



# OpenShift Container Platform

Red Hat CoreOS

Hakam Abdelqader



# 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



phillips 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 AtomicAge



## 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.

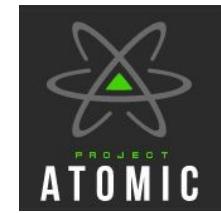
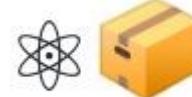
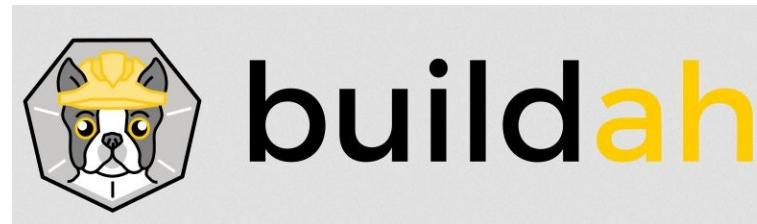
# CoreOS Projects and Tooling

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

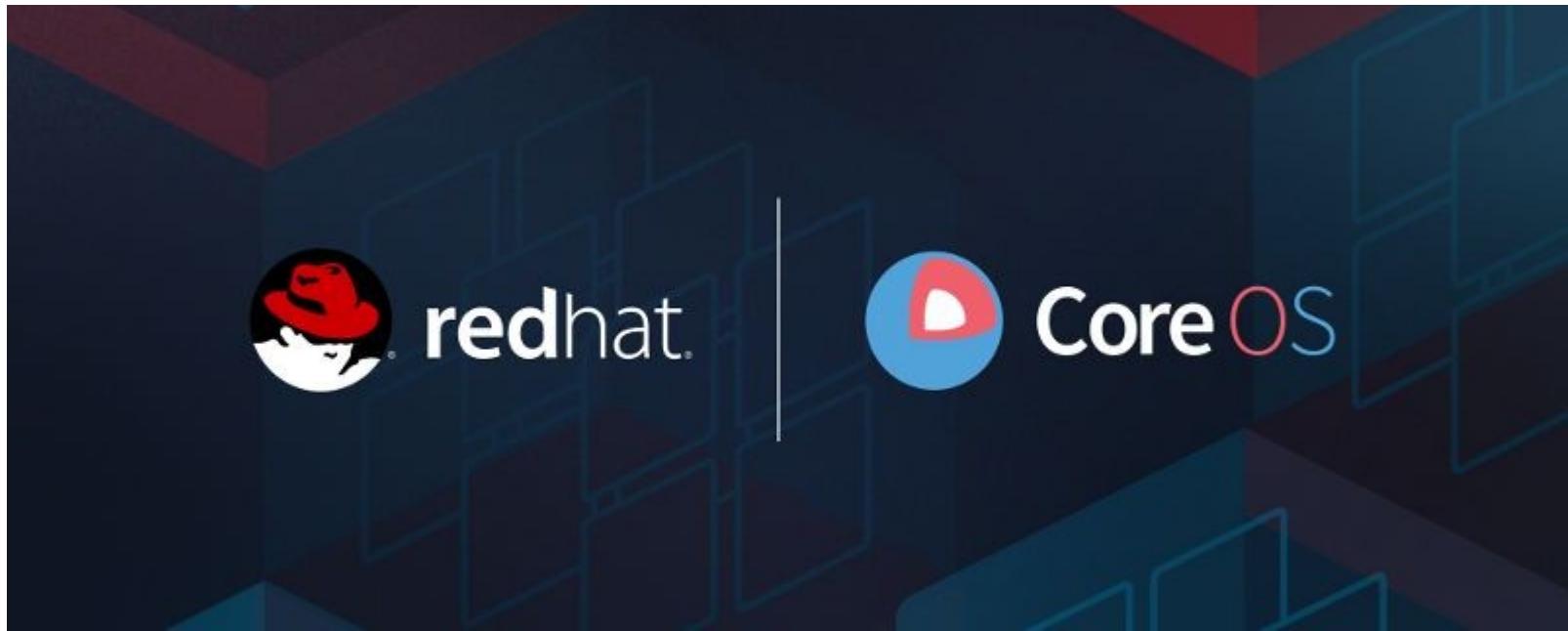


# Project Atomic Projects and Tooling

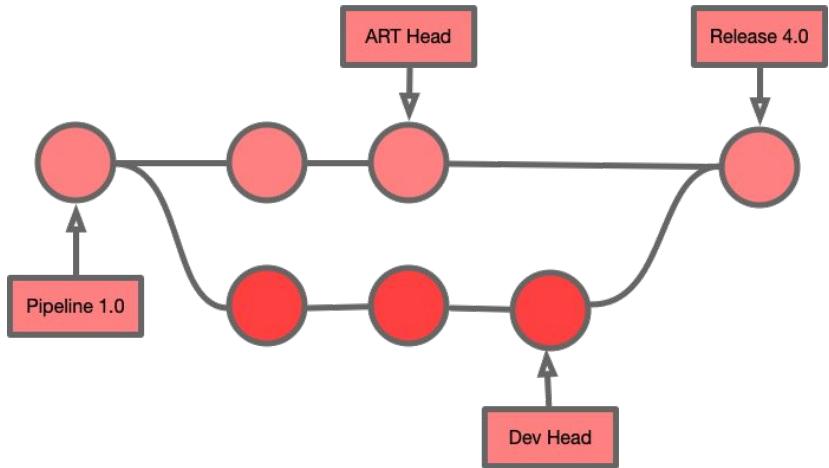
- ostree
- rpm-ostree
- System-containers
- atomic-cli
- buildah
- skopeo
- cri-o
- cockpit
- ... and much much more!



# 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**

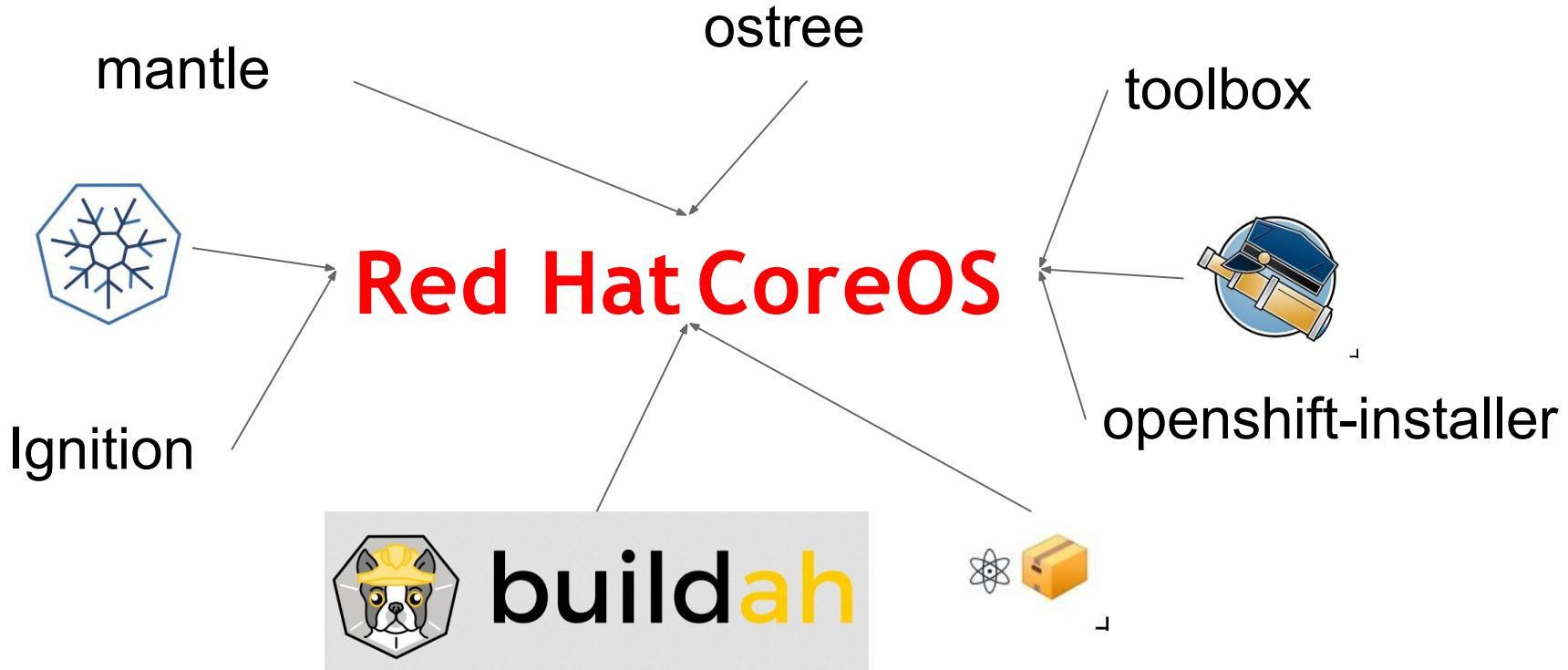
- Support specific tools and use cases

## **Focus on the Cluster**

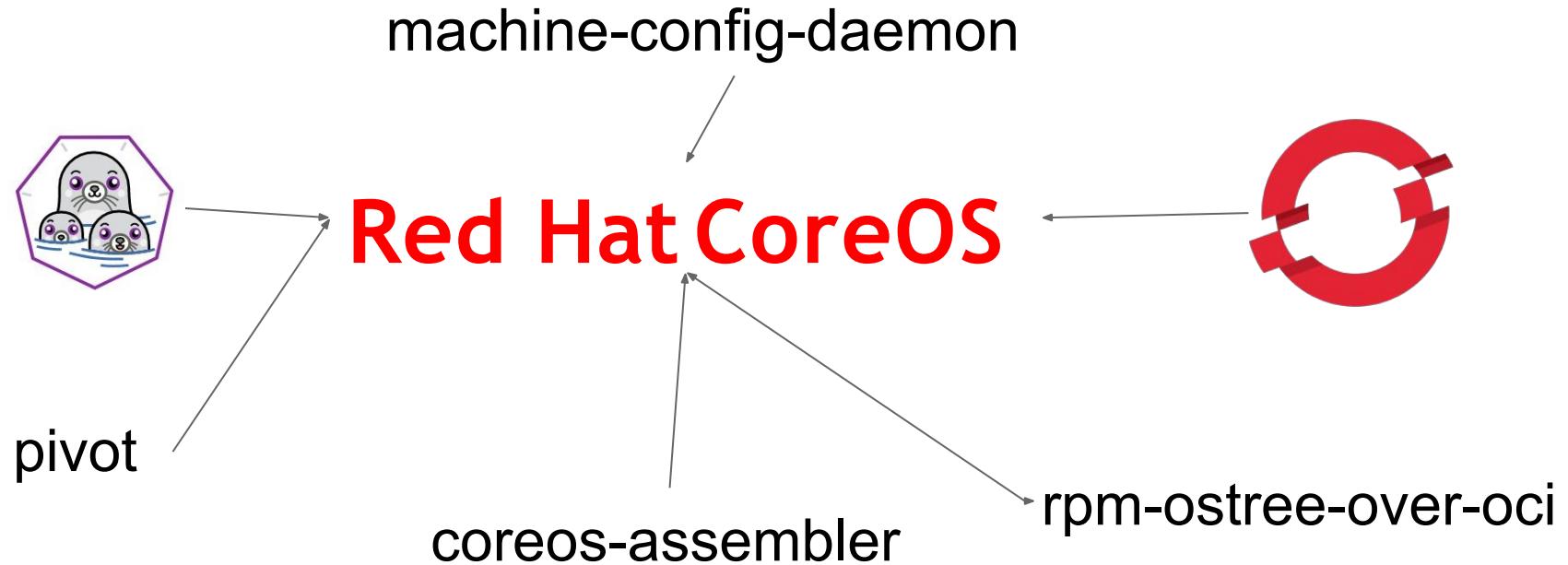
- Embed Openshift packages
- Push management to the cluster



# Combining Forces



And picking up more!

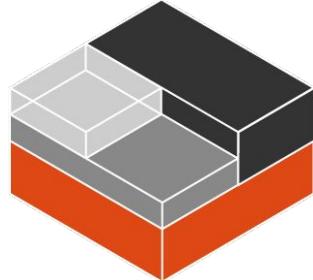


# A Wealth of Operating Systems

Use cases

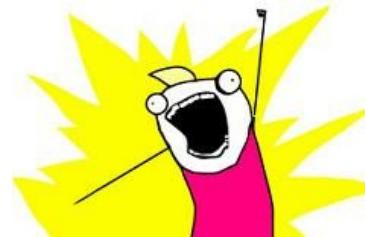
## Container Linux

Designed for general container workloads



## RHEL

Designed for General Use

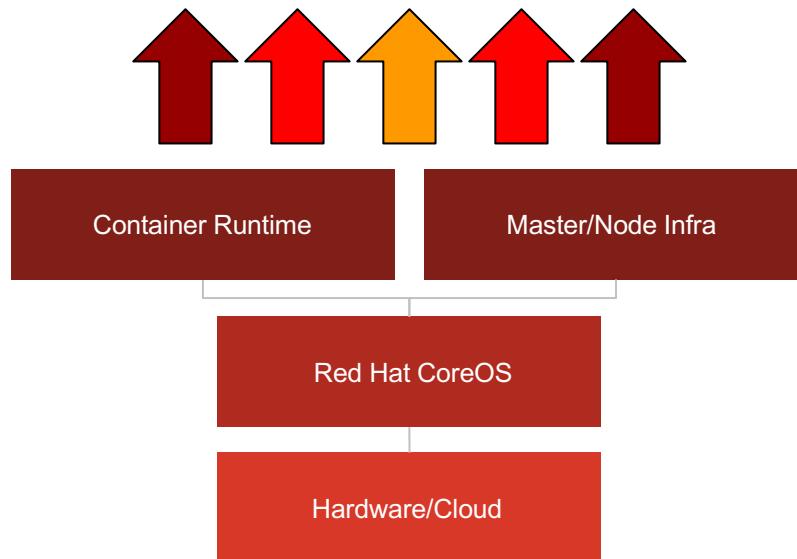


## RHCOS

Designed to power the container scheduler



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



# A Wealth of Operating Systems

## Runtimes

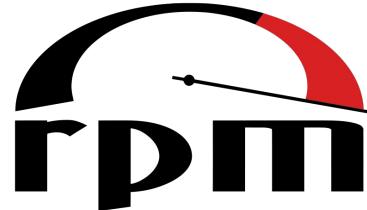
### Container Linux

Provides multiple runtimes



### RHEL

Can install runtimes



### RHCOS

Provides one runtime to satisfy the cluster



# A Wealth of Operating Systems

## Content

### Container Linux

Exploded content on the  
filesystem  
Gentoo Based  
Gentoo Kernel



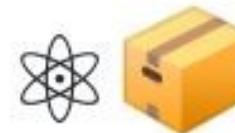
### RHEL

RPMs  
RHEL Content  
RHEL kernel



### RHCOS

RPM-OStree  
RHEL Content(\*)  
RHEL kernel



# A Wealth of Operating Systems

## Update Sources

### Container Linux

Omaha  
Protocol/CoreUpdate



### RHEL

RHEL repos, Satellite



### RHCOS

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



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

[https://commons.wikimedia.org/wiki/File:Downtown\\_Cincinnati\\_viewed\\_from\\_Mt\\_At\\_Adams.jpg](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



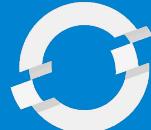
[https://commons.wikimedia.org/wiki/File:Rack\\_Servers\\_Fujitsu\\_Primergy\\_2.jpg](https://commons.wikimedia.org/wiki/File:Rack_Servers_Fujitsu_Primergy_2.jpg)



# FULL STACK AUTOMATED INSTALL

OPENSIFT 3

OPENSIFT PLATFORM



OPERATING SYSTEM



INFRASTRUCTURE

OPENSIFT 4

OPENSIFT PLATFORM



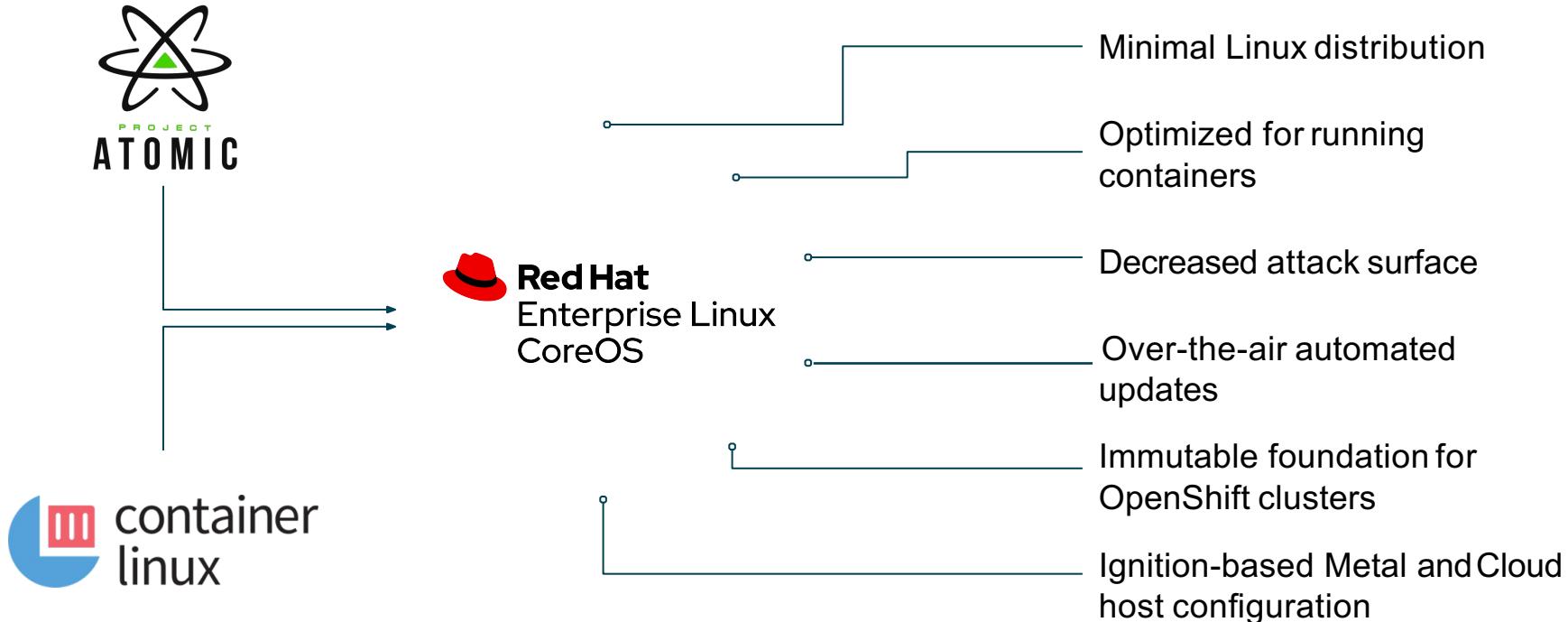
OPERATING SYSTEM



RED HAT®  
ENTERPRISE  
LINUX CoreOS

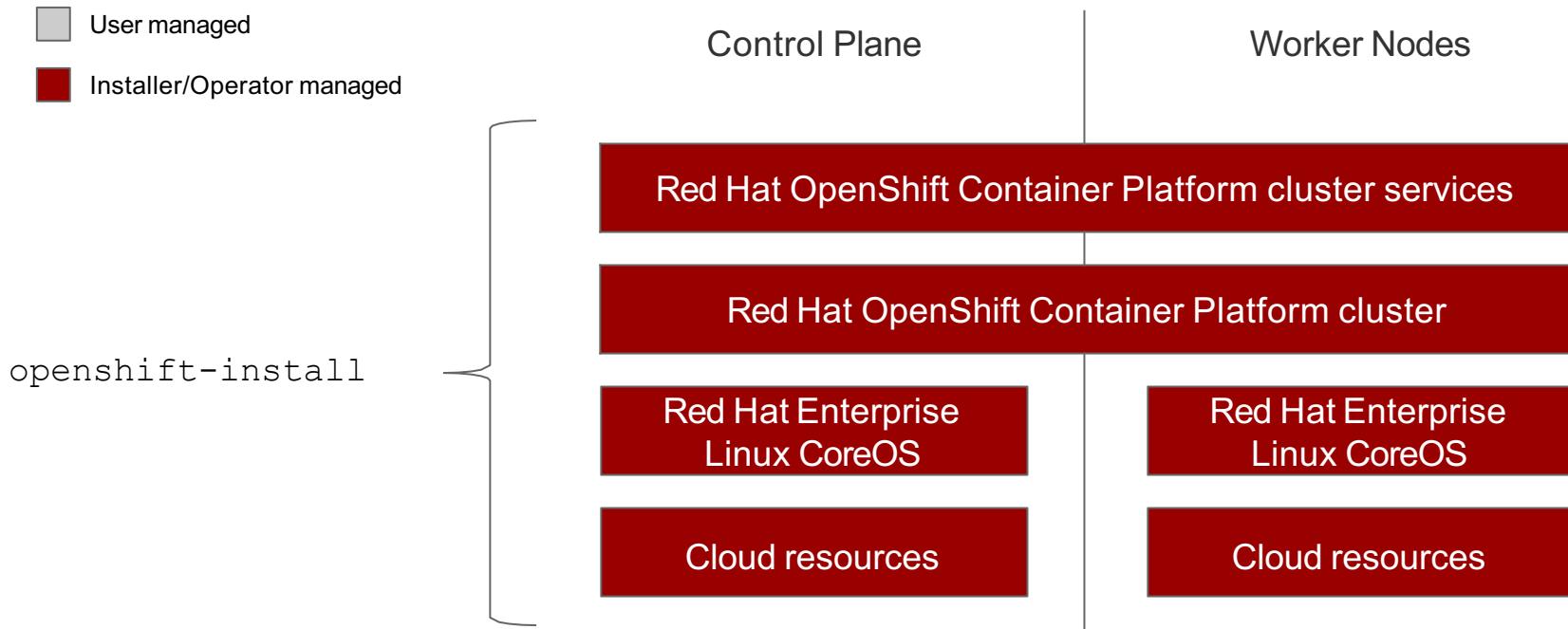


# RHEL COREOS



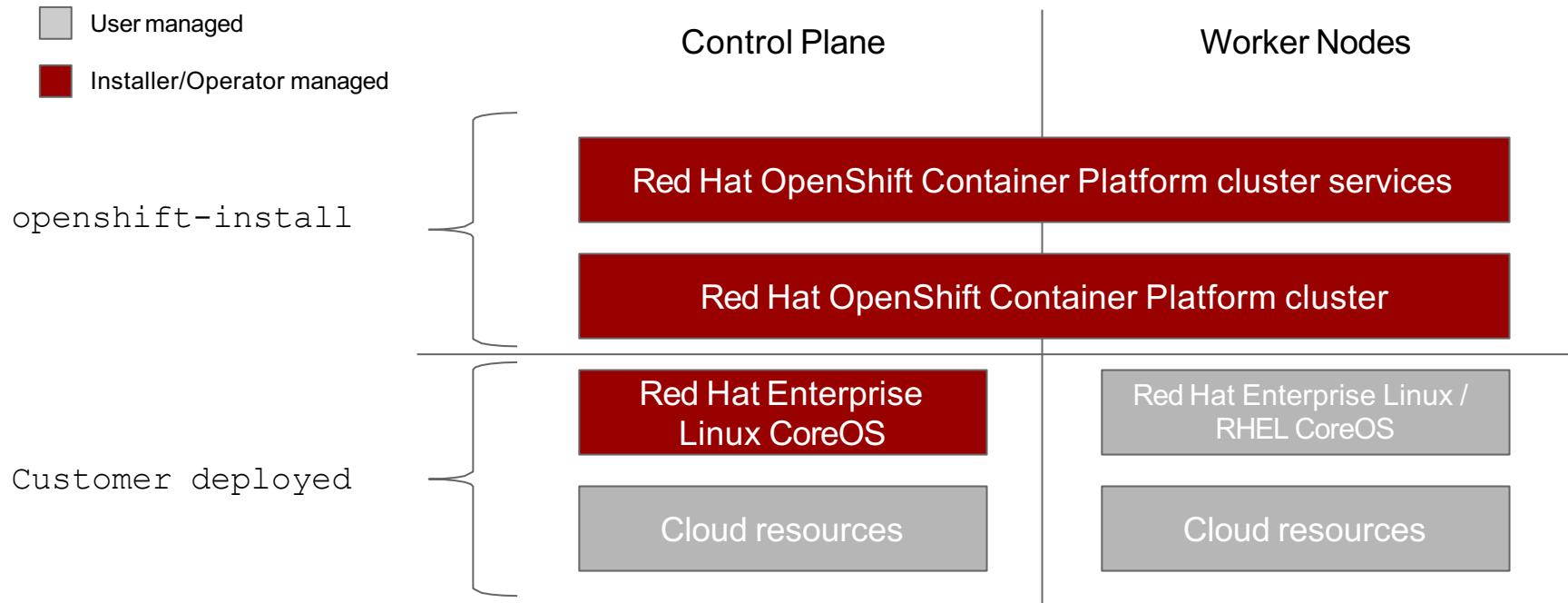
# INSTALLER PROVISIONED INFRASTRUCTURE (IPI)

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

The screenshot shows the Red Hat OpenShift web console interface. The left sidebar is titled "RED HAT OPENSHIFT" and includes navigation links for Workloads, Networking, Storage, Builds, Monitoring, Administration (Cluster Settings, Namespaces, Nodes, Machine Deployments, Machine Sets), and CRDs. The main content area is titled "Machines" and displays a table of machine details. The table columns are NAME, NAMESPACE, REGION, and AVAILABILITY ZONE. The machines listed are:

NAME	NAMESPACE	REGION	AVAILABILITY ZONE
robszumski-0100-master-0	openshift-cluster-api	us-east-2	us-east-2a
robszumski-0100-master-1	openshift-cluster-api	us-east-2	us-east-2b
robszumski-0100-master-2	openshift-cluster-api	us-east-2	us-east-2c
robszumski-0100-worker-us-east-2a-86wfh	openshift-cluster-api	us-east-2	us-east-2a
robszumski-0100-worker-us-east-2b-sp8wx	openshift-cluster-api	us-east-2	us-east-2b
robszumski-0100-worker-us-east-2c-vjflw	openshift-cluster-api	us-east-2	us-east-2c

A "Filter Machines by name..." input field is located at the top right of the table.

The screenshot shows the Red Hat OpenShift web console interface. The left sidebar is titled "RED HAT OPENSHIFT" and includes navigation links for Workloads, Networking, Storage, Builds, Monitoring, Administration (Cluster Settings, Namespaces, Nodes, Machine Deployments, Machine Sets), and CRDs. The main content area is titled "Machine Set Details" and displays the configuration for "robszumski-0100-worker-us-east-2a". The "YAML" tab is selected, showing the YAML representation of the machine set definition. The YAML code is as follows:

```
spec:
  metadata:
    creationTimestamp: null
  providerSpec:
    values:
      userSecret:
        name: worker-user-data
      placement:
        availabilityZone: us-east-2a
      region: us-east-2
      keyName: null
      credentialsSecret: null
      instanceType: M4.large
      metadata:
        creationTimestamp: null
        publicIp: null
      securityGroups:
        - id: null
          kind: AWSMachineProviderConfig
          loadBalancers: null
          tags:
            - name: openshiftClusterID
            - name: robszumski-0100_worker_sg
```

At the bottom of the screen, there are "Save", "Reload", and "Cancel" buttons, and a "Download" button on the far right.



# OVER-THE-AIR UPDATES

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

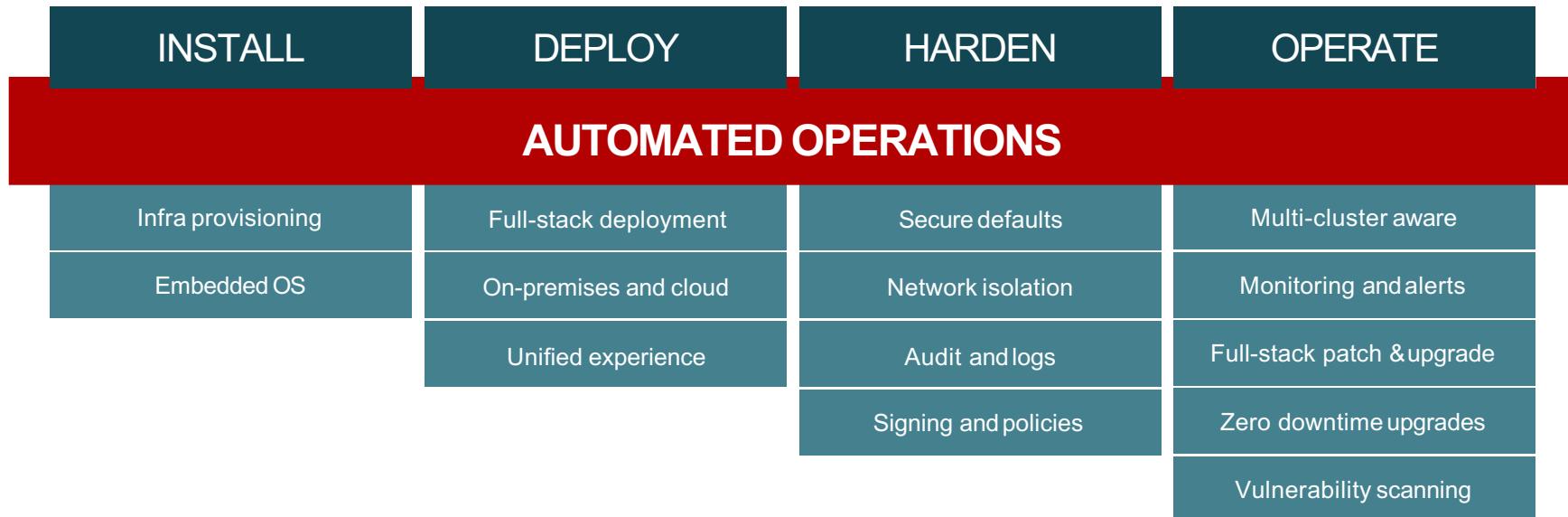
The screenshot shows the Red Hat OpenShift web interface. The left sidebar has a dark theme with white text and includes links for Home, Catalog, Workloads, Networking, Storage, Builds, Monitoring, Administration (with a dropdown menu showing Cluster Settings, Namespaces, and Nodes), and Cluster Settings. The main content area is titled "Cluster Settings" and has tabs for Overview, Global Configuration, and Cluster Operators. The Overview tab is selected. It displays cluster information: CHANNEL fast, UPDATE STATUS 4.1.0-0.2, and CURRENT VERSION 4.0.0-0.2. Below this, it shows the CLUSTER ID (784ce289-02aa-4d32-8796-cd4a0619499c) and CURRENT PAYLOAD (empty). At the bottom right is a blue "Update" button.

# PROVIDER ROADMAP FOR RED HAT OPENSHIFT 4

	Installer Provisioned Infrastructure (IPI)	User Provisioned Infrastructure (UPI)
 <b>OPENSHIFT</b> by Red Hat <b>4.1</b>		  
 <b>OPENSHIFT</b> by Red Hat <b>4.2</b>	 Microsoft Azure  Google Cloud Platform  RED HAT OPENSTACK PLATFORM	
 <b>OPENSHIFT</b> by Red Hat <b>4.3</b>	 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



