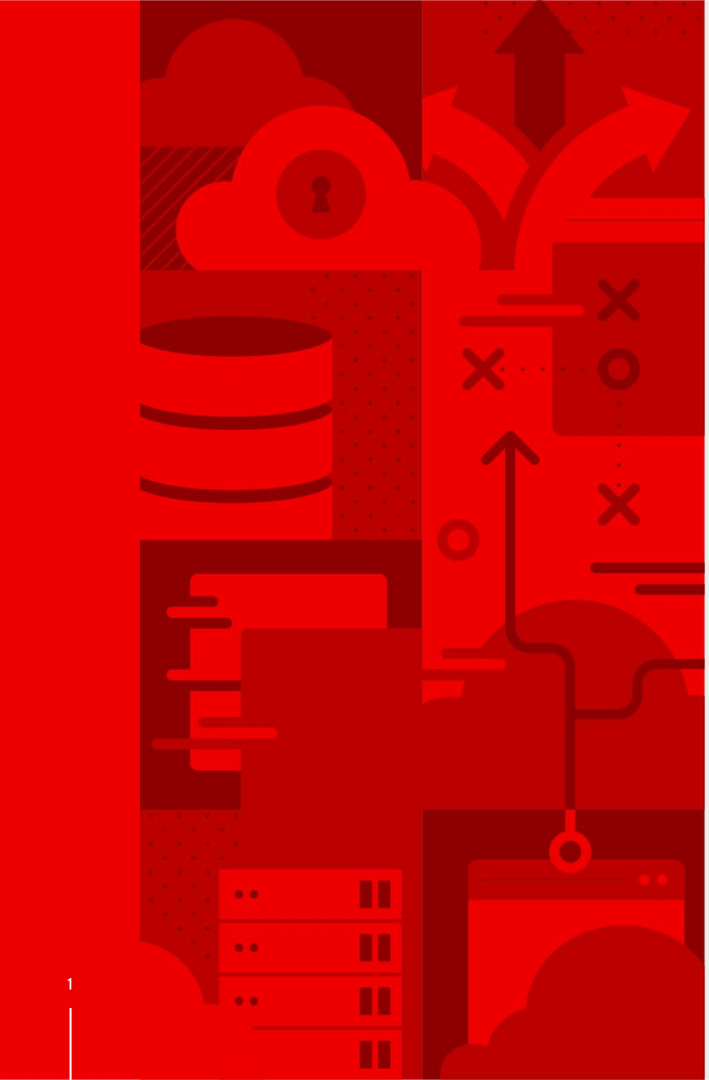


OPENSHIFT CONTAINER PLATFORM

TECHNICAL OVERVIEW

in linkedin.com/company/red-hat

f facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

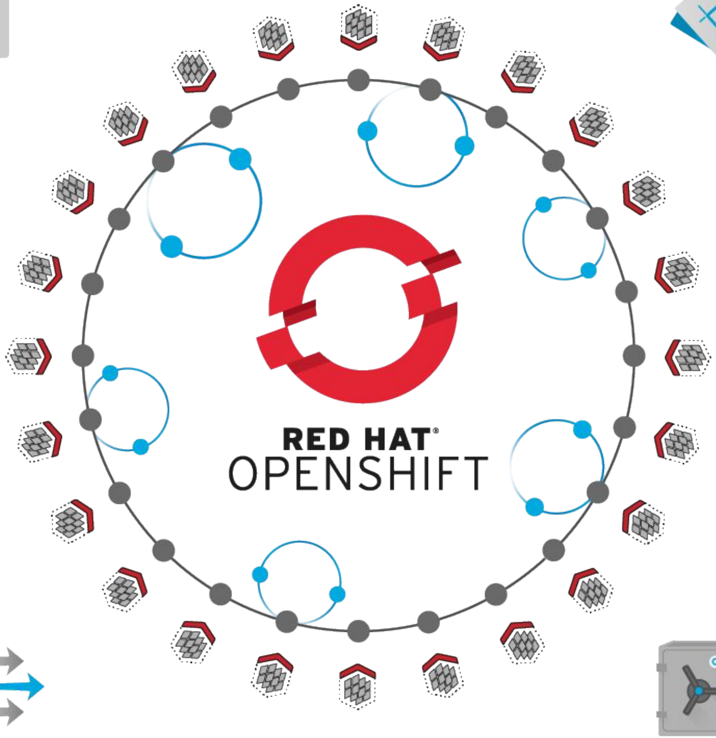
Alfred Bach
Principal Solution Architect
EMEA Partner Team

Red Hat

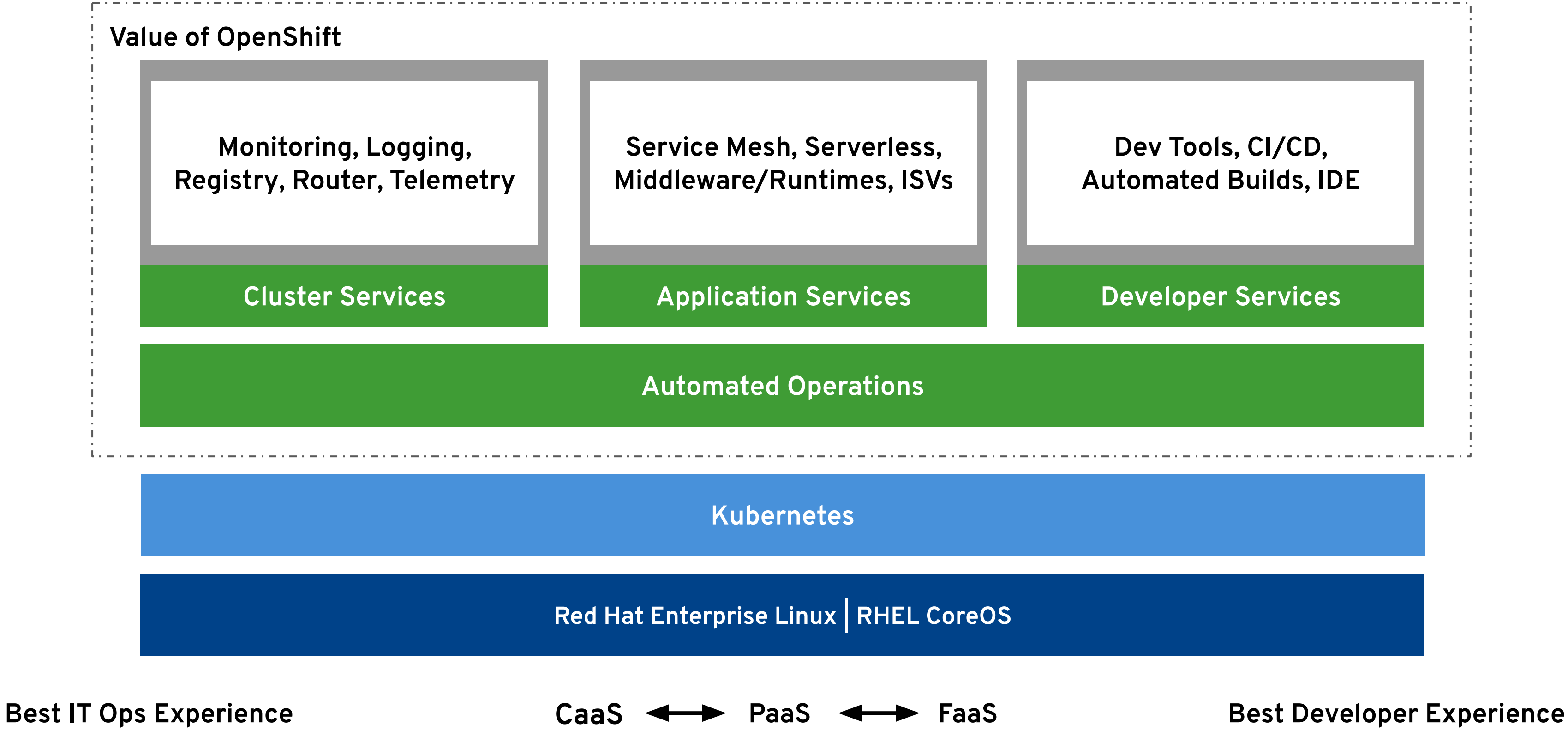
Functional overview

OPENSHIFT CONTAINER PLATFORM | Technical Value

- Self-Service
- Multi-language
- Automation
- Collaboration
- Multi-tenant



- Standards-based
- Web-scale
- Open Source
- Enterprise Grade
- Secure



Value of OpenShift

Monitoring, Logging, Registry, Router, Telemetry

Cluster Services

Service Mesh, Serverless, Middleware/Runtimes, ISVs

Application Services

Dev Tools, CI/CD, Automated Builds, IDE

Developer Services

Automated Operations

Kubernetes

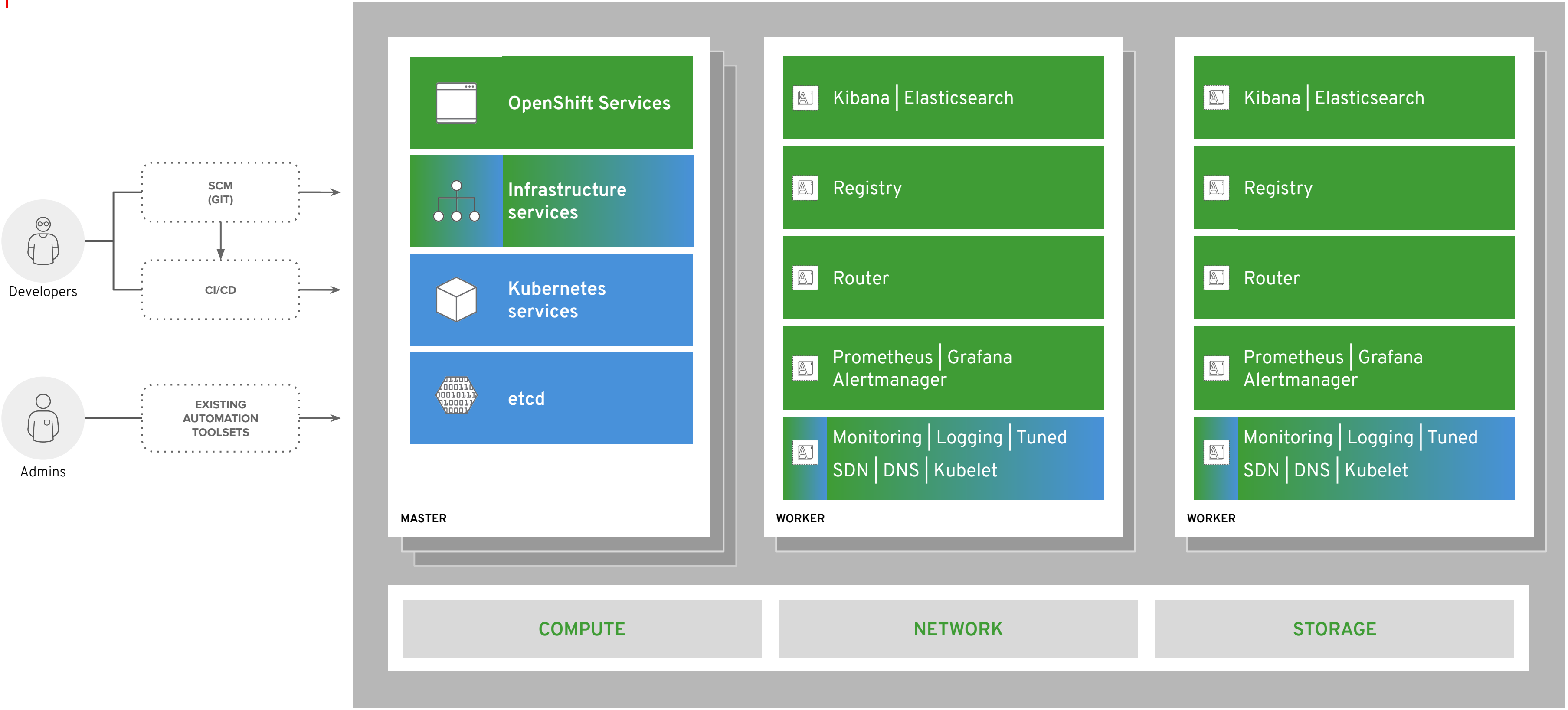
Red Hat Enterprise Linux | RHEL CoreOS

Best IT Ops Experience

CaaS ⟷ PaaS ⟷ FaaS

Best Developer Experience

OPENSHIFT CONTAINER PLATFORM | Architectural Overview



Developers

SCM (GIT)

CI/CD

Admins

EXISTING AUTOMATION TOOLSETS

MASTER

OpenShift Services

Infrastructure services

Kubernetes services

etcd

WORKER

Kibana | Elasticsearch

Registry

Router

Prometheus | Grafana Alertmanager

Monitoring | Logging | Tuned SDN | DNS | Kubelet

WORKER

Kibana | Elasticsearch

Registry

Router

Prometheus | Grafana Alertmanager

Monitoring | Logging | Tuned SDN | DNS | Kubelet

COMPUTE

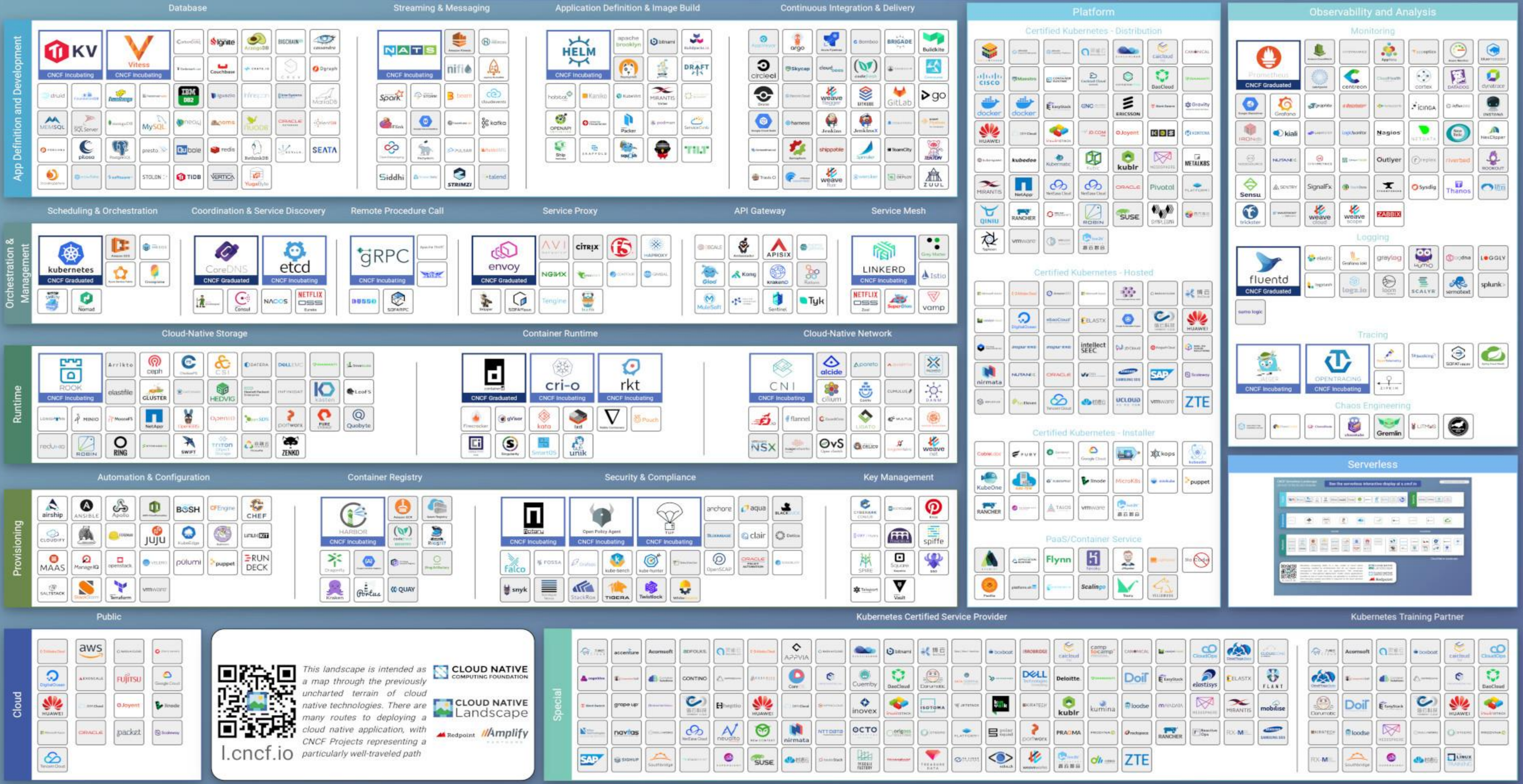
NETWORK

STORAGE

CNCF Cloud Native Landscape
2019-07-12T03:51:02Z 024e93b

Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at l.cncf.io

Greyed logos are not open source



This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path

l.cncf.io

CLOUD NATIVE COMPUTING FOUNDATION

CLOUD NATIVE Landscape

Redpoint

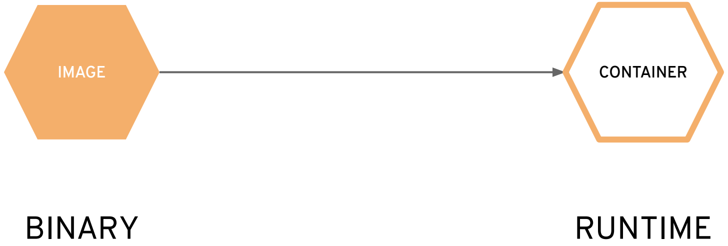
Amplify PARTNERS

kubernetes
11004
kubernetes
4+
11004
@datamattsson
IDEAS INCLUDED
Pod
Service
StatefulSet
DaemonSet
Deployment

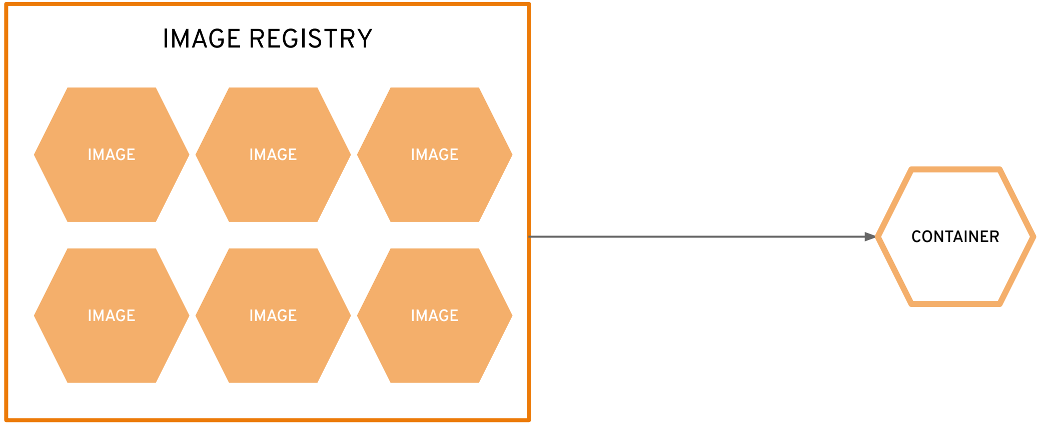
OpenShift and Kubernetes core concepts

a container is the smallest compute unit

containers are created from container images



container images are stored in an image registry



an image repository contains all versions of an image in the image registry

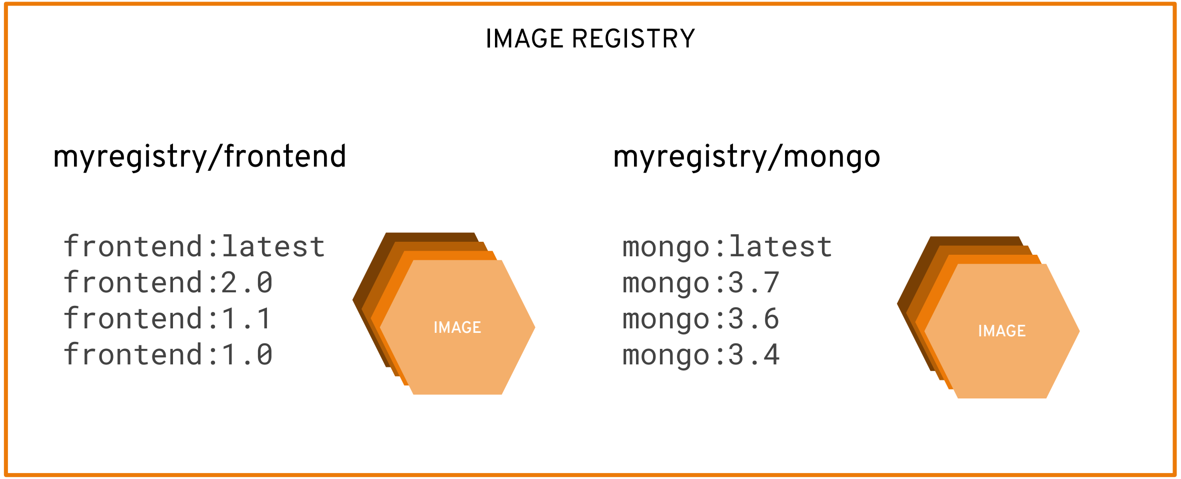


IMAGE REGISTRY

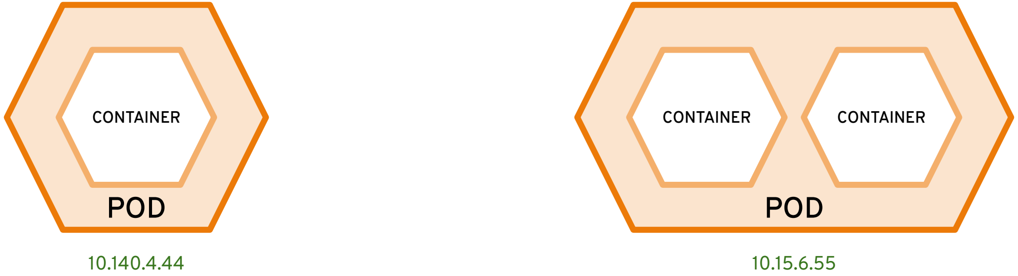
myregistry/frontend

```
frontend:latest
frontend:2.0
frontend:1.1
frontend:1.0
```

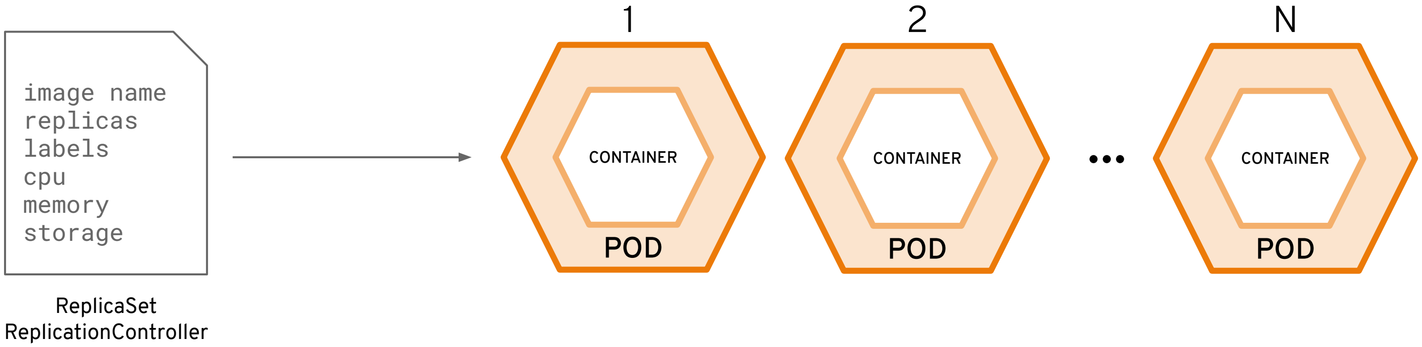
myregistry/mongo

```
mongo:latest
mongo:3.7
mongo:3.6
mongo:3.4
```

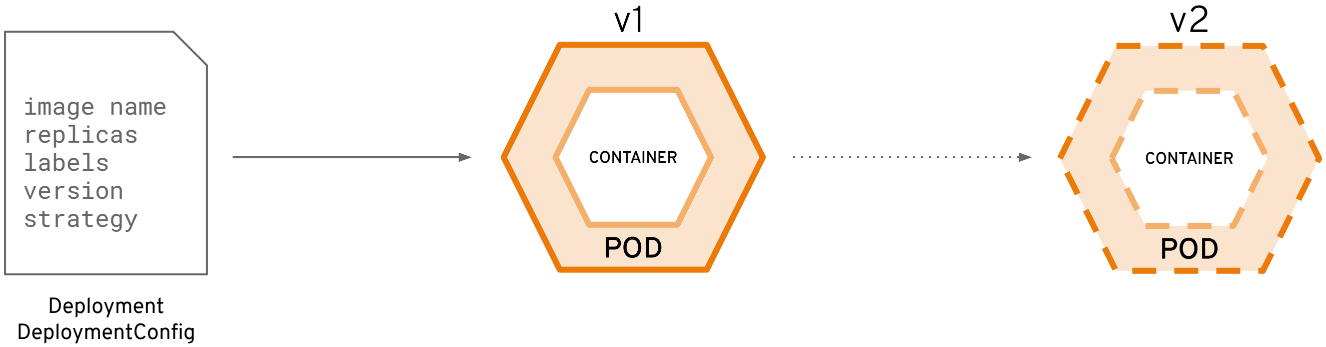
containers are wrapped in pods which are units of deployment and management



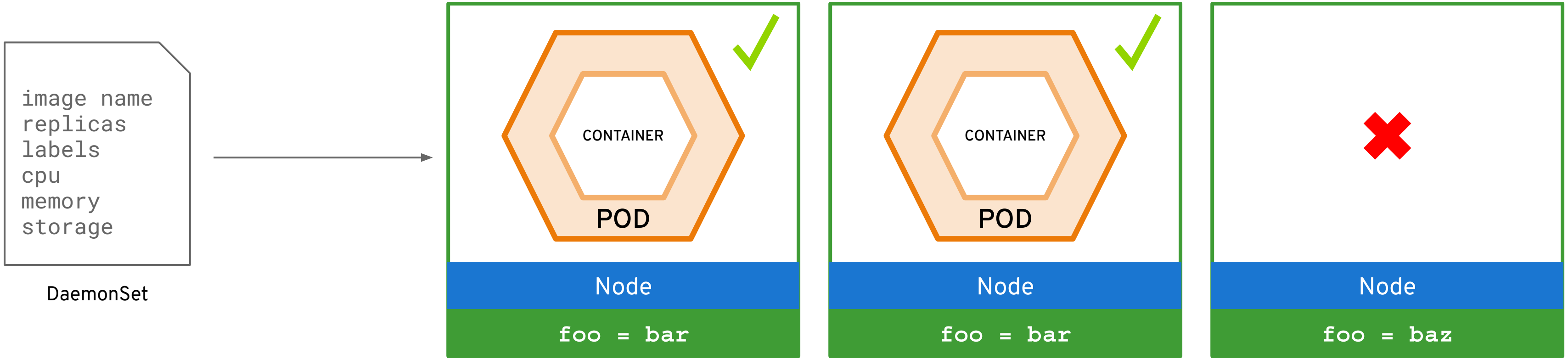
ReplicationControllers & ReplicaSets ensure a specified number of pods are running at any given time



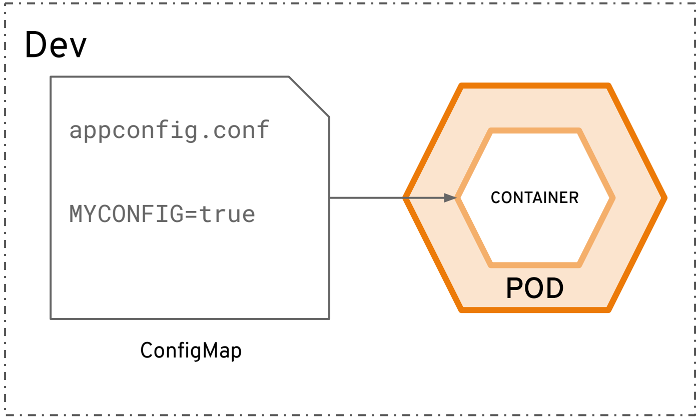
`Deployments` and `DeploymentConfigurations` define how to roll out new versions of Pods

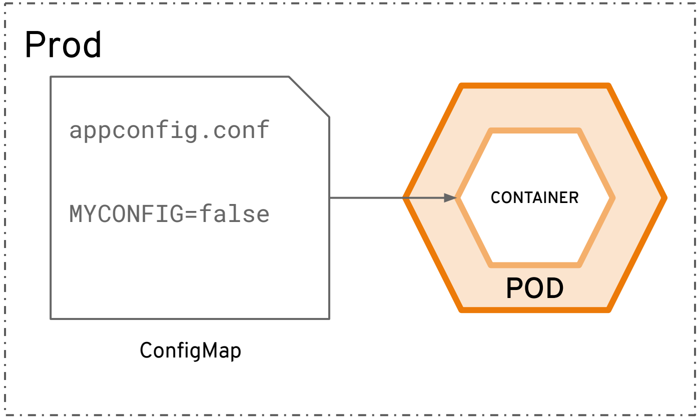


a daemonset ensures that all (or some) nodes run a copy of a pod

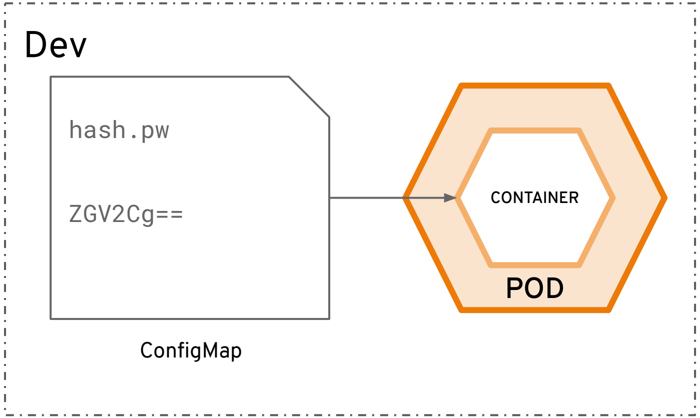


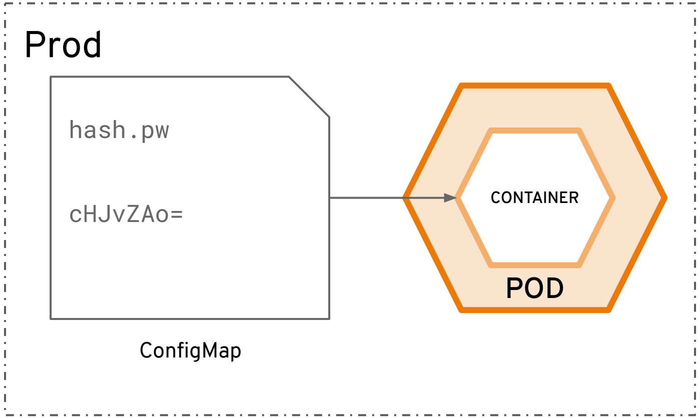
`configmaps` allow you to decouple configuration artifacts from image content



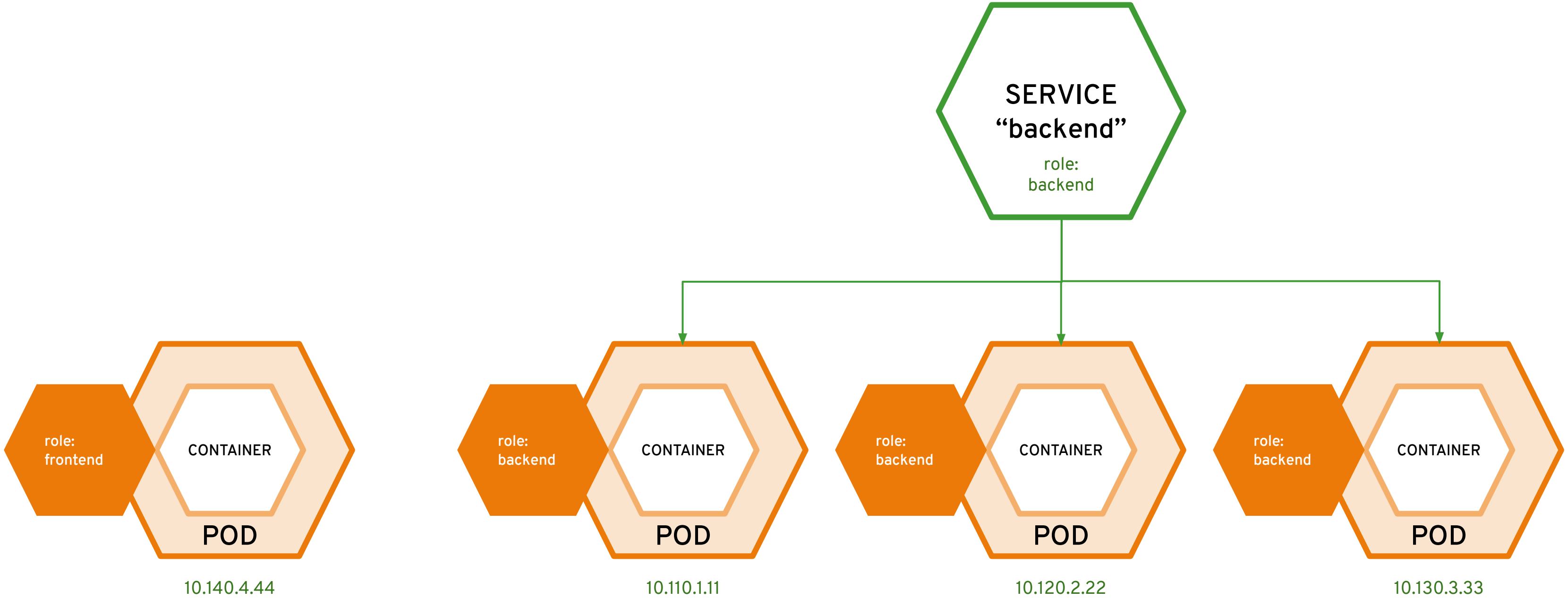


`secrets` provide a mechanism to hold sensitive information such as passwords

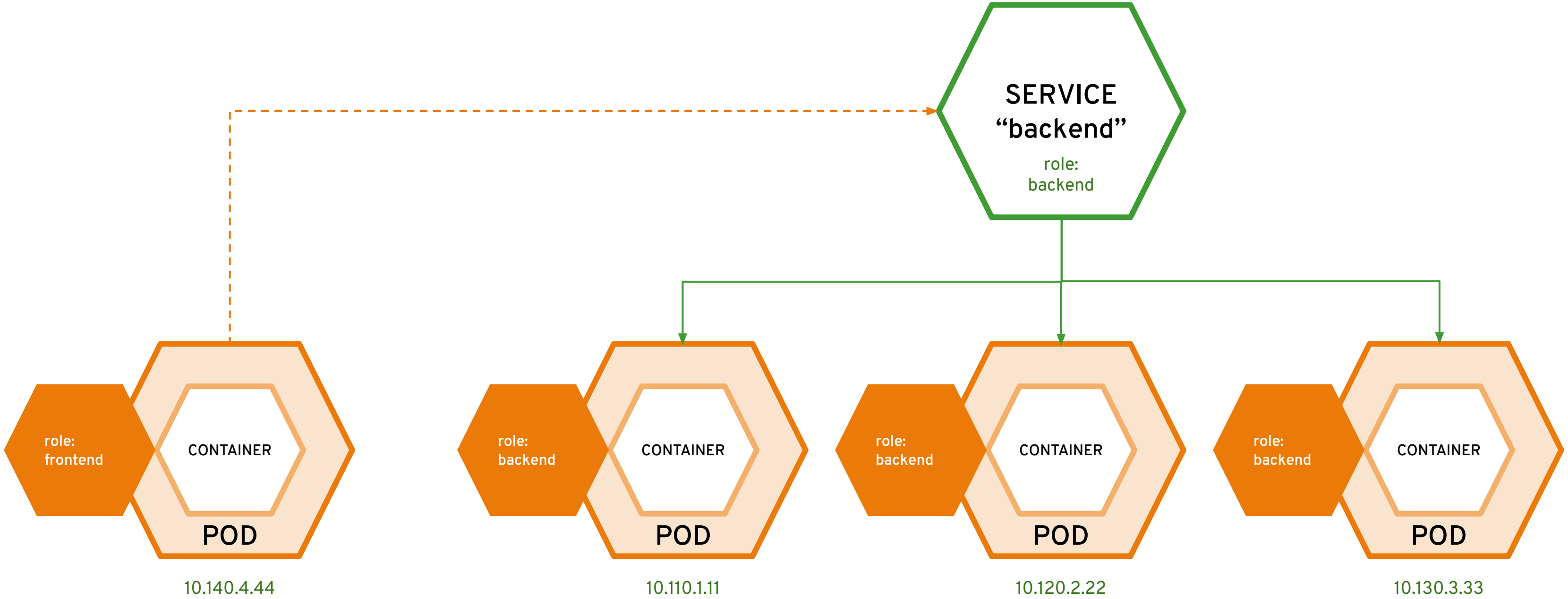




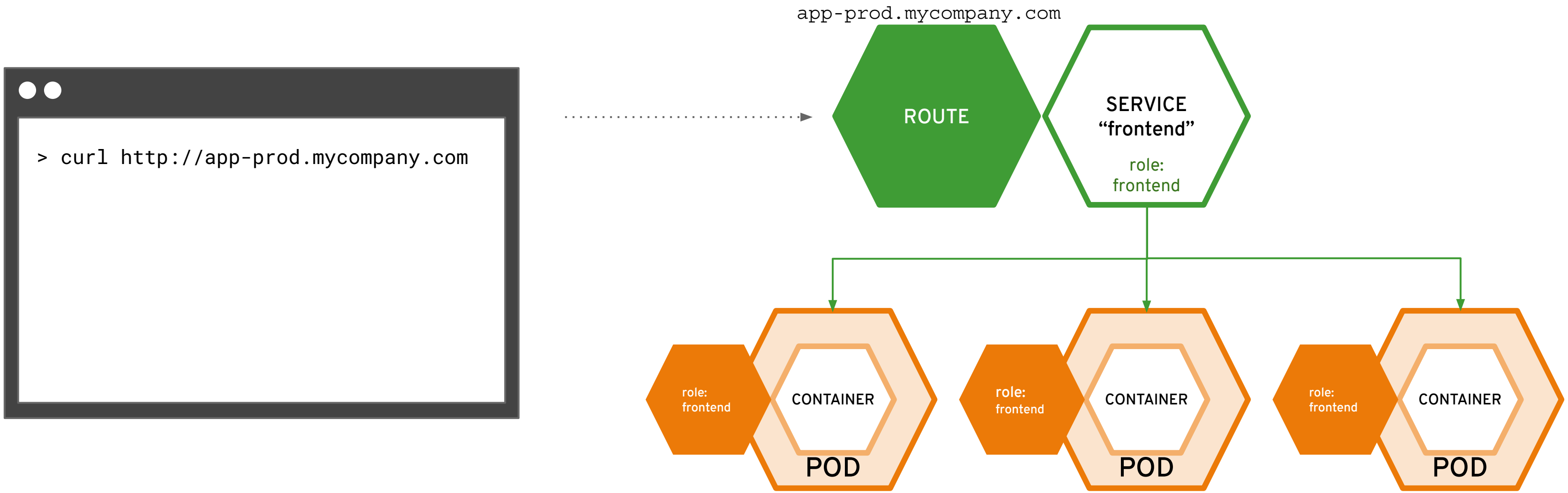
services provide internal load-balancing and service discovery across pods



apps can talk to each other via services

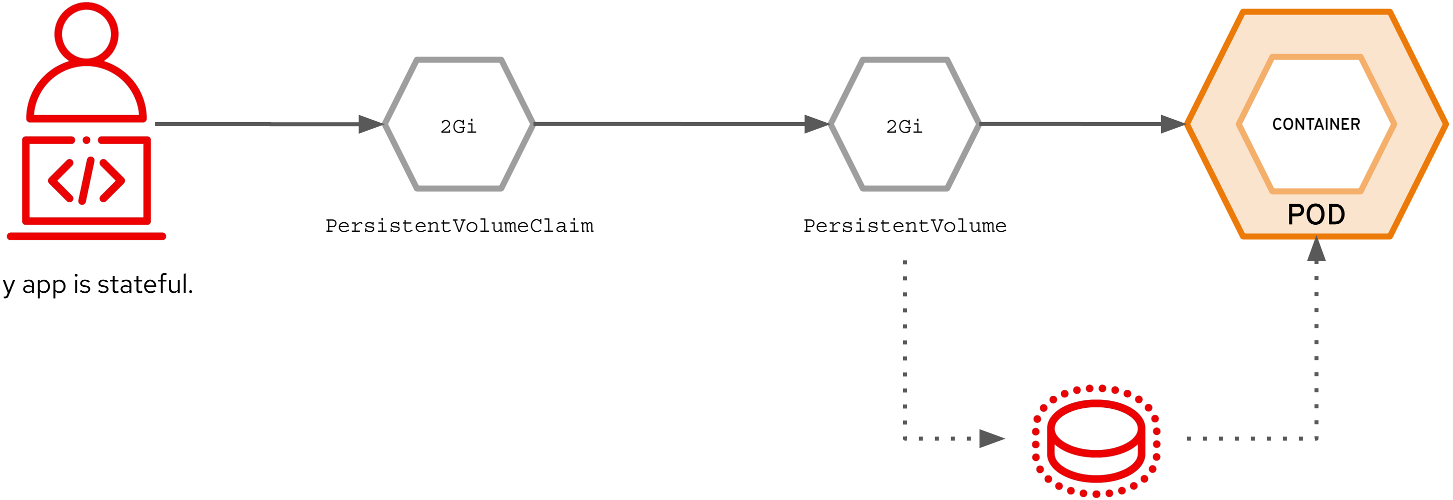


routes make services accessible to clients outside the environment via real-world urls



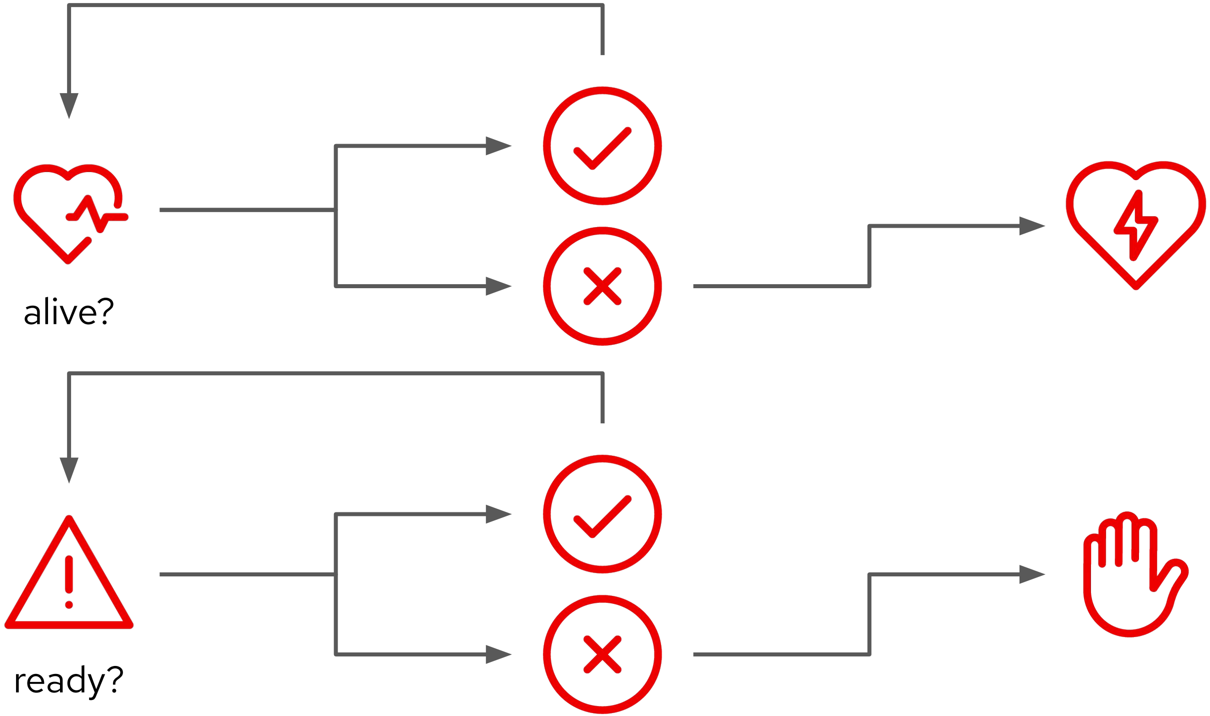
```
> curl http://app-prod.mycompany.com
```

Persistent Volume and Claims

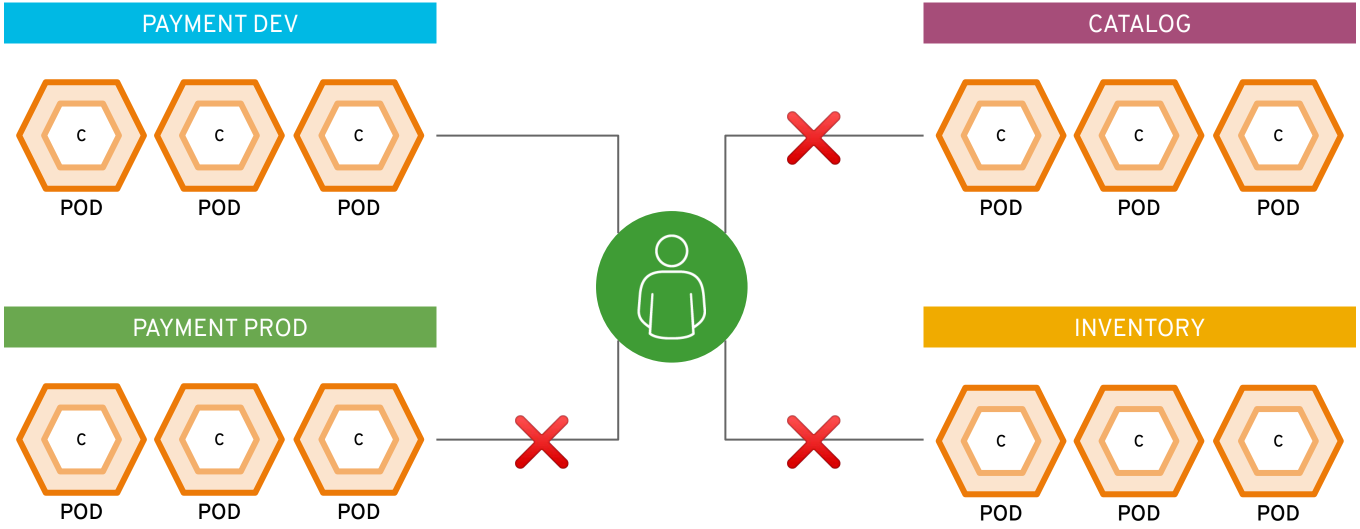


My app is stateful.

Liveness and Readiness



projects isolate apps across environments, teams, groups and departments



OpenShift 4 Architecture

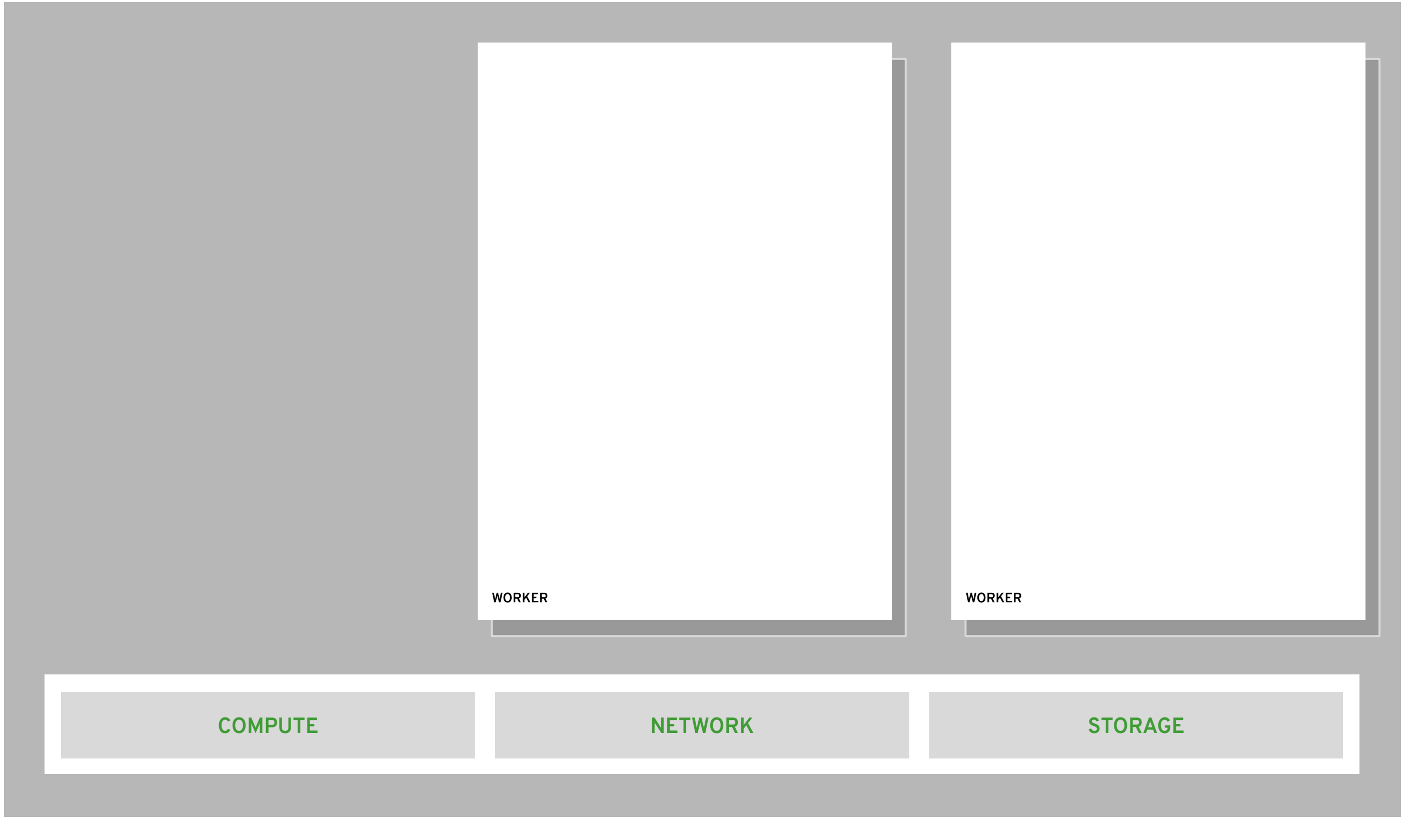
your choice of infrastructure

COMPUTE

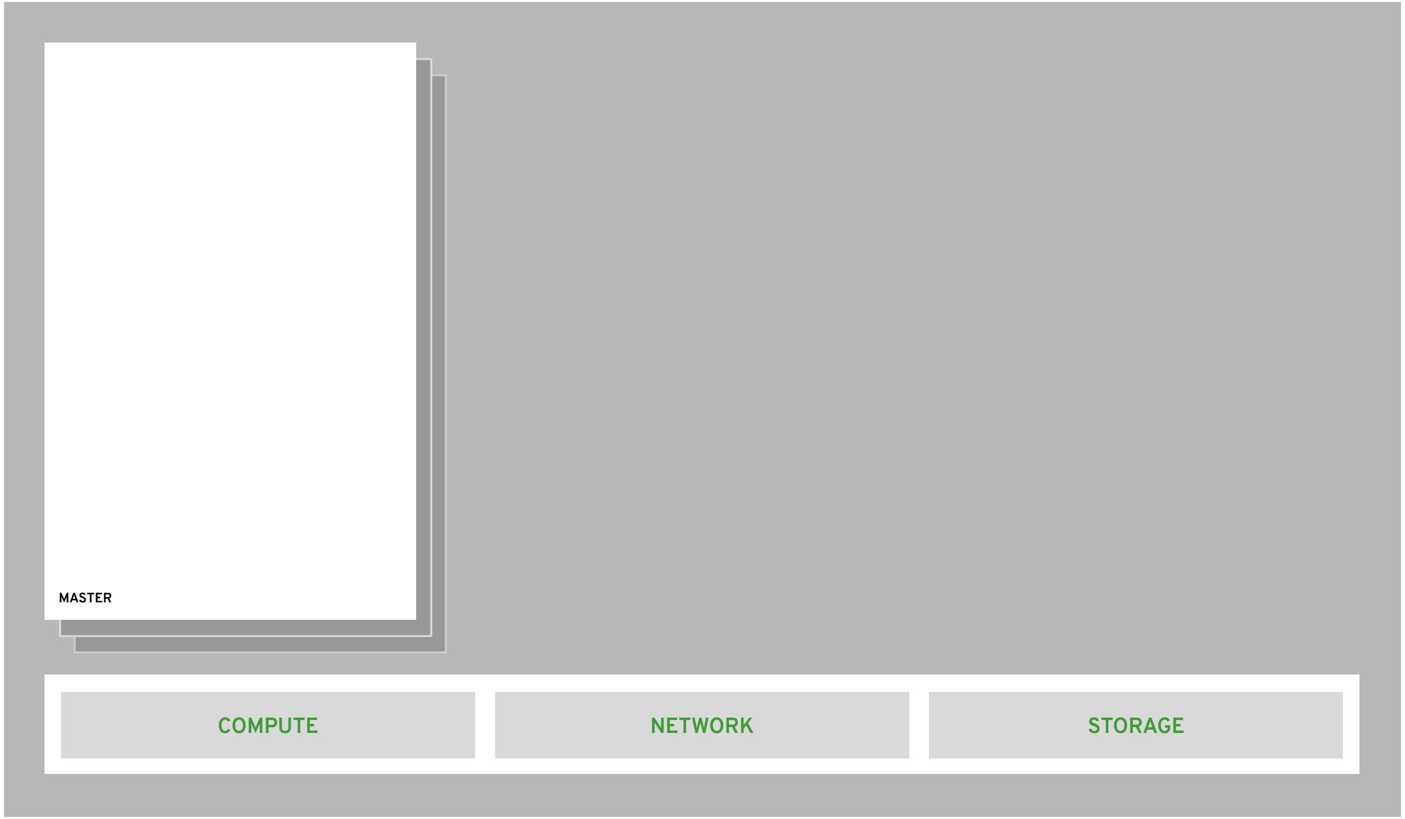
NETWORK

STORAGE

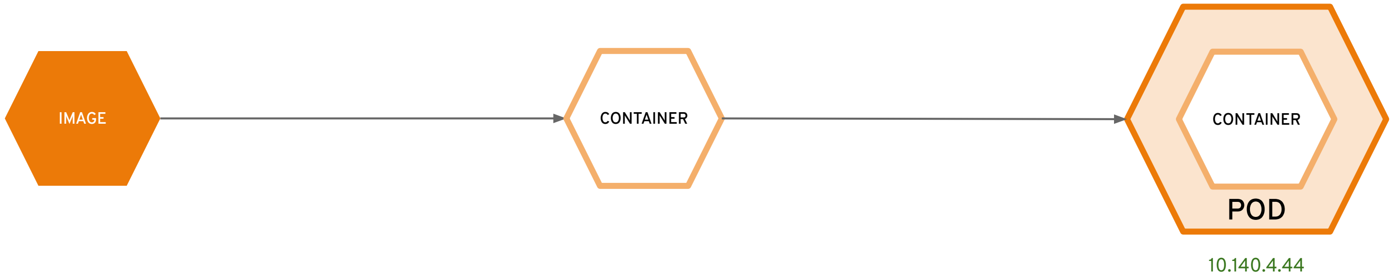
workers run workloads



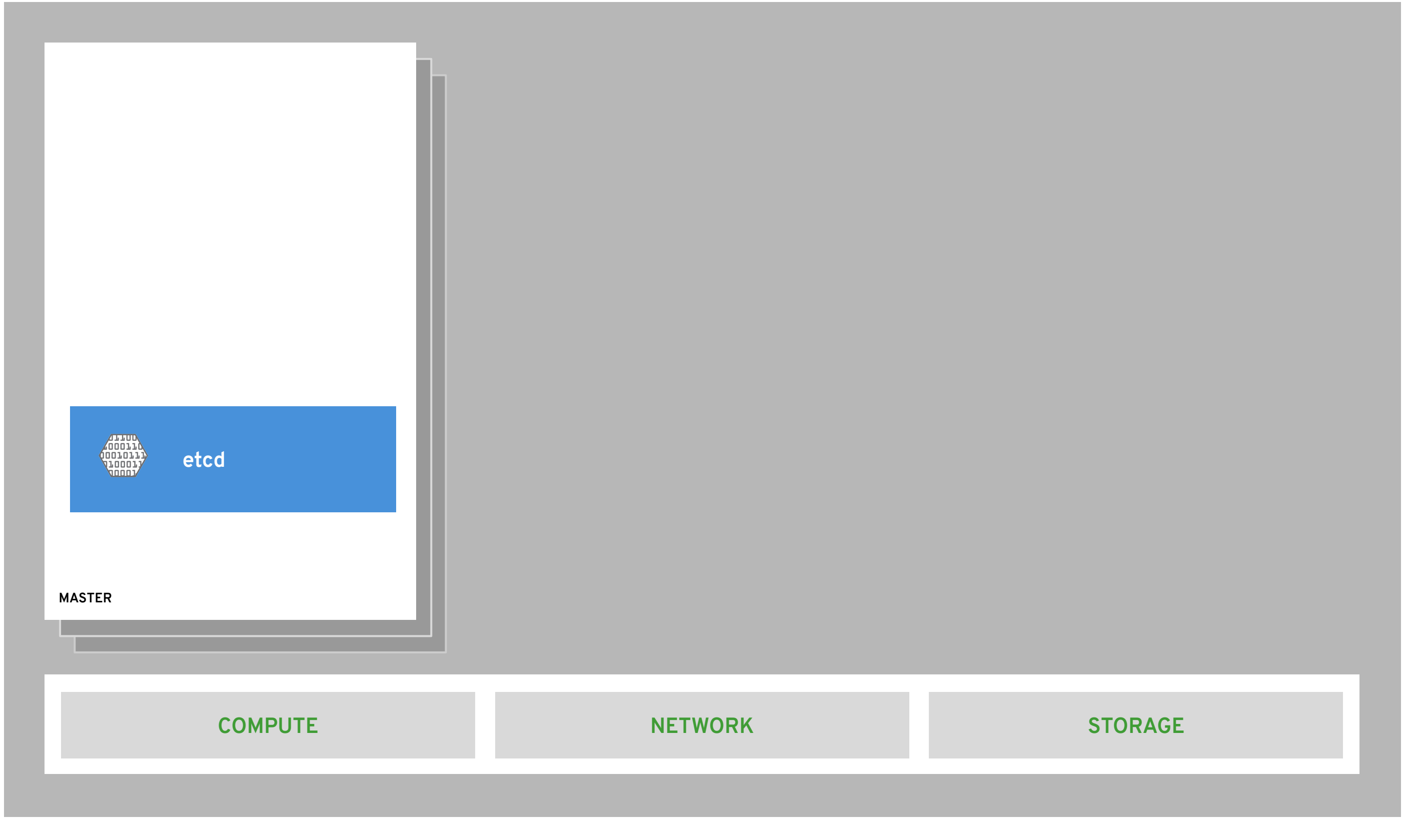
masters are the control plane



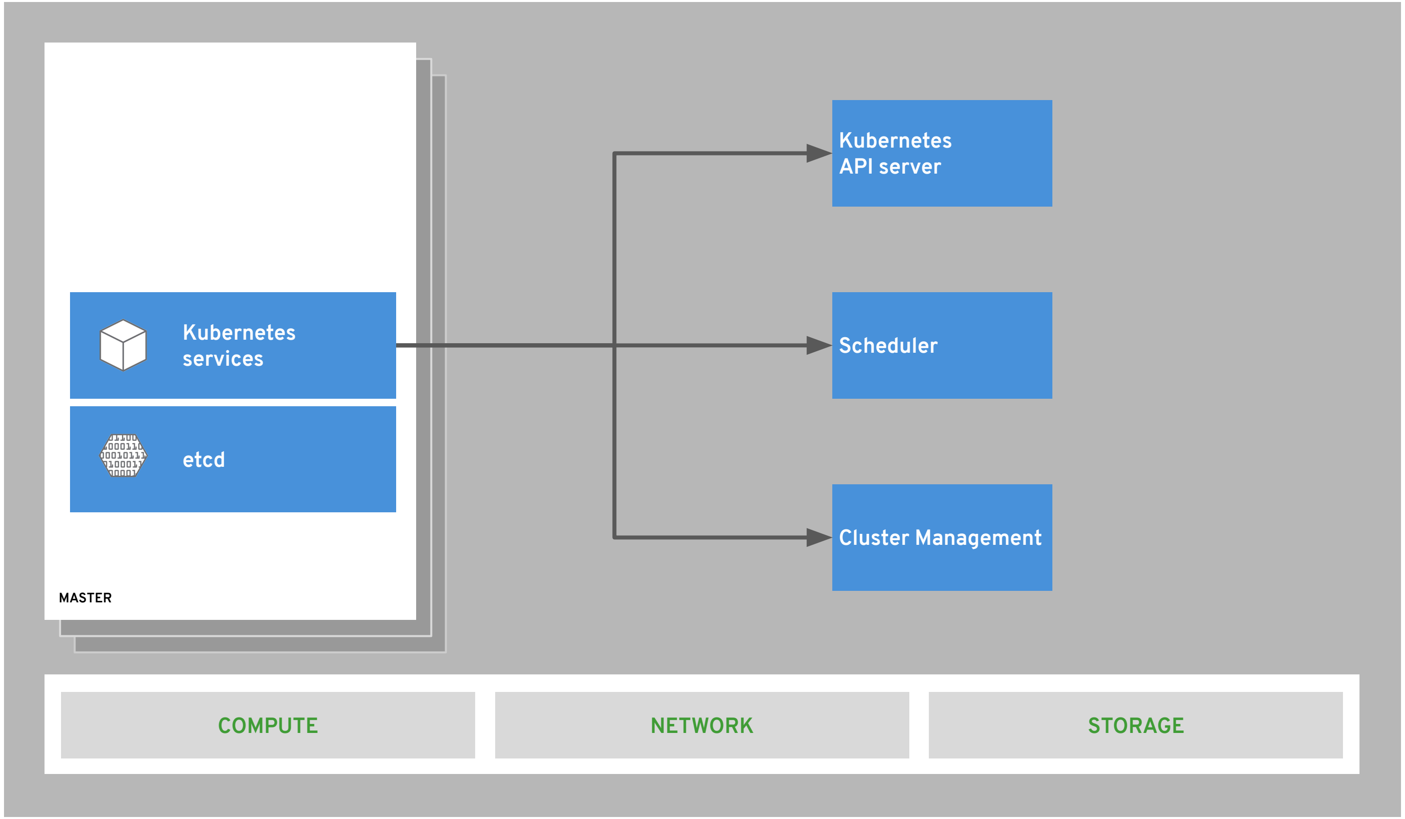
everything runs in pods



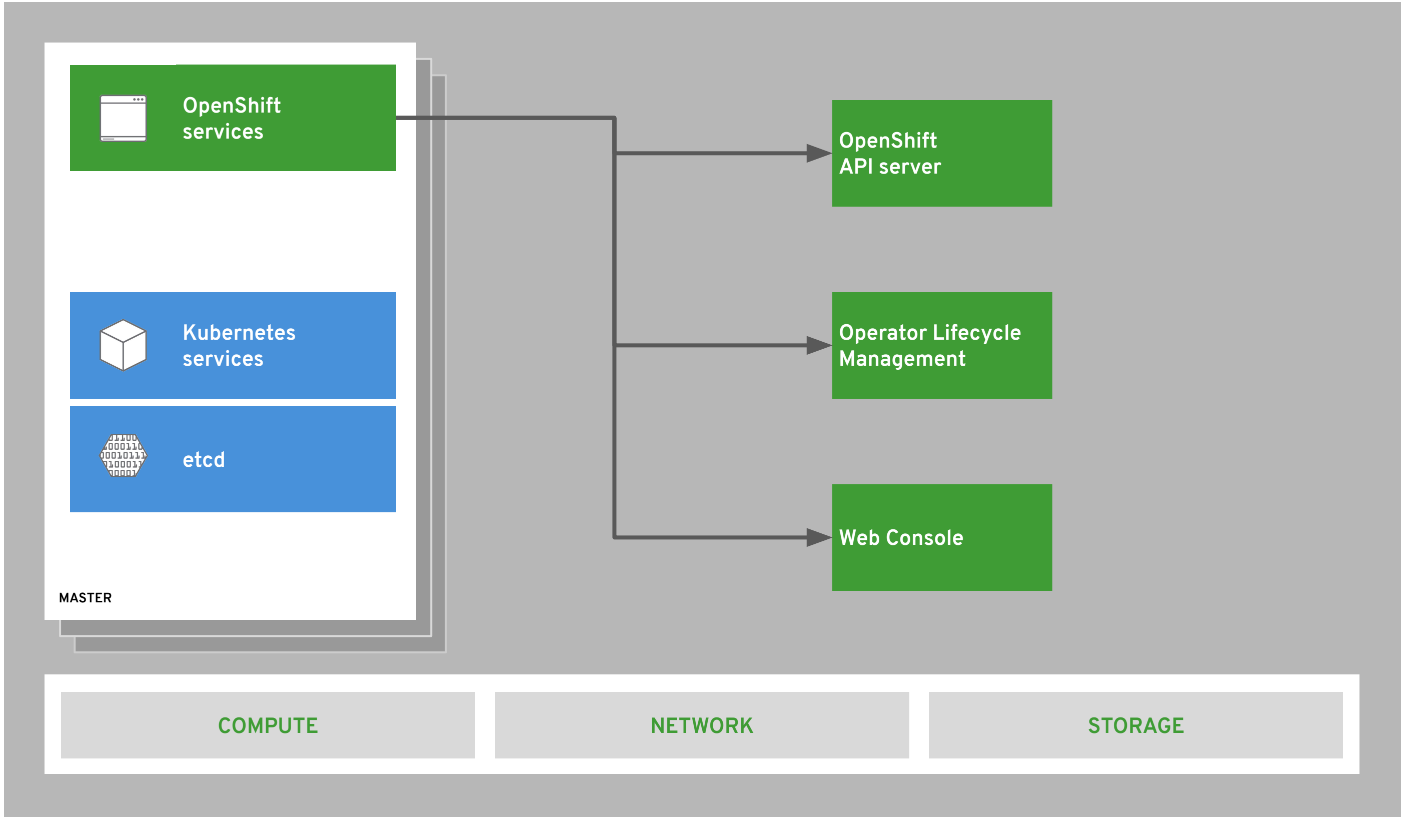
state of everything



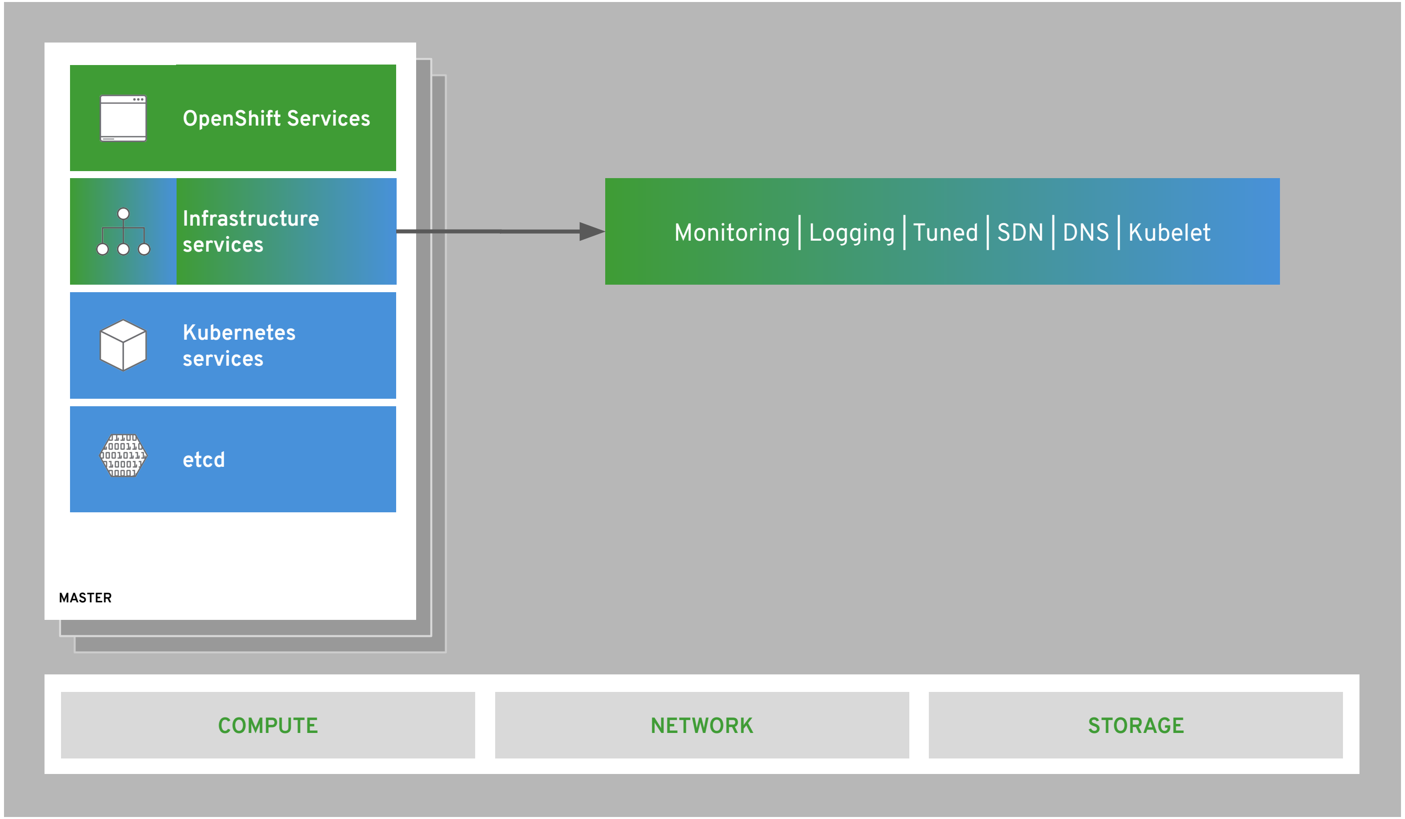
core kubernetes components



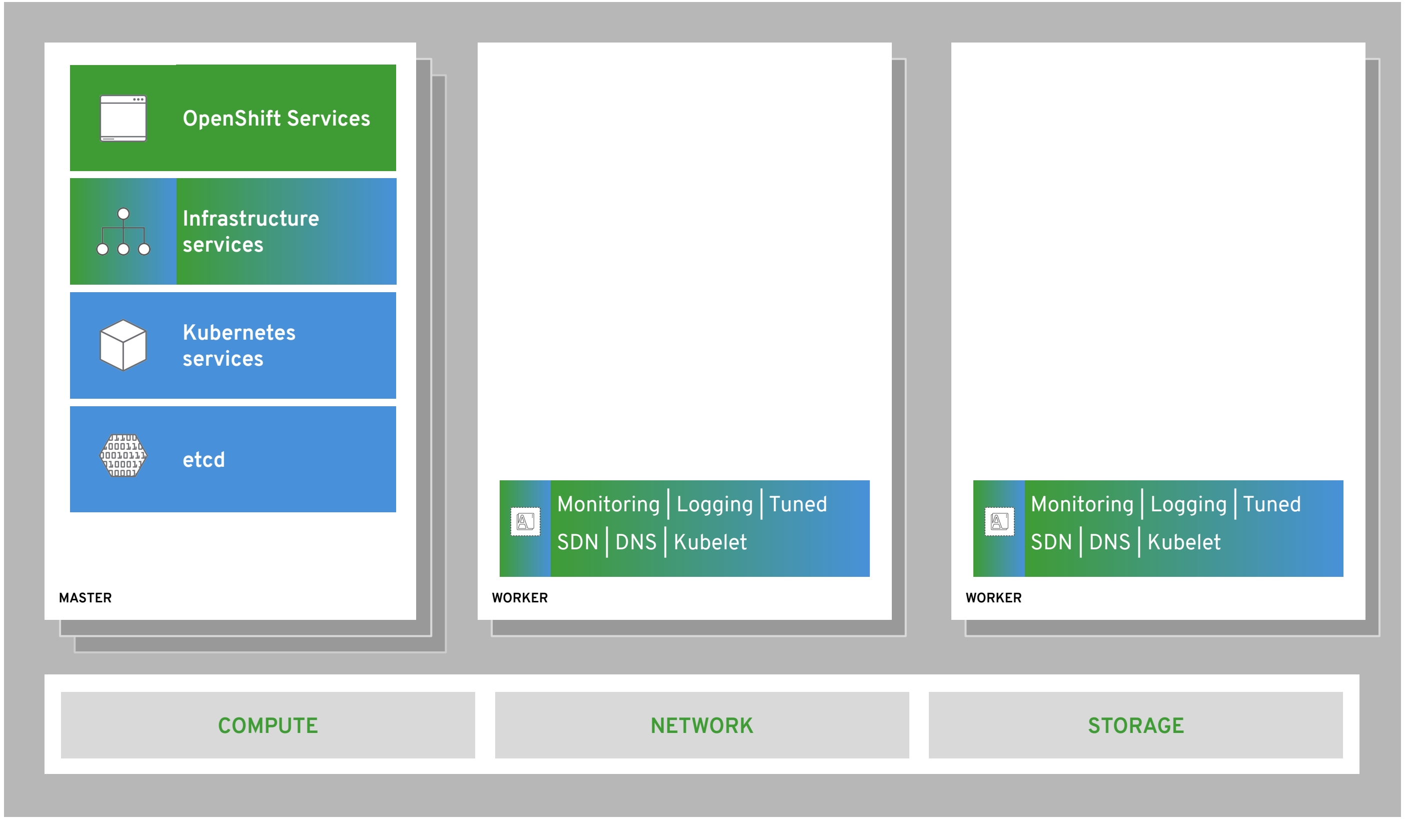
core OpenShift components



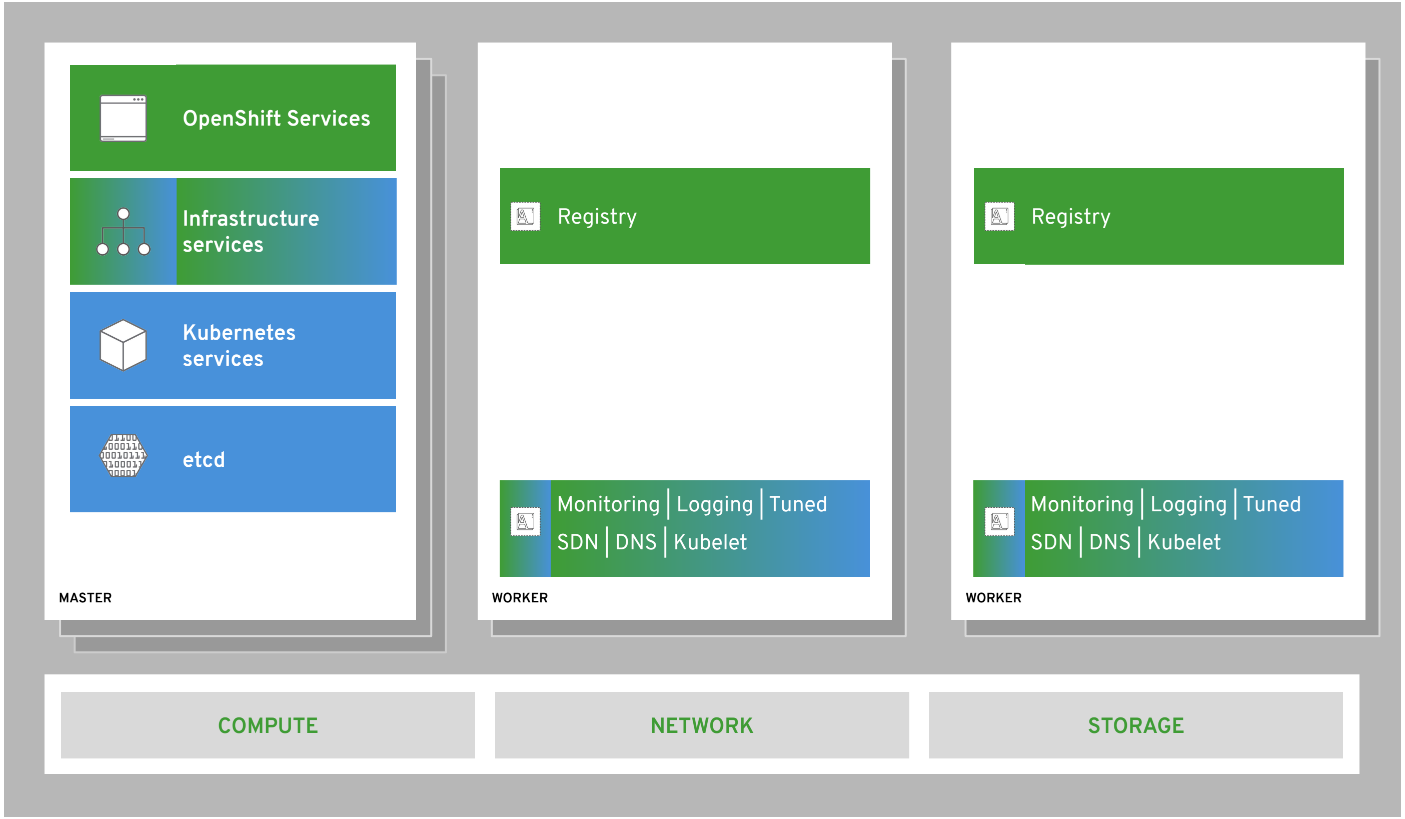
internal and support infrastructure services



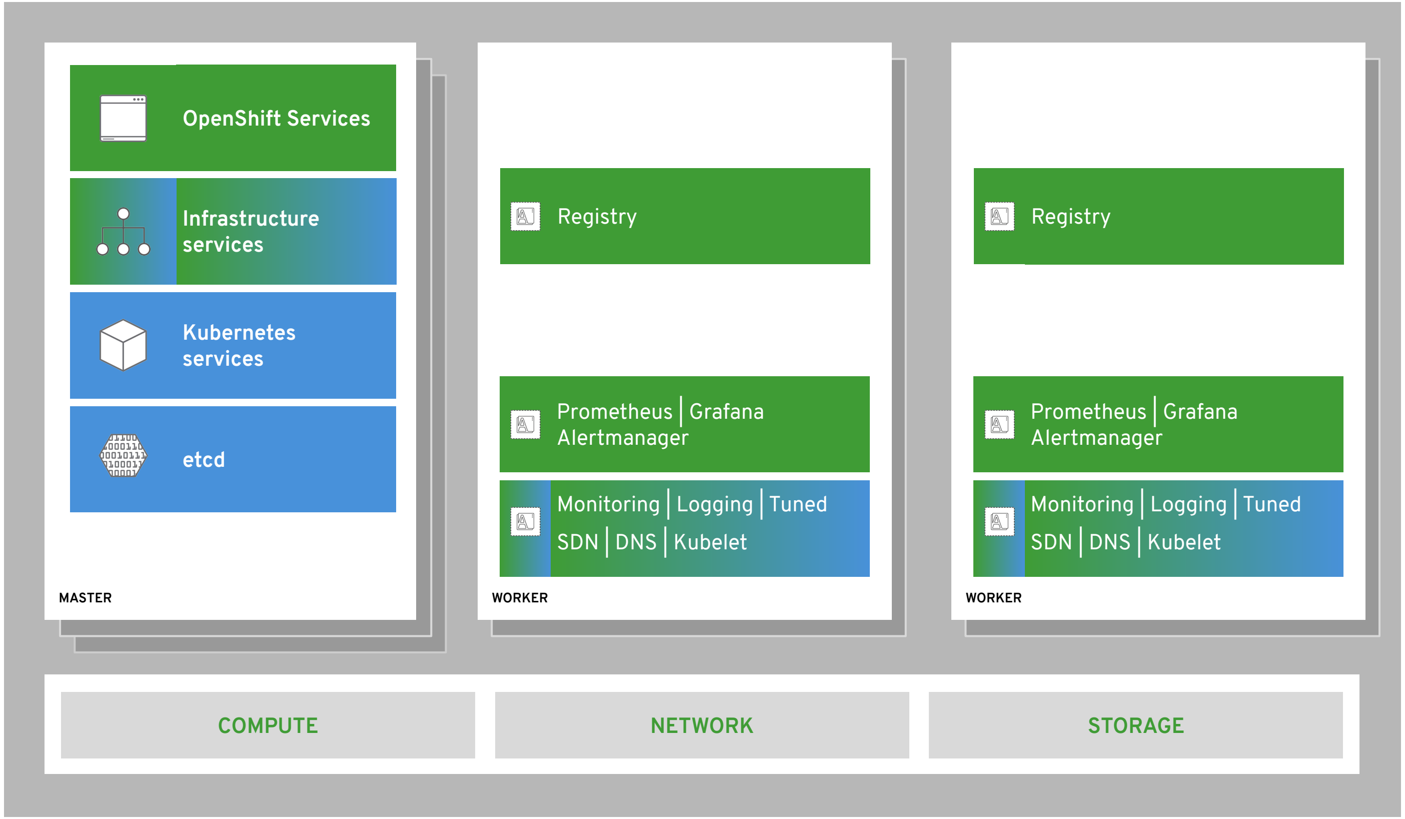
run on all hosts



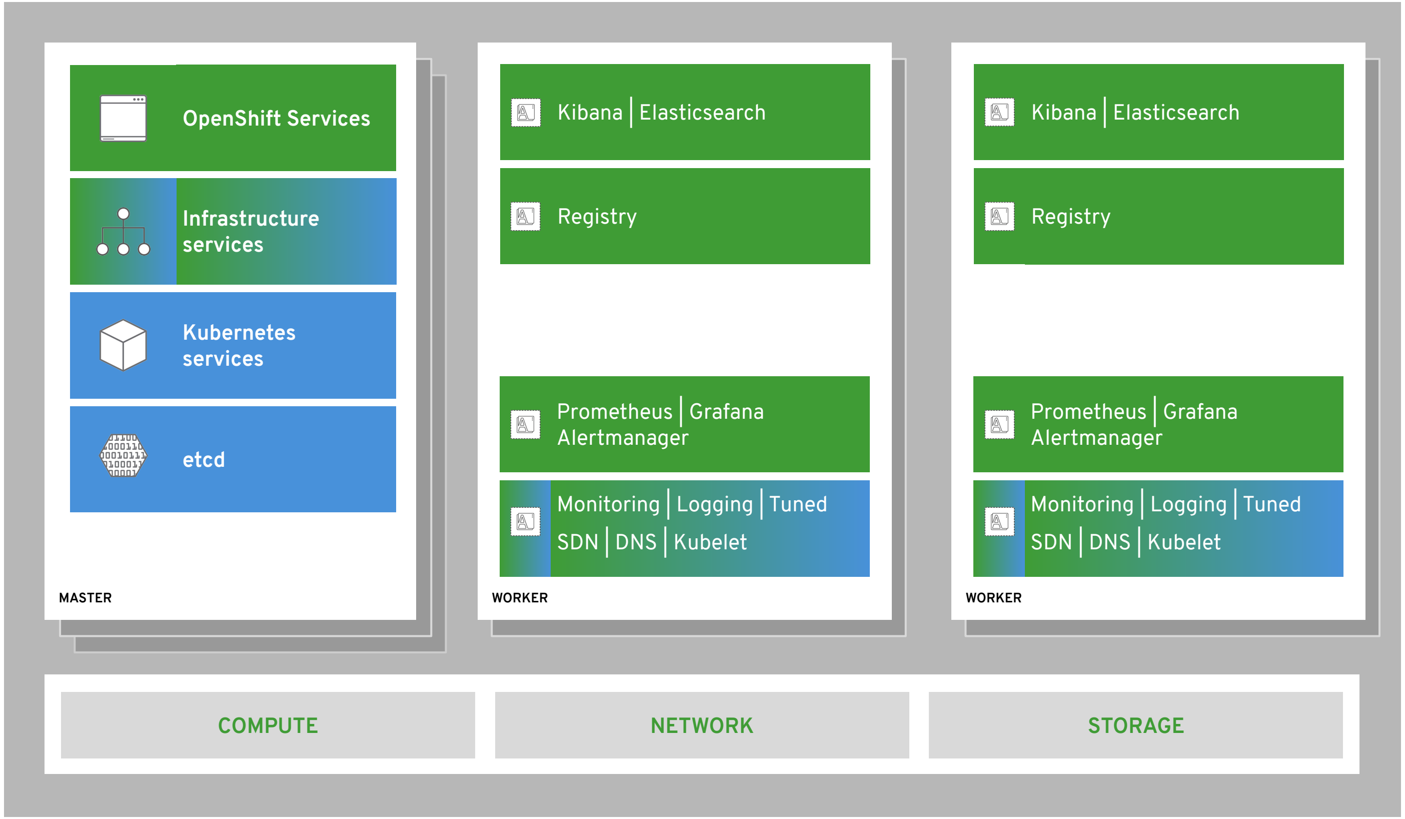
integrated image registry



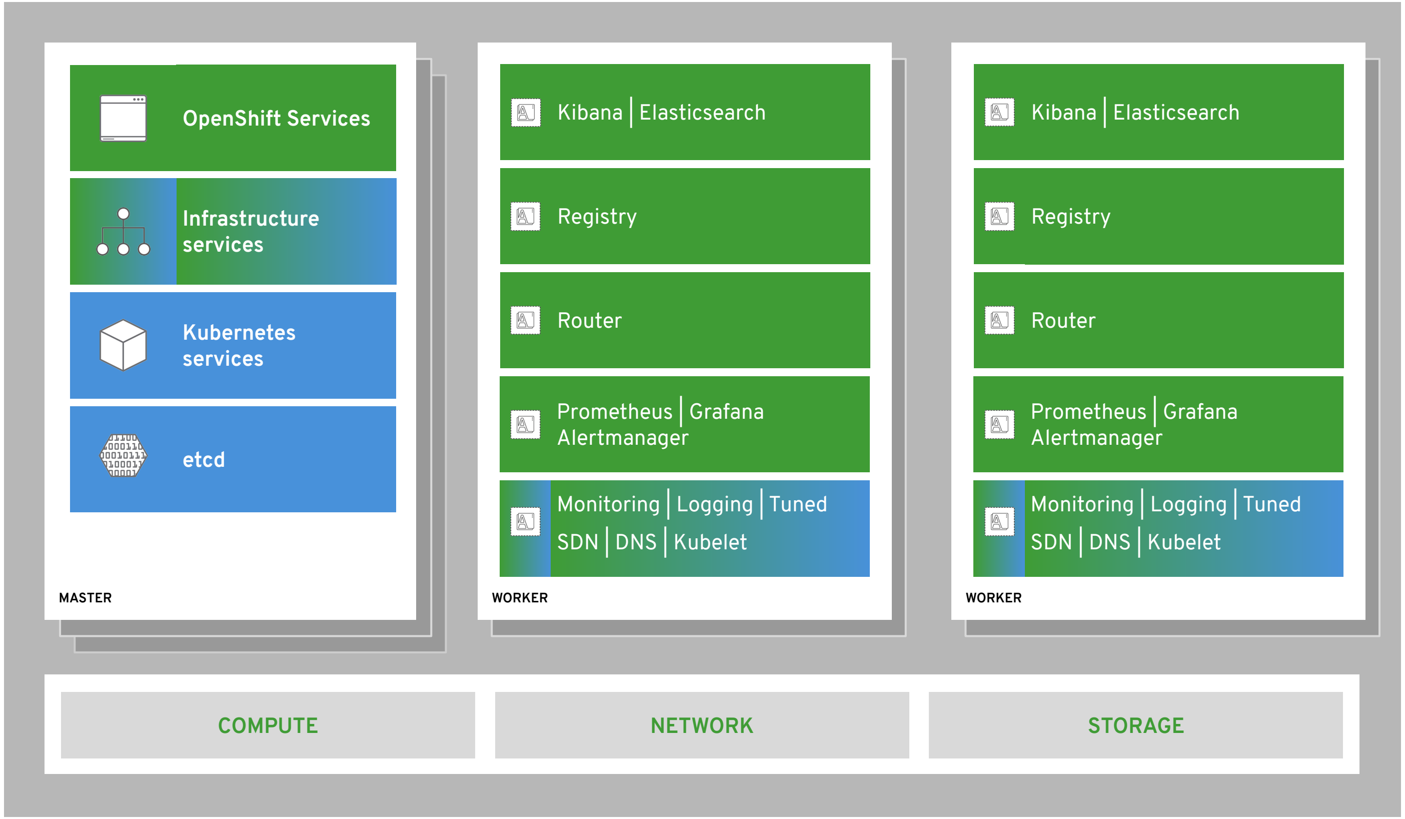
cluster monitoring



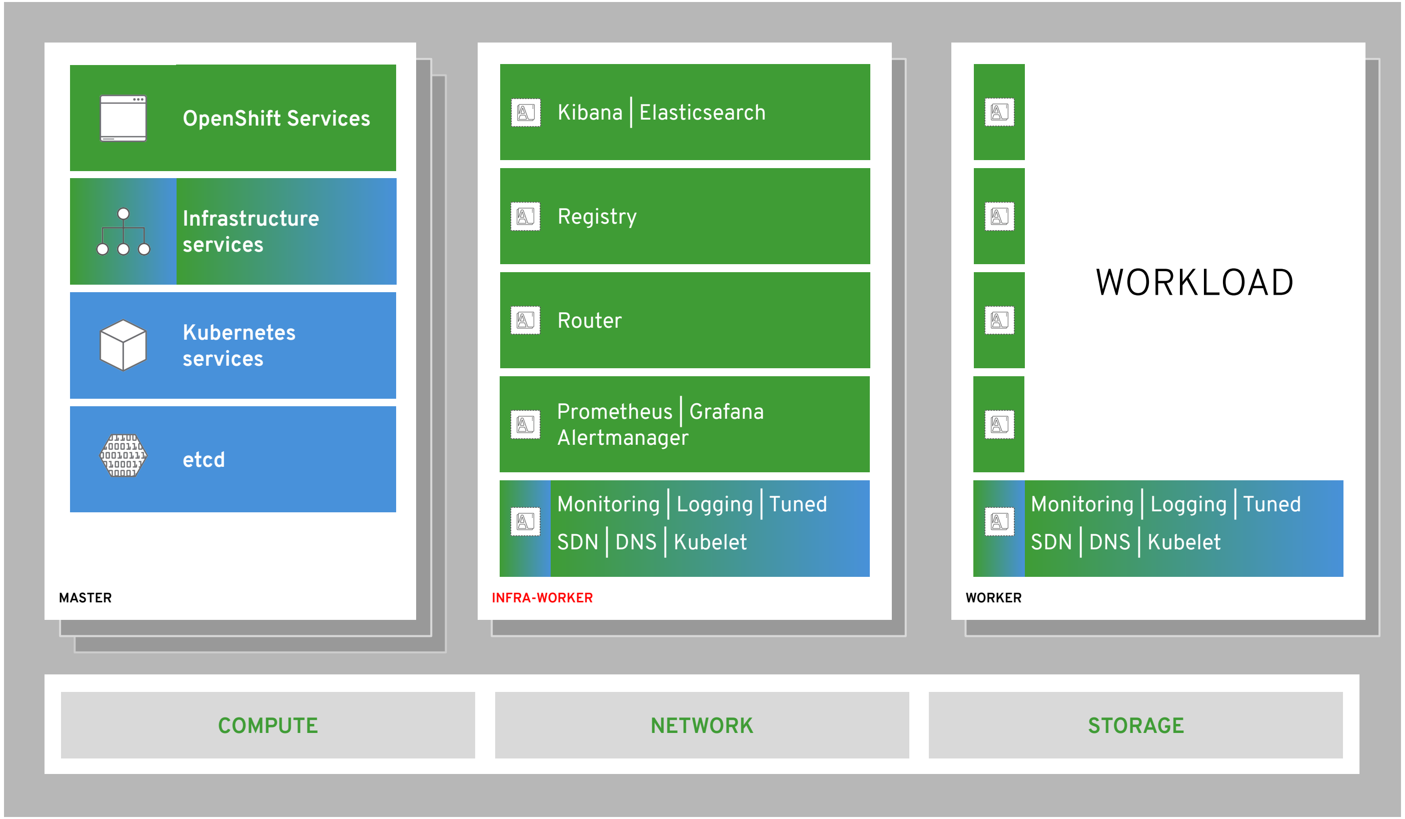
log aggregation



integrated routing



Concept of “InfraNodes”



OpenShift Services

Infrastructure services

Kubernetes services

etcd

MASTER

Kibana | Elasticsearch

Registry

Router

Prometheus | Grafana
Alertmanager

Monitoring | Logging | Tuned
SDN | DNS | Kubelet

INFRA-WORKER

WORKLOAD

Monitoring | Logging | Tuned
SDN | DNS | Kubelet

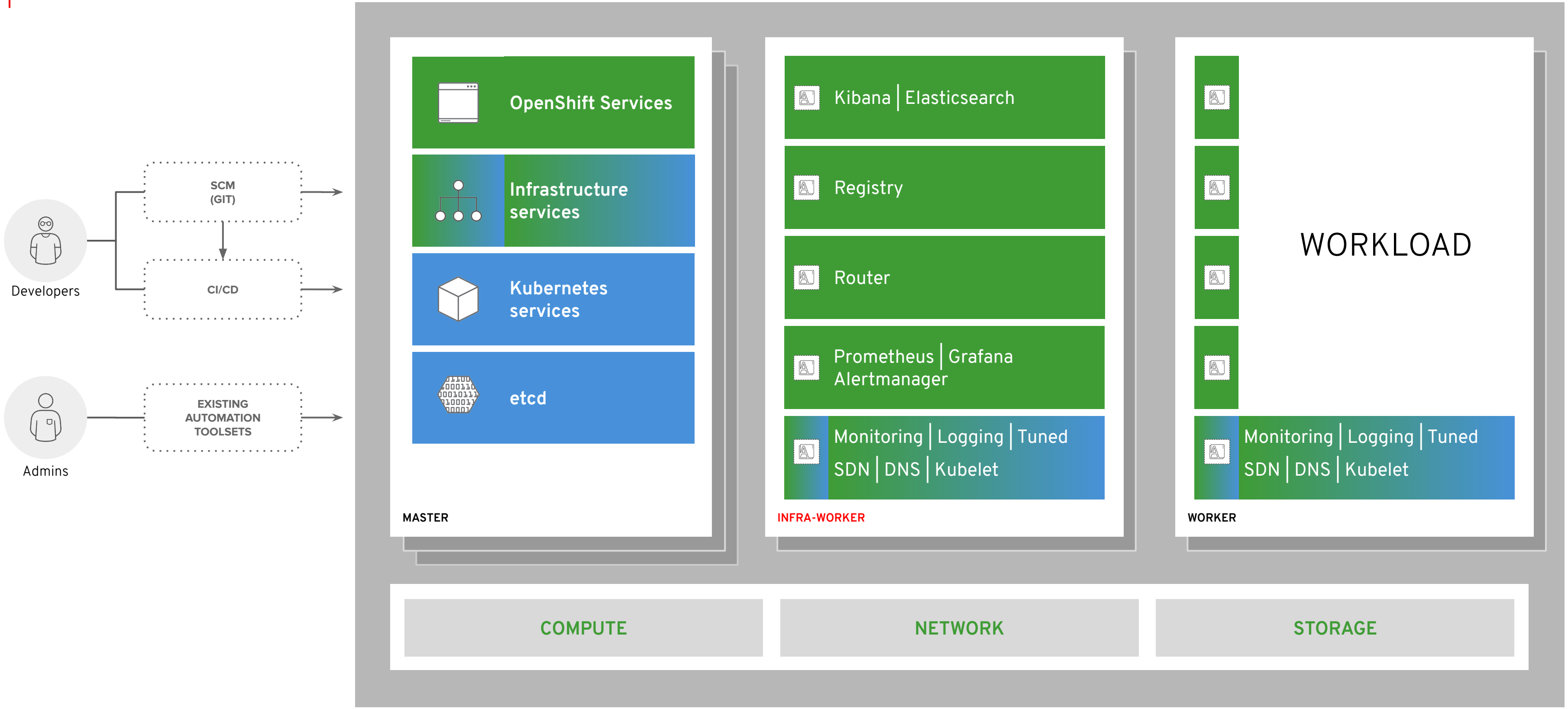
WORKER

COMPUTE

NETWORK

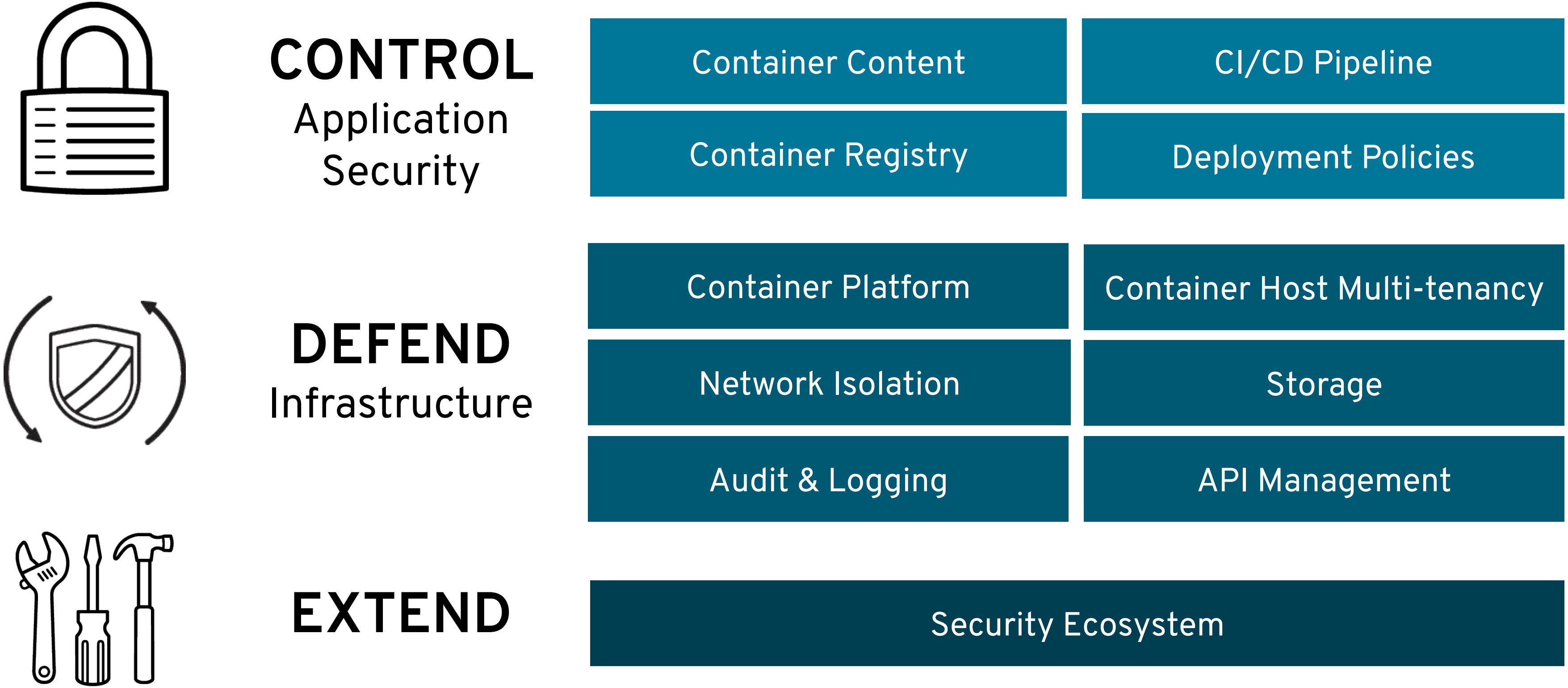
STORAGE

dev and ops via web, cli, API, and IDE



OpenShift Security

Features, mechanisms and processes for container and platform isolation



CONTROL
Application Security

- Container Content
- CI/CD Pipeline
- Container Registry
- Deployment Policies

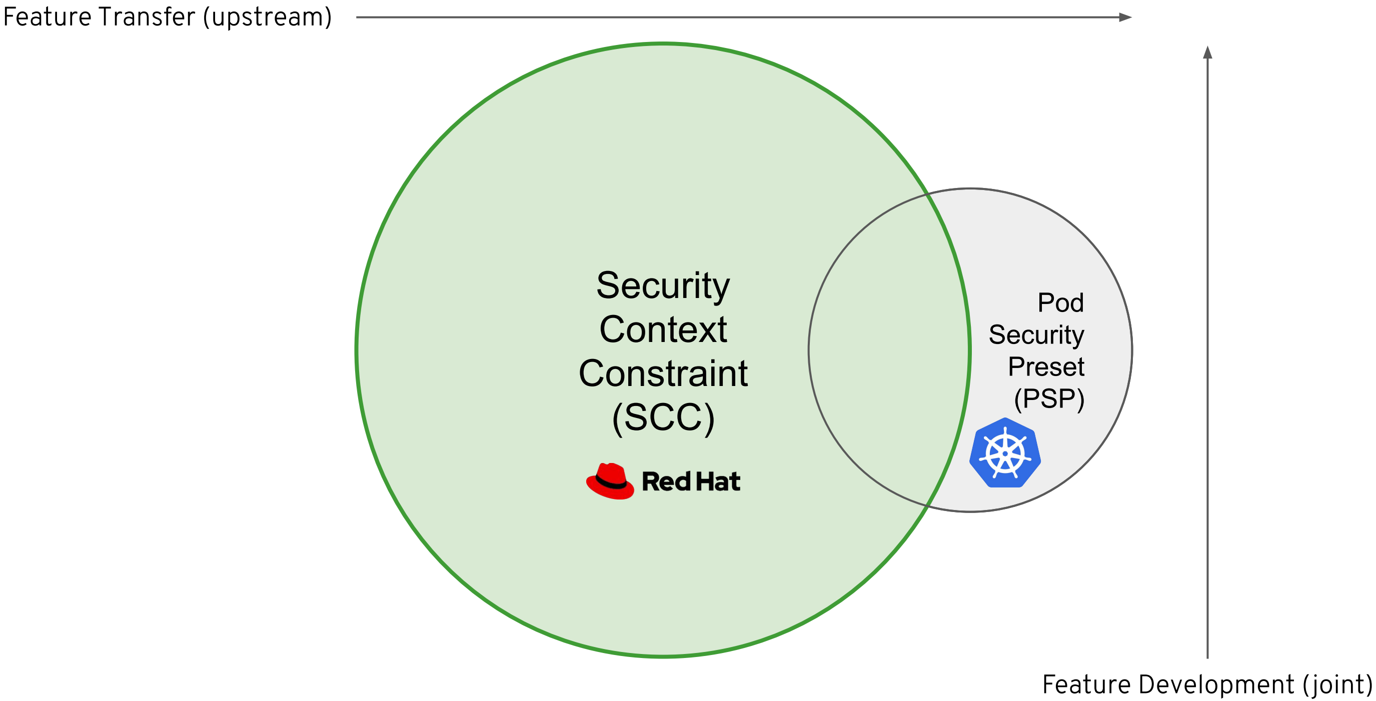
DEFEND
Infrastructure

- Container Platform
- Container Host Multi-tenancy
- Network Isolation
- Storage
- Audit & Logging
- API Management

EXTEND

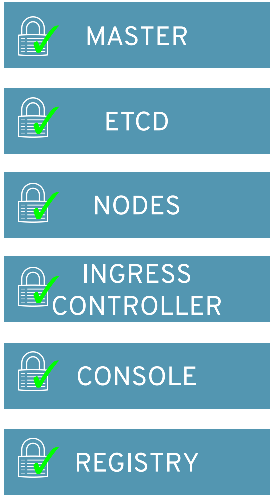
- Security Ecosystem

Extended Depth of Protection


Feature Transfer (upstream)
Security Context Constraint (SCC)
Red Hat
Pod Security Preset (PSP)
Feature Development (joint)

Certificates and Certificate Management

- OpenShift provides its own internal CA
- Certificates are used to provide secure connections to
  - master (APIs) and nodes
  - Ingress controller and registry
  - etcd
- Certificate rotation is automated
- Optionally configure external endpoints to use custom certificates



MASTER

ETCD

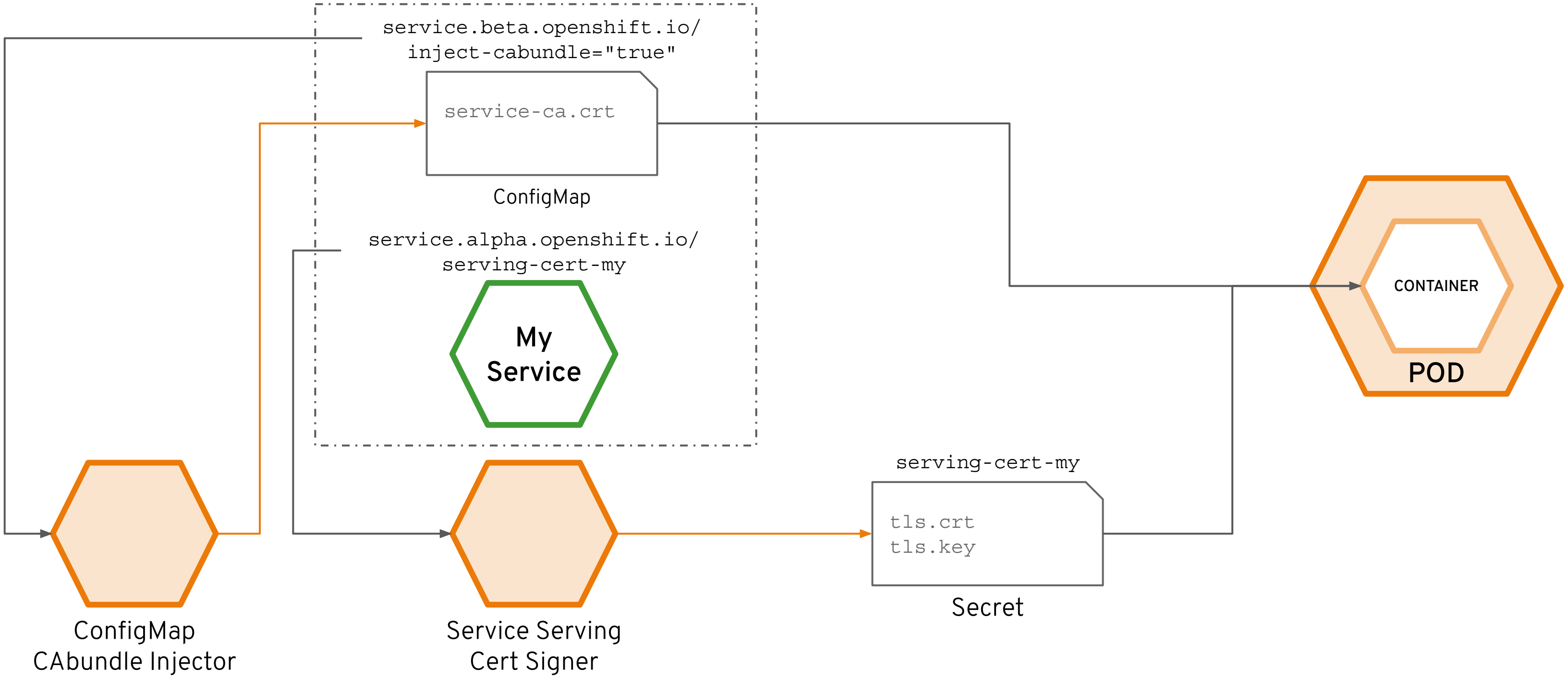
NODES

INGRESS CONTROLLER

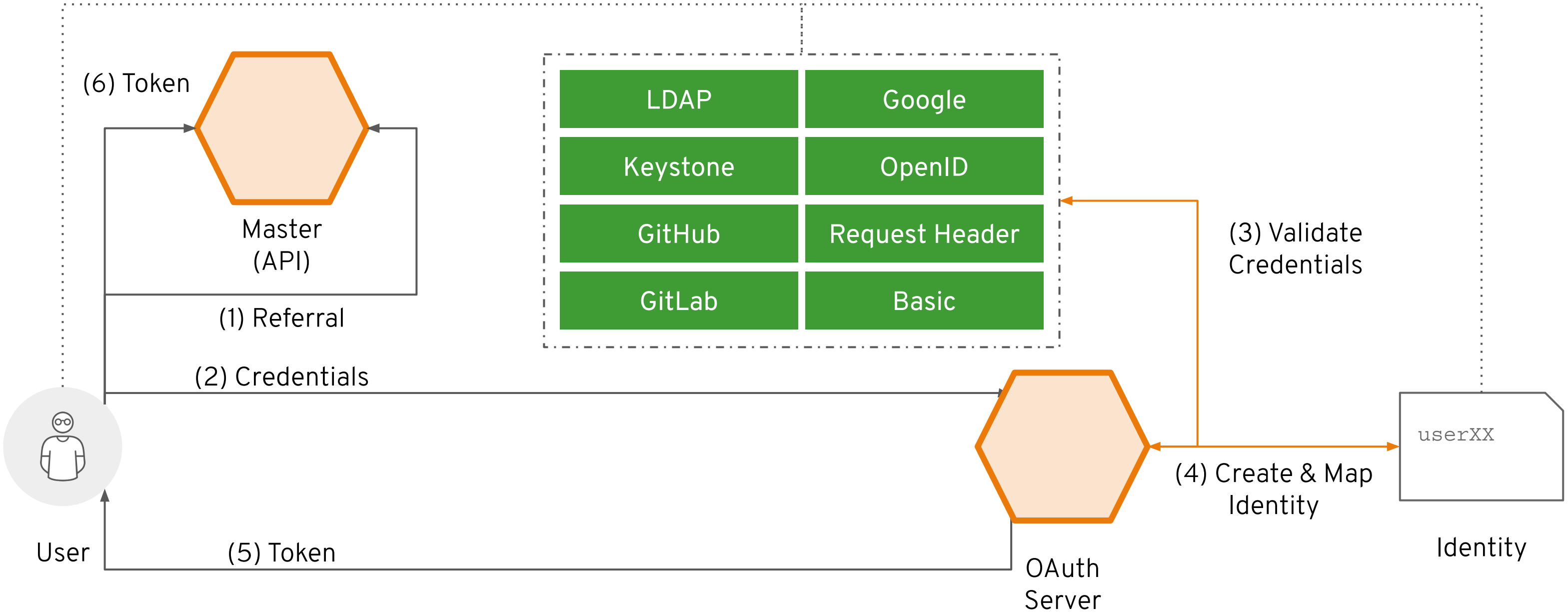
CONSOLE

REGISTRY

Service Certificates



Identity and Access Management



Fine-Grained RBAC

- Project scope & cluster scope available
- Matches request attributes (verb,object,etc)
- If no roles match, request is denied (deny by default)
- Operator- and user-level roles are defined by default
- Custom roles are supported

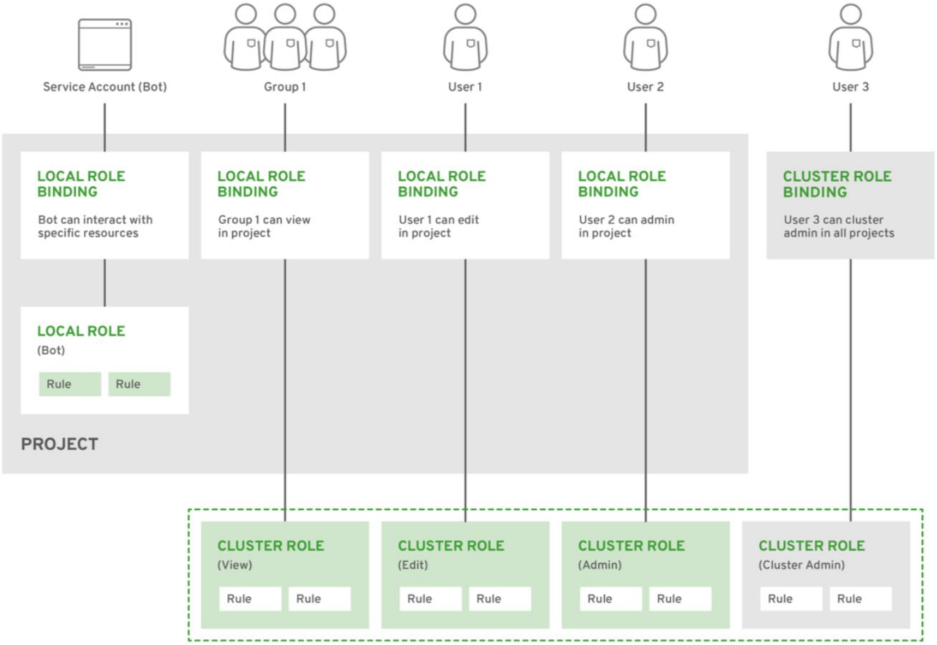


Figure 12 - Authorization Relationships

OpenShift Monitoring

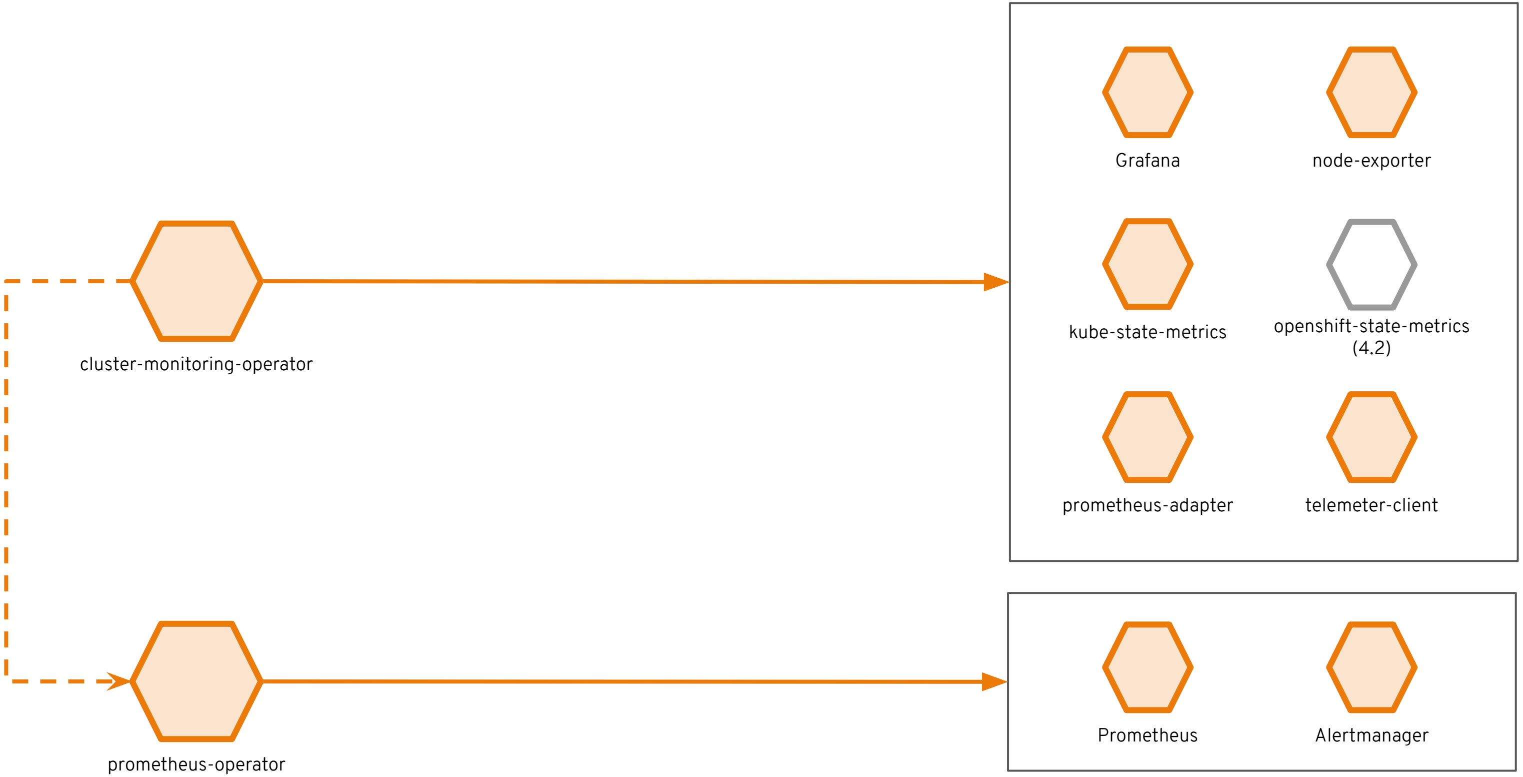
An integrated cluster monitoring and alerting stack

OpenShift Cluster Monitoring

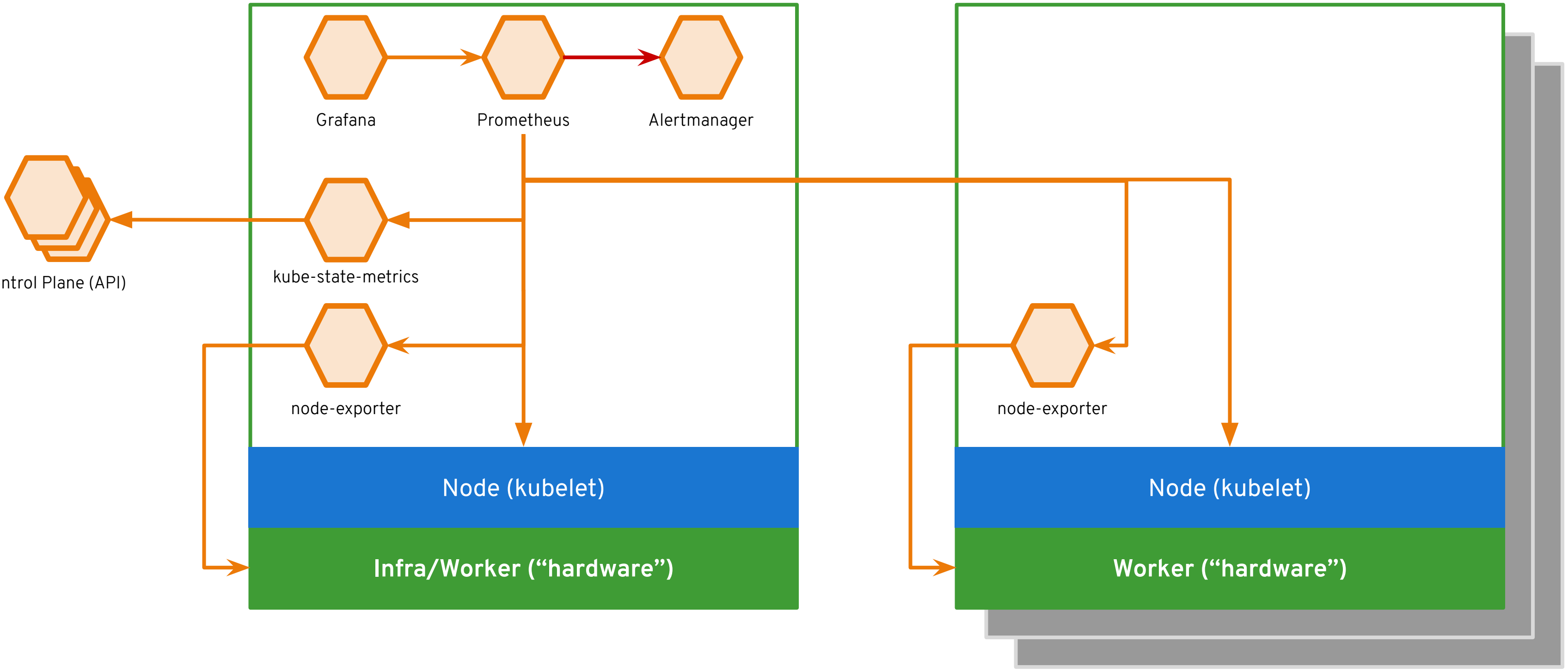
Metrics collection and storage via Prometheus, an open-source monitoring system time series database.

Alerting/notification via Prometheus' Alertmanager, an open-source tool that handles alerts send by Prometheus.

Metrics visualization via Grafana, the leading metrics visualization technology.


cluster-monitoring-operator
prometheus-operator
Grafana
node-exporter
kube-state-metrics
openshift-state-metrics (4.2)
prometheus-adapter
telemeter-client
Prometheus
Alertmanager

OPENSHIFT MONITORING | Prometheus, Grafana and Alertmanager Wiring



Red Hat

OpenShift Logging

An integrated solution for exploring and corroborating application logs

Observability via log exploration and corroboration with EFK

Components

- **Elasticsearch:** a search and analytics engine to store logs
- **Fluentd:** gathers logs and sends to Elasticsearch.
- **Kibana:** A web UI for Elasticsearch.

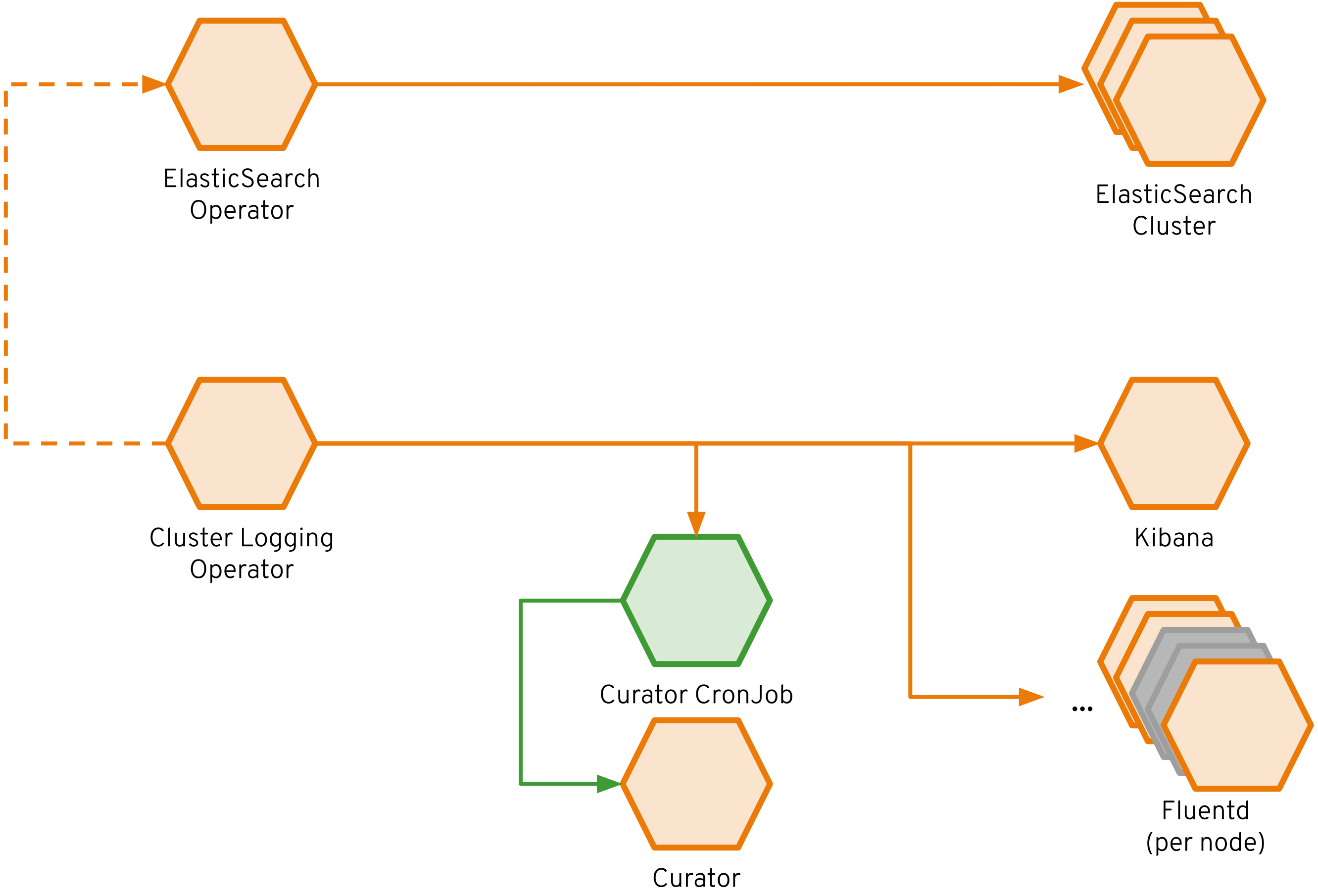
Access control

- Cluster administrators can view all logs
- Users can only view logs for their projects

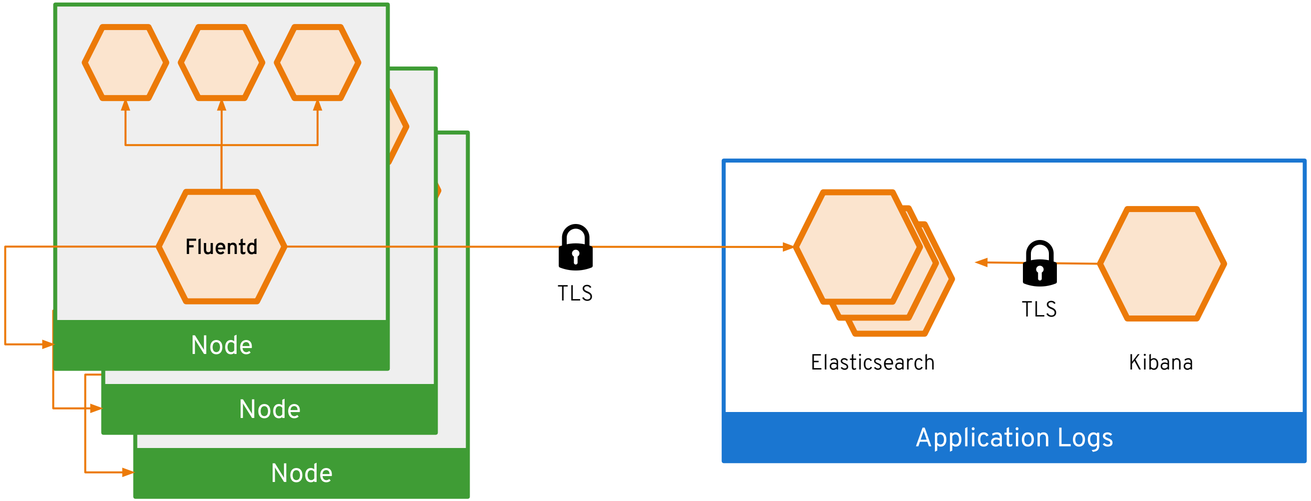
Ability to forward logs elsewhere

- External elasticsearch, Splunk, etc

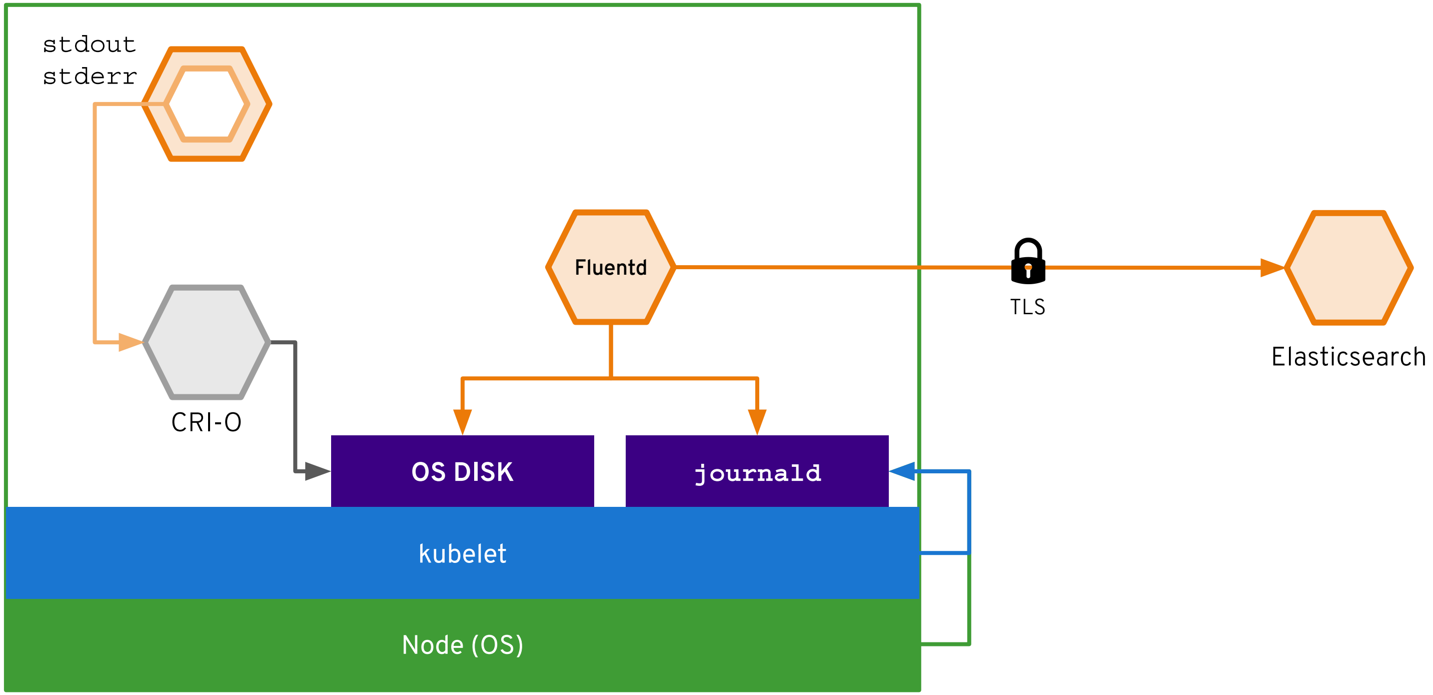
Operator & Operand Relationships



Log data flow in OpenShift



Log data flow in OpenShift



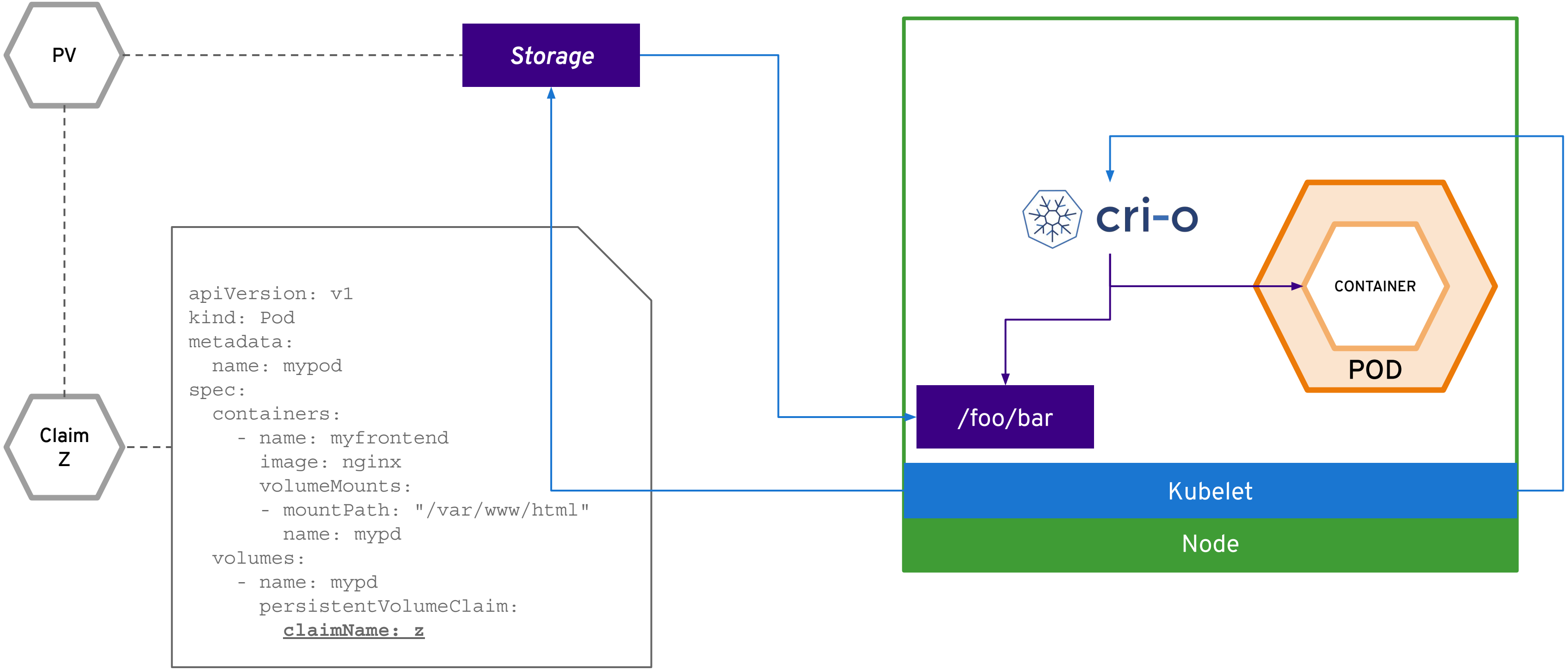
Persistent Storage

Connecting real-world storage to your containers to enable stateful applications

A broad spectrum of static and dynamic storage endpoints

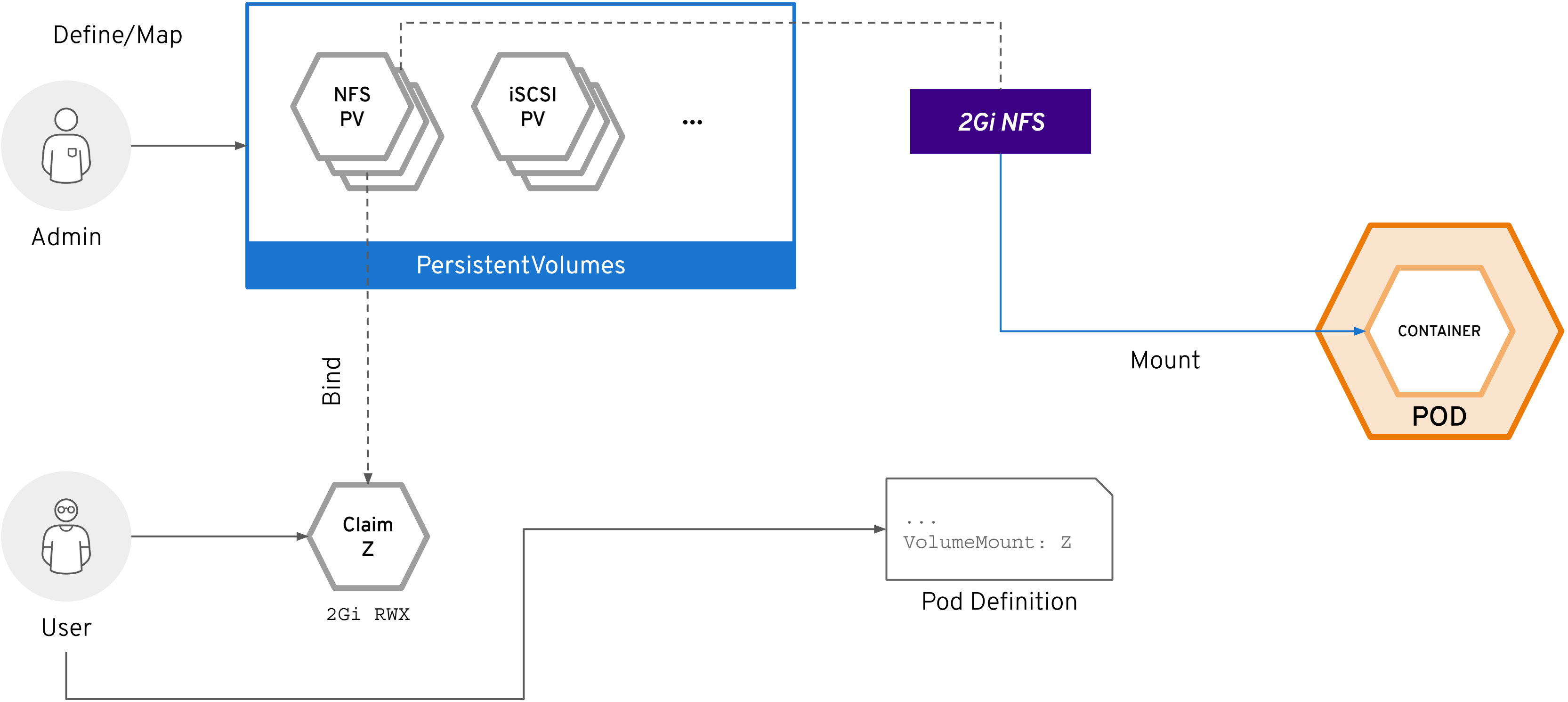
- NFS
- OpenStack Cinder
- iSCSI
- Azure Disk
- AWS EBS
- FlexVolume
- GlusterFS
- Ceph RBD
- Fiber Channel
- Azure File
- GCE Persistent Disk
- VMWare vSphere VMDK
- NetApp Trident*
- Container Storage Interface (CSI)**

PV Consumption



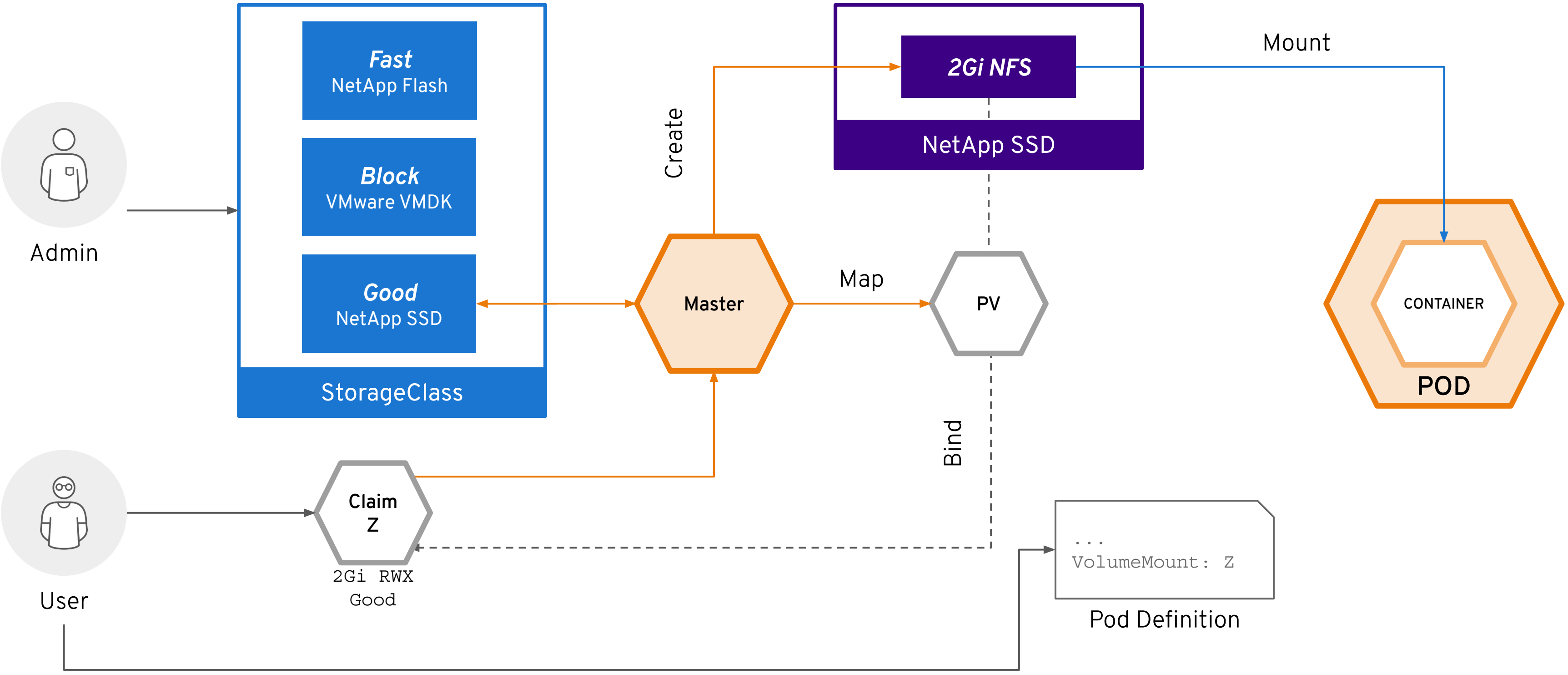
```yaml
apiVersion: v1
kind: Pod
metadata:
  name: mypod
spec:
  containers:
    - name: myfrontend
      image: nginx
      volumeMounts:
      - mountPath: "/var/www/html"
        name: mypd
  volumes:
    - name: mypd
      persistentVolumeClaim:
        claimName: z
```

Static Storage Provisioning



```
...
VolumeMount: Z
```

Dynamic Storage Provisioning


Admin
Fast
NetApp Flash
Block
VMware VMDK
Good
NetApp SSD
StorageClass
Create
Master
2Gi NFS
NetApp SSD
Mount
Map
PV
CONTAINER
POD
Bind
User
Claim
Z
2Gi RWX
Good
...
VolumeMount: Z
Pod Definition