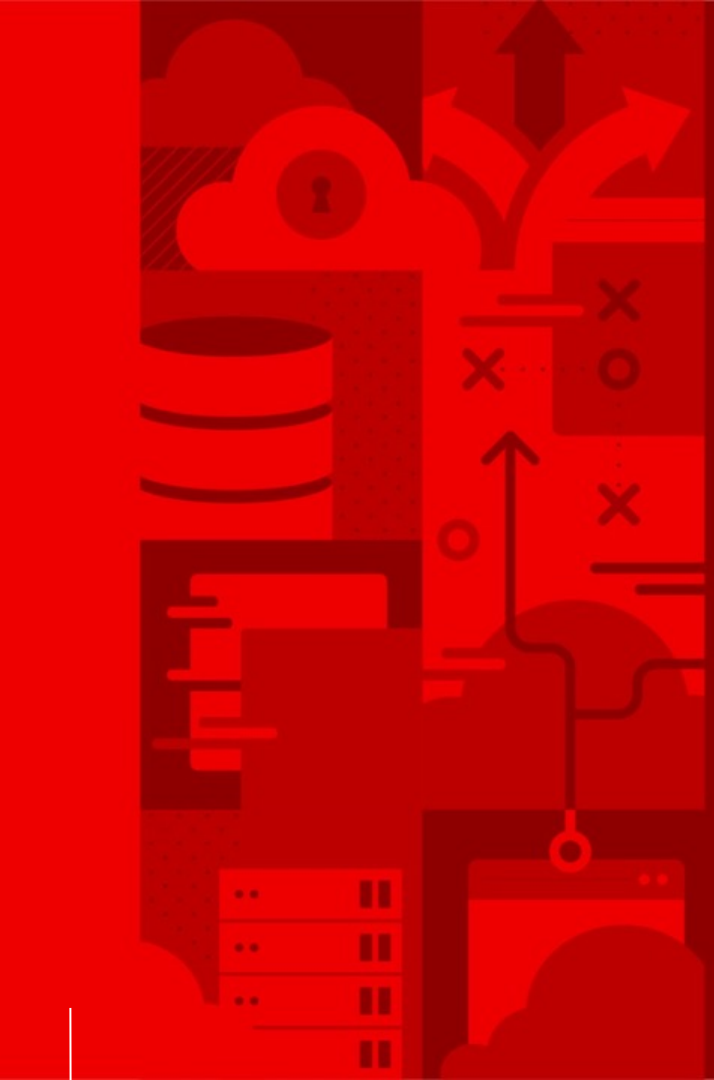


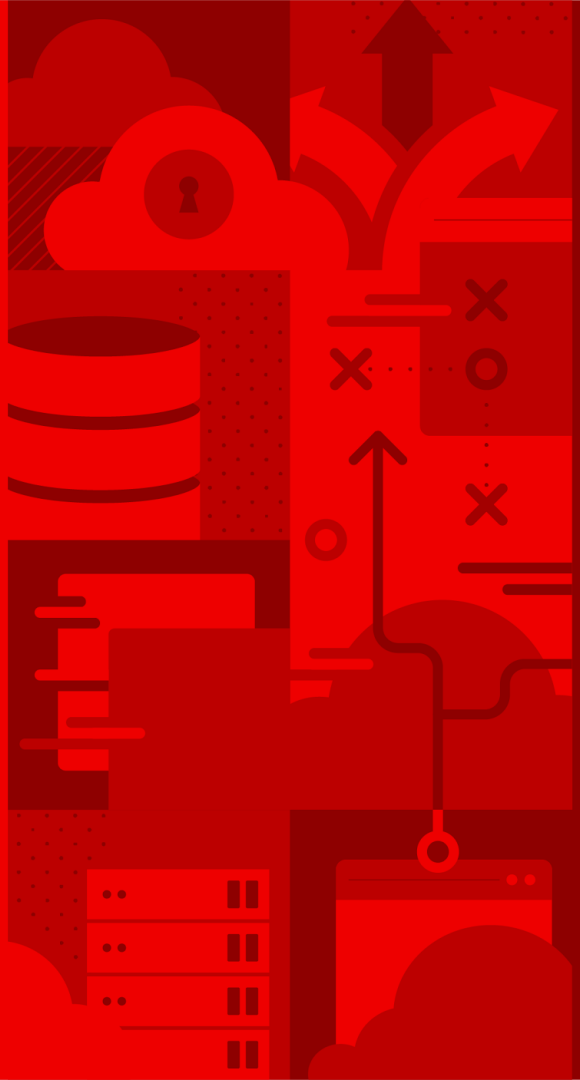
OpenShift Container Platform 4

Emre Özkan
Solution Architect

Red Hat

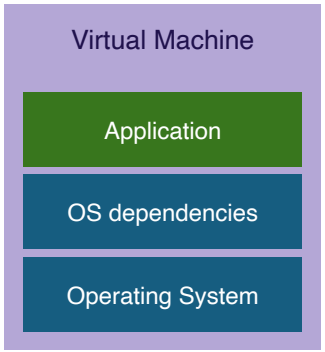
Agenda

- OpenShift and Kubernetes Core Concepts
- OpenShift 4 Architecture
- OpenShift Virtualization
- OpenShift Security
- OpenShift Developer Services

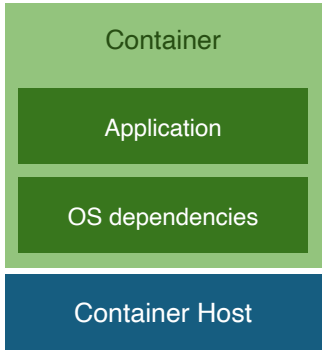


OpenShift and Kubernetes core concepts

VIRTUAL MACHINES AND CONTAINERS



- ✚ VM Isolation
- ▬ Complete OS
- ▬ Static Compute
- ▬ Static Memory
- ▬ High Resource Usage



- ✚ Container Isolation
- ✚ Shared Kernel
- ✚ Burstable Compute
- ✚ Burstable Memory
- ✚ Low Resource Usage

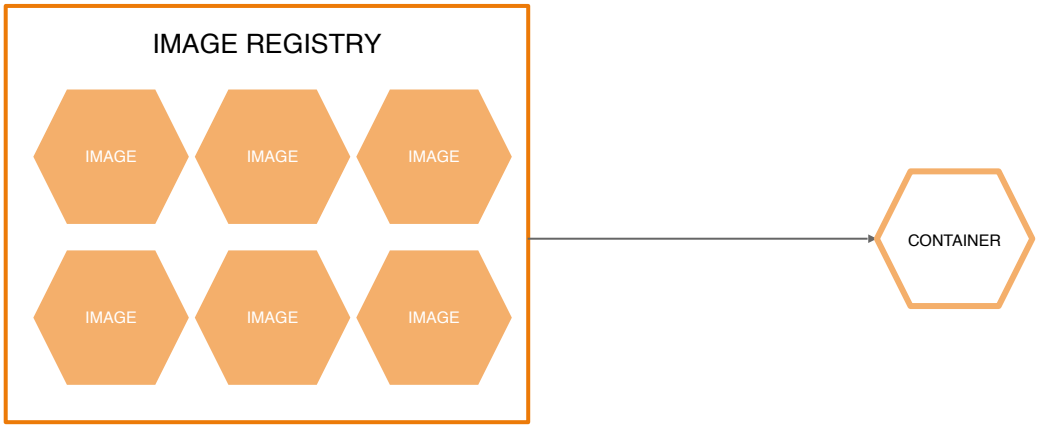
a container is the smallest compute unit

containers are created from container images

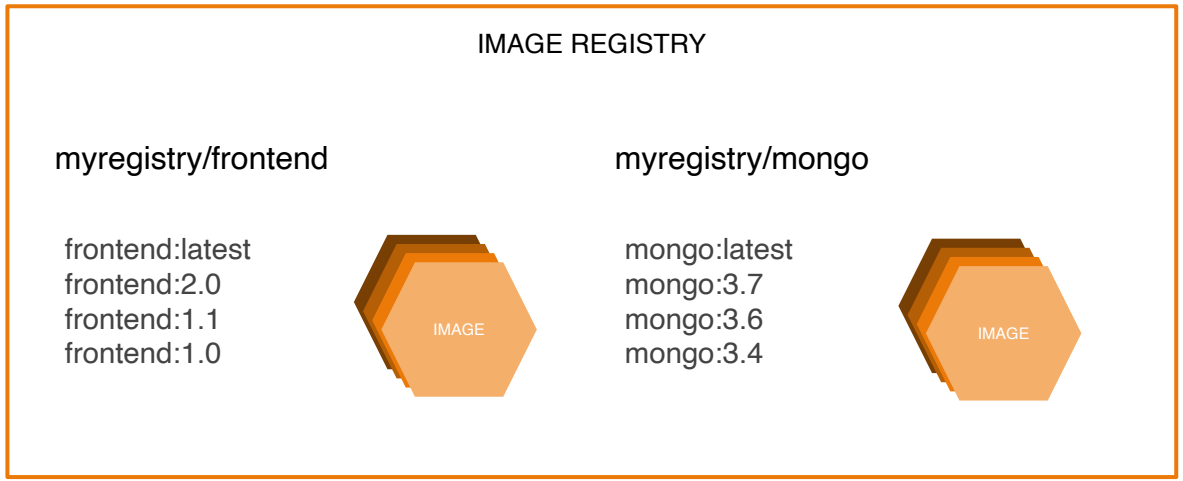
BINARY

RUNTIME

container images are stored in an image registry

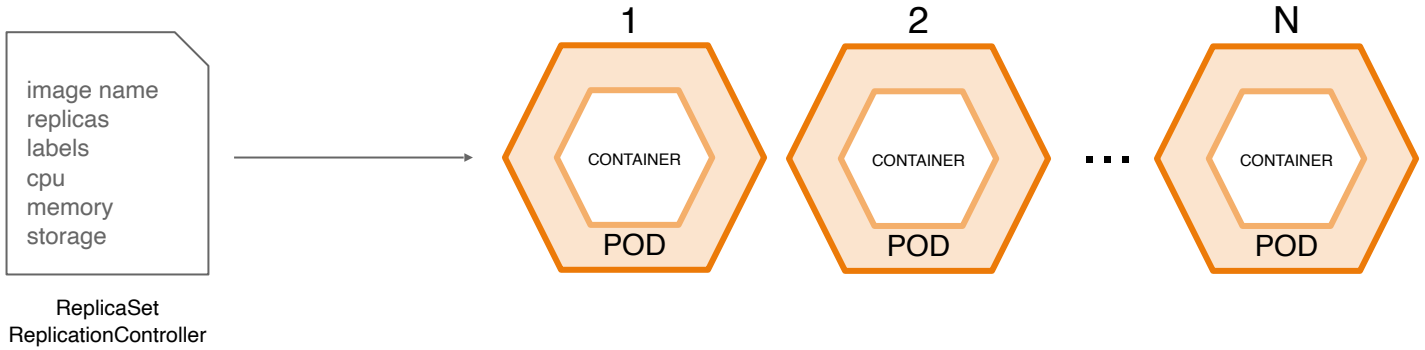


an image repository contains all versions of an image in the image registry

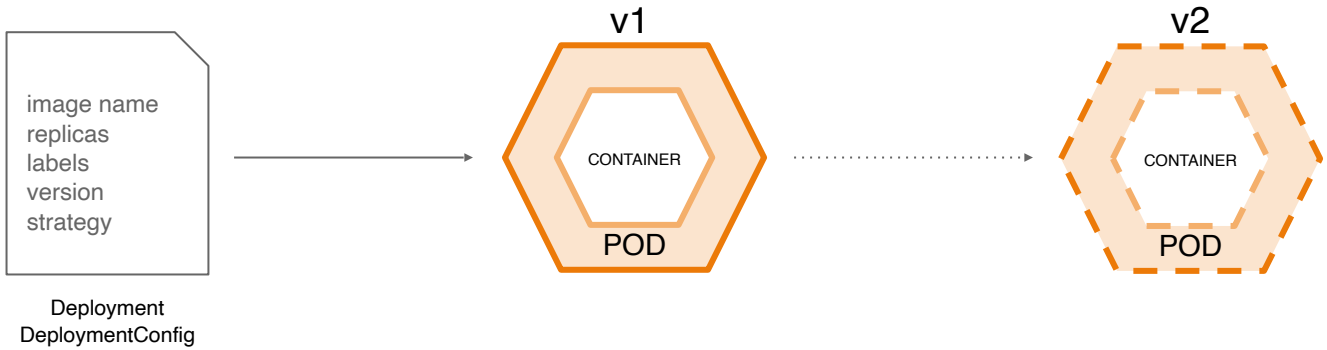


containers are wrapped in pods which are units of deployment and management

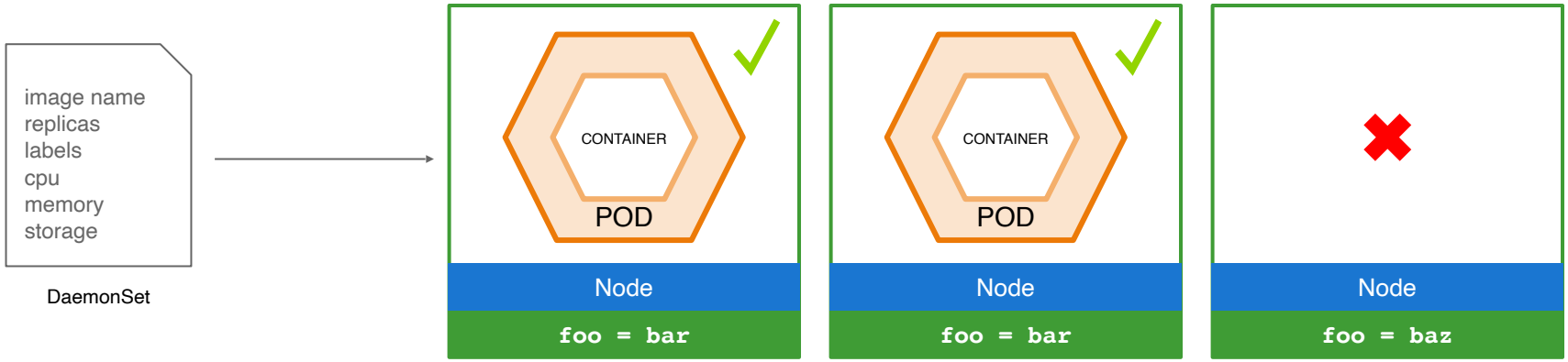
`ReplicationControllers` & `ReplicaSets` ensure a specified number of pods are running at any given time



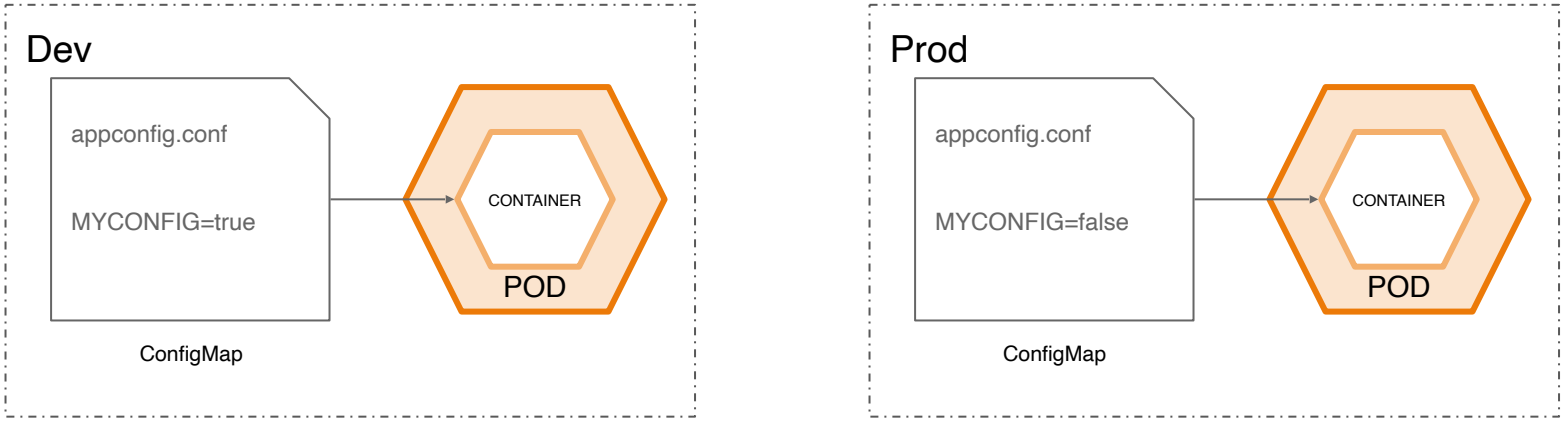
`Deployments` and `DeploymentConfigurations` define how to roll out new versions of Pods



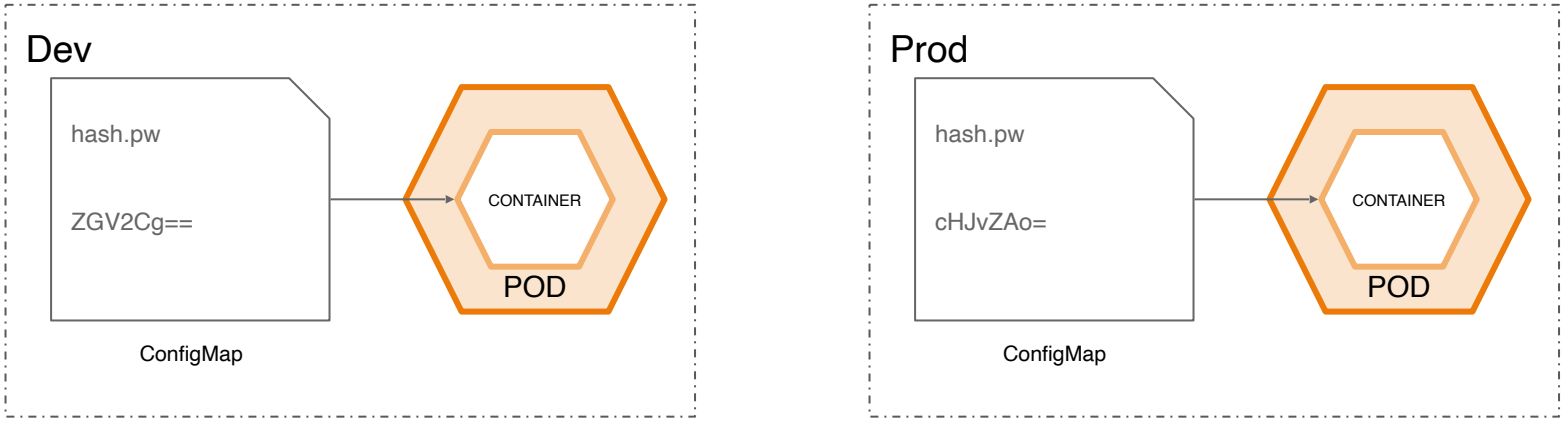
a `daemonset` ensures that all (or some) nodes run a copy of a pod



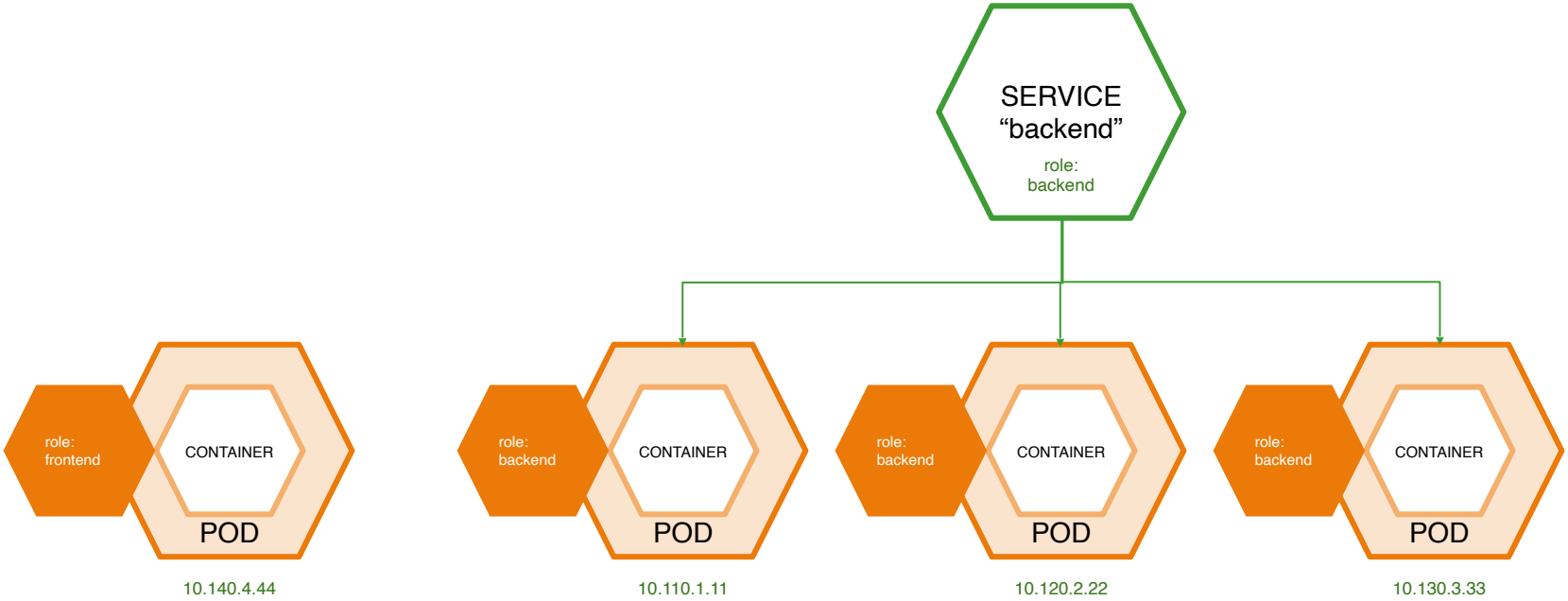
`configmaps` allow you to decouple configuration artifacts from image content



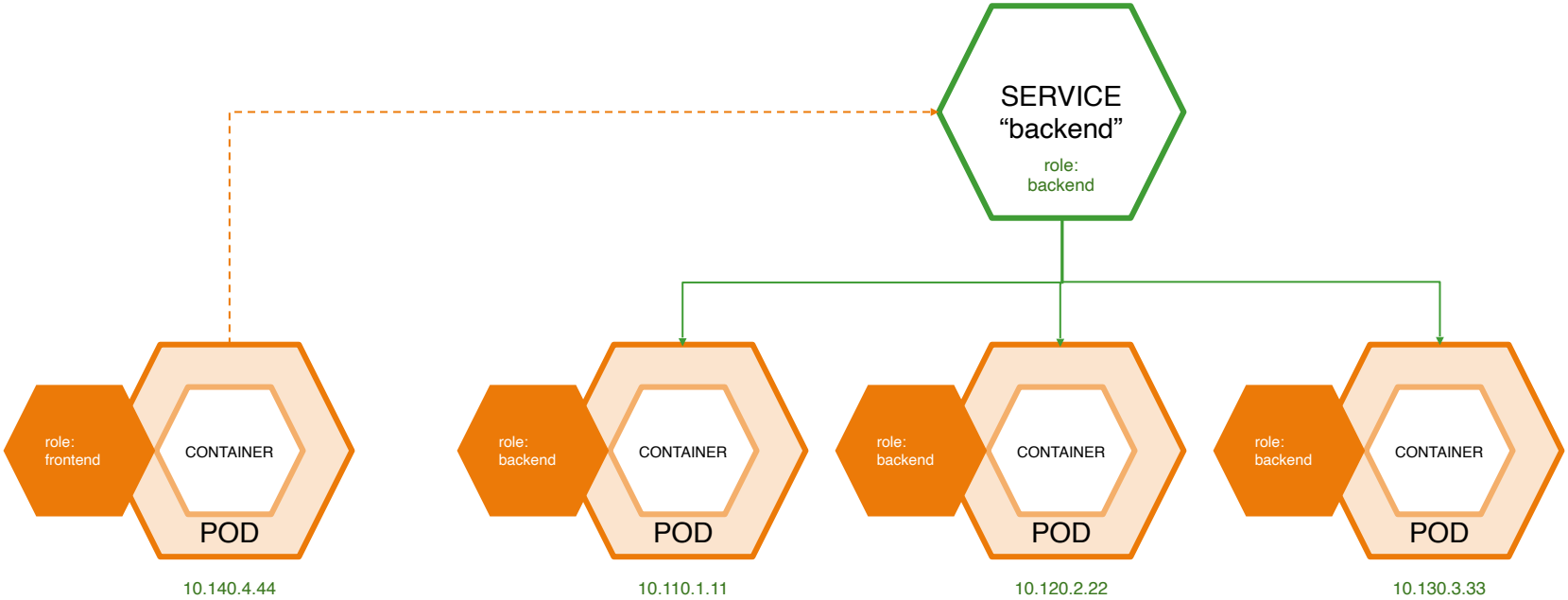
`secrets` provide a mechanism to hold sensitive information such as passwords



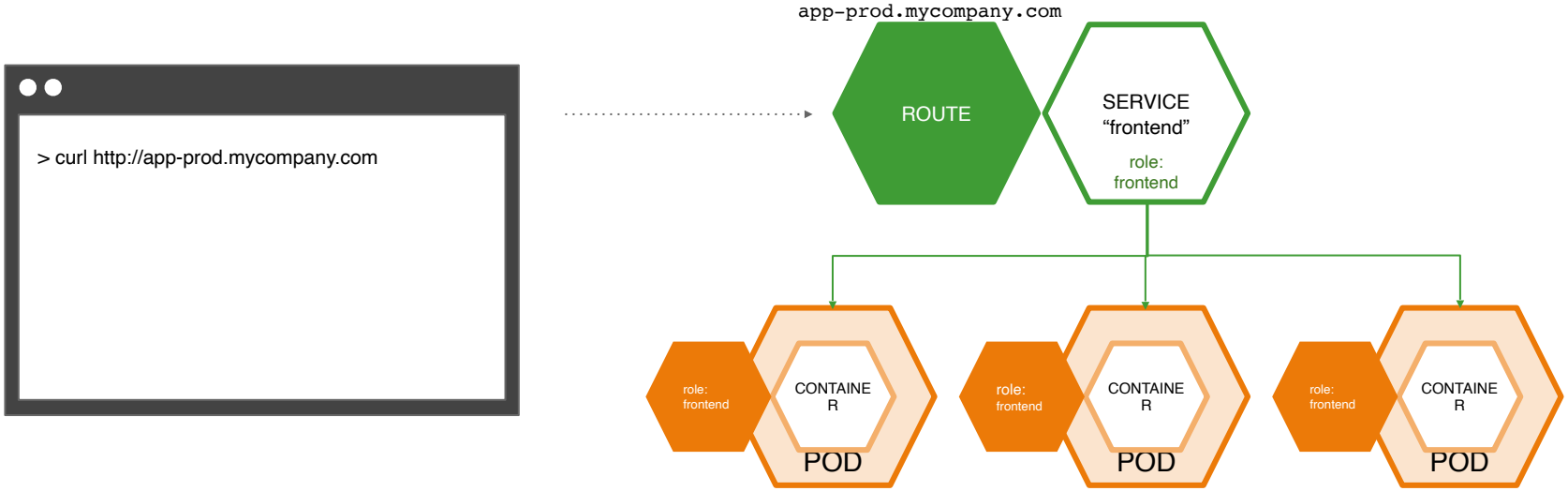
services provide internal load-balancing and service discovery across pods



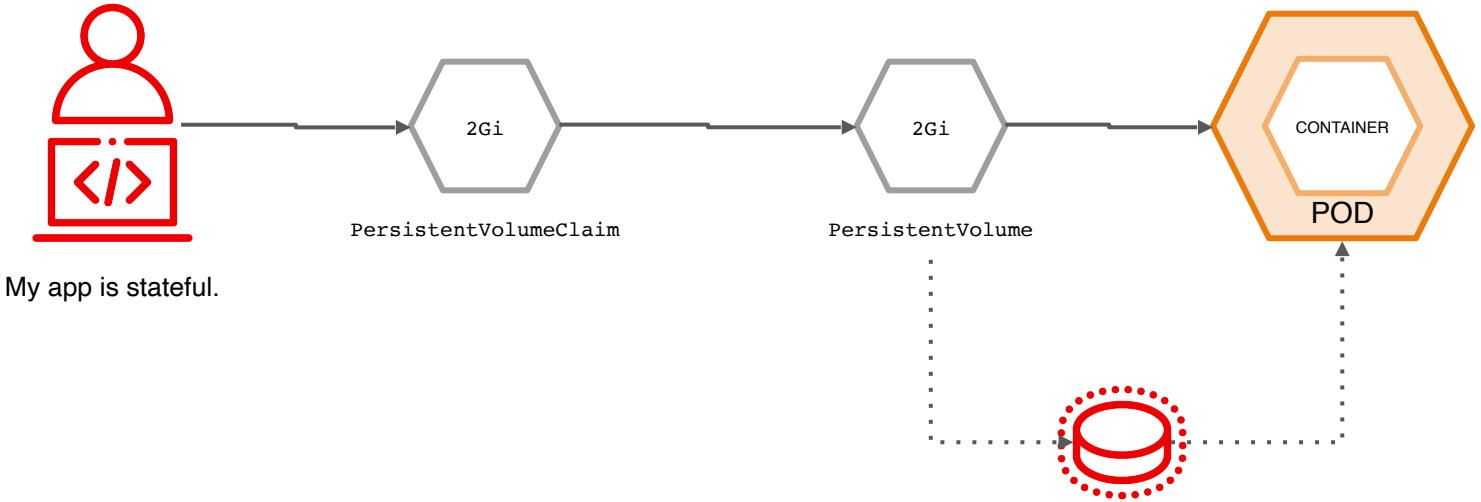
apps can talk to each other via services



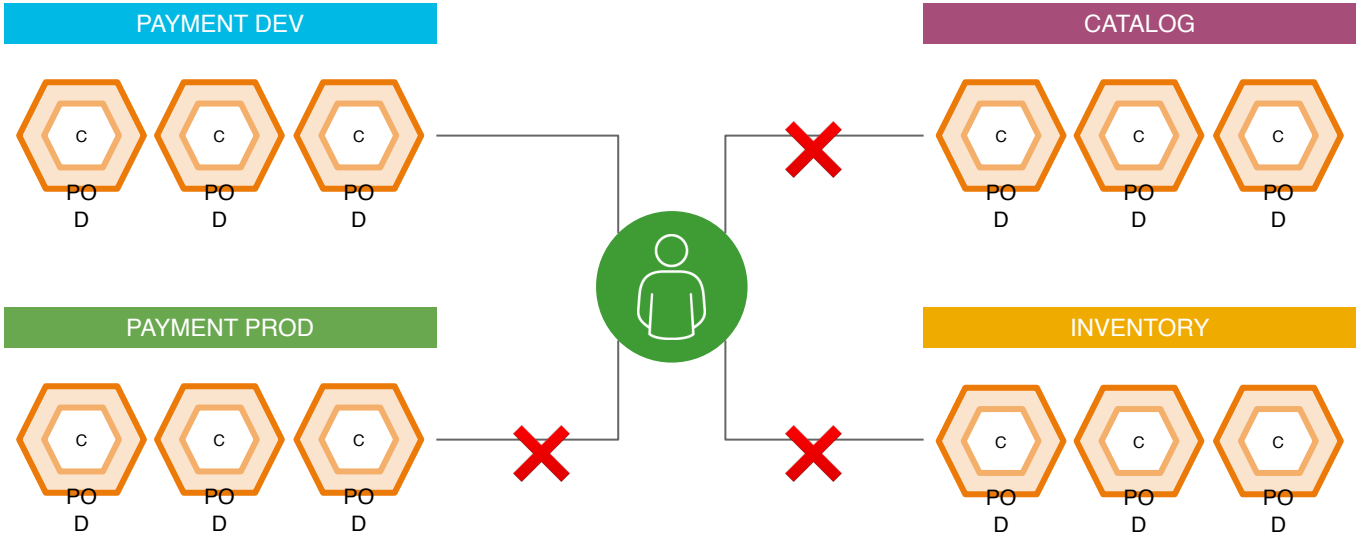
`routes` make services accessible to clients outside the environment via real-world urls



Persistent Volume and Claims

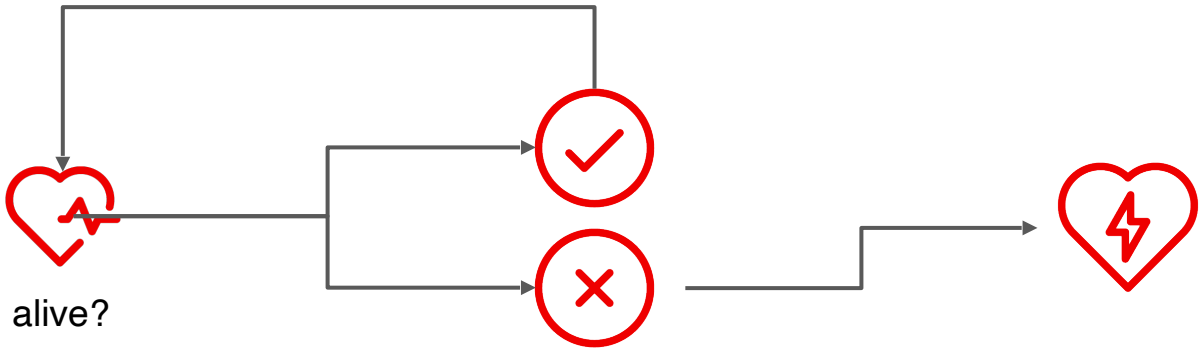


projects isolate apps across environments, teams, groups and departments

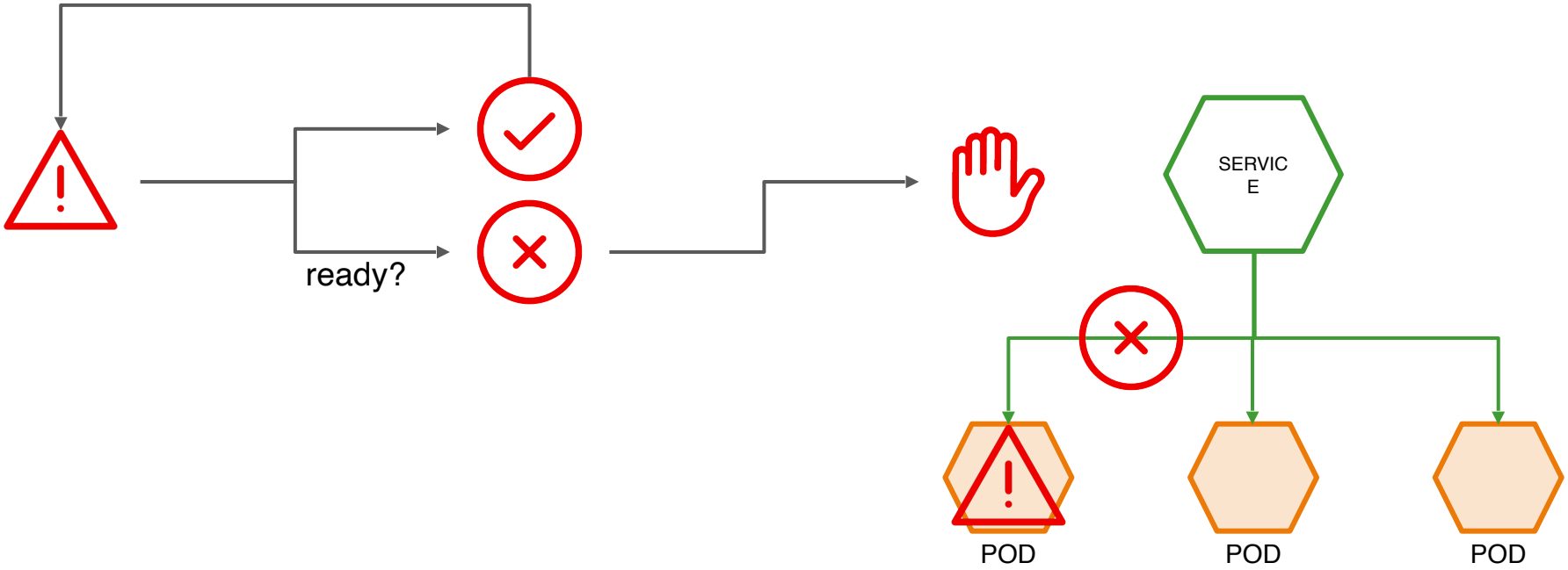


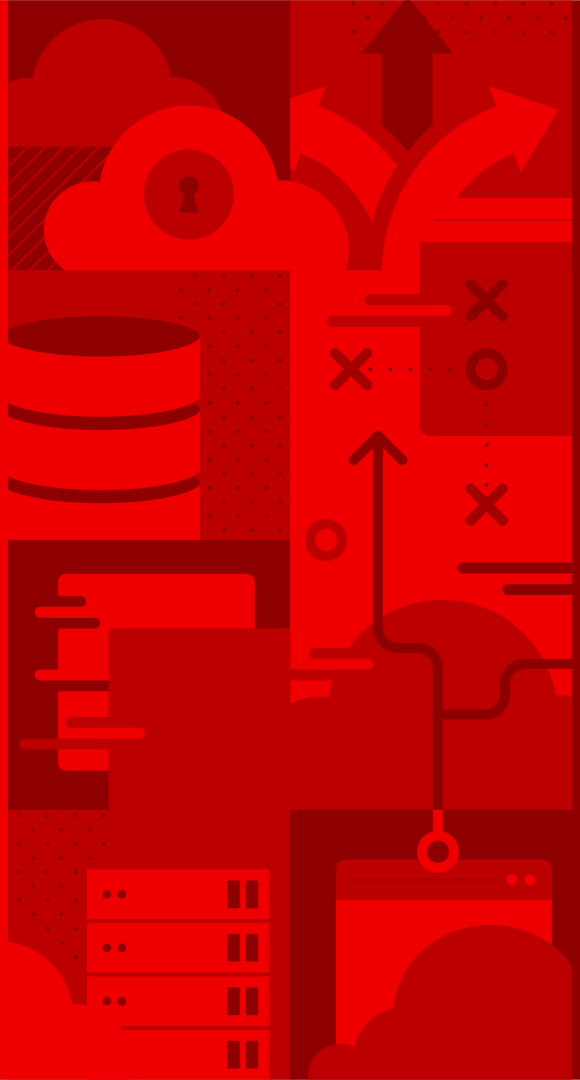
Red Hat

Liveness Probes



Readiness Probes



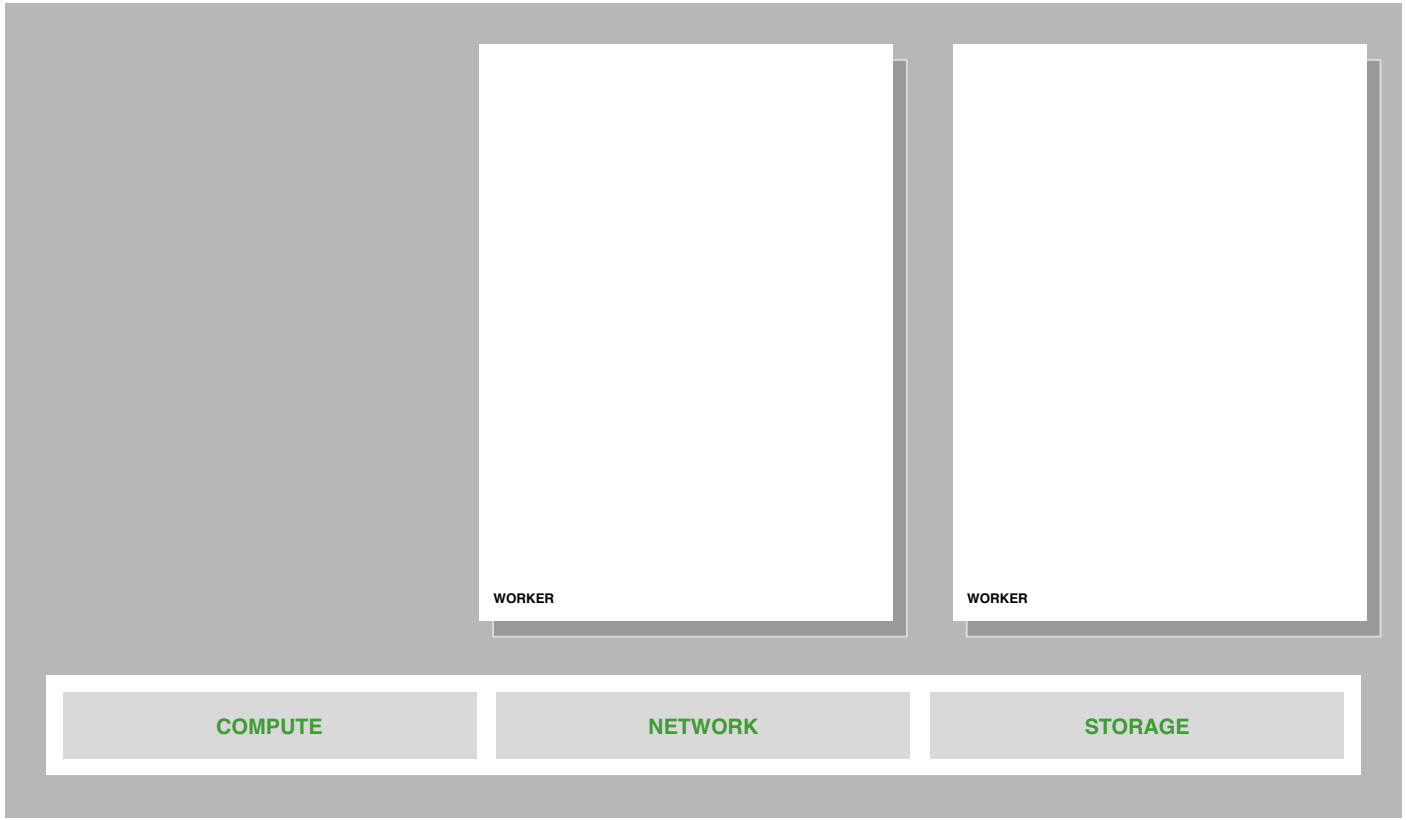


OpenShift 4 Architecture

your choice of infrastructure

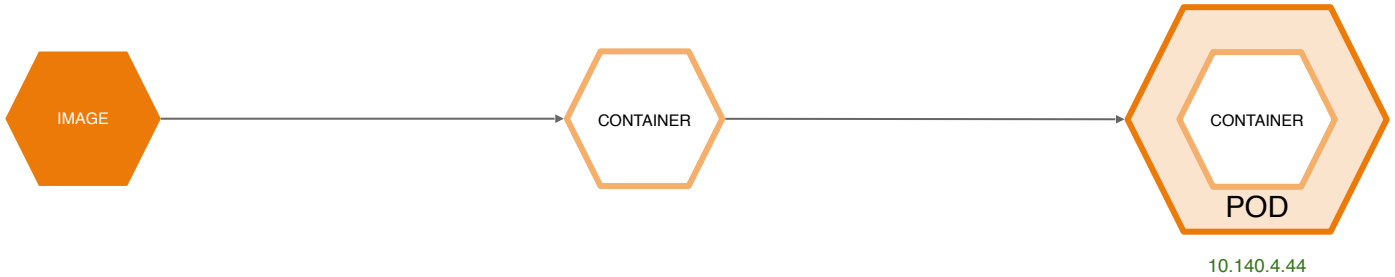
COMPUTE	NETWORK	STORAGE

workers run workloads

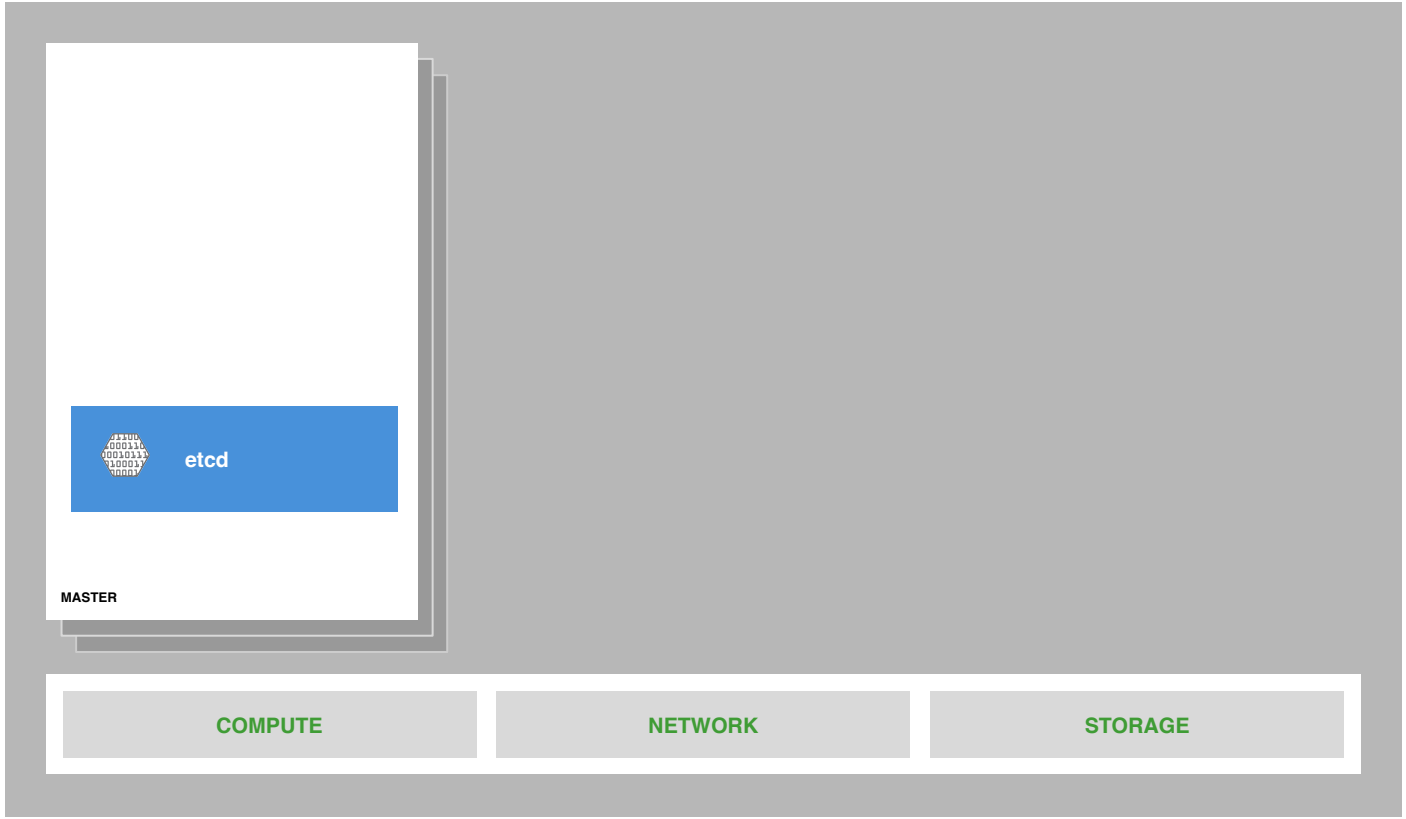


masters are the control plane

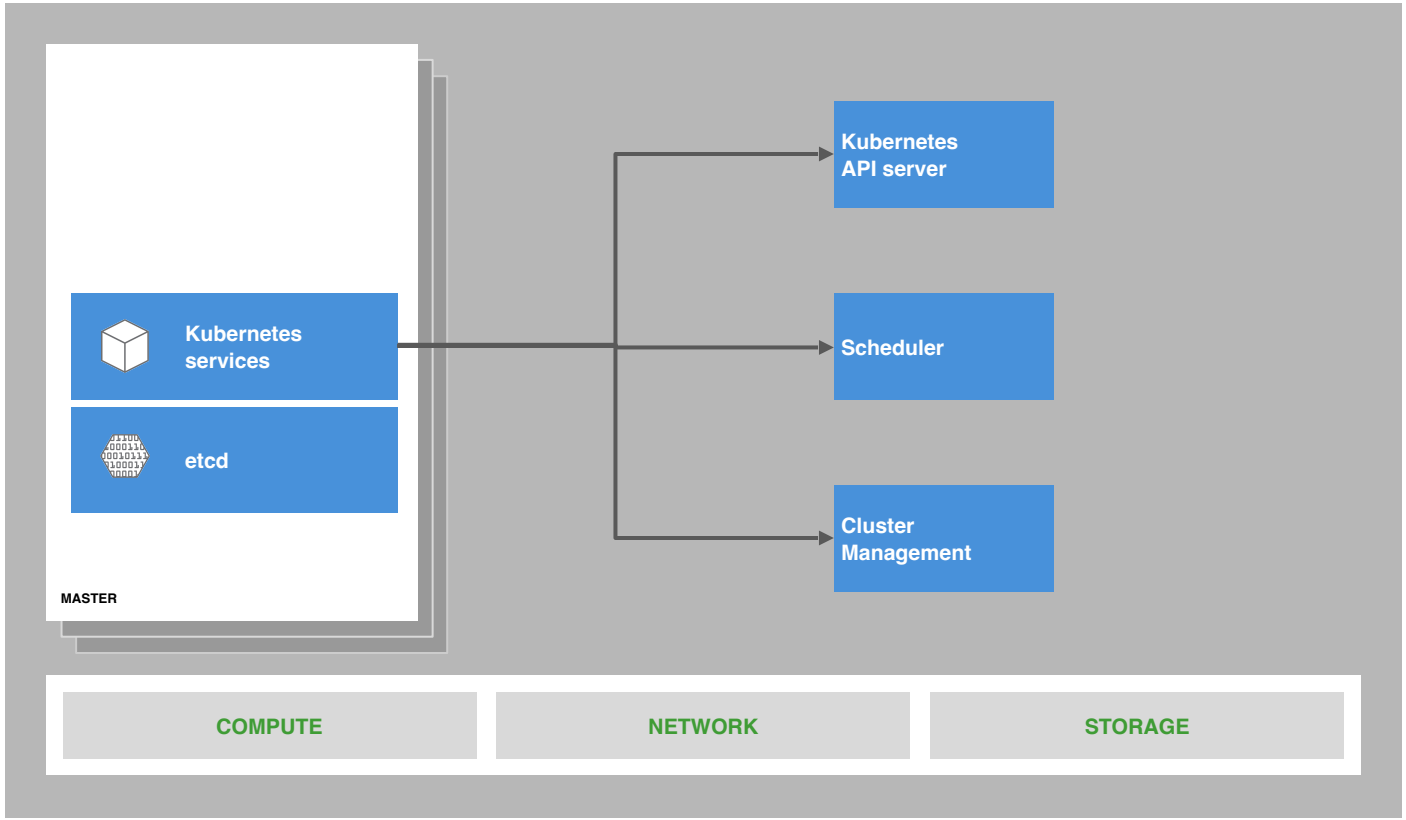
everything runs in pods



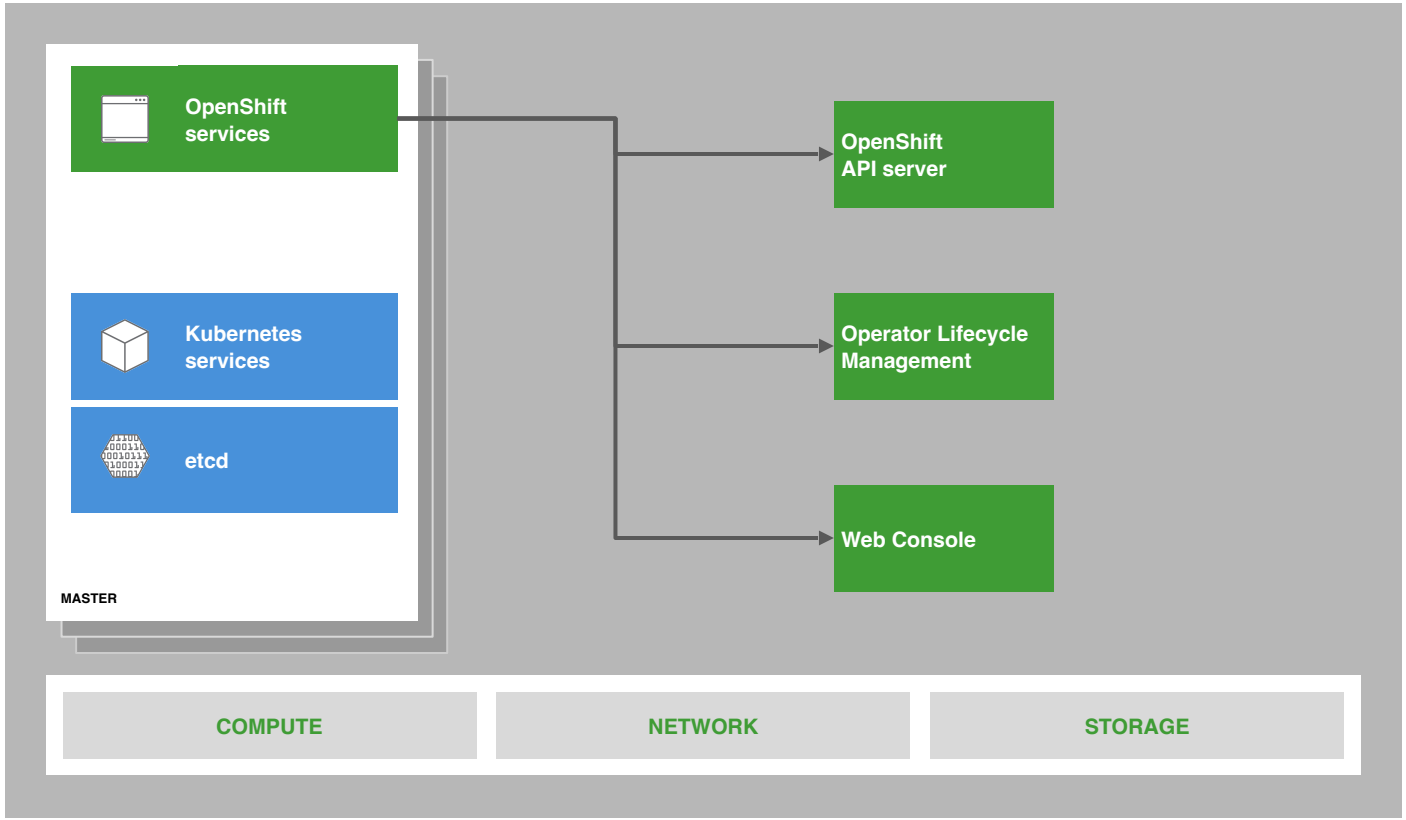
state of everything



core kubernetes components

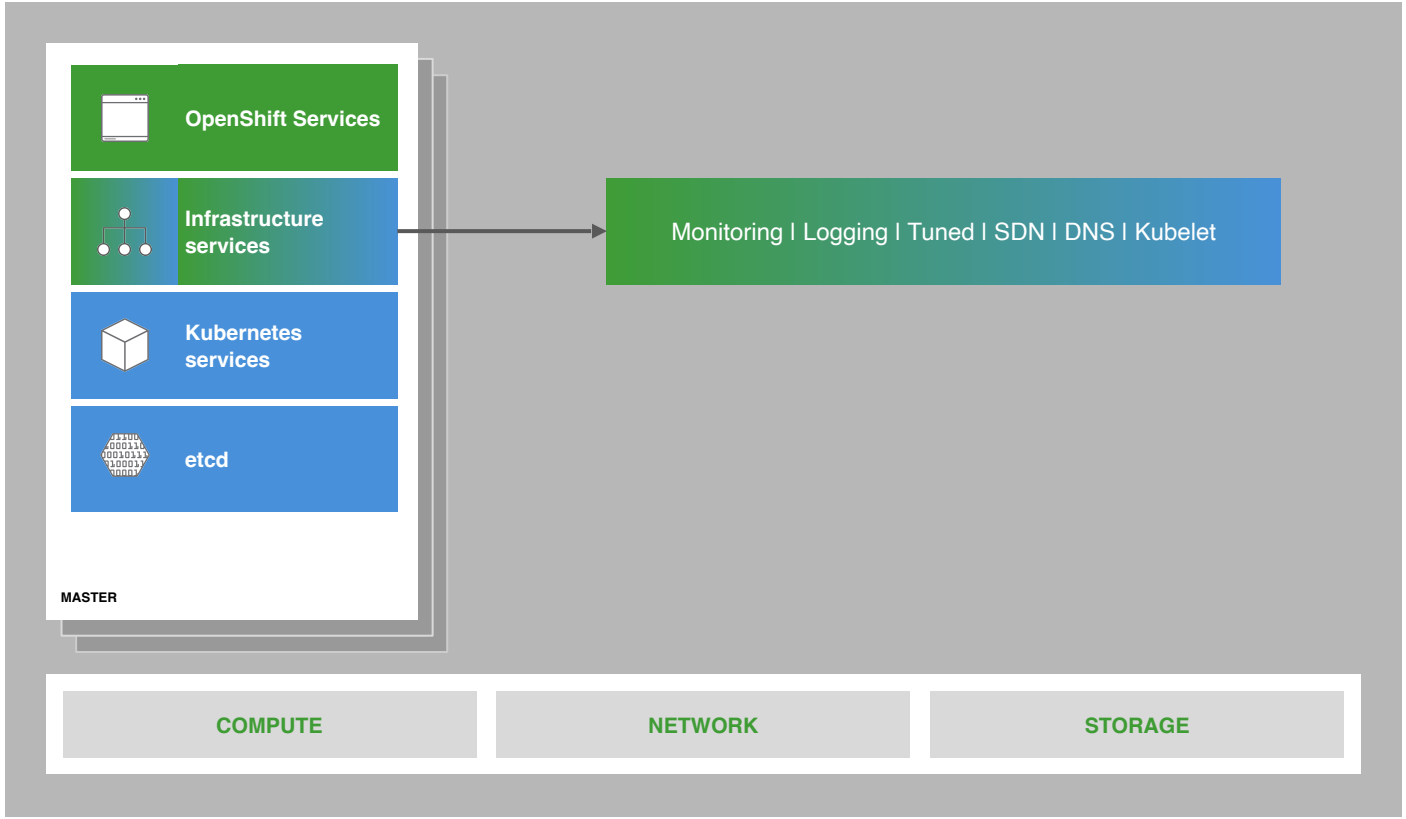


core OpenShift components

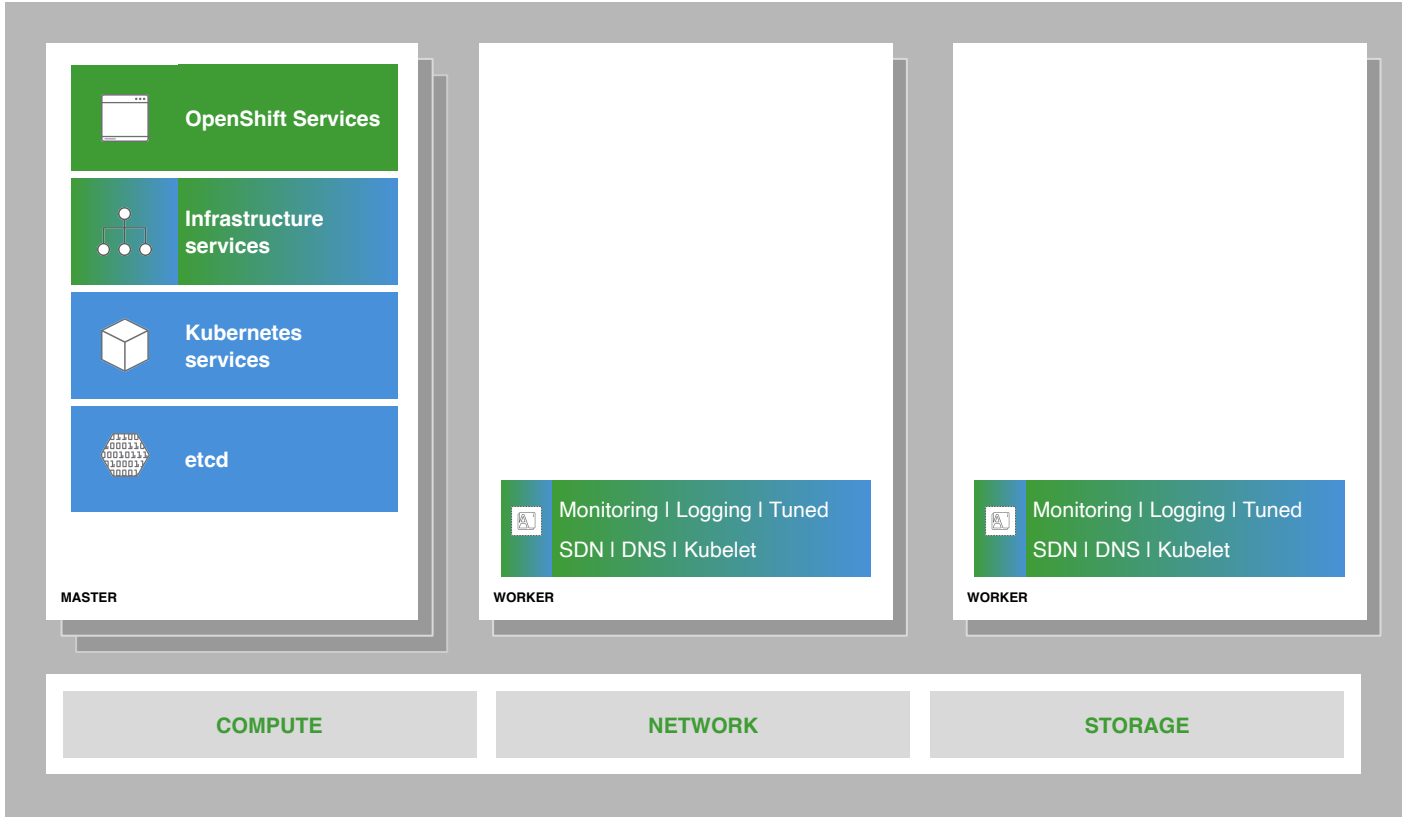


Red Hat

internal and support infrastructure services

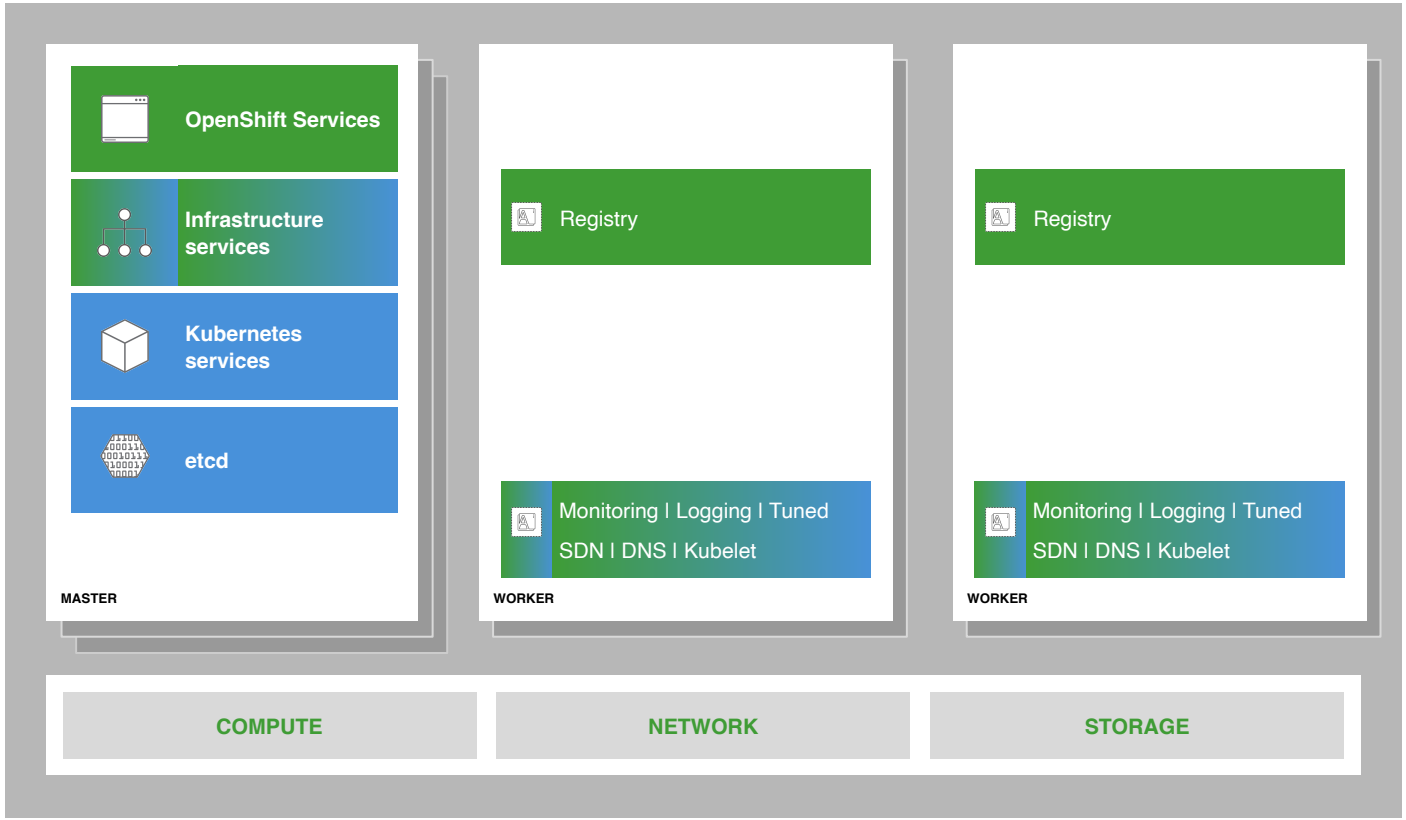


run on all hosts



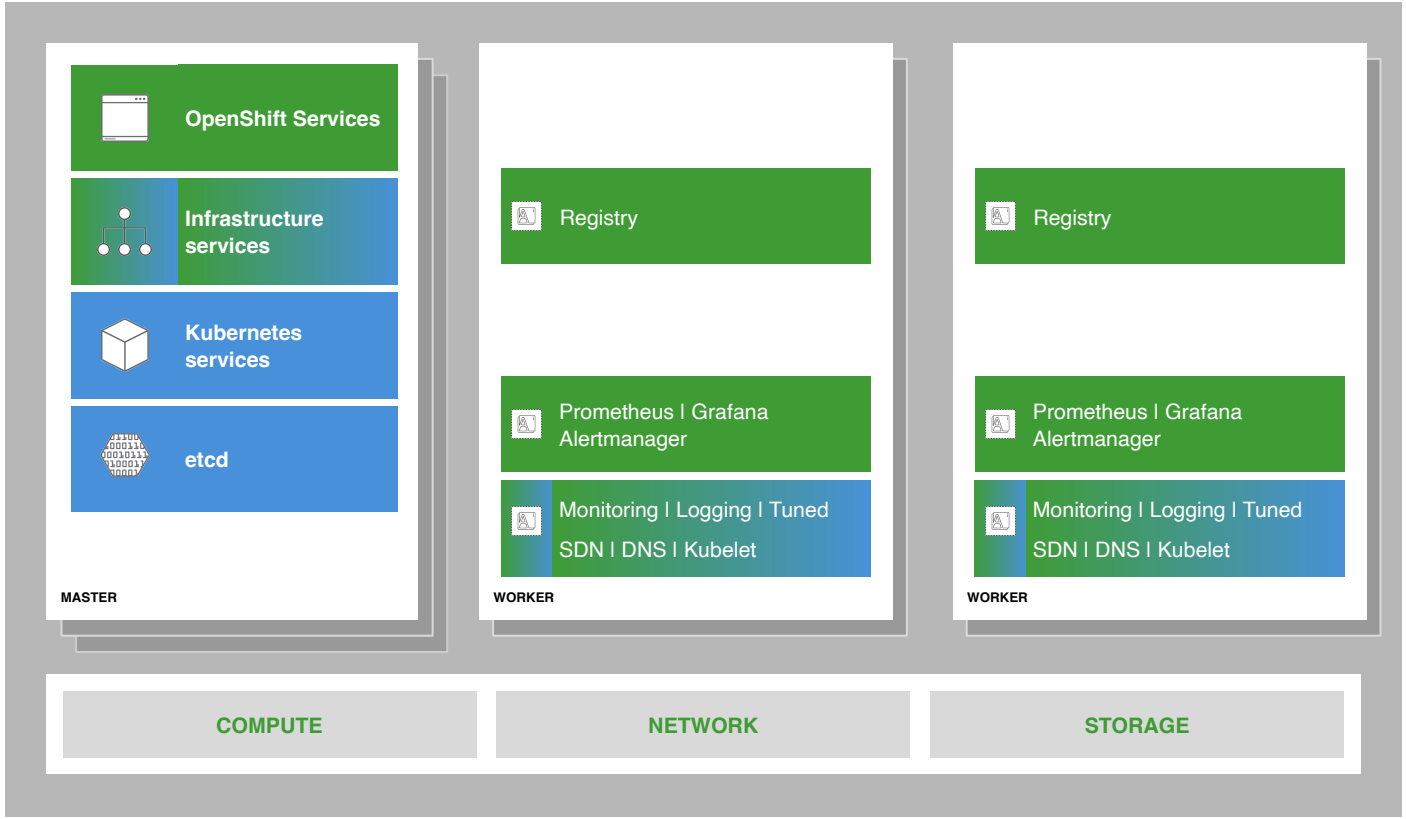
Red Hat

integrated image registry



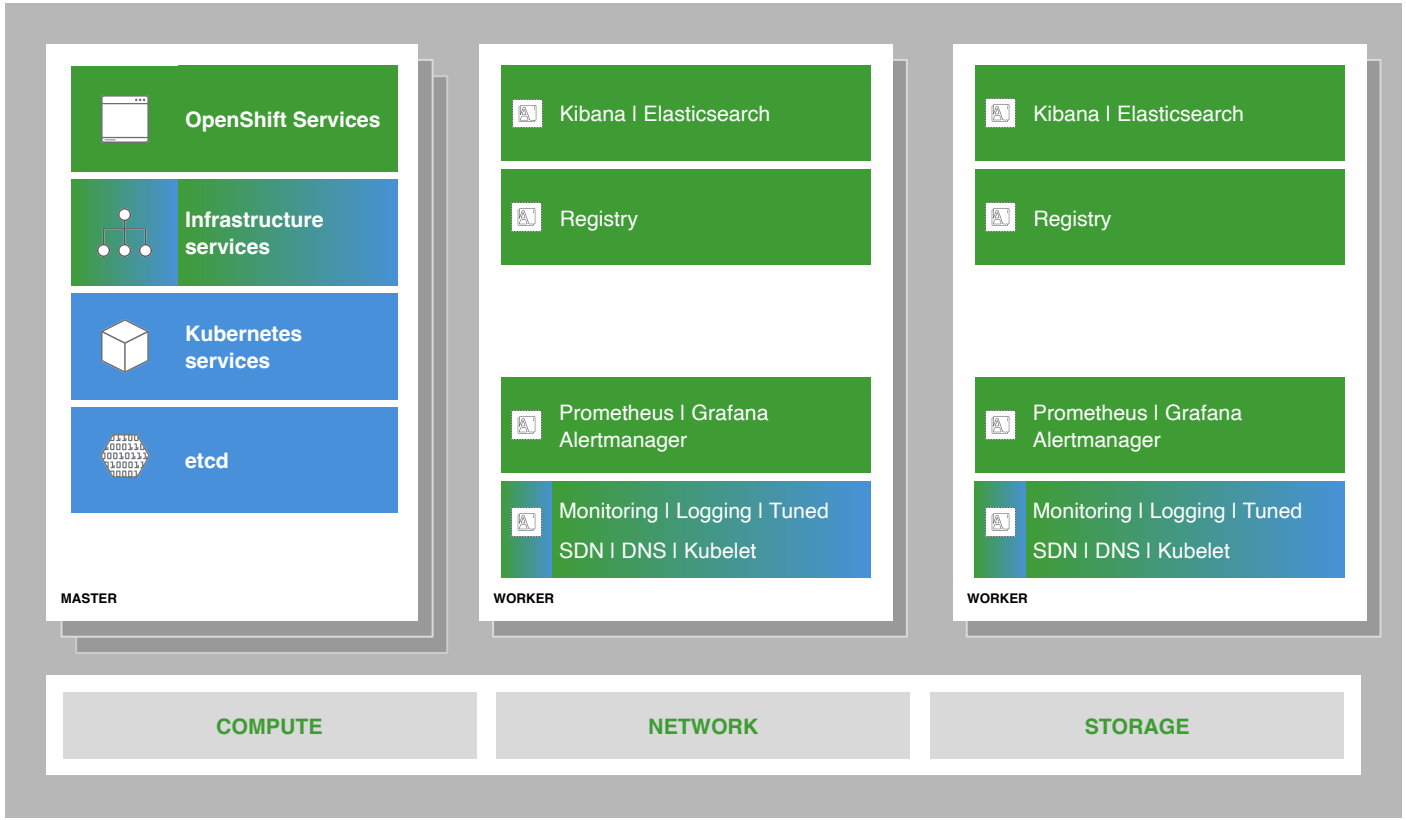
Red Hat

cluster monitoring

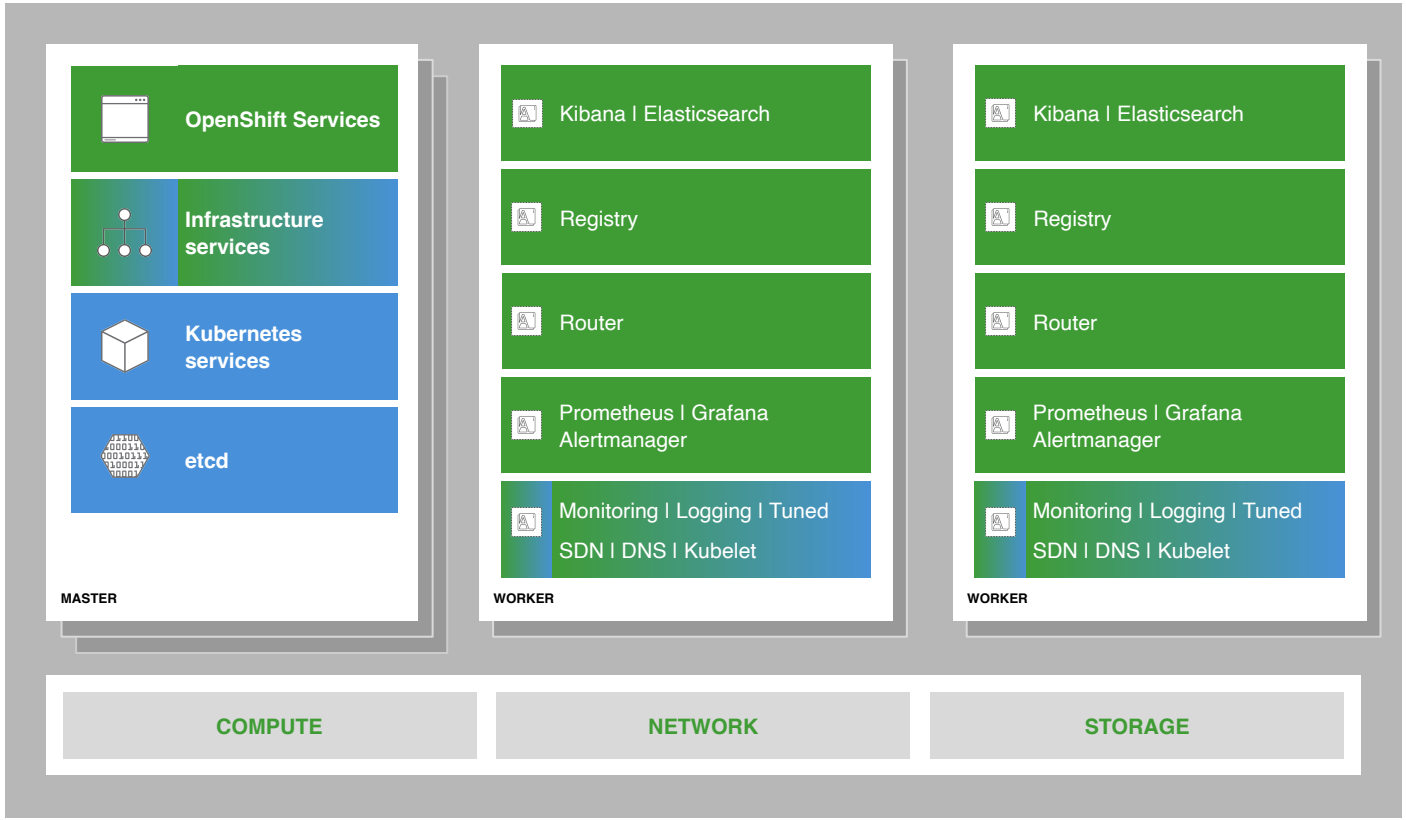


Red Hat

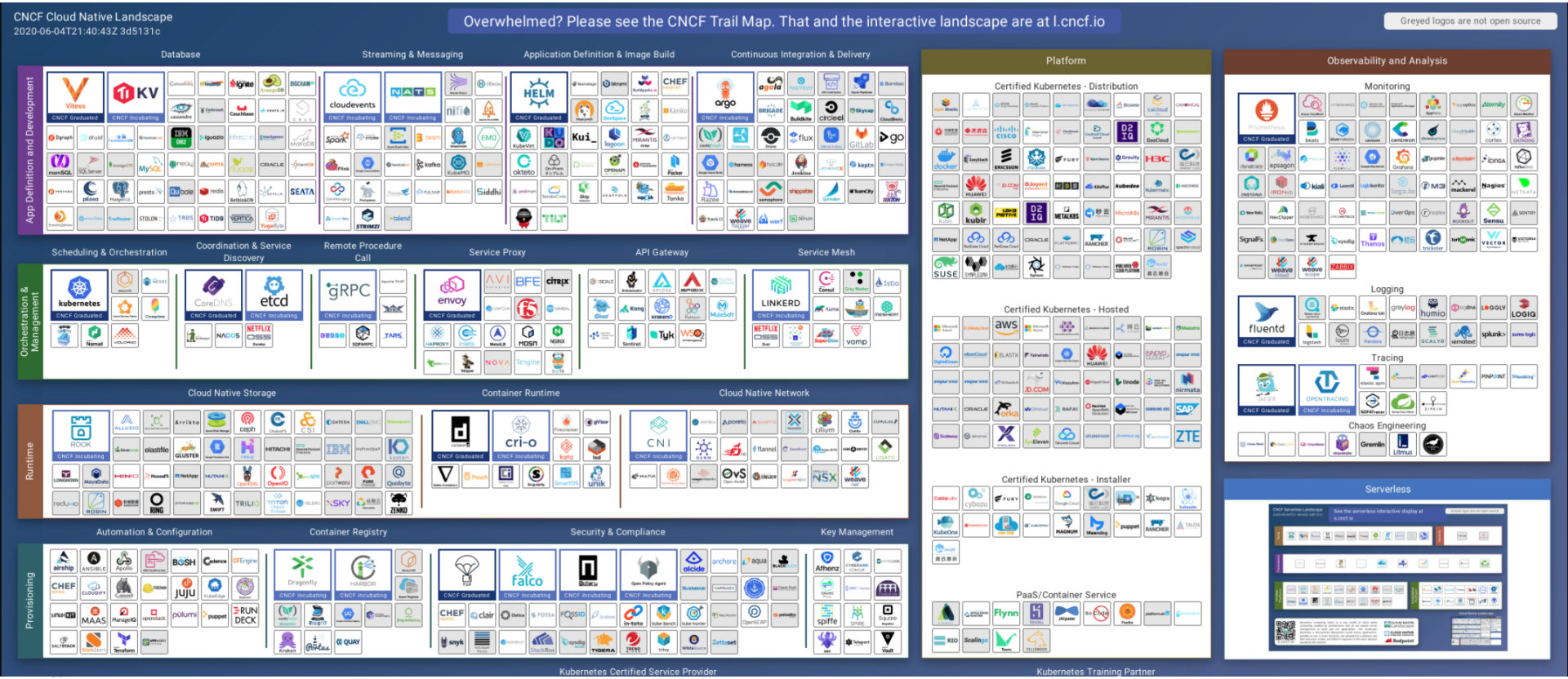
log aggregation



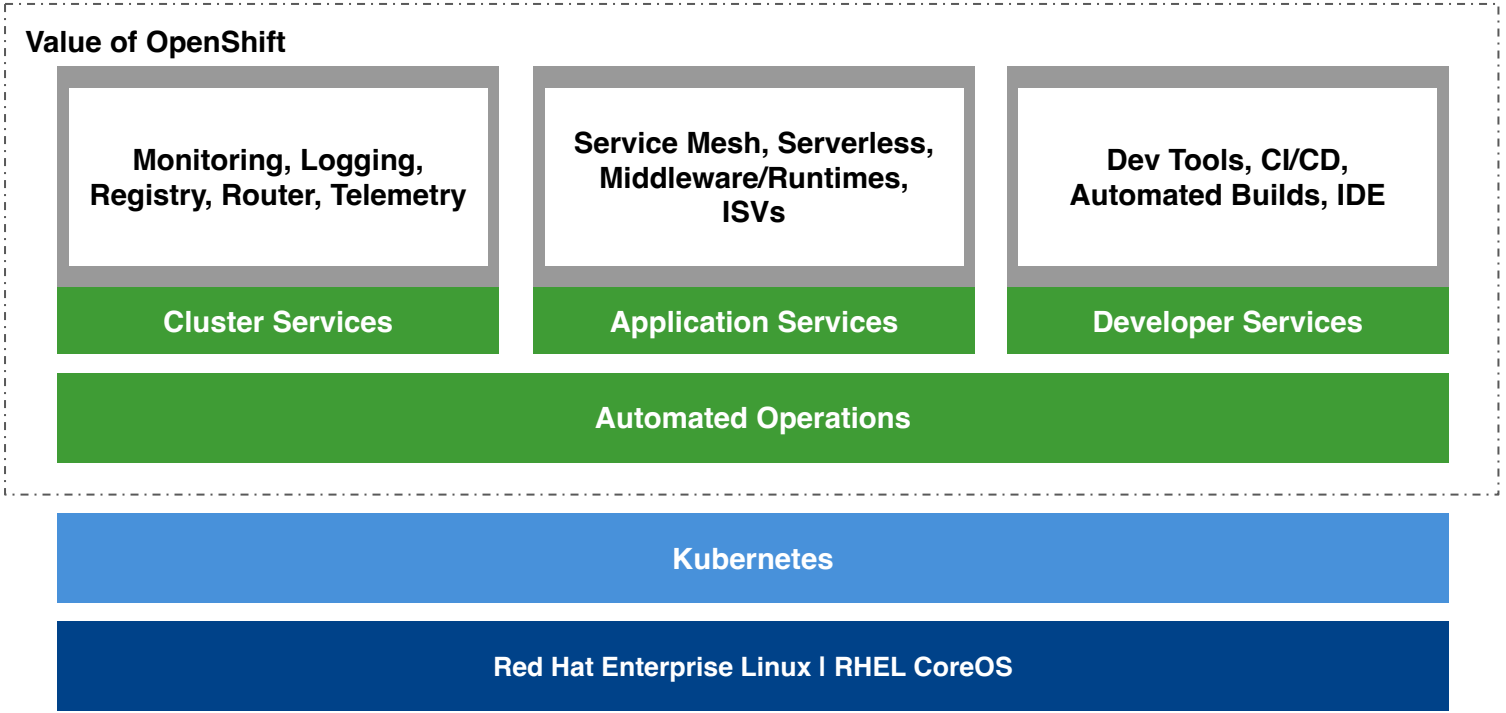
integrated routing



The Cloud Native App Dev Challenge



Red Hat

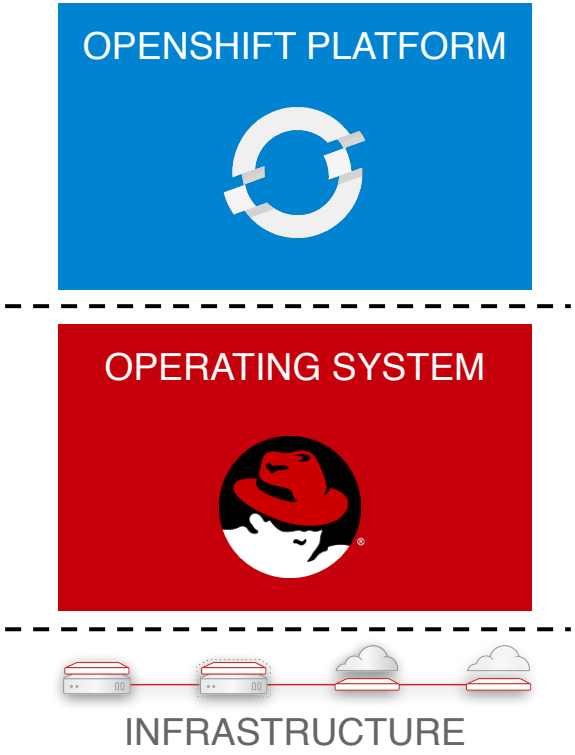


Best IT Ops Experience CaaS ⟷ PaaS ⟷ FaaS **Best Developer Experience**

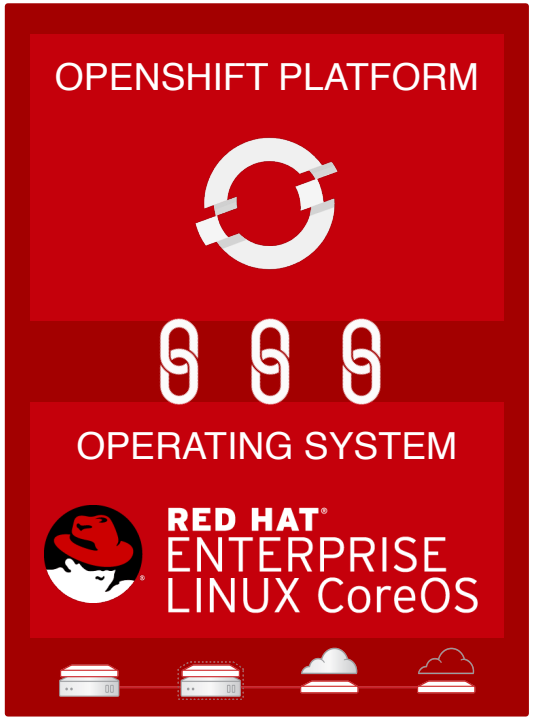
Red Hat

FULL STACK AUTOMATED INSTALL

OPENSHIFT 3



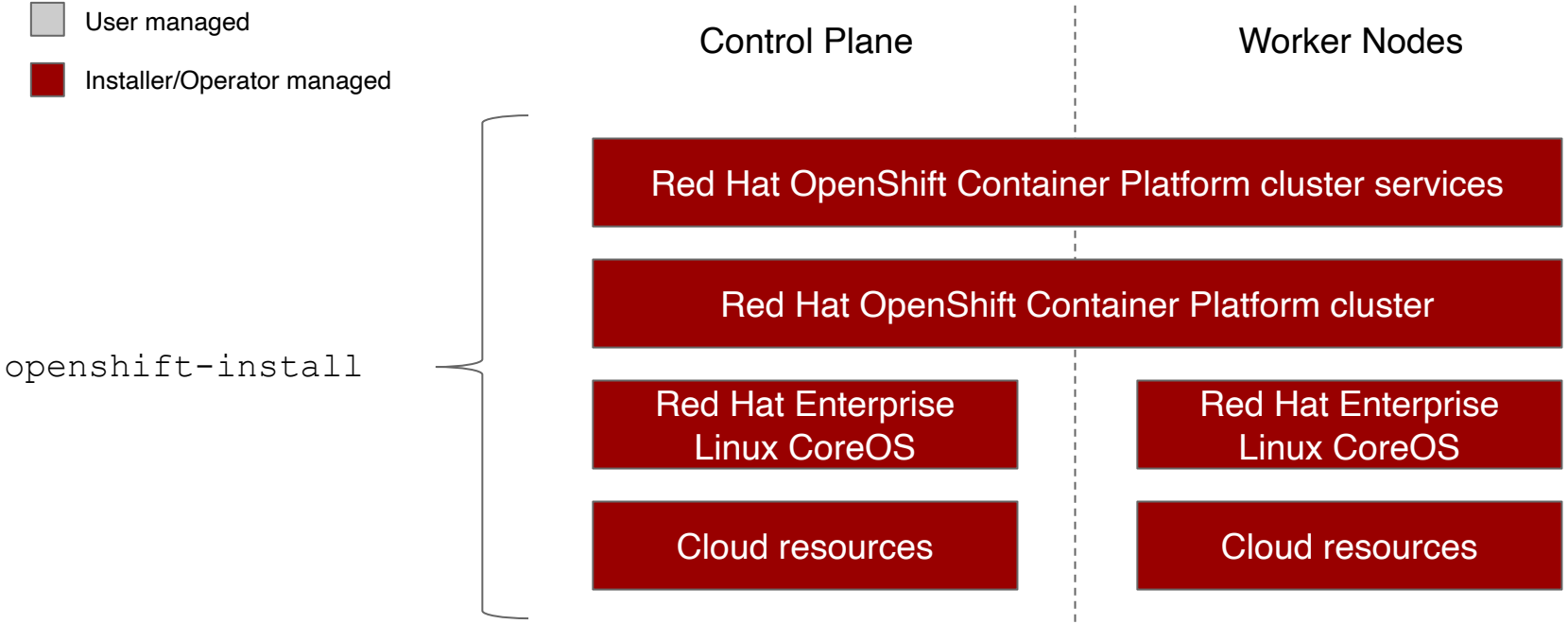
OPENSHIFT 4



Red Hat

INSTALLER PROVISIONED INFRASTRUCTURE (IPI)

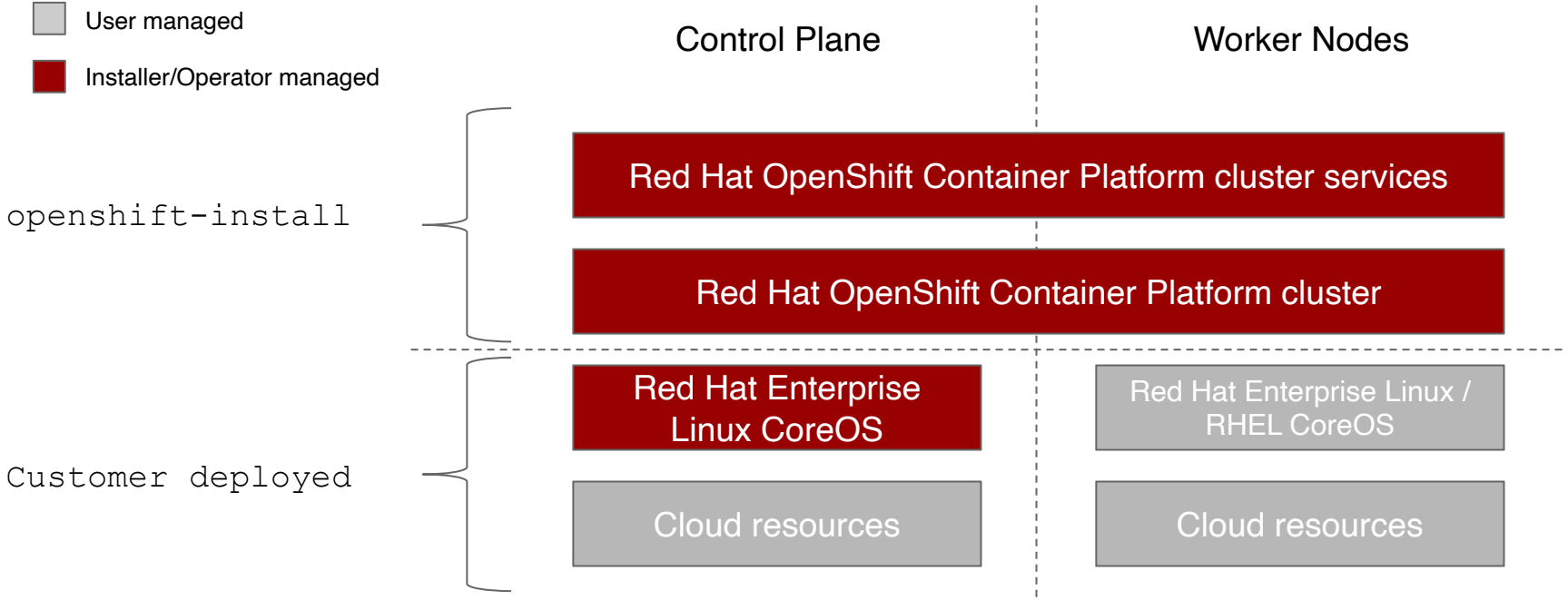
Day 1: OpenShift install - Day 2: Operators



Red Hat

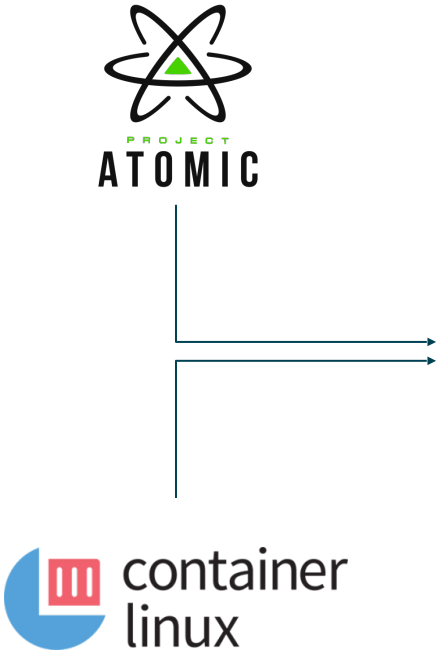
USER PROVISIONED INFRASTRUCTURE (UPI)

Day 1: OpenShift install - Day 2: Operators + Customer Managed Nodes & Infra



Red Hat

Red Hat Enterprise Linux CoreOS



Red Hat
Enterprise Linux
CoreOS

- Minimal Linux distribution
- Optimized for running containers
- Decreased attack surface
- Over-the-air automated updates
- Immutable foundation for OpenShift clusters
- Ignition-based Metal and Cloud host configuration

Red Hat

Immutable Operating System

Red Hat Enterprise Linux CoreOS is versioned with OpenShift

CoreOS is tested and shipped in conjunction with the platform.

Red Hat runs thousands of tests against these configurations.

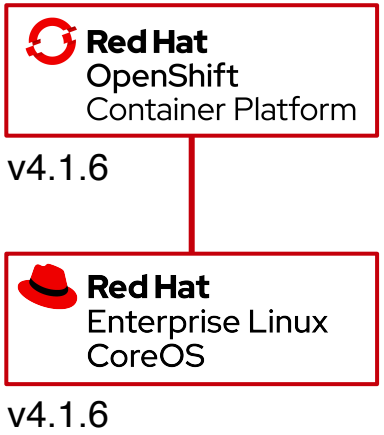
Red Hat Enterprise Linux CoreOS is managed by the cluster

The Operating system is operated as part of the cluster, with the config for components managed by Machine Config Operator:

- CRI-O config
- Kubelet config
- Authorized registries
- SSH config

RHEL CoreOS admins are responsible for:

Nothing. 😀🙌



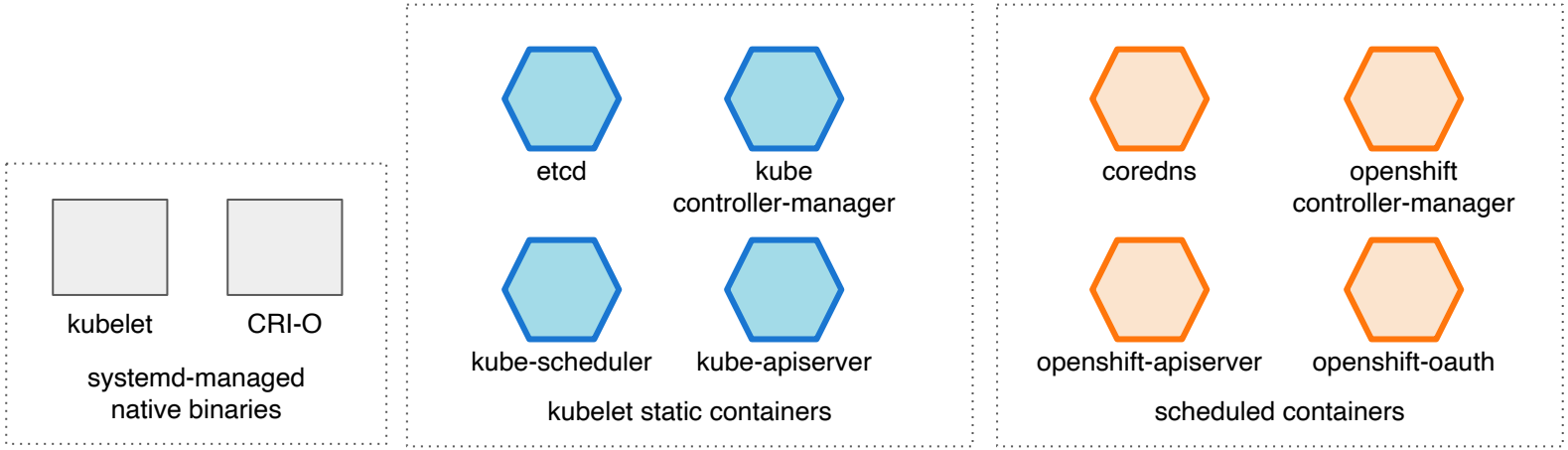
A lightweight, OCI-compliant container runtime

Minimal and Secure Architecture

Optimized for Kubernetes

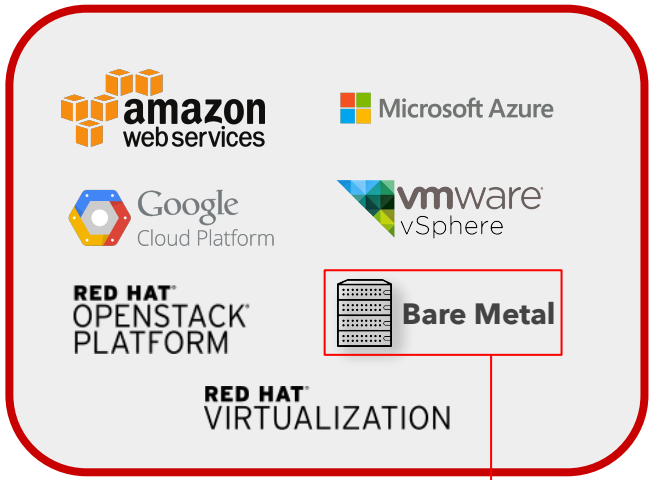
Runs any OCI-compliant image (including docker)

CoreOS “pod” architecture



Supported Providers

Full Stack Automation (IPI)



New addition in OCP 4.6

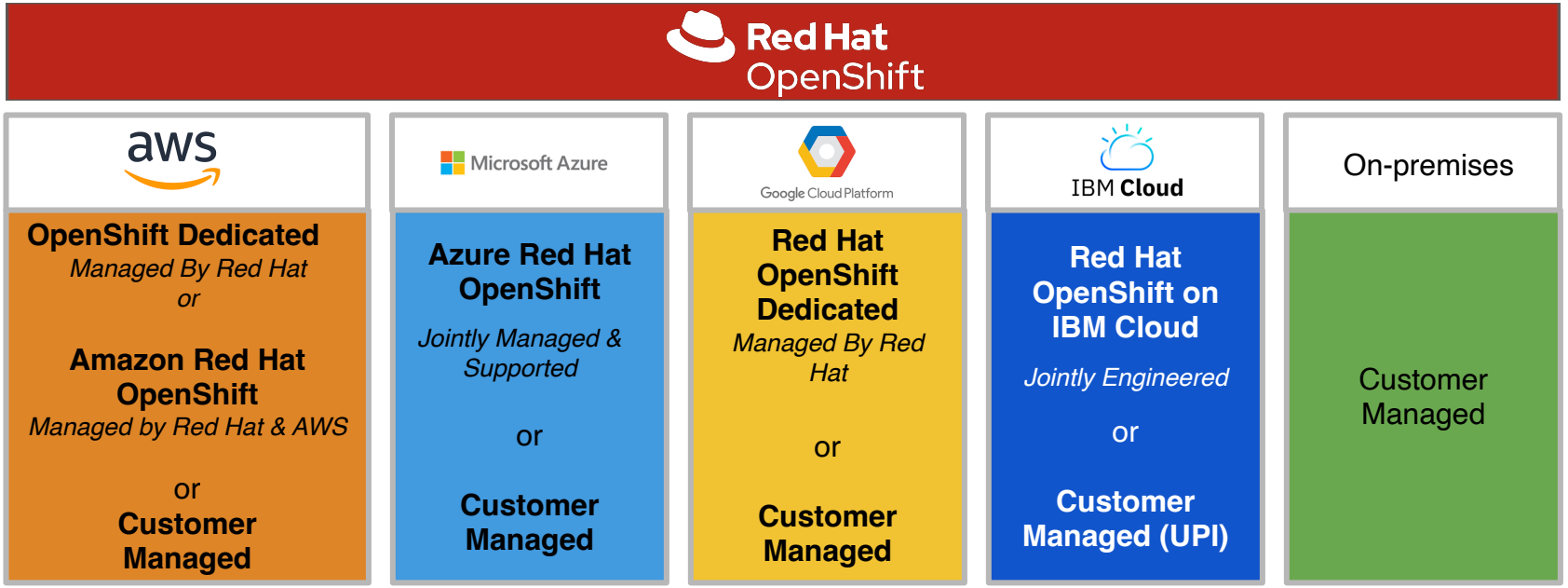
Pre-existing Infrastructure (UPI)

Now supports deploying to VMware vSphere 7.0

Generally Available

Product Manager(s): Katherine Dubé (AWS, Azure, GCP), Maria Bracho (VMware), Peter Lauterbach (RHV & OCP Virtualization), Ramon Acedo Rodriguez (OSP, BM), & Duncan Hardie (IBM Z & Power)

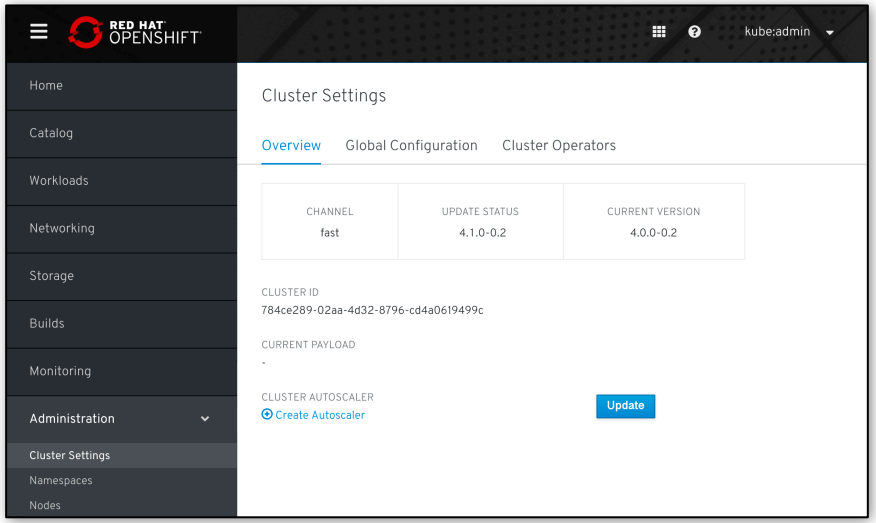
OpenShift offers the broadest set of hybrid cloud services



Red Hat

OVER-THE-AIR UPDATES

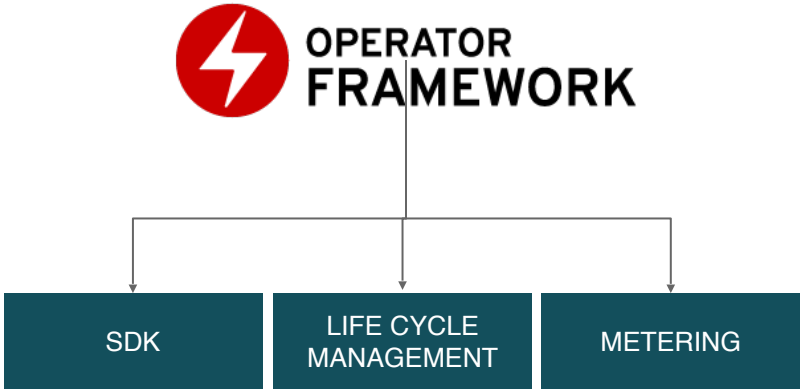
- OpenShift retrieves list of available updates
- Admin selects the target version
- OpenShift is updated over the air
- Auto-update support



Red Hat

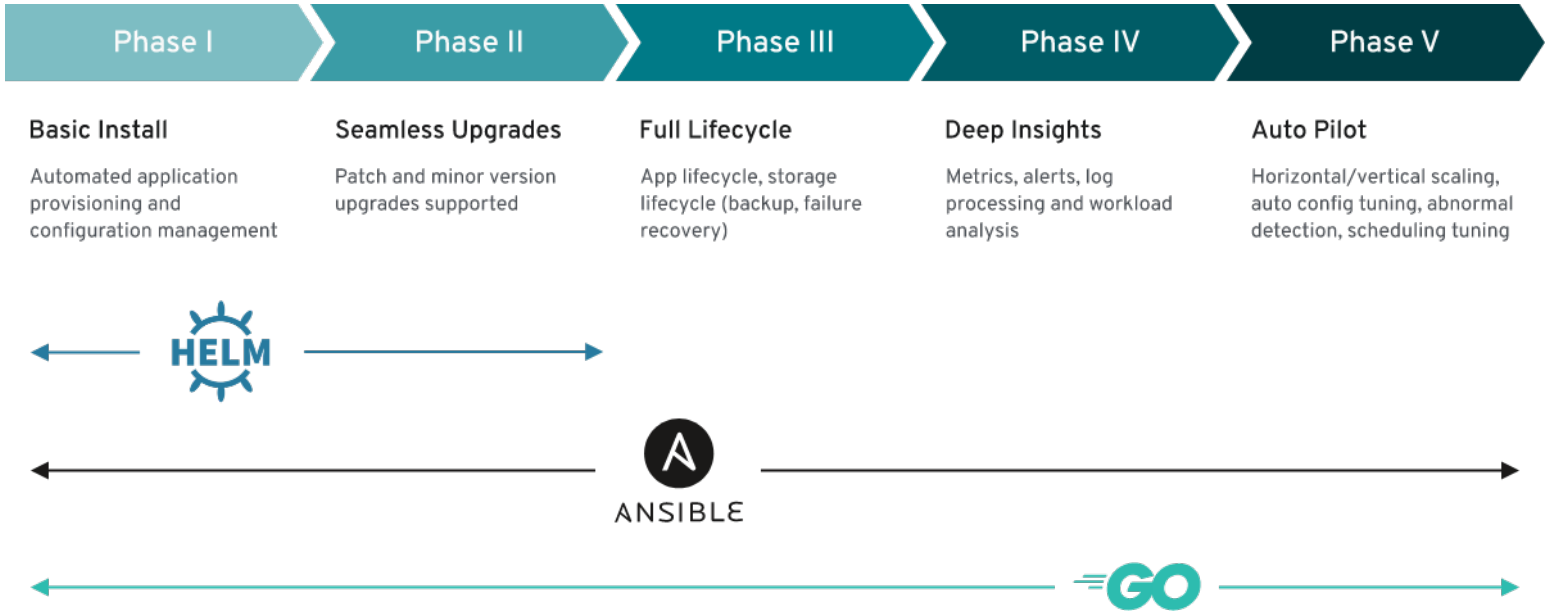
OPERATOR FRAMEWORK

Operators codify operational knowledge and workflows to automate life cycle management of containerized applications with Kubernetes



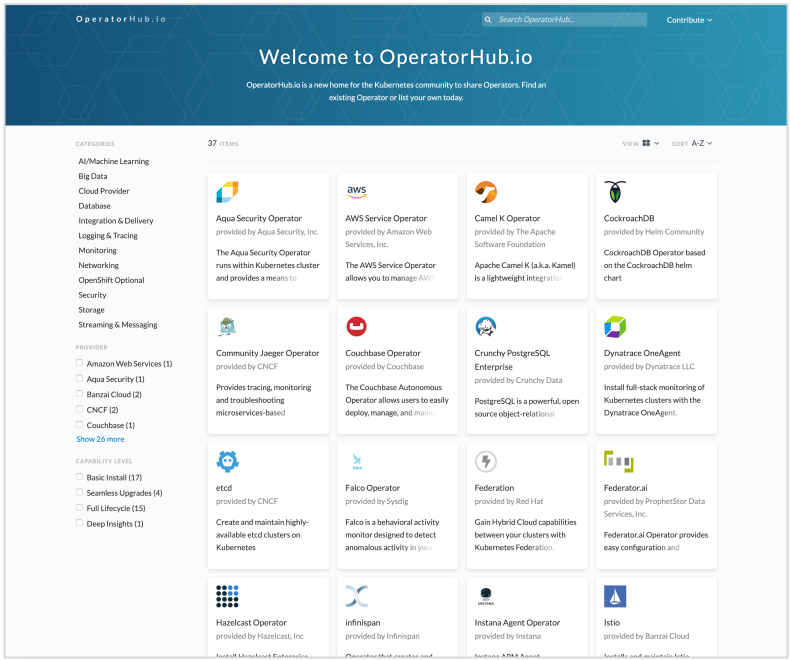
Red Hat

OPERATOR FRAMEWORK



Red Hat

OperatorHub.io Ecosystem

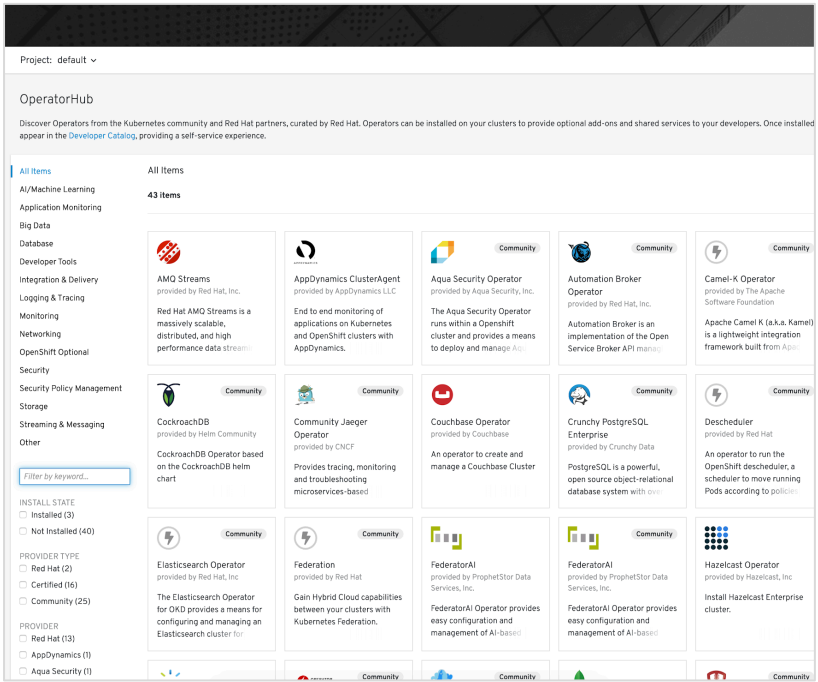


The public registry for finding Kubernetes Operator backed services

Red Hat

OperatorHub in OpenShift

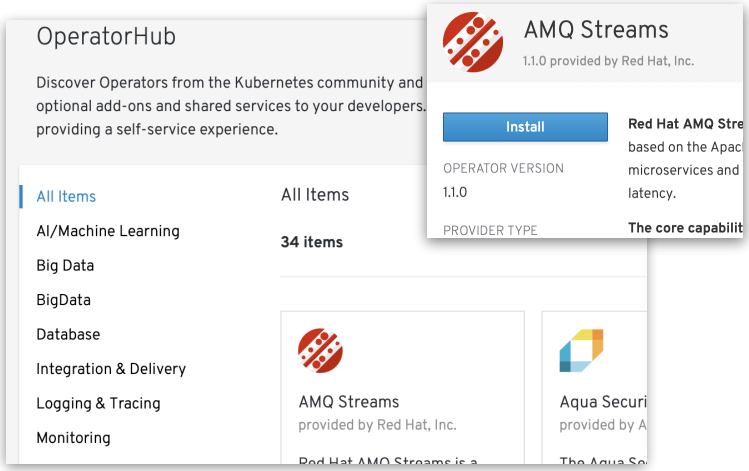
The embedded registry for Community and Certified Operators from Red Hat and Partners, tested and verified on OpenShift 4



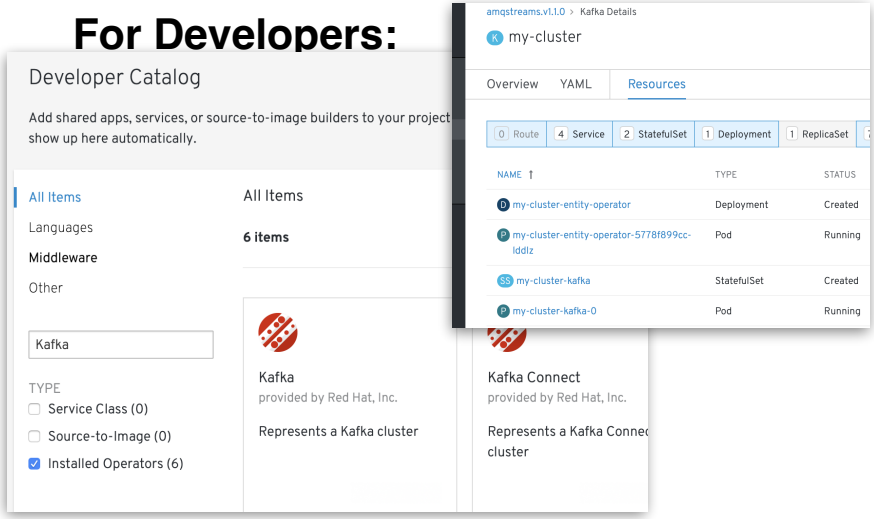
Red Hat

OperatorHub in OpenShift

For Cluster Admins:



For Developers:



- Developers can’t see admin screens
- Operator capabilities are exposed in Catalog
- Self-service management

- Discovery/install/upgrade of Operators
- Community, Red Hat products, Certified ISVs
- Granular access via specific Projects

Red Hat

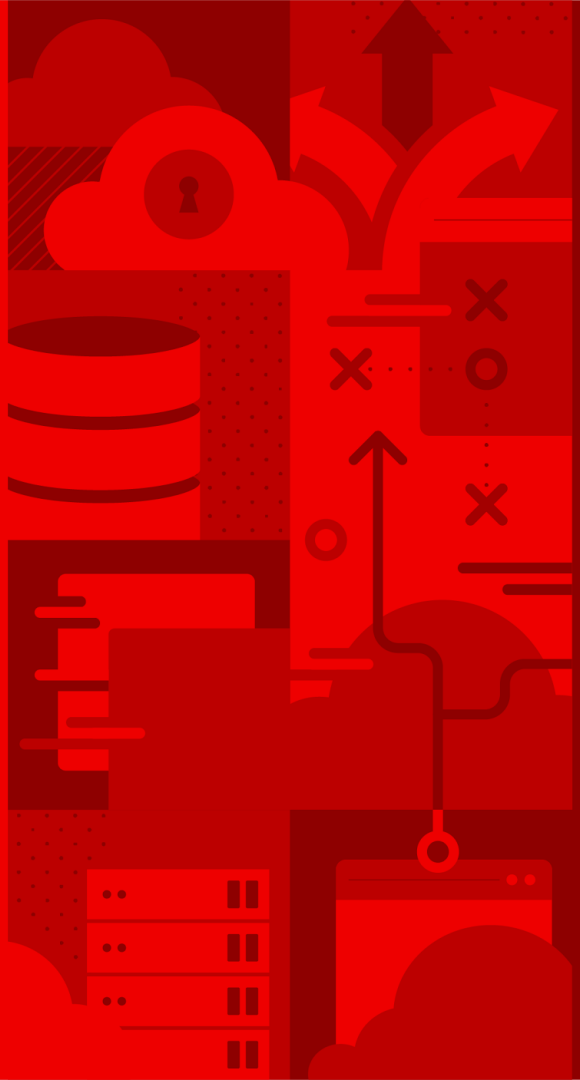
Machine Config Operator

A Kube-native way to configure hosts

OS configuration is stored and applied across the cluster via the Machine Config Operator.

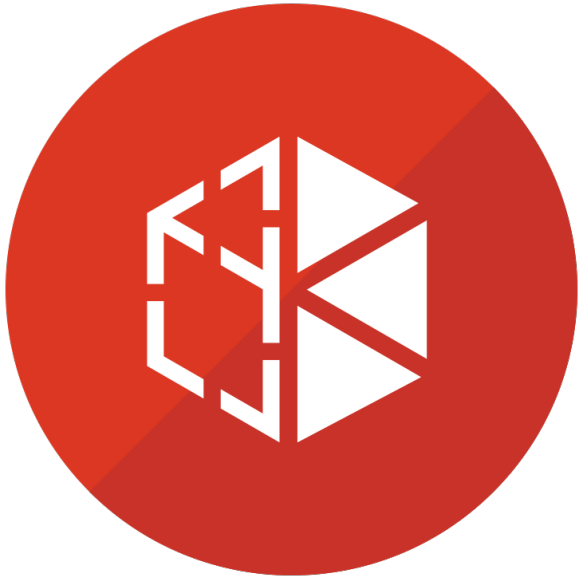
- Subset of ignition modules applicable post provisioning
  - SSH keys
  - Files
  - systemd units
  - kernel arguments
- Standard k8s YAML/JSON manifests
- Desired state of nodes is checked/fixed regularly
- Can be paused to suspend operations

```
# test.yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: test-file
spec:
  config:
    storage:
      files:
      - contents:
          source: data:,hello%20world%0A
          verification: {}
        filesystem: root
        mode: 420
        path: /etc/test
```



OpenShift Virtualization

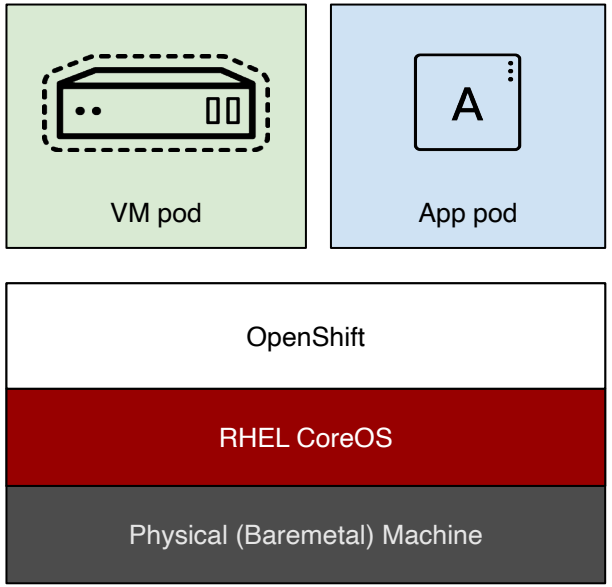
OpenShift Virtualization



A virtualization API and runtime for OpenShift, built on KubeVirt, to run and manage virtual machines using a Kubernetes-native way

Virtual machines in a container world

- Provides a way to transition application components which cannot be directly containerized into a Kubernetes system
  - Integrates directly into existing k8s clusters
  - Follows Kubernetes paradigms:
    - Container Networking Interface (CNI)
    - Container Storage Interface (CSI)
    - Custom Resource Definitions (CRD, CR)
- Schedule, connect, and consume VM resources as container-native
- VMs and containers living side-by-side



Virtualization native to Kubernetes

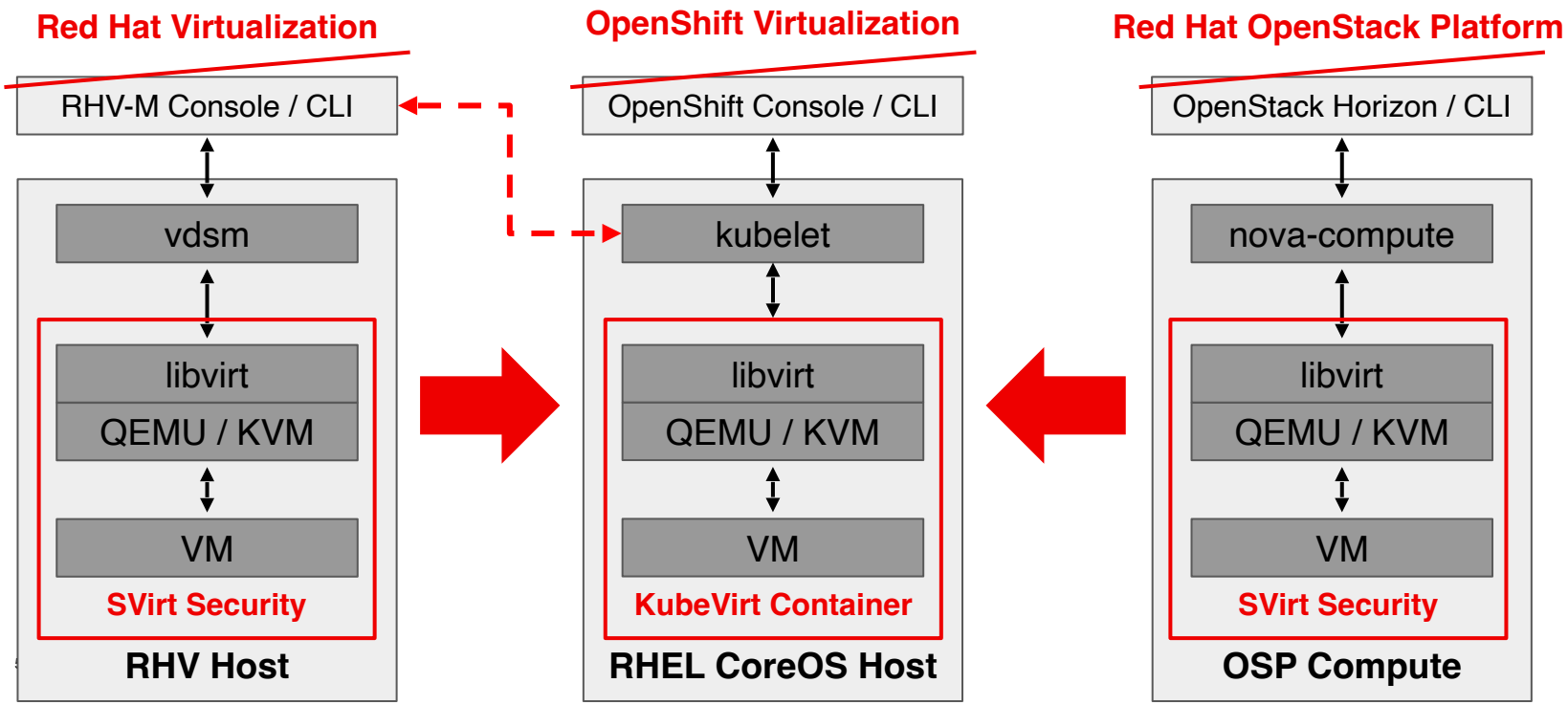
- New CustomResourceDefinitions (CRDs) for native VM integration, for example:
  - `VirtualMachine`
  - `VirtualMachineInstance`
  - `VirtualMachineInstanceMigration`
  - `DataVolume`

- Operators are a Kubernetes-native way to introduce new capabilities

```yaml
apiVersion: kubevirt.io/v1alpha3
kind: VirtualMachine
metadata:
  labels:
    app: demo
    flavor.template.kubevirt.io/small: "true"
  name: rhel
spec:
  dataVolumeTemplates:
  - apiVersion: cdi.kubevirt.io/v1alpha1
    kind: DataVolume
    metadata:
      creationTimestamp: null
      name: rhel-rootdisk
    spec:
      pvc:
        accessModes:
        - ReadWriteMany
        resources:
          requests:
            storage: 20Gi
        storageClassName: managed-nfs-storage
        volumeMode: Filesystem
```

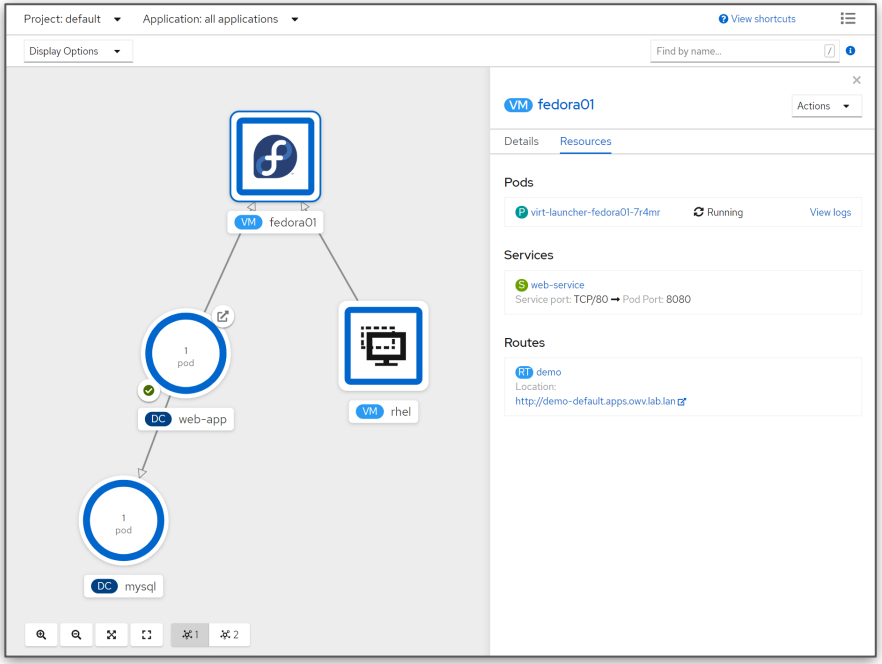
Containerizing KVM

Same trusted, mature KVM-based stack, wrapped in modern management and automation



Using VMs and containers together

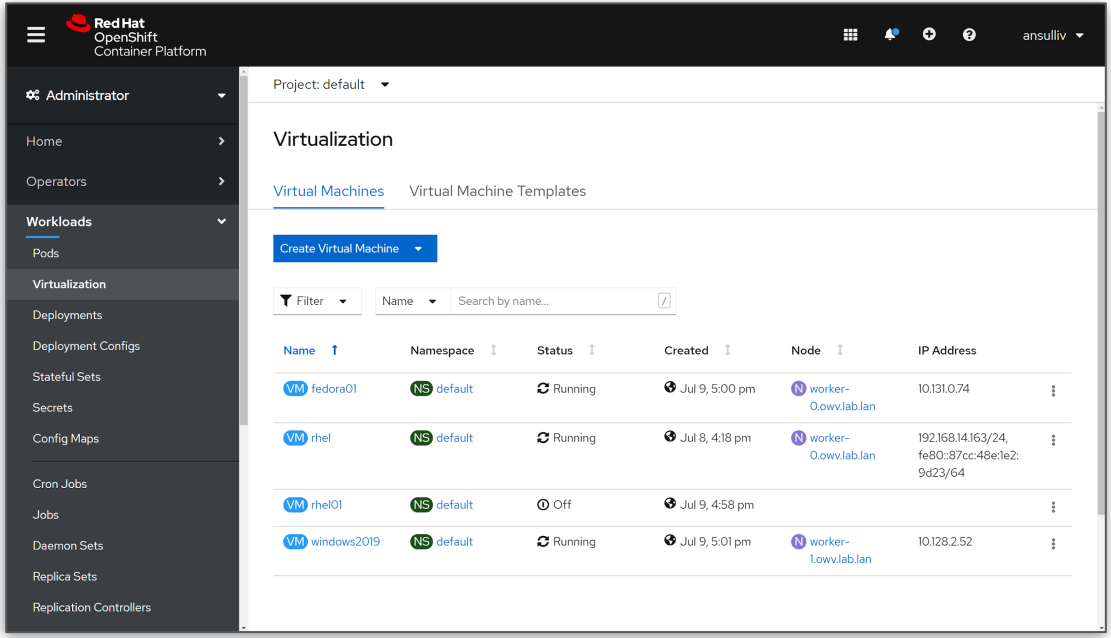
- Virtual Machines connected to pod networks are accessible using standard Kubernetes methods:
  - Service
  - Route
  - Ingress
- Network policies apply to VM pods the same as application pods
- VM-to-pod, and vice-versa, communication happens over SDN or ingress depending on network connectivity



Red Hat

Virtual Machine Management

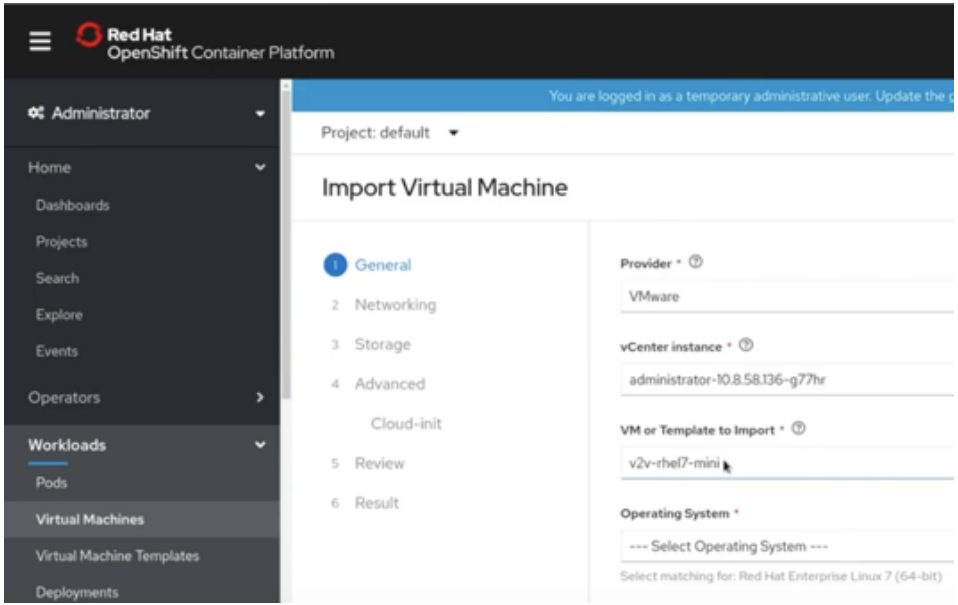
- Create, modify, and destroy virtual machines, and their resources, using the OpenShift web interface or CLI
- Use the `virtctl` command to simplify virtual machine interaction from the CLI



Red Hat

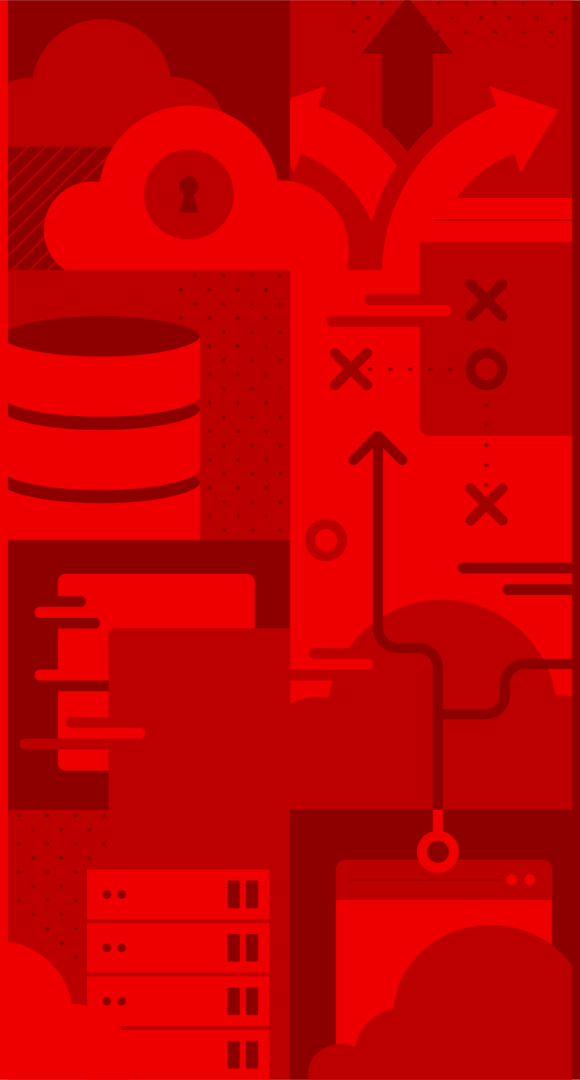
Modernize existing virtual machine workloads

Supports VMware & Red Hat Virtualization (now), Red Hat OpenStack Platform (later)



1. Run Red Hat Migration Analytics from cloud.redhat.com to select best candidates for import to OpenShift
2. For single VMs, run the Import Virtual Machine workflow from OpenShift
3. For multiple VMs, leverage the Red Hat Migration tool for batch import (longer term)
4. Import as a single VM or create a template for multiple ones

Red Hat



OpenShift Security

Red Hat

CONTROL
Application Security

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

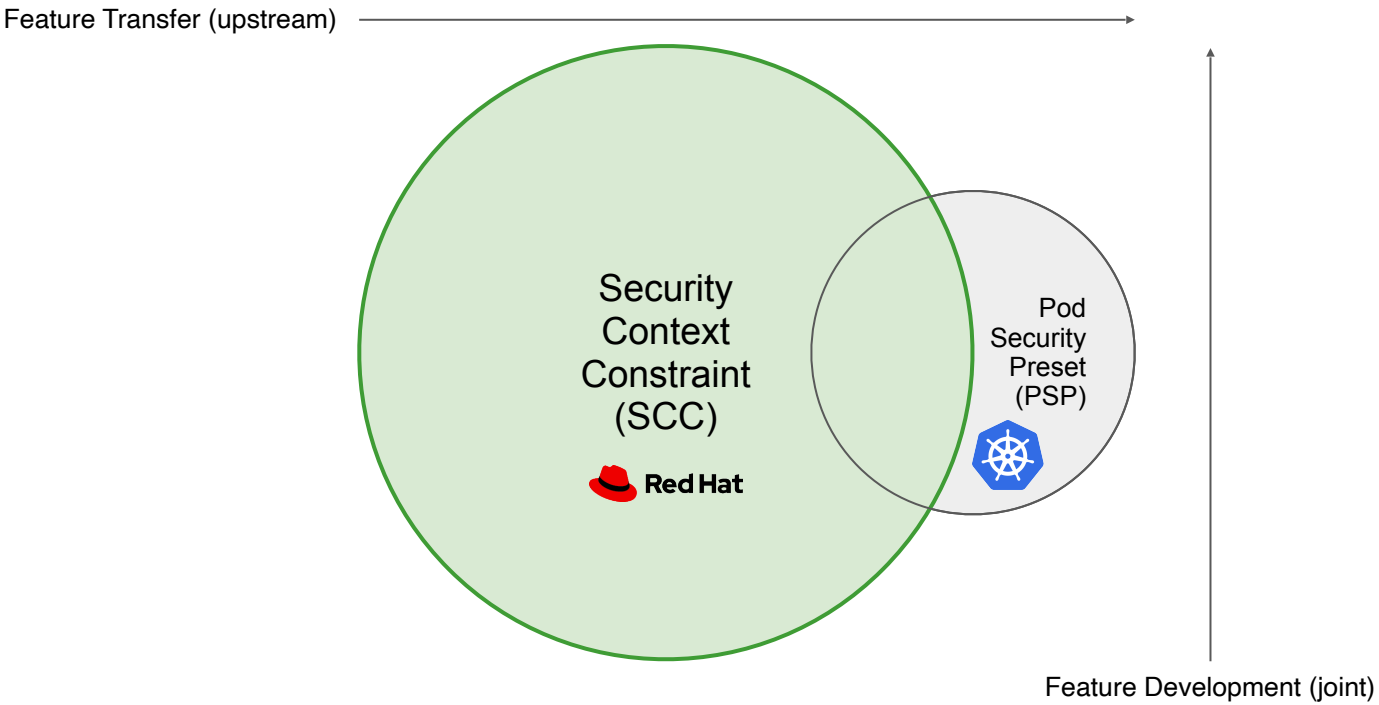
DEFEND
Infrastructure

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

EXTEND

- Security Ecosystem

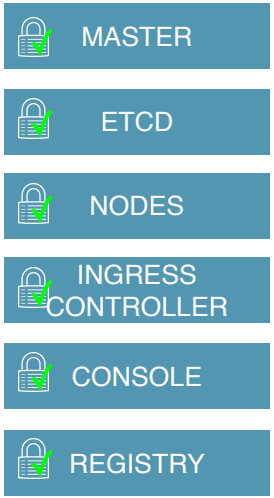
Extended Depth of Protection



Red Hat

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



Container Security Operator (CSO) and Quay

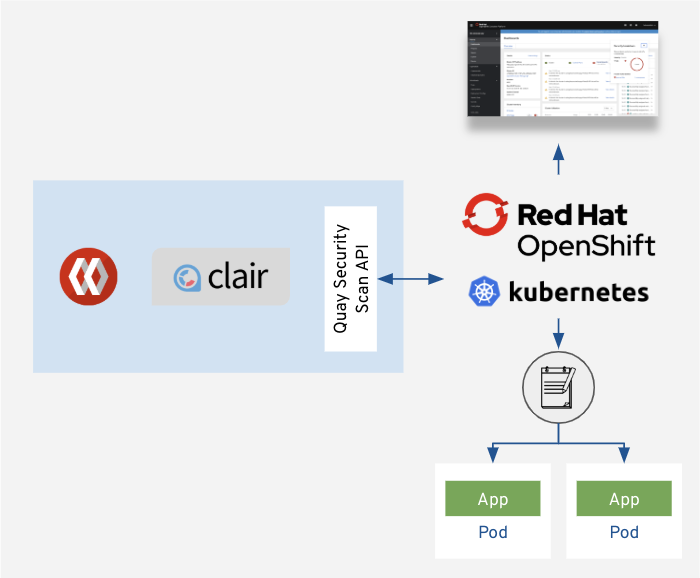
What is it?

- Container Security Operator (CSO) runs on OpenShift and watches pod objects

Why do you need it?

- Easily visualize image security vulnerability data from Quay / Clair

How does it work?

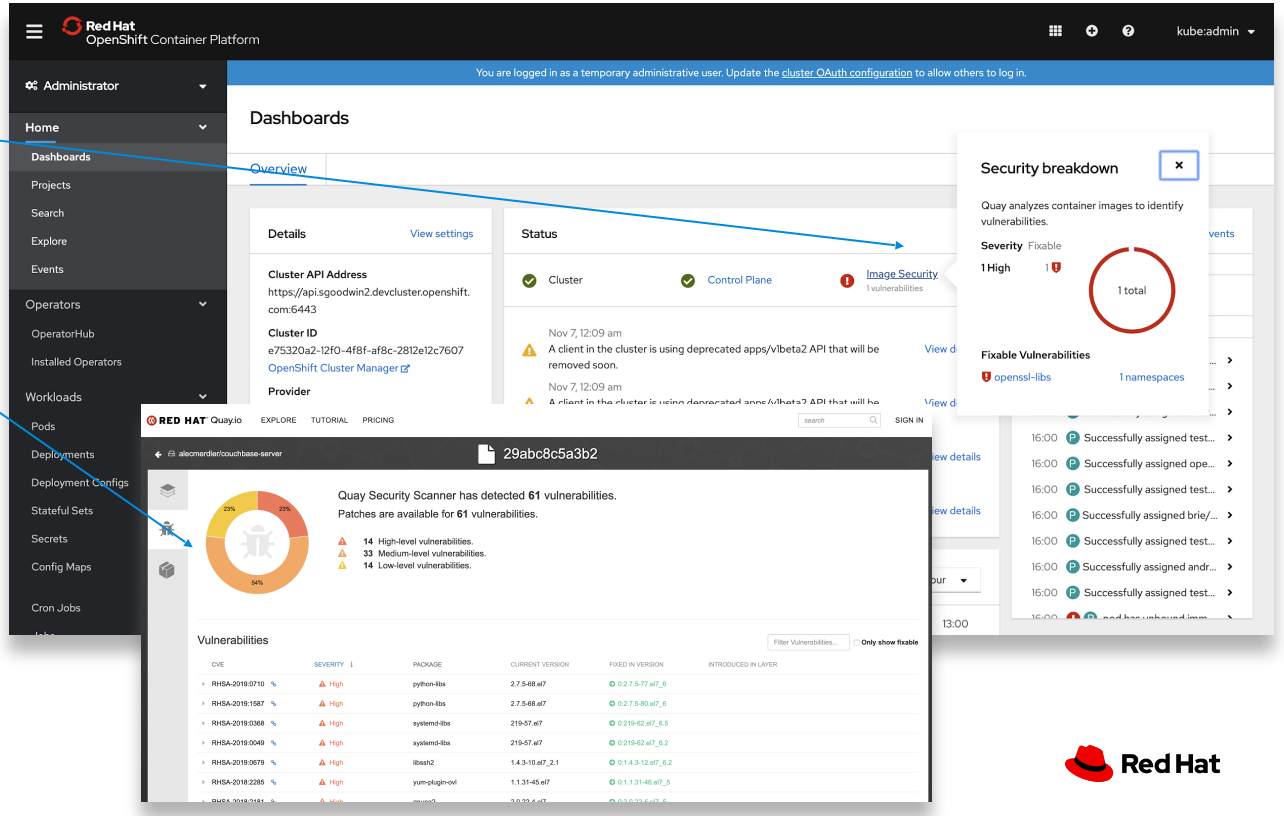


Red Hat

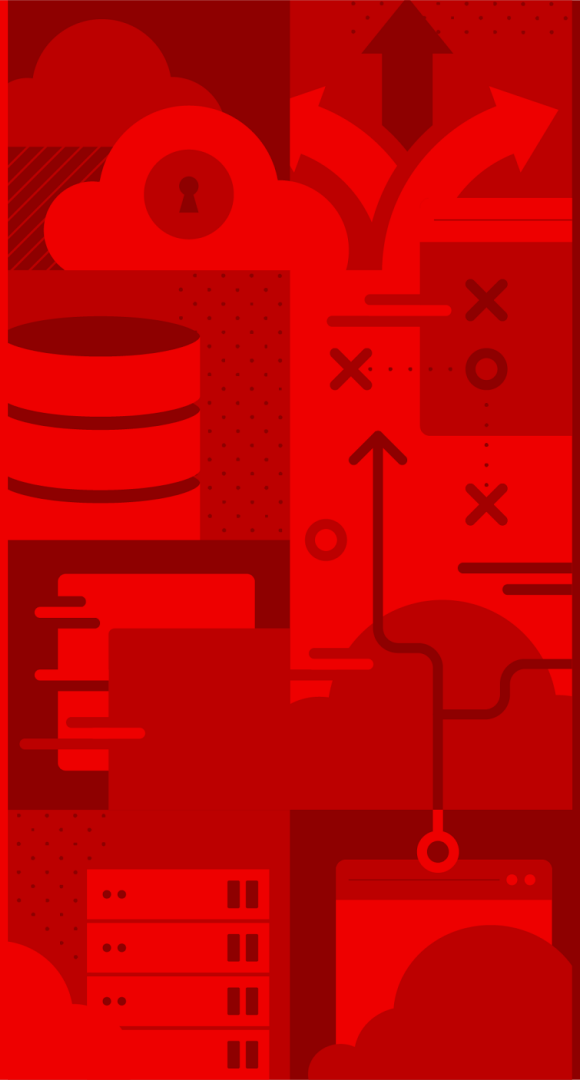
View Image Security Vulnerabilities in OpenShift

See all your Container Vulnerabilities right from the Console Dashboard

- Link out to **Red Hat Quay** for more in depth information
- The Quay Operator supports both **On-premise and External** Quay Registries
- Currently uses **Clair for Security Scan**; Planning to expand to other Vendors(TwistLock, Aqua, e.g.)
- *Only works for images managed by Quay*



Red Hat

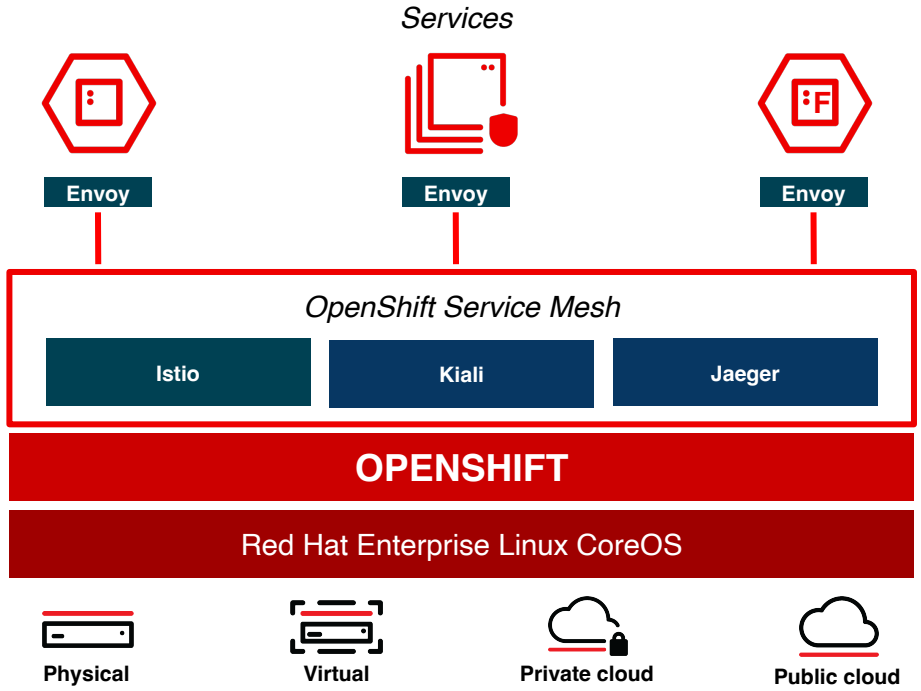


OpenShift Developer Services

Red Hat

Openshift Service Mesh

- Connect services securely with zero-trust network policies.
- Automatically secure your services with managed authentication, authorization and encryption.
- Control traffic to safely manage deployments, A/B testing, chaos engineering and more.
- See what's happening with out of the box distributed tracing, metrics and logging.
- Manage OpenShift Service Mesh with the **Kiali** web console.



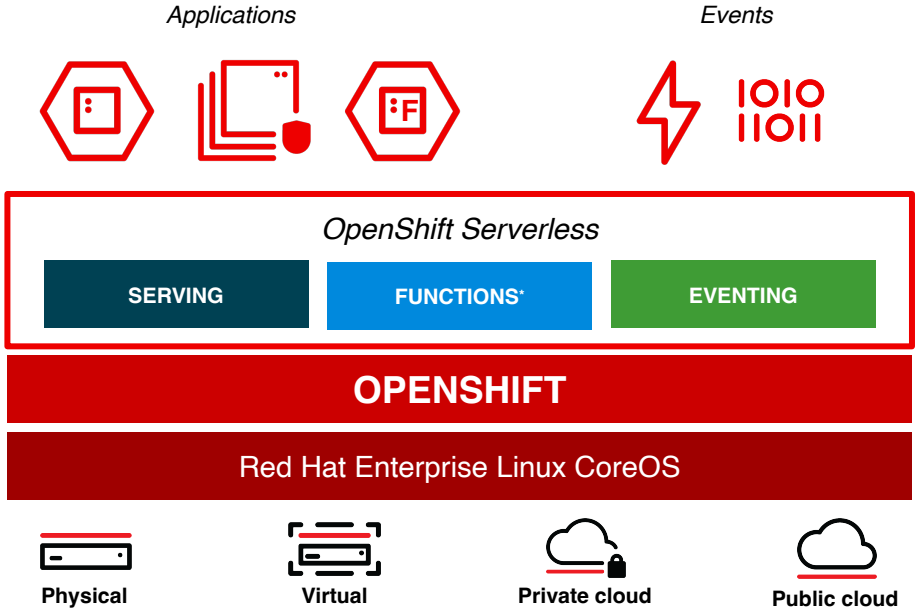
Red Hat

Generally Available

Openshift Serverless

Event-driven serverless containers and functions

- Deploy and run **serverless containers**
- Use any programming language or runtime
- Modernize existing applications to run serverless
- Powered by a rich ecosystem of event sources
- Manage serverless apps natively in Kubernetes
- Based on open source project **Knative**
- Run anywhere OpenShift runs



* Functions are currently a work in progress initiative

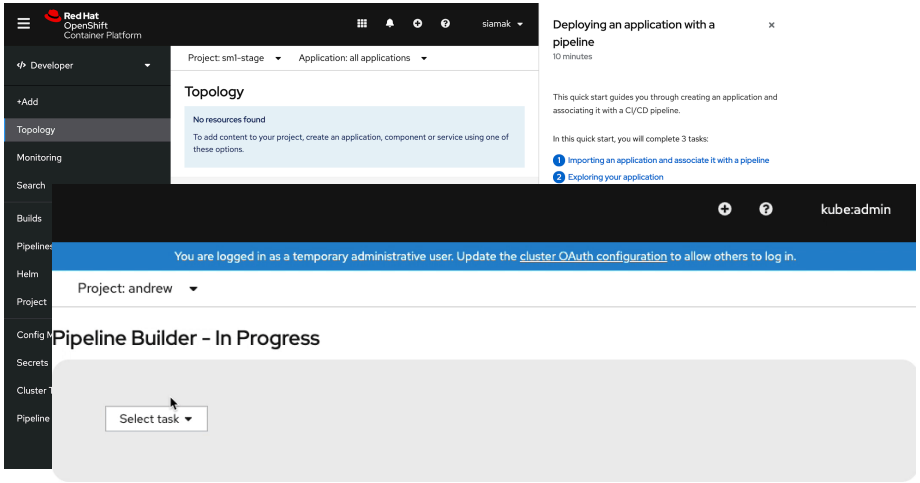
Red Hat

Cloud-native CI/CD with OpenShift Pipelines

Tech Preview

TEKTON

- Pipeline templates for serverless when importing application (+Add)
- Pipeline templates use workspaces instead of PipelineResources
- Default workspace per PipelineRun or globally
- Expanded Task library
  - Helm tasks
  - Skopeo tasks
  - Trigger Jenkins jobs from Tekton
- Support for disconnected clusters
- Pipeline metrics in cluster monitoring
- Pipeline Quick Start tours in Dev Console
- Enhancements in Tekton CLI: workspaces, results



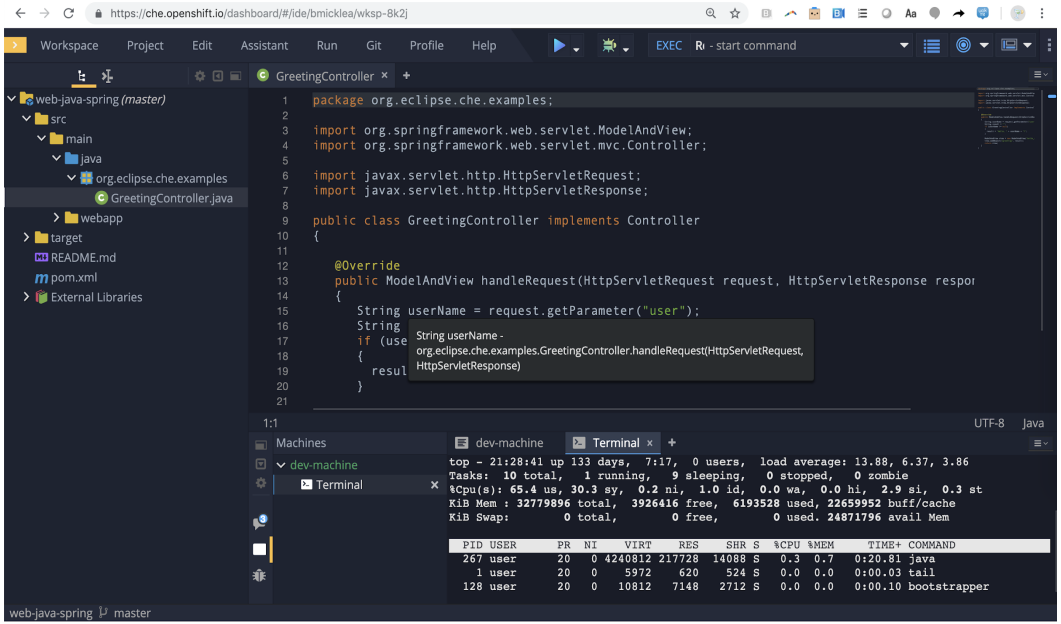
Product Manager: Siamak Sadeghianfar

* Available through the OpenShift Pipelines operator “preview” channel

Red Hat

CodeReady Workspaces

- Web-based Eclipse Che IDE
- Developer workspaces in pods
- Bundled development stacks
- Available in OperatorHub



Podman and Buildah

podman

A docker-compatible CLI for containers

- Remote management API via Varlink
- Image/container tagging
- Advanced namespace isolation

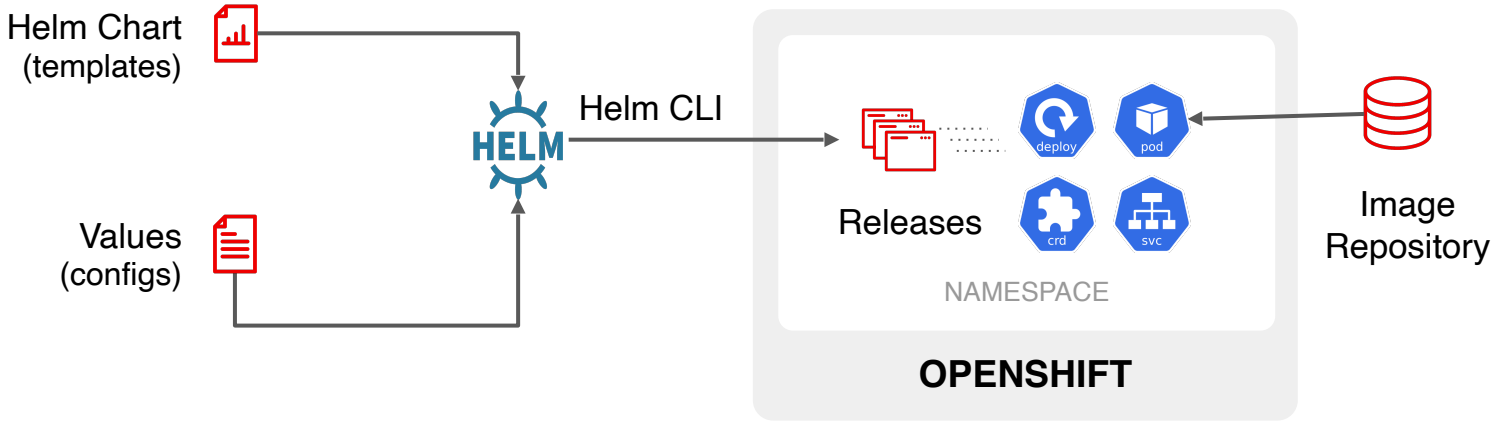
buildah

Secure & flexible OCI container builds

- Integrated into OCP build pods
- Performance improvements for knative enablement
- Image signing improvements

Helm 3 on OpenShift

Helm is a package manager for Kubernetes applications and helps to define, install and update apps

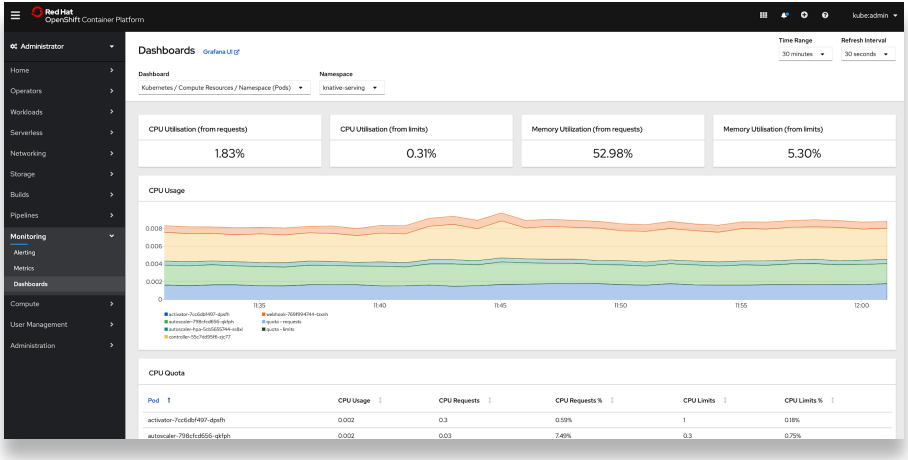


Product Manager: Siamak Sadeghianfar

Metrics Dashboard

At-a-glance views for your mission critical OpenShift components right from the OpenShift Console.

- Offers a single, centralized place for all OpenShift components to provide insights into critical KPIs back to you.
- Switch between dashboards, representing different parts of your cluster.
- Filter by different criterias defined by a dashboards and different time ranges.



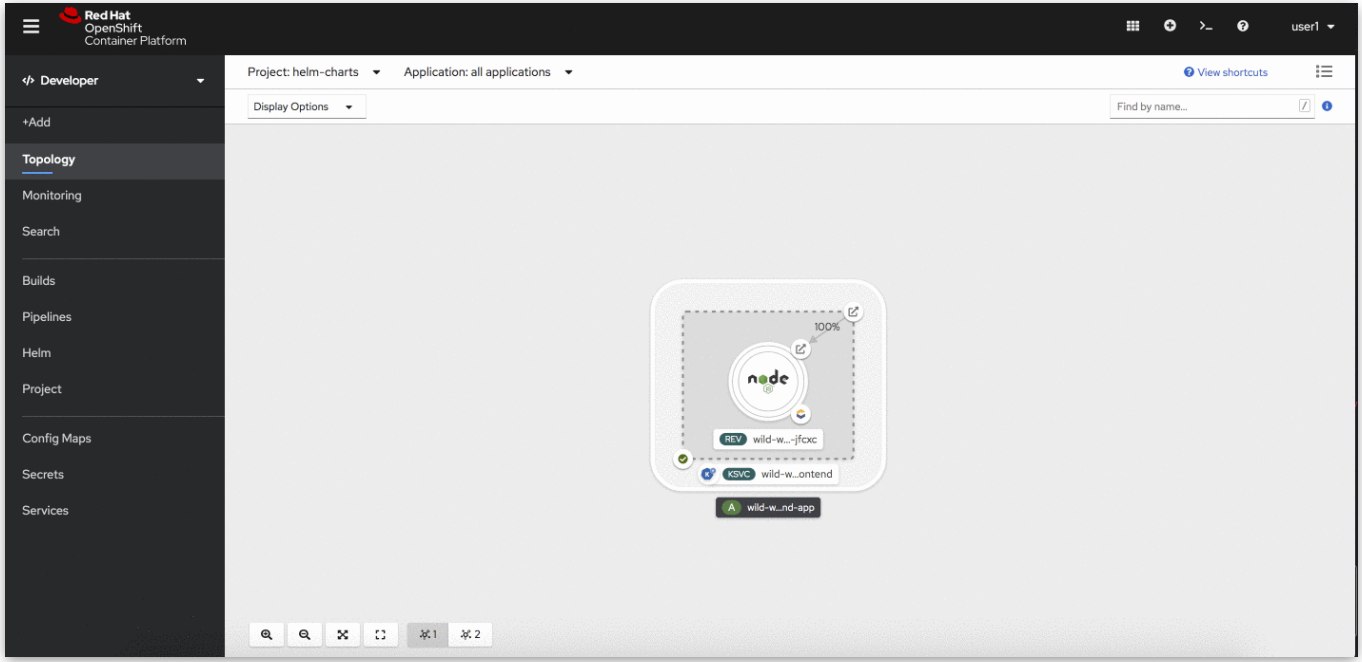
Red Hat

Easy access to Web Terminal

Tech Preview

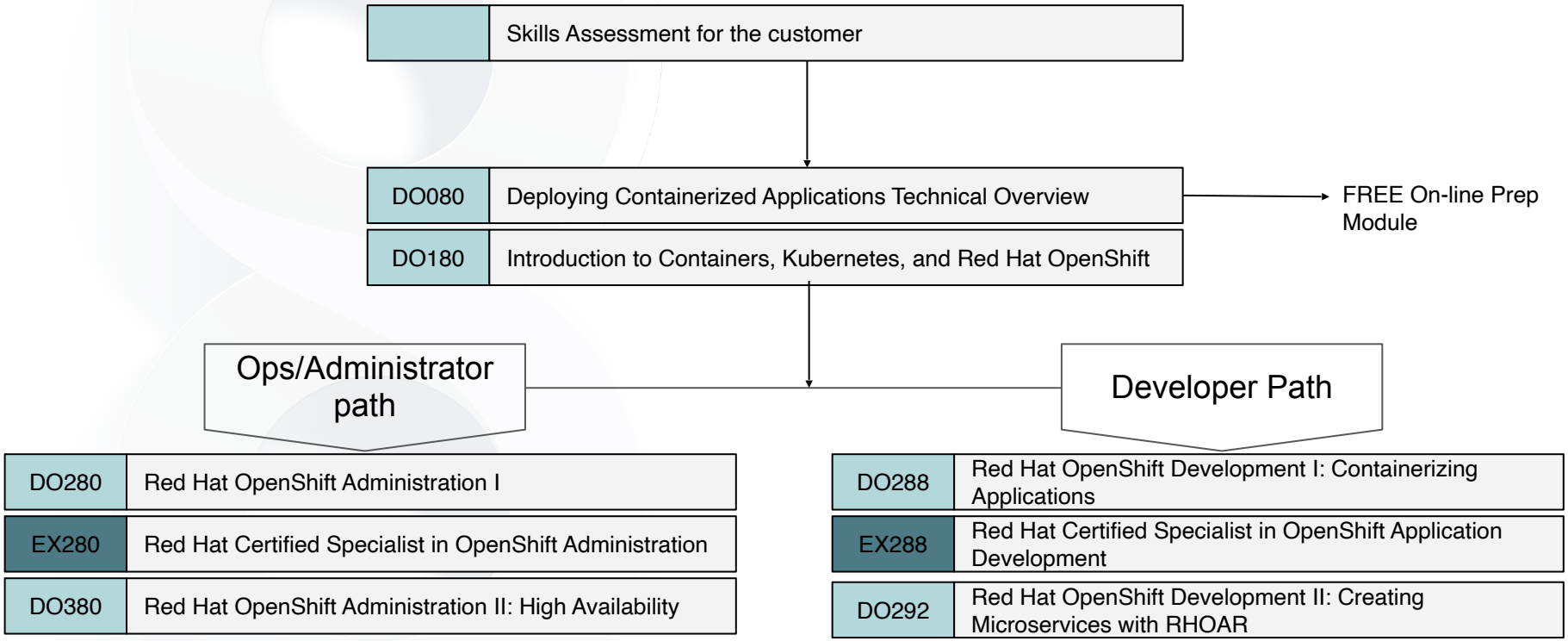
Use CLIs direct from web console, and fully authenticated when you need them.

- oc, odo, kubectl
- Terminal can be minimized and opened in new tab
- History is not retained between sessions
- Not supported for cluster admins
- Operator enabled
- Available in first z stream



Red Hat

Unlock the potential - get skilled



Red Hat

RED HAT LEARNING SUBSCRIPTION

BASIC, STANDARD & DEVELOPER

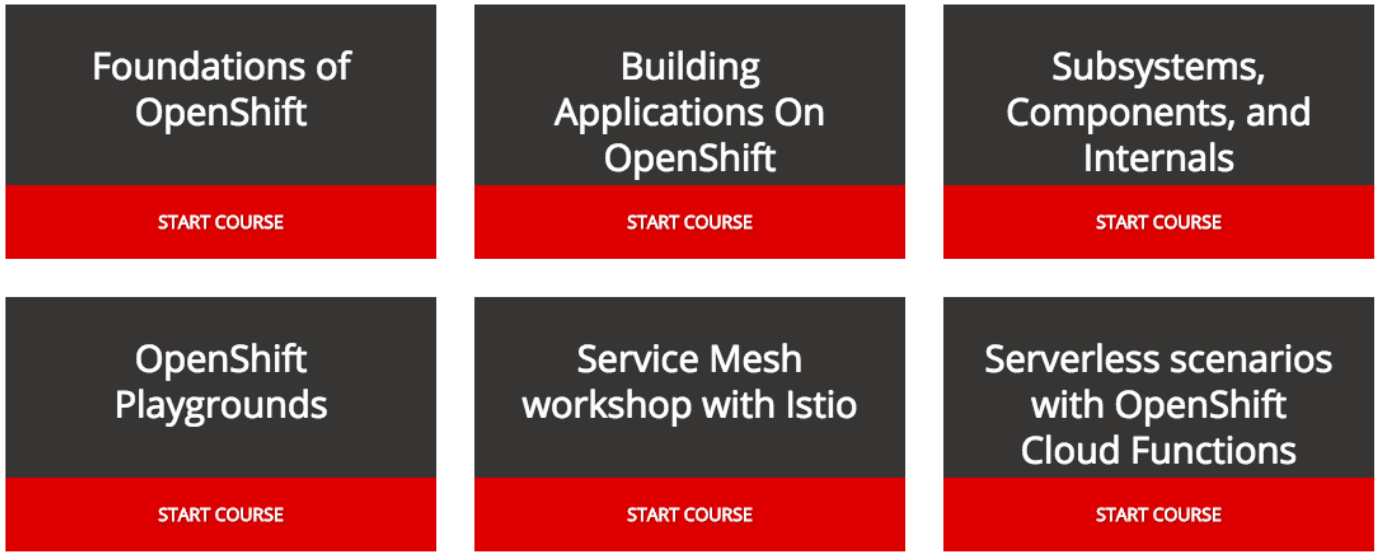
	Online Red Hat courses	Hands-on labs	Instructor videos	Video courses	Expert seminars	Instructor office hours	Learning paths	Certification exams
BASIC	X	X	X	X				
DEVELOPER	X	X	X	X				X
STANDARD	X	X	X	X	X	X	X	X

Simple, flexible, on-demand training

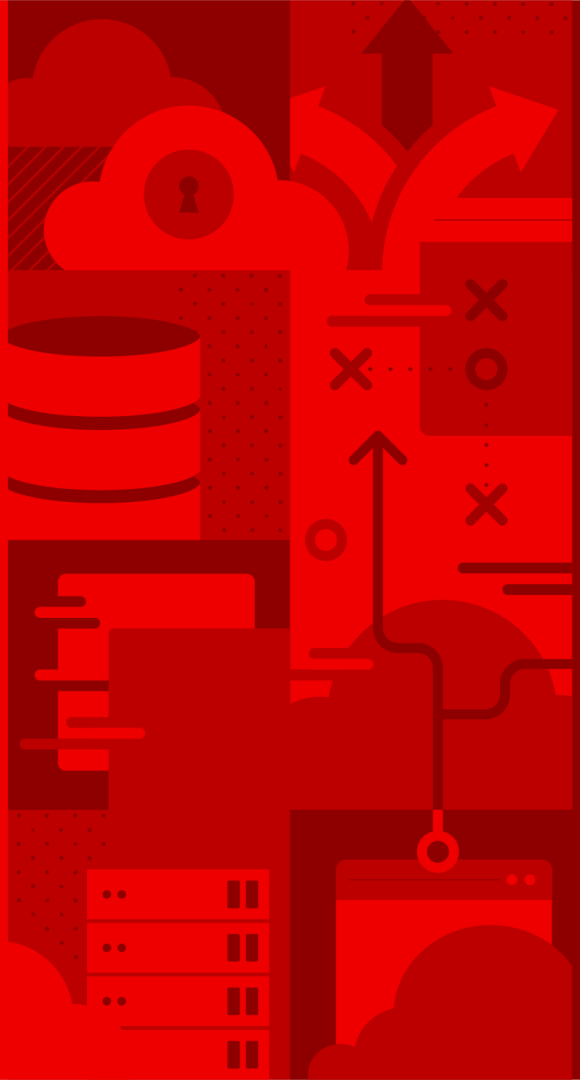
- Annual subscription offering, no prerequisite required
- On-demand access, 24 hours per day, 7 days per week, worldwide
- Includes Red Hat online and video Training courses and hands-on labs
- Interactive learning interface allows users and managers to track progress

Red Hat

LEARN.OPENSHIFT.COM

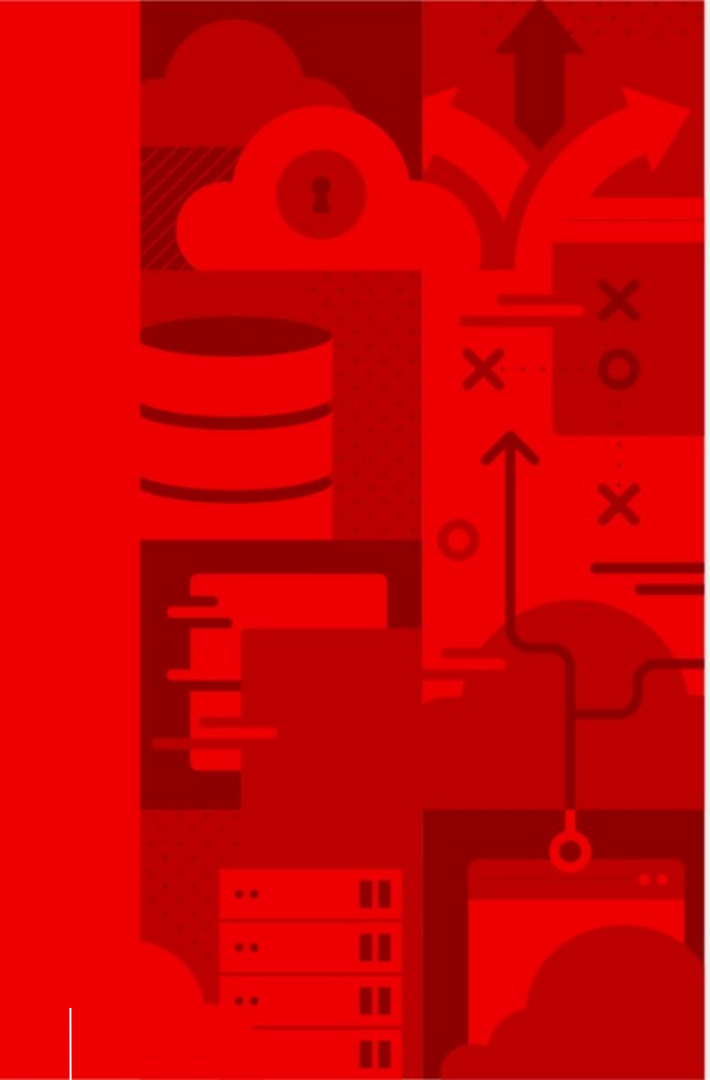


Interactive Learning Scenarios provide you with a pre-configured OpenShift instance, accessible from your browser without any downloads or configuration.



Demo

Red Hat



Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat