Docker on Shared Linux Systems: Mitigating Risk

Scott Nolin

6/22/2017

Docker Users = root (scary root)

Worse because it can’t be audited like sudo, and users can run commands and cause havoc by accident.

But people want it, it will happen.

How to (politely) own a docker system

docker run -v /etc:/work -t alpine /bin/sh -c 'echo "scottn ALL=(ALL) NOPASSWD:ALL" > /work/sudoers.d/scottn_test‘

Congratulations, you’re root!

But all users are trusted!

- Consider accidental damage. Do you have other filesystems mounted?

But . . . SELinux!

- They fixed that as a bug:

https://github.com/docker/compose/issues/643

Add support for :z and :Z to change SELinux labels on the fly

Unless I misunderstand (I might) – this means users get a free and easy ‘chcon’

User Namespaces to the rescue (except…)

- Defeated with `--userns=host`
- Docker supports authorization plugins that could disable that. Some do exist, another layer of software you must manage and run as a service. Example: https://github.com/vancluever/docker-denyusernshost

Thoughts?