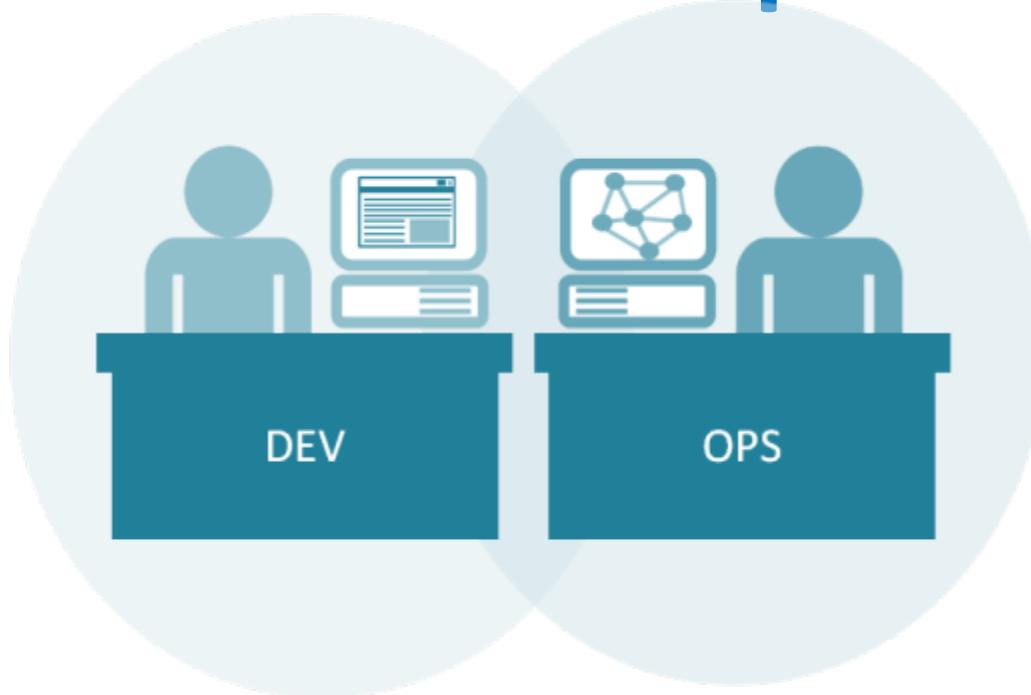


Docker

Container Implementation

Boot Camp



Welcome!

Logistics (breaks,
facilities, lunch, etc.)

Rules of Engagement

Introductions

Let's Get Started!

Instructor Information



Who is your instructor?
A little about me...

Introductions

What is your
Name and
Job Role?

Your
company or
team?

Expectations
for the class?

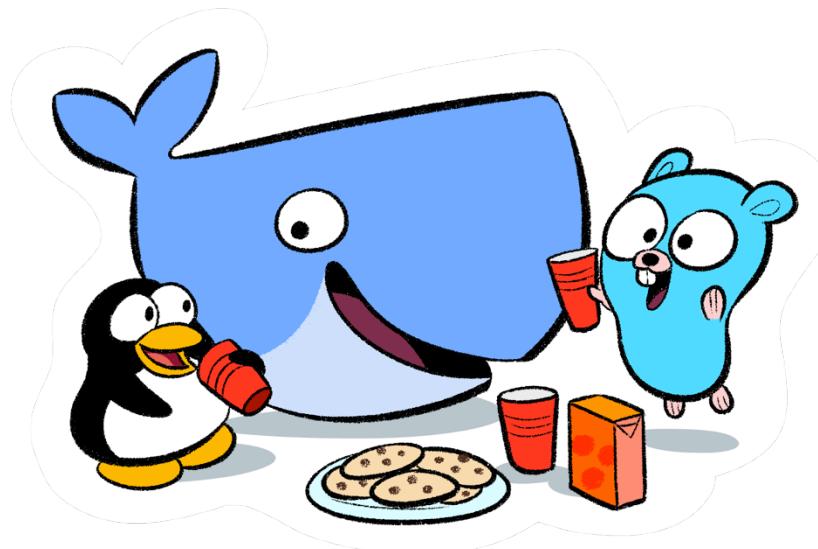
Something
interesting
about
yourself?

What to expect from this class

- Flexibility
- Conversations
- Literacy and awareness on many of the principles, tools, and practices surrounding Docker as part of a DevOps architecture.
- An effort to focus on your own situations and challenges so you can act on what you learn.

Part 1: DevOps Docker

Introduction to Docker



What is Docker?

The Docker Project

Open Source Project

- 2B+ Docker Image Downloads
- 2000+ contributors
- 40K+ GitHub stars
- 200K+ Dockerized apps
- 240 Meetups in 70 countries
- 95K Meetup members

Docker Inc

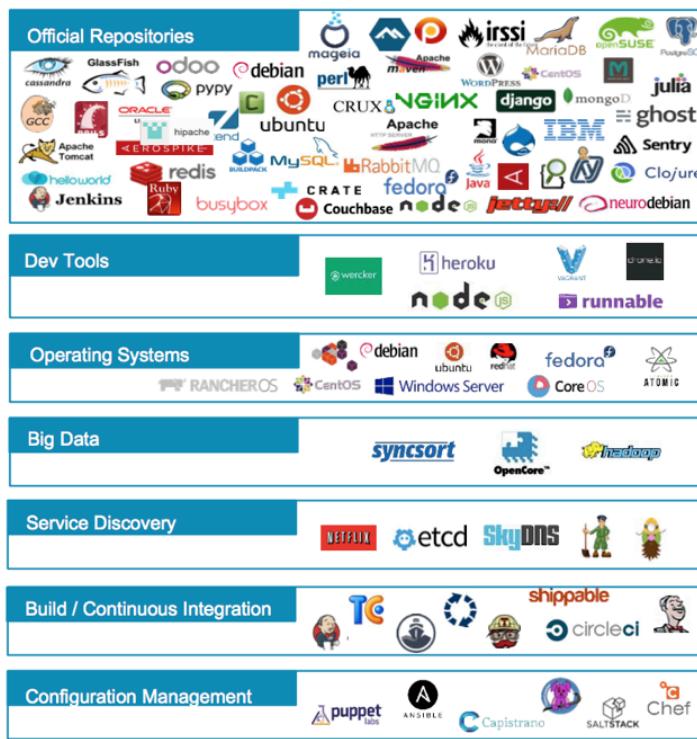
Containers as a Service provider

- Integrated platform for dev and IT
- Commercial technical support

Docker project sponsor

- Primary sponsor of Docker project
- Supports project maintainers

Docker ecosystem

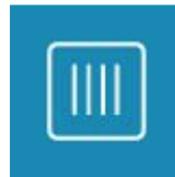


Docker Basics



Docker Image

- The basis of a Docker container



Docker Container

- The standard unit in which the application service resides



Docker Engine

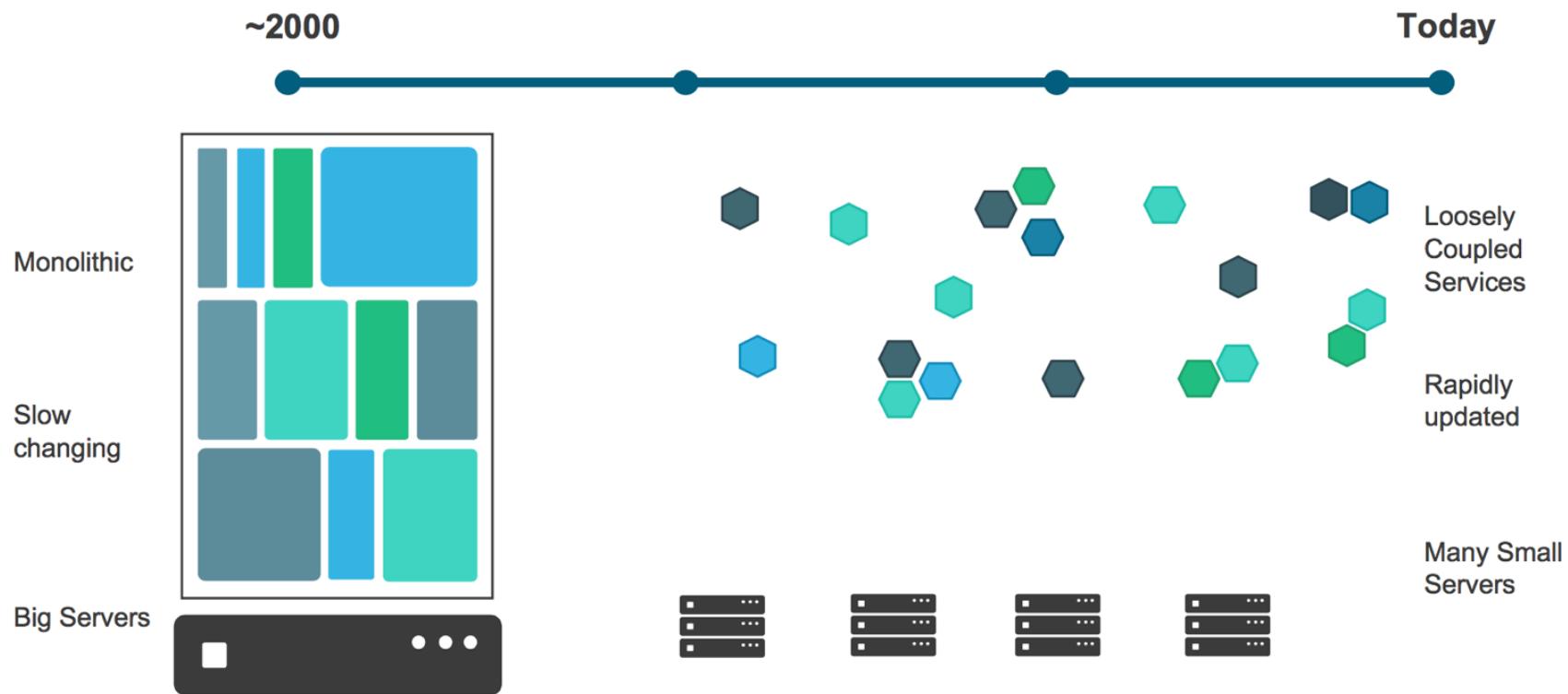
- Creates, ships and runs Docker containers deployable on physical or virtual host locally, in a datacenter or cloud service provider



Docker Registry

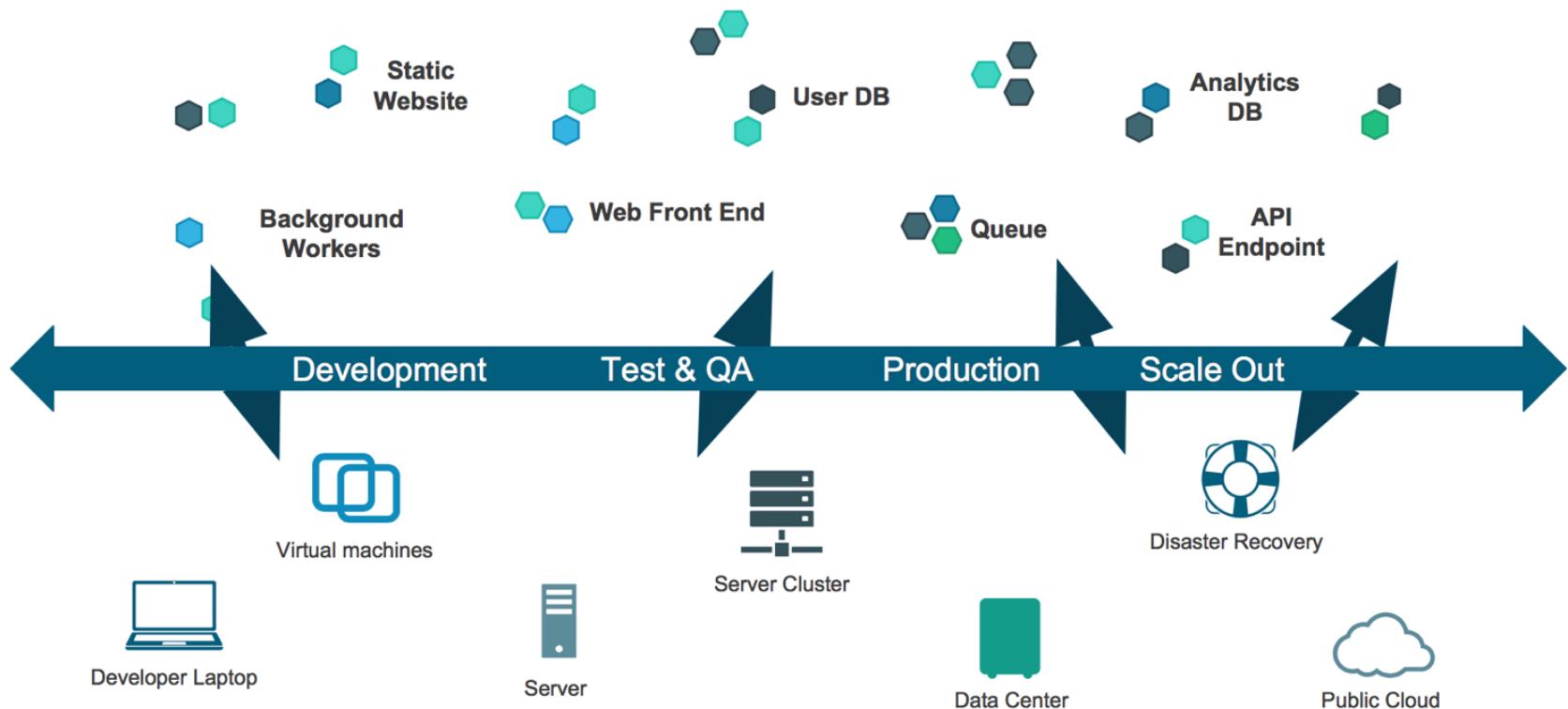
- On-premises registry for image storing and collaboration

Application Evolution



Challenge: The Dependency Matrix

“It works on MY machine.”



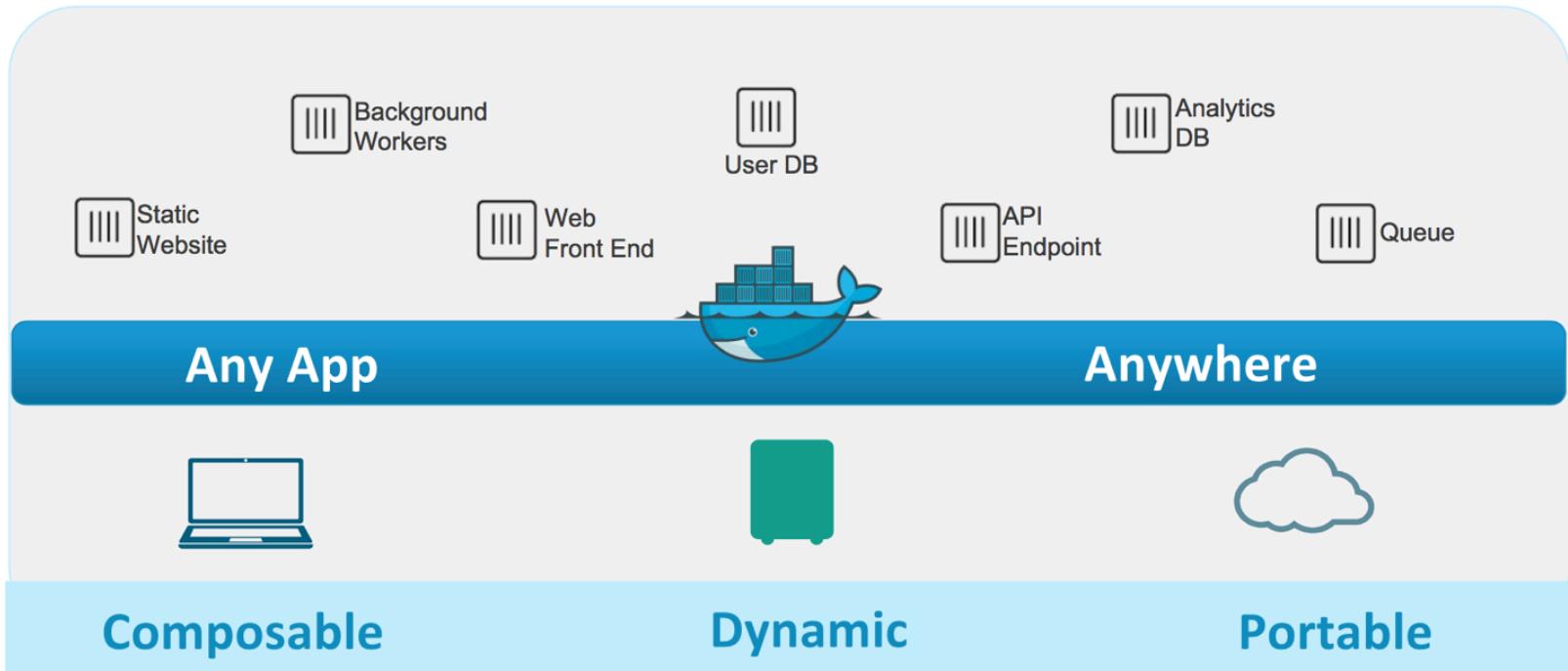
Containers as a Solution



Container

- Packages up software binaries and dependencies
- Isolates software from each other
- Container is a standard format
- Easily portable across environment
- Allows ecosystem to develop around its standard

Containers as a Solution



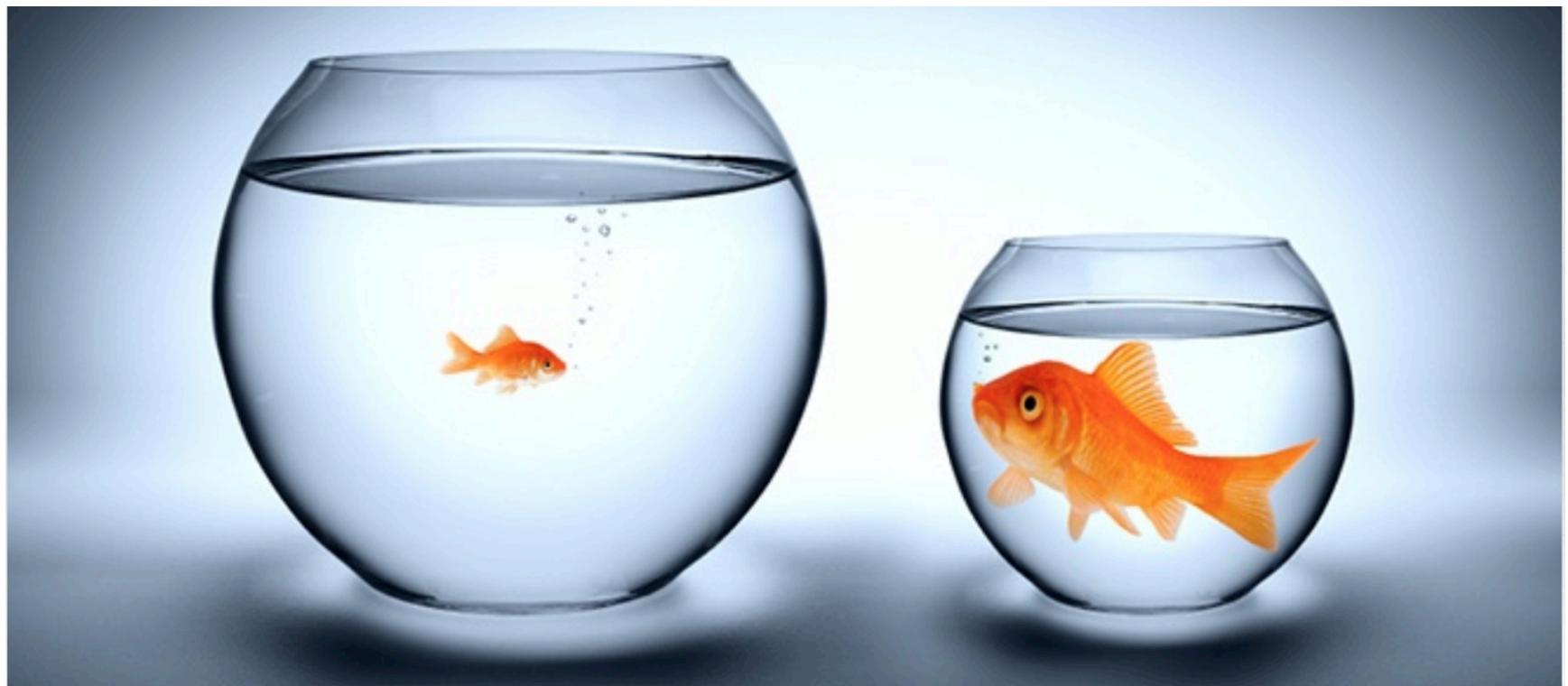
Developer Benefits

- Build once... (finally) run anywhere
 - A clean, safe, hygienic and portable runtime environment for your app.
 - No worries about missing dependencies, packages and other pain points during subsequent deployments.
 - Run each app in its own isolated container, so you can run various versions of libraries and other dependencies for each app without worrying
 - Automate testing, integration, packaging... anything you can script
 - Reduce/eliminate concerns about compatibility on different platforms, either your own or your customers.
 - Cheap, zero-penalty containers to deploy services? A VM without the overhead of a VM? Instant replay and reset of image snapshots? That's the power of Docker

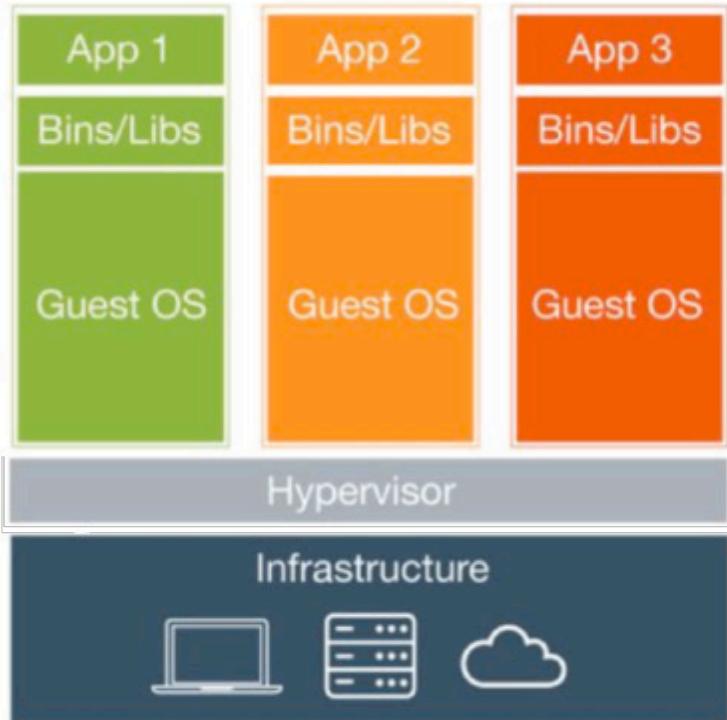
Operational Benefits

- Configure once...run anything
 - Make the entire lifecycle more efficient, consistent, and repeatable
 - Increase the quality of code produced by developers.
 - Eliminate inconsistencies between development, test, production, and customer environments
 - Support segregation of duties
 - Significantly improves the speed and reliability of continuous deployment and continuous integration systems
 - Because the containers are so lightweight, address significant performance, costs, deployment, and portability issues normally associated with VM

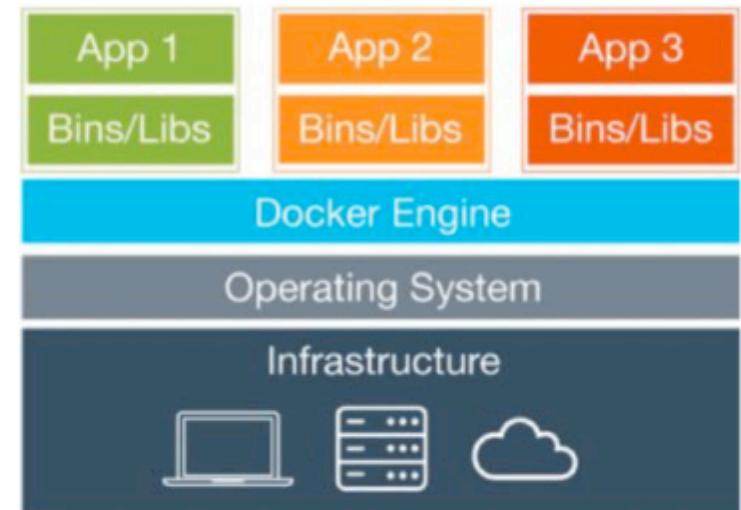
VMs vs. Containers



VMs vs. Containers



Virtual Machines



Containers

VMs vs. Containers

Virtual Machines (VMs)	Containers
Represents hardware-level virtualization	Represents operating system virtualization
Heavyweight	Lightweight
Slow provisioning	Real-time provisioning and scalability
Limited performance	Native performance
Fully isolated and therefore more secure (maybe)	Process-level isolation and therefore less secure (maybe)

VMs vs. Containers

Simulates a physical machine

Provides a local file system

Can be accessed over a network

Full and independent guest operating system

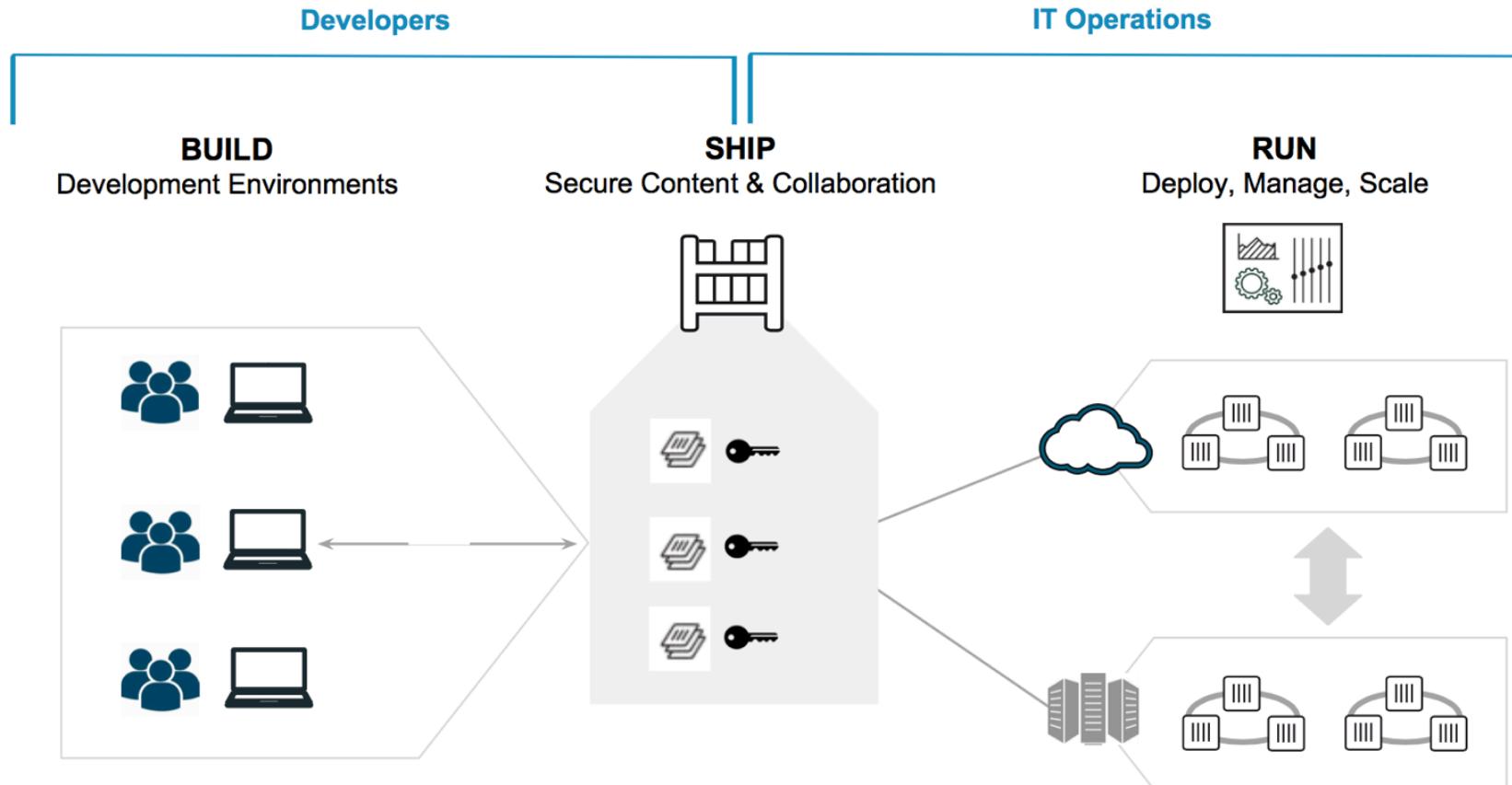
Virtualized device drivers

Strong resource and memory management

Huge memory foot-print

Needs a hypervisor

Dev/Ops Container Workflow



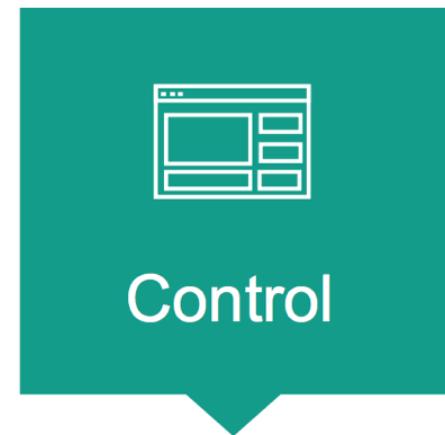
Container Benefits



Innovation
at speed



Frictionless
movement



Manage and
secure at scale

Docker CE vs. Docker EE

	COMMUNITY EDITION	ENTERPRISE EDITION BASIC	ENTERPRISE EDITION STANDARD	ENTERPRISE EDITION ADVANCED
Container engine and built in orchestration, networking, security	✓	✓	✓	✓
Docker Certified - Infrastructure, Plugins and ISV (independent software vendors) Containers		✓	✓	✓
Image Management (private registry, caching)	Cloud hosted repos		✓	✓
Docker Datacenter - Integrated container app management			✓	✓
Docker Datacenter - Multi-tenancy with RBAC, LDAP/AD support			✓	✓
Integrated secrets mgmt, image signing policy			✓	✓
Image security scanning	Preview			✓
Support	Community	Biz Day or 24x7	Biz Day or 24x7	Biz Day or 24x7
Pricing	Free	\$750/node/year	\$1,500/node/year	\$2,000/node/year

Installing Docker

- Docker container engine is built from and on top of the Linux kernel, so it needs Linux to run natively*
 - Docker is increasingly being packaged with newer Linux distributions
 - Docker is also available on MacOS and Windows through the use of lightweight Linux VMs - HyperV-based on Windows, HyperKit-based on MacOS
- * Native Windows containers can also be used with Docker for Windows if you have very specific versions of Windows.

Prerequisite: Connect to Classroom VM



CLASSROOM WORK

- \$ ssh student@FQDN
 - student password = DockerStudentPW0

FQDN = The fully qualified domain name of the machine assigned to you by your instructor. This will commonly be in the form docker#.domain.com (where # is your student number as assigned to you by your instructor).

Prerequisite: Add & Update Repos



CLASSROOM WORK

Done already in AWS instances

```
$ sudo apt-get update  
  
$ sudo apt-get -y install apt-transport-https ca-certificates curl  
  
$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -  
  
$ sudo add-apt-repository \  
  "deb [arch=amd64] https://download.docker.com/linux/ubuntu \  
  $(lsb_release -cs) \  
  stable"  
  
$ sudo apt-get update
```

Also at

<https://docs.docker.com/engine/installation/>

Install Docker-CE



CLASSROOM WORK

```
$ sudo apt-get -y install docker-ce
```

```
$ sudo docker run hello-world
```

Done already in AWS instances

Also at

<https://docs.docker.com/engine/installation/linux/docker-ce/ubuntu/#install-using-the-repository>

Installing Docker Script

- It's good to install Docker the “hard” way at least once so you understand what is involved.
 - There is a Docker-maintained community script that will install the latest release on your Linux machine (most popular flavors) available at <https://get.docker.com/>
 - Run ‘curl -sSL https://get.docker.com/ | sh’ in your terminal
 - The script will also install a Union File System driver and verify Docker engine functionality

Docker Basics

\$ sudo docker version

```
● ○ ● 🏠 cludwig — student@docker-proto: ~ — ssh student@...
student@docker-proto:~$ sudo docker version
Client:
  Version:      17.03.1-ce
  API version:  1.27
  Go version:   go1.7.5
  Git commit:   c6d412e
  Built:        Mon Mar 27 17:14:09 2017
  OS/Arch:      linux/amd64

Server:
  Version:      17.03.1-ce
  API version:  1.27 (minimum version 1.12)
  Go version:   go1.7.5
  Git commit:   c6d412e
  Built:        Mon Mar 27 17:14:09 2017
  OS/Arch:      linux/amd64
  Experimental: false
student@docker-proto:~$
```

Docker Basics

\$ sudo docker info

```
cludwig — student@docker-proto: ~ — ssh student@13.82.176.214 — 95x29
student@docker-proto:~$ sudo docker info
Containers: 1
Running: 0
Paused: 0
Stopped: 1
Images: 1
Server Version: 17.03.1-ce
Storage Driver: aufs
  Root Dir: /var/lib/docker/aufs
  Backing Filesystem: extfs
  Dirs: 3
  Dirperm1 Supported: true
Logging Driver: json-file
Cgroup Driver: cgroupfs
Plugins:
  Volume: local
  Network: bridge host macvlan null overlay
Swarm: inactive
Runtimes: runc
Default Runtime: runc
Init Binary: docker-init
containerd version: 4ab9917febca54791c5f071a9d1f404867857fcc
runc version: 54296cf40ad8143b62dbcaa1d90e520a2136ddfe
init version: 949e6fa
Security Options:
  apparmor
  seccomp
    Profile: default
Kernel Version: 4.4.0-78-generic
```

Docker Basics

- Standard command format:
 - docker [NOUN] verb
- \$ sudo docker --help #displays help and management subcommands (nouns)
- \$ sudo docker NOUN --help
- There are reasonable defaults and short forms of option flags for many things. i.e.:
 - “docker pull” assumes “image”
 - “docker stop” assumes “container”
 - can use “img” instead of “image”
 - can use “con” instead of “container”, etc.

Docker Basics

Determine the status of the Docker service

- \$ sudo service docker status

```
[ubuntu@ubuntu-xenial:~/docker$ sudo service docker status
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2016-11-29 14:12:54 UTC; 2h 47min ago
       Docs: https://docs.docker.com
 Main PID: 1204 (dockerd)
    Tasks: 22
   Memory: 82.9M
      CPU: 1min 31.242s
     CGroup: /system.slice/docker.service
             └─1204 /usr/bin/dockerd -H fd://
                  ├─1212 docker-containerd -l unix:///var/run/docker/libcontainerd/docker-containerd.sock --shim docker-containerd-shim --metrics-interval=0 --start-ti
Nov 29 16:29:33 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:29:33.147992827Z" level=info msg="Layer sha256:6fc2e4ad81348c14fd2d7e3880b5db2bbc2f699a5cdcf18b
Nov 29 16:29:36 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:29:36.424426912Z" level=info msg="Layer sha256:a21398f45083710727f6f382cf232d5d50d4dc9589d6ff5
Nov 29 16:30:09 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:30:09.788820380Z" level=info msg="Layer sha256:9359188bd45e8c8b98fc0f0297ba87b4f5ed64e9dc8fbfa7
Nov 29 16:30:09 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:30:09.913582571Z" level=info msg="Layer sha256:9359188bd45e8c8b98fc0f0297ba87b4f5ed64e9dc8fbfa7
Nov 29 16:30:28 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:30:28.557526233Z" level=info msg="Layer sha256:be3b076c597ddeb0e264d732927a160c2e91c78516c84a1
Nov 29 16:30:50 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:30:50.018714100Z" level=info msg="Layer sha256:47e85df6c4115d2974ab00ef823c215917dae0a9011f4262
Nov 29 16:30:56 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:30:56.620202459Z" level=info msg="Layer sha256:ce06475a45c5830b905647755ce0324b8c313502bf66ea0c
Nov 29 16:31:14 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:31:14.829527550Z" level=info msg="Layer sha256:2b9628b0eba7b5a870fd354986be4d15e605d51c8f97f2a
Nov 29 16:31:15 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:31:15.102270791Z" level=info msg="Layer sha256:c8f15147c2663dc3d68f177fffc0934bb2c04e25eddc6007
Nov 29 16:32:33 ubuntu-xenial dockerd[1204]: time="2016-11-29T16:32:33.801824138Z" level=info msg="Layer sha256:72deb7ae364e53981d0d1befdf7d9c5b15208f93cd8e169b
lines 1-22/22 (END)
```

Docker Hello World(s)

```
[vagrant@vagrant-ubuntu-trusty-64:~$ docker run -it hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world

c04b14da8d14: Pull complete
Digest: sha256:0256e8a36e2070f7bf2d0b0763dbabdd67798512411de4cdcf9431a1feb60fd9
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker Hub account:
https://hub.docker.com

For more examples and ideas, visit:
https://docs.docker.com/engine/userguide/]

vagrant@vagrant-ubuntu-trusty-64:~$ ]
```

Docker Hello World(s)

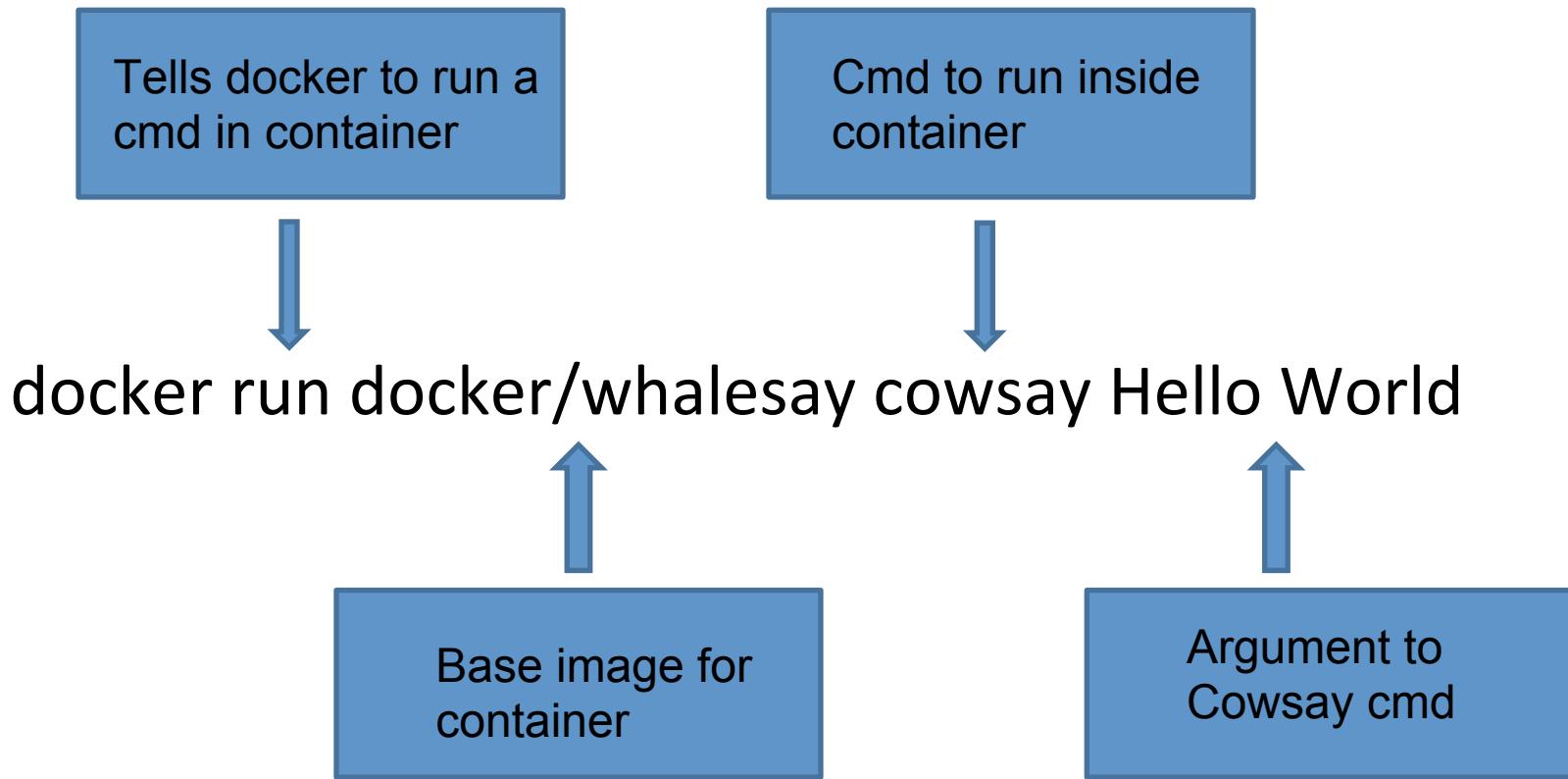
```
$ sudo docker run docker/whalesay cowsay Hello World
```

```
[student@docker-proto:~$ sudo docker run docker/whalesay cowsay Hello World
Unable to find image 'docker/whalesay:latest' locally
latest: Pulling from docker/whalesay
e190868d63f8: Pull complete
909cd34c6fd7: Pull complete
0b9bfabab7c1: Pull complete
a3ed95caeb02: Pull complete
00bf65475aba: Pull complete
c57b6bcc83e3: Pull complete
8978f6879e2f: Pull complete
8eed3712d2cf: Pull complete
Digest: sha256:178598e51a26abbcc958b8a2e48825c90bc22e641de3d31e18aaaf55f3258ba93b
Status: Downloaded newer image for docker/whalesay:latest

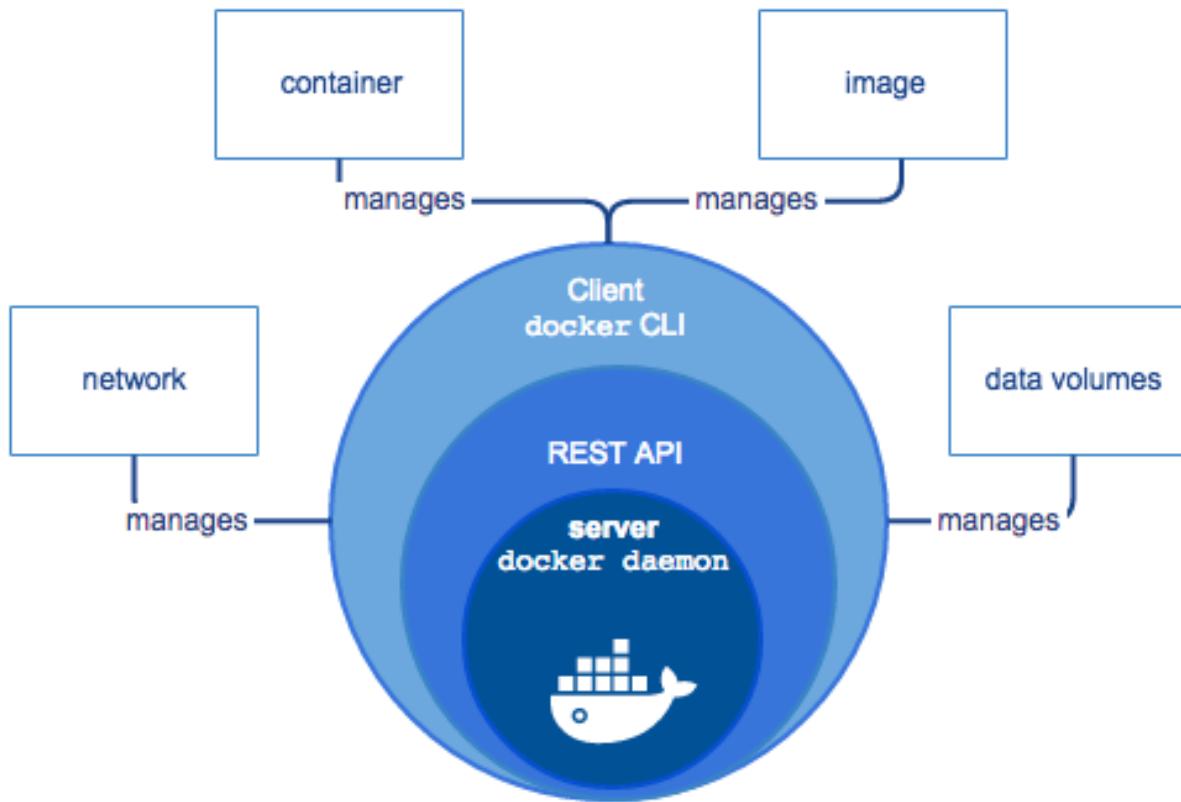
< Hello World >
-----
\ \
  \
    \
      ## .
        ==
      ## ## ## ===
      ## ## ## ## ====
    /:::::::::::__/_/ ====
~~~ {~~ ~~~~ ~~~ ~~~~ ~~~ ~~~ / ===== ~~~
      \_____ o   _/
        \_\_\_\_/_/
          \_\_\_\_/_/
student@docker-proto:~$
```



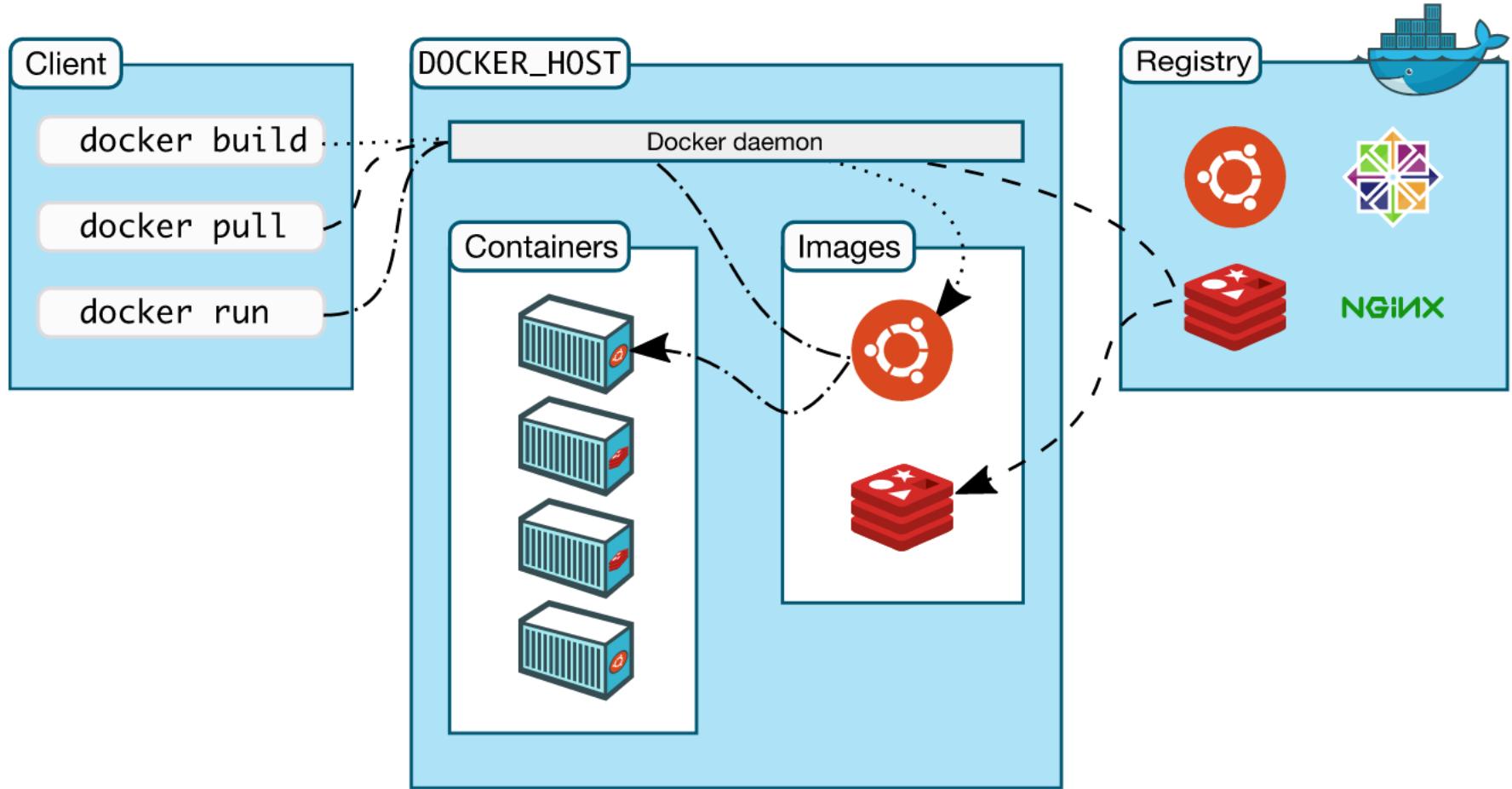
Docker Hello World(s)



What is 'Docker Engine'?



How is Docker Architected?



No ‘sudo’ Configuration

Done already in AWS instances

- Run docker without sudo

– <https://docs.docker.com/engine/installation/linux/linux-postinstall/>

1. Create Docker group:

– `$ sudo groupadd docker`

2. Add your user to docker group:

– `$ sudo usermod -aG docker $USER`

3. Log out and log back in:

– `$ exit # then log back in`

Docker Webapp & Hello World



CLASSROOM WORK

20 minutes

Exercise 2.1 in Docker Labs

<https://github.com/docker/labs/blob/master/beginner/chapters/webapps.md>

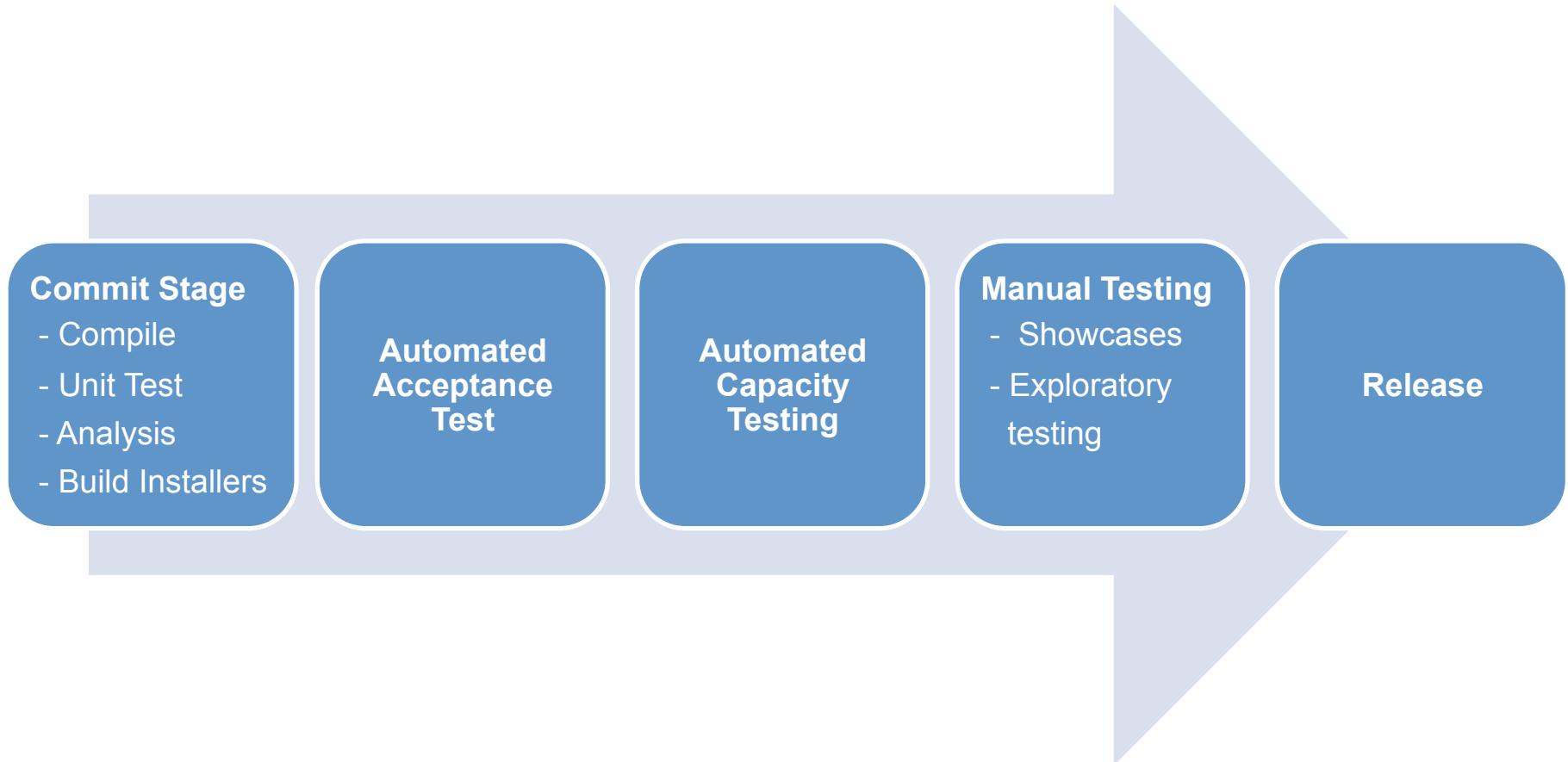
Do only exercise 2.1

So far !!

- Basic difference between VMs and Containers
- Installing Docker
- Images:- Hello World, whalesay, static-website in action

Where Containers are used?

- For automated testing & CICD



Where Containers are used?

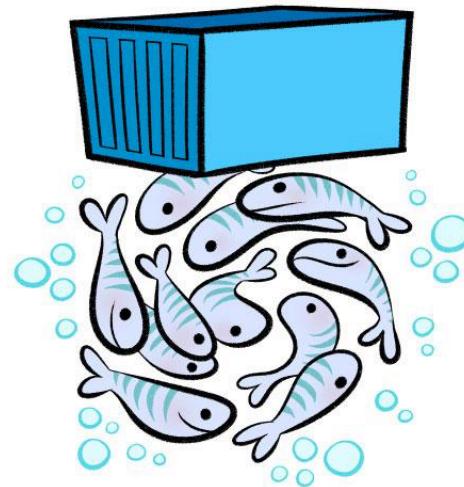
- DevOps (Mostly in all types of Automation)
- Automated testing (Unit, acceptance and stress testing)
- CICD (if not tested on production-like environment, CICD will be risky)
- Microservices
- Less risky deployment architectures
- Chef kitchen test
- Not only used for testing but is used in production (along with container orchestration) in B2C and B2B organizations

Advantage of using Containers

- Developers testing their code in Prod environments
- Lesser hand-offs and drastically lesser waiting time (to get new environment setup)
 - Reduce technical debt
- Overall system resilience - Service failure does not kill the application & may be invisible to users
- Scalability
 - Seamless replication
- High Availability
- Less risky patterns for rolling updates available
- Prevent server sprawl and Jenga infrastructure

Part 2: DevOps Docker

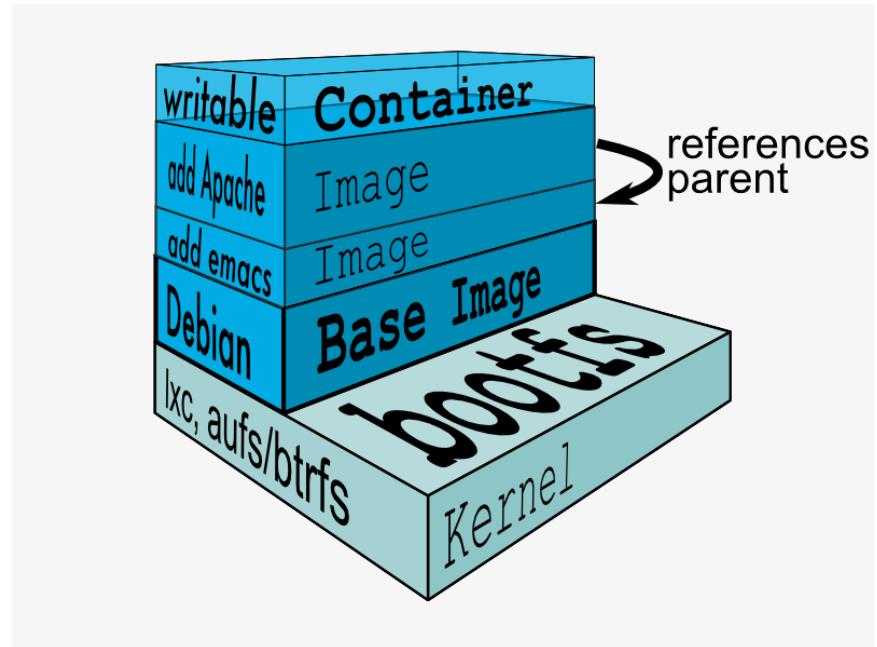
Docker Images



Docker Union File System

AuFS (AnotherUnionFS) is a multi-layered filesystem that implements union mount

- allows several filesystems or directories to be simultaneously mounted and visible through a single mount point
- appears to be one filesystem to the end user



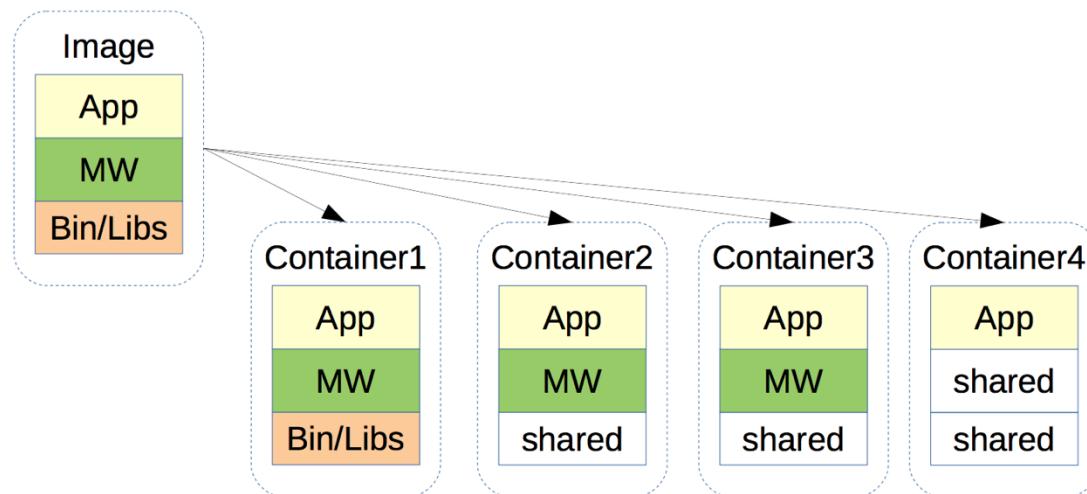
Example Docker Layers



Docker Layer – Each Docker image is composed of a series of layers. Docker uses Union File Systems to combine these into a single image. The combination of these layers gives the illusion of a traditional file system. Only the top layer is writeable.

Benefits of Union File Systems

- Files are shared across containers
- Storage and memory spaces are saved
- Faster deployment of containers



Docker Hub

- Docker's first-party cloud-based registry
 - Hosts a broad repository of Docker images
 - Contains nearly any popular open source technology including MariaDB, Jenkins, Cloudera, etc
 - Contains 'Official images' from vendors such as Canonical, Oracle, Red Hat, etc
 - Provides one free private Docker repo, more for a paid subscription

Docker Hub

A screenshot of a web browser window showing the Docker Hub search results for the query "mariadb". The search bar at the top contains "mariadb". Below the search bar, there is a message about the Docker Store and a navigation bar with "Explore" and "Help" links, along with "Sign up" and "Log In" buttons. The main content area displays a list of 1096 repositories. Each repository entry includes a thumbnail icon of a blue ship, the repository name, its status (e.g., "official" or "public | automated build"), the number of stars, the number of pulls (prefixed with "M+", "K+", or "1.4K"), and a "DETAILS" button.

Repository	Status	Stars	Pulls	Actions
mariadb	official	935	5M+	PULLS DETAILS
bitnami/mariadb	public automated build	21	1M+	PULLS DETAILS
million12/mariadb	public automated build	9	10K+	PULLS DETAILS
maxexcloo/mariadb	public automated build	4	1.4K	PULLS DETAILS

\$ Few Basic Commands

\$ docker search [searchterm]

```
student@docker-proto:~$ docker search mariadb
NAME                           DESCRIPTION                                     STARS      OFFICIAL   AUTOMATED
mariadb                         MariaDB is a community-developed fork of M...    1346      [OK]
bitnami/mariadb                 Bitnami MariaDB Docker Image                   34        [OK]
paintedfox/mariadb              A docker image for running MariaDB 5.5, a ...    29        [OK]
million12/mariadb               MariaDB 10 on CentOS-7 with UTF8 defaults       14        [OK]
toughiq/mariadb-cluster         Dockerized Automated MariaDB Galera Cluste...    11        [OK]
webhippie/mariadb               Docker images for mariadb                      9         [OK]
panubo/mariadb-galera          MariaDB Galera Cluster                     7         [OK]
gists/mariadb                  MariaDB on Alpine                        7         [OK]
kakilangit/mariadb              Docker for MariaDB with OQGraph & TokuDB E...    6         [OK]
maxexcloo/mariadb              Service container with MariaDB installed a...    4         [OK]
tianon/mariadb                 DEPRECATED; use mariadb:*= -- ↴ "I just met...    4         [OK]
takaomag/mariadb               docker image of archlinux (mariadb)           2         [OK]
desertbit/mariadb              This is an extended docker image of the of...    1         [OK]
drupaldocker/mariadb            MariaDB for Drupal                      1         [OK]
tcaxias/mariadb                MariaDB container                      1         [OK]
jpc0/mariadb                   Mariadb, so I can have it on my raspberry       1         [OK]
lucidfrontier45/mariadb        Mariadb with some customizable properties       0         [OK]
vger/mariadb                   MariaDB image, based on Debian Jessie           0         [OK]
yannickvh/mariadb              Custom build of MariaDB based on the offic...    0         [OK]
dogstudio/mariadb              MariaDB Container for Dogs                  0         [OK]
objectstyle/mariadb             ObjectStyle MariaDB Docker Image             0         [OK]
nimmis/mariadb                 MariaDB multiple versions based on nimmis/...    0         [OK]
rkrahlf/mariadb                A docker image for MariaDB                      0         [OK]
mmckeenn/mariadb               MariaDB image based on openSUSE Tumbleweed       0         [OK]
danielsreichenbach/mariadb    Minimal MariaDB container to be used as co...    0         [OK]
student@docker-proto:~$
```

Docker image commands

```
[ubuntu@ip-10-0-0-117:~/code/multistage$ docker image --help

Usage: docker image COMMAND

Manage images

Options:
  --help    Print usage

Commands:
  build      Build an image from a Dockerfile
  history    Show the history of an image
  import     Import the contents from a tarball to create a filesystem image
  inspect    Display detailed information on one or more images
  load       Load an image from a tar archive or STDIN
  ls         List images
  prune     Remove unused images
  pull       Pull an image or a repository from a registry
  push       Push an image or a repository to a registry
  rm        Remove one or more images
  save      Save one or more images to a tar archive (streamed to STDOUT by default)
  tag       Create a tag TARGET_IMAGE that refers to SOURCE_IMAGE

Run 'docker image COMMAND --help' for more information on a command.
```

Docker Container commands

```
[ubuntu@ip-10-0-0-117:~/code/multistage$ docker container --help

Usage: docker container COMMAND

Manage containers

Options:
  --help    Print usage

Commands:
  attach      Attach local standard input, output, and error streams to a running container
  commit      Create a new image from a container's changes
  cp          Copy files/folders between a container and the local filesystem
  create      Create a new container
  diff        Inspect changes to files or directories on a container's filesystem
  exec        Run a command in a running container
  export      Export a container's filesystem as a tar archive
  inspect    Display detailed information on one or more containers
  kill        Kill one or more running containers
  logs       Fetch the logs of a container
  ls          List containers
  pause      Pause all processes within one or more containers
  port        List port mappings or a specific mapping for the container
  prune      Remove all stopped containers
  rename     Rename a container
  restart    Restart one or more containers
  rm          Remove one or more containers
  run         Run a command in a new container
  start      Start one or more stopped containers
  stats      Display a live stream of container(s) resource usage statistics
  stop       Stop one or more running containers
  top         Display the running processes of a container
  unpause    Unpause all processes within one or more containers
  update     Update configuration of one or more containers
  wait       Block until one or more containers stop, then print their exit codes

Run 'docker container COMMAND --help' for more information on a command.
```

\$ docker image pull [imageName]

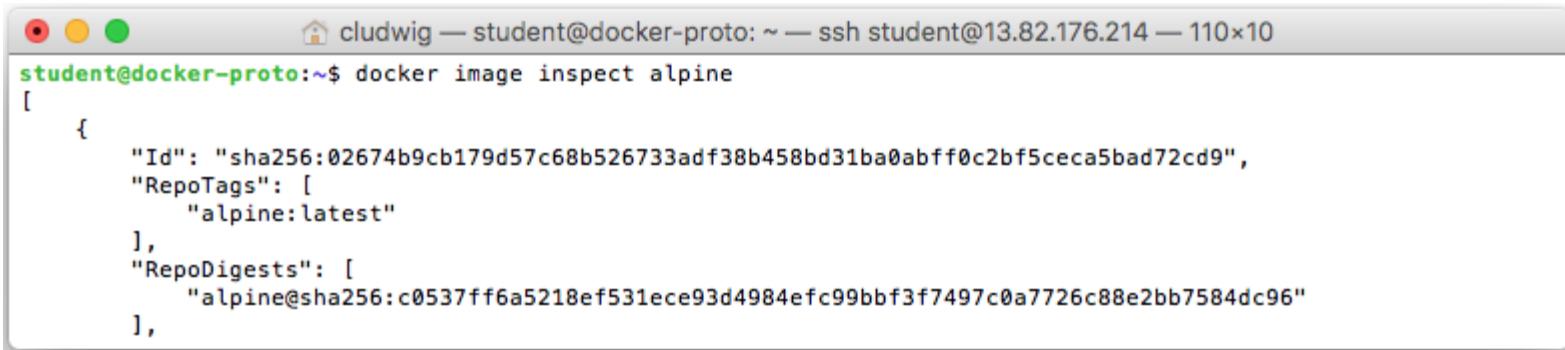
```
[student@docker-proto:~$ docker image pull alpine
Using default tag: latest
latest: Pulling from library/alpine
cfc728c1c558: Pull complete
Digest: sha256:c0537ff6a5218ef531ece93d4984efc99bbf3f7497c0a7726c88e2bb7584dc96
Status: Downloaded newer image for alpine:latest
```

Best Practice: Choose the smallest base images possible

Debian – 123 MB
Alpine – 5 MB

```
[student@docker-proto:~$ docker image list
REPOSITORY          TAG      IMAGE ID   CREATED    SIZE
alpine              latest   02674b9cb179  11 days ago  3.99 MB
hello-world         latest   48b5124b2768  4 months ago  1.84 kB
dockersamples/static-site  latest   f589ccde7957  14 months ago  191 MB
docker/whalesay     latest   6b362a9f73eb  24 months ago  247 MB
student@docker-proto:~$
```

\$ docker inspect [image | container]

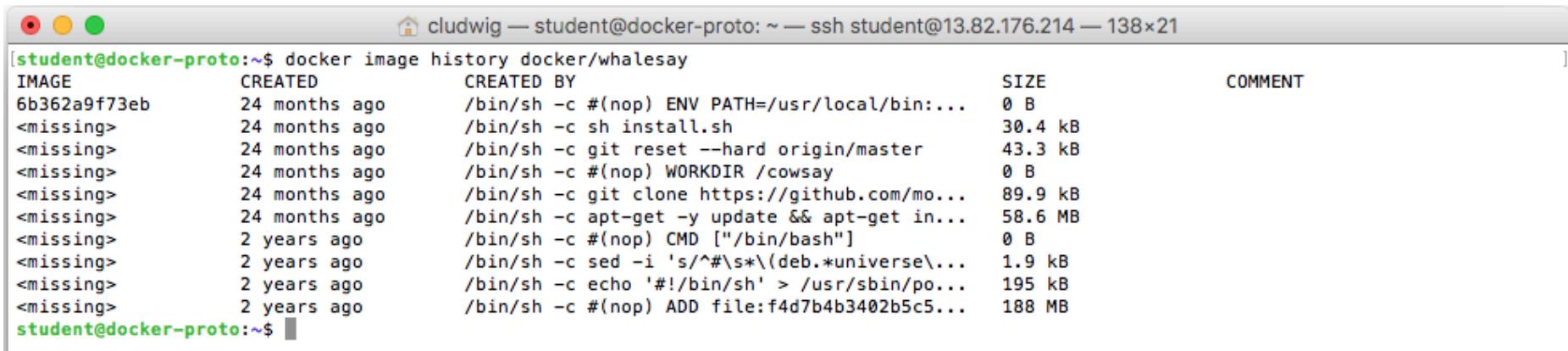


```
student@docker-proto:~$ docker image inspect alpine
[
  {
    "Id": "sha256:02674b9cb179d57c68b526733adf38b458bd31ba0abff0c2bf5ceca5bad72cd9",
    "RepoTags": [
      "alpine:latest"
    ],
    "RepoDigests": [
      "alpine@sha256:c0537ff6a5218ef531ece93d4984efc99bbf3f7497c0a7726c88e2bb7584dc96"
    ],
  }
]
```

- **ID** The unique identifier for the container
- **State** This stanza has various status flags and the process id for the container. Using the `ExitCode` from this `State` element a [graceful shutdown](#) or recovery process could be initiated. The following format will return just the `ExitCode` of the most recently run container:

```
docker inspect -f '{{.State.ExitCode}}' $(docker ps -lq)
```
- **Image** The image this container is running.
- **NetworkSettings** The network environment for the container and therefore for the application(s) within the image.
- **LogPath** The system path to this container's log file.
- **RestartCount** Keeps track of the number of times the container has been restarted. This value is the key value used when defining a container's [restart policy](#).
- **Name** The user defined name for the container.
- **Volumes** Defines the volume mapping between the host system and the container.
- **HostConfig** Key configurations for how the container will interact with the host system. These could take CPU and memory limits, networking values, or device driver paths.
- **Config** The runtime configuration options set when the docker run command was executed. Part of this configuration is another "Image" value. This image `{{.Config.Image}}` is the tagged image which may be different than the image listed in `{{ Image}}`

\$ docker image history docker/whalesay



```
cludwig — student@docker-proto: ~ — ssh student@13.82.176.214 — 138x21
[student@docker-proto:~$ docker image history docker/whalesay
IMAGE          CREATED      CREATED BY
6b362a9f73eb  24 months ago  /bin/sh -c #(nop) ENV PATH=/usr/local/bin:...
<missing>      24 months ago  /bin/sh -c sh install.sh
<missing>      24 months ago  /bin/sh -c git reset --hard origin/master
<missing>      24 months ago  /bin/sh -c #(nop) WORKDIR /cowsay
<missing>      24 months ago  /bin/sh -c git clone https://github.com/mo...
<missing>      24 months ago  /bin/sh -c apt-get -y update && apt-get in...
<missing>      2 years ago   /bin/sh -c #(nop) CMD ["/bin/bash"]
<missing>      2 years ago   /bin/sh -c sed -i 's/^#\!*/deb.*universe\...
<missing>      2 years ago   /bin/sh -c echo '#!/bin/sh' > /usr/sbin/po...
<missing>      2 years ago   /bin/sh -c #(nop) ADD file:f4d7b4b3402b5c5...
student@docker-proto:~$ ]
```

Use history to view layers in an image

Docker Interactive Mode

Best Practice: Run containers in interactive mode while developing docker images

```
[ubuntu@instance-41:~/flask-app$ sudo docker run -t -i ubuntu /bin/bash
Unable to find image 'ubuntu:latest' locally
latest: Pulling from library/ubuntu
6bbebd9b76a4: Pull complete
fc19d60a83f1: Pull complete
de413bb911fd: Pull complete
2879a7ad3144: Pull complete
668604fde02e: Pull complete
Digest: sha256:2d44ae143feeb36f4c898d32ed2ab2dffeb3a573d2d8928646dfc9cb7deb1315
Status: Downloaded newer image for ubuntu:latest
root@a4b1111d9d0e:/# ]
```

Docker Interactive Mode

Create a terminal
To use

```
docker run -t -i ubuntu /bin/bash
```

Interactive mode

Docker Interactive Mode

Attach to a running container and shell instance

```
docker attach some_container #by Name
```

Attach to a running container by starting a new shell instance

```
docker exec -it some_container /bin/bash #by Name
```

Docker Interactive Mode

Quick Tip: Be aware that alpine and other distros may have a different entry point (sh vs bash)

```
docker run -it alpine /bin/sh
```

See all containers

- \$ docker container ls #show running

```
student@docker-proto:~$ docker container ls
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
NAMES
e63ebe9ecaa2      dockersamples/static-site "/bin/sh -c 'cd /u..."  8 hours ago       Up 8 hours          0.0.0.0:327
69->80/tcp, 0.0.0.0:32768->443/tcp   dreamy_galileo
```

- \$ docker container ls -a #show all containers
(including running, stopped, exited, etc.)

```
student@docker-proto:~$ docker container ls -a
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
NAMES
e63ebe9ecaa2      dockersamples/static-site "/bin/sh -c 'cd /u..."  8 hours ago       Up 8 hours          0.0.
0:32769->80/tcp, 0.0.0.0:32768->443/tcp   dreamy_galileo
16528921a105      dockersamples/static-site "/bin/sh -c 'cd /u..."  14 hours ago      Exited (137) 8 hours ago
edb964673b1b      docker/whalesay      "cowsay Hello World"  15 hours ago      Exited (0) 15 hours ago
31f3c64d31a1      hello-world        "/hello"           22 hours ago      Exited (0) 22 hours ago
student@docker-proto:~$
```

Docker Working with Images and Containers



CLASSROOM WORK

20 minutes

Practice Docker image and container commands

- Pull image ubuntu
 - Inspect the image
 - start a container in detach mode (and inspect the container)
 - exit the container
 - start a container in interactive mode (and inspect the container)
 - exit without stopping the container (cntrl P Q)
- Pull image redis
 - Inspect the image
 - start a container in detach mode (and inspect the container)
 - start a container with all ports published
 - Start a container with 6379 port published as 1001
 - Install redis-tools in the host and connect to redis-cli and set some values, get some values
 - Run:- docker container stats

\$docker container stats

```
[student@docker-proto:~$ docker container ls
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
NAMES
e63ebe9ecaa2      dockersamples/static-site   "/bin/sh -c 'cd /u..."   8 hours ago       Up 8 hours        0.0.0.0:32768->80/tcp, 0.
0.0.0.0:32768->443/tcp   dreamy_galileo
[student@docker-proto:~$ docker container stats e63
CONTAINER          CPU %               MEM USAGE / LIMIT     MEM %           NET I/O          BLOCK I/O         PIDS
e63                0.00%              1.562 MiB / 667.2 MiB  0.23%          4.29 kB / 12.4 kB  73.7 kB / 12.3 kB  3
```

- Provides the CPU, memory, network, and other monitoring KPI's of a docker container.
- Multiple containers can be profiled as well
- All containers can be profiled by leaving out the container id(s)

Removing Docker Containers & Images

```
#!/bin/bash
```

```
# Remove all stopped containers
docker container prune [-f]
```

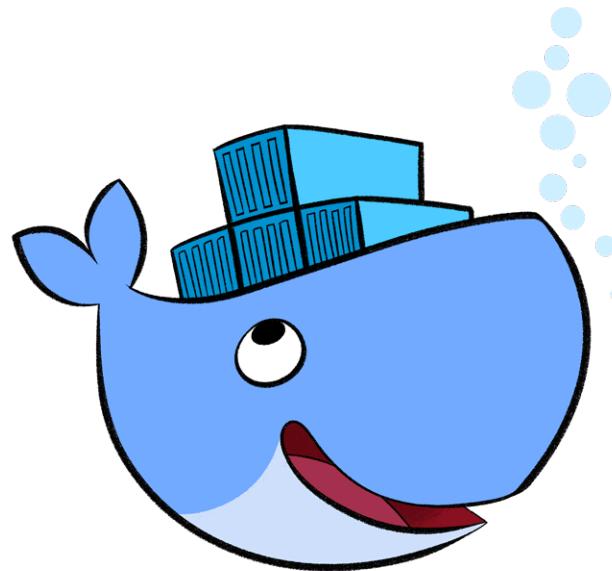
```
# Remove all unused images
docker image prune [-f] [-a]
```

-f option skips confirmation.
-a option (for images) removes ALL unused images, not just those that were left behind when a container was removed (dangling).

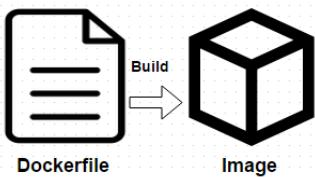
Best Practice: Prevent image inflation and regularly clean up images

Part 3: DevOps Docker

Docker Files



Dockerfile



```
1 FROM ubuntu:14.04
2
3 # install cowsay, and move the "default.cow" out of the way so we can overwrite it with "docker.cow"
4 RUN apt-get update && apt-get install -y cowsay --no-install-recommends && rm -rf /var/lib/apt/lists/* \
5     && mv /usr/share/cowsay/cows/default.cow /usr/share/cowsay/cows/orig-default.cow
6
7 # "cowsay" installs to /usr/games
8 ENV PATH $PATH:/usr/games
9
10 COPY docker.cow /usr/share/cowsay/cows/
11 RUN ln -sv /usr/share/cowsay/cows/docker.cow /usr/share/cowsay/cows/default.cow
12
13 CMD ["cowsay"]
14
```

- Docker images are built, layer by layer, from a base image
- Images are composed of layers, each with a simple command such as
 - Run a shell command
 - Add a file or directory
 - Create an environment variable
 - Modify permissions
 - Execute process or script

Dockerfile

Dockerfile format

```
#Comment  
INSTRUCTION arguments
```

Command	Description
FROM	The base image to use in the build. This is mandatory and must be the first command in the file
MAINTAINER	An optional value for the maintainer of the script
RUN	Executes a command and save the result as a new layer This executes during build time
CMD	The command that runs when the container starts Doesn't execute during built time whereas RUN executes during build time
ENV	Sets an environment variable in the new container
COPY	Copies a file from source to destination in the file system of the container
ADD	Remote URL support and Copies a file from the host system onto the container
ENTRYPOINT	Primary command to run whenever the image is executed
EXPOSE	Opens a port for linked containers
ONBUILD	A command that is triggered when the image in the Dockerfile is used as a base for another image It behaves as if a RUN instruction is inserted immediately after the FROM instruction of the downstream Dockerfile
USER	Sets the default user within the container
VOLUME	Creates a shared volume that can be shared among containers or by the host machine
WORKDIR	Set the default working directory for the container for other instructions like RUN, CMD, COPY, ADD, ENTRYPOINT
LABEL	Add metadata to the image; LABEL key=value

Dockerfile

FROM command

The first instruction in a Dockerfile is a FROM command, to specify the Image from which you are building from.

FROM <image>

FROM <Image>:<tag>

FROM ubuntu:14.04

Dockerfile

MAINTAINER command

This lets you know who to consult (or blame ☺) for any dockerfile issues

MAINTAINER Santa Claus “santa@abc.org”

ENV command

Used to provide environment variables for containers.

ENV <key> <value>

ENV PATH \$PATH:/usr/foo

Dockerfile

RUN command

Executes commands and commits the results in a new layer.

`RUN <command>`

`RUN apt-get update`

CMD command

Can only be one in a dockerfile. The CMD instruction provides defaults to an executing container and can be overridden with arguments to docker run.

`CMD ["cowsay"]`

Dockerfile

ADD/COPY command

Places files onto a file system. ADD performs the same as copy, but also allows the <src> to be a URL. It will also unpack recognized compression formats.

COPY <src> <dest>

ADD <src> <dest>

EXPOSE command

Informs Docker that the container listens on a network port at runtime. Ports of a container are still not accessible to the host unless –p flag is passed to the Docker run command when the container is invoked.

EXPOSE 80

Dockerfile

Best Practices for writing Dockerfiles:

- Use `.dockerignore` to exclude any unnecessary files and improve Docker's performance
- Run a single process per container to simplify scale and reuse
- Minimize layers per container
- Sharing base images is a common among development teams
- When possible, base from tiny images such as Alpine Linux
- For production: specify version of the base image (do not use latest)
- For production: use image sha digest rather than image name

Dockerfile

- Dockerfile build syntax

```
docker build .
```

```
docker build -t <namespace/image name:versiontag> /path
```

```
docker build -t myimage/kafka .
```

*** Be aware that when you run 'docker build .', all files in the current folder get uploaded to docker engine. This may be undesirable, and use of .dockerignore will assist with this situation.*

- Then run the newly created image

```
Docker run –t myname/jenkins
```

Docker Create your first image



CLASSROOM WORK

20 minutes

- Create an image
 - Use ubuntu as base image
 - Update apt-get, install tree and wget packages
 - Make two directories using two separate RUN commands
 - copy a local file to the image
 - Make the image return a bash
- Build the image
 - Inspect the image and recursively go to parent images and check the “cmd” to verify layers
 - Run a container; check the directory and the copied file
 - Exit the container (cntrl P Q => so it doesn’t exit)
 - Run “docker exec” to run unix cmds in container from the host
 - From the host, attach to the running container
 - Kill the container, re-start it using “docker start”

Dockerfile Exercises



CLASSROOM WORK

20 minutes

Exercise 2.2 & 2.3 in Docker Labs

<https://github.com/docker/labs/blob/master/beginner/chapters/webapps.md>

NB: You can skip the second part of step 2.3.4 (“Push Your Image”) unless you want to first create yourself an account at hub.docker.com.

Dockerfile Optimization

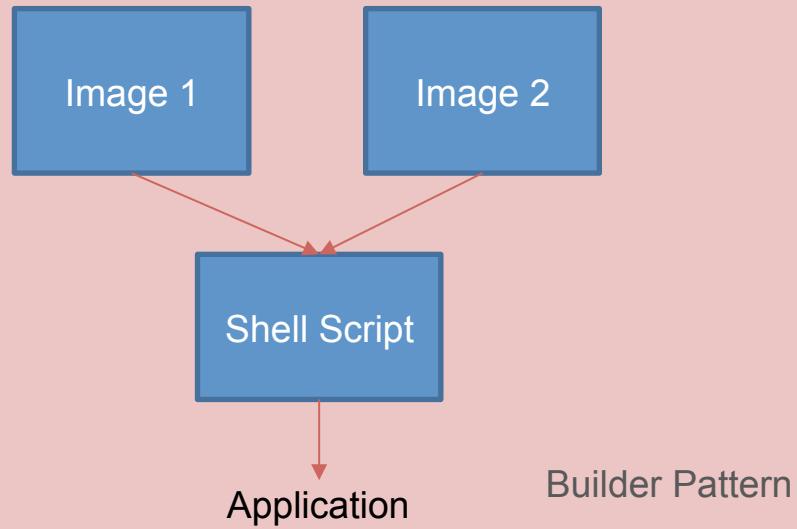


CLASSROOM WORK

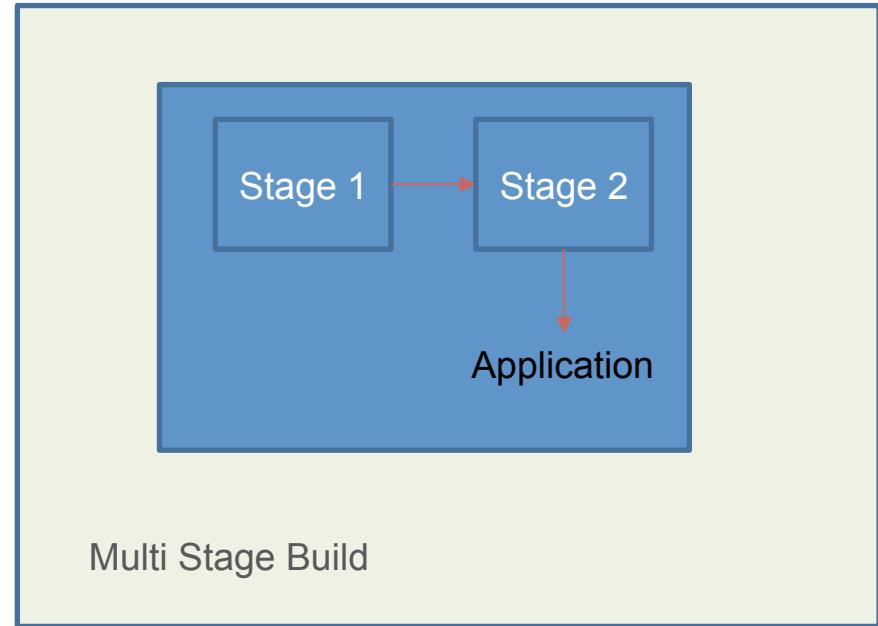
This exercise covers optimizing dockerfile to reduce the number of layers

https://github.com/docker/dceu_tutorials/blob/master/11-infrastructure-as-code.md

Multi-stage Build



Builder Pattern



Multi Stage Build

- **Builder Pattern:** Common practice to maintain two dockerfiles. One for development and other for production that contains application and only things needed to run the application

This is not ideal !!!!

- **Multi-Stage Build:** One stage to another

Multi-stage Build

- New as of Docker 17.05
- Allows “ship artifacts, not build environments”
- Ideal for languages like Go, where binaries are built in a heavyweight environment, but can ship the binary in a lightweight container.

```
# first stage does the building
# for UX purposes, I'm naming this stage `build-stage`

FROM golang:1.8 as build-stage
WORKDIR /go/src/github.com/codeship/go-hello-world
COPY hello-world.go .
RUN go build -o hello-world .

# starting second stage
FROM alpine:latest

# copy the binary from the `build-stage`
COPY --from=build-stage /go/src/github.com/codeship/go-hello-world/hello-world /bin

CMD hello-world
```

```
$ docker images
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
single-stage	latest	58328409dbf7	2 minutes ago	704MB
multi-stage	latest	9af3c2a2bf40	23 minutes ago	5.54MB

Docker Monitoring

<https://github.com/google/cadvisor> -

Monitor the system from inside the Docker container!



cAdvisor

```
sudo docker run --volume=/:/rootfs:ro --volume=/var/run:/var/run:rw --volume=/sys:/sys:ro --volume=/var/lib/docker/:/var/lib/docker:ro --publish=8080:8080 --detach=true --name=cadvisor1 google/cadvisor:latest
```

yourdockerhost:8080

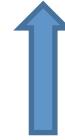
The screenshot shows the cAdvisor web interface at `http://yourdockerhost:8080/containers/13.82.176.214:8080/containers/`. The top navigation bar includes back, forward, and search icons, along with various browser extensions. The main page has a header "Usage" and a "Overview" section featuring five gauge charts for CPU, Memory, and three different file systems (FS #1, FS #2, FS #3). Below this is a "Processes" table listing the following data:

User	PID	PPID	Start Time	CPU %	MEM %	RSS	Virtual Size	Status	Running Time	Command	Container
root	11,956	11,939	13:05	7.60	3.80	25.69 MiB	307.25 MiB	Ssl	00:00:01	cadvisor	/docker/7d2e7e08c4d694428
root	5,160	1	May21	0.20	8.90	59.48 MiB	398.33 MiB	Ssl	00:03:18	dockerd	/system.slice/docker.service
root	1,571	1,151	May21	0.10	3.50	23.83 MiB	212.40 MiB	Sl	00:01:30	python3	/system.slice/walinuxagent
root	1	0	May21	0.00	0.80	5.87 MiB	37.18 MiB	Ss	00:00:23	systemd	/init.
root	2	0	May21	0.00	0.00	0.00 MiB	0.00 MiB	S	00:00:00	kthreadd	

Running a Private Docker Registry

- docker run -d -p 5000:5000 registry

```
[ubuntu@instance-41:~/app$ sudo docker pull registry
Using default tag: latest
latest: Pulling from library/registry
3690ec4760f9: Already exists
930045f1e8fb: Pull complete
feeaa90cbdbc: Pull complete
61f85310d350: Pull complete
b6082c239858: Pull complete
Digest: sha256:1152291c7f93a4ea2ddc95e46d142c31e743b6dd70e194af9e6ebe530f782c17
Status: Downloaded newer image for registry:latest
[ubuntu@instance-41:~/app$ sudo docker run -d -p5000:5000 registry
64730d7011f71d463d480982a765624b4f353e2f2c7003779281cf453c8b2178
```



Push/Pull enabled
from private registry

Docker Registry

- Tag an image
 - `docker tag ubuntu localhost:5000/myubuntu:0.1`
- Push the tagged image to registry
 - `docker push localhost:5000/myubuntu:0.1`
- Verify the pushed image
 - `docker rmi -f ubuntu`
 - `docker rmi -f localhost:5000/myubuntu:0.1`
 - `docker pull localhost:5000/myubuntu:0.1`
 - Run a container from the above image

Docker Registry Search

- **Search Registry**

- <https://docs.docker.com/registry/spec/api/#listing-repositories>

```
curl -XGET http://localhost:5000/v2/_catalog
```

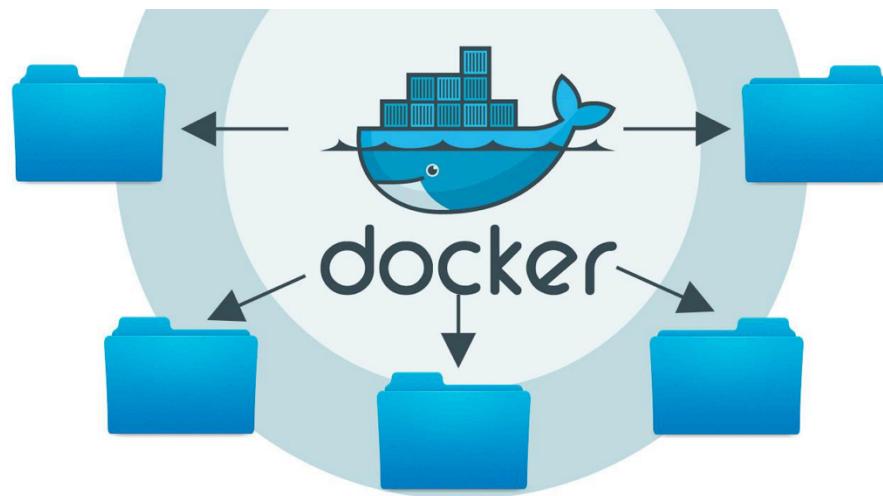
- **List Image Tags**

- <https://docs.docker.com/registry/spec/api/#listing-image-tags>

```
curl -XGET http://localhost:5000/v2/myubuntu/tags/list
```

Part 4: DevOps Docker

Docker Volumes



Data volumes

A *data volume* is a specially-designated directory within one or more containers that bypasses the [*Union File System*](#). Data volumes provide several useful features for persistent or shared data:

- Volumes are initialized when a container is created. If the container's base image contains data at the specified mount point, that existing data is copied into the new volume upon volume initialization. (Note that this does not apply when [mounting a host directory](#).)
- Data volumes can be shared and reused among containers.
- Changes to a data volume are made directly.
- Changes to a data volume will not be included when you update an image.
- Data volumes persist even if the container itself is deleted.

Data volumes are designed to persist data, independent of the container's lifecycle. Docker therefore *never* automatically deletes volumes when you remove a container, nor will it "garbage collect" volumes that are no longer referenced by a container.

Adding a data volume

- You can add a **data volume** to a container using the -v flag with the docker create and docker run command. You can use the -v multiple times to mount multiple data volumes. Now, mount a single volume in your web application container.
 - `docker run -it --name test1 -v data2:/data ubuntu`
 - In addition to creating a volume using the -v flag you can also **mount a directory** from your Docker engine's host into a container
 - `docker run -it --name test1 -v /home/ubuntu/src:/data ubuntu`
- This command mounts the host directory, /home/ubuntu/src, into the container at /data.

Docker volume commands

Command	Description
docker volume create	Create a volume
docker volume ls	List volumes
docker volume inspect	Detailed information on volume
docker volume rm	Remove volume

Working with Volumes

```
[ubuntu@instance-41:~$ docker volume create --name myvolume  
myvolume  
[ubuntu@instance-41:~$ docker volume ls  
DRIVER          VOLUME NAME  
local            030f652ad7ea6766f3d17a421233896b78296cf89d9bc816c69e6084df1aa24d  
local            94ed6b916617b932638619fcdbfc77d843175a57c520d02d3162f5750916409  
local            myvolume  
[ubuntu@instance-41:~$ docker volume inspect myvolume  
[  
 {  
   "Name": "myvolume",  
   "Driver": "local",  
   "Mountpoint": "/var/lib/docker/volumes/myvolume/_data",  
   "Labels": {},  
   "Scope": "local"  
 }  
]  
[ubuntu@instance-41:~$ docker volume rm myvolume  
myvolume -
```

Dangling Volumes

- If container is deleted with a volume attached, the volume remains. Sometimes removing all such ‘dangling’ volumes is desired
 - \$ docker volume prune

Dangling Volumes

- Before

```
[ubuntu@instance-41:~$ docker volume ls
DRIVER          VOLUME NAME
local           030f652ad7ea6766f3d17a421233896b78296cf89d9bc816c69e6084df1aa24d
local           1e16af70af2319707350ce672c0af925c010561a5f75f83393674b5f20df7074
local           94ed6b916617b932638619fcbdbfc77d843175a57c520d02d3162f5750916409
```

- After

```
ubuntu@instance-41:~$ docker volume prune
030f652ad7ea6766f3d17a421233896b78296cf89d9bc816c69e6084df1aa24d
1e16af70af2319707350ce672c0af925c010561a5f75f83393674b5f20df7074
94ed6b916617b932638619fcbdbfc77d843175a57c520d02d3162f5750916409
ubuntu@instance-41:~$ docker volume ls
DRIVER          VOLUME NAME
```

Docker Volumes Exercise



CLASSROOM WORK

30 minutes

<https://goo.gl/gR6XTI>

(https://github.com/docker/dceu_tutorials/blob/master/07-volumes.md)

Docker “--volumes-from”

volumes-from

- docker volume create --name backup
- docker volume create --name logs
- docker run -it --name master -v backup:/backup -v logs:/logs ubuntu bash
- create sample files in backup & logs folders in container
- You can stop the container, but do not remove it
- Create another container using master volumes
 - docker run -it --name slave1 --volumes-from master ubuntu bash
- check the 2 folders ; exit

Remote Volumes

<https://container42.com/2014/03/29/docker-quicktip-4-remote-volumes/>

Docker Volume Plugin - Flocker

<https://clusterhq.com/flocker/>



When container moves, its data volume stays in place.
Database starts on new server without any data.



When container moves, data volume moves with it.
Your database gets to keep its data!

Docker Cheat Sheet



Docker Cheat Sheet



Glossary

Layer - a set of read-only files to provision the system

Image - a read-only layer that is the base of your container. Might have a parent image

Container - a runnable instance of the image

Registry / Hub - central place where images live

Docker machine - a VM to run Docker containers (Linux does this natively)

Docker compose - a utility to run multiple containers as a system

Useful one-liners

Download an image

```
docker pull image_name
```

Start and stop the container

```
docker [start|stop] container_name
```

Create and start container, run command

```
docker run -ti --name container_name  
image_name command
```

Create and start container, run command, destroy container

```
docker run --rm -ti image_name command
```

Example filesystem and port mappings

```
docker run -it --rm -p 8080:8080 -v  
/path/to/agent.jar:/agent.jar -e  
JAVA_OPTS="--javaagent:/agent.jar"  
tomcat:8.0.29-jre8
```

Docker cleanup commands

Kill all running containers

```
docker kill $(docker ps -q)
```

Delete dangling images

```
docker rmi $(docker images -q -f  
dangling=true)
```

Remove all stopped containers

```
docker rm $(docker ps -a -q)
```

Docker machine commands

Use docker-machine to run the containers

Start a machine

```
docker-machine start machine_name
```

Configure docker to use a specific machine

```
eval "$(docker-machine env machine_name)"
```

Docker compose syntax

docker-compose.yml file example

```
version: "2"  
services:  
web:  
  container_name: "web"  
  image: java:8 # image name  
  # command to run  
  command: java -jar /app/app.jar  
  ports: # map ports to the host  
    - "4567:4567"  
  volumes: # map filesystem to the host  
    - ./myapp.jar:/app/app.jar  
mongo: # container name  
  image: mongo # image name
```

Create and start containers

```
docker-compose up
```

Interacting with a container

Run a command in the container

```
docker exec -ti container_name command.sh
```

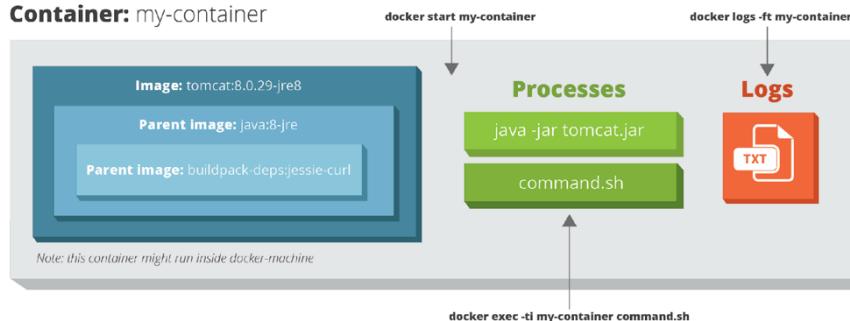
Follow the container logs

```
docker logs -ft container_name
```

Save a running container as an image

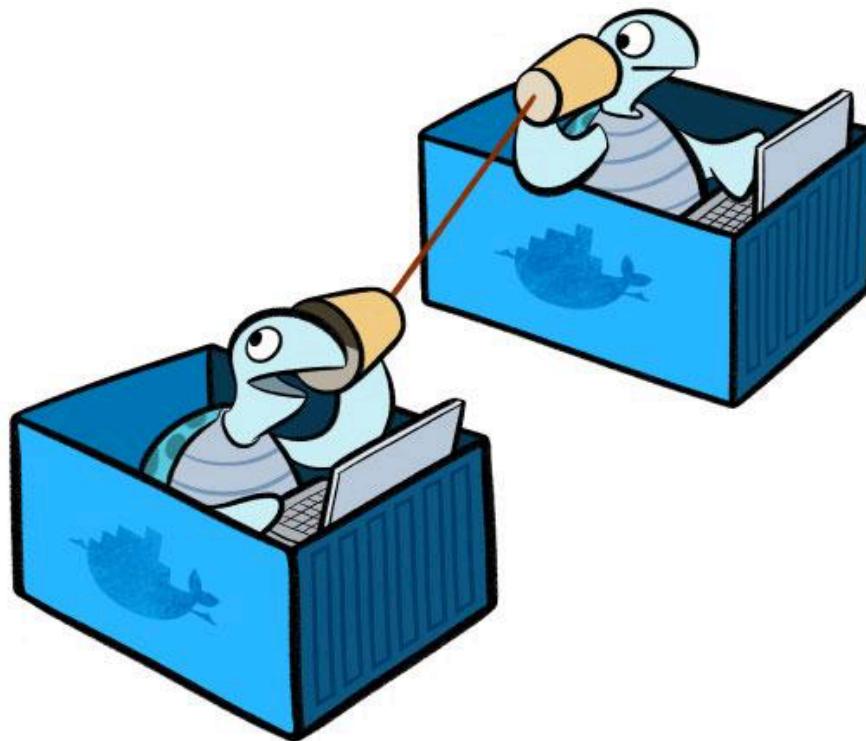
```
docker commit -m "commit message" -a "author"  
container_name username/image_name:tag
```

Container: my-container



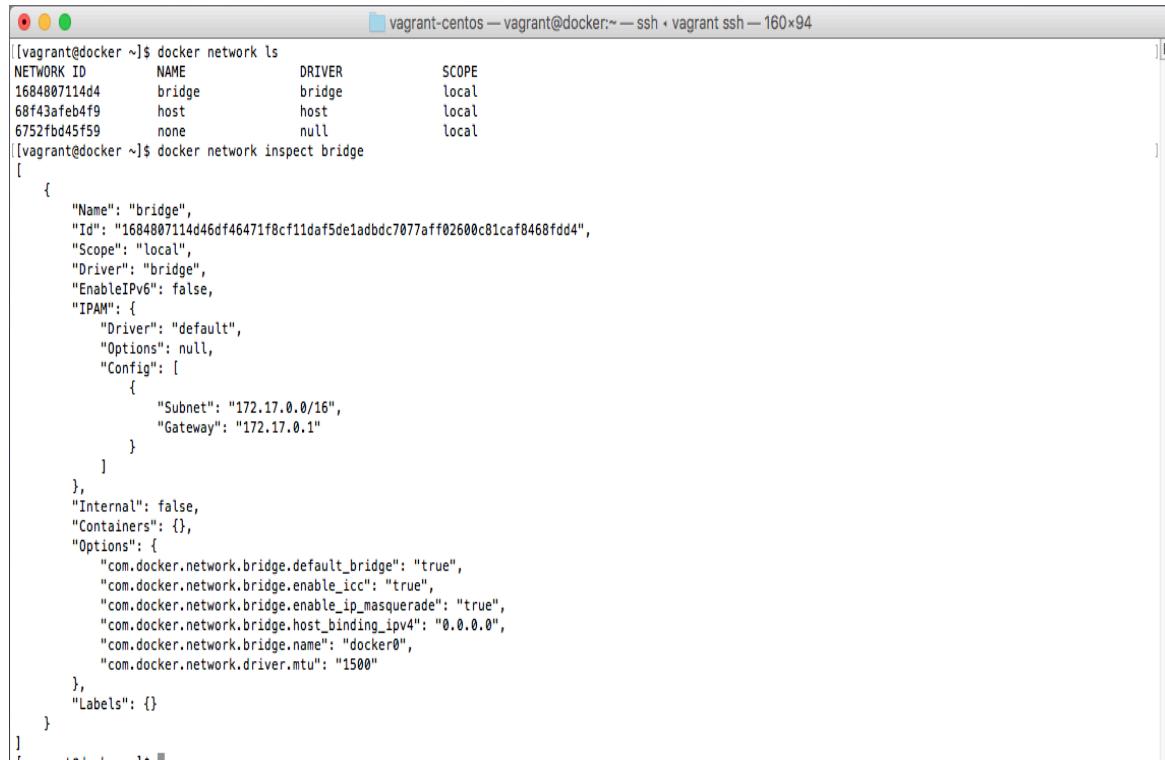
BROUGHT TO YOU BY
JRebel

Docker Networking



Docker Network Defaults

- Three networks are created by default (bridge, host & none)
 - **docker network ls**
- We can easily inspect the bridge network
 - **docker network inspect bridge**
- We see that a 172.17.0.0/16 address space is allocated. Created Containers are given an IP in this space by default.



```
vagrant-centos — vagrant@docker:~ — ssh + vagrant ssh — 160x94
[vagrant@docker ~]$ docker network ls
NETWORK ID      NAME      DRIVER      SCOPE
1684807114d4    bridge    bridge      local
68f43afeb4f9    host      host       local
6752fbdb45f59   none     null       local
[vagrant@docker ~]$ docker network inspect bridge
[
  {
    "Name": "bridge",
    "Id": "1684807114d46df46471f8cf11daf5de1adbdcc077aff02600c81caf8468fdd4",
    "Scope": "local",
    "Driver": "bridge",
    "EnableIPv6": false,
    "IPAM": {
      "Driver": "default",
      "Options": null,
      "Config": [
        {
          "Subnet": "172.17.0.0/16",
          "Gateway": "172.17.0.1"
        }
      ],
      "Internal": false,
      "Containers": {}
    },
    "Options": {
      "com.docker.network.bridge.default_bridge": "true",
      "com.docker.network.bridge.enable_icc": "true",
      "com.docker.network.bridge.enable_ip_masquerade": "true",
      "com.docker.network.bridge.host_binding_ipv4": "0.0.0.0",
      "com.docker.network.bridge.name": "docker0",
      "com.docker.network.driver.mtu": "1500"
    },
    "Labels": {}
  }
]
```

Docker Network Defaults

```
vagrant-centos — vagrant@docker:~ — ssh + vagrant ssh — 160x94
[vagrant@docker ~]$ docker run --name some-ghost -p 8080:2368 -d ghost
53e5d4de5054ca0b3cfaab91476f6901f373df3e4b215c2af855cc14be62a464
[vagrant@docker ~]$ docker network inspect bridge
[{"Name": "bridge",
 "Id": "1684807114d46df46471f8cf11daf5de1adbdc7077aff02600c81caf8468ffdd4",
 "Scope": "local",
 "Driver": "bridge",
 "EnableIPv6": false,
 "IPAM": {
   "Driver": "default",
   "Options": null,
   "Config": [
     {
       "Subnet": "172.17.0.0/16",
       "Gateway": "172.17.0.1"
     }
   ]
 },
 "Internal": false,
 "Containers": {
   "53e5d4de5054ca0b3cfaab91476f6901f373df3e4b215c2af855cc14be62a464": {
     "Name": "some-ghost",
     "EndpointID": "e02d6b898b3d89ee192bbf228d467d49d8f811948a7bc79543524112148fa7f",
     "MacAddress": "02:42:ac:11:00:02",
     "IPv4Address": "172.17.0.2/16",
     "IPv6Address": ""
   }
 },
 "Options": {
   "com.docker.network.bridge.default_bridge": "true",
   "com.docker.network.bridge.enable_icc": "true",
   "com.docker.network.bridge.enable_ip_masquerade": "true",
   "com.docker.network.bridge.host_binding_ipv4": "0.0.0.0",
   "com.docker.network.bridge.name": "docker0",
   "com.docker.network.driver.mtu": "1500"
 },
 "Labels": {}
}
]
[vagrant@docker ~]$ ping 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.049 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.080 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.183 ms
^C
--- 172.17.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.049/0.104/0.183/0.057 ms
```

- Created container is attached to bridge network by default
 - Can be attached to user created networks as well with `--network` flag
- Container is assigned 172.17.0.2 ip in the bridge network and appears in the docker inspect command
- The container can then be pinged at 172.17.0.2

Docker network commands

Command	Description
docker network create	Create a network
docker network ls	List networks
docker network inspect	Detailed information on network
docker network rm	Remove network
docker network disconnect	Disconnect container from network
docker network connect	Connect container to network

Docker Overlay Networks

- Overlay networking for Docker Engine swarm mode comes secure out of the box. By default all nodes encrypt and authenticate ***network information*** they exchange using the AES algorithm in GCM mode. Manager nodes in the swarm rotate the key used to encrypt gossip data every 12 hours.
- You can also encrypt ***data*** exchanged between containers on different nodes on the overlay network. When you enable overlay encryption, Docker creates IPSEC tunnels between all relevant* nodes attached to the overlay network. These tunnels also use the AES algorithm in GCM mode and manager nodes automatically rotate the keys every 12 hours.
- To enable encryption, when you create an overlay network pass the --opt encrypted flag:

```
$ docker network create --opt encrypted --driver  
overlay my-multi-host-network
```

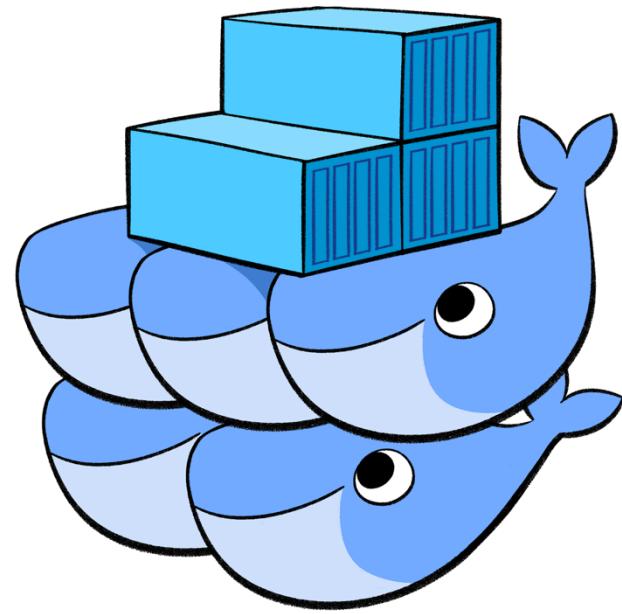
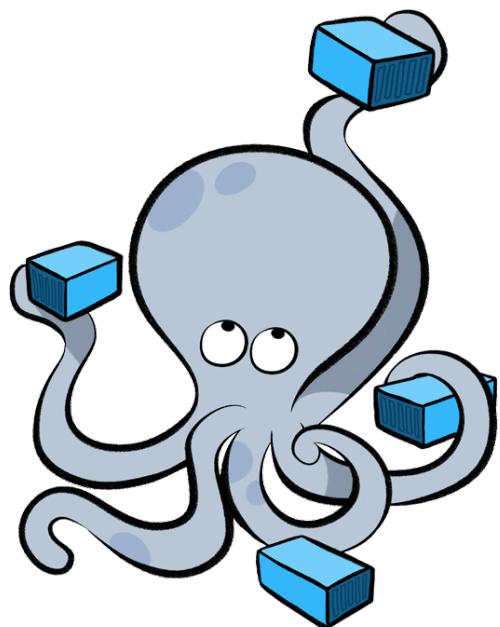
Docker Networks Exercise

- Run a redis container with default network
- Run a ubuntu container with default network
- Install redis-tools in host and check if you can connect to redis container and add some data
- Install redis-tools in ubuntu container and check if you can connect to redis container. (optional: create an image with redis-tools and ubuntu)
- Create a bridge network (bridgea)
- Run a ubuntu container with bridgea network and the new image, check if you can connect to redis – probably not
- Connect this new ubuntu container with “bridge” network, and check again if you can connect to the redis container

** keep inspecting network and container after every step

Part 5: DevOps Docker

Docker Compose/Swarm



Launching multiple containers is clumsy



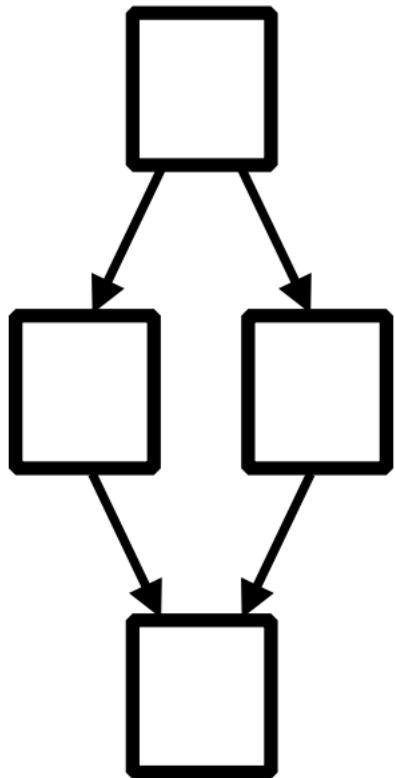
```
$ docker pull redis:latest
```

```
$ docker build -t web .
```

```
$ docker run -d --name=db redis:latest redis-server --  
appendonly yes
```

```
$ docker run -d --name=web --link db:db -p  
5000:5000 -v `pwd`:/code web python app.py
```

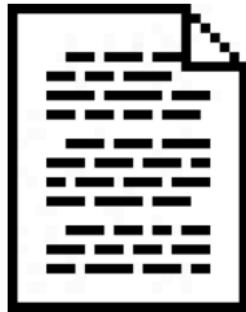
Launching multiple containers is clumsy



```
$ docker pull ...  
$ docker pull ...  
$ docker build ...  
$ docker build ...
```

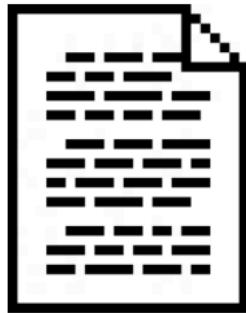
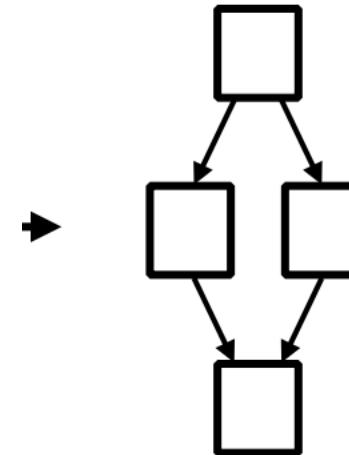
```
$ docker run ...  
$ docker run ...  
$ docker run ...  
$ docker run ...
```

Docker Compose or Swarm launches app with a single command



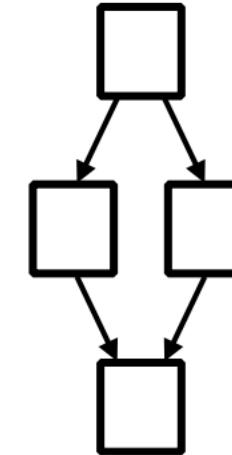
Text file

→ \$ docker-compose up



Text file

→ \$ docker stack deploy



Docker Compose commands

Command	Description
docker-compose up	(Re)build services
docker-compose kill	Kill the containers
docker-compose logs	Show the logs of the containers
docker-compose down	Stop and remove images, containers, volumes and networks
docker-compose rm	Remove stopped containers

Docker Compose to deploy a cluster



CLASSROOM WORK

First, install Compose:

<https://github.com/docker/compose/releases>

Then, Compose “Getting Started” Lab:

<https://docs.docker.com/compose/gettingstarted/>

Docker Swarm commands

Command	Description
<code>docker swarm init</code>	Create a swarm
<code>docker stack deploy</code>	Deploy the swarm
<code>docker stack services</code>	Show swarm services
<code>docker stack rm</code>	Remove stack

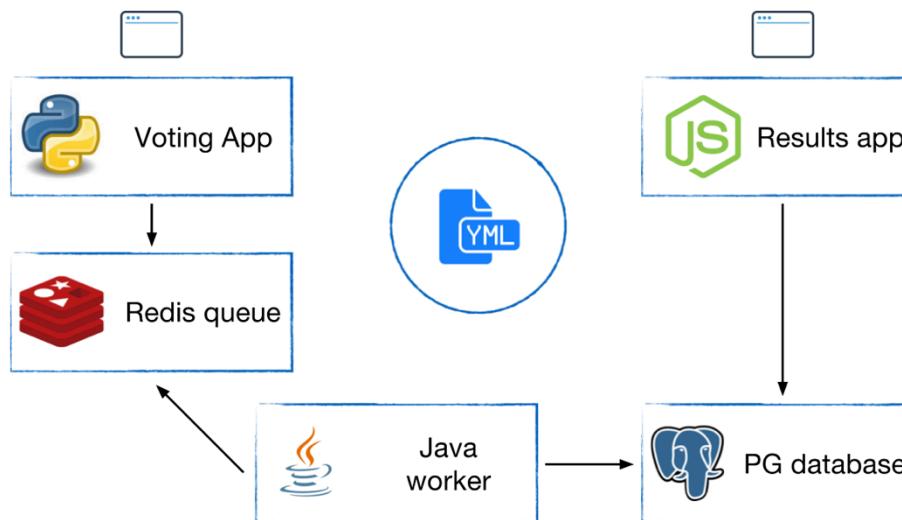
Docker Swarm to deploy a cluster



CLASSROOM WORK

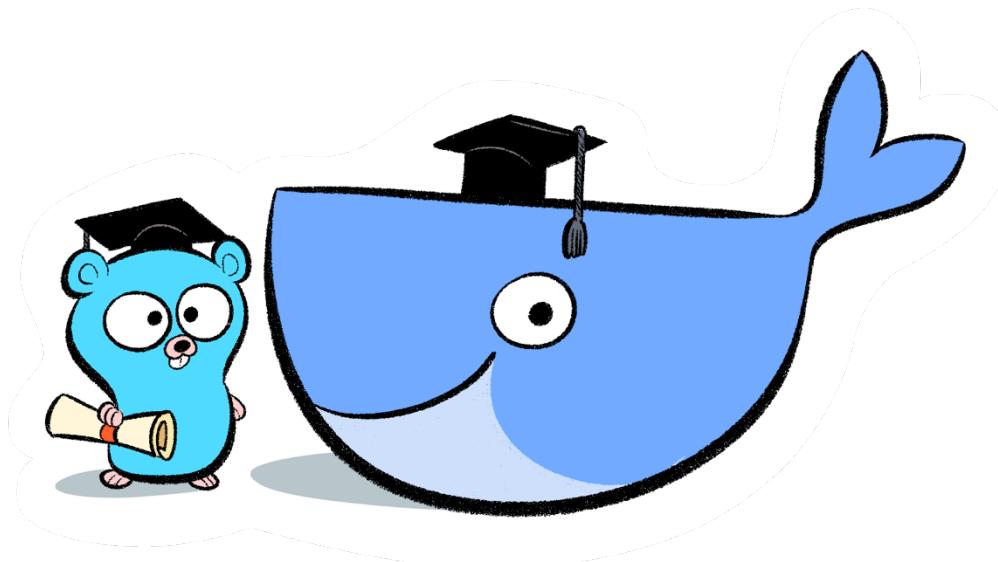
Exercise 3.0 in Docker Labs

<https://github.com/docker/labs/blob/master/beginner/chapters/votingapp.md>

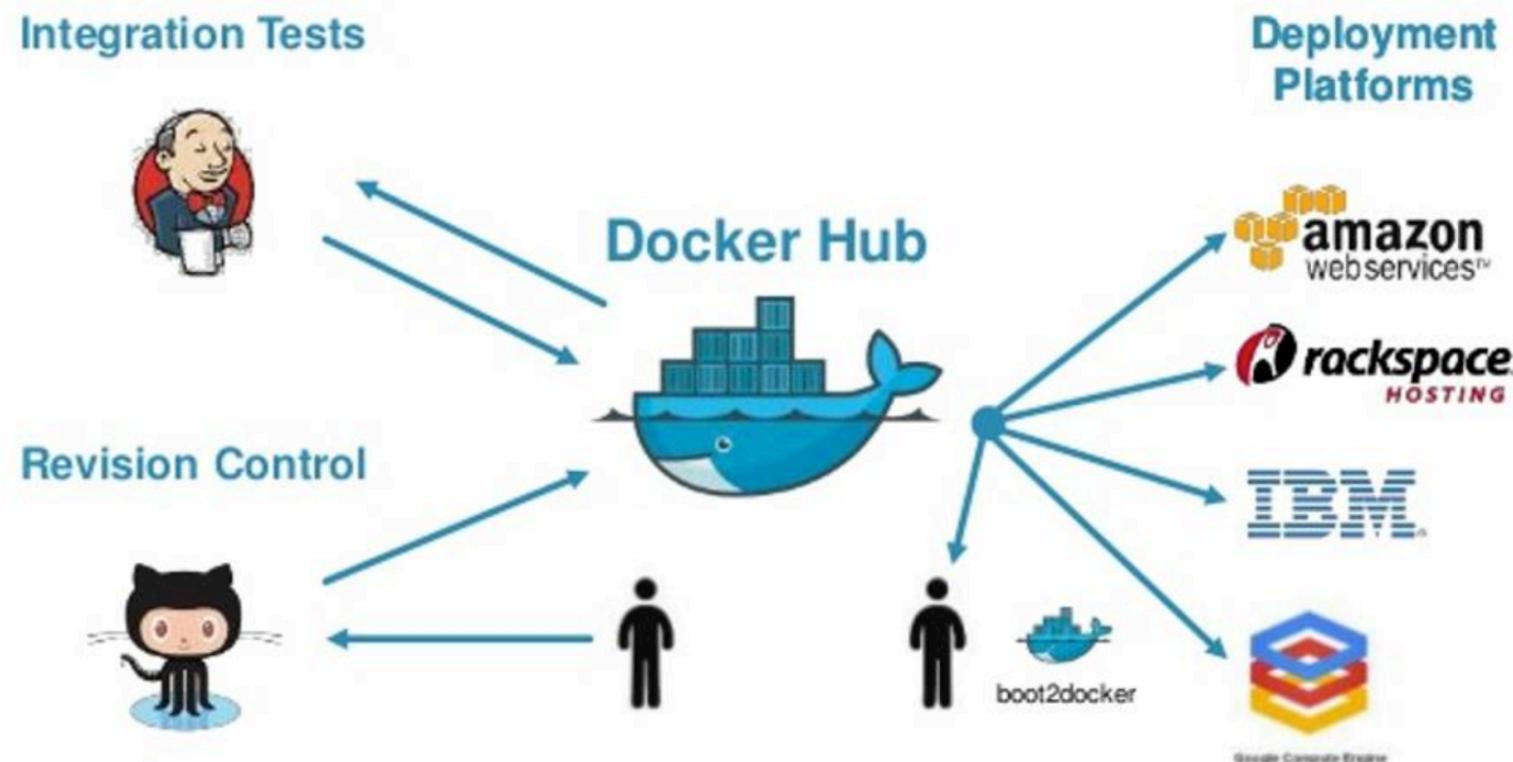


Part 6: DevOps Docker

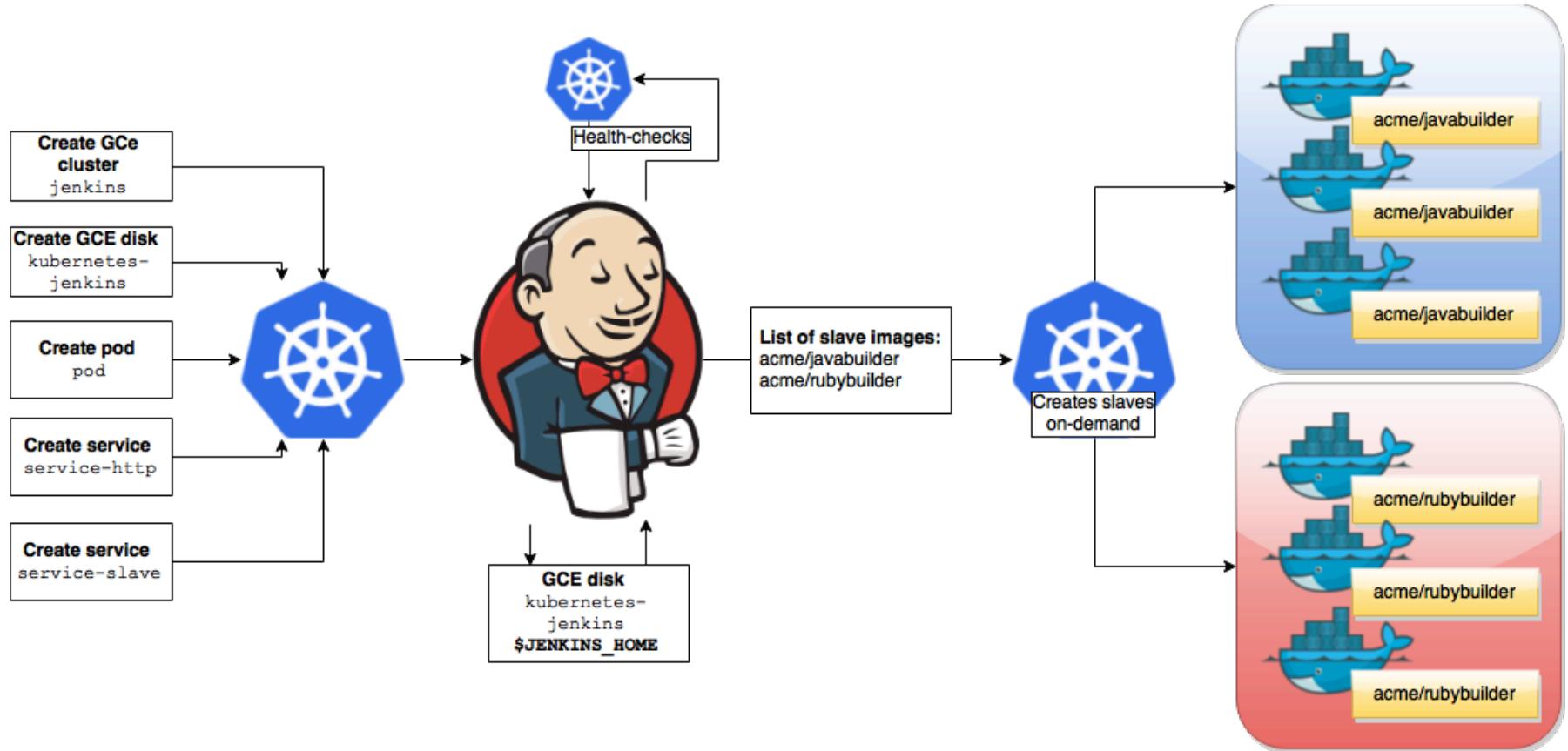
Docker Patterns



Docker Patterns

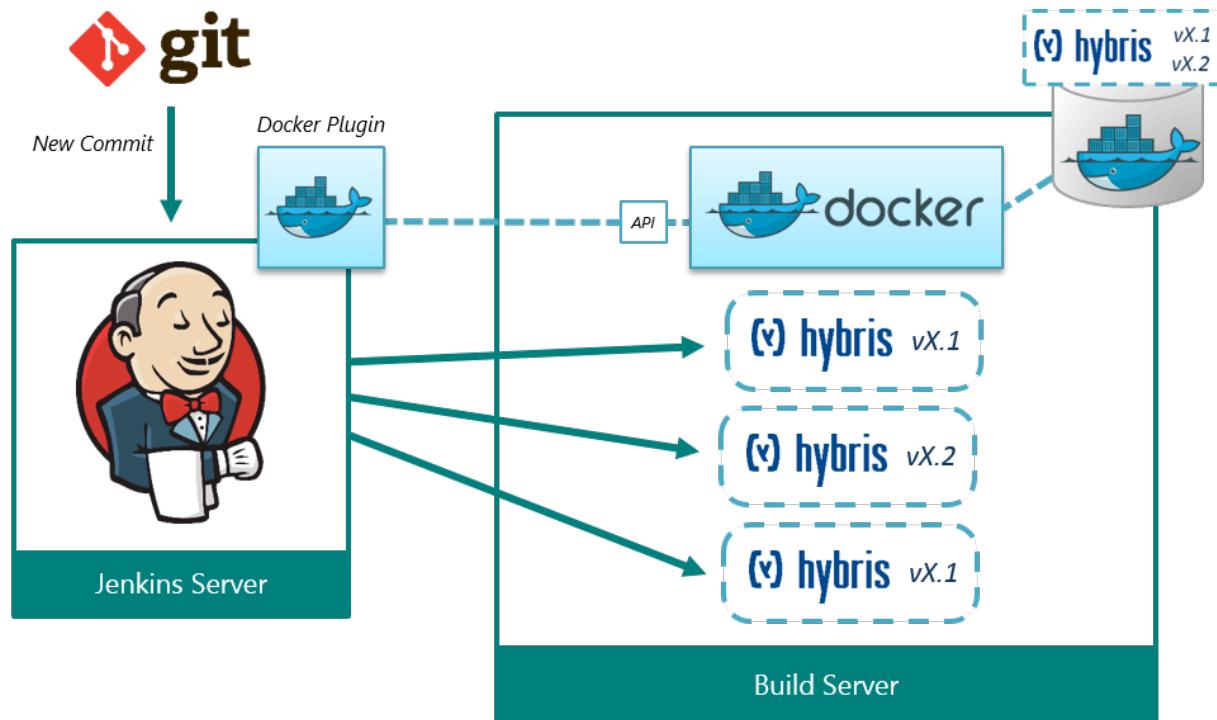


Jenkins Continuous Integration-Cloudbees



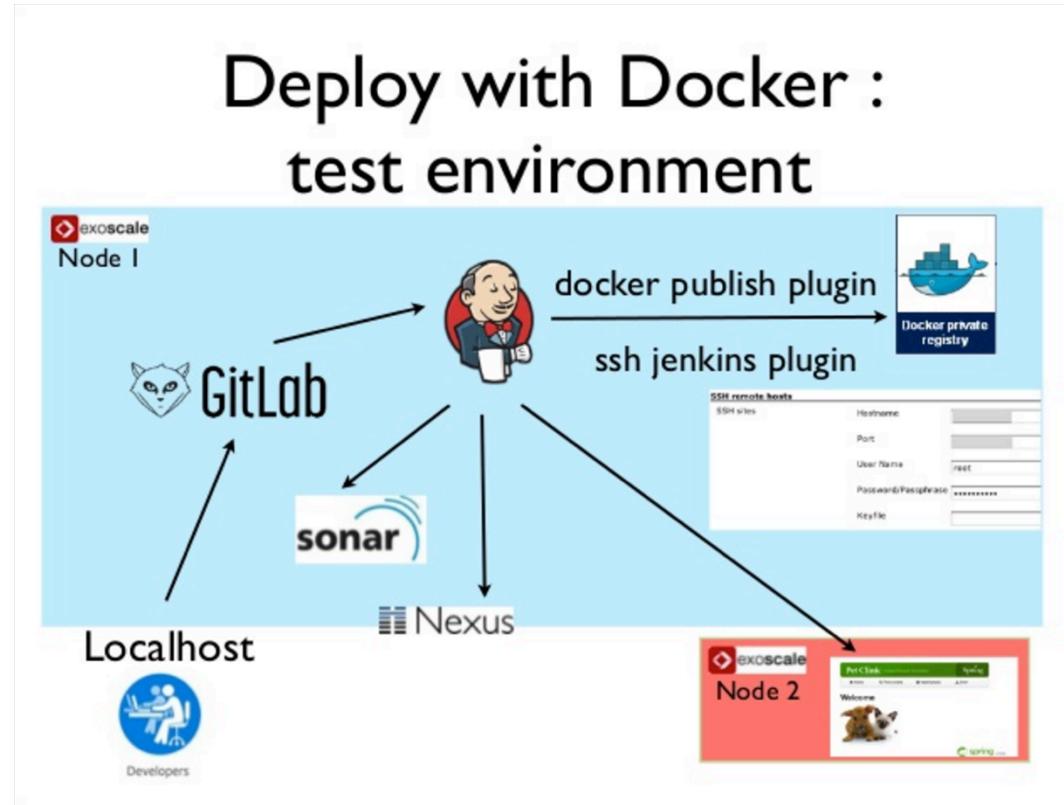
Link to Blog: Clustering Jenkins
<http://bit.ly/2a092Xo>

According to Michael Duke



Link to Blog: Docker as Jenkins Build Solution
<http://bit.ly/2a57Za8>

According to Julia Mateo



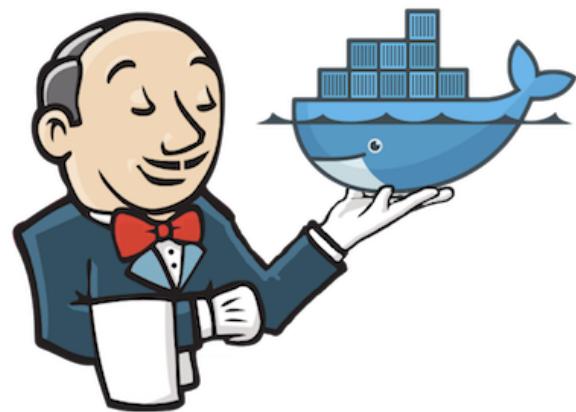
Link to Presentation: Continuous Delivery
<http://bit.ly/2aHZj9o>

Docker and Jenkins

Docker and Jenkins, a popular open source continuous integration tool, is a fairly common pattern, enough so that it is worth going into an example.

Spin up Jenkins in
a Docker
Container

Enable Jenkins to
create other
containers on the
Docker Host computer



How to run a ‘Host’ Docker command inside a ‘Client’ Docker container?

- Mount a Docker socket
 - Issuing a Docker run command with the Docker socket will enable you to manage host containers from within the client container
 - ‘`docker run -v /var/run/docker.sock:/var/run/docker.sock`’

Docker and Jenkins, Part 1



CLASSROOM WORK

Part 1, Jenkins Exercise in Docker Tutorials

This assignment is to set up a dockerfile that uses an official Jenkins image from Docker Hub, build an image with that image as a starting point, run a Jenkins container using the new image, and successfully get a Docker Hello world container running on the host but orchestrated from Jenkins in the container.

This exercise will help you practice Docker volume syntax as well as configure a client container (our Jenkins container) such that it can make calls to its host Docker engine.

Estimated time to complete: 20-30 min

Solution:

<https://github.com/papaludwig/docker-tutorials/tree/master/jenkins>

Sharing Persistent Volumes

```
[ubuntu@ubuntu-xenial:~/docker-workshop/jenkins$ docker create -v /var/jenkins_home --name jenkinstore library/jenkins
eef810fbad2247678db46187c0dec05d86a93397f27b40aff30640957977e15
[ubuntu@ubuntu-xenial:~/docker-workshop/jenkins$ docker volume ls
DRIVER          VOLUME NAME
local           e99cc1a13396614cd1d6eaf0b44be7544c6af0560a4ca93c8605e3bcfa0a7161

ubuntu@ubuntu-xenial:~/docker-workshop/jenkins$ docker volume inspect e99cc1a13396614cd1d6eaf0b44be7544c6af0560a4ca93c8605e3bcfa0a7161
[
  {
    "Name": "e99cc1a13396614cd1d6eaf0b44be7544c6af0560a4ca93c8605e3bcfa0a7161",
    "Driver": "local",
    "Mountpoint": "/var/lib/docker/volumes/e99cc1a13396614cd1d6eaf0b44be7544c6af0560a4ca93c8605e3bcfa0a7161/_data",
    "Labels": null,
    "Scope": "local"
  }
]

[ubuntu@ubuntu-xenial:~/docker-workshop/jenkins$ docker run --volumes-from jenkinstore --name jenkin1 -p 8080:8080 -p 50000:50000 library/jenkins
Running from: /usr/share/jenkins/jenkins.war
webroot: EnvVars.masterEnvVars.get("JENKINS_HOME")
Nov 23, 2016 4:58:27 PM Main deleteWinstoneTempContents

ubuntu@ubuntu-xenial:~/docker-workshop/jenkins$ docker run --volumes-from jenkinstore --name jenkin2 -p 8080:8080 -p 50000:50000 library/jenkins
Running from: /usr/share/jenkins/jenkins.war
webroot: EnvVars.masterEnvVars.get("JENKINS_HOME")
Nov 23, 2016 5:03:06 PM Main deleteWinstoneTempContents
WARNING: Failed to delete the temporary Winstone file /tmp/winstone/jenkins.war
```

Docker and Jenkins, Part 2



CLASSROOM WORK

Part 2, Shared Volumes Exercise in Docker workshop

The second assignment is to successfully share a persistent storage volume between two different Jenkins containers. Simulate the scenario of restoring your Jenkins state after a failure of the first container using the storage volume.

This exercise of sharing volumes could be extended to some simple open source databases as well.

Estimated time to complete: 15-25 min

Solution:

<https://github.com/papaludwig/docker-tutorials/tree/master/sharedvolume>

Docker and Jenkins, Part 3



CLASSROOM WORK

Part 3, Set up a Continuous Integration example.

Get a three-stage continuous integration pipeline working within your Jenkins container. This may involve installing additional plugins to your Jenkins instance (automate within your dockerfile) and adjusting the permissions on the Docker run command.

Estimated time to complete: 20-30 min

Solution:

<https://github.com/papaludwig/docker-tutorials/tree/master/ciexample>

Docker and Jenkins, Part 4



CLASSROOM WORK

Part 4, Call Continuous Integration Container from Docker Compose

Take the working code from Part 3 and summarize it with a call to Docker Compose. Docker Compose is a much more convenient interface and scales better when multiple containers must be invoked.

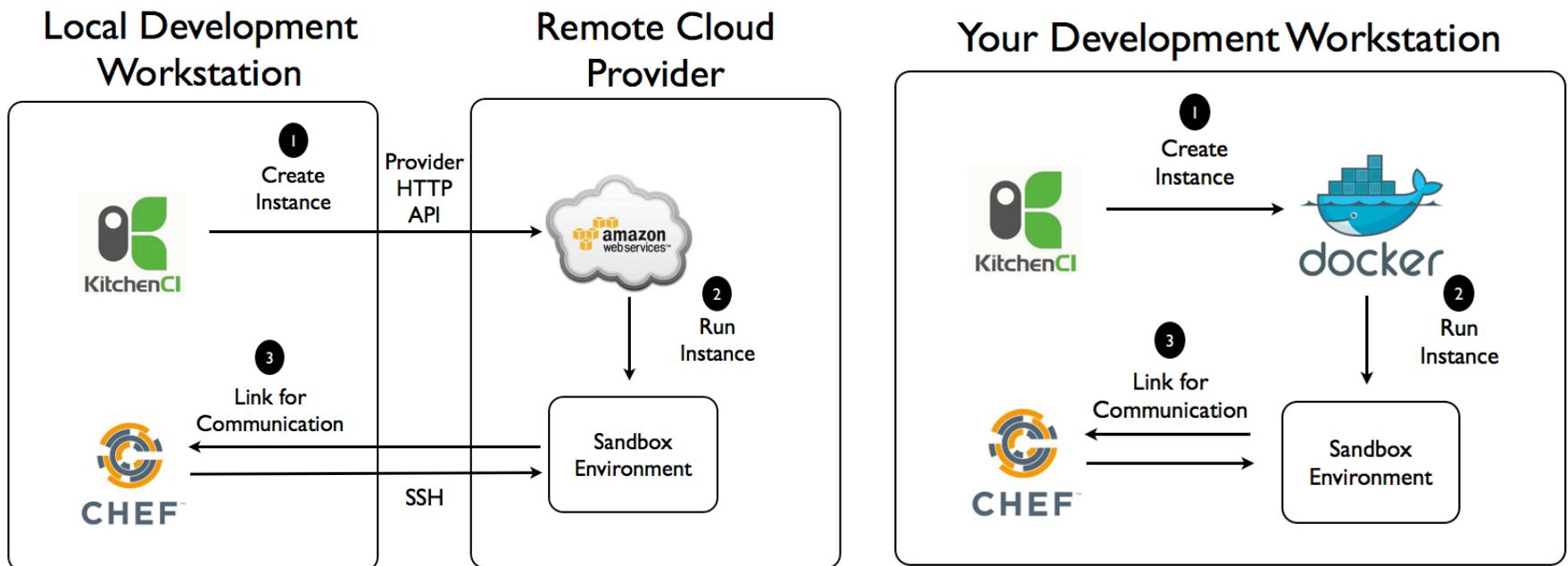
Bonus: Configure Jenkins container to skip setup workflow

Estimated time to complete: 15-25 min

Solution:

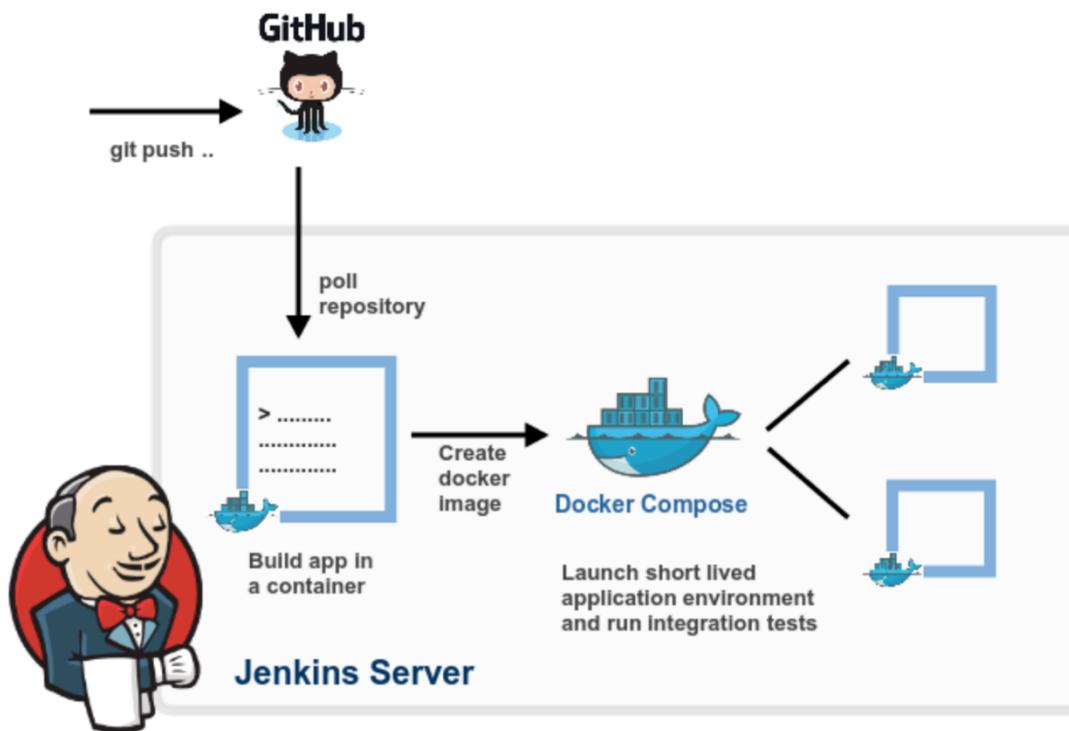
<https://github.com/papaludwig/docker-tutorials/tree/master/compose>

According to Mischa Taylor



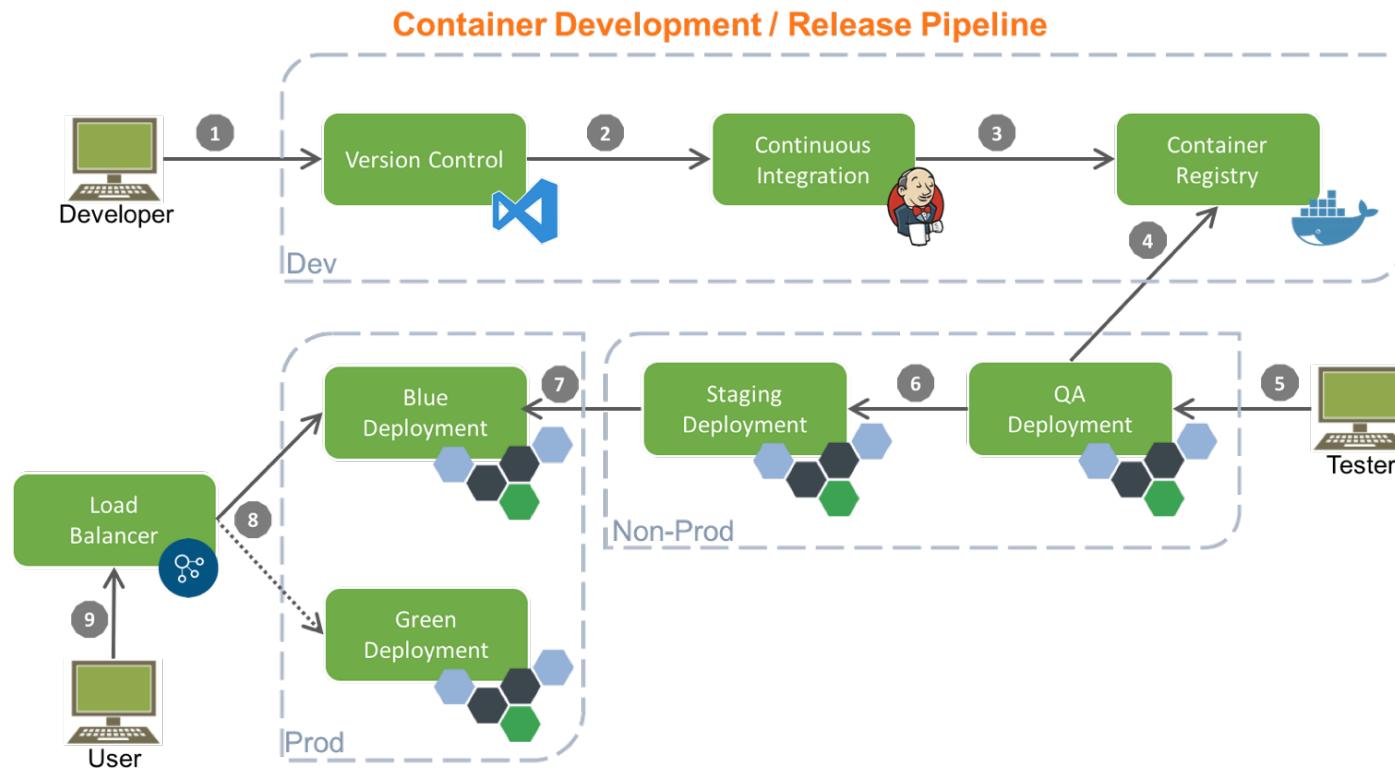
Link to Blog: Survey of Test Kitchen Providers
<http://bit.ly/2a56kS2>

According to Rancher



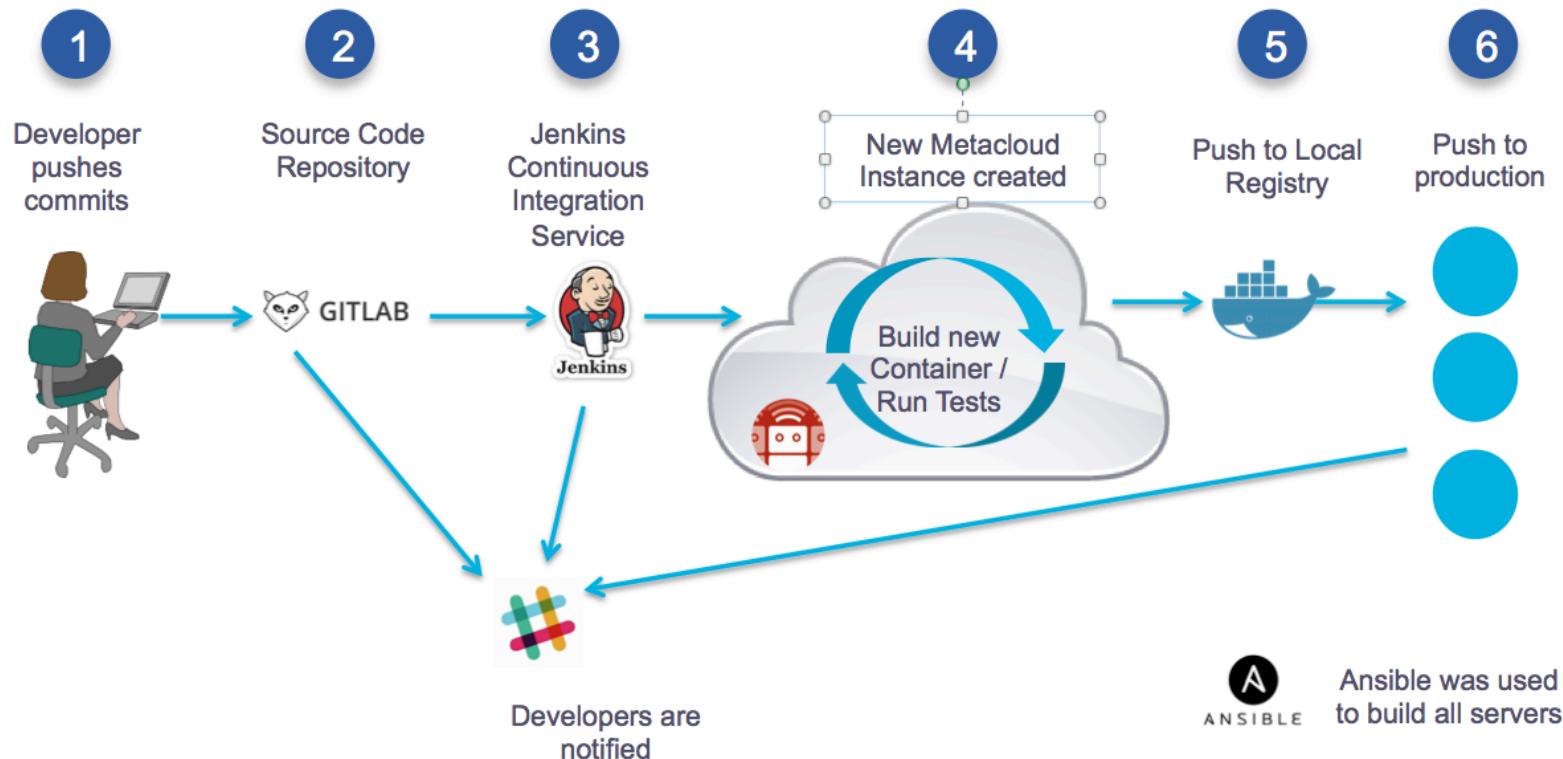
Link to Blog: Docker-based Build Pipelines
<http://bit.ly/2aHtu0K>

According to Robert Greiner



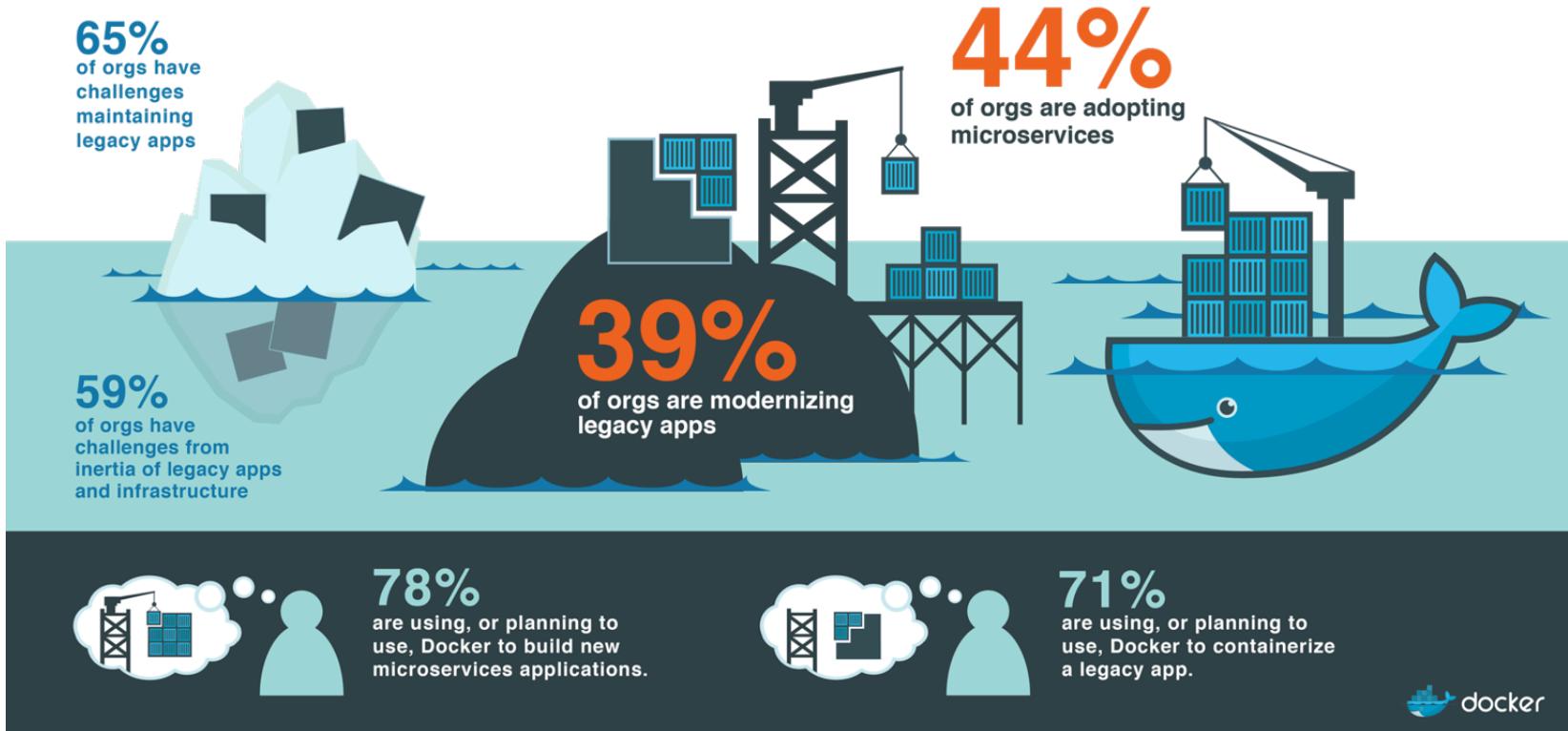
Link to Blog: Continuous Integration with Docker
<http://bit.ly/2aeA1io>

According to Vallard



Link to Blog: Continuous Delivery of a Simple Web Application
<http://bit.ly/2asS8G3>

Docker Adoption & Usage Data



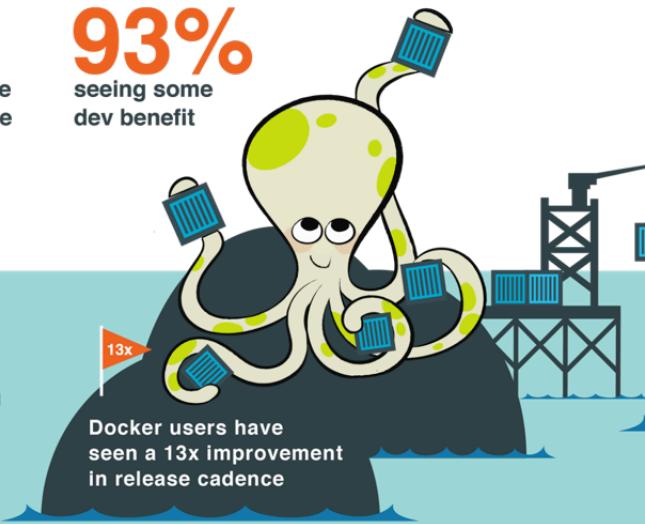
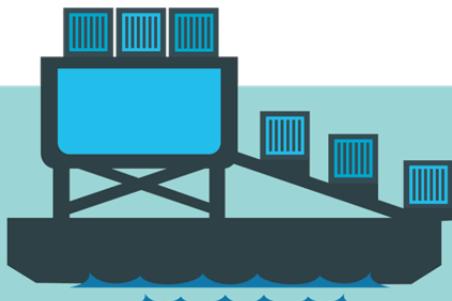
Docker Adoption & Usage Data

45%
of Docker users have
been able to increase
the frequency of
software releases

93%
seeing some
dev benefit

57%
Docker users
have seen
improvements
in operational
environment
management

85%
seeing some
ops benefit



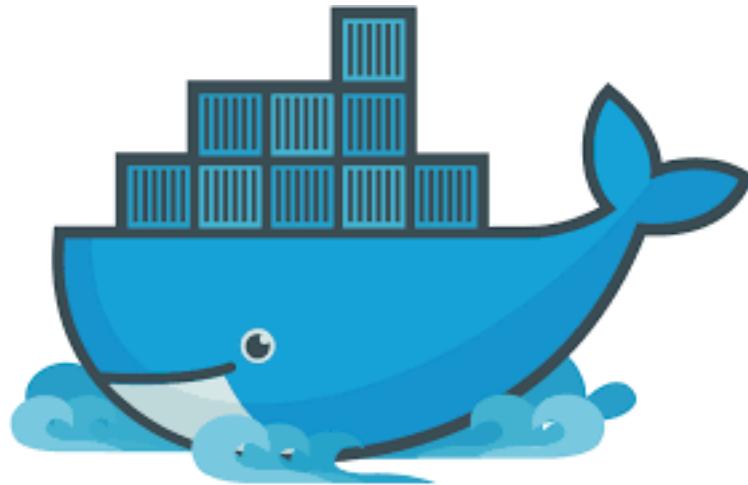
70%
of Docker users say
*'Docker has dramatically
transformed... etc'*



62%
have seen improved MTTR
on software issues.



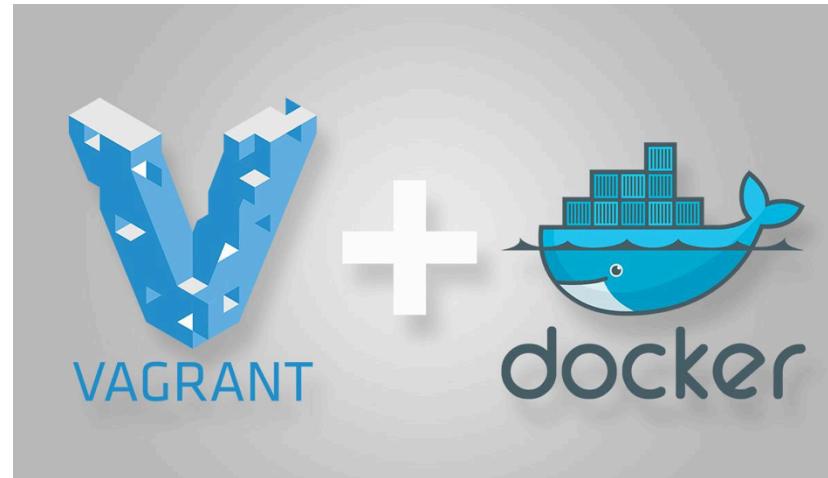
Local Docker Development



MacOS & Windows - The Old-Old Way

Vagrant Recipe for Local Docker Dev

1. Install Vagrant
<https://www.vagrantup.com/>
2. Install VirtualBox
<https://www.virtualbox.org/wiki/Downloads>
3. Git clone
<https://github.com/russmckendrick/monitoring-docker.git>
4. Enter vagrant-centos dir
 - cd vagrant-centos
5. Launch Centos VM (with docker installed)
 - vagrant up
6. Connect to Centos VM
 - vagrant ssh
7. Verify success!
 - docker run hello-world



MacOS & Windows - The Less-Old Way

Use Docker Toolbox / Machine Locally

- Ideal for older Mac and Windows systems that do not meet the requirements of Docker for Mac or Docker for Windows.
1. Install Docker Toolbox
<https://docs.docker.com/toolbox/overview/>
 - This one step gets you:
 - Native Docker CLI client
 - VirtualBox
 - Docker Machine (which can bring up a local Linux VM using VirtualBox)
 - Docker Compose
 - Kitematic (Docker GUI)
 - Docker QuickStart shell



MacOS & Windows - The New Way

Docker for Mac / Docker for Windows

- Simple one-step install
- Docker for Mac requires Mac OS 10.11 or newer running on 2010 or newer Mac hardware
- Docker for Windows requires 64bit Windows 10 Pro Enterprise and Education and Microsoft Hyper-V
- Both tools provide the full Docker environment as well as a convenient GUI for managing volumes, utilization, and networking
- Under the hood, it's docker-machine



Docker Machine - Docker Engine Provisioning

- Machine lets you create Docker hosts on your computer, on cloud providers, and inside your own data center. It creates servers, installs Docker on them, then configures the Docker client to talk to them. It also can provision Swarm clusters.
- ```
$ docker-machine create \
-d virtualbox default
```
- ```
$ docker-machine create \
-d digitalocean \
--digitalocean-access-token xxxxx \
docker-sandbox
```
- ```
$ docker-machine create -d amazonec2 \
access-key AKI***** \
--amazonec2-secret-key 8T93C***** \
aws-sandbox
```
- Local and Cloud drivers available



# New in Docker for Windows / Docker 1.13

## Native Windows Containers

- Certain very new versions of “Windows 10 Pro Enterprise and Education” and “Windows Server 2016” now have Windows kernels that support containerization and can be used to run native Windows Containers that run Windows applications in a container environment
- Requires Docker for Windows, and supports shared-kernel (“Windows Server Containers”) and VM-based (“Hyper-V Containers”)

Part 7: DevOps Docker

# Docker Security

---



# Security For Docker Images

- Secure Registry/Mirror Access
- Getting trustworthy images
  - trusted sources
    - docker hub / docker store
    - official images
    - pull by digest
  - private registry
  - building secure
- Docker Content Security
  - Docker Notary
    - Digitally signed images
      - "only signed content in production"
    - Yubico Keys can be used for code signing

# Docker Content Trust



## CLASSROOM WORK

In this exercise, we'll learn how to enable Docker Content Trust and sign images.

<https://github.com/docker/labs/blob/master/security/trust/README.md>

(Skip Step 5)

# Docker Bench Security

Docker Bench is an automated script that checks for dozens of best-practices around deploying Docker in production

<https://github.com/docker/docker-bench-security>

Run with the following command  
(available at the github page above)

```
docker run -it --net host --pid host --cap-add audit_control \
-v /var/lib:/var/lib \
-v /var/run/docker.sock:/var/run/docker.sock \
-v /usr/lib/systemd:/usr/lib/systemd \
-v /etc:/etc --label docker_bench_security \
docker/docker-bench-security
```

```
[vagrant@centos ~] vagrant@centos ~$ vagrant ssh - - ssh - vagrant ssh - 160 > 94
[b4/systemd:/usr/lib/systemd -v /etc/etc --label docker_bench_security /var/run/docker.sock:/var/run/docker.sock \v - /usr/lib
latest: Pulling from docker/docker-bench-security
462337f00000: Pull complete
865be1e00000: Pull complete
353237f00000: Pull complete
4886ba220000: Pull complete
Digest: sha256:3f884ca9ba3ba4bc9382b25c68728aaac2c58864d17c5a983285f155696bb
Status: Downloaded newer image for docker/docker-bench-security:latest
Docker Best Security v1.1.0
Docker, Inc. (c) 2015-
Checks for dozens of common best-practices around deploying Docker containers in production.
Inspired by the CIS Docker 1.11 Benchmarks
https://benchmarks.cisecurity.org/downloads/show-single/index.cfm?file=deckr16.110

Initializing Thu Dec 1 21:05:27 GMT 2016

[INFO] 1 - Host Configuration
[WARN] 1.1 - Create a separate partition for containers
[PASS] 1.2 - Use an updated Linux Kernel
[PASS] 1.4 - Ensure all non-root services from the host - Network
[PASS] 1.5 - Keep Docker up to date
[INFO] 1.6 - Using 1.12.3 which is current as of 2016-10-26
[INFO] 1.7 - Check with your operating system vendor for support and security maintenance for docker
[INFO] 1.8 - Docker daemon is maintained by the vendor to control Docker daemon
[INFO] 1.9 - docker:992:vagrant
[WARN] 1.7 - Failed to inspect: auditctl command not found.
[WARN] 1.8 - Failed to inspect: curl command not found.
[WARN] 1.9 - Failed to inspect: auditctl command not found.
[WARN] 1.10 - Failed to inspect: auditctl command not found.
[INFO] 1.11 - Audit Docker files and directories - docker.socket
[INFO] 1.12 - Audit Docker files and directories - /etc/default/docker
[INFO] 1.13 - Audit Docker files and directories - /etc/docker/daemon.json
[INFO] 1.14 - Audit Docker files and directories - /usr/bin/docker-containedr
[INFO] 1.15 - Audit Docker files and directories - /usr/bin/docker-runc
[INFO] 1.16 - Audit Docker files and directories - /usr/bin/docker-runcon
[INFO] 1.17 - Audit Docker files and directories - /var/run/docker.sock

[INFO] 2 - Docker Daemon Configuration
[WARN] 2.1 - Restrict network traffic between containers
[INFO] 2.2 - Set the log level
[PASS] 2.3 - Allow Docker to make changes to iptables
[PASS] 2.4 - Do not use insecure registries
[PASS] 2.5 - Do not use the aufs storage driver
[INFO] 2.6 - Docker daemon is listening on TCP port 2375
[INFO] 2.7 - Set default ulimit as appropriate
[INFO] 2.8 - Ensure ulimit values do not appear to be set
[WARN] 2.8 - Enable user namespace support
[PASS] 2.9 - Confirm default cgroup usage
[PASS] 2.10 - Do not change base device size until needed
[INFO] 2.11 - Use /dev/null as the base device
[WARN] 2.12 - Configure centralized and remote logging
[WARN] 2.13 - Disable operations on legacy registry (v1)

[INFO] 3 - Docker Daemon Configuration Files
[PASS] 3.1 - Verify that docker.service file ownership is set to root:root
[PASS] 3.2 - Verify that docker.service file permissions are set to 644
[INFO] 3.3 - Verify that docker.socket file ownership is set to root:root
[INFO] 3.4 - Verify that docker.socket file permissions are set to 644
[INFO] 3.5 - Verify that /etc/docker directory ownership is set to root:root
[PASS] 3.6 - Verify that /etc/docker directory permissions are set to 755
[INFO] 3.7 - Verify that /etc/docker/certificates directory ownership is set to root:root
[INFO] 3.8 - Verify that /etc/docker/certificates directory file permissions are set to 444
[INFO] 3.9 - Verify that TLS CA certificate file ownership is set to root:root
[INFO] 3.10 - Verify that TLS CA certificate file permissions are set to 444
[INFO] 3.11 - Verify that Docker server certificate file ownership is set to root:root
[INFO] 3.12 - No TLS Server certificate found
[INFO] 3.13 - Verify that Docker server certificate file permissions are set to 444
[INFO] 3.14 - Verify that TLS Server certificate found
[INFO] 3.15 - Verify that Docker server key file permissions are set to 400
[INFO] 3.16 - Verify that Docker socket file ownership is set to root:socket
[INFO] 3.17 - Verify that Docker socket file permissions are set to 666
[INFO] 3.18 - Verify that daemon.json file ownership is set to root:root
[INFO] 3.19 - Verify that daemon.json file permissions are set to 644
```





# Security

*10-15 Minutes*

---

# Docker Bench Results Discussion

<https://www.nearform.com/blog/securing-docker-containers-on-aws/>

# (Some) Docker Security Best Practices

- Access to Docker host = full access to all running containers and any new ones
- Docker containers can attach to volumes in read only mode with :ro option
  - Docker run -d -v /some/volume:ro jenkins
- Start Docker containers with the -u flag so that they run as an ordinary user instead of root. Consider dropping SUID support entirely in production containers
- Mitigate DoS by limiting CPU, RAM, Sockets that each container can consume
- Use seccomp (seccomp) to block system calls at kernel level. Use strace to determine kernel calls made, then create a profile file in json format and start the container using that profile file
  - docker run --rm -it --security-opt seccomp=custom\_profile.json custom\_app
- Log to stdout / stderr - so you can see with docker logs and docker can move to syslogs (for capture/rotate by ELK, etc.)

# Docker Security

- Stay up to date with the discussion at Docker's user group, forum, github issues, and IRC channel
  - <https://groups.google.com/forum/#!forum/docker-dev>
  - <https://forums.docker.com/>
  - <https://github.com/docker/docker/issues>
  - <https://docs.docker.comopensource/get-help/>
  - IRC #docker & #docker-dev

# Docker Security Scanning (formerly Project Nautilus)

- Docker Security Scanning conducts binary level scanning of your images before they are deployed, provides a detailed bill of materials (BOM) that lists out all the layers and components, continuously monitors for new vulnerabilities, and provides notifications when new vulnerabilities are found.
- Available for private Docker Hub repositories (potentially free)
- Available as a paid service to Docker Cloud customers, maintainers of “Official” repositories on Docker Hub, and Docker EE Advanced

<https://github.com/docker/labs/blob/master/security/scanning/README.md>

# Clair by CoreOS

- Robust free and open source image security scanning tool
- <https://github.com/coreos/clair>
- Static analysis of images for known vulnerabilities
- Integrates into CI pipelines

# **Swarm Mode Security**

- Swarm Mode was designed with security in mind
  - Keys required to join a swarm
    - Key rotation features built-in
  - All node communications (management channel) are encrypted.
    - Certificates required for node communications
    - Certificate rotation features built-in
  - Overlay network management channel communications encrypted by default
    - Overlay network data may be easily encrypted by setting flag at network creation time
    - Key and certificate rotation features built-in

# Swarm Security Basics



## CLASSROOM WORK

In this exercise, we'll play with some of Swarm's built-in service node management security features.

<https://github.com/docker/labs/blob/master/security/swarm/README.md>

# Secrets Management

- ENV variables - NOT recommended
  - General-purpose Key/Value Pair solutions
    - Vault
    - Keywhiz
  - Embedded in orchestration
    - Docker 1.13+ - recommended
    - Kubernetes secrets
  - Custom solutions
    - Make sure you care as much as Docker et al.

# Swarm Secrets Management



## CLASSROOM WORK

In this exercise, we'll use Docker's secrets objects to share a secret across nodes in a swarm.

1. Make sure your host is not participating in a swarm
  - a. docker swarm leave
2. Create (and join) a new swarm:
  - a. mkdir ~./secrets
  - b. cd ~./secrets
  - c. docker swarm init

<https://github.com/docker/labs/tree/master/security/secrets>

# **eval( this.class );**

- Please fill out our online course evaluation, which gives you immediate access to your certificate of completion.
  - All responses are confidential even though an email address is requested.
1. Go to: **www.metricsthatmatter.com/ASPE**
  2. From the drop down menu choose **Docker Containerization Boot Camp, site, instructor name, class start date**
  3. Enter email address, answer the questions, provide desired written feedback, and click submit.

# **THANK YOU !!!**