The Future of Fedora CoreOS

Fedora's Flock Contributor Conference - Prague - 2025

Dusty Mabe
Senior Principal Engineer at Red Hat

Agenda

- Recent Developments
- Metrics
- The Future!
- Questions?

Recent Developments in Fedora CoreOS

Recent Developments

- Switched to using **OSBuild** for disk image building
- Switched newly deployed nodes to **OCI registry updates**
- Added the **Hetzner Platform** and disk images
- Added **Kubevirt** images for **s390x**
- In Progress: Switching **existing** nodes to **OCI updates**
- In Progress: **Proxmox** Enablement

Recent Developments

HETZNER

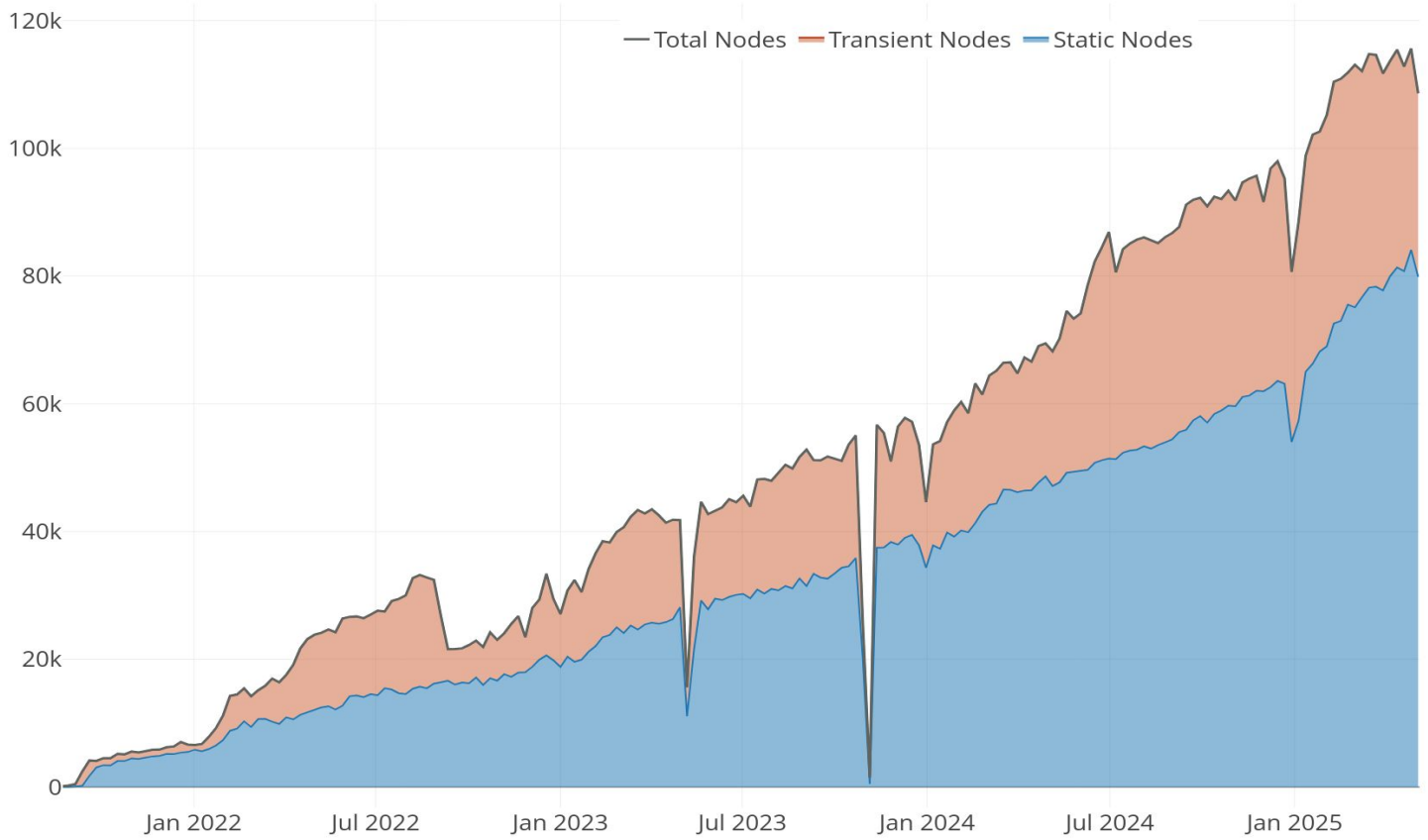
KubeVirt

PROXMOX

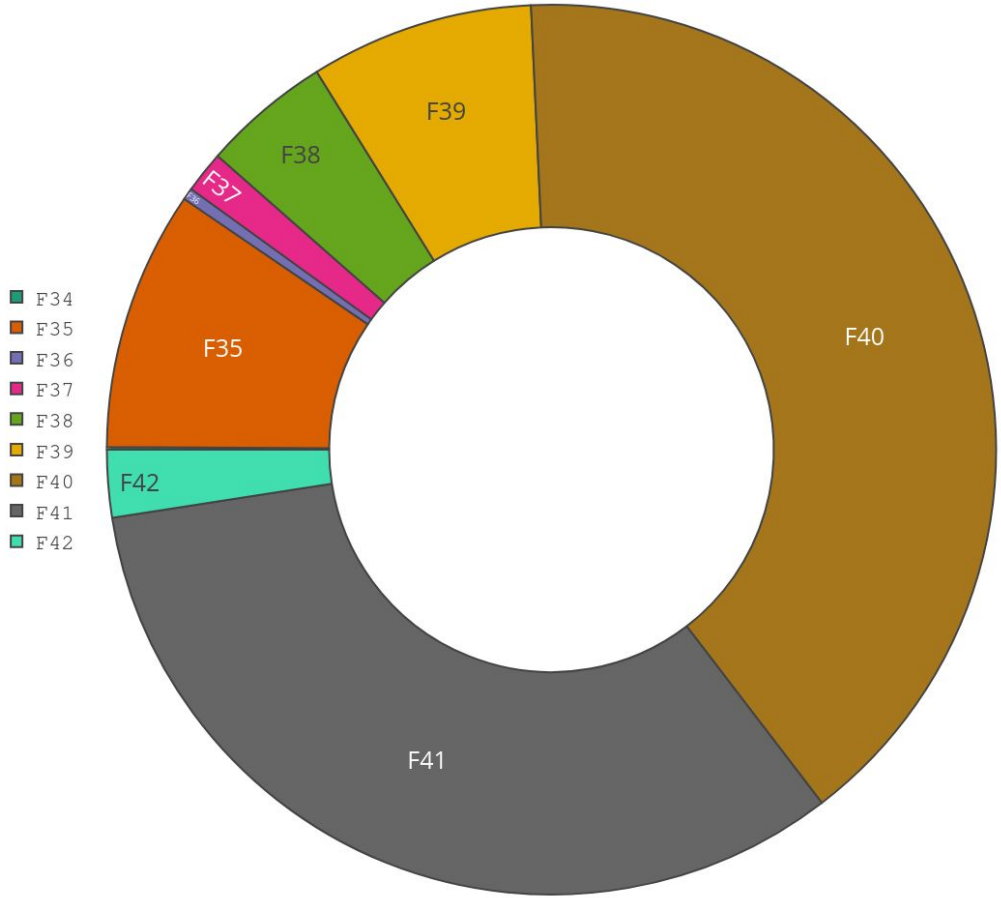
Platform Offerings for CoreOS

Metrics

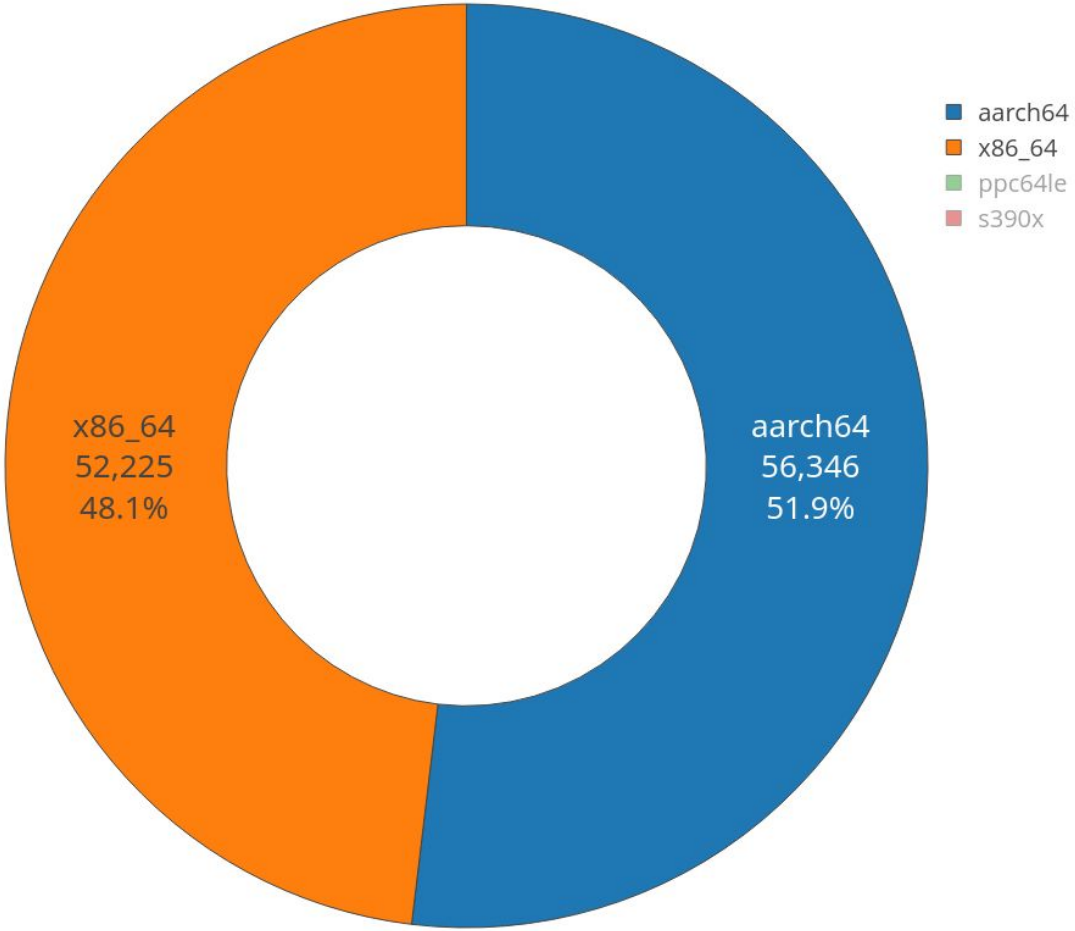
Metrics: All Nodes (2025/05)



Metrics: by Fedora Release (2025/05)



Metrics: by Architecture (2025/05)



Podman Machine/Desktop

podman desktop

Documentation Core Values Features Downloads Extend Blog

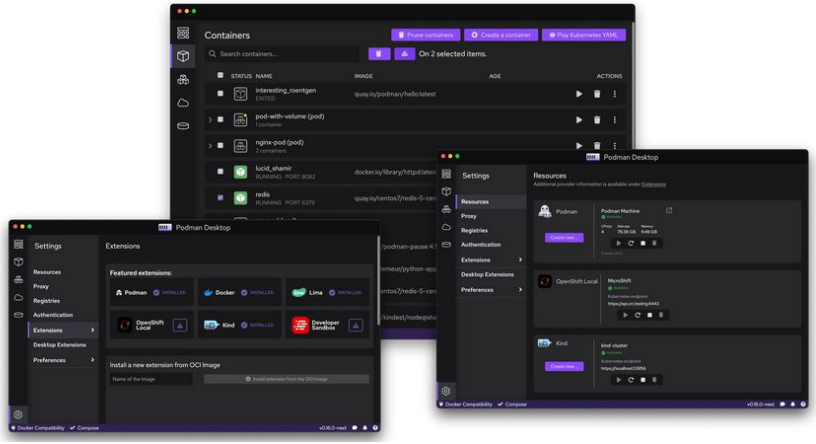
Containers and Kubernetes for application developers

Podman Desktop is an open source graphical tool enabling you to seamlessly work with containers and Kubernetes from your local environment.

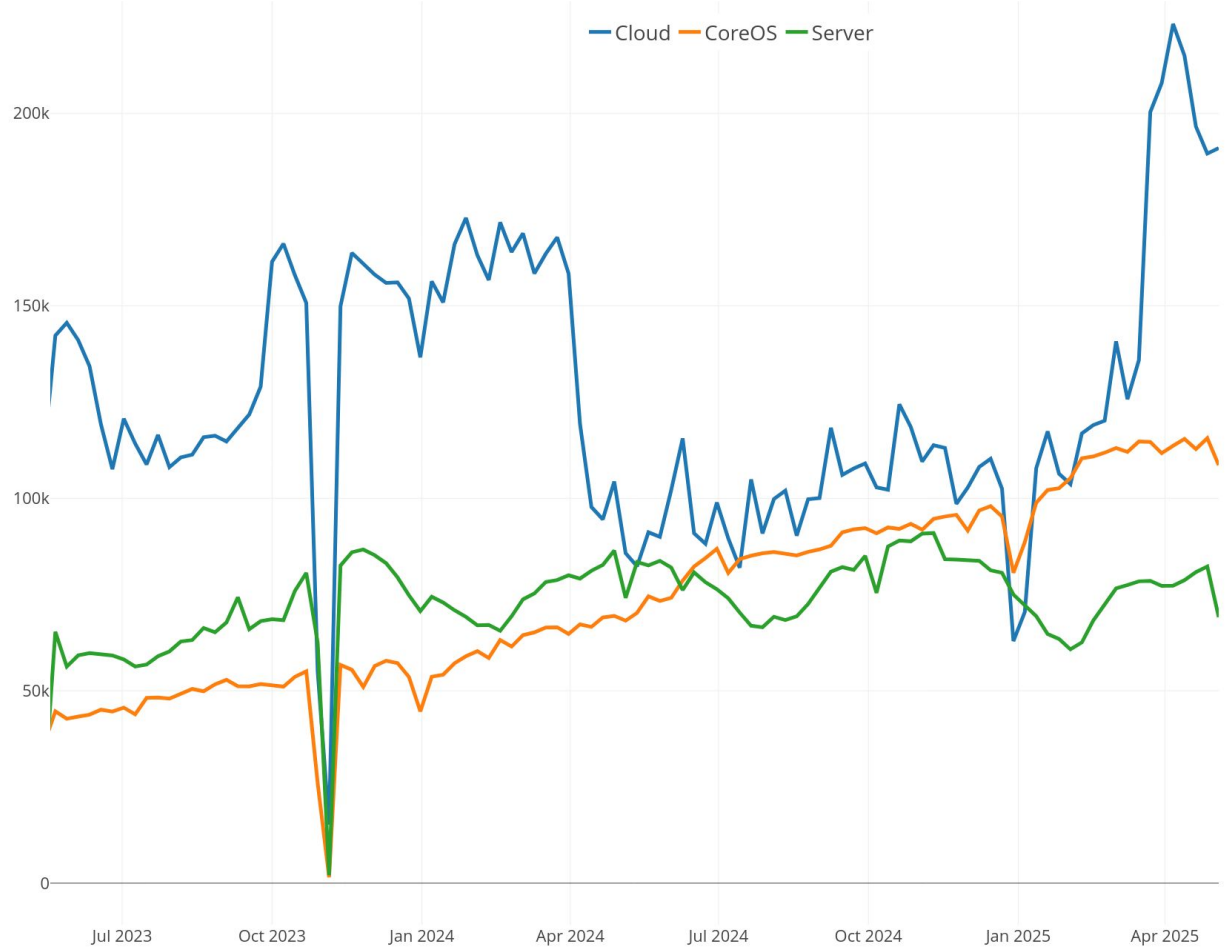
Download Now

For Linux *(browser-detected)*

Other downloads



Total Node Count Cloud/CoreOS/Server



The Future

The Future

But what is **bootc**?

1

The **bootc** Tech (software)

- /bin/bootc upgrade
- /bin/bootc install
- /bin/bootc status

2

The **bootc** Base Images

- Actual container images
- Can be used as a building block
- Offered for Fedora/CentOS

But what is **bootc**?

1

The **bootc** Tech (software)

```
[core@cosa-devsh ~]$
[core@cosa-devsh ~]$ sudo bootc status
● Booted image: quay.io/fedora/fedora-coreos:rawhide
        Digest: sha256:72baa141a3af2293cdc30cce56fe56e9d4c07cf5b8e7f161d3d3c86b6624ac18 (amd64)
       Version: 43.20250530.91.0 (2025-05-30T10:09:32Z)

  Rollback image: quay.io/fedora/fedora-coreos:rawhide
          Digest: sha256:a9dcd82df641ca9f3d3b375d30400bd41d1b1b0c317a046f7c8e11f4580080f7 (amd64)
         Version: 43.20250530.dev.0 (2025-05-30T12:24:12Z)
[core@cosa-devsh ~]$
[core@cosa-devsh ~]$ sudo bootc upgrade
No changes in quay.io/fedora/fedora-coreos:rawhide => sha256:72baa141a3af2293cdc30cce56fe56e9d4c07c
No update available.
```

But what is **bootc**?

2

The **bootc** Base Images

Base images

This project closely tracks CentOS and Fedora, and aims to tightly integrate with their underlying lifecycle as well as release and test infrastructure, and in particular the CentOS Stream versions are the upstream for the RHEL product.

These are the default "full" images:

- CentOS Stream 9: `quay.io/centos-bootc/centos-bootc:stream9` (source repo)
- Fedora: `quay.io/fedora/fedora-bootc:42` (source repo)
- CentOS Stream 10 (in development): `quay.io/centos-bootc/centos-bootc:stream10` (source repo)

For RHEL, see RHEL 9 Image Mode. Note that at the current time the RHEL product is Tech Preview status and this is also true of the upstream; the contents and interfaces of the base images are still subject to change.

But what is **bootc**?

2

The **bootc** Base Images

Containerfile

```
FROM quay.io/fedora/fedora-bootc:42
# The default package drops content in /var/www, and on bootc systems
# we have /var as a machine-local mount by default. Because this content
# should be read-only (at runtime) and versioned with the container image,
# we move it to /usr/share/www instead.
RUN dnf -y install httpd && \
    systemctl enable httpd && \
    mv /var/www /usr/share/www && \
    echo 'd /var/log/httpd 0700 - - -' > /usr/lib/tmpfiles.d/httpd-log.conf && \
    sed -ie 's,/var/www,/usr/share/www,' /etc/httpd/conf/httpd.conf
# Further, we also disable the default index.html which includes the operating
# system information (bad idea from a fingerprinting perspective), and crucially
# we inject our own content as part of the container image build.
# This is a key point: In this model, the webserver content is lifecycled exactly
# with the container image build, and you can change it "day 2" by updating
# the image. The content is underneath the /usr readonly bind mount - it
# should not be mutated per machine.
RUN rm /usr/share/httpd/noindex -rf
COPY index.html /usr/share/www/html
EXPOSE 80
```

Future CoreOS

1 & 2

- **Will leverage BOTH:**
  - The **bootc** tech
    - Active Development
    - Exciting new features
  - The **bootc** base images

Future CoreOS - **bootc** tech

- Logically Bound Images
  - **bootc** will ensure configured container images are bound to an update. The update won't proceed without them.

```
FROM quay.io/myorg/myimage:latest
COPY ./my-app.image /usr/share/containers/systemd/my-app.image
COPY ./my-app.container /usr/share/containers/systemd/my-app.container
RUN <<EOF
    ln -s /usr/share/containers/systemd/my-app.image \
          /usr/lib/bootc/bound-images.d/my-app.image
    ln -s /usr/share/containers/systemd/my-app.container \
          /usr/lib/bootc/bound-images.d/my-app.container
EOF
```

https://bootc-dev.github.io/bootc/logically-bound-images.html

Future CoreOS - **bootc** tech

- Out-Of-Band Configuration Management (future feature)
  - Using configmaps/overlays
    - `bootc config add [--root=/etc] \`
      `https://examplecorp.com/config.yml`
    - OR
    - `bootc config add [--root=/etc] \`
      `registry:quay.io/examplecorp/config-server-base:latest`
    - OR
    - `bootc config add [--root=/etc] \`
      `https://github.com/myapp/myapp-config.git#main`

https://github.com/bootc-dev/bootc/issues/22

Future CoreOS - **bootc** tech

- Out-Of-Band Configuration Management (future feature)
  - Using configmaps/overlays

```
variant: fcos
version: 1.6.0
config-maps:
  - github.com/myapp/myappconfig
    ref: main
```

https://github.com/bootc-dev/bootc/issues/22

Future CoreOS - **bootc** tech

- Factory Reset (future feature)
  - Being able to re-install in place
    - Option to keep OR discard data
    - Useful in bare metal environments
      - or any env that isn't easily provisionable

https://github.com/bootc-dev/bootc/issues/404

Future CoreOS - **bootc** tech

- Confidential Compute

https://github.com/coreos/fedora-coreos-tracker/issues/1719

Future CoreOS - **bootc** tech

- Confidential Compute

Confidential computing is a security and privacy-enhancing computational technique focused on protecting data in use. Confidential computing can be used in conjunction with storage and network encryption, which protect data at rest and data in transit respectively.[1][2] It is designed to address software, protocol, cryptographic, and basic physical and supply-chain attacks, although some critics have demonstrated architectural and side-channel attacks effective against the technology.[3]

The technology protects data in use by performing computations in a hardware-based trusted execution environment (TEE).[3] Confidential data is released to the TEE only once it is assessed to be trustworthy. Different types of confidential computing define the level of data isolation used, whether virtual machine, application, or function, and the technology can be deployed in on-premise data centers, edge locations, or the public cloud. It is often compared with other privacy-enhancing computational techniques such as fully homomorphic encryption, secure multi-party computation, and Trusted Computing.

Confidential computing is promoted by the Confidential Computing Consortium (CCC) industry group, whose membership includes major providers of the technology.[4]

https://en.wikipedia.org/wiki/Confidential_computing

Future CoreOS - **bootc** tech

- Confidential Compute (future feature)
  - **UKI** -> Unified Kernel Image
    - A Unified Kernel Image (UKI) is a combination of an **UEFI boot stub program**, a **Linux kernel** image, an optional **initrd**, and further resources (like **cmdline args**) in a single UEFI PE file.
    - This single file **can be signed** to provide secureboot like guarantees over your kernel + initrd + kernel command line.
    - **ComposeFS**+**EROFS**+**fsverity** can then be used to verify we are booting into exactly what was requested via those signed kernel command line arguments.

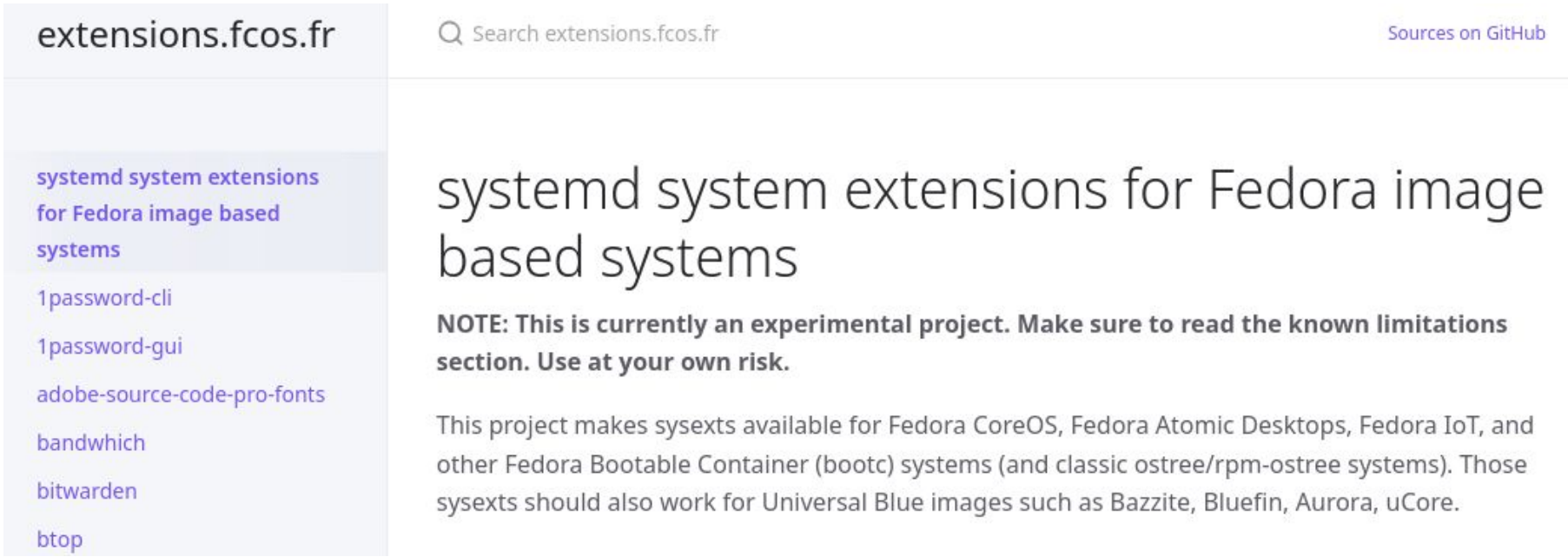
https://github.com/coreos/fedora-coreos-tracker/issues/1719

Future CoreOS - **bootc** tech

- systemd system extensions (sysexts)
  - Allow for you to deliver some extensions to base software
  - overlay on top of /usr/
    - merged/unmerged on demand
  - bootc could help us manage these
    - https://github.com/bootc-dev/bootc/issues/7
  - Timothee has been exploring these from a CoreOS and Atomic Desktops perspective: https://travier.github.io/fedora-sysexts/

Future CoreOS - **bootc** tech

- systemd system extensions (sysexts)



https://travier.github.io/fedora-sysexts/

Future CoreOS - **bootc** base images

- Ultimately the CoreOS end user experience stays the same
  - This is an implementation detail of how we build FCOS
- Leverage shared base image with other Fedora Editions
- Bring some CoreOS tests to build out **bootc** base image CI
  - Other Fedora SIGs contribute their tests

What is **bootc** missing?

- No more distributing updates via OSTree
  - Fedora 42 CoreOS migrating to OCI based updates
- Less info about the content inside
  - RPMs aren't tracked like they were with RPM-OSTree
    - bootc meant to be OS/distro agnostic
- Package Layering
  - Major feature for FCOS users
- Client Side Initramfs Generation/Tracking

The Future

bootc & CoreOS: complement each other

- CoreOS -> directly consume
  - provision CoreOS vanilla images -> apps run via containers
  - follow updates from CoreOS published update graph
- bootc -> build your own
  - exactly what you need, nothing you don’t
  - apps run either directly or via containers; you choose
  - must create/own build pipeline for updates
  - future future: build your own update graph

bootc & CoreOS: user experience

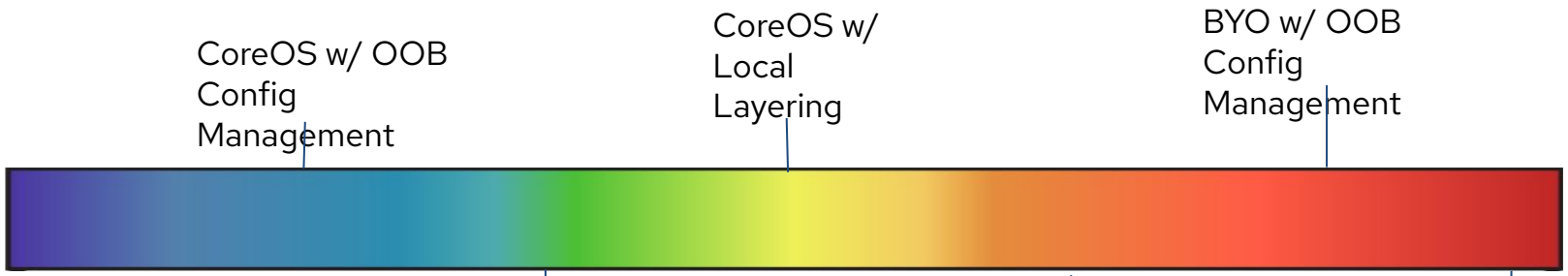
Shifting User Responsibility

CoreOS: Try it out

bootc: Make it your own

bootc & CoreOS: Together

Provide a Spectrum of Solutions for the Community



Questions?

Get involved!

- Web: https://fedoraproject.org/coreos/
- Issues: https://github.com/coreos/fedora-coreos-tracker/issues
- Forum: https://discussion.fedoraproject.org/tag/coreos
- Mailing list: coreos@lists.fedoraproject.org
- Matrix: **#coreos:fedoraproject.org**