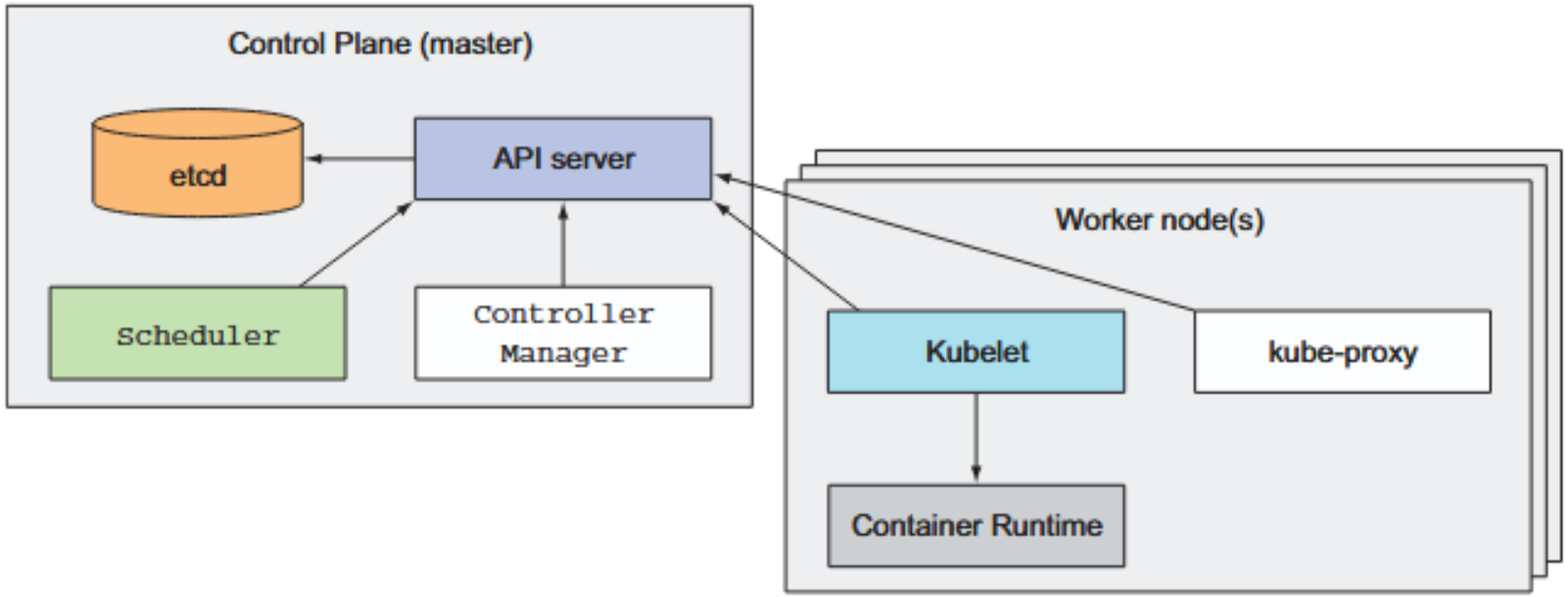
Kubernetes Workshop

What is Kubernetes?

- Greek for “helmsman of a ship”
- Project that spun out of Google
- Container orchestration platform
- Self-healing
- Autoscaling

Kubernetes Architecture



Control Plane Components

- **API Server:** Front door, all communication goes through here
- **Etcd:** Database, stores all cluster state
- **Scheduler:** Decides which node runs which Pod
- **Controller Manager:** Reconciliation loops, fixes differences between desired and actual state

Worker Node Components

- **Kubelet:** Agent on each node, ensures containers are running, reports status
- **Container Runtime:** Runs containers (containerd, CRI-O)
- **kube-proxy:** Network rules, routes traffic to Pods

Azure Kubernetes Service (AKS)

- Azure handles the control plane
- Cluster nodes are virtual machines
- Integration with other Azure services

Labs

- 1.00: Create an AKS cluster with the Azure CLI

kubectl

- Command-line tool to interact with K8s
- Talks to the API server
- Imperative

```
kubectl <verb> <resource> [name] [flags]
```

https://kubernetes.io/docs/reference/generated/kubectl/kubectl-commands

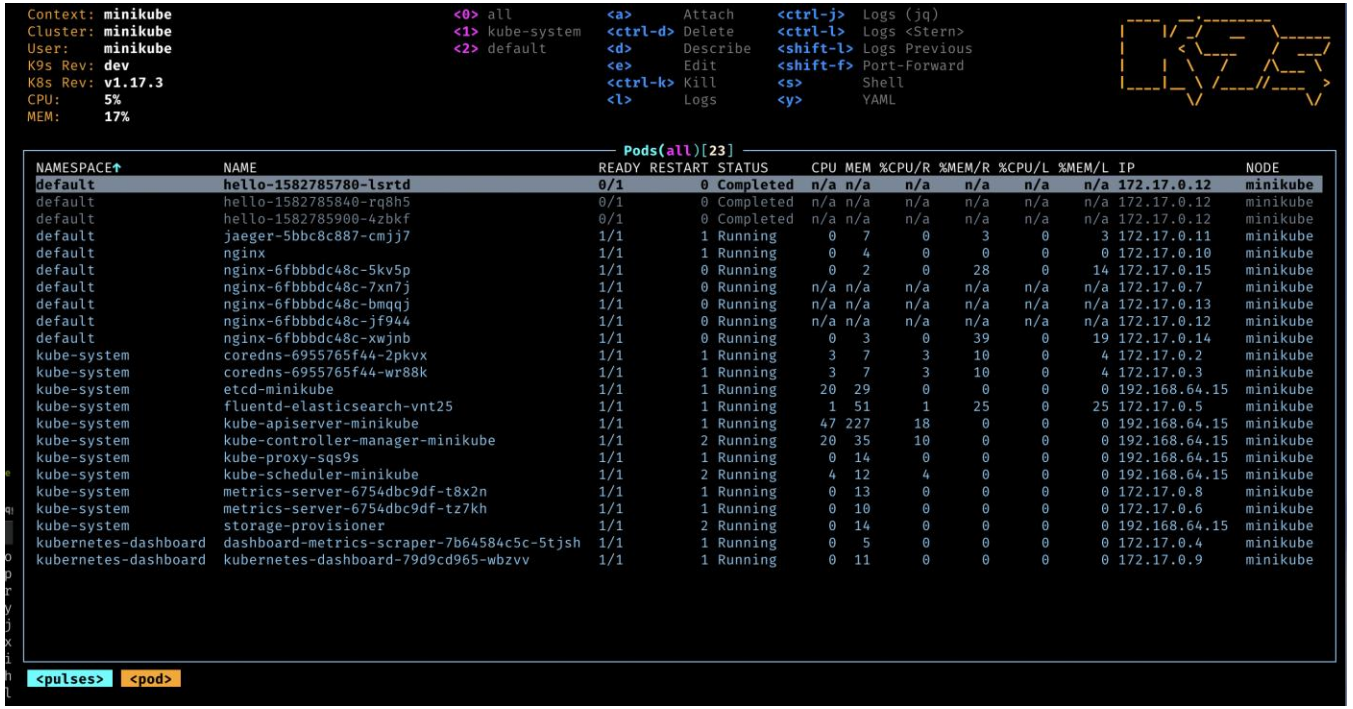
Manifests

- YAML
- Declarative
- GitOps

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: web
  labels:
    app: web
spec:
  containers:
    - name: nginx
      image: nginx:1.25
```

k9s

- Terminal UI to interact with Kubernets clusters
- https://k9scli.io/



Namespaces

- Virtual clusters within a cluster
- Isolate resources by team, environment, or project
- Resources in different namespaces can have the same name

```yaml
apiVersion: v1
kind: Namespace
metadata:
  name: prod
```

Default Namespaces

- default: The default namespace for any object without a namespace
- kube-system: Acts as the home for objects and resources created by Kubernetes itself
- kube-public: A special namespace; readable by all users that is reserved for cluster bootstrapping and configuration.

Pod

- Smallest deployable unit
- Wraps one or more containers
- Containers in a Pod share:
  - Network
  - Storage
  - Lifecycle
- Pods are ephemeral

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: nginx
spec:
  containers:
  - name: nginx
    image: nginx:1.28.1
    ports:
    - containerPort: 80
```

Labels and Selectors

- Key-value pairs attached to objects
- Identify, describe and group related objects
- Selectors use labels to filter or select objects

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: nginx
  labels:
    app: nginx
    env: prd
spec:
  containers:
  - name: nginx
    image: nginx:1.28.1
    ports:
    - containerPort: 80
```

Workloads

Deployments

- Manage one or more identical pods
- Most common way to run stateless apps
- Self-healing
- Scaling
- Rolling updates
- Rollbacks

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: web
spec:
  replicas: 3
  selector:
    matchLabels:
      app: web
  template:
    metadata:
      labels:
        app: web
    spec:
      containers:
        - name: nginx
          image: nginx:1.25
          ports:
            - containerPort: 80
```

DaemonSet

- Run exactly ONE pod per node
- Use cases
  - Monitoring agents
  - Log collectors
  - Backups
  - Security agents
  - Network plugins

```yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  name: fluentd
spec:
  selector:
    matchLabels:
      name: fluentd
  template:
    metadata:
      labels:
        name: fluentd
    spec:
      containers:
        - name: fluentd
          image: fluent/fluentd
```

Job

- Runs a task to completion
- Guarantees successful completion
- Retries on failure
- Perfect for:
  - Migrations
  - Batch processing
  - One-off tasks

```yaml
apiVersion: batch/v1
kind: Job
metadata:
  name: db-migration
spec:
  template:
    spec:
      containers:
        - name: migrate
          image: myapp
          command: ["python", "manage.py", "migrate"]
      restartPolicy: Never
  backoffLimit: 3
  ttlSecondsAfterFinished: 60
```

CronJob

- Scheduled Jobs
- Cron format (UTC!)

```yaml
apiVersion: batch/v1
kind: CronJob
metadata:
  name: backup
spec:
  schedule: "0 2 * * *"
  concurrencyPolicy: Forbid
  jobTemplate:
    spec:
      template:
        spec:
          containers:
            - name: backup
              image: backup-tool
          restartPolicy: Never
```

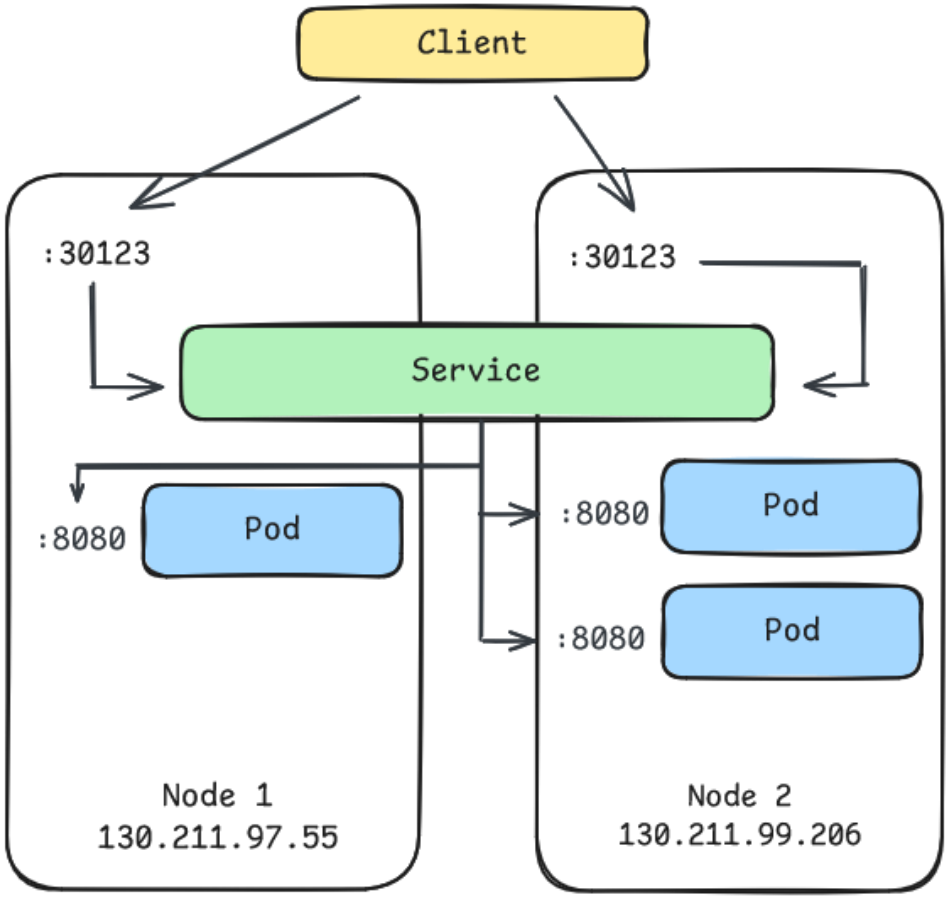
Networking

ClusterIP Service

- Default Service type
- Internal-only

```yaml
apiVersion: v1
kind: Service
metadata:
  name: nginx-service
spec:
  selector:
    app: nginx
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
```

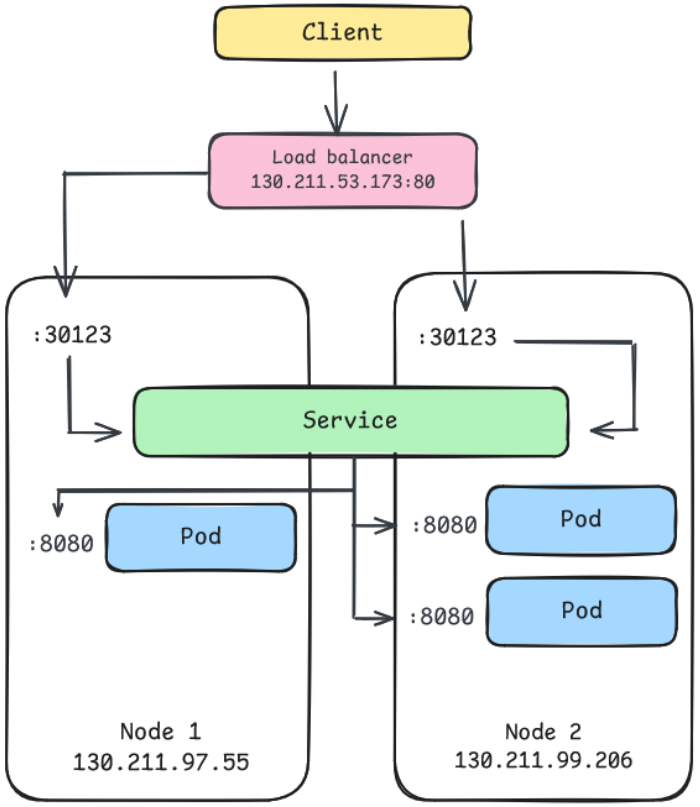
NodePort Service




```yaml
apiVersion: v1
kind: Service
metadata:
  name: my-app
spec:
  type: NodePort
  selector:
    app: my-app
  ports:
    - port: 80
      targetPort: 8080
      nodePort: 30080
```

LoadBalancer Service

- Azure automatically provisions an Azure Load Balancer




```yaml
apiVersion: v1
kind: Service
metadata:
  name: web
  annotations:
    # For internal LB (not public)
    service.beta.kubernetes.io/azure-load-balancer-internal: "true"
spec:
  type: LoadBalancer
  selector:
    app: web
  ports:
    - port: 80
```

Ingress

- HTTP/HTTPS routing at Layer 7
- Single point off entry for multiple services
- Path-based and host-based routing
- TLS termination
- AKS options:
  - Nginx Ingress Controller
  - Application Gateway Ingress Controller (AGIC)
- Retires in March 2026

Gateway API

- Next-generation replacement for Ingress
- More expressive, more features
- Azure App Gateway for Containers

Labs

- 1.01: Imperative commands
- 1.02: Create a Pod
- 1.03: Create a Deployment
- 1.04: Create a Job and CronJob
- 1.05: Create a Service

Storage

Container Storage Interface (CSI)

- Standard interface between Kubernetes and storage providers
- Allows any vendor to write a storage driver
- Runs as Pods in your cluster
- Azure Disk CSI Driver (block storage)
- Azure Files CSI Driver (file shares)
- Azure Blob CSI Driver (object storage)

PersistentVolumes (PV)

- Static or dynamic provisioning
- Reclaim policies
  - Retain: keep data after PV deleted

  Delete

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: my-pv
spec:
  capacity:
    storage: 100Gi
  accessModes:
    - ReadWriteOnce
  persistentVolumeReclaimPolicy: Retain
  storageClassName: managed-csi
  csi:
    driver: disk.csi.azure.com
    volumeHandle: /subscriptions/.../disks/<disk-name>
    volumeAttributes:
      fsType: ext4
```

PersistentVolumeClaims (PVC)

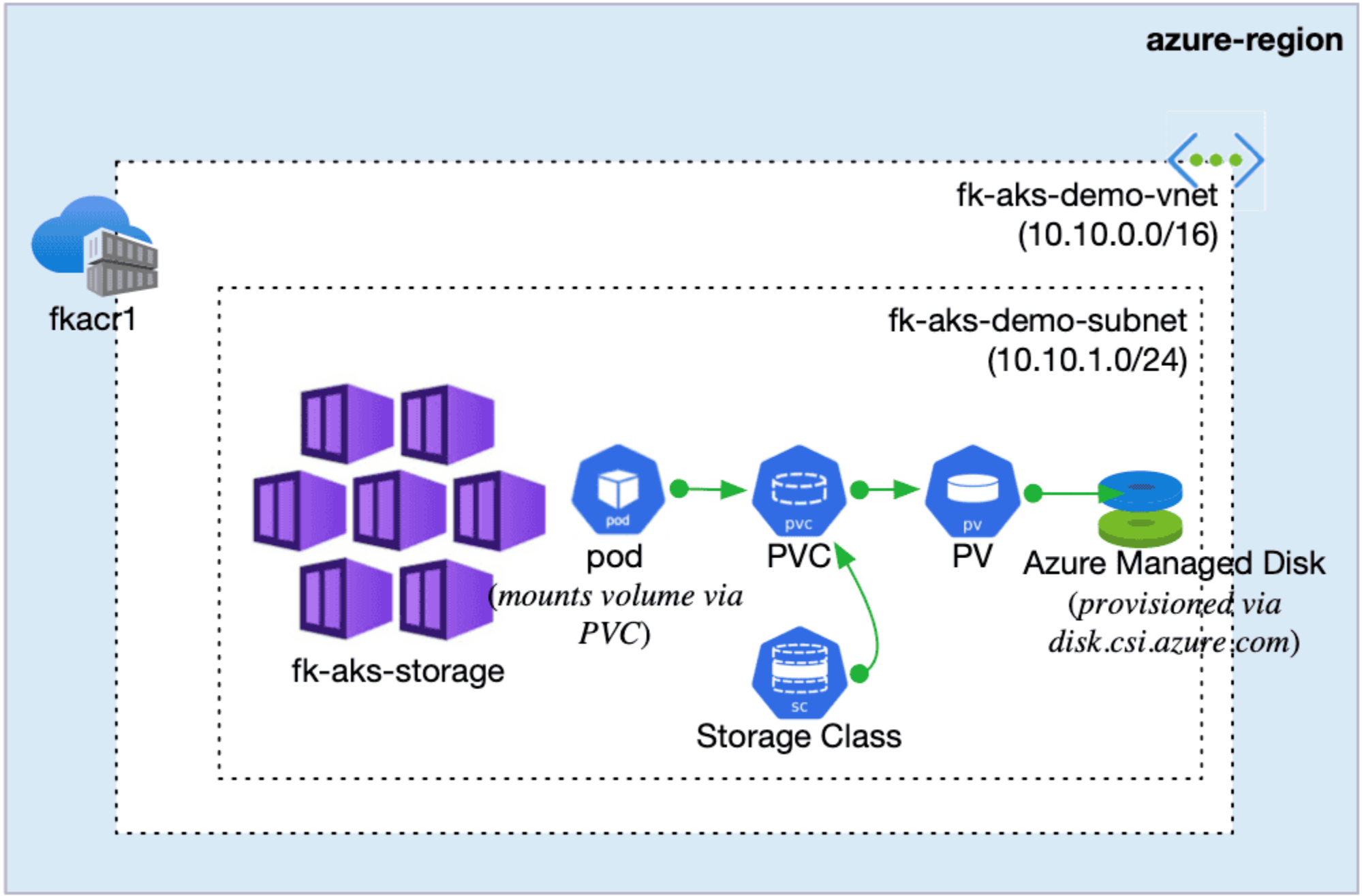
- A request for storage
- Specifies size, access mode, storage class
- Kubernetes finds or creates matching PV

```yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-data
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 50Gi
  storageClassName: managed-csi-premium
```

StorageClasses (SC)

- Defines a "class" of storage
- Enables dynamic provisioning

```yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: managed-csi-premium
provisioner: disk.csi.azure.com
parameters:
  skuName: Premium_LRS
reclaimPolicy: Delete
volumeBindingMode: WaitForFirstConsumer
allowVolumeExpansion: true
```


azure-region
fk-aks-demo-vnet
(10.10.0.0/16)
fkacr1
fk-aks-demo-subnet
(10.10.1.0/24)
fk-aks-storage
pod
(mounts volume via PVC)
PVC
PV
Azure Managed Disk
(provisioned via disk.csi.azure.com)
Storage Class

Init containers and sidecars

Init Containers

- Run **before** app containers start
- Run to completion
- Run in order

Sidecar Containers

- Start before the app
- Run alongside the app
- Shutdown after the app

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: web
spec:
  initContainers:
    - name: log-shipper
      image: fluent/fluent-bit:4.2.2
      restartPolicy: Always
  containers:
    - name: app
      image: nginx:1.29
```

Configuration

ConfigMaps

- Store configuration outside the pod and inject it at runtime
- **Non-sensitive** data:
  - Environment variables
  - Config files

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: app-config
data:
  DATABASE_HOST: "db.example.com"
  LOG_LEVEL: "info"
  MAX_CONNECTIONS: "100"
```

Secrets

- **Sensitive** data:
  - Passwords
  - API keys
  - SSH keys
- **Not encrypted by default**
- Base64 encoded

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: db-credentials
type: Opaque
data:
  username: YWRtaW4=
  password: c3VwZXJzZWNyZXQxMjM=
```

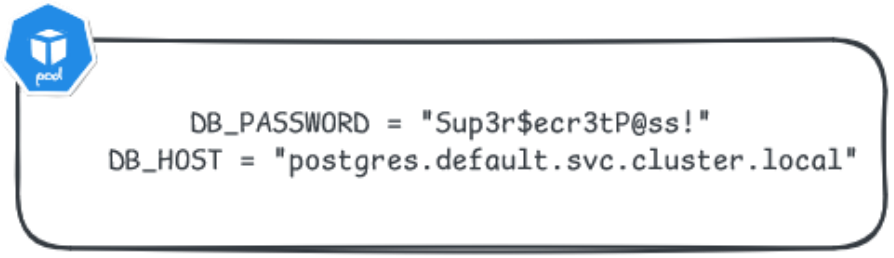
```yaml
apiVersion: v1
kind: Secret
metadata:
  name: db-credentials
type: Opaque
stringData:
  username: admin
  password: supersecret123
```

Environment Variables

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: app-config
data:
  DATABASE_HOST: "postgres.default.svc.cluster.local"
```

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: app-secrets
type: Opaque
stringData:
  DATABASE_PASSWORD: "Sup3r$ecr3tP@ss!"
```

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: myapp
spec:
  containers:
    - name: app
      image: busybox
      env:
        - name: DB_HOST
          valueFrom:
            configMapKeyRef:
              name: app-config
              key: DATABASE_HOST
        - name: DB_PASSWORD
          valueFrom:
            secretKeyRef:
              name: app-secrets
              key: DATABASE_PASSWORD
```



Volumes

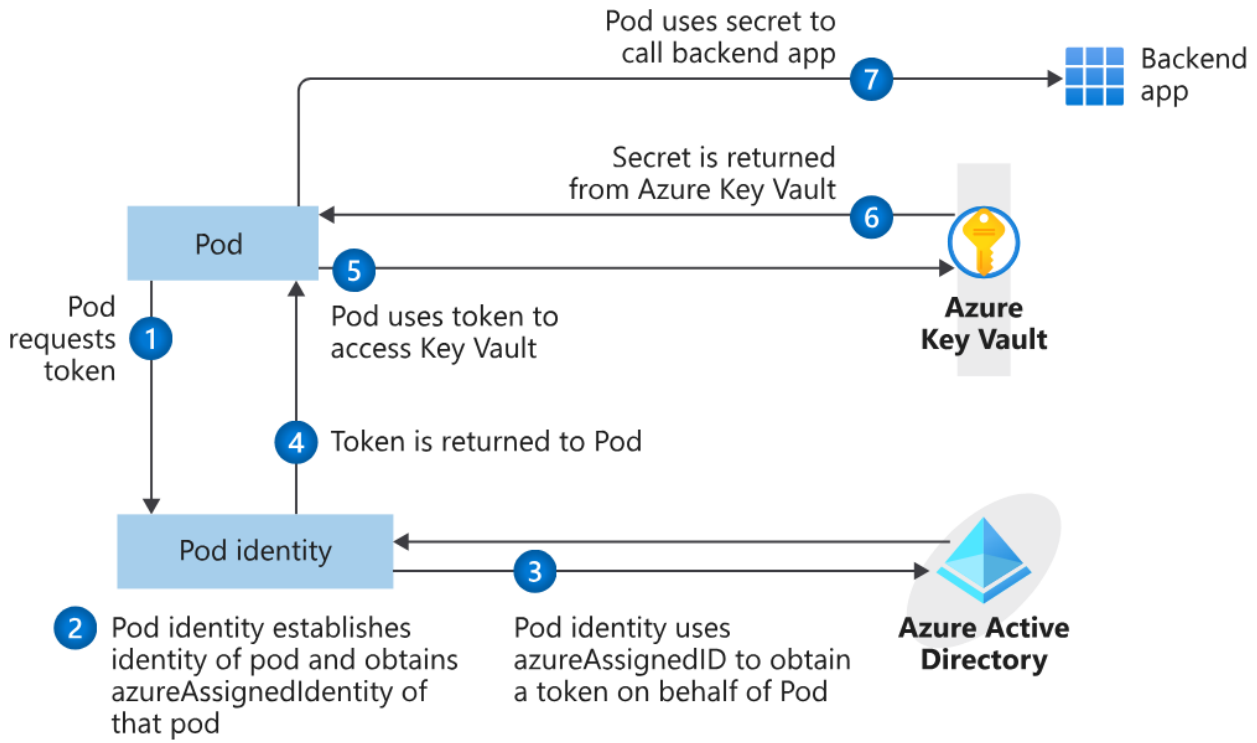
```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: app-config
data:
  nginx.conf: |
    server {
      listen 80;
      location / {
        root /usr/share/nginx/html;
      }
      location /api {
        proxy_pass http://api-service:8080;
      }
    }
```

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: tls-secret
type: kubernetes.io/tls
stringData:
  tls.crt: |
    -----BEGIN CERTIFICATE-----
    MIIDazCCAlOgAwIBAgIUH2oBMr...
    -----END CERTIFICATE-----
  tls.key: |
    -----BEGIN PRIVATE KEY-----
    MIIEvQIBADANBgkqhkiG9w0B...
    -----END PRIVATE KEY-----
```

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: myapp
spec:
  containers:
    - name: app
      image: busybox
      volumeMounts:
        - name: config
          mountPath: /etc/app/config
        - name: tls
          mountPath: /etc/ssl/app
          readOnly: true
  volumes:
    - name: config
      configMap:
        name: app-config
    - name: tls
      secret:
        secretName: tls-secret
        defaultMode: 0400
```

Azure Key Vault

- Secrets Store CSI driver (native)
- External Secrets Operator



Labs

- 1.06: Storage
- 1.07: Init container and sidecars
- 1.08: ConfigMaps and Secrets