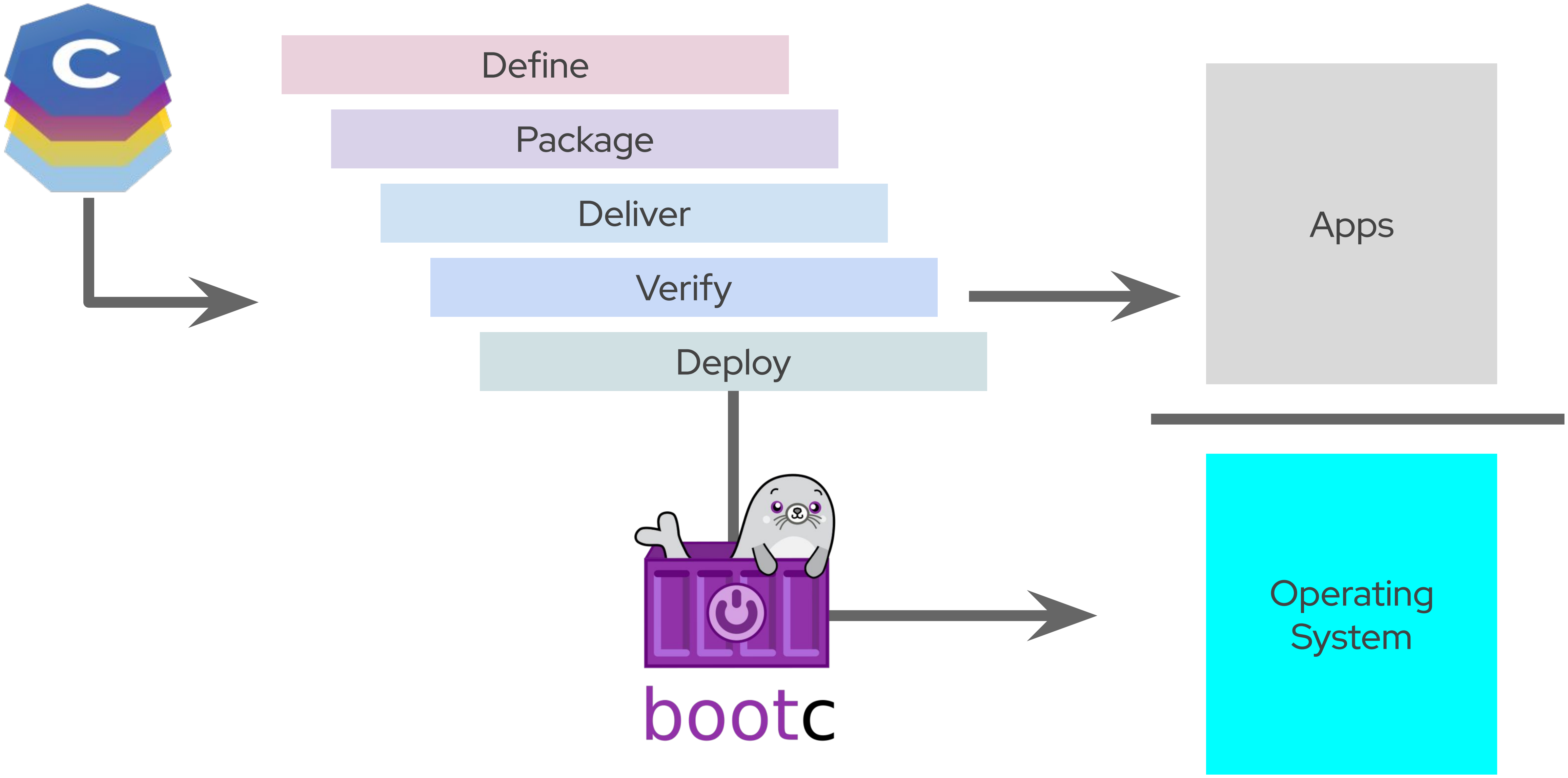
fedora

Upstream Developments in Bootable Containers

Ben Breard
Nerd from Product Management

✉ bbreard@redhat.com
🌐 https://mrguitar.net



Define

Package

Deliver

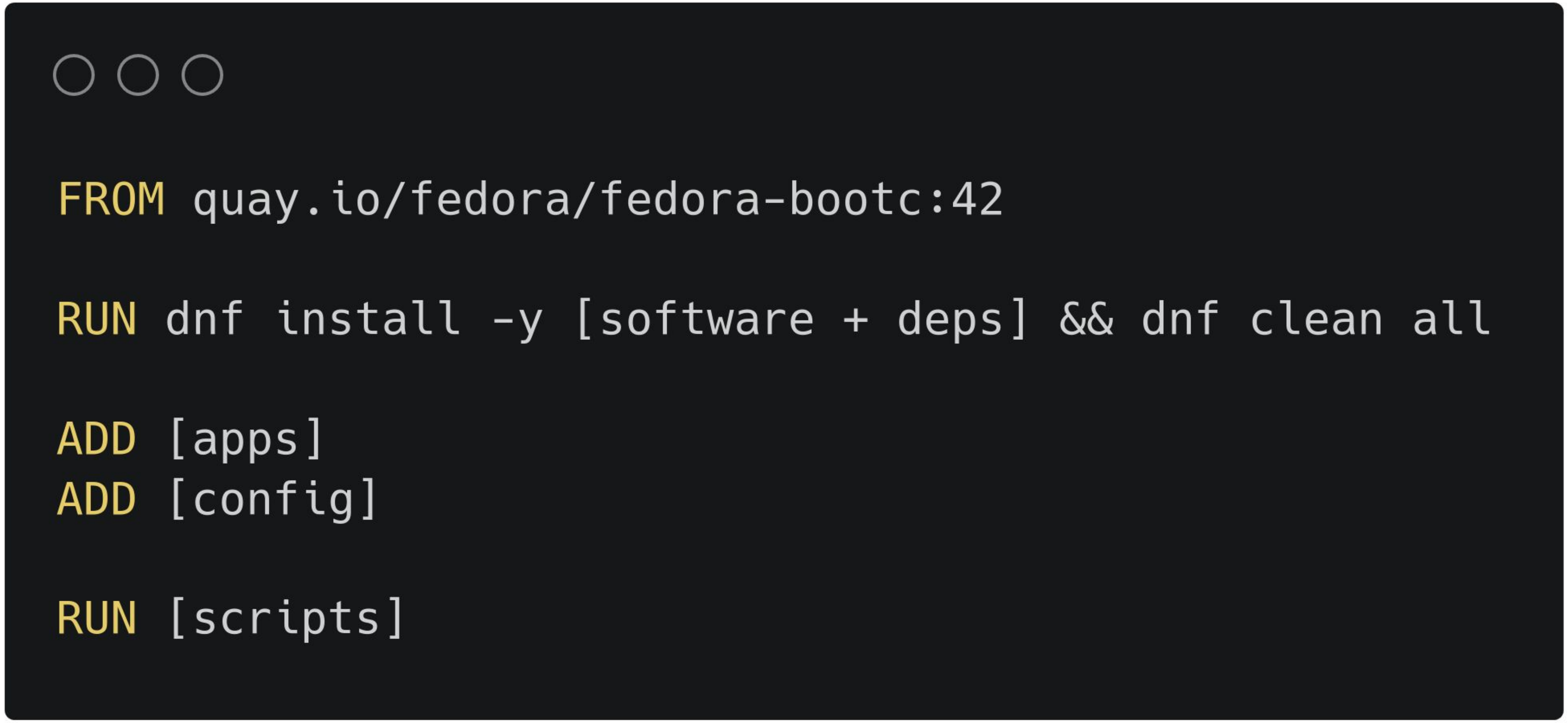
Verify

Deploy

Apps

Operating System

bootc

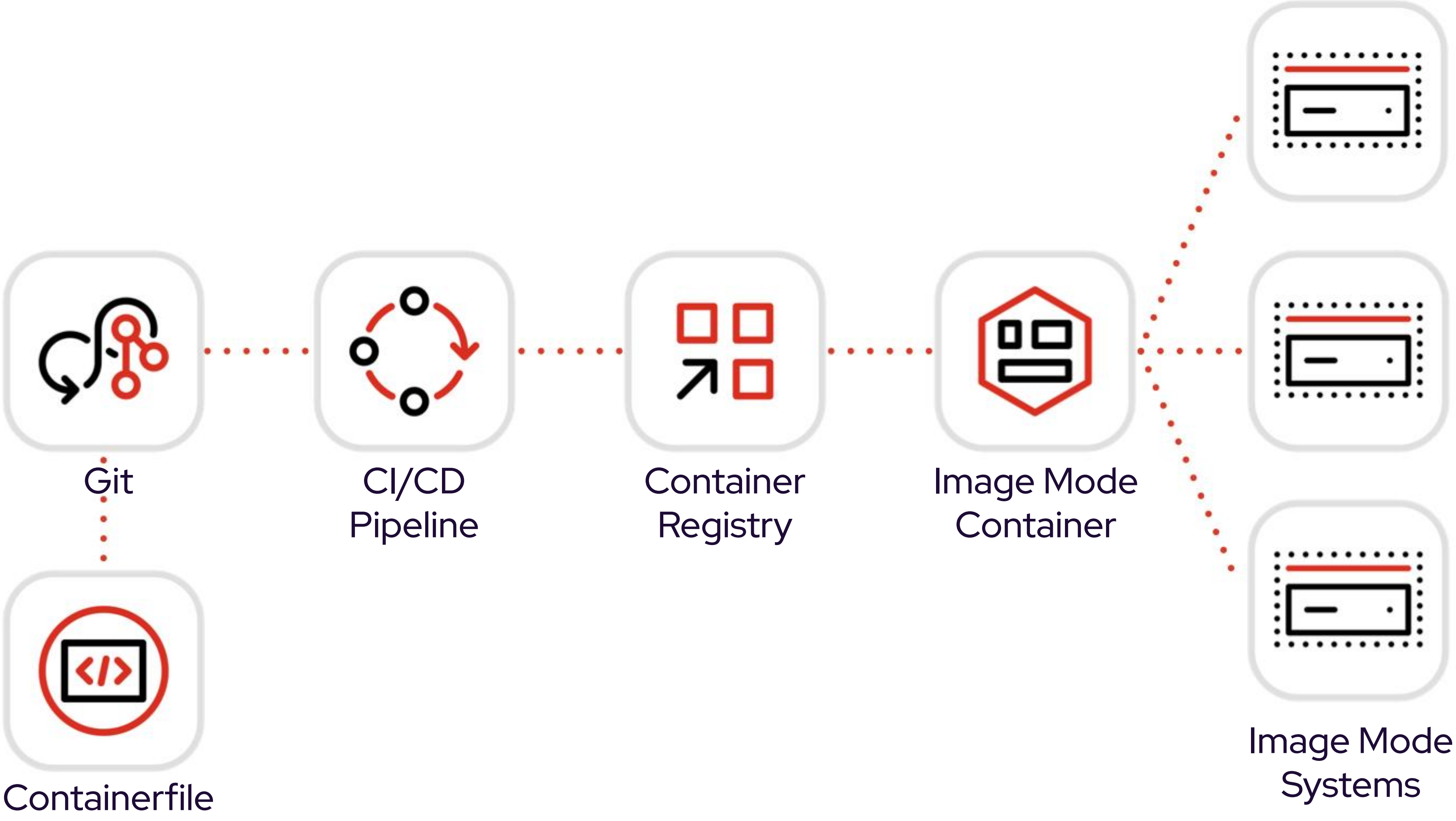


```
FROM quay.io/fedora/fedora-bootc:42

RUN dnf install -y [software + deps] && dnf clean all

ADD [apps]
ADD [config]

RUN [scripts]
```


Git
CI/CD Pipeline
Container Registry
Image Mode Container
Containerfile
Image Mode Systems

bootc Upstream

Milestones

- High velocity: 26 releases
- November ‘24 APIs declared stable
- CNCF Sandbox contribution
- Legit upstream docs and getting started guides

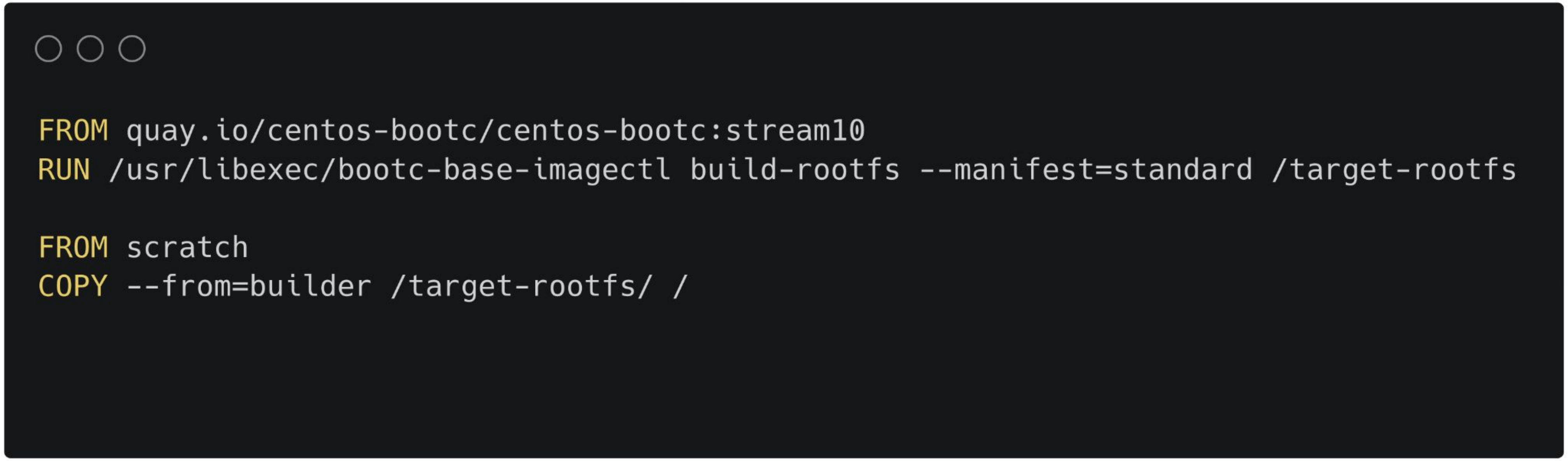
Adoption Stats:

- Lots of derivative distros
- Consolidation point for rpm-ostree variants.
- Matrix members? ~183

Base images

- Fedora & Red Hat derivatives well covered
  - `quay.io/fedora/fedora-bootc:42`
  - `quay.io/centos-bootc/centos-bootc:stream10`
  - `registry.redhat.io/rhel10/rhel-bootc:10.0`
- Ongoing work on others (Arch, Debian etc.); one pain point is bootloaders
- Aiming to make bootc a first-class citizen native to the OS/distro; versioning, testing etc

Images from scratch



```
FROM quay.io/centos-bootc/centos-bootc:stream10
RUN /usr/libexec/bootc-base-imagectl build-rootfs --manifest=standard /target-rootfs

FROM scratch
COPY --from=builder /target-rootfs/ /
```

- Base image acts as a builder for new base images!
- Can work in a familiar dockerfile multi-stage build
- Content sets: minimal & standard

- Can build from pinned RPM versions
- Also, new **rechunk** operation
- Ongoing work on non-Fedora derivatives!

bootc

A/B booting of container images

`bootc upgrade`

Download and stage an updated container image.

- Automatic updates on by default. Configurable using bootc-fetch-apply-updates.timer

`bootc rollback`

Rollback to the previous state. Staged updates are discarded

`bootc switch`

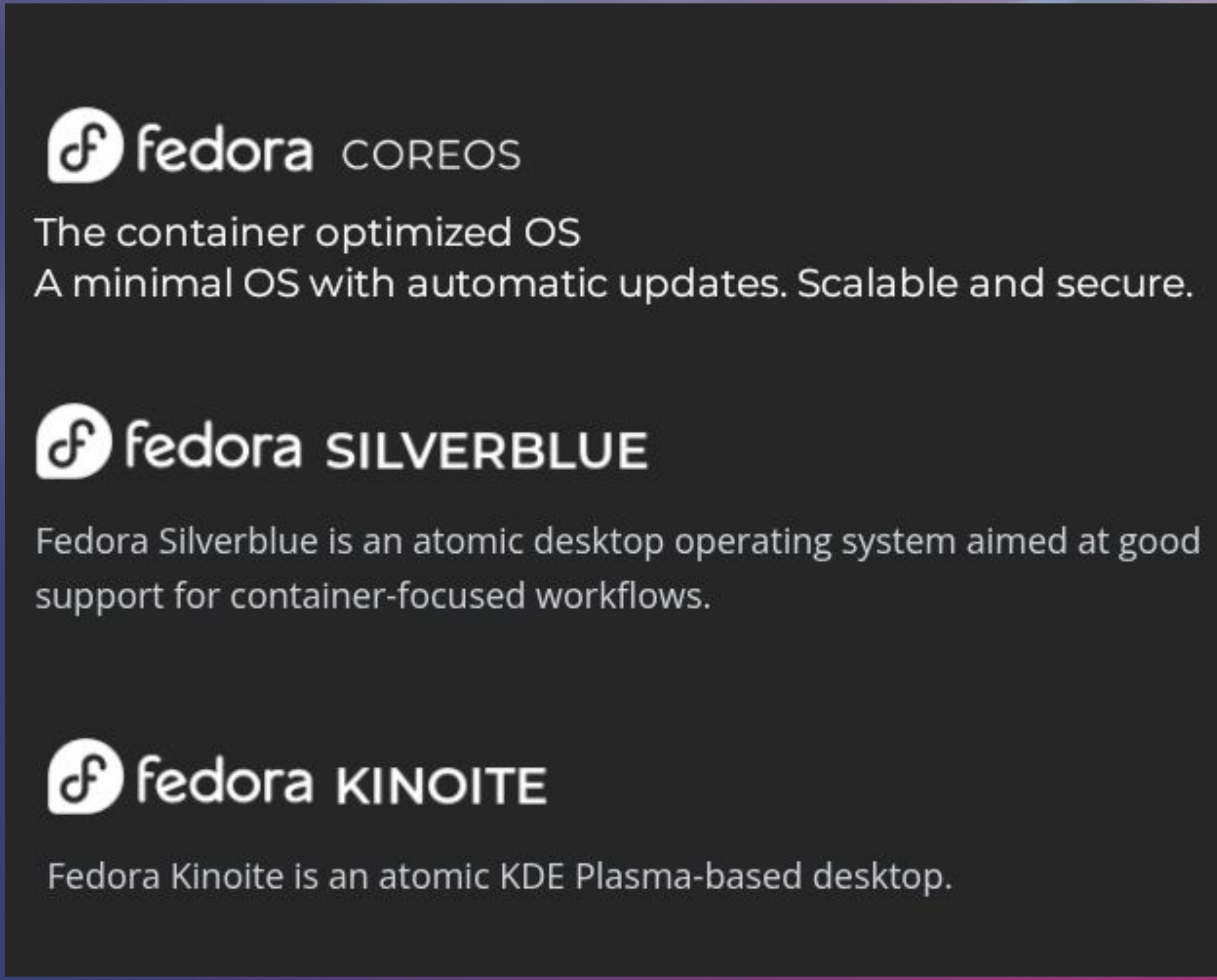
Change to a different reference image

`bootc install`

Install container image **`to-disk`** or **`to-filesystem`**

- Man page
- https://github.com/containers/bootc
- https://github.com/containers/podman-desktop-extension-bootc

Fedora CoreOS & Atomic Desktops



fedora COREOS

The container optimized OS
A minimal OS with automatic updates. Scalable and secure.

fedora SILVERBLUE

Fedora Silverblue is an atomic desktop operating system aimed at good support for container-focused workflows.

fedora KINOITE

Fedora Kinoite is an atomic KDE Plasma-based desktop.

universal blue

Powered by the future, delivered today.

Aurora

Aurora is a clean and reliable desktop operating system for every type of user. Many batteries included.

bazzite

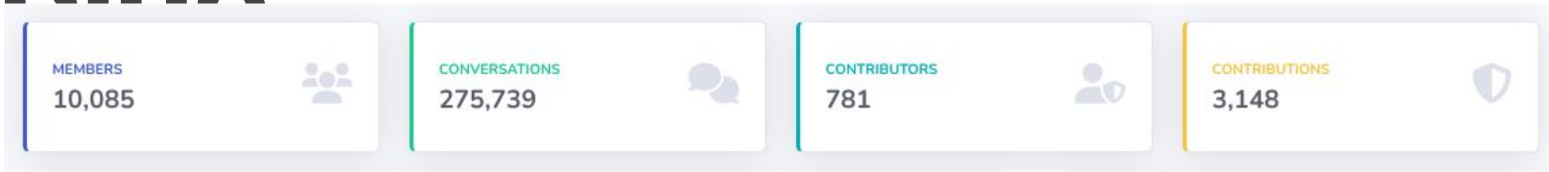
The next generation of Linux Gaming for all of your devices - including your favorite handheld.

project Bluefin

The next generation Linux workstation, designed for reliability, performance, and sustainability.

uCore

An OCI base image of Fedora CoreOS with batteries included; a lightweight server image including most used services or the building blocks to host them.

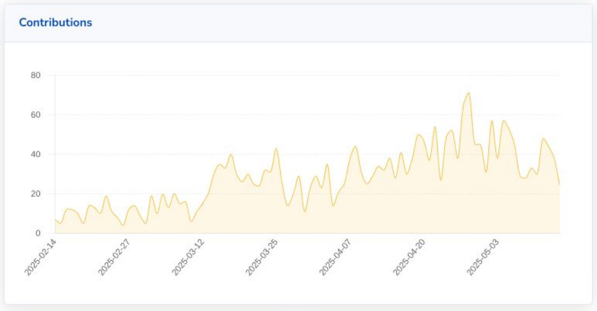


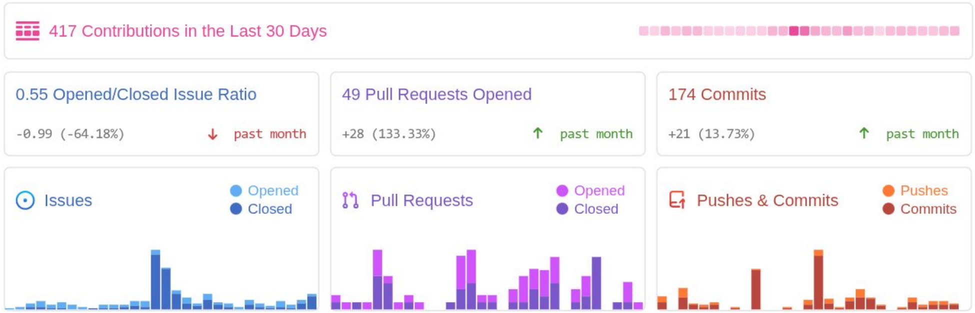
MEMBERS 10,085

CONVERSATIONS 275,739

CONTRIBUTORS 781

CONTRIBUTIONS 3,148


Contributions

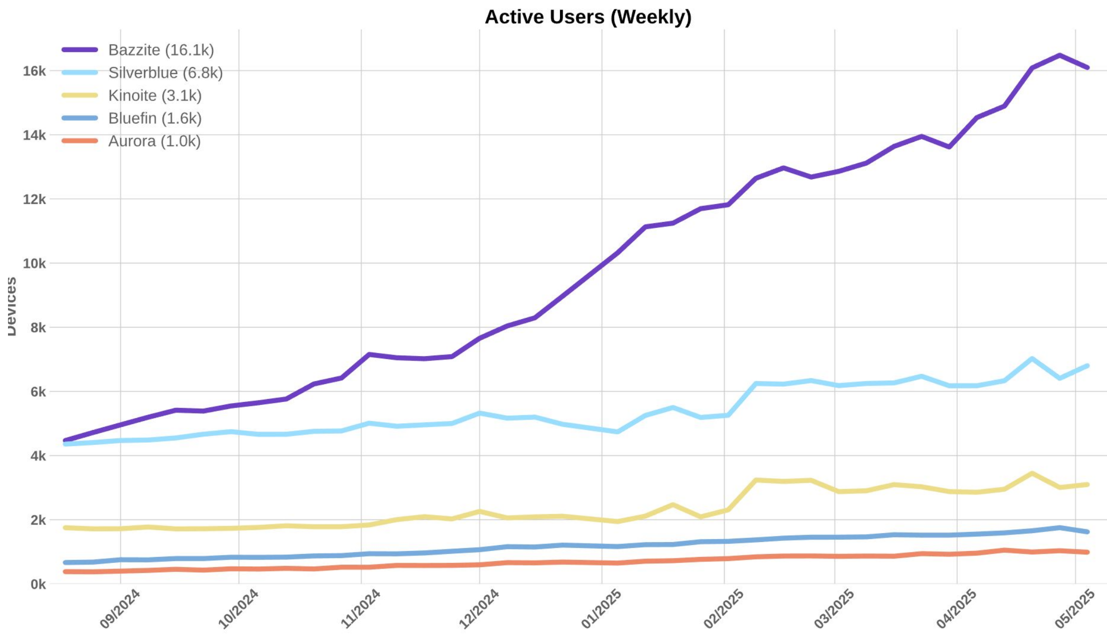


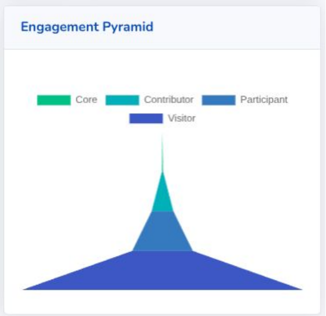
417 Contributions in the Last 30 Days

0.55 Opened/Closed Issue Ratio — -0.99 (-64.18%) ↓ past month

49 Pull Requests Opened — +28 (133.33%) ↑ past month

174 Commits — +21 (13.73%) ↑ past month


Active Users (Weekly)

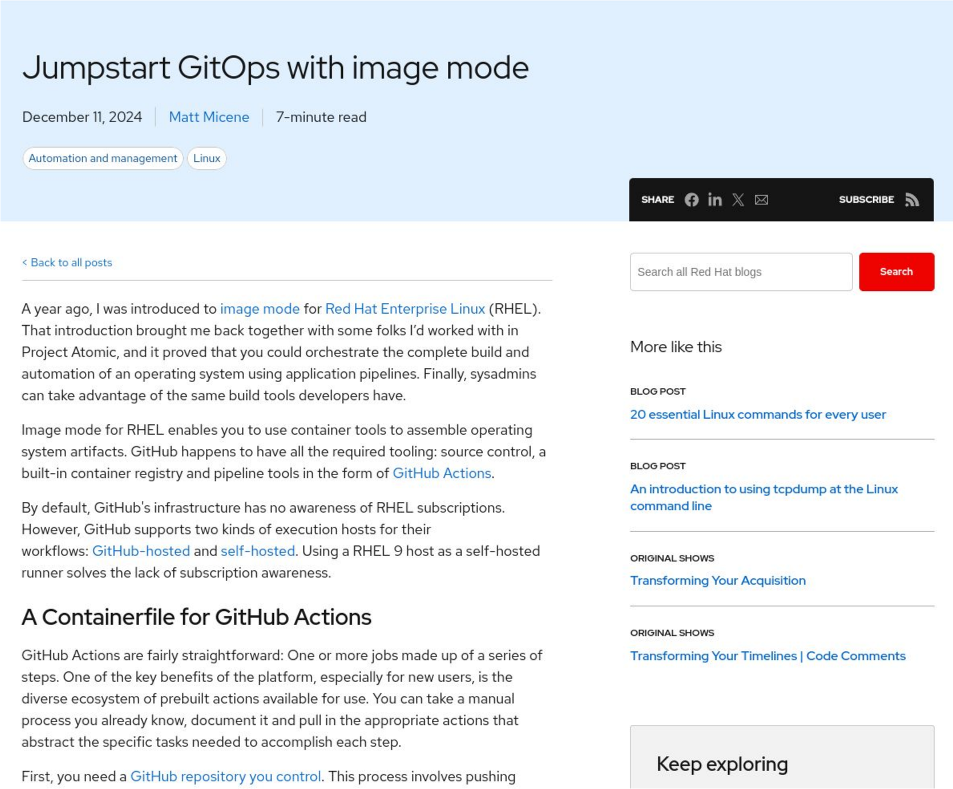

Engagement Pyramid

Red Hat

GitOps at the OS-level

Build smarter. Run smoother.

GitOps Jumpstart



Jumpstart GitOps with image mode

December 11, 2024 | Matt Micene | 7-minute read

Automation and management | Linux

A year ago, I was introduced to image mode for Red Hat Enterprise Linux (RHEL). That introduction brought me back together with some folks I'd worked with in Project Atomic, and it proved that you could orchestrate the complete build and automation of an operating system using application pipelines. Finally, sysadmins can take advantage of the same build tools developers have.

Image mode for RHEL enables you to use container tools to assemble operating system artifacts. GitHub happens to have all the required tooling: source control, a built-in container registry and pipeline tools in the form of GitHub Actions.

By default, GitHub's infrastructure has no awareness of RHEL subscriptions. However, GitHub supports two kinds of execution hosts for their workflows: GitHub-hosted and self-hosted. Using a RHEL 9 host as a self-hosted runner solves the lack of subscription awareness.

A Containerfile for GitHub Actions

GitHub Actions are fairly straightforward: One or more jobs made up of a series of steps. One of the key benefits of the platform, especially for new users, is the diverse ecosystem of prebuilt actions available for use. You can take a manual process you already know, document it and pull in the appropriate actions that abstract the specific tasks needed to accomplish each step.

First, you need a GitHub repository you control. This process involves pushing

More like this

BLOG POST
20 essential Linux commands for every user

BLOG POST
An introduction to using tcpdump at the Linux command line

ORIGINAL SHOWS
Transforming Your Acquisition

ORIGINAL SHOWS
Transforming Your Timelines | Code Comments

Keep exploring

Rule #1: All changes happen in the repo. Period!
Fight the temptation to vim that config file!

Rule #2: Time-based models are your best friend
Outage windows can be difficult to negotiate and coordinate. Only play this game where absolutely necessary, for everything else only **schedule regular reboots**.

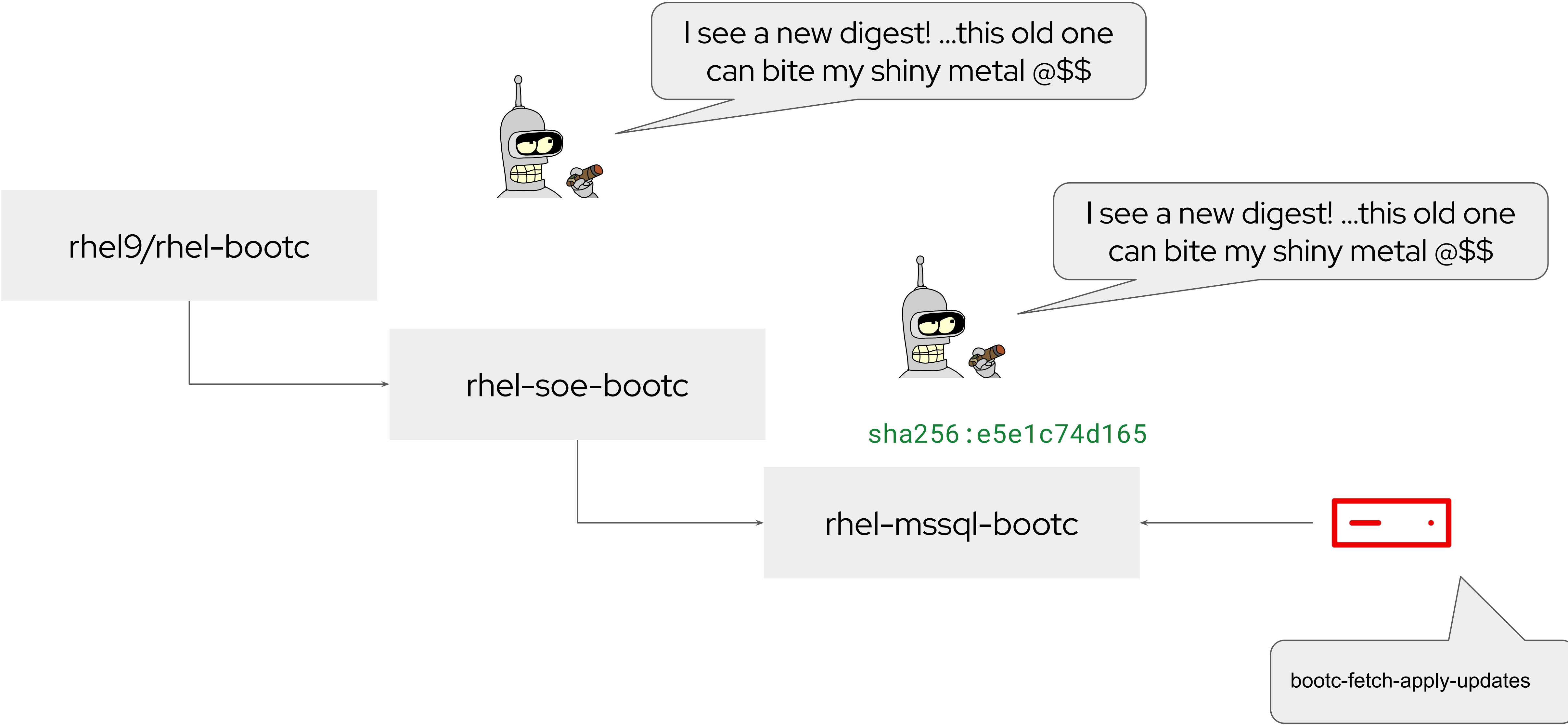
Rule #3: Build early and often
Just because an image is built doesn't mean we have to ship it, or apply it. Building early gets us ahead of CVEs!

Rule #4: Trust your pipelines and auto-updates
Where appropriate, leverage end-2-end automation. Only use manual releases when absolutely required.

Template: https://github.com/redhat-cop/redhat-image-mode-actions/

Image updates with Renovate Bot

```
FROM registry.redhat.io/rhel9/rhel-bootc@sha256:a7aabe61cc7a52ed
```



I see a new digest! ...this old one can bite my shiny metal @$$
I see a new digest! ...this old one can bite my shiny metal @$$

rhel9/rhel-bootc

rhel-soe-bootc

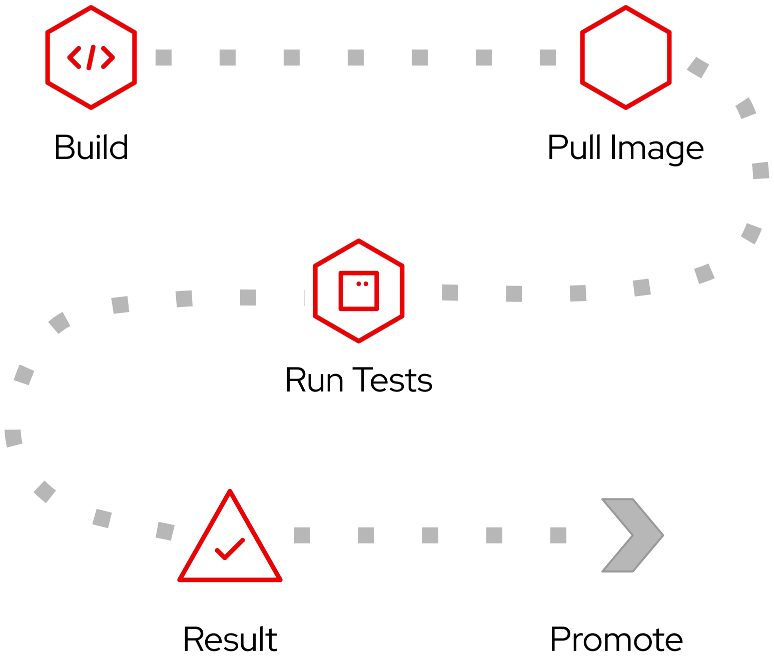
sha256:e5e1c74d165

rhel-mssql-bootc

bootc-fetch-apply-updates

Validating OS updates has never been easier

CI pipelines used for apps now work with the OS



Test/validate as a container

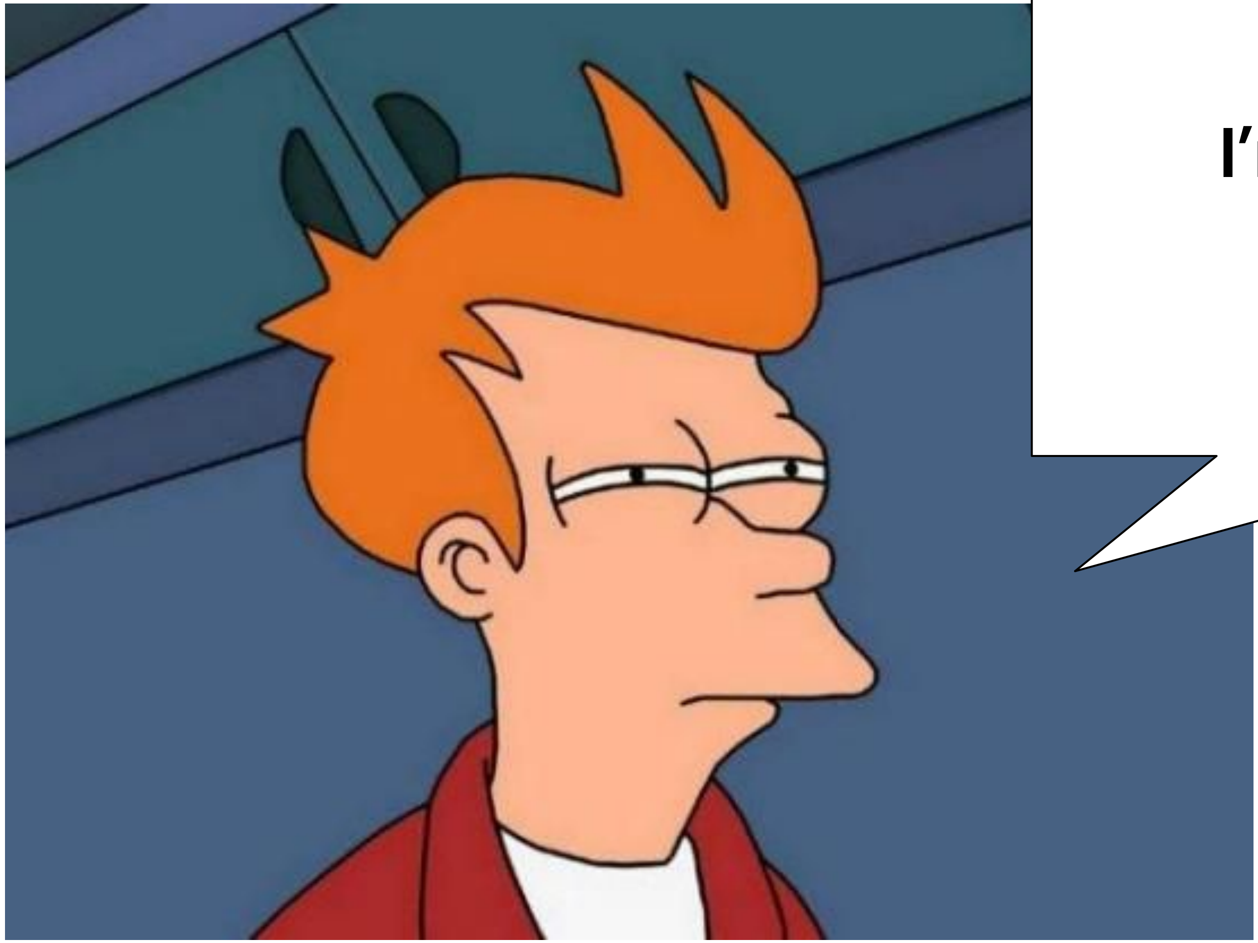
Bootc images are deployed as bare metal or VMs, but we can also run and test them **as containers**. This enables faster and lighter weight testing/validation of each build’s userspace.

Easy pipeline integration

Containers have broad support across Github, Gitlab, Gitea, Circle CI, Jenkins, etc for the common container related tasks and testing. Use any system you like..

Simple promotion through registry tagging

Tags are a powerful tool to identify dev → test → prod promotions.



I’m skeptical. Show me!

SHUT UP AND TAKE
MY MONEY
quickmeme.com

Use Cases

Where does image mode fit today?

Use Cases Blog

AI/ML Stacks

Perfectly version app dependencies from kernel, GPU & accelerator drivers, frameworks, runtimes, etc

1:1 App/Host

Manage the OS AND app as a single unit

Edge appliances

Easily manage a fleet of systems with registries and auto-updates

Standalone container hosts

Use common toolchains and pipelines to build containerized applications and the hosting OS

Thank you!

Get involved:
Forum https://discussion.fedoraproject.org/tag/bootc-initiative
Matrix https://matrix.to/#/#bootc:fedoraproject.org

Images:
quay.io/fedora/fedora-bootc:42
quay.io/centos-bootc/centos-bootc:stream10

Projects:
https://podman-desktop.io/
projectbluefin.io