Fedora IoT & Fedora CoreOS

Peter Robinson & Timothée Ravier

IoT & CoreOS teams at Red Hat

https://getfedora.org/iot/ & https://getfedora.org/coreos

fedora-iot & fedora-coreos on freenode.net

Agenda

- Common parts in Fedora CoreOS and Fedora IoT
- What is specific to Fedora IoT?
- What is specific to Fedora CoreOS?

Fedora CoreOS and Fedora IoT

- Based on Fedora: Built from Fedora RPMs
- Ship podman by default to run containers
  - Moby engine (Docker) also available on Fedora CoreOS for compatibility
- SELinux enforcing by default
  - Isolates containers from each others
  - Prevents compromised apps from gaining further access

Fedora CoreOS and Fedora IoT

- Uses rpm-ostree technology:
  - "Like git for your Operating System"
    - System shipped as a versioned base image (32.20200615.2.0 - 86c0246)
    - Atomic updates, rollbacks and package overrides
  - Leverages read-only filesystem mounts (/, /usr & /boot)
    - All data goes in /var and system configuration in /etc
    - Ensures that changes to the system are tracked by rpm-ostree
    - Avoids some forms of accidental and malicious damage

Fedora IoT specific features

Philosophy behind Fedora IoT

- Immutable infrastructure
  - Packages can be layered, but...
- User software runs in containers
  - Host updates are more reliable
- TPM2 to provide hardware root of trust for Edge
- TPM2, IMA to provide data security for edge devices
- Management with an Ansible Collection with Edge focus
- Greenboot for updates healthcheck for automated rollbacks
- Image Builder with osbuild for installer/updates creation

Targeted architectures and platforms

- Support x86_64, aarch64 and ARMv7
- Support for Fedora container build pipeline
- Only support devices with UEFI support
- All SoCs that Fedora Arm supports but requires SBBR/EBBR
- Some example devices include:
    - NVIDIA Jetson Xavier series
    - Compulabs Fitlet2
    - Solid-run Honeycomb and Humminboards
    - Raspberry Pi series of devices

Onboarding with Zezere

- A proof of concept for minimal touch onboarding
- Will evolve to support FIDO IoT spec
- https://github.com/fedora-iot/zezere

Fedora IoT Security

Aiming for similar security to the data centre without the security and access control of 4 walls:

- TPM2 critical for non recoverability of critical information
- IMA for measurement and attestation
- UEFI Secure boot to verify the boot process
- Emerging hardware secure enclave technologies with software
- Emerging security initiatives like PARSEC
- A number of other initiatives around security
- Industry engagement such as TCG/IETF/FIDO

Where are people using Fedora IoT

- Various prototypes in industrial including vision use cases
- Healthcare and aged care
- 3D printers and other devices
- Retail and point of sale
- Home automation and monitoring
- Home brewing

Fedora CoreOS specific features

Philosophy behind Fedora CoreOS

- Automatic updates
  - no interaction for administrators
  - staying up to date -> security fixes applied
- All nodes start from ~same starting point
  - Use Ignition to provision a node wherever it's started
  - Bare metal and cloud based instances share provisioning
- Immutable infrastructure
  - Need a change? Update configs and re-provision.
- User software runs in containers
  - Host updates are more reliable

Features: Automatic Updates

- Fedora CoreOS features Automatic Updates by default
  - Automatic updates → Reliable updates
    - Extensive tests in automated CI pipelines
    - Several update streams to preview what’s coming
      - Users run various streams to help find issues
    - Managed upgrade rollouts over several days
      - Halt the rollout if issues are found
  - For when things go wrong
    - rpm-ostree rollback can be used to go back

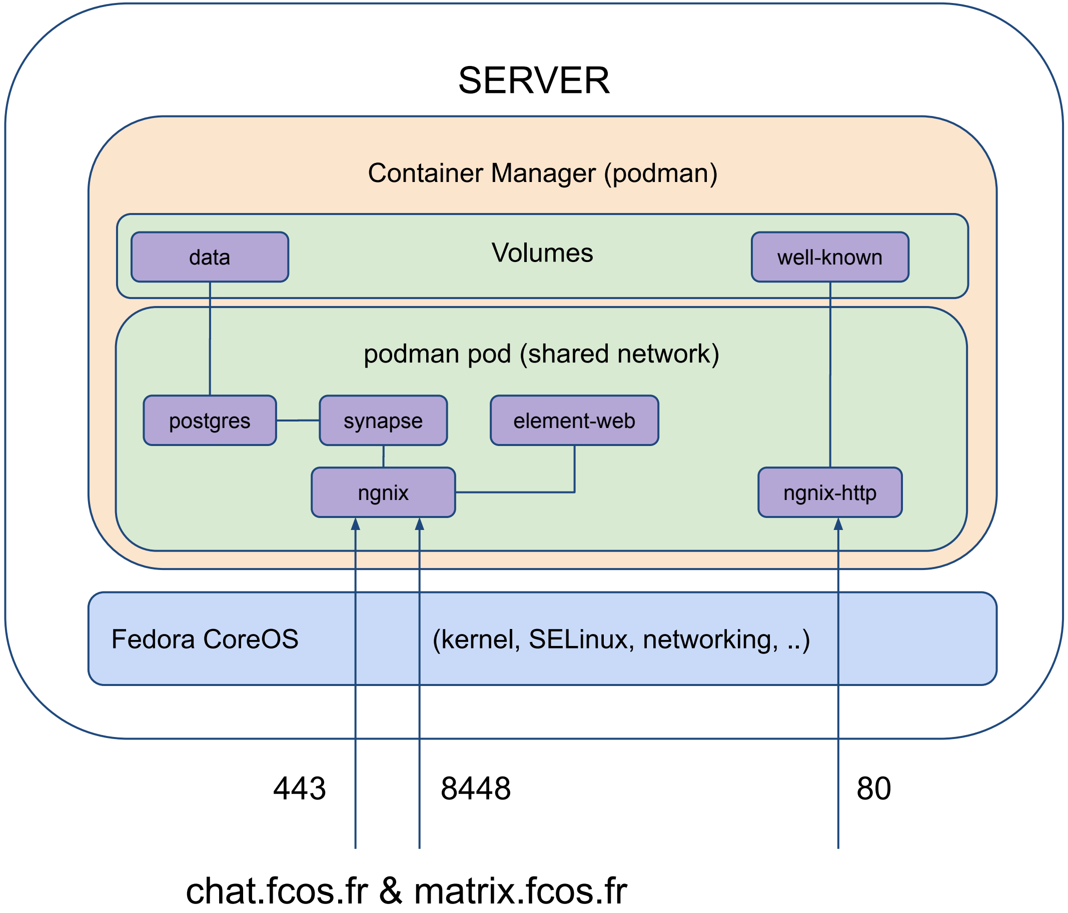
Features: Automated Provisioning

- Fedora CoreOS uses Ignition to automate provisioning
    - Any logic for machine lifetime is encoded in the config
        - Very easy to automatically re-provision nodes
    - Same starting point whether on bare metal or cloud
        - Use Ignition everywhere as opposed to kickstart for bare metal and cloud-init for cloud

Targeted architectures and platforms

- Currently x86_64 only
  - Support for aarch64, ppc64le, s390x planned
- Baremetal
- Offered on (or for) a plethora of cloud/virt platforms
  - Alibaba, AWS, Azure, DigitalOcean, Exoscale, GCP, Openstack, Vultr, VMWare, QEMU/KVM

Example use case


SERVER
Container Manager (podman)
data
Volumes
well-known
podman pod (shared network)
postgres
synapse
element-web
ngnix
ngnix-http
Fedora CoreOS
(kernel, SELinux, networking, ..)
443
8448
80
chat.fcos.fr & matrix.fcos.fr

[matrix]

https://github.com/travier/fedora-coreos-matrix
https://fedoramagazine.org/deploy-your-own-matrix-server-on-fedora-coreos/

Get involved!

- Website: https://getfedora.org/coreos
- Docs: https://docs.fedoraproject.org/en-US/fedora-coreos/
- Issues: https://github.com/coreos/fedora-coreos-tracker/issues
- Forum: https://discussion.fedoraproject.org/c/server/coreos
- Mailing list: coreos@lists.fedoraproject.org
- IRC: freenode #fedora-coreos

- Website: https://getfedora.org/iot/
- Docs: https://docs.fedoraproject.org/en-US/iot/
- Issues: https://pagure.io/fedora-iot/issues
- Upstream projects: https://github.com/fedora-iot/
- Forum: https://discussion.fedoraproject.org/c/server/iot
- Mailing list: iot@lists.fedoraproject.org
- IRC: freenode #fedora-iot