



# OPENShift CONTAINER PLATFORM

TECHNICAL OVERVIEW



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



[twitter.com/RedHat](https://twitter.com/RedHat)

JOSHUA SMITH  
SOLUTION ARCHITECT





# Why This Matters

# APP DELIVERY: SPEED AND STABILITY

## SPEED

- Manual builds and deployment

## STABILITY

- Manual builds and deployment

# APP DELIVERY: SPEED AND STABILITY

## SPEED

- Manual builds and deployment
- Rebuilding between environments

## STABILITY

- Manual builds and deployment
- Differences between environments

# APP DELIVERY: SPEED AND STABILITY

## SPEED

- Manual builds and deployment
- Rebuilding between environments
- Waiting for infrastructure

## STABILITY

- Manual builds and deployment
- Differences between environments
- Over-capacity infrastructure

# APP DELIVERY: SPEED AND STABILITY

## SPEED

- Manual builds and deployment
- Rebuilding between environments
- Waiting for infrastructure
- Clunky division of manual tasks

## STABILITY

- Manual builds and deployment
- Differences between environments
- Over-capacity infrastructure
- Clunky division of manual tasks

# APP DELIVERY: SPEED AND STABILITY

## SPEED

- Manual builds and deployment
- Rebuilding between environments
- Waiting for infrastructure
- Clunky division of manual tasks
- Complicated builds

## STABILITY

- Manual builds and deployment
- Differences between environments
- Over-capacity infrastructure
- Clunky division of manual tasks
- Complicated builds

# APP DELIVERY: SPEED AND STABILITY

## SPEED

- Manual builds and deployment
- Rebuilding between environments
- Waiting for infrastructure
- Clunky division of manual tasks
- Complicated builds
- Waiting for deploy outages

## STABILITY

- Manual builds and deployment
- Differences between environments
- Over-capacity infrastructure
- Clunky division of manual tasks
- Complicated builds
- Deploy outages

# APP DELIVERY: SPEED AND STABILITY

## PAIN

- Manual builds and deployment
- Rebuilding between environments
- Waiting for infrastructure
- Clunky division of manual tasks
- Complicated builds
- Waiting for deploy outages

## STABILITY

- Manual builds and deployment
- Differences between environments
- Over-capacity infrastructure
- Clunky division of manual tasks
- Complicated builds
- Deploy outages

# APP DELIVERY: SPEED AND STABILITY

## PAIN

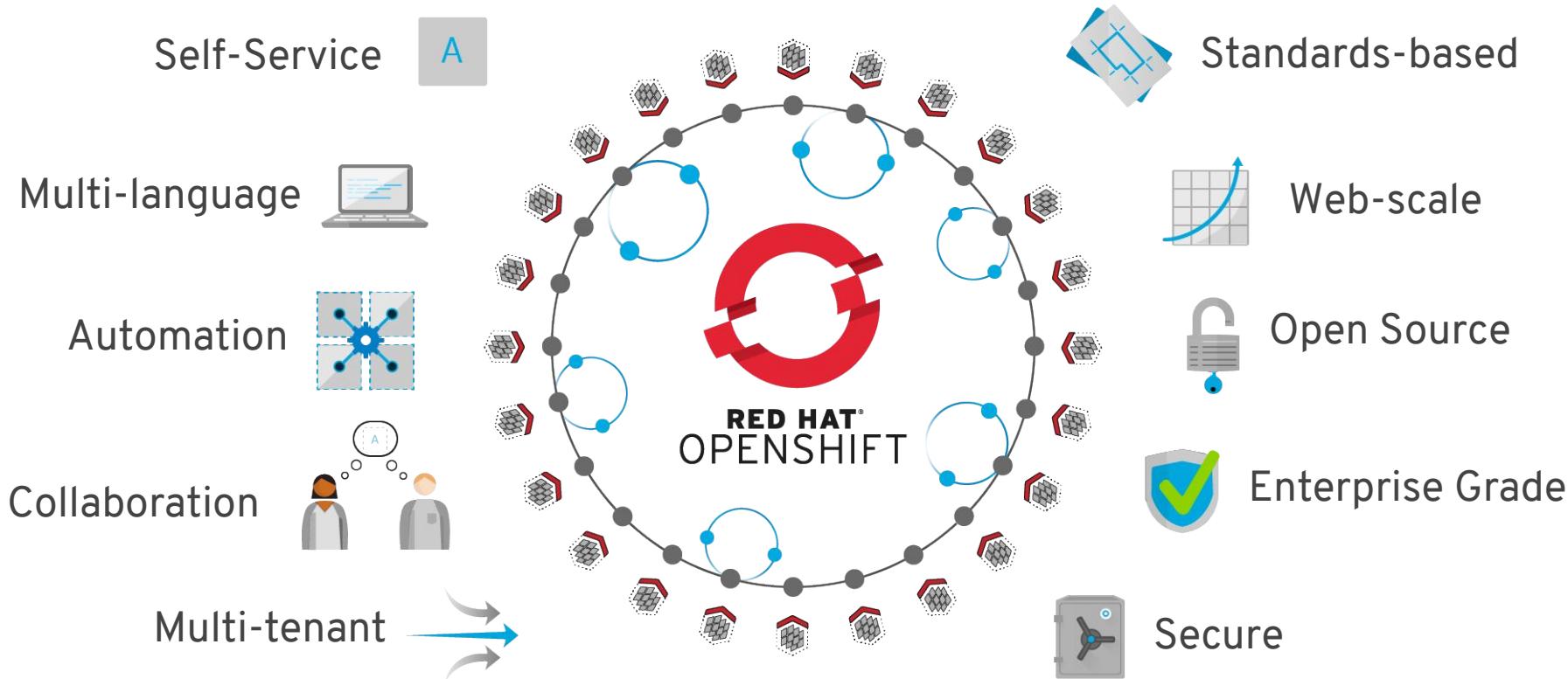
- Manual builds and deployment
- Rebuilding between environments
- Waiting for infrastructure
- Clunky division of manual tasks
- Complicated builds
- Waiting for deploy outages

## IN-STABILITY

- Manual builds and deployment
- Differences between environments
- Over-capacity infrastructure
- Clunky division of manual tasks
- Complicated builds
- Deploy outages



# OpenShift Introduction



### 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

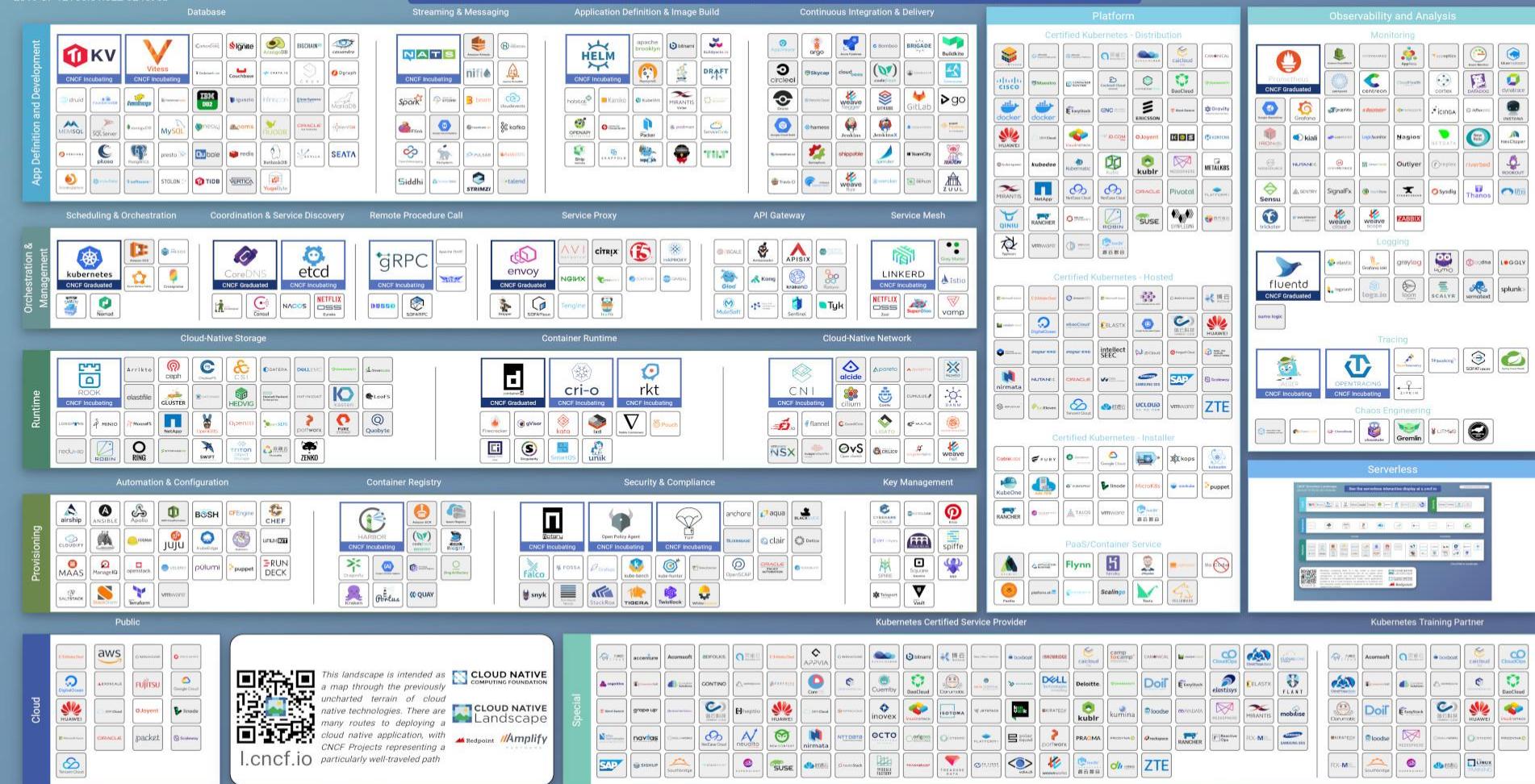
Kubernetes

Red Hat Enterprise Linux | RHEL CoreOS

Best IT Ops Experience

CaaS  $\longleftrightarrow$  PaaS  $\longleftrightarrow$  FaaS

Best Developer Experience



# By the Numbers...



**531%**  
5-year ROI

**66%**

Faster development  
life cycle

**36%**

More applications  
per year

**8 MONTHS**

Payback  
period

**US\$1.29M**

Average annual  
benefits per  
100 developers

The Business Value of Red Hat OpenShift, IDC #US41845816, October 2017,  
<https://www.redhat.com/en/resources/The-Business-Value-of-Red-Hat-OpenShift>.



**10x**

Increased application development throughput from 20 to 200 changes a day

**OpenShift on AWS & private cloud**

The Hilton logo, featuring the word "Hilton" in a large, bold, serif font inside a black rectangular border.

**Months → Days**

Improved time to market by accelerating development time

**OpenShift on AWS**

**50%**

Reduction in development time for new services and APIs. Launched a new cloud platform in 10 days

**OpenShift on AWS, Azure, & private cloud**



Source:

Cathay Pacific: Red Hat press release, [Cathay Pacific Takes Customer Experiences to New Heights with Red Hat's Hybrid Cloud Technologies](#), May 2018.

Hilton: Red Hat case study, [Hilton enhances digital guest experience with Red Hat container and automation technology](#), October 2018.

Schiphol: Red Hat case study, [Amsterdam Airport Schiphol builds agile cloud with Red Hat](#), August 2017.

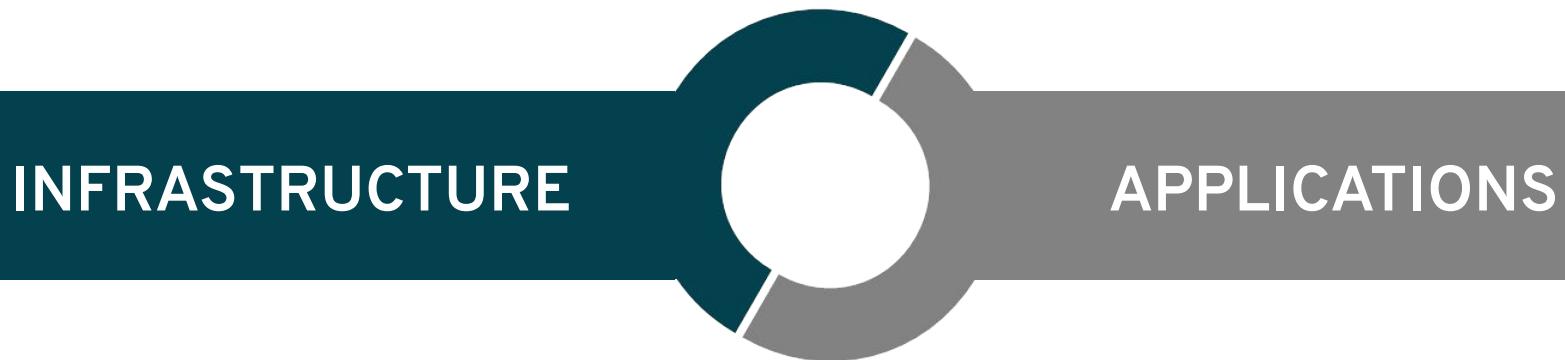




# Containers: Core Concepts

# WHAT ARE CONTAINERS?

It Depends Who You Ask

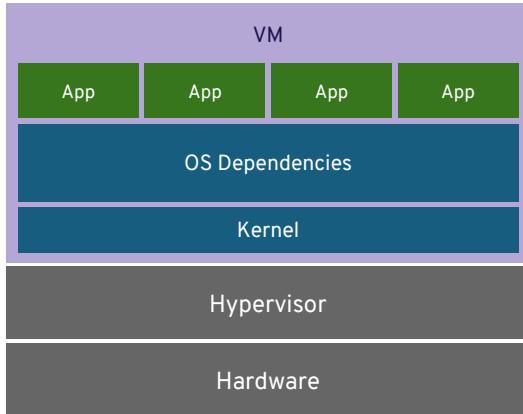


- Application processes on a shared kernel
- Simpler, lighter, and denser than VMs
- Portable across different environments
- Package apps with all dependencies
- Deploy to any environment in seconds
- Easily accessed and shared

*Both are correct!*

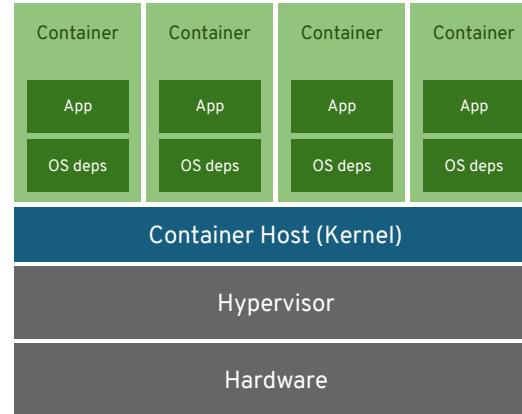
# VIRTUAL MACHINES VS. CONTAINERS

VIRTUAL MACHINES



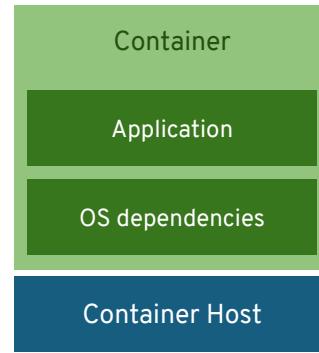
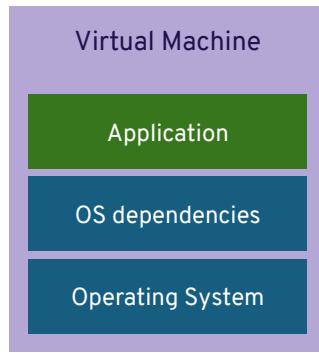
VM abstracts the hardware

CONTAINERS



Container isolates processes:  
abstracts OS *and* hardware

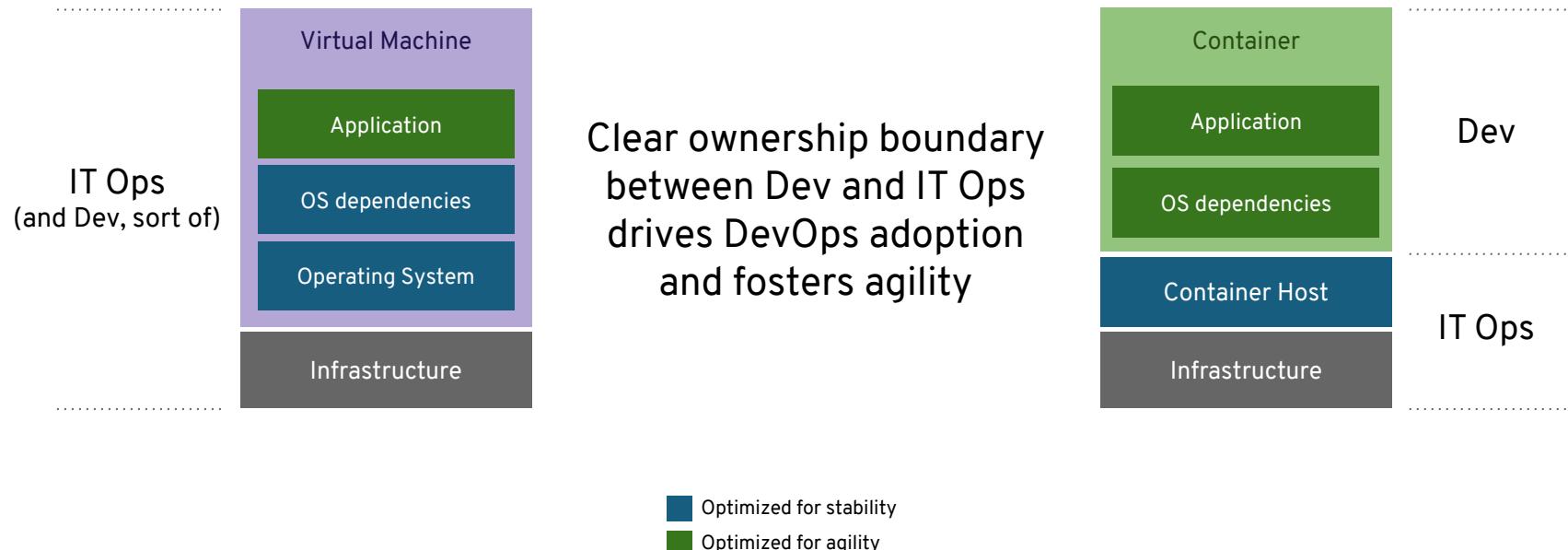
# VIRTUAL MACHINES AND CONTAINERS



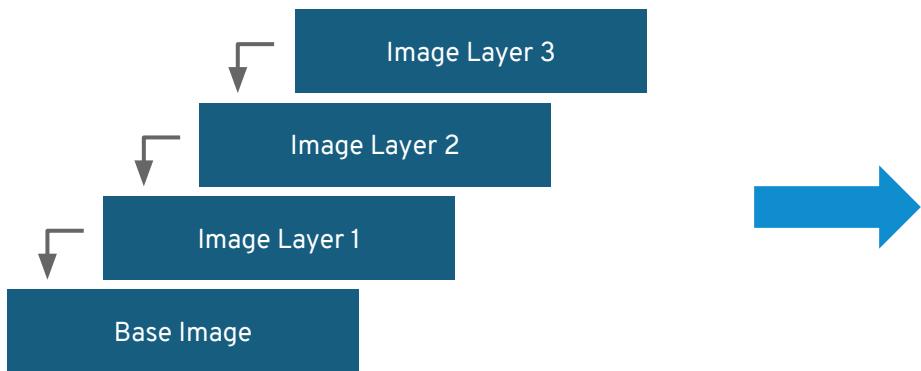
- + VM Isolation
- Complete OS
- Static Compute
- Static Memory
- High Resource Usage
- VM Drift

- + Container Isolation
- + Shared Kernel
- + Burstable Compute
- + Burstable Memory
- + Low Resource Usage
- + Build Once, Deploy Anywhere

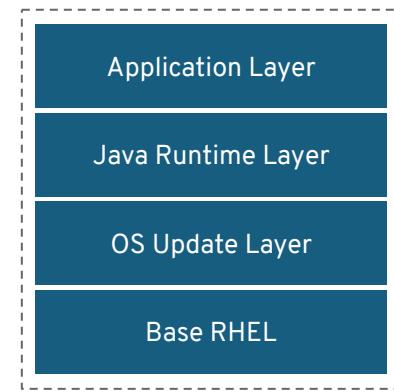
# VIRTUAL MACHINES VS. CONTAINERS



# RAPID SECURITY PATCHING USING CONTAINER IMAGE LAYERING



Container Image Layers



Example Container Image



# OpenShift and Kubernetes: Core Concepts

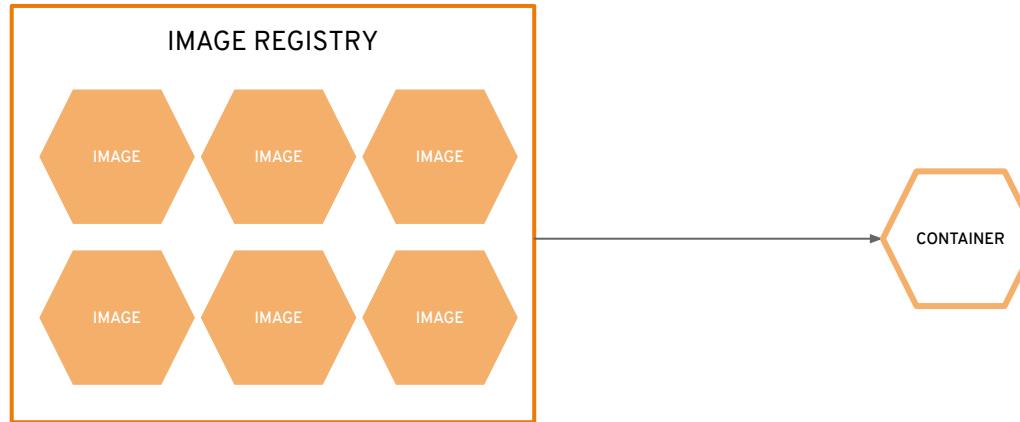
# a container is the smallest compute unit



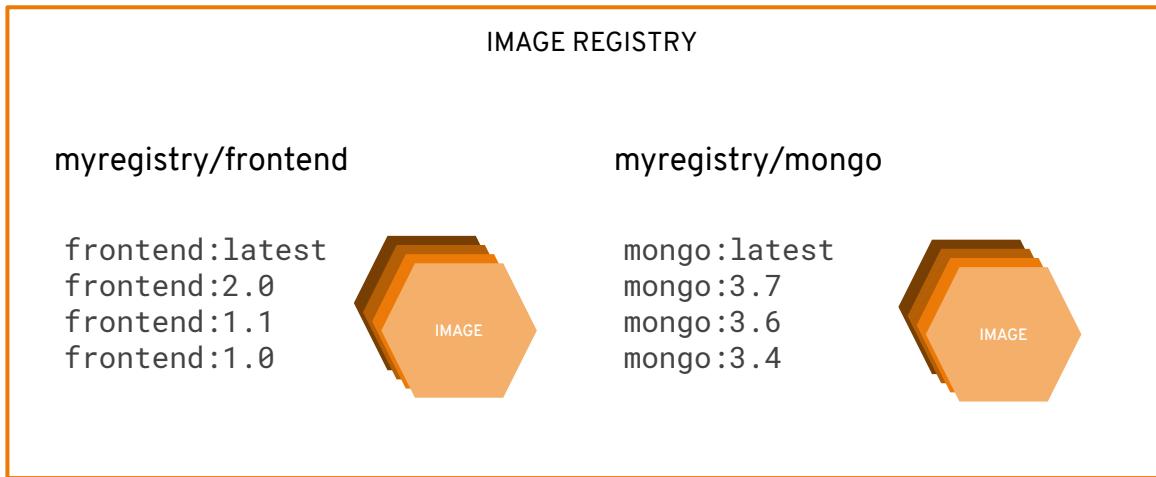
# containers are created from container images



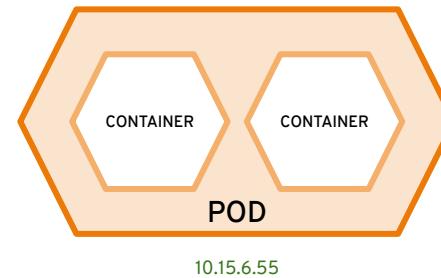
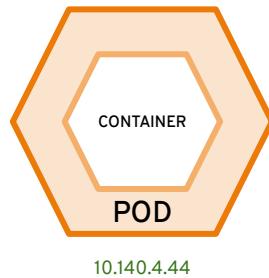
# container images are stored in an image registry



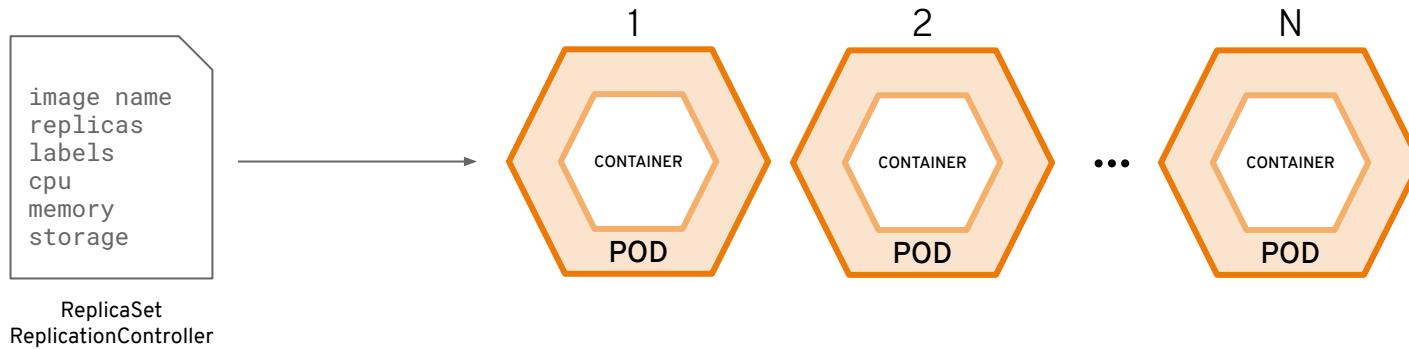
# an image repository contains all versions of an image in the image registry



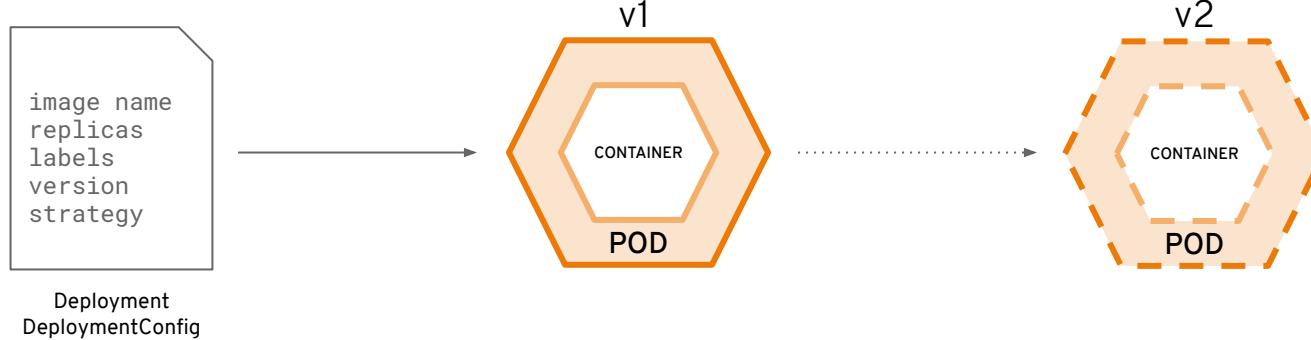
containers are wrapped in pods which are units of deployment and management



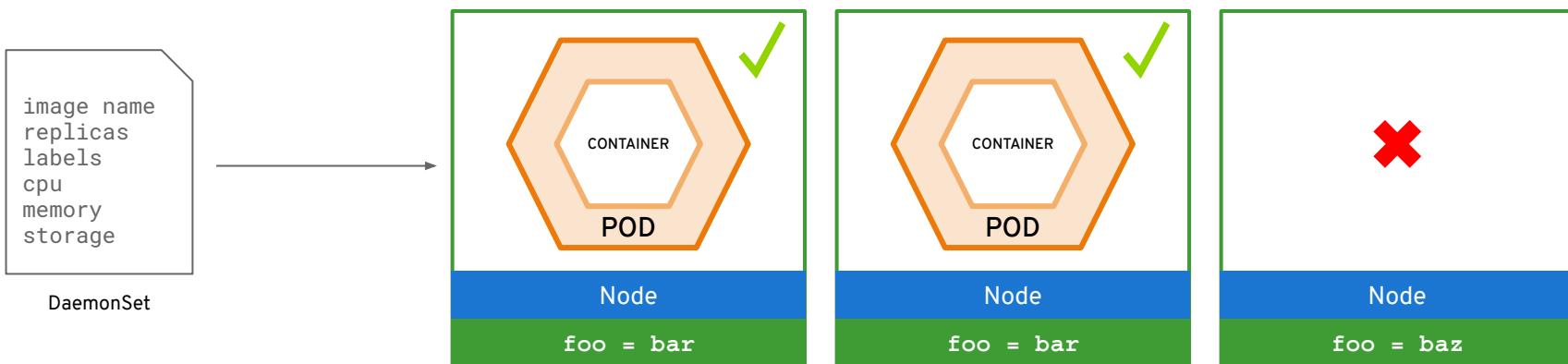
# ReplicationControllers & ReplicaSets ensure a specified number of pods are running at any given time



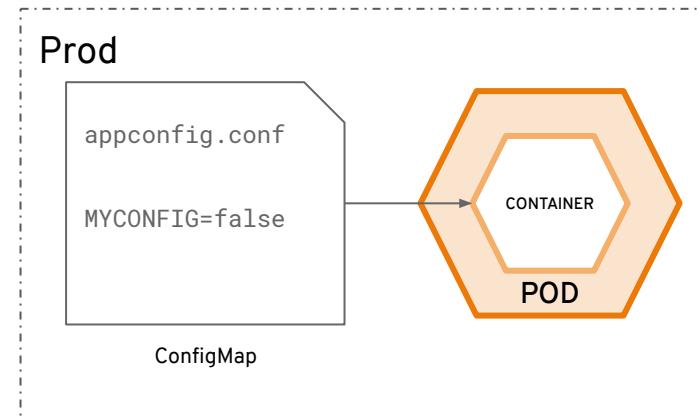
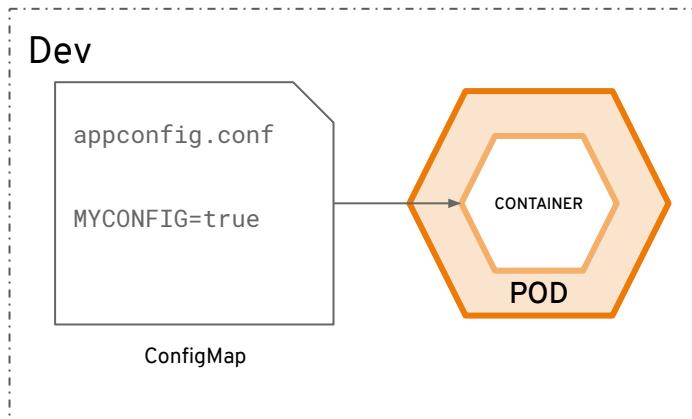
# Deployments and DeploymentConfigurations define how to roll out new versions of Pods



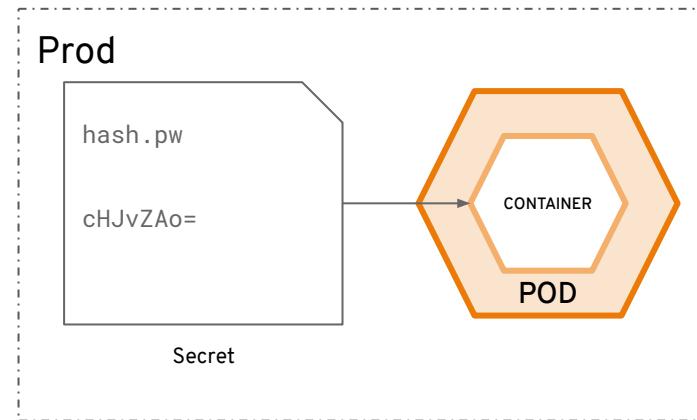
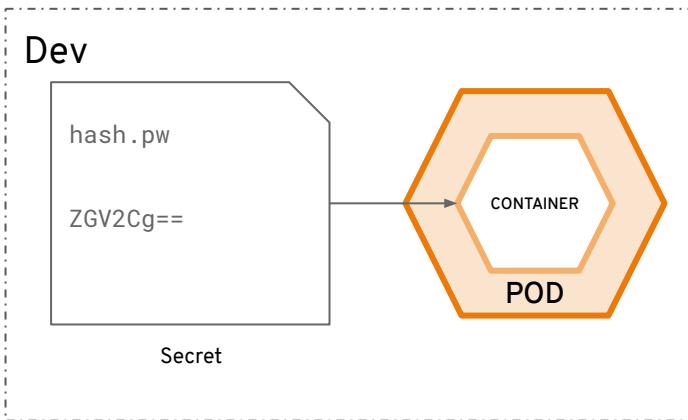
a daemonset ensures that all  
(or some) nodes run a copy of a pod



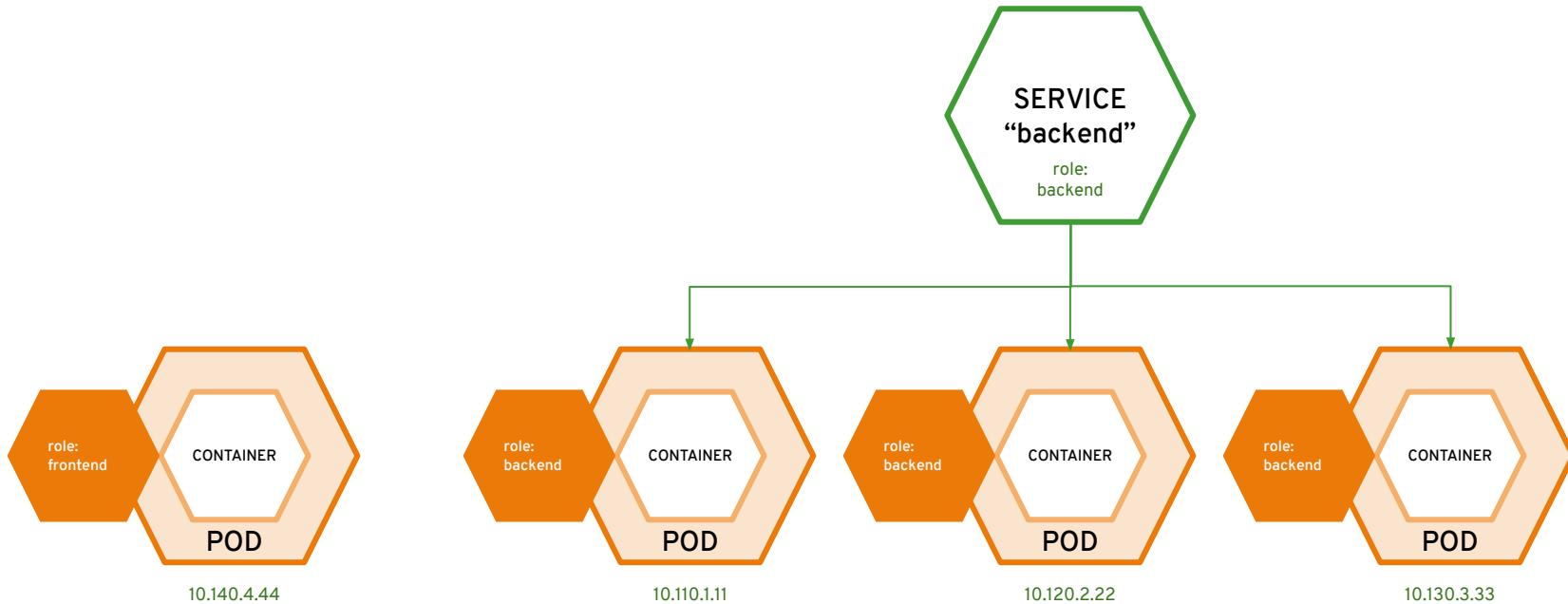
configmaps allow you to decouple configuration artifacts from image content (and application code!)



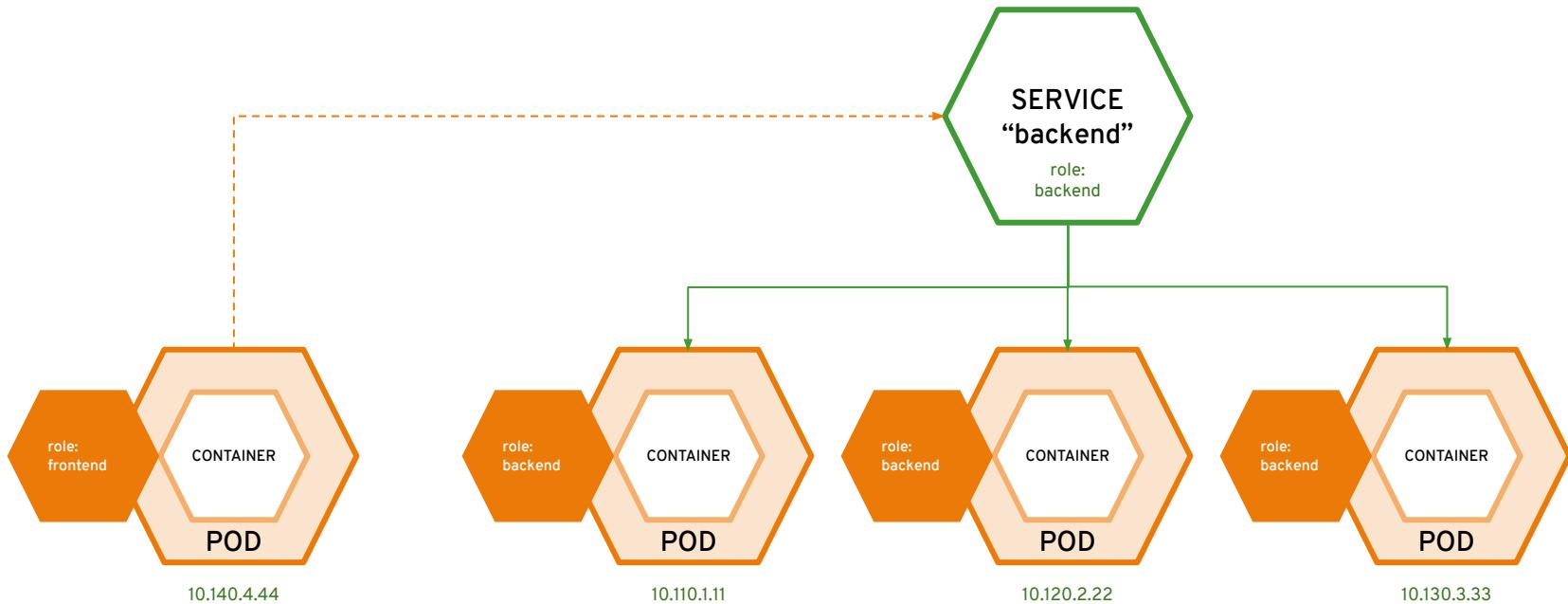
secrets provide a mechanism to hold sensitive information such as passwords



services provide internal load-balancing  
and service discovery across pods

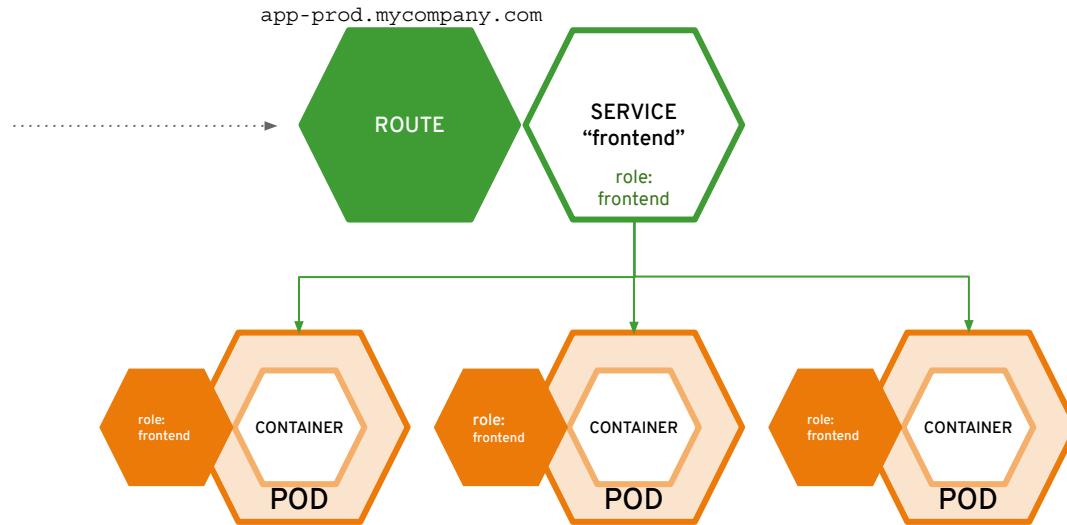


also, apps can talk to each other via services

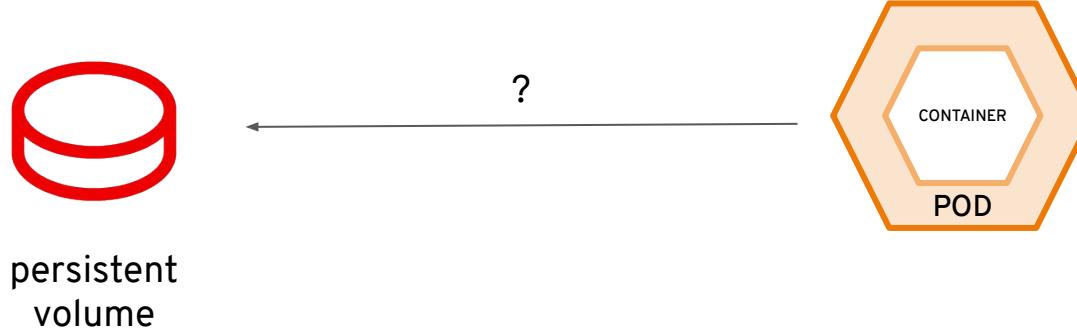


# routes make services accessible to clients outside the environment via real-world urls

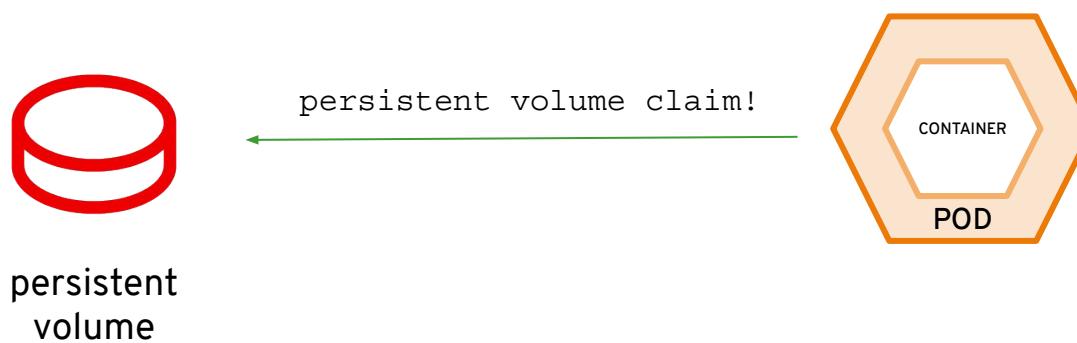
```
> curl http://app-prod.mycompany.com
```



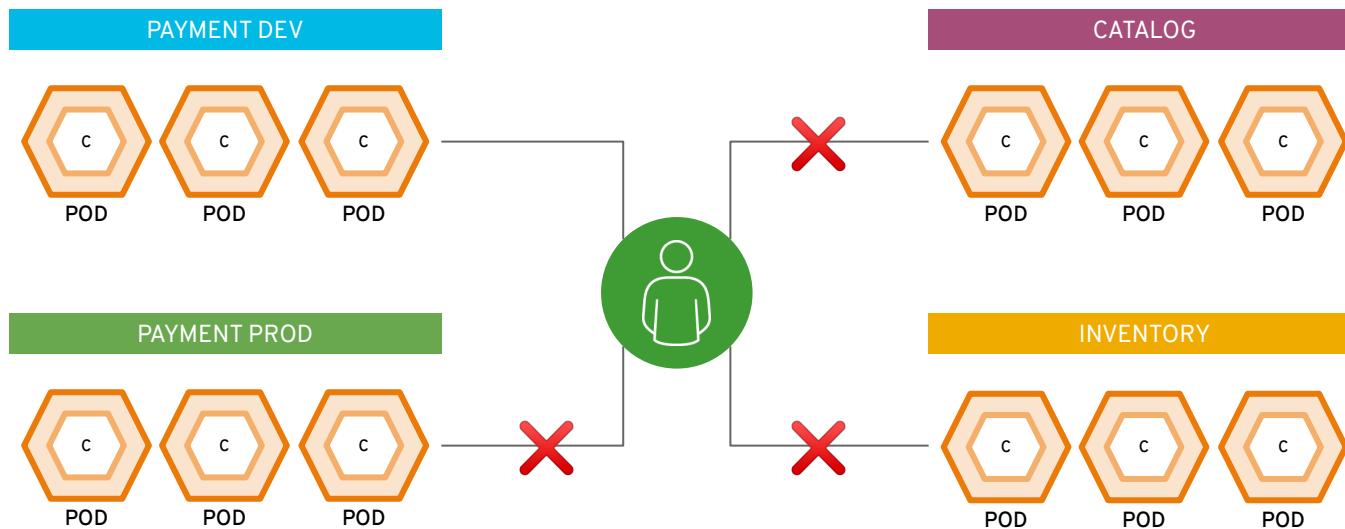
# Kubernetes storage



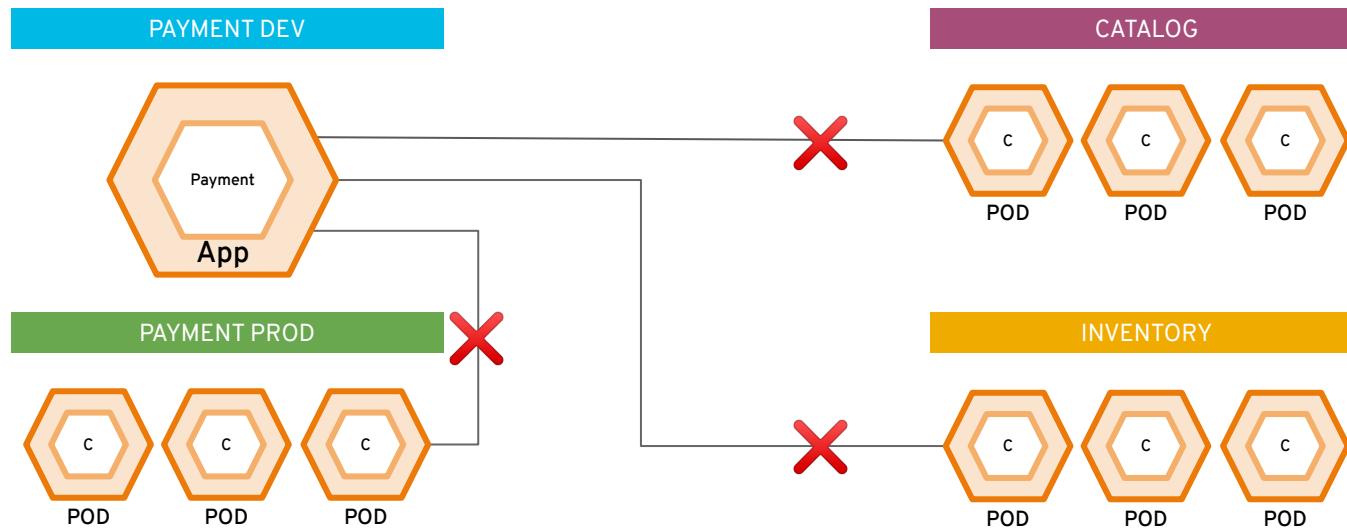
# Kubernetes storage



projects isolate **apps** across environments,  
teams, groups and departments



networking plugins isolate **app-to-app access** across environments, teams, groups and departments



# OpenShift 4 Architecture

# your choice of infrastructure

COMPUTE

NETWORK

STORAGE

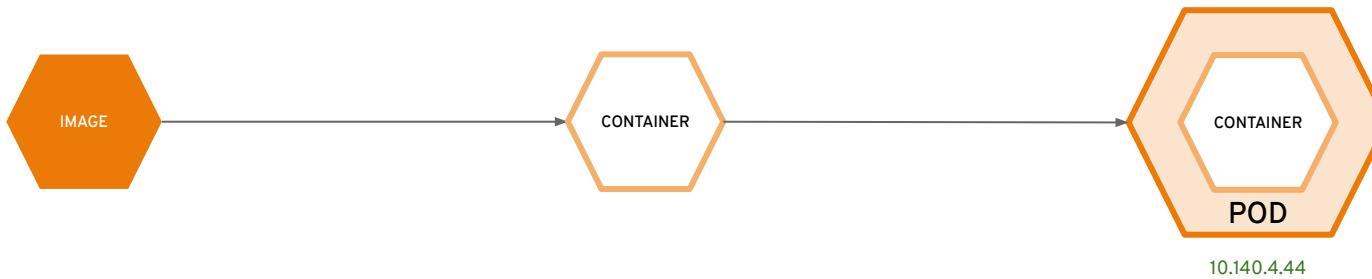
# workers run workloads



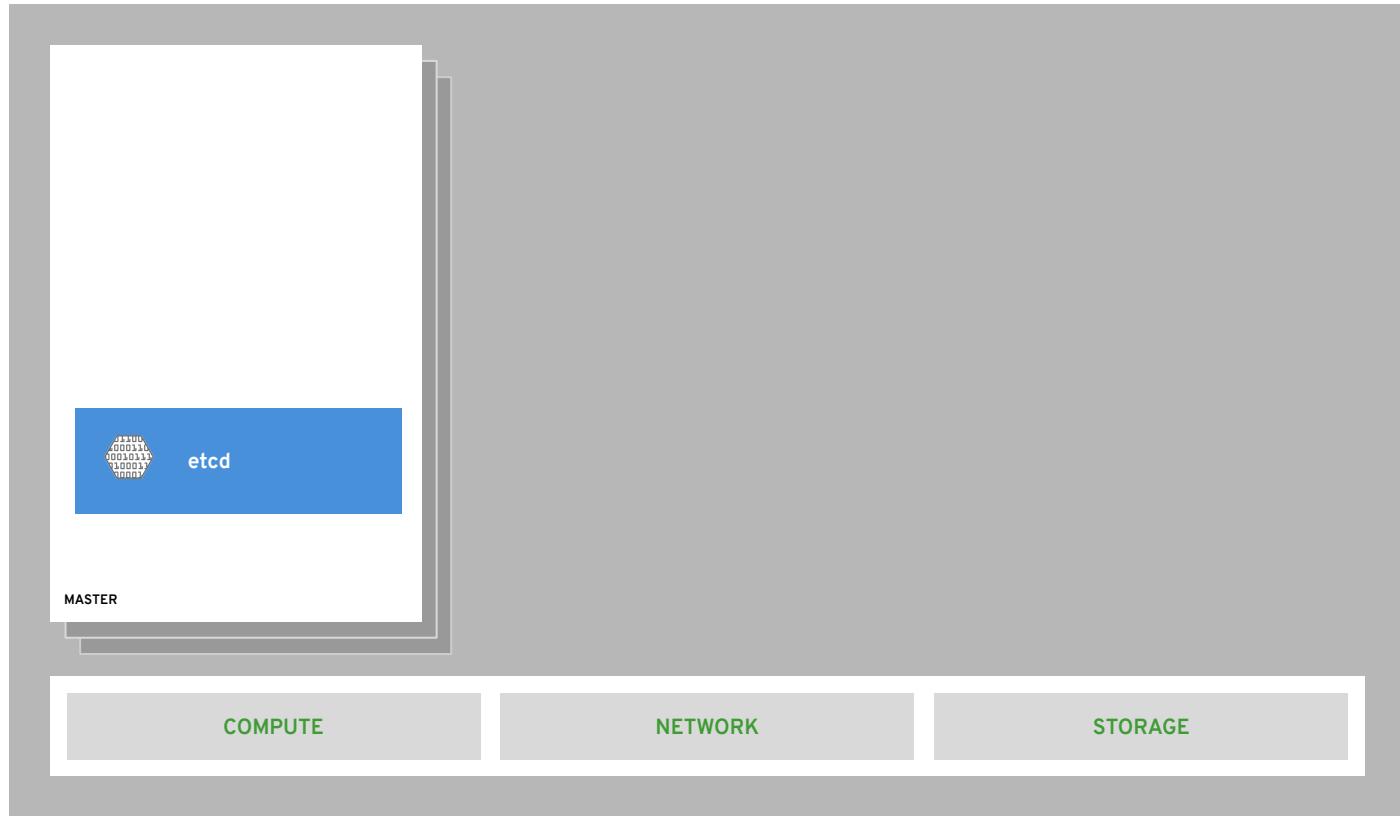
# masters are the control plane



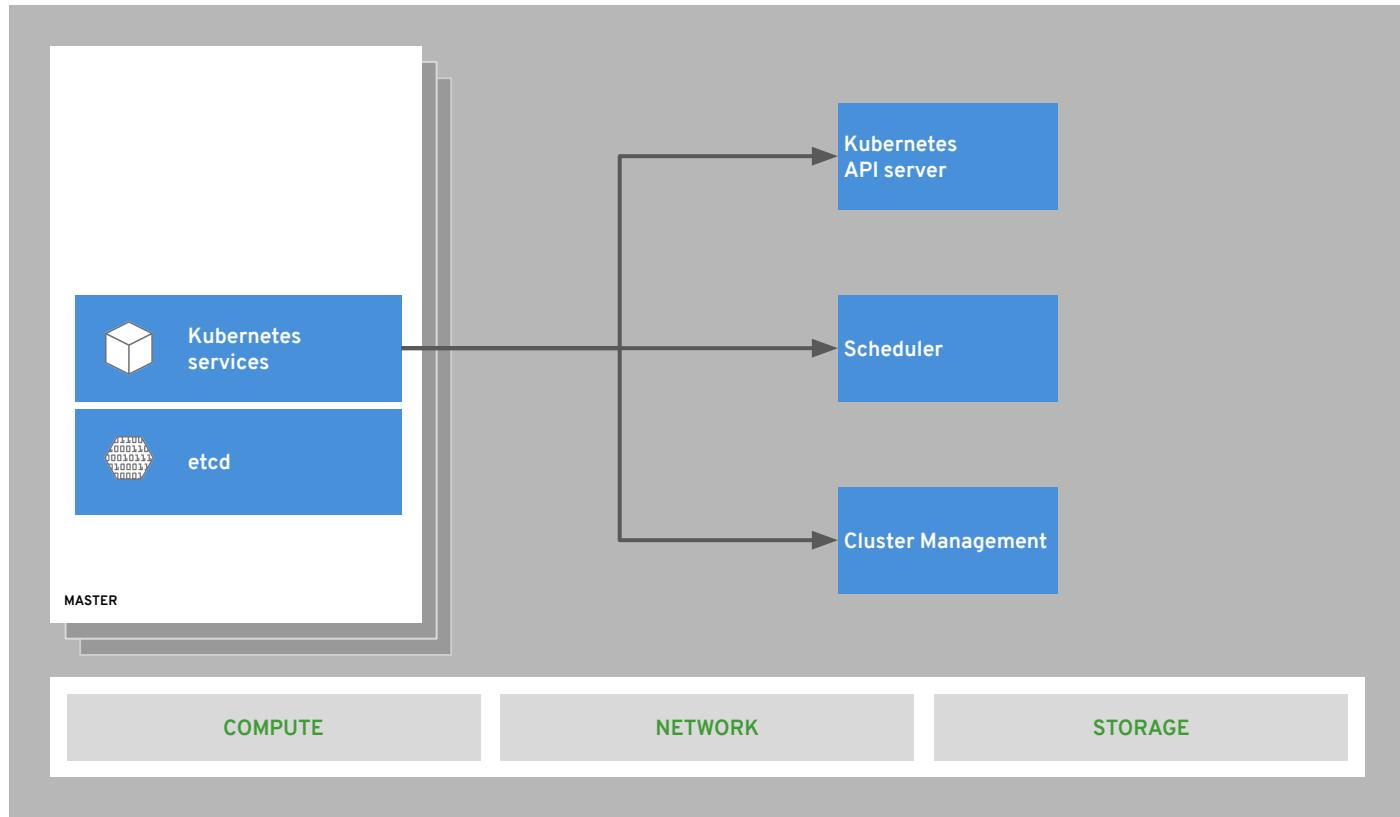
# everything runs in pods



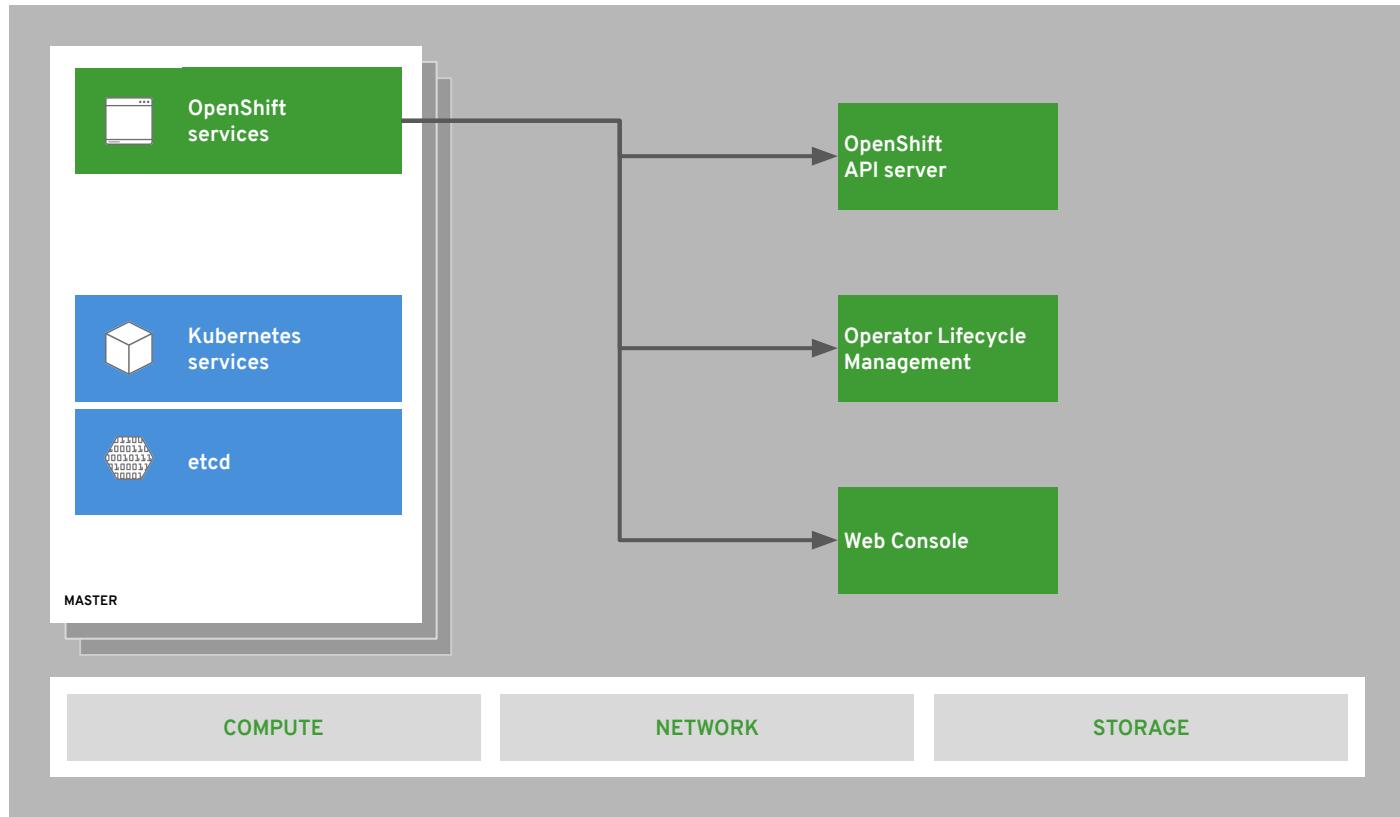
# state of everything



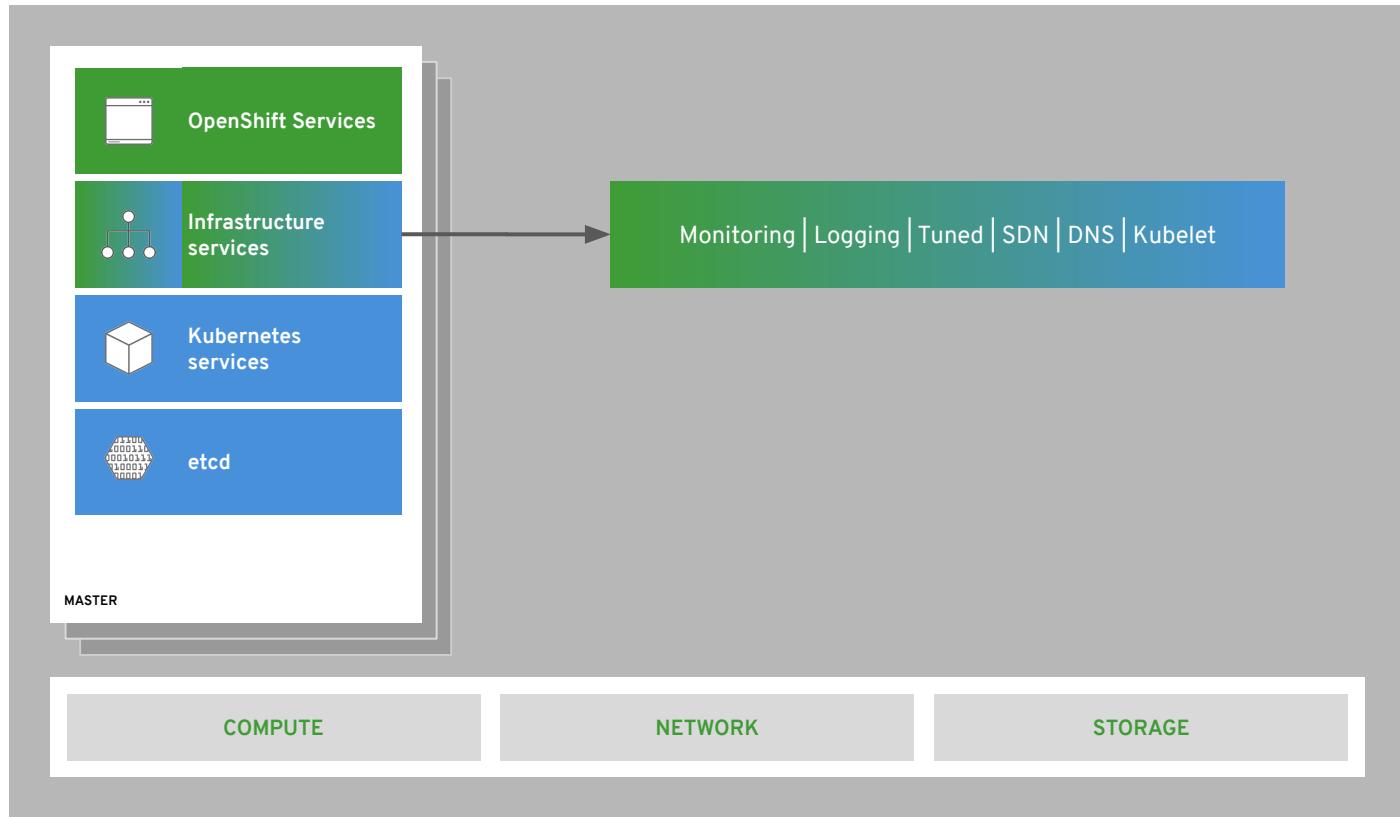
# core kubernetes components



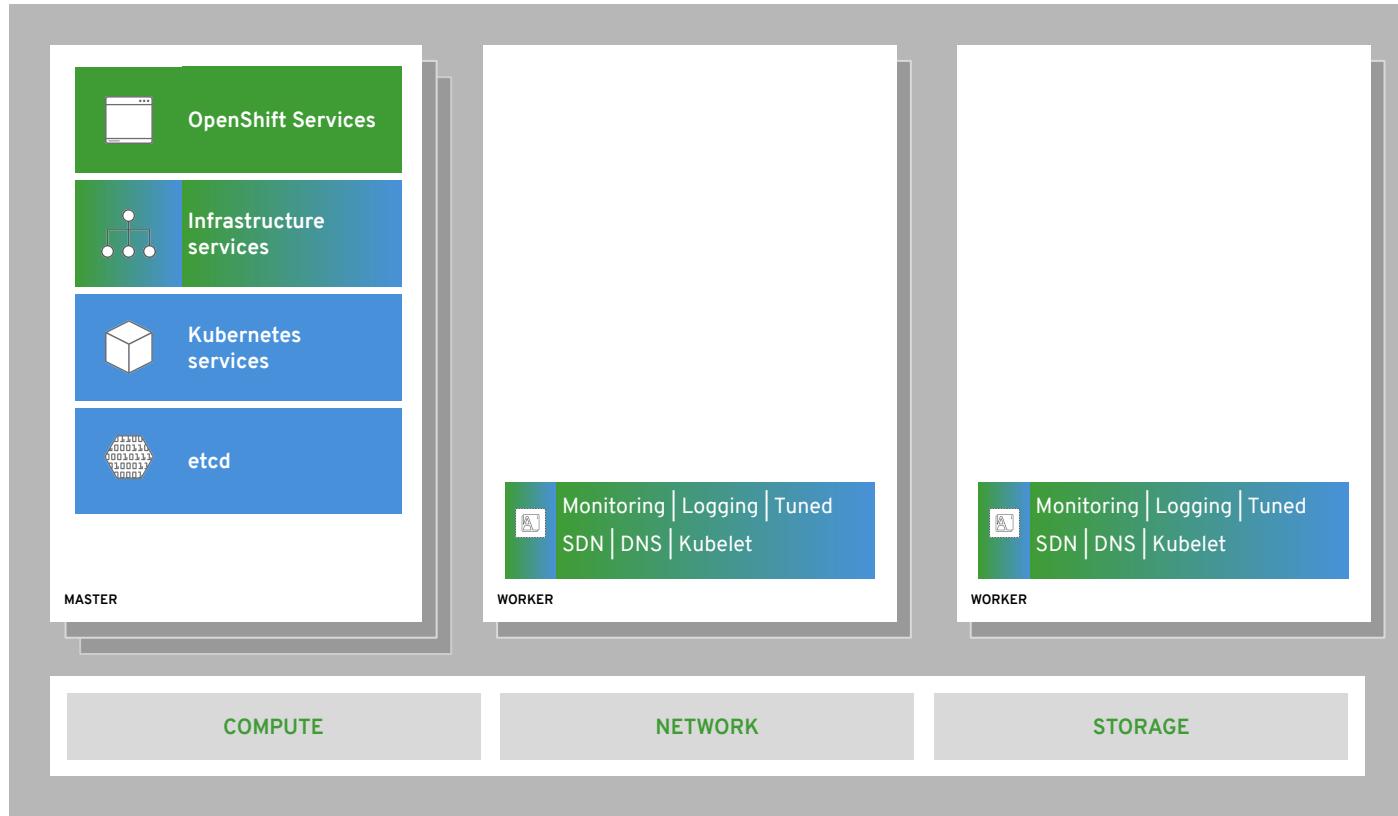
# core OpenShift components



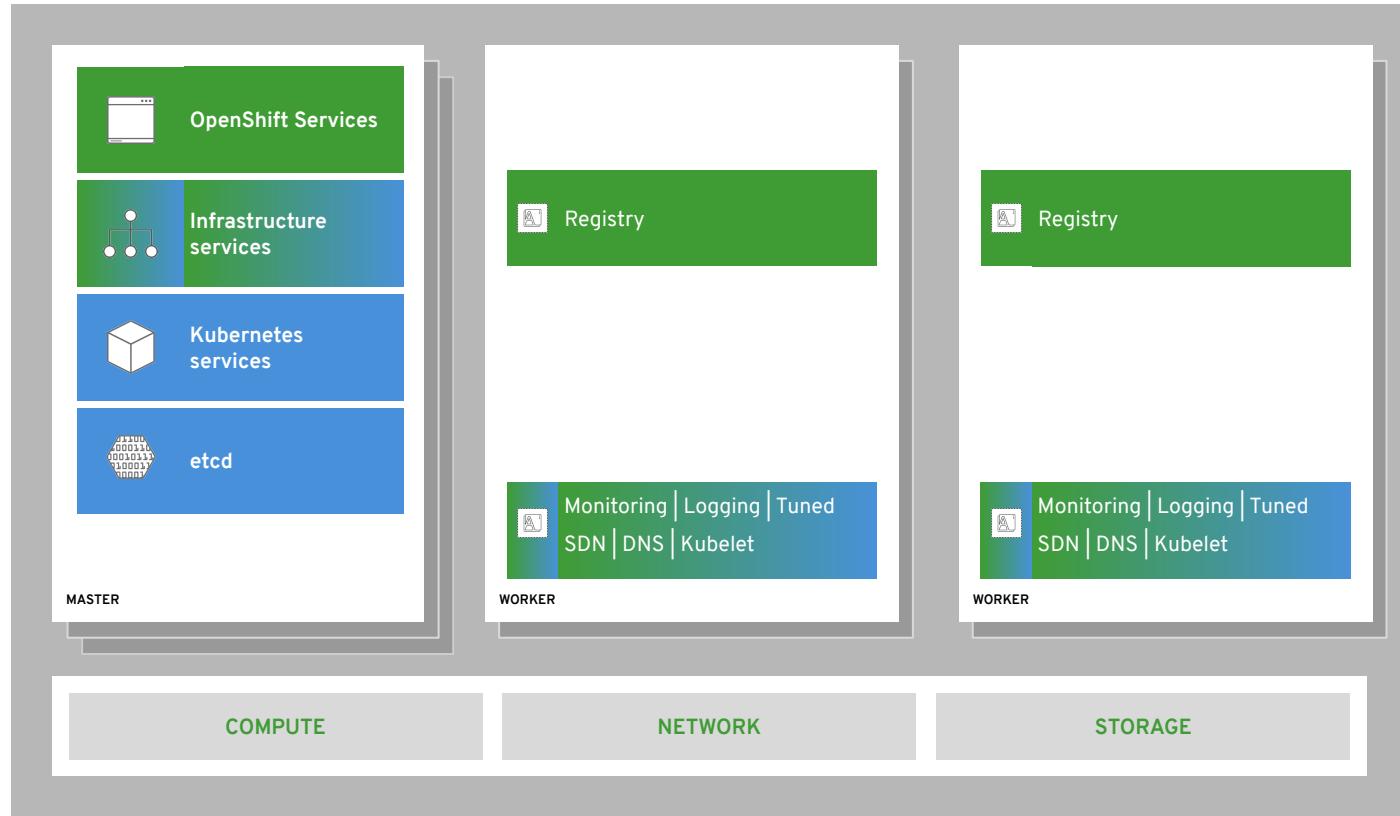
# internal and support infrastructure services



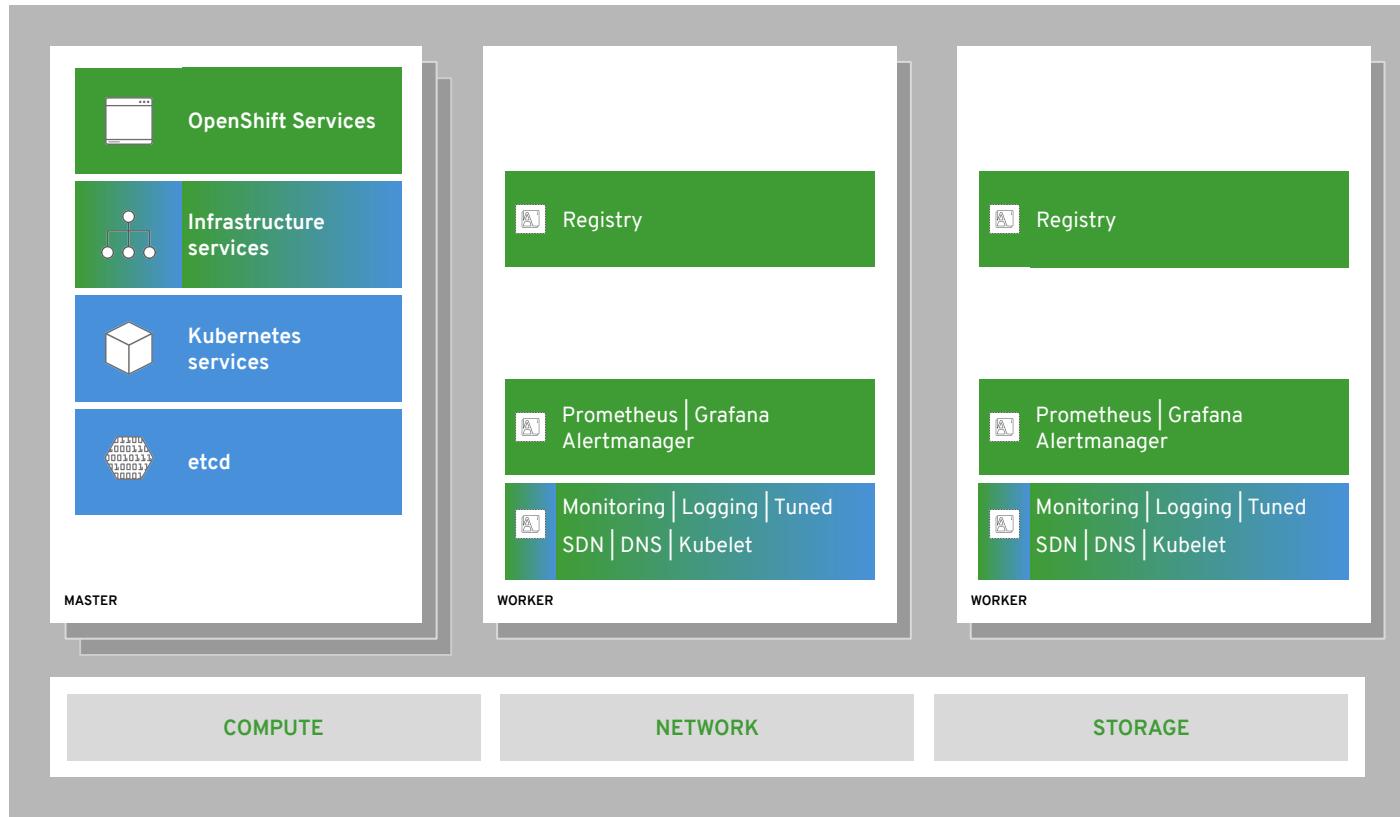
run on all hosts



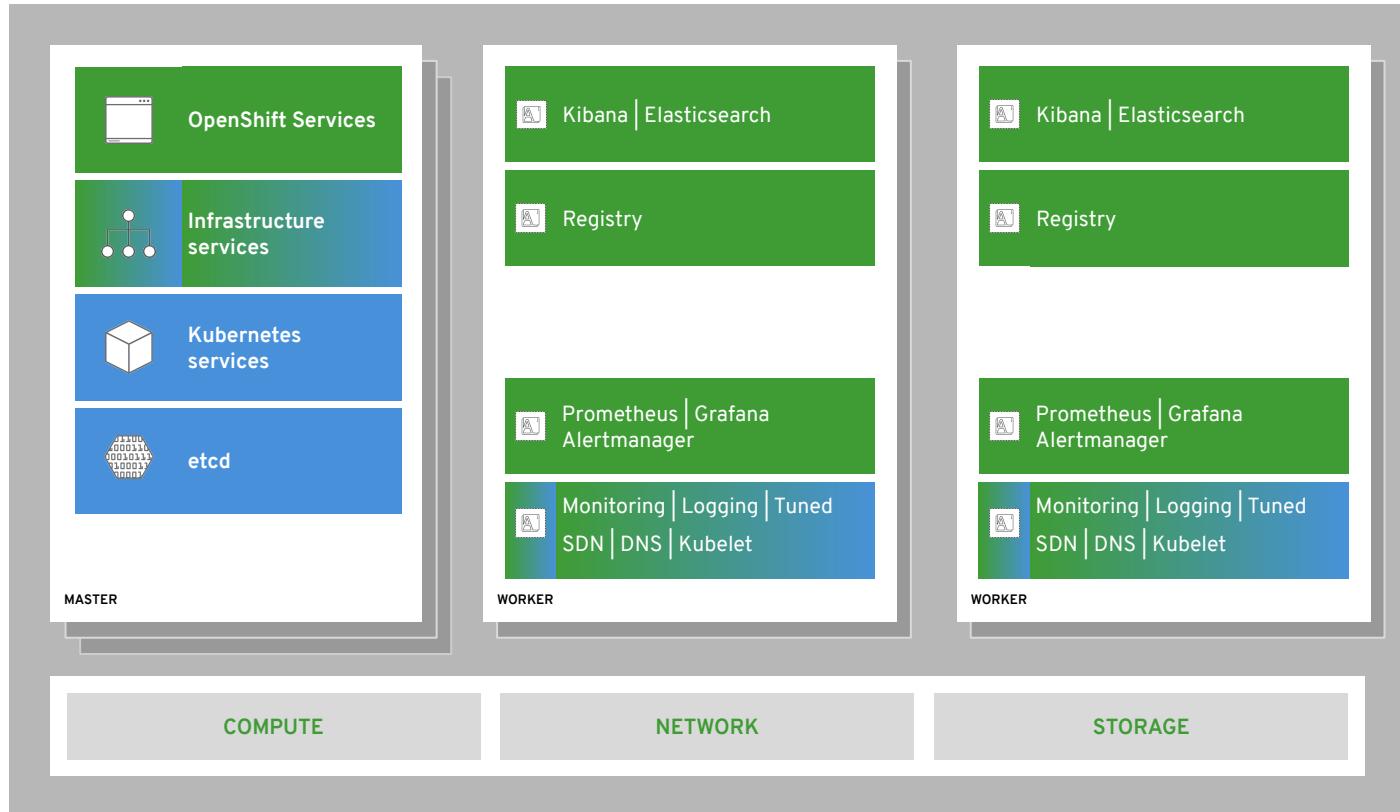
# integrated image registry



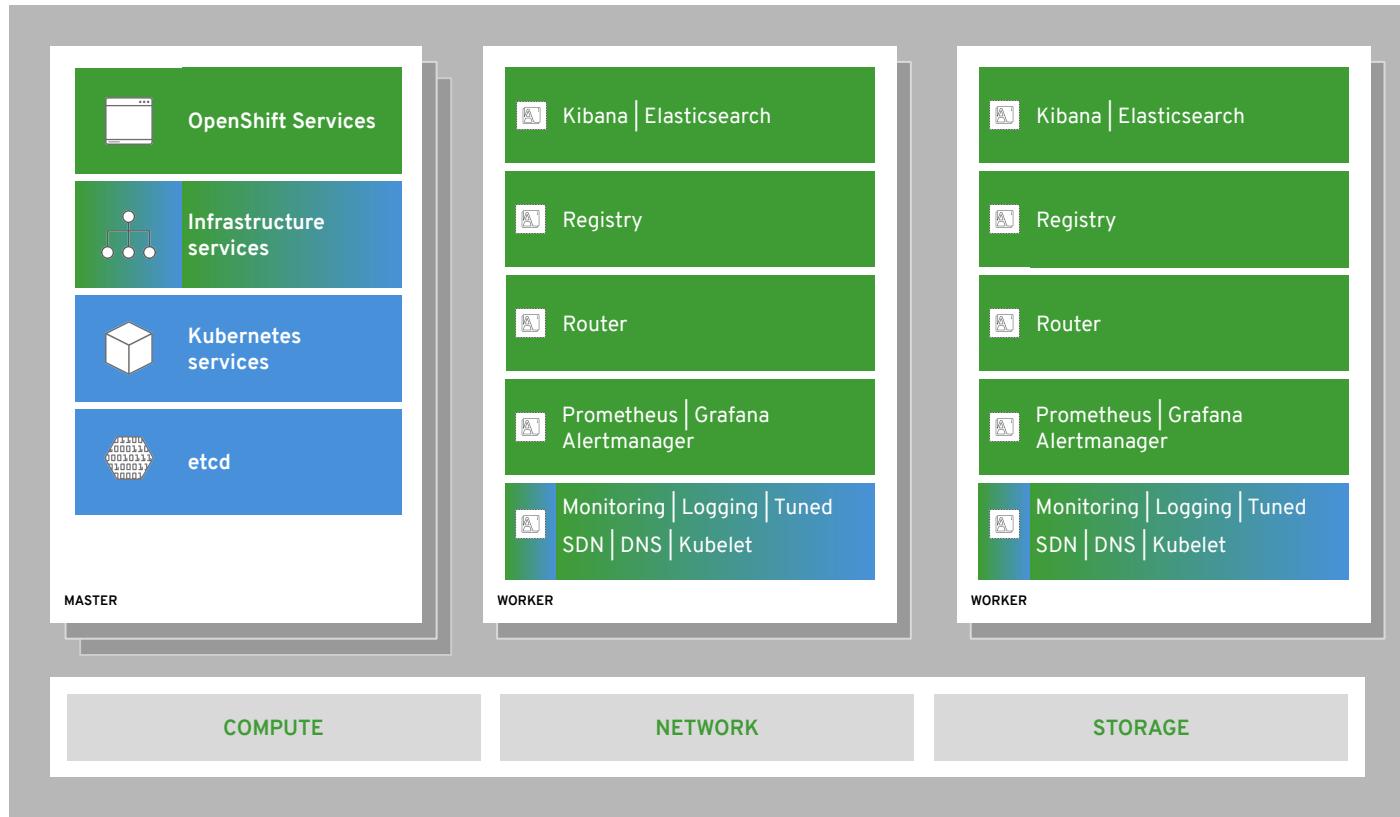
# cluster monitoring



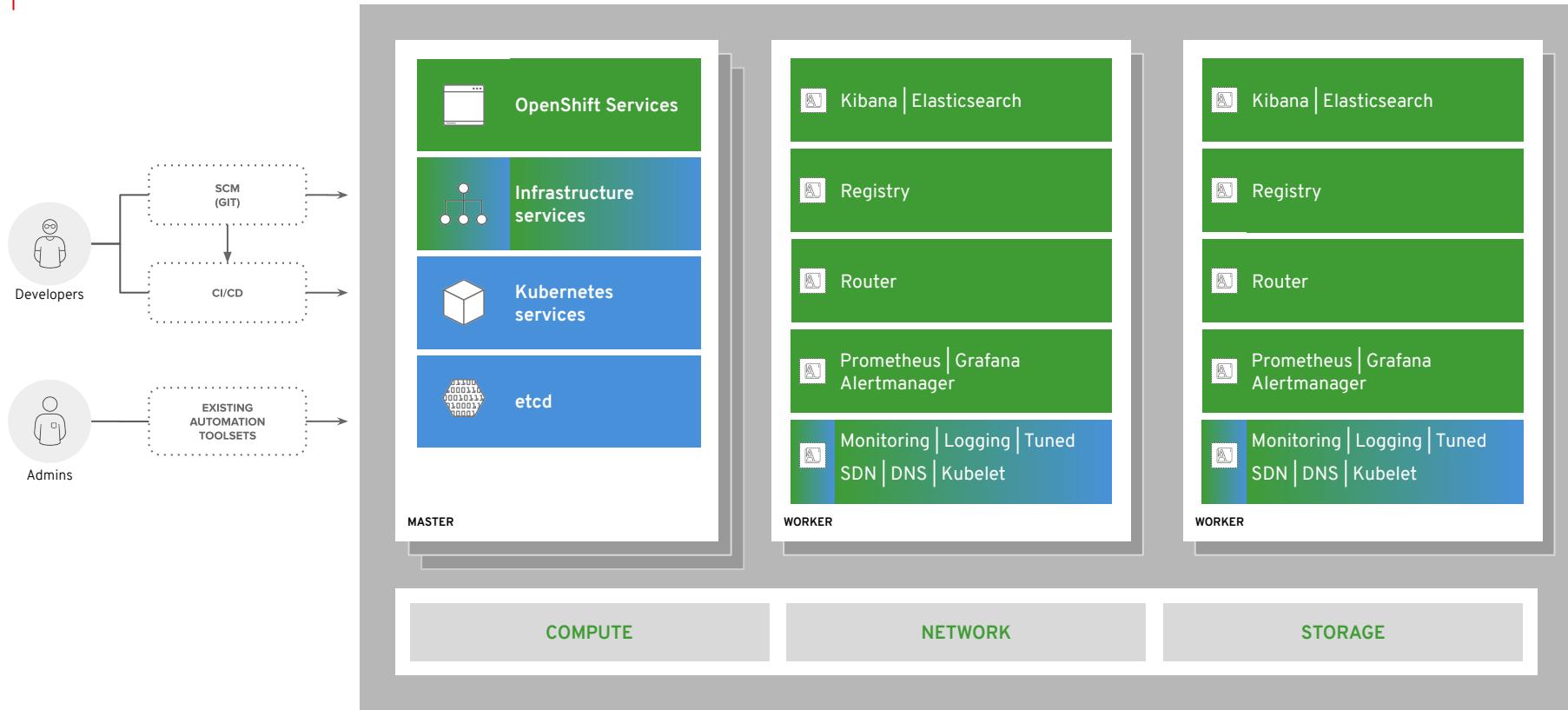
# log aggregation



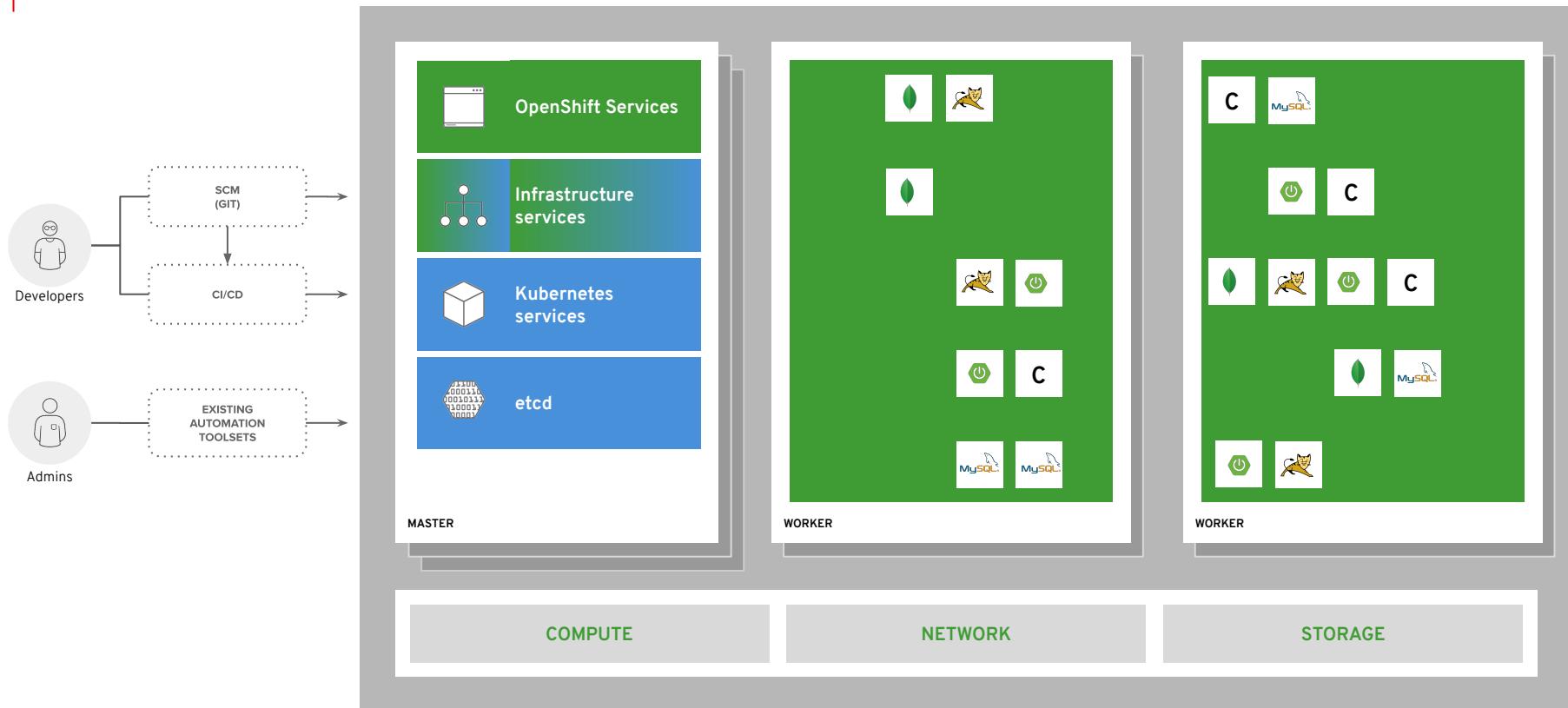
# integrated routing



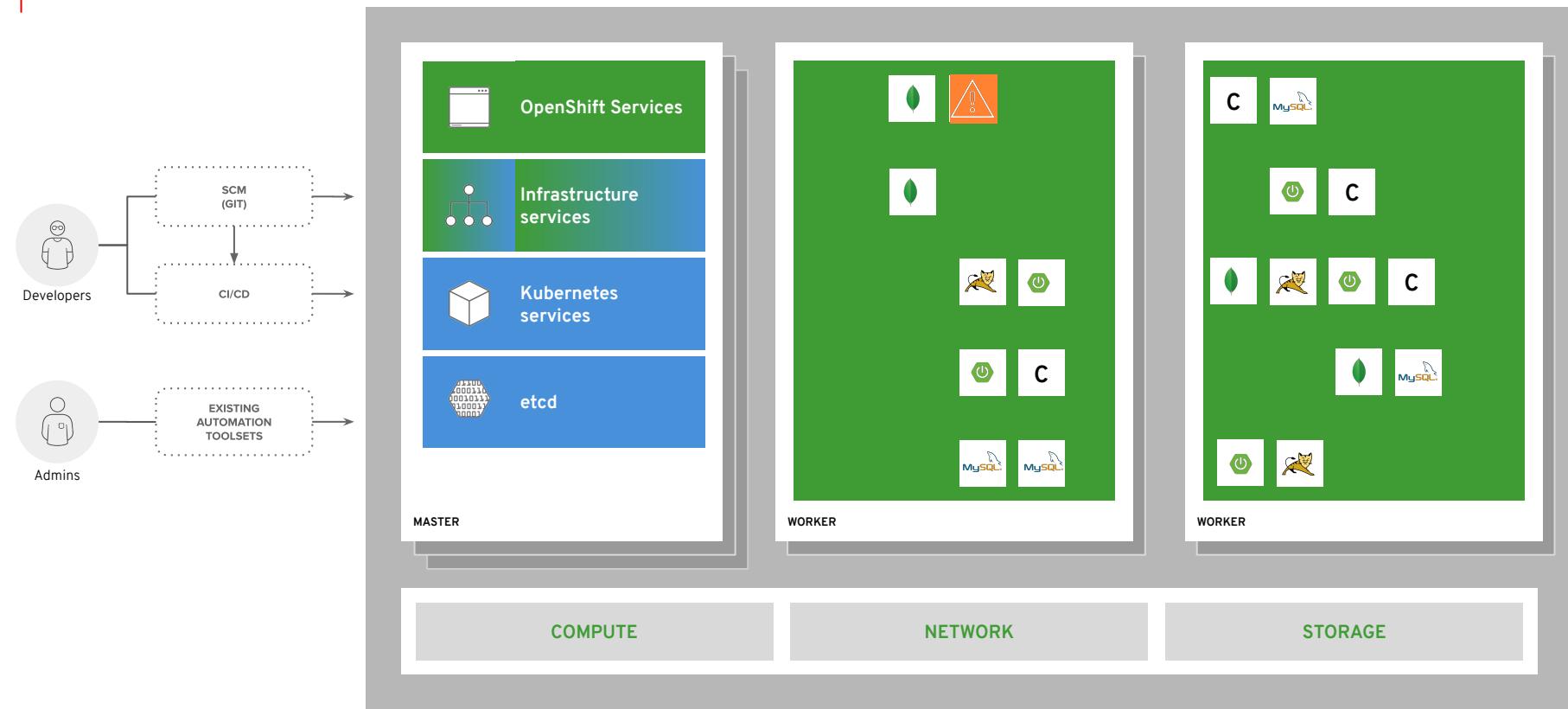
# dev and ops via web, cli, API, and IDE



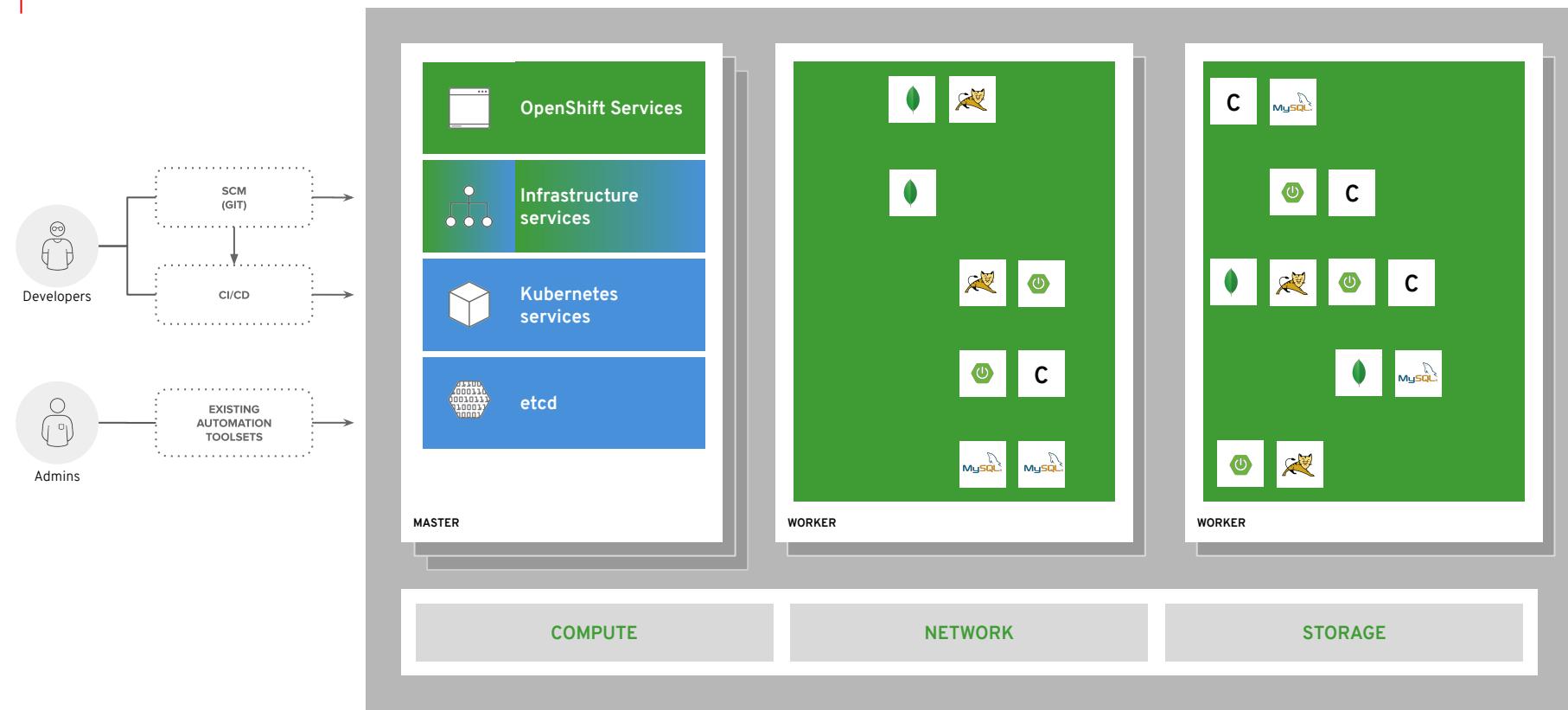
# applications also run on workers



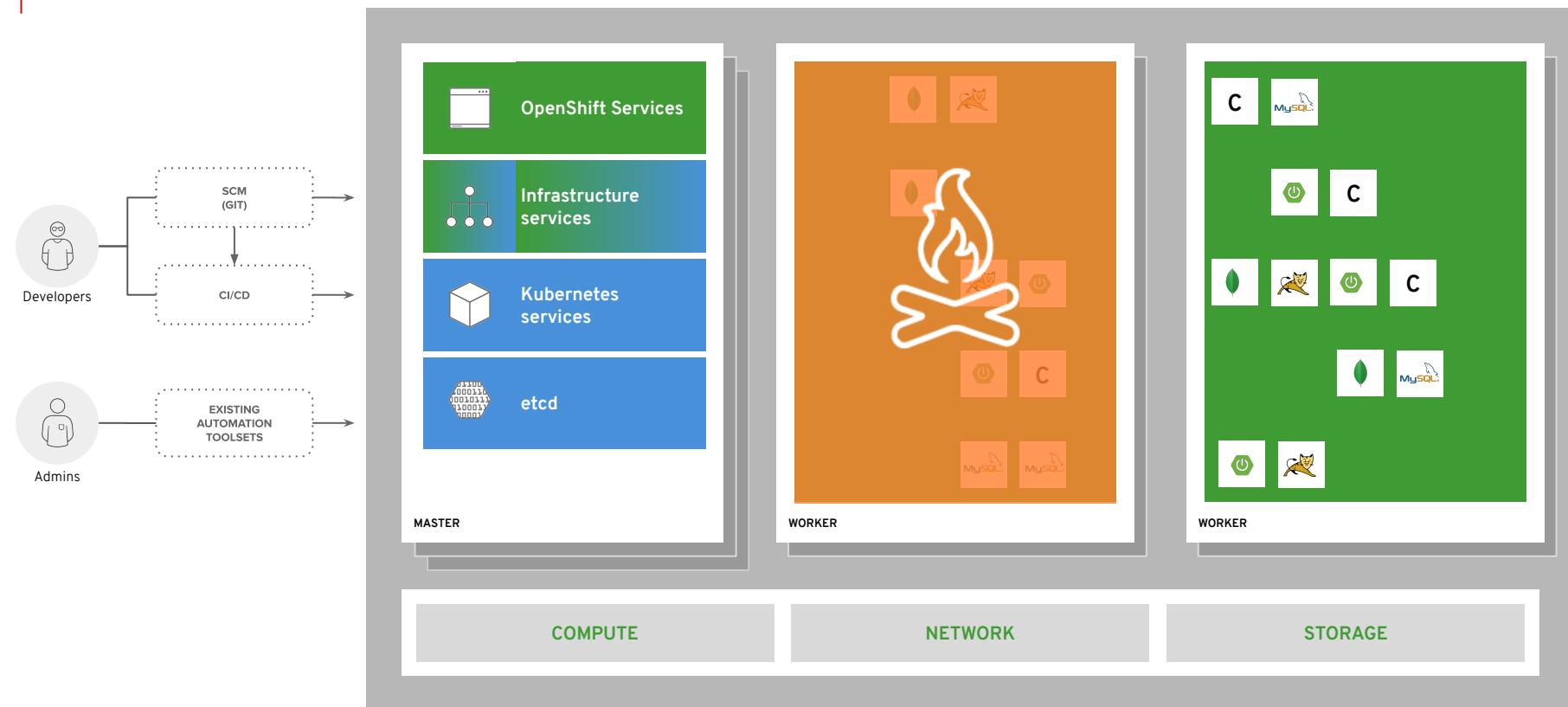
# auto-healing failed pods



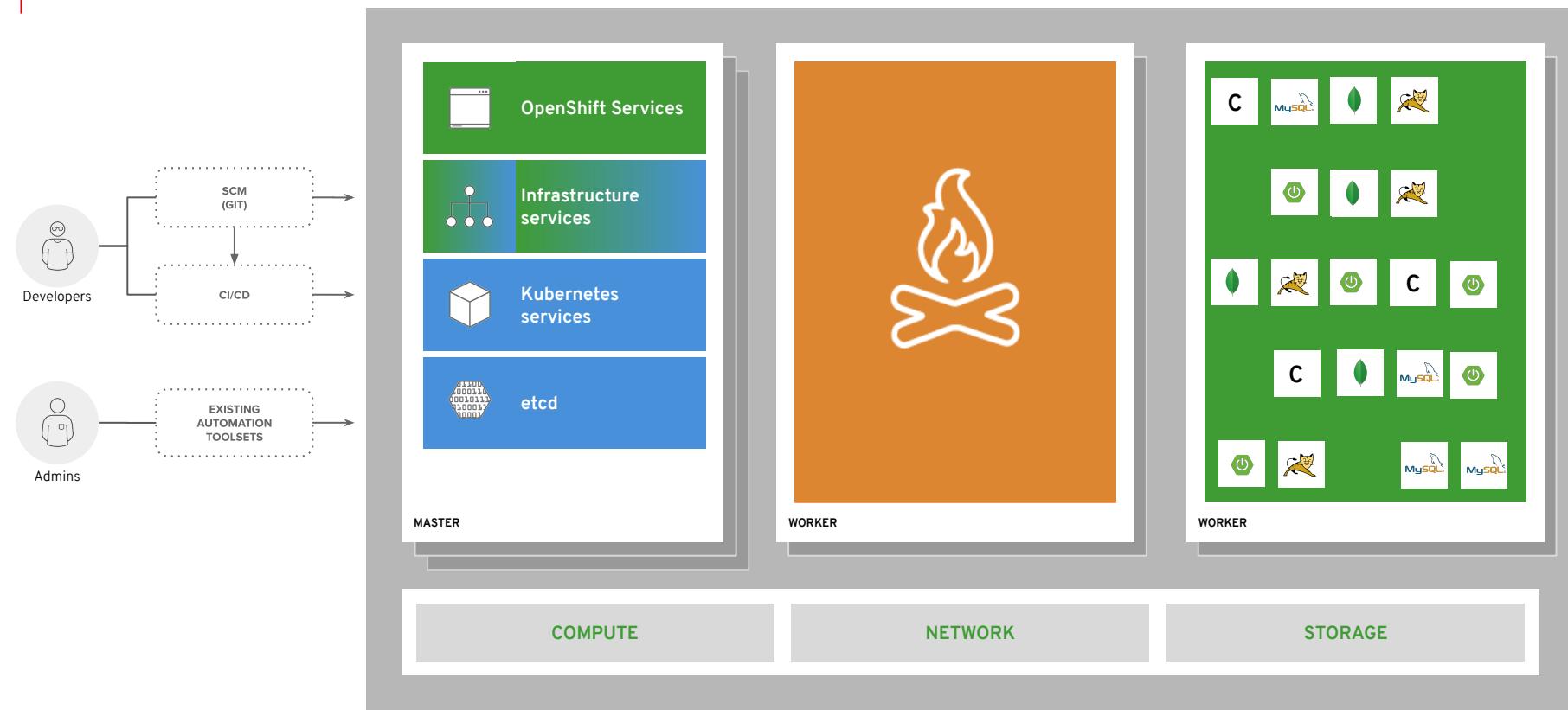
# auto-healing failed pods



# auto-healing for failed nodes



# auto-healing for failed nodes





# OpenShift installation

# Installation Paradigms

## OPENSIFT CONTAINER PLATFORM

### Full Stack Automated

Simplified opinionated “Best Practices” for cluster provisioning

Fully automated installation and updates including host container OS.



**Red Hat**  
Enterprise Linux  
CoreOS

### Pre-existing Infrastructure

Customer managed resources & infrastructure provisioning

Plug into existing DNS and security boundaries



**Red Hat**  
Enterprise Linux  
CoreOS



**Red Hat**  
Enterprise Linux

## HOSTED OPENSIFT

### Azure Red Hat OpenShift

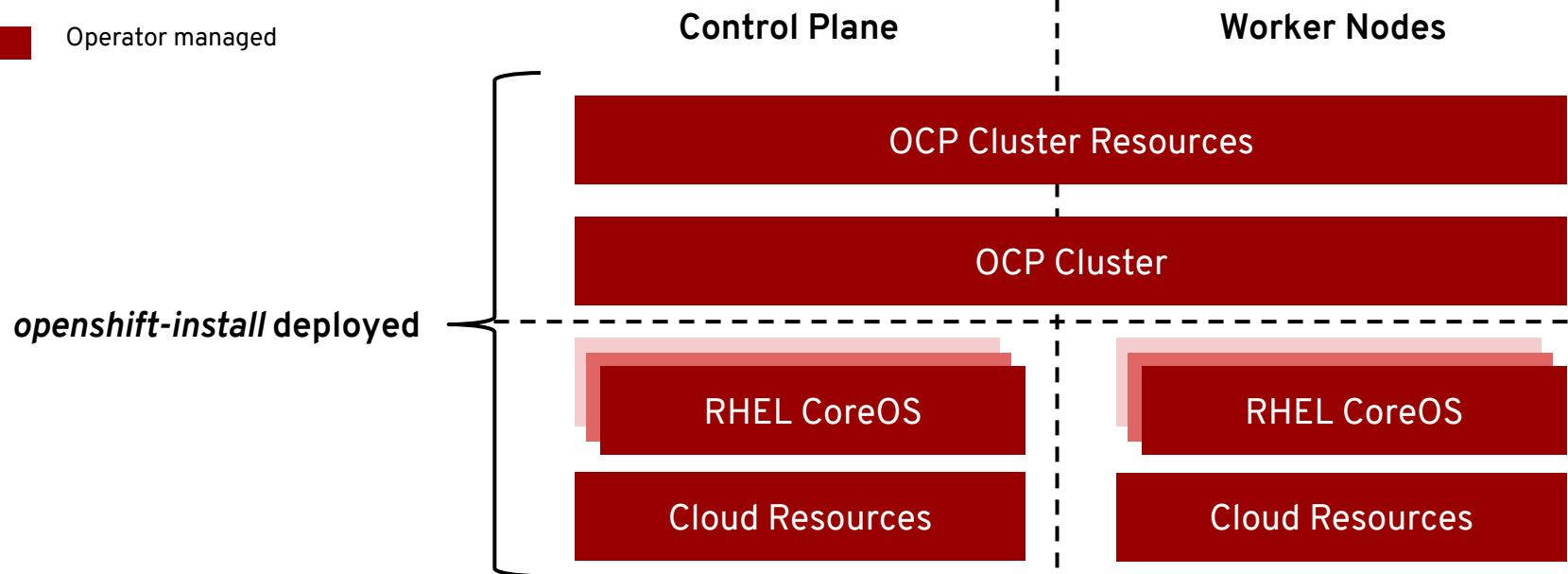
Deploy directly from the Azure console. Jointly managed by Red Hat and Microsoft Azure engineers.

### OpenShift Dedicated

Get a powerful cluster, fully Managed by Red Hat engineers and support.

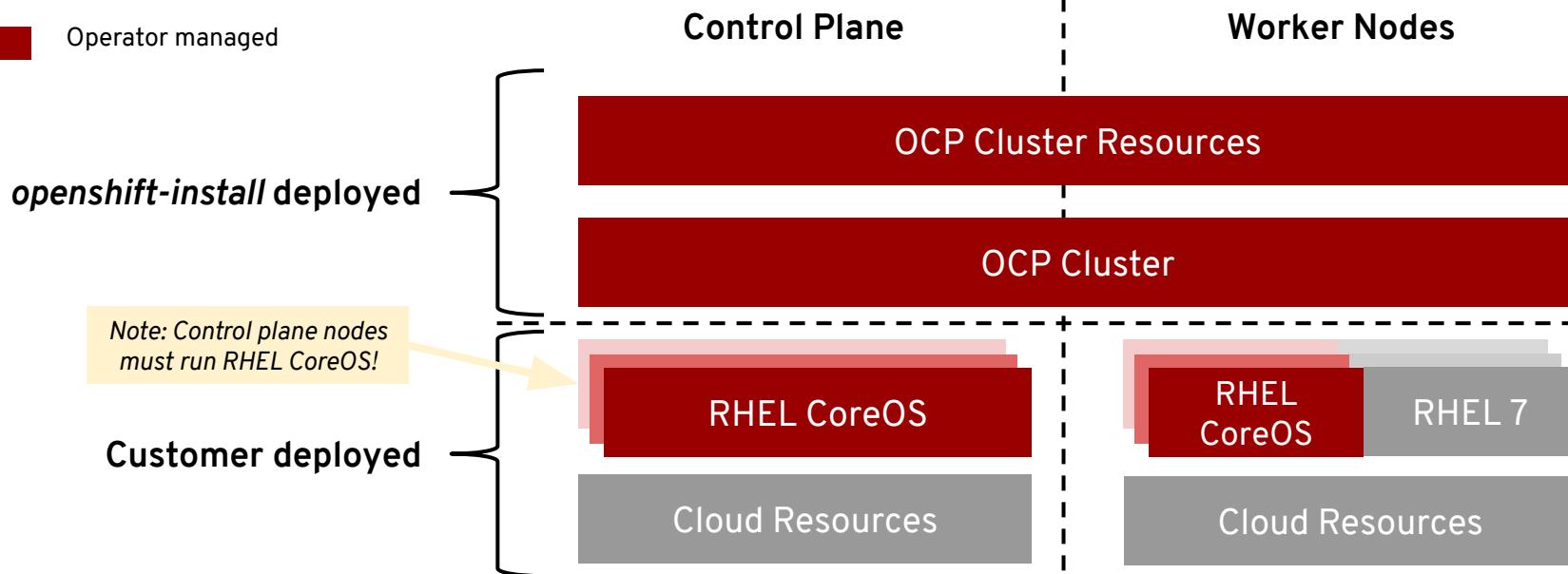
# Full-stack Automated Installation

- User managed
- Operator managed



# Pre-existing Infrastructure Installation

- User managed
- Operator managed

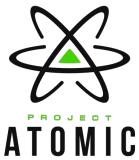




# Operations and infrastructure deep dive

# Red Hat Enterprise Linux CoreOS: The OpenShift Operating System

# IMMUTABLE INFRASTRUCTURE WITH RED HAT COREOS



**RED HAT®**  
CoreOS

- Minimal Linux distribution
- Optimized for running containers
- Decreased attack surface
- Over-the-air automated updates
- Immutable foundation for OpenShift
- Bare-metal and cloud host configuration

# 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.

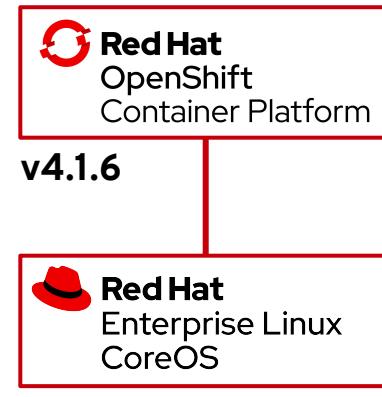
**Red Hat Enterprise Linux CoreOS is managed by the cluster**

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

Operator:

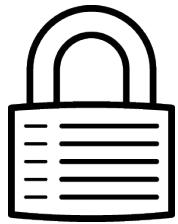
- CRI-O config
- Kubelet config
- Authorized registries
- SSH config

**RHEL CoreOS admins are responsible for:**  
Nothing. 😊



# OpenShift Security

Features, mechanisms  
and processes for  
container and platform  
isolation



## CONTROL

### Application Security



## DEFEND

### Infrastructure



## EXTEND

Container Content	CI/CD Pipeline
Container Registry	Deployment Policies
Container Platform	Container Host Multi-tenancy
Network Isolation	Storage
Audit & Logging	API Management
Security Ecosystem	

## 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

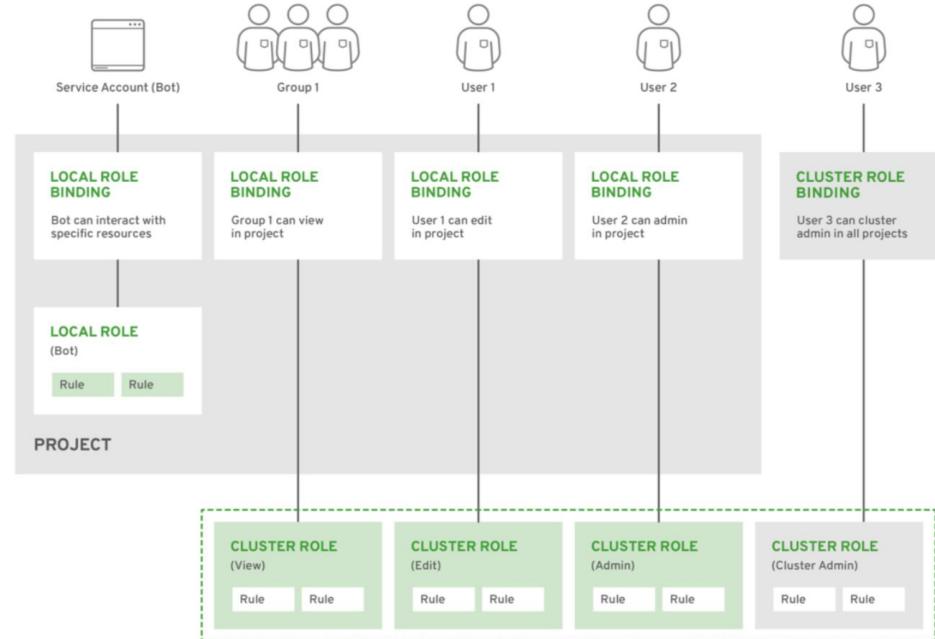


Figure 12 - Authorization Relationships

# Operator Framework

Open source toolkit to  
manage application  
instances on Kubernetes

# WHY OPERATOR FRAMEWORK?



# Kubernetes-native day 2 management

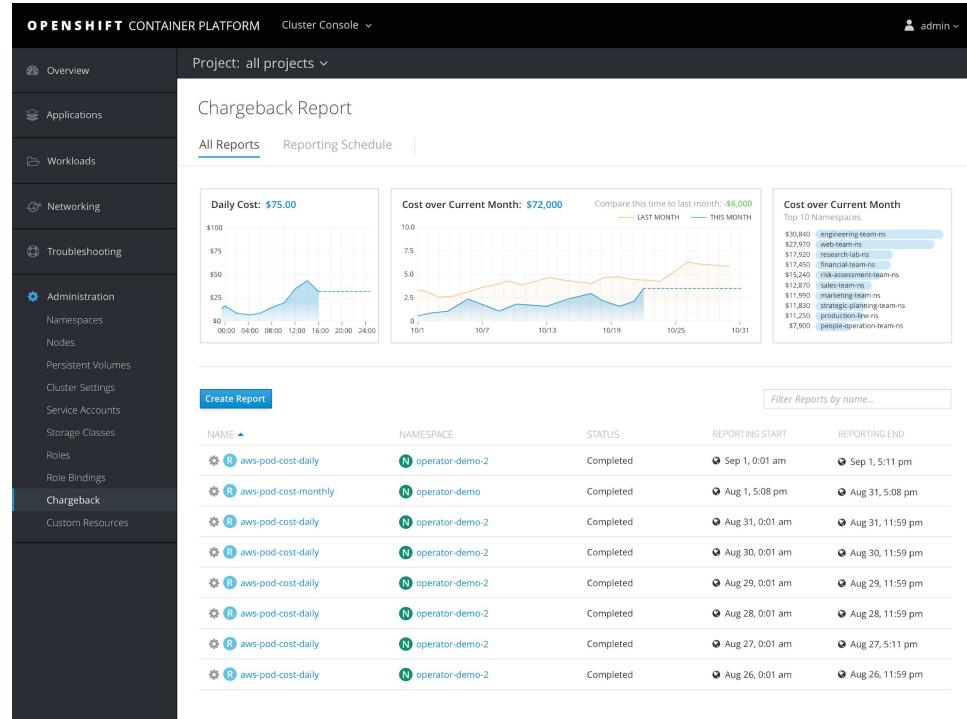


 A white icon showing four arrows pointing outwards from a central point, forming a cross shape.	Flexible app architectures	 A white icon containing mathematical symbols: a right-angle bracket with $\pi$ , a circle with $\odot$ , a square root symbol with $\sqrt{x+y}$ , a circled question mark with $(42)$ , a circle with $e=mc^2$ , and a infinity symbol with $\%$ .	No reinvention of core concepts
 A white icon showing a square with a curved arrow inside, followed by a checkmark inside a square.	Uniform deploy and debug	 A white icon showing two overlapping circles, one solid and one dashed.	Truly hybrid

Operators **codify operational knowledge** and workflows to automate lifecycle management of containerized applications with Kubernetes.

# METERING OPERATOR

- Based on Prometheus
- Reports namespace, pods and custom label query
- Easy to process by accounting or custom software



# THE INDUSTRY IS ALIGNING BEHIND THE KUBERNETES OPERATOR FRAMEWORK



60+ Certified ISV Operators in Red Hat Early Access Program

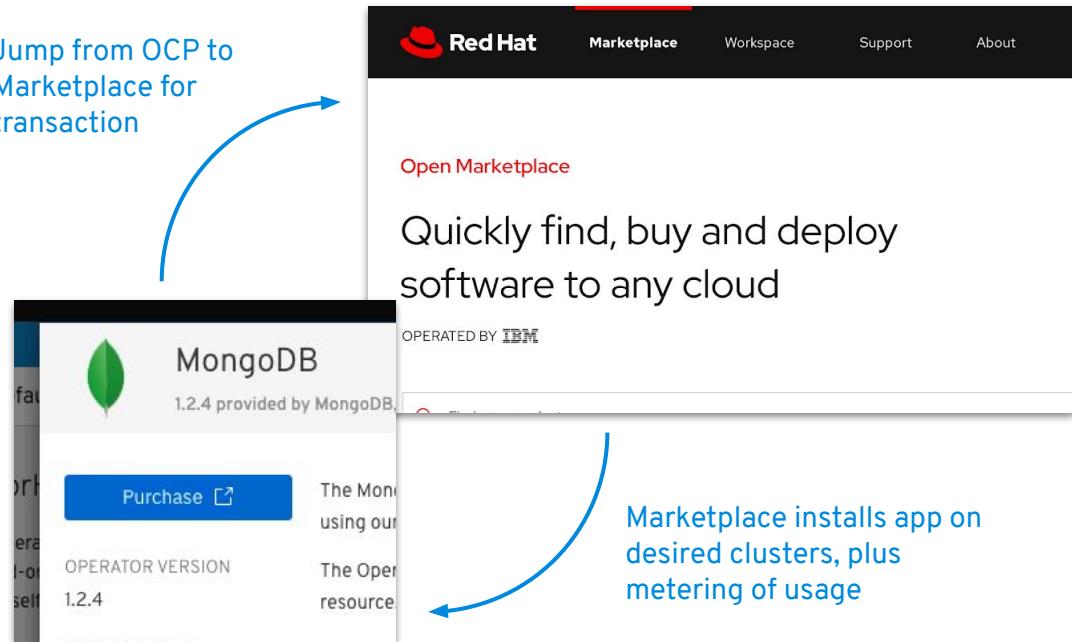
# Open Marketplace in collaboration with IBM

## New ability to sell ISV software

Builds on our Operator certification program to allow customers to purchase enterprise licenses from partners

- Jointly developed with IBM
- IBM will handle L1-L3 support
- Multi-cluster workflow
- Quotas, approval flow and more
- Developers access installed apps through Dev Catalog

Jump from OCP to Marketplace for transaction



# 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 sent by Prometheus.



**Metrics visualization** via  
Grafana, the leading metrics  
visualization technology.

# OpenShift Logging

An integrated solution for  
exploring and  
corroborating application  
logs

# Observability via 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

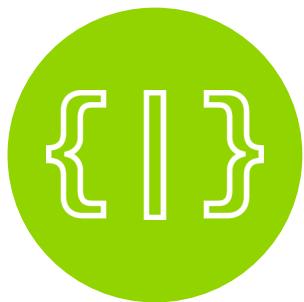
## Ability to forward logs elsewhere

- External elasticsearch, Splunk, etc

# Build and Deploy Container Images

Tools and automation  
that makes developers  
productive quickly

# Build Containers for Cloud-Native Architecture



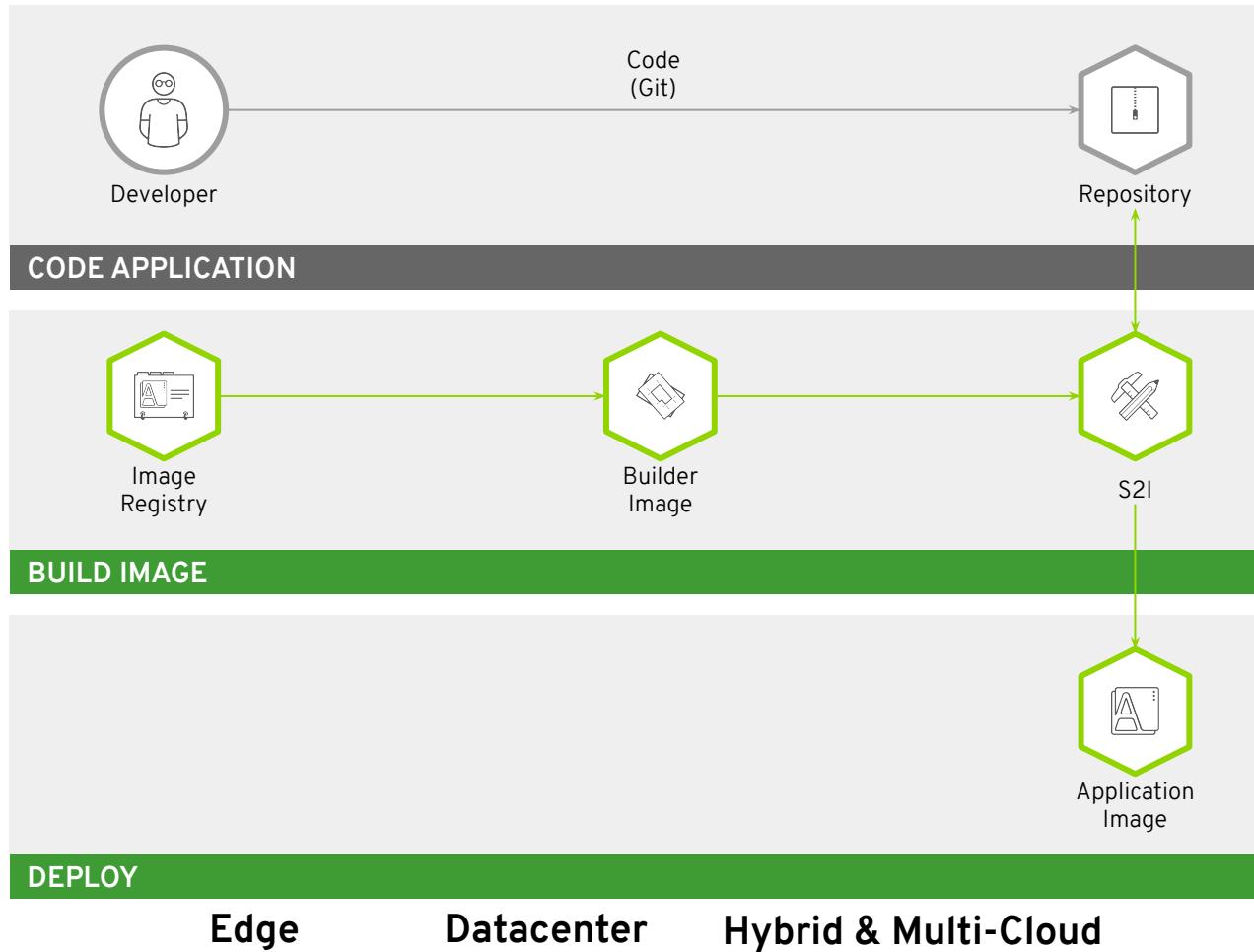
DEPLOY YOUR  
SOURCE CODE

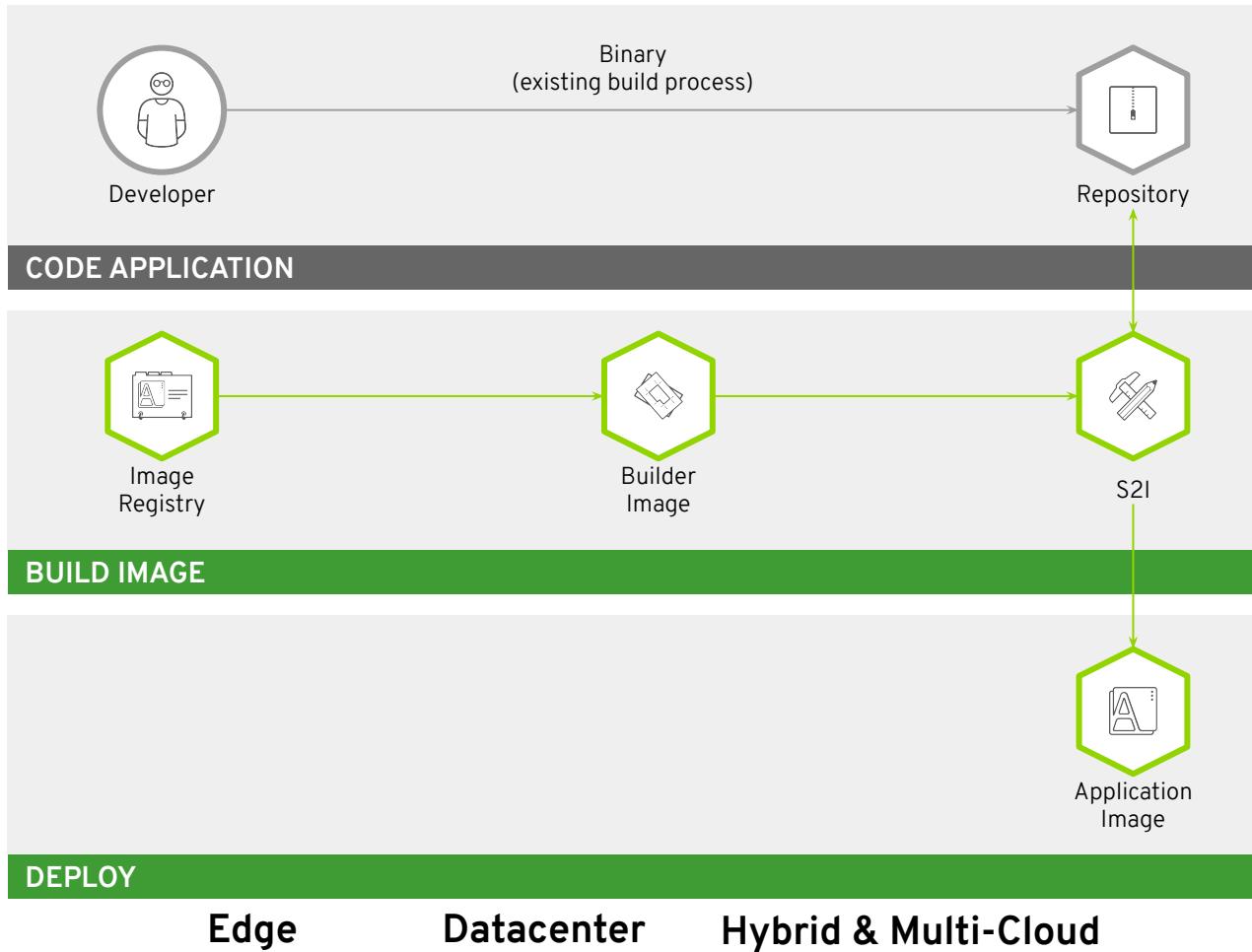


DEPLOY YOUR  
APP BINARY



DEPLOY YOUR  
CONTAINER IMAGE





# Reference Architectures & Road Map

Reference Information

# OPENSHIFT ROADMAP

Q3 CY2019 OpenShift 4.2		Q1 CY2020 OpenShift 4.3		CY2020 OpenShift 4.4+	
HOSTED	PLATFORM	HOSTED	PLATFORM	HOSTED	PLATFORM
HOSTED	PLATFORM	HOSTED	PLATFORM	HOSTED	PLATFORM
	<ul style="list-style-type: none"><li>Developer Console GA</li><li>OpenShift Serverless (Knative) - TP</li><li>OpenShift Pipelines (Tekton) DP3</li><li>CodeReady Containers GA</li><li>Developer CLI (odo) GA</li></ul>		<ul style="list-style-type: none"><li>OpenShift Pipelines (Tekton) TP</li><li>Helm 3 TP</li></ul>		<ul style="list-style-type: none"><li>OpenShift Serverless (Knative) GA</li><li>Guided application creation</li><li>OpenShift Pipelines (Tekton) GA</li><li>Helm 3 GA</li></ul>
	<ul style="list-style-type: none"><li>OperatorHub Enhancements</li><li>Operator Deployment Field Forms</li><li>Application Migration Console</li></ul>		<ul style="list-style-type: none"><li>Metering for Services</li><li>Windows Containers (Planned)</li><li>GPU Metering</li><li>Application Operator Binding - DP</li></ul>		<ul style="list-style-type: none"><li>Monitor application workloads</li><li>Simplify OLM interactions</li><li>Improving native developer console for monitoring and troubleshooting</li></ul>
	<ul style="list-style-type: none"><li>Kubernetes 1.14 w/ CRI-O runtime</li><li>Disconnected Install and Update</li><li>Automated Installer for Azure, GCP, &amp; OSP</li><li>Pre-existing Infra Installer for GCP</li><li>Cluster-wide Egress Proxy</li><li>OVN Tech Preview</li><li>OpenShift Container Storage 4.2 (1 month after)</li></ul>		<ul style="list-style-type: none"><li>Kubernetes 1.16 w/ CRI-O runtime</li><li>Private/Internal Clusters support from the installer</li><li>Deploy to pre-existing VPC &amp; Subnets</li><li>FIPS</li><li>Pre-existing Infra Installer for Azure (4.3.z)</li><li>OpenShift Container Storage 4.3</li></ul>		<ul style="list-style-type: none"><li>OVN GA w/ Windows Networking Integration (Planned)</li><li>Windows Containers GA</li><li>Multi-cluster summary dashboards</li><li>Centralized cluster updates</li><li>Compliance operator</li><li>Node problem detector</li><li>IPv6 (single/dual on control plane)</li><li>HTTP/2 Support</li><li>CSI certification suite</li></ul>
	<ul style="list-style-type: none"><li>Insights Operator</li><li>Azure Red Hat OpenShift new features (monitoring, logging)</li></ul>		<ul style="list-style-type: none"><li>Subscription Mgmt Improvements (cloud.redhat.com)</li><li>Azure Red Hat OpenShift new features (private clusters)</li><li>Azure Red Hat OpenShift preview of 4.x</li><li>OSD on Google Cloud preview on 4.x</li></ul>		<ul style="list-style-type: none"><li>Enhanced consumption building</li><li>Regulatory compliance</li><li>Machine autoscaling</li><li>Google cloud platform</li></ul>

# REFERENCE ARCHITECTURES

[OpenShift on VMware vCenter](#)

[OpenShift on Red Hat OpenStack Platform](#)

[OpenShift on Amazon Web Services](#)

[OpenShift on Google Cloud Platform](#)

[OpenShift on Microsoft Azure](#)

[OpenShift on Red Hat Virtualization](#)

[OpenShift on HPE Servers with Ansible Tower](#)

[OpenShift on VMware vCenter 6 with Gluster](#)

[Deploying an OpenShift Distributed Architecture](#)

[OpenShift Architecture and Deployment Guide](#)

[OpenShift Scaling, Performance, and Capacity Planning](#)

[Application Release Strategies with OpenShift](#)

[Building Polyglot Microservices on OpenShift](#)

[Building JBoss EAP 6 Microservices on OpenShift](#)

[Building JBoss EAP 7 Microservices on OpenShift](#)

[Business Process Management with JBoss BPM Server on OpenShift](#)

[Build and Deployment of Java Applications on OpenShift](#)

[Building Microservices on OpenShift with Fuse Integration...](#)

[JFrog Artifactory on OpenShift Container Platform](#)

[Spring Boot Microservices on Red Hat OpenShift](#)

[API Management with Red Hat 3scale on OpenShift](#)

[App CI/CD on OCP with Jenkins](#)

# LEARN MORE - TRAINING FOR FREE

- [OpenShift Interactive Learning Portal](#) - An online interactive learning environment where you can run through various scenarios related to using OpenShift.
- [OpenShift Cookbook](#) - Recipes of common tasks that users could need to do on OpenShift.
- [CodeReady Containers](#) - OpenShift on your laptop
- [OpenShift Online](#) - A shared public hosting environment for running your applications using OpenShift.
- [OpenShift.io](#) - An online development environment for planning, creating and deploying hybrid cloud services using OpenShift.
- [OpenShift Dedicated](#) - A dedicated hosting environment for running your applications, managed and supported for you by Red Hat.
- [OpenShift Container Platform](#) - The Red Hat supported OpenShift product for installation on premise or in hosted cloud environments.

The following free online eBooks are also available for download related to OpenShift.

- [OpenShift for Developers](#)