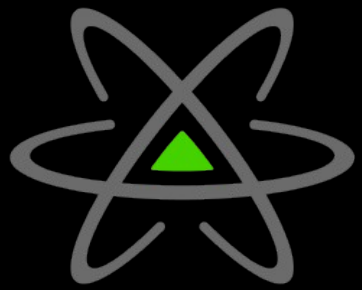


Introduction to Atomic: Tailoring a Trusted OS for Containers

Joe Brockmeier
jzb@redhat.com
@jzb

Introduction

- What is Project Atomic?
- Anatomy of an Atomic Host
- Coming Soon
- Getting Involved

PROJECT ATOMIC

(I don’t need to explain containers, right? Good.)

PROJECT ATOMIC

What is Project Atomic?

PROJECT
ATOMIC

Project Atomic 101

- Upstream community for developing tools and patterns for developing Atomic hosts.
- Umbrella project for Red Hat's efforts around developing, building, running, and managing containers.
- *Not* a new distribution – Atomic Hosts are built from CentOS, Fedora, or Red Hat Enterprise Linux.

PROJECT ATOMIC

Why Atomic?

- We can run Linux containers on CentOS, Fedora, and RHEL already!
- Provide a streamlined host optimized for running and managing containers.
- All applications should be deployed as containers, rather than installing on the host.
- Host should be “cattle” and updates should be easy to deploy and manage.

PROJECT ATOMIC

What Atomic Hosts Provide

- Streamlined host based on CentOS, Fedora, or RHEL packages + container stack.
- rpm-ostree
- /usr/bin/atomic
- Docker
- Kubernetes
- Cockpit
- Super Privileged Containers (SPC)

PROJECT ATOMIC

What Atomic Hosts Won't Provide

- Atomic hosts are "immutable" – don't expect to install packages on running systems
- Official images are **minimal** – that means your favorite tool probably won't be added
  - *Aside from Atomic development or troubleshooting, you should never be logged into an Atomic Host*
- More than necessary

PROJECT ATOMIC

CentOS, Fedora, or RHEL?

- Aside from rpm-ostree, all of the components that make up an Atomic Host are shared w/the parent distribution.
- You want support? Go RHEL Atomic Host.
- CentOS Atomic is currently under development, and hasn't released any “official” images.
- Fedora 21 released in December – developed by the Cloud Working Group.
- A CentOS rebuild of RHELAH is coming soon.

PROJECT ATOMIC

rpm-ostree's history

- OStree initially developed for GNOME continuous by Colin Walters
- The rpm-ostree stuff came slightly later
- "Git for operating systems"
  - bootable, immutable, & versioned filesystem trees
  - works on top of any *nix filesystem
  - support for UID/GID, extended attr, handling bootloader, and more.

PROJECT ATOMIC

Why rpm-ostree?

- “Atomic” updates make more sense for an immutable system
- Preserves the tooling to create packages, allows re-use of RPMs rather than re-inventing the wheel
- Easy rollback in the event you need to return to known-good tree
- Clean transaction for updates

PROJECT ATOMIC

How rpm-ostree works (high level)

- Filesystem is read-only, except /var and /etc
- /etc is 3-way merged when you do an update
- All data (e.g. containers) is unchanged on upgrade
- Problem with an upgrade? `rpm-ostree rollback`

PROJECT ATOMIC

/usr/bin/atomic

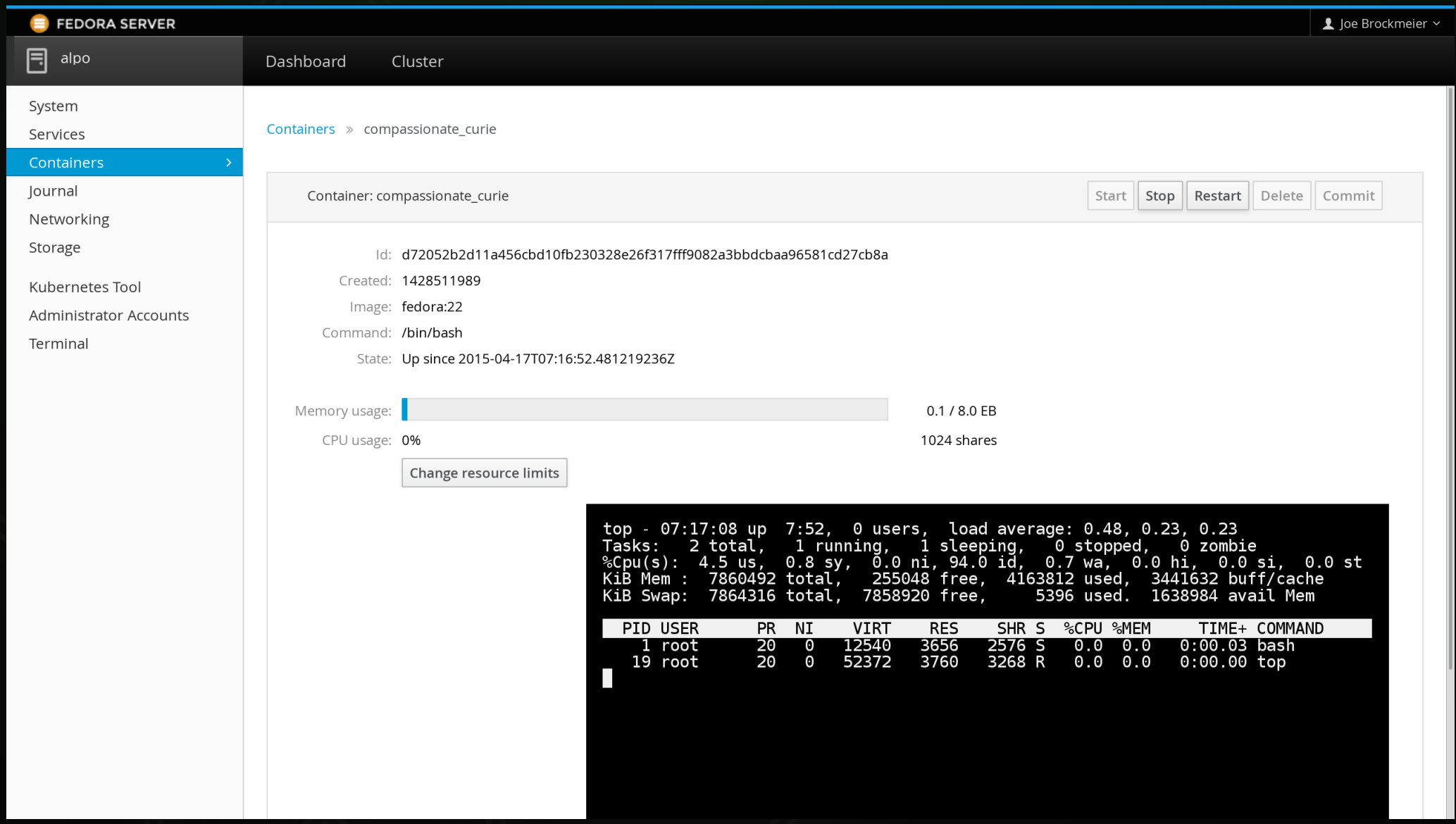
- Coherent entry point to the system: manage host and containers with the atomic command.
- Fill gaps in Linux container implementations.
  - *e.g.* “atomic install foo” can install a container with its k8s configuration and/or systemd unit file.
  - “atomic run” grabs the LABEL “run” with its Docker cmd line. Saves the user much typing.
- The “atomic host” command can be used for rpm-ostree updates.

PROJECT ATOMIC

Cockpit

- Cockpit started prior to Atomic
- Server manager for administering Linux servers via the Web browser
- Doesn't interfere with normal admin tools
- Designed to be multi-server
- Support for managing containers, Kubernetes
- http://cockpit-project.org/

PROJECT ATOMIC



PROJECT ATOMIC

Changes to ’docker search’ & ’docker pull’

- We *mostly* ship vanilla Docker
- Additional registries for 'docker search' & 'docker pull'
- We add the RHEL registry to grab official RHEL content*
- Docker search lists fully qualified image name
- Ability to block registries
- Can warn on “push” to ensure private images aren't pushed to public registry

PROJECT ATOMIC

Super-Privileged Containers (SPC)

- We mean it when we say “run everything in containers” on Atomic
- Usually containers have limited interaction w/the host
- SPC containers can be run with `atomic run` which saves the need for long docker commands to enble privileges

PROJECT ATOMIC

Shipping Super-Privileged Containers (SPC)

- RHEL Atomic Tools Container Image – debugging tools like strace, traceroute, man pages, etc. needed to troubleshoot an image.
- RHEL Atomic rsyslog Container Image – runs rsyslogd service to send logs to central server, etc. (journald collects data either way)
- RHEL Atomic sadc Container Image – runs sadc from sysstat to be used w/`sar`
- More to come!

PROJECT ATOMIC

Nulecule (in early development)

- Specification for multi-container application w/dependencies (“Atomic App”)
- Lets developer describe application, sysadmin define parameters for app at runtime
- Creates super-orchestration parameters for Kubernetes
- Defines on-demand scheduling of resource utilization
- Basis for policy-based orchestration via Mesos
- Supports Docker, ACI and potentially other container formats
- github.com/projectatomic/nulecule

PROJECT ATOMIC

Kubernetes

- Initially used GearD from OpenShift, phased out in favor of Kubernetes
- Working with upstream to improve / develop Kubernetes for container management

PROJECT ATOMIC

Pulling the Pieces Together

PROJECT ATOMIC

Fedora Atomic Hosts

- Work is being done through the Cloud Work Group & will be part of the Cloud Product
- First release in Fedora 21
- Adding new image formats in Fedora 22, updated Cockpit, etc.
- Moving to 2-week release cycle based on Rawhide or -current soon

PROJECT ATOMIC

CentOS 7 Atomic Hosts

- Work is being done through CentOS Atomic SIG
- CentOS-based Atomic Hosts are still in development, working out a few details like signing
- Will be providing a rebuild of RHEL Atomic Host soon
- CentOS SIG / Project Atomic will be providing a faster-moving release with packages in development soon

PROJECT ATOMIC

Getting Involved

- Website: projectatomic.io
- Github: github.com/projectatomic
- Facebook.com/projectatomic
- Twitter: @projectatomic
- Mailing Lists:

  http://www.projectatomic.io/community/

PROJECT ATOMIC

Thank you!

jzb@redhat.com
Twitter: @jzb
@projectatomic

PROJECT ATOMIC