What is Red Hat CoreOS?

Jeff Ligon and Steve Milner
2019-26-01
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

@phllips 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
CoreOS Projects and Tooling

- etcd
- Ignition
- mantle
- fleet
- torcx
- rkt
- toolbox
- Flannel
- operators
- … and much much more!
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.
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
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
And this started

4.0
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

- mantle
- ostree
- toolbox
- openshift-installer

Red Hat CoreOS

Ignition
And picking up more!

- machine-config-daemon
- pivot
- coreos-assembler
- rpm-ostree-over-oci
### A Wealth of Operating Systems

**Use cases**

<table>
<thead>
<tr>
<th>Container Linux</th>
<th>RHEL</th>
<th>RHCOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed for general container workloads</td>
<td>Designed for General Use</td>
<td>Designed to power the container scheduler</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Container Linux</th>
<th>RHEL</th>
<th>RHCOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Omaha Protocol/CoreUpdate</td>
<td>RHEL repos, Satellite</td>
<td>MCO/MCD looks for the reference in the release payload found in Cincinnati</td>
</tr>
</tbody>
</table>

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

https://commons.wikimedia.org/wiki/File:Downtown_Cincinnati_viewed_from_Mt_Alt_Adam.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
Simplified Update Flow

Openshift → Machine Config → OSIImageURL → Container Registry → MCD → Red Hat CoreOS

- rpm-ostree
- pivot

→ Reboot
OTA Updates via MCO

http://github.com/openshift/machine-config-operator
OTA Updates via MCO
http://github.com/openshift/machine-config-operator
OTA Updates via MCO

http://github.com/openshift/machine-config-operator
OTA Updates via MCO

http://github.com/openshift/machine-config-operator
Roadmap
Roadmap

Streamline
Roadmap

Community/Tools
Roadmap

Platforms
Some Sources

- rpm-ostree: https://github.com/projectatomic/rpm-ostree/
- ostree: https://github.com/ostreedev/ostree
- pivot: https://github.com/openshift/pivot
- coreos-assembler: https://github.com/coreos/coreos-coreos-assembler
- kola: https://github.com/coreos/mantle/tree/master/kola
- machine-config-daemon: https://github.com/openshift/machine-config-operator/
- ore: https://github.com/coreos/mantle/tree/master/cmd/ore
- os: https://github.com/openshift/os/
Questions?

Jeff Ligon: https://twitter.com/jeffro_ligon
Steve Milner: https://twitter.com/ashcrow