DOCKER ADVANCED FEATURES

ANTONIO MURDACA

Associate Software Engineer

Docker Core maintainer

Twitter: @runc0m (that is a zero, damn)

Email: runcom@redhat.com

NOT GOING TO TALK ABOUT ...

`docker run`

containers orchestration

USER NAMESPACES

Processes inside containers run (mostly) as **root**

Daemon option: `--userns-remap=default`

```
$ cat /etc/subuid
dockremap:100000:65536 # root is UID 100000 outside the container
```

The same applies to GIDs

USER NAMESPACES: THE BAD

https://docs.docker.com/engine/reference/commandline/daemon/#user-namespace-known-restrictions

No containers with `--privileged` (WIP)

Not per container

Lack of filesystem support

```
echo 1 > /proc/sys/kernel/userns_restrict
```

PLUGINS

Docker has a generic Plugin API (RPC-style JSON over HTTP)

Plugins are *discovered* (usually by name)

Configure Docker to use plugin e.g. `--authorization-plugin=$NAME`

Plugins implements a given API - see github.com/docker/go-plugins-helper

PLUGINS TYPES

Volumes

Network

Authorization

Authentication (yet to come)

https://github.com.com/docker/go-plugins-helpers

LOGGING DRIVERS

json file, syslog, splunk, journald, gelf, gcp, fluentd, etw, aws, amqp (coming), windows (coming) ... WHAT?

Pluggability?

SECURITY PROFILES

Seccomp, Apparmor

SELINUX

The best security measure (I might be biased)

`setenforce 0` (http://stopdisablingselinux.com/)

THAT'S ABOUT IT
THANKS!