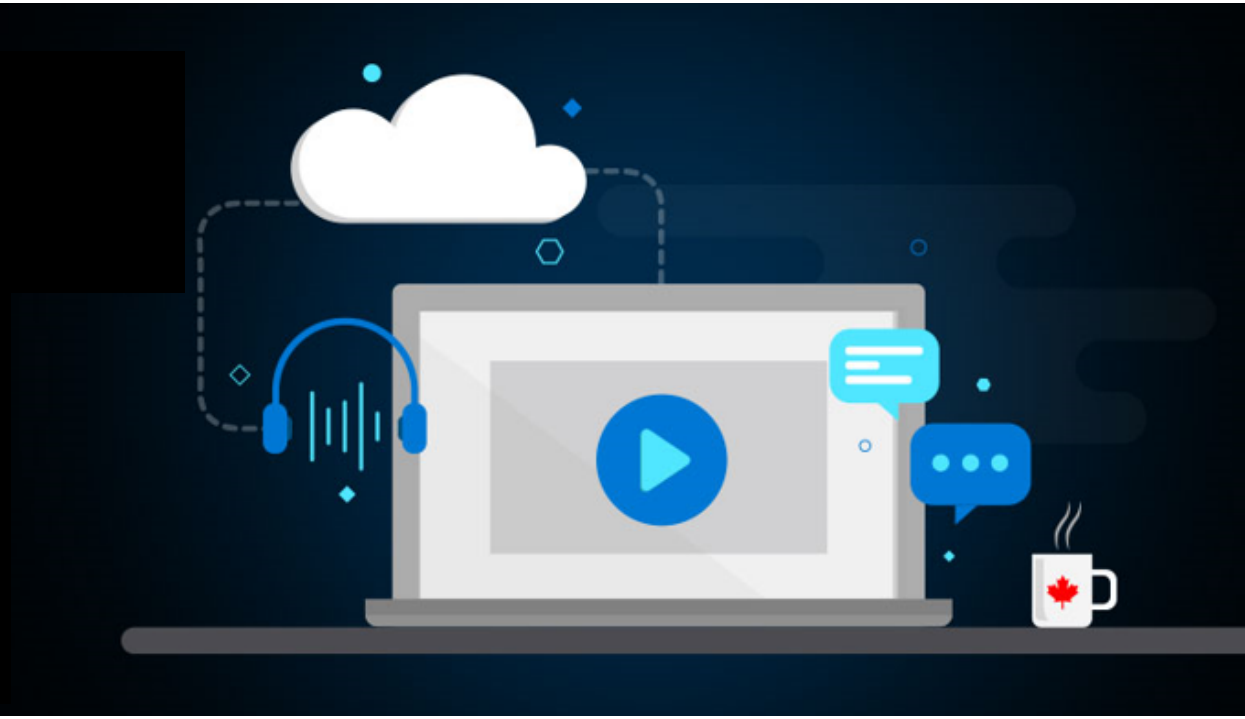
Microsoft

Série numérique
infonuagique Microsoft

Apprenez à votre rythme sur les sujets abordés incluent l'IA, analytiques, l'Internet des objets, la modernisation, la sécurité et encore plus, tous propulsé par le nuage.

www.aka.ms/CloudDigitalSeries



Webinaire: **10 bonnes pratiques pour sécuriser un cluster AKS**

Présentateur: Maxime Coquerel

Microsoft Azure

Développez et déployez
dans le nuage informatique { }

10 bonnes pratiques pour sécuriser un cluster AKS

Le 4 mars 2020 | De 13h à 14h, heure de l'Est

Maxime Coquerel

Microsoft MVP – Azure
Director Cloud Security Architect

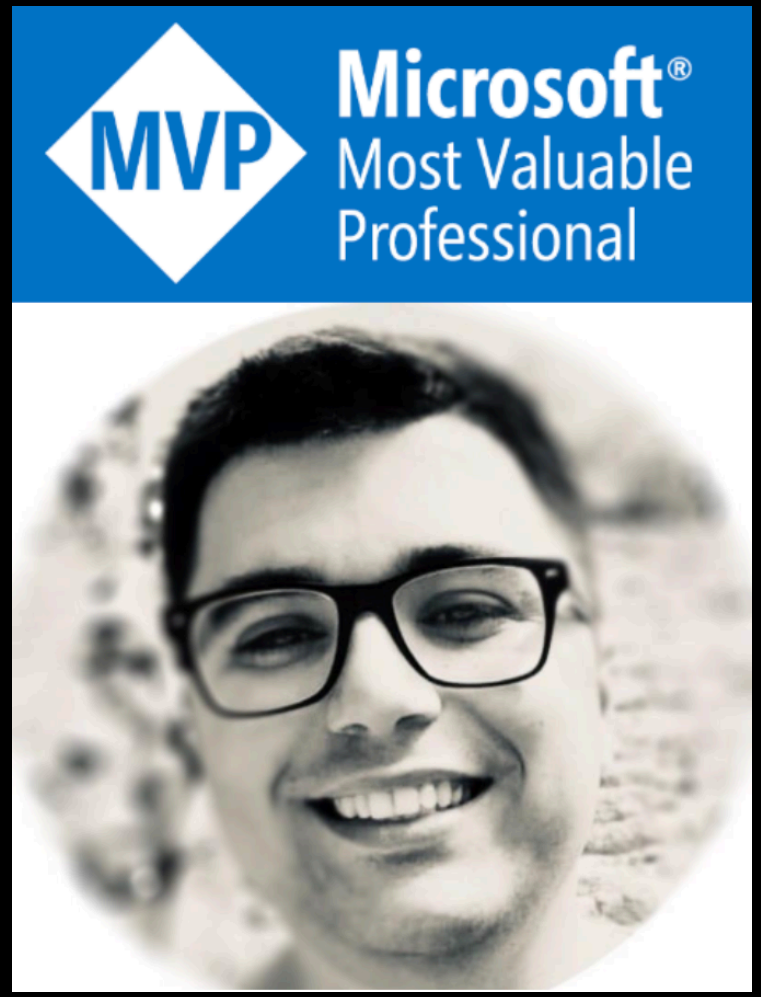
Email : max.coquerel@live.fr

Blog : zigmax.net (since 2012)

Github : https://github.com/zigmax

Twitter : @zig_max

Open Source Contributeur (Kubernetes / VSCode)

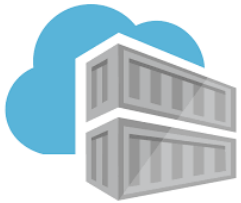


Introduction

Introduction / Glossaire

- **AKS** : Azure Kubernetes Service

- **ACR** : Azure Container Registry

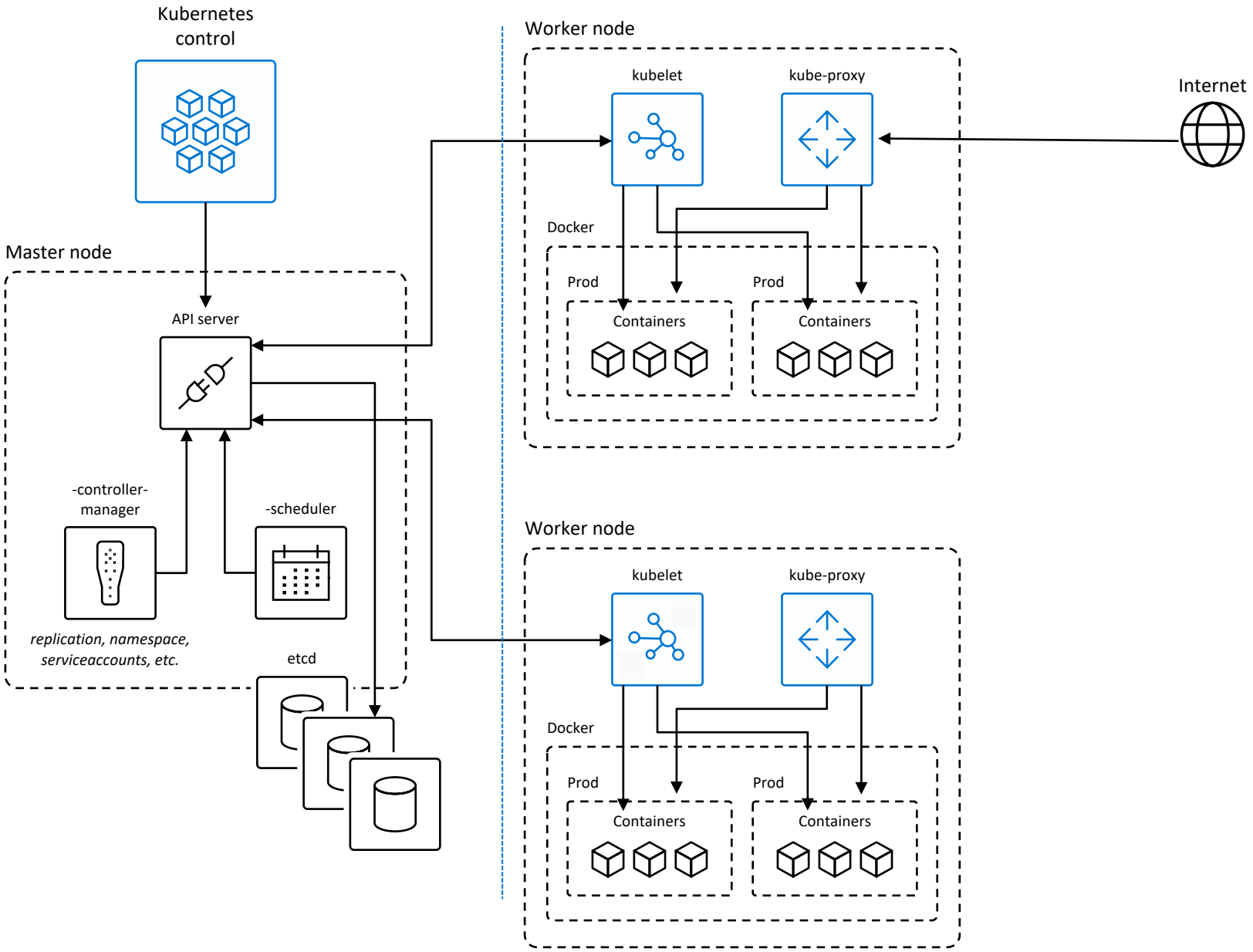


- **AKV** : Azure Key Vault

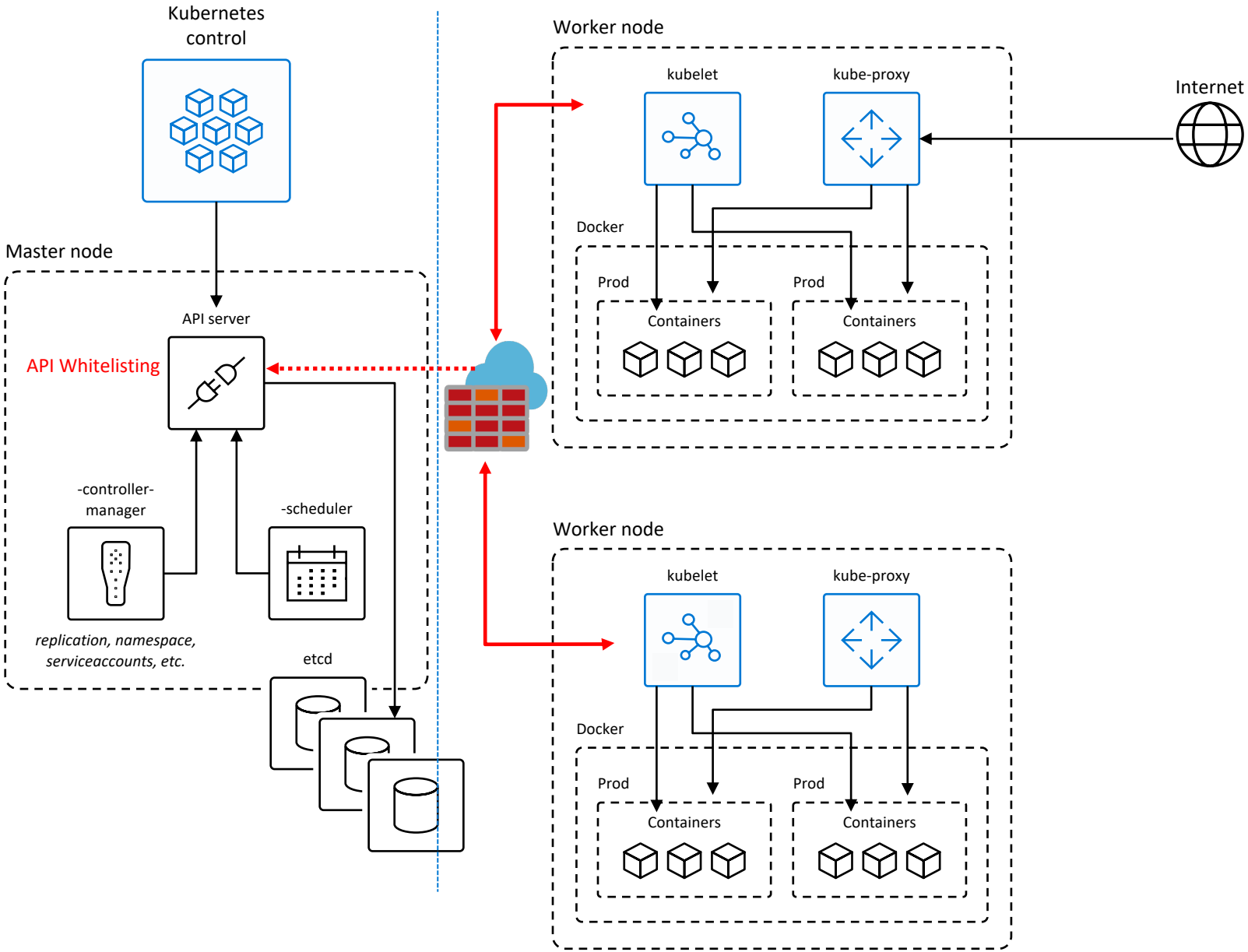
- **Docker**
- **Node ou Worker Node**
- **Pod**
- **API Serveur**
- **Ingress Controller**

Architecture

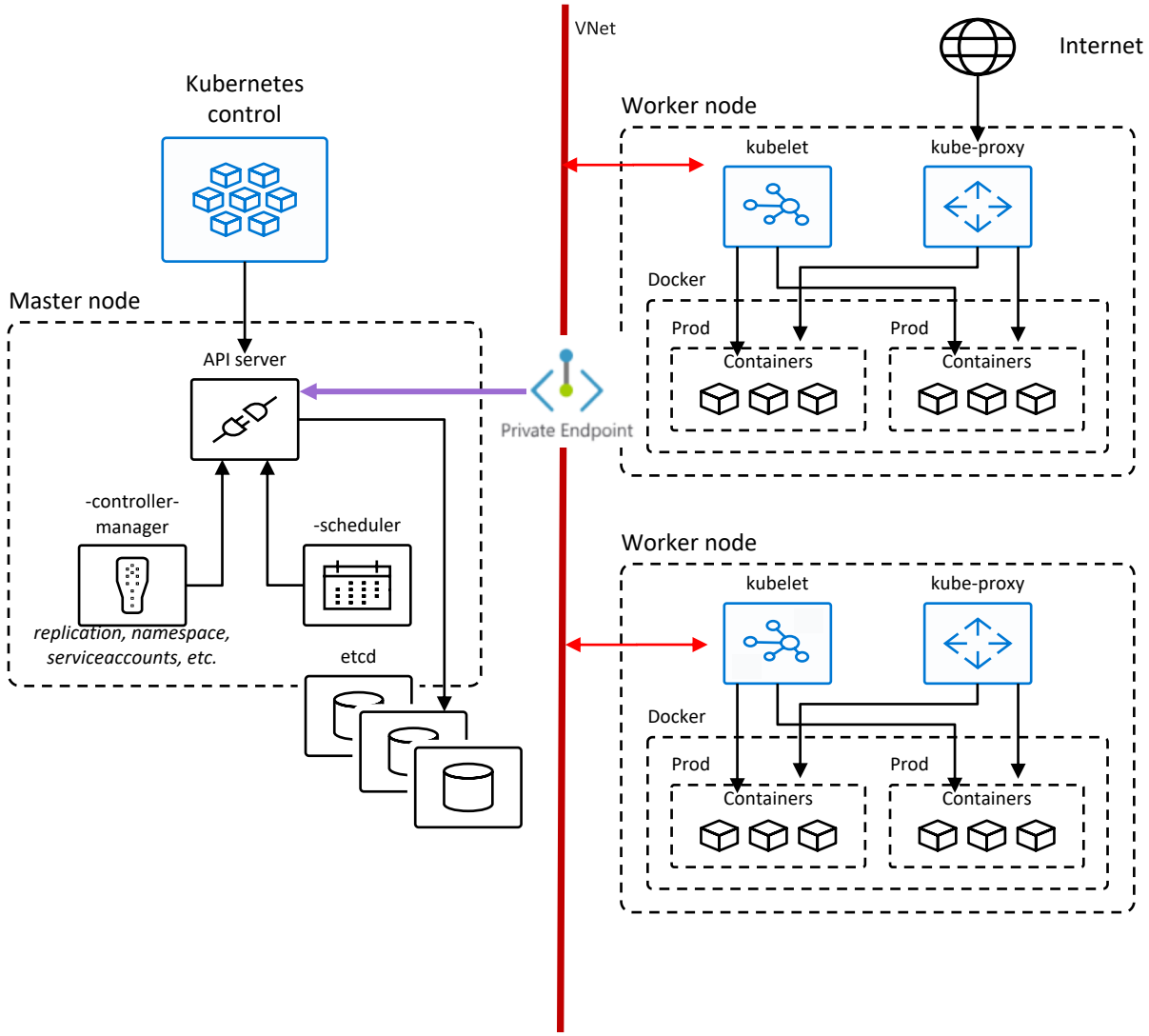
Azure Kubernetes Service (AKS) - Architecture



#1 - Restreindre l’accès à API Server de votre cluster AKS



#2 - Azure Kubernetes Service (AKS) – Private Cluster



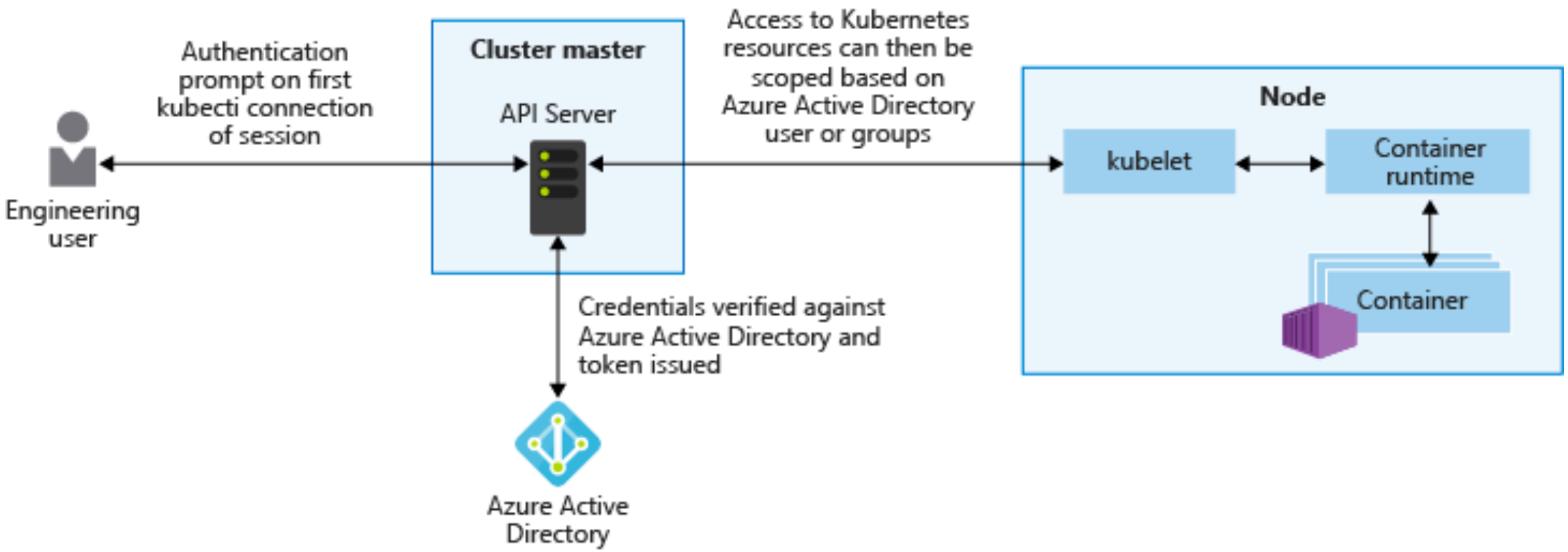

```
az aks create \
    --resource-group $RG_NAME \
    --name $CLUSTER_NAME \
    --load-balancer-sku standard \
    --enable-private-cluster \
    -- ...
```

Azure AKS Private Cluster:

- West US
- West US 2
- East US 2
- **Canada Central**
- North Europe
- West Europe
- Australia East

AKS Cluster

#3 - Azure Kubernetes Services (AKS) – RBAC



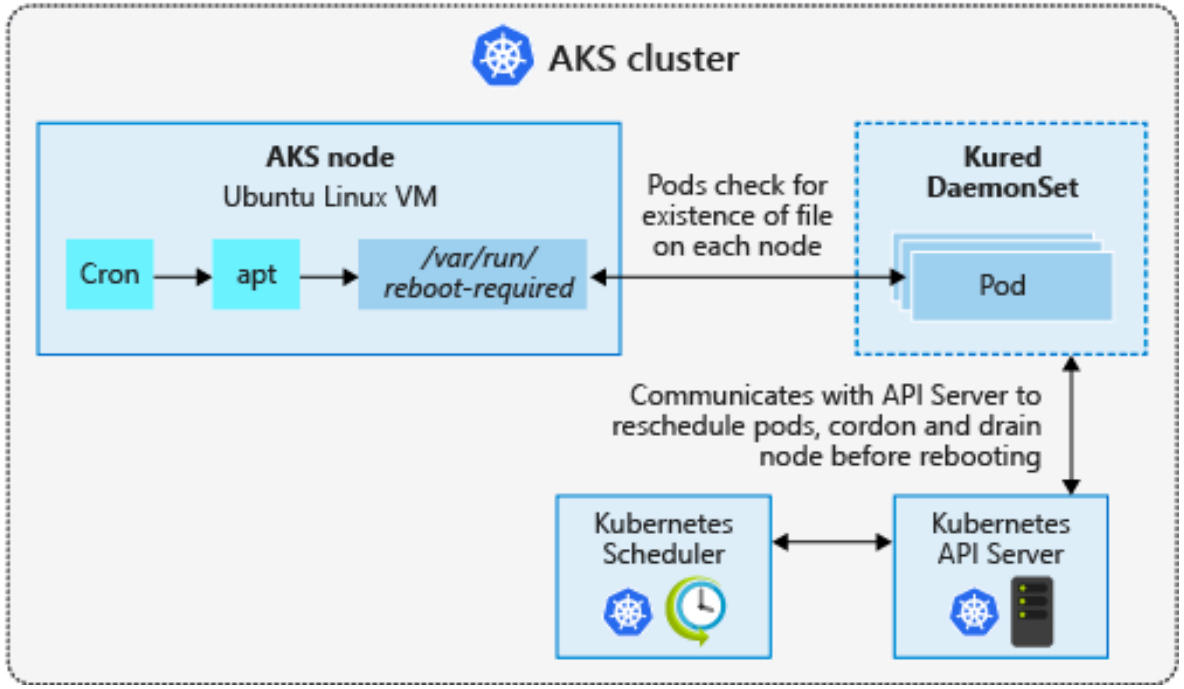
#4 - Planifier les mises à jour de vos clusters AKS

- Kubernetes Reboot Daemon (**KURED**)

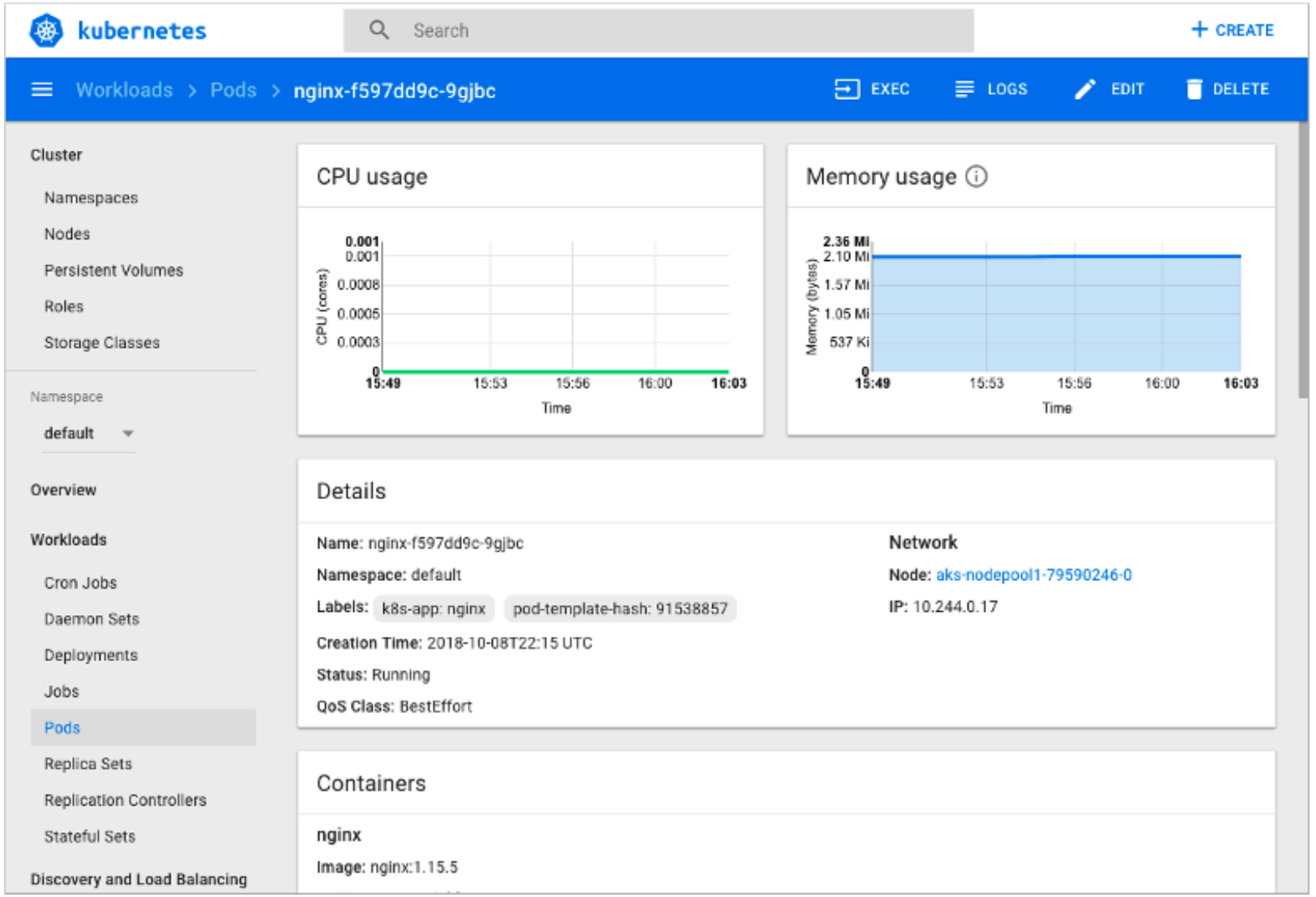
- Microsoft est responsable de déployer les mises à jour de sécurité sur vos nodes, **mais vous avez la responsabilité de redémarrer vos nodes afin que les mises à jour soient appliquées.**

- Quand une mise à jour est installée et que celle-ci nécessite un redémarrage, un fichier « **/var/run/reboot-required** » est créé sur chaque node de votre cluster.

- Dans un second temps, le daemon Kured va vérifier l'existence de ce fichier (par défaut chaque 60 min) et redémarrer chaque node l'un après l'autre, après avoir déplacé les pods sur un autre node de votre cluster.



#5 - Désactiver le dashboard de votre cluster AKS



az aks disable-addons -a kube-dashboard --resource-group Nom_RG --name Nom_AKS_Cluster

Kubernetes Pods

#6 – Sécuriser les Pods de votre cluster!

- **POD Security Policy (PSP)**

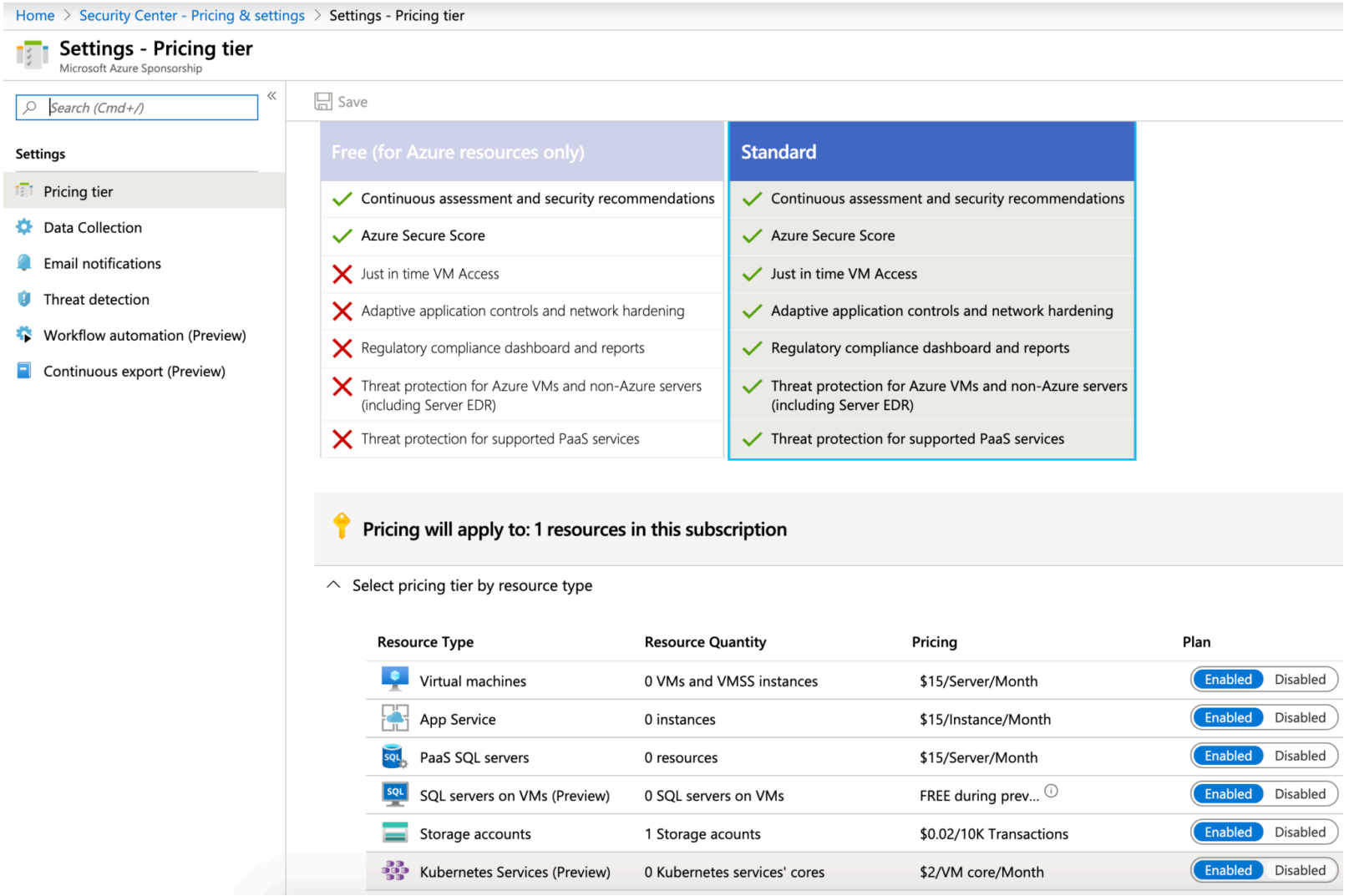
```
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: default
spec:
  hostNetwork: false
  privileged: false
  runAsUser:
    rule: RunAsAny
  fsGroup:
    rule: RunAsAny
  supplementalGroups:
    rule: RunAsAny
  seLinux:
    rule: RunAsAny
```

```
az aks update \
    --resource-group myResourceGroup \
    --name myAKSCluster \
    --enable-pod-security-policy
```

Control Aspect	Field Names
Running of privileged containers	privileged
Usage of root namespaces	hostPID, hostIPC
Usage of host networking and ports	hostNetwork, hostPorts
Usage of volume types	volumes
Usage of the host filesystem	allowedHostPaths
White list of FlexVolume drivers	allowedFlexVolumes
Allocating an FSGroup that owns the pod's volumes	fsGroup

Azure Security Center

#7 - Détecter les menaces de vos clusters AKS avec Azure Security Center !



PREVIEW - Privileged container detected

Filter

Attacked Resource	Count	Activity time	Environme...	State	Severity
AKSDEMOMAX	1	11/22/19, 02:51 PM	Azure	Active	Low

PREVIEW - Privileged container detected

AKSDEMOMAX

Learn more

General information

DESCRIPTION	Kubernetes audit log analysis detected a new privileged container. A privileged container has access to the node's resources and breaks the isolation between containers. If compromised, an attacker can use the privileged container to gain access to the node.
ACTIVITY TIME	Friday, November 22, 2019, 2:51:54 PM
SEVERITY	Low
STATE	Active
ATTACKED RESOURCE	AKSDEMOMAX
SUBSCRIPTION	Microsoft Azure Sponsorship (7db5e03c-f3c2-48b1-b326-aa53faaaafc3)
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Kubernetes Service

... > Security alerts > PREVIEW - Privileged container detected > PREVIEW - Privileged container detected

PREVIEW - Privileged container detected

AKSDEMOMAX

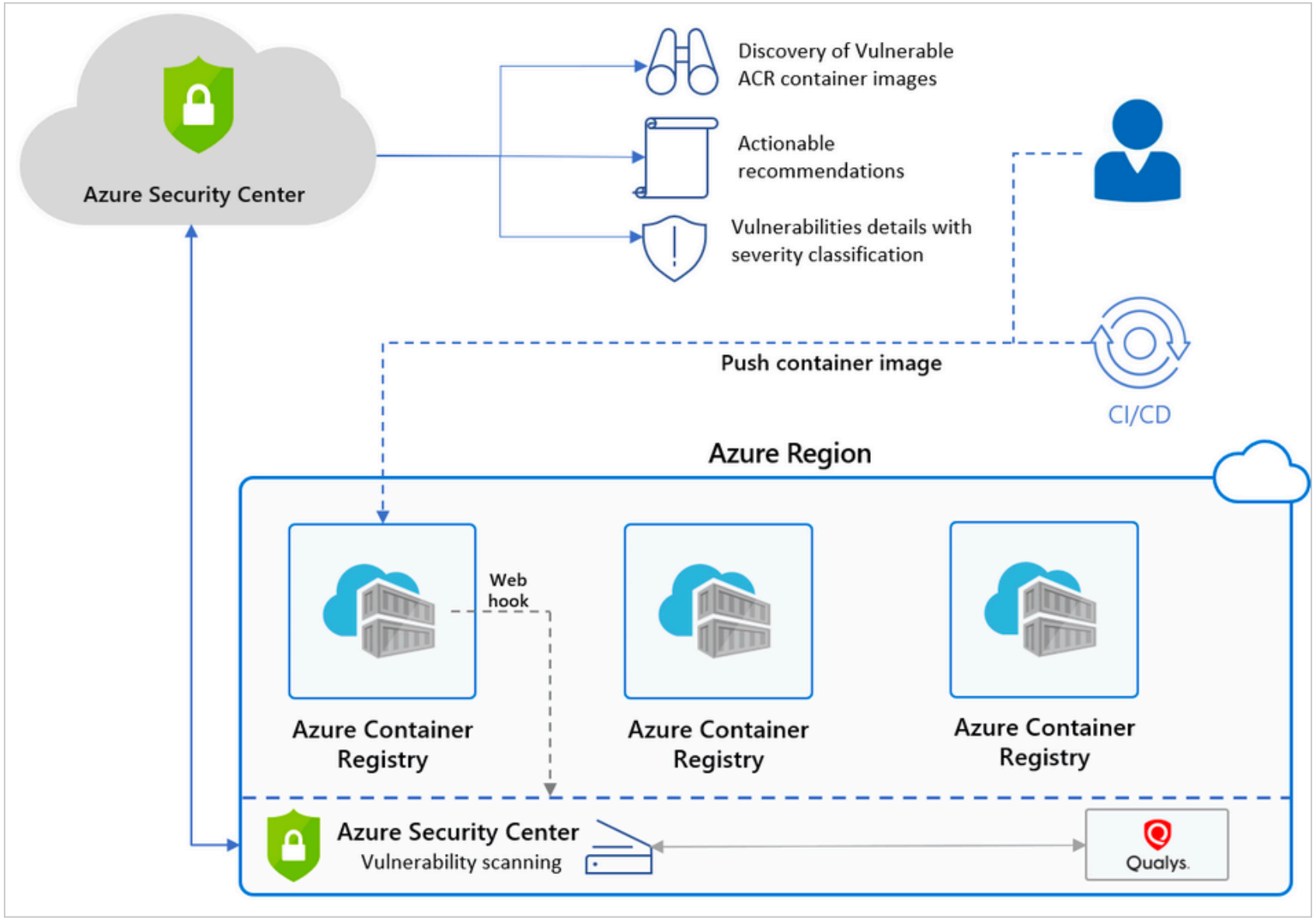
Learn more

DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure
RESOURCE TYPE	Kubernetes Service
CONTAINER NAME	nsenter
CONTAINER IMAGE	alexeiled/nsenter:2.34
NAMESPACE	default
POD NAME	maxime-nsenter-aks-nodepool1-29366245-vmss000000

Remediation steps

REMEDIATION STEPS	Find the container in the alert details. If the container doesn't need to run in privileged mode, remove the privileges from the container. If the container is not legitimate, escalate the alert to the information security team.

8 - Scanner les images de vos containers avec Azure Security Center



acrmaxi

Container registry security health

Resource health

acrmaxi

Total recommendations

1

Recommendations summary

High	1
Medium	0
Low	0

Container registry information

Resource Name	acrmaxi
Resource Group	acrmaxime
Subscription	Microsoft Azure Sponsorship
Login server	acrmaxi.azurecr.io
Repository count	2
Image count	2

Recommendation list

Recommendations (1) | Passed assessments (0) | Unavailable assessments (0)

Recommendation	Status
Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) (Preview)	High

Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) (Preview)

Unhealthy registries
1 / 1

Severity
High

Total vulnerabilities
32

Vulnerabilities by severity

High	3
Medium	29
Low	0

Registries with most vulnerabilities

acrmaxi	32

Total vulnerable images
1
Out of 1

Description

Container image vulnerability assessment scans your registry for security vulnerabilities on each pushed container image and exposes detailed findings for each image. Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks (powered by Qualys).

General Information

User impact	Low
Implementation effort	Moderate

LEARN MORE
Learn more about recommendations
Learn how to disable the recommendation

Threats

Remediation steps

Security Checks

Findings

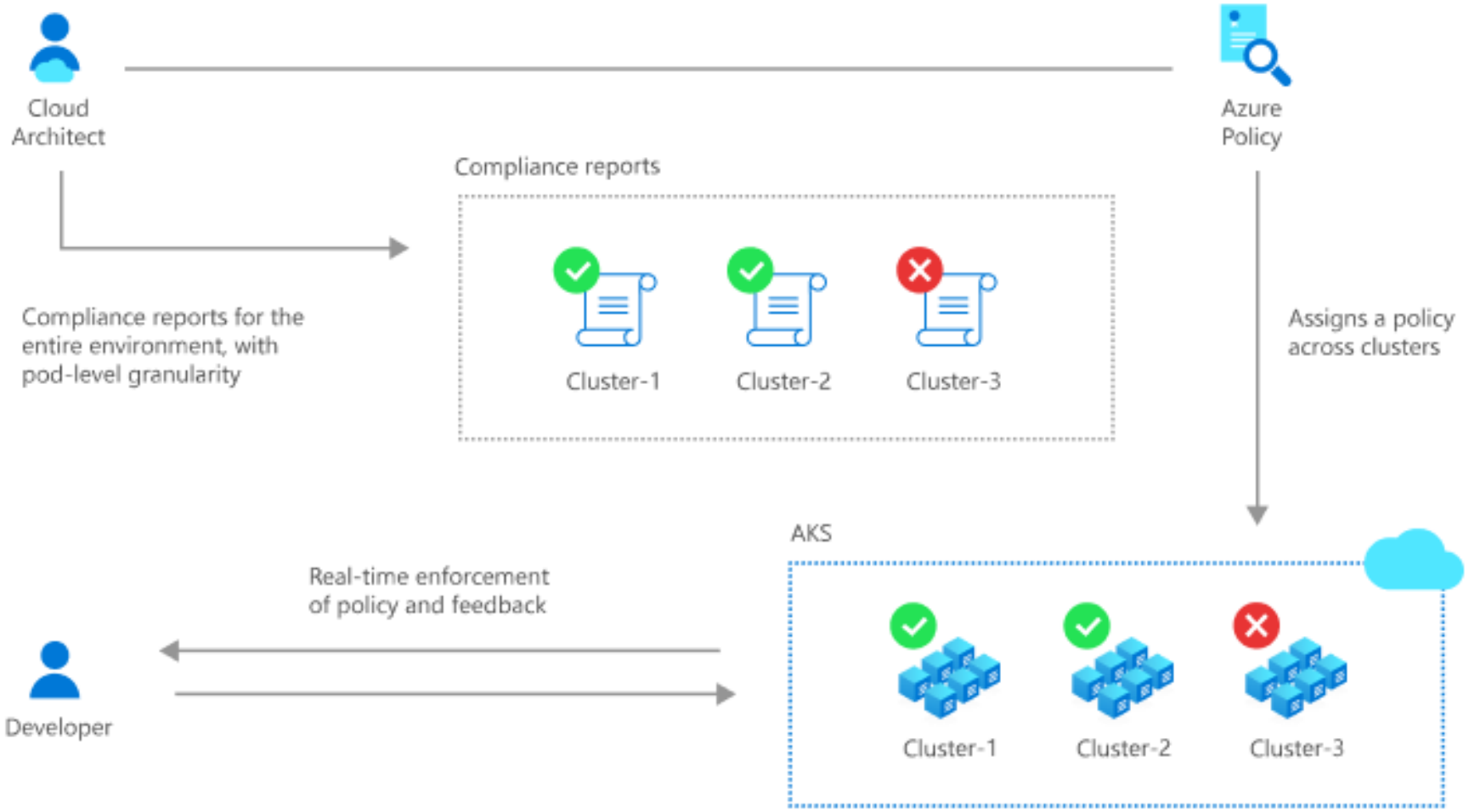
Search to filter items...

ID	Security Check	Category	Severity
196813	Ubuntu Security Notification for Eglibc, Glibc Vulnerability (USN-...	Ubuntu	High
197022	Ubuntu Security Notification for Eglibc, Glibc Vulnerabilities (USN...	Ubuntu	High

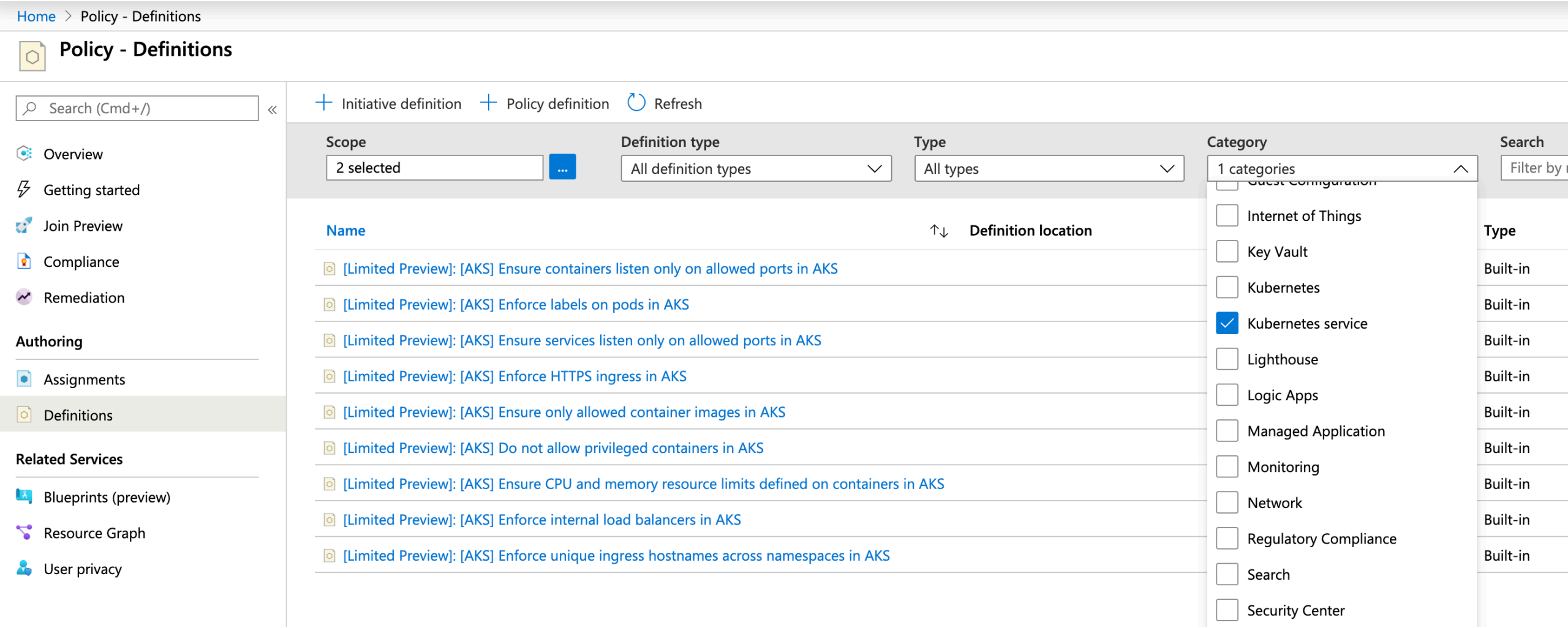
Take action | Remediate

Was this recommendation useful? Yes No

#9 - Azure Policy pour AKS

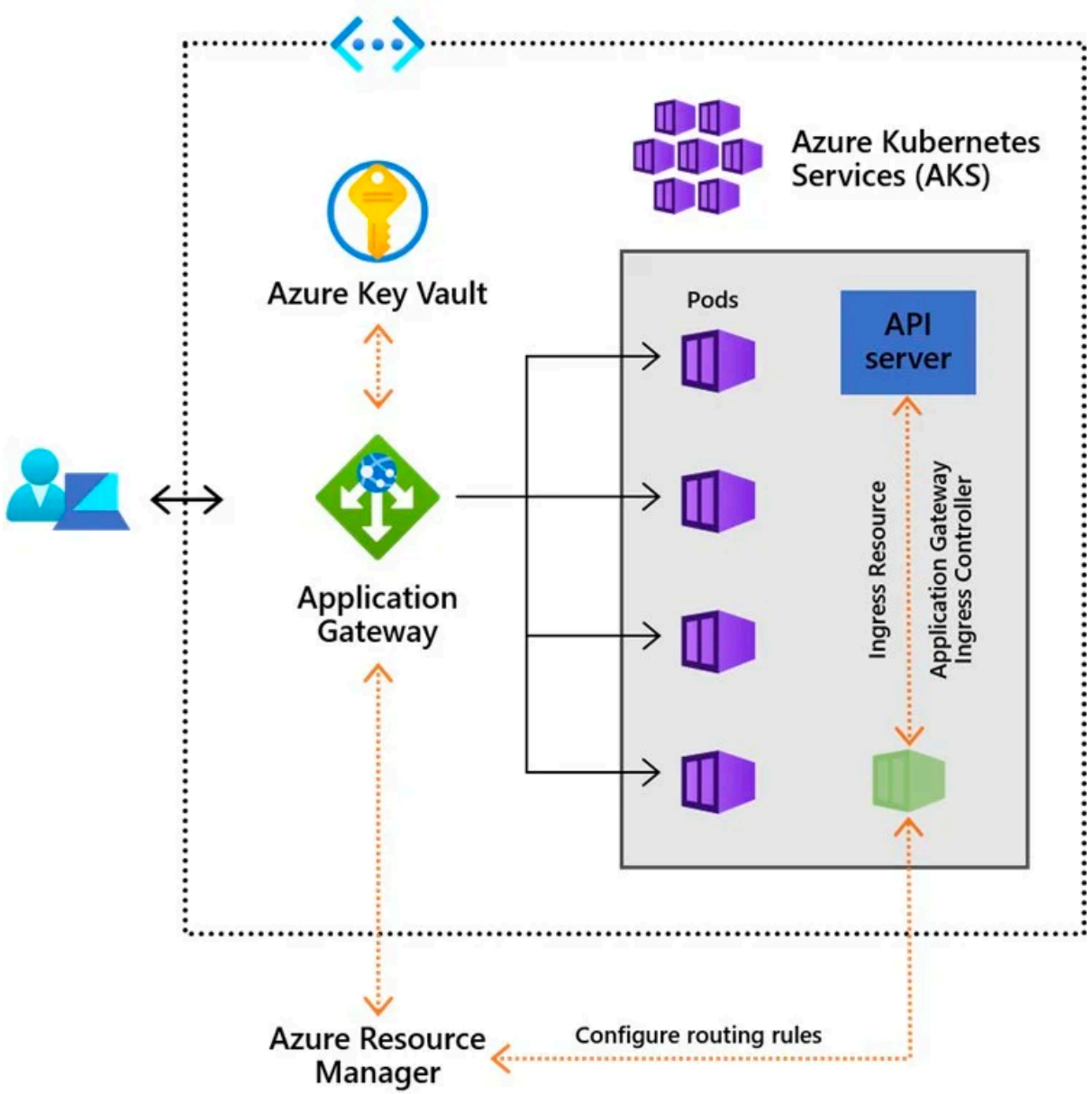


#9 - Azure Policy pour AKS



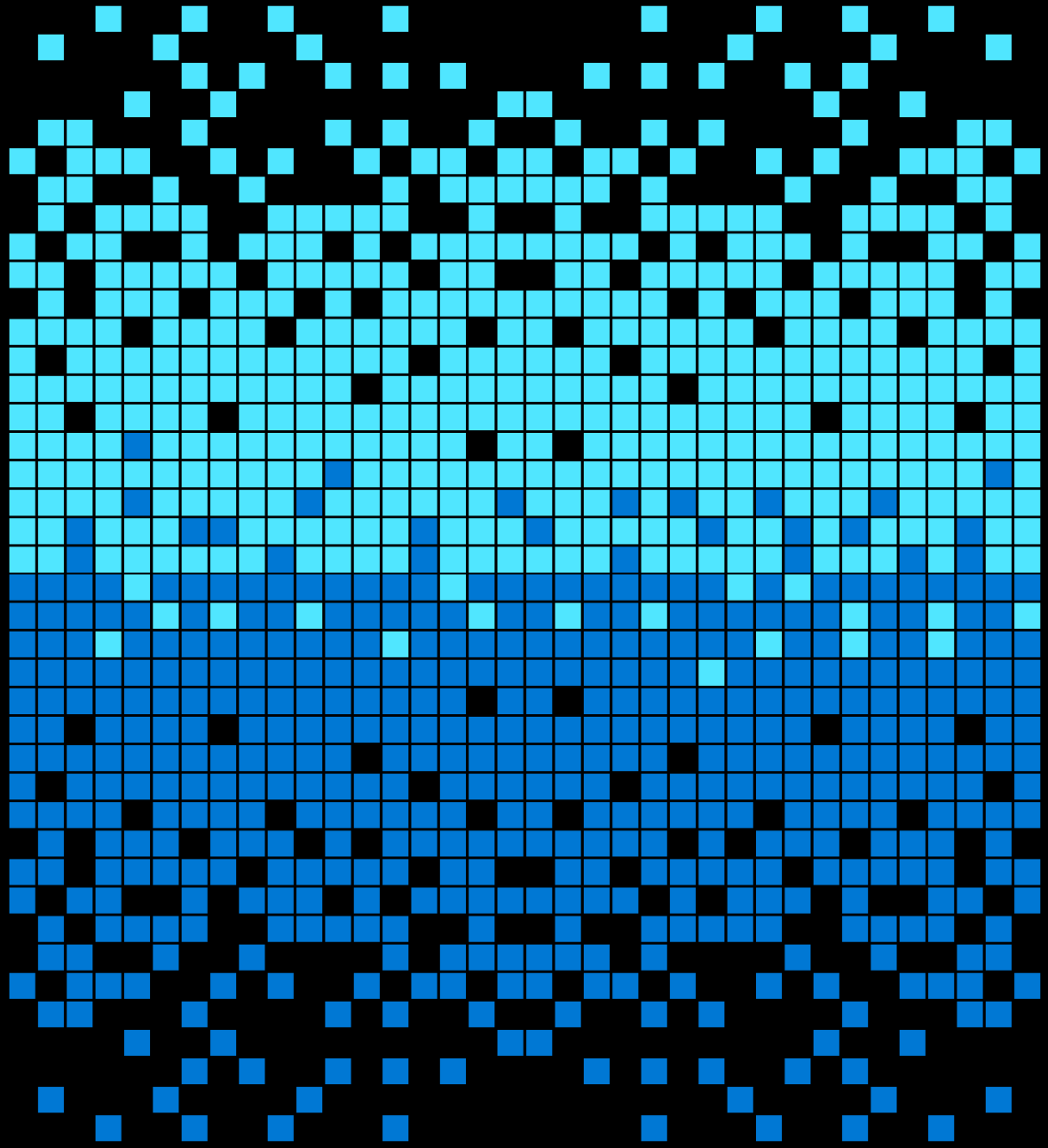
Exposer vos services en sécurité

#10 - Azure Application Gateway Ingress Controller



Microsoft

Merci



Les prochaines étapes de votre parcours d'apprentissage

Inscrivez-vous au prochain webinaire:

www.aka.ms/CloudDigitalSeries

Inscrivez-vous à un apprentissage technique ou à une atelier-pratique:

www.aka.ms/MicrosoftTrainingDaysCanada

www.aka.ms/AzureHands-OnLabs

Pour plus de ressources, veuillez visiter :

www.aka.ms/MSLearn