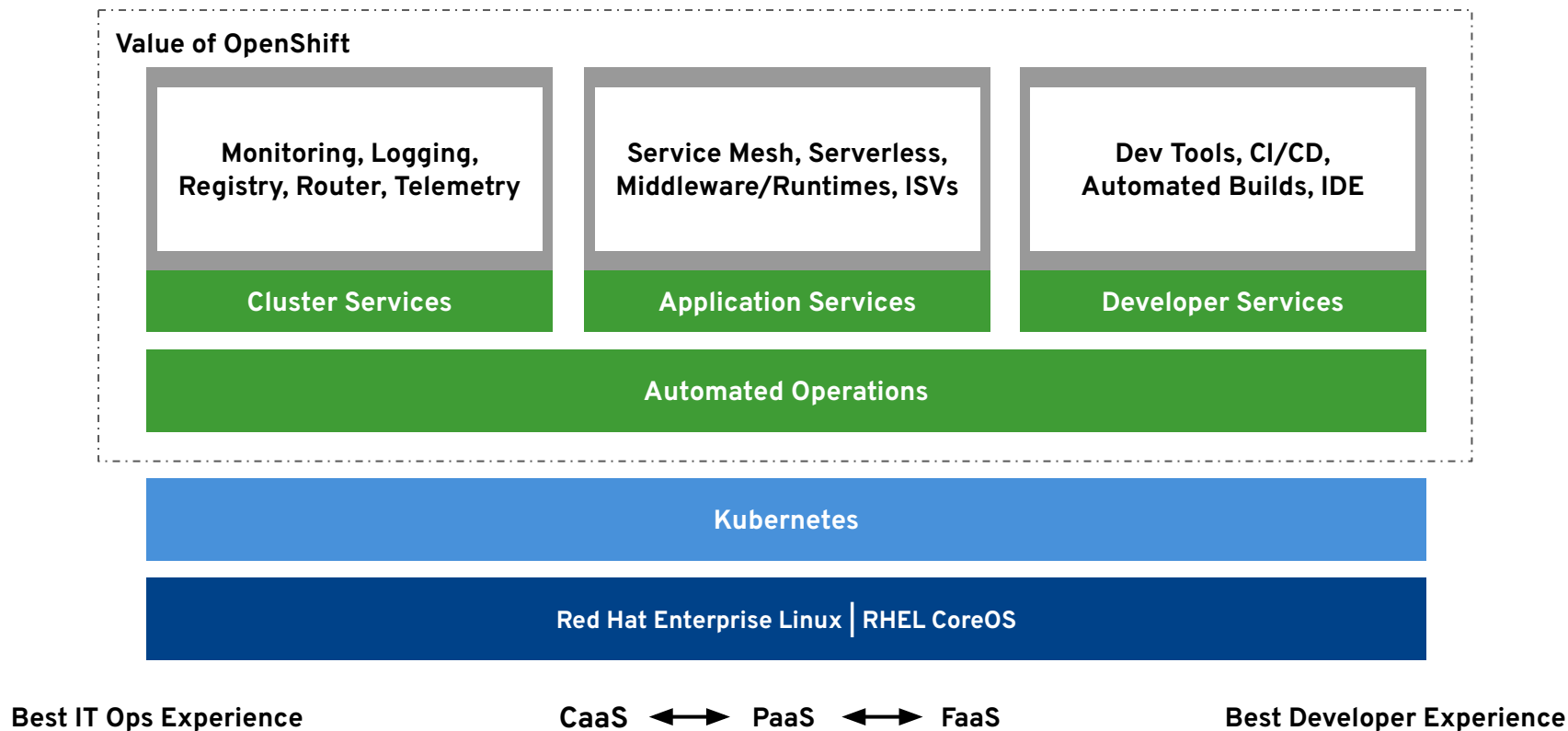


Red Hat Partner Bootcamp

OpenShift Topics

Alfred Bach
Principal Solution
Architect
Red Hat EMEA





Database

Streaming & Messaging

Application Definition & Image Build

Continuous Integration & Delivery

Platform

Observability and Analysis

App Definition and Development



Orchestration & Management



Cloud-Native Storage

Container Runtime

Cloud-Native Network

Runtime



Automation & Configuration

Container Registry

Security & Compliance

Key Management

Provisioning

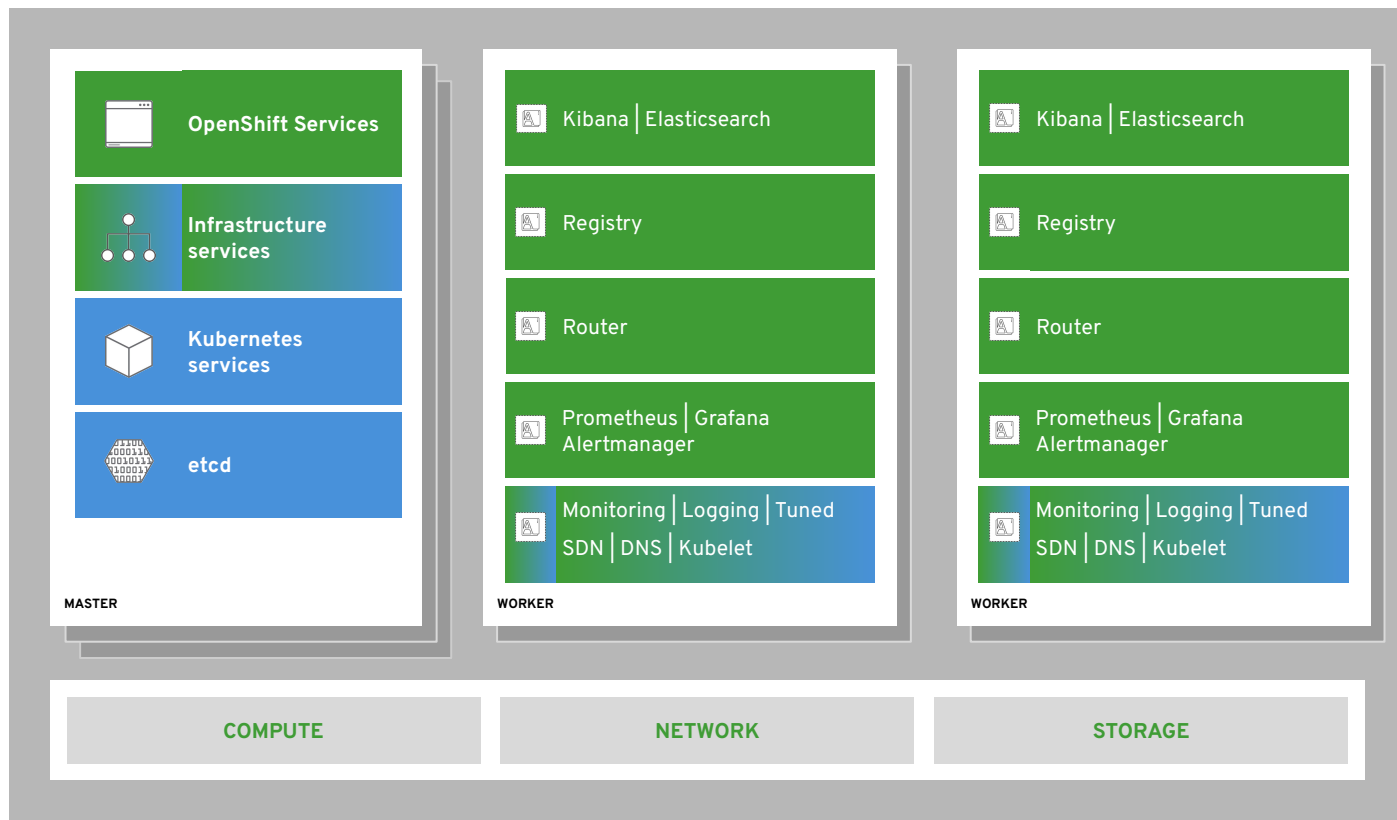
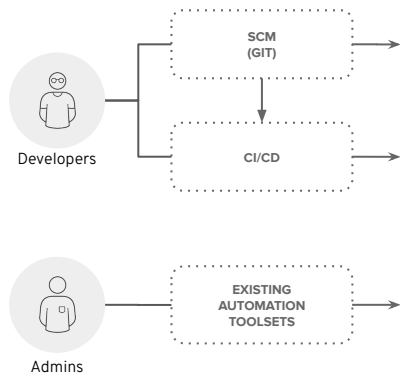



Public

Kubernetes Certified Service Provider

Kubernetes Training Partner







OpenShift and Kubernetes core concepts

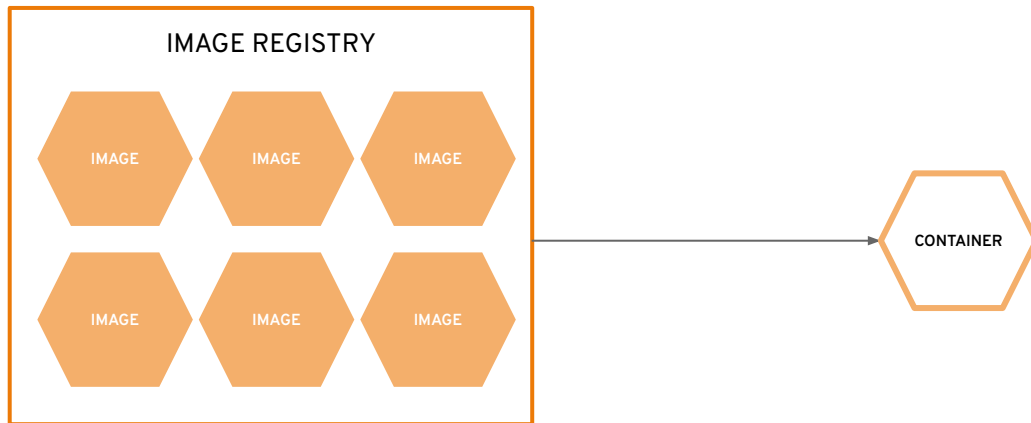
a container is the smallest compute unit



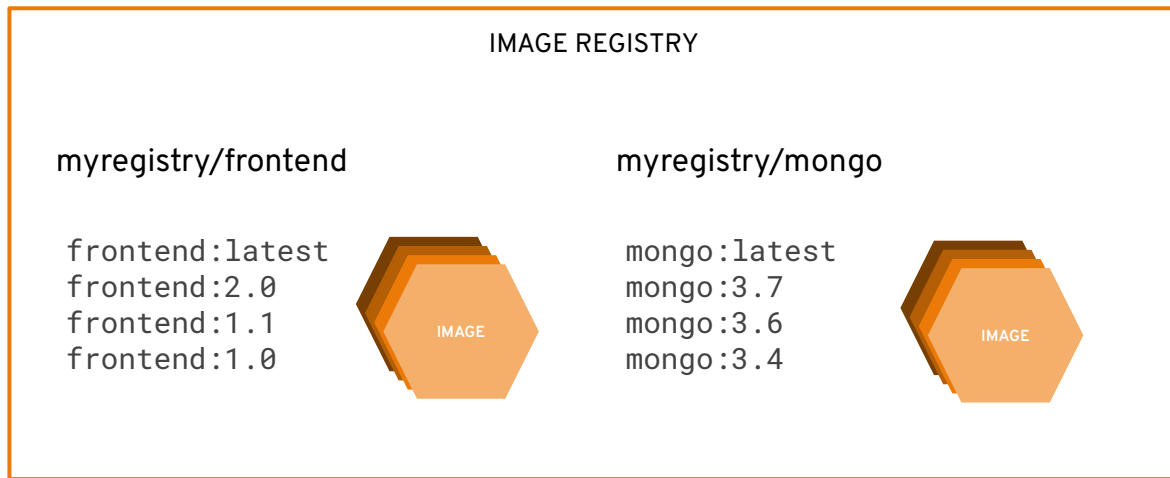
containers are created from container images



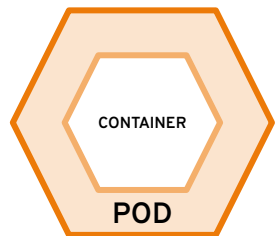
container images are stored in an image registry



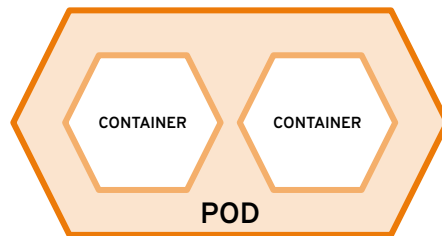
an image repository contains all versions of an image in the image registry



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

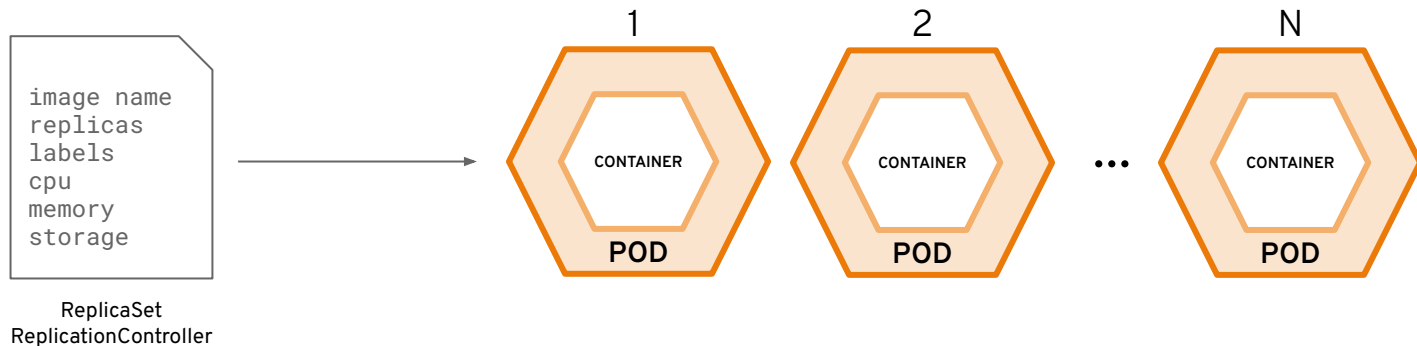


10.140.4.44

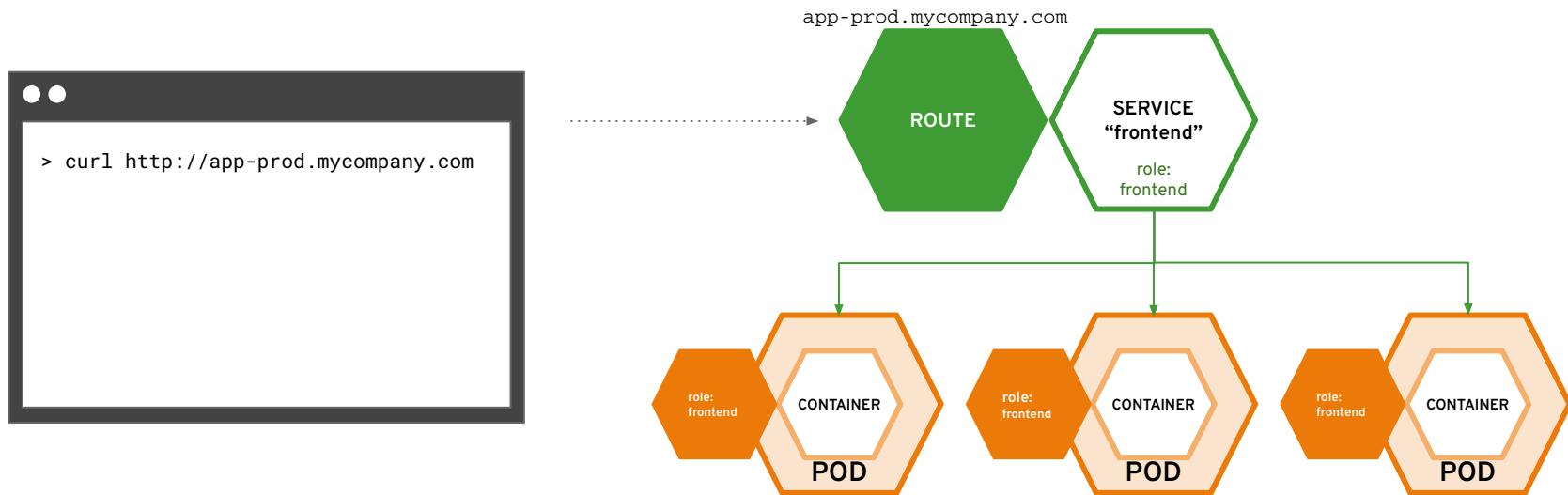


10.15.6.55

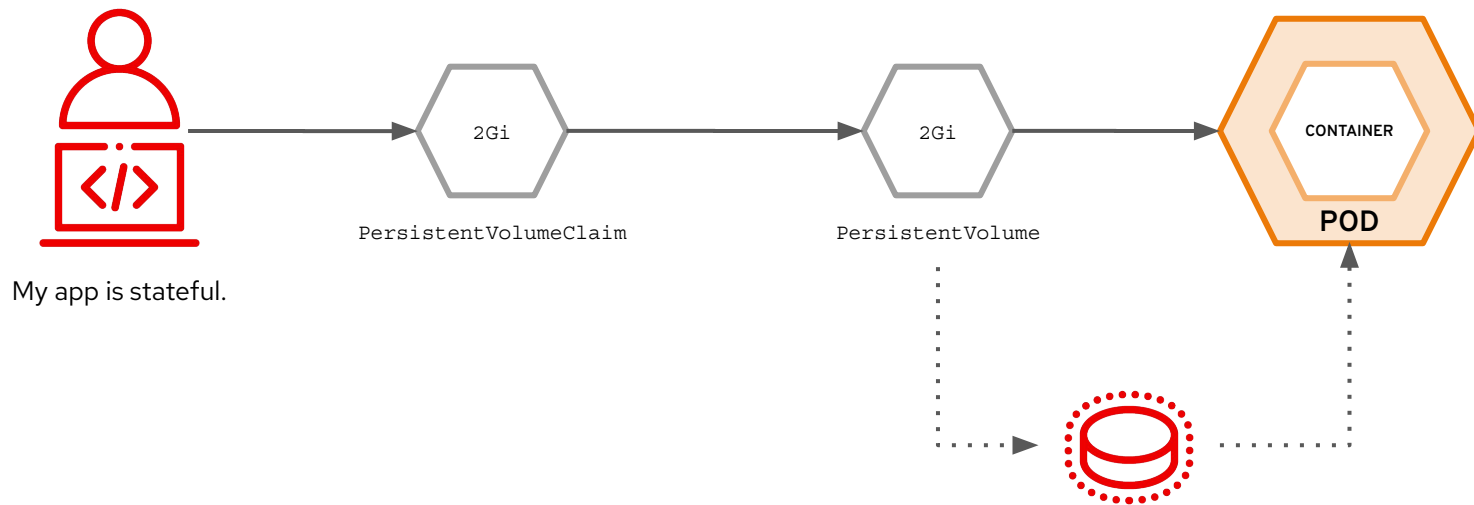
ReplicationControllers & ReplicaSets ensure a specified number of pods are running at any given time



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



Persistent Volume and Claims





OpenShift 4 Architecture

your choice of infrastructure

COMPUTE

NETWORK

STORAGE

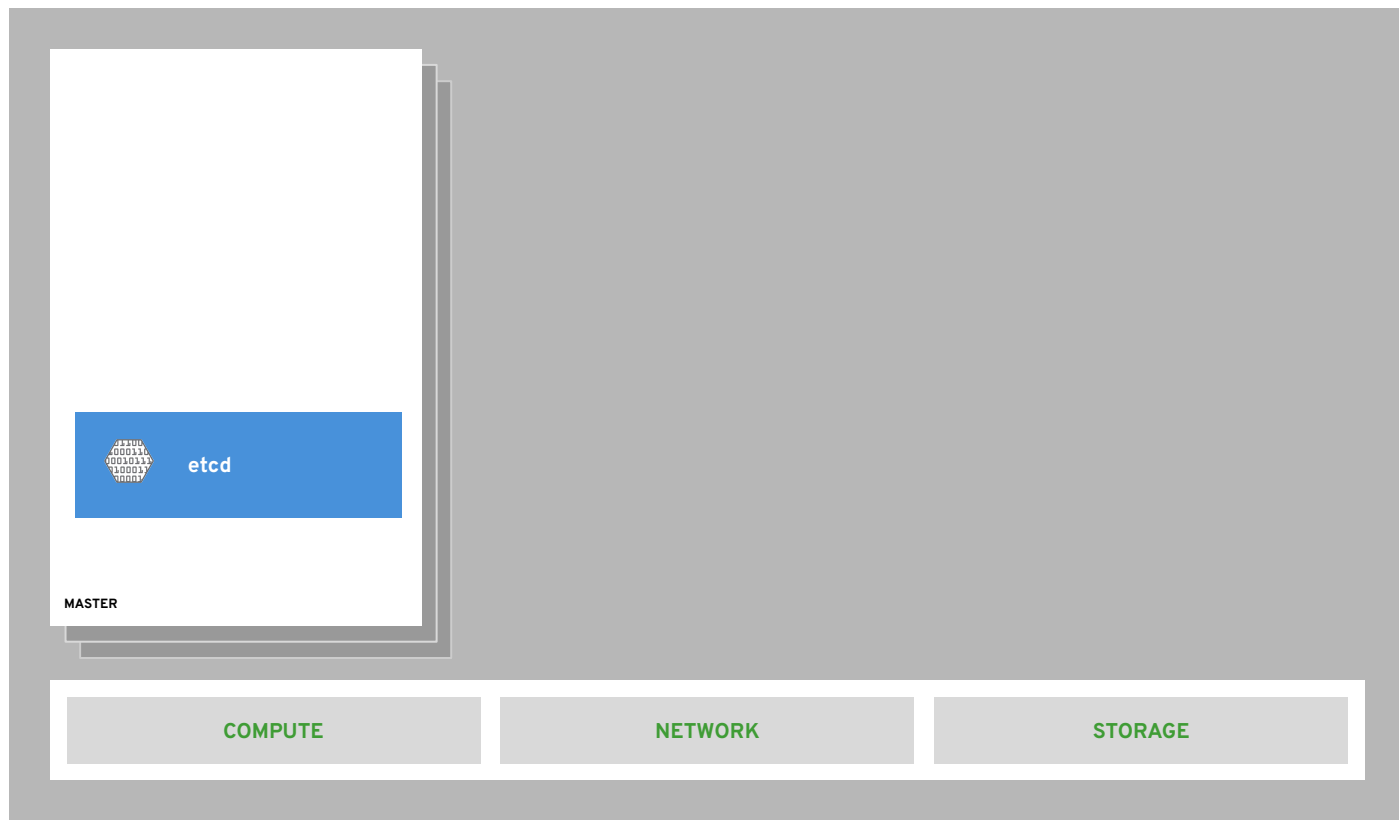
workers run workloads



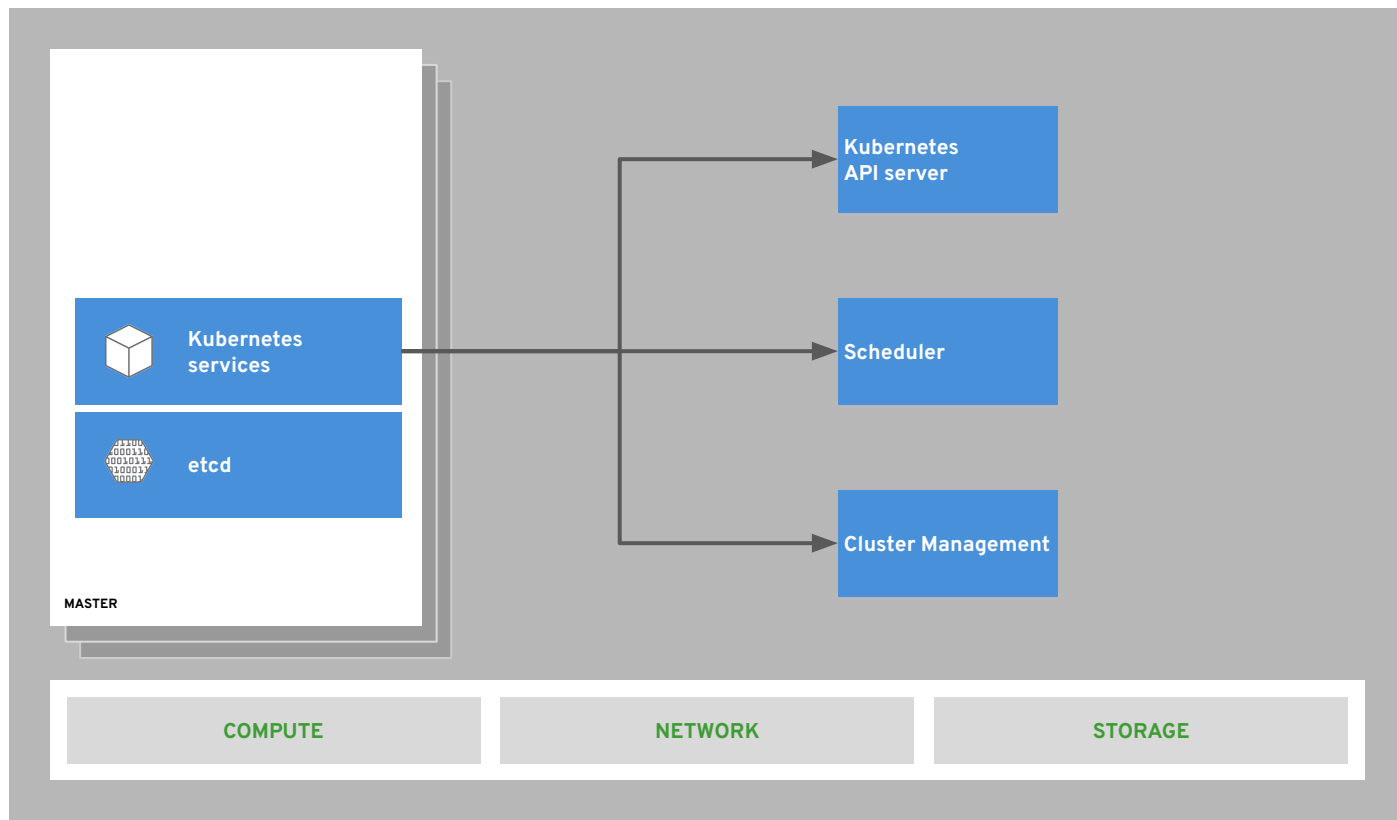
masters are the control plane



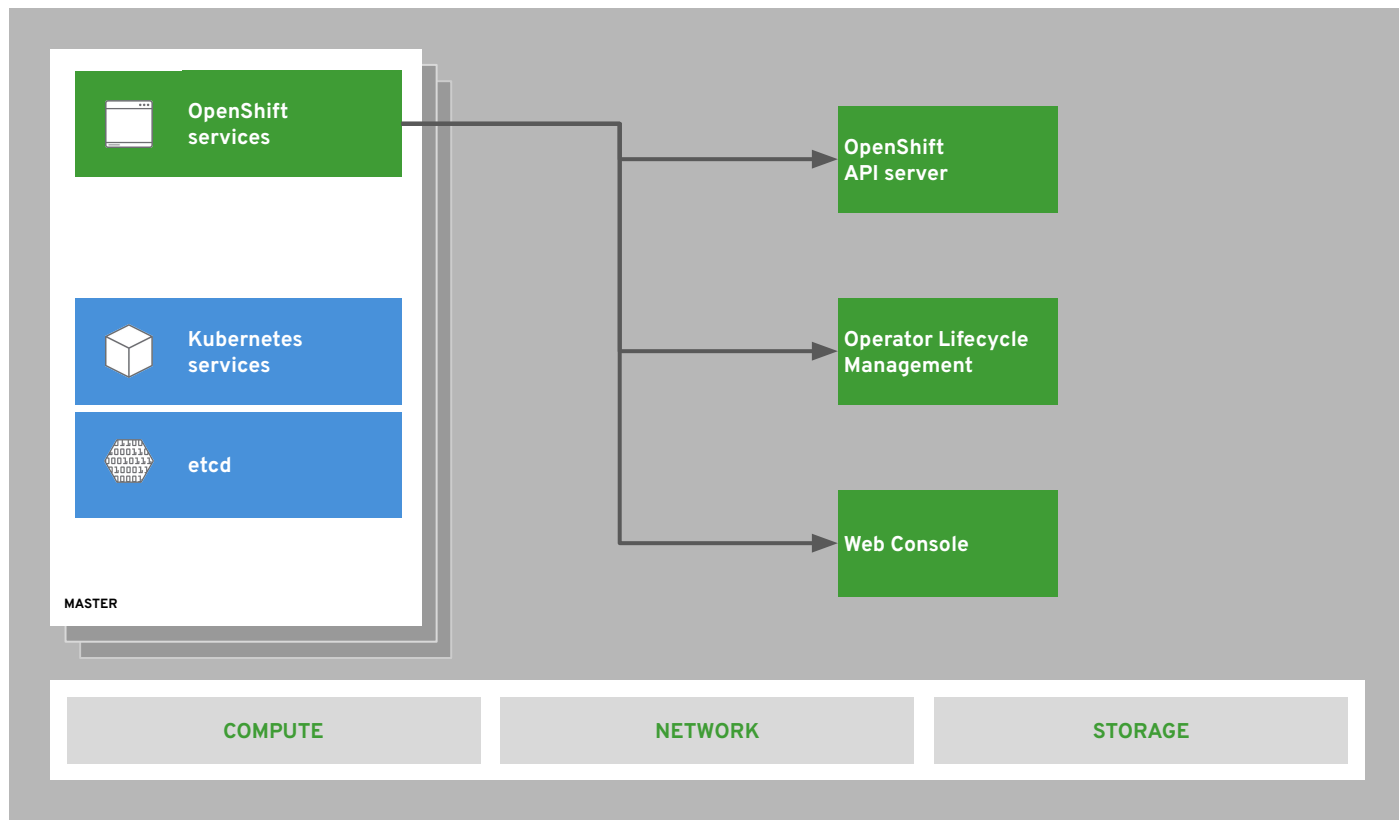
state of everything



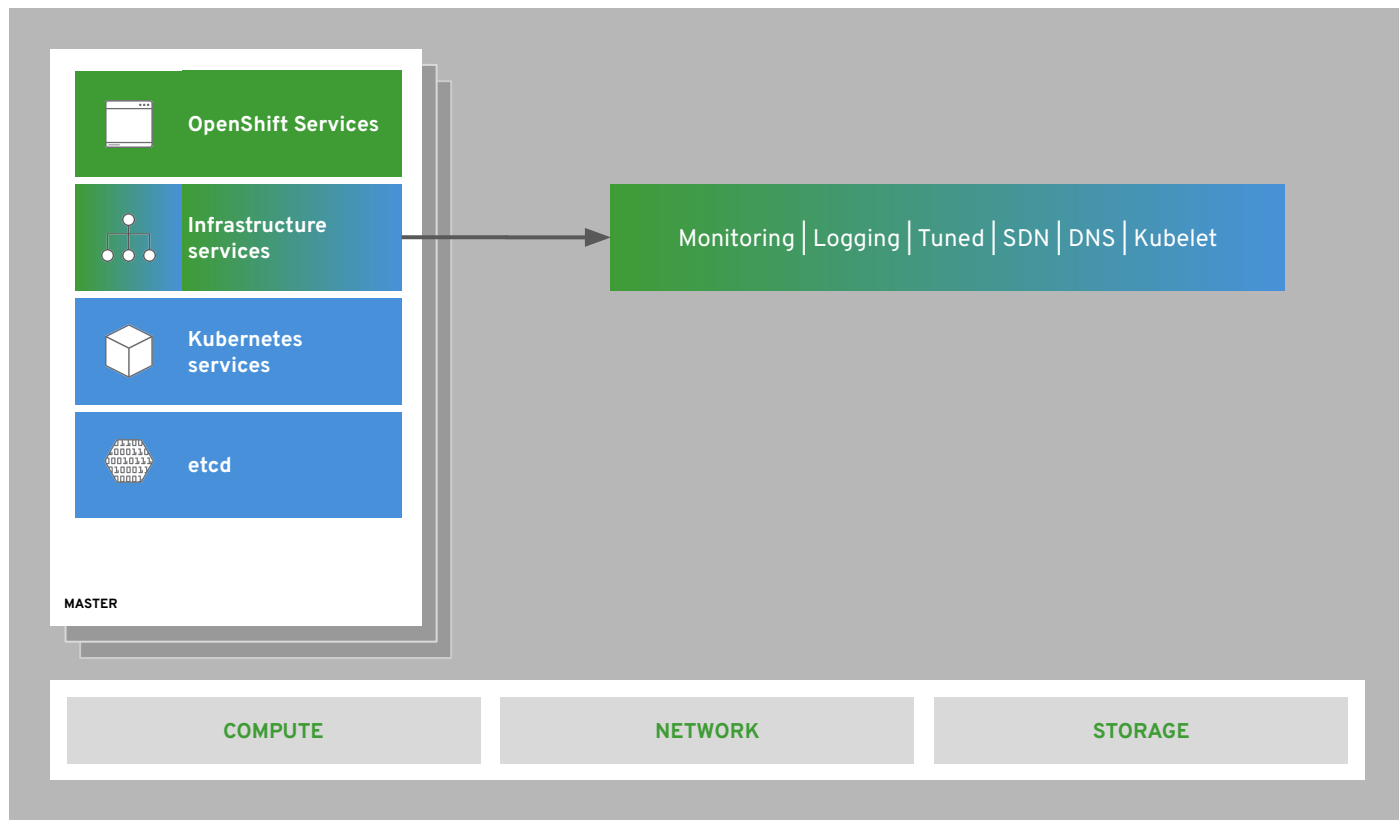
core kubernetes components



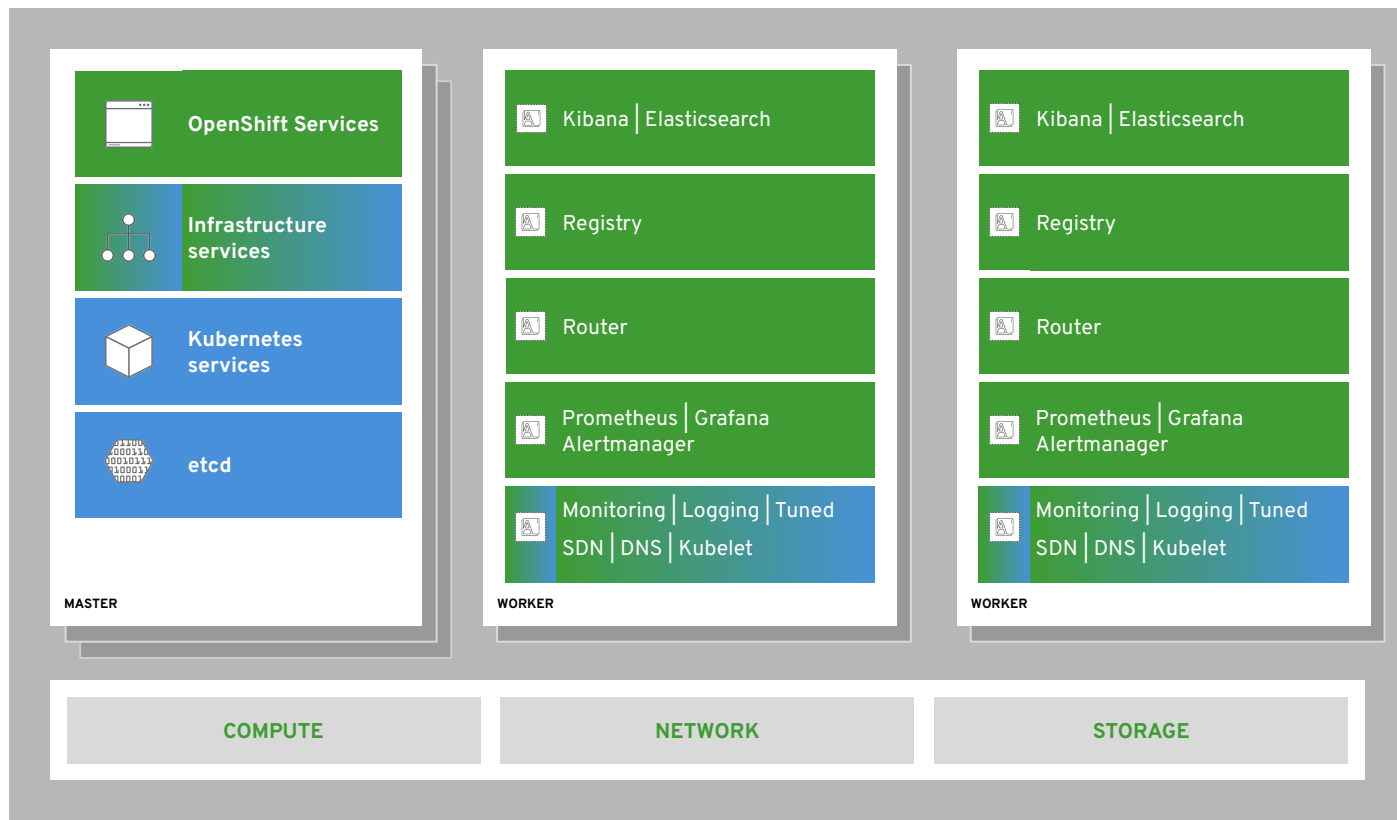
core OpenShift components



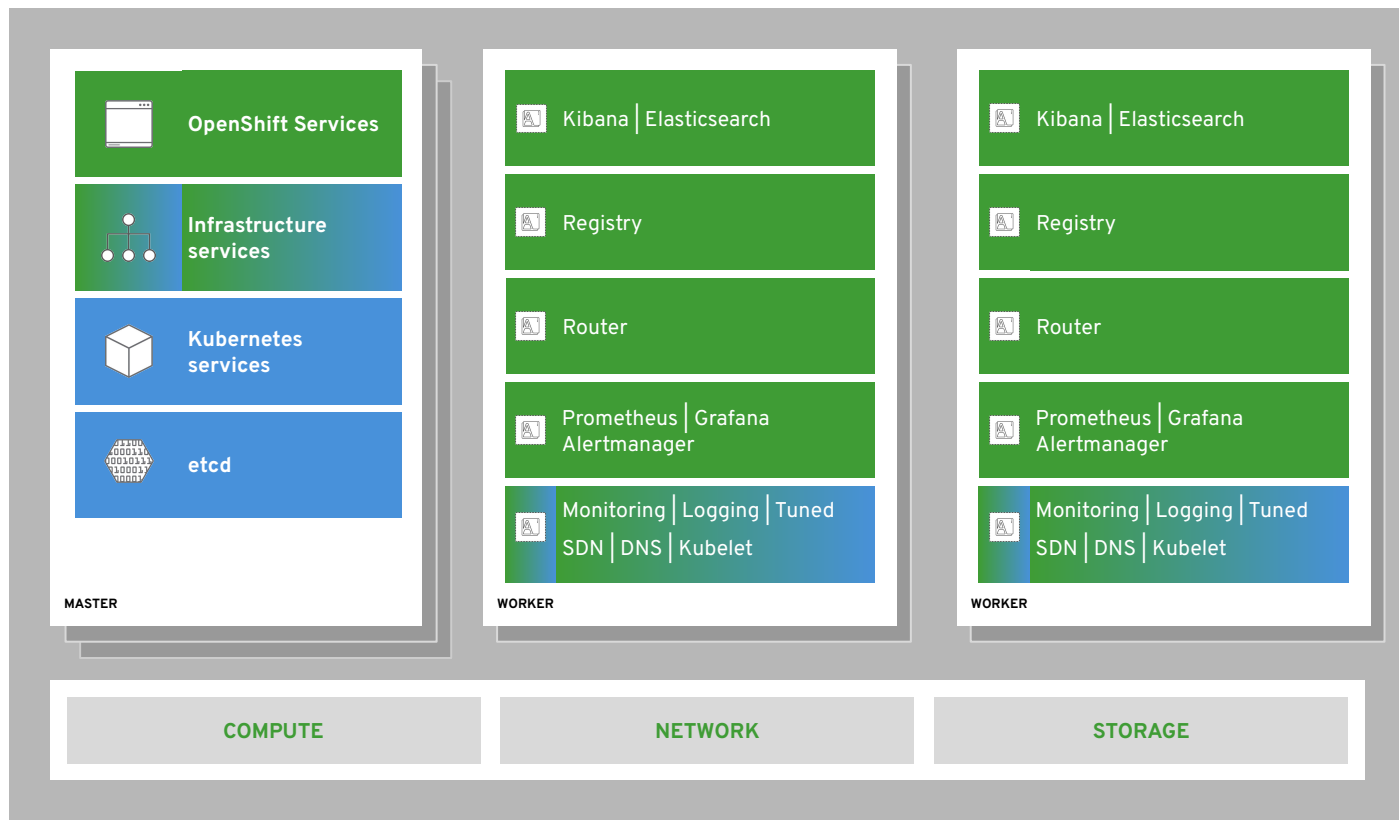
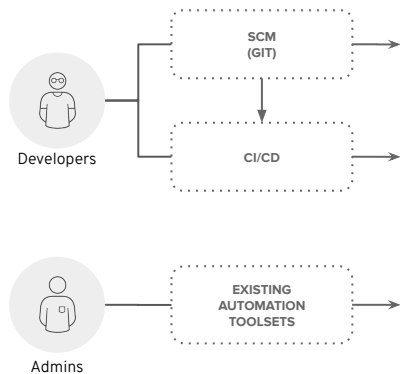
internal and support infrastructure services



integrated routing



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



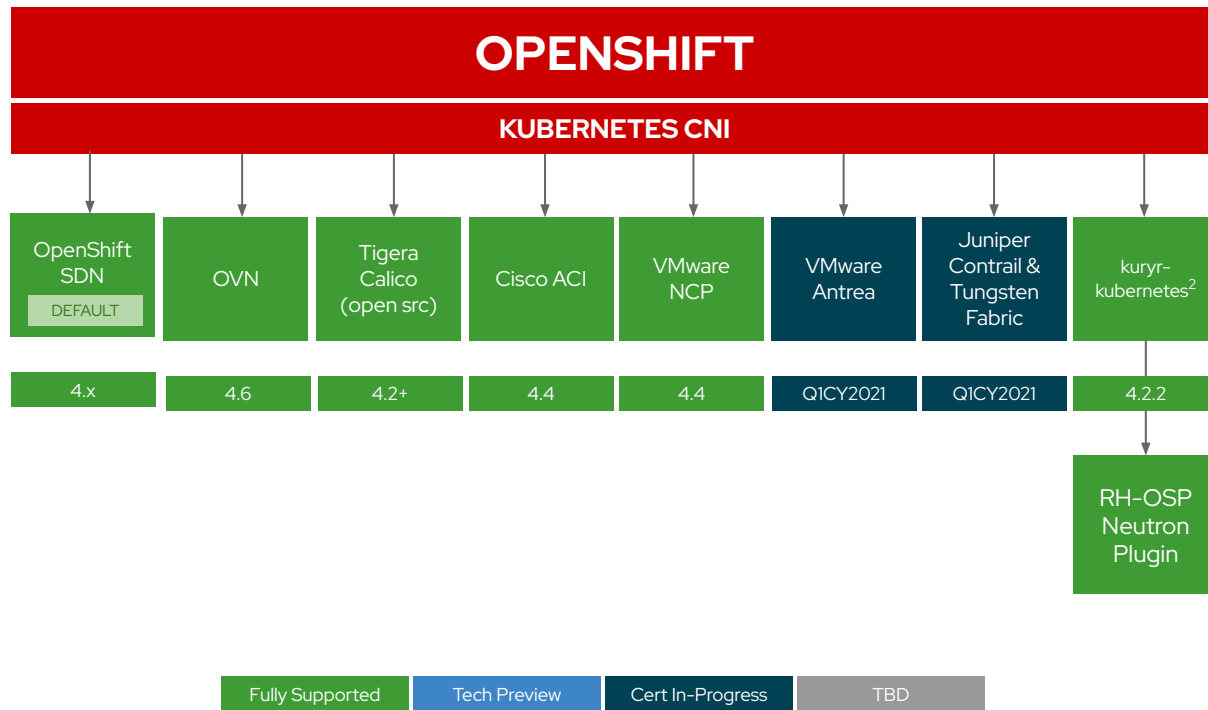
Networking

A pluggable model for
network interface
controls in kubernetes

OpenShift Networking Plug-ins

3rd-party Kubernetes CNI plug-in certification primarily consists of:

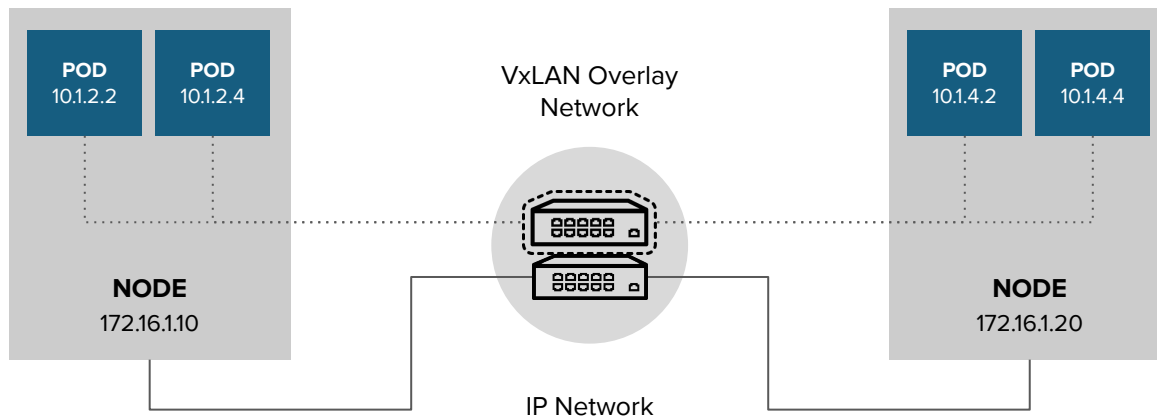
1. Formalizing the partnership
2. Certifying the container(s)
3. Certifying the Operator
4. Successfully passing the same Kubernetes networking conformance tests that OpenShift uses to validate its own SDN



OpenShift SDN

An Open
vSwitch-based
Software Defined
Network for
kubernetes

OpenShift SDN high-level architecture



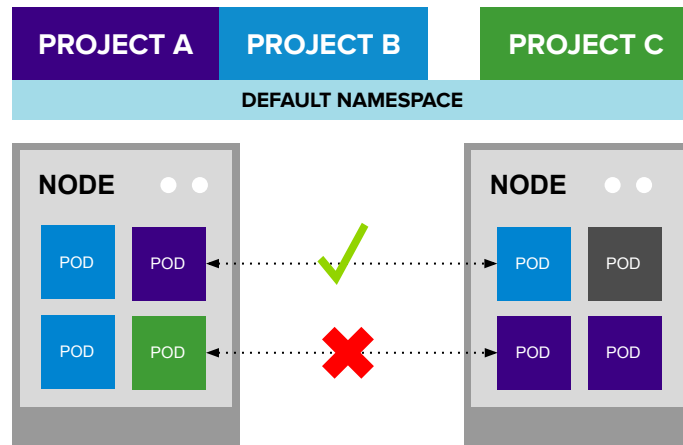
OpenShift SDN “flavors”

OPEN NETWORK (Default)

- All pods can communicate with each other across projects

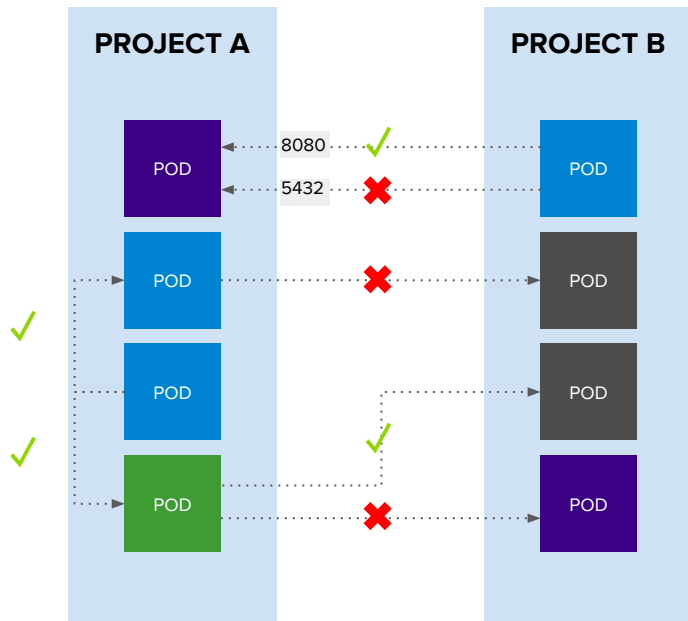
MULTI-TENANT NETWORK

- Project-level network isolation
- Multicast support
- Egress network policies



Multi-Tenant Network

NetworkPolicy



Example Policies

- Allow all traffic inside the project
- Allow traffic from green to gray
- Allow traffic to purple on 8080

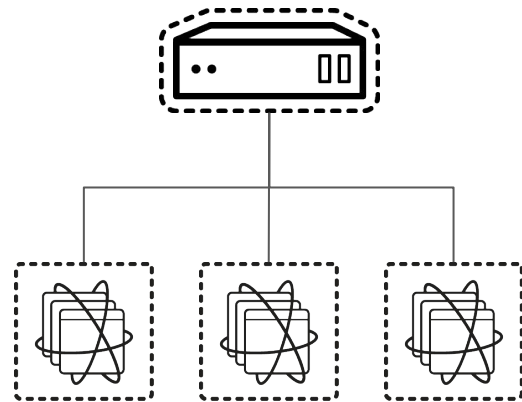
```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
    - ports:
        - protocol: tcp
          port: 8080
```

routes and ingress

How traffic enters the
cluster

Routing and Load Balancing

- Pluggable routing architecture
 - HAProxy Router
 - F5 Router
- Multiple-routers with traffic sharding
- Router supported protocols
 - HTTP/HTTPS
 - WebSockets
 - TLS with SNI
- Non-standard ports via cloud load-balancers, external IP, and NodePort

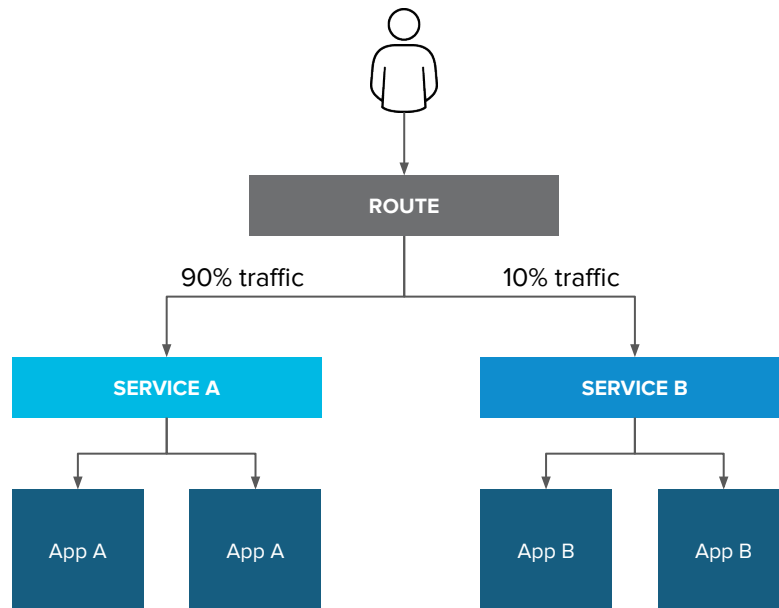


Routes vs Ingress

Feature	Ingress	Route
Standard Kubernetes object	X	
External access to services	X	X
Persistent (sticky) sessions	X	X
Load-balancing strategies (e.g. round robin)	X	X
Rate-limit and throttling	X	X
IP whitelisting	X	X
TLS edge termination	X	X
TLS re-encryption	X	X
TLS passthrough	X	X
Multiple weighted backends (split traffic)		X
Generated pattern-based hostnames		X
Wildcard domains		X

Router-based deployment methodologies

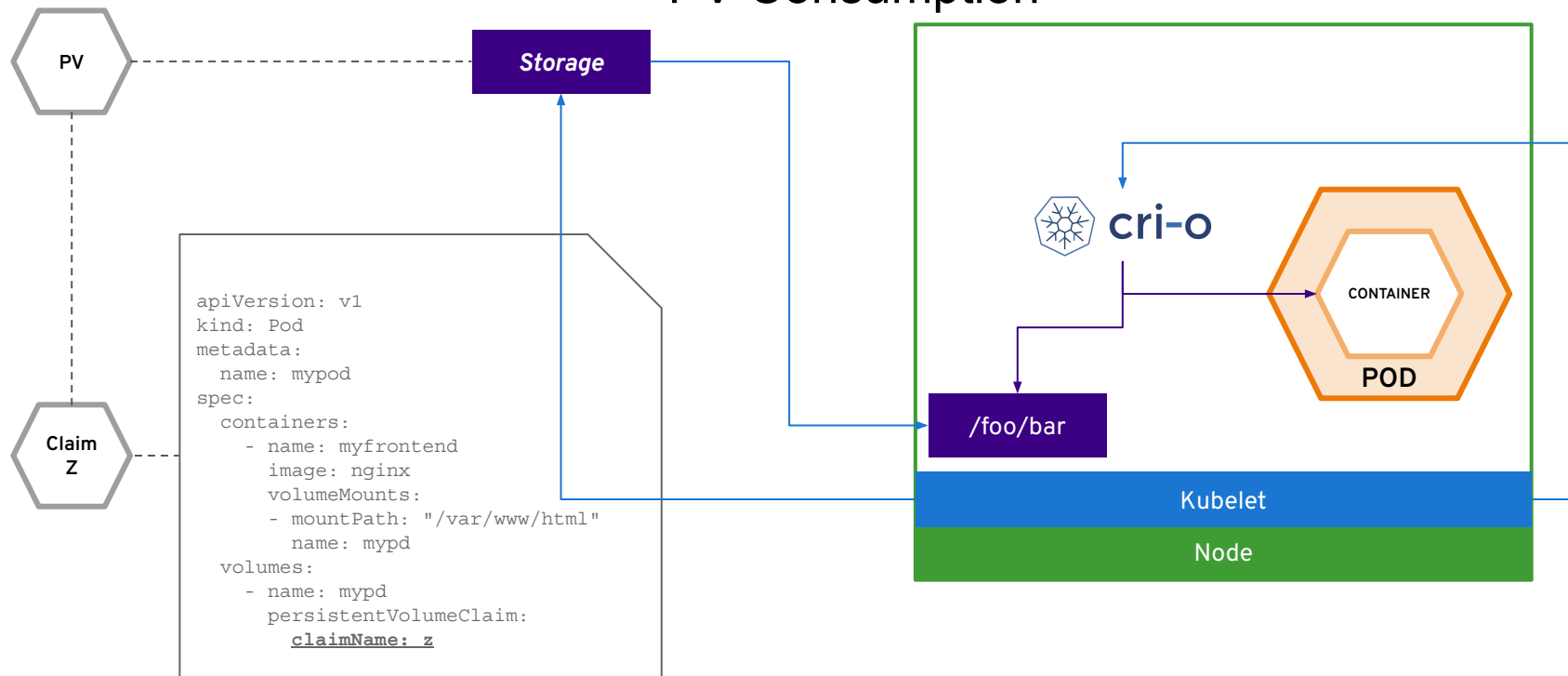
Split Traffic Between
Multiple Services For A/B
Testing, Blue/Green and
Canary Deployments



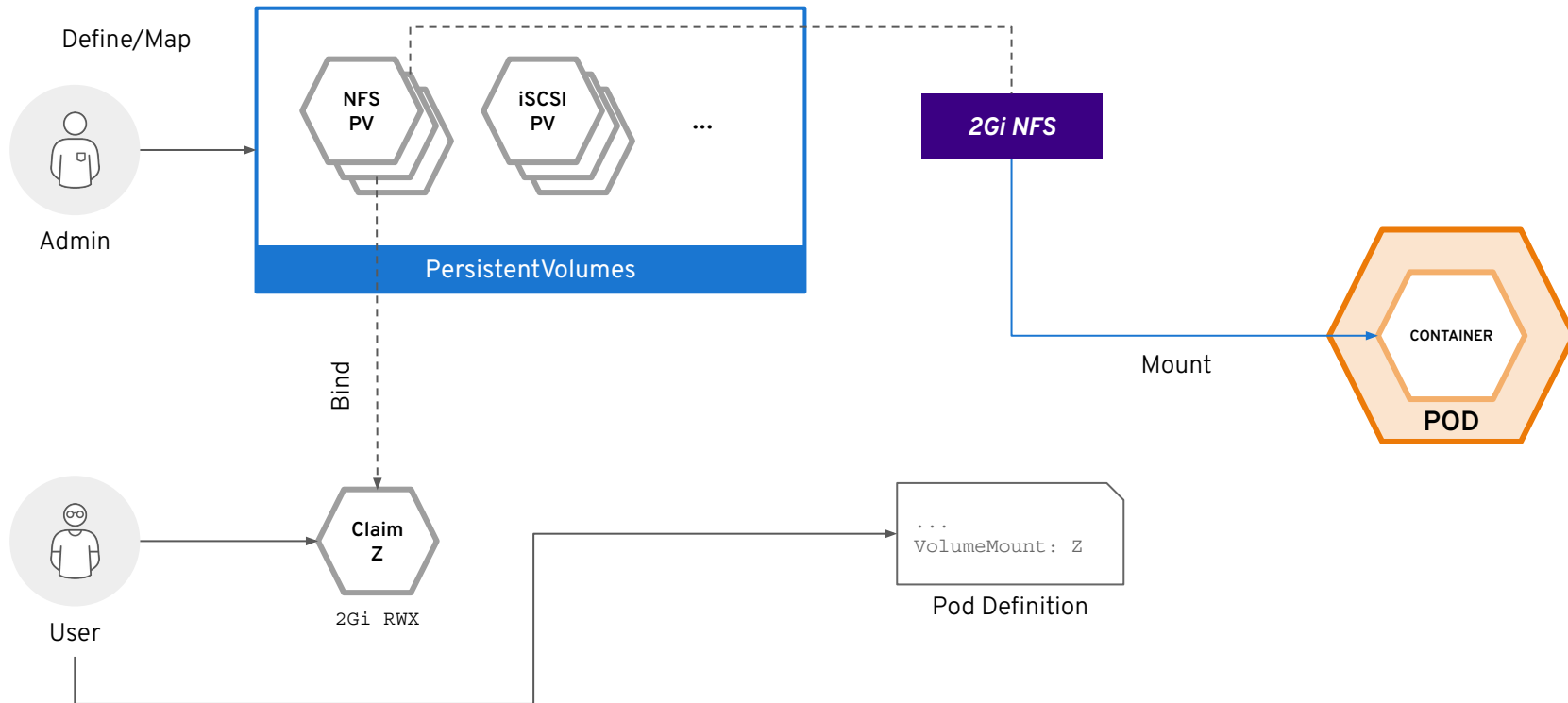
Persistent Storage

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

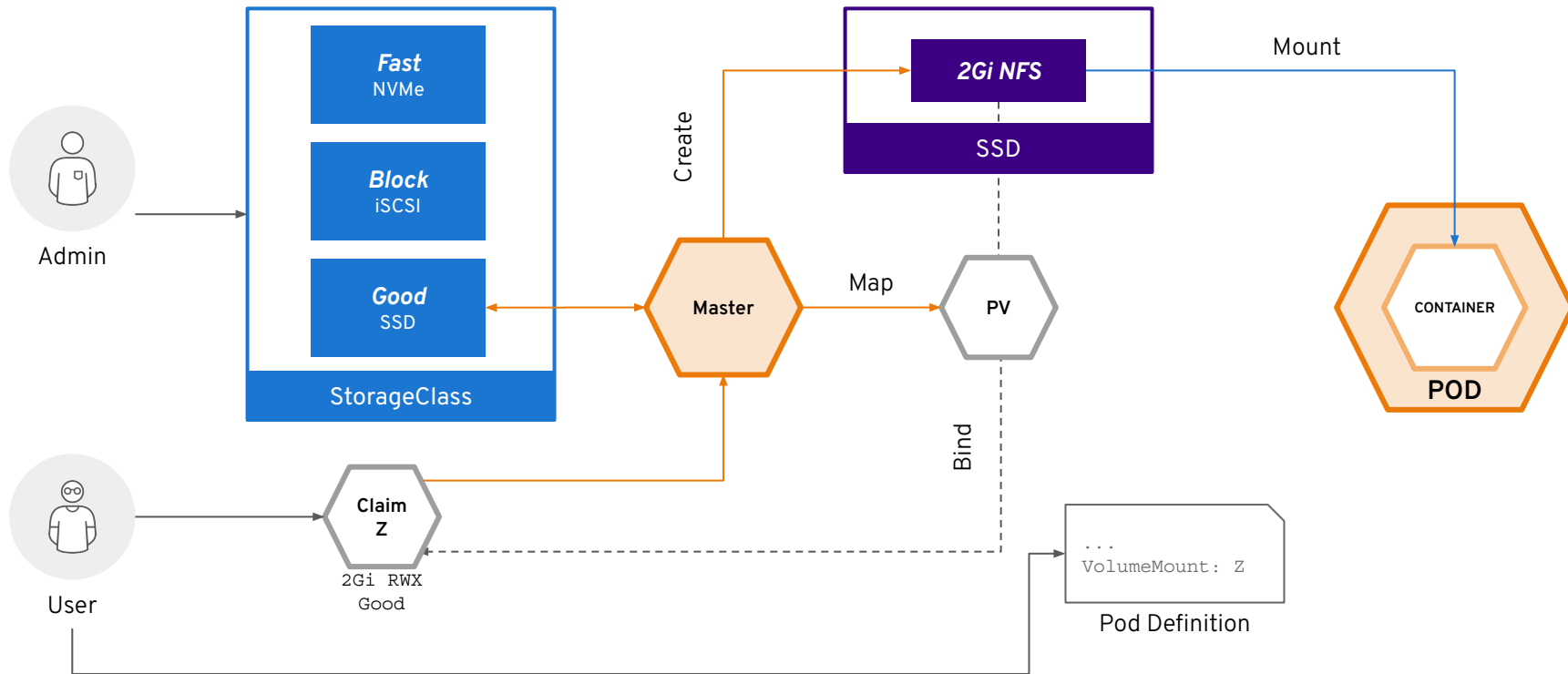
PV Consumption



Static Storage Provisioning



Dynamic Storage Provisioning



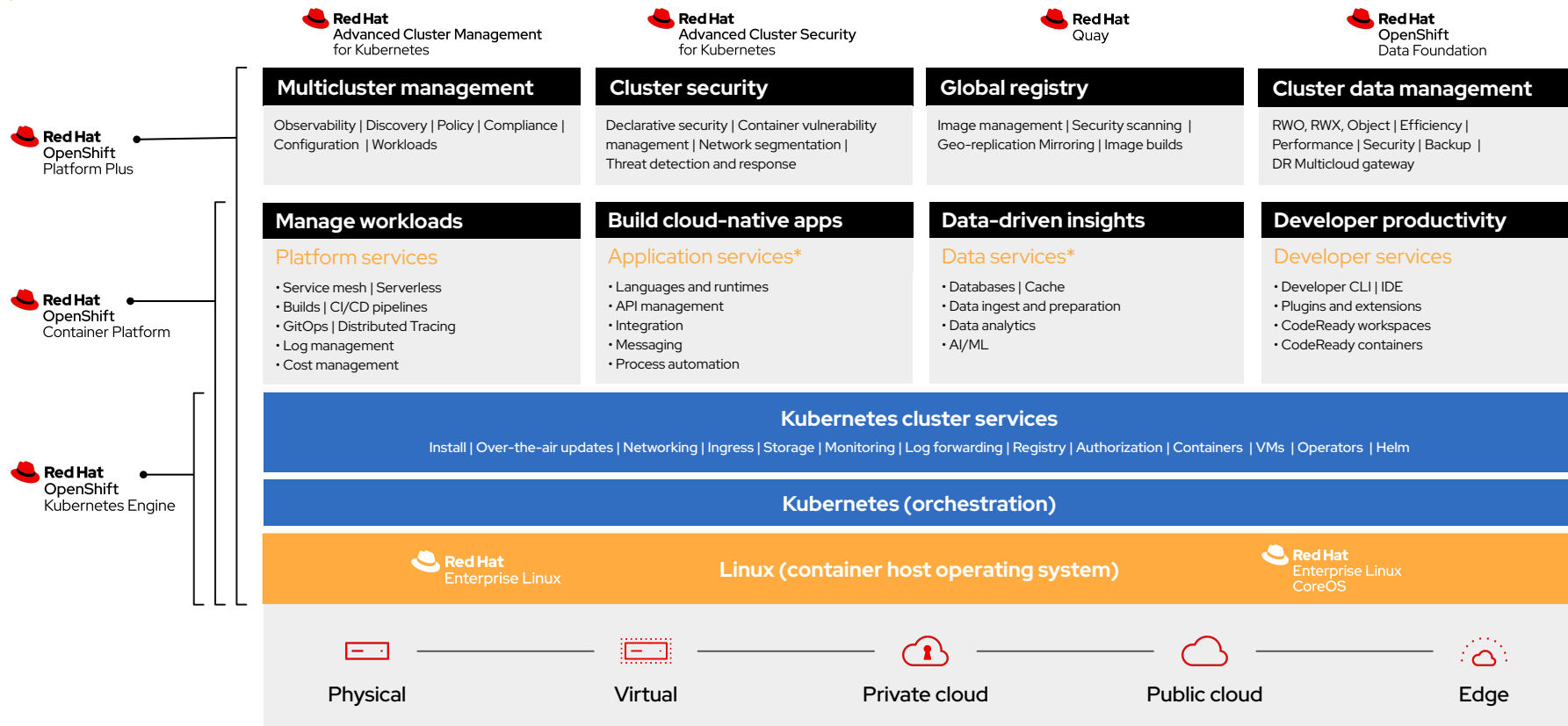


OpenShift Plus

As part of Partner Boot Camp

Alfred Bach
Principal Solution Architect

Red Hat open hybrid cloud platform



* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application Services and Red Hat Data Services portfolios.

** Disaster recovery, volume and multicloud encryption, key management service, and support for multiple clusters and off-cluster workloads requires OpenShift Data Foundation Advanced

Why Red Hat Advanced Cluster Management is important

Why you should care

- ▶ App modernization is a top industry priority.
- ▶ Kubernetes is platform modernization.
- ▶ Enterprises are rapidly adopting Kubernetes.
- ▶ There is intense competition for Kubernetes.
- ▶ Not all Kubernetes solutions are equal.
- ▶ Kubernetes management is complicated.

Key solutions



Move quickly and win the platform



Use the best, most complete
solution - OpenShift



Differentiate and win Red Hat
OpenShift Container Platform



Recognize VMware as the biggest threat



Multicluster lifecycle management



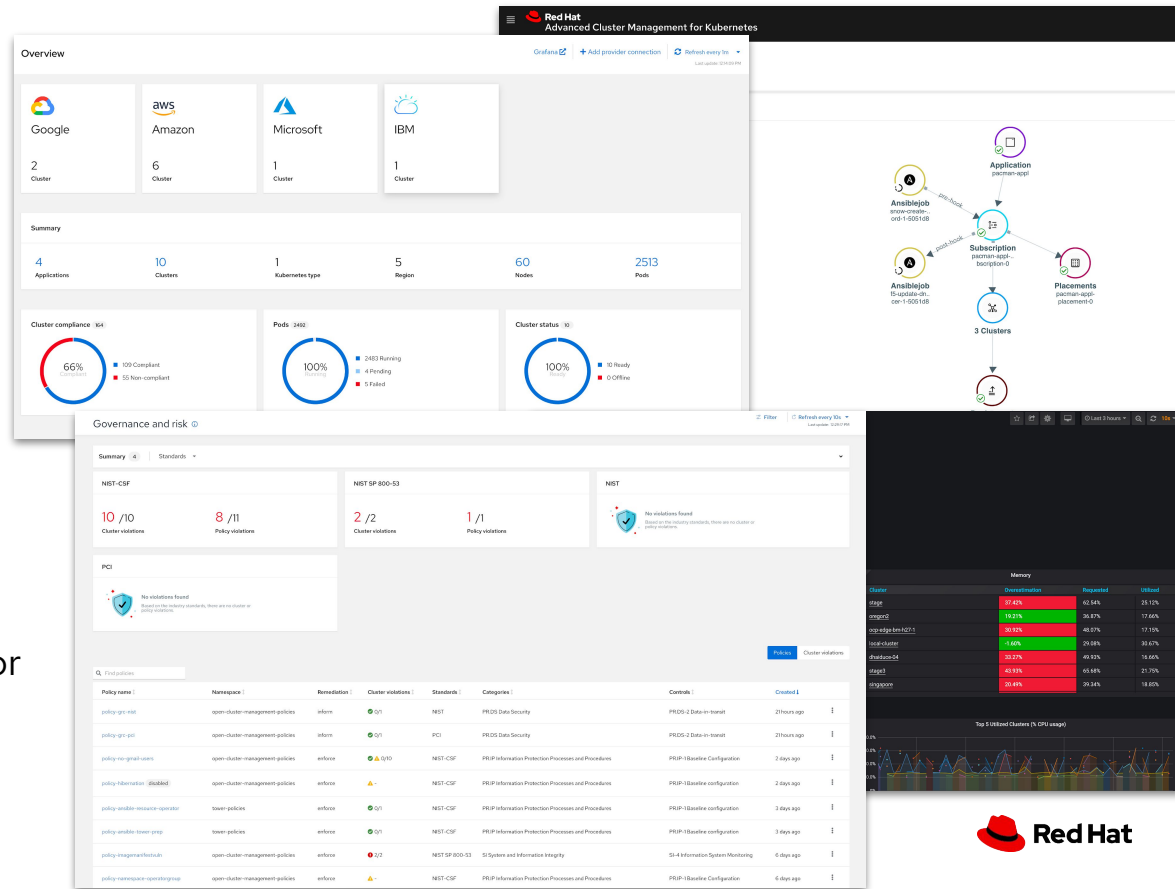
Policy driven governance, risk, and compliance



Advanced application lifecycle management



Multicluster observability for health and optimization



Red Hat Advanced Cluster Security for Kubernetes

A cloud workload protection platform and cloud security posture management to enable you to “shift left”

Shift left

Secure supply chain

Extend scanning and compliance into development (DevSecOps)

Cloud security posture management (CSPM)

Secure infrastructure

Leverage built-in Kubernetes CSPM to identify and remediate risky configurations

Cloud workload protection (CWPP)

Secure workloads

Maintain and enforce a “zero-trust execution” approach to workload protection

Red Hat OpenShift provides a secure foundation



Detect

Trusted content

Container registry

Build management

CI/CD pipeline



Protect

Kubernetes platform lifecycle

Identity and access management

Platform data

Deployment policies



Respond

Container isolation

Network isolation

Application access and data

Observability

Build

Deploy

Run

DevSecOps

A layered approach to container and Kubernetes security

RHACS delivers security depth to entire application lifecycle

Detect

Trusted content
Container registry
Build management
CI/CD pipeline

Protect

Kubernetes platform lifecycle
Identity and access management
Platform data
Deployment policies

Respond

Container isolation
Network isolation
Application access and data
Observability



Vulnerability analysis

App config analysis

APIs for CI/CD integrations

Image assurance and policy
admission controller

Compliance assessments

Risk profiling

Runtime behavioral analysis

Auto-suggest network policies

Threat detection / incident
response

Build

Deploy

Run

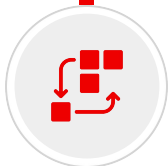
DevSecOps



Industry-leading, **trusted**, and **open source registry platform** operating at scale since 2014



Built to **efficiently manage content** under governance and security **controls** globally



Runs **everywhere**, easy to **integrate** and **automate** but works best with **OpenShift**



Developed in **collaboration** with a broad open source, customer, and ecosystem **community**

Red Hat Quay Key Features

Massive Scale Testing Quay.io
Real Time Garbage Collection
Automated Squashing

SCALABILITY

Seamless Git Integration
Build Workers
Webhooks

BUILD AUTOMATION

Extensible API
Webhooks, OAuth
Robot Accounts

INTEGRATION

REGISTRY

High Availability
Full Standards / Spec Support
Long-Term Protocol Support
Application Registry
Enterprise Grade Support
Regular Updates

SECURITY

Vulnerability Scanning
Logging & Auditing
Notifications & Alerting

CONTENT DISTRIBUTION

Geo-Replication
Repository Mirroring
Air-Gapped Environments

ACCESS CONTROL

Authentication Providers
Fine-Grained RBAC
Organizations & Teams

Red Hat Data Foundation in a nutshell

CONFIDENTIAL designer



Data efficiency

- Erasure coding
- Compression
- Performance



Data resilience

- Snapshots
- Clones
- Backup
- Recovery
- Business continuity
- Disaster recovery



Data security

- At rest encryption
- In flight encryption
- Key management



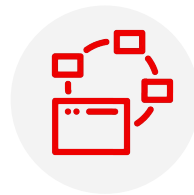
Data governance

- WORM
- Auditing
- Compliance
- SEC & FINRA
- GDPR



Data discovery

- Cataloging
- Tagging
- Search



Traditional, static approach

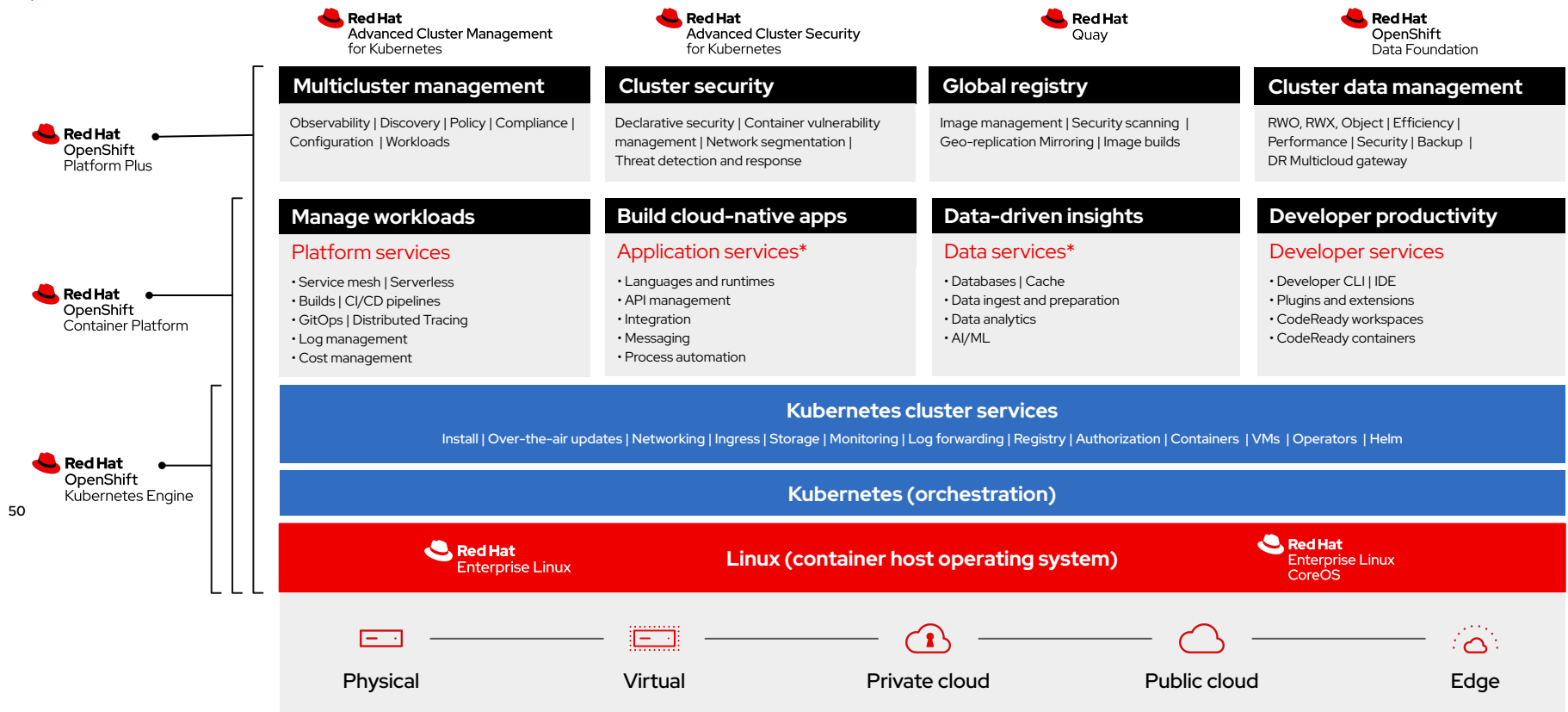
- Focus on improving efficiency
- Infrastructure-up view
- Poor performance at scale
- Disconnected
- Manual, monolithic and rigid

Dynamic, data foundation approach

- Focus on innovation
- Application-oriented view
- Highly scalable
- Always-on
- Automated, on-demand, and flexible

Red Hat open hybrid cloud platform

CONFIDENTIAL designator



* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application Services and Red Hat Data Services portfolios.

** Disaster recovery, volume and multicloud encryption, key management service, and support for multiple clusters and off-cluster workloads requires OpenShift Data Foundation Advanced

V0000000



OpenShift Partner Education Plan

Infrastructure / Architecture

INITIAL

[OpenShift Architecture Workshop](#)

or [OpenShift Infra Arch DLP](#)

or GLS/PTP DO280

ADVANCED

[Hybrid Cloud Architecture Workshop](#) (2-day HC Workshop)

or HybridCloud Hackerton (Q4/23)

or GLS/PTP DO380*

*(not the complete content covered in DO380)

EXPERT (each one Day)

[ACM Workshop](#)

[Storage Foundation Workshop](#)

[Security Workshop \(focus on ACS\)](#)

[Hybrid Cloud NetWorking WS](#)
(Service Mesh, Cilium, Scupper)



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHat