Understanding Azure Kubernetes Service Configuration Options

James Bannan
AZURE CONSULTANT

@jamesbannan www.jamesbannanit.com

Module Overview

AKS Prerequisites and Considerations

AKS Networking

AKS Identity and RBAC

AKS Storage

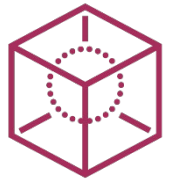
AKS Scaling

Prerequisites and Considerations

Things to Check Before You Start

Azure AD permissions: Service Principal creation & AKS deployment

Subscription resource limits and restrictions



Registration of `Microsoft.ContainerService` **namespace**

Some Things You May Need

Azure CLI: Windows/Linux/Mac, or Azure Cloud Shell

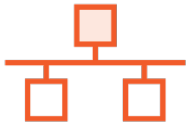
kubectl: Use native package management or `az aks install-cli`

SSH key pair: Automatically generated or `ssh-keygen -t rsa -b 2048`

Azure Kubernetes Service Networking

AKS Networking Considerations

Integration: Are the clusters fully self-contained?

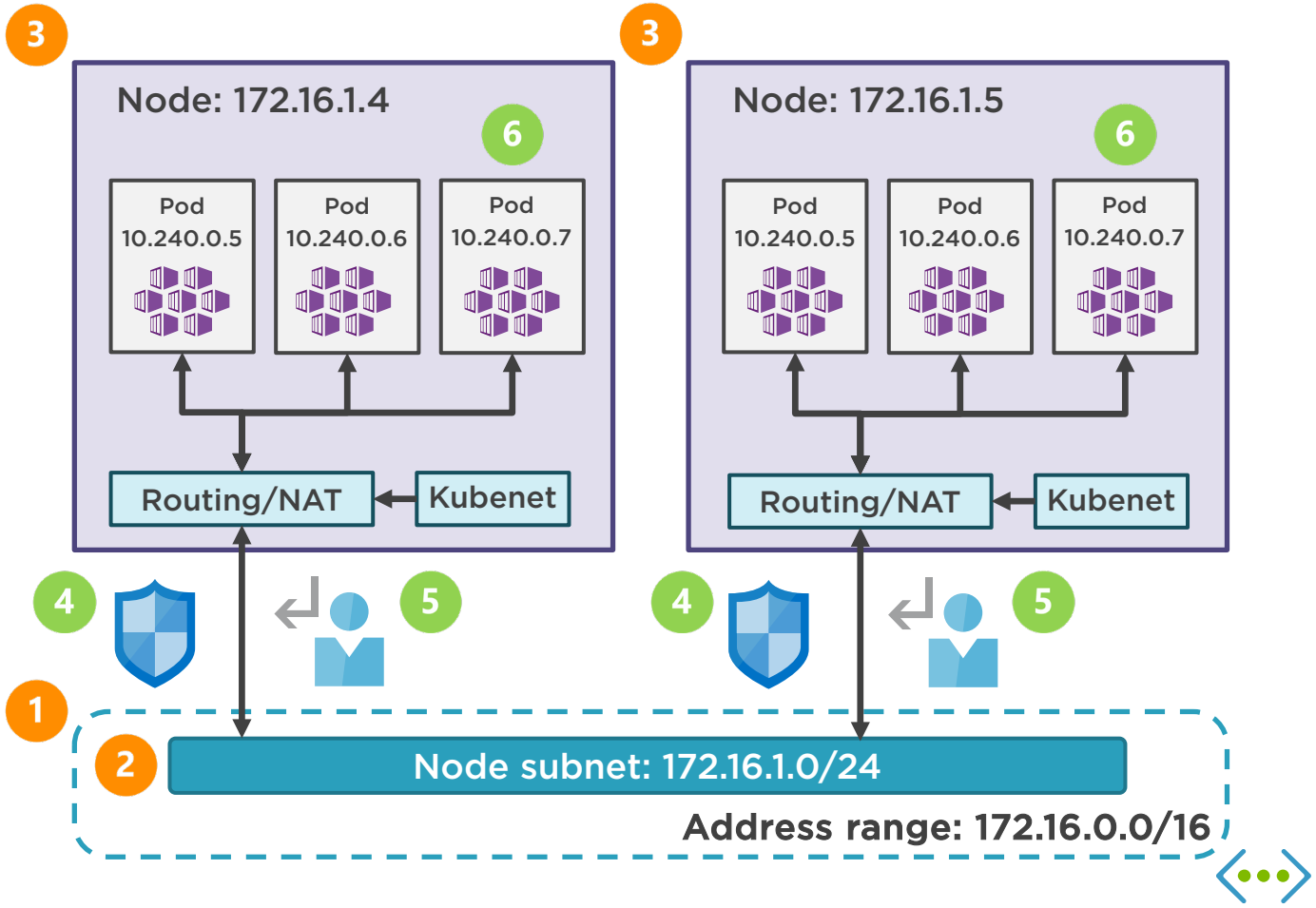


Access: How are services running in the clusters to be reached?

Isolation: Do the cluster pods need to be accessed directly?

AKS Networking: Kubenet

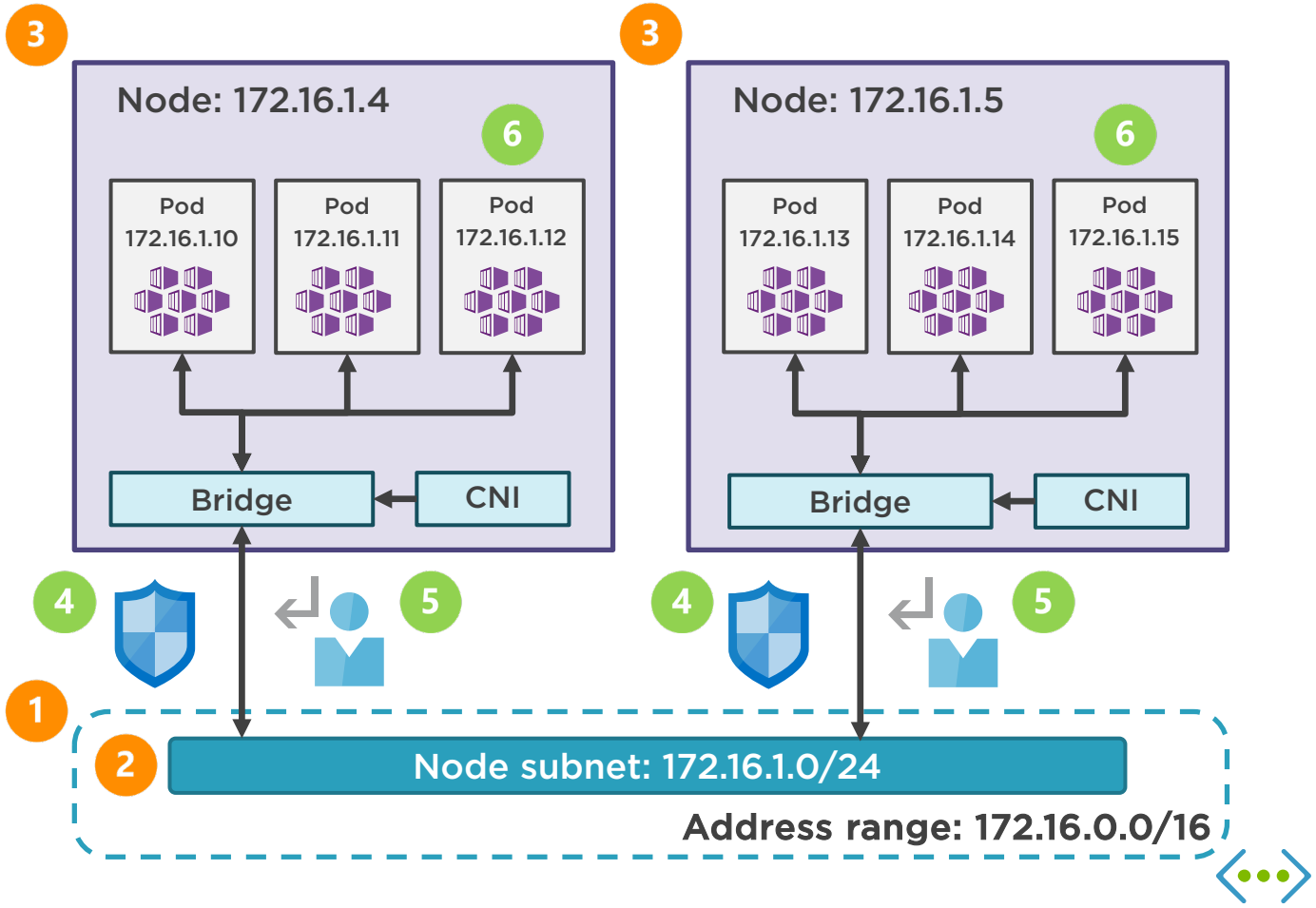
1. Azure Virtual Network
2. Virtual Network Subnet
3. Cluster Nodes
4. Network Security Groups
5. User Defined Routes
6. Cluster Pods



https://docs.microsoft.com/en-au/azure/aks/configure-kubenet

AKS Networking: Container Networking Interface

1. Azure Virtual Network
2. Virtual Network Subnet
3. Cluster Nodes
4. Network Security Groups
5. User Defined Routes
6. Cluster Pods



https://docs.microsoft.com/en-au/azure/aks/configure-azure-cni

Kubenet (Basic) vs Azure CNI (Advanced)

Kubenet	Azure CNI
IP addresses are private to the cluster	IP addresses are taken from the subnet
AKS master manages network resources	Network resources managed independently
Pods are accessed via load balancers	Pods can be access directly
Pod-VM connectivity initiated by pod	Pod-VM connectivity initiated by pod or VM

https://docs.microsoft.com/en-au/azure/aks/concepts-network#compare-network-models

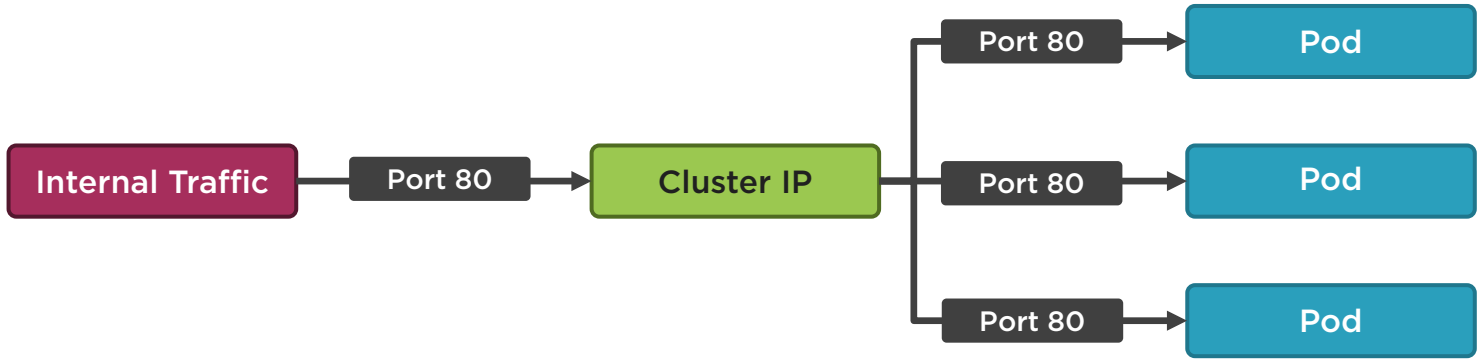
Azure CNI: Planning Considerations

- Network must allow outbound connectivity
- Only one AKS cluster per subnet
- IP addresses are reserved for each cluster node
- Up to 250 pods per node (default is 30 pods)
- Plan for additional network resources
- Service principal requires Network Contributor rights

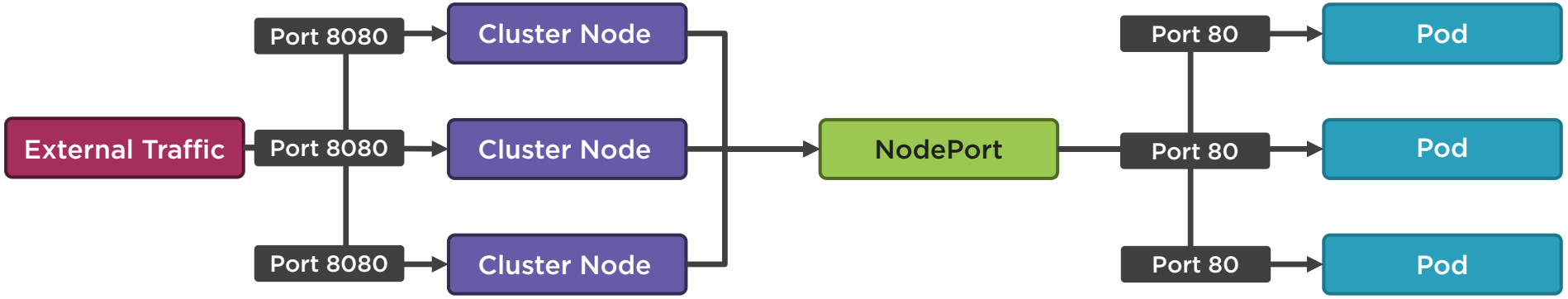
https://docs.microsoft.com/en-au/azure/aks/configure-azure-cni

Publishing Kubernetes Services

`ClusterIP`: **An internal IP within the cluster.**



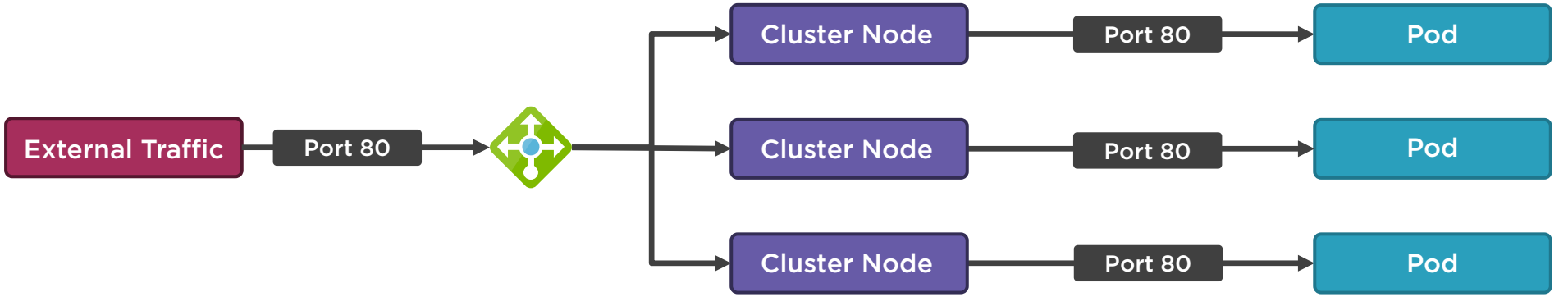
`NodePort`: **Port mapping from node to application.**



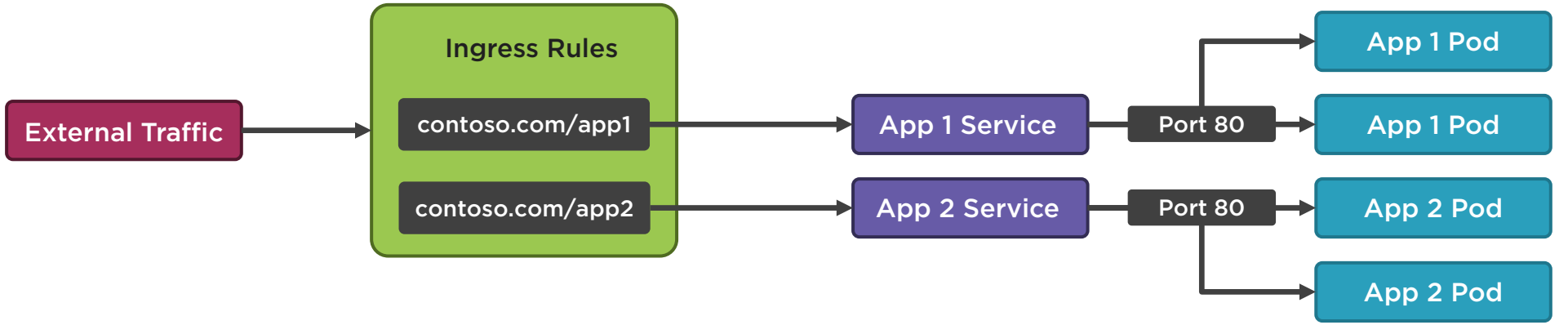
https://docs.microsoft.com/en-au/azure/aks/concepts-network

Publishing Kubernetes Services

`LoadBalancer`: **Exposes** `NodePort` **and** `ClusterIP` **services to external traffic.**



`Ingress`: **Layer 7 controller to distribute application traffic based.**

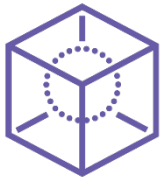


https://docs.microsoft.com/en-au/azure/aks/concepts-network

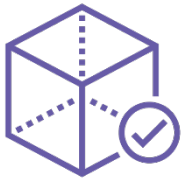
AKS Identity and RBAC

Service Principal Considerations

Represents the “identity” of each AKS cluster



Best practise to have a dedicated service principal per cluster



Used to delegate access to resources outside the cluster

Credentials should be regularly rotated

Azure Active Directory Integration

Tokens generated using Open ID Connect

Webhook Token Authentication used to validate supplied tokens

Only supported on new AKS clusters

Map Azure AD groups to `Roles` **and** `ClusterRoles` **using** `RoleBindings`

AKS Storage

Kubernetes Storage Options

Container FS

Local filesystem in each container. Data is linked to container lifecycle.

Volume

Storage shared between containers in a pod. Data is linked to pod lifecycle.

Persistent Volume

Long-term independent resource. Data is linked to cluster lifecycle.

https://kubernetes.io/docs/concepts/storage/

AKS Storage Solutions

Creation Method	Storage Access Requirements: Single node/pod	Storage Access Requirements: Multiple nodes/pods
Dynamic	**Azure Disk** **Use `default` or `managed-premium` classes to provision a new disk**	**Azure Files** **Use `azure-file` storage class to provision new Storage Account**
Static	**Azure Disk** **Create a new disk and specify resource ID as `azureDisk` volume**	**Azure Files** **Create an `azureFile` volume with a Kubernetes secret from storage key**

https://docs.microsoft.com/en-us/azure/aks/concepts-storage

AKS Scaling

Options to Scale AKS

Manual: Use `az aks scale` to increase or decrease the node count

Virtual Node: Burst out using Azure Container Instances

Cluster Autoscaler (Preview): Use VMSS to enable automatic scaling

https://docs.microsoft.com/en-au/azure/aks/concepts-scale

Scaling with Virtual Nodes

Ensure the `Microsoft.ContainerInstance` provider is registered

Validate ACI regional and functional limitations

Only supported on AKS clusters with CNI (advanced) networking

https://docs.microsoft.com/en-au/azure/aks/virtual-nodes-cli

Cluster Autoscaler (Preview) Functionality

Cluster autoscaler: Scales node count to support new pods

Horizontal pod autoscaler: Scaled pods to support service requirements

Supports multiple node pools feature (preview)

https://docs.microsoft.com/en-au/azure/aks/cluster-autoscaler

Cluster Autoscaler (Preview) Considerations

Preview features are not supported in production

Requires `VMSSPreview` provider feature registration on subscription

Not supported on pre-existing AKS clusters

https://docs.microsoft.com/en-au/azure/aks/cluster-autoscaler

Module Overview

AKS Prerequisites and Considerations

AKS Networking

AKS Identity and RBAC

AKS Storage

AKS Scaling

Coming next:
Deploying Azure Kubernetes Service