

Secure AKS control plane

Public
Private
VNET Integration

Houssem Dellai

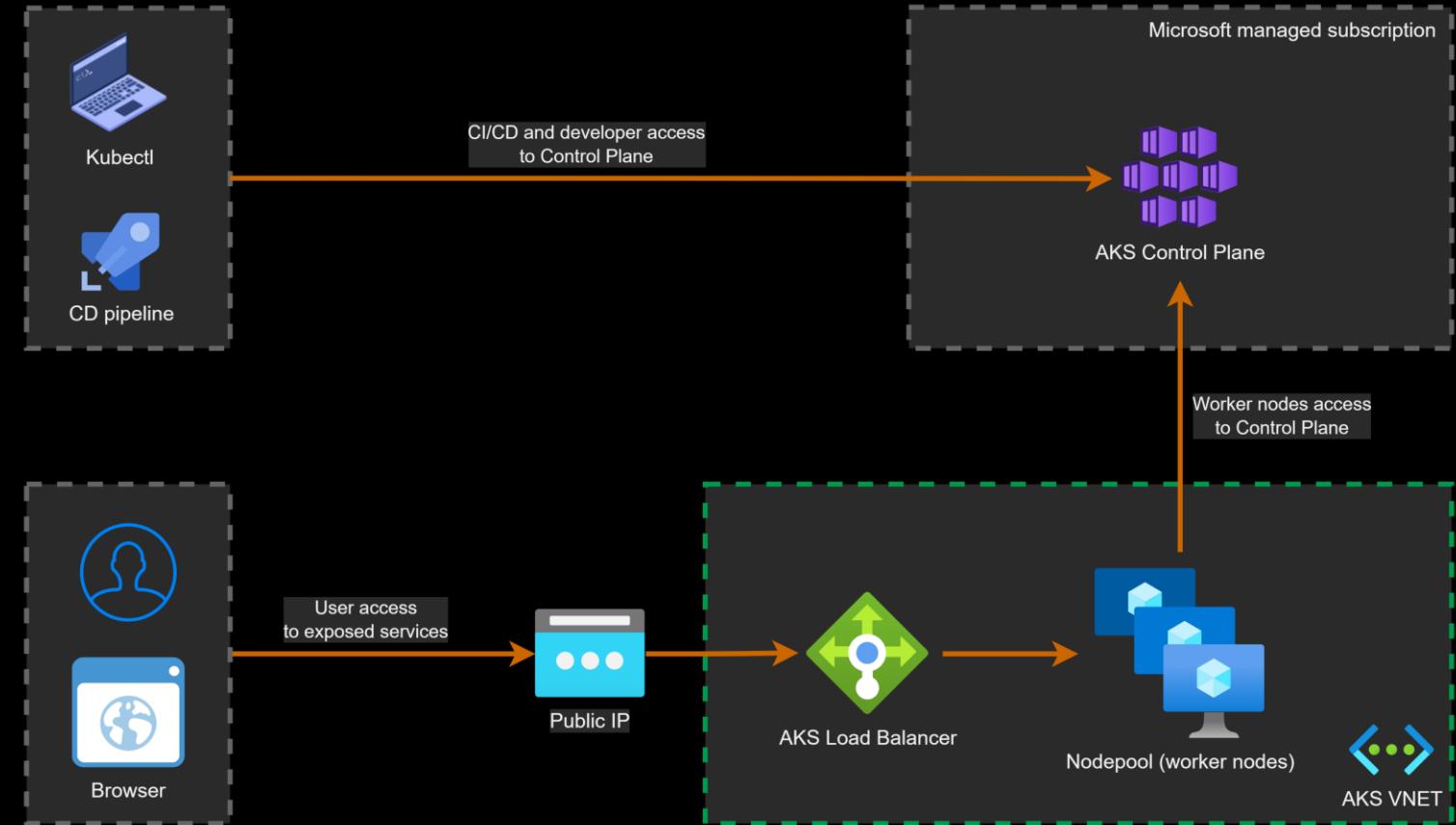


Access to AKS Control Plane and to exposed services

User access to exposed services in the cluster

Developer/DevOps/Ops and DevOps pipelines access to AKS Control Plane to deploy and configure apps

Worker Nodes (Nodepool) access to Control Plane (API Server)



AKS control plane access options



Public cluster (public FQDN and public IP for Control Plane)



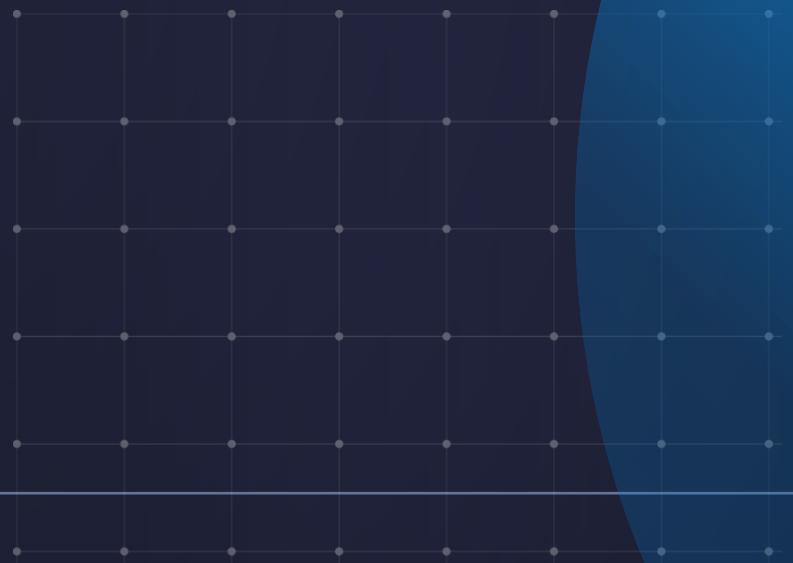
Private cluster using Private Endpoint (private IP for Control Plane)



Public cluster using VNET Integration



Private cluster using VNET Integration

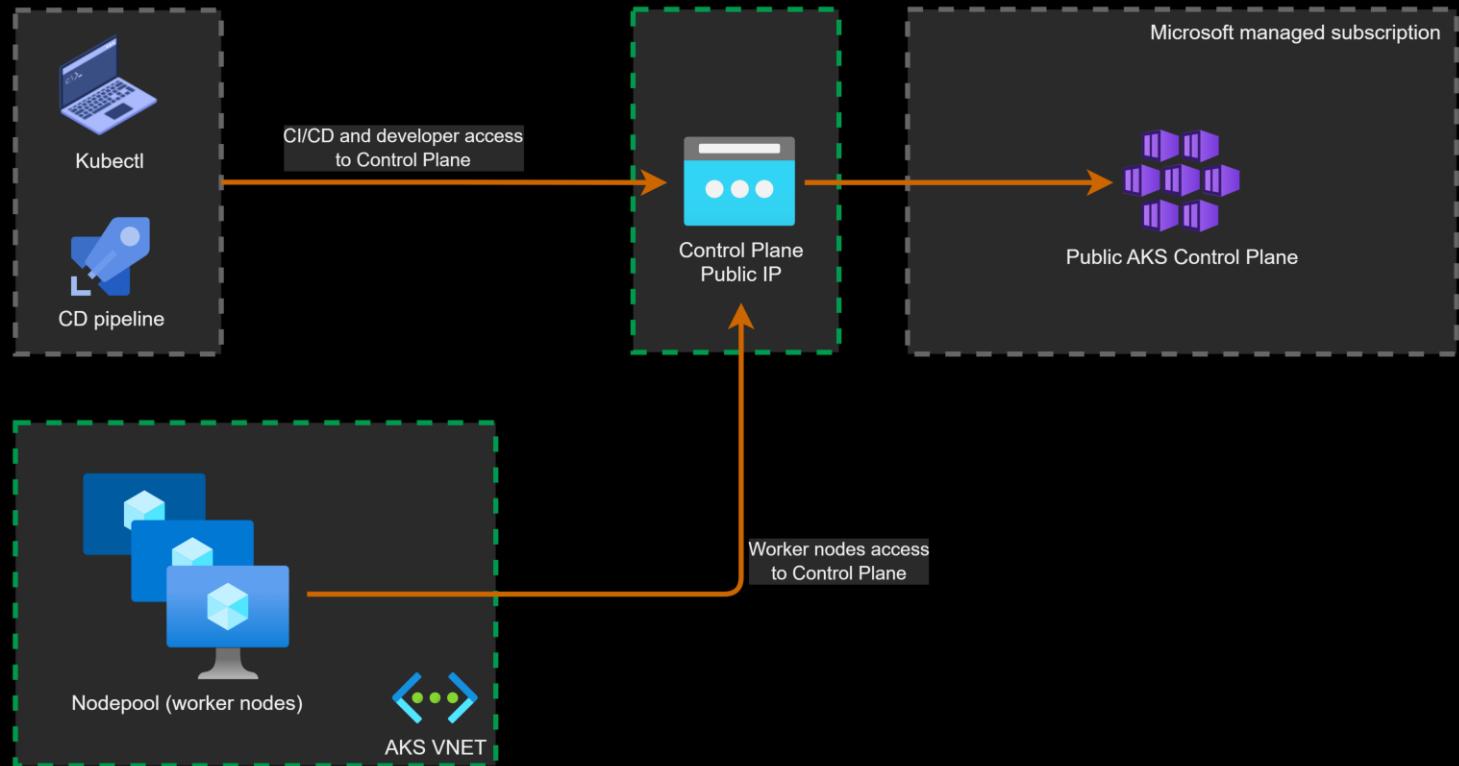


Public AKS cluster access

Control Plane is exposed on public FQDN and public IP address.

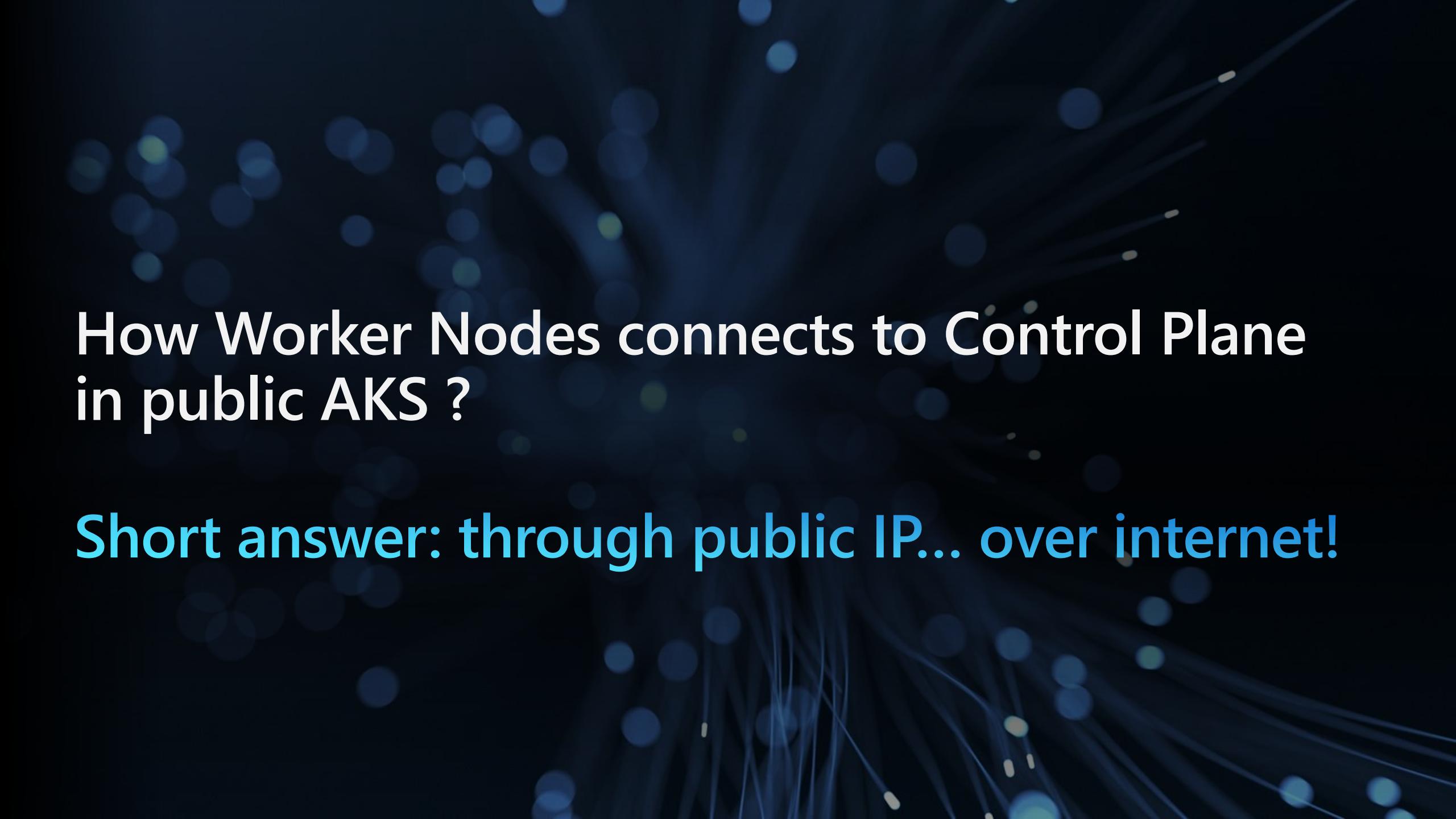
Control Plane endpoint is exposed to the internet.

Authorized IP ranges: whitelist IPs to access Control Plane.



Create public AKS cluster

```
$  
$ az group create -n rg-aks-public -l westeurope #^C  
$ az aks create -n aks-cluster -g rg-aks-public #^C  
$  
$ az aks show -n aks-cluster -g rg-aks-public --query fqdn  
The behavior of this command has been altered by the following extension: aks-preview  
"aks-cluste-rg-aks-public-17b128-587be53f.hcp.westeurope.azmk8s.io"  
$  
$ nslookup aks-cluste-rg-aks-public-17b128-587be53f.hcp.westeurope.azmk8s.io  
Server: bbox.lan  
Address: 2001:861:5e62:69c0:861e:a3ff:fea2:796c  
  
Non-authoritative answer:  
Name: aks-cluste-rg-aks-public-17b128-587be53f.hcp.westeurope.azmk8s.io  
Address: 20.103.218.175  
  
$ az aks show -n aks-cluster -g rg-aks-public --query privateFqdn  
The behavior of this command has been altered by the following extension: aks-preview  
$
```



How Worker Nodes connects to Control Plane
in public AKS ?

Short answer: through public IP... over internet!

In public cluster,
Worker Nodes
connects to Control
Plane through public
IP.

```
$  
$ kubectl get svc  
NAME          TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)  
kubernetes   ClusterIP  10.0.0.1        <none>          443/TCP  
$  
$ kubectl describe svc kubernetes  
Name:           kubernetes  
Namespace:      default  
Labels:         component=apiserver  
                provider=kubernetes  
Annotations:  
Selector:       <none>  
Type:           ClusterIP  
IP Family Policy: SingleStack  
IP Families:    IPv4  
IP:             10.0.0.1  
IPs:            10.0.0.1  
Port:           https  443/TCP  
TargetPort:     443/TCP  
Endpoints:      20.103.218.175:443  
Session Affinity: None  
Events:  
$  
$  
$ kubectl get endpoints  
NAME          ENDPOINTS      AGE  
kubernetes   20.103.218.175:443  114m  
$
```

Public AKS cluster resources

MC_rg-aks-public_aks-cluster_westeurope   

 MC_rg-aks-public_aks-cluster_westeurope Resource group

Search   Create  Manage view  Delete resource group  Refresh  Export to CSV  Open query

 Overview  Activity log  Access control (IAM)  Tags  Resource visualizer  Events

 Settings  Deployments  Security

| <input type="checkbox"/> | Name ↑↓ | Type ↑↓ | Location ↑↓ |
|--------------------------|--------------------------------------|---------------------------|-------------|
| <input type="checkbox"/> | 8ae47ad6-184d-4390-bae3-1bc8b1faee28 | Public IP address | West Europe |
| <input type="checkbox"/> | aks-agentpool-32818330-nsg | Network security group | West Europe |
| <input type="checkbox"/> | aks-agentpool-32818330-routetable | Route table | West Europe |
| <input type="checkbox"/> | aks-cluster-agentpool | Managed Identity | West Europe |
| <input type="checkbox"/> | aks-nodepool1-25482467-vmss | Virtual machine scale set | West Europe |
| <input type="checkbox"/> | aks-vnet-32818330 | Virtual network | West Europe |
| <input type="checkbox"/> | kubernetes | Load balancer | West Europe |

Private AKS cluster access

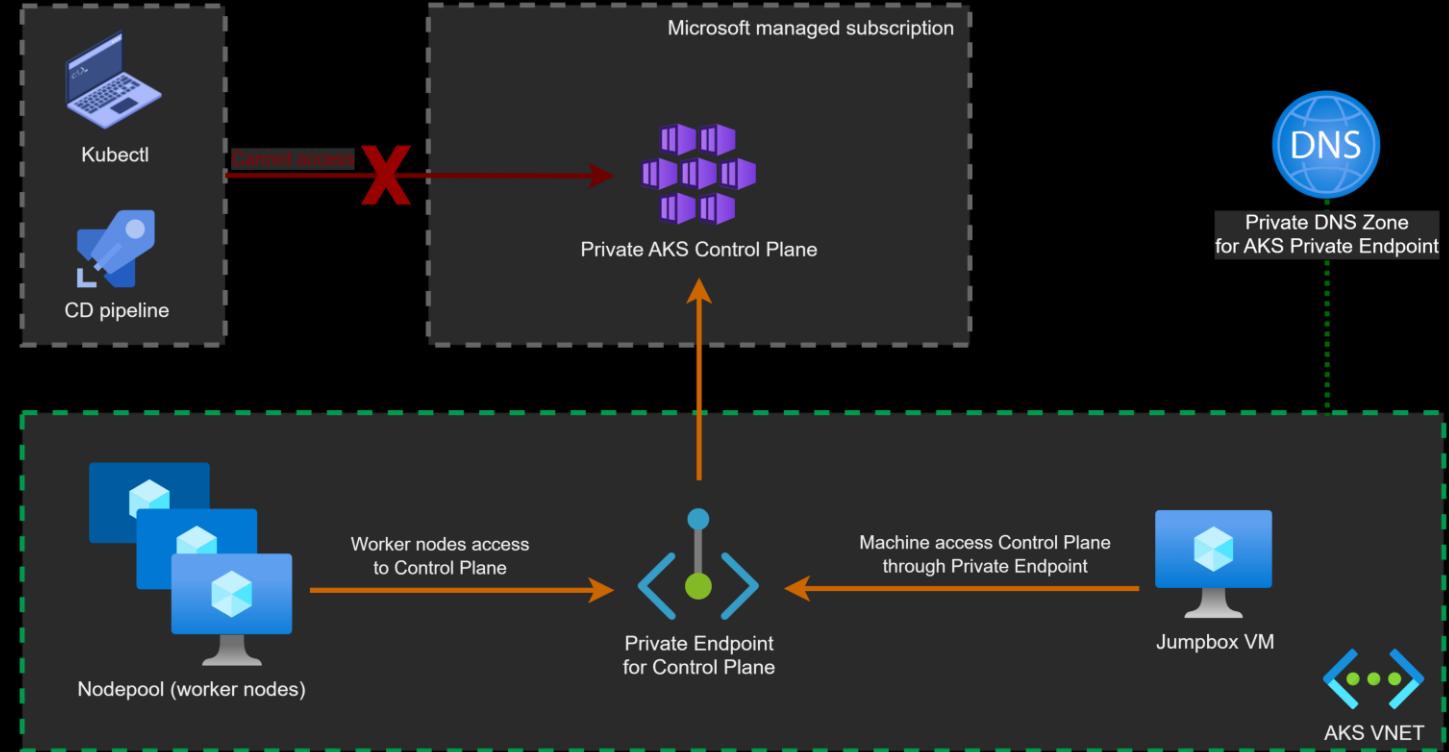
Control Plane is exposed on public FQDN but with private IP address.

Control Plane endpoint is NOT exposed to the internet.

Public FQDN could be disabled or enabled.

Worker Nodes connects to Control Plane through Private Endpoint.

Private FQDN is resolvable only through Private DNS Zone.



Creating private AKS cluster

```
$  
$ az group create -n rg-aks-private -l westeurope #^C  
$ az aks create -n aks-cluster -g rg-aks-private --enable-private-cluster #^C  
$  
$ az aks show -n aks-cluster -g rg-aks-private --query fqdn  
The behavior of this command has been altered by the following extension: aks-preview  
"aks-cluste-rg-aks-private-17b128-32f70f3f.hcp.westeurope.azmk8s.io"  
$  
$ nslookup aks-cluste-rg-aks-private-17b128-32f70f3f.hcp.westeurope.azmk8s.io  
Server: bbox.lan  
Address: 2001:861:5e62:69c0:861e:a3ff:fea2:796c  
  
Non-authoritative answer:  
Name: aks-cluste-rg-aks-private-17b128-32f70f3f.hcp.westeurope.azmk8s.io  
Address: 10.224.0.4  
  
$ az aks show -n aks-cluster -g rg-aks-private --query privateFqdn  
The behavior of this command has been altered by the following extension: aks-preview  
"aks-cluste-rg-aks-private-17b128-6d8d6675.628fd8ef-83fc-49d4-975e-c765c36407d7.privatelink.westeurope.azmk8s.io"  
$  
$ nslookup aks-cluste-rg-aks-private-17b128-6d8d6675.628fd8ef-83fc-49d4-975e-c765c36407d7.privatelink.westeurope.azmk8s.io  
Server: bbox.lan  
Address: 2001:861:5e62:69c0:861e:a3ff:fea2:796c  
  
*** bbox.lan can't find aks-cluste-rg-aks-private-17b128-6d8d6675.628fd8ef-83fc-49d4-975e-c765c36407d7.privatelink.westeurope.azm  
k8s.io: Non-existent domain  
$  
$  
$ az aks update -n aks-cluster -g rg-aks-private --disable-public-fqdn #^C  
$  
$ az aks show -n aks-cluster -g rg-aks-private --query fqdn  
The behavior of this command has been altered by the following extension: aks-preview  
$
```

Private AKS cluster resources

Adds Private Endpoint and private DNS Zone.

MC_rg-aks-private_aks-cluster_westeurope ↗ ☆ ... X

Resource group

Search

+ Create ⚙️ Manage view Delete resource group ⟳ Refresh ⬇️ Export to CSV 🔗 Open query ...

| ▢ | Name ↑↓ | Type ↑↓ | Location ↑↓ |
|--|---|---------------------------|-------------|
| <input checked="" type="checkbox"/> | DNS 628fd8ef-83fc-49d4-975e-c765c36407d7.privatelink.westeurope... | Private DNS zone | Global |
| <input type="checkbox"/> | 🌐 814943a9-32a5-453c-9b0d-e75f1c4ccc1b | Public IP address | West Europe |
| <input type="checkbox"/> | 🛡️ aks-agentpool-42463278-nsg | Network security group | West Europe |
| <input type="checkbox"/> | 👤 aks-agentpool-42463278-routetable | Route table | West Europe |
| <input type="checkbox"/> | 🔑 aks-cluster-agentpool | Managed Identity | West Europe |
| <input type="checkbox"/> | _VMSS aks-nodepool1-26304092-vmss | Virtual machine scale set | West Europe |
| <input type="checkbox"/> | VN aks-vnet-42463278 | Virtual network | West Europe |
| <input checked="" type="checkbox"/> | ⬇️ kube-apiserver | Private endpoint | West Europe |
| <input checked="" type="checkbox"/> | NIC kube-apiserver.nic.034f2df2-f105-48cc-b3e3-761fdde3d4f3 | Network Interface | West Europe |
| <input type="checkbox"/> | 📍 kubernetes | Load balancer | West Europe |

Private DNS Zone for private cluster

Control Plane (API Server) is projected into the AKS Subnet through Private Endpoint.

Dashboard > Resource groups > MC_rg-aks-private_aks-cluster_westeurope >

 628fd8ef-83fc-49d4-975e-c765c36407d7.privatelink.westeurope.azmk8s.io ⚡ ☆ ...

Private DNS zone

Search

 Record set  Move  Delete zone  Refresh

 Overview 

 Essentials

You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

| Name | Type | TTL | Value | Auto registered | ... |
|---|------|------|---|-----------------|-----|
| @ | SOA | 3600 | Email: azureprivatedns-hos... Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1 | False | ... |
| aks-cluste-rg-aks-private-17b128-6d8d6675 | A | 300 | 10.224.0.4 | False | ... |

 Monitoring

Public AKS cluster with VNET Integration access

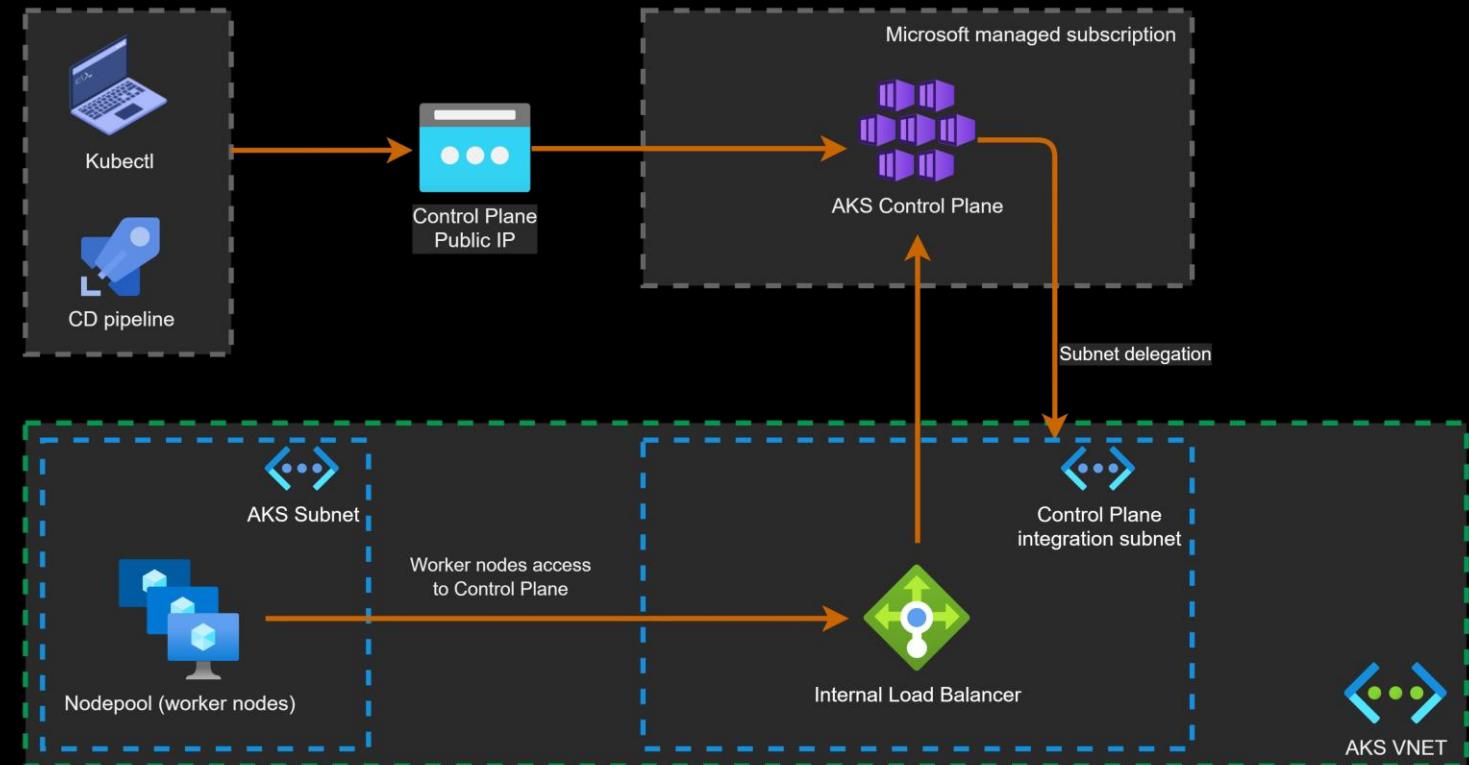
Control Plane is exposed on public FQDN with public IP address.

Control Plane endpoint is exposed to the internet.

Public FQDN could NOT be disabled except on private cluster.

DevOps CD pipelines could access through public or private IP.

Worker Nodes access Control Plane through internal Load Balancer (private IP).



Creating public AKS cluster with VNET Integration

```
$  
$ az group create -n rg-aks-public-vnet-integration -l eastus2 #^C  
$ az aks create -n aks-cluster -g rg-aks-public-vnet-integration --enable-apiserver-vnet-integration #^C  
$  
$ az aks show -n aks-cluster -g rg-aks-public-vnet-integration --query fqdn  
The behavior of this command has been altered by the following extension: aks-preview  
"aks-cluste-rg-aks-public-vn-17b128-2ab6e274.hcp.eastus2.azmk8s.io"  
$  
$ nslookup aks-cluste-rg-aks-public-vn-17b128-2ab6e274.hcp.eastus2.azmk8s.io  
Server: bbox.lan  
Address: 2001:861:5e62:69c0:861e:a3ff:fea2:796c  
  
Non-authoritative answer:  
Name: aks-cluste-rg-aks-public-vn-17b128-2ab6e274.hcp.eastus2.azmk8s.io  
Address: 20.94.16.207  
  
$ az aks show -n aks-cluster -g rg-aks-public-vnet-integration --query privateFqdn  
The behavior of this command has been altered by the following extension: aks-preview  
$  
$
```

How Worker Nodes access Control Plane ?

Through Control Plane private IP, not the public IP.

```
$  
$ az aks get-credentials --resource-group rg-aks-public-vnet-integration --name aks-cluster  
The behavior of this command has been altered by the following extension: aks-preview  
Merged "aks-cluster" as current context in C:\Users\hodellai\.kube\config  
$  
$ kubectl get svc  
NAME      TYPE      CLUSTER-IP      EXTERNAL-IP      PORT(S)      AGE  
kubernetes   ClusterIP   10.0.0.1        <none>           443/TCP    178m  
$  
$ kubectl describe svc kubernetes  
Name:            kubernetes  
Namespace:       default  
Labels:          component=apiserver,  
                 provider=kubernetes  
Annotations:     <none>  
Selector:        <none>  
Type:            ClusterIP  
IP Family Policy: SingleStack  
IP Families:    IPv4  
IP:              10.0.0.1  
IPs:             10.0.0.1  
Port:            https 443/TCP  
TargetPort:      443/TCP  
Endpoints:       10.226.0.4:443  
Session Affinity: None  
Events:  
$
```

Public AKS with VNET Integration resources

MC_rg-aks-public-vnet-integration_aks-cluster_eastus2

Resource group

Search

Create Manage view Delete resource group Refresh Export to CSV Open query

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

| Name ↑↓ | Type ↑↓ | Location ↑↓ | ... |
|--------------------------------------|---------------------------|-------------|-----|
| aks-agentpool-24148516-nsg | Network security group | East US 2 | ... |
| aks-agentpool-24148516-routetable | Route table | East US 2 | ... |
| aks-cluster-agentpool | Managed Identity | East US 2 | ... |
| aks-nodepool1-19806001-vmss | Virtual machine scale set | East US 2 | ... |
| aks-vnet-24148516 | Virtual network | East US 2 | ... |
| cb68c42a-d176-4116-9a39-8ef58b209f68 | Public IP address | East US 2 | ... |
| kube-apiserver | Load balancer | East US 2 | ... |
| kubernetes | Load balancer | East US 2 | ... |

Public cluster and VNET Integration changes

Dashboard > Resource groups > MC_rg-aks-public-vnet-integration_aks-cluster_eastus2 > kube-apiserver

kube-apiserver | Frontend IP configuration

Load balancer

Search

+ Add Refresh Give feedback

Filter by name...

| Name ↑↓ | IP address ↑↓ |
|-------------------------|---------------|
| kube-apiserver-frontend | 10.226.0.4 |

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

AKS VNET Integration creates new Subnet in AKS VNET.

It injects the ILB and configure delegation.

AKS VNET Integration creates internal Load Balancer.

ILB private IP address is used to access the Control Plane.

Dashboard > Resource groups > MC_rg-aks-public-vnet-integration_aks-cluster_eastus2 > aks-vnet-24148516

aks-vnet-24148516 | Subnets

Virtual network

Search

+ Subnet + Gateway subnet Refresh Manage users Delete

Search subnets

| Name ↑↓ | IPv4 ↑↓ | Delegated to ↑↓ |
|----------------------|---------------|---|
| aks-subnet | 10.224.0.0/16 | - m - |
| aks-apiserver-subnet | 10.226.0.0/28 | - 1. Microsoft.ContainerService/managedClusters |

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Settings

Address space Connected devices Subnets

Private AKS cluster with VNET Integration access

Control Plane is exposed only on Private IP on internal Load Balancer.

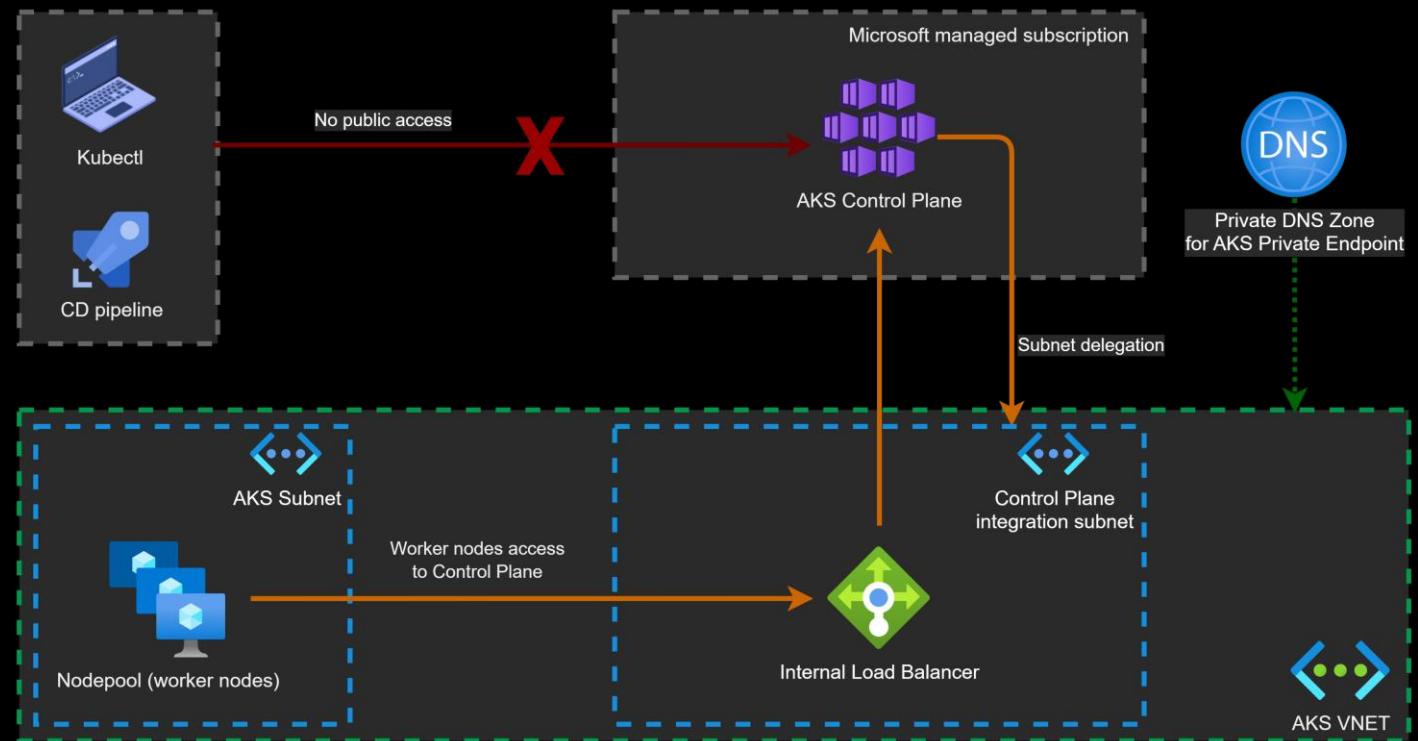
Control Plane have public FQDN exposed to the internet.

Public FQDN references a private IP, could be disabled.

DevOps CD pipelines could only access through private IP (internal LB).

Nodes access Control Plane through internal Load Balancer (private IP).

No Private Endpoint created although the cluster is private.



Create private AKS cluster with VNET Integration

```
$  
$ az group create -n rg-aks-private-vnet-integration -l eastus2 #^C  
$ az aks create -n aks-cluster -g rg-aks-private-vnet-integration --enable-apiserver-vnet-integration --enable-private-cluster #^C  
$  
$ az aks show -n aks-cluster -g rg-aks-private-vnet-integration --query fqdn  
The behavior of this command has been altered by the following extension: aks-preview  
"aks-cluste-rg-aks-private-v-17b128-4948be0c.hcp.eastus2.azurek8s.io"  
$  
$ nslookup aks-cluste-rg-aks-private-v-17b128-4948be0c.hcp.eastus2.azurek8s.io  
Server: bbox.lan  
Address: 2001:861:5e62:69c0:861e:a3ff:fea2:796c  
  
Non-authoritative answer:  
Name: aks-cluste-rg-aks-private-v-17b128-4948be0c.hcp.eastus2.azurek8s.io  
Address: 10.226.0.4  
  
$ az aks show -n aks-cluster -g rg-aks-private-vnet-integration --query privateFqdn  
The behavior of this command has been altered by the following extension: aks-preview  
"aks-cluste-rg-aks-private-v-17b128-38360d0d.2788811a-873a-450d-811f-b7c7cf918694.private.eastus2.azurek8s.io"  
$  
$ nslookup aks-cluste-rg-aks-private-v-17b128-38360d0d.2788811a-873a-450d-811f-b7c7cf918694.private.eastus2.azurek8s.io  
Server: bbox.lan  
Address: 2001:861:5e62:69c0:861e:a3ff:fea2:796c  
  
*** bbox.lan can't find aks-cluste-rg-aks-private-v-17b128-38360d0d.2788811a-873a-450d-811f-b7c7cf918694.private.eastus2.azurek8s.io: Non-existent domain  
$
```

Private cluster with VNET Integration

Adds internal Load Balancer and private DNS Zone.



MC_rg-aks-private-vnet-integration_aks-cluster_eastus2

Resource group



Search



+ Create



Manage view



Delete resource group



Refresh



Export to CSV



Open query

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

| Name ↑↓ | Type ↑↓ | Location ↑↓ |
|--|---------------------------|-------------|
| <input checked="" type="checkbox"/> 2788811a-873a-450d-811f-b7c7cf918694.private.eastus2.azmk8s.io | Private DNS zone | Global |
| <input type="checkbox"/> aks-agentpool-32355157-nsg | Network security group | East US 2 |
| <input type="checkbox"/> aks-agentpool-32355157-routetable | Route table | East US 2 |
| <input type="checkbox"/> aks-cluster-agentpool | Managed Identity | East US 2 |
| <input type="checkbox"/> aks-nodepool1-16418076-vmss | Virtual machine scale set | East US 2 |
| <input type="checkbox"/> aks-vnet-32355157 | Virtual network | East US 2 |
| <input type="checkbox"/> c0bfc51d-1754-4391-b34b-deea123f28e5 | Public IP address | East US 2 |
| <input checked="" type="checkbox"/> kube-apiserver | Load balancer | East US 2 |
| <input type="checkbox"/> kubernetes | Load balancer | East US 2 |

Private cluster and VNET Integration changes

Private DNS Zone point to the private IP of Control Plane.

The screenshot shows the Azure portal interface for managing a Private DNS zone. The URL in the address bar is: Dashboard > Resource groups > MC_rg-aks-private-vnet-integration_aks-cluster_eastus2 > 2788811a-873a-450d-811f-b7c7cf918694.private.eastus2.azmk8s.io

The main content area displays the zone name **2788811a-873a-450d-811f-b7c7cf918694.private.eastus2.azmk8s.io**. Below it are navigation buttons: **Record set**, **Move**, **Delete zone**, and **Refresh**.

The left sidebar contains the following navigation items:

- Overview (selected)
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings section includes:

- Virtual network links
- Properties
- Locks

Monitoring section is also present.

The **Essentials** section provides a search bar for record sets and a note: "You can search for record sets that have been loaded on this page. If you don't see what you're looking for, to load." It also has a "Search record sets" input field.

A table lists the record sets:

| Name | Type | TTL | Value |
|---|------|------|---|
| @ | SOA | 3600 | Email: azureprivatedns-host.microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1 |
| aks-cluste-rg-aks-private-v-17b128-38360d0d | A | 300 | 10.226.0.4 |

How to access a private cluster



Kubectl command invoke –command “kubectl get pods”



JumpBox VM inside the AKS VNET or peered network



Use an Express Route or VPN connection



Use a private endpoint connection

Recap: private, public and VNET integration for AKS

| | Public FQDN | Private FQDN | Public FQDN could be disactivated | How to access Control Plane |
|------------------------------------|--------------------|--|--|--|
| Public cluster | Yes (public IP) | No | No | Public IP/FQDN for Control Plane |
| Private cluster | Yes (private IP) | Yes (Private Endpoint) | Yes | Private Endpoint + Private DNS Zone |
| VNET Integration + public cluster | Yes (public IP) | Yes (private IP of internal Load Balancer) | No | VNET Integration + Internal Load Balancer |
| VNET Integration + private cluster | Yes (private IP) | Yes (private IP of internal Load Balancer) | Yes | VNET Integration + Internal Load Balancer + Private DNS Zone |

More resources

Create a private Azure Kubernetes Service cluster

<https://learn.microsoft.com/en-us/azure/aks/private-clusters>

Create an Azure Kubernetes Service cluster with API Server VNet Integration (PREVIEW)

<https://learn.microsoft.com/en-us/azure/aks/api-server-vnet-integration>