



FOREMAN

Katello

Bootable Containers

& other container features

Ian Ballou

GitHub: [ianballou](#)

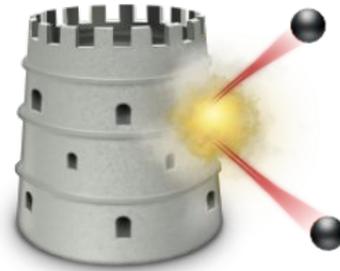
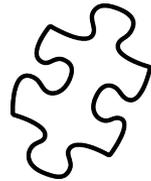
Matrix: [iballou](#)



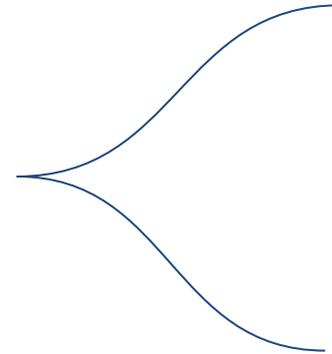
The Stack



Foreman



Katello



Candlepin



Pulp



Foreman



Provisioning



Configuration



Monitoring



New Container Features

- OCI Flatpaks
- Bootable containers
 - Host registration
 - Booted container overview
 - Transient installation support
 - Transient package tracking *
- New container images UI
- Load balanced container content via smart proxies

* pending [subscription-manager adoption](#)



Bootable Containers?

- Container images used to provision and update OSTree-based immutable machines
- Built to work with bootc



bootc



Bootable Containers?

“The [bootc documentation](#) summarizes bootable containers as "transactional, in-place operating system updates using OCI/Docker container images". In other words, updates to the operating system (OS) are shipped by using container images. That implies that the Linux kernel, the bootloader, drivers, etc. are all part of the container image which renders the container image "bootable".”

- <https://docs.fedoraproject.org/en-US/bootc/getting-started/>



Bootable Containers

“Bootc container images differ technically from application containers in two important ways:

- bootc images use OSTree inside the container
- A bootc image has a kernel and enough other packages to boot a physical or virtual machine.”

- <https://www.redhat.com/en/blog/image-mode-red-hat-enterprise-linux-quick-start-guide>



Some bootc Facts



- bootc is the interface for managing bootable containers
- bootc install - provisions container to disk
 - Anaconda & other tools automate this
- bootc upgrade - pull new content with existing tag
 - Auto-updates by default
- bootc switch - switch to a different bootc container image
- bootc rollback - go back to the last image
- Install RPMs via ``dnf --transient ...``
 - If you dare! They will be gone at reboot.



Bootable Containers in Foreman

- bootc data now in Foreman inventory
 - bootc facts uploaded via subscription-manager
- Overview of all booted container images
- Transient package installation support

Image mode details 	
Modify via remote execution	
Running image	quay.io/centos-bootc/centos-bootc:stream10
Running image digest	sha256:54256a998f0c62e16f3927c82b570f90bd8449a52e03daabd5fd16d6419fd572
Staged image	—
Staged image digest	—
Available image	—
Available image digest	—
Rollback image	quay.io/centos-bootc/centos-bootc:stream10
Rollback image digest	sha256:9ed49e9b189f5dae5a01ea9abdcef0884616300b565d32061aea619f2e916be3



Booted containers overview



FOREMAN



Booted container images

<input type="text" value="Search"/>	<input type="button" value="→"/>	<input type="button" value="🔖"/>	<input type="button" value="▼"/>	1 - 2 of 2	<input type="button" value="←"/>	<input type="button" value="→"/>
Image name ↑	Image digests	Hosts				
▼ quay.io/centos-bootc/centos-bootc:stream10	3	4				
	Image digest	Hosts				
	sha256:54256a998f0c62e16f3927c82b570f90bd8449a52e03daabd5fd16d6419fd572	1				
	sha256:54256a998f0c62e16f3927c82b570f90bd8449a52e03daabd5fd16d6419fd573	2				
	sha256:54256a998f0c62e16f3927c82b570f90bd8449a52e03daabd5fd16d6419fd574	1				
▶ quay.io/centos-bootc/centos-bootc:stream9	1	1				



Transient RPM Package Tracking

- Pass DNF transience via subscription-manager profile
- Copy RUN install command from transient packages
- Future ideas TBD

Copy ContainerFile command

Copy the command below and add it to your Containerfile to incorporate **5** selected packages in your next image. This will ensure packages are installed permanently.

```
> RUN install \ mysql-connector-python \ pino-logger...
```

Copy

Cancel



Transient RPM Package Tracking

Package name ↓	Persistence ↑ ⓘ	Status ↓	Installed version ↓	Upgradable to
<input type="checkbox"/> 389-ds-base	Persistent	↑ Upgradable	32:9.11.4-19.P2.el7_8.2.x86_64	42:9.11.4-19.P2.el7_8.2.x86_64
<input type="checkbox"/> 389-ds-base-libs	Transient	✓ Up-to-date	32:9.11.4-19.P2.el7_8.2.x86_64	-
<input type="checkbox"/> abrt	Transient	✓ Up-to-date	32:9.11.4-19.P2.el8_8.2.x86_64	-
<input type="checkbox"/> abrt-addon-vmcore	Persistent	↑ Upgradable	0.301-4.el9.noarch	0.301-4.el10.noarch
<input type="checkbox"/> bash	Persistent	↑ Upgradable	5.1.8-5.el9.x86_64	5.1.8-9.el9.x86_64
<input type="checkbox"/> bzip2	Transient	✓ Up-to-date	1.0.8-8.el9.x86_64	-
<input type="checkbox"/> c-ares	Transient	✓ Up-to-date	1.17.1-5.el9.x86_64	-
<input type="checkbox"/> dbus	Persistent	↑ Upgradable	1.12.20-6.el9.x86_64	dbus-1.12.20-9.el9.x86_64
<input type="checkbox"/> device-mapper	Transient	✓ Up-to-date	1.02.185-3.el9.x86_64	-
<input type="checkbox"/> device-mapper-event	Persistent	↑ Upgradable	1.02.185-3.el9.x86_64	1.02.185-9.el9.x86_64



Provisioning bootable containers

Options

1. Rely on Anaconda's ostreecontainer kickstart command
2. Create a disk image from a bootc container image via [bootc-image-builder](#)



Kickstart solution



Image provisioning

- Create a [kickstart script](#) with `ostreecontainer`
- Assign bootc container via host parameters with variable in KS script
- Populate `kickstart_kernel_cus` `tom_options` with `inst.stage2`



Network provisioning

- Create a [kickstart script](#) with `ostreecontainer`
- Assign bootc container via host parameters with variable in KS script
- Populate `kickstart_kernel_cus` `tom_options` with `inst.stage2`



Kickstart solution



Image provisioning

- Associate KS script with operating system
- Use mkksiso to point image installation media at bootc kickstart script
- `"inst.ks.sendmac
inst.ks=http://katello.com/unattended/provision"`



Network provisioning

- Associate KS script with operating system
- Provision host following normal Foreman network provisioning documentation



Kickstart solution



Image provisioning

- Associate image with a compute resource via hypervisor
- Provision the host following normal Foreman image provisioning documentation



Network provisioning

- ...



Future feature proposals



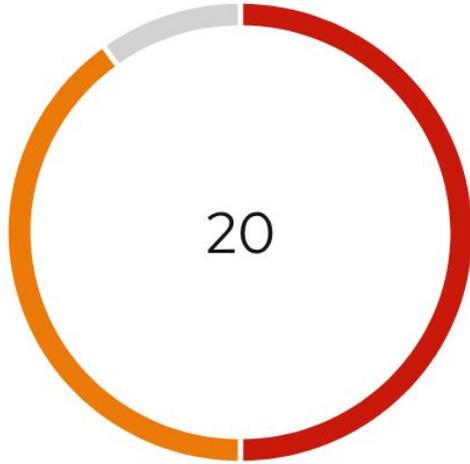
Improved bootc Machine Provisioning



- Provisioning templates
 - Kickstart - `ostreecontainer` host parameter
 - Bootloader config - `inst.stage2`
 - Since `url` isn't supported with `ostreecontainer`
- Associating a host to a container image
 - API support for assigning container image
 - Host creation UI image selector
 - With auto-fill for synced bootc images?



Container vulnerability tracking



Quay Security Reporting has detected 20 vulnerabilities

Patches are available for 20 vulnerabilities

Advisories

 Only show fixable

1 - 20 of 20

1 of 1

Advisory	Severity	Package	Current Ver...	Fixed in V...
> GHSA-38jv-5279-wg99	High	urllib3	1.26.5	→ 2.6.3
> GHSA-gm62-xv2j-4w53	High	urllib3	1.26.5	→ 2.6.0



Container vulnerability tracking

- Katello should not rely on upstream reporting
 - Only works when syncing, not pushing
- Idea: use Quay's [Clair](#) ?
 - Scans [vulnerability databases](#) like [OSV](#) and distributor DBs e.g. Debian & Red Hat.
 - Webhooks on DB updates
 - Returns vulnerabilities per container manifest



Container vulnerability tracking



- Clair & Katello continued
 - Clair needs manifests on disk - no 'on demand'
 - Vulnerability data on request?
 - Or computed asynchronously?
 - Deployment model
 - Ideally containerized
 - Communication through smart proxy?
 - "Smart proxies connect Foreman to services"



Demo



Other container features



New Container UI

Container images ?

 Synced  Booted

Labels and annotations

View labels and annotations for image
sha256:35cb6558e3105826f52e1279db8428aa8bedb117405a7ecca83e389506687eb5.

14 labels and annotations

- redhat.id=centos
- ostree.linux=5.14.0-476.el9.x86_64
- ostree.commit=fb33c150d27bc2148d9296b06788016ff5a33feae3e772f1482b4c5ae83f4b44
- ostree.bootable=true
- containers.bootc=1
- redhat.compose-id=CentOS-Stream-9-20240710.0
- redhat.version-id=9
- io.buildah.version=1.29.1
- ostree.final-diffid=sha256:12787d84fa137cd5649a9005efe98ec9d05ea46245fdc50aeb7dd007f2035b1
- rpmmtree.inpuhash=af728b5f18e55be3c5ab9ed5a8bd463f5149d20272e2f9b1a41ec9ee8ba3e954

Show 4 more

Close

Q Search



1 - 20 of 9541



Tag ↑	Manifest digest	Type	Product	Labels Annotations
> uclibc	sha256:44ed92a03339544d9c16da4c8d10354d8e6f7958168f40eeaae1e15a332bbda3	List	Buttermilk Biscuits	N/A
▼ stream9-1720594390	sha256:0beb3d9e1760c44bfa7bbfd43c91ef53e84c62db3d37a397a05a997b9b294c7b	List	Buttermilk Biscuits	See child manifests
	sha256:35cb6558e3105826f52e1279db8428aa8bedb117405a7ecca83e389506687eb5	Bootable		View here
	sha256:2e2295283f13417c4ab997baa786e46554fbcf2f4451eda4f81fdd97830e27b6	Bootable		View here
> stream9-1720472304	sha256:e9d2dc79768fab8839eaecee47d6c99eb9d4ae8e88747394759edfdfe42fb6c7	List	Buttermilk Biscuits	See child manifests



sha256:35cb6558e310

Name

stream9-1720594390

Creation

October 16, 2025 at 04:16 PM

Repositories

[centos-bootc](#)

Modified

October 16, 2025 at 04:16 PM

Digest

sha256:35cb6558e3105826f52e1279db8428aa8bedb117405a
7ecca83e389506687eb5 

Type

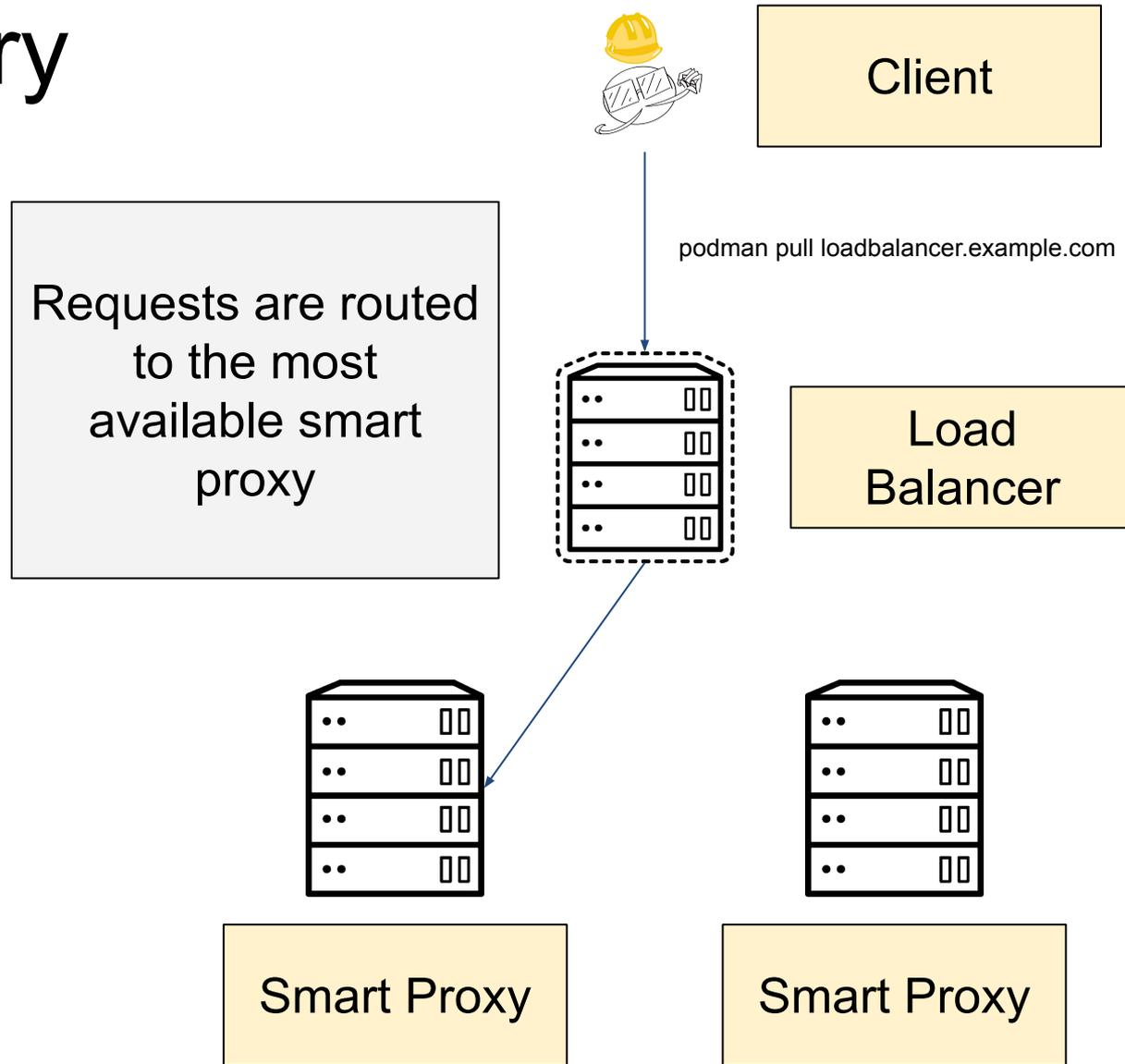
Bootable

▼ Content views, lifecycle environments, pullable paths

Environment 	Content view 	Repository 	Pullable path 
Library	 Default Organization View 1.0	centos-bootc	centos9-katello-devel-2.porcino.example.com/default_organization/buttermilk_biscuits/centos-bootc:stream9-1720594390 
Library	 Component 124.0	centos-bootc	centos9-katello-devel-2.porcino.example.com/default_organization/library/component_1/buttermilk_biscuits/centos-bootc:stream9-1720594390 



Load-Balanced Registry



LB Details

- Container content requests to smart proxies have redirects:
 - Client contacts Container Gateway
 - Container Gateway contacts Pulp
 - Pulp returns the content's **location**
 - Container Gateway redirects the client to that location
- Previously, the **location** tied redirects to one Pulp
- Now, the **location** is swapped out for the LB



OCI Flatpaks

- Upstream remote scanning
- Create repositories from Flatpaks scanned upstream
- Host-specific index proxies
- Certificate authentication

Create Flatpak Remote ✕

Add Red Hat Flatpak remote ✕

To continue with Red Hat Flatpak remote, you need to generate your username and password in access.redhat.com/terms-based-registry/

[Add Red Hat flatpak remote](#) [Generate username and password](#) 

Name *

URL *

Username

Provide credentials if the registry requires authentication

Password



OCI Flatpaks

Flatpak remotes > Fedora

Fedora

Scan

URL: <https://registry.fedoraproject.org>

Remote repositories

This is a list of scanned flatpaks. Mirroring a scanned flatpak creates a repository in the product of your choice. Sync the repository after mirroring it from this remote to distribute its content.

Name ↑	ID ↓	Application name	Last mirrored	Mirror
Oad	1	com.playOad.zeroad	✔ about 1 month ago	Mirror
abiword	2	com.abisource.AbiWord	Never	Mirror
adw-gtk3-theme	3	org.fedoraproject.Gtk3theme.adw	Never	Mirror





FOREMAN

Thanks!

<https://theforeman.org>

<https://github.com/Katello/katello>