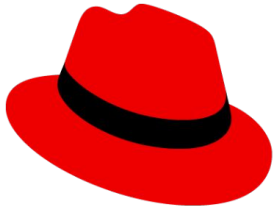
Linaro Connect
MADRID 2024 | MAY 14-17 2024

Leveraging Atomic Updates with OSTree for Automotive

Eric Curtin @ecurtin@treehouse.systems

Red Hat In-Vehicle Operating System

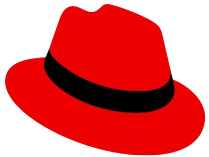
- Red Hat In-Vehicle Operating System provide an open and secure Linux-based foundation for software-defined vehicles.
- We can think of it as Red Hat Enterprise Linux for vehicles.



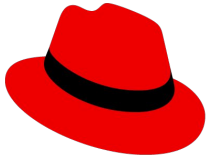
Red Hat
In-Vehicle
Operating System

OSTree

- OSTree is an update system for Linux-based operating systems that performs atomic updates of complete filesystem trees.
- Related project for handling rpms with OSTree, rpm-ostree, not covered here.
- As seen in:



Red Hat Enterprise Linux CoreOS



Red Hat Device Edge

Red Hat In-Vehicle Operating System

- Image-based operating system
- AB updates
- Atomic (transactional) updates, rollbacks
- Health-checking
- Automated rollbacks
- OTA (over-the-air) updates
- Immutability
- Integrity protection
- Tamper protection
- Secure boot

Package based vs Image based updates

Package based

- Runs install scripts on the client
- Non-deterministic installs/rollbacks
- No firmware/bootloader level rollbacks available
- Initramfs/rootfs cannot be secured with server-side signatures
- Only day-0 install can be accurately tested
- Package-based delta updates
- Does not require a reboot to update

Package based vs Image based updates

Package based

- Runs install scripts on the client
- Non-deterministic installs/rollbacks
- No firmware/bootloader level rollbacks available
- Initramfs/rootfs cannot be secured with server-side signatures
- Only day-0 install can be accurately tested
- Package-based delta updates
- Does not require a reboot to update

Image based

- Runs install scripts on the build server
- Deterministic installs/rollbacks
- Firmware/bootloader level rollbacks available
- Initramfs/rootfs can be secured with server-side signatures
- Installs that have gone through update cycles can be accurately tested
- Image-based delta updates, less bandwidth used
- Requires a reboot to update

Greenboot

- Health-checking framework
- Can mark a boot as healthy/unhealthy (green/red)
- Based on boot counters
- The bootloader or firmware stores a boot counter, if a device fails to boot X amounts of times we rollback

Composefs

- An opportunistically sharing verified image filesystem
- Content sharing results in:
  - efficient storage usage
  - low number of OTA bytes transferred
- Utilizes fs-verity for integrity protection
- Extends secure boot chain of trust from initramfs to rootfs
- Utilizes erofs to provide a read-only content store

Directories

/ is read-only (composefs)

/var is read-writable

/etc is a transient writable overlayfs over a base default /etc

Other directories are symlinks to these ones, examples from /:

srv -> var/srv

mnt -> var/mnt

OTA updates

Publish an OSTree server

On the build server:

- Build an OSTree repo using Automotive Image Builder
- Publish this repo using a http server

On the vehicle:

- Run “rpm-ostree upgrade”
- Reboot

Static Deltas (using existing OTA transport)

On the build server:

- Generate a static delta using “ostree static-delta generate”
- Deliver the file using existing OTA transport

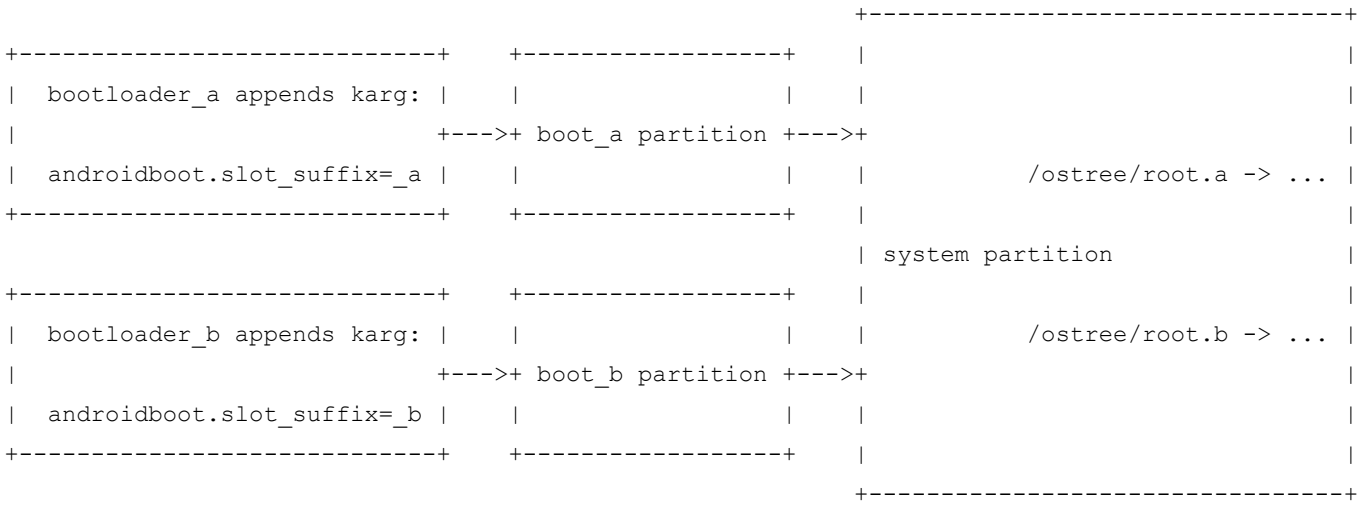
On the vehicle:

- Apply the static delta “ostree static-delta apply-offline”
- Run “rpm-ostree rebase”
- Reboot

AB updates

- Some ARM boards apply AB updates down to the lower levels of the software stack at the firmware or bootloader level.
- In these partitions, not even filesystems exist.
- OSTree may be used to handle updates at this level.

From AB partitions to composefs



Automotive Image Builder

```
# automotive-image-builder --container build
  images/minimal.mpp.yml --export qcow2 --target qemu vm.qcow2
```

- Wrapper around podman (with --container) and osbuild
- Can compose images for aarch64 and x86_64

Other build techniques:

https://sigs.centos.org/automotive/building/

Automotive Image Runner

```
# automotive-image-runner --nographics vm.qcow2
```

- This script was formerly named runvm
- Wrapper around qemu
- Runs vms and emulators
- Works on Linux/macOS
- We also have OCI containers, etc.

Contacts (for more information)

Automotive documentation: https://sigs.centos.org/automotive/

Automotive mailing list: centos-automotive-sig@centos.org

Automotive SIG Matrix: https://matrix.to/#/#centos-automotive-sig:fedoraproject.org

Fedora Atomic Desktop SIG Matrix: https://matrix.to/#/#atomic-desktops:fedoraproject.org

GitLab: https://gitlab.com/CentOS/automotive

Linaro Connect
MADRID 2024 | MAY 12-17 2024

Thank you