Red Hat OpenShift

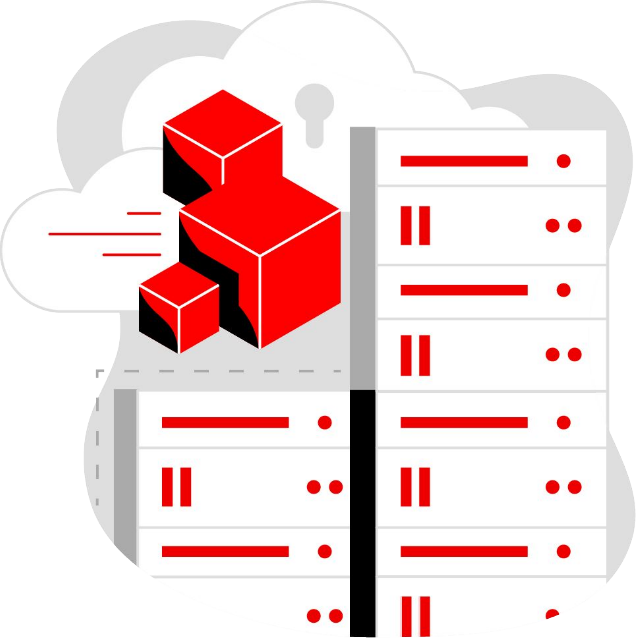
Booting Containers with CoreOS Layering

Colin Walters
Software Engineering

Zack Zlotnik
Software Engineering

Mark Russell
Product Management

We’re on a journey - with you

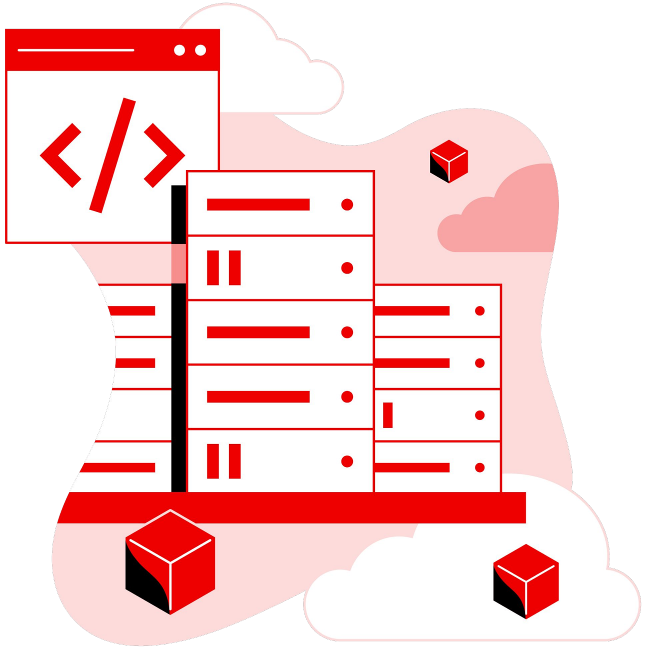


OpenShift 3 to OpenShift 4 was a major leap

- Opinionated openshift-install
- Cluster version operator, second level operators
- RHEL CoreOS - ignition (works across cloud and metal!), API-managed, image-based & purpose built
- Upgrades and configuration through Machine Config Operator

Evolving RHEL CoreOS

Available today in OCP 4.13



Enabling customization and simpler configuration management in OpenShift 4.13+

- Install 3rd party add-ons including kernel drivers
- Install additional RHEL content
- Simpler configuration file management (optional)
- MachineConfig API is preserved
- Currently Day-2 only

What is CoreOS Layering?

Container images, everywhere

CoreOS Layering is a technology that puts the OS root filesystem in a standard OCI container image.

- Resulting container images are a transport format for updating the operating system root filesystem.
- Container image contents are written to a standard {xfs,ext4} filesystem, ostree used in the background to manage kernel/bootloader
- Anything built to use standard container images suddenly now interoperates with CoreOS images

Photo by Valdas Miskinis
https://pixabay.com/photos/container-storage-trade-haulage-4203677/

Fedora CoreOS example

Single host customization

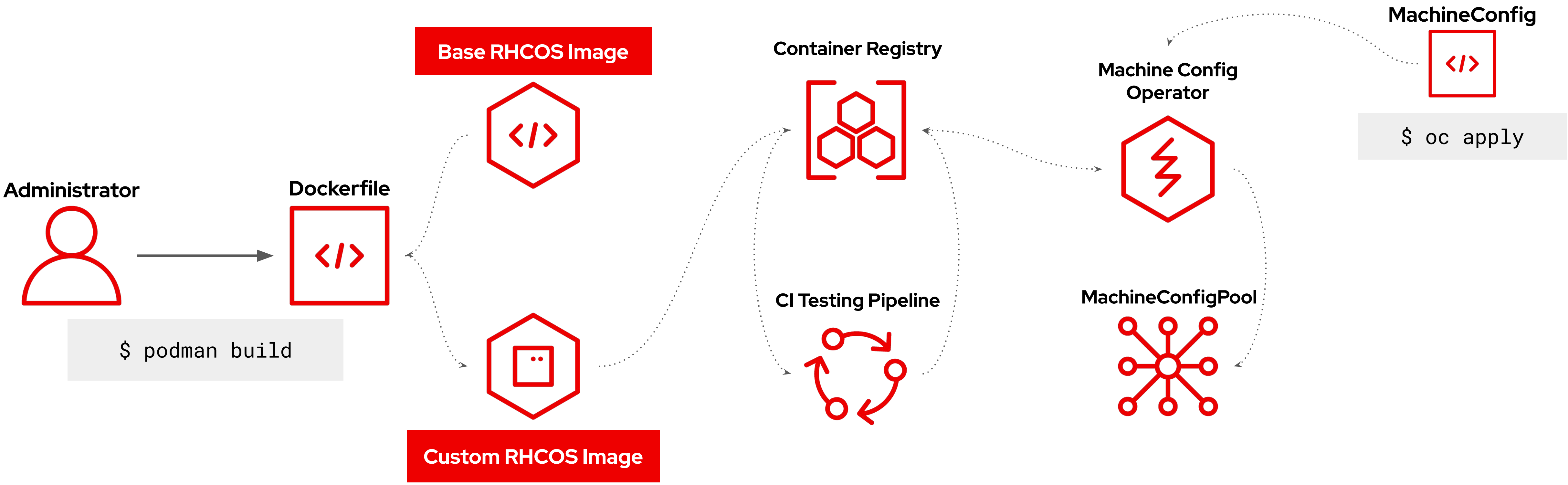
```
FROM quay.io/fedora/fedora-coreos:stable
ADD configure-firewall-playbook.yml .
RUN rpm-ostree install firewalld ansible && \
    ansible-playbook -vvv configure-firewall-playbook.yml && \
    rpm -e ansible && \
    rpm-ostree cleanup -m && \
    ostree container commit
```

Source:
https://github.com/coreos/layering-examples/blob/main/ansible-firewalld/Containerfile

GA in 4.13

Off-cluster Builds

Build, Test, Deploy



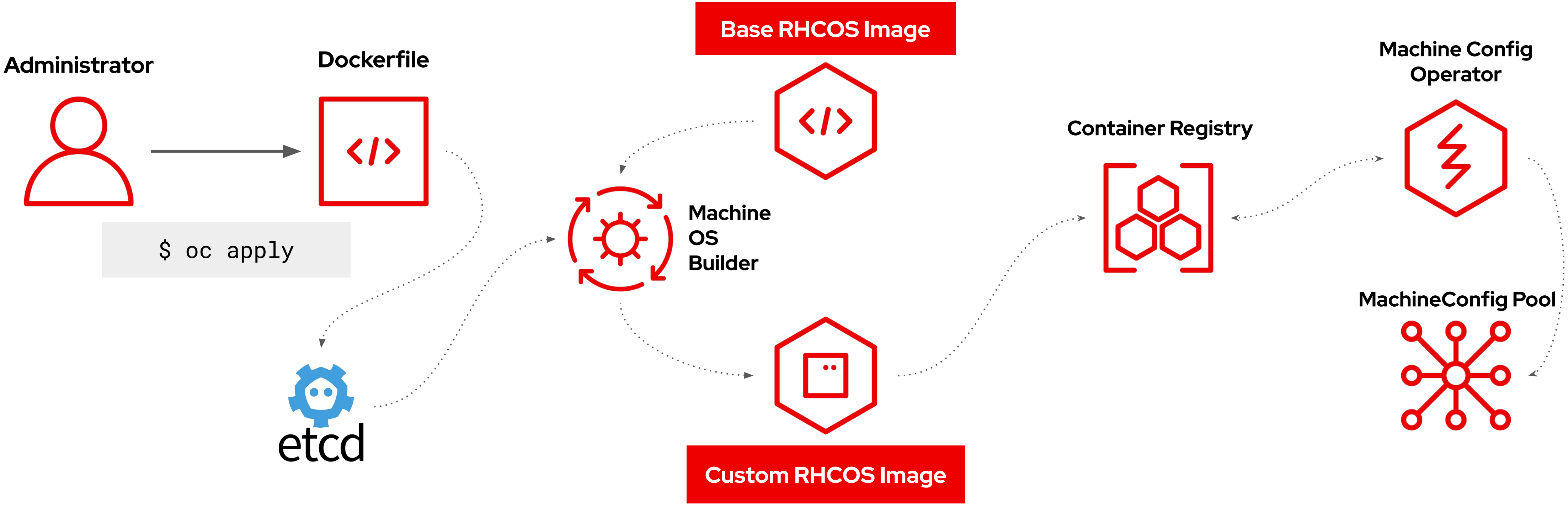
```
$ podman build
```

```
$ oc apply
```

Dev Preview in 4.14

On-cluster Builds

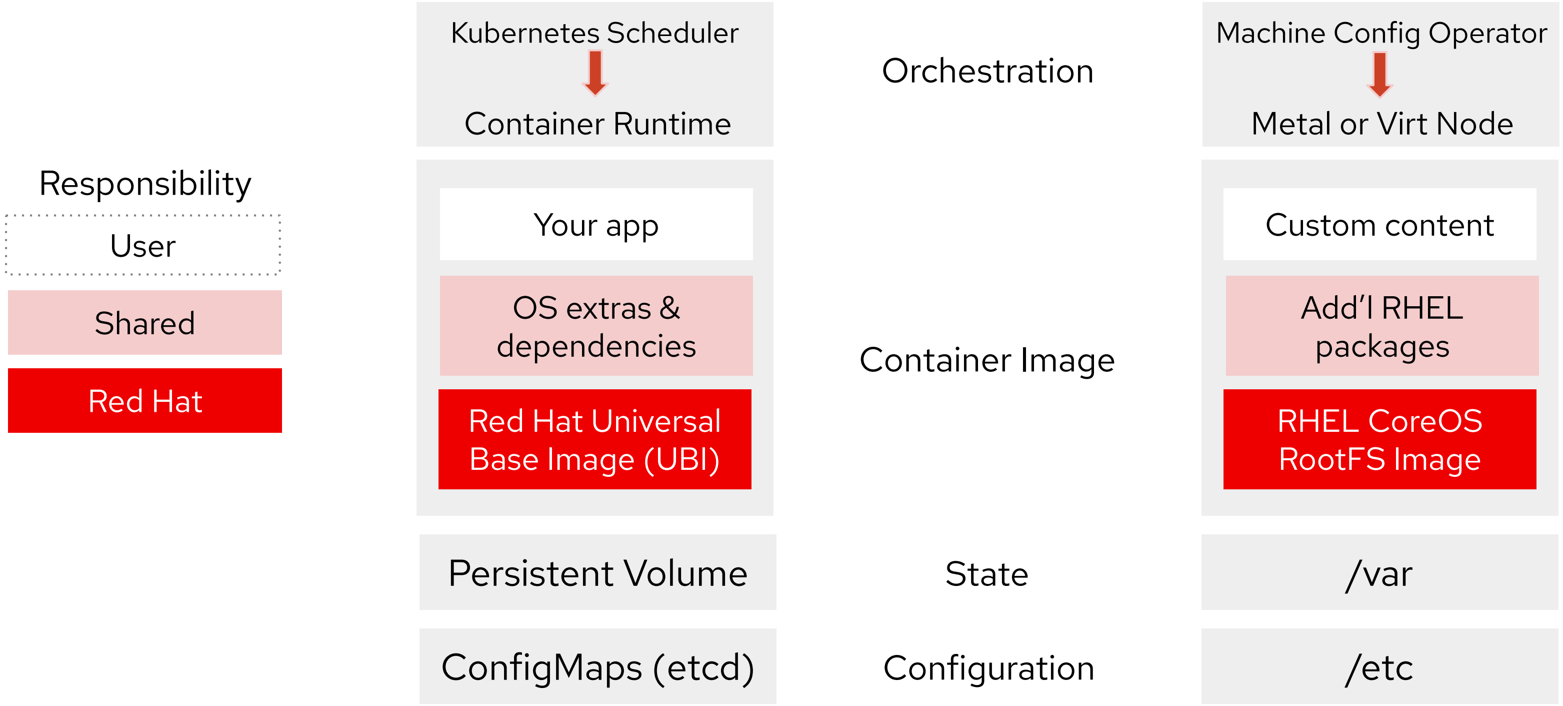
Make it so!



```
$ oc apply
```

Red Hat

A common model for apps and operating systems



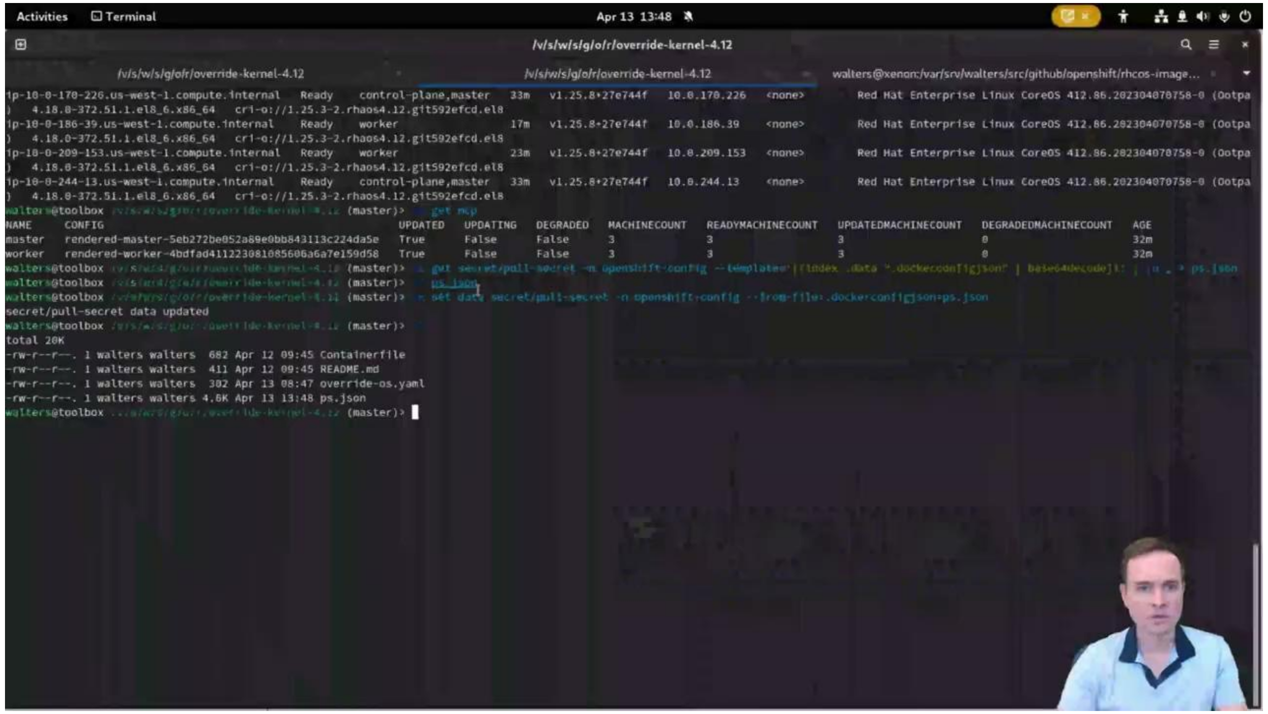
Responsibility

- User
- Shared
- Red Hat

Kubernetes Scheduler ↓ Container Runtime	Orchestration	Machine Config Operator ↓ Metal or Virt Node
Your app OS extras & dependencies Red Hat Universal Base Image (UBI)	Container Image	Custom content Add’l RHEL packages RHEL CoreOS RootFS Image
Persistent Volume	State	/var
ConfigMaps (etcd)	Configuration	/etc

https://access.redhat.com/third-party-software-support

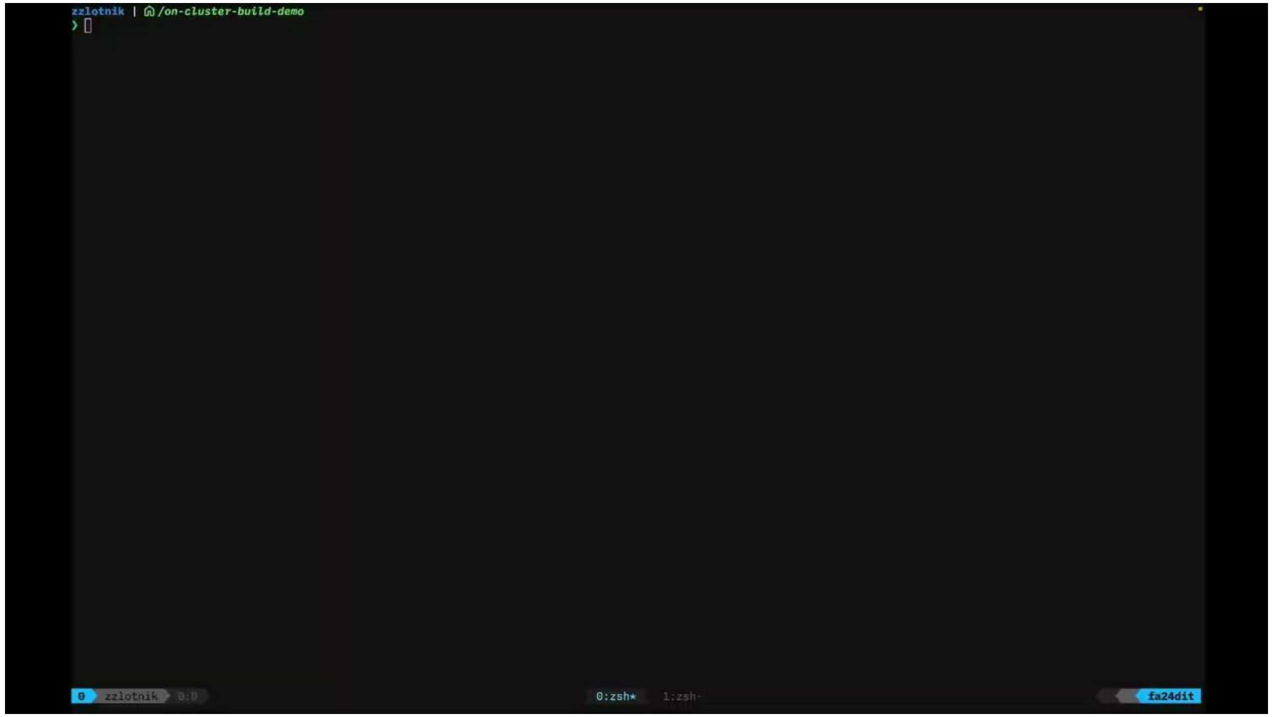
Demo 1



Activities
Terminal
Apr 13 13:48
/v/s/w/s/g/o/r/override-kernel-4.12
/v/s/w/s/g/o/r/override-kernel-4.12
/v/s/w/s/g/o/r/override-kernel-4.12
walters@xenon:/var/srv/walters/src/github/openshift/rhcos-image...

```
ip-10-0-170-226.us-west-1.compute.internal   Ready    control-plane,master   33m   v1.25.8+27e744f   10.0.170.226   <none>        Red Hat Enterprise Linux CoreOS 412.86.202304070758-0 (Ootpa
)   4.18.0-372.51.1.el8_6.x86_64   cri-o://1.25.3-2.rhaos4.12.git592efcd.el8
ip-10-0-186-39.us-west-1.compute.internal    Ready    worker                 17m   v1.25.8+27e744f   10.0.186.39    <none>        Red Hat Enterprise Linux CoreOS 412.86.202304070758-0 (Ootpa
)   4.18.0-372.51.1.el8_6.x86_64   cri-o://1.25.3-2.rhaos4.12.git592efcd.el8
ip-10-0-209-153.us-west-1.compute.internal   Ready    worker                 23m   v1.25.8+27e744f   10.0.209.153   <none>        Red Hat Enterprise Linux CoreOS 412.86.202304070758-0 (Ootpa
)   4.18.0-372.51.1.el8_6.x86_64   cri-o://1.25.3-2.rhaos4.12.git592efcd.el8
ip-10-0-244-13.us-west-1.compute.internal    Ready    control-plane,master   33m   v1.25.8+27e744f   10.0.244.13    <none>        Red Hat Enterprise Linux CoreOS 412.86.202304070758-0 (Ootpa
)   4.18.0-372.51.1.el8_6.x86_64   cri-o://1.25.3-2.rhaos4.12.git592efcd.el8
walters@toolbox /v/s/w/s/g/o/r/override-kernel-4.12 (master)> oc get mcp
NAME     CONFIG                                             UPDATED   UPDATING   DEGRADED   MACHINECOUNT   READYMACHINECOUNT   UPDATEDMACHINECOUNT   DEGRADEDMACHINECOUNT   AGE
master   rendered-master-5eb272be052a89e0bb843113c224da5e   True      False      False      3              3                   3                     0                      32m
worker   rendered-worker-4bdfad411223081085606a6a7e159d58   True      False      False      3              3                   3                     0                      32m
walters@toolbox /v/s/w/s/g/o/r/override-kernel-4.12 (master)> oc get secret/pull-secret -n openshift-config --template='{{index .data ".dockerconfigjson" | base64decode}}' | jq . > ps.json
walters@toolbox /v/s/w/s/g/o/r/override-kernel-4.12 (master)> e ps.json
walters@toolbox /v/s/w/s/g/o/r/override-kernel-4.12 (master)> oc set data secret/pull-secret -n openshift-config --from-file=.dockerconfigjson=ps.json
secret/pull-secret data updated
walters@toolbox /v/s/w/s/g/o/r/override-kernel-4.12 (master)> l
total 20K
-rw-r--r--. 1 walters walters  682 Apr 12 09:45 Containerfile
-rw-r--r--. 1 walters walters  411 Apr 12 09:45 README.md
-rw-r--r--. 1 walters walters  302 Apr 13 08:47 override-os.yaml
-rw-r--r--. 1 walters walters 4.8K Apr 13 13:48 ps.json
walters@toolbox .../w/s/g/o/r/override-kernel-4.12 (master)> 
```

Demo 2



```
zzlotnik | /on-cluster-build-demo
❯ 
```

```
0  zzlotnik  0:0                      0:zsh*   1:zsh-                      fa24dit
```

Off-cluster vs. On-cluster

Manage the pipeline OR let OpenShift do it for you

Off-cluster building is great for

✓ Production support today

✓ Taking ownership & responsibility for OS updates

✓ Creating custom test pipelines

✓ Centralizing image builds for many clusters

✓ Integrating with an existing CI/CD and build systems

Machine OS Builder is great for

✓ Easy, automatic builds

✓ Ensuring that OpenShift upgrades automatically merge with your custom content

✓ Temporary requirements, e.g. a test or hotfix package

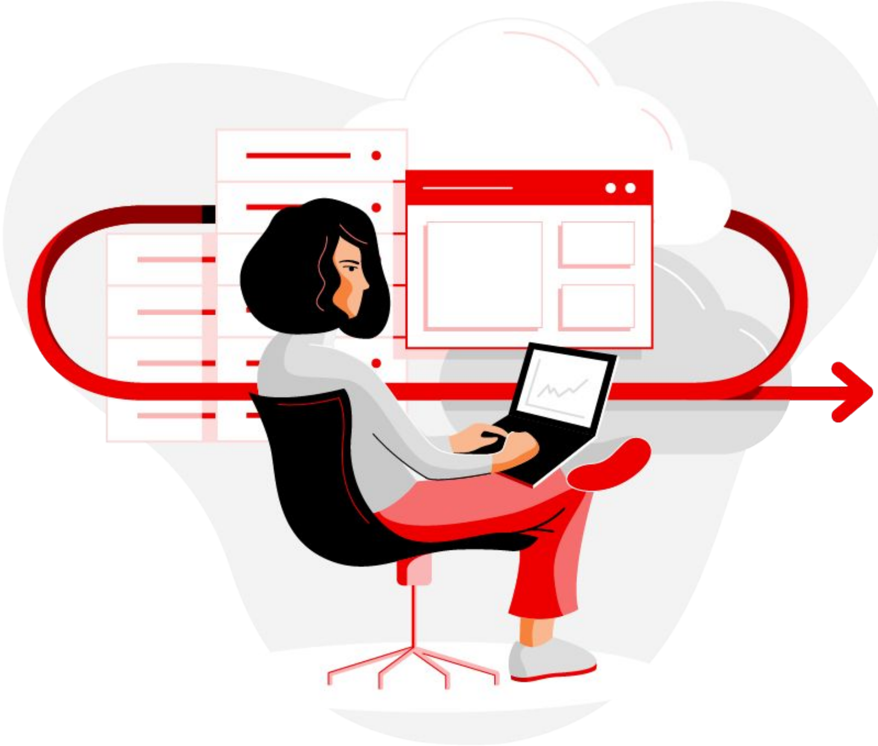
Important notes!

- Enabling off-cluster builds means taking **responsibility** for OS image updates
- Staying up to date is a virtue
- Standard Red Hat support policies apply for third party add-ons
- Currently Day-2 **only**

https://access.redhat.com/third-party-software-support
https://docs.openshift.com/container-platform/4.13/post_installation_configuration/coreos-layering.html

What's next?

More flexibility, less toil



Development priorities:

- Day-0 custom install media for new machines
- Machine OS Builder service to GA
- Console integration
- What do you think? Declarative interfaces?
- What enhancements would you like to see for for on-cluster builds?

Red Hat
Enterprise Linux
CoreOS

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

- linkedin.com/company/red-hat
- youtube.com/OpenShift
- facebook.com/redhatinc
- twitter.com/OpenShift