redhat.

OpenShift Container Platform

Red Hat CoreOS

Hakam Abdelqader

IBM Cloud

What will you learn from this talk?

- When/why did container focused distributions start appearing
- History of Container Linux + Atomic
- Red Hat CoreOS Use Cases
- Foundation for Immutable Host Talks

Where did it start?

v94.0.0

 **philips** released this on Oct 3, 2013 · 586 commits to master since this release

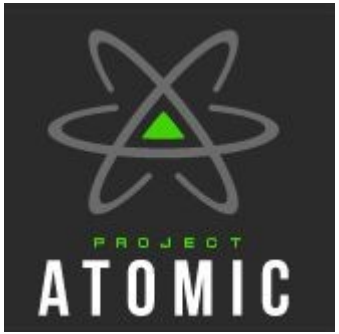
Assets 2

Source code (zip)

Source code (tar.gz)

- Git is now included by default as a number of people use it for shipping around assets, code, etc like a distributed rsync
- Docker is upgraded to 0.6.3
- xz is included to support new compression types
- Custom OEMs can be provided via the cpio on PXE images

Then Came the Atomic Age



Announcing Project Atomic: An Operating System Concept for Running Docker Containers

by Joe Brockmeier – Tuesday 15 April 2014

As most folks know, Red Hat has already been working hard on Docker support in Red Hat Enterprise Linux. Today we're taking the wraps off a new operating system concept for running Docker containers called Project Atomic. This concept, known as an Atomic Host, will provide users with a familiar host environment for Docker containers that allows atomic updates to the host OS as well as containerized applications.

The CentOS Project, Fedora Project, and Red Hat will be taking the technologies developed under Project Atomic to deliver Atomic Hosts for running containerized applications. The Fedora Project's Atomic Initiative has evaluation builds available today, with CentOS images coming soon.

IBM

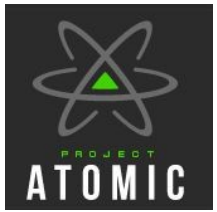
CoreOS Projects and Tooling

- etcd
- Ignition
- mantle
- fleet
- torcx
- rkt
- toolbox
- Flannel
- operators
- … and much much more!

IBM

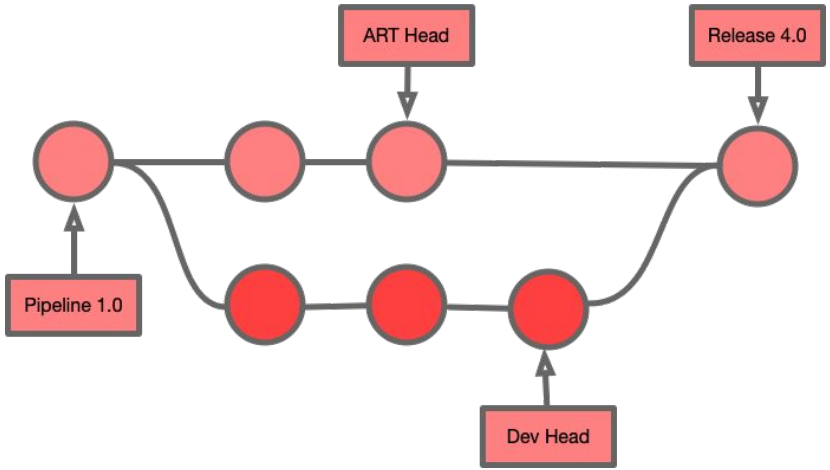
Project Atomic Projectsand Tooling

- ostree
- rpm-ostree
- System-containers
- atomic-cli
- buildah
- skopeo
- cri-o
- cockpit
- … and much much more!



Last Year This Happened

Transactional Updates via OSTree



Like Git for the Operating System

Treat every system file as a hard link to a version of the OS.

Download only the files that have changed between versions on disk.

Update which version the links point then reboot.

Rollbacks between any version still on disk

And this started

Deciding on Philosophy

Minimal
- In terms of provided packages

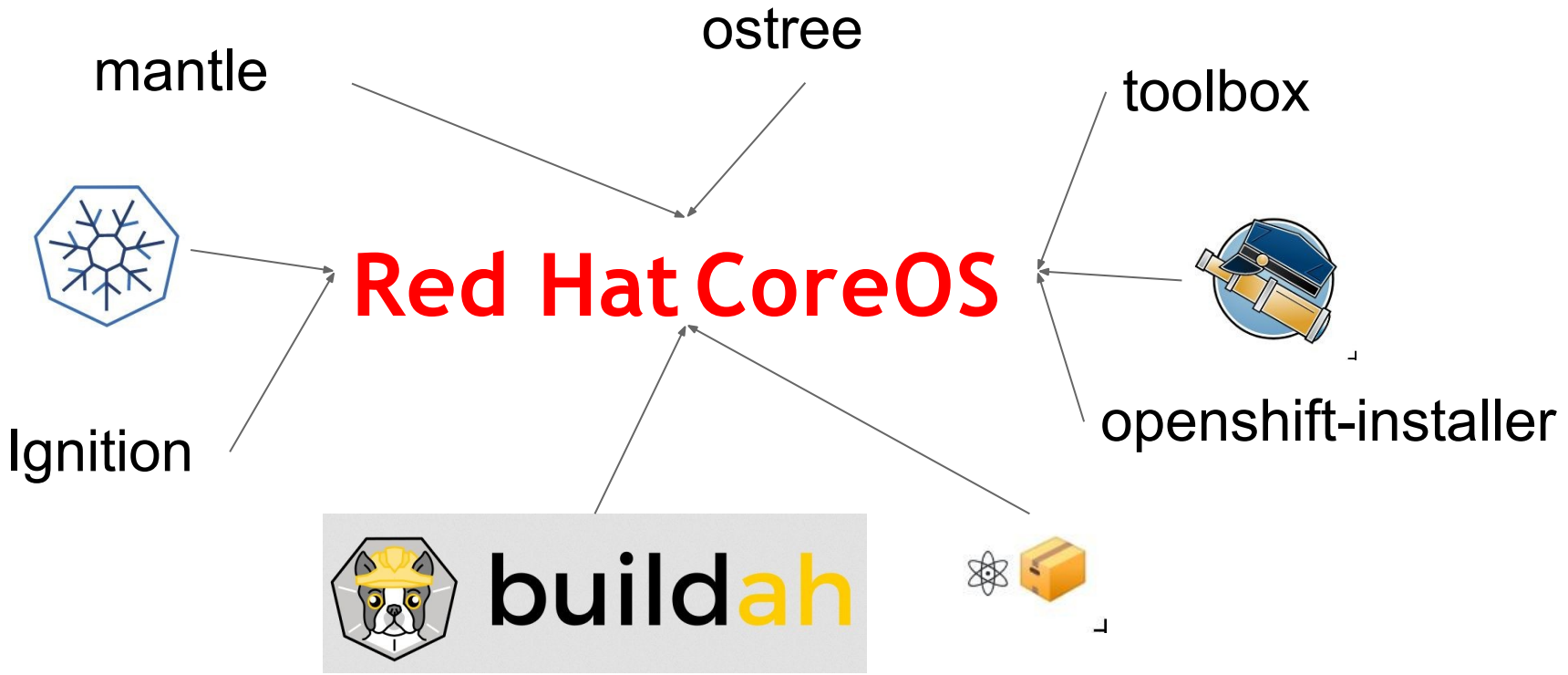
“**Immutable**”
- Controlled mutability

Effortless Management
- SSH usage is not required

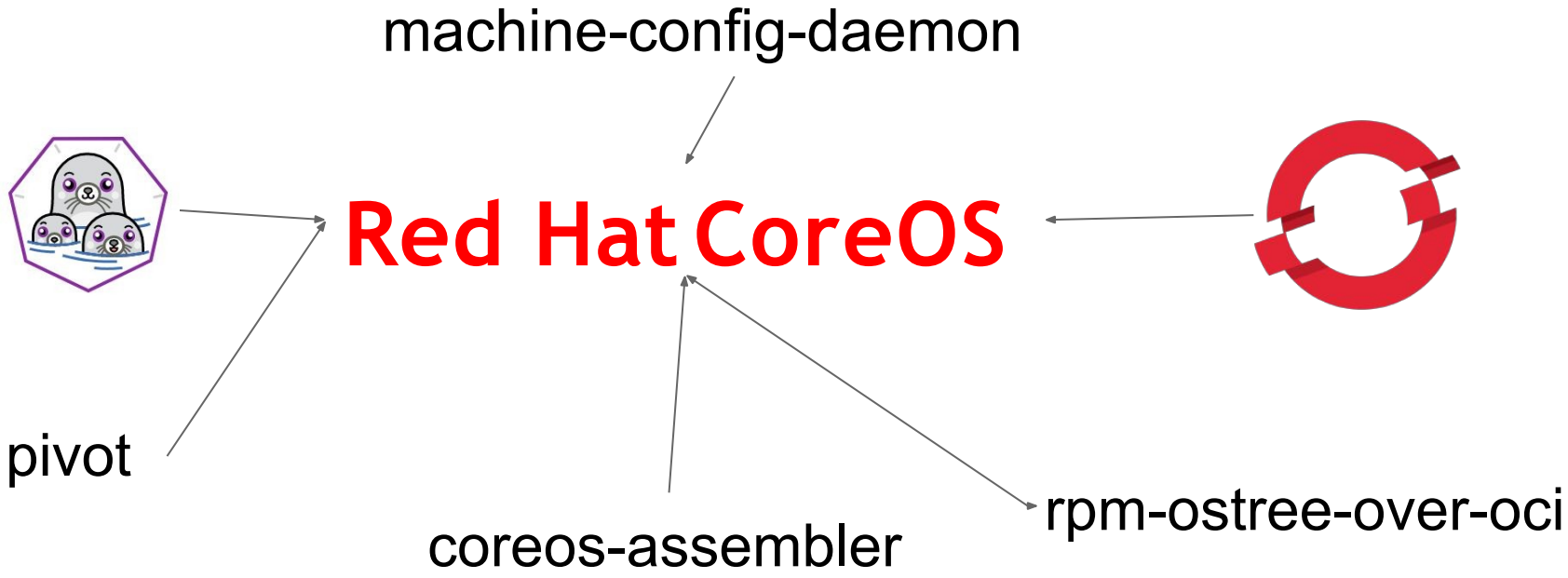
Opinionated
- Support specific tools and use cases

Focus on the Cluster
- Embed Openshift packages
- Push management to the cluster

Combining Forces



And picking upmore!

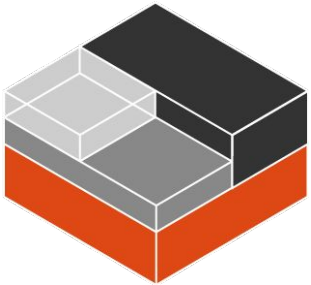


A Wealth of Operating Systems

Use cases

Container Linux

Designed for general container workloads



RHEL

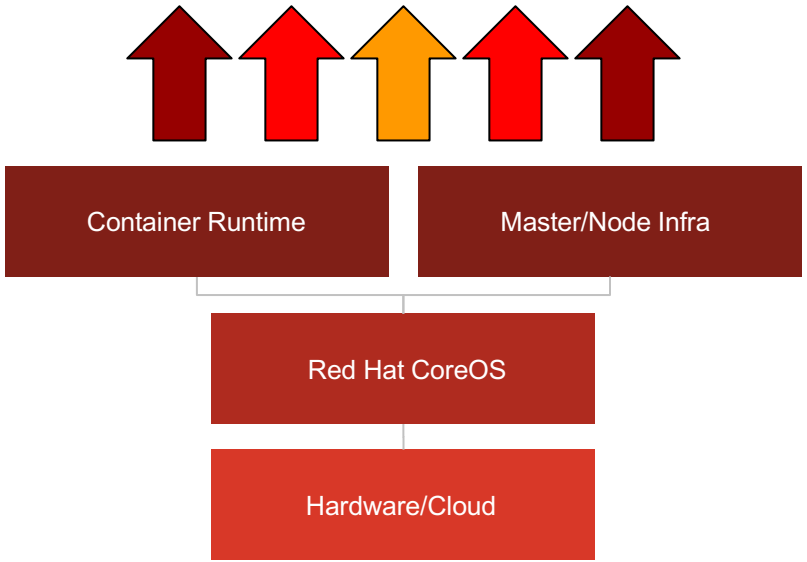
Designed for General Use

RHCOS

Designed to power the container scheduler

IBM

Red Hat CoreOS is the abstraction layer between hardware and the container scheduling infrastructure

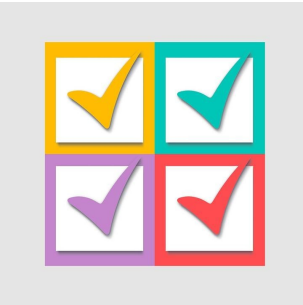


A Wealth of Operating Systems

Runtimes

Container Linux

Provides multiple runtimes



RHEL

Can install runtimes

RHCOS

Provides one runtime to satisfy the cluster

IBM

A Wealth of Operating Systems

Content

Container Linux

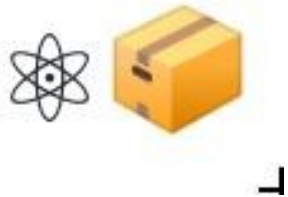
Exploded content on the filesystem
Gentoo Based
Gentoo Kernel

RHEL

RPMs
RHEL Content
RHEL kernel

RHCOS

RPM-OStree
RHEL Content(*)
RHEL kernel



A Wealth of Operating Systems

Update Sources

Container Linux

Omaha Protocol/CoreUpdate

https://commons.wikimedia.org/wiki/File:Omaha.jpg

RHEL

RHEL repos, Satellite

RHCOS

MCO/MCD looks for the reference in the release payload found in Cincinnati

https://commons.wikimedia.org/wiki/File:Downtown_Cincinnati_viewed_from_Mt_At_Adams.jpg

Red Hat CoreOS Security

- Inherits Security from RHEL
  - Same kernel-level support as RHEL
  - SELinux enforcing
  - CVE updates directly from RHEL
- Immutable is securable
  - Minimal configuration == minimal configuration drift
  - Fully configured via the cluster (no SSH/config-mgmt vectors)
- Enables Security via OpenShift
  - One-click orchestrated rolling upgrades reduces ops overhead
  - Future work:
    - SSH access taints nodes as unschedulable
    - automatically alert/quarantine vulnerable nodes

Focusing on the Cluster

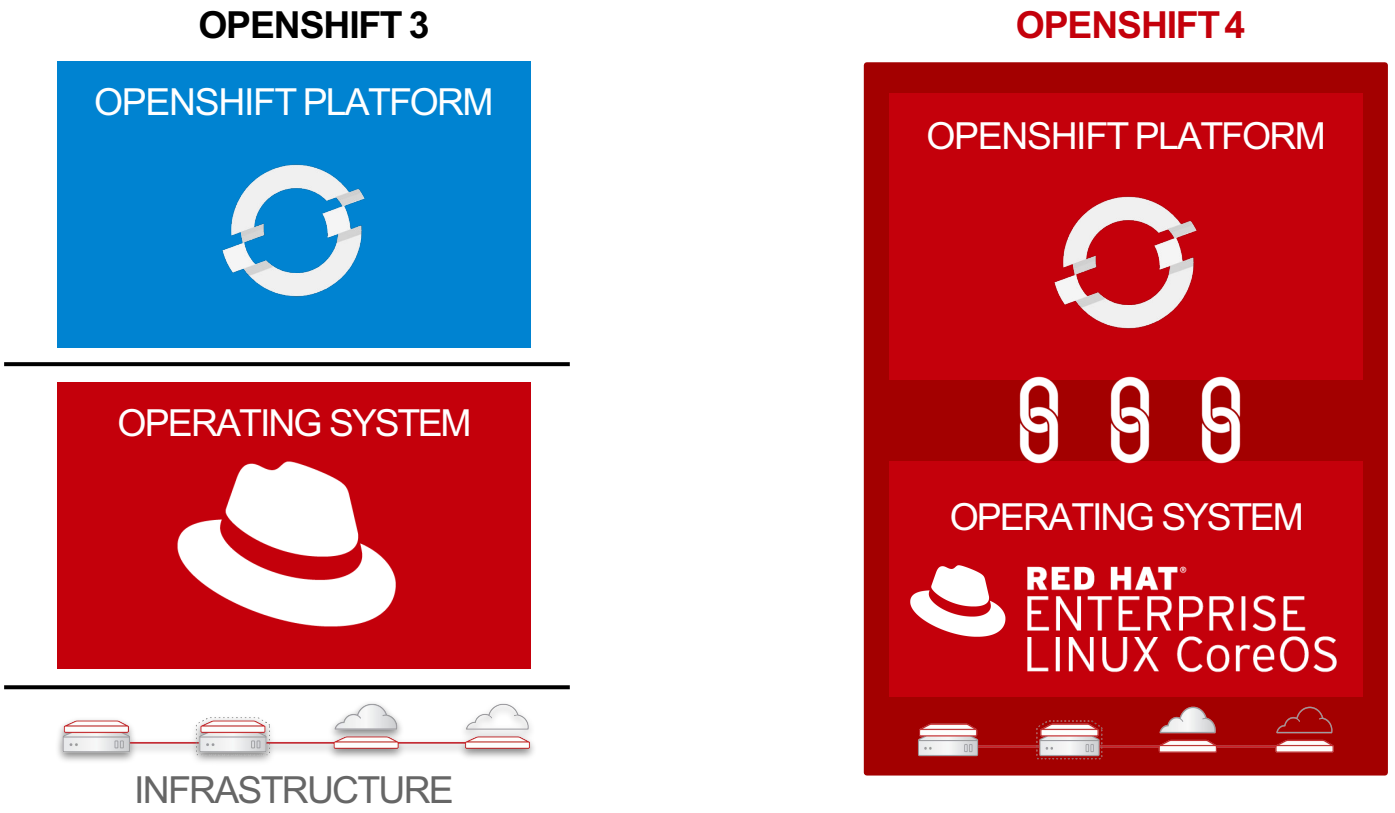
Red Hat CoreOS (RHCOS):

- Is **only** meant to be used with OpenShift
- is a component of OpenShift
- Cluster and Operating System are **versioned together**
- should be managed **through** the cluster
- reports when directly accessed
- ties the container runtime to the version of kubernetes

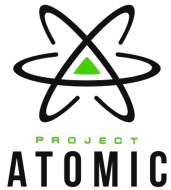
https://commons.wikimedia.org/wiki/File:Rack_Servers_Fujitsu_Primergy_2.jpg

IBM

FULL STACK AUTOMATED INSTALL



RHEL COREOS

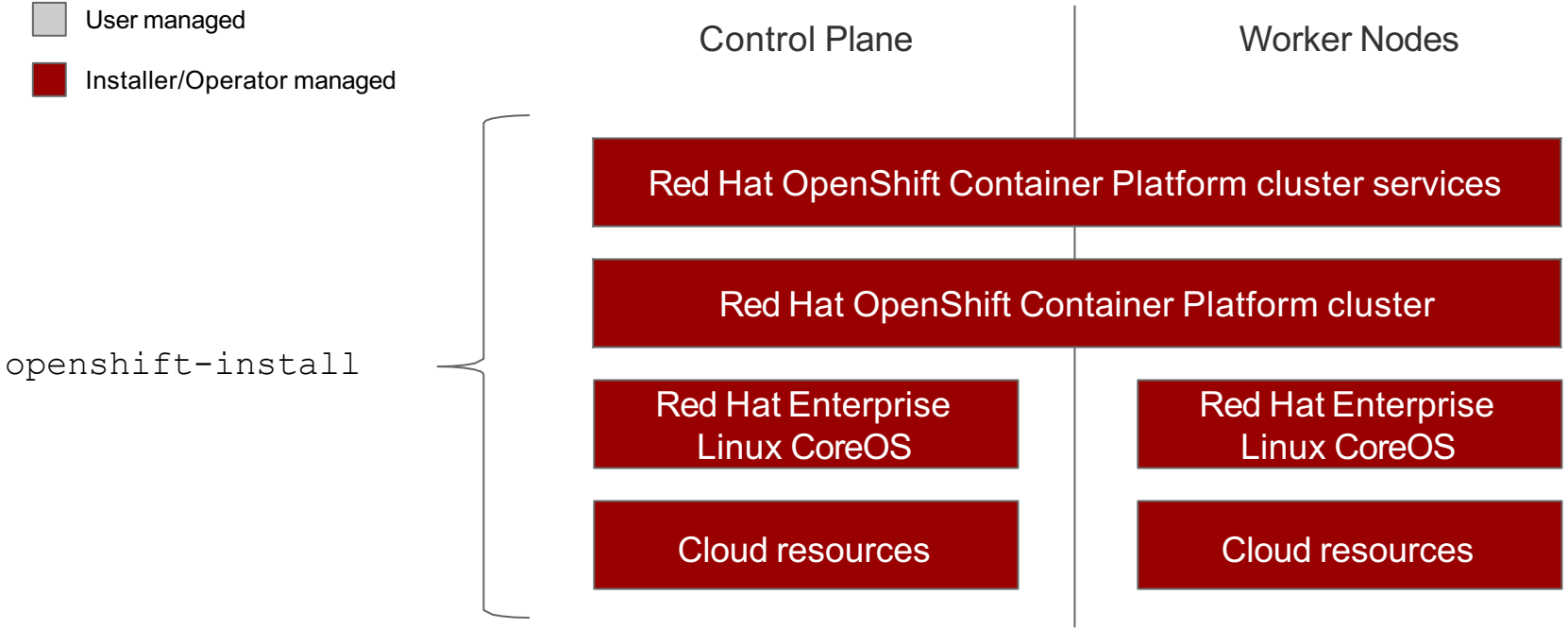


Red Hat
Enterprise Linux
CoreOS

- 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

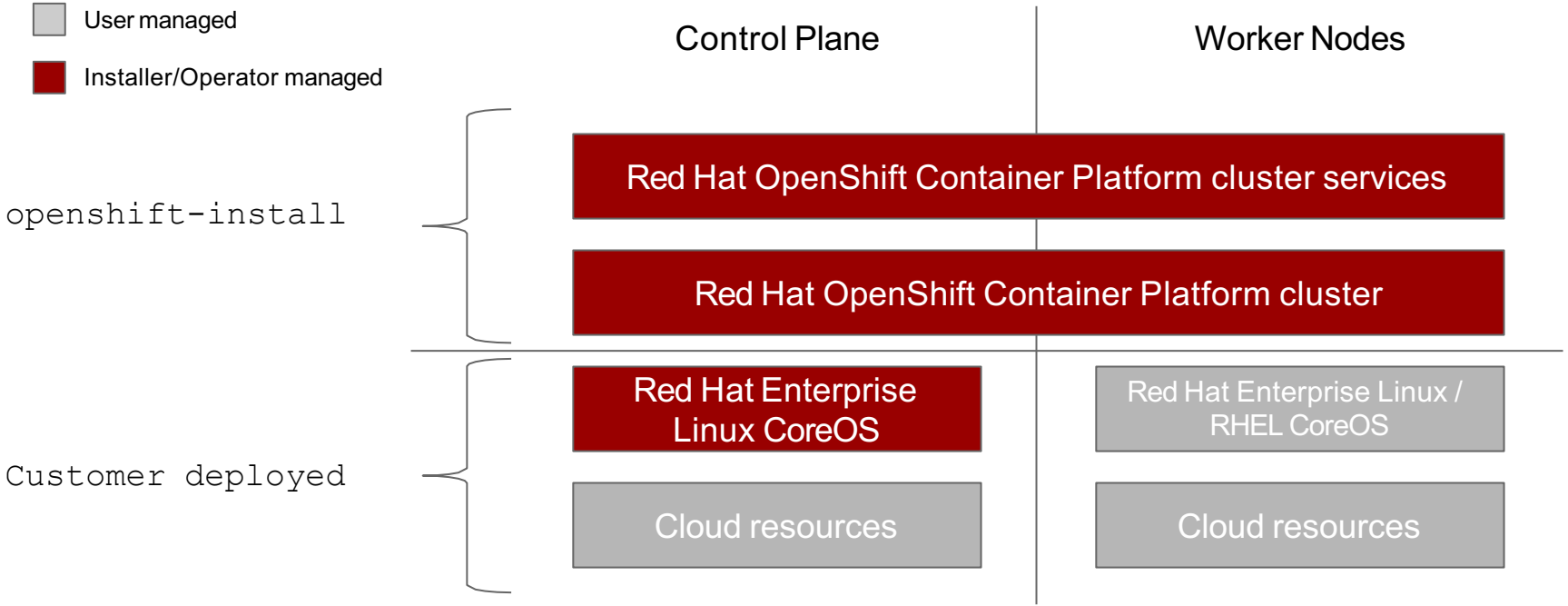
INSTALLER PROVISIONED INFRASTRUCTURE (IPI)

Day 1:OpenShift install - Day 2: Operators



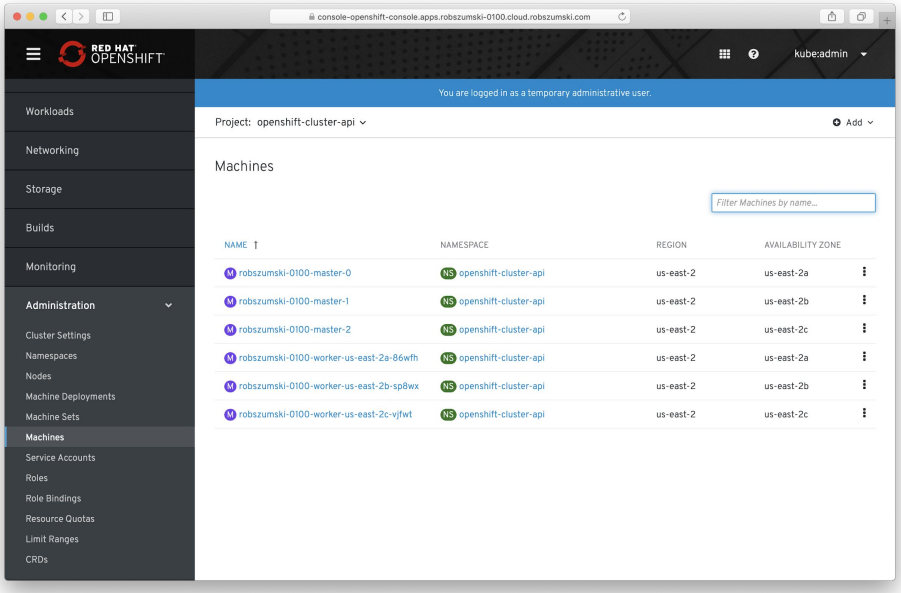
USER PROVISIONED INFRASTRUCTURE (UPI)

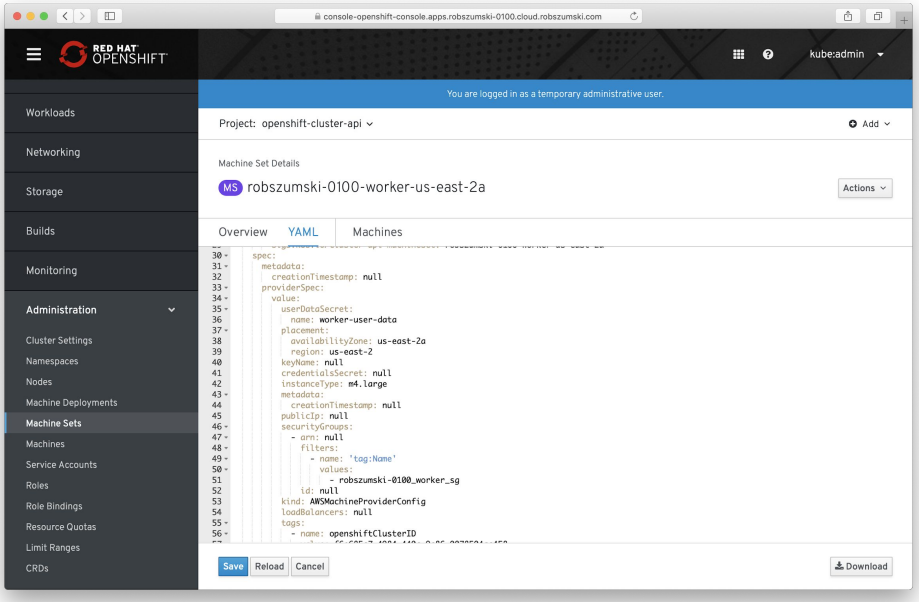
Day 1: OpenShift install - Day 2: Operators + Customer Managed Nodes & Infra



USING KUBERNETES TO PROVISION KUBERNETES CLUSTERS

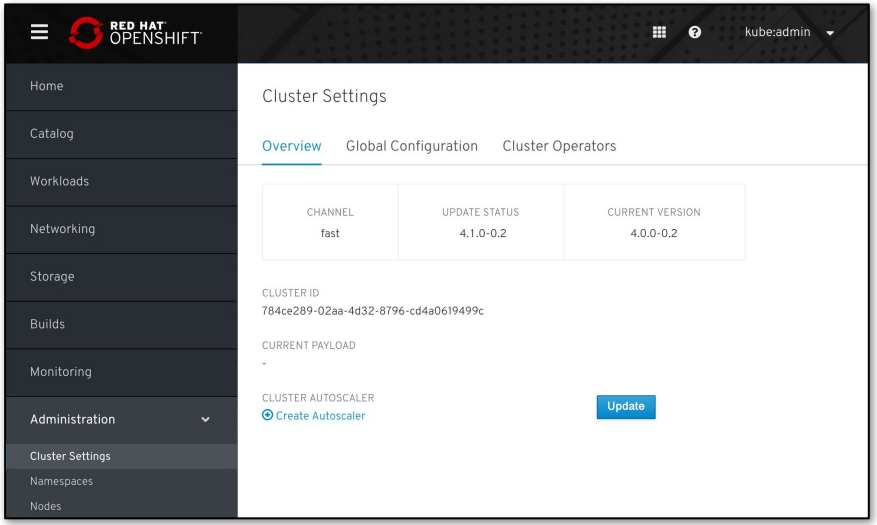
KUBERNETES MACHINE API OPERATOR





OVER-THE-AIR UPDATES

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

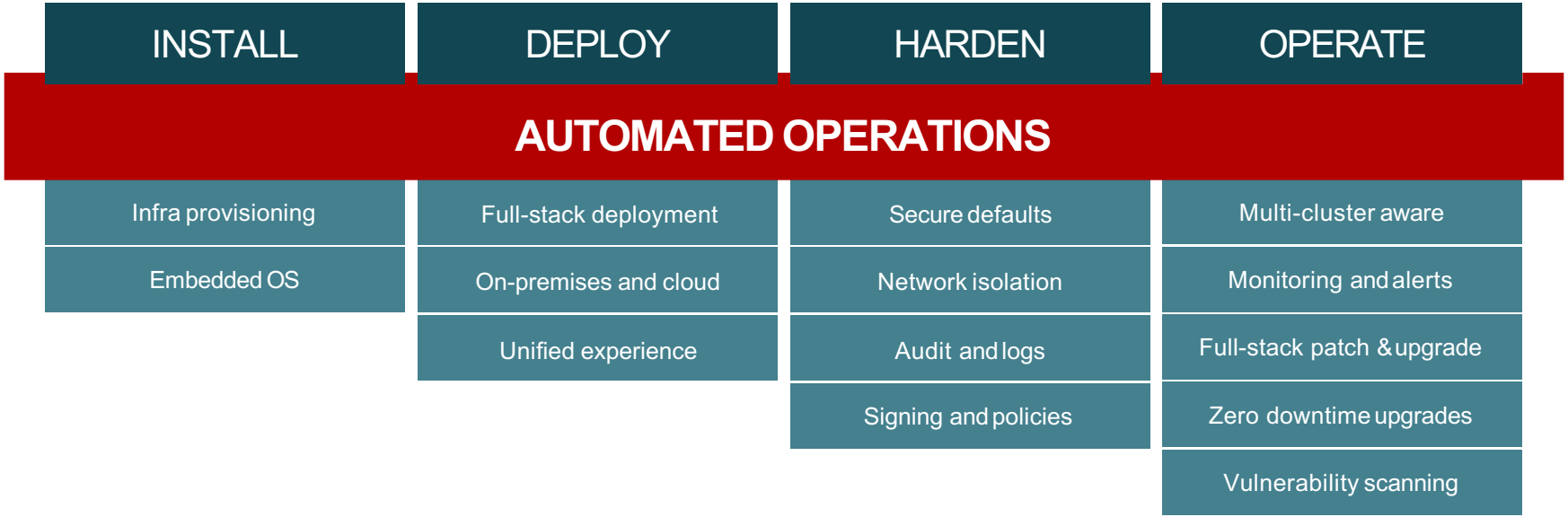


PROVIDER ROADMAP FOR RED HAT OPENSHIFT 4

	Installer Provisioned Infrastructure (IPI)	User Provisioned Infrastructure (UPI)
OPENSHIFT by Red Hat 4.1	amazon web services	amazon web services, vmware vSphere, Baremetal
OPENSHIFT by Red Hat 4.2	Microsoft Azure, RED HAT OPENSTACK PLATFORM, Google Cloud Platform	–
OPENSHIFT by Red Hat 4.3	Alibaba Cloud, IBM Cloud, Baremetal	Microsoft Azure, Google Cloud Platform, RED HAT OPENSTACK PLATFORM, RED HAT VIRTUALIZATION

AUTOMATED CONTAINER OPERATIONS

Fully automated day-1 and day-2 operations



CRI-O Support in OpenShift

CRI-O tracks and versions identical to Kubernetes, simplifying support permutations

CRI-O 1.12 	Kubernetes 1.12 	OpenShift 4.0 
CRI-O 1.13 	Kubernetes 1.13 	OpenShift 4.1 
CRI-O 1.14 	Kubernetes 1.14 	OpenShift 4.2