

OpenShift, Containers & Kubernetes, A New Era Begins...

August 2019

Nick Barcet
Senior Director Technology,
OCTO/CPBU, Red Hat

Andrea Cucurull
CoSP Industry Technical
Specialist, Intel

Address Key Challenges to Transformation

Challenges addressed

Automation

Standard Interfaces

Resource Management

Data Plane Acceleration

Platform Security

Containers

Address Key Challenges to Transformation

Challenges addressed

Deliver

Automation

Standard Interfaces

Resource Management

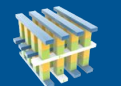
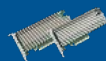
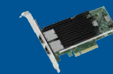
Data Plane Acceleration

Platform Security

Containers

Platform TECHNOLOGIES

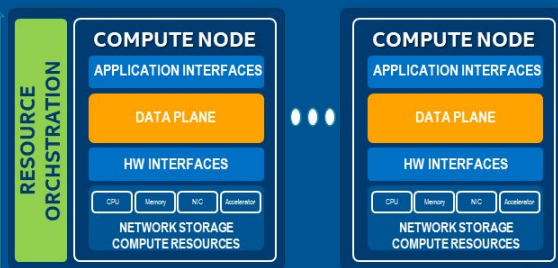
Open-Source Software
Exposing Intel Technology Value



Intel® Ethernet
Controller

Intel® QuickAssist
Technology

intel® OPTANE DC
PERSISTENT MEMORY



Address Key Challenges to Transformation

Challenges addressed

Automation

Standard Interfaces

Resource Management

Data Plane Acceleration

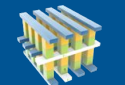
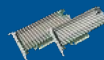
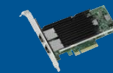
Platform Security

Containers

Deliver

Platform TECHNOLOGIES

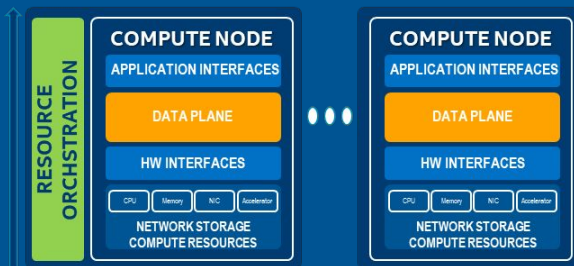
Open-Source Software
Exposing Intel Technology Value



Intel® Ethernet
Controller

Intel® QuickAssist
Technology

intel OPTANE DC
PERSISTENT MEMORY



ACCELERATE

OPEN SOURCE



Enablement TOOLS

<https://networkbuilders.intel.com/>

EXPERIENCE KITS

intel select
solution



Address Key Challenges in Containers

Challenges addressed

ENABLING TECH.

ECOSYSTEM ADOPTION

Kubernetes Networking



Data Plane Acceleration



Resource Management
Enhanced Platform Awareness
(EPA)



Telemetry



MULTUS



USERSPACE CNI



DPDK



SR-IOV



DPDK



BOND-CN



Node Feature Discovery
(Intel® AVX; SR-IOV; etc)



CPU Manager for
Kubernetes (CMK)



Native Huge page
support for Kubernetes



Device Plugin
(SR-IOV, Intel® QAT, GPU)



Topology Manager
(NUMA)



collectd



OPEN SOURCE



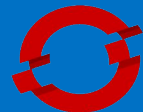
kubernetes



CNI



GitHub



RED HAT®
OPENSIFT
Container Platform

<https://networkbuilders.intel.com/network-technologies/container-experience-kits>

Address Key Challenges in Containers

Challenges addressed

Multiple network interfaces for VNFs	
High performance Data Plane (E-W)	
High performance Data Plane (N-S)	
Fail-over and high availability of networking	
Ability to request/allocate platform capabilities	
CPU Core-Pinning and isolation for K8s pods	
Dynamic Huge Page allocation	
Discovery, Advertise, schedule and manage devices with K8s	
Guarantee NUMA node resource alignment	
Platform telemetry information	

ENABLING TECH.

	
	 
	 
	 
	Node Feature Discovery (Intel® AVX; SR-IOV; etc)
	CPU Manager for Kubernetes (CMK)
	Native Huge page support for Kubernetes
	Device Plugin (SR-IOV, Intel® QAT, GPU)
	Topology Manager (NUMA)
	

ECOSYSTEM ADOPTION

Open Source: CNI plug-in – V3.1 Mar '19
Open Source: Userspace CNI – V1.1 Aug'18
Open Source: SR-IOV CNI plugin v1.0.0 6th Dec '18, Next release planned: v3.0 Mar'19
Open Source: CNI plug-in – v1.0 Dec '17
Open Source: v0.3.0 Sep'18. Upstream K8s: Host target K8s SIG Mar '19
Open Source: CMK v1.3 Sept'18 Upstream K8s: Phase 1 - v1.8 Sep '17
Upstream K8s: Beta - v1.10 Dec '17
Open Source: SR-IOV v2.0.0 4th Dec '18, QAT v1.0 v1.0 Aug'18, FPGA & GPU May '18
Upstream K8s: Planned k8s v1.15 Jun'19
Upstream collectd: v5.7.2 Jun '17, v5.8.0 Nov. '17

CONTAINER CHALLENGES

Container Security

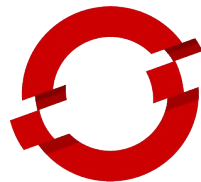
Image scanning, patching and compliance.

Day 2 Management

Install, upgrade and maintenance.
Integrate existing enterprise technology.

Application Delivery

Monitoring, metering and management.
Integrate existing developer tools.



RED HAT®
OPENS SHIFT®

CONFIDENTIAL Designator

Trusted enterprise Kubernetes

Continuous security, world-class support and services, and deep expertise to confidently run any application.

A cloud-like experience, everywhere

Full-stack automated operations on a consistent foundation across on-premises or hybrid cloud infrastructure.

Empowering developers to innovate

Get applications to production sooner with a wide range of technologies and streamlined workflows.



Trusted enterprise Kubernetes

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

A cloud-like experience, everywhere

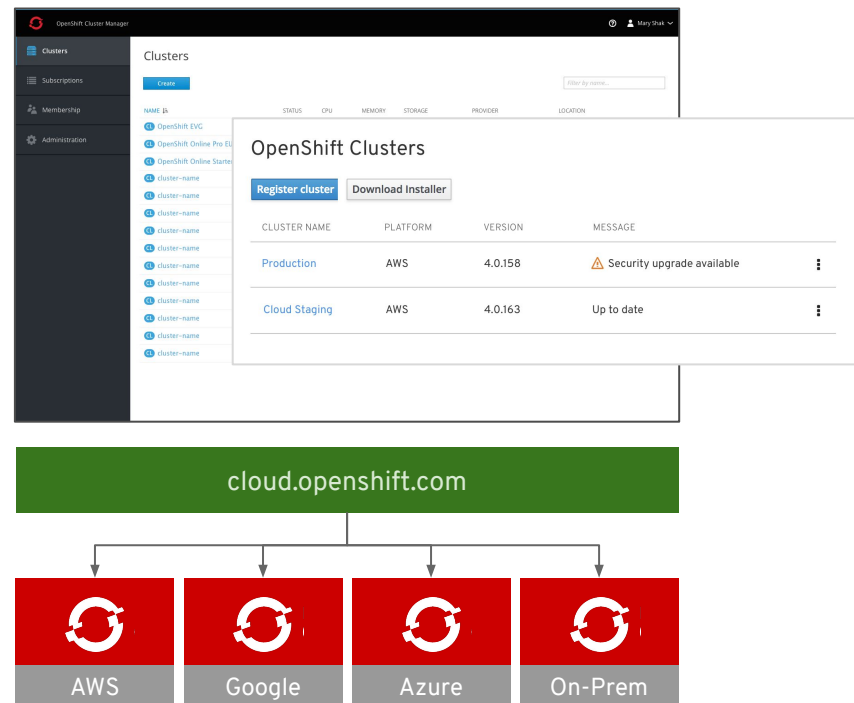
- Hybrid, Multi-Cluster Management
- Operator Framework
- Operator Hub & Certified ISVs

Empowering developers to innovate

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

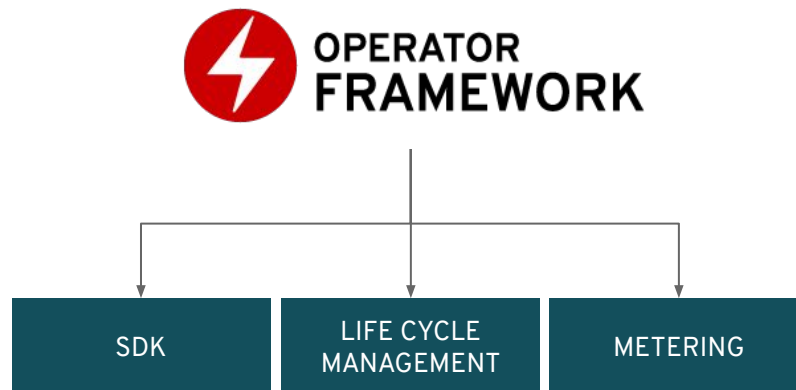
UNIFIED HYBRID CLOUD

- Cloud-based 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



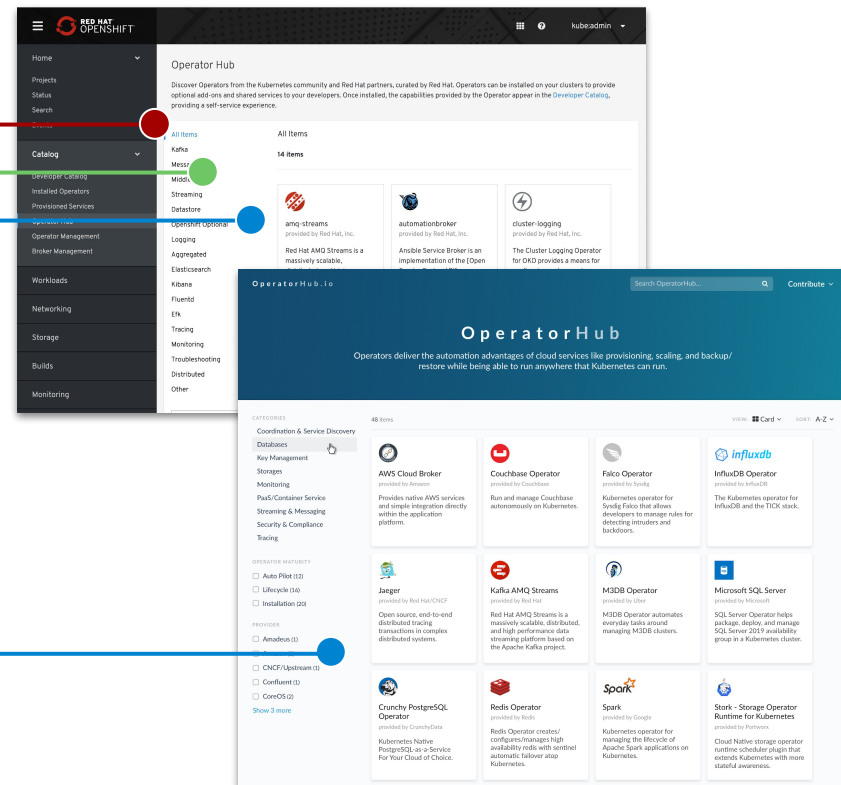
OPERATOR HUB

CONFIDENTIAL Designer

- Launched with AWS, Microsoft, and Google
- Discover and install optional components and apps
- Upstream & downstream content
- ISV partners will support their own Operators

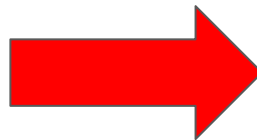
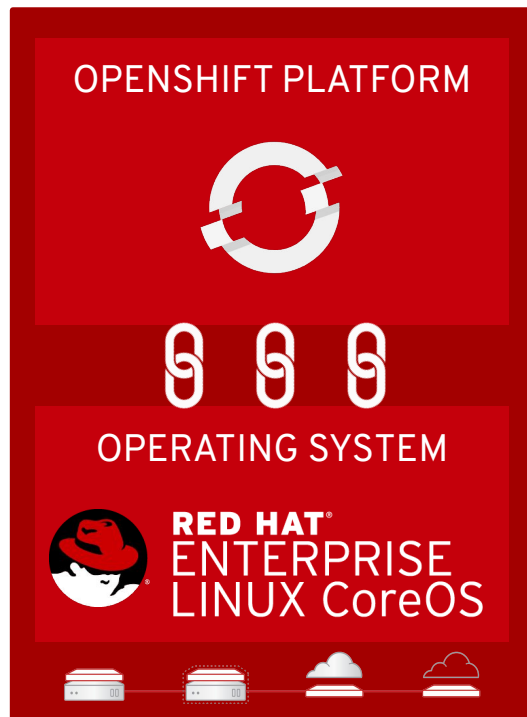
TYPES OF OPERATORS

Red Hat products
ISV partners
Community

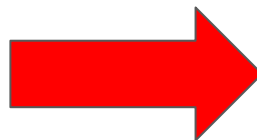


OpenShift 4 for NFV - Investment Priorities

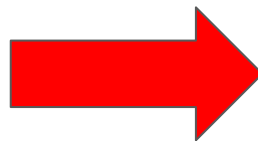
CONFIDENTIAL Designator



CNF
Operator



Day 2 Mgmt
Multi Cluster Mgmt



Platform NFV
Enhancements
(SR-IOV, Multus, ...)

CNF certification on OpenShift

Activities in progress*

- Testing and developing OpenShift with multiple partners (Samsung, Huawei, Affirmed, Altiostar)
- Fall - First demo with partners
- November 2019 Kubecon NA - Launch OpenShift as Telco initiative

* Plans have yet to be fully committed, could be changed at any time

CNF certification on OpenShift

Activities in progress*

- Testing and developing OpenShift with multiple partners (Samsung, Huawei, Affirmed, Altiostar)
- Fall - First demo with partners
- November 2019 Kubecon NA - Launch OpenShift as Telco initiative

* Plans have yet to be fully committed, could be changed at any time

PROJECT FOUNDATION

A vision for the longer term

KEY MARKET TRENDS



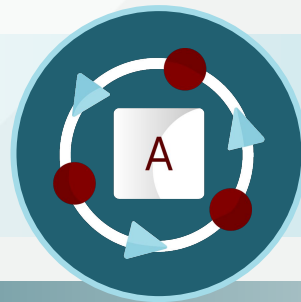
GENERALIST IT STAFF

Infrastructure admins,
general operator



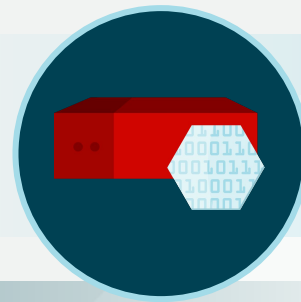
CLOUD NATIVE IS THE NEW NORMAL

Driven by the rise of Kubernetes
for container orchestration



WORKLOAD OPTIMIZATION

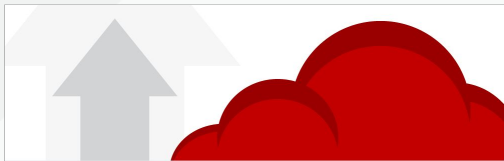
On-prem capabilities for low
latency, data intensive
workloads



HYPERCONVERGENCE

Simplicity and consolidation of
infrastructure

CUSTOMER CHALLENGES



—
Enjoy simplicity of
public cloud in an
on-prem environment



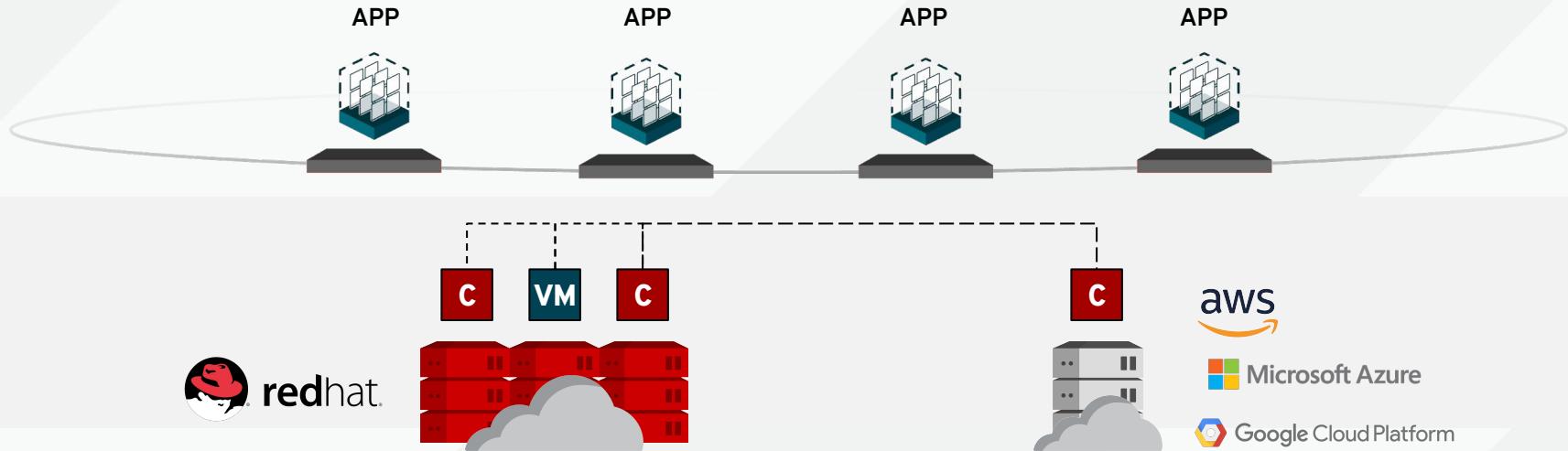
—
Create a consistent
experience across
public and on-prem



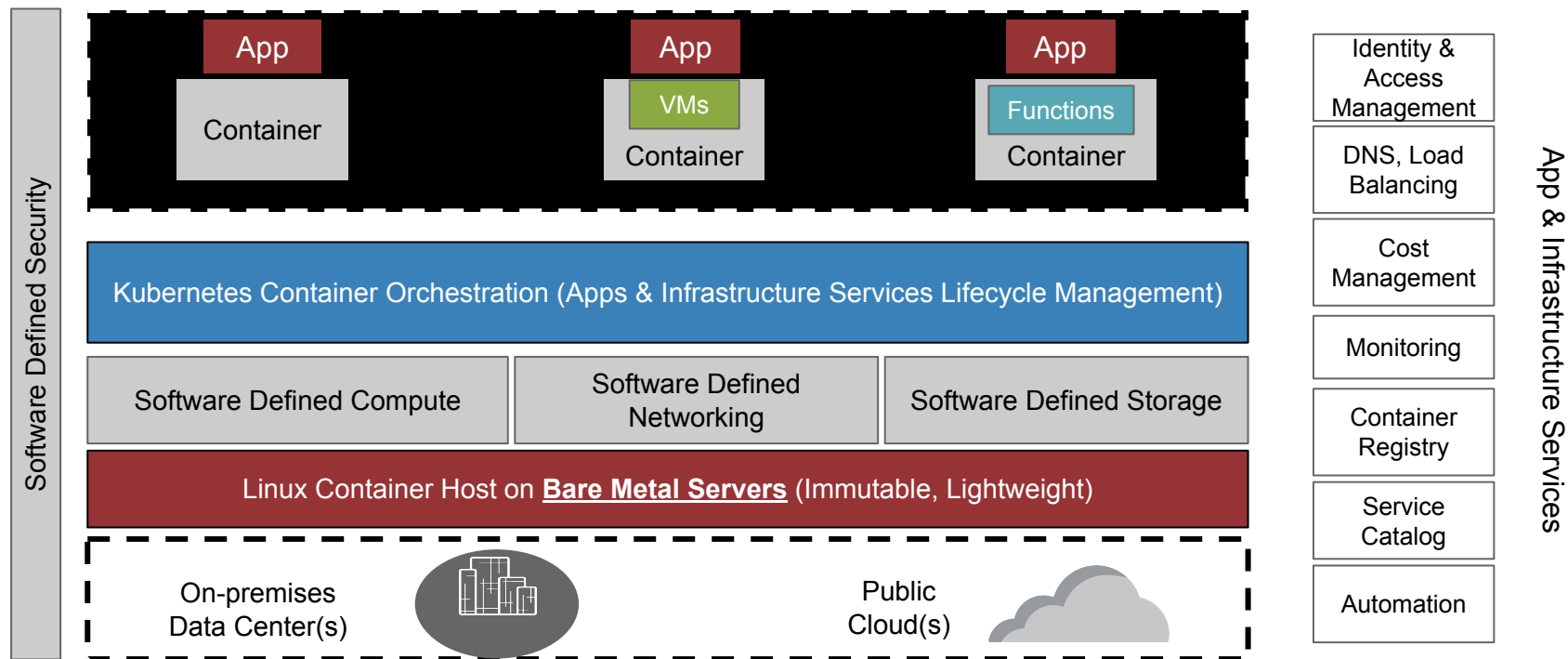
—
Plan for growth in
container adoption
while still running VMs

KUBERNETES NATIVE INFRASTRUCTURE

Unified foundation, hybrid interoperability



KUBERNETES NATIVE INFRASTRUCTURE CONCEPTUAL ARCHITECTURE VISION



WHAT IS CONTAINER-NATIVE VIRTUALIZATION?



Add virtual machines to your OpenShift projects as easily as application containers.
Easily leverage existing VM-based services from your new workloads!

CONTAINER-NATIVE VIRTUALIZATION

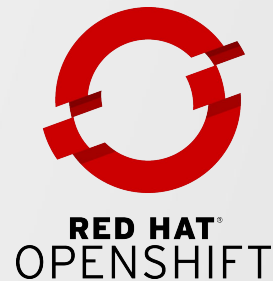
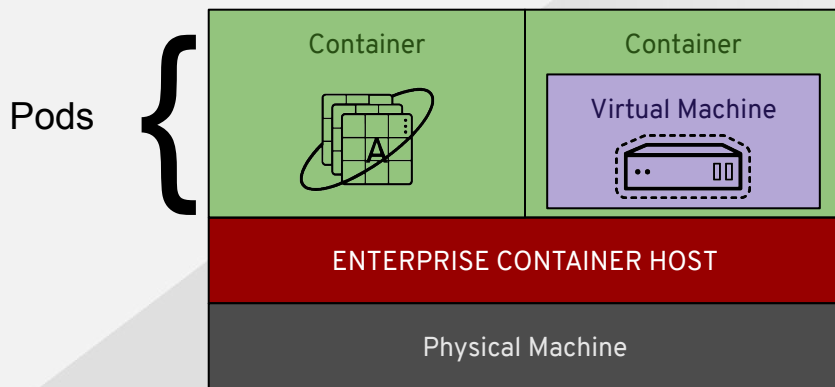
The screenshot displays the OpenShift Virtual Machines management interface. On the left, there is a sidebar with 'Virtual Machines' and 'Templates' sections. The main area shows a 'Virtual Machines' header with a 'Create Virtual Machine' button and a search filter. Below is a table listing five VMs, all in the 'my-test-project' namespace. A context menu is open over the table, showing actions like 'Connect to Console', 'Edit', 'Delete', 'Suspend', 'Reboot', 'Force Reboot', 'Shutdown', 'Force Shutdown', and 'Migrate'. A hand cursor is pointing at the 'Migrate' option.

NAME	NAMESPACE	STATUS	AGE	NODE	IP ADDRESS
VM VM-name-1	NS my-test-project	ⓘ	3d, 4h	Node 1	xxx.xxx.xxx.xxx
VM VM-name-2	NS my-test-project	ⓘ	3d, 4h	Node 1	xxx.xxx.xxx.xxx
VM VM-name-3	NS my-test-project	✖	3d, 4h	Node 1	xxx.xxx.xxx.xxx
VM VM-name-4	NS my-test-project	⚙	3d, 4h	Node 2	xxx.xxx.xxx.xxx
VM VM-name-5	NS my-test-project	⚡	3d, 4h	Node 2	xxx.xxx.xxx.xxx

Leverages tried and trusted RHEL & RHV (KVM) virtualization capabilities.

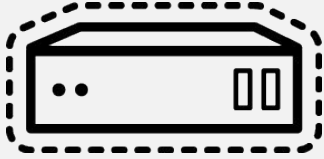
Technology Preview access in OpenShift.

TOGETHER AT LAST

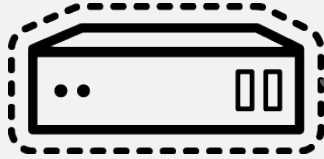


Resultant virtual machines are able to run side by side directly on the same OpenShift nodes as application containers.

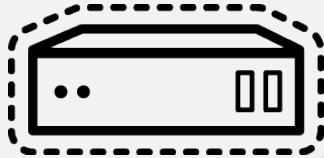
EXAMPLE USE CASE - START WITH A VM



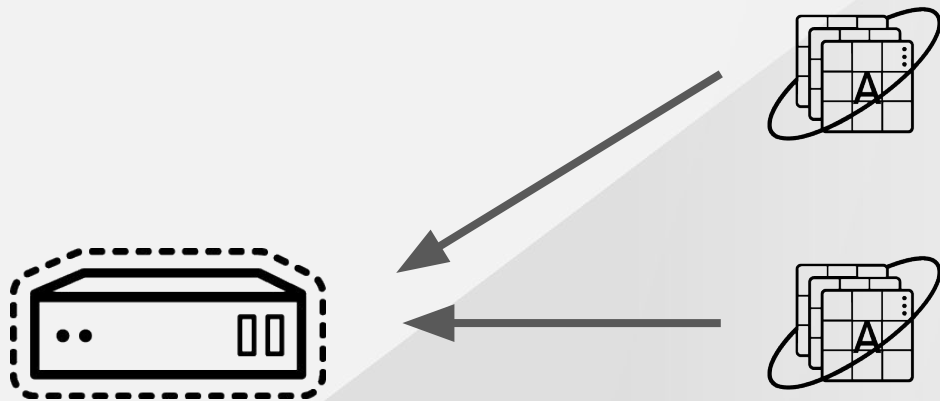
EXAMPLE USE CASE - IMPORT IT!



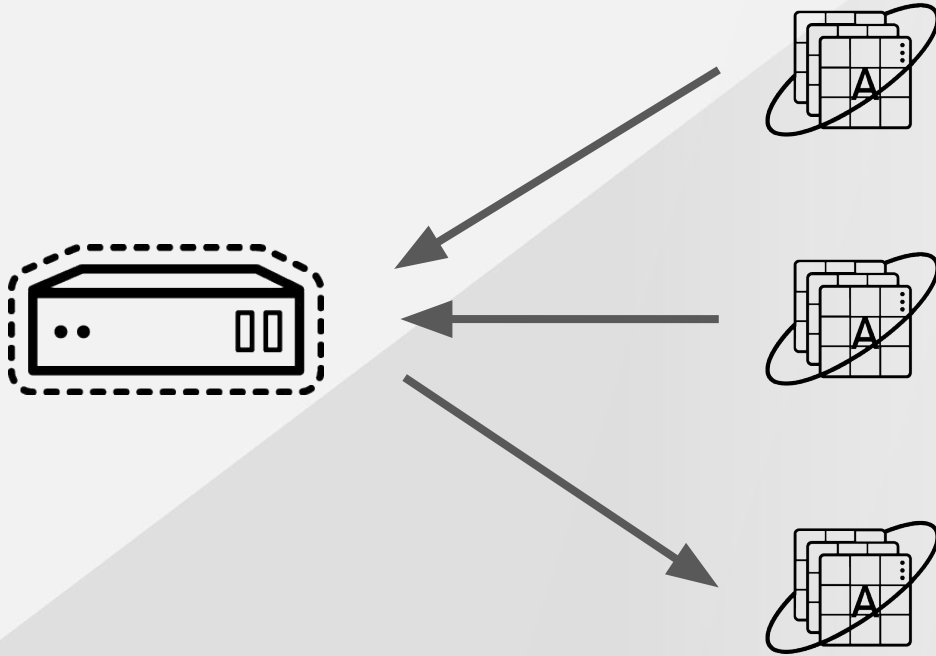
Import Using V2V or from an image.



EXAMPLE USE CASE - BUILD NEW SERVICES

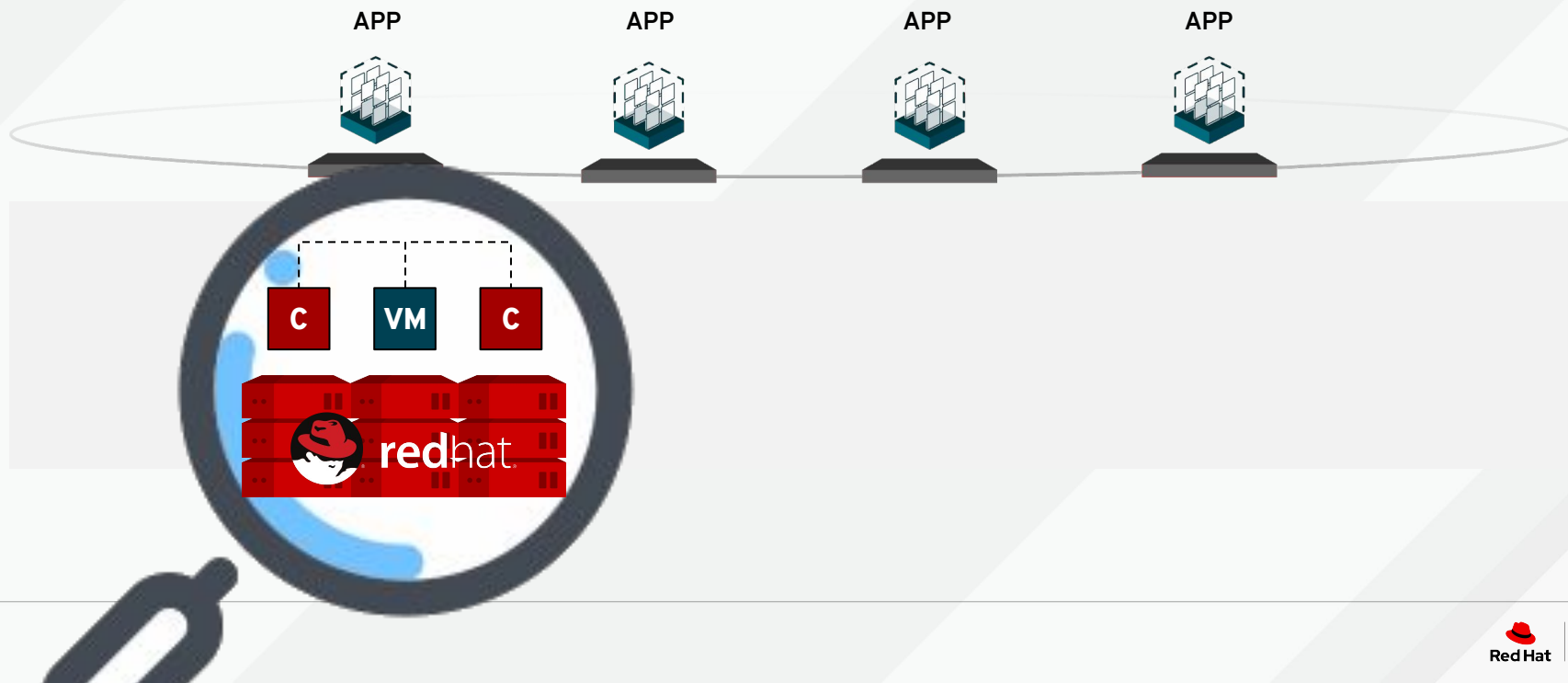


EXAMPLE USE CASE - START DECOMPOSING



INTRODUCING RHHI NEXT

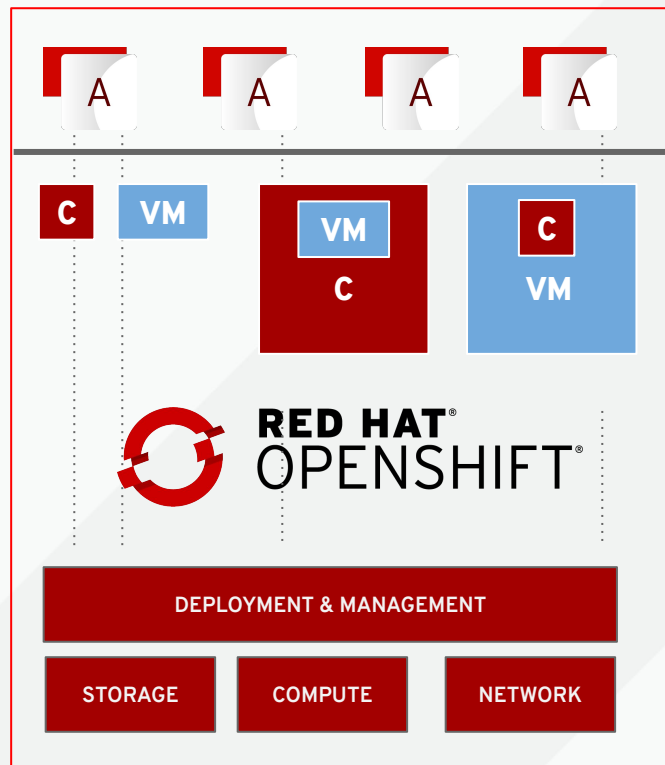
POWERED BY OPENSIFT CONTAINER PLATFORM



WHAT IS RHHI NEXT?

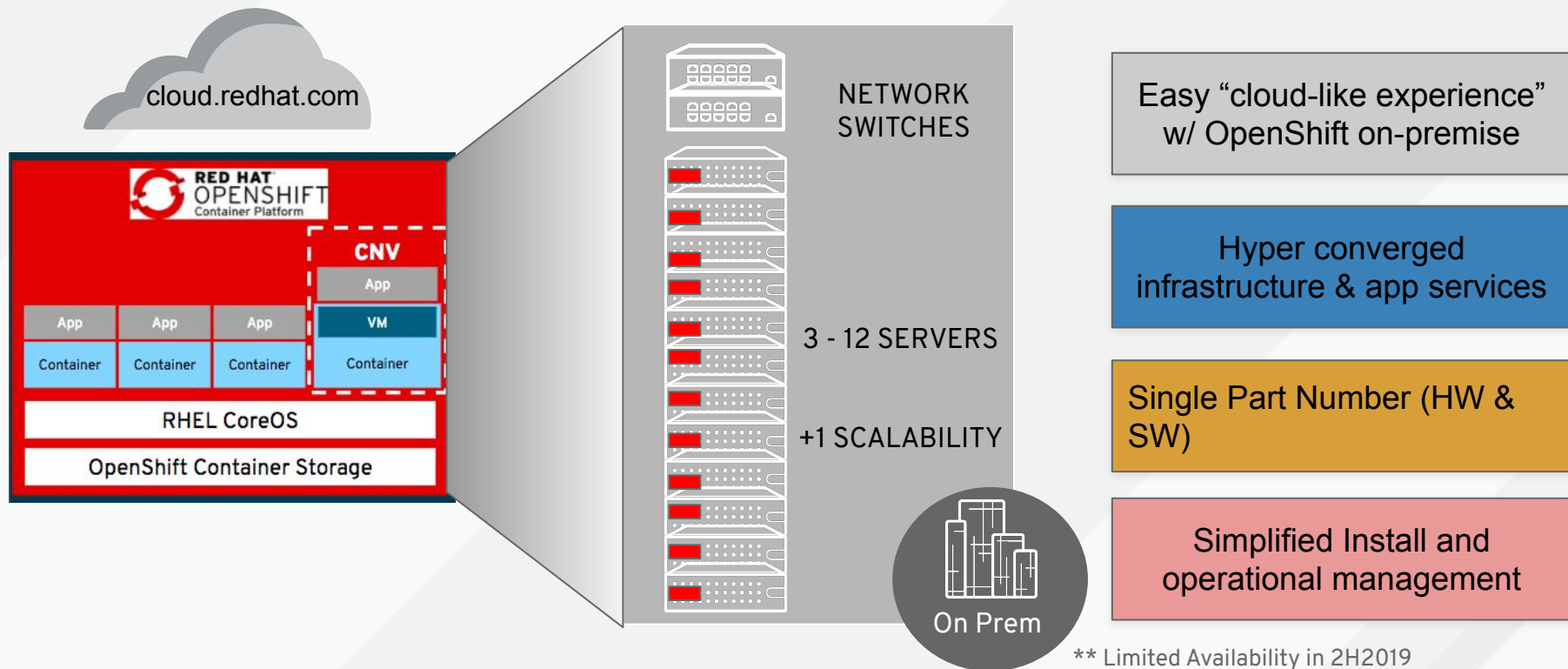
Enterprises are willing to pay a premium for completeness, consistency, and simplicity

Unified platform for
container and VM
workloads under
common management
control



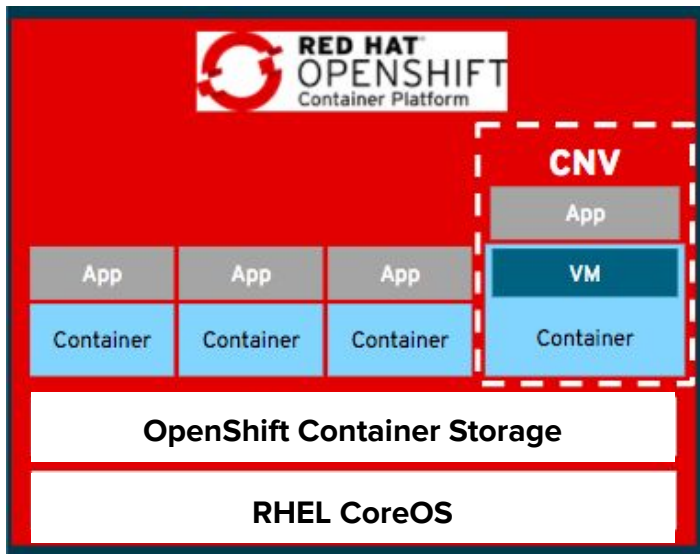
Storage, compute, and
networking tightly
integrated into OpenShift
for seamless customer
experience

RHHI Next



** Limited Availability in 2H2019

WHAT IS IN THE PRODUCT?



- OpenShift Container Platform
- OpenShift Container Storage
- Container-native Virtualization
- RHEL CoreOS
- Industry Standard Server Hardware
- Network Switches (optional)

CUSTOMER BENEFITS



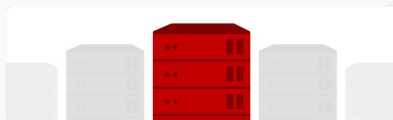
Get the infrastructure for your on-prem app dev up and running quickly



Hyperconverged infrastructure makes it easier to order, install and manage



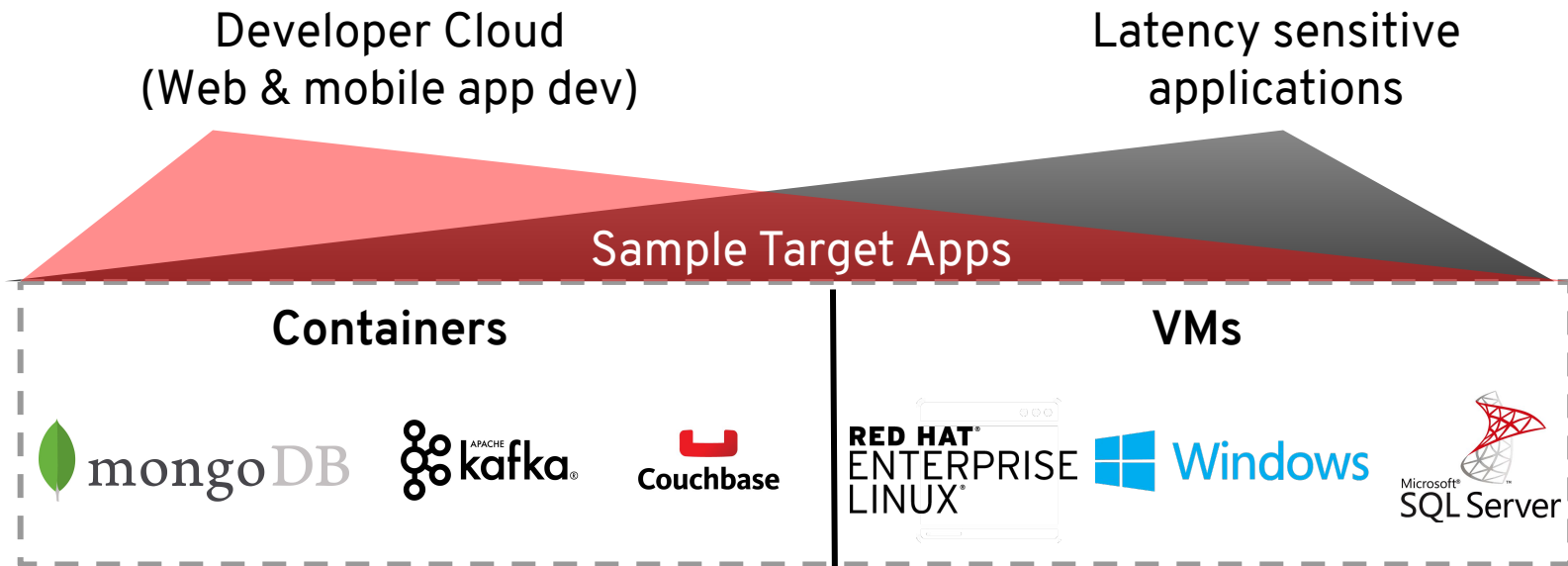
Run virtualized workloads side-by-side with newer container workloads



Consistent operational management with public cloud using with OpenShift

INITIAL TARGET USE CASES

Quick way to get started with full container infrastructure

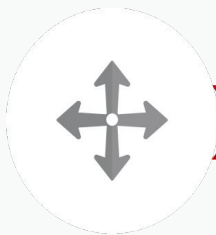


HOW DOES IT WORK?

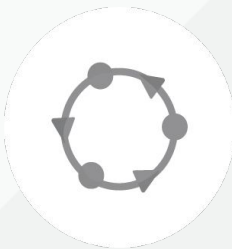
Simplified install and operations



Choose config and
order single part
number (HW&SW)
via partner



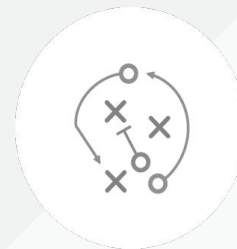
Customer racks
and networks the
servers



Run quick deploy
utility

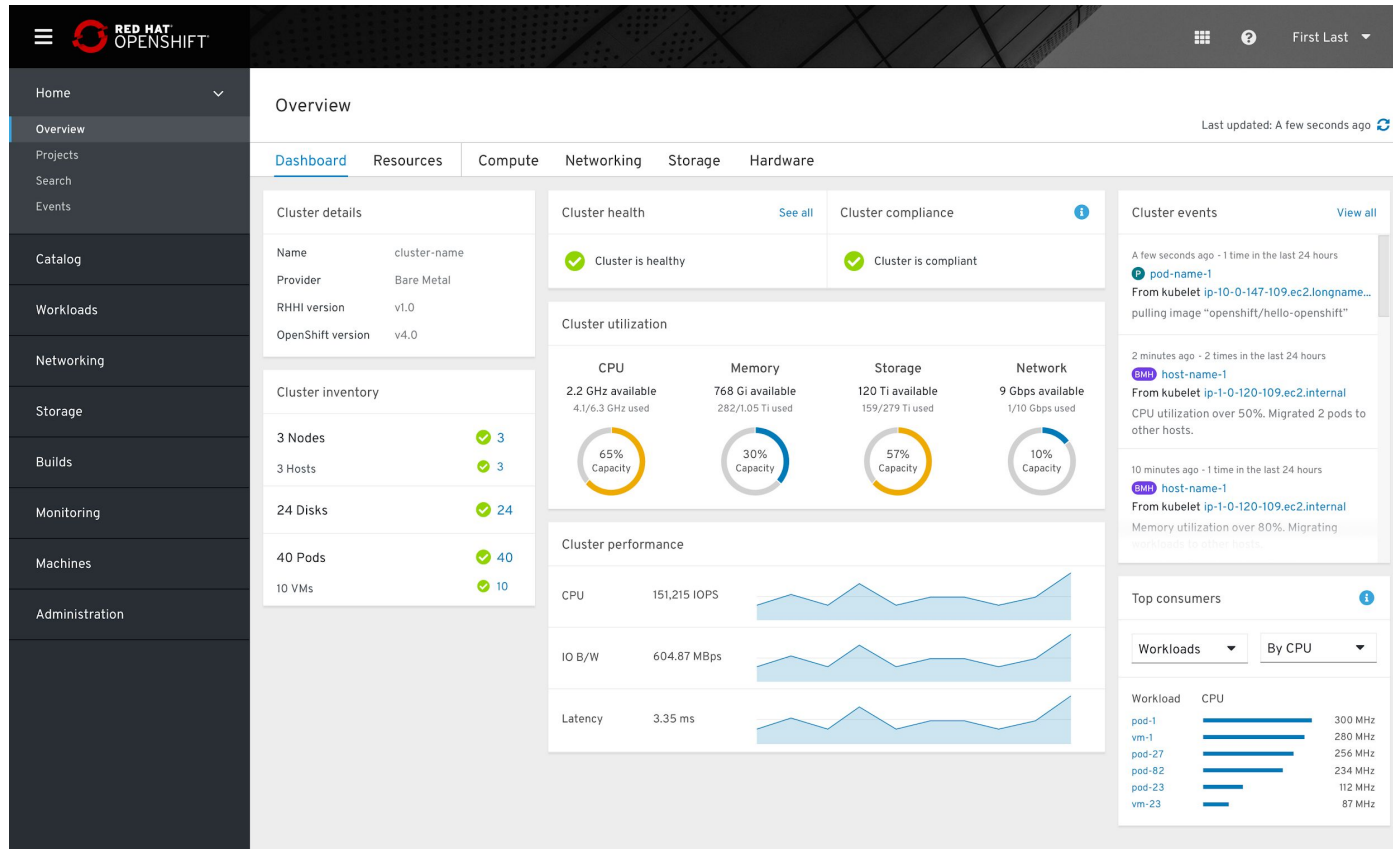


GUI wizard installs
all services with
appropriate config



Over the air
software updates

OPENSIFT CONSOLE PROVIDES DAY 2 AUTOMATION



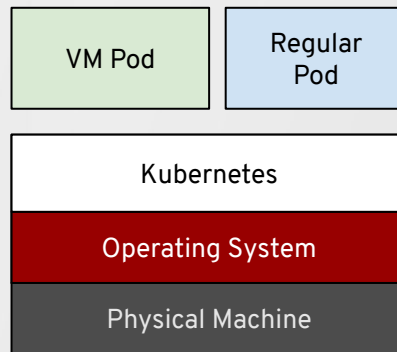
LET'S GO A LITTLE DEEPER...

KUBEVIRT: THE CNV UPSTREAM



<http://kubevirt.io>

- Integrates directly into existing Kubernetes clusters
- Uses a k8s-native approach whenever possible
- Leverage Container Networking Interface (CNI), Container Storage Interface (CSI), and other k8s-native integrations

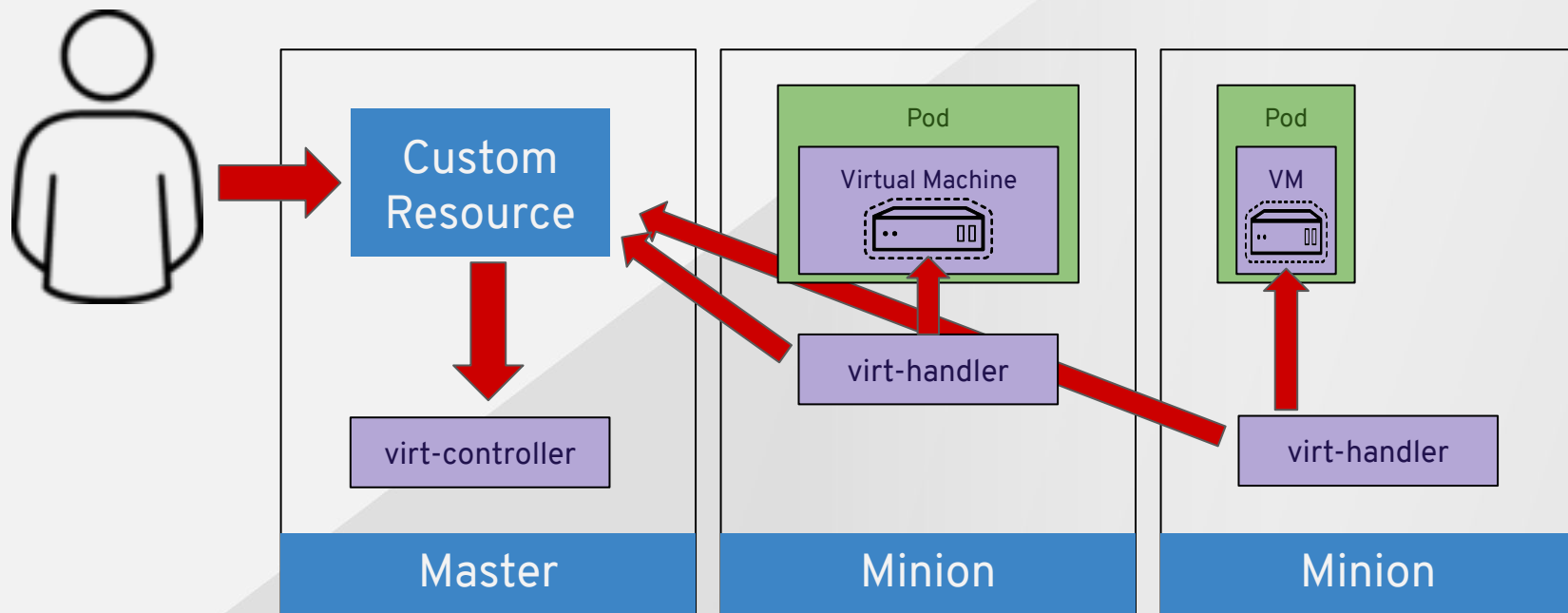


COMPONENTS OF CNV

- **KubeVirt**
The virtual machine operator
<https://github.com/kubevirt/kubevirt/>
- **OpenShift Web Console**
With UI extensions
<https://github.com/kubevirt/web-ui>
- **Containerized Data Importer (CDI)**
Importing disks
<https://github.com/kubevirt/containerized-data-importer>
- **Containerized Virt-v2v**
Importing a whole virtual machine
<https://github.com/kubevirt/v2v-job>



KUBEVIRT ANATOMY



CUSTOM RESOURCE DEFINITIONS

- Build on Kubernetes, adding new API-level resources.
- Declarative when paired with a controller.

```
$ kubectl get crds
NAME                                                    AGE
datavolumes.cdi.kubevirt.io                          5m
virtualmachineinstancepresets.kubevirt.io             5m
virtualmachineinstancereplicaset.kubevirt.io         5m
virtualmachineinstances.kubevirt.io                  5m
virtualmachines.kubevirt.io                          5m
```

A WORD OF CAUTION

In a TELCO context, do not expect RHHI NEXT to support:

- SR-IOV
- DPDK
- VPP
- Real Time Kernel
- ...

in the near future.

Nor should you expect to go beyond the scale described soon....





KUBERNETES OPERATORS

A tool to reduce operational complexity

KUBERNETES ADOPTION PHASES

1. Stateless apps

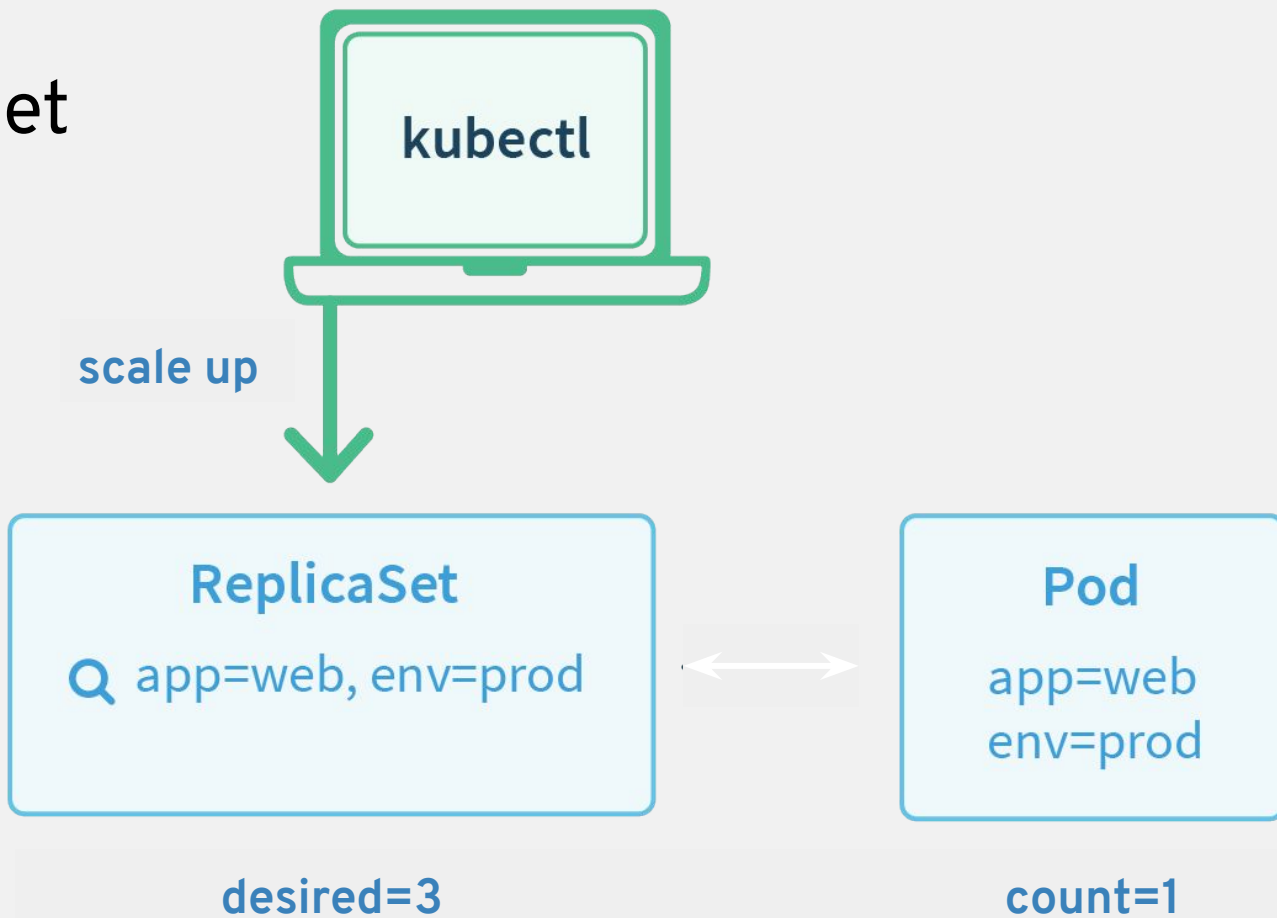
ReplicaSets

Deployments

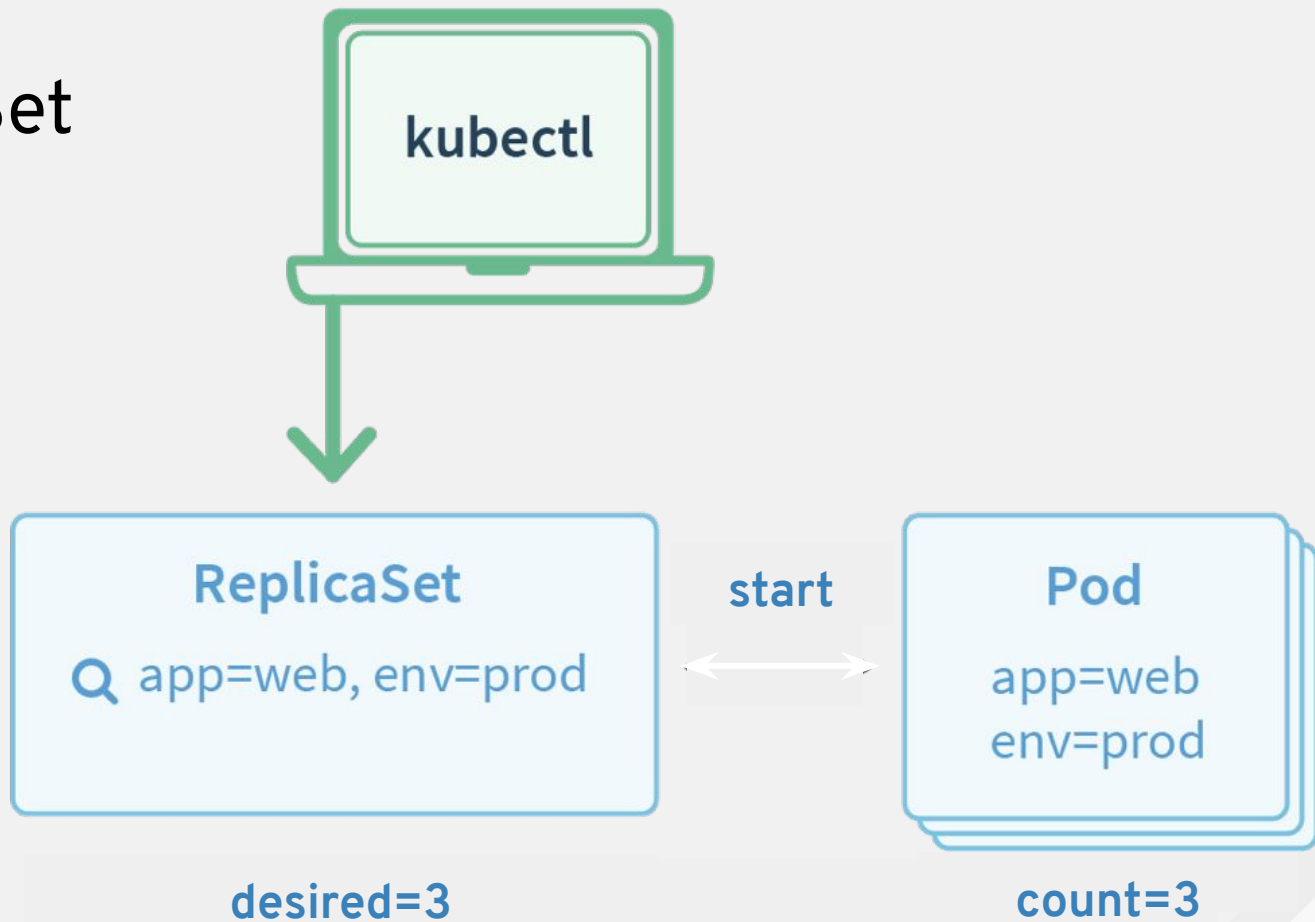
Scaling stateless apps: **easy**

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


ReplicaSet



ReplicaSet



What about apps that **store data**?

Creating a database is **easy**

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

KUBERNETES ADOPTION PHASES

1. Stateless apps

ReplicaSets
Deployments

2. Stateful apps

StatefulSets
Storage/CSI

Running a database **over time** is harder



 Resize/Upgrade

 Reconfigure

 Backup

 Healing



KUBERNETES ADOPTION PHASES

1. Stateless apps

ReplicaSets
Deployments

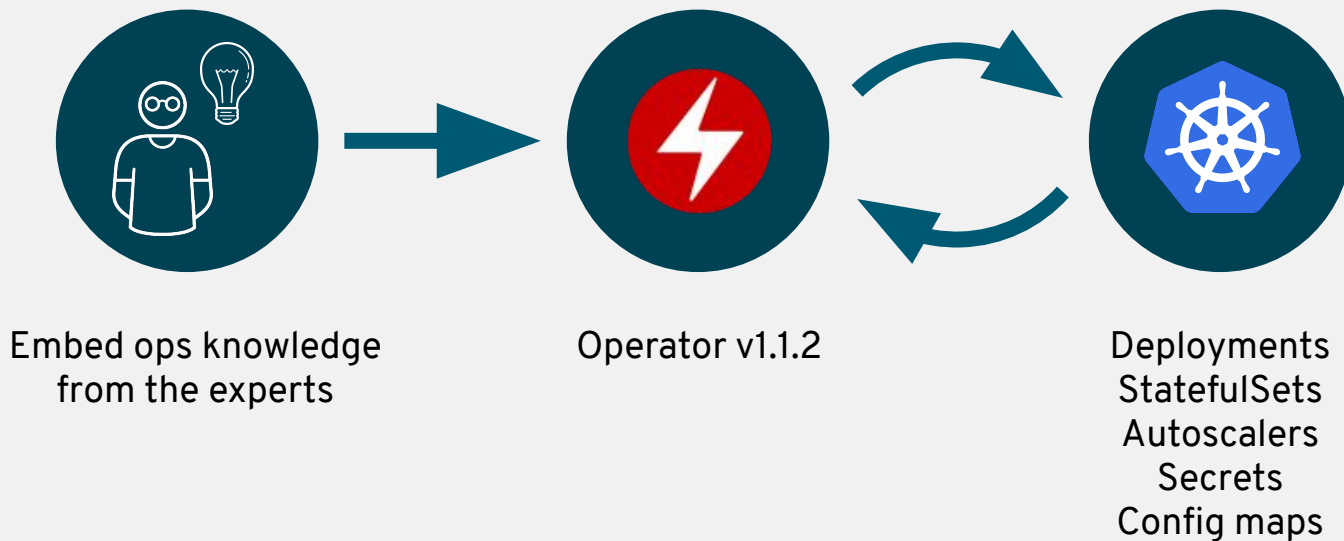
2. Stateful apps

StatefulSets
Storage/CSI

3. Distributed systems

Data rebalancing
Autoscaling
Seamless upgrades

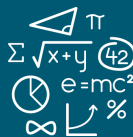
WHAT IS AN OPERATOR?



OPERATORS FOR ALL



Flexible app
architectures



No reinvention
of core concepts



Uniform deploy
and debug



Truly hybrid

Example: etcd Operator

What is etcd?

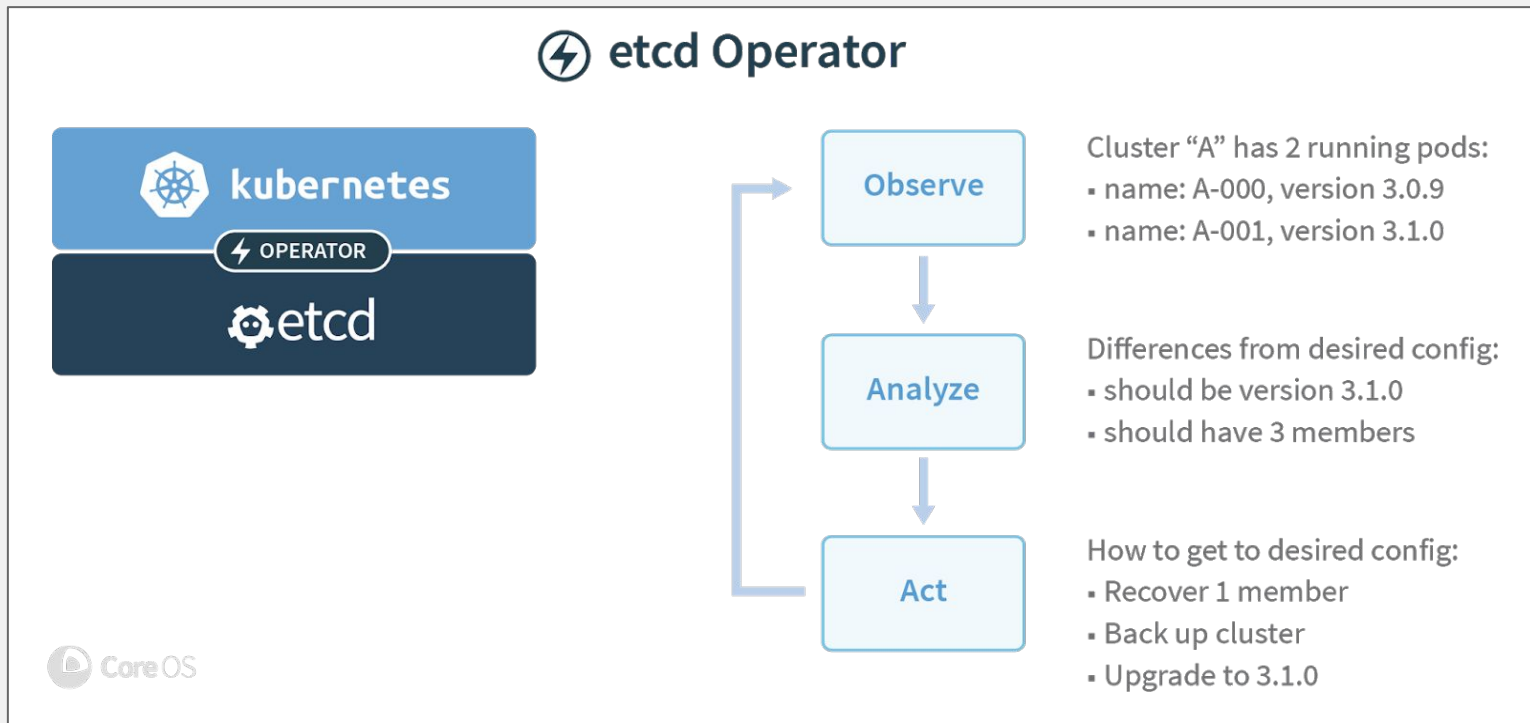


- distributed key-value store
- primary datastore of Kubernetes
- stores and replicates all Kubernetes cluster state

Example: etcd Operator

```
kind: EtcdCluster
apiVersion: etcd.database.coreos.com/v1beta2
metadata:
  name: example-etcd-cluster
spec:
  size: 3
  version: "3.1.0"
```

Example: etcd Operator



YES, I WANT THAT!

How do I get it?



For Builders and the community

- Easily create application on Kubernetes via a common method
- Provide standardized set of tools to build consistent apps

For application consumers and Kubernetes users

- Keep used apps up to date for security and app lifecycle management
- Consume Kube-native applications easily and correctly



**OPERATOR
SDK**

Build



**OPERATOR
LIFECYCLE MANAGER**

Run

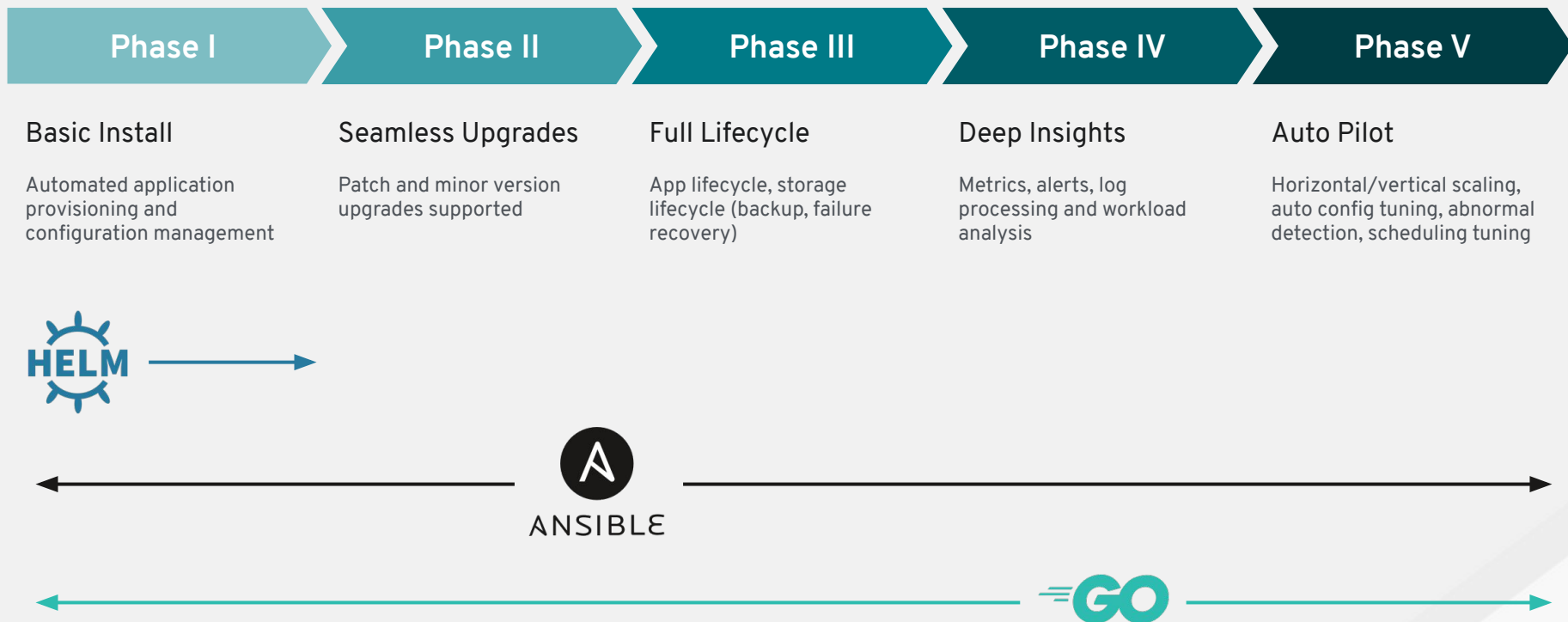


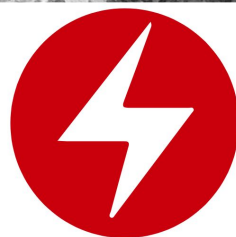
**OPERATOR
METERING**

Operate

<https://github.com/operator-framework>

OPERATOR MATURITY MODEL

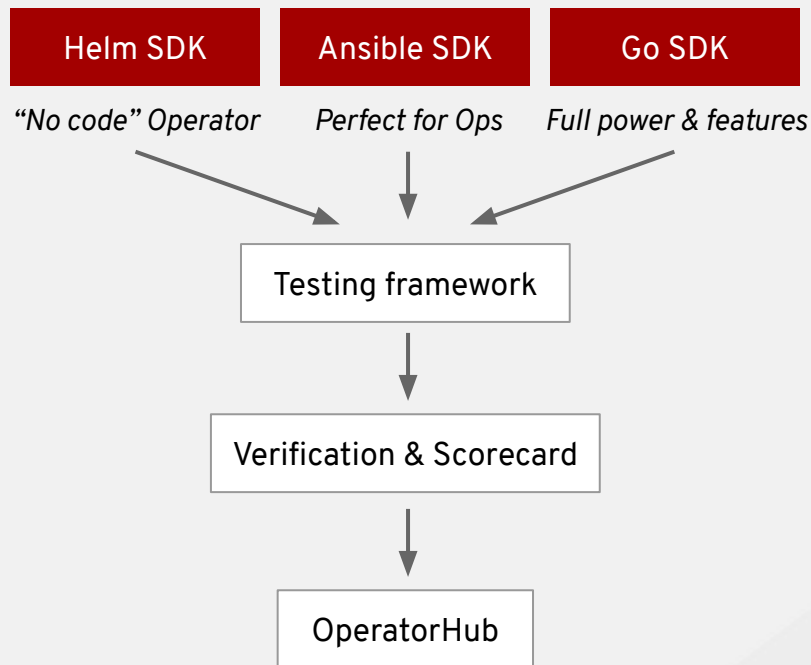




**OPERATOR
SDK**

OPERATOR SDK

- “No code” improvements to Helm SDK user experience
- Testing is extremely important for Operators, we have a testing framework built in
- SDK includes a “scorecard” to ensure your Operator is technically correct

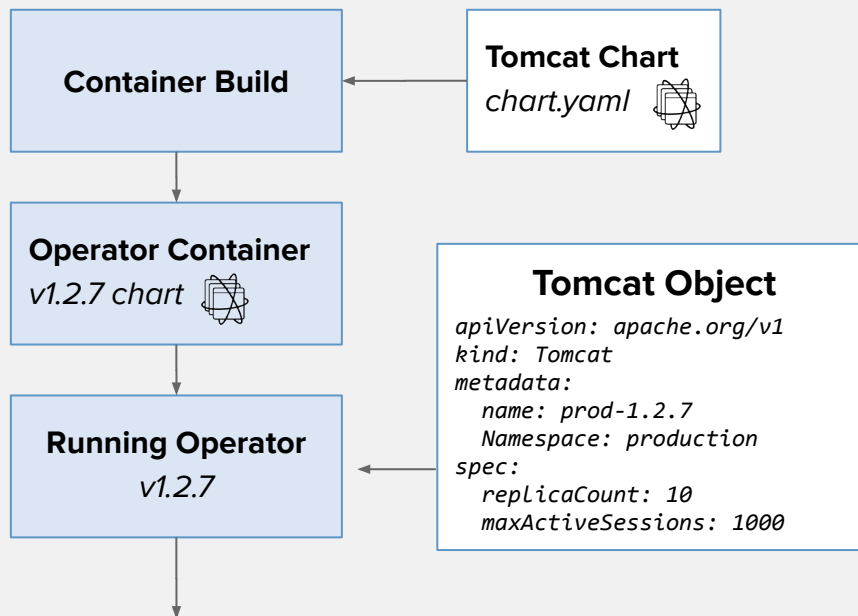


HELM SDK

- Easiest way to get started – “no code”
- Use templating from Helm
- Connect values.yaml to Kubernetes object

```
$ operator-sdk new tomcat-operator  
--type=helm  
--helm-chart=stable/tomcat
```

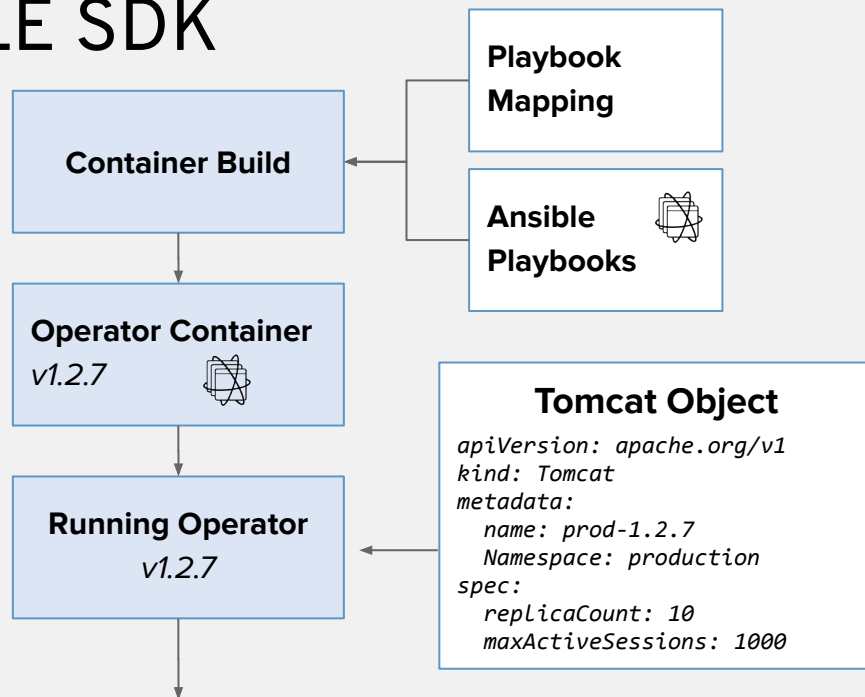
HELM SDK



```
$ oc get Tomcats --all-namespaces
NAMESPACE   NAME           READY   STATUS    RESTARTS   AGE
production   prod-1.2.7     1/1     Running   0           4d
staging      staging-v1.2.8 1/1     Running   1           2h
```

ANSIBLE SDK

- Run Ansible playbooks in an Operator fashion
- Great for Ops teams that aren't traditional devs
- Takes the human out of the loop
- Connects the playbooks to Kubernetes events like Node failures



```
$ oc get Tomcats --all-namespaces
```

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
production	prod-1.2.7	1/1	Running	0	4d
staging	staging-v1.2.8	1/1	Running	1	2h

GO SDK

- Best way to get to a Level 5 “Auto Pilot” Operator
- Use the same tools Kubernetes developers use upstream
- Popular for database & storage vendors
- Built-in testing framework

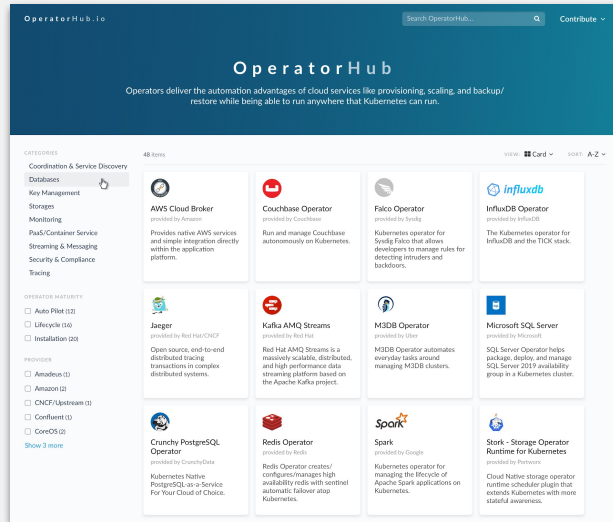
```
if tomcats.length != desired {  
    //initial deployment  
}  
  
foreach tomcats as tomcat {  
    if tomcat.Spec.Replicas != size {  
        //fix size  
    }  
}
```


OPERATORS ACROSS THE INDUSTRY



Lower barrier to entry

Don't have to be an expert in
administering the app



<https://operatorhub.io>



AWS Service Operator

The AWS Service Operator allows you to manage AWS resources using Kubernetes Custom Resource Definitions.

[Home](#) > AWS Service Operator

AWS Service Operator

The AWS Service Operator allows you to manage AWS resources using Kubernetes Custom Resource Definitions. Using the AWS Service Operator enables a gitops workflow to drive your infrastructure to the desired state leveraging Kubernetes Custom Resource Definitions (CRD), the Kubernetes internal control loop, and AWS CloudFormation orchestration.

In order to run the Operator the node will need AWS IAM privileges. This can be done through a service like [kube2iam](#). If you are using an Amazon Elastic Container Service for Kubernetes (EKS) cluster, you most likely provisioned this with CloudFormation.

The command shown below will use the CloudFormation stacks to try to update the proper Instance Policy with the correct permissions. Make sure to replace `${STACK_NAME}` with the nodegroup stack name from the CloudFormation console. A more limited IAM role may be substituted if desired.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/AdministratorAccess --role-name $(aws cloudformation describe-stacks --stack-name ${STACK_NAME} --output json | jq -r ".Stacks[0].Outputs[0].OutputValue" | sed -e 's/.*/\\\\/g')
```

Before running this operator, you will need to create a Secret that contains your `cluster-name`, `region`, and `account-id`. You can do so based off the template below:

[Install](#)

OPERATOR VERSION

0.0.1

CAPABILITY LEVEL ②

- ☒ Basic Install
- ☐ Seamless Upgrades
- ☐ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

PROVIDER

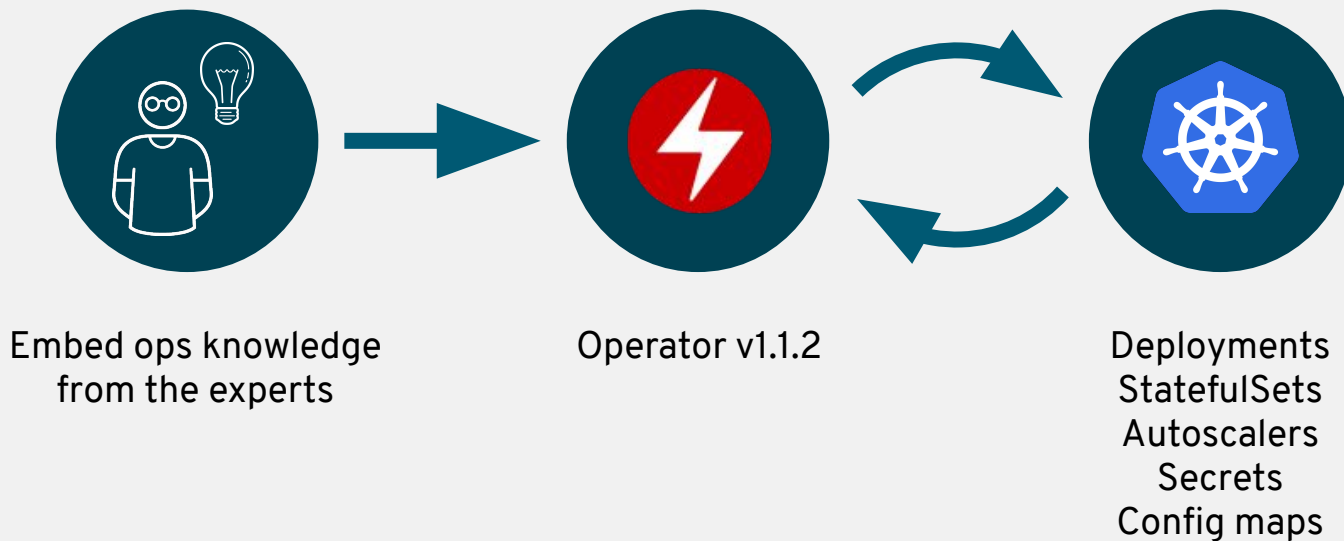
Amazon Web Services, Inc.



OPERATOR LIFECYCLE MANAGER



BREAKING DOWN AN OPERATOR



BREAKING DOWN AN OPERATOR

Cluster actions

- Install the CRDs and make sure nothing else owns those CRDs
- Verify dependent CRDs exist

Run the Operator(s)

- Pull and run the container as a Deployment
- Watch the correct namespaces with a Service Account

Permissions

- Minimal set of permissions to function
- Bind those to the Service Account

BREAKING DOWN AN OPERATOR

Cluster actions

- Install the CRDs and make sure nothing else overlaps
- Verify dependent CRDs exist

Run the Operator(s)

- Pull and run the container as a Deployment
- Watch the correct namespaces with a Service Account

Permissions

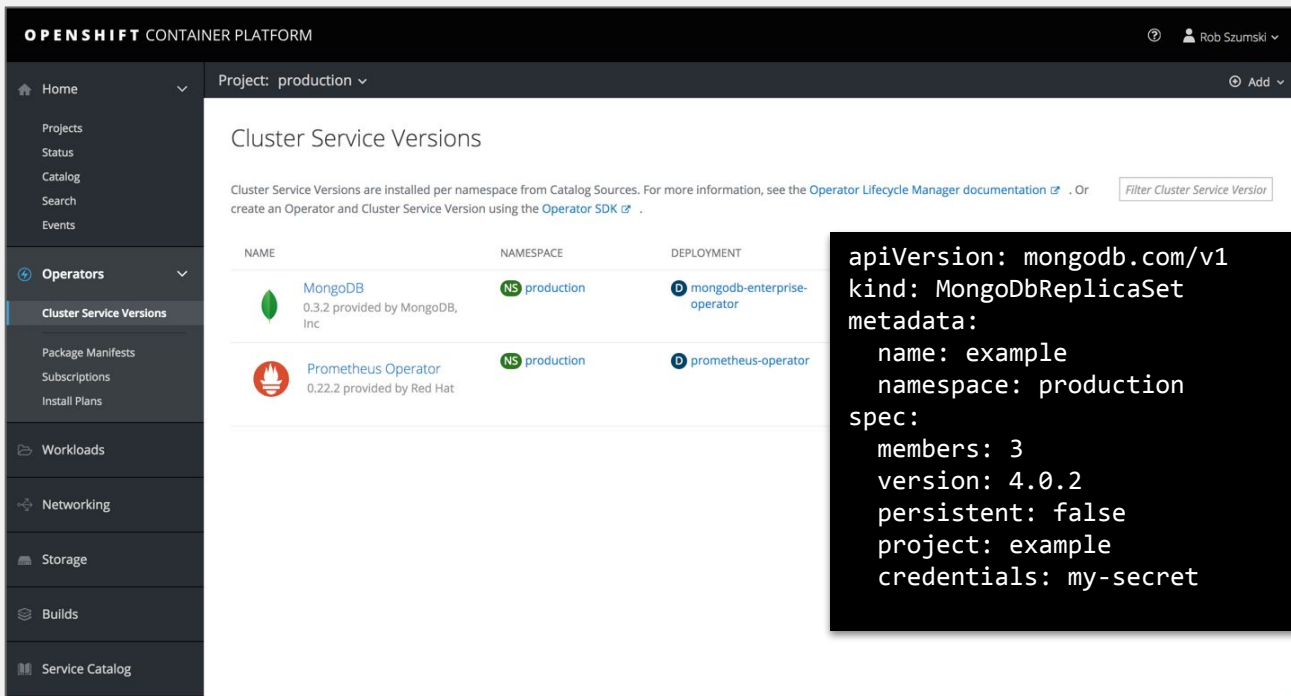
- Minimal set of permissions to function
- Bind those to the Service Account

```
apiVersion: operators.coreos.com/v1alpha1
kind: ClusterServiceVersion
...
customResourceDefinitions:
  owned:
    ...
  required:
    ...
install:
  strategy: Deployment
  clusterPermissions:
    ...
  permissions:
    ...
  spec:
    deployments:
      ...
```

TAKE A LOOK AT A REAL CSV

[aws-service.v0.0.1.clusterserviceversion.yaml](#)

SELF-SERVICE FOR ENGINEERS



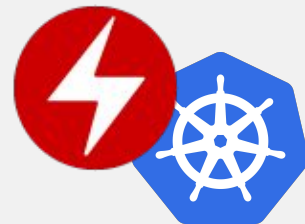
The screenshot shows the OpenShift Container Platform web console. The top navigation bar includes the OpenShift logo, the text "CONTAINER PLATFORM", a help icon, and the user name "Rob Szumski". The left sidebar contains a navigation menu with items: Home, Projects, Status, Catalog, Search, Events, Operators (selected), Cluster Service Versions, Package Manifests, Subscriptions, Install Plans, Workloads, Networking, Storage, Builds, and Service Catalog. The main content area is titled "Cluster Service Versions" and shows a table of installed versions for the "production" namespace.

NAME	NAMESPACE	DEPLOYMENT
 MongoDB 0.3.2 provided by MongoDB, Inc	 production	 mongodb-enterprise-operator
 Prometheus Operator 0.22.2 provided by Red Hat	 production	 prometheus-operator

```
apiVersion: mongodb.com/v1
kind: MongoDBReplicaSet
metadata:
  name: example
  namespace: production
spec:
  members: 3
  version: 4.0.2
  persistent: false
  project: example
  credentials: my-secret
```


SIMPLER GITOPS FOR ENGINEERS

GitHub



```
apiVersion: mongodb.com/v1
kind: MongoDBReplicaSet
metadata:
  name: example
  namespace: pr
spec:
  members: 3
  version: 4.0.
  persistent: f
  project: exam
  credentials:
    apiVersion: mongodb.com/v1
    kind: CustomFrontend
    metadata:
      name: frontend
      namespace: production
    spec:
      database-name: example
      highly-available: true
      resources:
        cores: 1
        memory: 1024
```

Deployments
StatefulSets
Autoscalers
Secrets
ConfigMaps
Service Accounts
Limits/Quotas
PersistentVolumes

FULL CONTROL FOR ADMINS

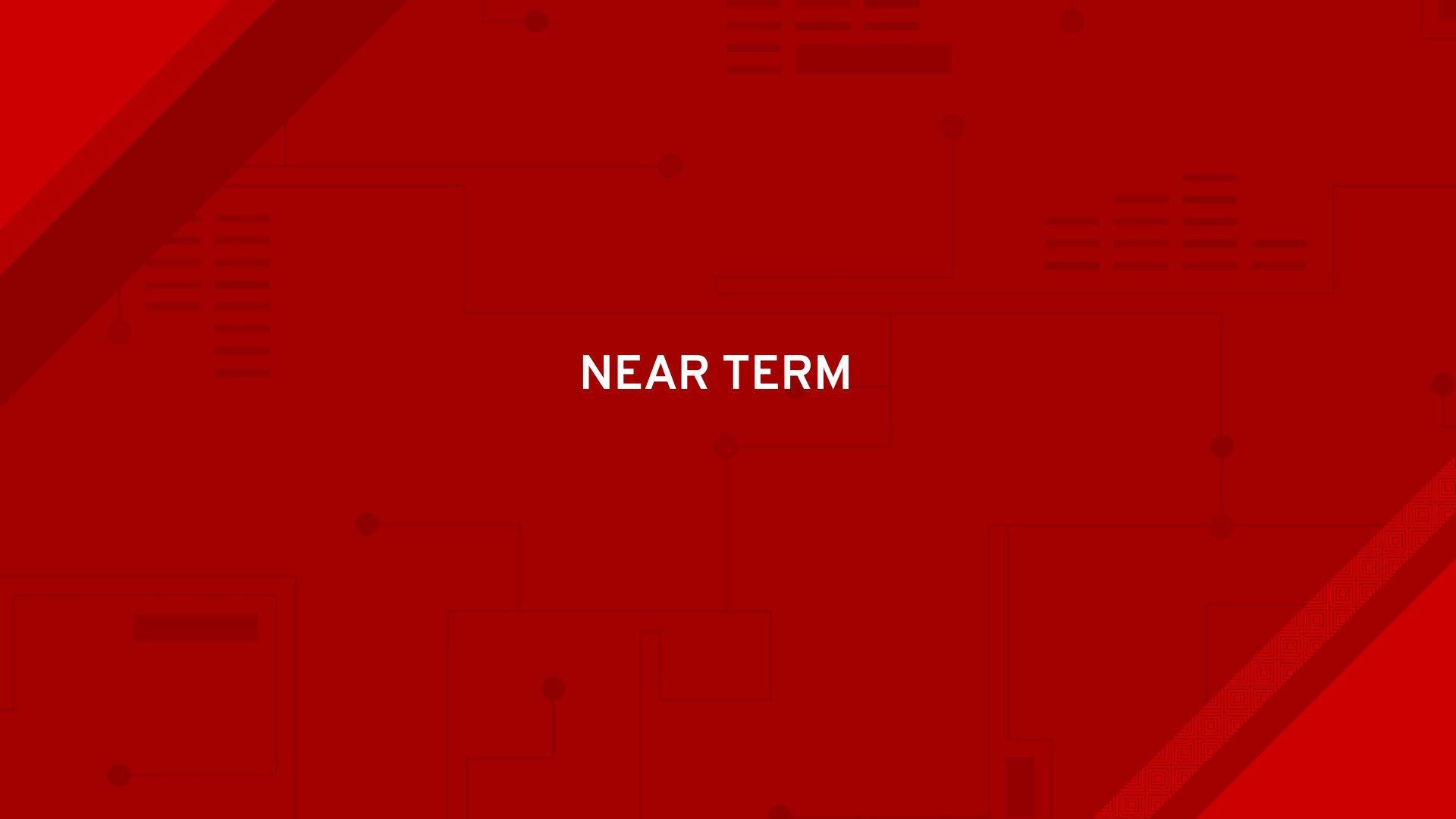
OPENSIFT CONTAINER PLATFORM ? Rob Szumski

Project: all projects + Add

Subscriptions

[Create Subscription](#) Filter Subscriptions by package...

NAME ↑	NAMESPACE	STATUS	CHANNEL	APPROVAL STRATEGY
SUB amq-streams-fzs9	NS staging	✓ Up to date	preview	Automatic ⋮
SUB couchbase-enterprise-7qn82	NS rob-dev	✓ Up to date	preview	Automatic ⋮
SUB etcd-x9fpg	NS tony-dev	✓ Up to date	alpha	Automatic ⋮
SUB federationv2-kqr4	NS rob-dev	✓ Up to date	alpha	Automatic ⋮
SUB mongodb-enterprise-g6s54	NS staging	✓ Up to date	preview	Automatic ⋮
SUB mongodb-enterprise-vqfbt	NS test	✓ Up to date	preview	Automatic ⋮
SUB mongodb-enterprise-wfg6x	NS production	✓ Up to date	preview	Automatic ⋮
SUB prometheus-9zp4t	NS staging	✓ Up to date	preview	Automatic ⋮
SUB prometheus-b54fp	NS test	✓ Up to date	preview	Automatic ⋮
SUB prometheus-plwxx	NS production	✓ Up to date	preview	Automatic ⋮



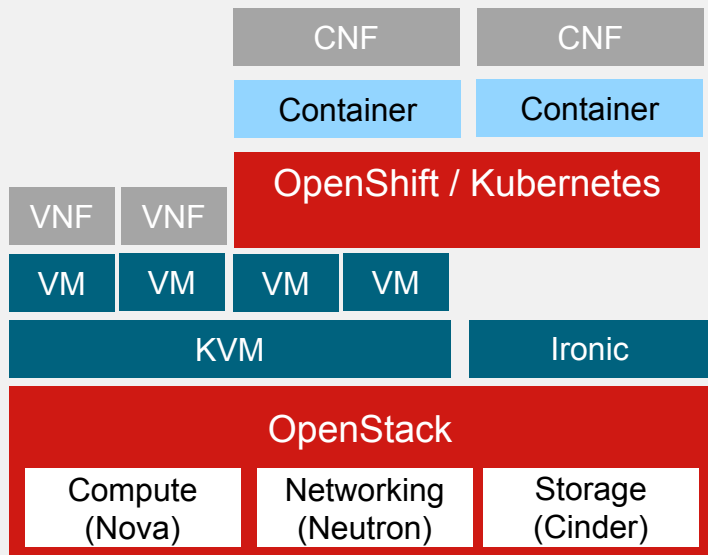
NEAR TERM

Rakuten 5G Ready Network



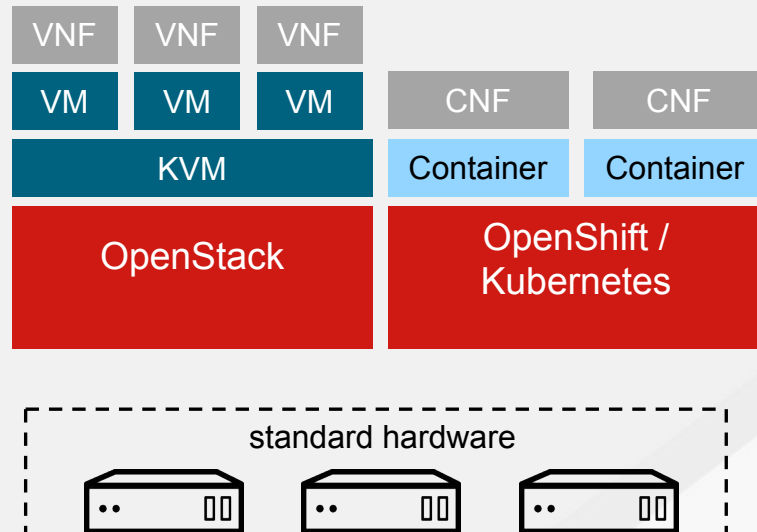
Choices for CY19/20

OpenShift on OpenStack (OpenStack Undercloud)



OR

OpenShift & OpenStack (OpenStack Undercloud)





redhat.

THANK YOU



plus.google.com/+RedHat



facebook.com/redhatinc



linkedin.com/company/red-hat



twitter.com/RedHatNews



youtube.com/user/RedHatVideos



redhat.®