Secure AKS control plane

Public
Private
VNET Integration

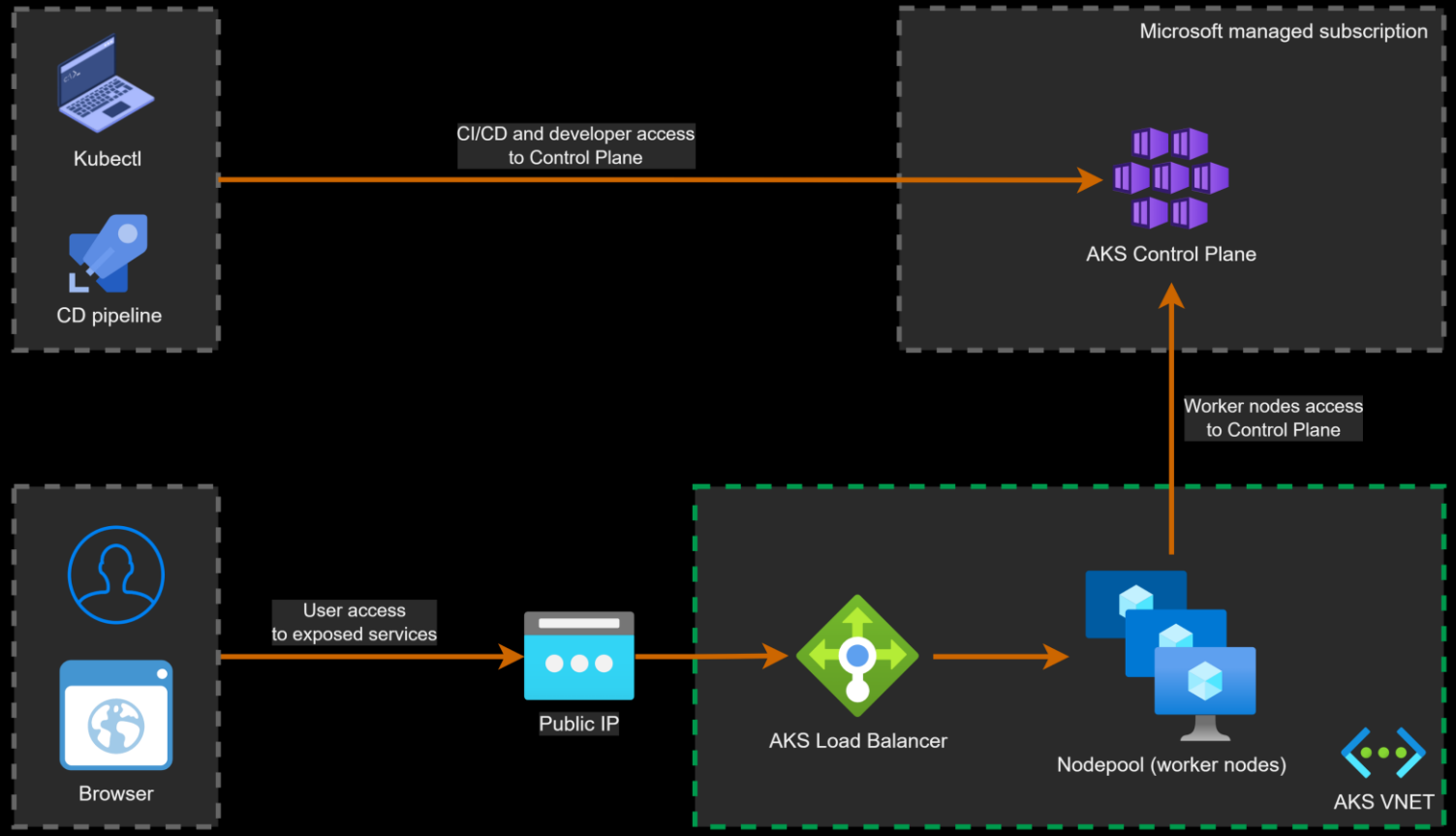
Houssem Dellai

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

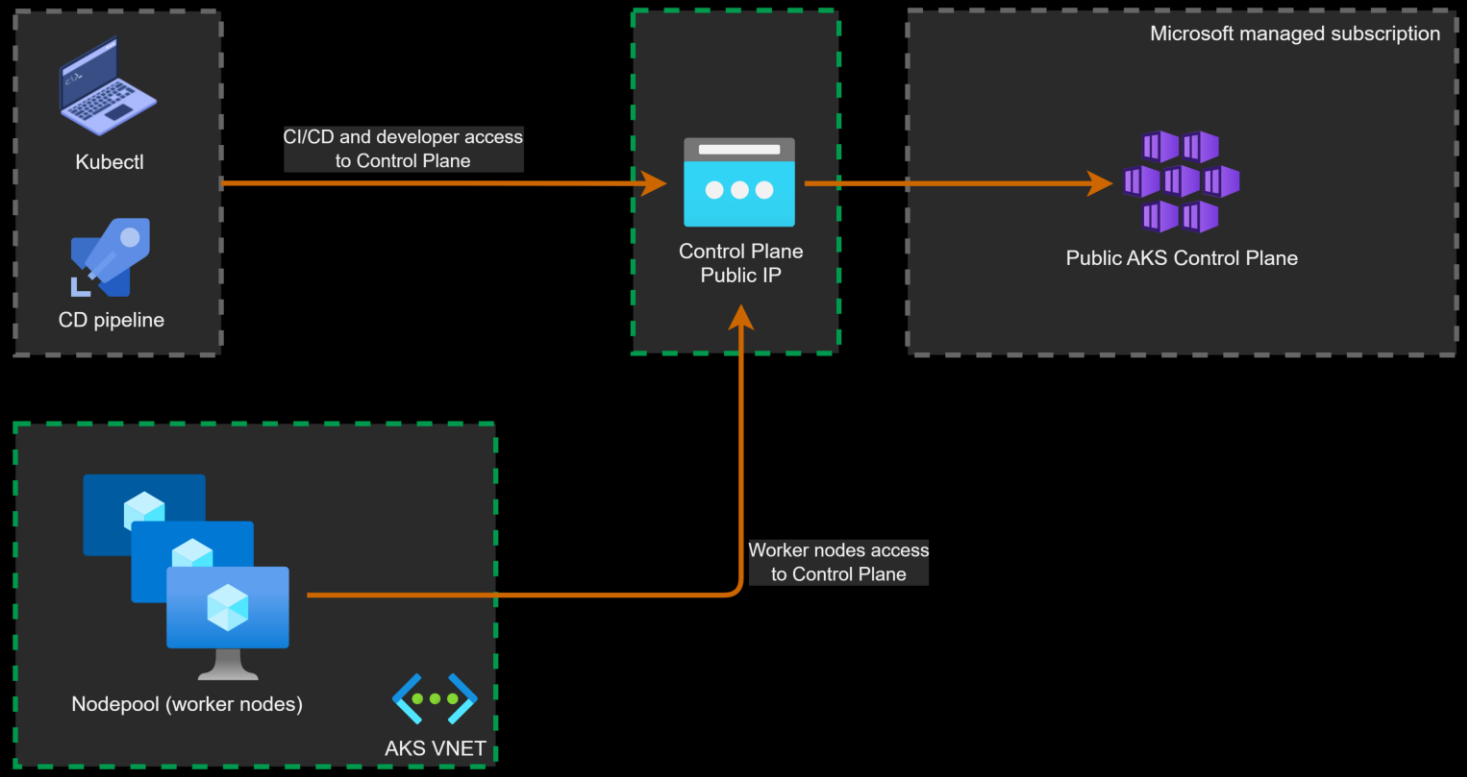
- Public cluster (public FQDN and public IP for Control Plane)
- Private cluster using Private Endpoint (private IP for Control Plane)
- Public cluster using VNET Integration
- Private cluster using VNET Integration

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
 $
```

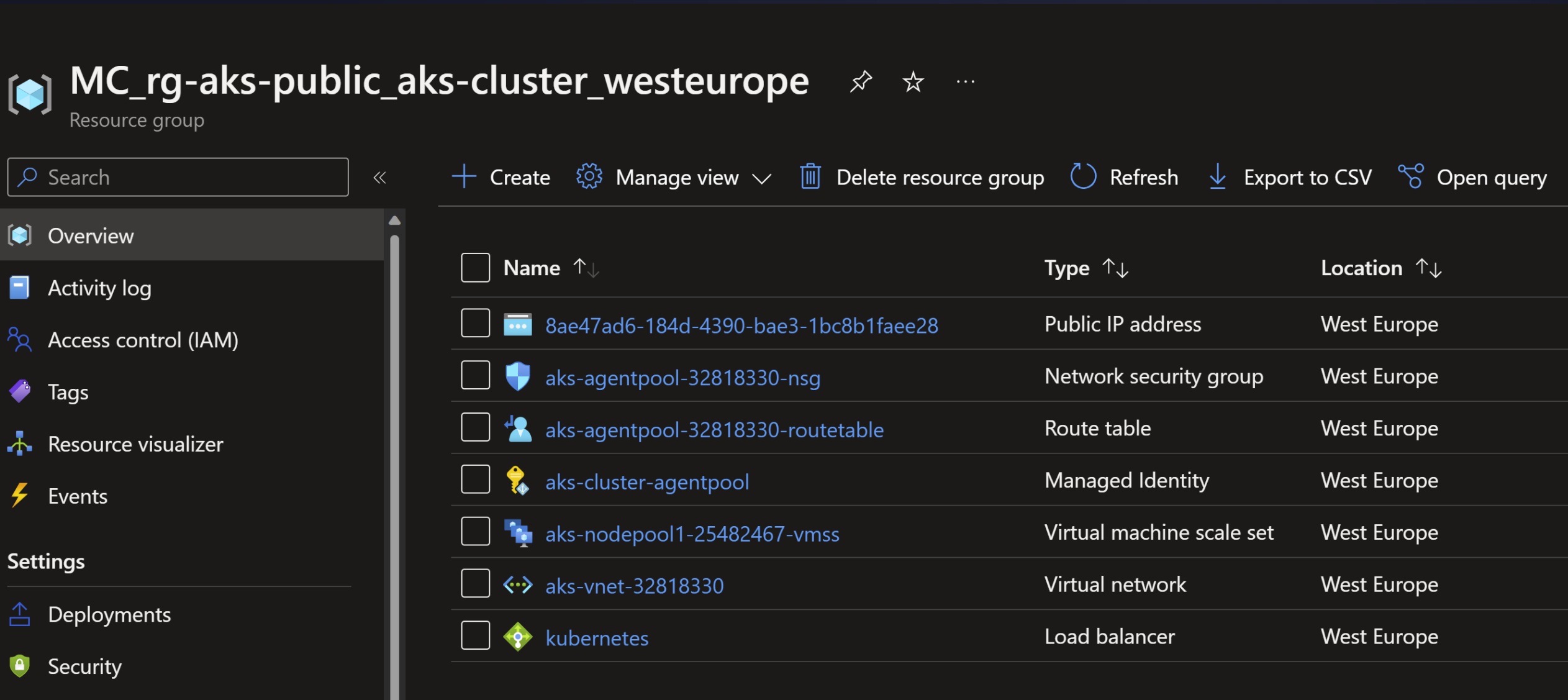
How Worker Nodes connects to Control Plane in public AKS ?

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:         <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:           20.103.218.175:443
Session Affinity:    None
Events:              <none>
 $
 $
 $ kubectl get endpoints
NAME         ENDPOINTS             AGE
kubernetes   20.103.218.175:443    114m
 $
```

Public AKS cluster resources



Private AKS cluster access

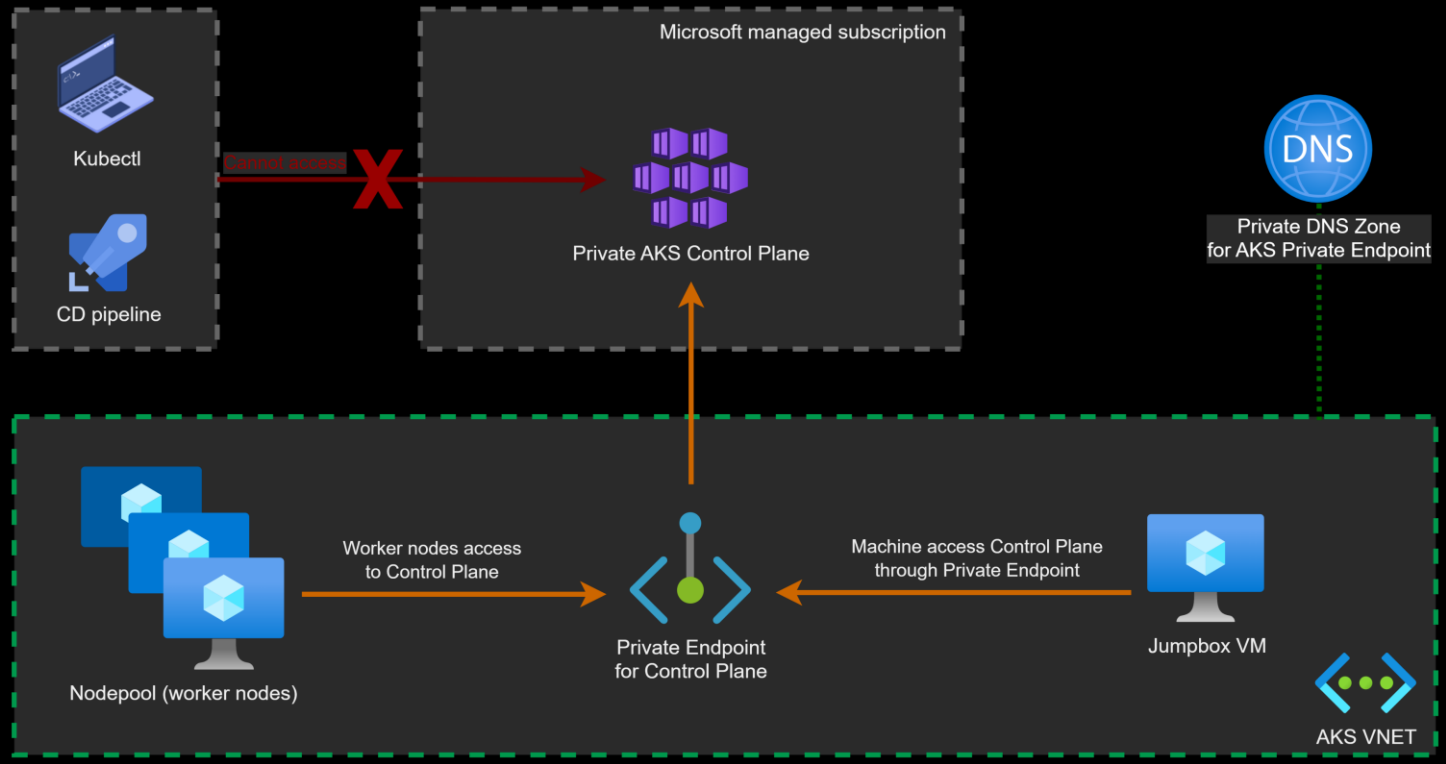
Control Plane is exposed on public FQDN but with private IP address.

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.



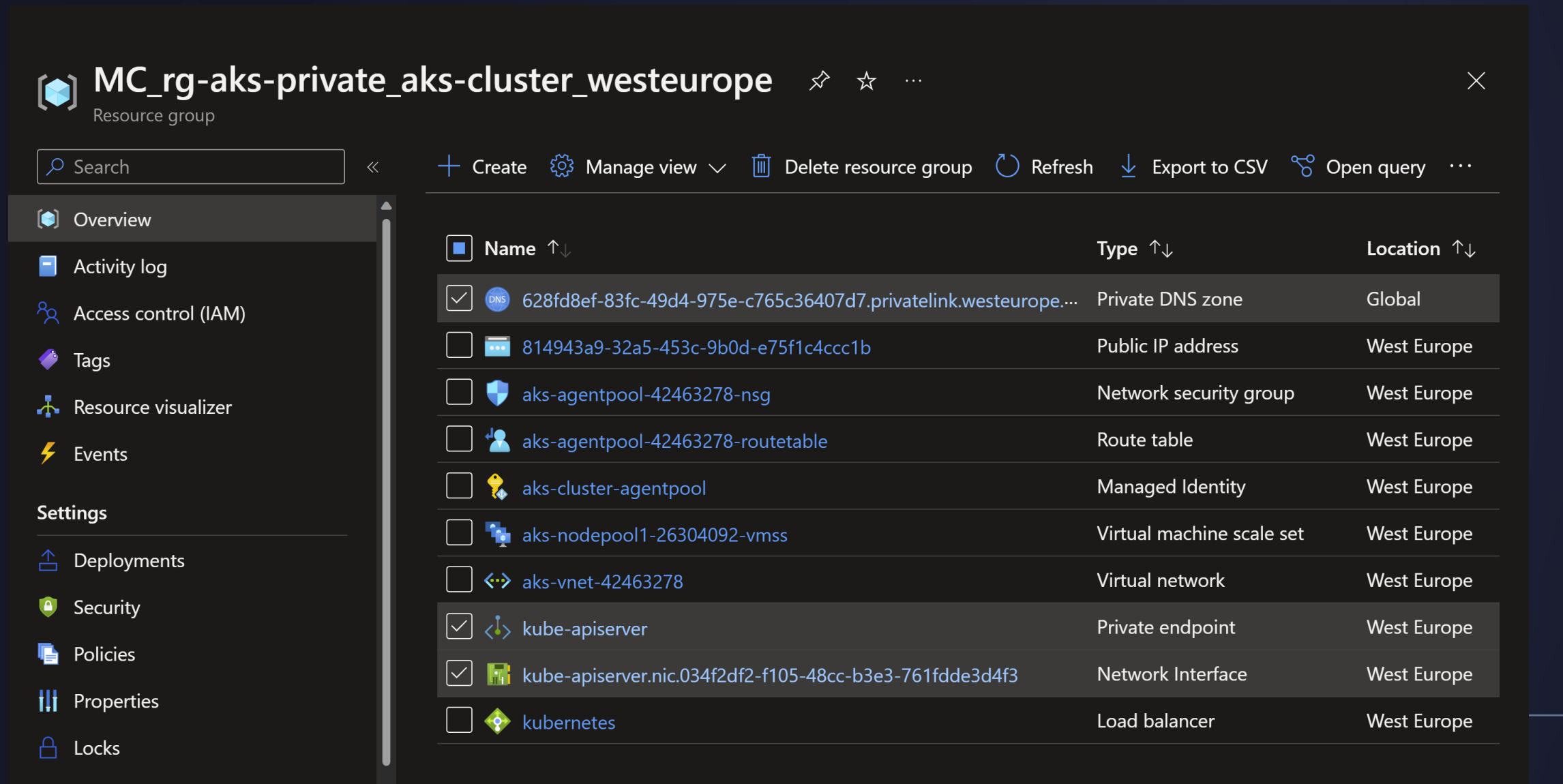
Creating private AKS cluster

```
 $
 $ 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
 $
```

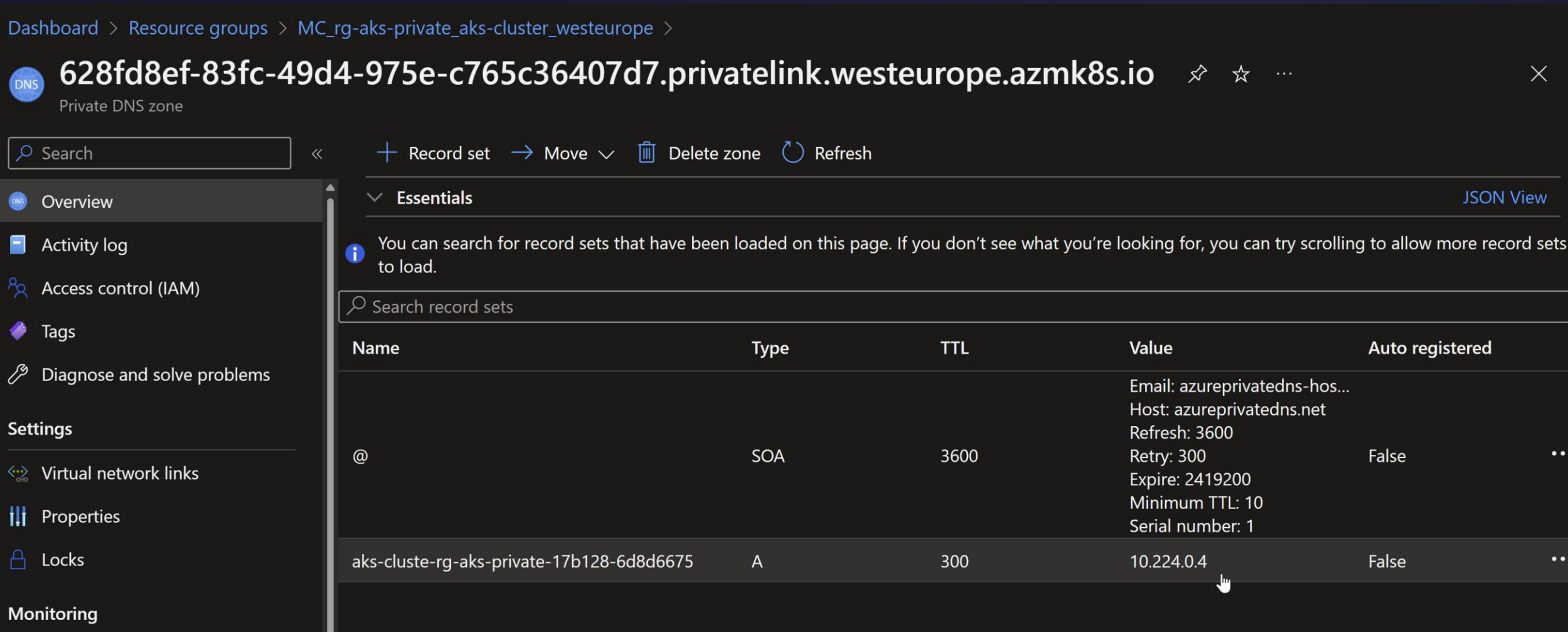
Private AKS cluster resources

Adds Private Endpoint and private DNS Zone.



Private DNS Zone for private cluster

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



Public AKS cluster with VNET Integration access

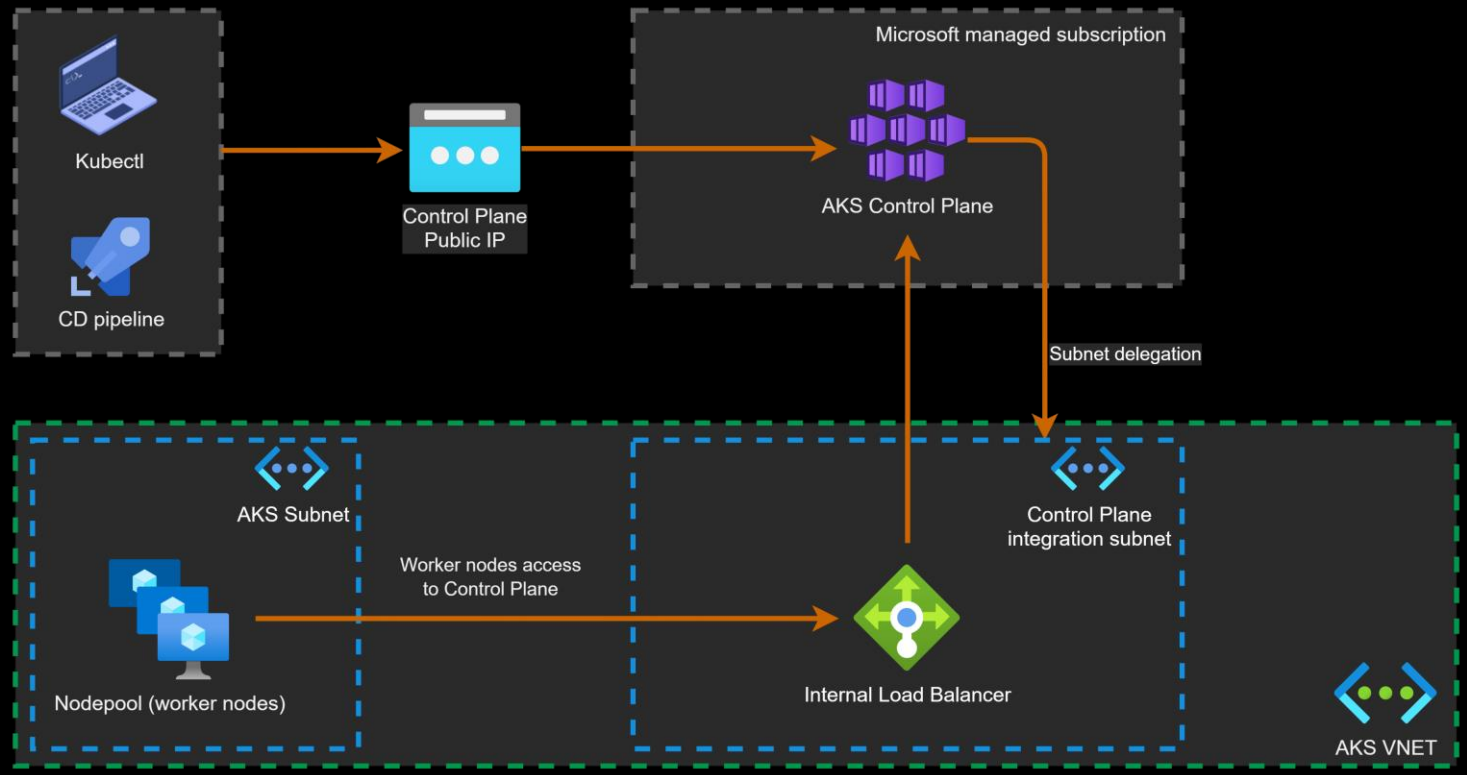
Control Plane is exposed on public FQDN with public IP address.

Control Plane endpoint is exposed to the internet.

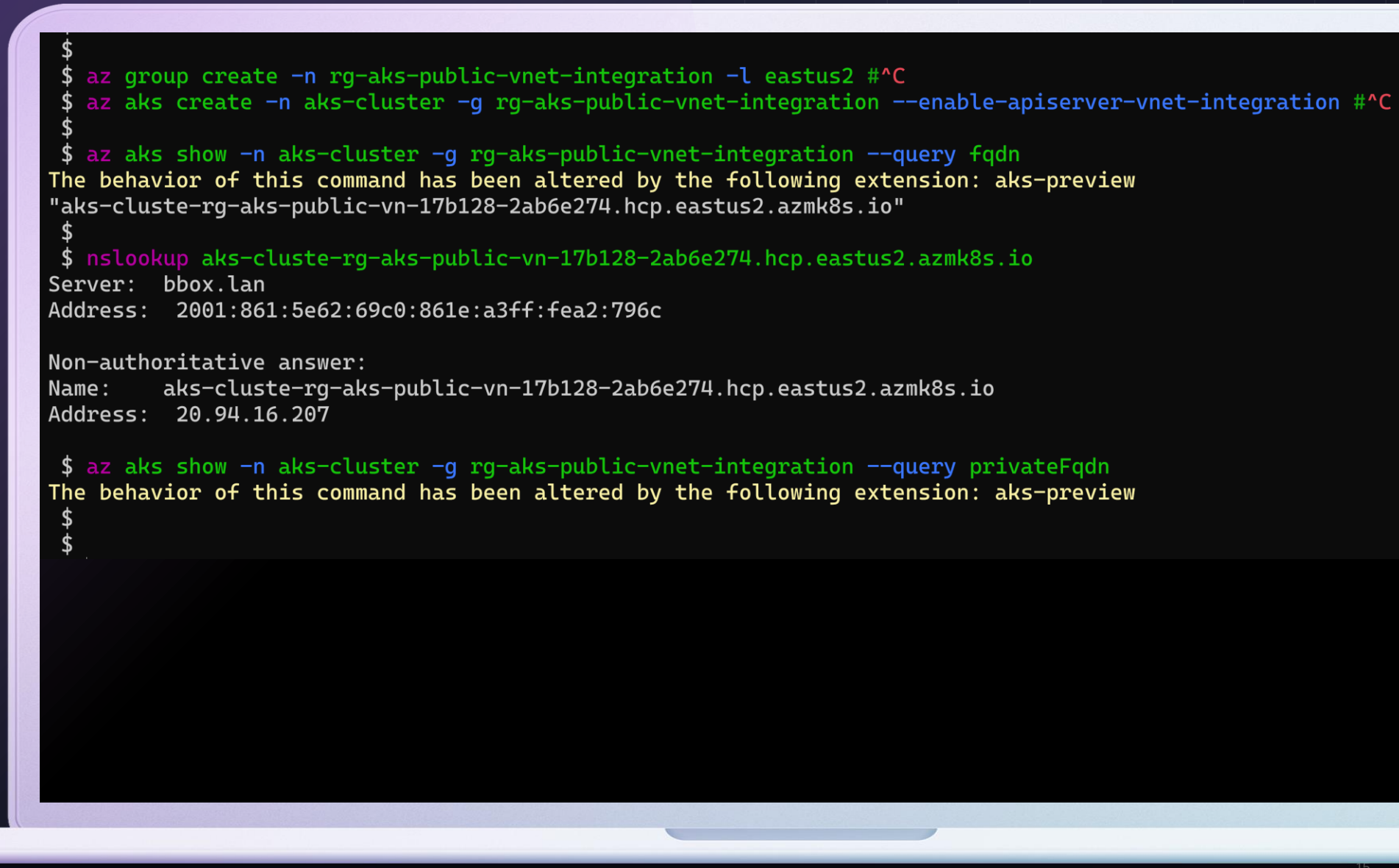
Public FQDN could NOT be disabled except on private cluster.

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

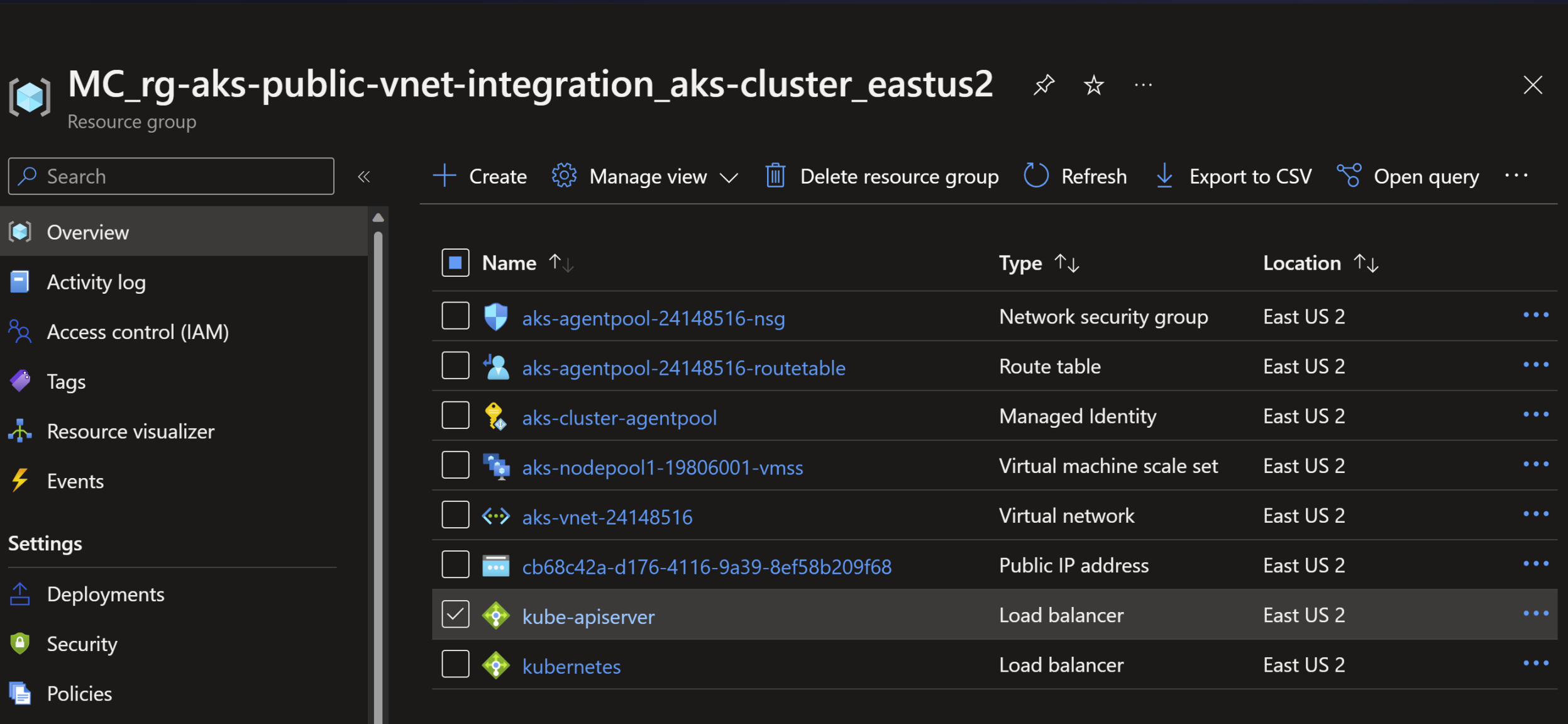


How Worker Nodes access Control Plane ?

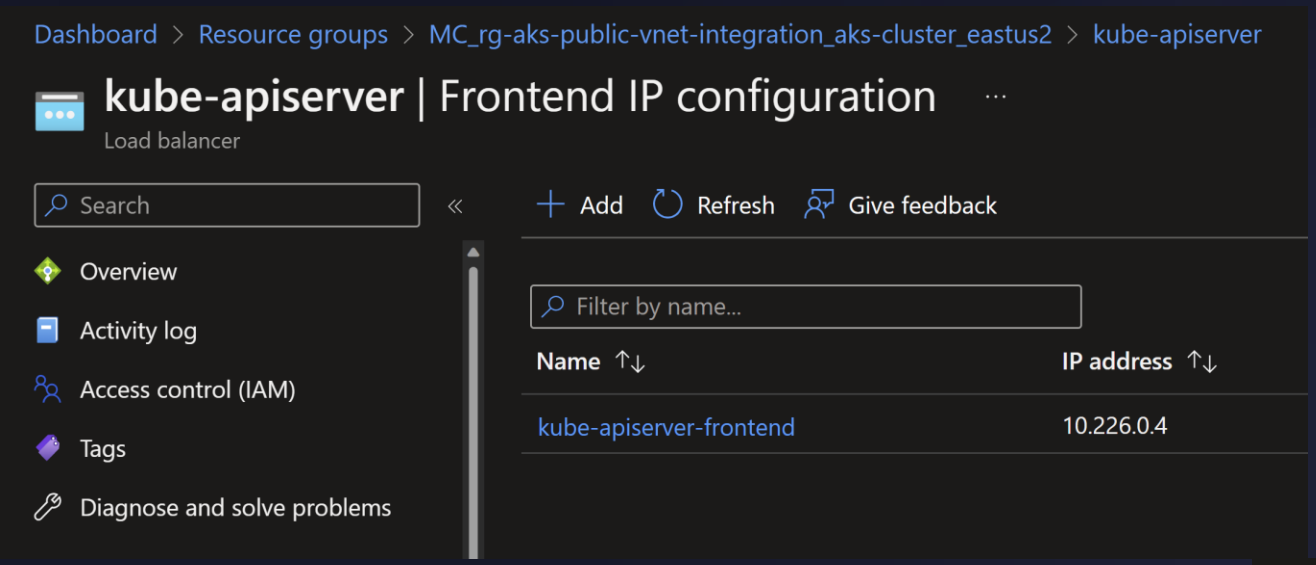
Through Control Plane private IP, not the public IP.

```
 $
 $ 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:            <none>
 $
```

Public AKS with VNET Integration resources



Public cluster and VNET Integration changes

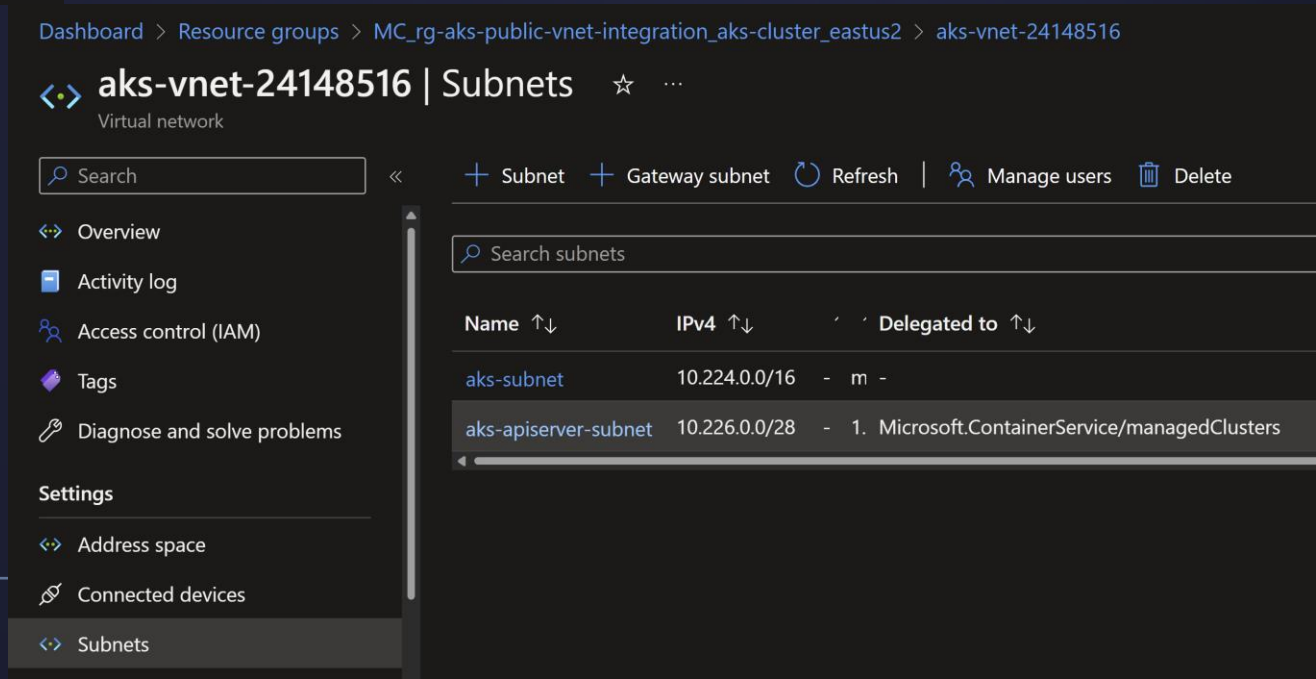


AKS VNET Integration creates internal Load Balancer.

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

AKS VNET Integration creates new Subnet in AKS VNET.

It injects the ILB and configure delegation.



Private AKS cluster with VNET Integration access

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

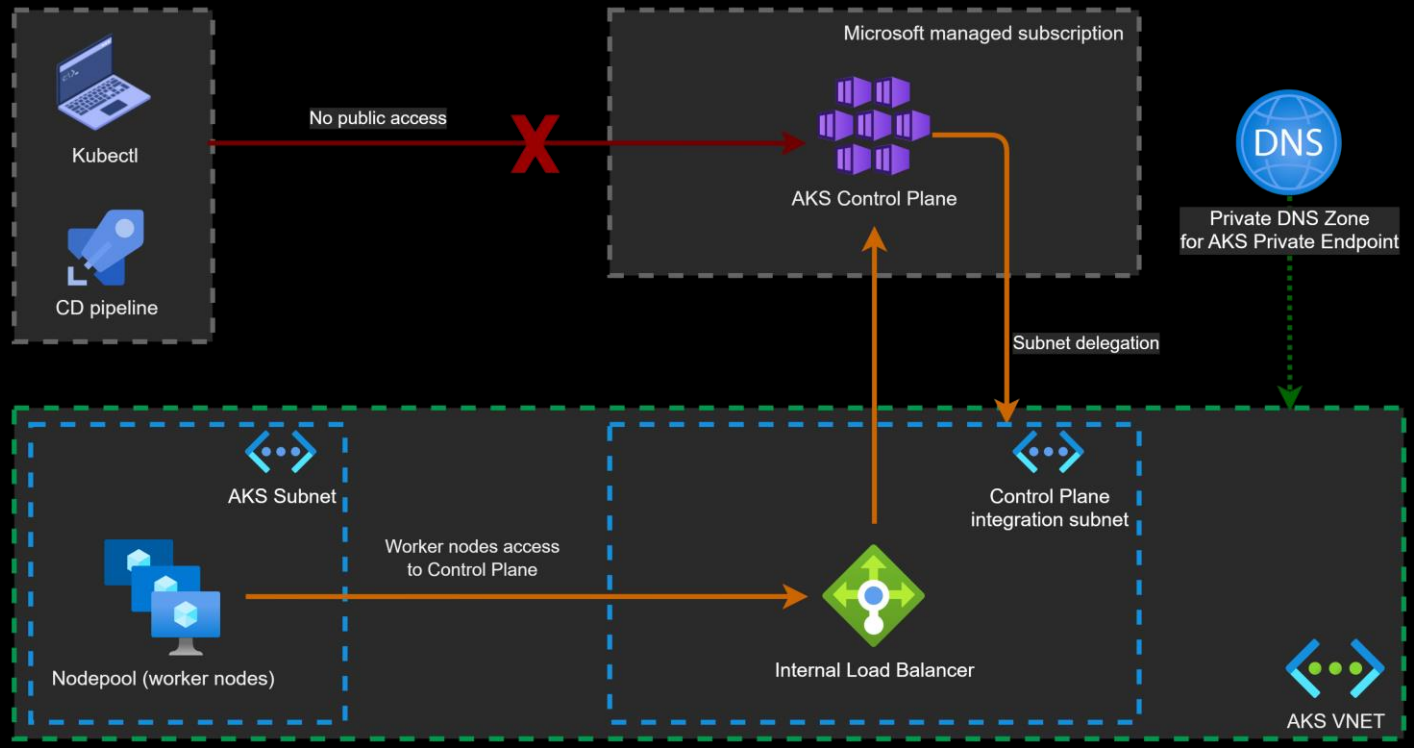
Control Plane have public FQDN exposed to the internet.

Public FQDN references a private IP, could be disabled.

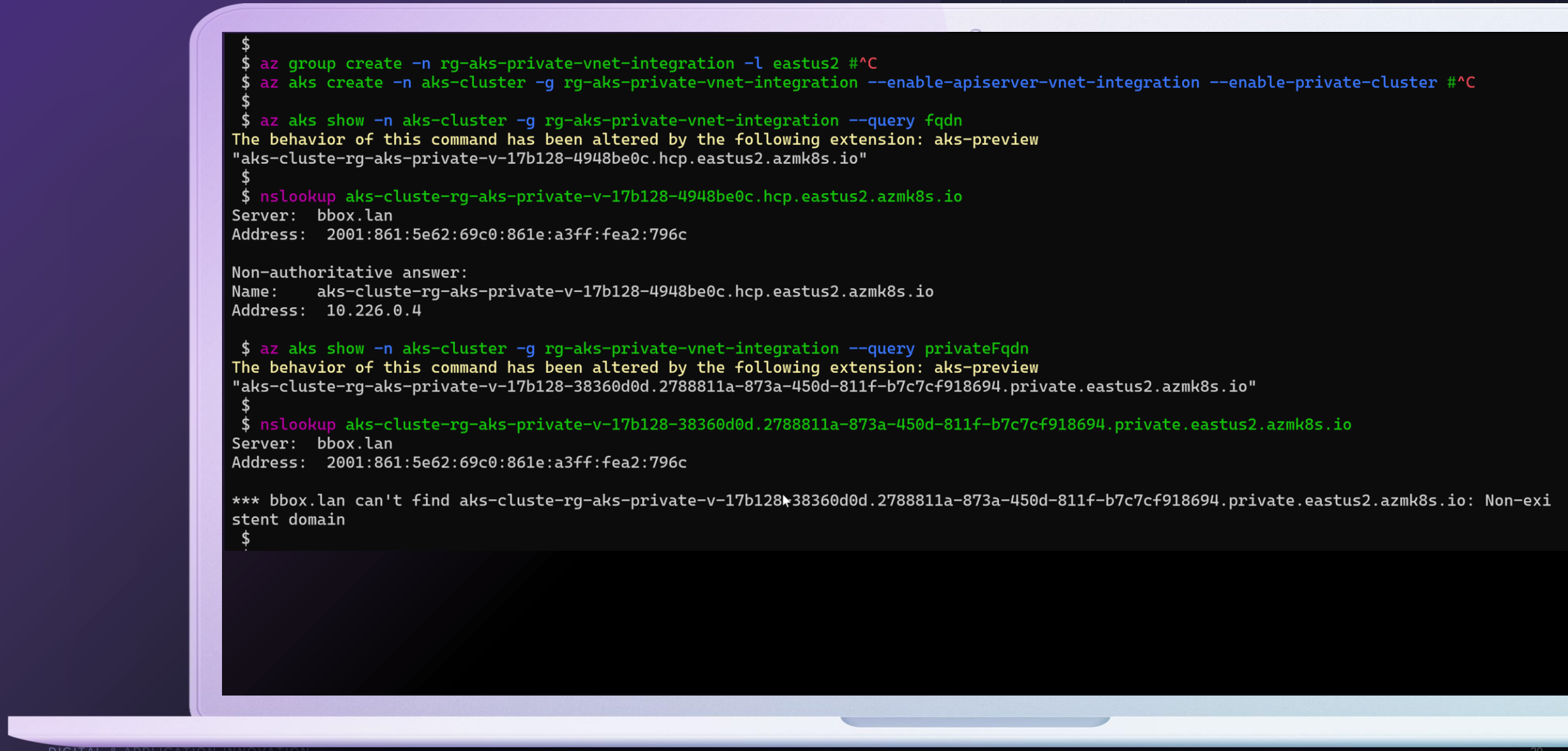
DevOps CD pipelines could only access through private IP (internal LB).

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

No Private Endpoint created although the cluster is private.

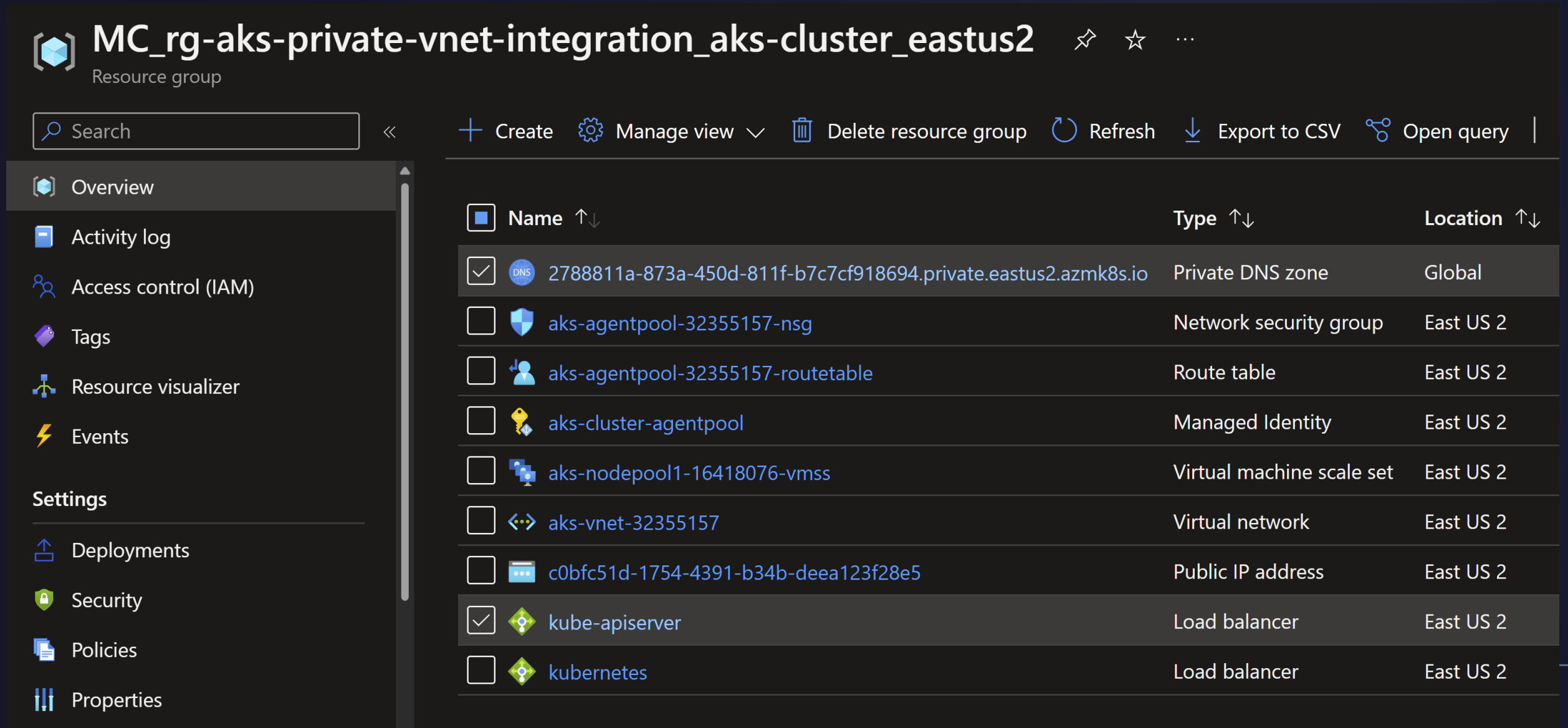


Create private AKS cluster with VNET Integration



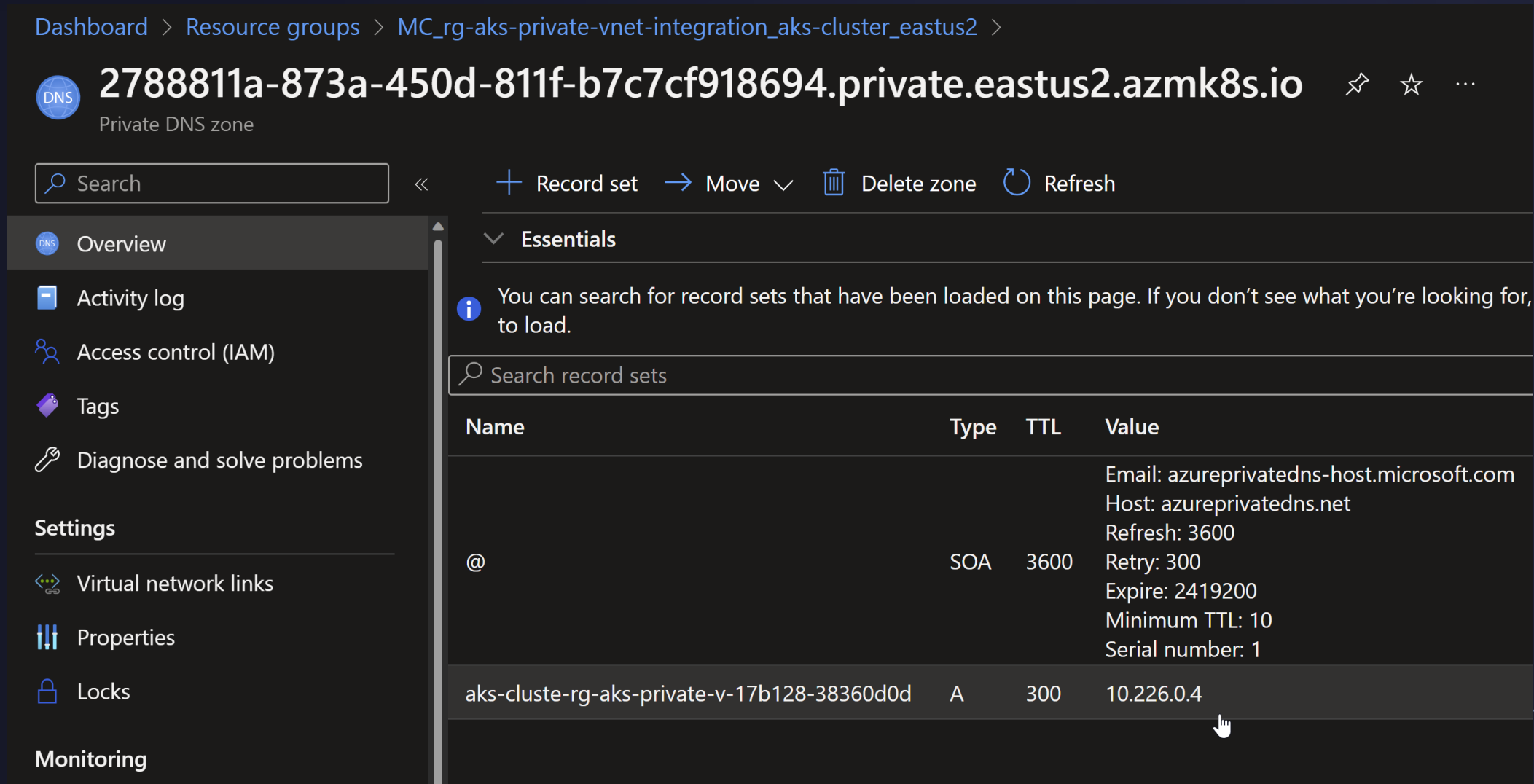
Private cluster with VNET Integration

Adds internal Load Balancer and private DNS Zone.



Private cluster and VNET Integration changes

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



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