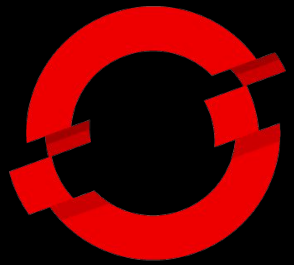


Red Hat OpenShift

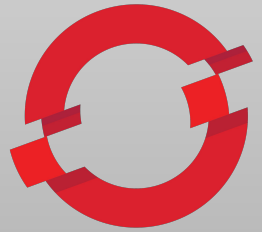
MELBOURNE MEETUP
May 29 2019

A BIG THANK YOU TO OUR HOSTS

High performance. Delivered.

Agenda

- OpenShift Commons and Summit Highlights
- Container Security Reference Architecture
- OpenShift 4 - The Automated Platform
- Quarkus - Supersonic Subatomic Java



OPENSHIFT

CoreOS

OpenShift Commons and Summit Highlights

OPENSHIFT COMMONS @ RED HAT SUMMIT 2019

MONDAY, MAY 6th, 9:00-6:00 PM - WESTIN BOSTON WATERFRONT

CUSTOMER SPEAKERS:

- NASA Langley
- RBC/Nvidia
- UPS
- NGA / Ampsight
- Volkswagen
- Best Buy Canada
- Eli Lilly and Co
- THYSSEN KRUPP ELEVATORS
- Telco panel:
  - Optus, Deutsche Telekom, Bell Canada, Vodafone Turkey
- FSI panel:
  - Asiakastieto, Banco Hipotecario
  - Pending: RBS, CIBC

EVENT SITE: https://commons.openshift.org/gatherings/Boston_2019.html

EXPECTING 750 - 1,000 ATTENDEES

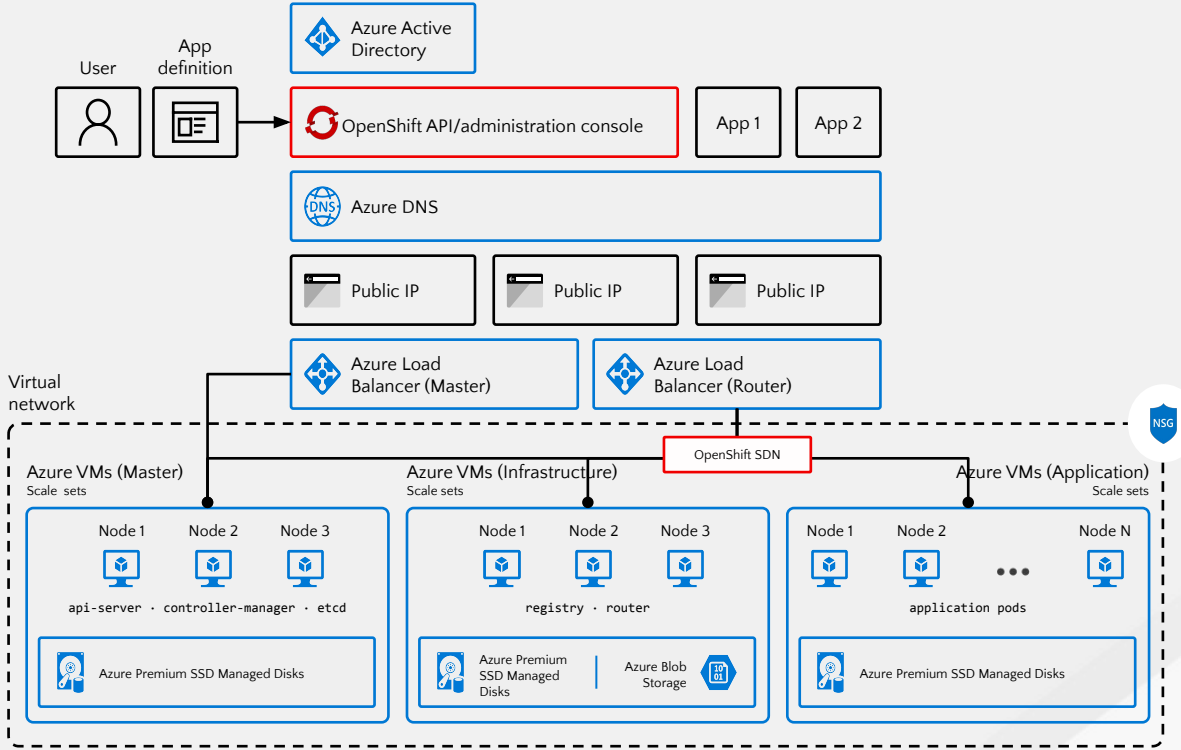
COMMONS REGISTRATION IS PART OF SUMMIT REGISTRATION

AZURE RED HAT OPENSHIFT LAUNCH

RUNNING YOUR OWN RED HAT OPENSHIFT CLUSTER

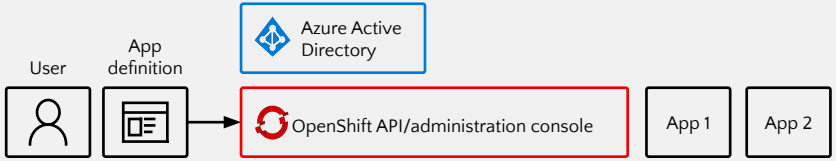
Responsibilities	
User management	
Project and quota management	
Application lifecycle	
Cluster creation	
Cluster management	
Monitoring and logging	
Network configuration	
Software and security updates	
Platform support	

Customer Microsoft and Red Hat



SIMPLIFY OPERATIONS WITH AZURE RED HAT OPENSHIFT

Responsibilities	
User management	Customer
Project and quota management	Customer
Application lifecycle	Customer
Cluster creation	Microsoft and Red Hat
Cluster management	Microsoft and Red Hat
Monitoring and logging	Microsoft and Red Hat
Network configuration	Microsoft and Red Hat
Software and security updates	Microsoft and Red Hat
Platform support	Microsoft and Red Hat



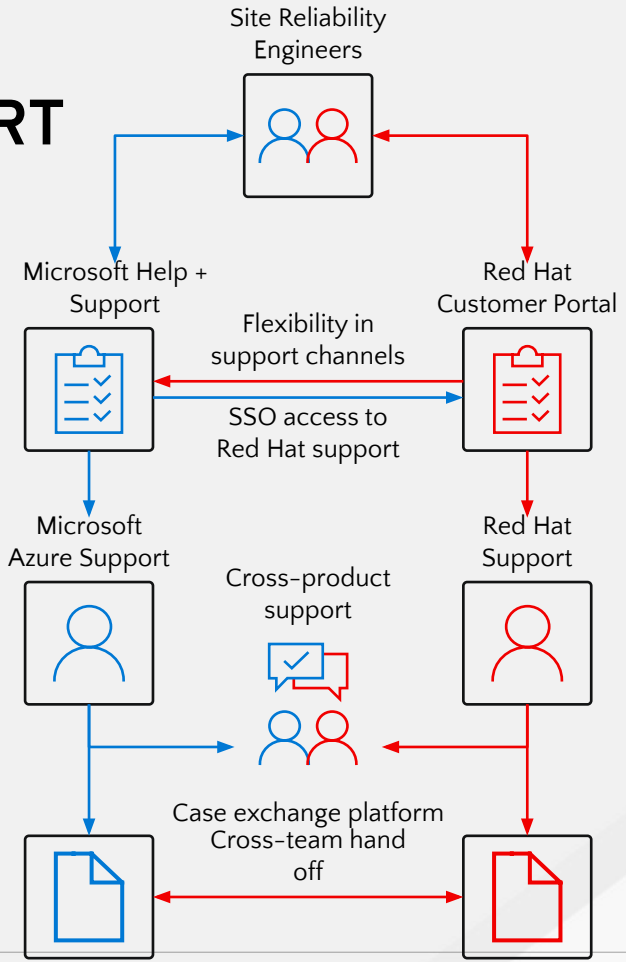
Let Microsoft and Red Hat...

- Manage all your clusters
- Monitor and operate your VMs
- Secure your nodes
- Manage environment patches

UNIFIED OPERATIONS AND SUPPORT

Jointly engineered, operated, and supported by Microsoft and Red Hat

- In-portal integrated support experience is available 24x7
- ISO 27001 compliant B2B communication channel
- Co-located support with Red Hat on-site team
- Integrated case systems
- Microsoft and Red Hat security response team collaboration



RED HAT® OPENSHIFT

Developer Preview: try.openshift.com

Trusted enterprise Kubernetes

- Trusted Host, Content, Platform
- Full Stack Automated Install
- Over the Air Updates & Day 2 Mgt

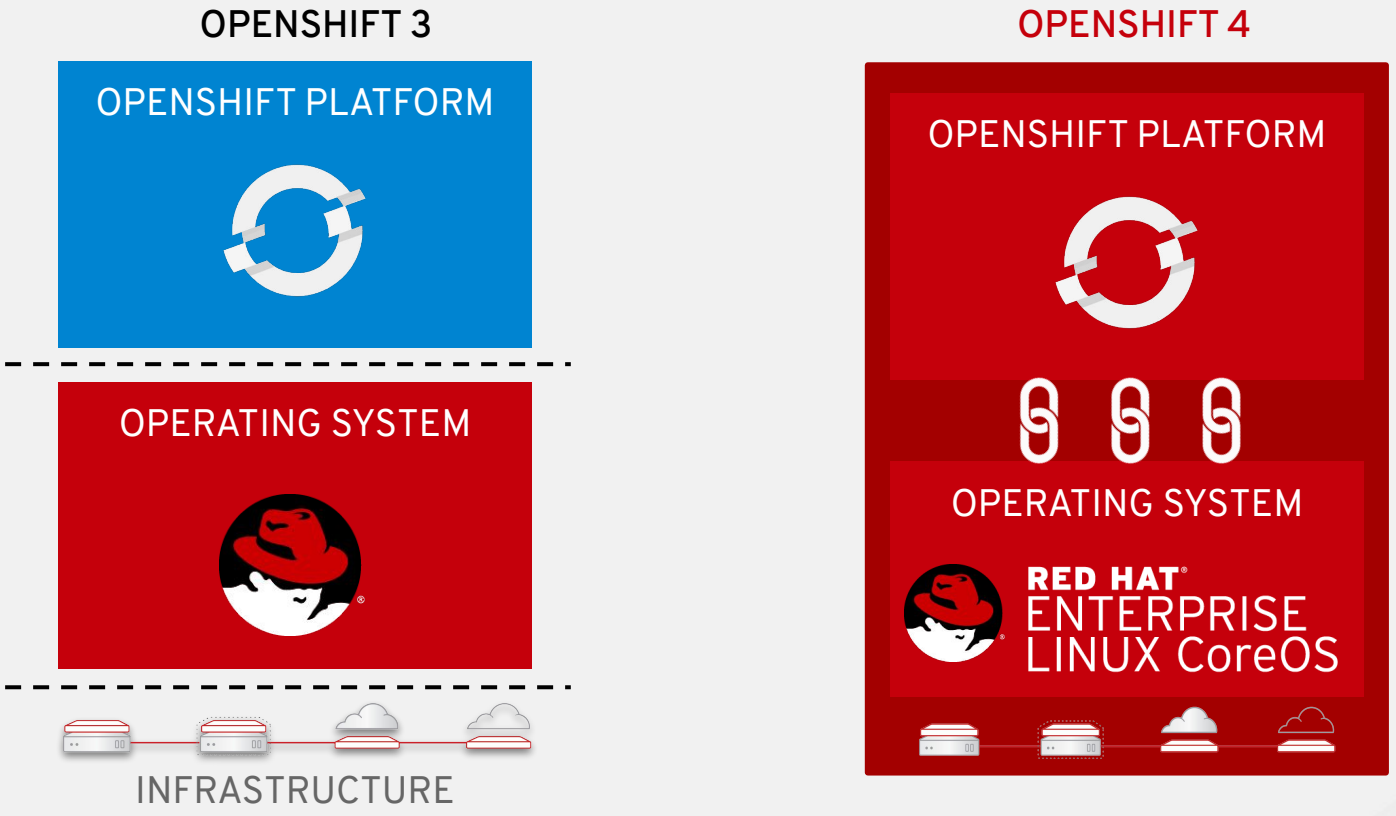
A cloud-like experience, everywhere

- Hybrid, Multi-Cluster Management
- Operator Framework
- Operator Hub & Certified ISVs

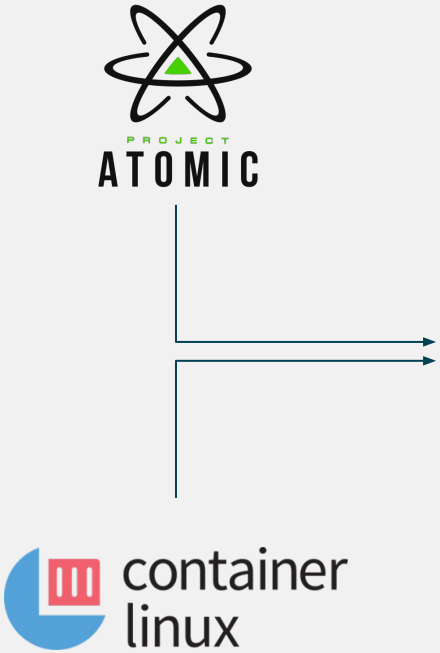
Empowering developers to innovate

- OpenShift Service Mesh (Istio)
- OpenShift Serverless (Knative)
- CodeReady Workspaces (Che)

FULL STACK AUTOMATED INSTALL



RHEL COREOS

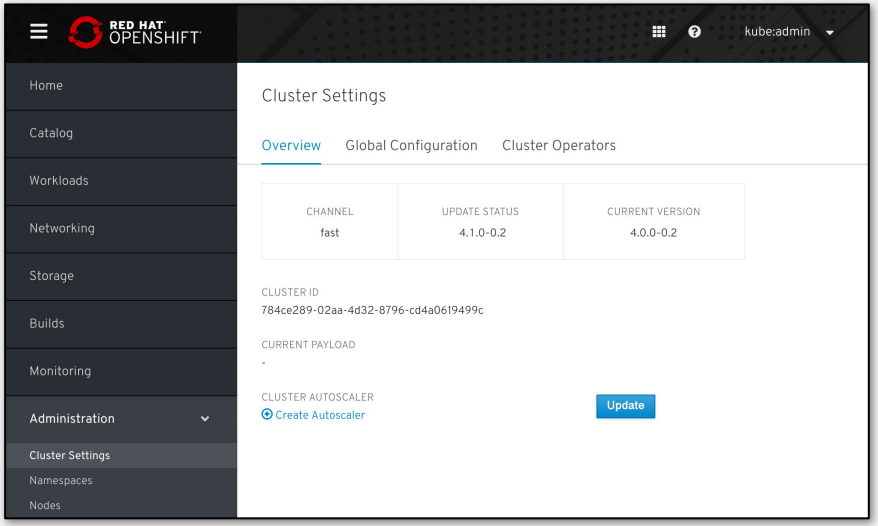


Red Hat
Enterprise Linux
CoreOS

- 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

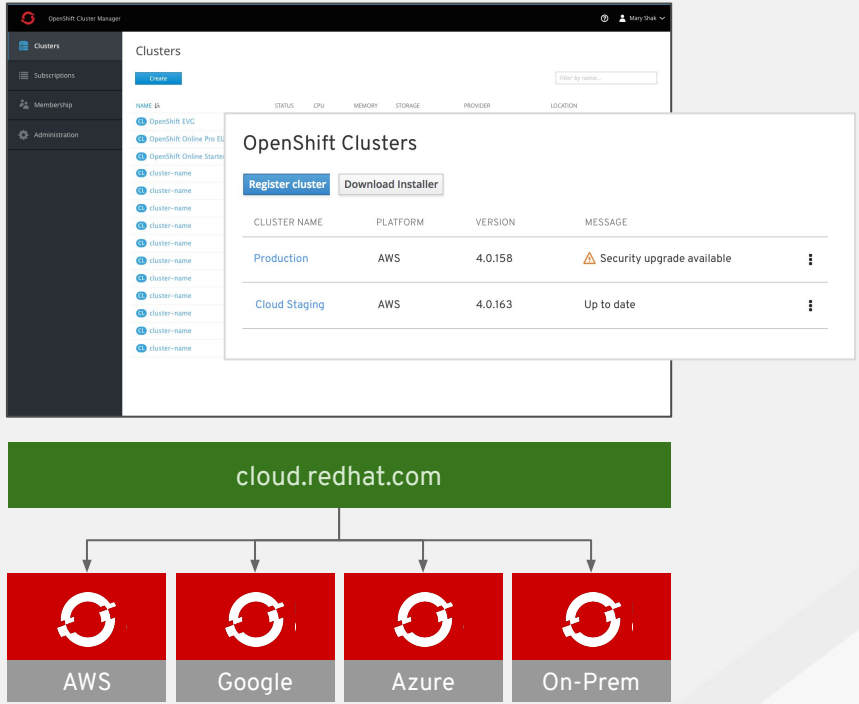
OVER-THE-AIR UPDATES

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



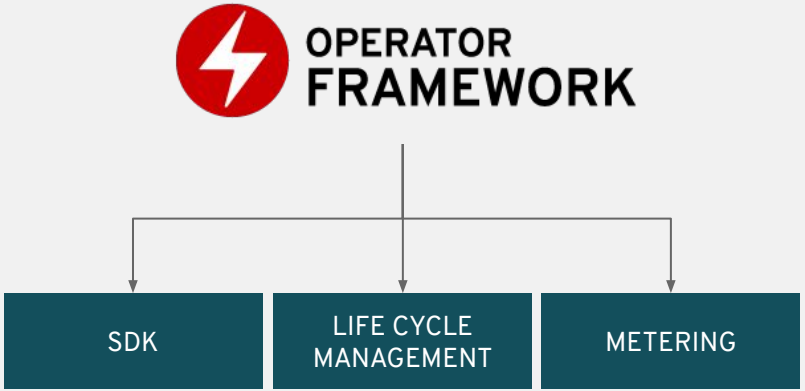
UNIFIED HYBRID CLOUD

- Multi-cluster management
  - New clusters on AWS, Azure, Google, vSphere, OpenStack, and bare metal
  - Register existing clusters
  - Including OpenShift Dedicated
- Management operations
  - Install new clusters
  - View all registered clusters
  - Update clusters



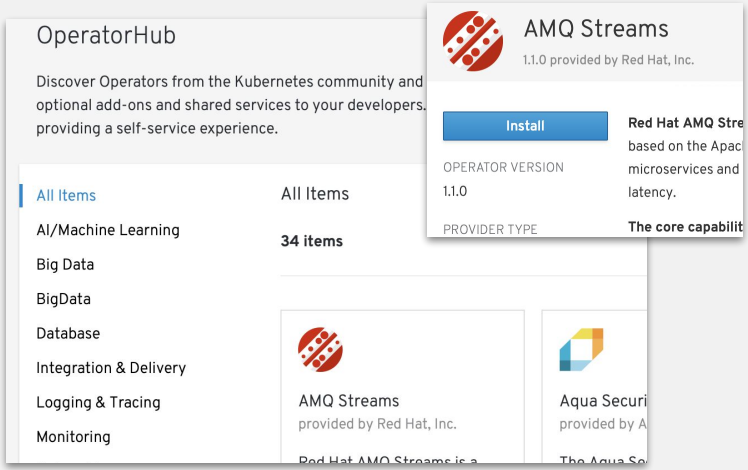
OPERATOR FRAMEWORK

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



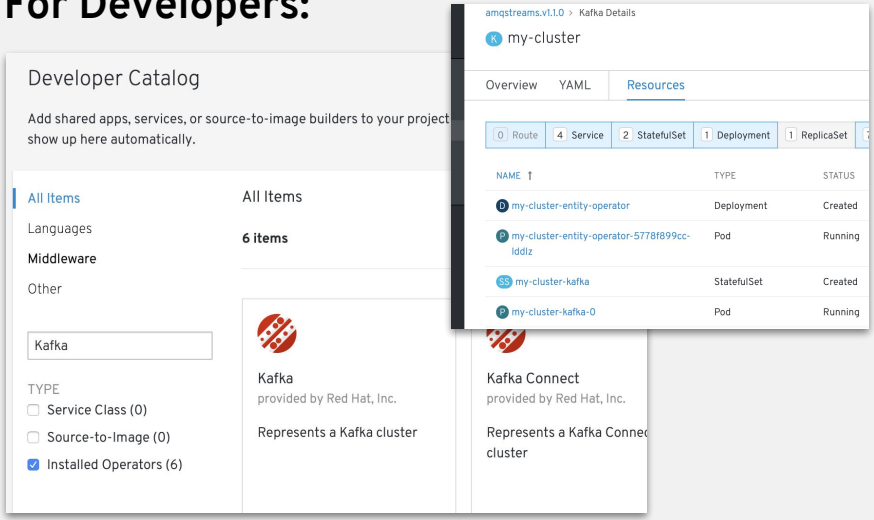
OPERATORHUB IN OPENSHIFT 4

For Cluster Admins:



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

For Developers:



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

CONTAINER TOOLS

OCI tooling to create, run, and manage, Linux Containers with a cluster-friendly life cycle

Light-weight runtime for the Kube CRI

- OCI compliant and docker compatible
- CLI via crictl
- Improved performance and scalability
- Continue to track the Kube CRI

Secure & flexible OCI container builds

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

docker-compatible CLI for containers

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

The intelligent OS for your next big thing.

Red Hat
Enterprise Linux 8

RED HAT ENTERPRISE LINUX 8

Modern foundation for the datacenter, powering current and next-gen workloads

Core Components Snapshot
4.18.x kernel
gcc 8.2, llvm 6.0
systemd 239
YUM 4 (DNF base)

Simplified repository layout
BaseOS: Foundational components
AppStream: Additional user space components

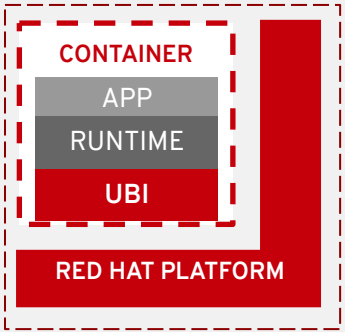
Content Flexibility via Application Stream
Perfectly embeds Software Collections & Extras content into RHEL

Enhanced security
System-wide crypto policies

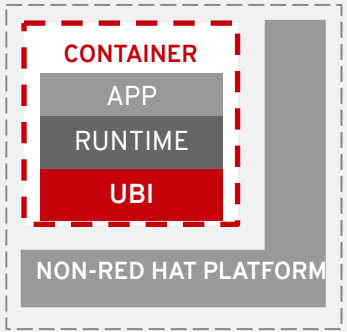
Available in OpenShift 4.1 for Worker Nodes

RED HAT UNIVERSAL BASE IMAGE (UBI)

The base image for all of your needs on: OpenShift, RHEL, or other platform of choice



Fully supported by Red Hat



Supported by end user

The Red Hat Universal Base Image is a freely useable and redistributable container image packed with all of the value of Red Hat Enterprise Linux

Development

- Minimal footprint
- Latest programming languages
- Makes ops happy

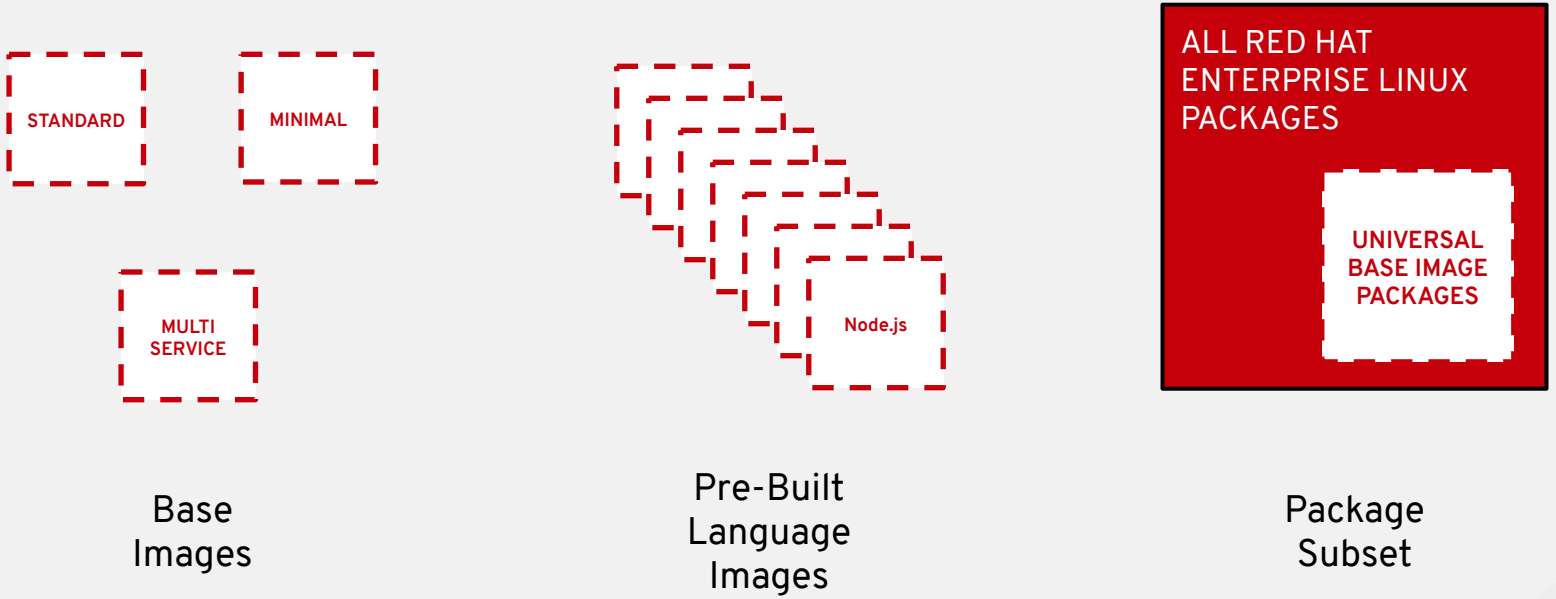
Production

- Performance
- Security
- Life cycle

Detailed Presentation

Red Hat Universal Base Image

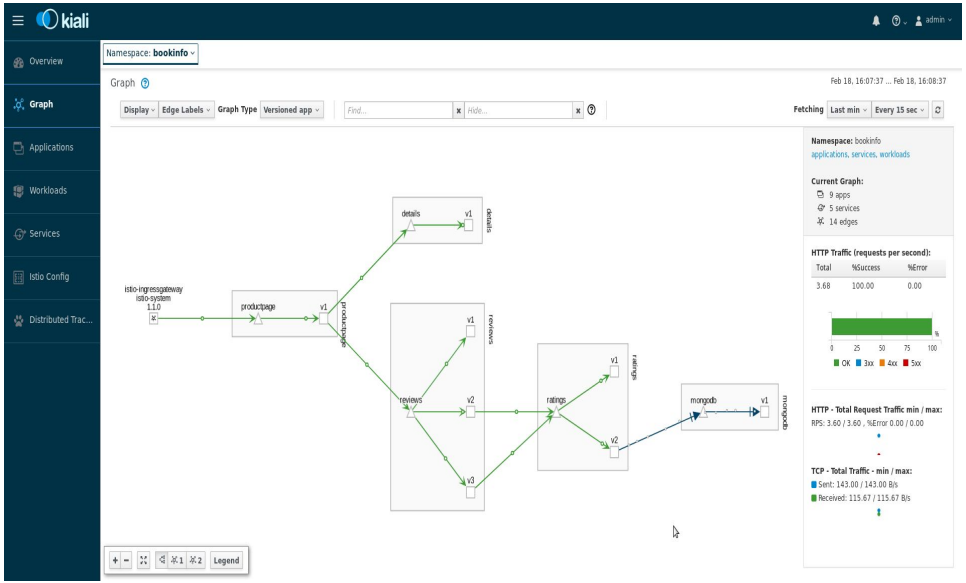
Enable an ecosystem of freely distributable operators for Kubernetes/OpenShift



Red Hat Service Mesh

Key Features

- A dedicated network for service to service communications
- Observability and distributed tracing
- Policy-driven security
- Routing rules & chaos engineering
- Powerful visualization & monitoring
- Will be available via OperatorHub

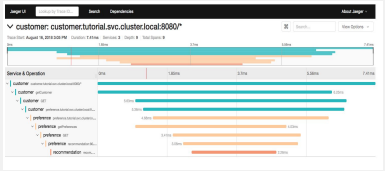


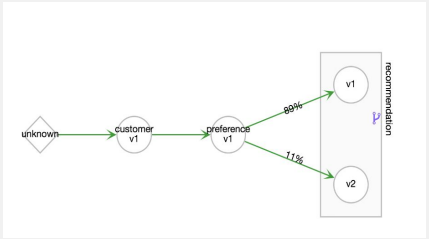
Product Manager: Brian 'redbeard' Harrington

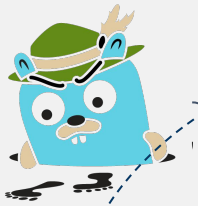
Generally Available in July

Red Hat

OPENSHIFT SERVICE MESH (OSM)







Jaeger

Secure

Istio

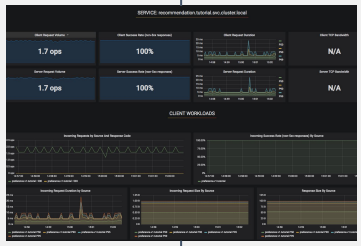
Observe

Connect

Control

Observe

Prometheus



Product Manager: Brian Harrington

redhat.

High performance. Delivered.

Container Security Reference Architecture

High performance. Delivered.

Security in OpenShift

AUTOMATED & INTEGRATED SECURITY

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

CONTENT: CONTAINER HEALTH INDEX

The following grades and icons are used with a brief explanation of how they are calculated.

Grade A: This image does not contain known unapplied errata that fix Critical or Important flaws.

Grade B: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 7 days and no missing Important flaw is older than 30 days.

Grade C: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 30 days and no missing Important flaw is older than 90 days.

Grade D: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 90 days and no missing Important flaw is older than 365 days.

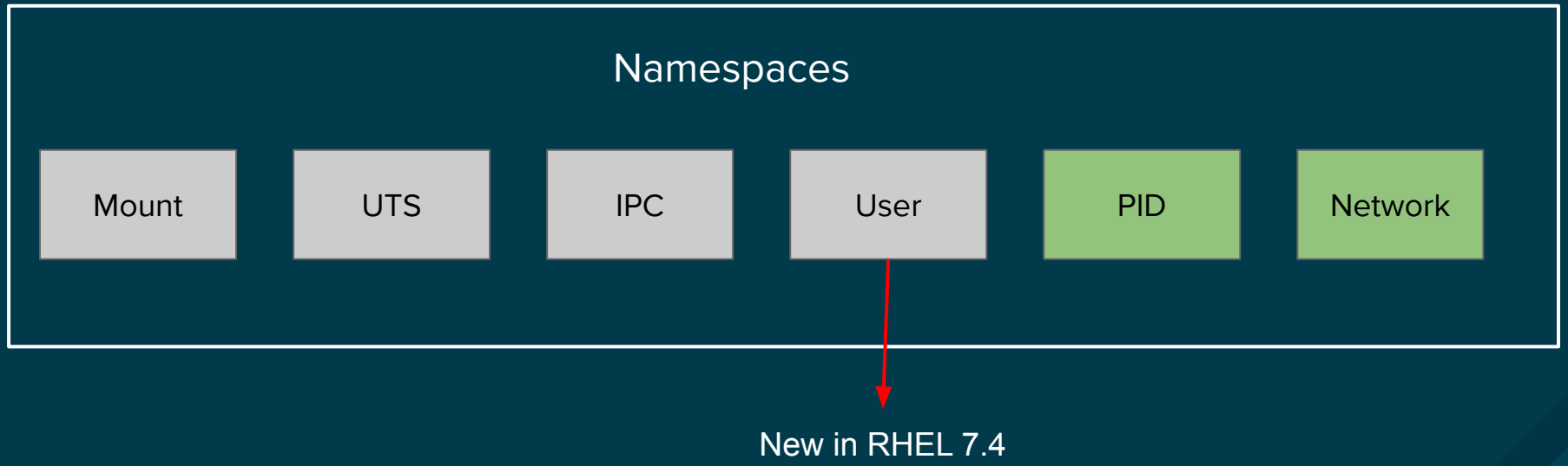
Grade E: This image may be missing Critical or Important security errata, but no missing Critical or Important flaw is older than 365 days.

Grade F: This image may be missing Critical or Important security errata, and they are older than 365 days. Or the container is out of its lifecycle.

Grade Unknown: This image cannot be scanned as it is missing metadata required to perform the Container Health Index calculation.

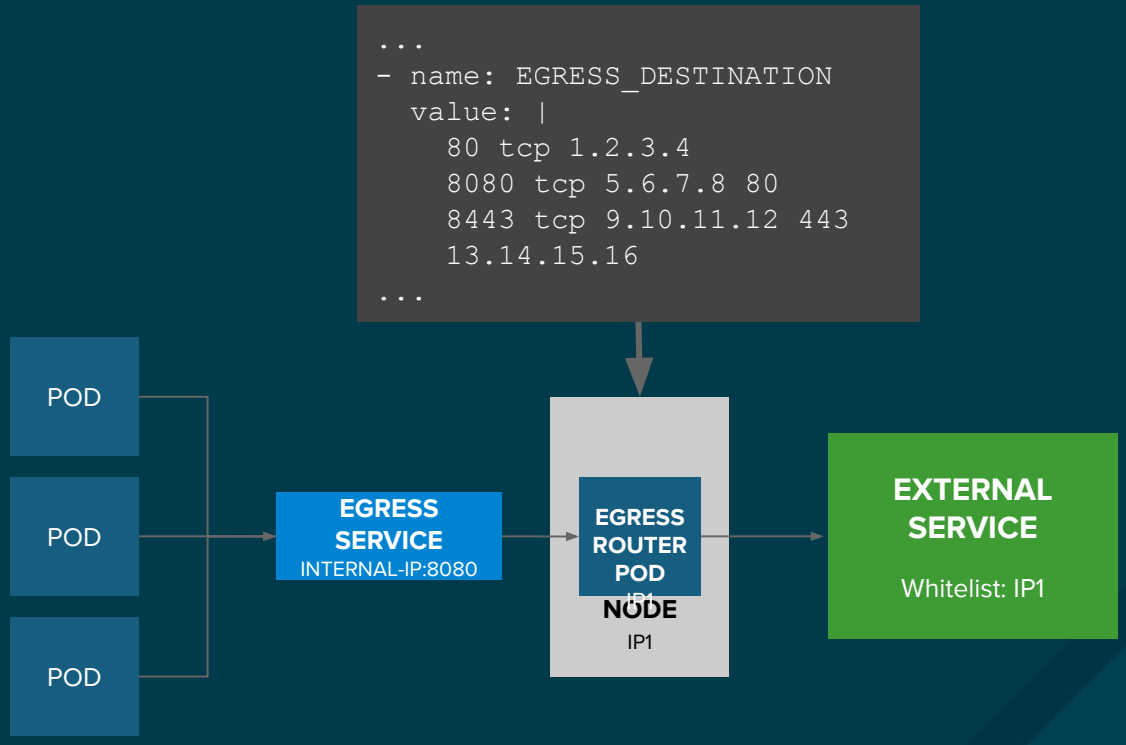
https://access.redhat.com/articles/2803031

NAMESPACES
Process Isolation



NETWORK DEFENSE: EGRESS ROUTER

The OpenShift egress router runs a service that redirects egress pod traffic to one or more specified remote servers, using a pre-defined source IP address that can be whitelisted on the remote server. The egress router can also be run as a proxy.



NETWORK POLICIES

Use of a NetworkPolicy allows for pod isolation.

The policy only has effect when the network plugin, like Project Calico, are capable of honoring them. If used with a plugin like flannel they will have no effect.

The use of matchLabels allows for more granular selection within the namespace which can be se- lected using a namespaceSelector. Using multiple labels can allow for complex application of rules.

https://kubernetes.io/docs/concepts/services-networking/network-policies/

```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:
    matchLabels:
      role: db
  policyTypes:
  - Ingress
  - Egress
  ingress:
  - from:
    - ipBlock:
        cidr: 172.17.0.0/16
        except:
        - 172.17.1.0/24
    - namespaceSelector:
        matchLabels:
          project: myproject
    - podSelector:
        matchLabels:
          role: frontend
    ports:
    - protocol: TCP
      port: 6379
  egress:
  - to:
    - ipBlock:
        cidr: 10.0.0.0/24
    ports:
    - protocol: TCP
      port: 5978
```


Aporeto

AquaSecurity

Avi Networks

big switch


Black Duck


Cisco Contiv

Contrail

dynatrace

f5

JFrog, Inc.

HashiCorp

NeuVector


NGINX

nuagenetworks

Portworx

Signal Sciences


Sonatype


Sysdig

Thales e-Security

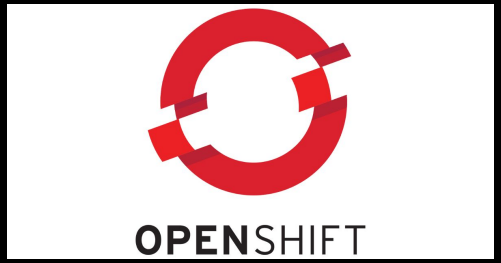

Tigera

Treasure Data


Tremolo

OPENSHIFT PRIMED PARTNERS

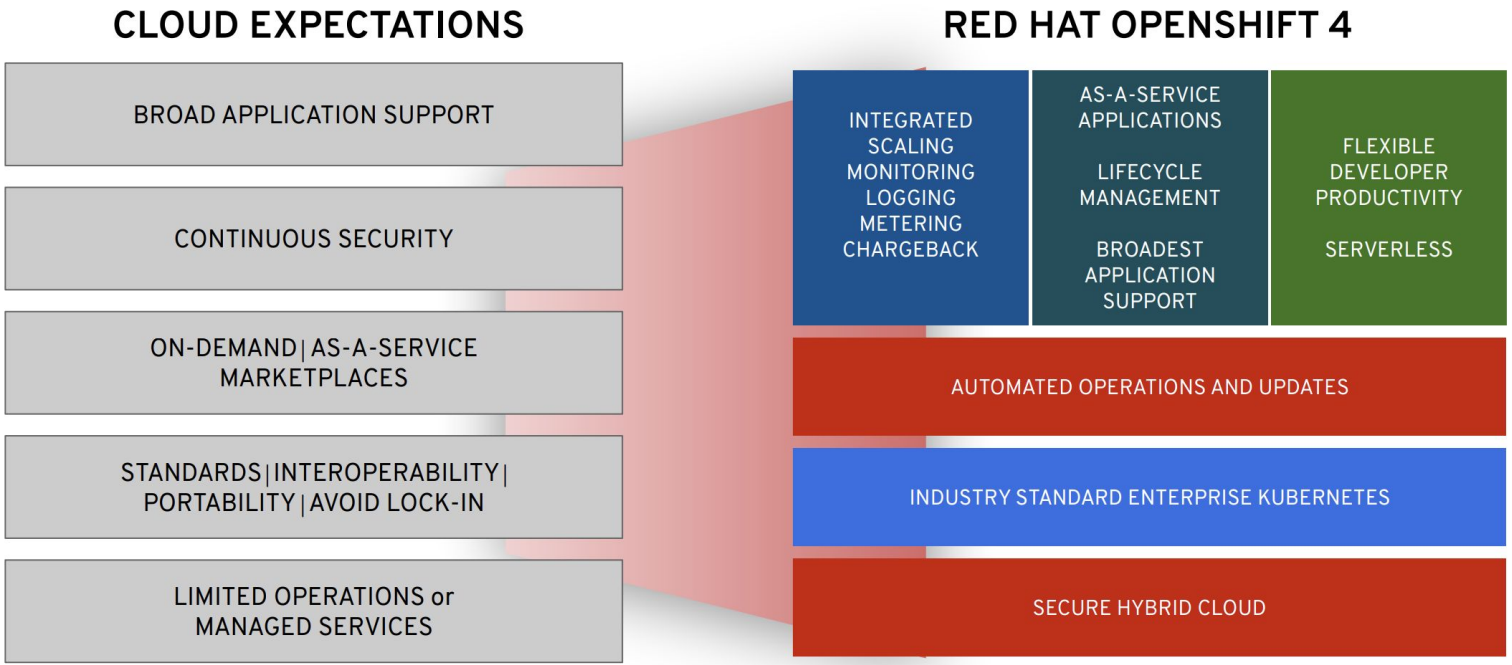
OpenShift 4 - The Automated Platform



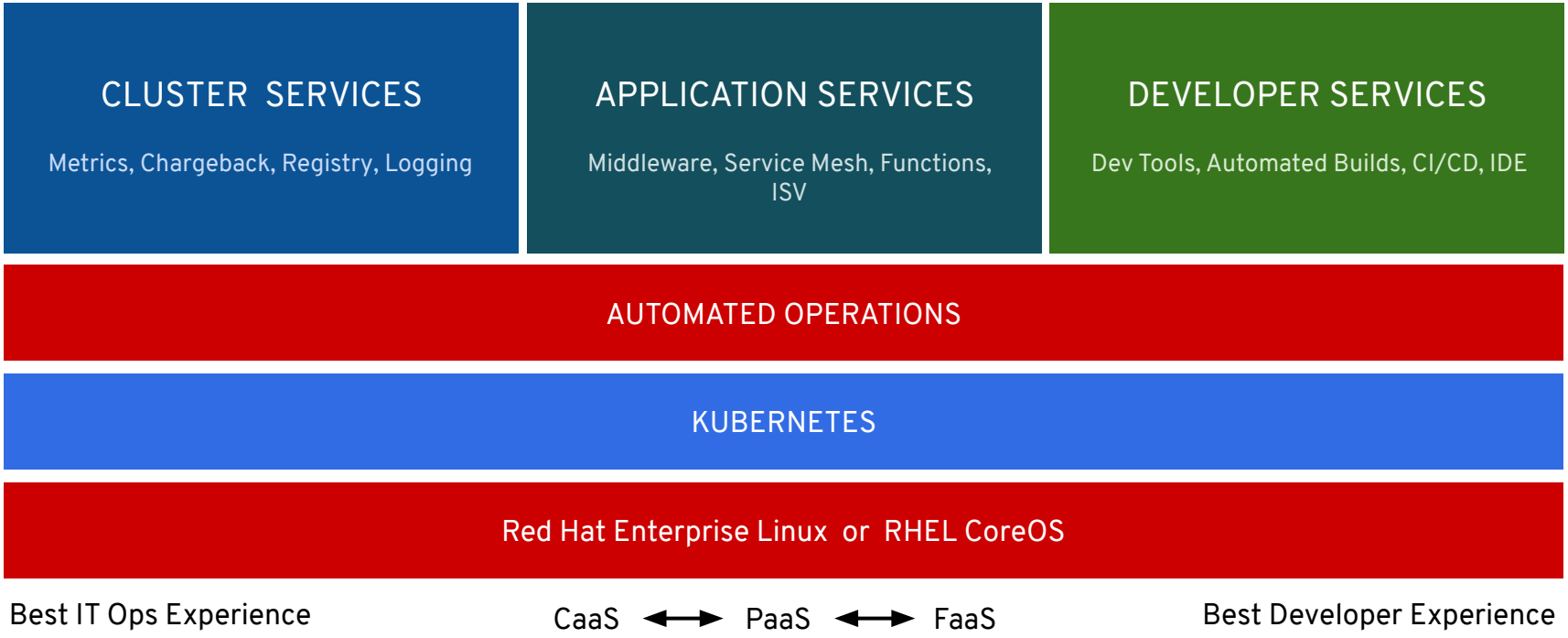
cri-o

Moving into the 3rd Era of Kubernetes

Bringing Learnings from the Public Cloud to the Hybrid Cloud

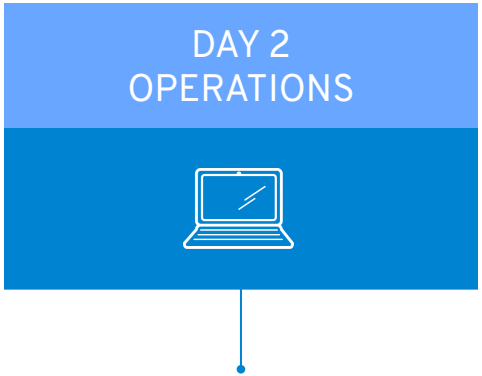


OpenShift 4 Platform



Red Hat

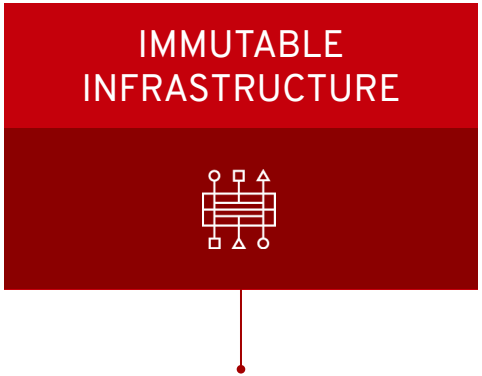
OpenShift 4.1 Workstreams Lifecycle



AWS Installer + bootstrapping

Autoscale out of the box

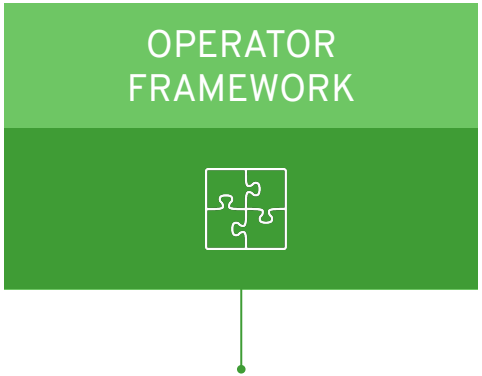
MachineSet node pools



Red Hat Enterprise Linux CoreOS

Discourage SSH/node mutation

Ignition for Machine config



SDK & testing tools

OperatorHub for discovery

OLM delivers upper stack services

Installation Experiences

OPENSHIFT CONTAINER PLATFORM

Full Stack Automated

Simplified opinionated "Best Practices" for cluster provisioning

Fully automated installation and updates including host container OS.

Pre-existing Infrastructure

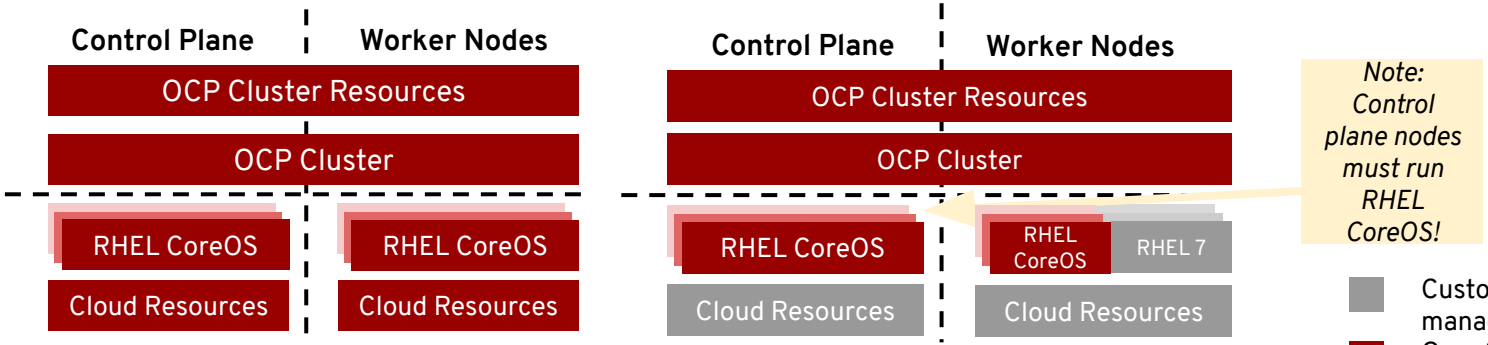
Customer managed resources & infrastructure provisioning

Plug into existing DNS and security boundaries

HOSTED OPENSHIFT

Azure Red Hat OpenShift
Deploy directly from the Azure console.

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



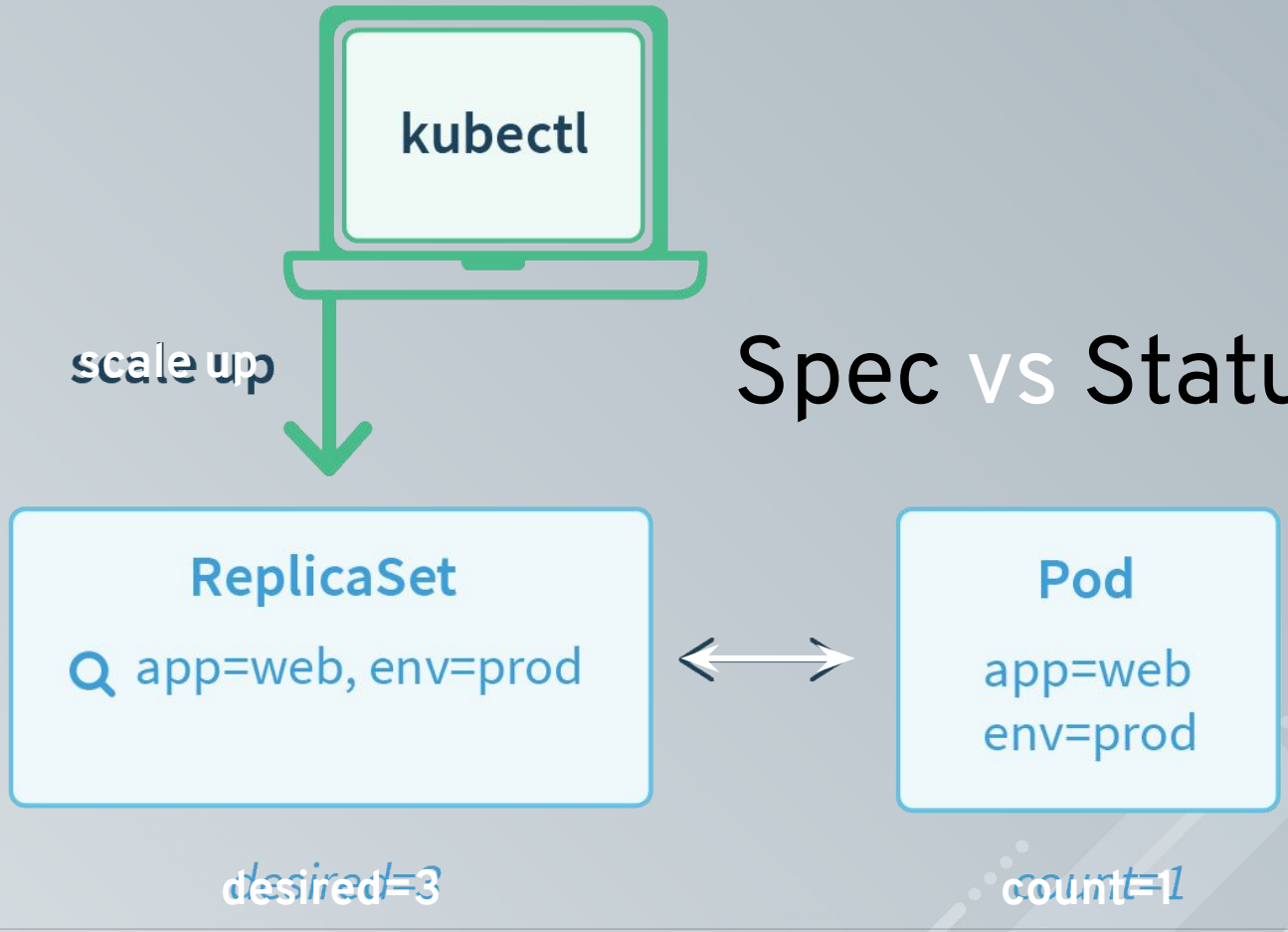
Red Hat

DEMO

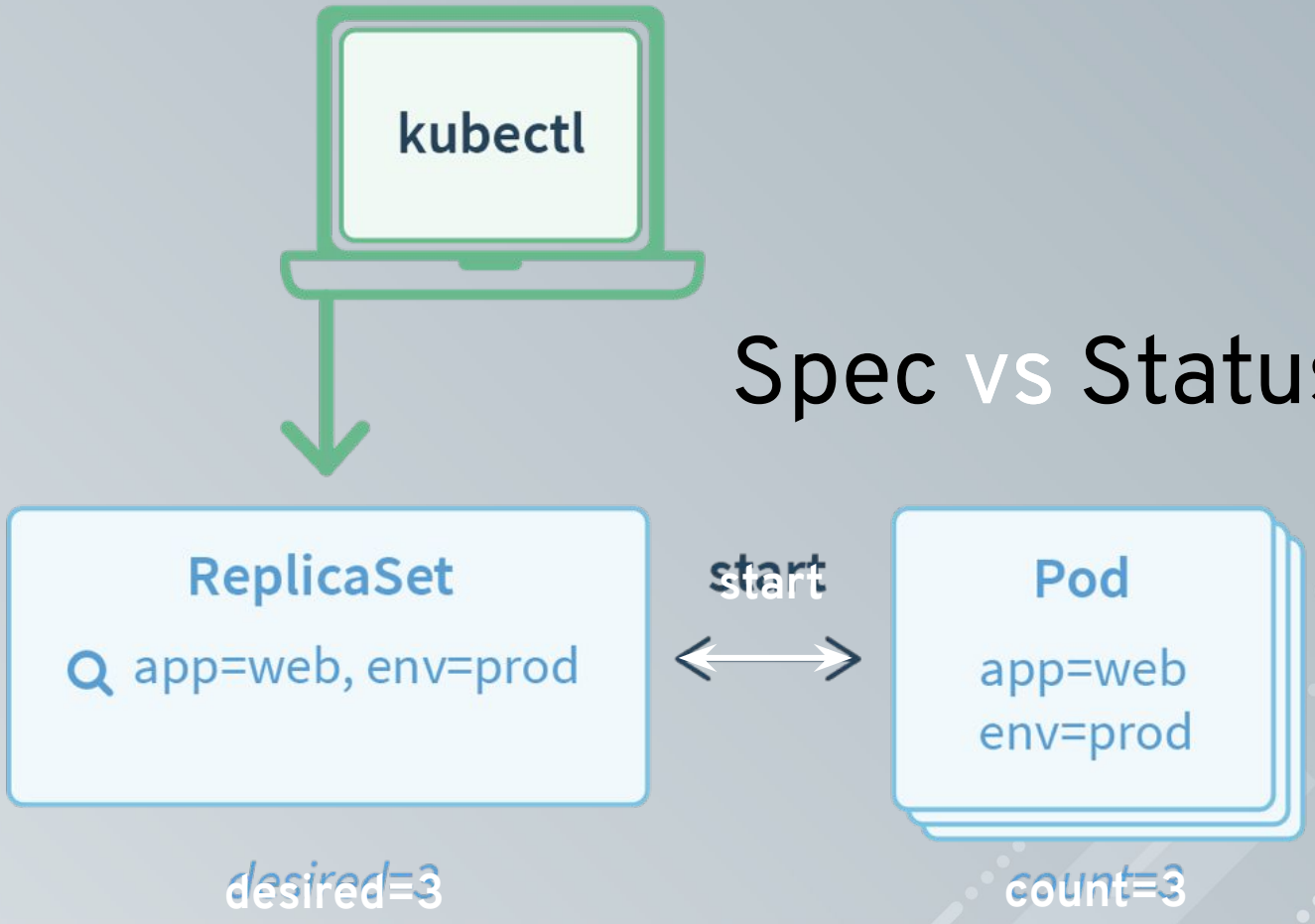
Operators

In Kubernetes
Scaling stateless apps: **easy**

```
$ kubectl scale deploy/staticweb --replicas=3
```


kubectl
scale up
Spec vs Status
ReplicaSet
app=web, env=prod
Pod
app=web
env=prod
desired=3
count=1

Spec vs Status



What about apps that **store data**?

In Kubernetes
Creating a database is **easy**

```
$ kubectl run db --image=quay.io/my/db
```

Running a database **over time** is harder

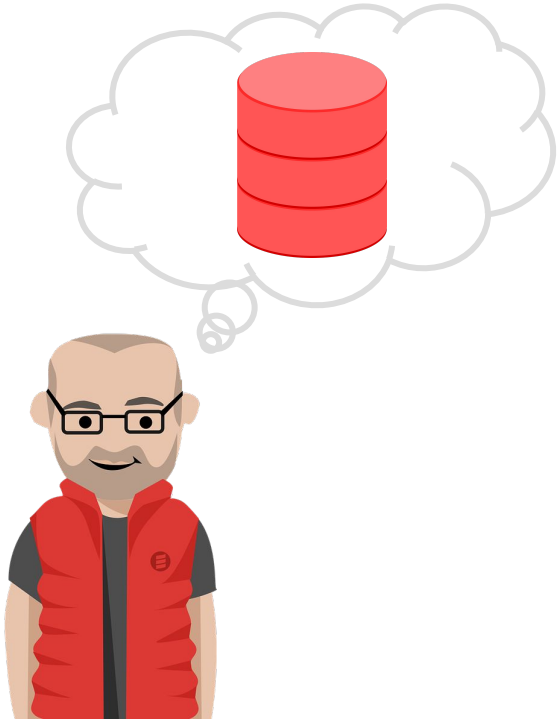
- Resize
- Reconfigure
- Backups
- Healing
- Patching
- Upgrades

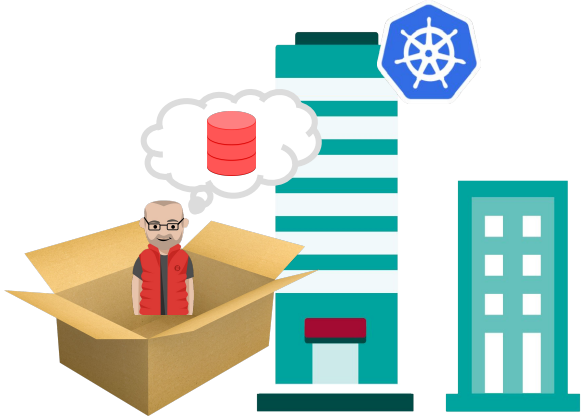
1. Every application on any platform must be **installed**, **configured**, **managed**, and **upgraded** over time

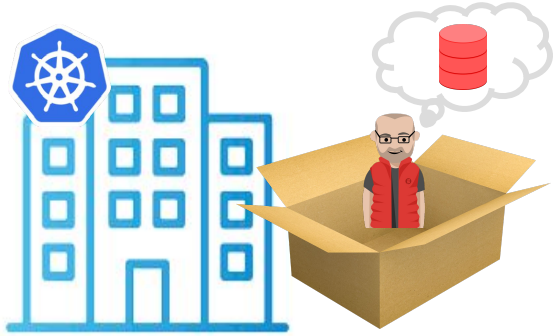
2. Patching is critical to Security


Anything not automated is slowing you down

If only Kubernetes knew...





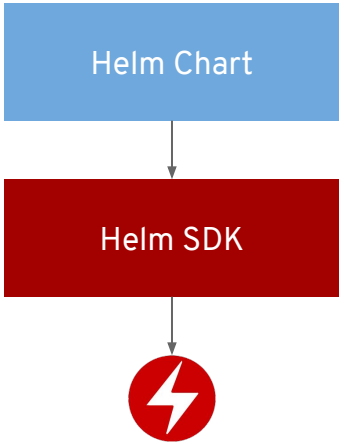


Operators are **automated software managers** that deal with installation and lifecycle of Kubernetes applications

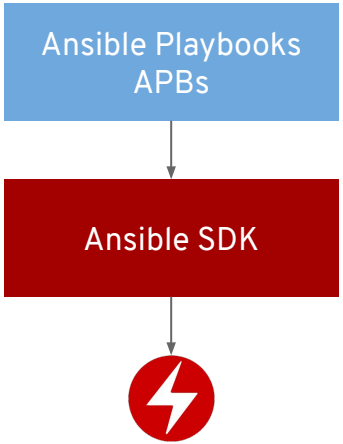
DEMO

OPERATOR SDK

Build Operators for your apps

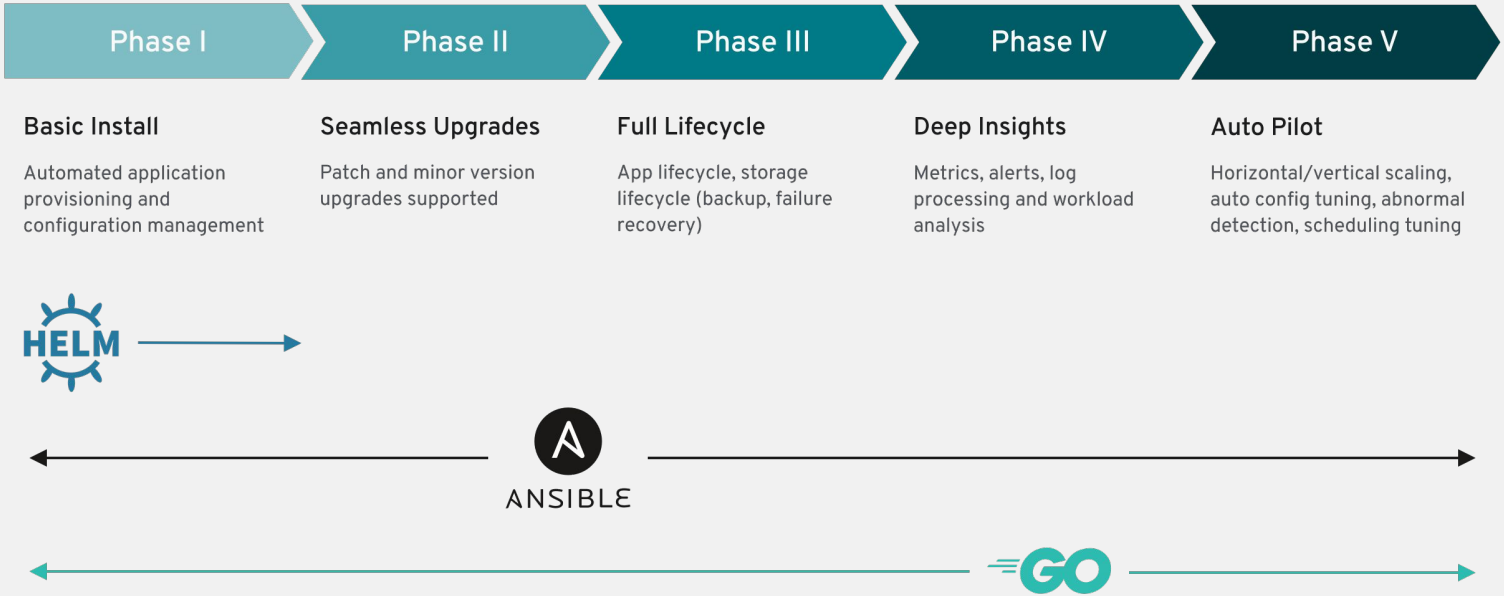


Build operators from Helm chart, without any coding



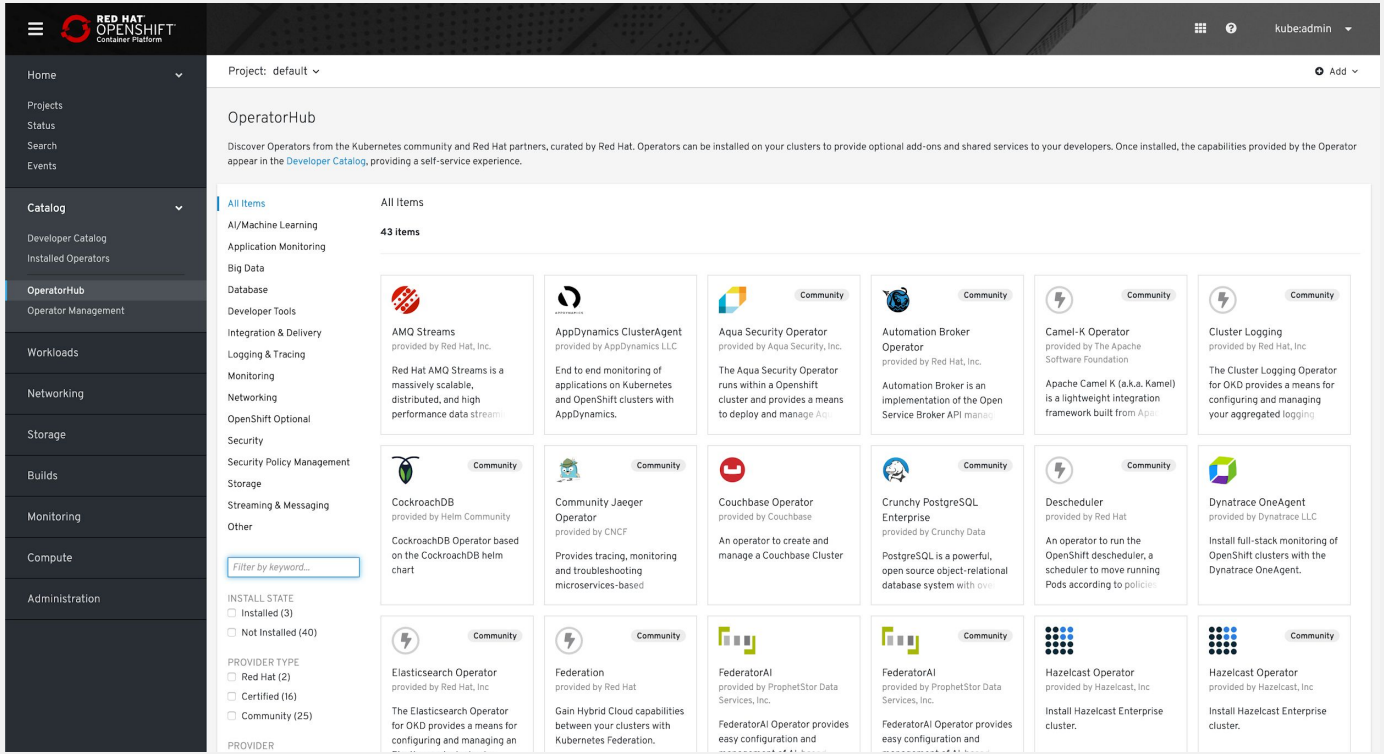
Build operators from Ansible playbooks and APBs

Build advanced operators for full lifecycle management


Phase I
Phase II
Phase III
Phase IV
Phase V
Basic Install
Automated application provisioning and configuration management
Seamless Upgrades
Patch and minor version upgrades supported
Full Lifecycle
App lifecycle, storage lifecycle (backup, failure recovery)
Deep Insights
Metrics, alerts, log processing and workload analysis
Auto Pilot
Horizontal/vertical scaling, auto config tuning, abnormal detection, scheduling tuning
HELM
ANSIBLE
GO

Operators for Developers

Ready-to-use Dev Tooling and Backend Operator from OperatorHub



PIPELINES IN OPENSHIFT 4

Cloud-native CI/CD for OpenShift

Support for existing investments in Jenkins

WHAT IS CLOUD-NATIVE CI/CD?

CONTAINERS

Built for containers and runs on Kubernetes

SERVERLESS

No CI/CD server to manage and maintain

DEVOPS

Microservices and distributed teams

Based on Tekton pipelines - set of shared, open source components for building Kubernetes-style CI/CD systems

Governed by the Continuous Delivery Foundation

Contributions from Google, Red Hat, Cloudbees, Pivotal, IBM and more

OpenShift Serverless + Azure Functions

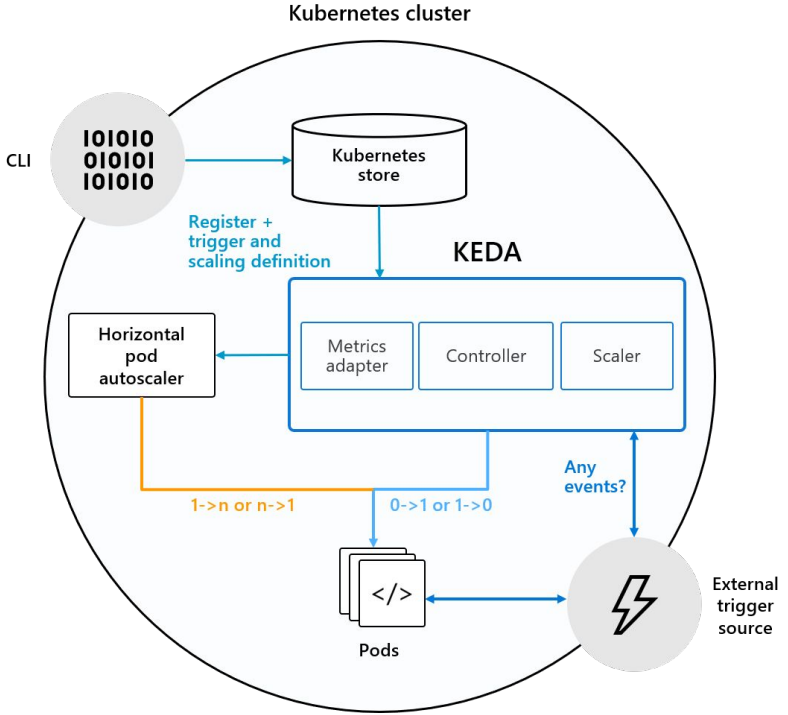
KEDA allows for fine grained autoscaling (including to/from zero) for event driven Kubernetes workloads. KEDA serves as a Kubernetes Metrics Server and allows users to define autoscaling rules using a dedicated Kubernetes custom resource definition.

Key Features

- Enable FaaS in OpenShift
- Polling based auto-scaling for Azure Queues, Kafka...
- Reuse Knative event sources, HTTP auto-scaling
- On premise or Any cloud.

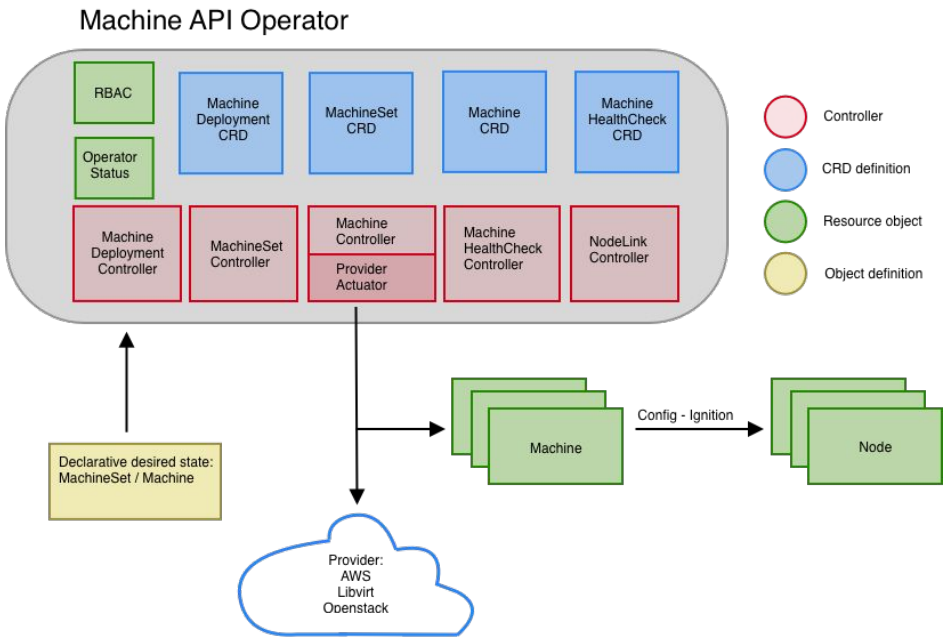
Learn more

https://github.com/kedacore/keda



Cloud API

- Provide a single view and control across multiple cluster types
- *Machine API:*
  - Set up definitions via CRDs
  - Machine: a node
  - MachineSet: think ReplicaSet
  - Actuators roll definitions across clusters
  - Nodes are drained before deletion
- *Cluster Autoscaler:* provide/remove additional nodes on demand
- AWS (4.1), Azure/GCP (target 4.2), VMWare (Future)



DEMO

2019 Roadmap

Q2 CY2019
OpenShift 4.1

DEV
- OpenShift Serverless (Knative) - DP
- OpenShift Pipelines (Tekton) Dev Preview
- CodeReady Workspaces
- CodeReady Containers Alpha
- Developer CLI (odo) Beta

APP
- OperatorHub
- Operator Lifecycle Manager
- Service Mesh (~2 month after)

PLATFORM
- Kubernetes 1.13 with CRI-O runtime
- RHEL CoreOS, RHEL7
- Automated Installer for AWS
- Pre-existing Infra Installer for Bare Metal, VMware, AWS
- Automated, one-click updates
- Multus (Kubernetes multi-network)
- Quay v3

HOSTED
- cloud.redhat.com - Multi-Cluster Mgmt
- OCP Cluster Subscription Management
- Azure Red Hat OpenShift
- OpenShift Dedicated consumption pricing

Q3 CY2019
OpenShift 4.2

DEV
- Developer Console GA
- OpenShift Serverless (Knative) - TP
- OpenShift Pipelines (Tekton) Tech Preview
- CodeReady Containers GA
- Developer CLI (odo) GA

APP
- GPU metering
- OperatorHub Enhancements
- Operator Deployment Field Forms
- Application Binding with Operators
- Application Migration Console

PLATFORM
- Kubernetes 1.14 w/ CRI-O runtime
- Disconnected Install and Update
- Automated Installer for Azure, OSP, GCP
- OVN Tech Preview
- FIPS
- Federation Workload API
- Automated App cert rotation
- OpenShift Container Storage 4.2

HOSTED
- cloud.redhat.com - Multi-Cluster Deployment
- Proactive Support Operator

Q4 CY19/Q1 CY20
OpenShift 4.3

DEV
- OpenShift Serverless (Knative) - GA
- OpenShift Pipelines (Tekton) GA

APP
- Metering for Services
- Windows Containers

PLATFORM
- Kubernetes 1.15 w/ CRI-O runtime
- Automated Installer for IBM Cloud, Alibaba, RHV, Bare Metal Hardware Appliance
- Pre-existing Infra Installer for Azure, OSP, GCP
- OVN GA w/ Windows Networking Integration

HOSTED
- cloud.redhat.com - Subscription Mgmt Consumption Improvements

QUARKUS

Supersonic. Subatomic. Java.

A stack to write Java apps

Cloud Native,

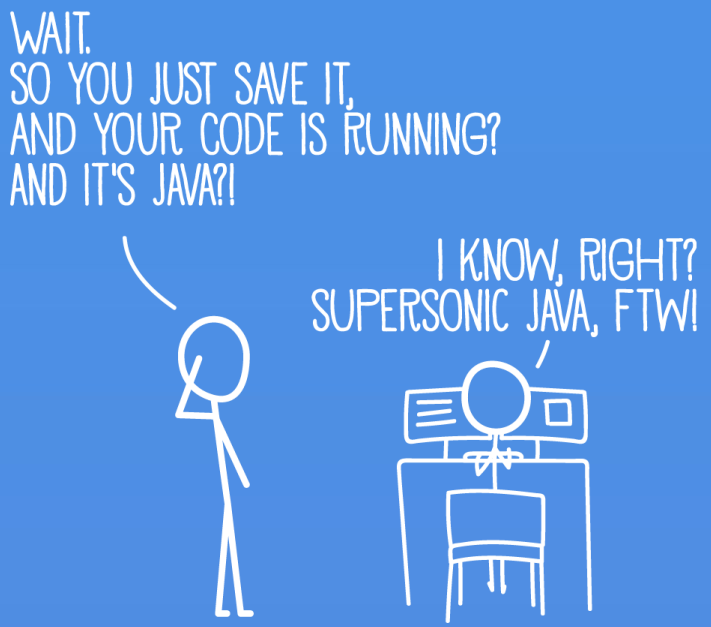
Microservices,

Serverless

Developer Joy

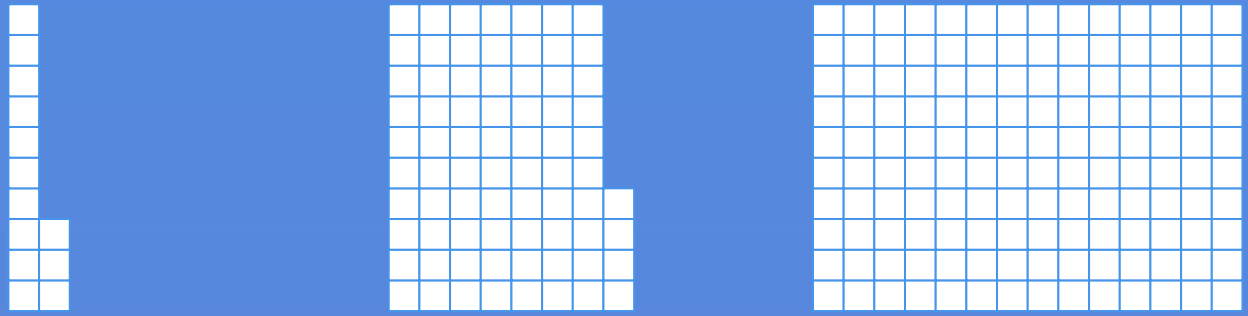
A cohesive platform for optimized developer joy:

- Based on standards, but not limited
- Unified configuration
- Zero config, live reload in the blink of an eye
- Streamlined code for the 80% common usages, flexible for the 20%
- No hassle native executable generation



Supersonic Subatomic Java

REST

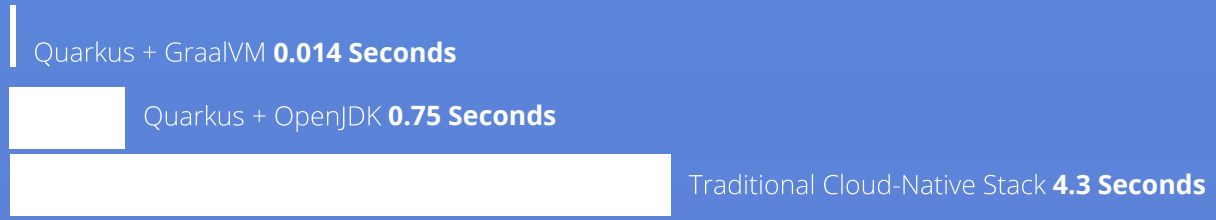


Quarkus + GraalVM
13 MB

Quarkus + OpenJDK
74 MB

Traditional Cloud-Native Stack
74 MB

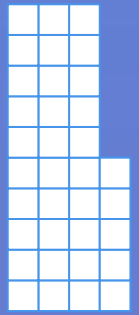
Memory (RSS) in Megabytes



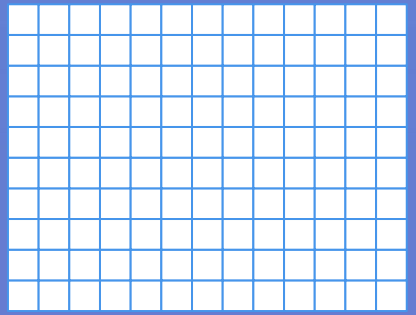
Boot + First Response Time (in seconds)

Supersonic Subatomic Java

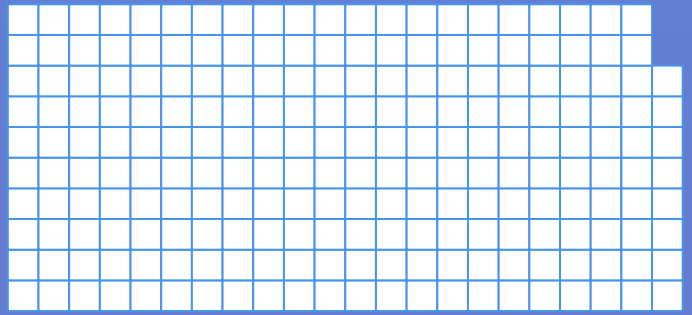
REST + CRUD



Quarkus + GraalVM
35 MB

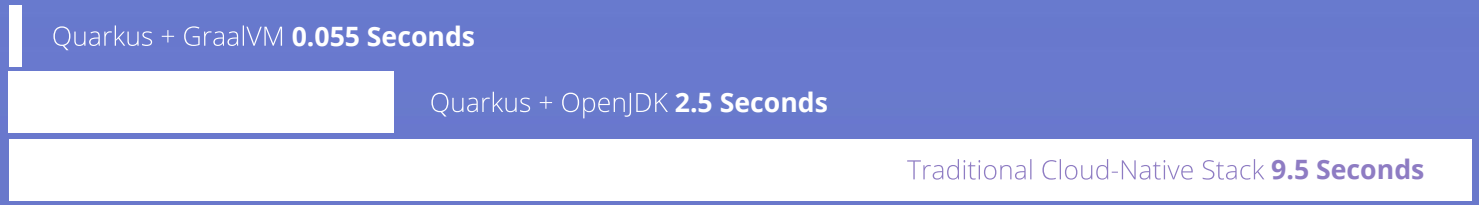


Quarkus + OpenJDK
130 MB



Traditional Cloud-Native Stack
218 MB

Memory (RSS) in Megabytes



Boot + First Response Time (in seconds)

Frameworks & Standards

Eclipse Vert.x

Hibernate

RESTEasy

Apache Camel

Eclipse MicroProfile

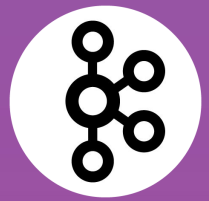
Netty

Kubernetes

OpenShift

Jaeger

Prometheus



Apache Kafka

Infinispan