Public
Cloud
Group

How to securely deploy Kubernetes on Azure .

CNCF Meetup Linz

Agenda.

01. —— Introduction

02. —— AKS and CNCF

03. —— Role-Based Access Control (RBAC)

04. —— Policy

05. —— Secrets Management

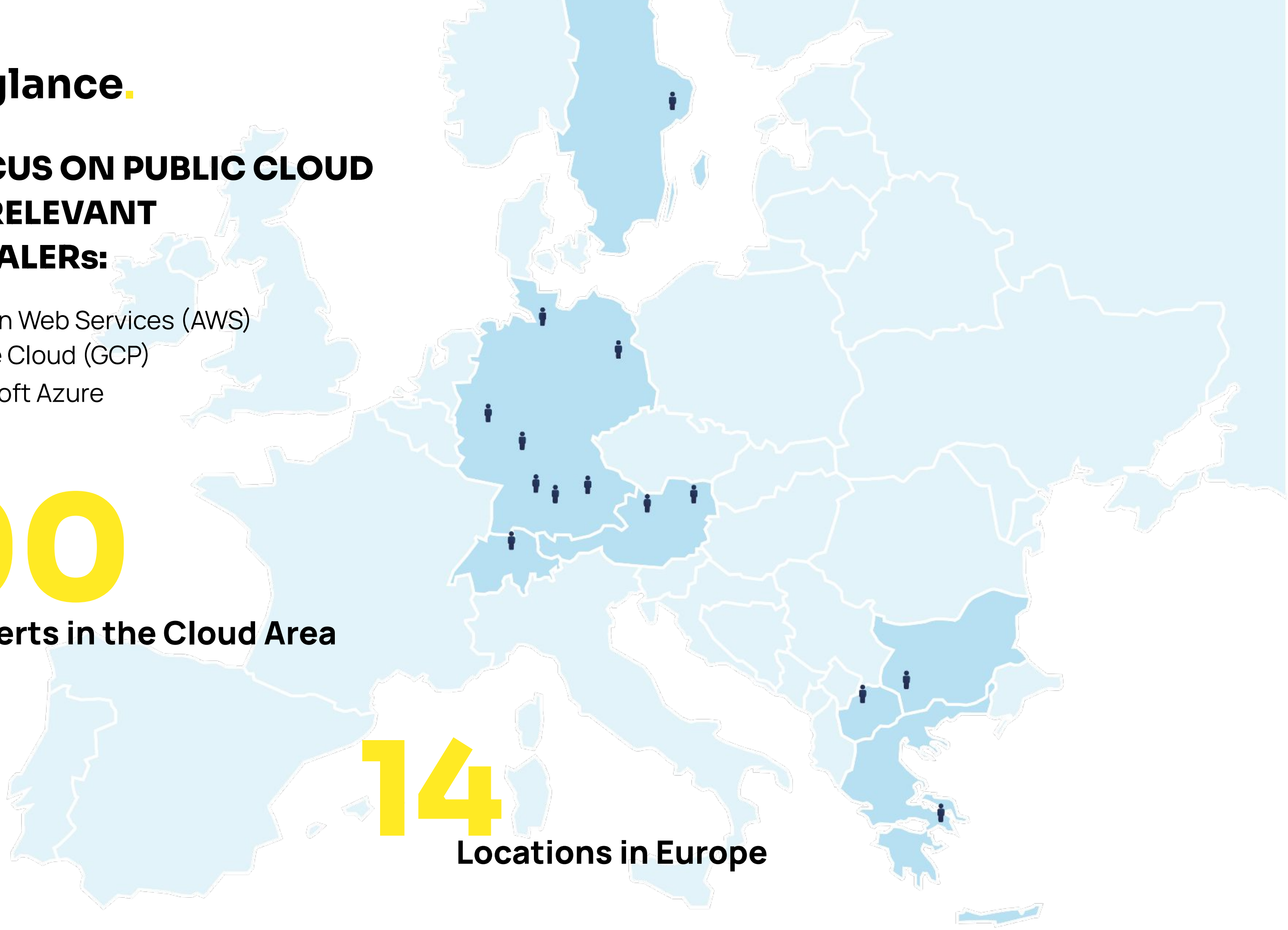
06. —— Workload Identities

07. —— Defender for Containers

At one glance.

100% FOCUS ON PUBLIC CLOUD FOR ALL RELEVANT HYPERSCALERs:

- Amazon Web Services (AWS)
- Google Cloud (GCP)
- Microsoft Azure



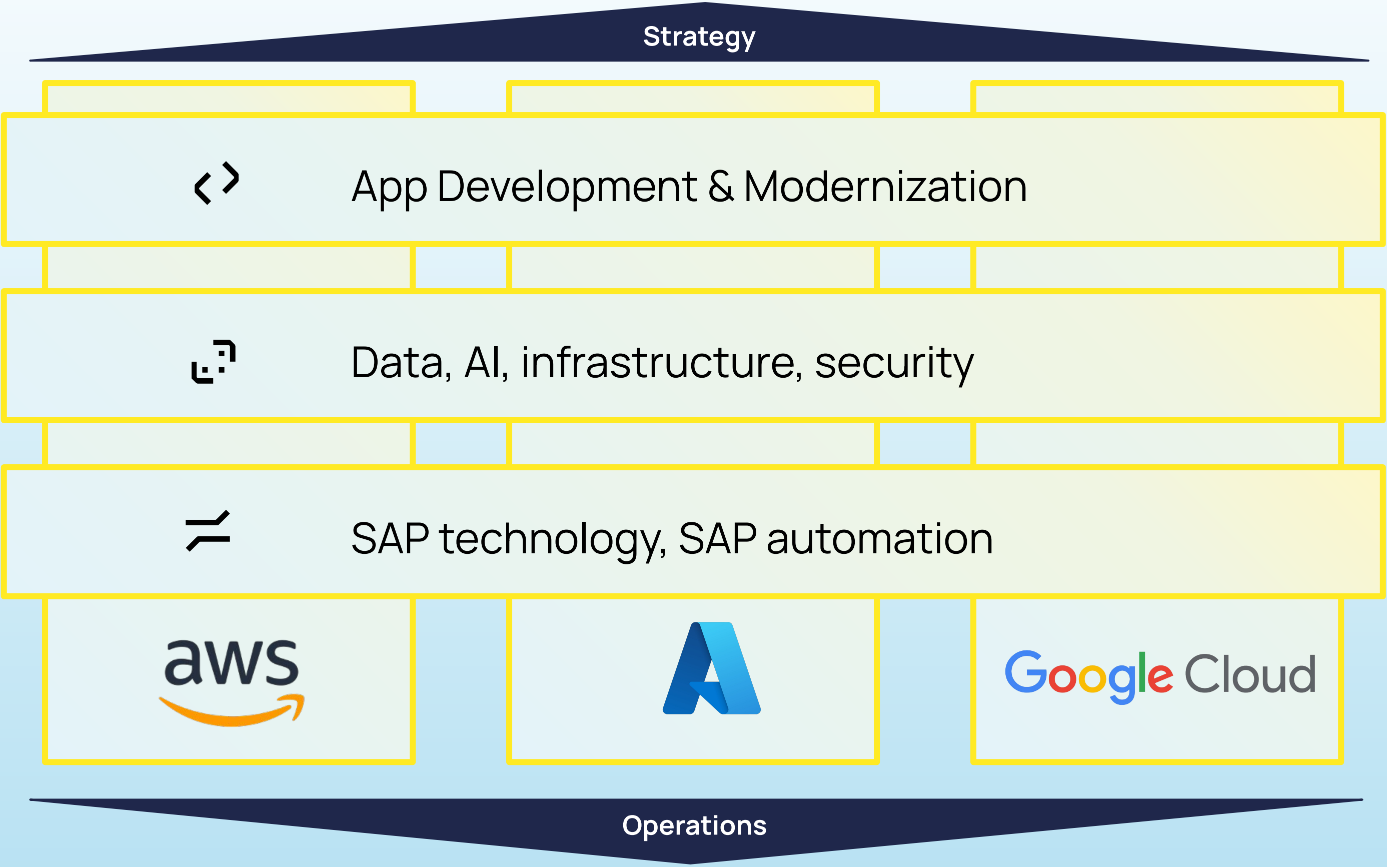
400

Experts in the Cloud Area

14

Locations in Europe

PCG – complete portfolio for the cloud-journey.



Strategy

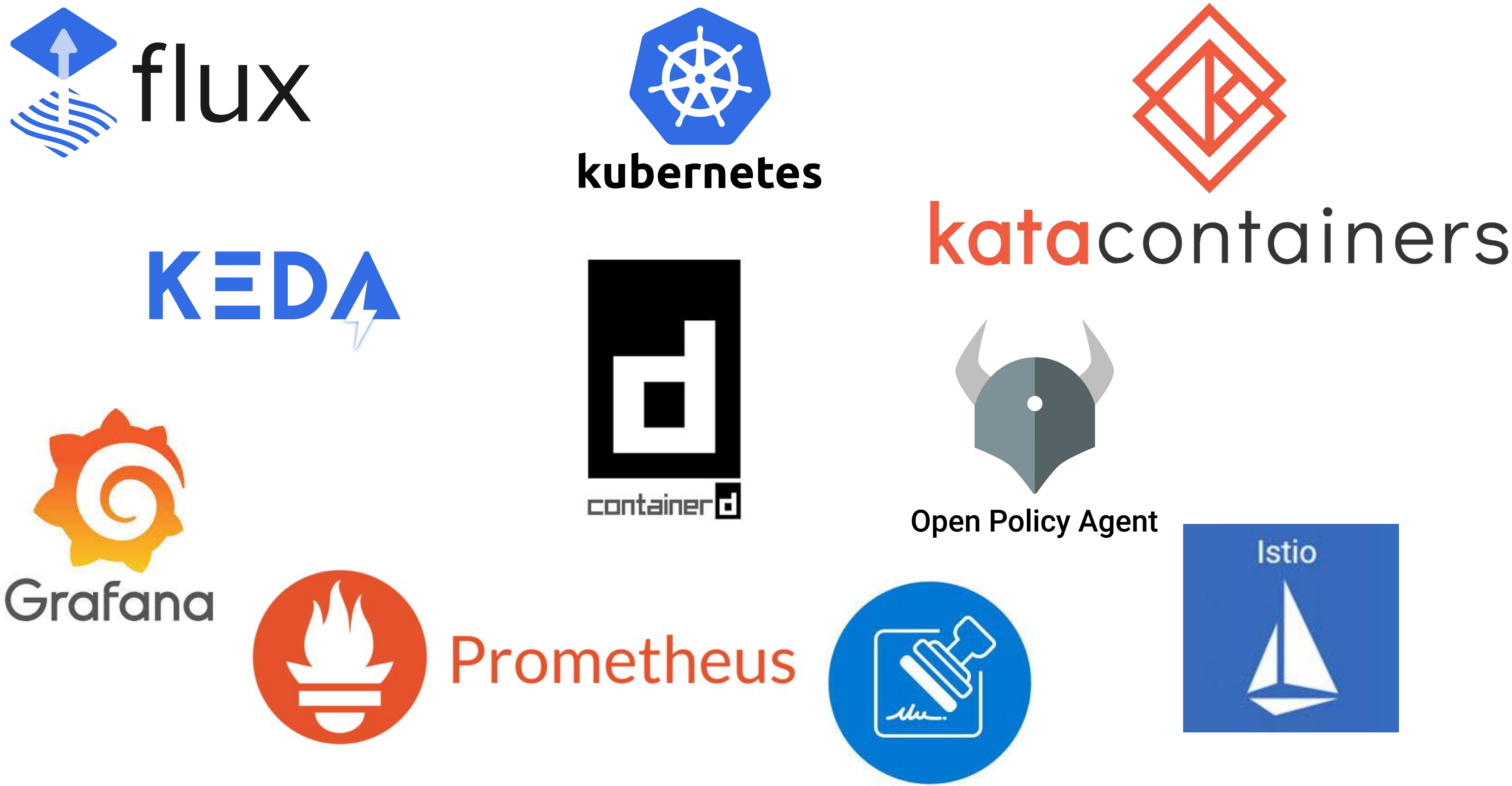
App Development & Modernization

Data, AI, infrastructure, security

SAP technology, SAP automation

Operations

Azure Kubernetes Service and CNCF

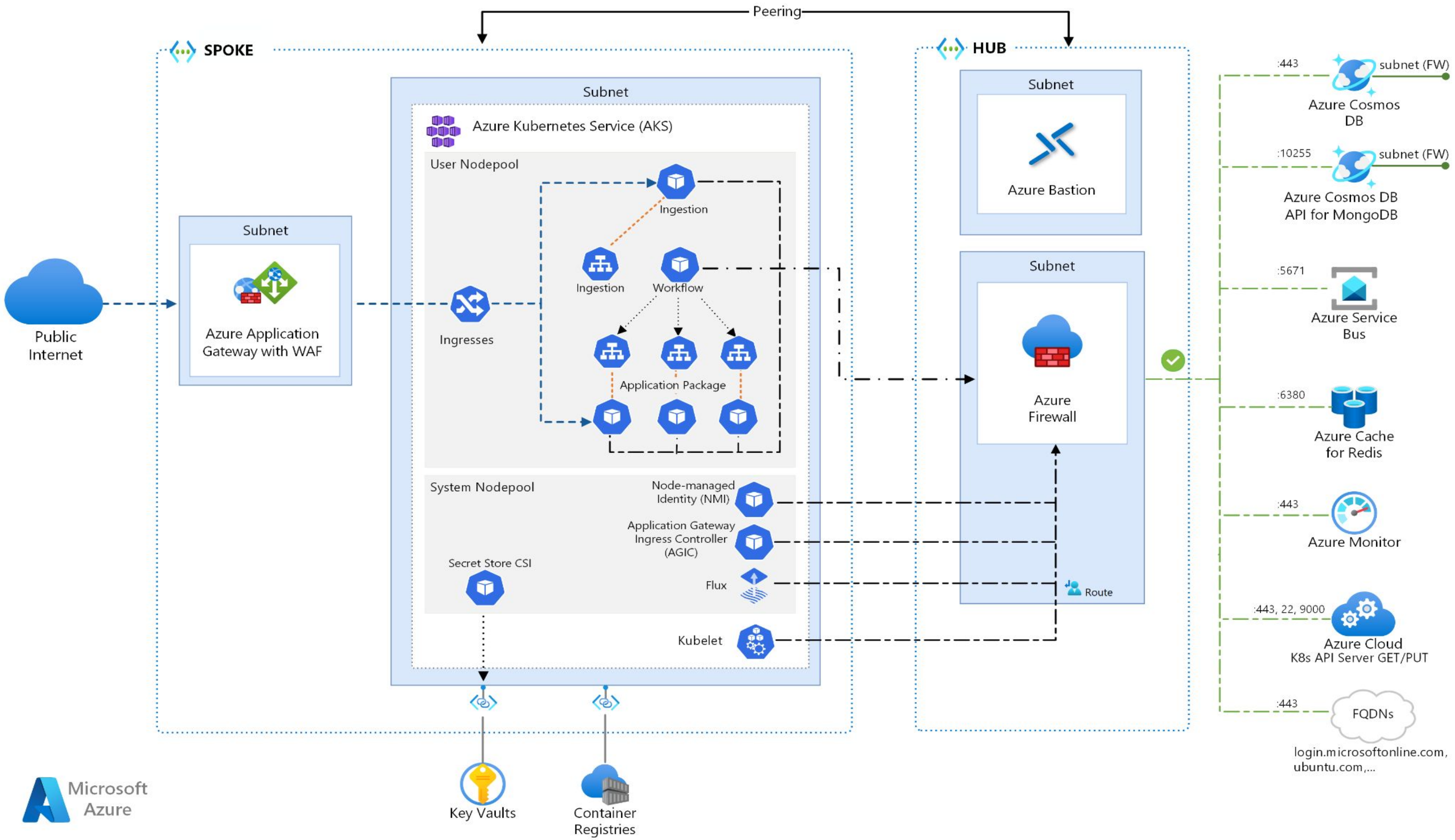


Azure Kubernetes Services (AKS)

What is Azure Kubernetes Service?

- managed Kubernetes service
- automatically creates and configures a control plane
- takes care of operations like health monitoring and maintenance
- only pay for worker nodes
- integrated with Entra ID (RBAC)
- autoscale clusters with KEDA (Kubernetes Event Driven Autoscaler)
- auto-upgrade Kubernetes and nodes (if you want)
- CNCF certified
- Compliant with SOC, ISO, PCI DSS

AKS Deployment Example

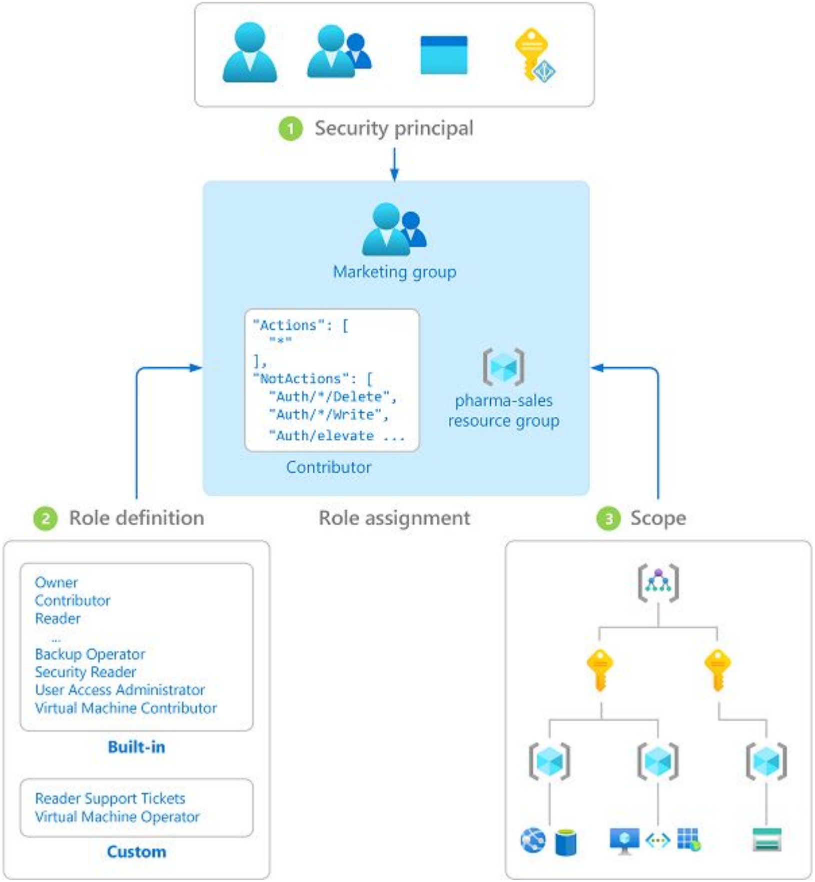


Microsoft Azure

AKS Security

- **Supply Chain Security**
  - Code analysis
  - Vulnerability and compliance scanning (Defender for Containers)
  - Image signing (Notary & Ratify)
  - Azure Policy *
- **Cluster Security**
  - Secure API endpoint (authorized IP-ranges & AKS private cluster)
  - Use Azure RBAC for access control (management and data planes) *
  - Use cluster auto-upgrade (if possible)
- **Node Security**
  - Automatically update node images
  - Disable SSH access (preview)
  - For potentially hostile workloads use compute isolation capabilities
    - AKS confidential compute nodes (based on Intel SGX)
    - Confidential Containers (preview) - based on Kata Containers (using AMD SEV-SNP)
    - Pod Sandboxing (preview)
- **Network Security**
  - Deploy a network policy engine to secure pod network communications (Calico, Cilium, NPM)
  - Deploy WAF for ingress (Application Gateway for Containers)
- **Application Security**
  - Continuous scanning of running pods (Defender for Containers) *
  - Use Azure Key Vault provider for Secrets Store CSI Driver for secrets management *

Azure Role Based Access Control (RBAC)



1 Security principal

Marketing group

```
"Actions": [
  "*"
],
"NotActions": [
  "Auth/*/Delete",
  "Auth/*/Write",
  "Auth/elevate ...
```

Contributor

pharma-sales resource group

2 Role definition

Role assignment

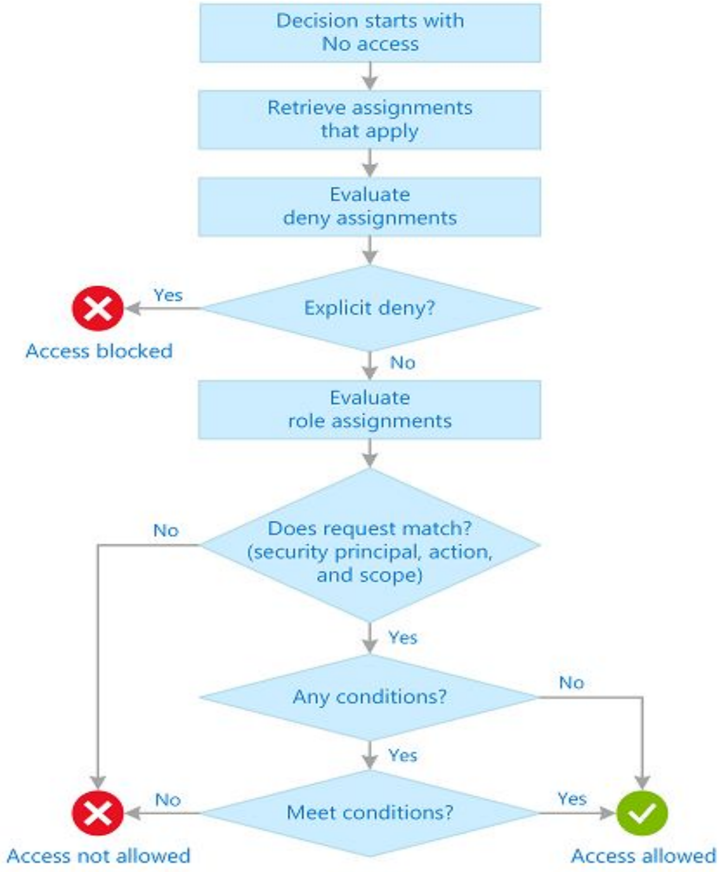
3 Scope

Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

Built-in

Reader Support Tickets
Virtual Machine Operator

Custom



Decision starts with No access

Retrieve assignments that apply

Evaluate deny assignments

Explicit deny?

Yes

Access blocked

No

Evaluate role assignments

Does request match? (security principal, action, and scope)

No

Yes

Any conditions?

No

Yes

Meet conditions?

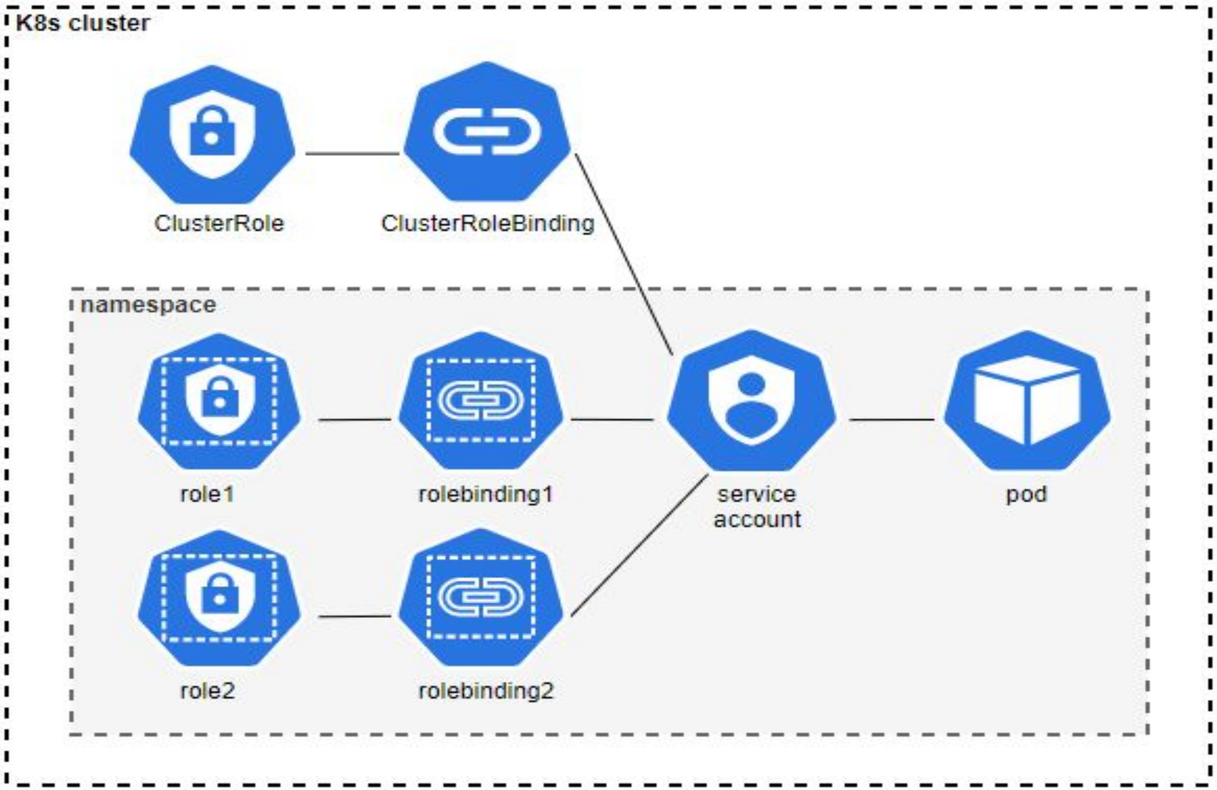
No

Access not allowed

Yes

Access allowed

Kubernetes RBAC



Source: Dynatrace

Azure RBAC for Azure Kubernetes Service

- **Authentication**
  - Kubernetes local accounts
  - Azure AD authentication
- **Authorization**
  - Kubernetes RBAC
  - Azure RBAC

- **Best practices**
  - Disable 'Kubernetes local accounts' → az aks get-credential with —admin doesn't work anymore!
  - Use Azure AD authentication with Azure RBAC
  - Azure RBAC roles needed:
    - Azure Kubernetes Server Cluster User Role (to be able to use az aks get-credential) **AND**
    - One of Azure Kubernetes Service RBAC roles (on cluster or cluster resources)
  - Use 'az role assignment' or Terraform to set role bindings within a cluster!

DEMO

Azure RBAC for AKS

- Azure RBAC example
- AKS RBAC configuration

Azure Policy

- **Governance for resource consistency, regulatory compliance, security, cost, and management**
- **Policy definition written in JSON**
- **Multiple policies form a policy initiative**
- **Remediation possible**
- **Possible actions**
  - Deny the resource change
  - Log the change to the resource
  - Alter the resource before the change
  - Alter the resource after the change
  - Deploy related compliant resources
  - Block actions on resources
- **Role needed:**
  - Resource Policy Contributor
  - Owner
- **Manage as code**

Azure Policy for AKS

Open Policy Agent

- Set policies for AKS management plane and in-cluster resources
- Use standard Azure interface
- Simple installation as a an add-on
- Implemented through GateKeeper via Open Policy Agent
-
- Resource consumption:
  - Small cluster: 2 vCPUs and 350 MB of memory per component
  - Large cluster (>500 Pods): 3 vCPUs and 600 MB of memory per component
- Only for linux containers!

DEMO

Azure Policy for AKS

- Azure Policies for AKS
- Show policy definition
- Show policy framework on cluster

Secrets Management

- **Workloads/ Pods need resources outside the cluster**
  - Storage Accounts, Databases,....

- **For resources on Azure protected by Entra ID you need an Entra ID credential**
  - E.g. Service Principle

Secrets Management

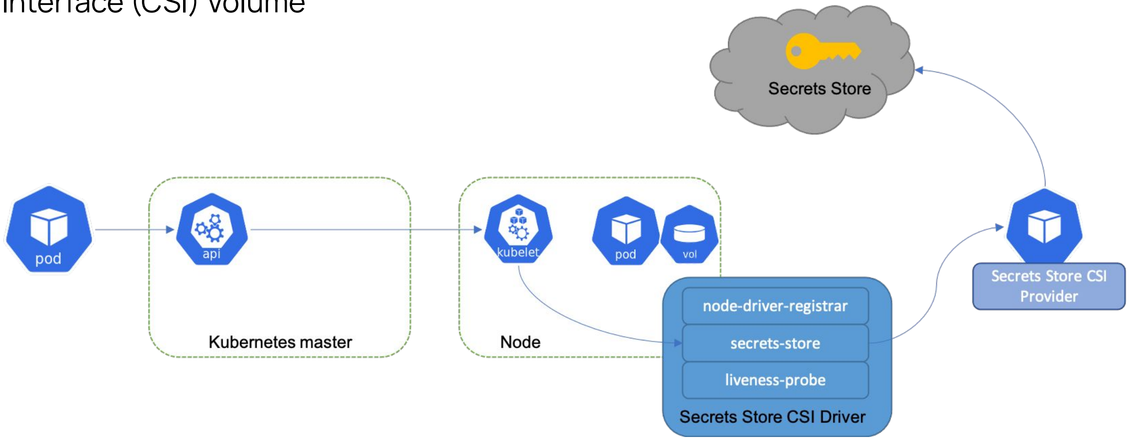
Two challenges:

1. Store the secret
2. Get the secret into AKS

Azure Key Vault Integration

- **Azure Key Vault**
  - Secret store
  - Keys, certificates,…

- **AddOn to integrate Azure Key Vault into AKS**
  - Via Container Storage Interface (CSI) Volume



https://secrets-store-csi-driver.sigs.k8s.io/concepts.html

DEMO

AKS Key Vault Integration

- Pod reads a BLOB from a Storage Account
- Store the connection string in Azure Key Vault
- Mount the secret into AKS

Azure Key Vault Integration

- **Recap DEMO**
  - Securely stored the secret in Azure Key Vault
  - Mounted it to AKS

- **BUT, we still have a secret to manage to access an Azure resource!**

Workload Identity on AKS

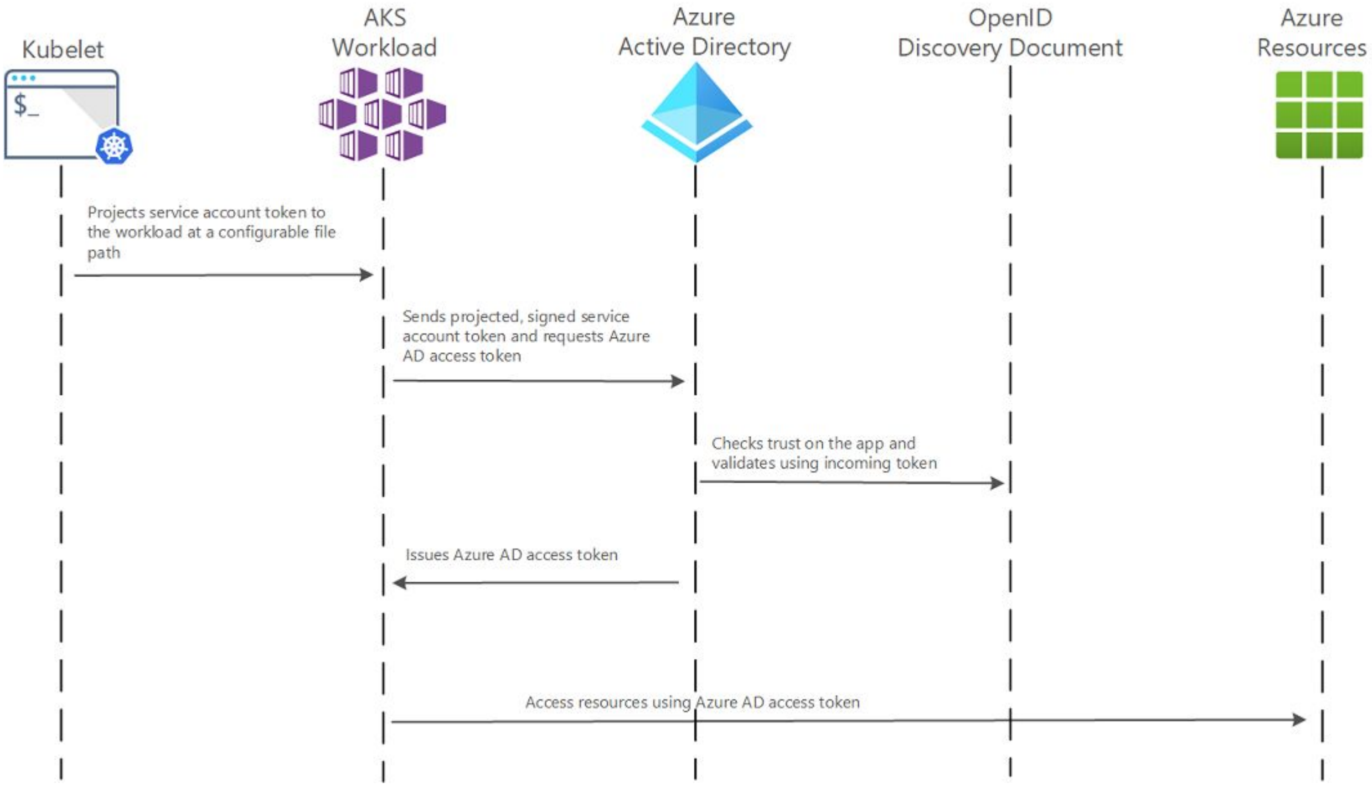
- **Access Microsoft Entra protected resources without needing to manage secrets**
  - Managed Identity
- **Assign Workload Identities to Pods**
- **OIDC**
- **Uses Kubernetes native resources**
- **Use of Azure RBAC**
- **Libraries**
  - Microsoft Authentication Library (MSAL)
  - Azure Identity client libraries

DEMO

AKS Workload Identity

- Use Workload Identity in a Pod to access an Azure Storage Account Blob

Workload Identity on AKS


Kubelet
AKS Workload
Azure Active Directory
OpenID Discovery Document
Azure Resources
$_
Projects service account token to the workload at a configurable file path
Sends projected, signed service account token and requests Azure AD access token
Checks trust on the app and validates using incoming token
Issues Azure AD access token
Access resources using Azure AD access token

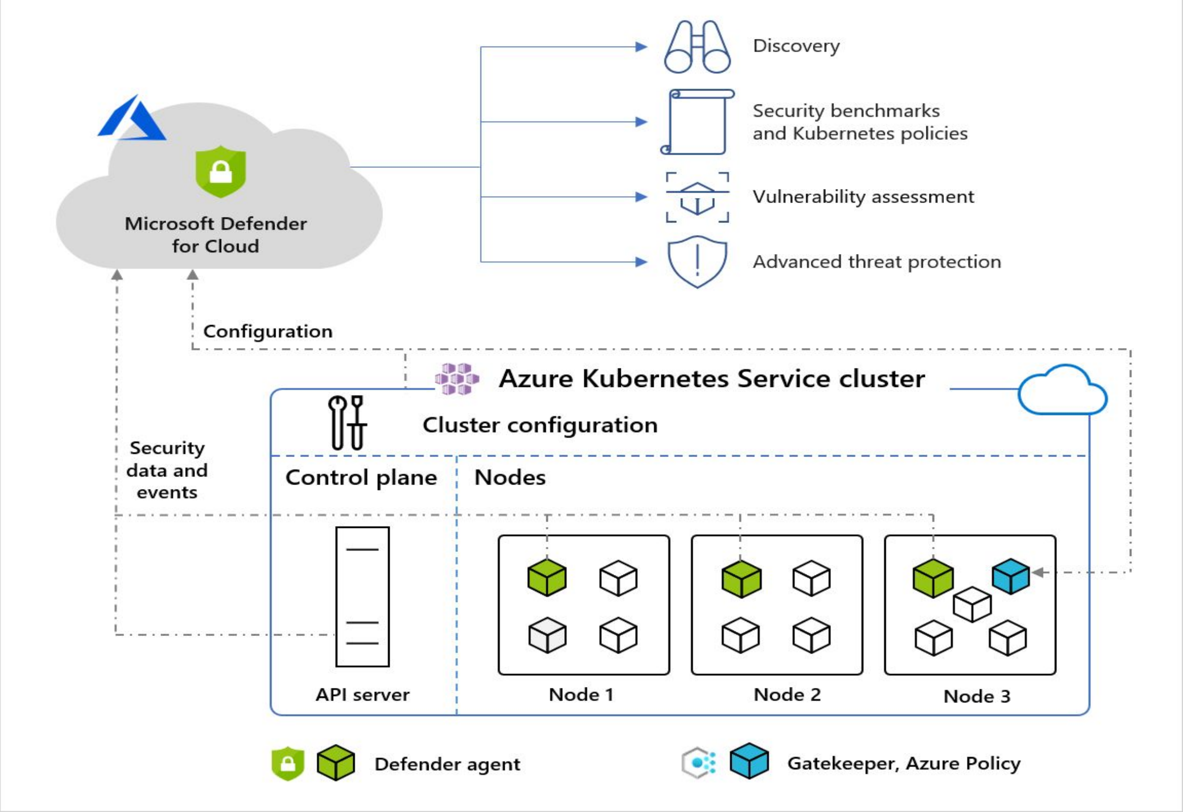
Defender for Containers

- **Cloud native solution to improve, monitor and maintain security of container assets**
    - Kubernetes Cluster, Nodes and Workloads
    - Container Registry, Images

- **Also for AWS or GCP**

- **Four core domains**
    - Security posture management
    - Vulnerability assessment
    - Run-time threat protection
    - Deployment & monitoring

Defender for Containers



Questions?

GET IN TOUCH WITH US

Let’s work together.

Public
Cloud
Group

Marcel Tober
Cloud Consultant Azure
marcel.tober@pcg.io

Andreas Wimmersberger
Senior Cloud Consultant
andreas.wimmersberger@pcg.io

PUBLIC CLOUD GROUP GMBH
Peter-Behrens-Platz 10
4020 Linz

VISIT OUR WEBSITE

With a product portfolio designed to accompany organizations of all sizes in their cloud journey and competence that is a synonym for highly qualified staff that customers and partners like to work with, PCG is positioned as a reliable and trustworthy partner for the hyperscalers, relevant and with repeatedly validated competence and credibility.

We have the highest partnership status with the three relevant hyperscalers. As experienced providers, we advise our customers independently.

aws