



# 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)





# Solving App Delivery Pain

# 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

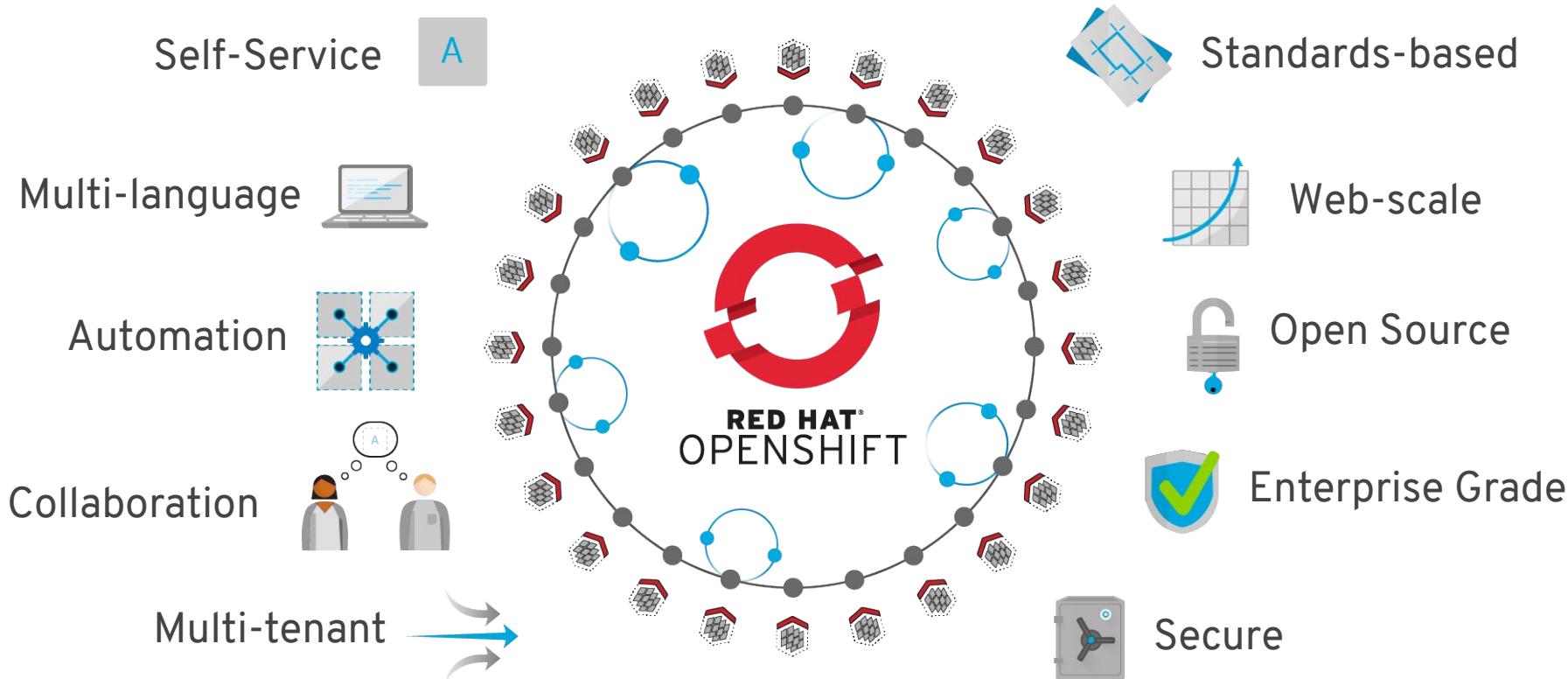
- Manual builds and deployment
- Rebuilding between environments
- Waiting for infrastructure
- Clunky division of manual tasks
- Complicated builds
- Waiting for deploy outages

## 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

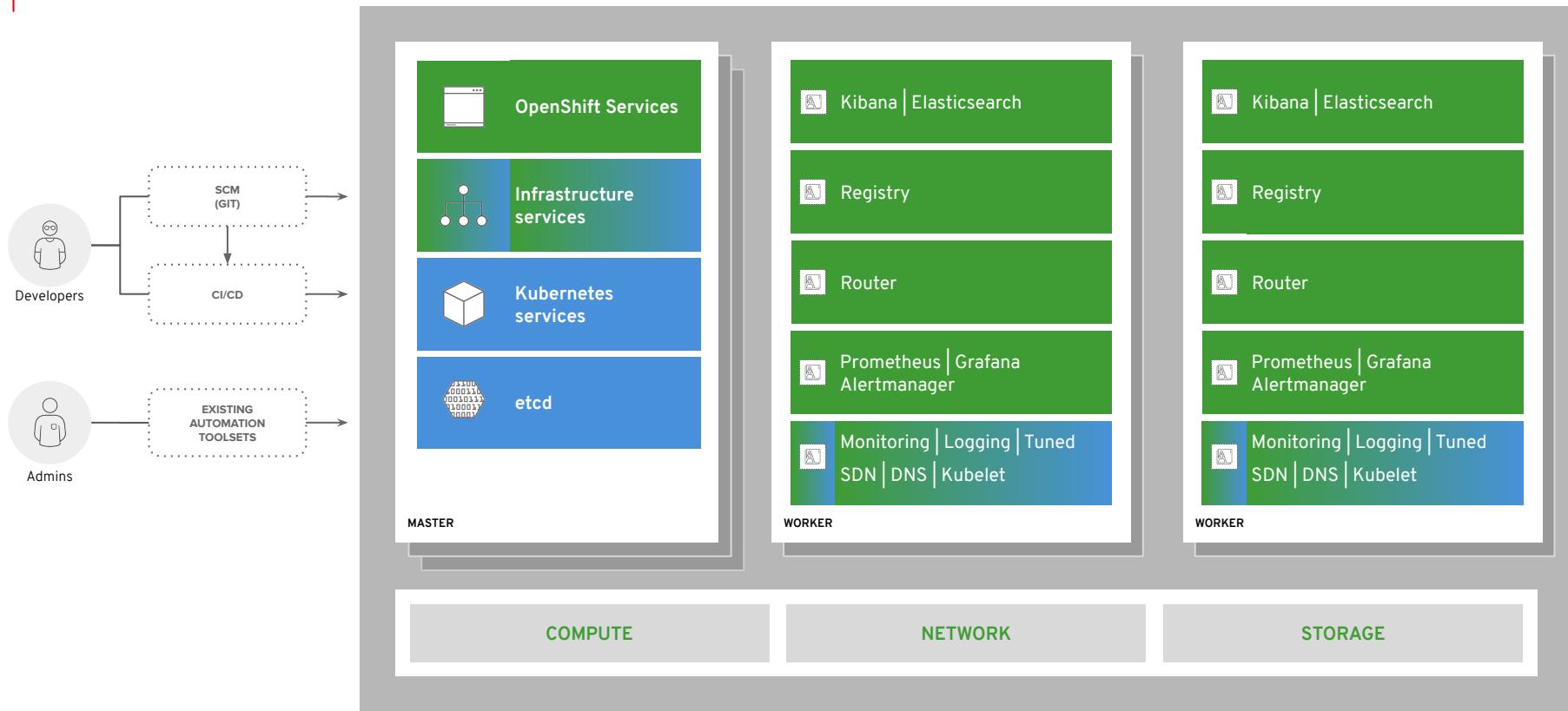
Kubernetes

Red Hat Enterprise Linux | RHEL CoreOS

Best IT Ops Experience

CaaS  $\longleftrightarrow$  PaaS  $\longleftrightarrow$  FaaS

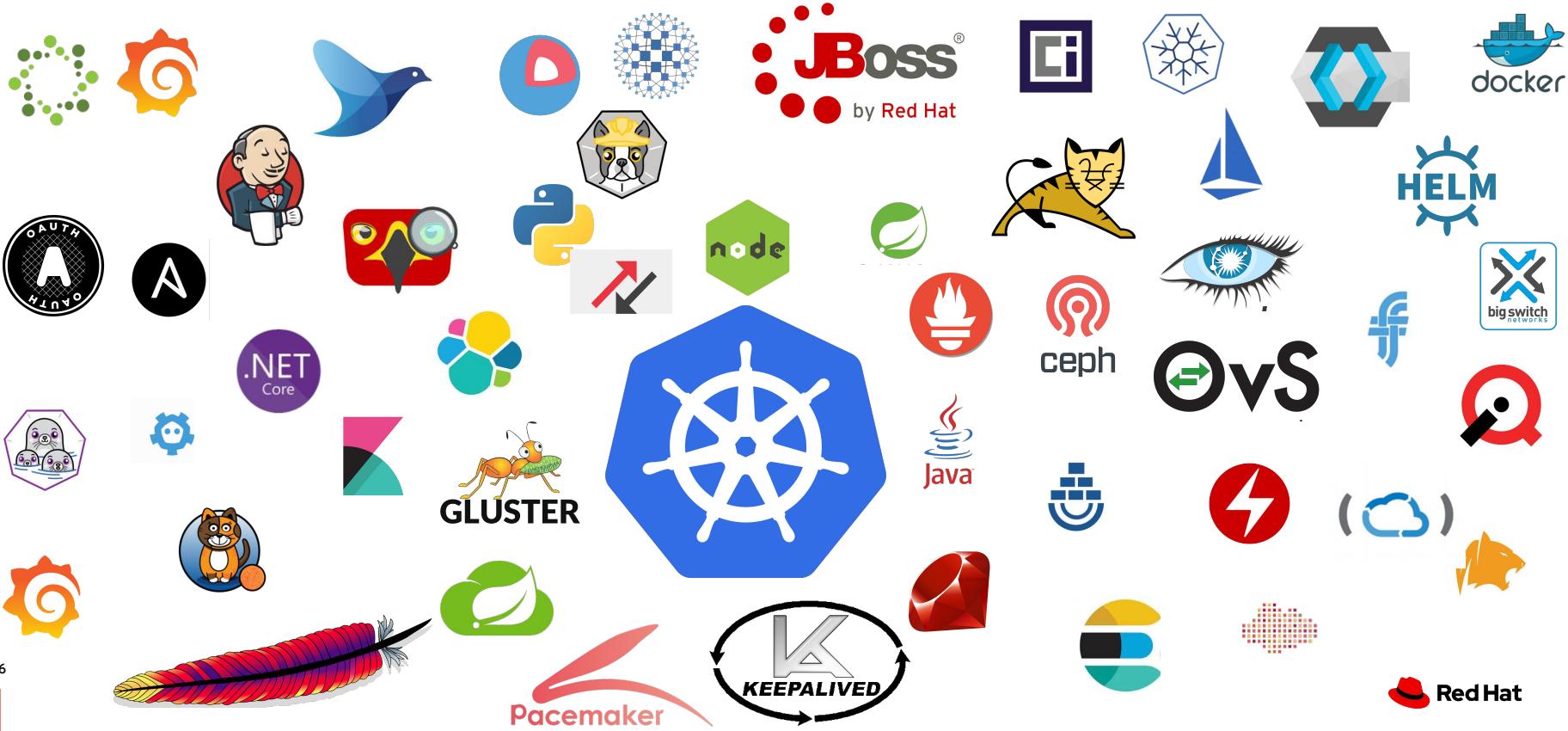
Best Developer Experience



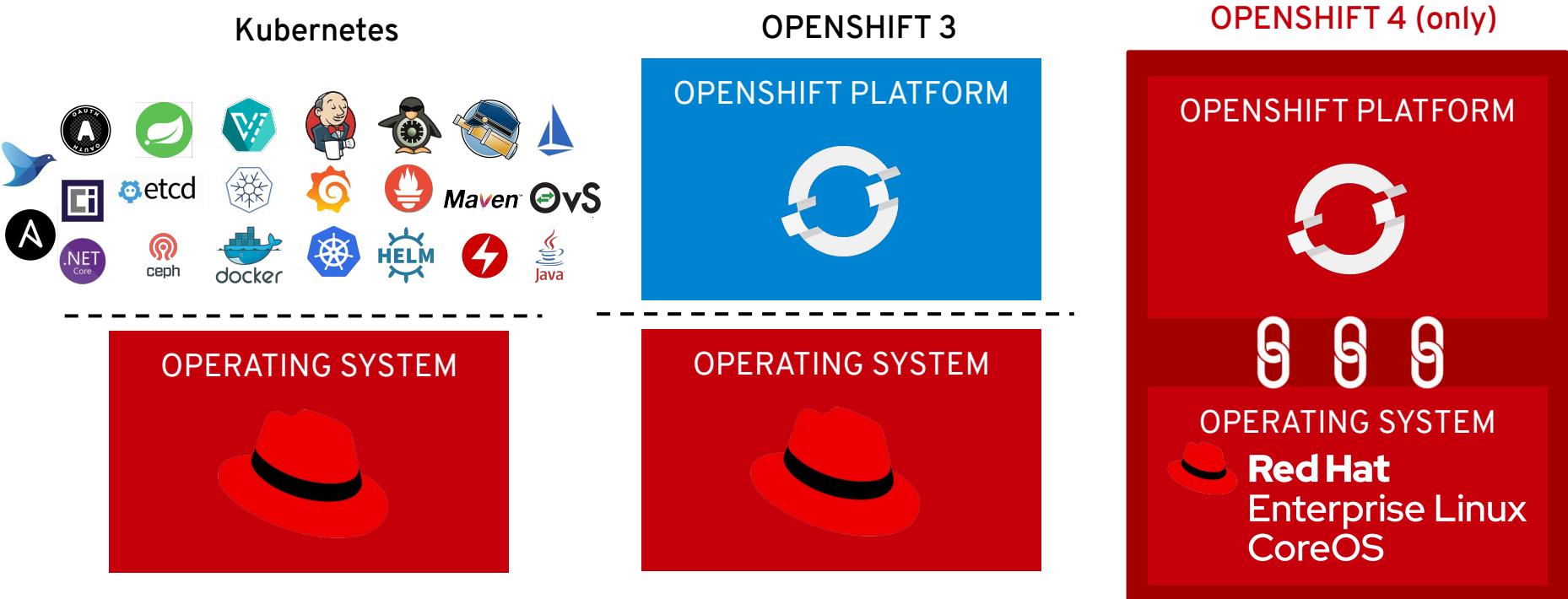
## Overwhelmed? Please see the CNCF Trail Map. That and the interactive landscape are at [l.cncf.io](https://l.cncf.io)

<p>The grid displays a comprehensive overview of CNCF projects across various categories. Projects are represented by icons, with some being 'Graduated' (blue background) and others 'Incubating' (white background). Categories include Database, Streaming &amp; Messaging, Application Definition &amp; Image Build, Continuous Integration &amp; Delivery, Platform, Observability and Analysis, Scheduling &amp; Orchestration, Coordination &amp; Service Discovery, Remote Procedure Call, Service Proxy, API Gateway, Service Mesh, Orchestration &amp; Management, Cloud-Native Storage, Container Runtime, Cloud-Native Network, Runtime, Automation &amp; Configuration, Container Registry, Security &amp; Compliance, Key Management, and Provisioning.</p>											
<p>This section highlights Kubernetes Certified Service Providers, showing a grid of logos for various companies that offer services based on Kubernetes technology.</p>											
<p>This section highlights Kubernetes Training Partners, showing a grid of logos for companies that provide training for Kubernetes.</p>											
<p>This section shows a grid of logos for various public cloud providers and related services.</p>											
<p>This section is labeled 'Special' and contains a grid of logos for various organizations and initiatives.</p>											
<p>This row contains a long grid of logos for a variety of other cloud native and related projects.</p>											

# OpenShift



# Kubernetes, OpenShift 3, Openshift 4



Single-Image Platform Packaging

# More Than 1,700 Red Hat OpenShift Customers



MODERNIZE APPS



WEB APPS



CLOUD NATIVE DEV



MULTI-CLOUD



MOBILE



BIG DATA | ANALYTICS



AI | ML



IOT



# 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, which consists of the word "Hilton" in a bold, black, 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

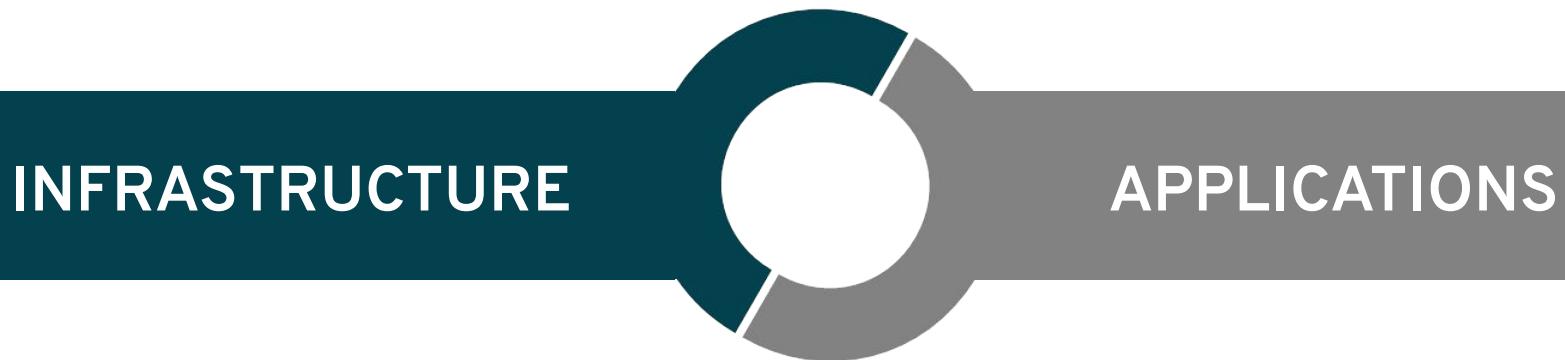
**OpenShift on AWS, Azure, & private cloud**



# Containers: Core Concepts

# WHAT ARE CONTAINERS?

It Depends Who You Ask

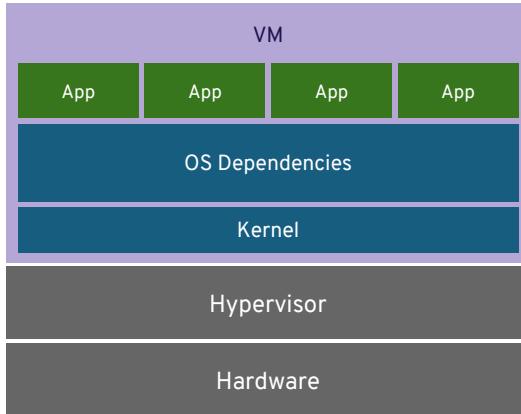


- Application processes on a shared kernel
- Simpler, lighter, and denser than VMs
- Portable across different environments
- Package apps with all dependencies
- Deploy to any environment in seconds
- Easily accessed and shared

*Both are correct!*

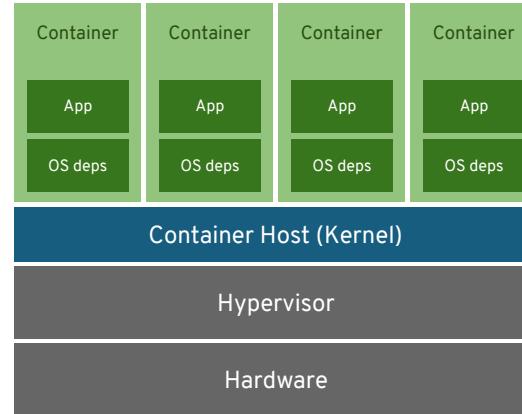
# VIRTUAL MACHINES VS. CONTAINERS

VIRTUAL MACHINES



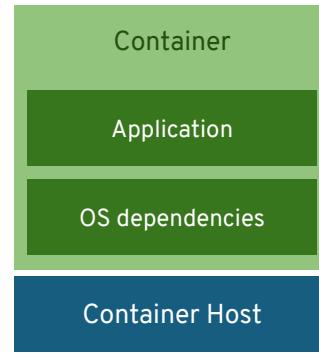
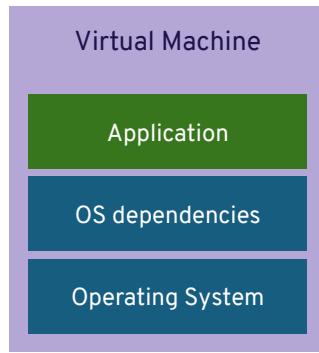
VM abstracts the hardware

CONTAINERS



Container isolates processes:  
abstracts OS *and* hardware

# VIRTUAL MACHINES AND CONTAINERS



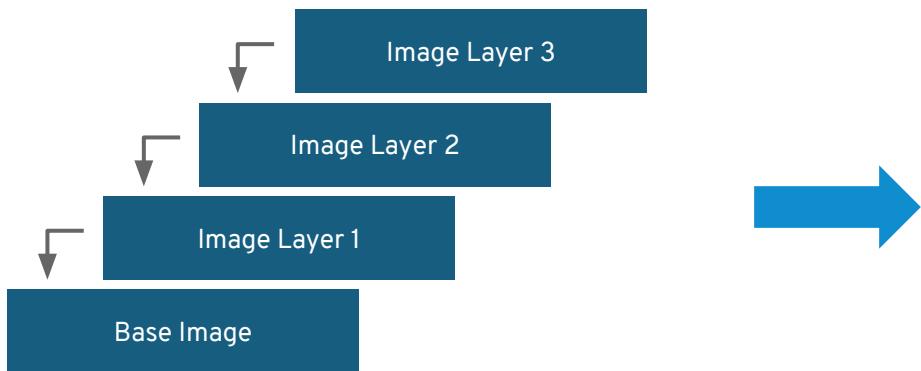
- + VM Isolation
- Complete OS
- Static Compute
- Static Memory
- High Resource Usage
- VM Drift

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

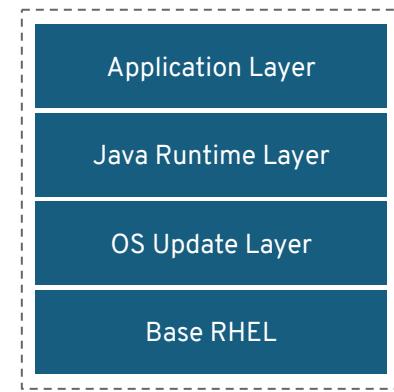
# VIRTUAL MACHINES VS. CONTAINERS



# RAPID SECURITY PATCHING USING CONTAINER IMAGE LAYERING



Container Image Layers



Example Container Image



# OpenShift and Kubernetes: Core Concepts

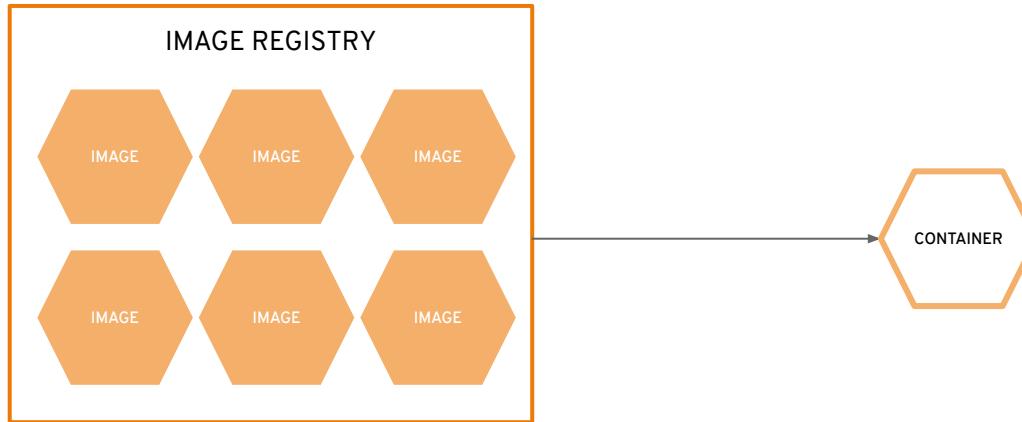
# a container is the smallest compute unit



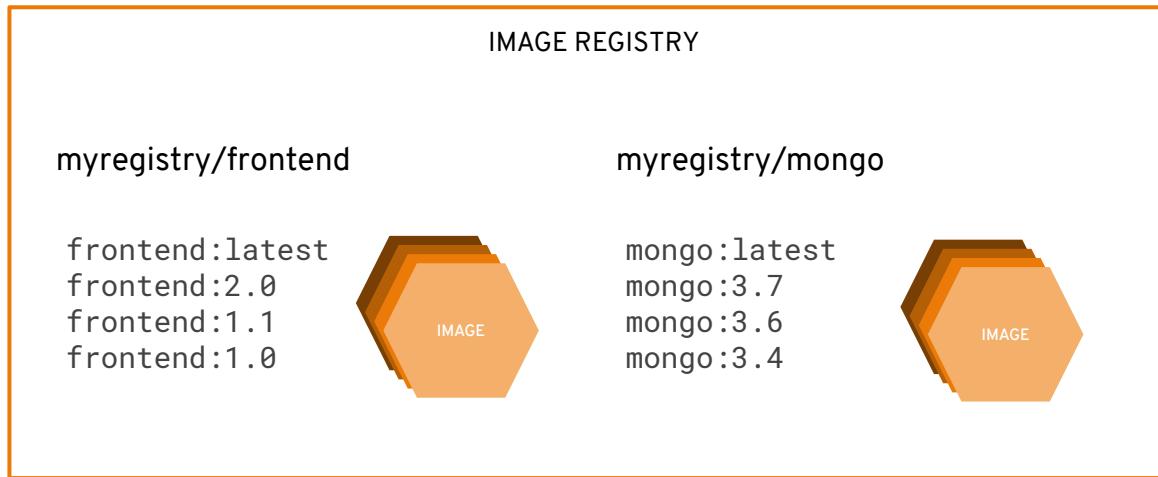
# containers are created from container images



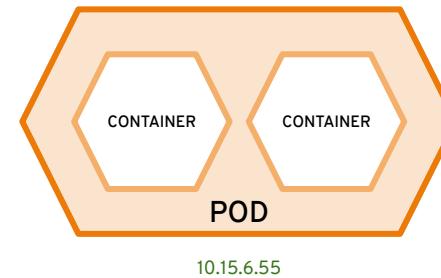
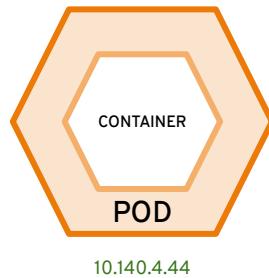
# container images are stored in an image registry



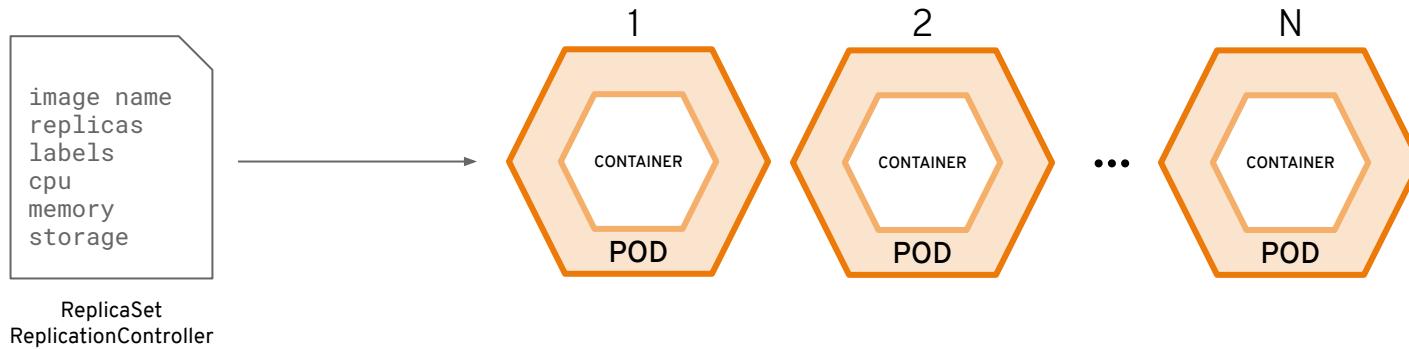
# an image repository contains all versions of an image in the image registry



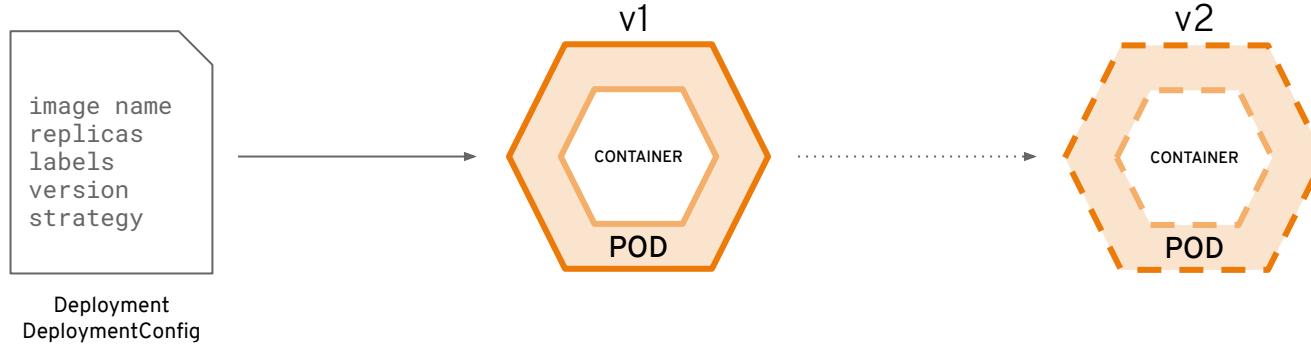
containers are wrapped in pods which are units of deployment and management



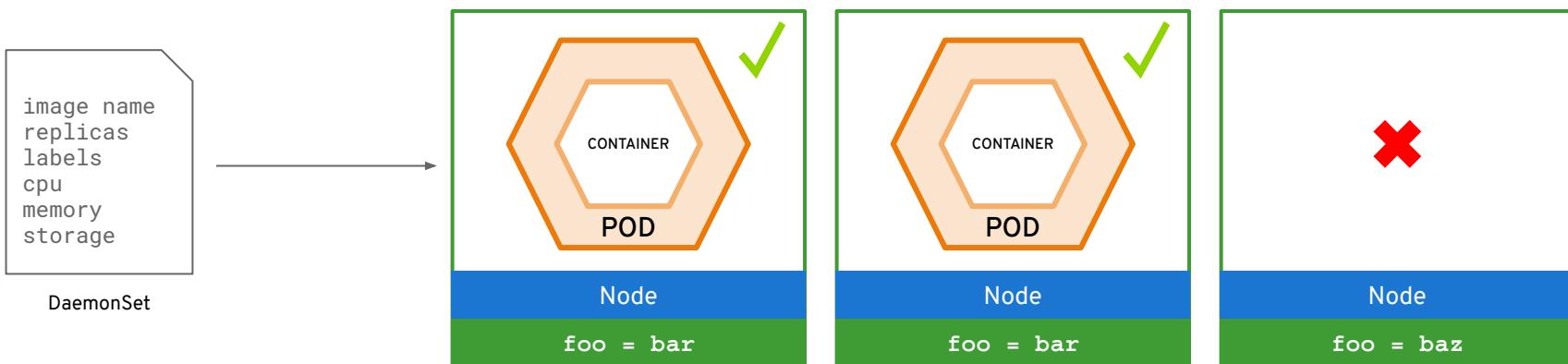
# ReplicationControllers & ReplicaSets ensure a specified number of pods are running at any given time



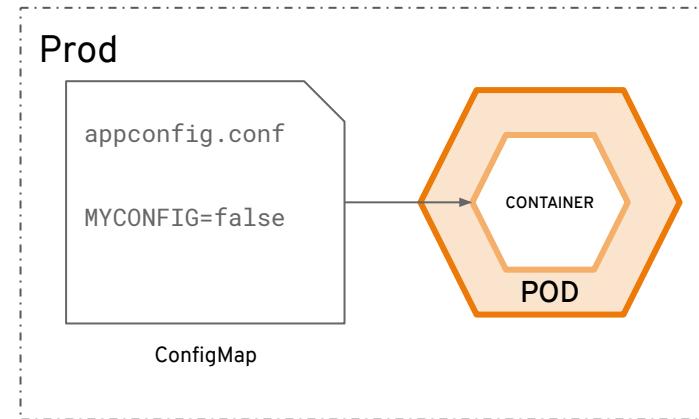
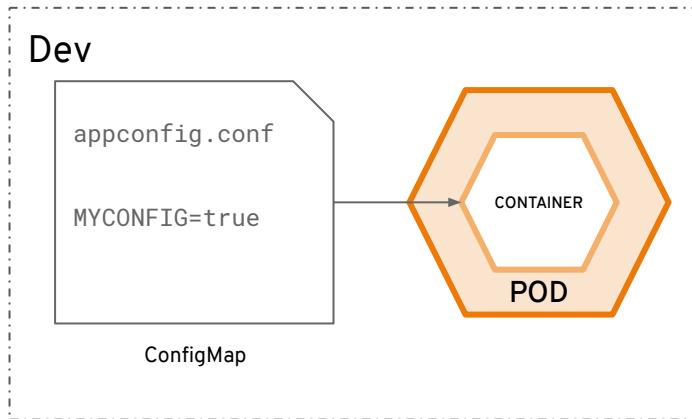
# Deployments and DeploymentConfigurations define how to roll out new versions of Pods



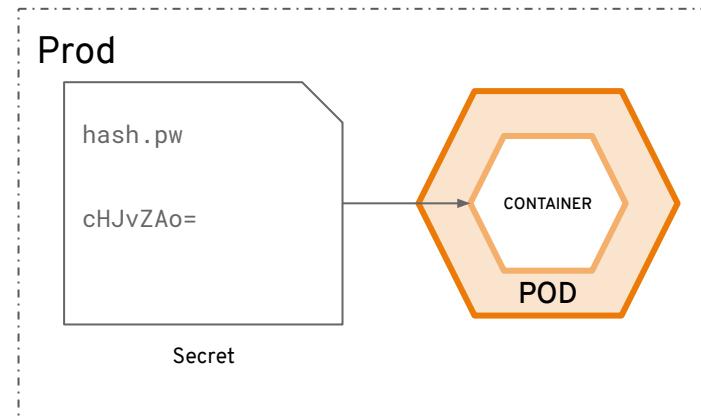
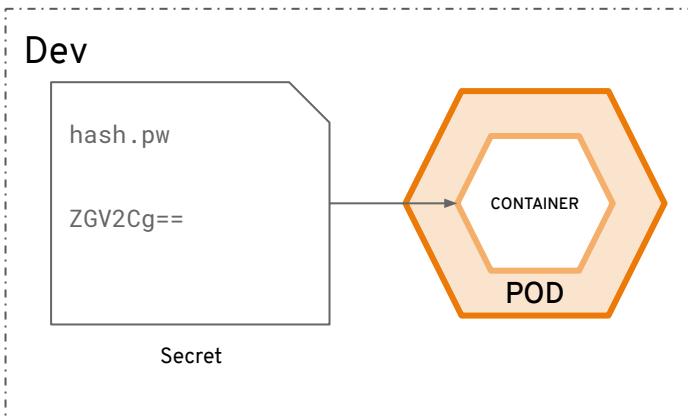
a daemonset ensures that all  
(or some) nodes run a copy of a pod



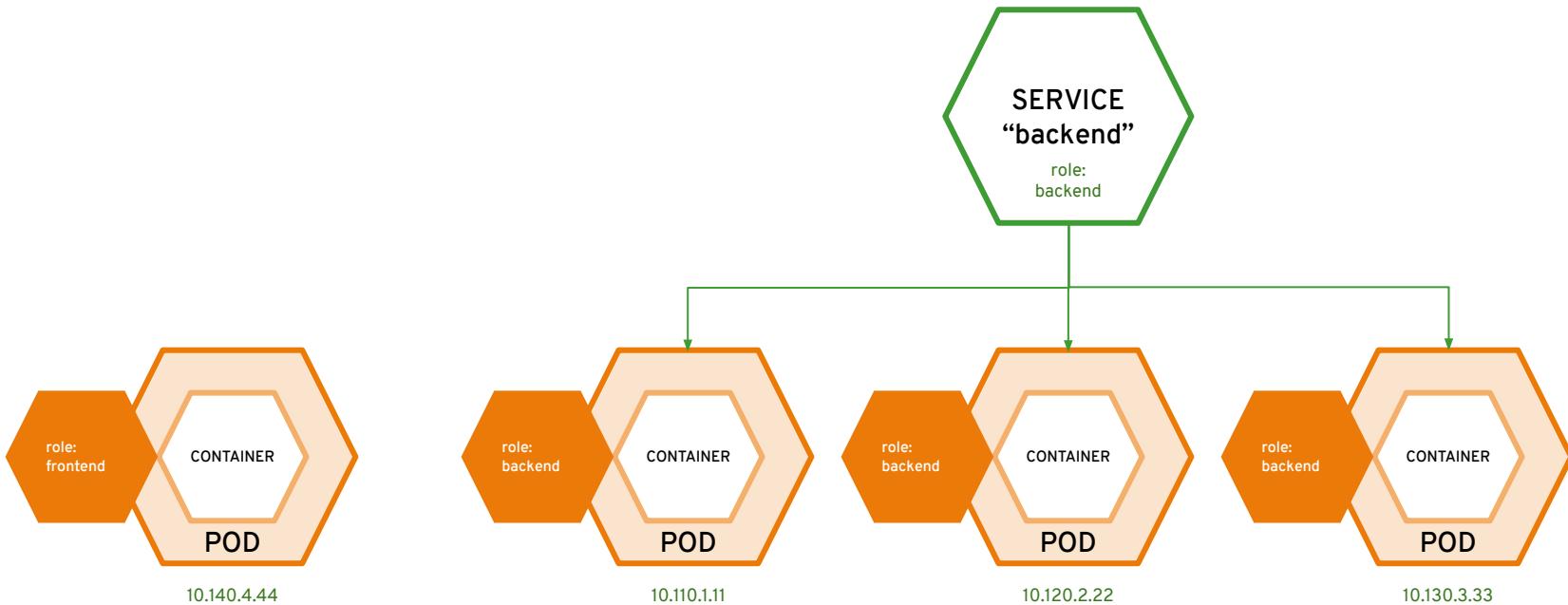
configmaps allow you to decouple configuration artifacts from image content (and application code!)



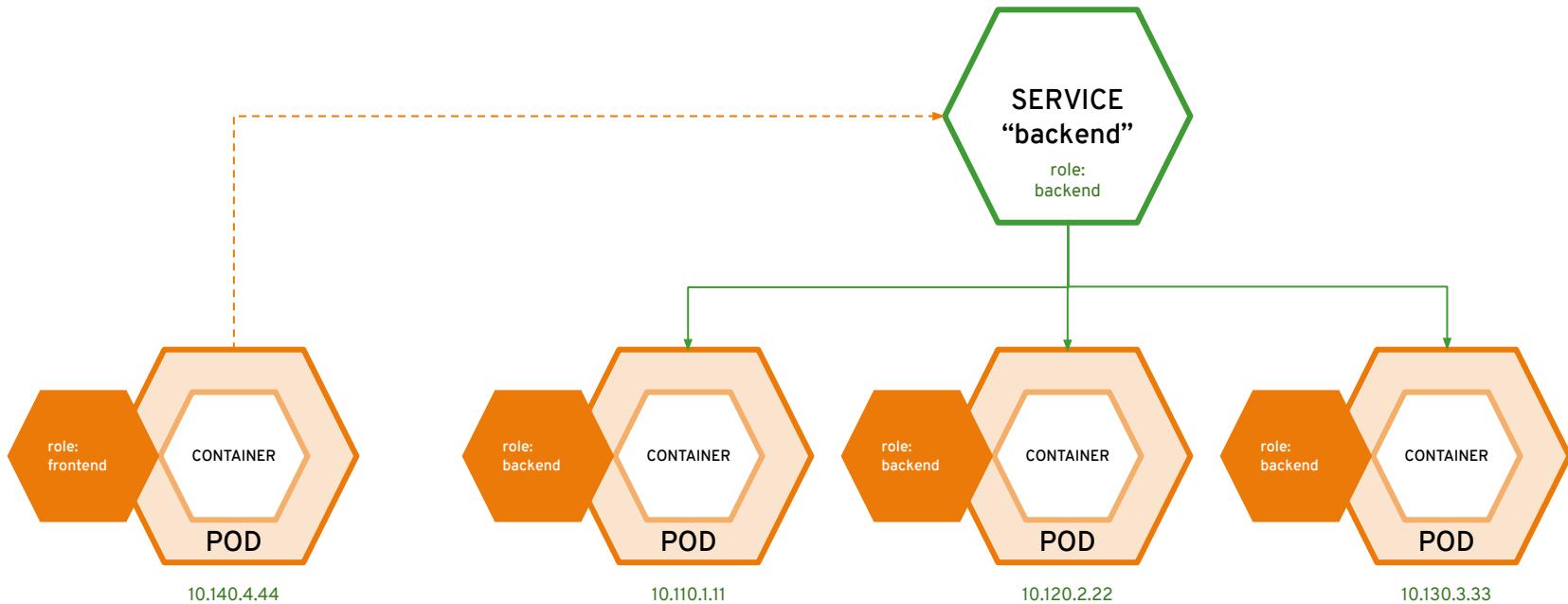
secrets provide a mechanism to hold sensitive information such as passwords



services provide internal load-balancing  
and service discovery across pods

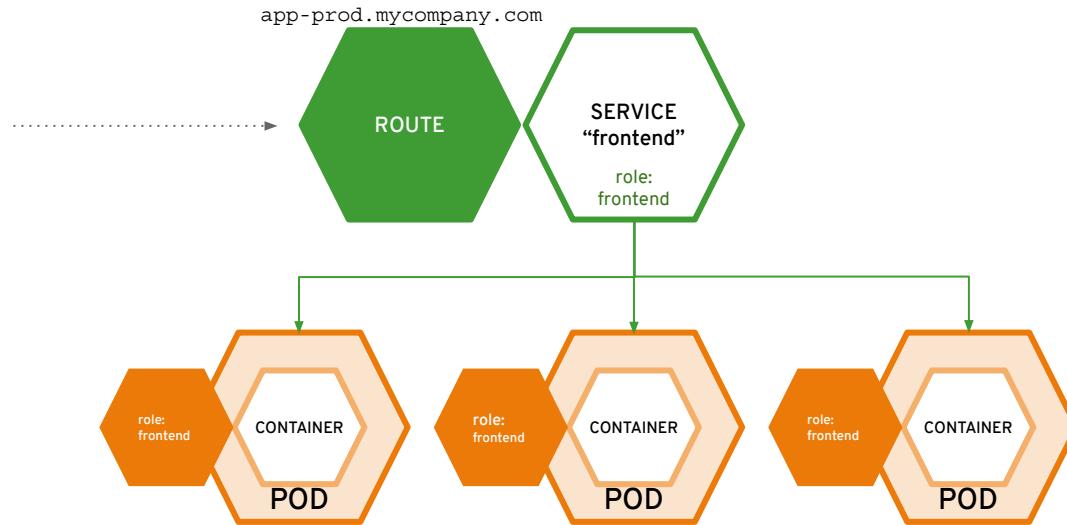


also, apps can talk to each other via services

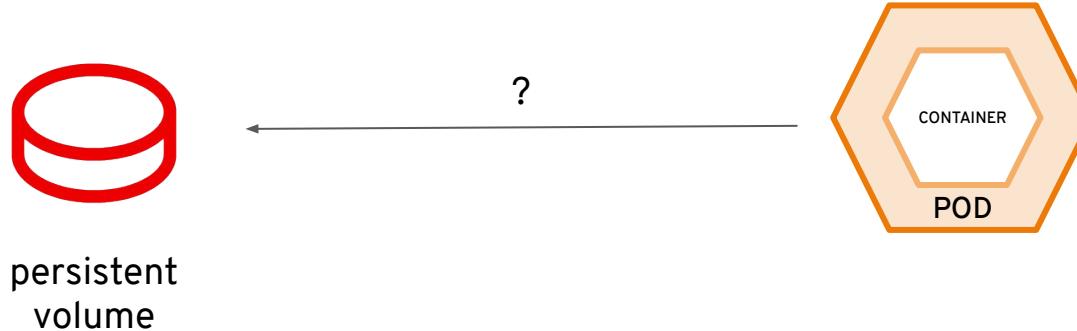


# routes make services accessible to clients outside the environment via real-world urls

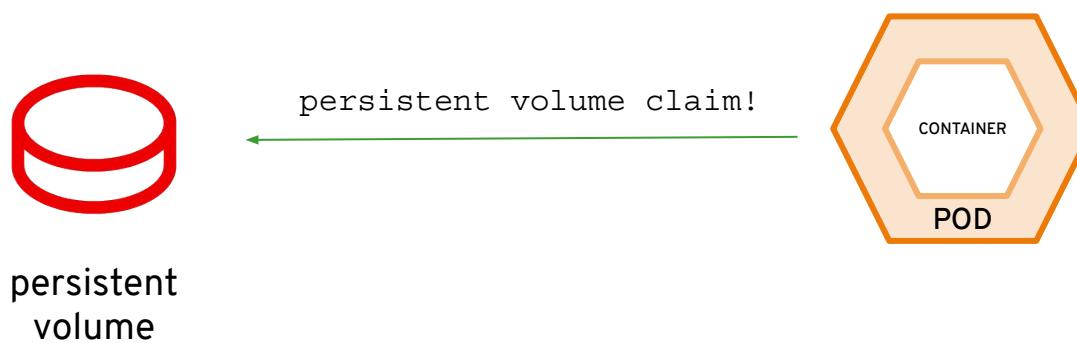
```
> curl http://app-prod.mycompany.com
```



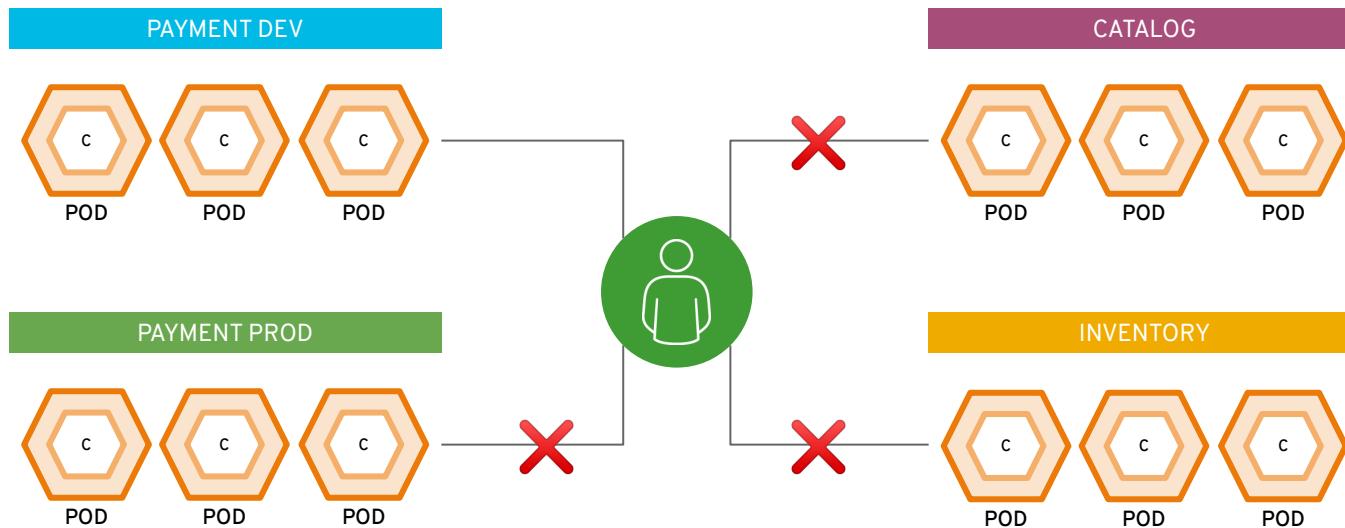
# Kubernetes storage



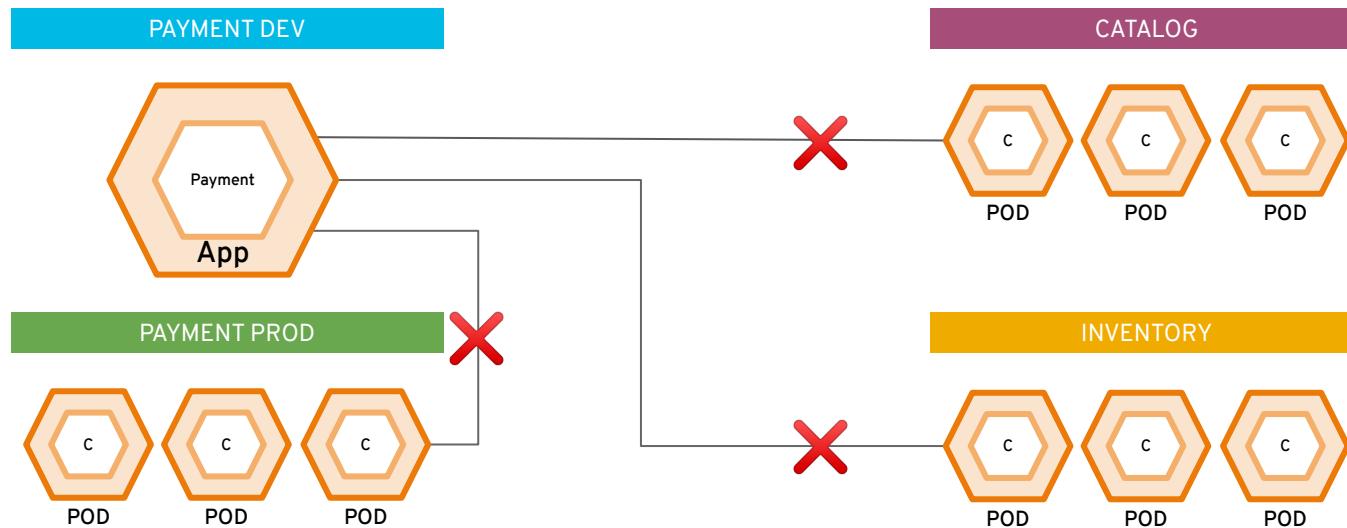
# Kubernetes storage



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



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



# Demo!





# OpenShift 4 Architecture

# your choice of infrastructure

COMPUTE

NETWORK

STORAGE

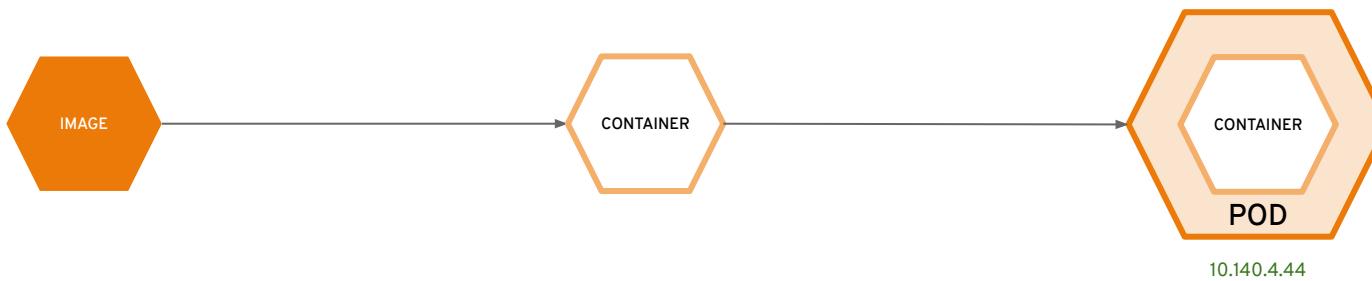
# workers run workloads



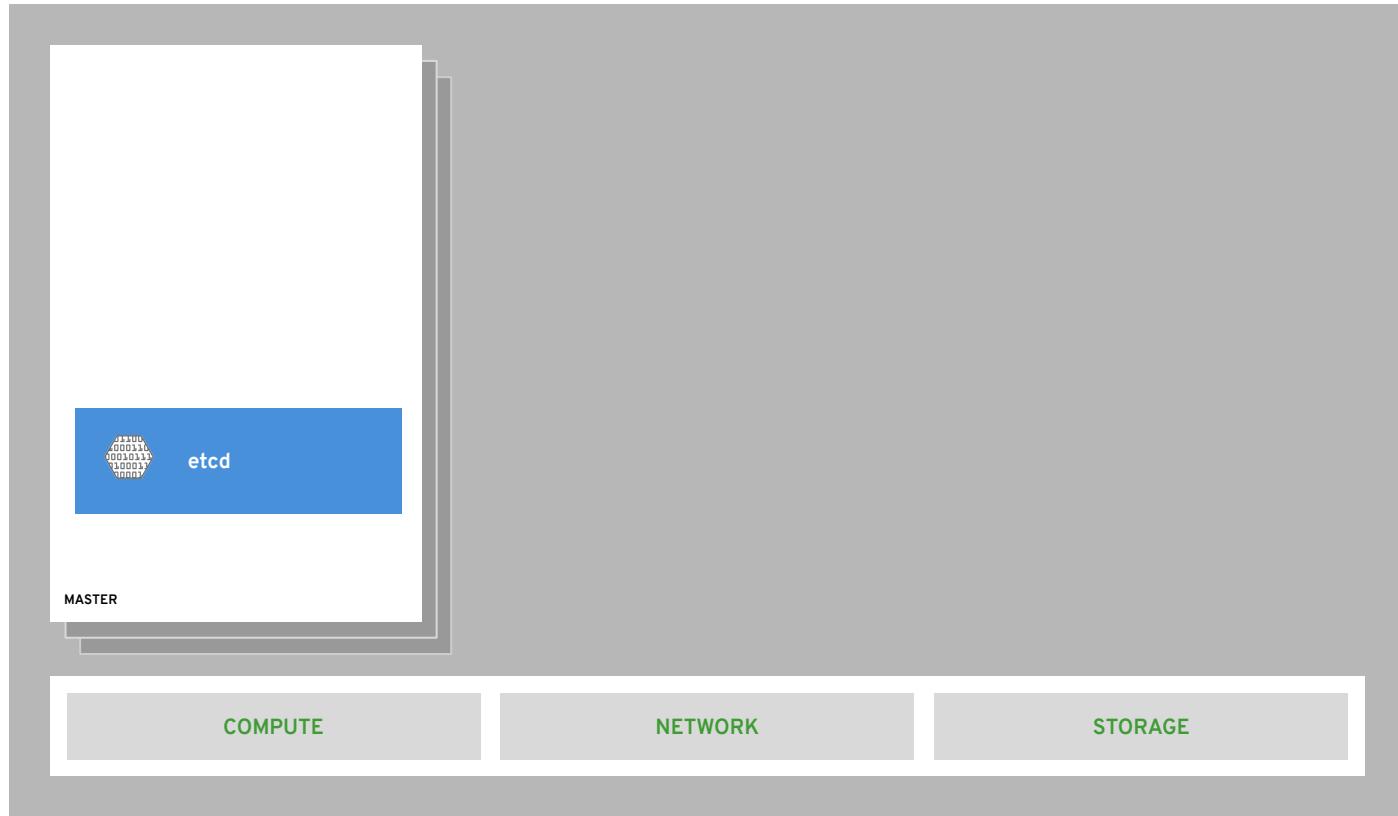
# masters are the control plane



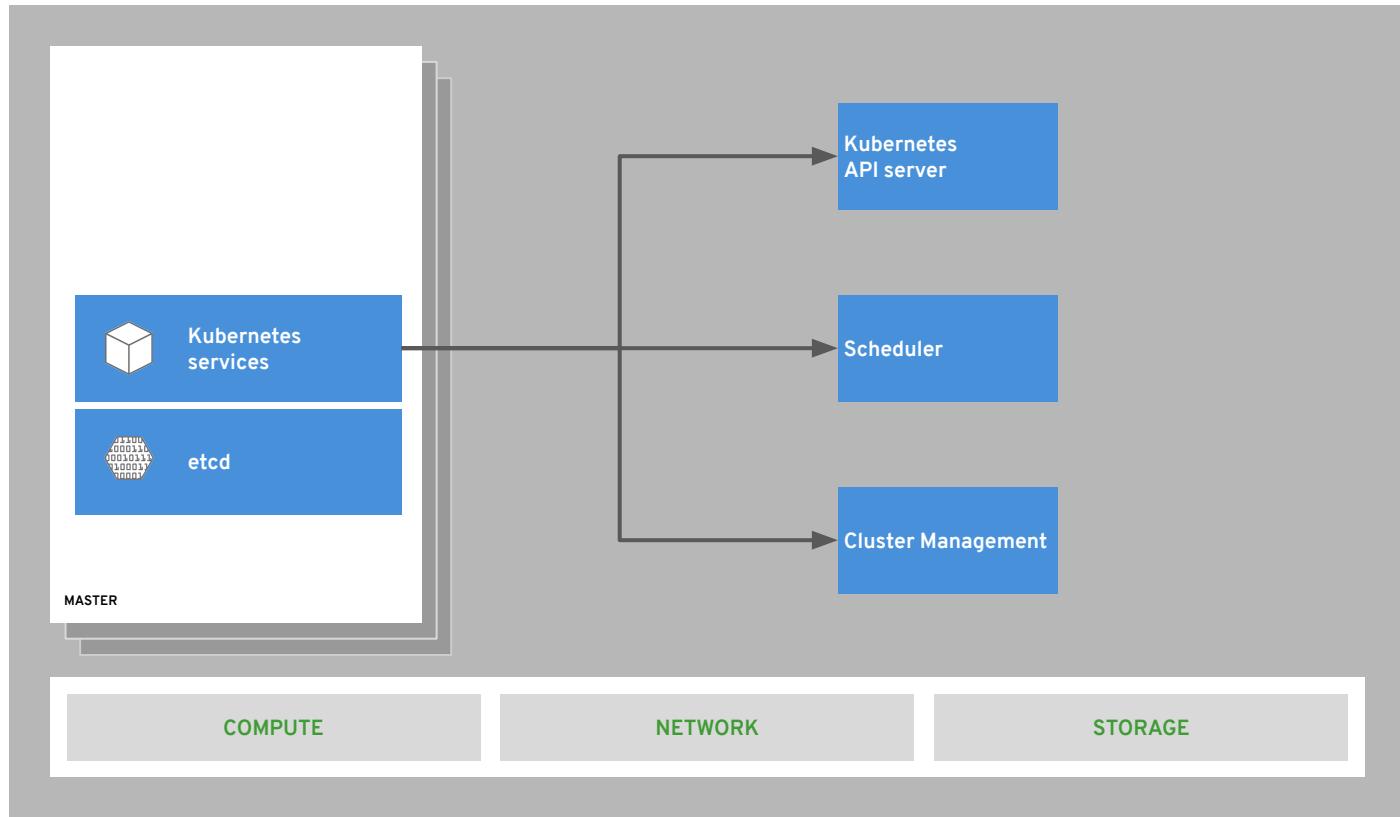
# everything runs in pods



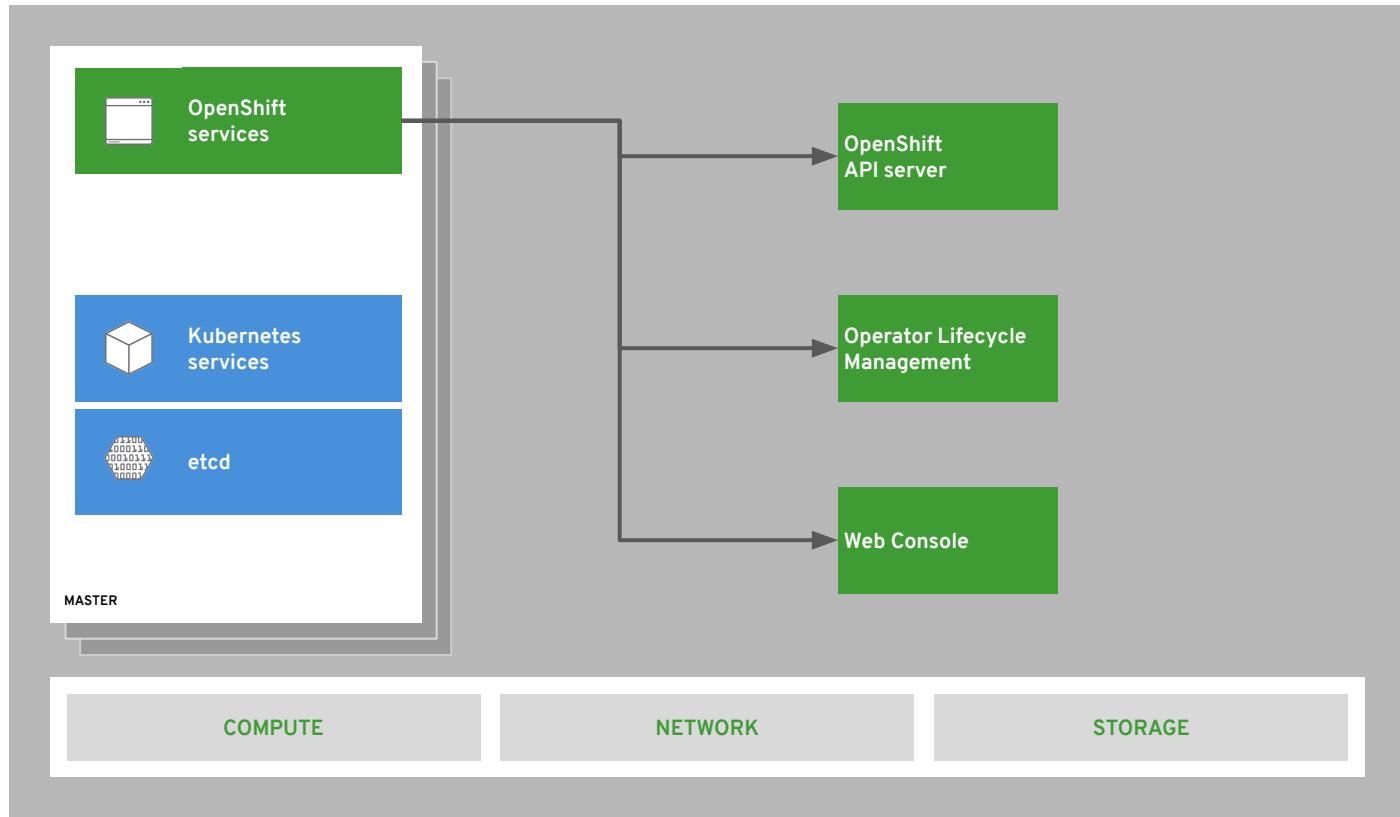
# state of everything



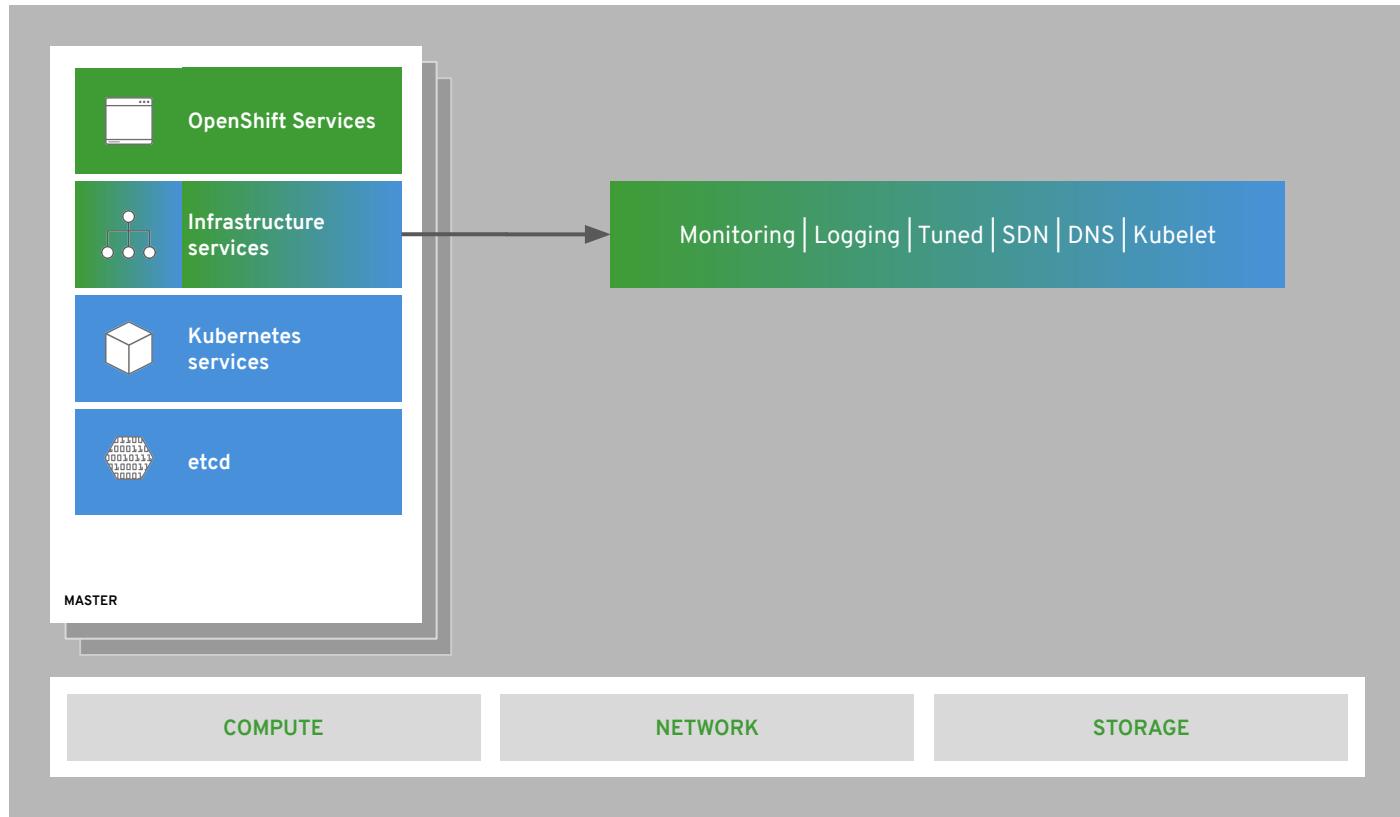
# core kubernetes components



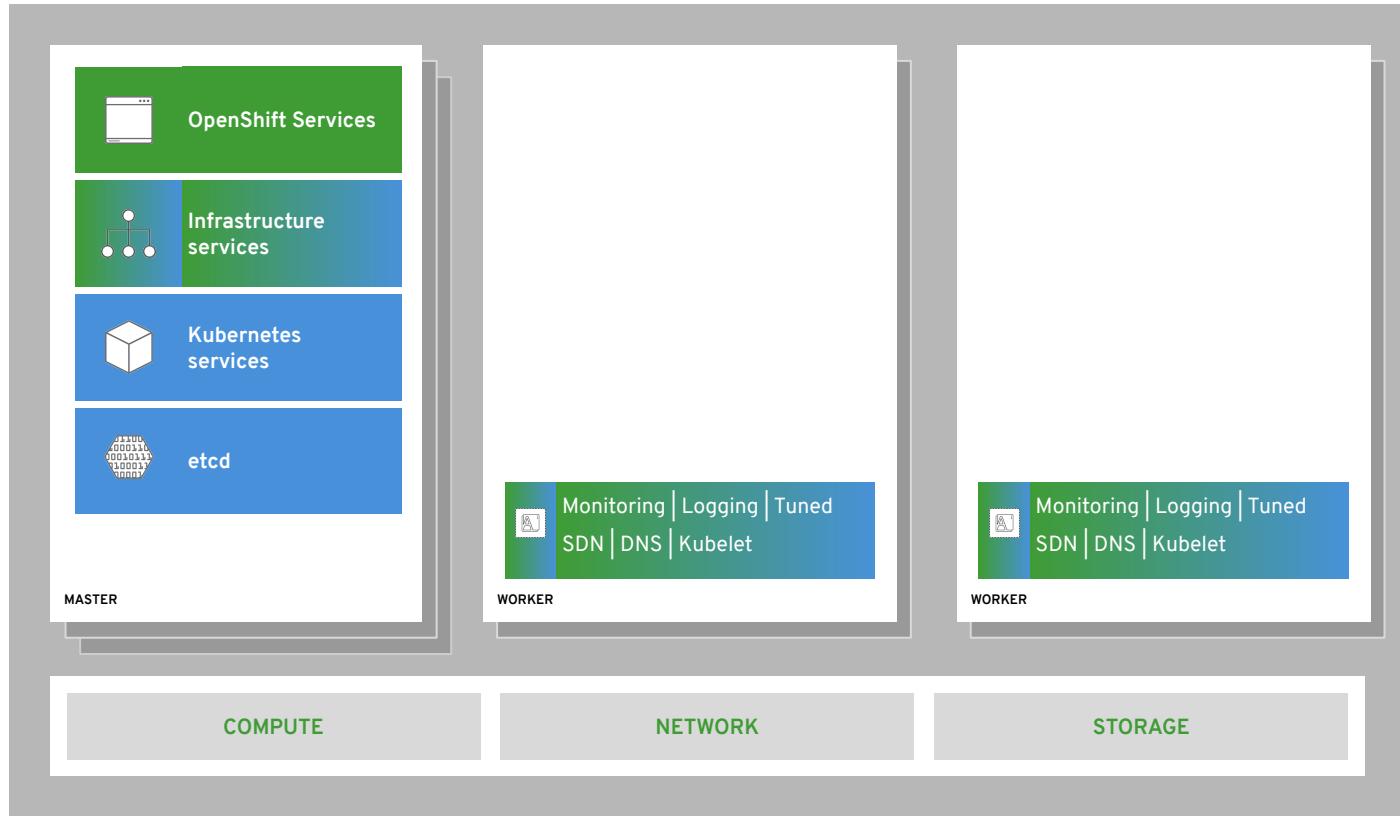
# core OpenShift components



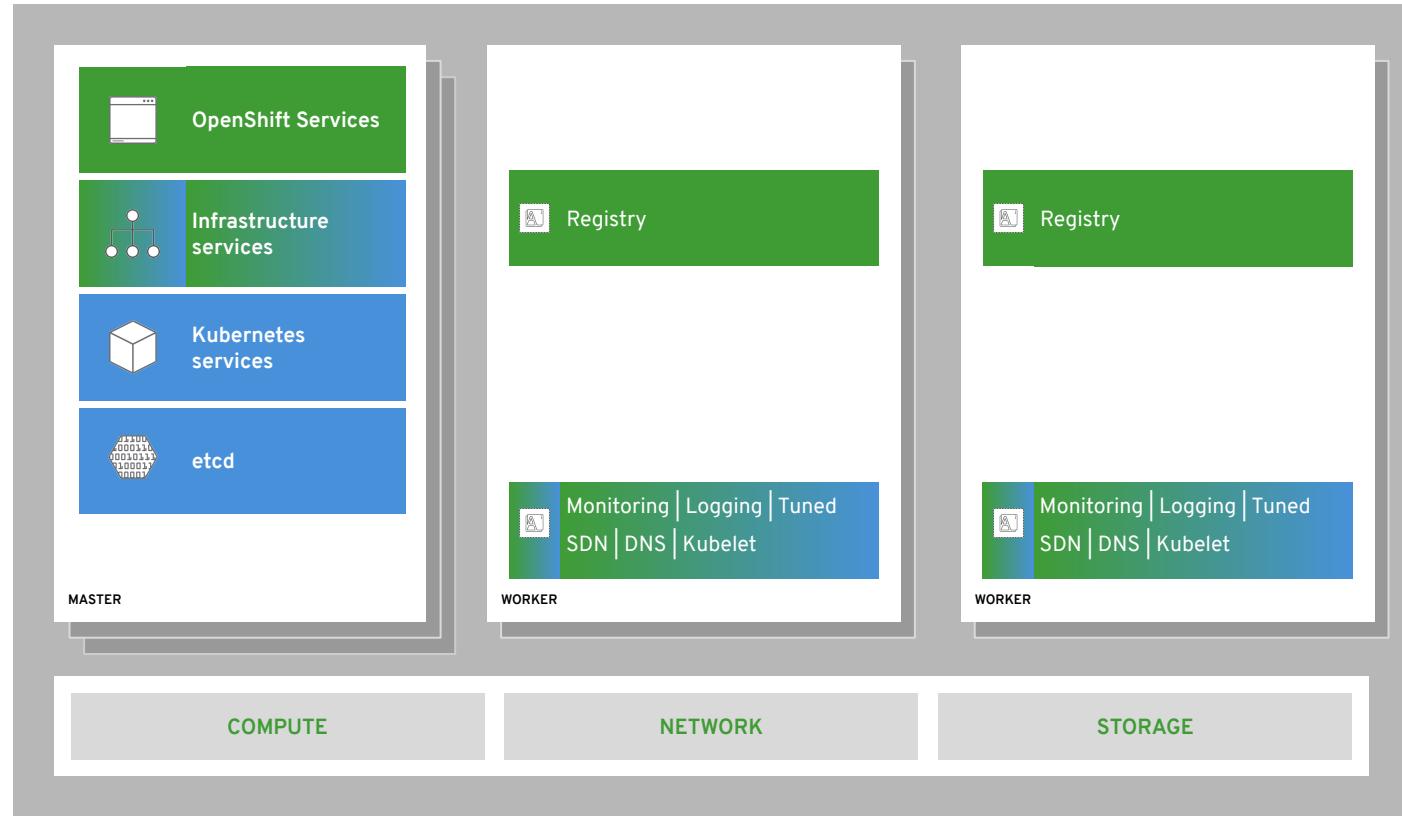
# internal and support infrastructure services



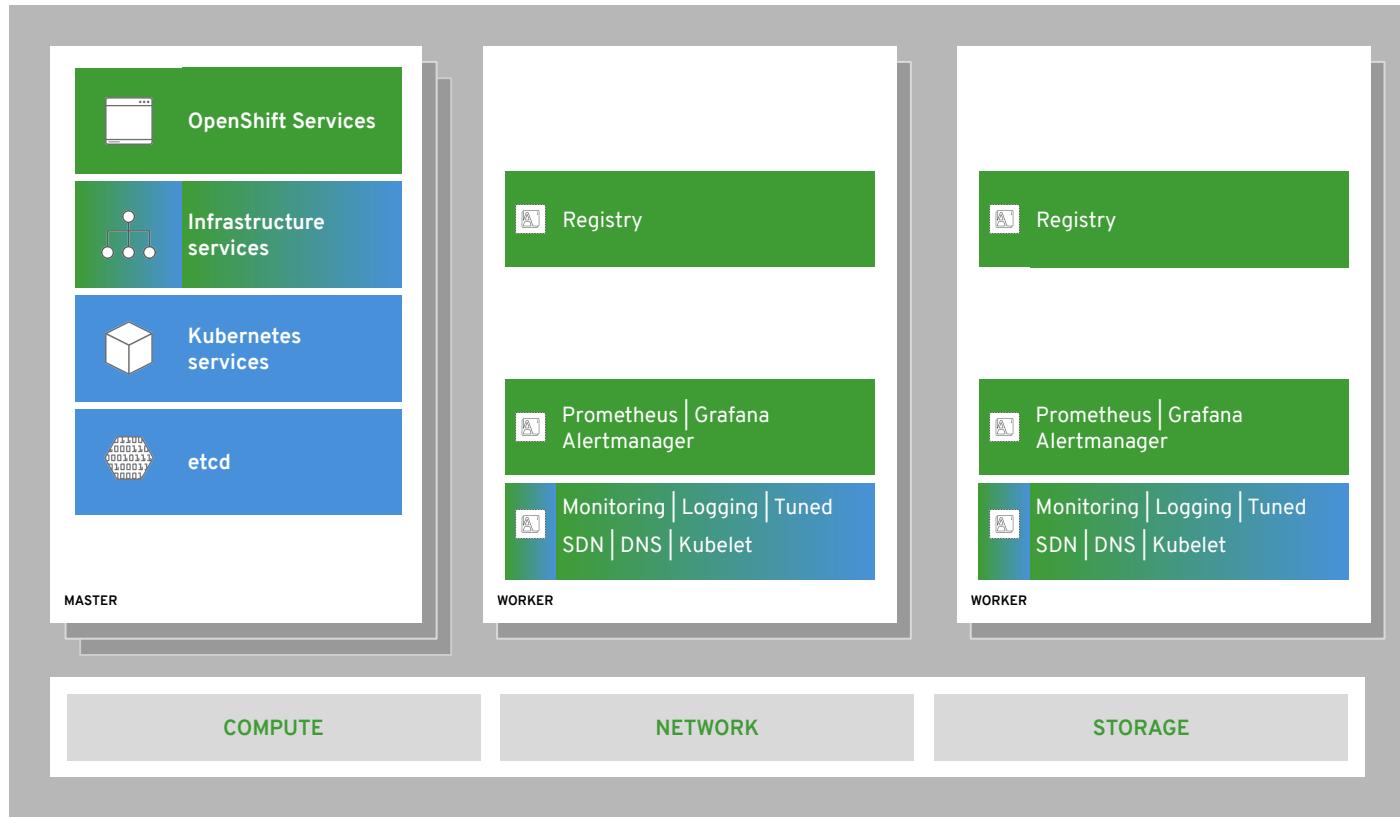
run on all hosts



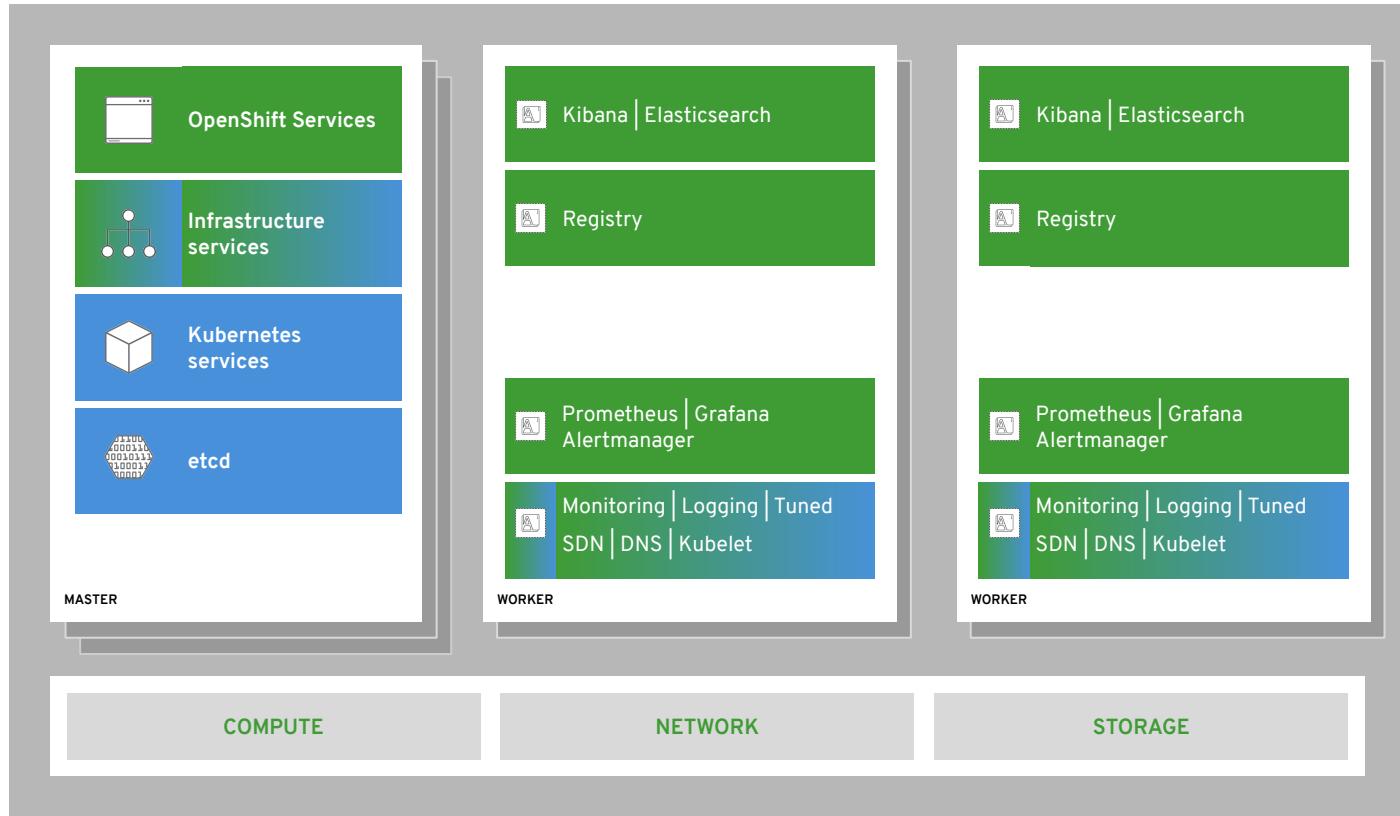
# integrated image registry



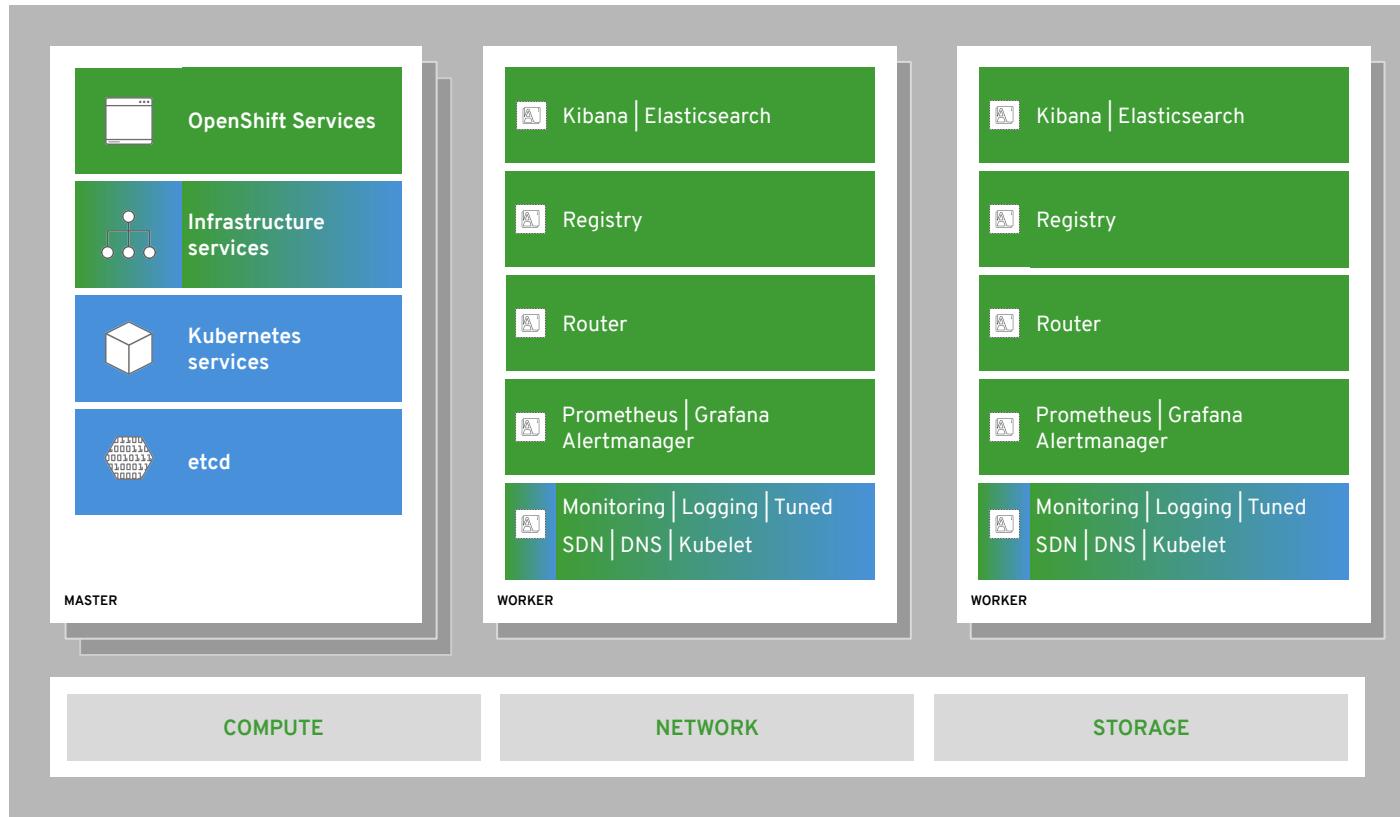
# cluster monitoring



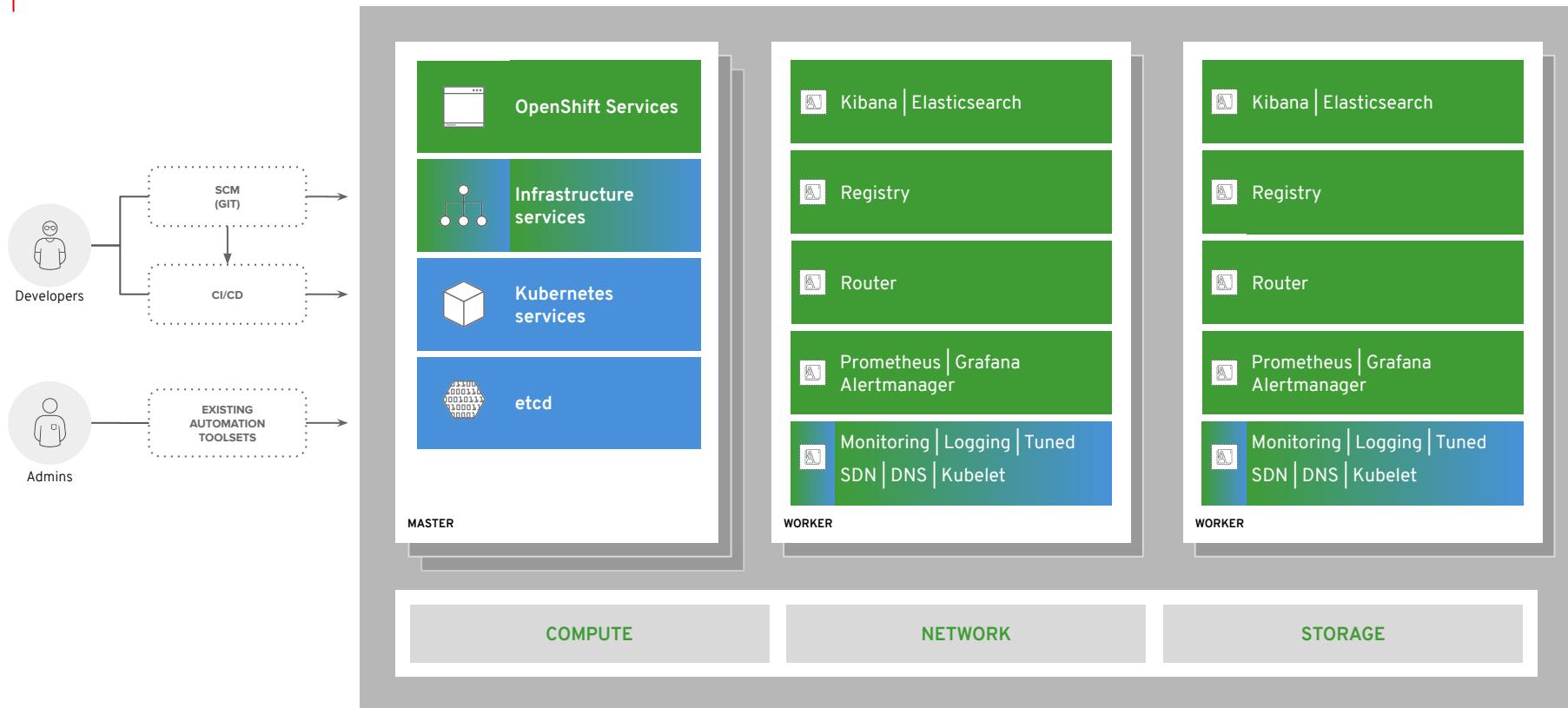
# log aggregation



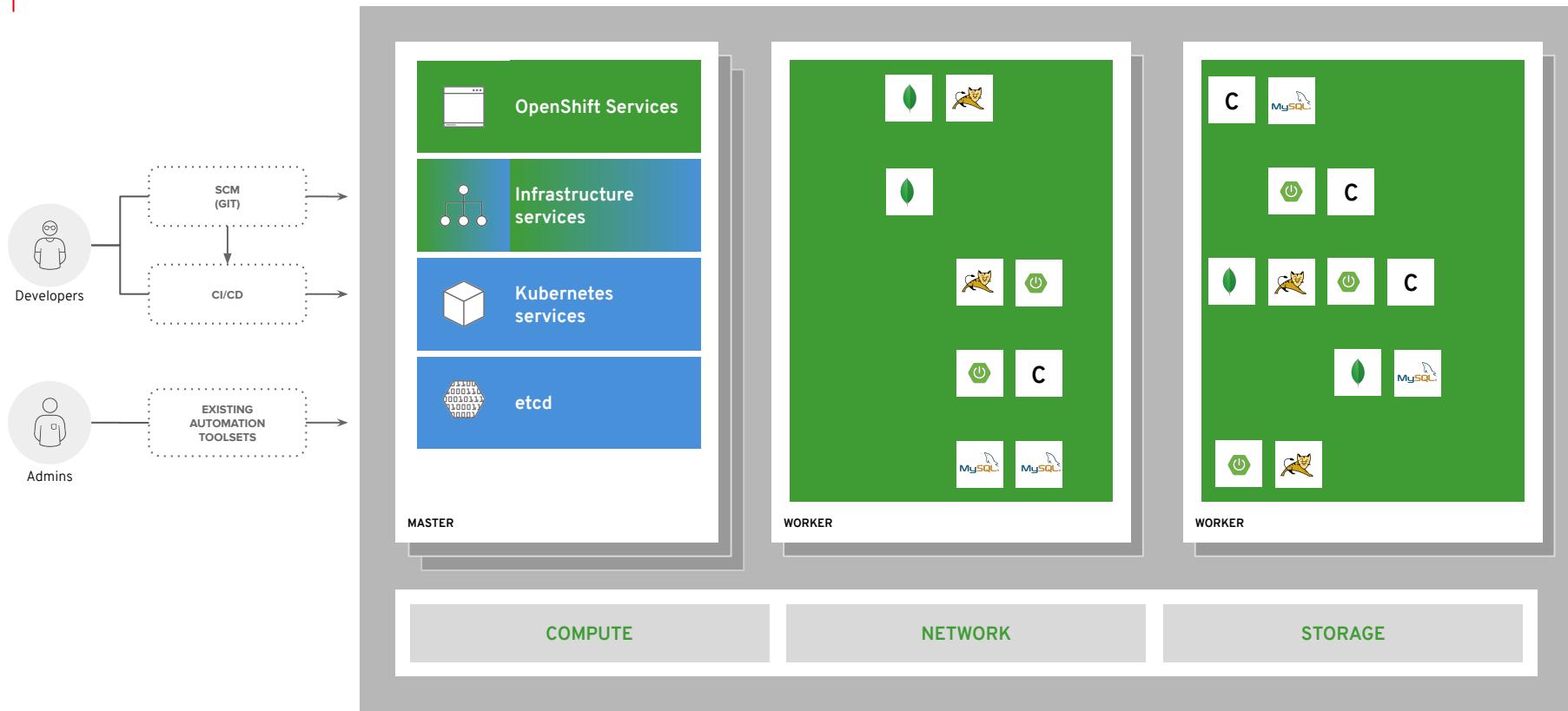
# integrated routing



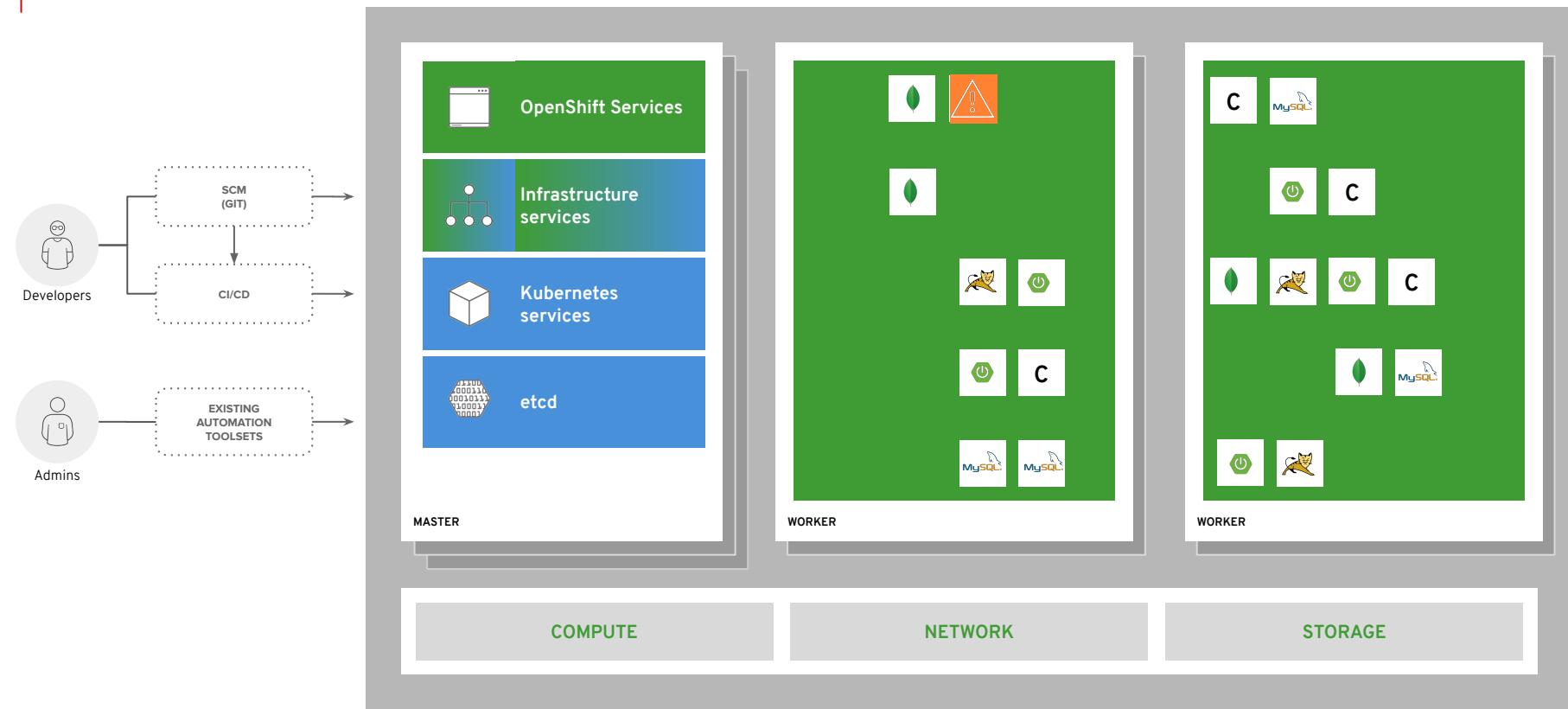
# dev and ops via web, cli, API, and IDE



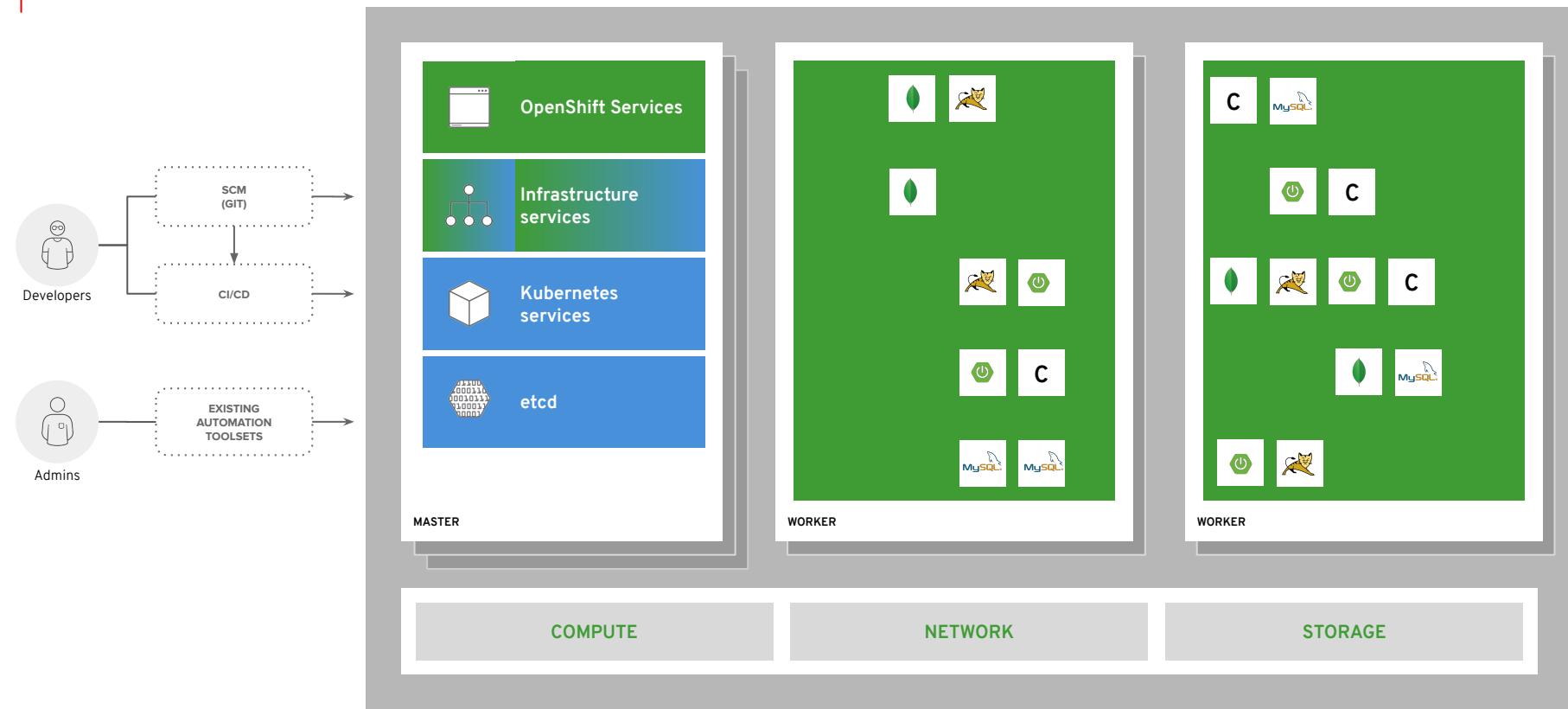
# applications also run on workers



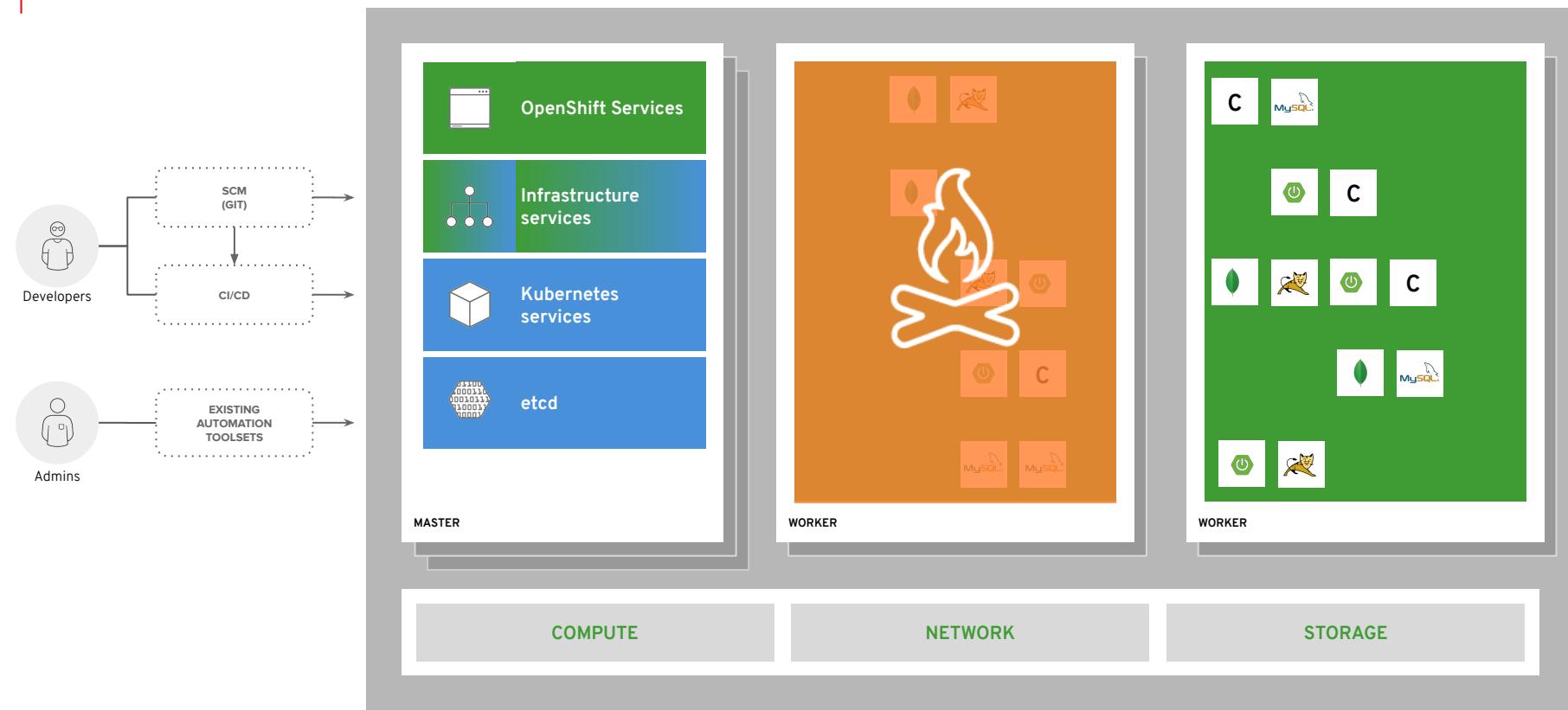
# auto-healing failed pods



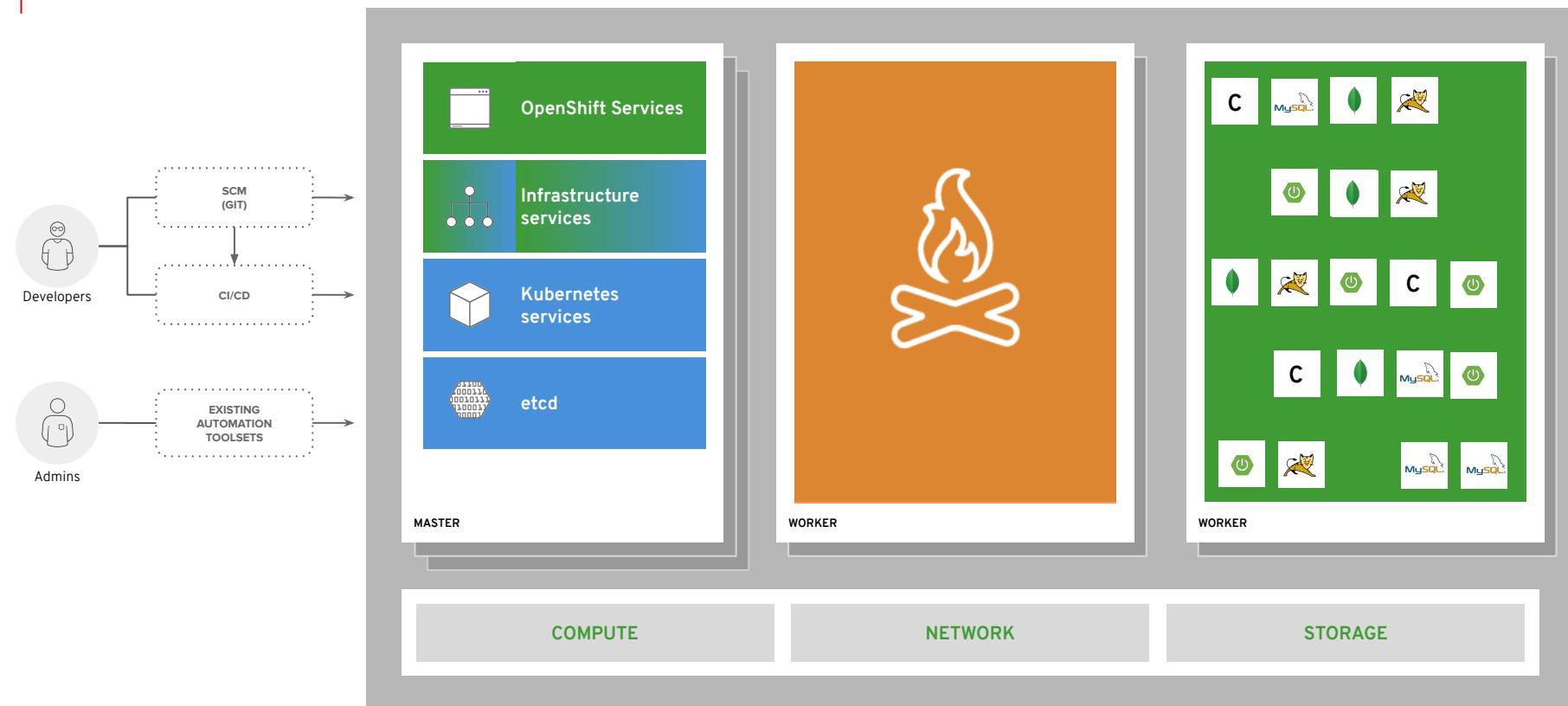
# auto-healing failed pods



# 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

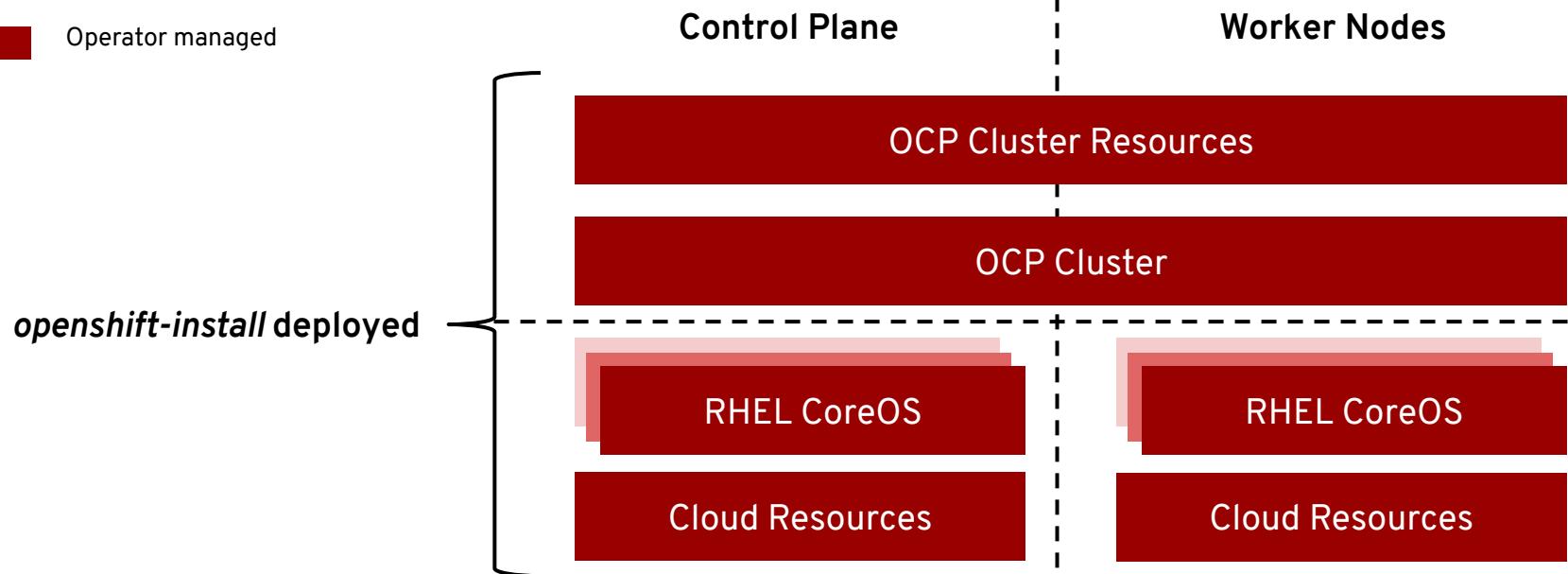
Deploy directly from the Azure console. Jointly managed by Red Hat and Microsoft Azure engineers.

### OpenShift Dedicated

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

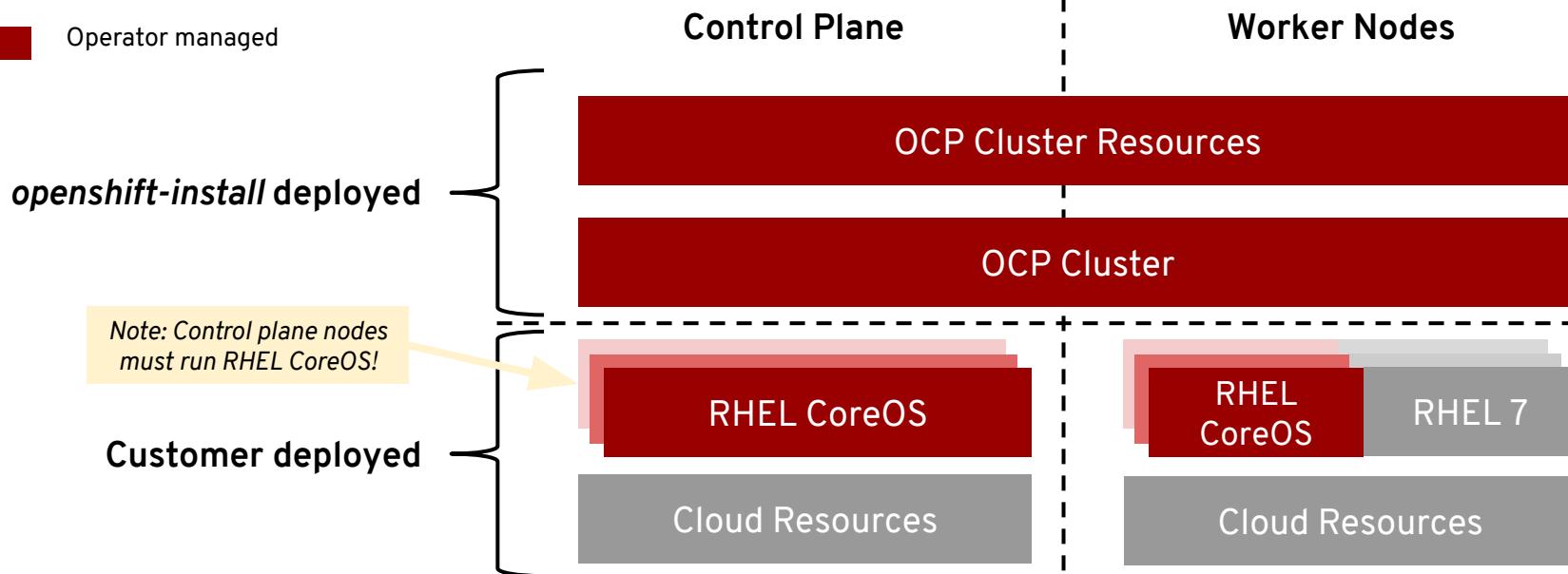
# Full-stack Automated Installation

- User managed
- Operator managed



# Pre-existing Infrastructure Installation

- User managed
- Operator managed

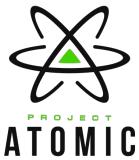




# Operations and infrastructure deep dive

# 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.

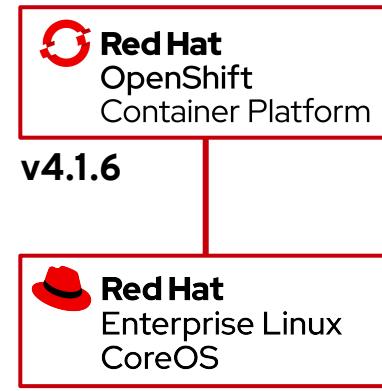
**Red Hat Enterprise Linux CoreOS is managed by the cluster**

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

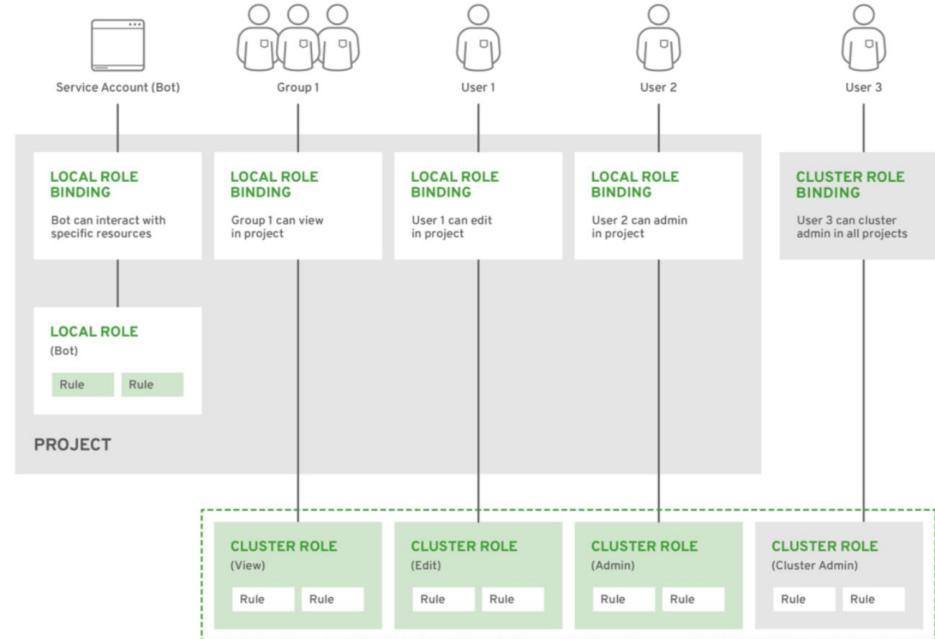


Figure 12 - Authorization Relationships

# Operator Framework

Open source toolkit to  
manage application  
instances on Kubernetes

# WHY OPERATOR FRAMEWORK?



# Kubernetes-native day 2 management

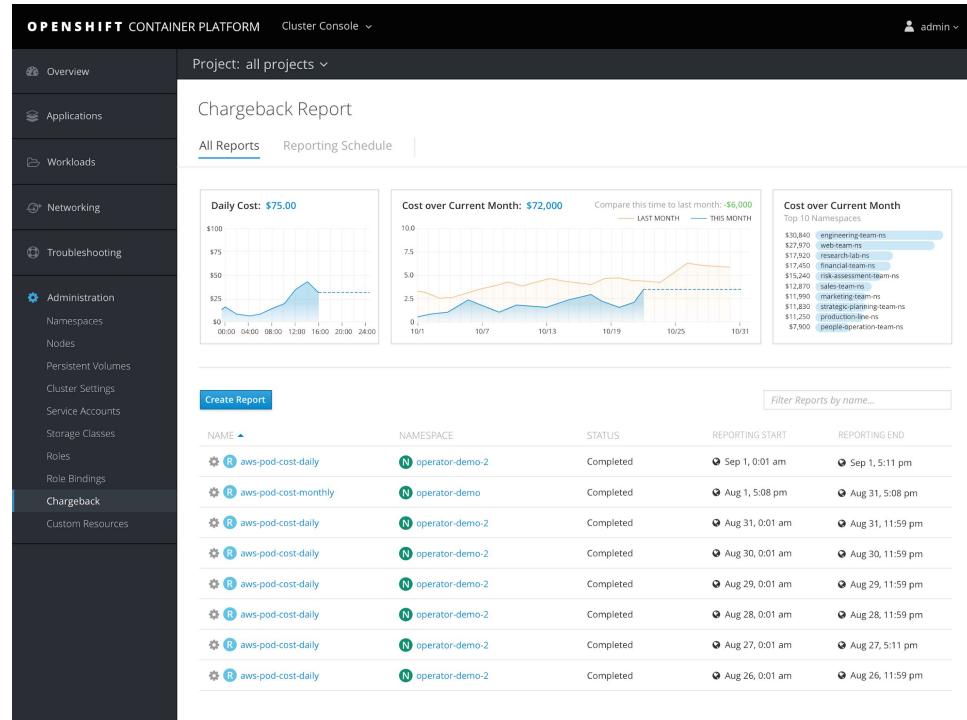


 A white icon consisting of four arrows pointing outwards from a central point, forming a cross shape.	Flexible app architectures	 A white icon containing mathematical symbols: a right-angle bracket with $\pi$ , a circle with $e=mc^2$ , and a double integral symbol.	No reinvention of core concepts
 A white icon showing a sequence of three boxes: a square with a dashed arrow, a curved arrow, and a box with a checkmark.	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

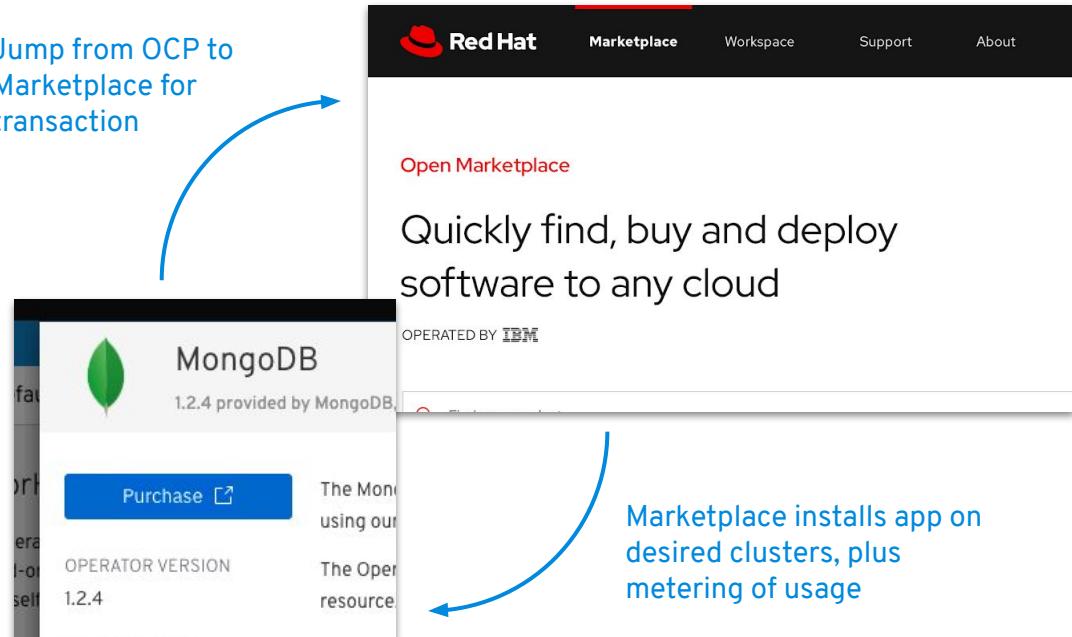
# Open Marketplace in collaboration with IBM

## 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

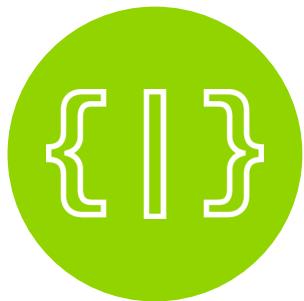
## Ability to forward logs elsewhere

- External elasticsearch, Splunk, etc

# Build and Deploy Container Images

Tools and automation  
that makes developers  
productive quickly

# Build Containers for Cloud-Native Architecture



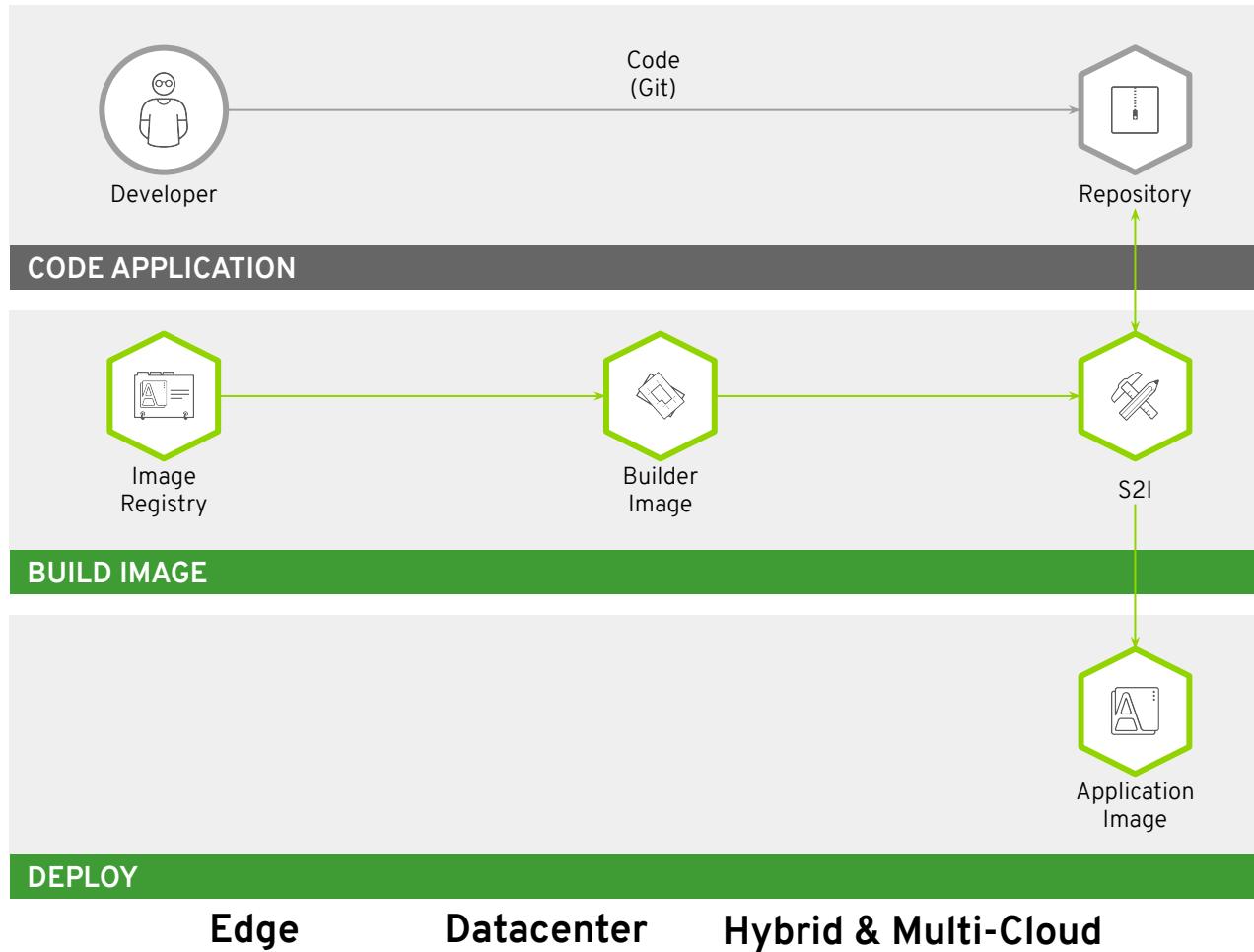
DEPLOY YOUR  
SOURCE CODE

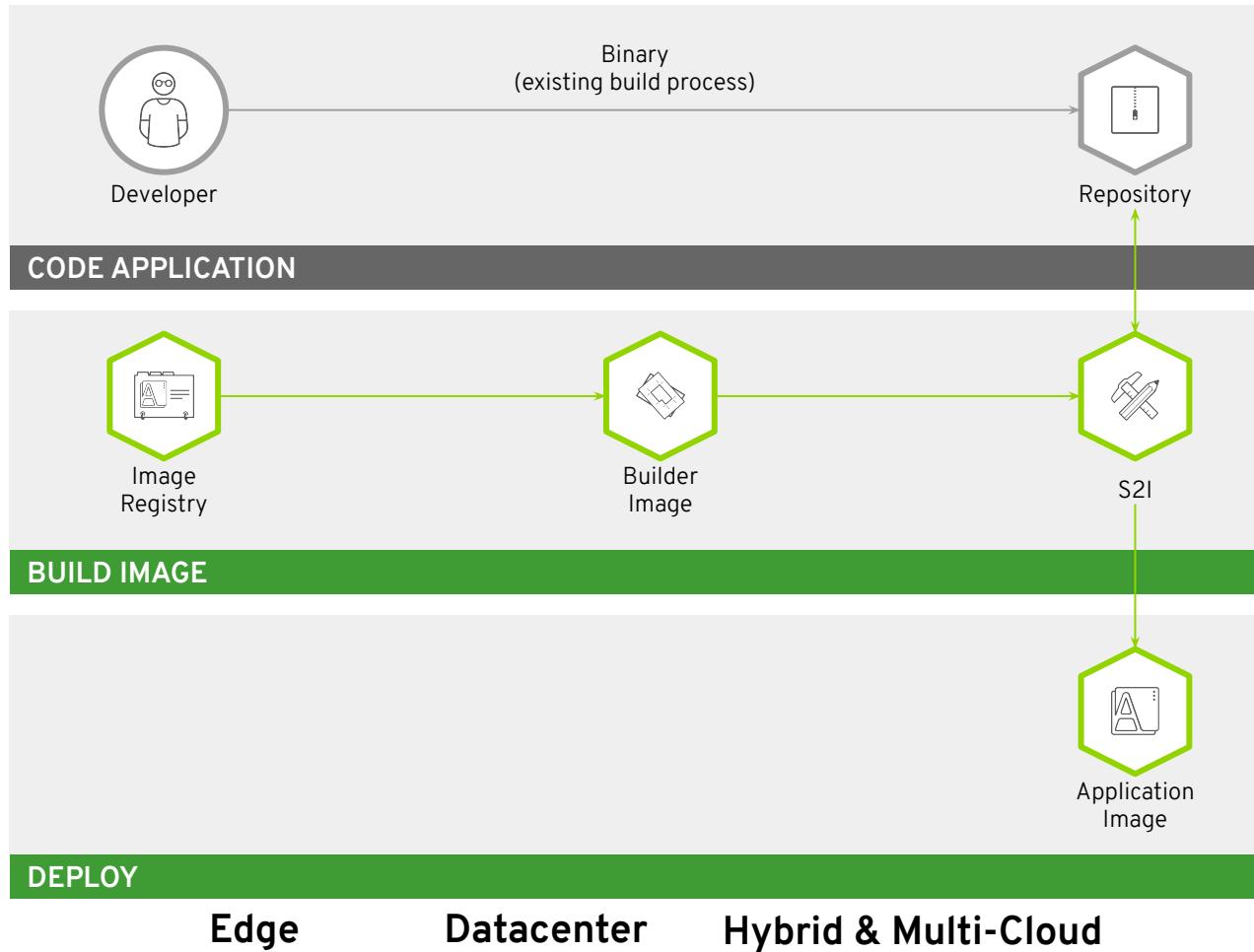


DEPLOY YOUR  
APP BINARY



DEPLOY YOUR  
CONTAINER IMAGE





# Road Map

Reference Information

# OpenShift Roadmap

Q2 2020 OpenShift 4.4		H2 2020 OpenShift 4.5/4.6		2021 OpenShift 4.7+			
HOSTED	PLATFORM	HOSTED	PLATFORM	HOSTED	PLATFORM		
HOSTED	PLATFORM	HOSTED	APP	HOSTED	APP		
<ul style="list-style-type: none"><li>• OpenShift Serverless (Knative) GA</li><li>• Guided application creation</li><li>• OpenShift Pipelines (Tekton) TP</li><li>• OpenShift Builds (v2) DP</li><li>• Jenkins Operator DP</li><li>• Helm 3 GA</li></ul> <ul style="list-style-type: none"><li>• Improved Dev Console for monitoring</li><li>• Helm Charts in Developer Catalog</li></ul> <ul style="list-style-type: none"><li>• Multi-cluster summary dashboards</li><li>• Centralized cluster updates</li><li>• OpenShift for IBM Power</li><li>• RHV (IPI), RHOSP (UPI), Azure (UPI)</li><li>• Native Metric Dashboards in the Console</li><li>• Descheduler (TP)</li><li>• HA Proxy 2.0</li><li>• SCTP support</li><li>• CSI snapshot/restore (TP)</li><li>• DNS Forwarding</li><li>• Cluster etcd managed by Operator</li><li>• Automated image pruning</li></ul> <ul style="list-style-type: none"><li>• OSD SOC2 Type 1 Certification</li><li>• OSD on GCP</li><li>• OSD private clusters</li><li>• Cost management GA</li></ul>	<th>DEV</th> <th>APP</th> <th>DEV</th> <th>APP</th> <th>DEV</th> <th>APP</th>	DEV	APP	DEV	APP	DEV	APP
		<ul style="list-style-type: none"><li>• OpenShift Serverless Eventing GA</li><li>• OpenShift Pipelines (Tekton) GA</li><li>• OpenShift Builds (v2) TP</li><li>• Jenkins Operator TP</li><li>• Simplify Operator Lifecycle interactions</li><li>• Build Operator catalogs in container images</li><li>• Helm workflows in Console</li><li>• Monitor application workloads</li><li>• VMware vSphere (IPI), RHV (UPI)</li><li>• AWS &amp; Azure custom regions &amp; endpoints</li><li>• Node Terminal Access in the Console</li><li>• Log forwarding GA</li><li>• OVN GA, OVN Egress Firewall/Router/IP</li><li>• Edge: 3-node clusters, remote workers</li><li>• Compliance Operator</li><li>• IPv6 (single/dual stack on control plane)</li><li>• HTTP/2 and gRPC Support for Router</li><li>• RHCOS installer, static networking UX</li><li>• Graceful shutdown and recovery procedure</li><li>• Logging: Elasticsearch v6</li><li>• AWS Spot instance support &amp; IAM Identity</li><li>• Windows Containers</li></ul> <ul style="list-style-type: none"><li>• OSD SOC &amp; ISO Certifications</li><li>• OSD RWX storage</li><li>• OSD log forwarding</li></ul>		<ul style="list-style-type: none"><li>• OpenShift Builds (v2) GA</li><li>• Jenkins Operator GA</li></ul> <ul style="list-style-type: none"><li>• Improvements to GitOps experience</li><li>• Improvements to Operator management</li><li>• Hybrid Operators with Operator-SDK</li></ul> <ul style="list-style-type: none"><li>• Microsoft Hyper-V (UPI)</li><li>• Single node cluster</li><li>• Enable user namespaces</li><li>• Utilize cgroups v2</li><li>• Keycloak/External IdP integration</li><li>• Priority and Fairness for APIserver</li><li>• Azure Hub and HCI plus other public clouds</li><li>• Network Enhancements derived from OVN</li></ul> <ul style="list-style-type: none"><li>• OSD enhanced consumption billing</li></ul>			

# 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](#)