Fedora CoreOS
What’s Now, What’s Next

Dusty Mabe - Red Hat
Principal Software Engineer

✉️ dusty@dustymabe.com
🌐 https://dustymabe.com
👥 dustymabe on freenode.net
Today’s Talk

- What Was
  - Container Linux
  - Atomic Host
- What’s Now
  - Fedora CoreOS
    - What is it?
    - What are the features?
    - What is the philosophy?
    - How does Fedora CoreOS Relate to Other Projects?
- What’s Next
  - Coming Features and Community Engagement
- Questions!
- Demo!
What Was
What Was

- Container Linux
  - Container Focused Operating System
  - Based on Gentoo
  - A/B partition image based update strategy
  - Used Ignition for Provisioning

- Atomic Host
  - Container Focused Operating System
  - Based on Fedora/RHEL, used RPMs as input
  - Used rpm-ostree technology for updates
  - Used Anaconda/Cloud-init for provisioning
What’s Now
Fedora CoreOS - Emerging Fedora Edition

- Came from the merging of two communities:
  - CoreOS Inc’s Container Linux
  - Project Atomic’s Atomic Host
- Incorporates Container Linux
  - Philosophy
  - Provisioning Stack
  - Cloud Native Expertise
- Incorporates Atomic Host
  - Fedora Foundation
  - Update Stack
  - SELinux Enhanced Security
Philosophy behind Container Linux

• 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
Fedora CoreOS Features
Features: Automatic Updates

• Fedora CoreOS features Automatic Updates by default
  o 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
  o For when things go wrong
    ■ rpm-ostree rollback can be used to go back
    ■ future: automated rollback
      • based on user specified health checks
Multiple Update Streams

• Offered update streams with automatic updates
  ○ **next** - experimental features, Fedora major rebases
  ○ **testing** - preview of what’s coming to stable
    ■ point in time snapshot of Fedora stable rpm content
  ○ **stable** - most reliable stream offered
    ■ promotion of testing stream after some bake time

• Goals
  ○ Publish new releases into update streams every two weeks
  ○ Find issues in next/testing streams before they hit stable
Fedora CoreOS Release Promotion

Release Nomenclature

1) OS content is snapped by date
e.g. 20200323

Fedora rpmbdb

2) Releases are promoted to testing & reflect the rpmbdb date
e.g. 31.20200323.2.0

Testing Stream

~2 week promotion

3) Testing is then promoted to stable & shows the same rpmbdb date
e.g. 31.20200323.3.0

Stable Stream
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
Ignition: Details

Ignition configs
- Declarative JSON documents provided via user data
- Runs exactly once, during the initramfs stage on first boot
- Can write files and systemd units, create users and groups, partition disks, create RAID arrays, format filesystems
- If provisioning fails, the boot fails (no half provisioned systems)
- Ignition configs are machine-friendly (JSON), currently spec v3

Writing Configs
- Fedora CoreOS Config Transpiler to translate to Ignition spec
  - Confis are Human friendly (YAML)
  - Ignition semantics, plus sugar for common operations
  - Transpiler catches common errors at build time

```json
{
  "ignition": {
    "config": {},
    "timeouts": {},
    "version": "3.0.0"
  },
  "passwd": {
    "users": [
      {
        "name": "core",
        "passwordHash": "$6$43y3tkl...",
        "sshAuthorizedKeys": [
          "key1"
        ]
      }
    ],
    "storage": {},
    "systemd": {}
  }
}
```
Features: Cloud Native & Container Focused

- Software runs in containers
  - podman or moby engine container runtimes
- Ready for clustered deployments
  - Spin up 100 nodes and have them join a cluster
    - Ignition configs used to automate cluster join
  - Spin down nodes when no longer needed
  - Spin up nodes again when load increases
- Offered on (or for) a plethora of cloud/virt platforms
  - Alibaba, AWS, Azure, DigitalOcean, Exoscale, GCP, Openstack, Vultr, VMWare, QEMU/KVM
Features: OS Versioning & Security

• Fedora CoreOS uses rpm-ostree technology
  ○ “Like git for your Operating System”
    ▪ 32.20200615.2.0 - 86c0246
    ▪ A single identifier tells you all software in that release
  ○ Uses read-only filesystem mounts
    ▪ Prevents accidental OS corruption (rm -rf)
    ▪ Prevents novice attacks from modifying system
• SELinux enforcing by default
  ○ Prevents compromised apps from gaining further access
What’s in the OS?

- Latest Fedora base components (built from RPMs)
- Hardware support
- Basic administration tools
- Container engines: podman, moby
- No python
Fedora CoreOS used in Other Projects

- **OKD**
  - Cluster controls OS upgrades with machine-config-operator
  - Upgrades are provided as machine-os-content containers
    - includes Fedora CoreOS + cluster dependencies
  - Cluster can manage and bring up new machines automatically
- **Typhoon**
  - Base OS option for community typhoon k8s distribution
- **OpenStack Magnum**
  - Base OS for the Magnum project that delivers kubernetes to Openstack users.
Fedora CoreOS and RHEL CoreOS

Common tooling & components - different scope and purpose

• RHEL CoreOS is not intended as a standalone OS
  • Based on RHEL package set
  • Component of OpenShift
  • Updates and configuration controlled by cluster operators

• Fedora CoreOS
  • Based on Fedora package set
  • Shares components and tooling with RHEL CoreOS
  • Standalone OS with auto-updates
What’s Next
What’s Next

• More Cloud Platforms
• Multi-arch support (aarch64, ppc64le, s390x)
• More FCCT human friendly helper functions
• Host extensions (more reliable package layering)
• More/improved documentation
• Tighter integrations with OKD
Get involved!

- Web: https://getfedora.org/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
Questions
Demo
Thank you!