AKS cluster with Azure CNI overlay

Last updated by | Michele Cereda | Nov 29, 2023 at 10:51 AM GMT+1

Contents

What is Azure CNI overlay

Azure Container Networking Interface (CNI) works by assigning each Pod IP address from AKS VNET. This address can come from a set of reserved IPs on each node or from a separate subnet just for the pods.

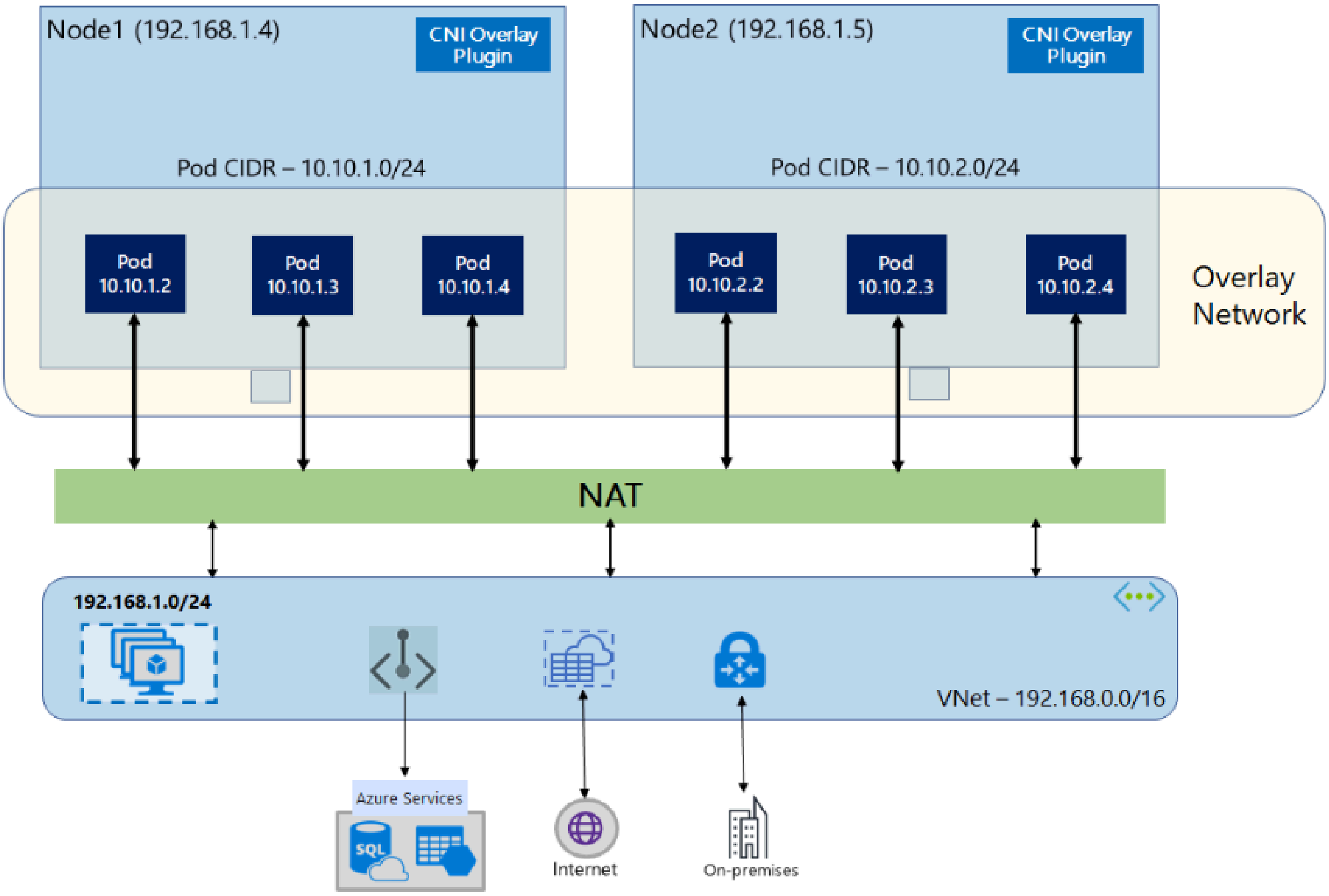
This method requires careful planning of IP addresses and can cause problems when you need to scale your clusters as your application grows.

With Azure CNI Overlay, the cluster nodes are placed in a special part of an Azure Virtual Network (VNet) called a subnet.

The pods are given IP addresses from a different range that is separate from the VNet where the nodes are located. The pods and nodes communicate with each other using an Overlay network.

Network Address Translation is used to connect with resources outside the cluster, using the node's IP address.

Architecture



This approach saves VNet IP addresses and allows you to easily expand your cluster to very large sizes. Another benefit is that the IP address range for pods can be reused in different AKS clusters, giving you more space for containerized applications in AKS.

Kubenet Vs Azure CNI overlay

Azure CNI overlay functionality similar to kubenet, However it has more advanced features compared with kubenet.

Azure CNI Overlay is a recommended solution if you don't want to assign VNet IP addresses to pods because of limited IP availability.

Kubenet, on the other hand, assigns IP addresses to pods from a different address space that is separate from the VNet, but it has limitations when it comes to scaling and other aspects.

For more differences and use cases refer official documentation:

Limitations of Azure CNI Overlay:

- You can't use Application Gateway as an Ingress Controller (AGIC) for an Overlay cluster.
- Windows support is still in Preview
- Windows Server 2019 node pools are not supported for Overlay
- Traffic from host network pods is not able to reach Windows Overlay pods.
- Virtual Machine Availability Sets (VMAS) are not supported for Overlay
- You can't use DCsv2-series virtual machines in node pools. To meet Confidential Computing requirements, consider using DCasv5 or DCadsv5-series confidential VMs instead.

How to Enable CNI overlay.

We can update existing Azure CNI clusters to CNI overlay, However updating existing clusters is still in preview.
Refer: https://learn.microsoft.com/en-us/azure/aks/azure-cni-overlay#upgrade-an-existing-cluster-to-cni-overlay-preview

Since updating existing cluster to Azure CNI overlay is still in preview, You can create a new cluster with Azure CNI overlay (GA Feature).

To avoid downtime you can use blue-green deployment method.
Refer: https://learn.microsoft.com/en-us/azure/architecture/guide/aks/blue-green-deployment-for-aks

We can enable CNI overlay either from command line or from bicep code.

Pre-requisites:

- You should use `az cli > 2.47` to make use of this Azure cni overlay flag.
- If you are using the Bicep way to create you should use API version `Microsoft.ContainerService/managedClusters@2023-03-01` or greater.

Creating New cluster

From CLI:

```
az aks create -n clusterName -g resourceGroup --location location --network-plugin azure --network-plugin-m
```

Note: Plan Pod CIDR based on how many pods you would like to run on the AKS cluster.

Using Bicep code:

Add below parameters under `networkprofile`

```
networkProfile: {
      ---
      networkPlugin: 'azure'
      networkPluginMode: 'overlay'
      podCidr: '10.230.0.0/16'
      ---

    }
```

PodCidr - IP address that you would like to assign to Pod's.

Updating existing cluster

We can update existing Azure CNI cluster to use CNI overlay using below commands, Since Updating is still in Pre-view we have to register preview feature as per below documentation.

Ref: https://learn.microsoft.com/en-us/azure/aks/azure-cni-overlay#register-the-azureoverlaypreview-feature-flag

Once Feature Registered we can update our Existing cluster using below command.

```
az aks update --name cluster-name--resource-group resourcerg --network-plugin-mode overlay --pod-cidr podci
```

Note:- Updating existing Azure CNI cluster to CNI overlay is still in Preview, Not recommended for production. If you you would like to explore use it in lower environment

For more information about Azure CNI overlay Refer: https://learn.microsoft.com/en-us/azure/aks/azure-cni-overlay