties in the node resource group, you could get unexpected results such as scaling and upgrading errors. AKS allows you to create and modify custom tags created by end users, and you can add those tags when [creating a node pool](#). You might want to create or modify custom tags, for example, to assign a business unit or cost center. This can also be achieved by creating Azure Policies with a scope on the managed resource group.

However, modifying any **Azure-created tags** on resources under the node resource group in the AKS cluster is an unsupported action, which breaks the service-level objective (SLO). For more information, see [Does AKS offer a service-level agreement?](#)

## What Kubernetes admission controllers does AKS support? Can admission controllers be added or removed?

AKS supports the following [admission controllers](#):

- *NamespaceLifecycle*
- *LimitRanger*
- *ServiceAccount*
- *DefaultStorageClass*
- *DefaultTolerationSeconds*
- *MutatingAdmissionWebhook*
- *ValidatingAdmissionWebhook*
- *ResourceQuota*
- *PodNodeSelector*
- *PodTolerationRestriction*
- *ExtendedResourceToleration*

Currently, you can't modify the list of admission controllers in AKS.

## Can I use admission controller webhooks on AKS?

Yes, you may use admission controller webhooks on AKS. It's recommended you exclude internal AKS namespaces, which are marked with the **control-plane label**. For example, by adding the below to the webhook configuration:

```
namespaceSelector:
 matchExpressions:
 - key: control-plane
 operator: DoesNotExist
```

AKS firewalls the API server egress so your admission controller webhooks need to be accessible from within the cluster.

## Can admission controller webhooks impact kube-system and internal AKS namespaces?

To protect the stability of the system and prevent custom admission controllers from impacting internal services in the kube-system, namespace AKS has an **Admissions Enforcer**, which automatically excludes kube-system and AKS internal namespaces. This service ensures the custom admission controllers don't affect the services running in kube-system.

If you have a critical use case for deploying something on kube-system (not recommended) in support of your custom admission webhook, you may add the below label or annotation so that Admissions Enforcer ignores it.

Label: `"admissions.enforcer/disabled": "true"` or Annotation: `"admissions.enforcer/disabled": true`

## Is Azure Key Vault integrated with AKS?

[Azure Key Vault Provider for Secrets Store CSI Driver](#) provides native integration of Azure Key Vault into AKS.

## Can I run Windows Server containers on AKS?

Yes, Windows Server containers are available on AKS. To run Windows Server containers in AKS, you create a node pool that runs Windows Server as the guest OS. Windows Server containers can use only Windows Server 2019. To get started, see [Create an AKS cluster with a Windows Server node pool](#).

Windows Server support for node pool includes some limitations that are part of the upstream Windows Server in Kubernetes project. For more information on these limitations, see [Windows Server containers in AKS limitations](#).

## Does AKS offer a service-level agreement?

AKS provides SLA guarantees as an optional feature with [Uptime SLA](#).

The Free SKU offered by default doesn't have a associated Service Level *Agreement*, but has a Service Level *Objective* of 99.5%. Transient connectivity issues are observed if there was an upgrade, unhealthy underlay nodes, platform maintenance, or an application overwhelms the API Server with requests, etc. If your workload doesn't tolerate API Server restarts, then we suggest using Uptime SLA.

## Can I apply Azure reservation discounts to my AKS agent nodes?

AKS agent nodes are billed as standard Azure virtual machines. If you've purchased [Azure reservations](#) for the VM size that you're using in AKS, those discounts are automatically applied.

## Can I move/migrate my cluster between Azure tenants?

Moving your AKS cluster between tenants is currently unsupported.

## Can I move/migrate my cluster between subscriptions?

Movement of clusters between subscriptions is currently unsupported.

## Can I move my AKS clusters from the current Azure subscription to another?

Moving your AKS cluster and its associated resources between Azure subscriptions isn't supported.

## Can I move my AKS cluster or AKS infrastructure resources to other resource groups or rename them?

Moving or renaming your AKS cluster and its associated resources isn't supported.

## Why is my cluster delete taking so long?

Most clusters are deleted upon user request; in some cases, especially where customers are bringing their own Resource Group, or doing cross-RG tasks deletion can take more time or fail. If you have an issue with deletes, double-check that you do not have locks on the RG, that any resources outside of the RG are disassociated from the RG, and so on.

## If I have pod / deployments in state 'NodeLost' or 'Unknown' can I still upgrade my cluster?

You can, but AKS doesn't recommend this. Upgrades should be performed when the state of the cluster is known and healthy.

## If I have a cluster with one or more nodes in an Unhealthy state or shut down, can I perform an upgrade?

No, delete/remove any nodes in a failed state or otherwise removed from the cluster prior to upgrading.

## I ran a cluster delete, but see the error

[Errno 11001] getaddrinfo failed

Most commonly, this is caused by users having one or more Network Security Groups (NSGs) still in use and associated with the cluster. Remove them and attempt the delete again.

## I ran an upgrade, but now my pods are in crash loops, and readiness probes fail?

Confirm your service principal hasn't expired. See: [AKS service principal](#) and [AKS update credentials](#).

## My cluster was working, but suddenly can't provision LoadBalancers, mount PVCs, etc.?

Confirm your service principal hasn't expired. See: [AKS service principal](#) and [AKS update credentials](#).

## Can I scale my AKS cluster to zero?

You can completely [stop a running AKS cluster](#), saving on the respective compute costs. Additionally, you may also choose to [scale or autoscale all or specific User node pools](#) to 0, maintaining only the necessary cluster configuration. You can't directly scale [system node pools](#) to zero.

## Can I use the virtual machine scale set APIs to scale manually?

No, scale operations by using the virtual machine scale set APIs aren't supported. Use the AKS APIs (`az aks scale`).

## Can I use virtual machine scale sets to manually scale to zero nodes?

No, scale operations by using the virtual machine scale set APIs aren't supported. You can use the AKS API to scale to zero non-system node pools or [stop your cluster](#) instead.

## Can I stop or de-allocate all my VMs?

While AKS has resilience mechanisms to withstand such a config and recover from it, this isn't a supported configuration. [Stop your cluster](#) instead.

## Can I use custom VM extensions?

No, AKS is a managed service, and manipulation of the IaaS resources isn't supported. To install custom components, use the Kubernetes APIs and mechanisms. For example, use DaemonSets to install required components.

## Does AKS store any customer data outside of the cluster's region?

No, all data is stored in the cluster's region.

## Are AKS images required to run as root?

The following images have functional requirements to "Run as Root" and exceptions must be filed for any policies:

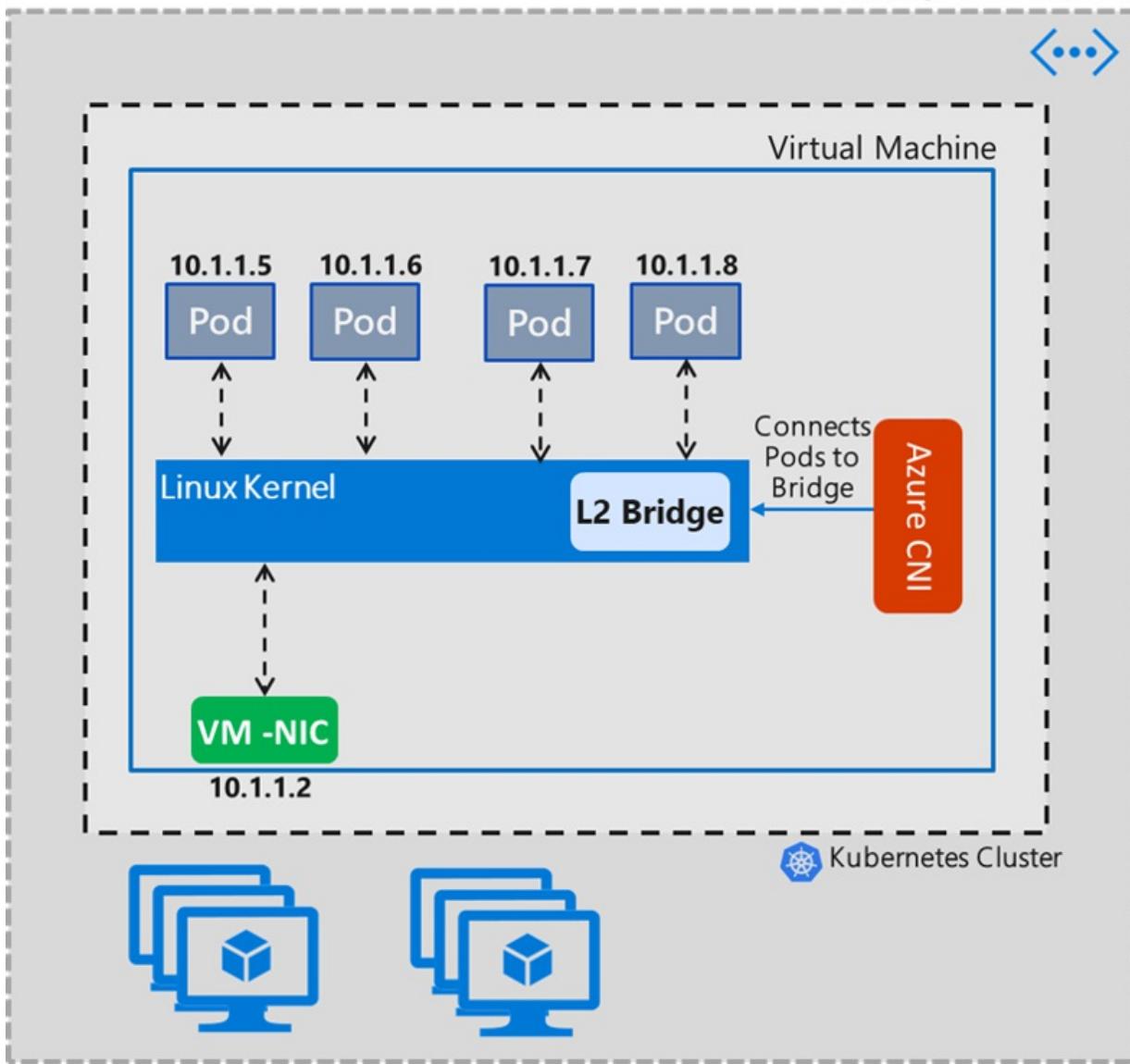
- [mcr.microsoft.com/oss/kubernetes/coredns](https://mcr.microsoft.com/oss/kubernetes/coredns)
- [mcr.microsoft.com/azuremonitor/containerinsights/ciprod](https://mcr.microsoft.com/azuremonitor/containerinsights/ciprod)
- [mcr.microsoft.com/oss/calico/node](https://mcr.microsoft.com/oss/calico/node)
- [mcr.microsoft.com/oss/kubernetes-csi/azuredisk-csi](https://mcr.microsoft.com/oss/kubernetes-csi/azuredisk-csi)

## What is Azure CNI Transparent Mode vs. Bridge Mode?

Starting with version 1.2.0, Azure CNI sets Transparent mode as default for single tenancy Linux CNI deployments. Transparent mode is replacing bridge mode. In this section, we will discuss more about the differences about both modes and what are the benefits/limitation for using Transparent mode in Azure CNI.

### Bridge mode

As the name suggests, bridge mode Azure CNI, in a "just in time" fashion, will create a L2 bridge named "azure0". All the host side pod `veth` pair interfaces will be connected to this bridge. So Pod-Pod intra VM communication and the remaining traffic goes through this bridge. The bridge in question is a layer 2 virtual device that on its own cannot receive or transmit anything unless you bind one or more real devices to it. For this reason, eth0 of the Linux VM has to be converted into a subordinate to "azure0" bridge. This creates a complex network topology within the Linux VM and as a symptom CNI had to take care of other networking functions like DNS server update and so on.

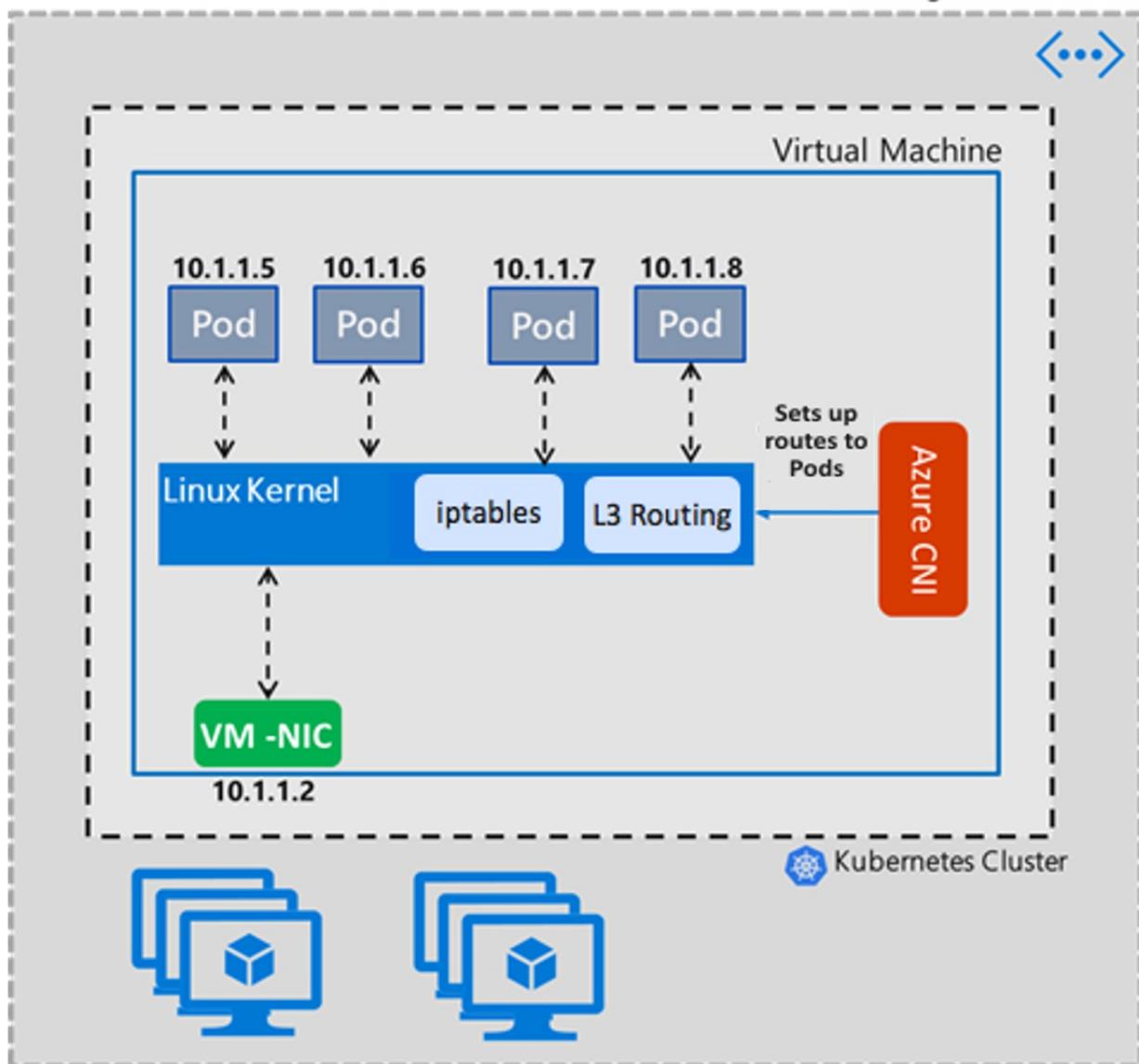


Below is an example of how the ip route setup looks like in Bridge mode. Regardless of how many pods the node has, there will only ever be two routes. The first one saying, all traffic excluding local on azure0 will go to the default gateway of the subnet through the interface with ip "src 10.240.0.4" (which is Node primary IP) and the second one saying "10.20.x.x" Pod space to kernel for kernel to decide.

```
default via 10.240.0.1 dev azure0 proto dhcp src 10.240.0.4 metric 100
10.240.0.0/12 dev azure0 proto kernel scope link src 10.240.0.4
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown
root@k8s-agentpool1-20465682-1:/#
```

### Transparent mode

Transparent mode takes a straight forward approach to setting up Linux networking. In this mode, Azure CNI won't change any properties of eth0 interface in the Linux VM. This minimal approach of changing the Linux networking properties helps reduce complex corner case issues that clusters could face with Bridge mode. In Transparent Mode, Azure CNI will create and add host-side pod `veth` pair interfaces that will be added to the host network. Intra VM Pod-to-Pod communication is through ip routes that the CNI will add. Essentially Pod-to-Pod communication is over layer 3 and pod traffic is routed by L3 routing rules.



Below is an example ip route setup of transparent mode, each Pod's interface will get a static route attached so that traffic with dest IP as the Pod will be sent directly to the Pod's host side `veth` pair interface.

```

10.240.0.216 dev azv79d05038592 proto static
10.240.0.218 dev azv8184320e2bf proto static
10.240.0.219 dev azvc0339d223b9 proto static
10.240.0.222 dev azv722a6b28449 proto static
10.240.0.223 dev azve7f326f1507 proto static
10.240.0.224 dev azvb3bfcdd75a proto static
168.63.129.16 via 10.240.0.1 dev eth0 proto dhcp src 10.240.0.4 metric 100
169.254.169.254 via 10.240.0.1 dev eth0 proto dhcp src 10.240.0.4 metric 100
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1 linkdown

```

### Benefits of transparent mode

- Provides mitigation for `conntrack` DNS parallel race condition and avoidance of 5-sec DNS latency issues without the need to set up node local DNS (you may still use node local DNS for performance reasons).
- Eliminates the initial 5-sec DNS latency CNI bridge mode introduces today due to "just in time" bridge setup.
- One of the corner cases in bridge mode is that the Azure CNI can't keep updating the custom DNS server lists users add to either VNET or NIC. This results in the CNI picking up only the first instance of the DNS server list. Solved in Transparent mode as CNI doesn't change any eth0 properties. See more [here](#).
- Provides better handling of UDP traffic and mitigation for UDP flood storm when ARP times out. In bridge mode, when bridge doesn't know a MAC address of destination pod in intra-VM Pod-to-Pod communication,

by design, this results in storm of the packet to all ports. Solved in Transparent mode as there are no L2 devices in path. See more [here](#).

- Transparent mode performs better in Intra VM Pod-to-Pod communication in terms of throughput and latency when compared to bridge mode.

## How to avoid permission ownership setting slow issues when the volume has a lot of files?

Traditionally if your pod is running as a non-root user (which you should), you must specify a `fsGroup` inside the pod's security context so that the volume can be readable and writable by the Pod. This requirement is covered in more detail in [here](#).

But one side-effect of setting `fsGroup` is that, each time a volume is mounted, Kubernetes must recursively `chown()` and `chmod()` all the files and directories inside the volume - with a few exceptions noted below. This happens even if group ownership of the volume already matches the requested `fsGroup`, and can be expensive for larger volumes with lots of small files, which causes pod startup to take a long time. This scenario has been a known problem before v1.20, and the workaround is setting the Pod run as root:

```
apiVersion: v1
kind: Pod
metadata:
 name: security-context-demo
spec:
 securityContext:
 runAsUser: 0
 fsGroup: 0
```

The issue has been resolved with Kubernetes version 1.20. For more information, see [Kubernetes 1.20: Granular Control of Volume Permission Changes](#).

## Can I use FIPS cryptographic libraries with deployments on AKS?

FIPS-enabled nodes are currently supported on Linux-based node pools. For more information, see [Add a FIPS-enabled node pool](#).

## Can I configure NSGs with AKS?

AKS doesn't apply Network Security Groups (NSGs) to its subnet and doesn't modify any of the NSGs associated with that subnet. AKS only modifies the network interfaces NSGs settings. If you're using CNI, you also must ensure the security rules in the NSGs allow traffic between the node and pod CIDR ranges. If you're using kubenet, you must also ensure the security rules in the NSGs allow traffic between the node and pod CIDR. For more information, see [Network security groups](#).

## How does Time synchronization work in AKS?

AKS nodes run the "chrony" service which pulls time from the localhost. Containers running on pods get the time from the AKS nodes. Applications launched inside a container use time from the container of the pod.

# Support and troubleshooting for Azure Kubernetes Service (AKS)

10/27/2022 • 2 minutes to read • [Edit Online](#)

Here are suggestions for where you can get help when developing your Azure Kubernetes Service (AKS) solutions.

## Self help troubleshooting



Various articles explain how to determine, diagnose, and fix issues that you might encounter when using Azure Kubernetes Service. Use these articles to troubleshoot deployment failures, security-related problems, connection issues and more.

For a full list of self help troubleshooting content, see [Azure Kubernetes Service troubleshooting documentation](#)

## Post a question on Microsoft Q&A



For quick and reliable answers on your technical product questions from Microsoft Engineers, Azure Most Valuable Professionals (MVPs), or our expert community, engage with us on [Microsoft Q&A](#), Azure's preferred destination for community support.

If you can't find an answer to your problem using search, submit a new question to Microsoft Q&A. Use one of the following tags when asking your question:

AREA	TAG
Azure Kubernetes Service	azure-kubernetes-service
Azure Container Registry	azure-container-registry
Azure storage accounts	azure-storage-accounts
Azure Managed Identities	azure-managed-identity
Azure RBAC	azure-rbac
Azure Active Directory	azure-active-directory
Azure Policy	azure-policy

AREA	TAG
Azure Virtual Machine Scale Sets	virtual-machine-scale-sets
Azure Virtual Network	azure-virtual-network
Azure Application Gateway	azure-application-gateway
Azure Virtual Machines	azure-virtual-machines

## Create an Azure support request



Explore the range of [Azure support options and choose the plan](#) that best fits, whether you're a developer just starting your cloud journey or a large organization deploying business-critical, strategic applications. Azure customers can create and manage support requests in the Azure portal.

- If you already have an Azure Support Plan, [open a support request here](#).
- To sign up for a new Azure Support Plan, [compare support plans](#) and select the plan that works for you.

## Create a GitHub issue



If you need help with the language and tools used to develop and manage Azure Kubernetes Service, open an issue in its repository on GitHub.

LIBRARY	GITHUB ISSUES URL
Azure PowerShell	<a href="https://github.com/Azure/azure-powershell/issues">https://github.com/Azure/azure-powershell/issues</a>
Azure CLI	<a href="https://github.com/Azure/azure-cli/issues">https://github.com/Azure/azure-cli/issues</a>
Azure REST API	<a href="https://github.com/Azure/azure-rest-api-specs/issues">https://github.com/Azure/azure-rest-api-specs/issues</a>
Azure SDK for Java	<a href="https://github.com/Azure/azure-sdk-for-java/issues">https://github.com/Azure/azure-sdk-for-java/issues</a>
Azure SDK for Python	<a href="https://github.com/Azure/azure-sdk-for-python/issues">https://github.com/Azure/azure-sdk-for-python/issues</a>
Azure SDK for .NET	<a href="https://github.com/Azure/azure-sdk-for-net/issues">https://github.com/Azure/azure-sdk-for-net/issues</a>
Azure SDK for JavaScript	<a href="https://github.com/Azure/azure-sdk-for-js/issues">https://github.com/Azure/azure-sdk-for-js/issues</a>
Terraform	<a href="https://github.com/Azure/terraform/issues">https://github.com/Azure/terraform/issues</a>

## Stay informed of updates and new releases



Learn about important product updates, roadmap, and announcements in [Azure Updates](#).

News and information about Azure Virtual Machines is shared at the [Azure blog](#).

## Next steps

Learn more about [Azure Kubernetes Service](#)