

AKS Security Simplified for Developers

Wolfgang Ofner

Senior Cloud Architect
Programming with Wolfgang



THE H@CK
SUMMIT

A lecture selected by a Program Council
consisting of recognized leaders in the field
of cybersecurity.

Warsaw,
13.10.2025 - 14.10.2025



OFFICIAL LECTURE OF THE HACK SUMMIT



Agenda



Authentication and
Authorization

Entra Workload ID

Private AKS Cluster

Azure Key Vault Provider for
Secrets

Wolfgang Ofner

Freelance Cloud Architect, Toronto, Canada
Focus on Azure, Kubernetes, and DevOps



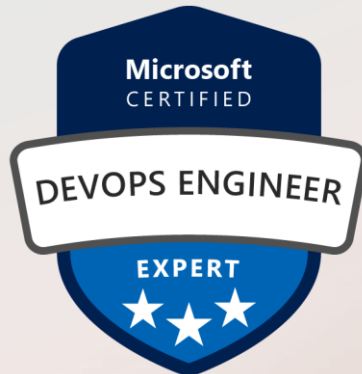
programmingwithwolfgang.com



[wolfgangofner](https://www.linkedin.com/in/wolfgangofner)



YouTube [@programmingwithwolfgang](https://www.youtube.com/@programmingwithwolfgang)



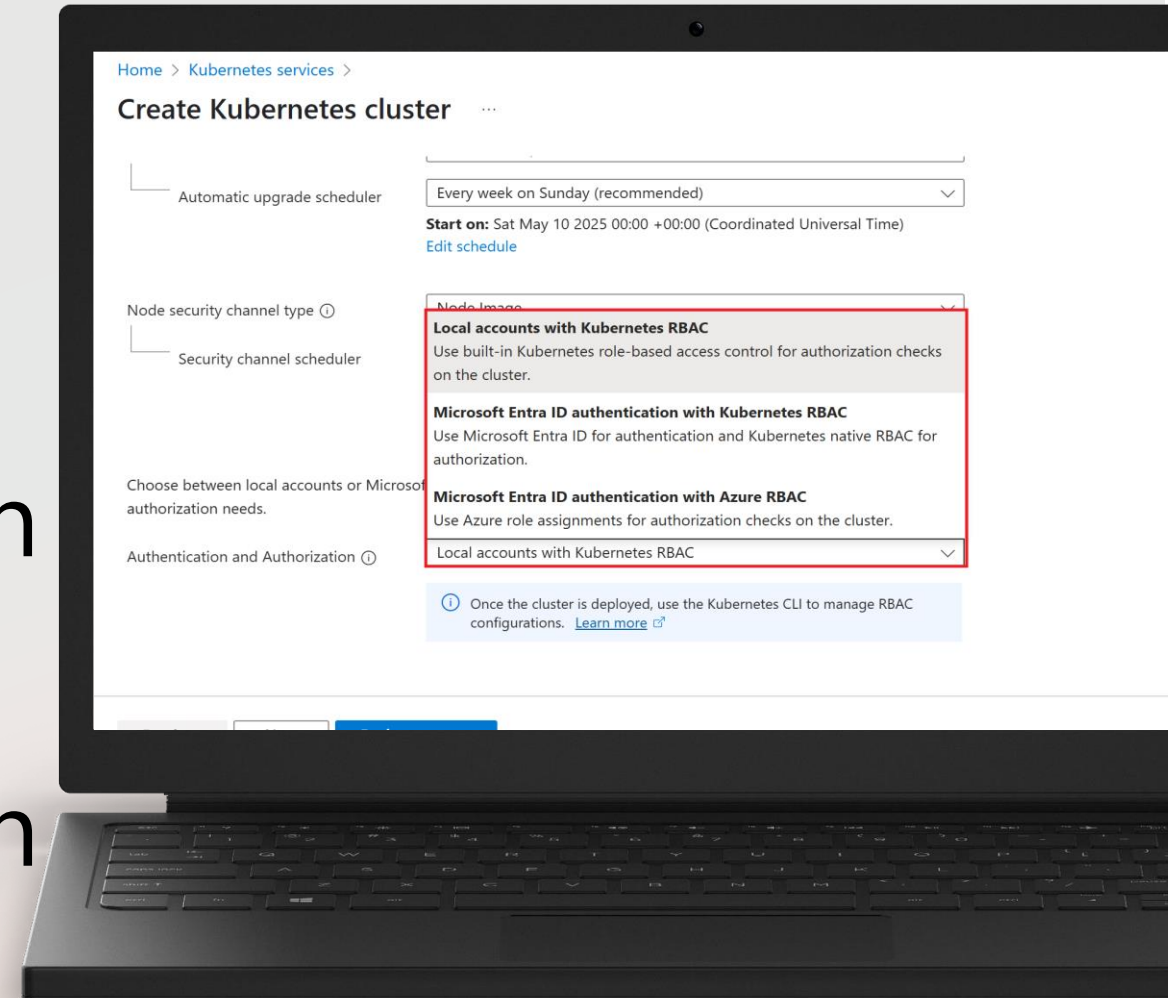
Authentication and Authorization

Authentication

Local Accounts with
Kubernetes RBAC

Entra ID Authentication with
Kubernetes RBAC

Entra ID Authentication with
Azure RBAC



Create Kubernetes cluster

✕

Automatic upgrade scheduler

Every week on Sunday (recommended) ▾

Start on: Sat May 10 2025 00:00 +00:00 (Coordinated Universal Time)
[Edit schedule](#)

Node security channel type ⓘ

Node Image ▾

Security channel scheduler

Choose between local accounts or Microsoft Entra ID for authentication and authorization needs.

Authentication and Authorization ⓘ

Local accounts with Kubernetes RBAC
Use built-in Kubernetes role-based access control for authorization checks on the cluster.

Microsoft Entra ID authentication with Kubernetes RBAC
Use Microsoft Entra ID for authentication and Kubernetes native RBAC for authorization.

Microsoft Entra ID authentication with Azure RBAC
Use Azure role assignments for authorization checks on the cluster.

Local accounts with Kubernetes RBAC ▾

ⓘ Once the cluster is deployed, use the Kubernetes CLI to manage RBAC configurations. [Learn more](#) ↗

Local Account with Kubernetes RBAC

Local Accounts K8s RBAC

Default authentication mode for AKS

No link between Microsoft Entra and AKS

Use K8s build-in authentication

Token is stored unencrypted in .kube config file

Local Accounts K8s RBAC

Only recommended when non of the users are in Entra

User management can become very challenging

Local accounts should be disabled for better security

```
apiVersion: v1
clusters:
- cluster:
  certificate-authority-data: LS0tLS1CR
  server: https://azurecloudnative-aks-
  name: AzureCloudNative-aks
contexts:
- context:
  cluster: AzureCloudNative-aks
  user: clusterUser_AzureCloudNative-rg_A
  name: AzureCloudNative-aks
current-context: AzureCloudNative-aks
kind: Config
preferences: {}
users:
- name: clusterUser_AzureCloudNative-rg_A
  user:
    client-certificate-data: LS0tLS1CRUdJ
    client-key-data: LS0tLS1CRUdJTjBSU0Eg
```

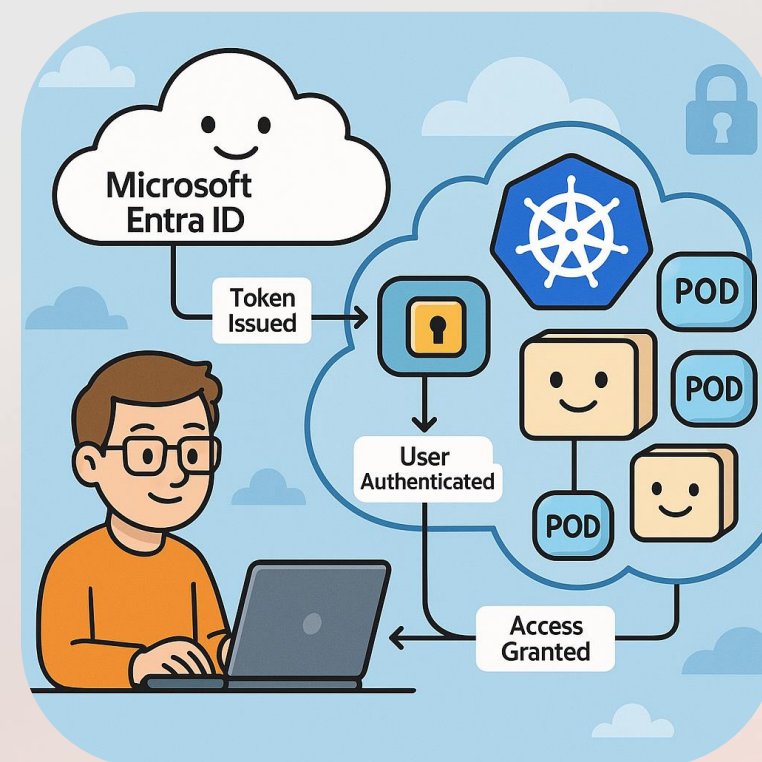
```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: LS0tLS1CRUdJTtIBDRVJUSUZJQ0FURS0tLS0tCk1JSUU2RENDQXRZDZ0
    server: https://azurecloudnative-aks-dns-537mjg6w.hcp.canadacentral1.azmk8s.io:443
  name: AzureCloudNative-aks
contexts:
- context:
    cluster: AzureCloudNative-aks
    user: clusterUser_AzureCloudNative-rg_AzureCloudNative-aks
  name: AzureCloudNative-aks
current-context: AzureCloudNative-aks
kind: Config
preferences: {}
users:
- name: clusterUser_AzureCloudNative-rg_AzureCloudNative-aks
  user:
    client-certificate-data: LS0tLS1CRUdJTtIBDRVJUSUZJQ0FURS0tLS0tCk1JSUZIakNDQXdhZ0F3SU
    client-key-data: LS0tLS1CRUdJTtIBSU0EgUFJJVkJFURSBLRVktLS0tLQpNSU1KSndJQkFBS0NBZ0VBN
```

Entra ID Authentication with Kubernetes RBAC

Entra ID with K8s RBAC

Authentication via Microsoft Entra

Authorization via K8s RBAC



Entra ID with K8s RBAC

Admin creates role bindings between K8s role and Entra user or group

Entra user or group needs "Azure Kubernetes Cluster User" role to download .kube config

Entra ID with K8s RBAC

Easier user management
than local accounts

Choose this option to
have a “portable” cluster

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: reader
  namespace: read
rules:
- apiGroups: [""]
  resources: ["pods", "services", "endpoints", "persistentvolumeclaims"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["apps"]
  resources: ["deployments", "daemonsets", "replicasets", "statefulsets"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["batch"]
  resources: ["jobs", "cronjobs"]
  verbs: ["get", "list", "watch"]
- apiGroups: ["extensions"]
  resources: ["ingresses"]
```

Entra ID with K8s RBAC

Auditing access to the cluster can be cumbersome

Access can be given to Entra users and groups

Management with Entra IDs

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: reader-user-binding
  namespace: read
subjects:
- kind: Group
  name: 24975d09-19e9-47a5-aa3b-e952c693c016 # Entra ID
  namespace: read
roleRef:
  kind: Role # or ClusterRole
  name: reader
  apiGroup: rbac.authorization.k8s.io
```

kind: Role

apiVersion: rbac.authorization.k8s.io/v1

metadata:

name: reader

namespace: read

rules:

- apiGroups: [""]

- resources: ["pods", "services", "endpoints", "persistentvolumeclaims",

- verbs: ["get", "list", "watch"]

- apiGroups: ["apps"]

- resources: ["deployments", "daemonsets", "replicasets", "statefulsets"]

- verbs: ["get", "list", "watch"]

- apiGroups: ["batch"]

- resources: ["jobs", "cronjobs"]

- verbs: ["get", "list", "watch"]

- apiGroups: ["extensions"]

- resources: ["ingresses"]


```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: reader-user-binding
  namespace: read
subjects:
  - kind: Group
    name: 24975d09-19e9-47a5-aa3b-e952c693c016 # Entra ID
    namespace: read
roleRef:
  kind: Role # or ClusterRole
  name: reader
  apiGroup: rbac.authorization.k8s.io
```

Entra ID with K8s RBAC

```
PS C:\Demo> kubectl get all -n read
```

NAME	READY	STATUS	RESTARTS	AGE
pod/nginx	1/1	Running	0	4m32s

```
Error from server (Forbidden): replicationcontrollers is forbidden: User "demo.user@programmingwithwolfgang.com" cannot list resource "replicationcontrollers" in API group "" in the namespace "read"
```

```
Error from server (Forbidden): horizontalpodautoscalers.autoscaling is forbidden: User "demo.user@programmingwithwolfgang.com" cannot list resource "horizontalpodautoscalers" in API group "autoscaling" in the namespace "read"
```

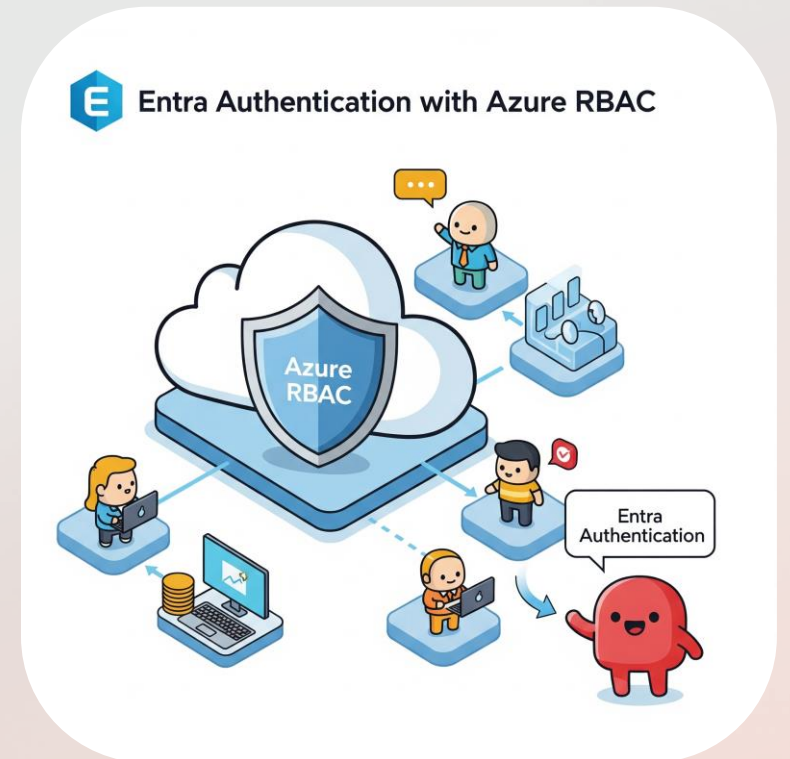
Entra ID Authentication with Azure RBAC

Entra Authentication with Azure RBAC

Manage access to the cluster with Azure only

Use Azure RBAC roles to manage permissions inside AKS

Recommended way to manage AKS cluster

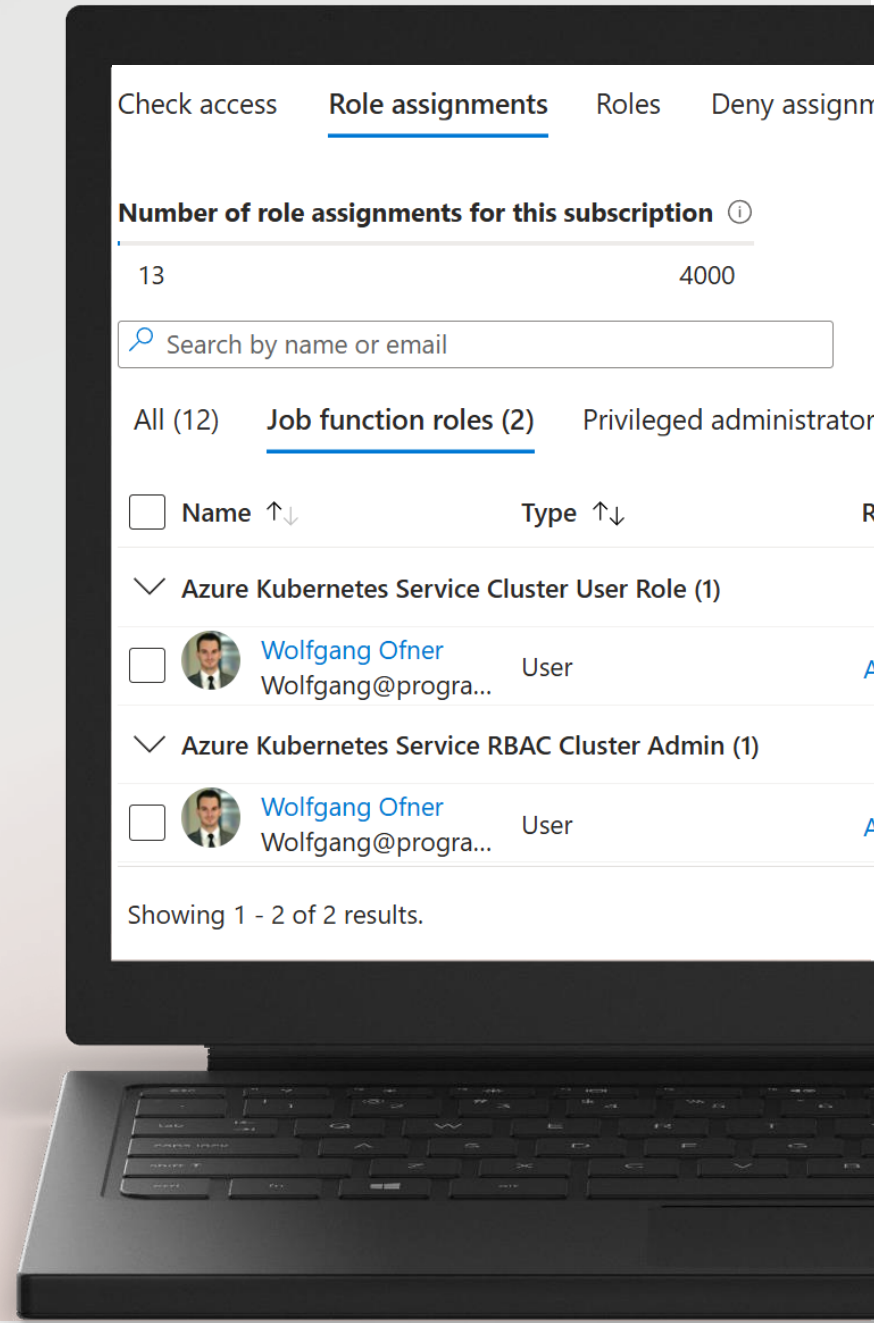


Entra Authentication with Azure RBAC

"Azure Kubernetes Service Cluster User Role" to download config

Assign built-in or custom roles

Namespace specific permissions can only be assigned via Azure CLI



Entra Workload Identity

Entra Workload Identity

Azure resource can have identities

Always use identities over username and password

AKS identity is not assigned to the pods



Entra Workload Identity

Entra Workload Identity gives a pod an identity

- Pods can access Azure resources with this identity
- `azure.workload.identity/use=true` label needed on pod
- OIDC Issuer must be enabled for the AKS cluster



Kubelet



AKS workload



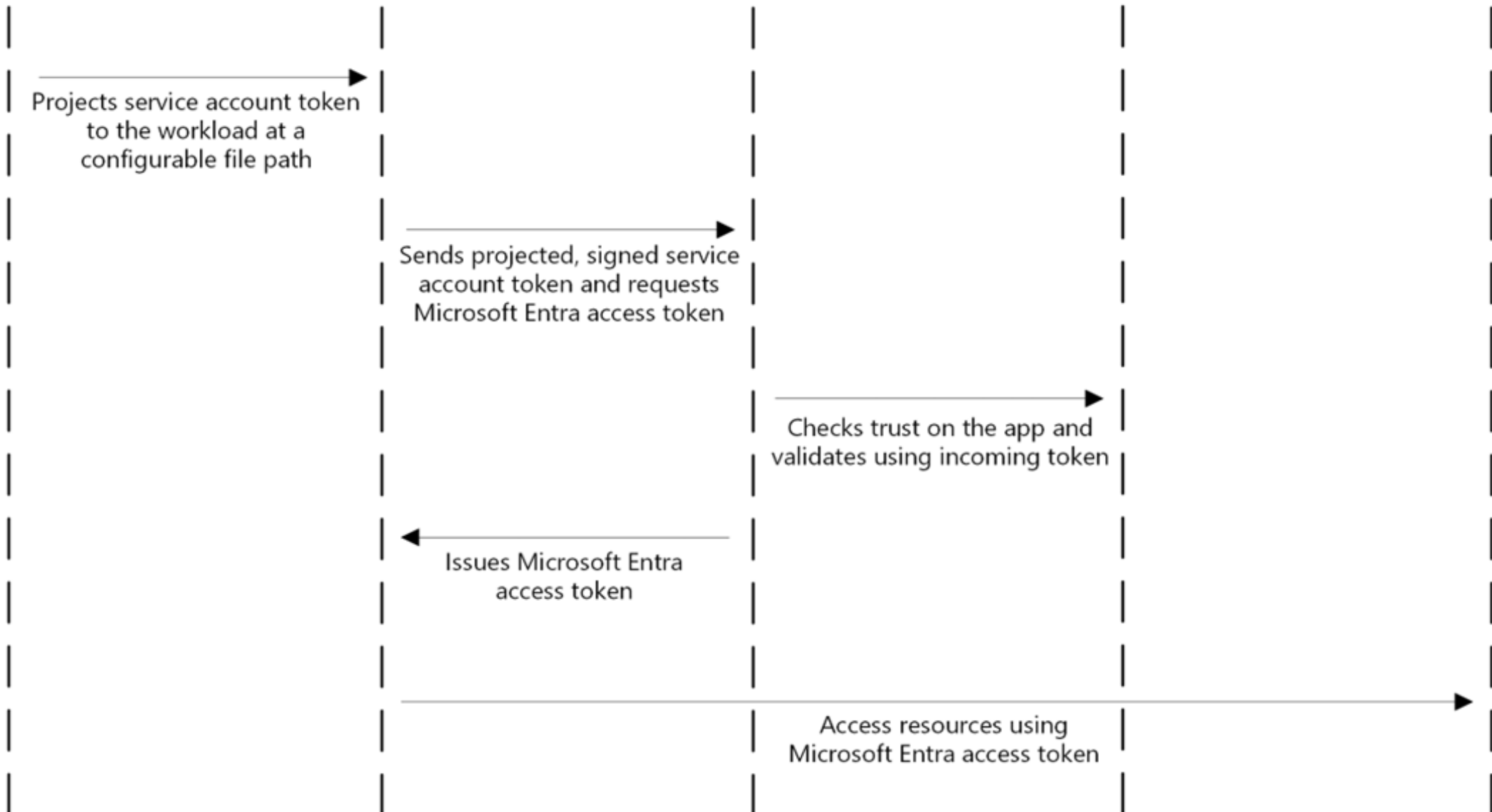
Microsoft Entra ID



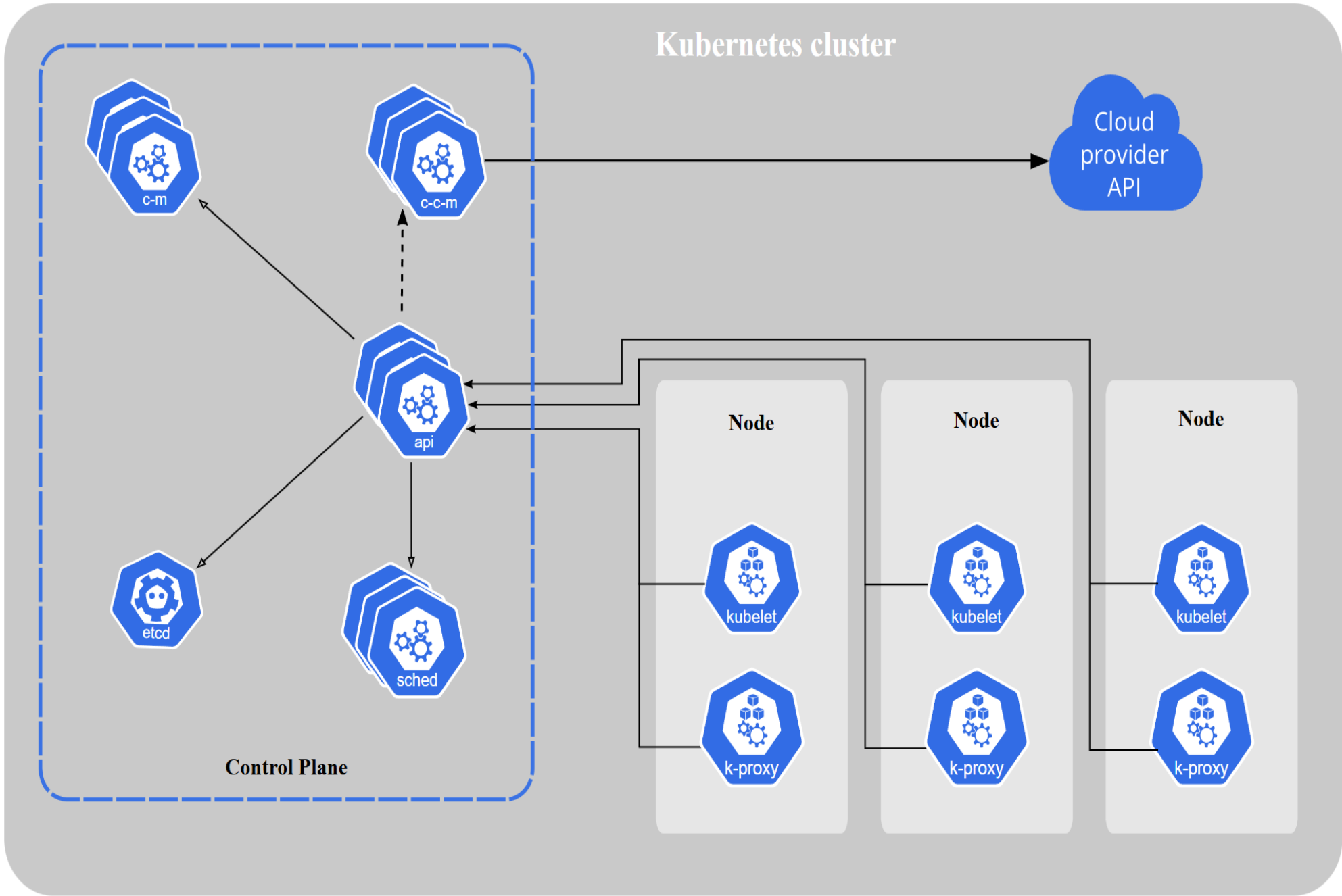
OpenID Discovery Document












Azure resources



Private AKS Cluster

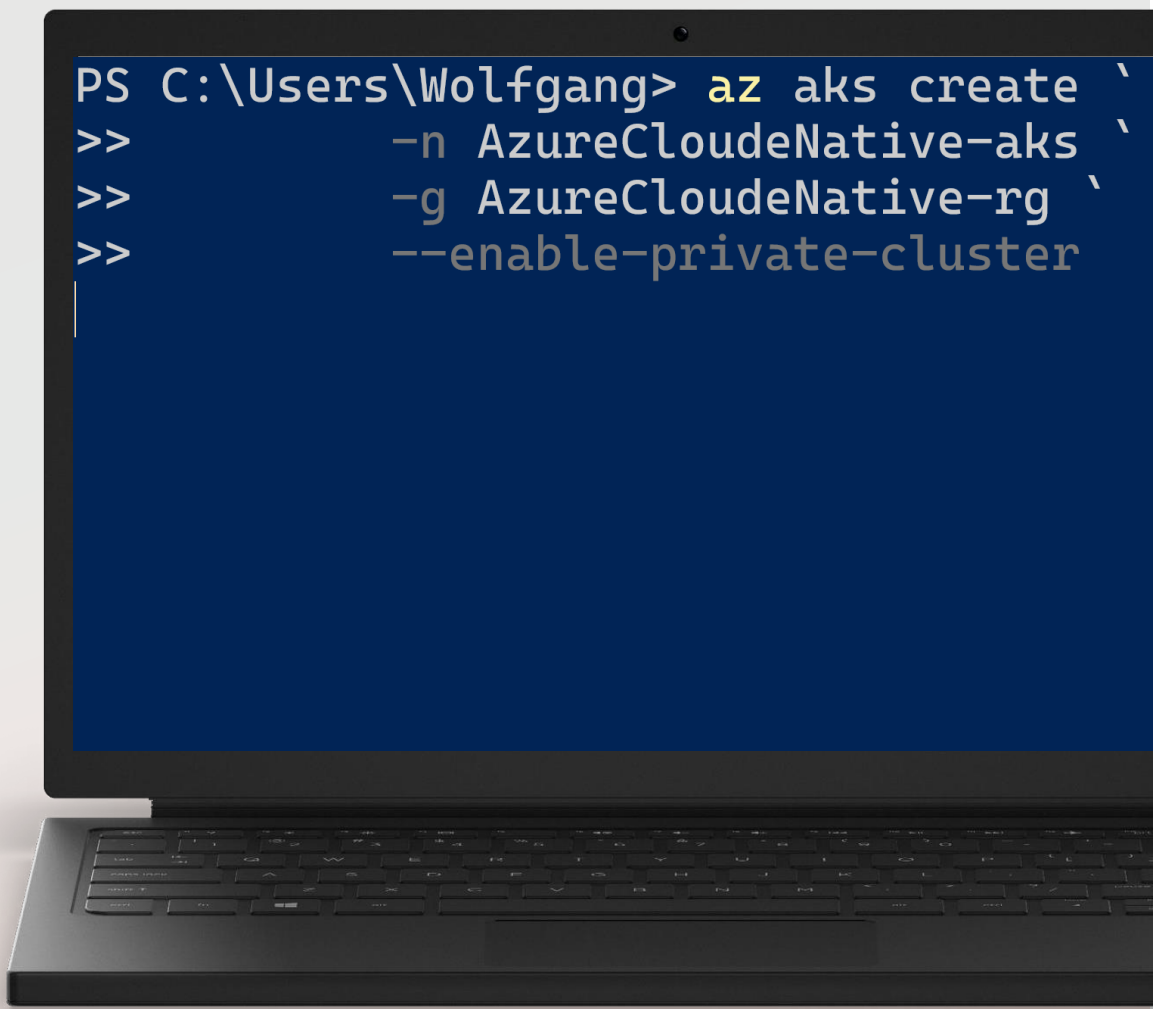


- API server**  api
- Cloud controller manager (optional)**  c-c-m
- Controller manager**  c-m
- etcd (persistence store)**  etcd
- kubelet**  kubelet
- kube-proxy**  k-proxy
- Scheduler**  sched
- Control plane** 
- Node** 

Private AKS Cluster

Disable public access to API

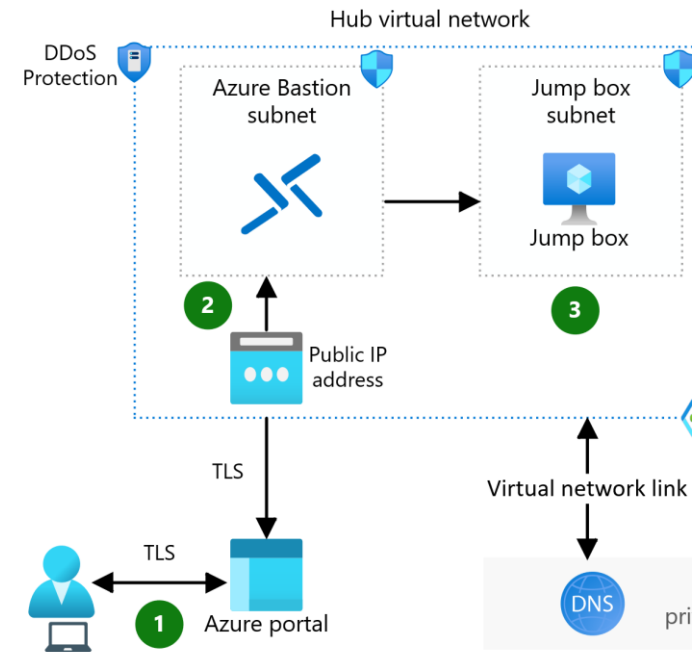
Communication between
Worker and Master nodes
over a private connection

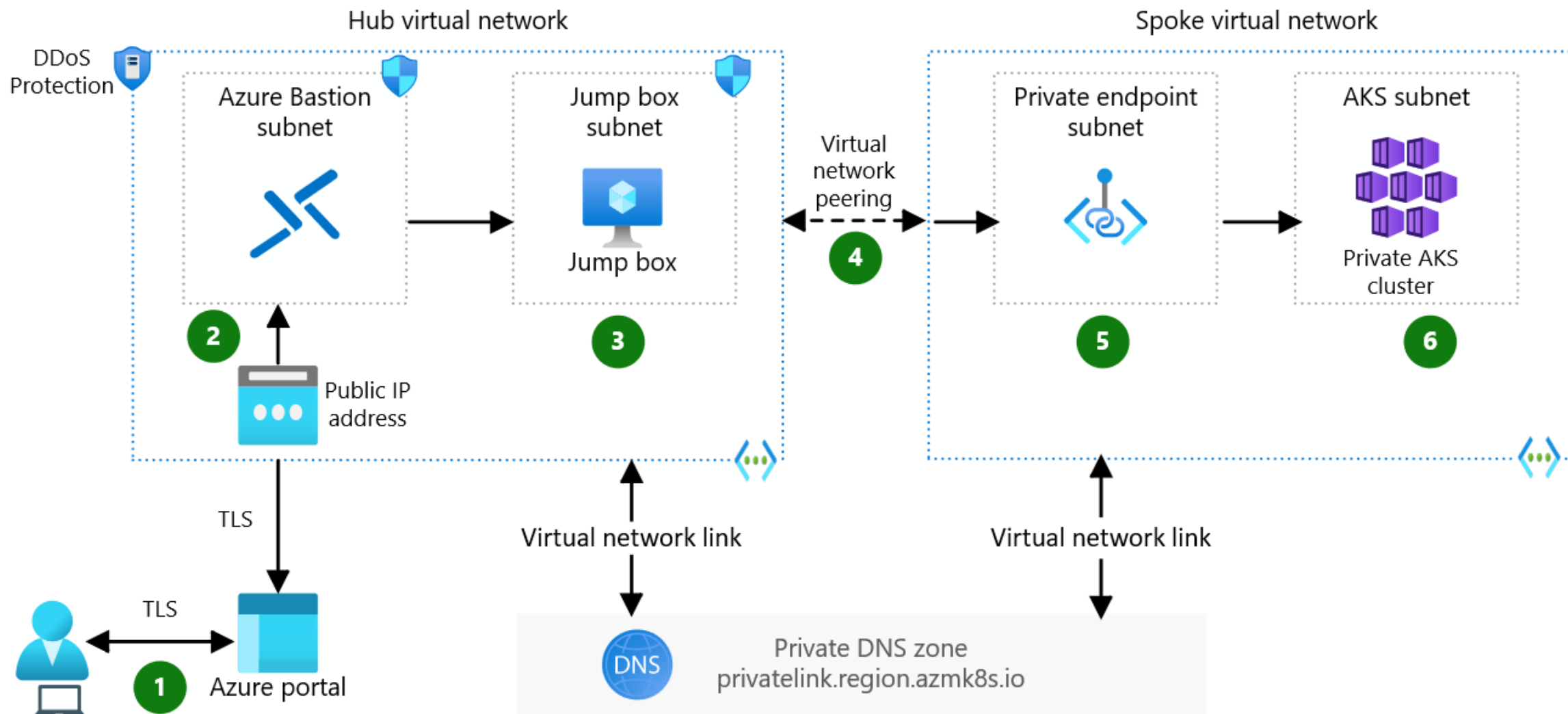


```
PS C:\Users\Wolfgang> az aks create `
>>     -n AzureCloudNative-aks `
>>     -g AzureCloudNative-rg `
>>     --enable-private-cluster
```

Private AKS Cluster

Use Azure Bastion and a Jump box



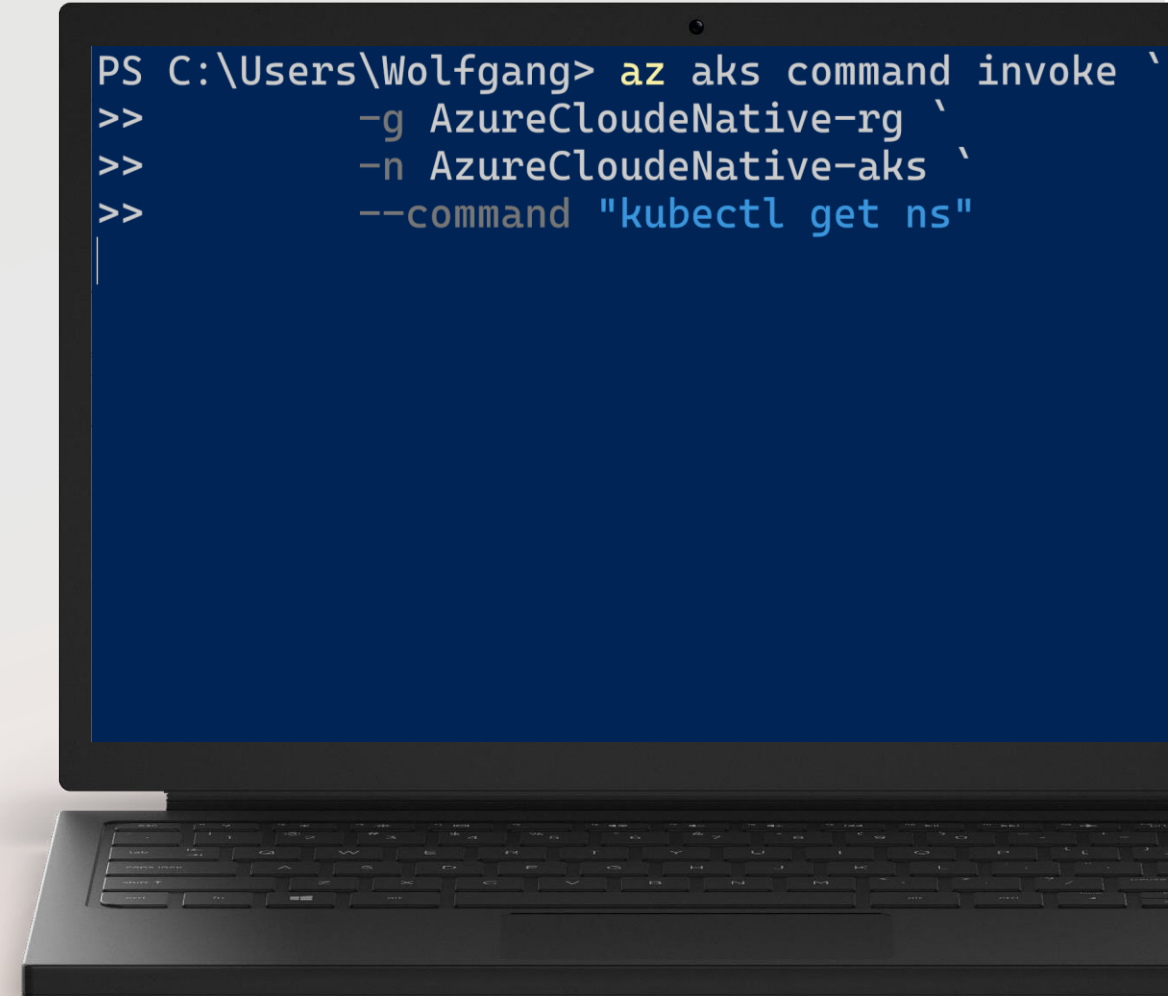


Private AKS Cluster

Use Azure Bastion and a
Jump box

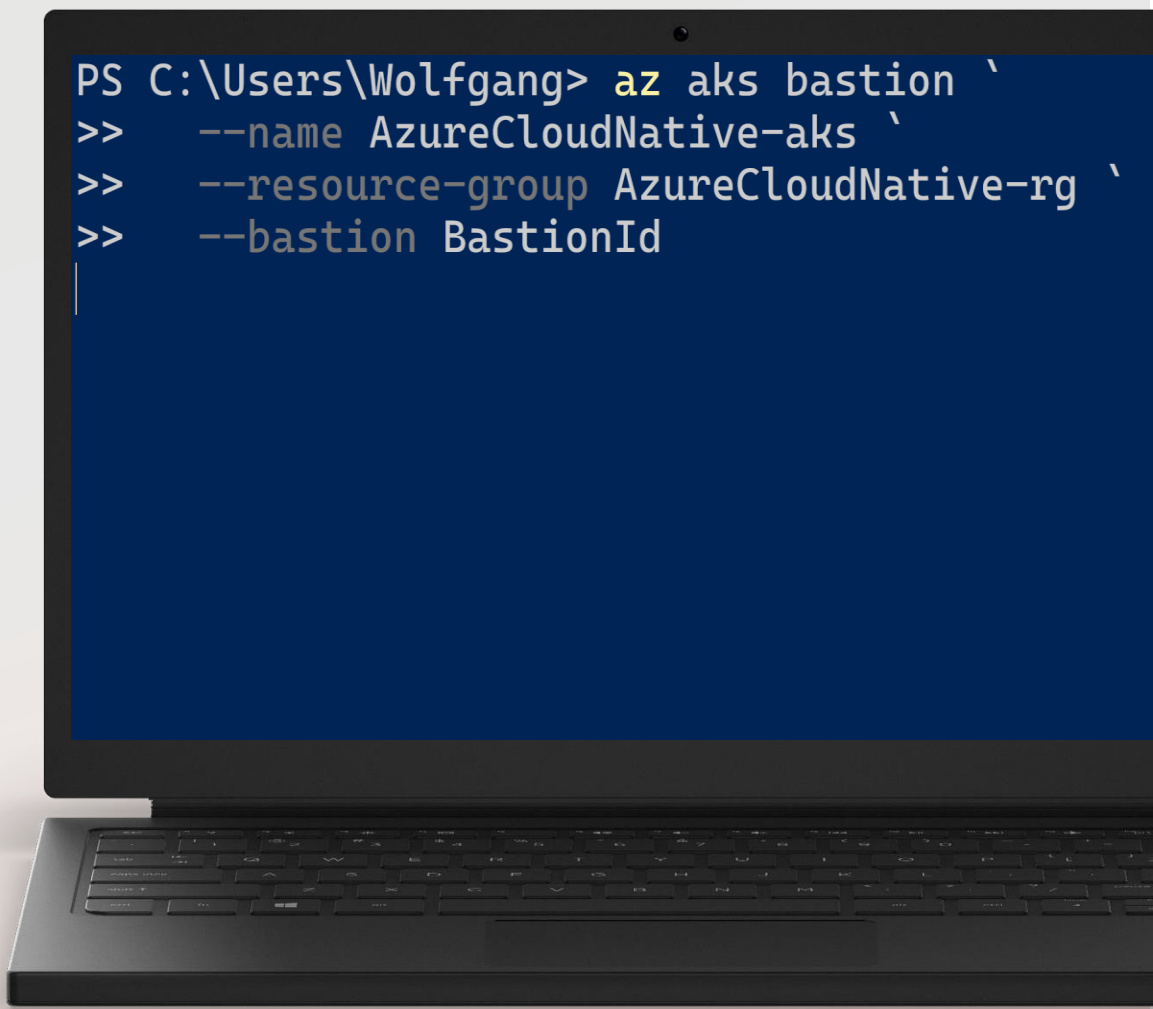
Wrap command with
"az aks command invoke"
command

VPN/ExpressRoute
connection

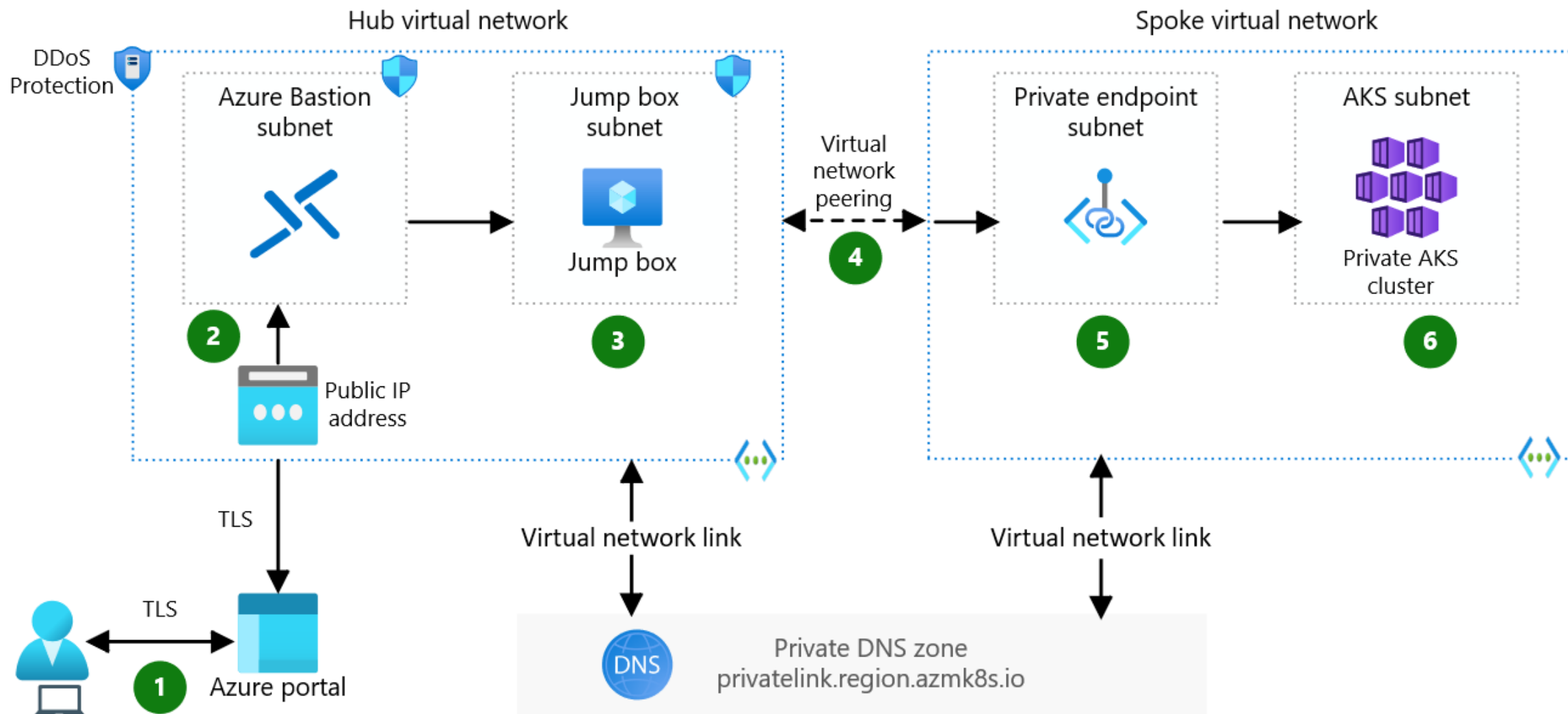


Private AKS Cluster

New feature to access AKS
through Azure Bastion



```
PS C:\Users\Wolfgang> az aks bastion `
>>   --name AzureCloudNative-aks `
>>   --resource-group AzureCloudNative-rg `
>>   --bastion BastionId
|
```

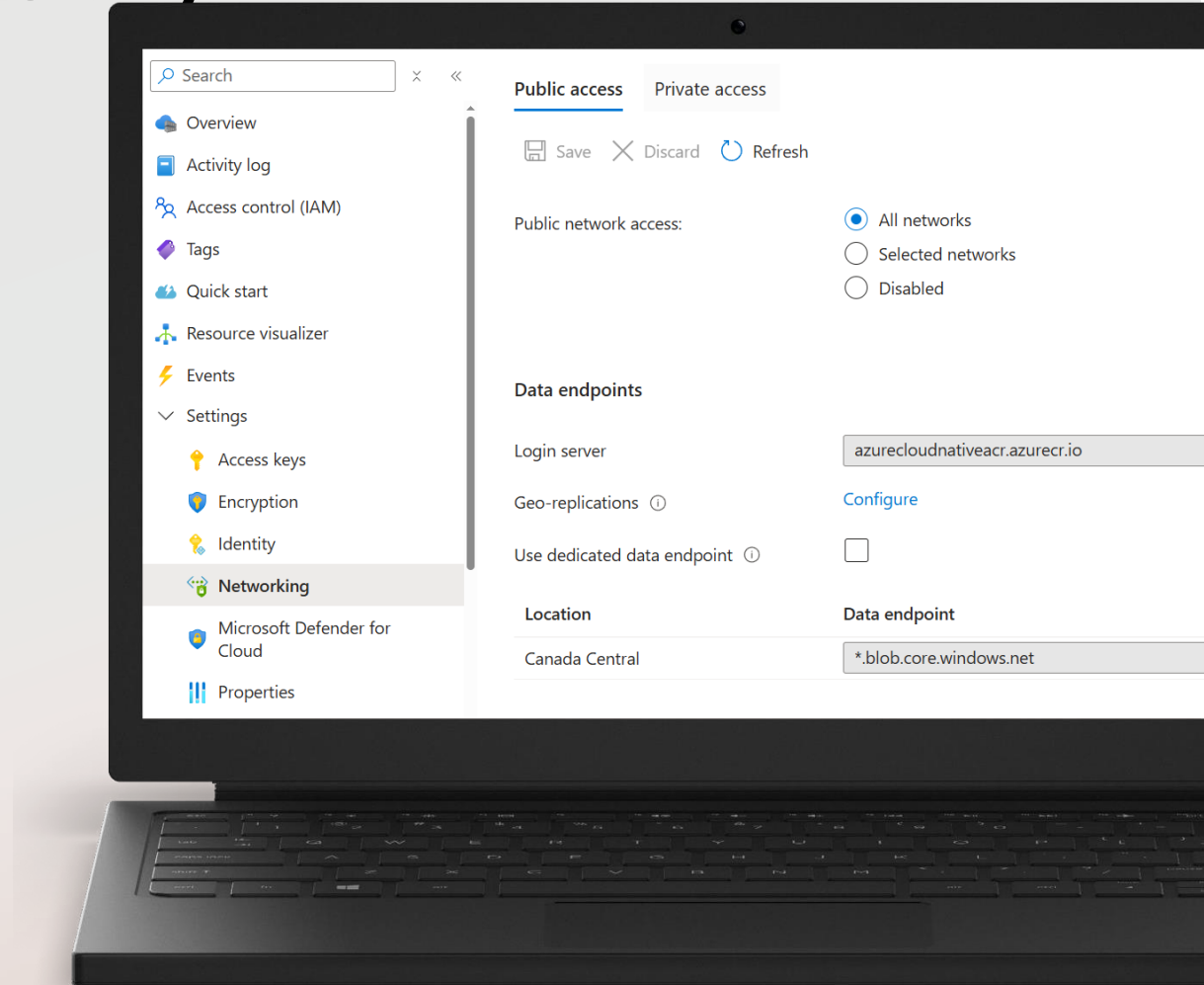
Private Azure Container Registry

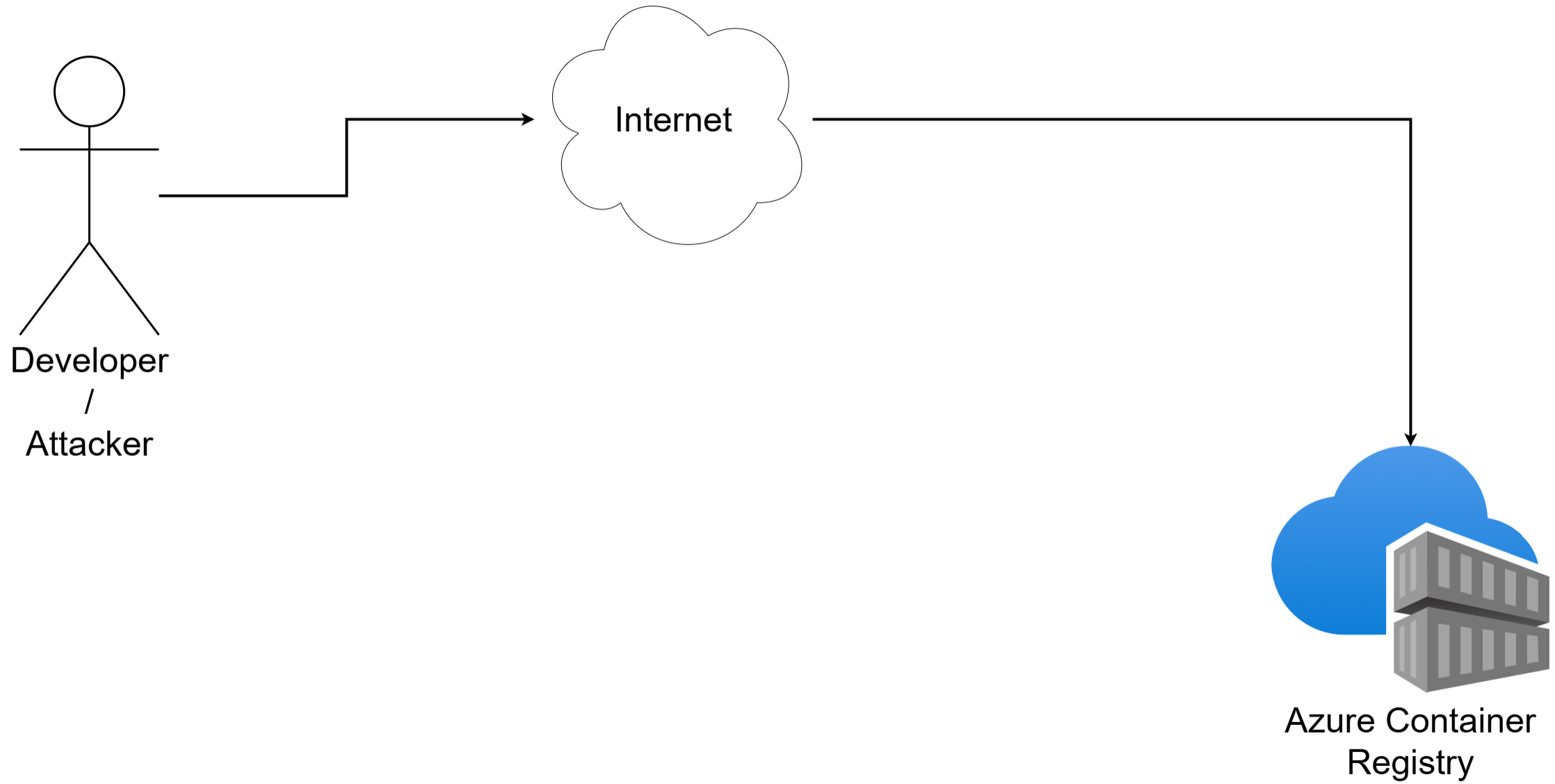
Azure Container Registry

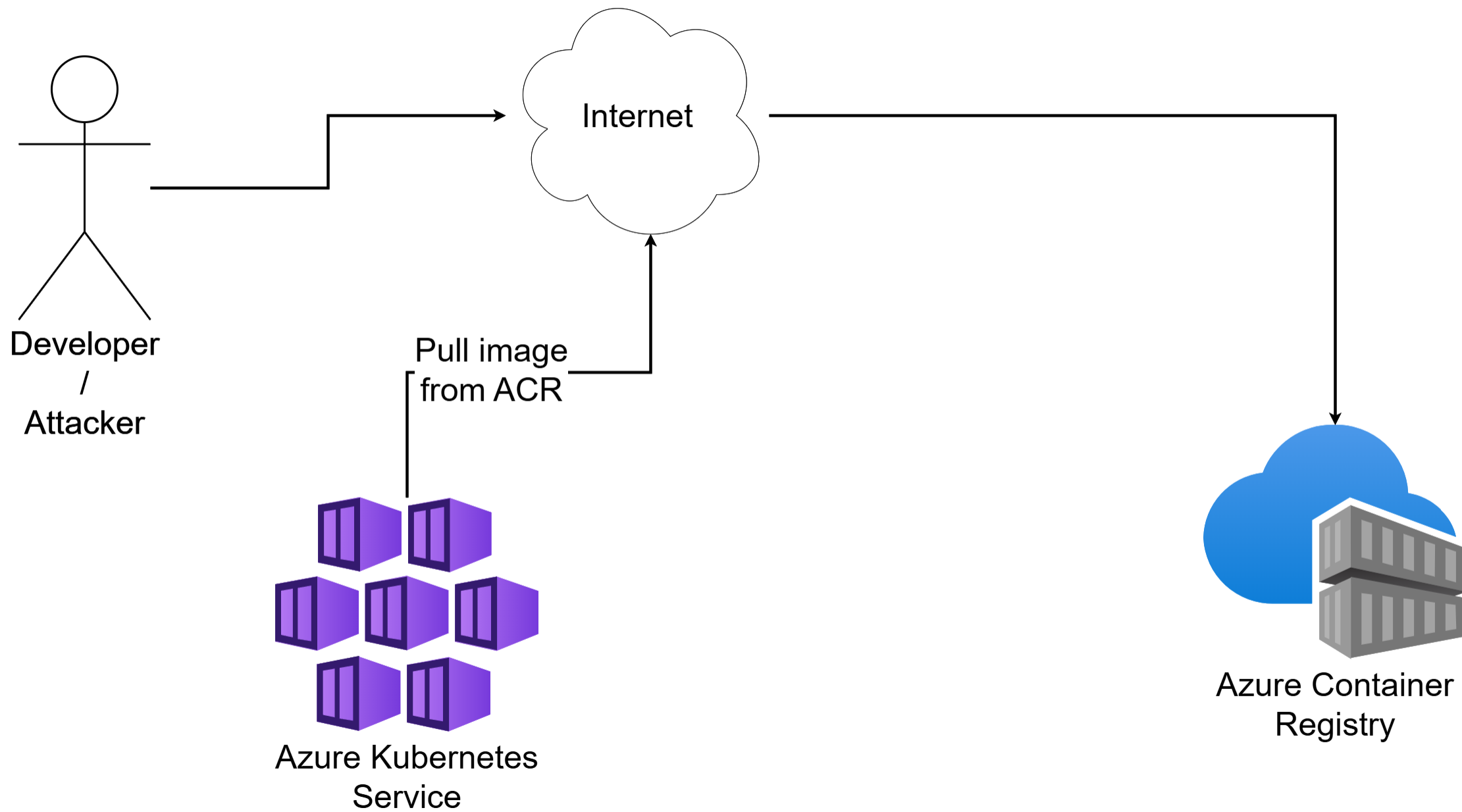
Store images in private registry

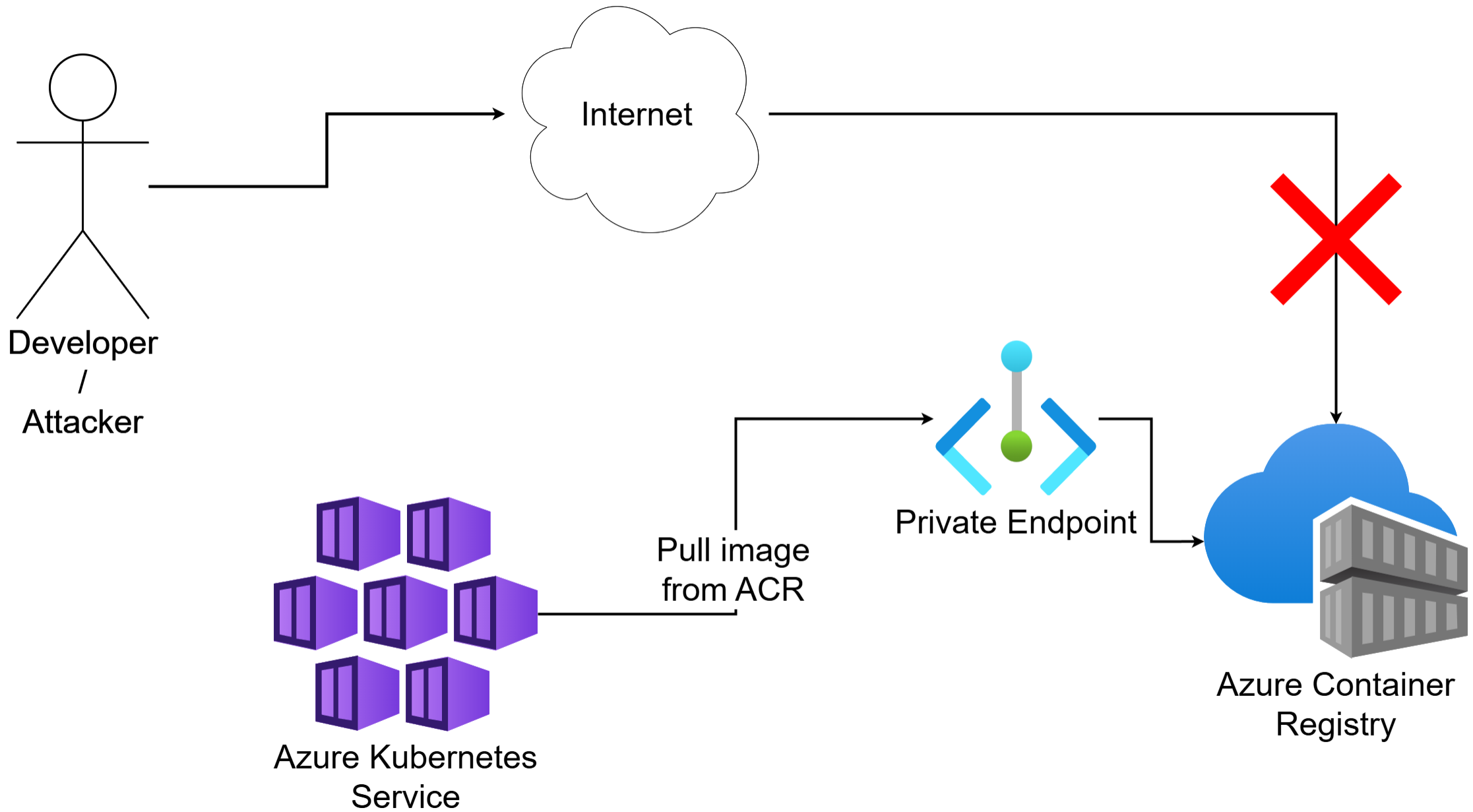
Keep everything private

AKS should download images over private connection









Azure Container Registry

No changes for pull operation necessary

Private DNS-Zone resolves
public FQDN

Build agent needs to push
images over private endpoint



Azure Key Vault Provider for Secrets Store CSI Driver

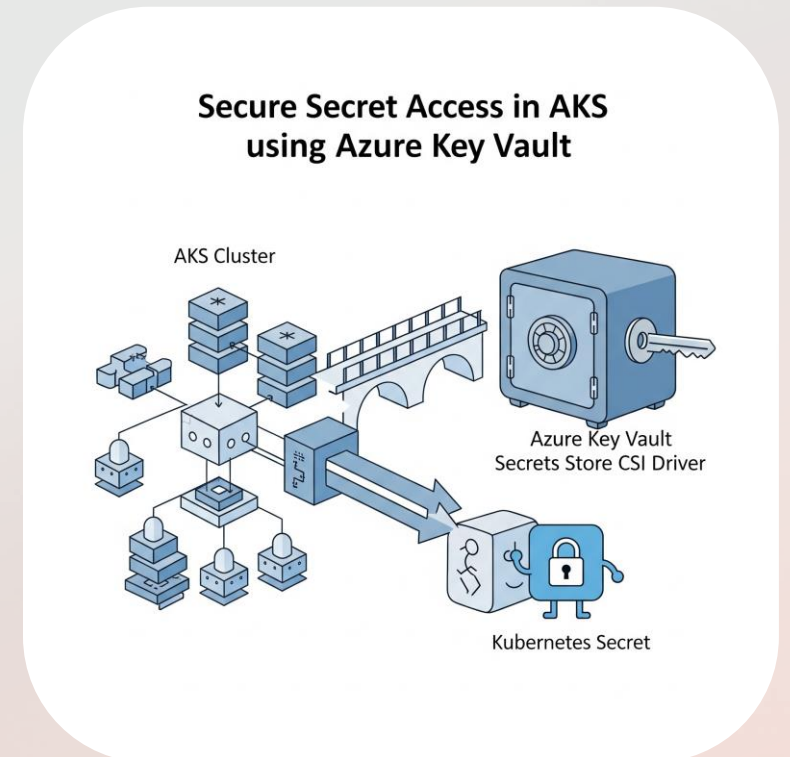
KV Secrets Store Provider

Mount secrets, keys, and certificates to pods

Auto-rotate secrets

Sync Azure Key Vault with Kubernetes secrets

Separation of concerns



Further Security Topics

Further Security Topics

Use Azure Linux as your node OS

Disable SSH access

Disable local accounts

Install the Azure Policy addon

Microsoft Defender for Containers

Setup your cluster using AKS Automatic

Further Security Topics

Only run signed images

Validate image integrity

Limit the pod privileges

Set the security context

Reduce the pod capabilities

Configure seccom (secure computing)

Thank you for watching!

Remember to leave your questions and rate the presentation in the section below.



THE H@CK
SUMMIT

A lecture selected by a Program Council consisting of recognized leaders in the field of cybersecurity.

Warsaw,
13.10.2025 - 14.10.2025



OFFICIAL LECTURE OF THE HACK SUMMIT

ACADEMIC PARTNERS