Getting Started with Azure Kubernetes Service

Srikant Sarwa

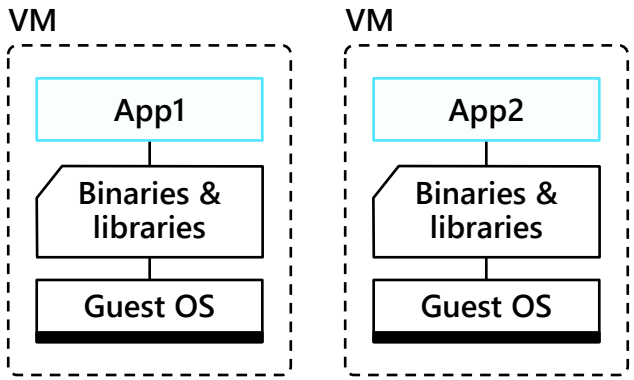
Senior Customer Engineer

Microsoft Azure – FastTrack for Azure

Agenda

- Containers – getting started
- Kubernetes – Architecture and basic terminology
- AKS – Azure’s managed service offering
- Best practices with Operational Guidance

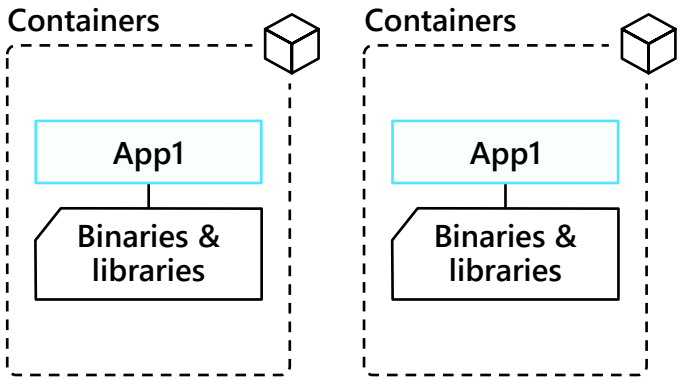
What is a container



Virtual machines

Virtualize the hardware

VMs as units of scaling

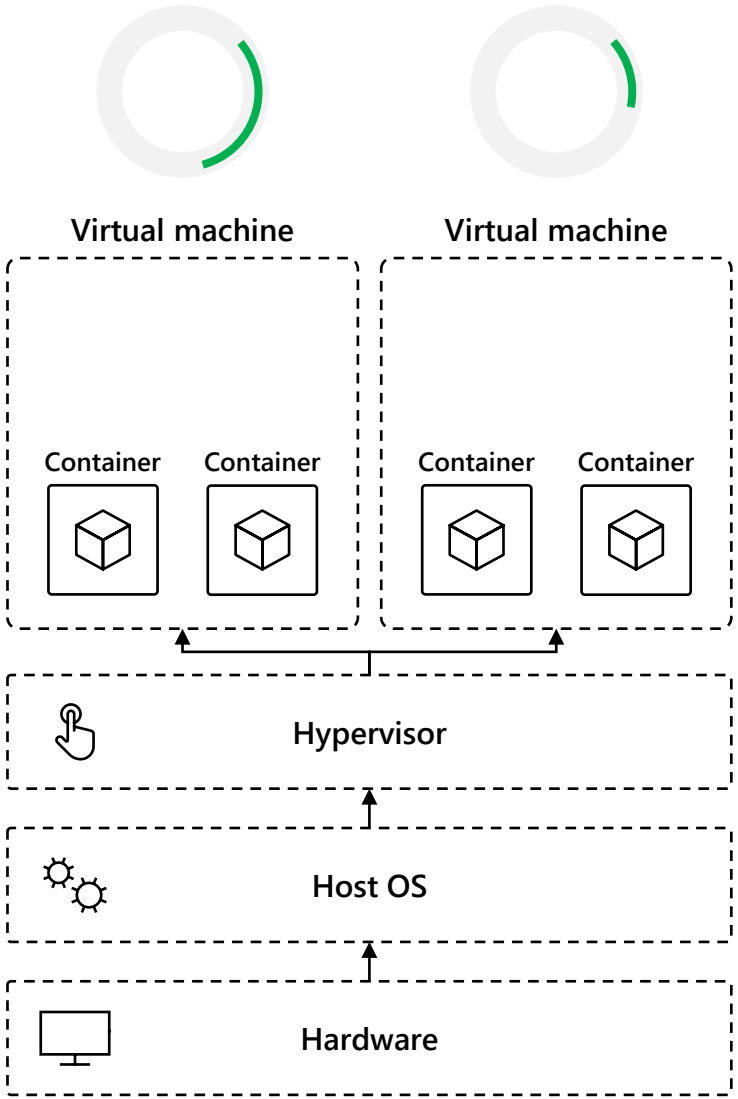


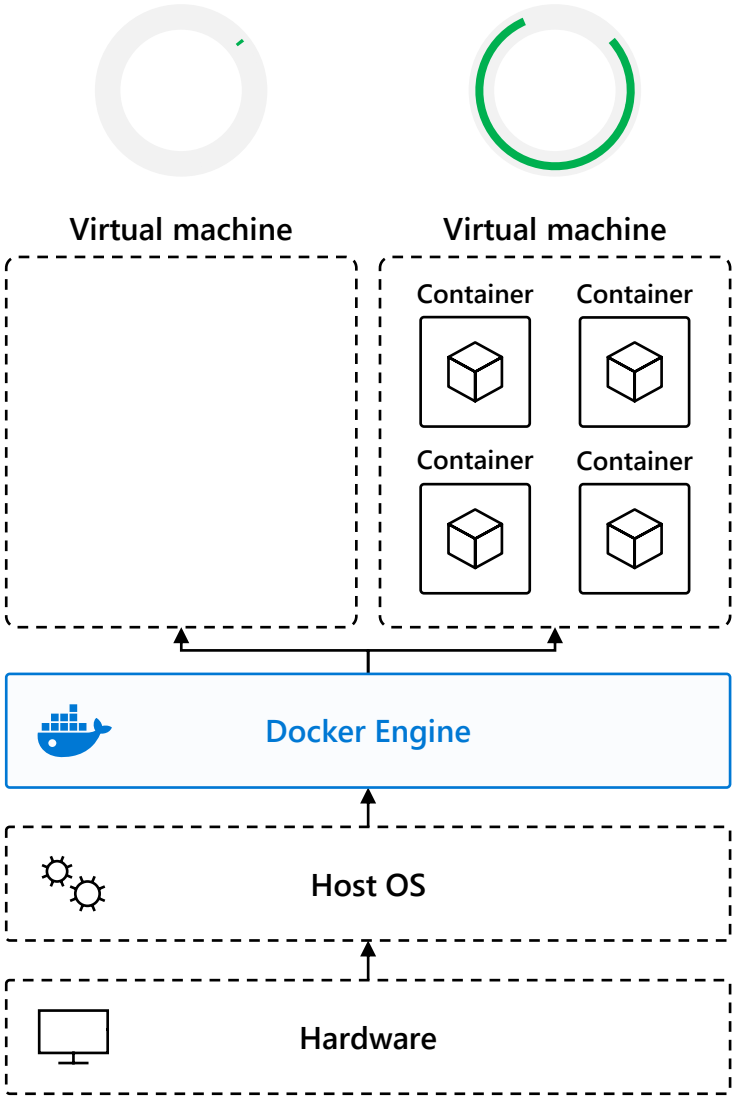
Containers

Virtualize the operating system

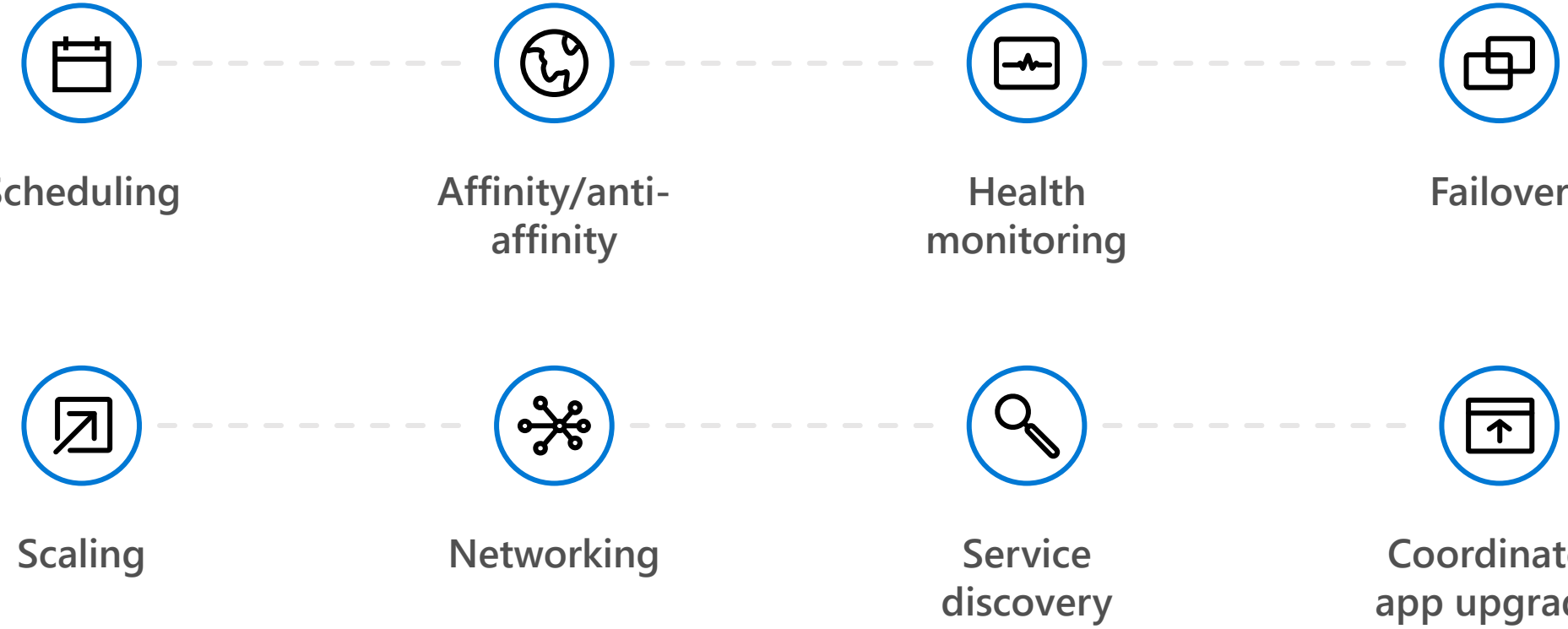
Applications as units of scaling

Traditional vs Modern approach on Containers



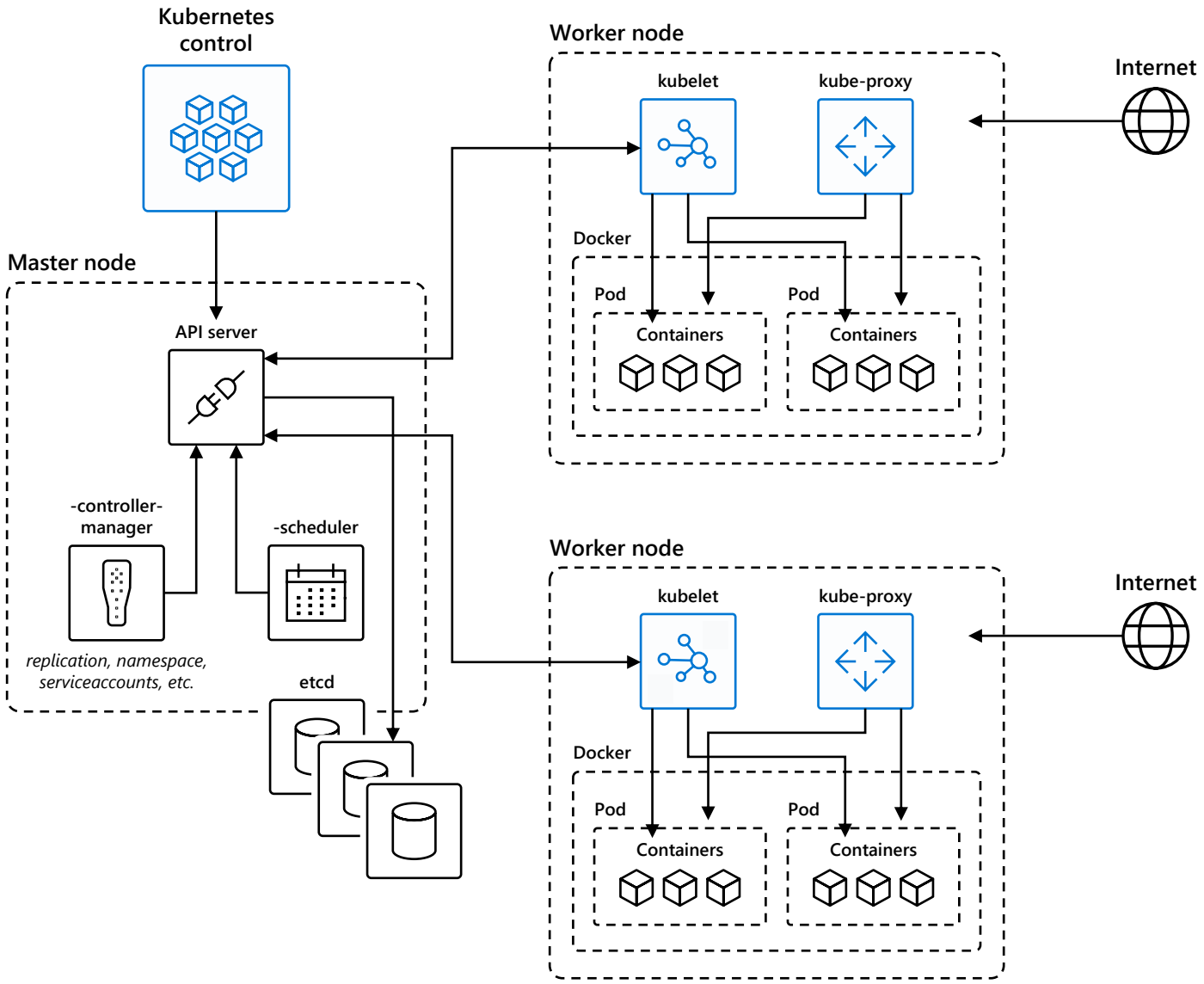


The elements of orchestration



Kubernetes Architecture

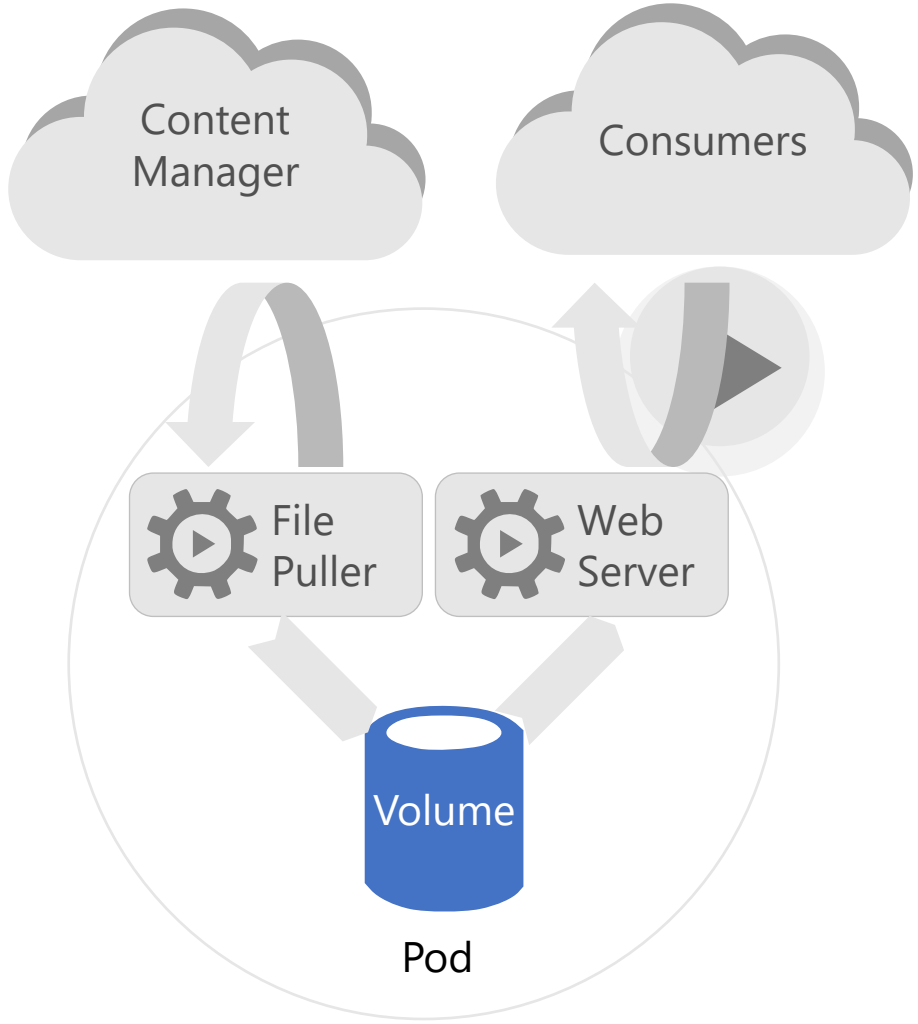
1. Kubernetes users communicate with API server and apply desired state
2. Master nodes actively enforce desired state on worker nodes
3. Worker nodes support communication between containers
4. Worker nodes support communication from the Internet



Kubernetes Resources

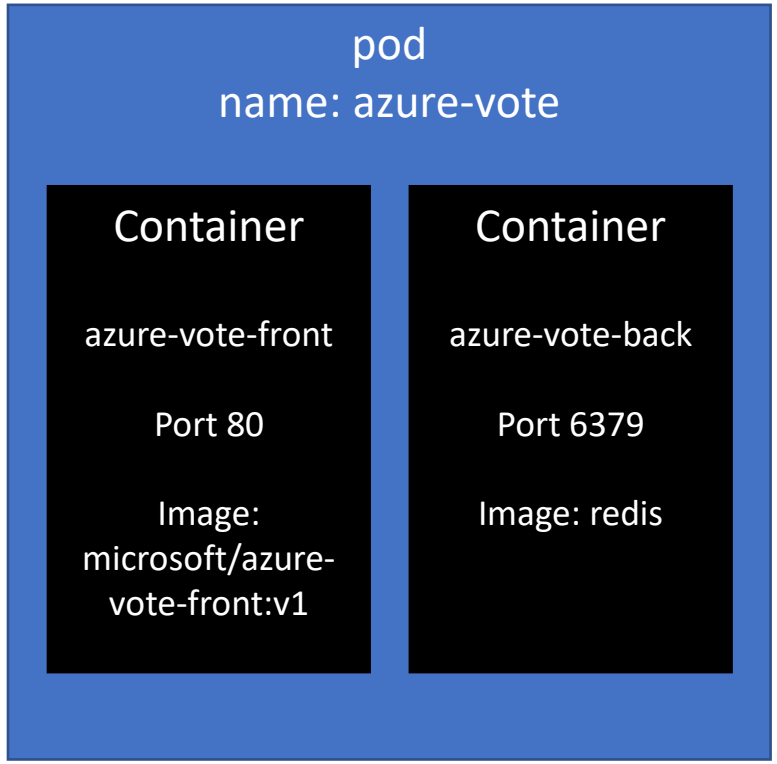
What is a pod?

- Pod is the basic building block in Kubernetes
- Pods are how containers are delivered
- Can be multiple containers (e.g. side car)
- Encapsulates container(s), storage, network IP, and options on how to run



Kubernetes manifest: Pod

```
apiVersion: v1
kind: Pod
metadata:
  name: azure-vote
  labels:
    app: web
spec:
  containers:
    - name: azure-vote-front
      image: microsoft/azure-vote-front:v1
      ports:
        - containerPort: 80
    - name: azure-vote-back
      image: redis
      ports:
        - containerPort: 6379
```



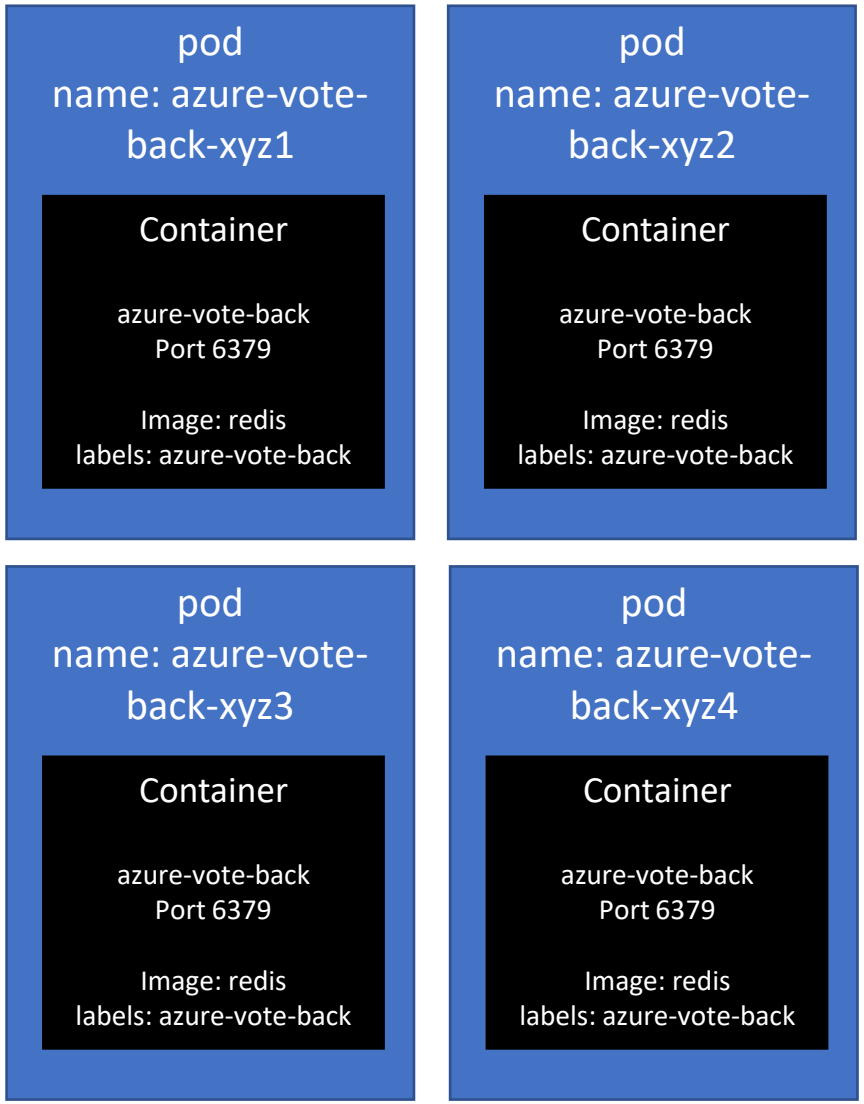
What is a deployment?

Deployment provides declarative updates for Pods and ReplicaSets.

- Create deployment to rollout **ReplicaSet**
- Declare new state for pods (eg – new imageTag)
- Rollback to earlier revision
- Scale up or down
- Check rollout history
- Clean-up older ReplicaSets

Kubernetes manifest: Deployment

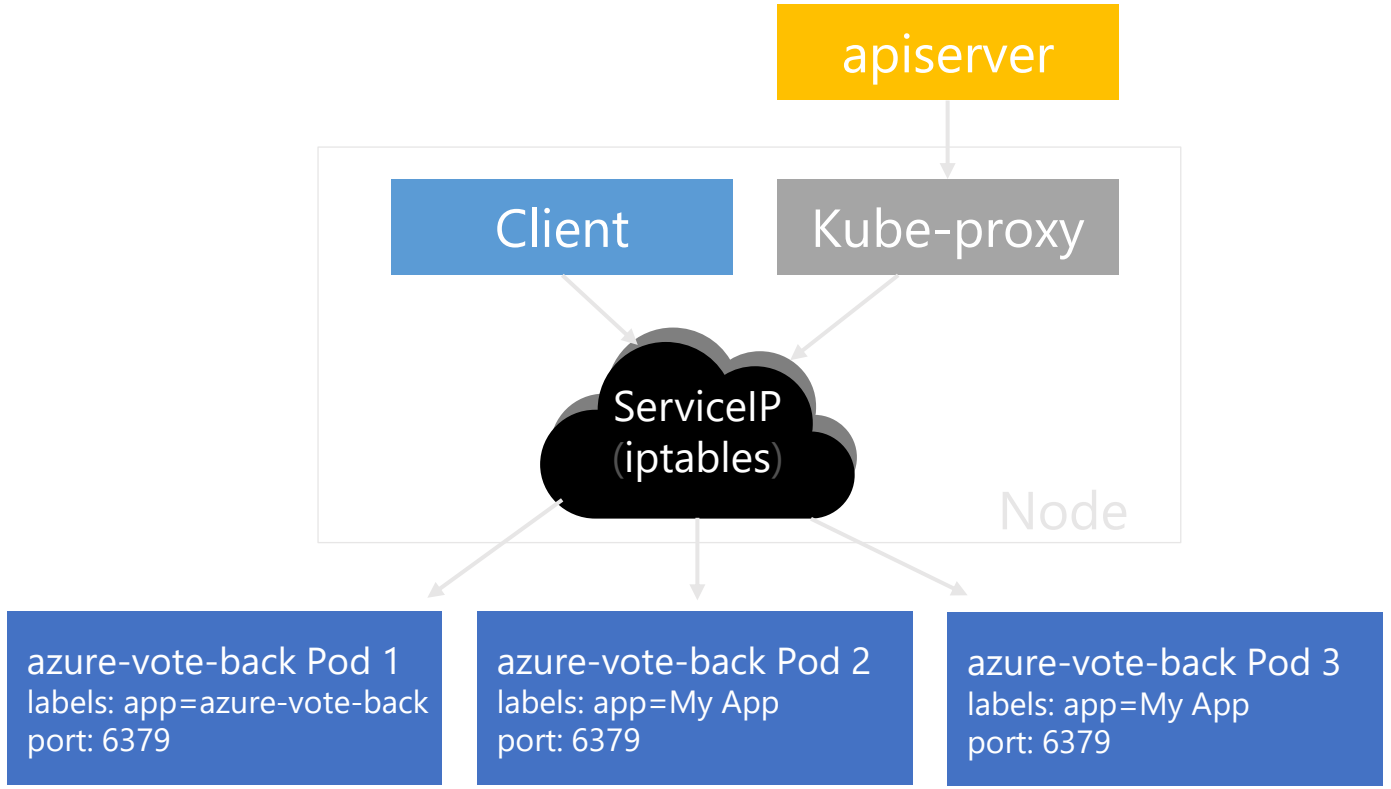
```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: azure-vote-back
spec:
  replicas: 4
  template:
    metadata:
      labels:
        app: azure-vote-back
    spec:
      containers:
      - name: azure-vote-back
        image: redis
        ports:
        - containerPort: 6379
```



What is a service?

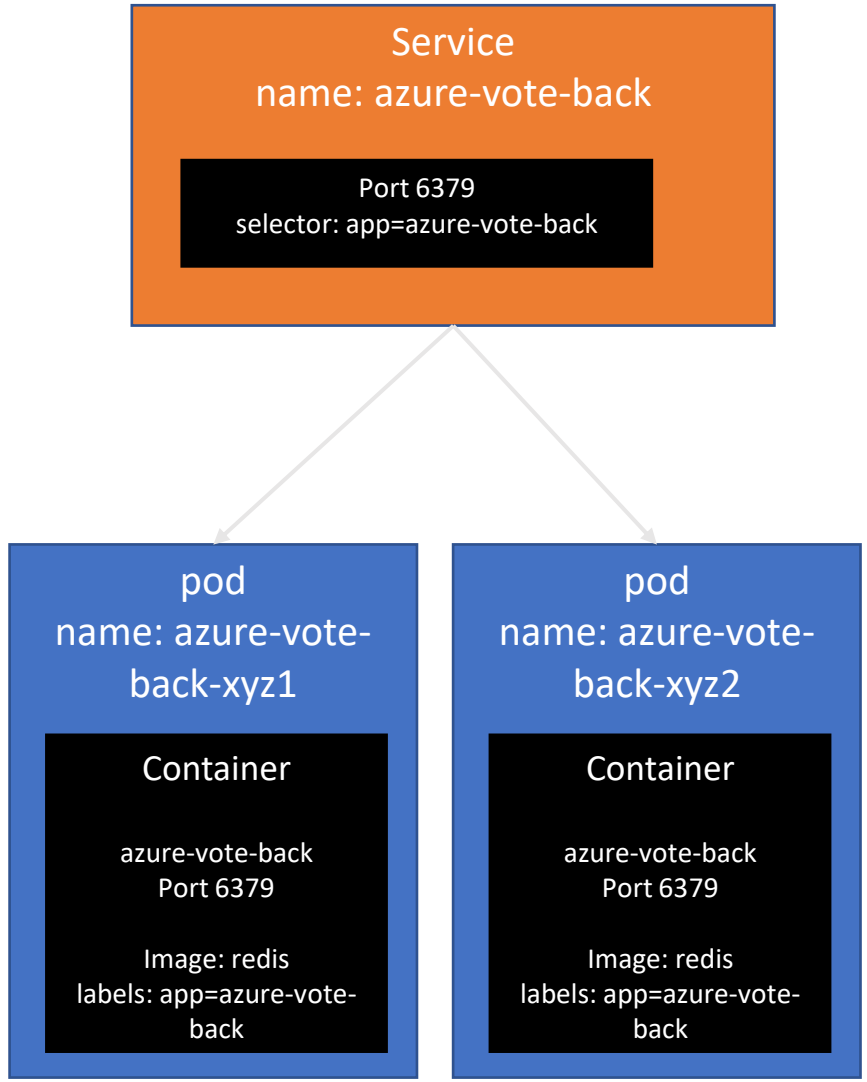
Essentially a load balancer in front of pods

- Defines a logical set of pods
- Identified/selected using Labels



Kubernetes manifest: Service

```
apiVersion: v1
kind: Service
metadata:
  name: azure-vote-back
spec:
  ports:
  - port: 6379
  selector:
    app: azure-vote-back
```

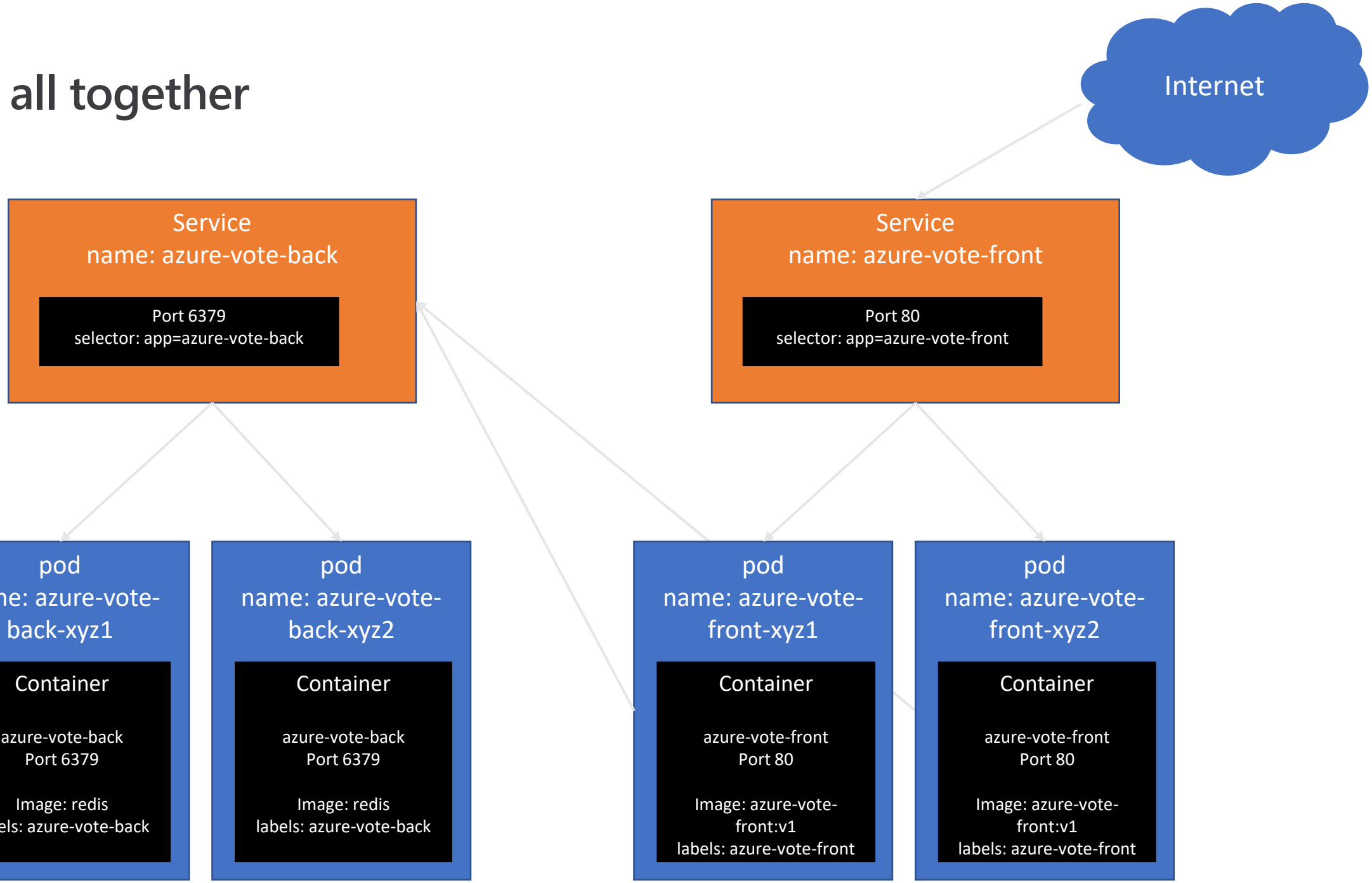


Namespaces

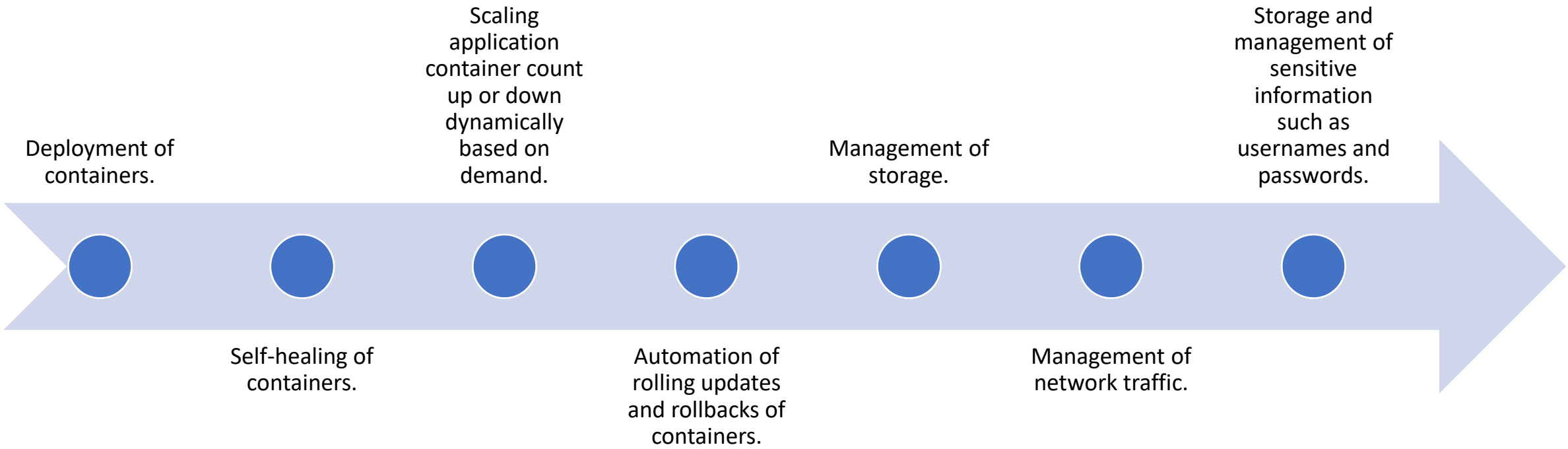
- multiple virtual clusters backed by the same physical cluster
- logical separation/isolation
- Every resource type is scoped to a namespace
  (except for nodes, persistentVolumes, etc.)
- Intended for environments with many users, teams, projects
- Kube-system namespace for dashboard etc.

```
root@srikantsarwa:~# kubectl get namespaces
NAME              STATUS   AGE
default           Active   3h1m
kube-node-lease   Active   3h1m
kube-public       Active   3h1m
kube-system       Active   3h1m
```

Bring it all together

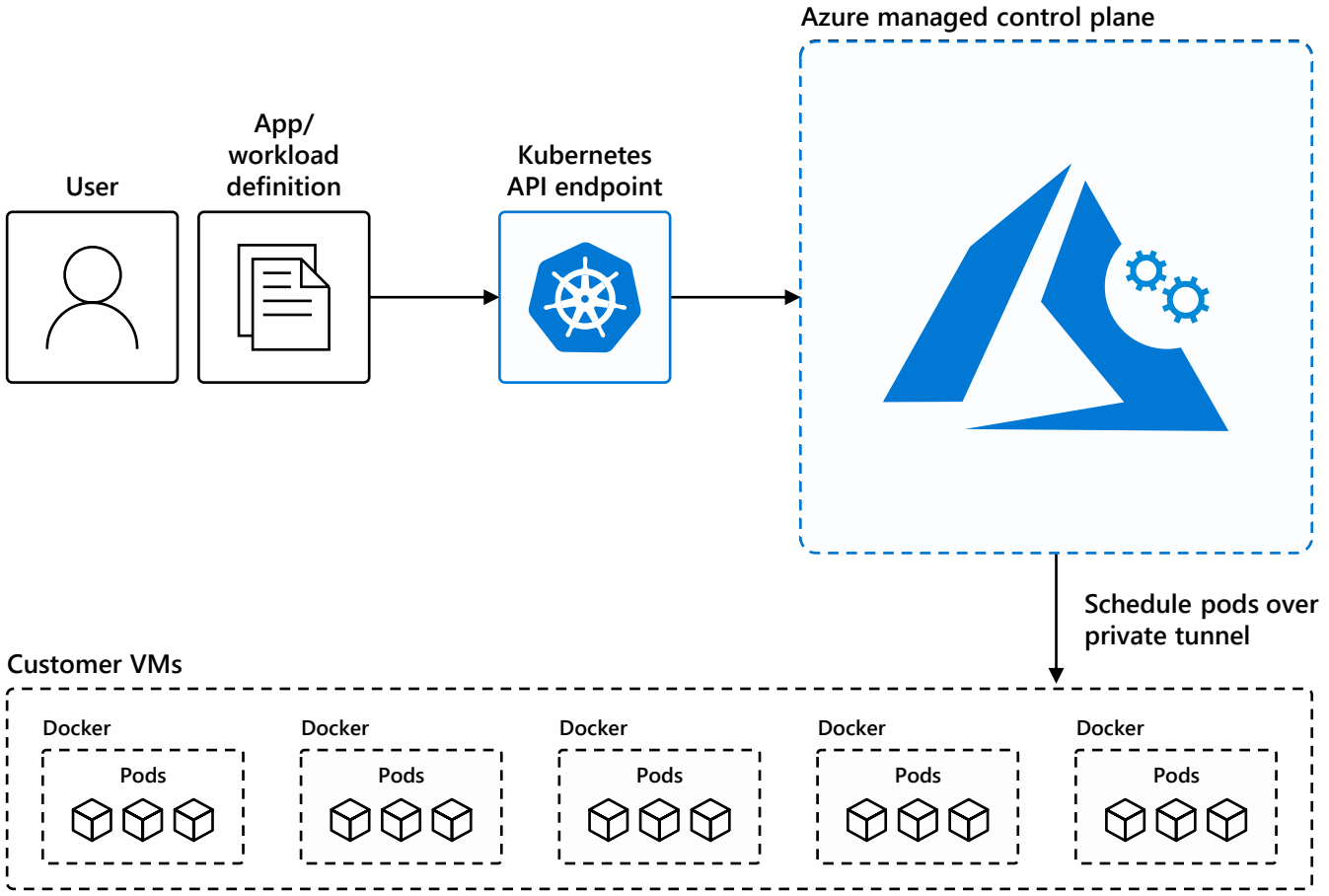


Kubernetes Benefits



Managed Kubernetes on Azure

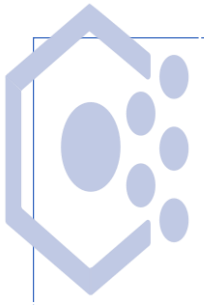
- Automated upgrades, patches
- High reliability, availability
- Easy, secure cluster scaling
- Self-healing
- API server monitoring
- At no charge



Best Practices for AKS

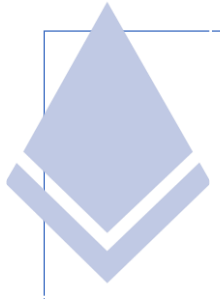
Networking configuration

- Network topology
- Plan the IP addresses
- Deploy Ingress resources



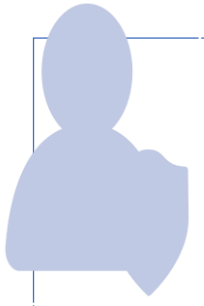
Cluster compute

- Compute for the base cluster
- Container image reference
- Policy management



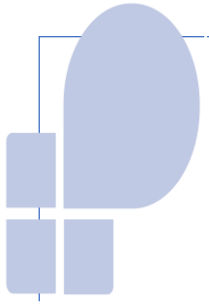
Identity management

- Integrate Azure AD for the cluster
- Integrate Azure AD for the workload



Secure data flow

- Secure the network flow
- Add secret management



Business continuity

- Scalability
- Cluster and node availability
- Availability and multi-region support

Operations

- Cluster and workload CI/CD pipelines
- Cluster health and metrics
- Cost management and reporting

Baseline AKS Cluster setup

Use Hub and Spoke Architecture for Networking design

- Hub VNET - Azure Firewall, Gateway, Bastion
- Spoke VNET - Application Gateway, Cluster Nodes

Container Image Reference

Make use of Azure Container Registry, AKS provides addon to attach the ACR

Pull images from authorized registries

Associate Kubernetes RBAC with Azure AD

Deploy Ingress Resource

Nginx, AGIC

Deploy WAF

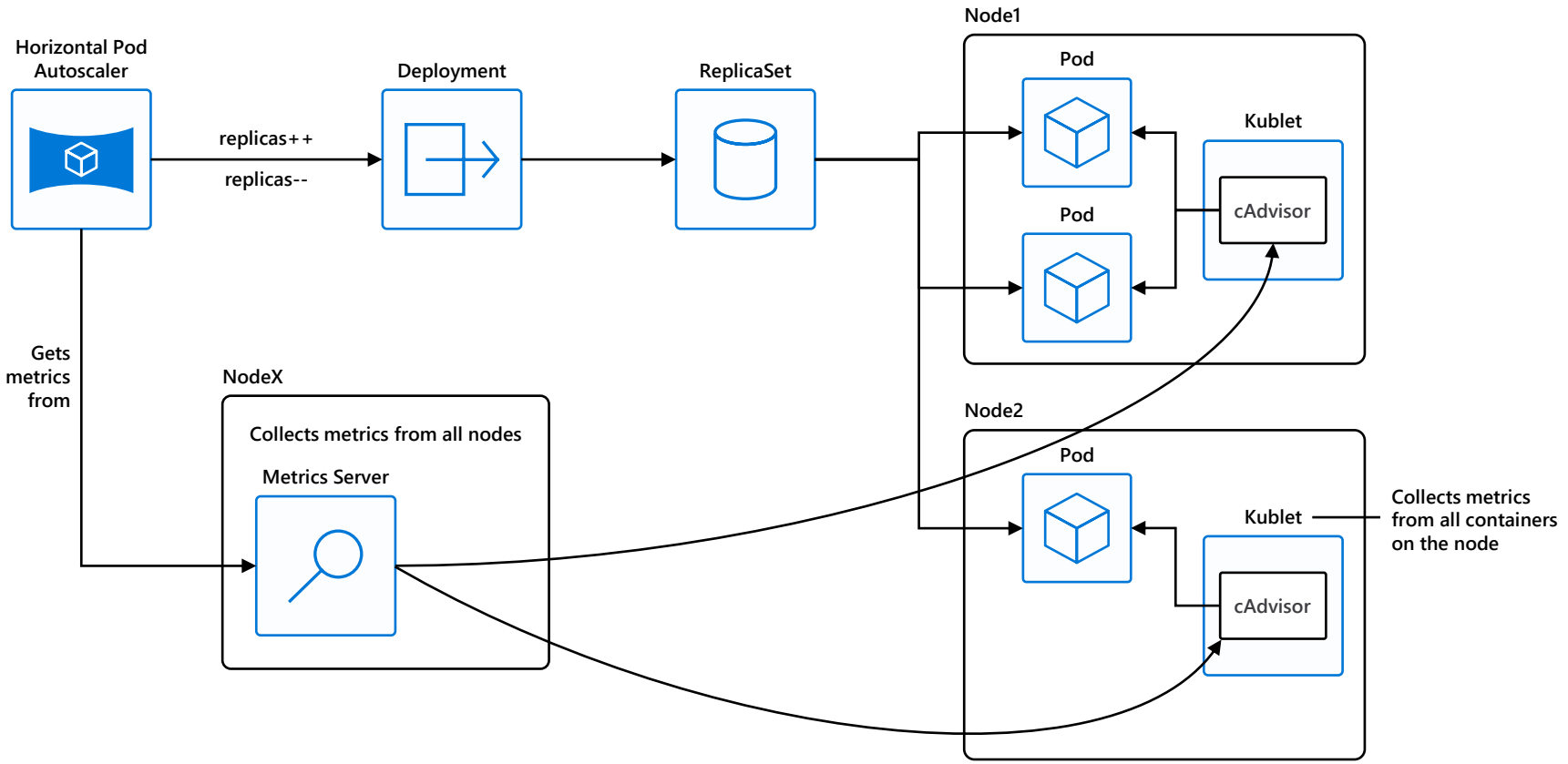
Use Azure Policy integrated with AKS

Node and pod scalability

Horizontal Pod Autoscaler

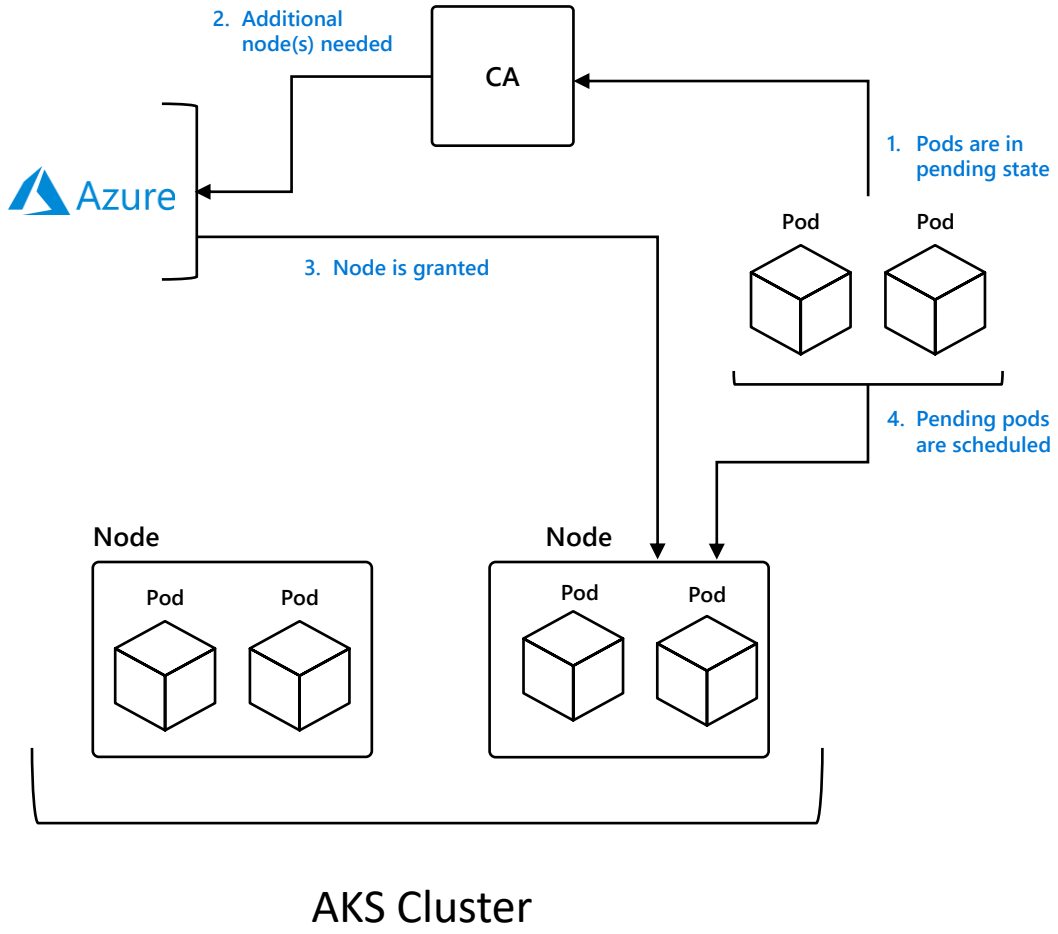
Cluster Autoscaler

Horizontal Pod Autoscaler

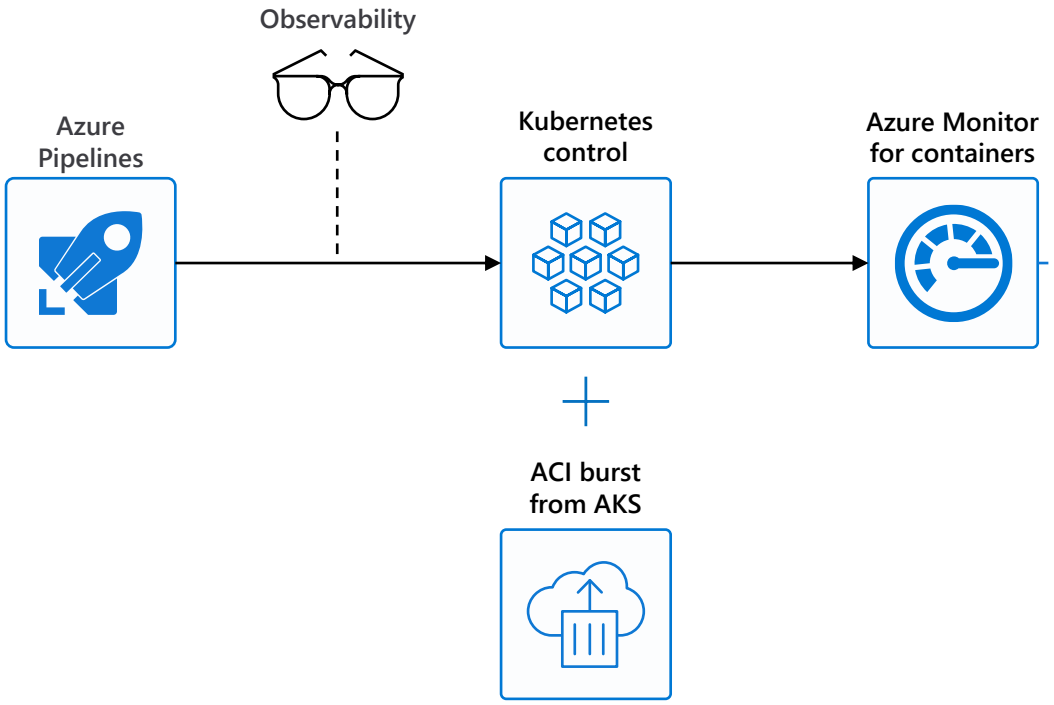


Cluster Autoscaler

- Scales nodes based on pending pods
- Scale up and scale down
- Reduces dependency on monitoring
- Removes need for users to manage nodes and monitor service usage manually



Azure Monitor for containers



Visualization
Visualize overall health and performance from clusters to containers with drill downs and filters

Insights
Provide insights with multi-cluster health roll up view

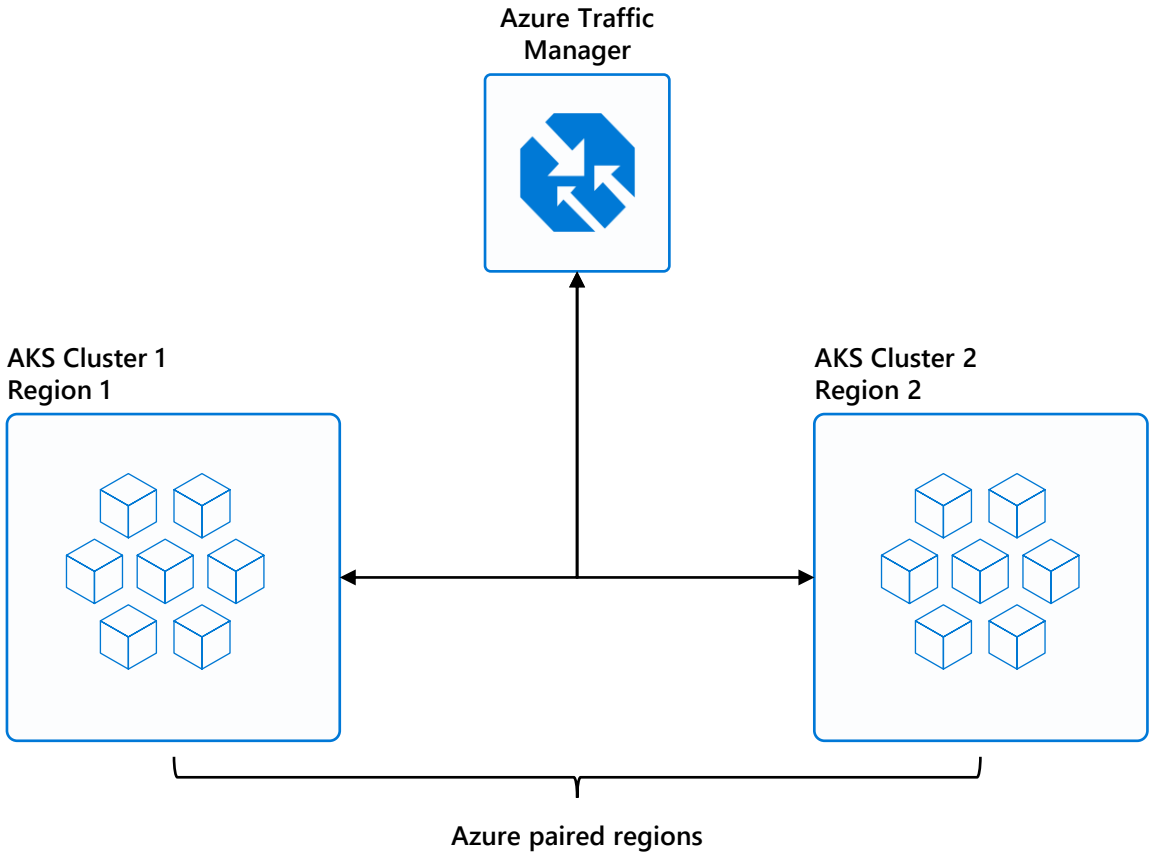
Monitor & Analyze
Monitor and analyze Kubernetes and container deployment performance, events, health, and logs

Response
Native alerting with integration to issue managements and ITSM tools

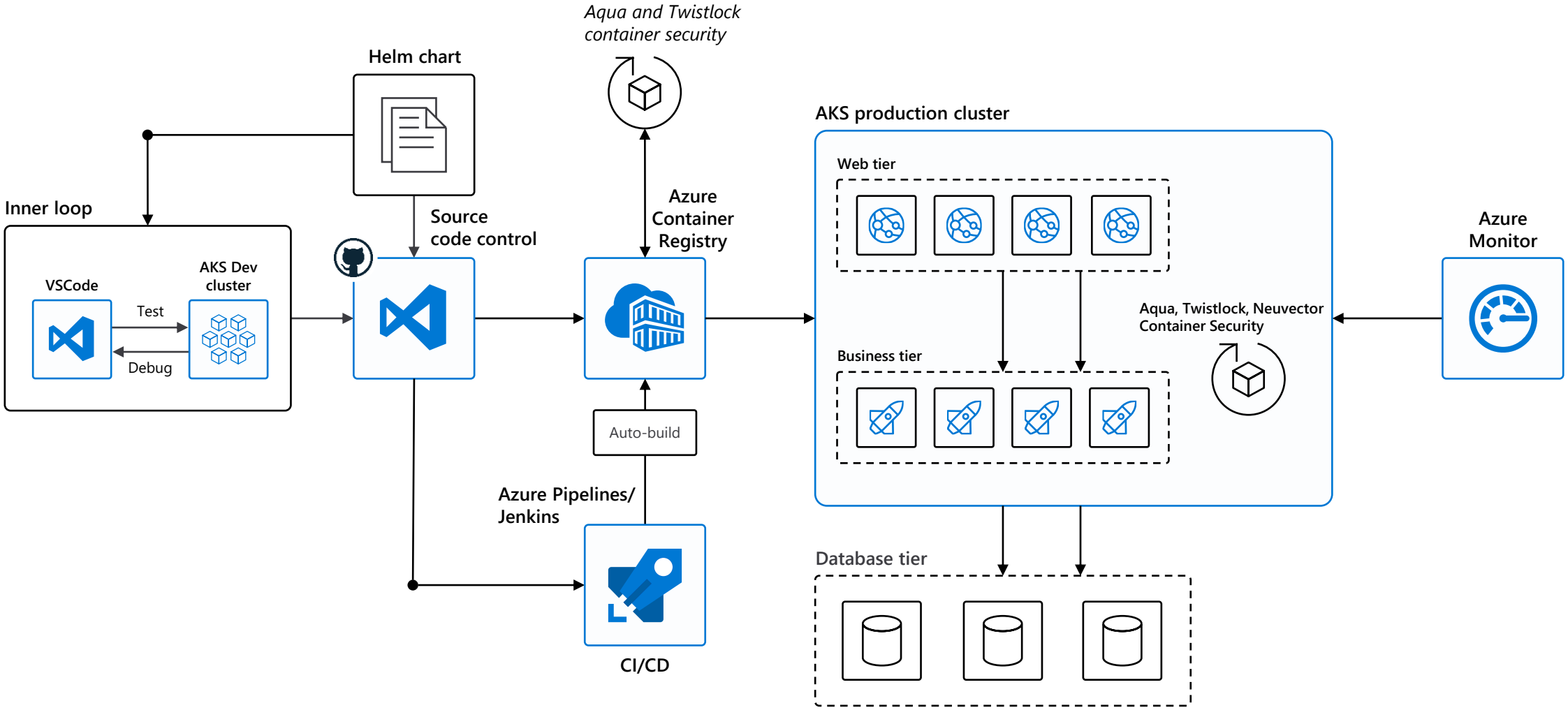
Observability
Observe live container logs on container deployment status

Multi-Region Clusters

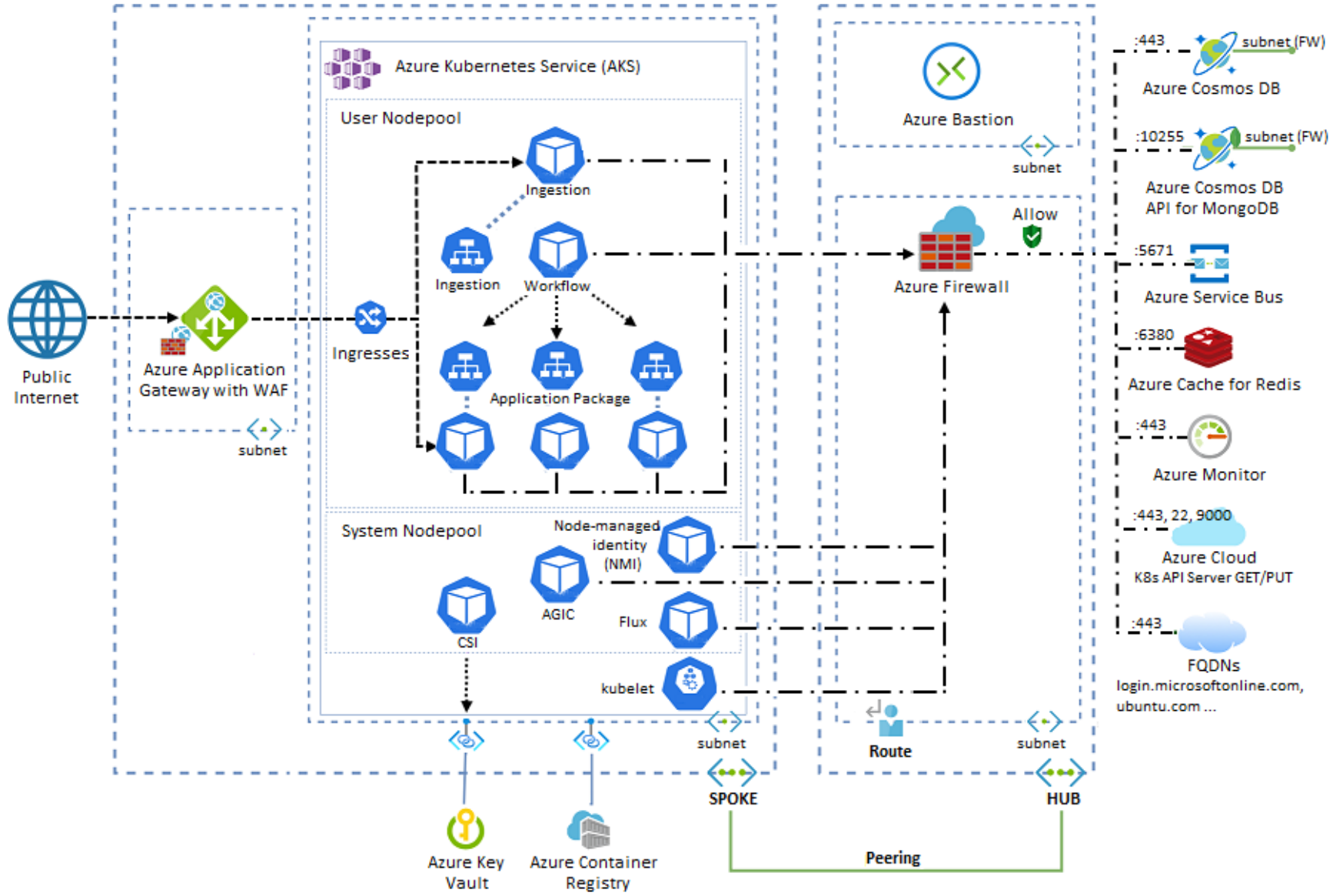
- Minimize downtime risk
- One live region
  - Another backup
  - Or weighted traffic
- A/B testing



DevOps


Aqua and Twistlock
container security
Helm chart
Inner loop
VSCode
AKS Dev
cluster
Test
Debug
Source
code control
Azure
Container
Registry
AKS production cluster
Web tier
Business tier
Aqua, Twistlock, Neuvector
Container Security
Azure
Monitor
Auto-build
Azure Pipelines/
Jenkins
CI/CD
Database tier

Production AKS Cluster workload Architecture



Containers in Azure

App Service

Deploy web apps or APIs using containers in a PaaS environment

Service Fabric

Modernize .NET applications to microservices using Windows Server containers

Kubernetes Service

Scale and orchestrate Linux containers using Kubernetes

Container Instance

Elastically burst from your Azure Kubernetes Service (AKS) cluster

Functions

Run code on-demand without having to explicitly provision or manage infrastructure

Batch

Run large-scale parallel and high-performance computing (HPC) applications efficiently in the cloud

IoT Edge

Move cloud analytics and custom business logic to devices

Ecosystem

Bring your Partner solutions that run great on Azure

Azure Container Registry

Docker Hub

Choice of developer tools and clients

Demo!!!

Questions?

References

- Kubernetes Core Concepts - https://docs.microsoft.com/en-us/azure/aks/concepts-clusters-workloads
- Baseline Architecture - https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/containers/aks/secure-baseline-aks
- AKS Cluster tutorial - https://docs.microsoft.com/en-us/azure/aks/tutorial-kubernetes-deploy-cluster
- AKS Checklist - https://www.the-aks-checklist.com
- CICD for Containers - https://docs.microsoft.com/en-us/azure/architecture/example-scenario/apps/devops-with-aks