Microsoft

Optimize your AKS Cluster for security and compliance

Kendall Roden & Ray Kao, Cloud Native Global Blackbelt

Agenda

01 Welcome and Introduction

02 Cluster set up

03 Set up walkthrough

04 Q&A

05 Review & next steps

Meet your instructors

@kendallroden

@RayKao

Webinar Series Overview

Last session (04/19/2021)
Configure your Cluster with Confidence

Today's Session
Optimize your Cluster for Security and Compliance

04/28/2021 @ 2 EST
Extend your Workload Capabilities

Review Cluster Baseline (Part I)

Compute and Infrastructure

- Managed Identity
- Uptime SLA
- System and User Node Pools

Process

- ACR integration
- Upgrade plan
- Azure AD + RBAC

Networking

- Azure CNI
- Network Policy with Calico

Observability

- Container monitoring & Log analytics

Questions about our setup…

- How “secure” is this?
- Is HTTPS communication over “public” internet, ok?
  - Stays within Azure Network but is not a “private link”
- How can we lock it down a bit more?
- How do we meet requirements if there are compliance/regulation requirements?

Security Considerations

CI/CD

- Container Image build best practices
- Vulnerability detection
- Compliance (CIS Alignment)
- Secrets Management

Cluster

- Pod security
- Node security
- Network security
- Identity and RBAC
- Cluster compliance (K8s CIS Benchmark, HIPPA, ISO 27001, etc.)
- Kubernetes Audit Logging

Host

- Vulnerability detection
- Compliance (Linux CIS)
- Host Runtime security

Cluster modifications for security and compliance

Compute and Infrastructure

- Managed Identity
- Uptime SLA
- System and User Node Pools

Process

- ACR integration
- Upgrade plan
- Azure AD + RBAC
- Azure Policy Integration
- Azure Security Center
- Pod Identity & Secret Store CSI Driver

Networking

- Azure CNI
- Network Policy with Calico
- Private Cluster
- AzFirewall integration
- Service Mesh

Observability

- Container monitoring & Log analytics
- Intra-cluster scanning

Today's cluster config

CloudNativeGBB/webinars(github.com)

```
2021-04-21-optimize-your-aks-cluster-for-security-and-compliance
    /bicep
    /terraform
    /slide-deck
    README.md (Guide)
```

We must shift how we do security

Traditional security controls do not apply in the Cloud Native world

- Manual configuration and controls
- Network security controls (firewalls & IPS/IDS) fail to see container traffic
- Reactive based security

- Roles + Responsibilities – Don’t just adopt what you are doing on-prem
- Policy – Enterprise Controls
- Security as Source Control – Treat Security like Code & Infra as Code

Process:
Azure Policy + Azure Security Center

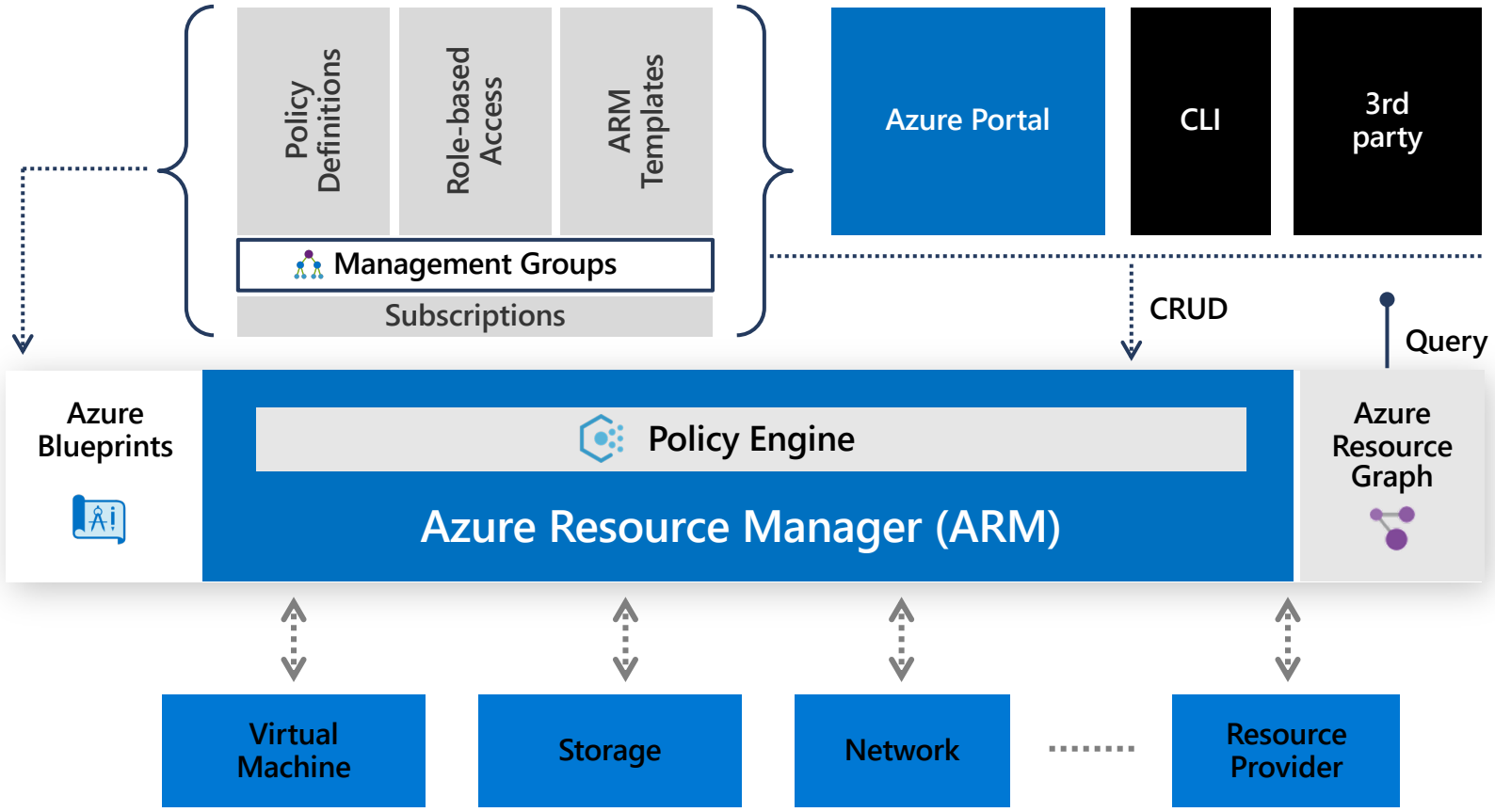
Enterprise Control Plane Architecture

Providing control over the cloud environment, without sacrificing developer agility

1. **Environment factory**
   Deploy and update cloud environments in a repeatable manner using composable artifacts

2. **Policy-based control**
   Real-time enforcement, compliance assessment and remediation at scale

3. **Resource visibility**
   Query, explore & analyze cloud resources at scale



Azure policy for enterprise-level compliance

- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation

Enforcement & Compliance

- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

Apply policies at scale

- Real time remediation
- Remediation on existing resources

Remediation

Let’s break down Azure Policy for Kubernetes

The what

- Extends Gatekeeper v3, an admission controller webhook for Open Policy Agent (OPA)
- Only supports Linux node pools & built-in policy definitions
- Should be scheduled to system node pool
- Add-on checks with Azure Policy for changes every 15 min
- If cluster sub is registered with ASC then ASC K8s policies are applied on the cluster automatically

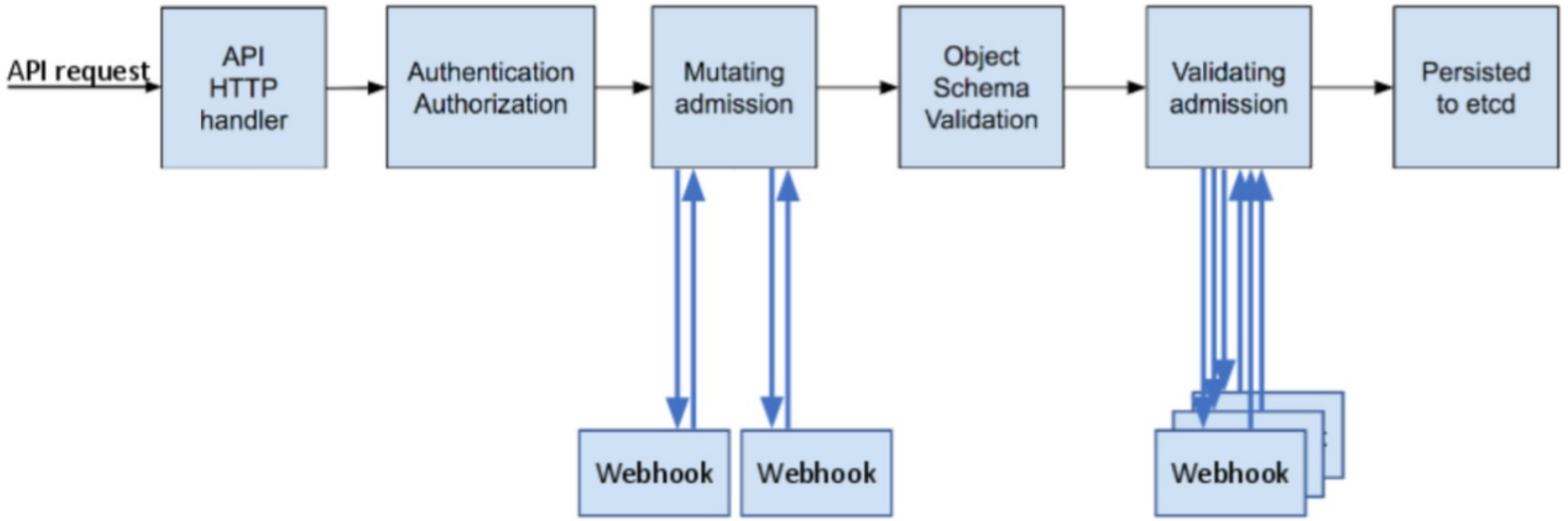
The why

- Shift security left - lower dev latency
- Replace Pod Security Policy functionality (undergoing deprecation)
- Consistent governance experience across Azure
- Offload management of Gatekeeper to MSFT
- Future extensibility when custom policies are supported

Open Policy Agent

CLOUD NATIVE COMPUTING FOUNDATION

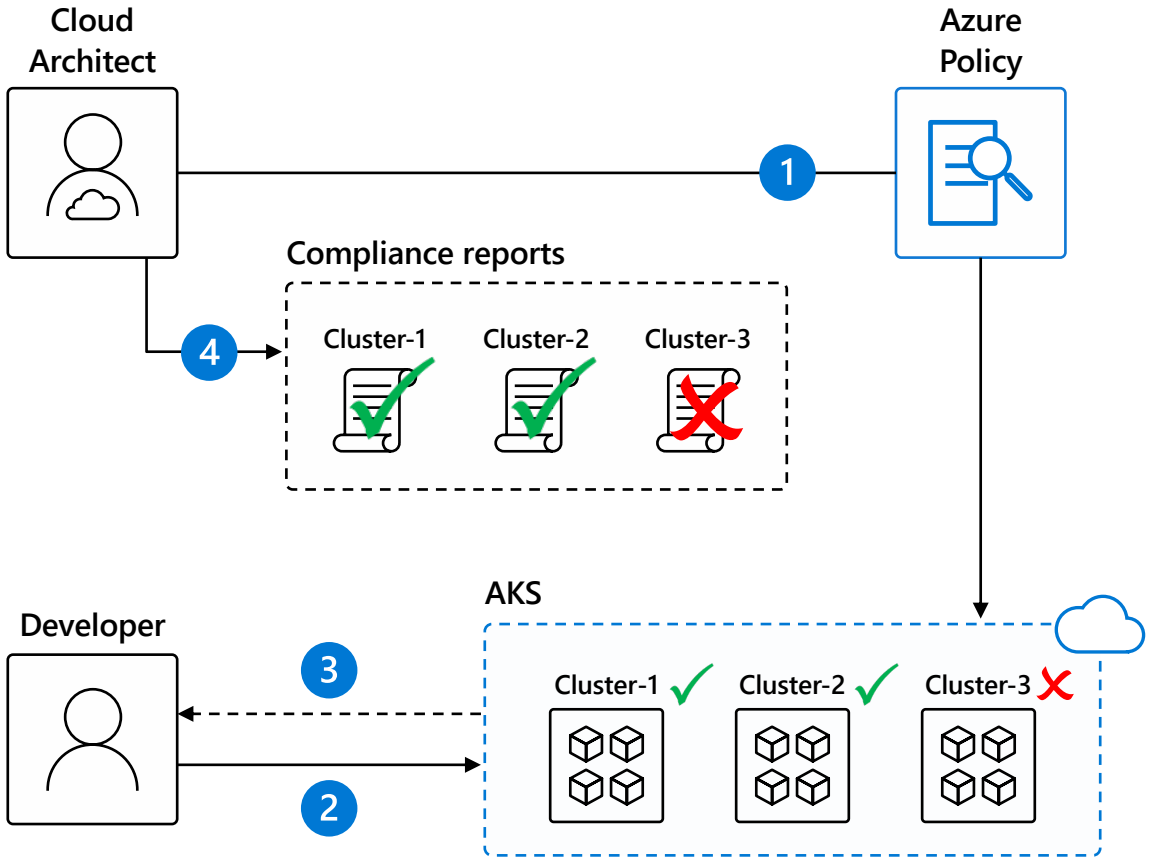
Dynamic Admission Control



Admission Controller Phases

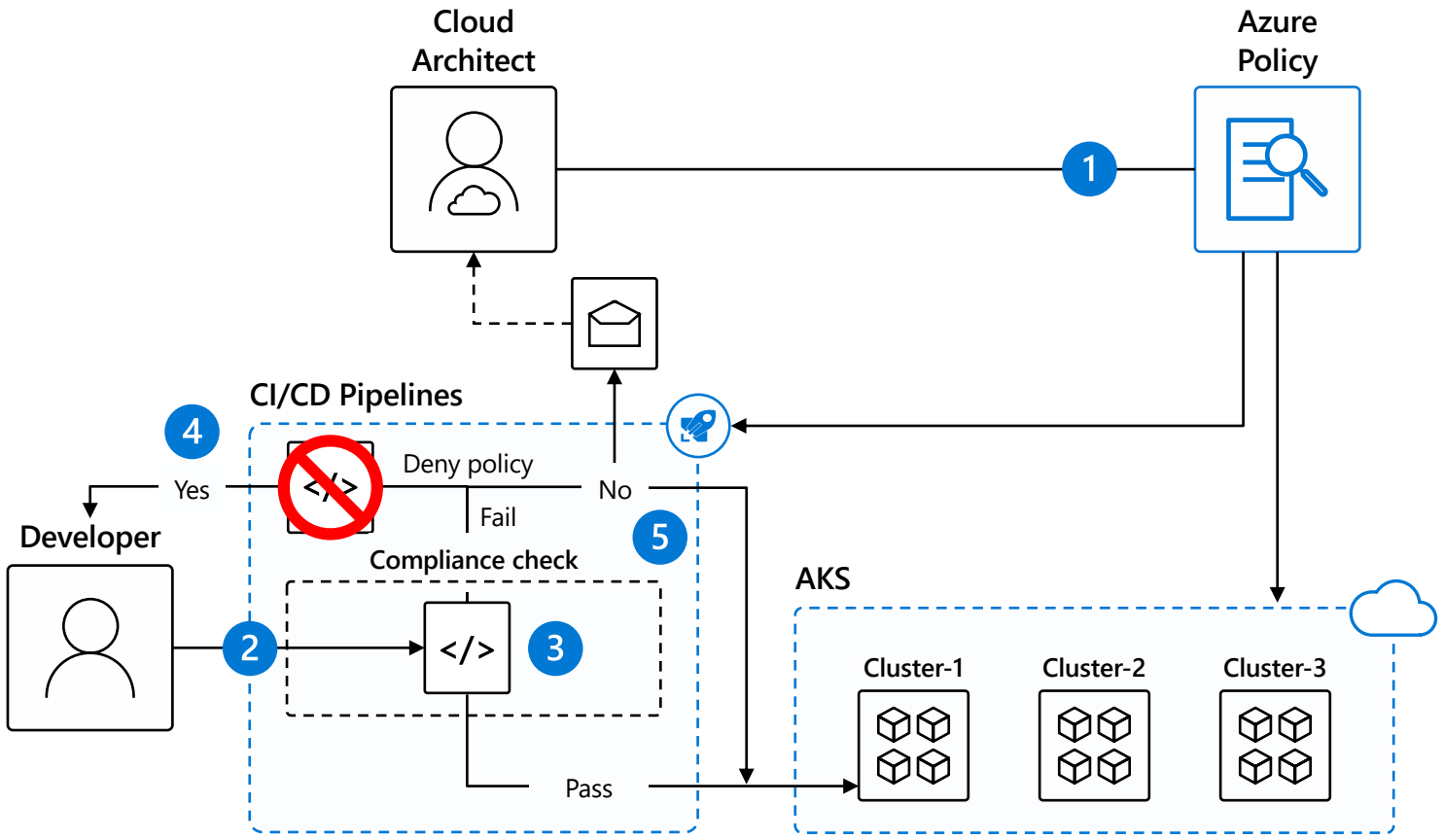
Azure Policy for clusters

1. Cloud architect assigns a deployment policy across cluster(s)
2. Developer uses standard Kubernetes API to deploy to the cluster
3. Real-time deployment enforcement (acceptance/denial) provided to developer based on policy
4. Cloud architect obtains compliance report for the entire environment and can drill down to individual pod level



Azure Pipelines build audit & enforcement using Azure Policy

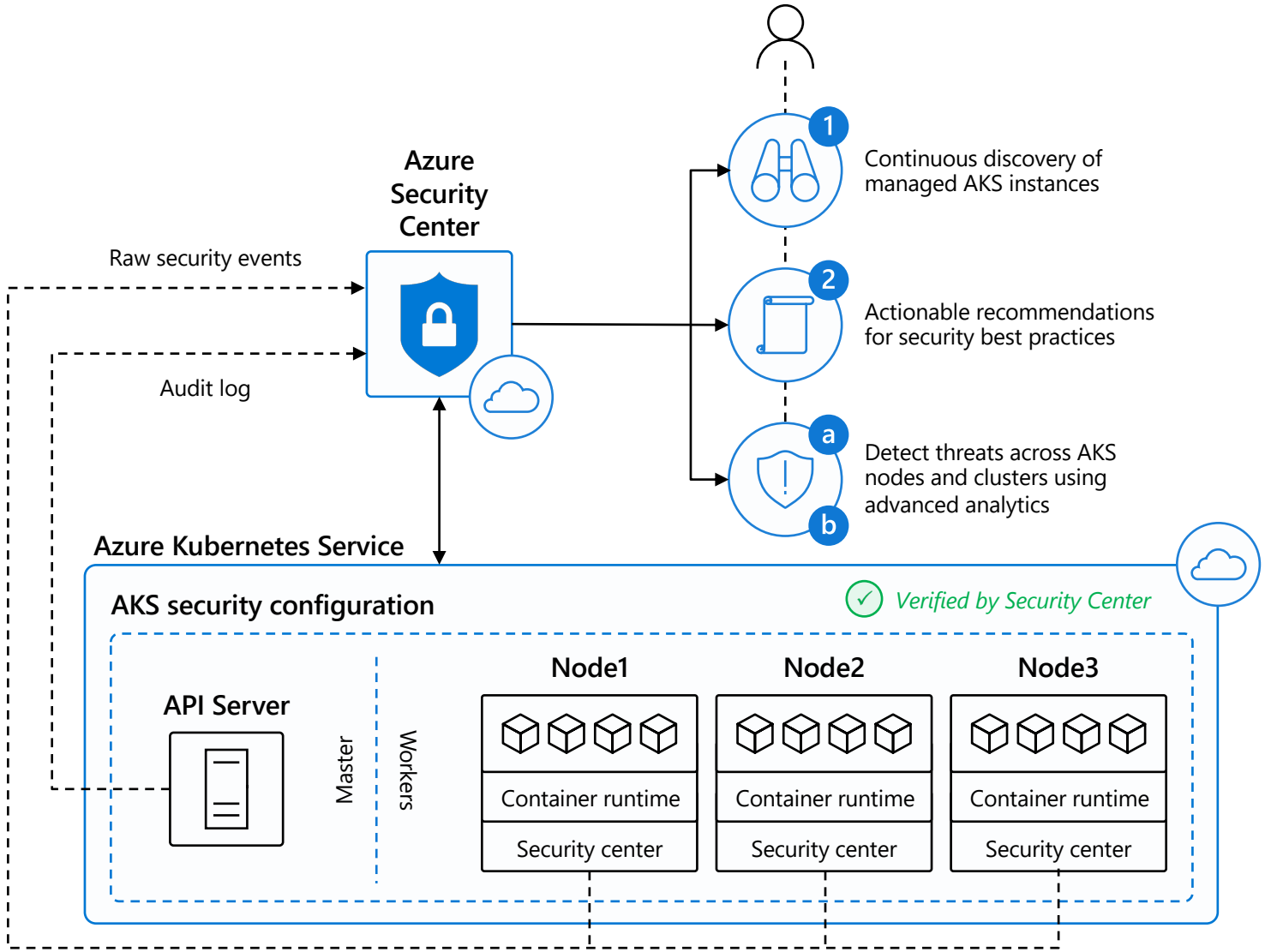
1. Cloud architect assigns a policy across clusters; policy can be set to block non-compliance (deny) or generate non-compliance warnings (audit)
2. Developer makes code change that kicks off a build on Azure Pipelines
3. Azure Pipelines evaluates the request for policy compliance
4. If policy is set to deny, Azure Pipelines rejects the build attempt if any non-compliance is identified
5. If policy is set to audit, a non-compliance event is logged and the build is allowed to proceed



AKS Support in Azure Security Center

1. For managed subscriptions, each new AKS cluster and node are discovered in ASC
2. ASC monitors AKS cluster for security misconfigurations and provides actionable recommendations for compliance with security best practices
3. ASC continuously analyzes AKS for potential threats based on:
    a. Raw security events such as network data and process creation
    b. Kubernetes log audit

...and reports any threats and malicious activity detected (e.g., "API requests to your cluster from a suspicious IP was detected")

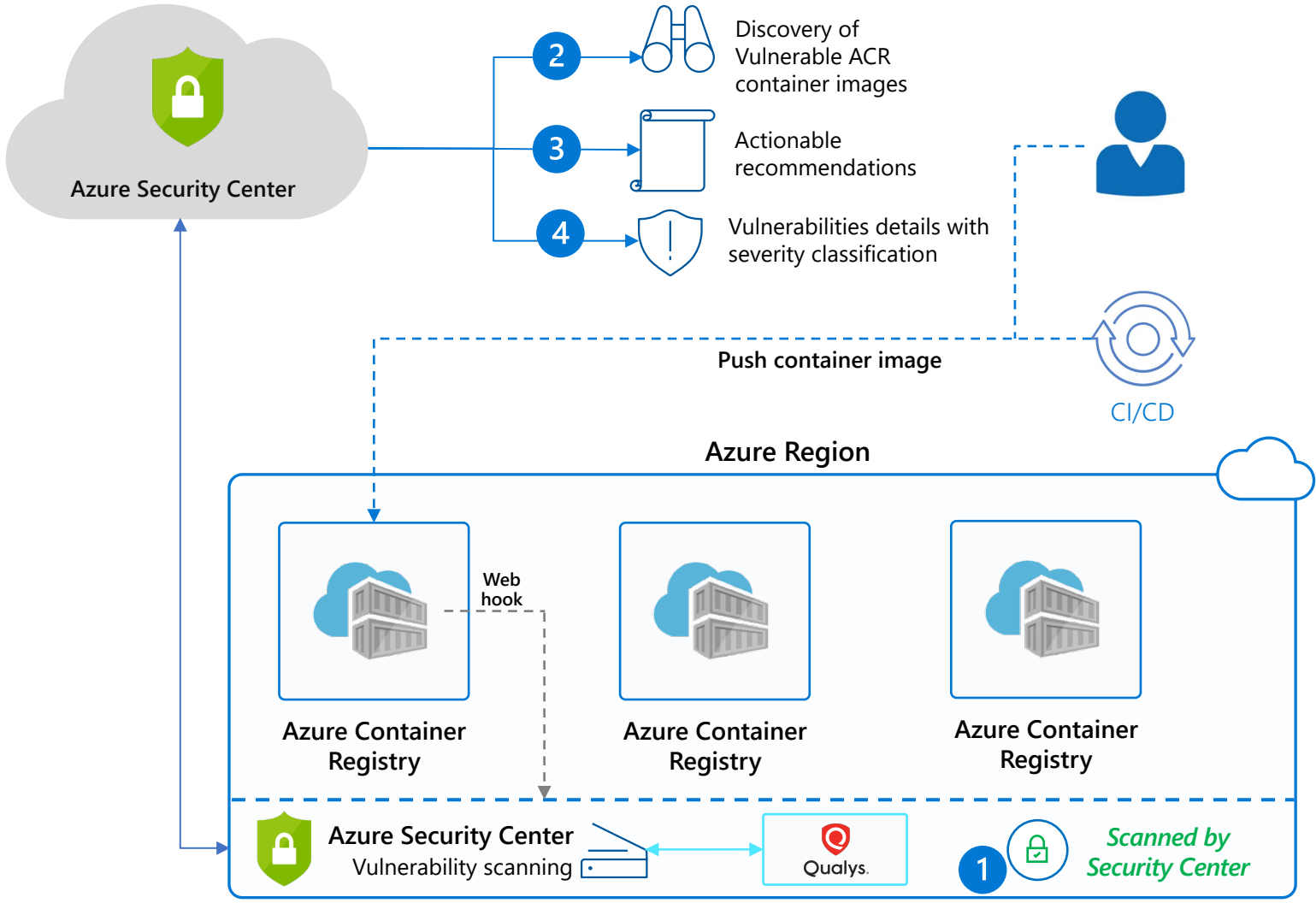


ACR Support in Azure Security Center

Capabilities

Seamless native solution through Security Center

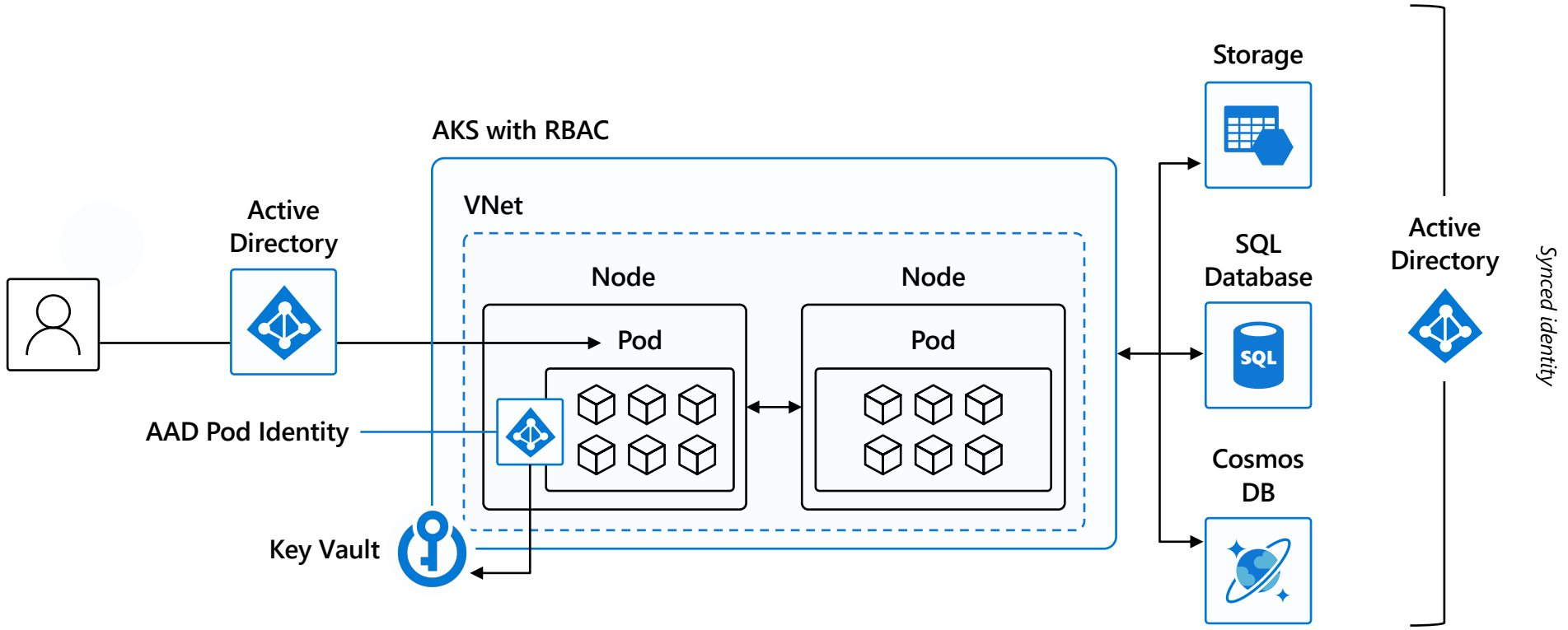
1. For registered subscriptions, when an image is pushed to an ACR, Security Center scans the image for vulnerabilities utilizing Qualys - a VA scanning market leader
2. Scanned ACR registries are discovered in Azure Security Center dashboard.
3. Security Center provides actionable recommendations for images with known vulnerabilities
4. Security Center provides details for each reported vulnerability along with severity classification and guidance to remediation



Process:
Pod Identity + Secret Store CSI Driver

Quick identity review

Use familiar tools like AAD for fine-grained identity and access control to Kubernetes resources from cluster to containers



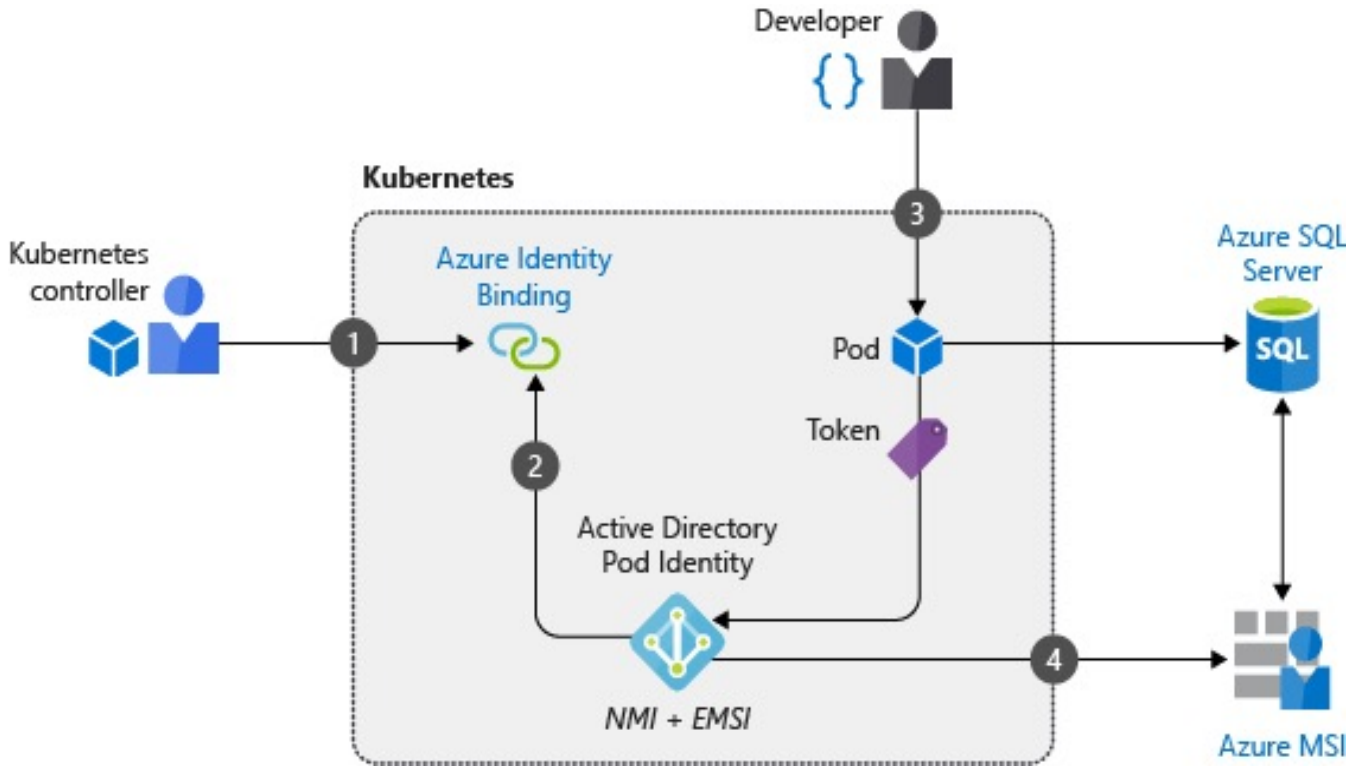
Azure AD Pod Identity

- AAD Pod Identity enables Kubernetes applications to access cloud resources securely with Azure Active Directory

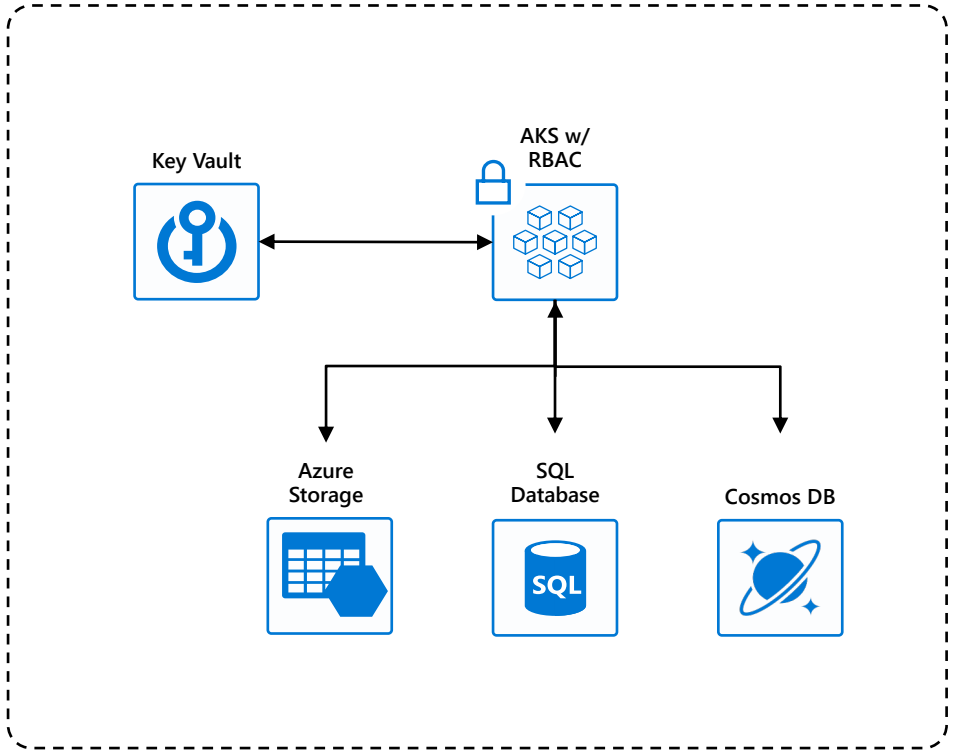
- Using Kubernetes primitives, administrators configure identities and bindings to match pods

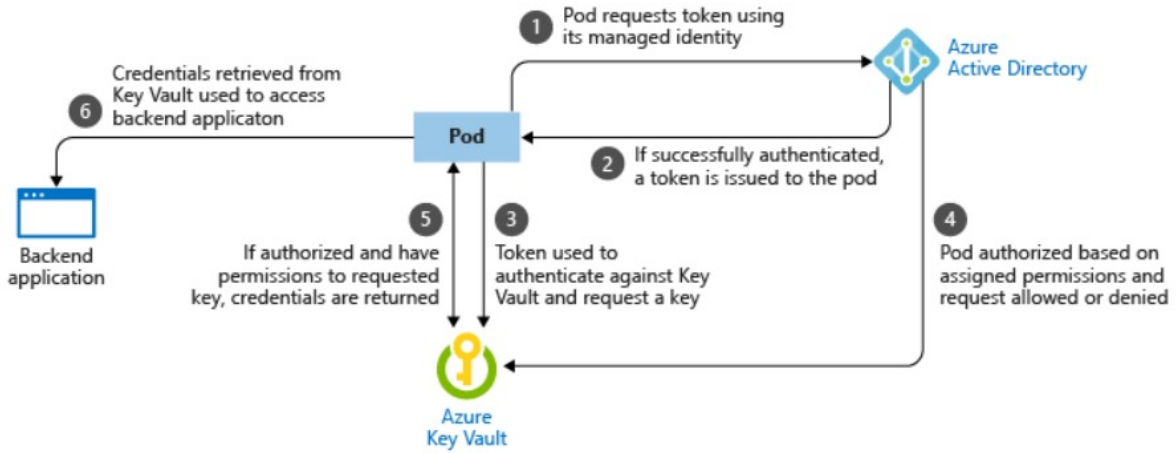
- Without any code modifications, your containerized applications can leverage any resource in the cloud that depends on AAD as an identity provider

Pod Identity in action

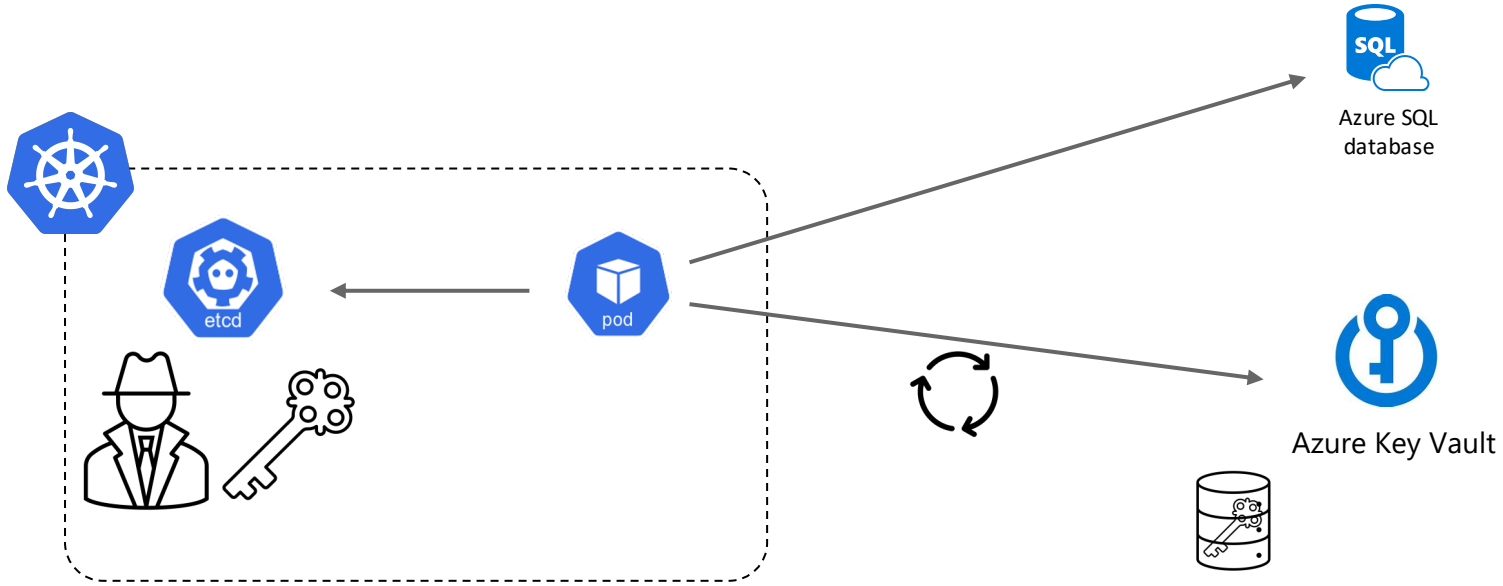


Securing workloads – Azure Key Vault





Enter Azure Key Vault Provider for Secrets Store CSI Driver

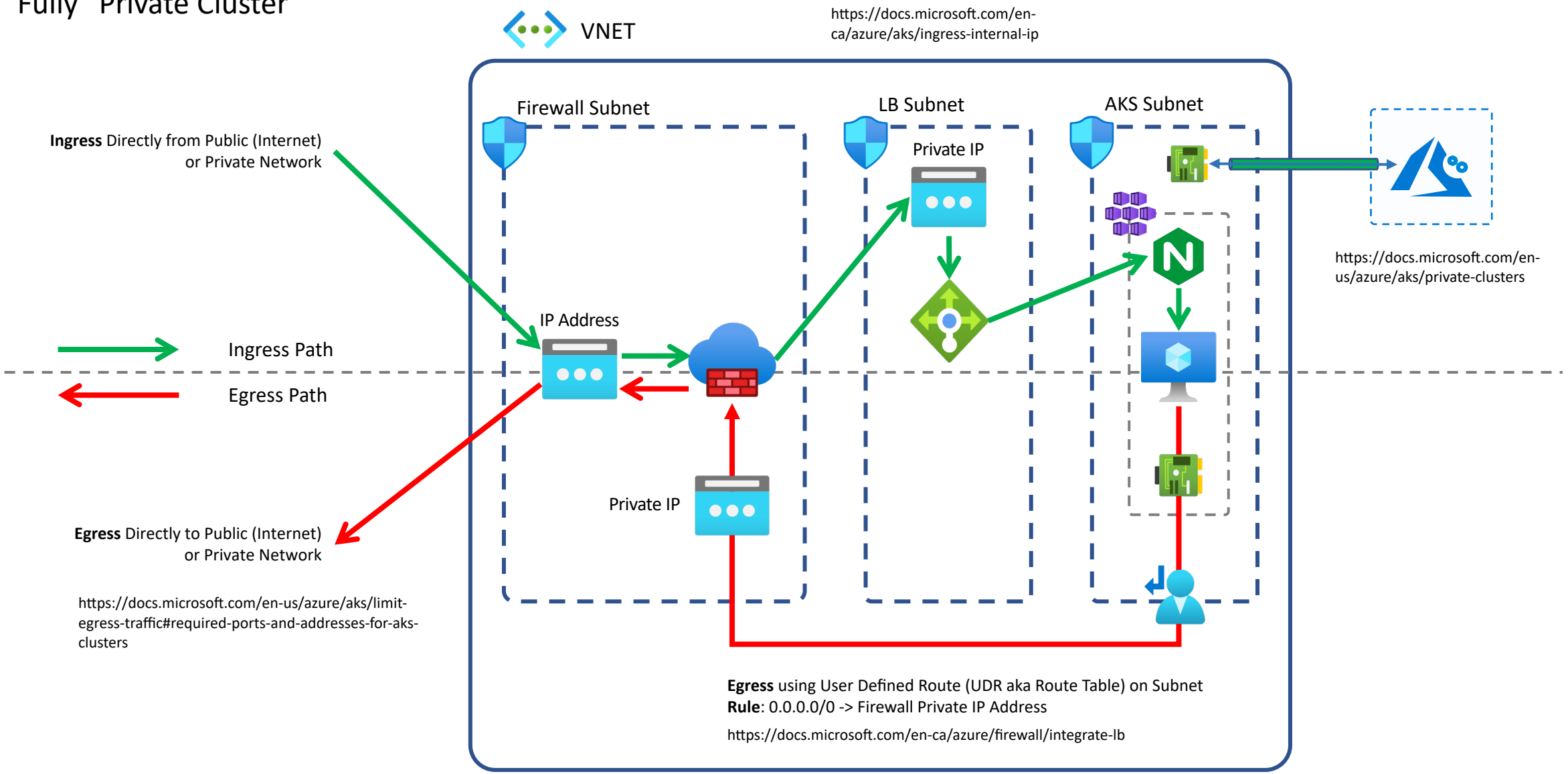


Recommendations

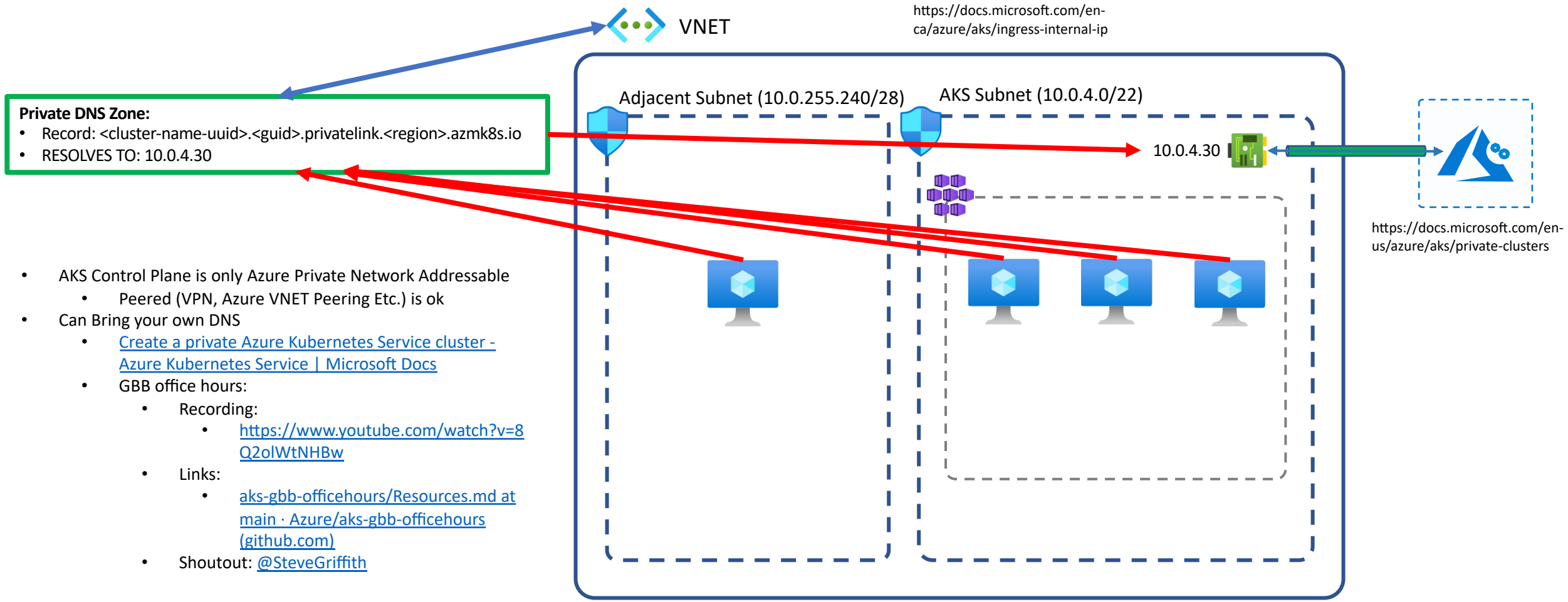
- Use Pod Identity + Azure Key Vault Provider for Secrets Store CSI Driver (keep an eye out for updates regarding pod identity)
- Easiest path is syncing to K8s secret, but this isn’t the most secure
- Consider dapr for abstracting secrets if other features of the product are compelling to you

Networking:
Private Clusters + related considerations

Fully “Private Cluster”

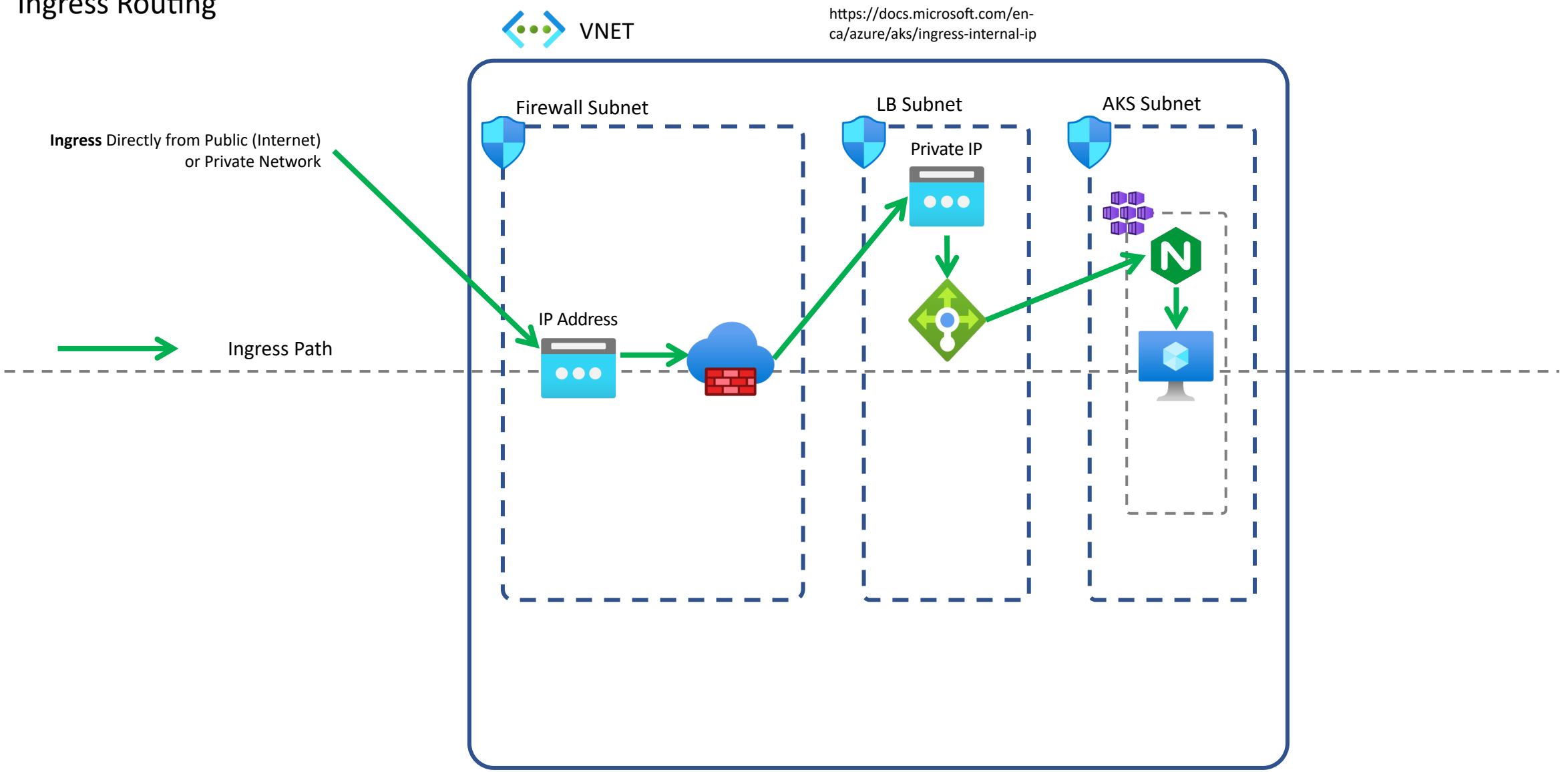


AKS “Private Cluster” – Control Plane over private networking (i.e. not public internet)

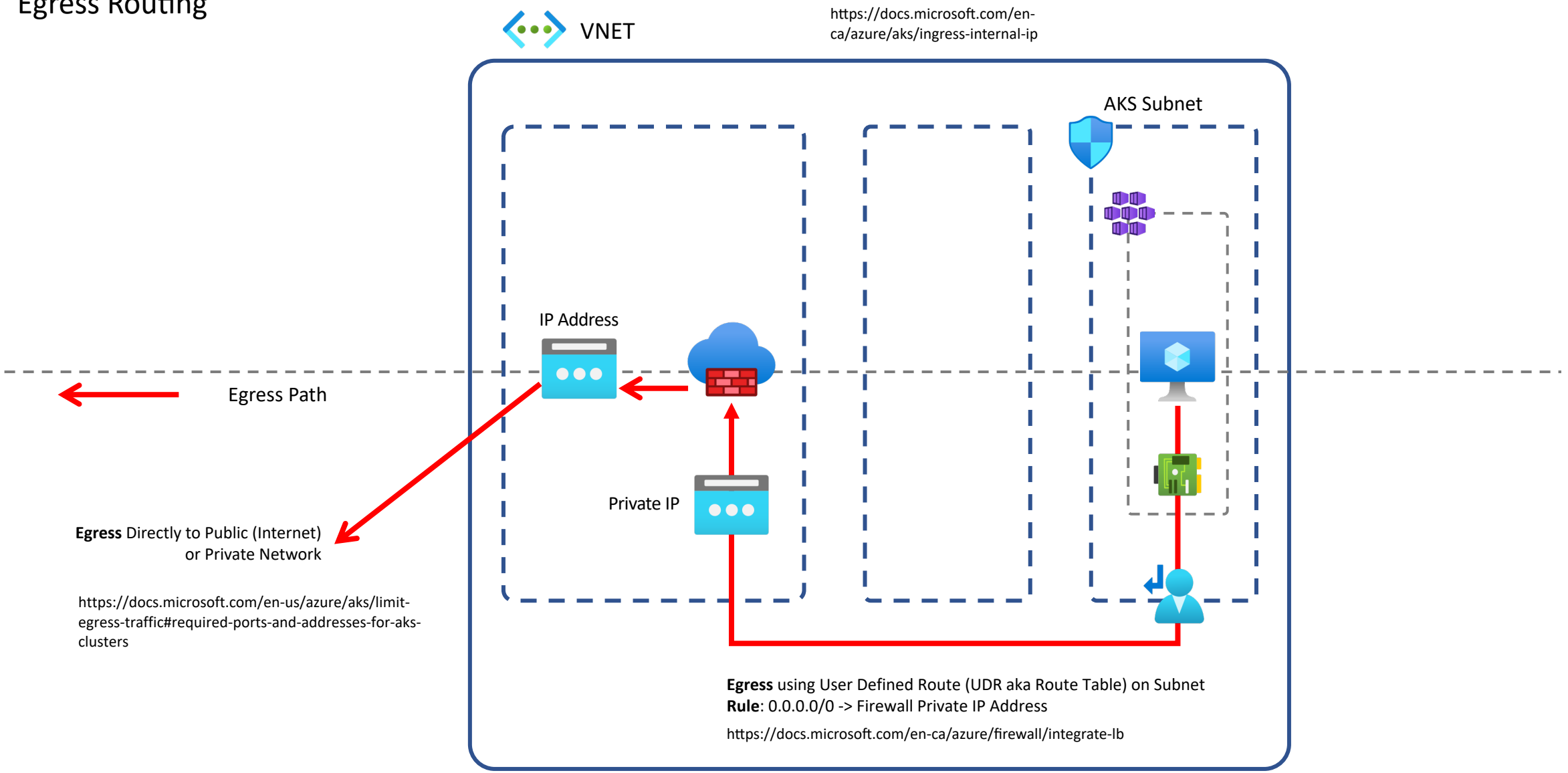


- AKS Control Plane is only Azure Private Network Addressable
  - Peered (VPN, Azure VNET Peering Etc.) is ok
- Can Bring your own DNS
  - Create a private Azure Kubernetes Service cluster - Azure Kubernetes Service | Microsoft Docs
  - GBB office hours:
    - Recording:
      - https://www.youtube.com/watch?v=8Q2olWtNHBw
    - Links:
      - aks-gbb-officehours/Resources.md at main · Azure/aks-gbb-officehours (github.com)
    - Shoutout: @SteveGriffith

Ingress Routing



Egress Routing



Networking + Observability: Service Mesh considerations

Do you need a Service Mesh?

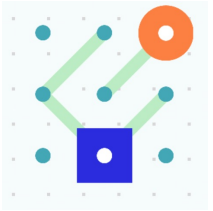
Scenarios

- Encrypt all cluster traffic
- Canary and Phased rollouts
- Traffic management
- Observability

Questions to ask

- Is an ingress controller sufficient?
- Can my environment handle the overhead?
- Can this be adopted incrementally?

Service Mesh Interface

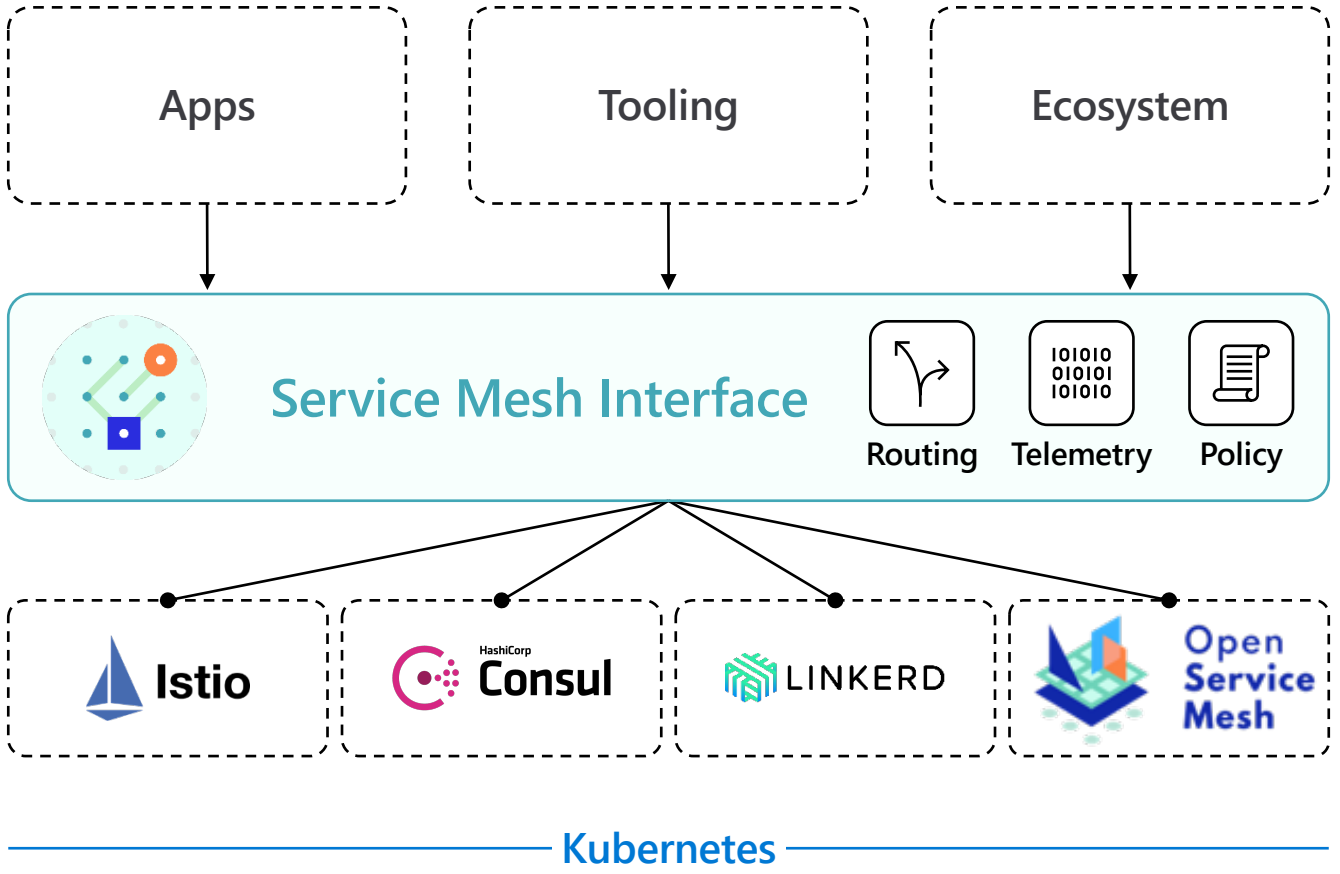


CLOUD NATIVE COMPUTING FOUNDATION

- A standard interface for service meshes on Kubernetes
- A basic feature set of the most common service mesh use cases
- Flexibility to support new service mesh capabilities over time
- Space for the ecosystem to innovate with service mesh technology

smi-spec.io

Service Mesh Interface



smi-spec.io

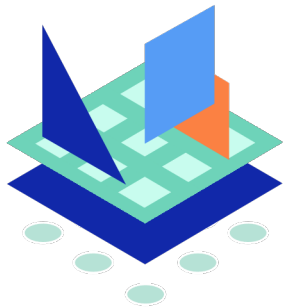
Service Mesh Landscape

- The original service mesh
- Purpose built
- Lightweight
- User Experience
- Kubernetes Only

- Developed Google+IBM
- Loosely based on Google Tech
- Feature rich
- Supports multi-cluster and VMs
- Complex (getting better)
- Envoy Proxy
- Feature rich

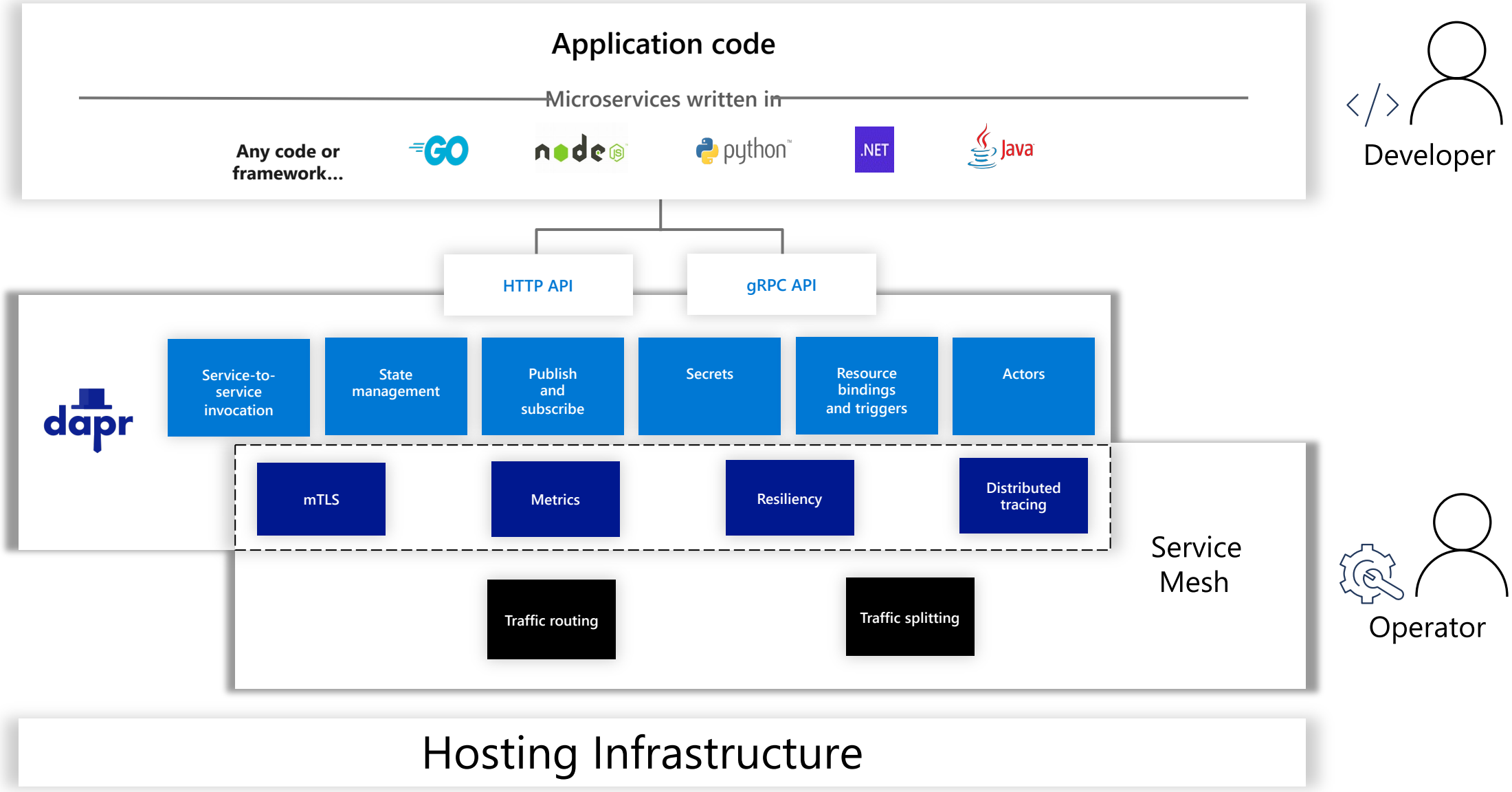
- Initially service discovery and distributed key/value store
- Rich support for hybrid architectures
- Lacks Observability features (getting better)
- Can be complex for initial setup/architecture
- Managed Service

Open Service Mesh



- AKS add-on in public preview
- Light-weight, extensible Cloud Native service mesh built on the CNCF envoy project
- Implements the most common service mesh features
- Quickly enable traffic shifting, mTLS, access control policies, etc. running in AKS

Dapr vs. Service Mesh



Observability:
Intra-cluster scanning

Intra-Cluster Scanning

- Control Plane (e.g. Kube-Hunter)
- Nodes
- Containers
- Monitoring/Logging
- Access Auditing
- Intelligent Logging/Reporting
- Anti-virus/Malware
- Node and Container “Recycling”/Ephemeral Lifecycles
  - Stateless vs. Stateful workloads

Some things to consider for scanning

- Kernel exploits
- DOS attacks from container (repeated socket opening/closing)
- Container privilege escalation
- Container runtime scanning

Tooling

- Aquasec
- Twistlock
- Snyk
- Sysdig
- Many others

Security & Governance Recommendations

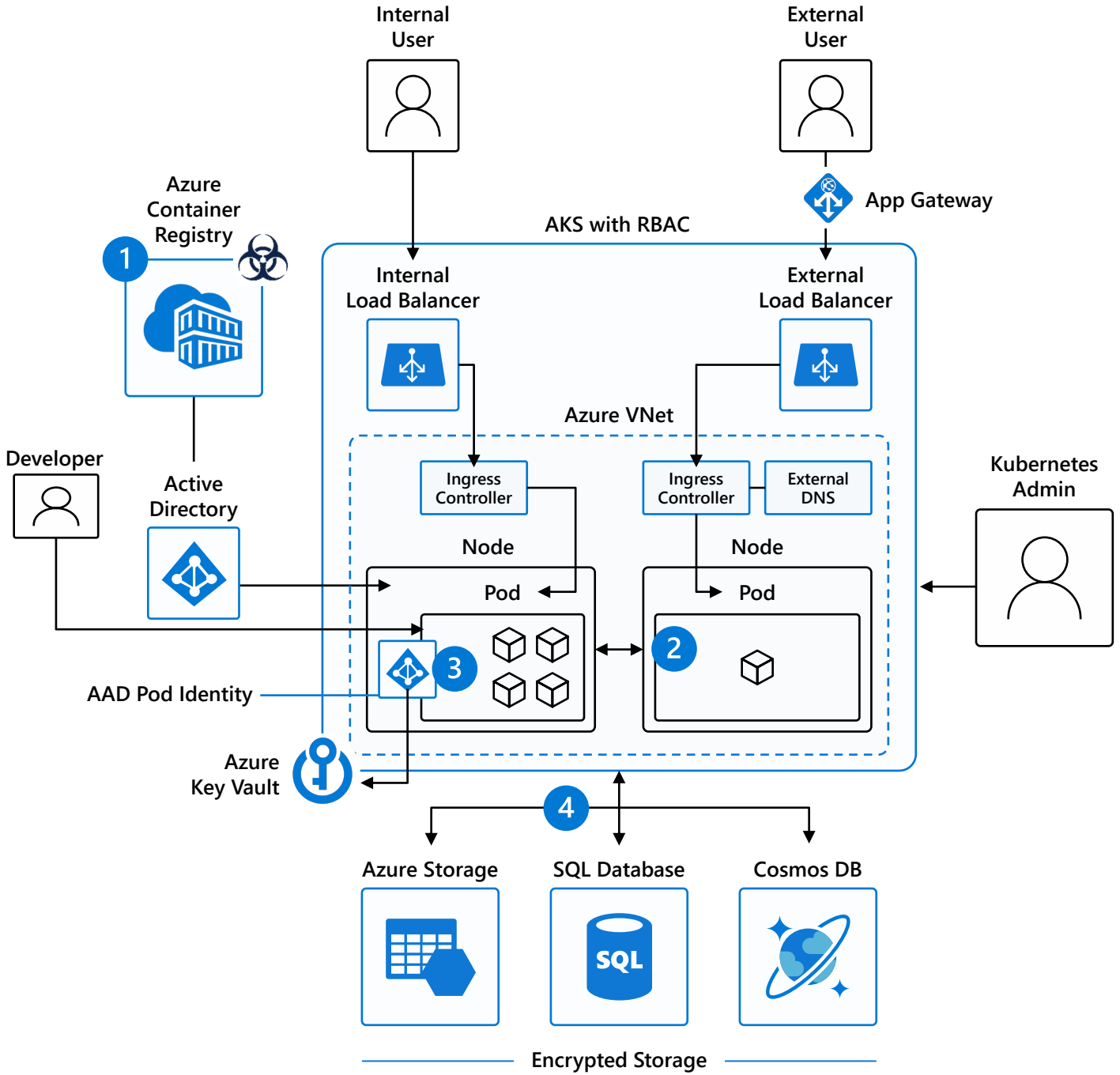
- Enable Azure Security Center (ASC) for AKS
- Enable Azure Policy for Policy Enforcement (e.g. Allowed Regions)
- Setup Egress Traffic Flow Patterns (Networking, Firewall, UDR, …)
- Capture AKS Control Plane Logs Related to AKS
- Use Azure AD, RBAC, Pod Identity, etc.

KEEP IN MIND: Cluster Practices

- Secure access to the API server and cluster nodes
- Secure container access to resources
- Regularly update to the latest version of Kubernetes
- Establish an upgrade strategy that works for your organization
- Determine a cost management strategy (i.e KubeCost)
- Evaluate if a service mesh is necessary for your organization
- **Ensure a container runtime security & image management solution is in place**

Security overview

1. **Image and container level security**
   - AAD authenticated Container registry access
   - ACR image scanning and content trust for image validation
2. **Node and cluster level security**
   - Automatic security patching nightly
   - Nodes deployed in private virtual network subnet w/o public addresses
   - Network policy to secure communication paths between namespaces (and nodes)
   - Pod Security Policies
   - K8s RBAC and AAD for authentication
   - Control egress traffic for AKS cluster nodes
3. **Pod level security**
   - Pod level control using AAD Pod Identity
   - Pod Security Context
4. **Workload level security**
   - Azure Role-based Access Control (RBAC) & security policy groups
   - Secure access to resources & services (e.g. Azure Key Vault) via Pod Identity
   - Storage Encryption
   - App Gateway with WAF to protect against threats and intrusions
   - Traffic management, resiliency, policy, security, strong identity, and observability to the workloads with Service Mesh



Additional Q&A

Join us for AKS Office Hours!

Hosted by the Cloud Native GBB Team every other Thursday from 11-12 CST!

- Provide AKS customers with updates pertaining to AKS and the Cloud Native Ecosystem
- Host a short talk and/or demo on Cloud Native technologies related to Kubernetes and AKS
- Collect feedback from customers on issues, blockers, use cases, and questions related to AKS

Other Resources

AKS Public Office Hours

https://aka.ms/akspublicofficehours

Microsoft Cloud Native GBB YouTube Channel:

https://www.youtube.com/channel/UCvdABD6_HuCG_to6kVprdjQ

Kubernetes Learning Path:

https://azure.microsoft.com/en-us/resources/kubernetes-learning-path/

AKS Checklist:

https://www.the-aks-checklist.com

AKS Solution Journey

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/containers/aks-start-here

AKS Workshop (MS Learn):

https://docs.microsoft.com/en-us/learn/modules/aks-workshop/

GBB AKS Secure Workshop:

https://github.com/CloudNativeGBB/aks-secure-workshop