Stateless Provisioning: Modern Practice in HPC

Leveraging Systemd, Ansible, and CI practices to provide policy compliant OS images for computational clusters

John Blaas
University of Colorado Boulder

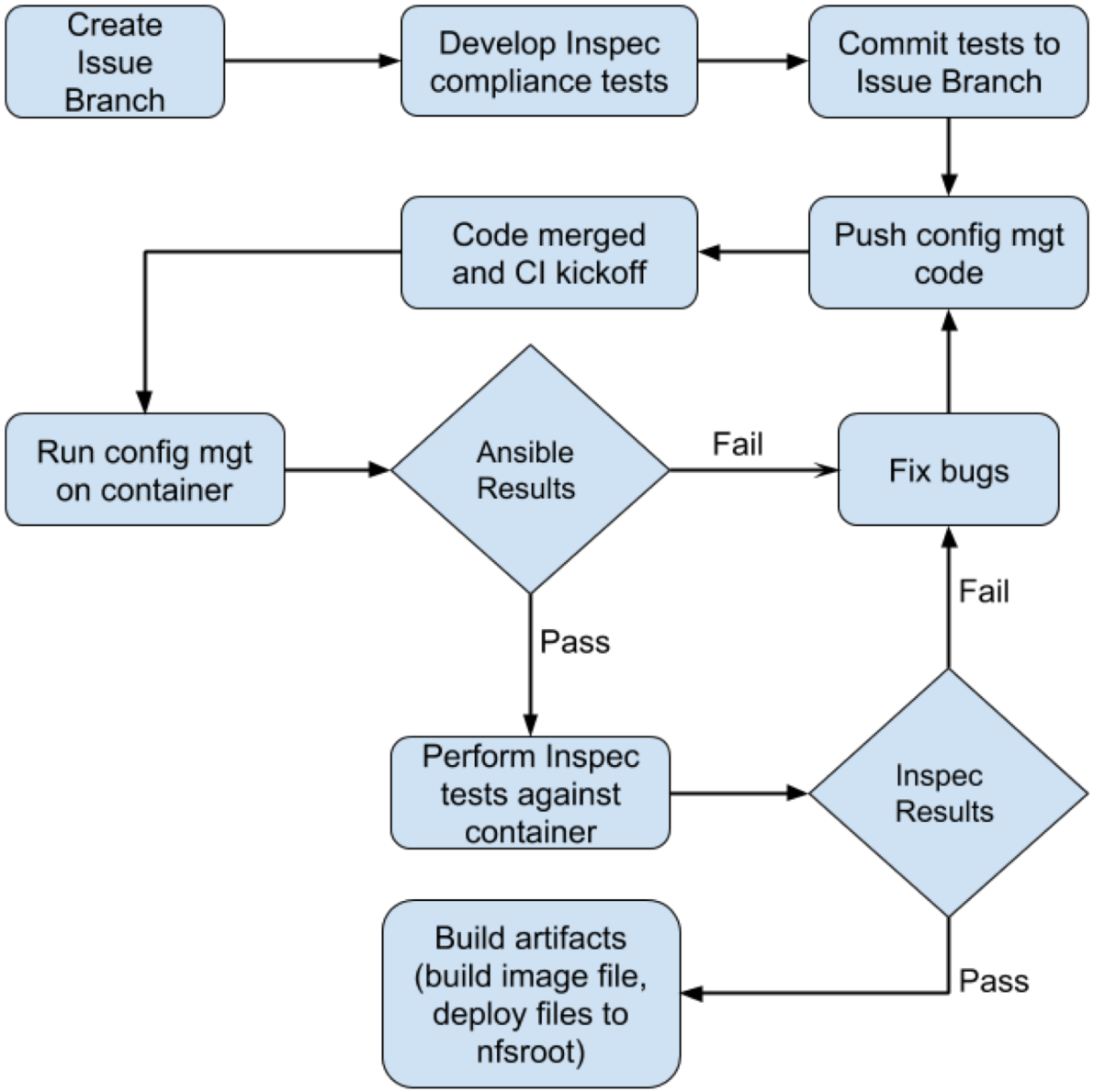
John Roberts
Argonne National Laboratory

Where we started

- OS image/directories as git repos
  - Worked well but can lead to fairly unwieldy git repos
  - Can’t be shared with others
  - Secrets in the repo
- Used chroot to apply updates and configuration against the image directories
  - For some updates this also required us to bind mount certain filesystems from the host OS as well
- Very little testing after an image had been built - relied on deploying an image to staging hardware first to reveal any issues.

Motivation

- Incorporate tests to verify the ultimate state of an image, strictly define our computing environment through these tests
- Provide stakeholders with better reports and audits of the environment we provide to users
- Lower barrier of entry for new system administrators in being able to contribute to the code base, configuration changes


Create Issue Branch
Develop Inspec compliance tests
Commit tests to Issue Branch
Push config mgt code
Code merged and CI kickoff
Run config mgt on container
Ansible Results
Fail
Fix bugs
Pass
Fail
Perform Inspec tests against container
Inspec Results
Build artifacts (build image file, deploy files to nfsroot)
Pass

What is systemd-nspawn?

- Improved chroot, no need to bind mount the usual suspects
- Tool that spawns unique namespaces
- Designed with building, testing, and debugging in mind
- Incredibly simple to get started with

```
> rpm -i --root=/tmp/centos7 centos7-release.rpm
> yum --installroot=/tmp/centos7 groupinstall Base
> systemd-nspawn -bD /tmp/centos7
```

What is Inspec?

- Compliance testing framework based on Serverspec
- Designed to have clear syntax and be platform agnostic
- Describes tests as a collection of controls which can be grouped into compliance profiles
- Allows you to define policy for the state of a node
- Tests can be run locally or with SSH
- Originally developed by the Chef team

Future Work

- Developing tests that can be used to train new system administrators in configuration management and where/how to define variables
- Publish Inspec compliance profiles that help define our computing environment
- Expose `group_vars` to condo node users so that they can have the option to self-manage their environment

Why not use X instead?

- You can substitute out the initial provisioning element to something else such as xCat, Warewulf, or your own custom provisioning framework.
- You can also use many other tools such as Cobbler, Foreman,etc to help you with managing DHCP,PXE,DNS
- You can even substitute out Inspec for another testing framework (Molecule, Testinfra, Goss)

Software we use

OS: Centos7 or RHEL7

Resource Manager: Slurm

Node Health Check: NHC

Git Repos: Gitlab-ce

Gitlabrunner: CI Runner

Config Mgmt: Ansible

Compliance Tests: Inspec