Securing Docker on the Cheap

Part 1 - Fundamentals

fork(4)

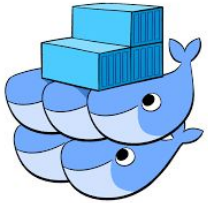
About Me

- Possessor of many hats
- Currently at LO3 Energy
- Formerly of Autodesk
- This talk brought to you by the letter ‘A’

But first....

The whale in the room

Orchestration platform agnostic



MESOSPHERE

DC/OS

Amazon ECS

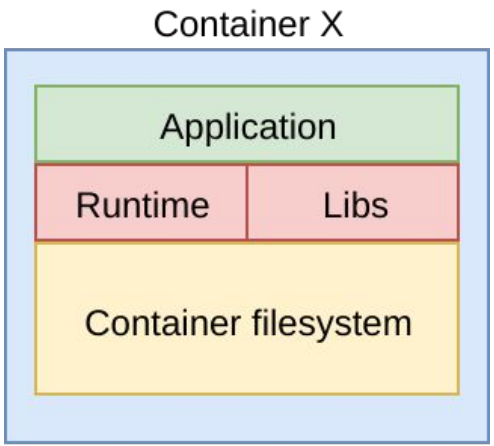
No experience required.

Docker 101

What is a container?

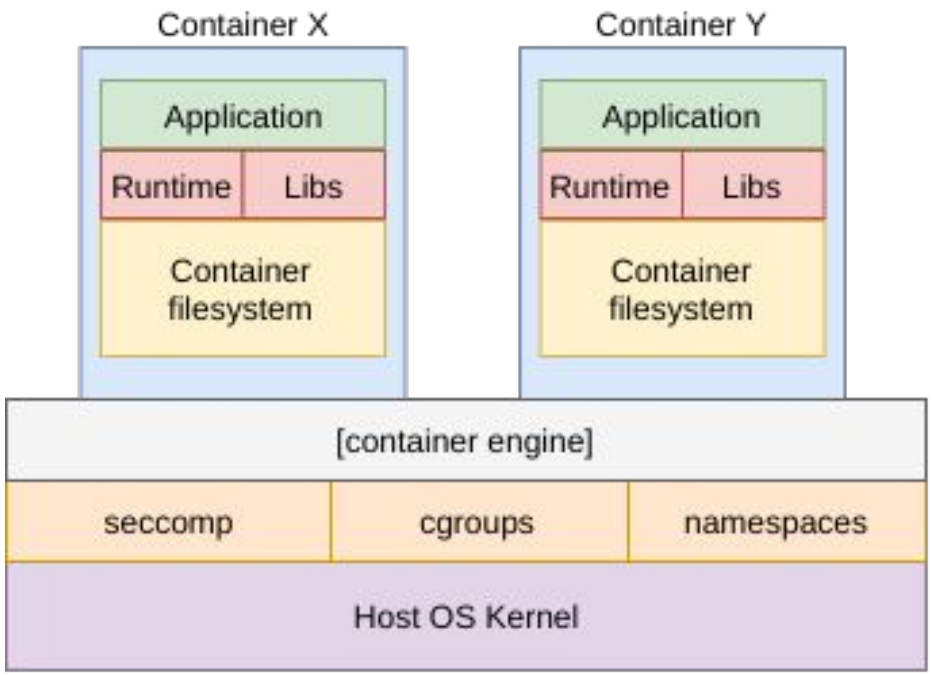
Perfect Packaging

- Everything needed for execution of the container is packaged together
  - Application code
  - Runtime environment
  - Dependency libraries
  - Even root filesystem
- Container “package” can be delivered to any host capable of executing that container



Intrinsic Isolation

- Pseudo-virtualization
- Isolated resources on top a of shared host kernel
- Container engine (LXC, Docker, etc.)
- Leverages control groups for resource allocation
- Namespaces provide isolation
- Has roots in chroot and FreeBSD jails



Why Docker?

Containers made easy

Adoption

Security Fundamentals

First...

Service Containers
vs
Tool Containers

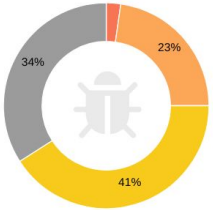
Security Starts at the Top

Sample Dockerfile

```
FROM ubuntu:16.04

RUN apt update && apt upgrade -y && apt install -y curl && \
   curl -sL https://deb.nodesource.com/setup_8.x | bash - && \
   apt install -y nodejs
EXPOSE 3000

ADD app.js /var/app/
ADD package.json /var/app/

WORKDIR /var/app
RUN npm install

CMD ["/usr/bin/node", "app.js"]
```


Know your FROM

Security scan of ubuntu:16.04



Quay Security Scanner has detected **44** vulnerabilities.

Patches are available for **5** vulnerabilities.

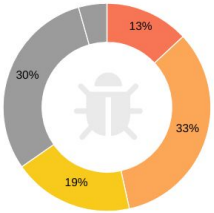
- **1** High-level vulnerabilities.
- **10** Medium-level vulnerabilities.
- **18** Low-level vulnerabilities.
- **15** Negligible-level vulnerabilities.

Image Vulnerabilities

Filter Vulnerabilities... | Only show fixable

CVE	SEVERITY	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN IMAGE
CVE-2018-10000	High	glibc	2.23-0ubuntu10	(None)	ADD file:4c266e490f4101f9726598...
CVE-2017-8804	7.8 / 10	glibc	2.23-0ubuntu10	(None)	ADD file:4c266e490f4101f9726598...
CVE-2016-1238	7.2 / 10	perl	5.22.1-9ubuntu0.2	(None)	ADD file:4c266e490f4101f9726598...
CVE-2018-6485	Medium	glibc	2.23-0ubuntu10	(None)	ADD file:4c266e490f4101f9726598...
CVE-2016-1585	Medium	apparmor	2.10.95-0ubuntu2.9	(None)	ADD file:4c266e490f4101f9726598...
CVE-2018-6913	Medium	perl	5.22.1-9ubuntu0.2	5.22.1-9ubuntu0.3	ADD file:4c266e490f4101f9726598...

Security scan of node:9.11.1



Quay Security Scanner has detected **634** vulnerabilities.

Patches are available for **6** vulnerabilities.

- **83** High-level vulnerabilities.
- **212** Medium-level vulnerabilities.
- **119** Low-level vulnerabilities.
- **192** Negligible-level vulnerabilities.
- **28** Unknown-level vulnerabilities.

Image Vulnerabilities

Filter Vulnerabilities... | Only show fixable

CVE	SEVERITY	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN IMAGE
CVE-2017-17458	10 / 10	mercurial	3.1.2-2+deb8u4	(None)	RUN apt-get update && apt-get i…
CVE-2017-18017	10 / 10	linux	3.16.51-3+deb8u1	(None)	RUN set -ex; apt-get update; ap…
CVE-2016-4448	10 / 10	libxml2	2.9.1+dfsg1-5+deb8u6	(None)	RUN set -ex; apt-get update; ap…
CVE-2015-1418	9.3 / 10	patch	2.7.5-1	(None)	RUN set -ex; apt-get update; ap…
CVE-2017-16997	9.3 / 10	glibc	2.19-18+deb8u10	(None)	ADD file:bc844c4763367b5f0ac7b9…
CVE-2016-3857	9.3 / 10	linux	3.16.51-3+deb8u1	(None)	RUN set -ex; apt-get update; ap…

Creating a Custom Base Container

Rules for a Quality Custom Base

- Starting tiny is better
- Patch as part of the build
- Build a shared service base
  - Install common tools
  - Install base runtime
- Leave the application specifics for downstream containers
- Leverage any hardening standards/tools for the OS
- Install only what you need
- Leave build tools on build containers

Pro-tip: `docker run -it [base-image]:[tag] /bin/sh` to experiment

Scratch Containers

- Docker images can be derived from tarballs
- Docker containers need a filesystem
- ...but that does not need to be a full base OS filesystem
- Docker images can be built directly
- `FROM scratch`
- Statically-linked executables (like Go) can be built directly into Docker images

Capabilities

Removing Capabilities

```
docker run --cap-drop SETUID --cap-drop CHOWN ubuntu
```

Adding Capabilities

```
docker run --cap-add RAW_IO
```

https://github.com/moby/moby/blob/master/oci/defaults.go

```go
func defaultCapabilities() []string {
    return []string{
        "CAP_CHOWN", "CAP_DAC_OVERRIDE", "CAP_FSETID",
        "CAP_FOWNER", "CAP_MKNOD", "CAP_NET_RAW",
        "CAP_SETGID", "CAP_SETUID", "CAP_SETFCAP",
        "CAP_SETPCAP", "CAP_NET_BIND_SERVICE",
        "CAP_SYS_CHROOT", "CAP_KILL", "CAP_AUDIT_WRITE",
    }
}
```

Secure Computing Mode (seccomp)

https://github.com/moby/moby/blob/master/profiles/seccomp/default.json

```
{
   “defaultAction”: “SCMP_ACT_ERRNO”,
   “archMap”: [],
   “syscalls: [
      {
         “names”: [ “chdir”, “chmod”, … ],
         “action”: “SCMP_ACT_ALLOW”,
         “args”: [],
         “comment”: “”,
         “includes”: {},
         “excludes”: {}
      }
   ]
}
```

```
docker run --security-opt
seccomp=/path/to/profile.json ubuntu: 16.04
```

Immutable Containers

```
docker run --read-only \
--tmpfs /tmp:rw,noexec,nosuid \
-v /host/path:/app/workdir [image]
```

Control Groups (cgroups)

Ok, what are control groups?

Docker && cgroups

Some cgroup Options

```
--cpu*
--blkio*
--device*
--memory*
```

https://docs.docker.com/engine/reference/commandline/run/#options

Other Tips

Don’t run as root

Avoid `--privileged`

Be intentional

Wrap-up

https://github.com/fork4/lfnw2018