Deploying and Managing Azure Kubernetes Service (AKS) Networking

Designing and Configuring Networking in AKS

Anthony E. Nocentino
Principal Architect

@nocentino www.nocentino.com

Course Overview

Designing and Configuring Networking in AKS

Accessing Applications Deployed in AKS

Designing and Configuring AKS for Business Continuity

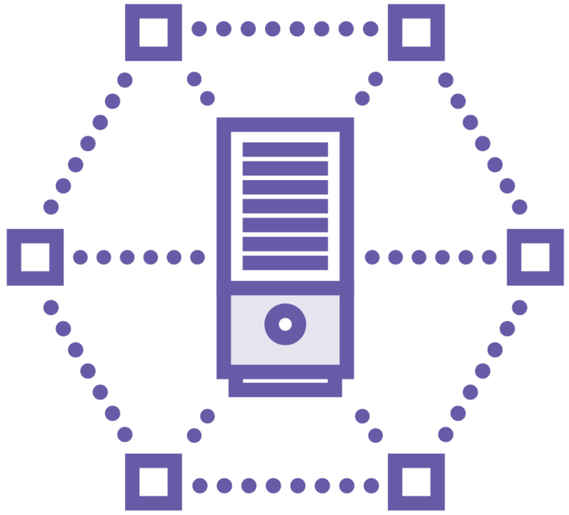
Overview

Understanding AKS networking

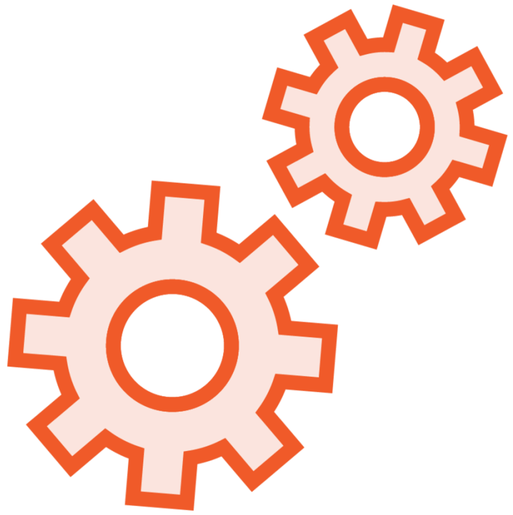
- **kubenet**
- **Azure CNI**

Deploying AKS networking

AKS Networking Overview



Azure Virtual Networks



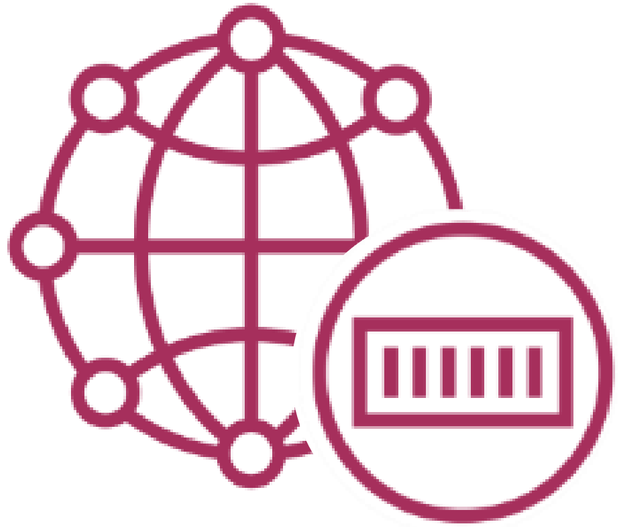
Services

Ingress

Network Policies

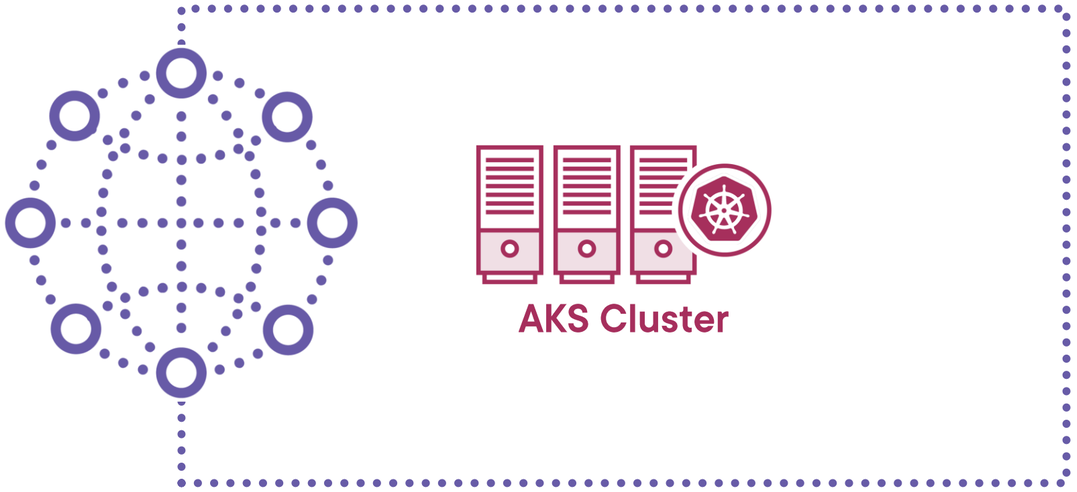
Azure Virtual Networks

kubenet



Azure CNI

Deploying a Cluster Into a Network

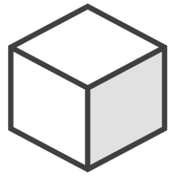


New Virtual Network

Existing Virtual Network

Pod Networking with kubenet

Nodes get IP address from the Azure virtual network subnet



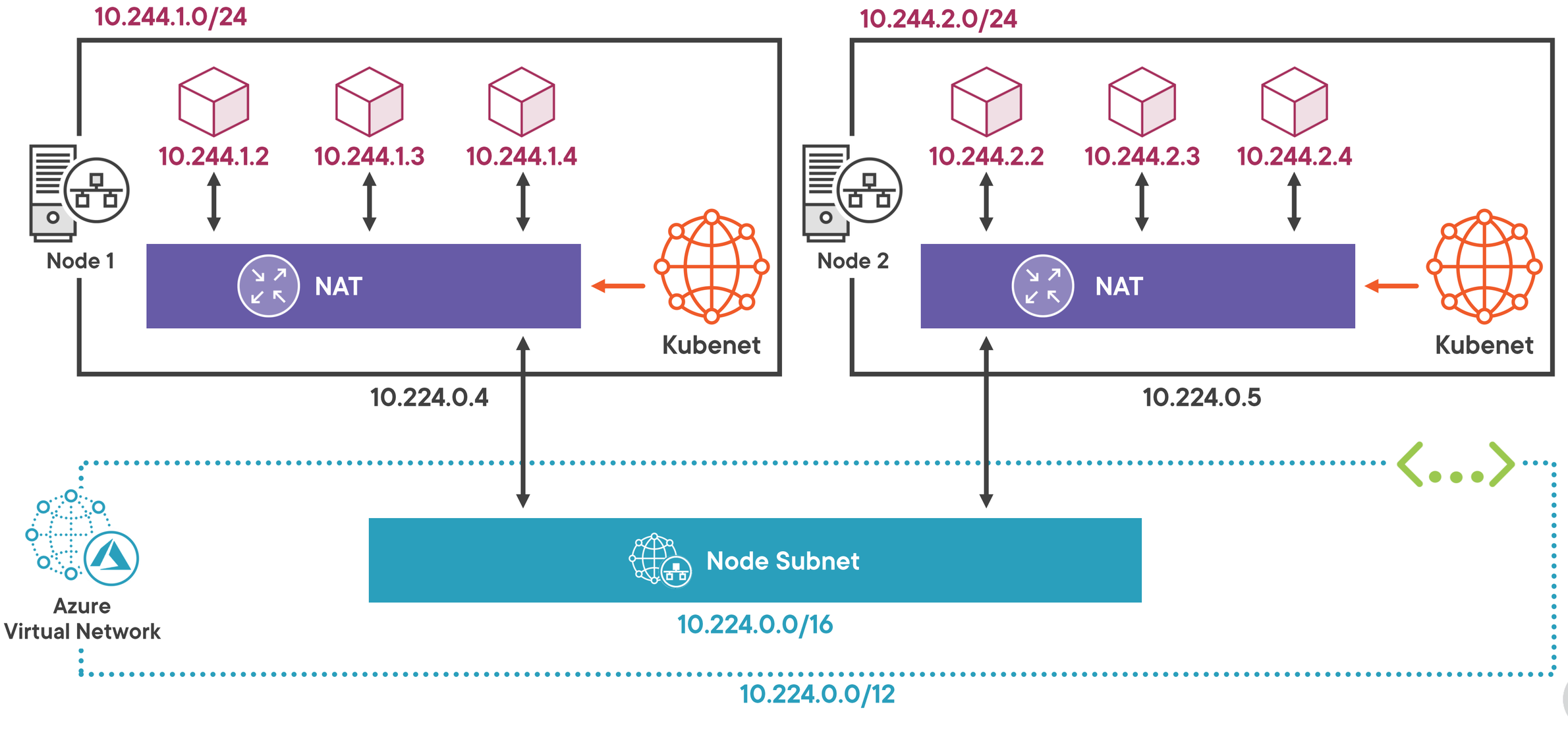
Default of 110 max pods per node but configurable up to 250

Network address translation (NAT) is used so pods can reach resources

Source IP address of traffic is translated to the Node's IP

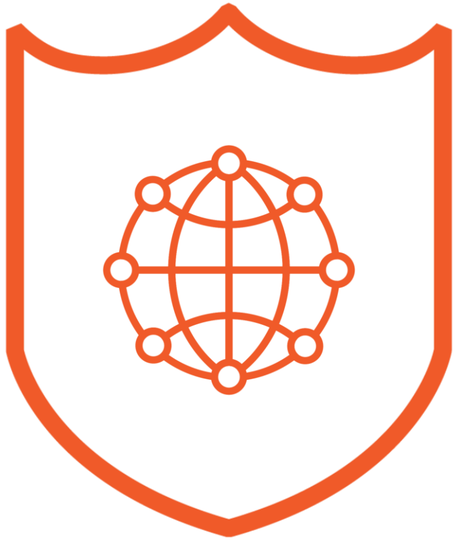
Reduces the number of IP addresses

Azure Virtual Networks - kubenet



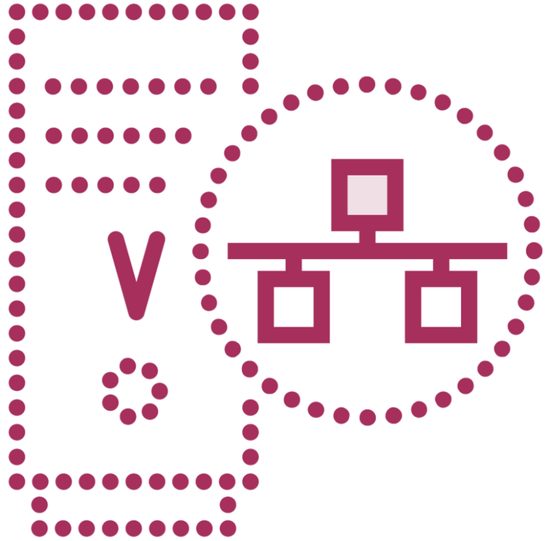
Using kubenet with Advanced Features

Azure Network Policies



Calico Network Policies

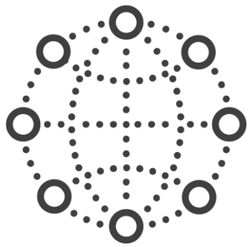
Windows Node Pools



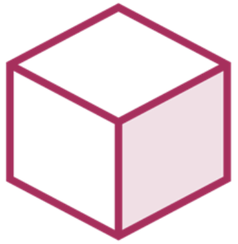
Virtual Node Add-On

Azure CNI

Pods are connected directly to the Virtual Network

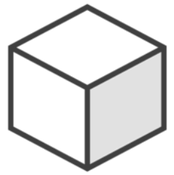


Every pod can be accessed directly

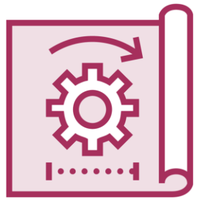


AKS cluster is connected to existing virtual network or created and configured with deployment

Azure CNI



Default to 30 max pods per node



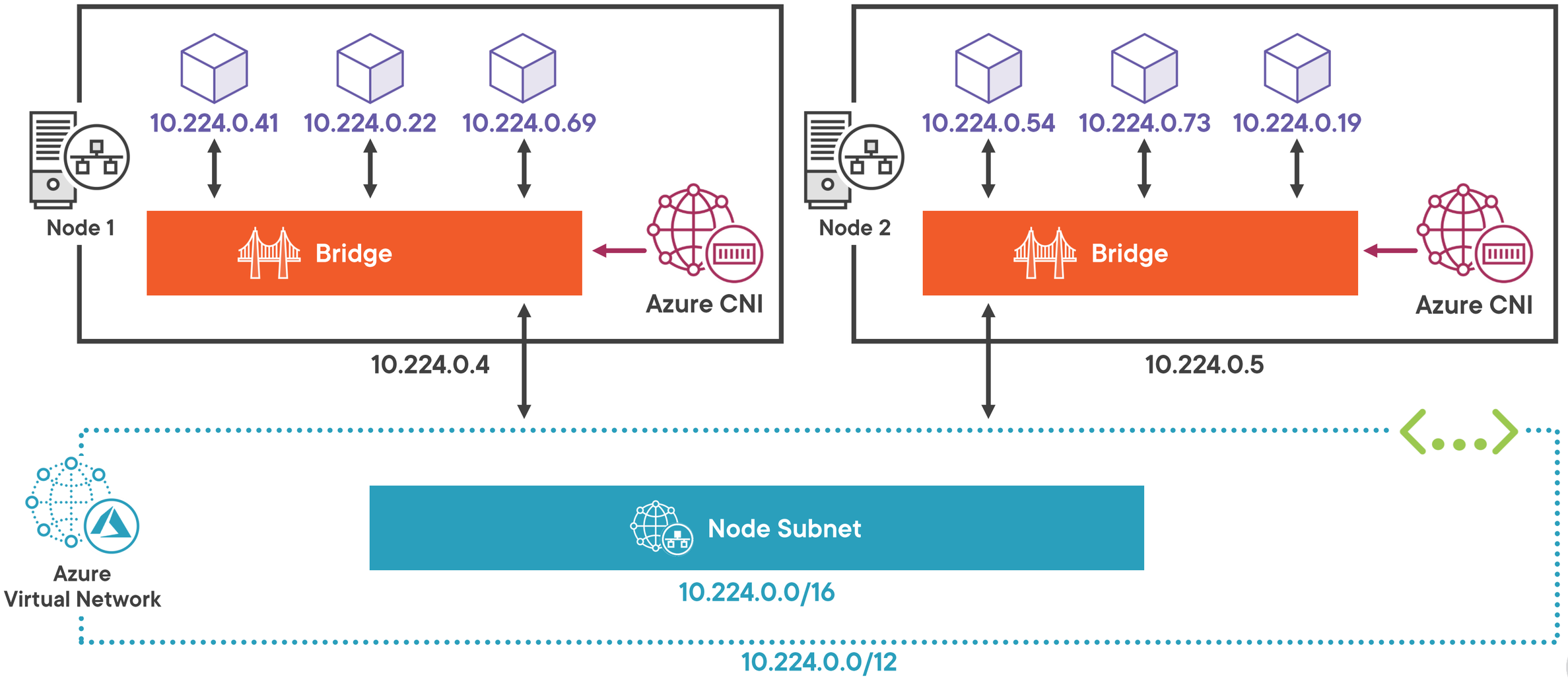
IP addresses must be planned in advance

Prevent IP address exhaustion

Traffic to from Pods on Nodes are not translated (NAT)

https://docs.microsoft.com/en-us/azure/aks/configure-azure-cni#plan-ip-addressing-for-your-cluster

Azure Virtual Networks - Azure CNI



Which To Use When?

Use Kubenet When

- Conserve IP addresses
- Pod communication is within the cluster
- 400 nodes per cluster
- Don’t need advanced AKS features such as virtual nodes, Azure Network Policy or Windows Nodes

Use Azure CNI When

- Pods require direct access to the network
- Pod communication is to resources outside
- Advanced AKS features such as virtual nodes, Azure Network Policy or Windows Nodes are needed

Deploying a Cluster to a New Virtual Network

```
az aks create \
    --resource-group "AKS-Cloud" \
    --generate-ssh-keys \
    --name AKSCluster1
```

Demo

Deploying a cluster to a new Virtual Network using kubenet

Investigate AKS Networking

Creating Networking Manually

Plan your IP addressing

Create Your Virtual Network and Subnet

Choose a security model for your cluster identity

Deploy your cluster into your Virtual Network

Test Networking

Deploying a Cluster to an Existing Virtual Network

```
az network vnet create \
--resource-group "AKS-Cloud-ExistingNetwork" \
--name network-existing \
--address-prefix 10.0.0.0/12 \
--subnet-name subnet-existing \
--subnet-prefix 10.1.0.0/16
```

```
az aks create \
--resource-group "AKS-Cloud-ExistingNetwork" \
--name ExistingNetwork \
--network-plugin azure \
--vnet-subnet-id $SUBNET_ID \
--enable-managed-identity
```

Demo

Deploying a cluster to an existing Virtual Network using Azure CNI

Summary

Understanding AKS networking

- kubenet
- Azure CNI

Deploying AKS networking

- Deploying into a new virtual network
- Deploying into an existing virtual network

Up Next:
Accessing Applications Deployed in AKS