kubernetes

Fabio Sforza

@fabio_sforza

@fsforza

- I Work in Relatech
- I am a DevOps Engineer
- I'm a sofa sportsman
- I'm a wasted talent in baking

kubernetes

Zero To Hero

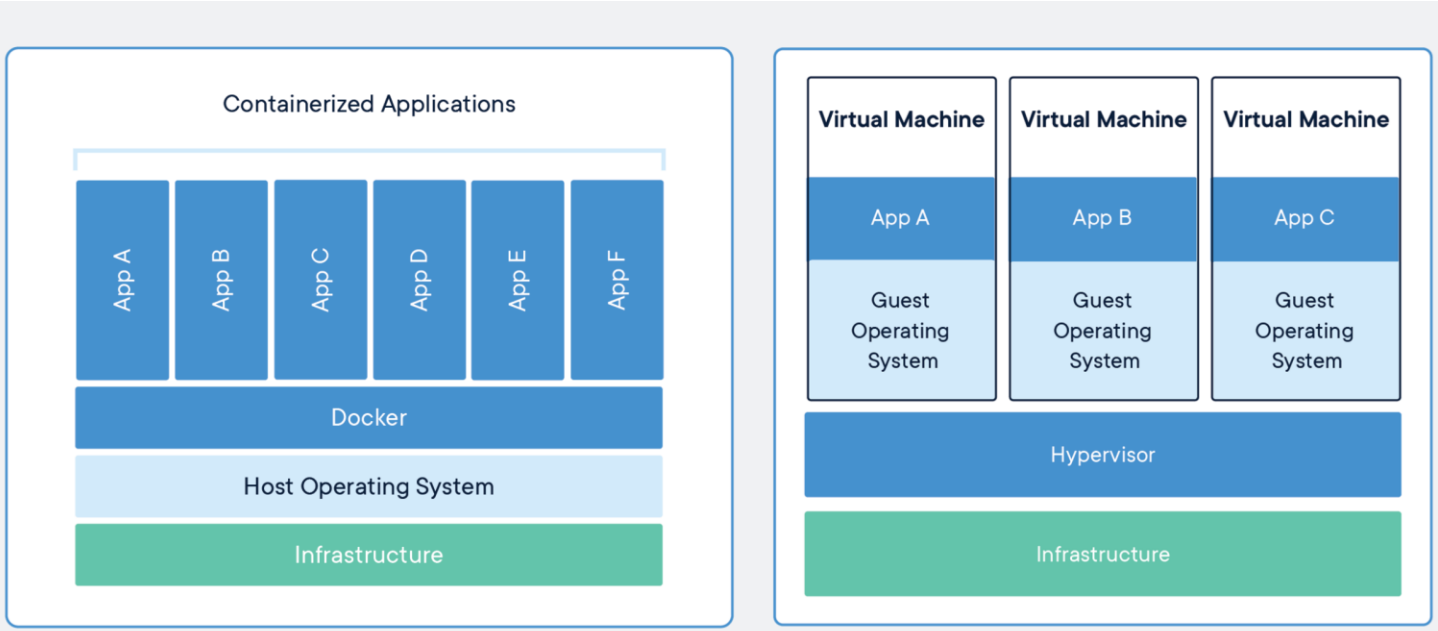
What is Kubernetes?

kubernetes

- It is an Open Source Project
- Initially developed by Google, with name **Borg**
- It is maintained by **CNCF**
- It is written in **Go**
- It is a Container Orchestrator

What is a Container?

kubernetes



CONTAINERS

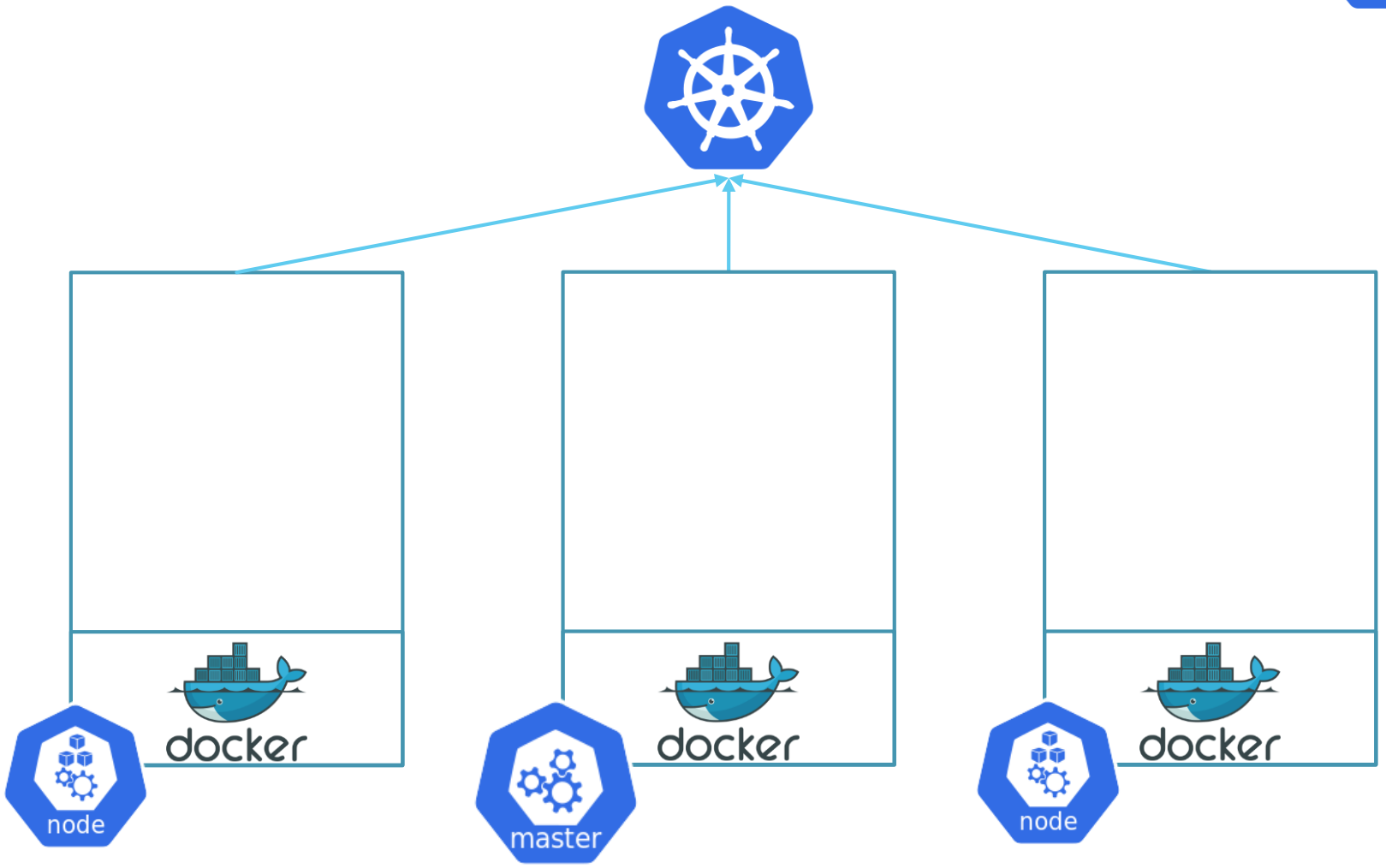
Containers are an abstraction at the app layer that packages code and dependencies together. Multiple containers can run on the same machine and share the OS kernel with other containers, each running as isolated processes in user space. Containers take up less space than VMs (container images are typically tens of MBs in size), can handle more applications and require fewer VMs and Operating systems.

VIRTUAL MACHINES

Virtual machines (VMs) are an abstraction of physical hardware turning one server into many servers. The hypervisor allows multiple VMs to run on a single machine. Each VM includes a full copy of an operating system, the application, necessary binaries and libraries - taking up tens of GBs. VMs can also be slow to boot.

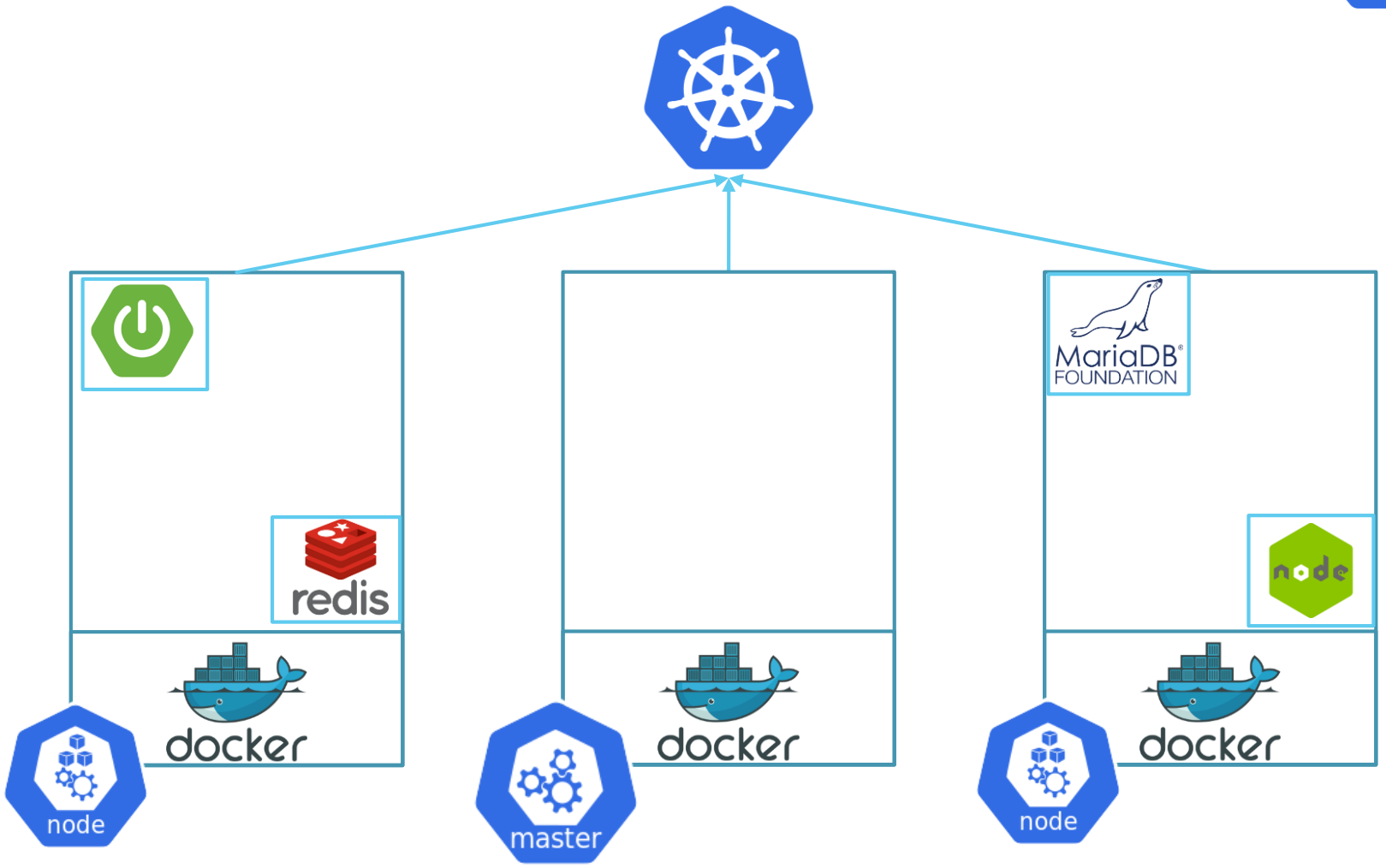
Kubernetes Cluster

kubernetes



Kubernetes Cluster

kubernetes

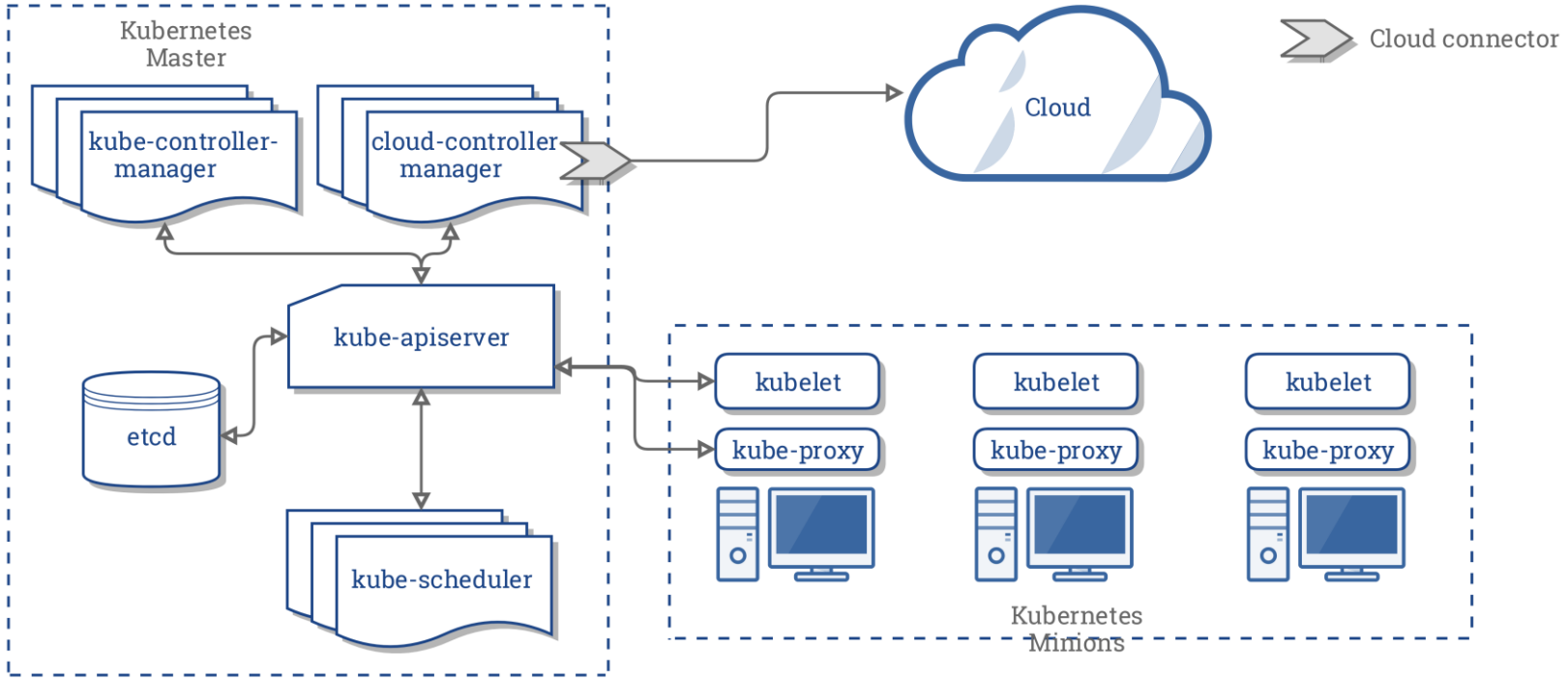


Production Features

kubernetes

- Application Horizontal Scaling
- HealthChecks
- Resource Quotas
- Rolling Update
- Externalized Configuration
- Secrets Handling
- Persistent Volumes
- Network Segmentation
- RBAC
- …

Kubernetes Architecture



Namespace

kubernetes

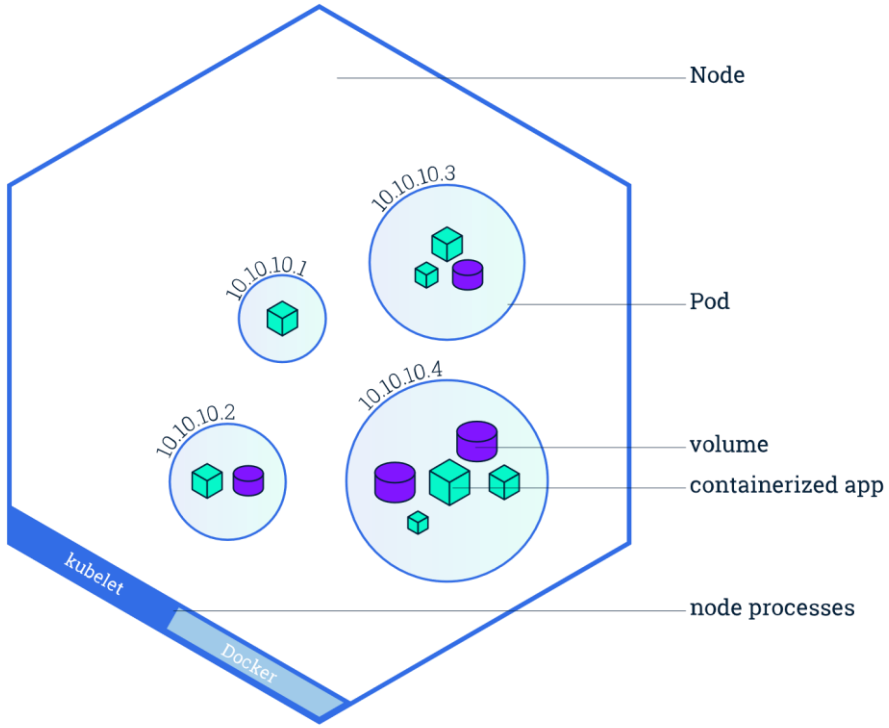
- Namespaces are a logical cluster or environment, and are the primary method of partitioning a cluster or scoping access.

```
$ kubectl get namespaces
NAME          STATUS    AGE
default       Active    1d
kube-system   Active    1d
kube-public   Active    1d
```

Pod

kubernetes

- **Atomic unit** or smallest "*unit of work*" of Kubernetes.
- Pods are **one or MORE containers** that share volumes, a network, and are a part of a **single context**.



Workloads

kubernetes

- Workloads are higher level objects that manage Pods.
  - **ReplicaSet**
  - **Deployment**
  - **StatefulSet**
  - **DaemonSet**
  - **Job**
  - **CronJob**

ReplicaSet

kubernetes

- Primary method of managing pod replicas and their lifecycle.
- Includes their scheduling, scaling, and deletion.
- Their job is simple: **Always ensure the desired number of pods are running.**

Deployment

kubernetes

- Declarative method of managing Pods via **ReplicaSets.**
- Provide rollback functionality and update control.

Persistent Volume

kubernetes

- A **PersistentVolume** (PV) represents a storage resource.
- PVs are a **cluster wide resource** linked to a backing storage provider: NFS, GCEPersistentDisk, Ceph, Azure Disk etc.
- Their lifecycle is handled independently from a pod
- **CANNOT** be attached to a Pod directly. Relies on a **PersistentVolumeClaim**

Persistent Volumes Claim

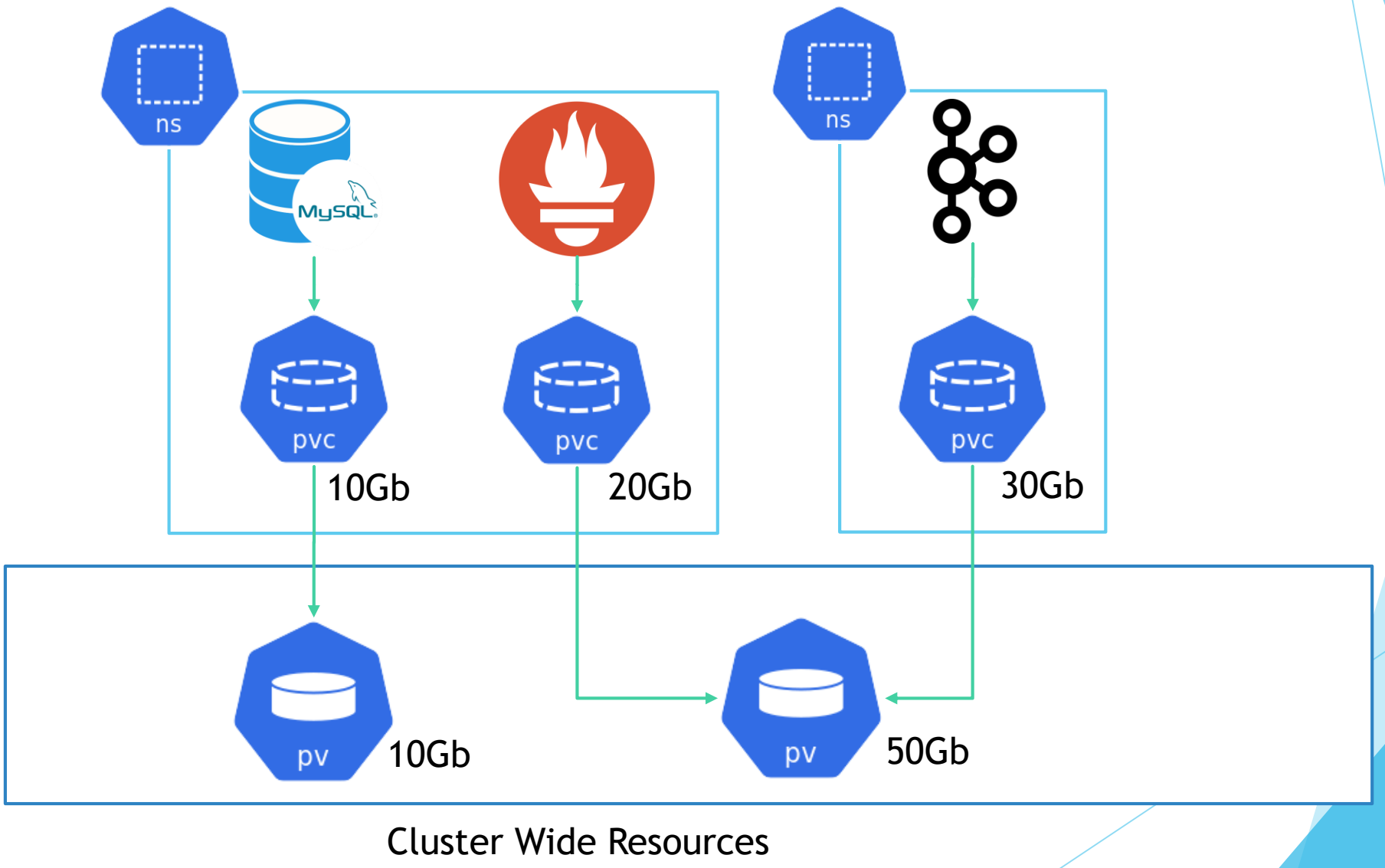
kubernetes

- A **PersistentVolumeClaim** (PVC) is a **namespaced** request for storage.

- Ensures that an application's '*claim*' for storage is portable across numerous backends or providers.

Persistent Volumes Claim

kubernetes



Service

kubernetes

- A set of routing rules that defines how to access the Pods.
- They define:
  - Static and Unique Cluster IP addresses
  - Static DNS names

Service

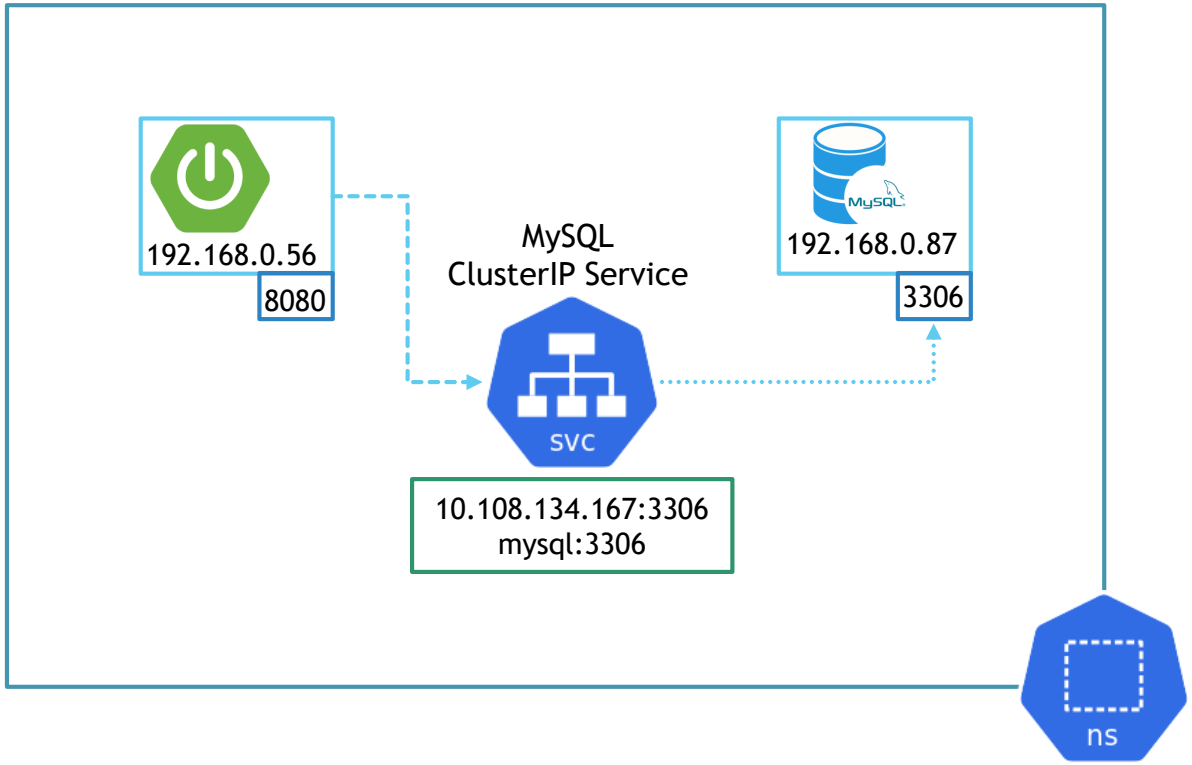
kubernetes

- Service Types:
  - **ClusterIP (default)**
  - **NodePort**
  - **LoadBalancer**
  - **ExternalName**

Service ClusterIP

kubernetes

- **ClusterIP** services exposes a pod on a strictly cluster internal virtual IP.



Configuration

kubernetes

- Kubernetes has an integrated pattern for decoupling configuration from application or container.

- This pattern makes use of two Kubernetes components: **ConfigMaps** and **Secrets.**

ConfigMap

kubernetes

- Externalized data stored within kubernetes.
- Can be referenced through several different means:
  - environment variable
  - a command line argument (via env var)
  - injected as a file into a volume mount
- Can be created from a manifest, literals, directories, or files directly.

Secret

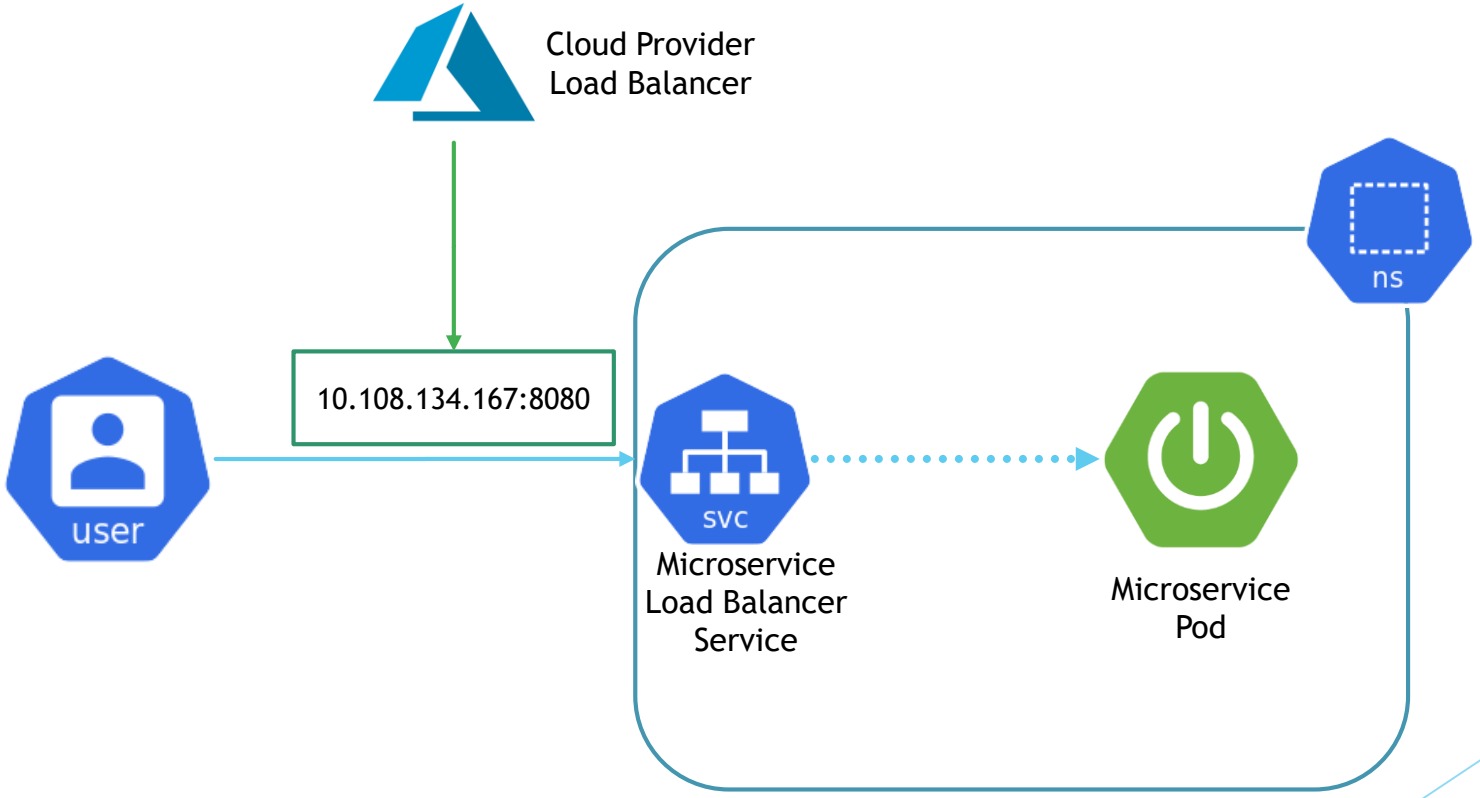
kubernetes

- Functionally identical to a ConfigMap.
- Stored as **base64 encoded content.**
- Ideal for username/passwords, certificates or other sensitive information that should not be stored in a container.
- Can be created from a manifest, literals, directories, or from files directly.

Service LoadBalancer

kubernetes

- Works in conjunction with an external system (**Cloud Provider**) to map a cluster external IP to the exposed service.



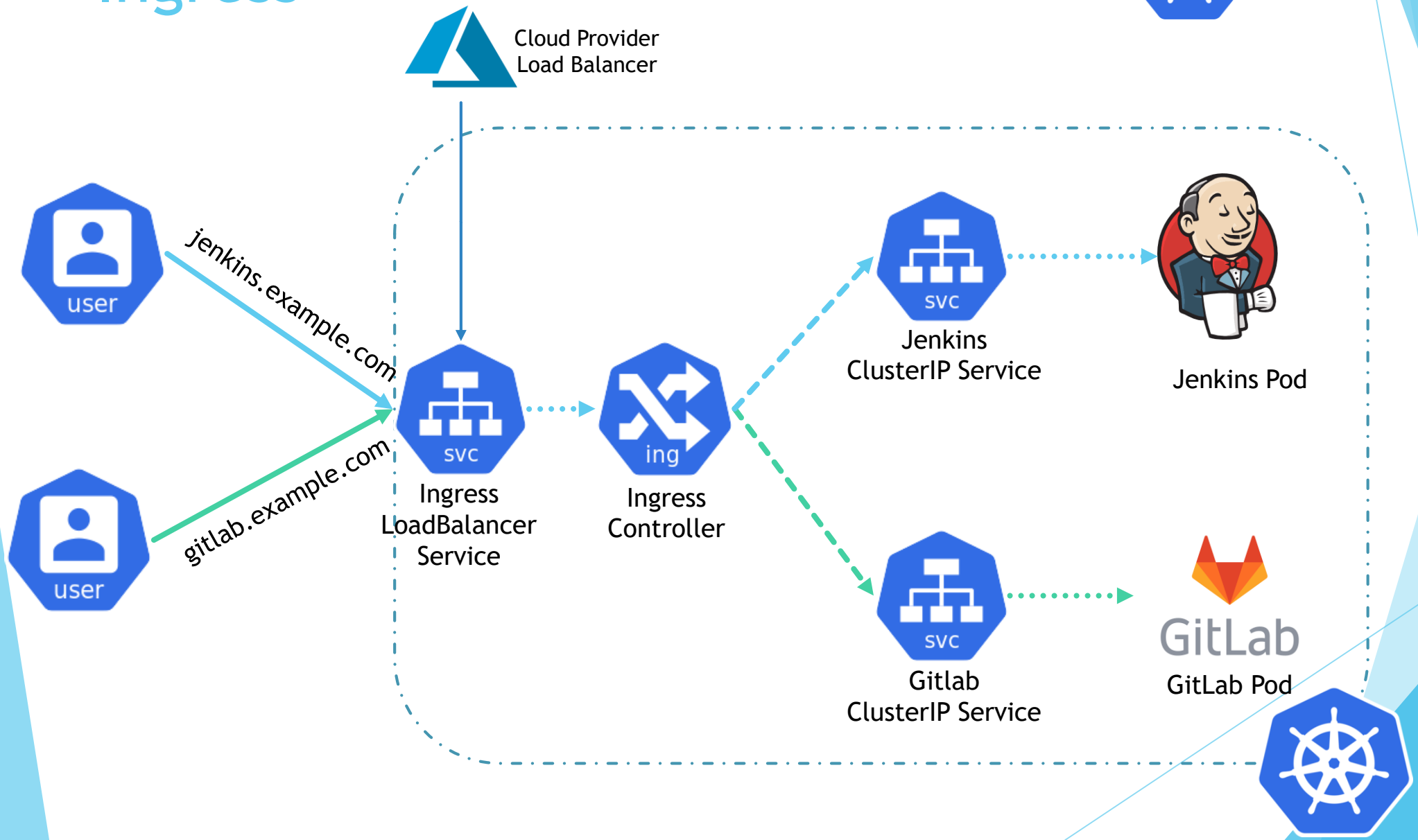
Ingress

kubernetes

- Is a Load Balancer placed in the context of Kubernetes
- Exposes a Service to external clients by reachable URLs
- Operate at the application layer of the network stack (HTTP/HTTPS)

Ingress

kubernetes



Thank you!

Questions?