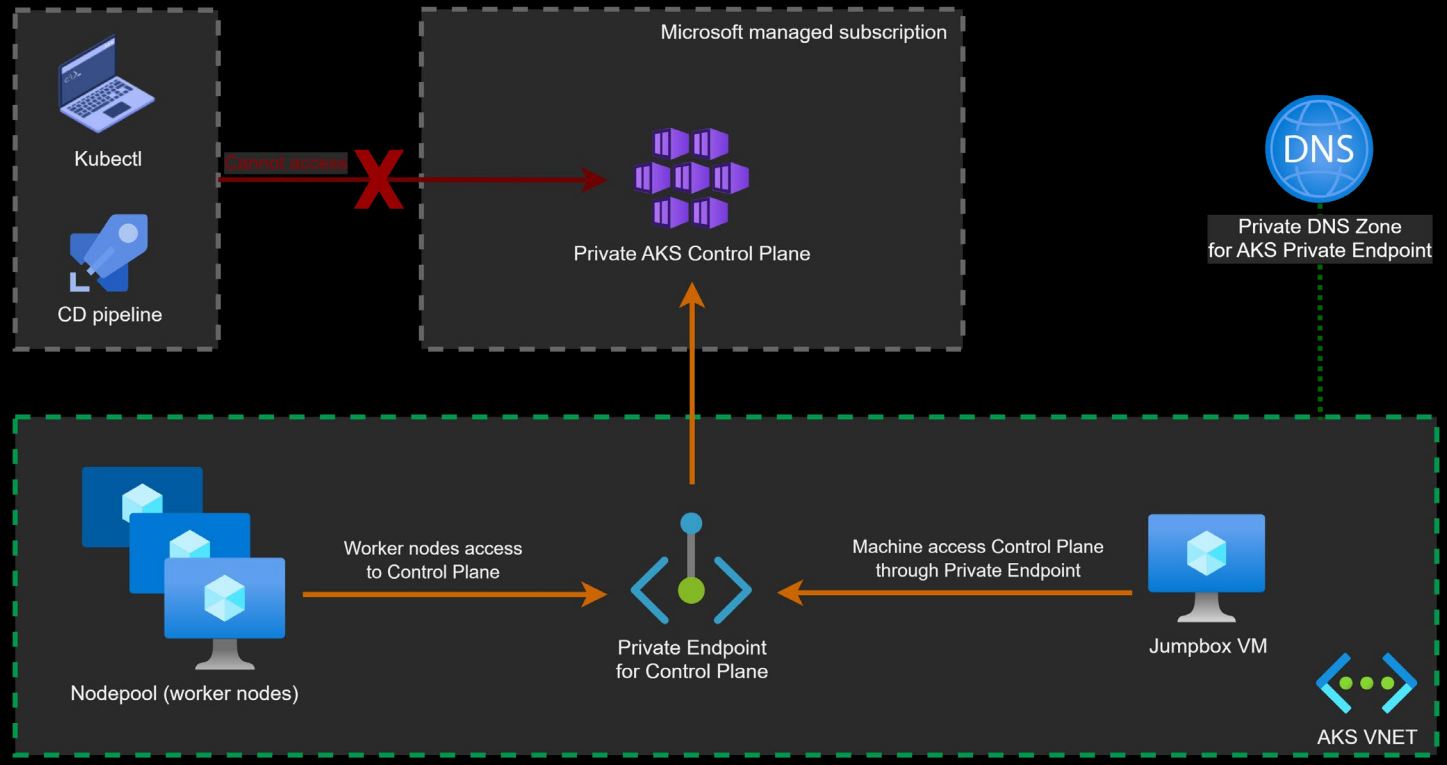
Decentralized vs Centralized

DNS resolution for private AKS



Public FQDN to resolve to private IP address

- AKS' control plane FQDN is publicly exposed.
- FQDN resolves to private IP address of PE.
- No need for Private DNS Zone.
- `--private-dns-zone="none"`

(won't create Private DNS Zone)

⚠️ Knowing the private IP could be a security issue.

```
nslookup aks-prbob7iw.hcp.swedencentral.azmk8s.io
Address: 10.1.0.4
```

Centralized DNS resolution

- AKS' control plane FQDN is exposed privately through Private DNS Zone.
- Private FQDN resolves to private IP address of PE.
- Private DNS Zone is linked to Hub, and also, to Spoke (internal technical requirement).
- One single centralized Private DNS Zone for all clusters.

⚠️ All clusters can access and modify Private DNS Zone.

- `--private-dns-zone="system"|"ZoneID"`

```
nslookup aks-89eprte0.202.privatelink.swedencentral.azmk8s.io
10.1.0.4
```

Decentralized DNS resolution

- AKS control plane FQDN is exposed privately through Private DNS Zone.
- Private FQDN resolves to private IP address of PE.
- Private DNS Zone is linked to Hub, and also, to Spoke (internal technical requirement).
- Each cluster/spoke have its own Private DNS Zone.

⚠️ Needs additional link to the Hub VNET (Azure Policy).

- `--private-dns-zone="system"|"ZoneID"`

```
nslookup aks-89eprte0.202.privatelink.swedencentral.azmk8s.io
10.1.0.4
```

Limitations with Private DNS Zones

- Private DNS Zone could be linked/attached to maximum 1000 VNETs.
- VNET could be linked/attached to maximum 1000 Private DNS Zones.
- VNET could be peered to maximum 500 VNETs.