**Content**

[1. Introduction 3](#_Toc68532366)

[1. Definition of docker 3](#_Toc68532367)

[2. Kernel 3](#_Toc68532368)

[3. Subsystem 4](#_Toc68532369)

[4. Chroot 4](#_Toc68532370)

[5. LXC – Linux Containers 4](#_Toc68532371)

[6. LMCFTY by Google 4](#_Toc68532372)

[7. Namespaces and cgroups 4](#_Toc68532373)

[8. COW – Copy On Write pattern 5](#_Toc68532374)

[9. Alpine 7](#_Toc68532375)

[10. Virtualization vs Containerization 8](#_Toc68532376)

[2. Dockerfile 9](#_Toc68532377)

[3. Docker commands 11](#_Toc68532378)

[4. Working with Docker 13](#_Toc68532379)

[1. Creating a Docker Image 13](#_Toc68532380)

[5. Docker compose – communication between the containers. 14](#_Toc68532381)

[1. docker-compose.yml 15](#_Toc68532382)

[2. docker compose commands 16](#_Toc68532383)

[6. Deployment of docker application 17](#_Toc68532384)

[1. Docker volumes 18](#_Toc68532385)

[7. Using Docker behind the proxy 19](#_Toc68532386)

[8. containerd 20](#_Toc68532387)

[9. Docker Swarm 22](#_Toc68532388)

[1. Swarm commands 22](#_Toc68532389)

[10. Kubernetes 23](#_Toc68532390)

[11. Mesos 24](#_Toc68532391)

[12. Helm 25](#_Toc68532392)

[13. TODO 26](#_Toc68532393)

1. Introduction
   1. Definition of docker

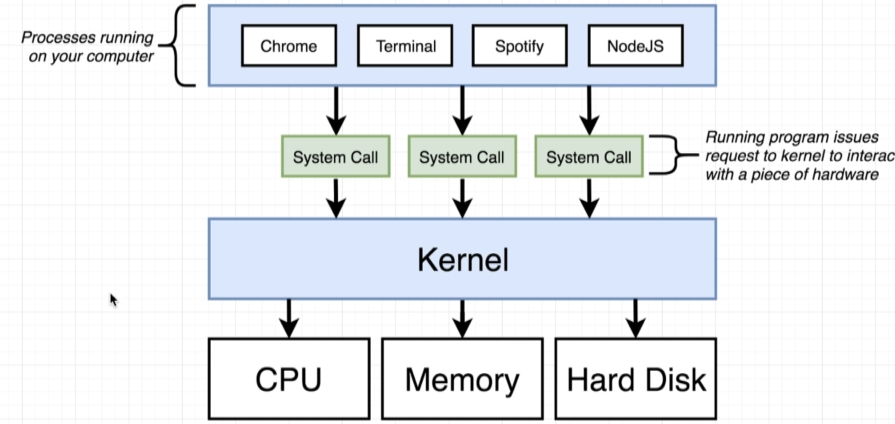
Docker describes themselves as "an open platform for developers and sysadmins to build, ship, and run distributed applications".

Docker is a revolutionary software development platform to deploy apps. Apps are packaged in containers that can be run on any OS.

Docker allows you to run containers. A container is a sandboxed process running an application and its dependencies on the host operating system. The application inside the container considers itself to be the only process running on the machine while the machine can run multiple containers independently.

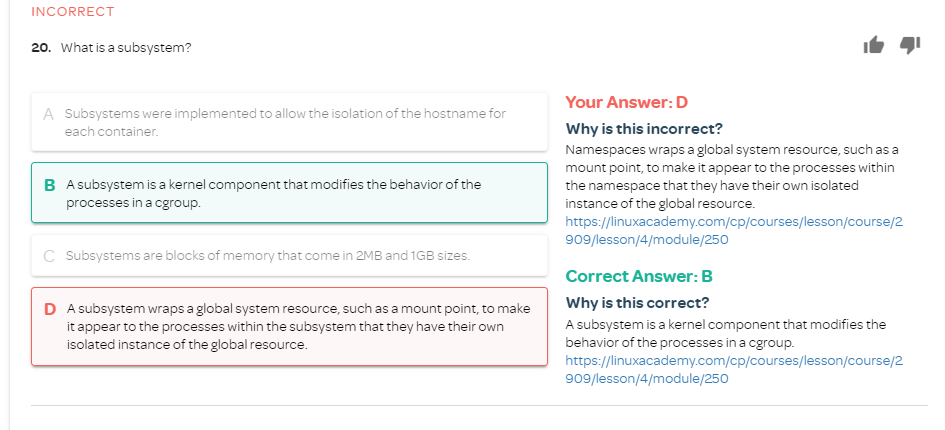
* 1. Kernel

**The Kernel** is a running software process that governs access between all the programs that are running on your computer and all the physical hardware that is connected to your computer as well. Intermediate layer that governs access between the programs and the actual hard drive.

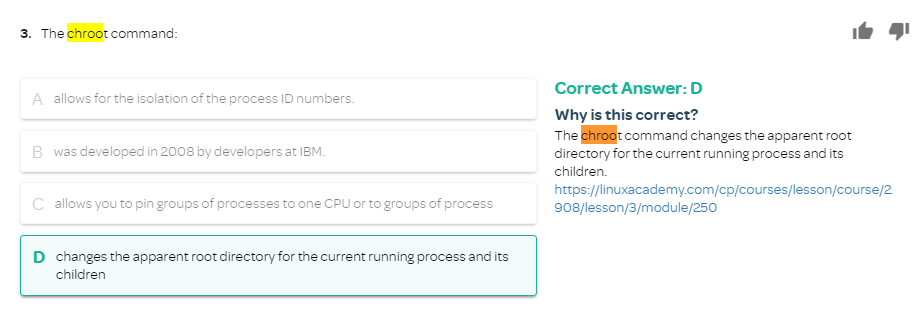


**CentOS** (Community Enterprise Operating System) is a Linux distribution that provides a free, enterprise-class, community-supported computing platform functionally compatible with its upstream source, Red Hat Enterprise Linux (RHEL).[5][6] In January 2014, CentOS announced the official joining with Red Hat while staying independent from RHEL,[7] under a new CentOS governing board.[8][9]

* 1. Subsystem



* 1. Chroot

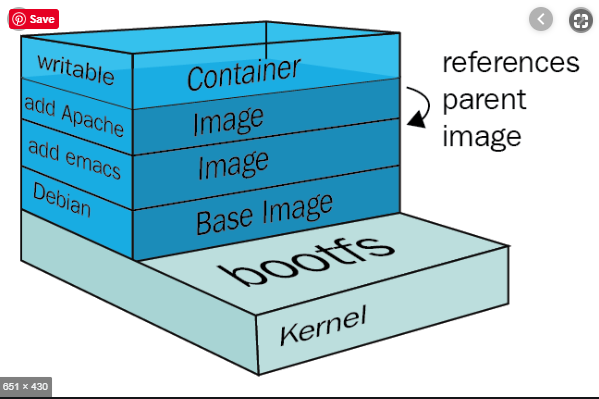


* 1. LXC – Linux Containers

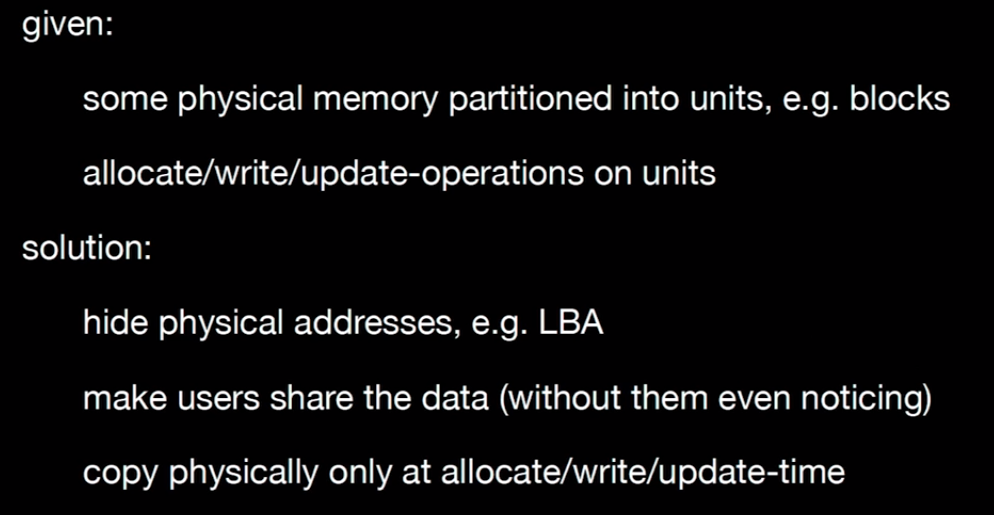
Let’s users create and manage system or application containers

* Chroot
* Kernel Namespaces
* SELLinux / Apparmor
* Seccomp policies
  1. LMCFTY by Google
  2. COW – Copy On Write pattern

Union Capable File System – Union Mounting – a way of combining multiple directories into one that appears to contain their combined contents.

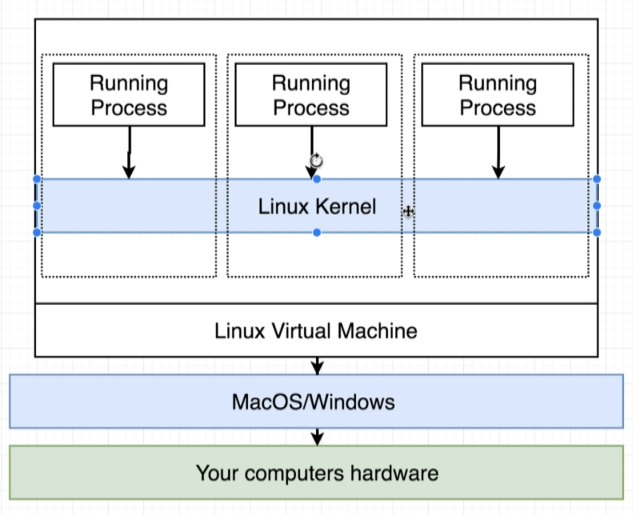


COW – Copy on write (pattern) – after you have hidden physical addresses, LBA (Logical Block Address) can point for the same Phy. Addr. While the files are identical, and only when updated, then duplicate the data.



Container is a running process along with a subset of physical resources on your there are allocated to that process specifically.

An image is really kind of a snapshot of the file system along with a very specific start up command. Namespacing and Control Groups are not are not included by default with all operating systems – they are linux specific.

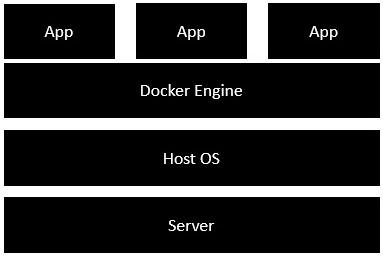
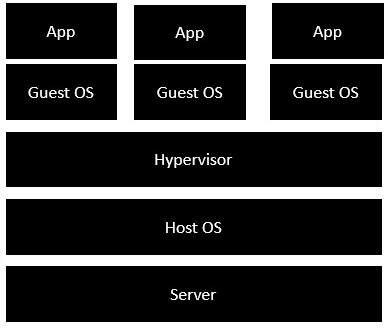


* 1. Alpine

Is a term in the docker world for an image that is as small and compact as possible. Many popular repositories are going to offer Apline versions of their image (node:alpine). In an alpine version of an image you’re not going to get a bunch of additional pre-installed programs. So the default node installation might include extra programs like say get or a package manager or text editor …

When alpine you get the absolute most strict down version. Only ping and node :D mbe text editor. If we need node and npm we are good to go w this.

* 1. Virtualization vs Containerization

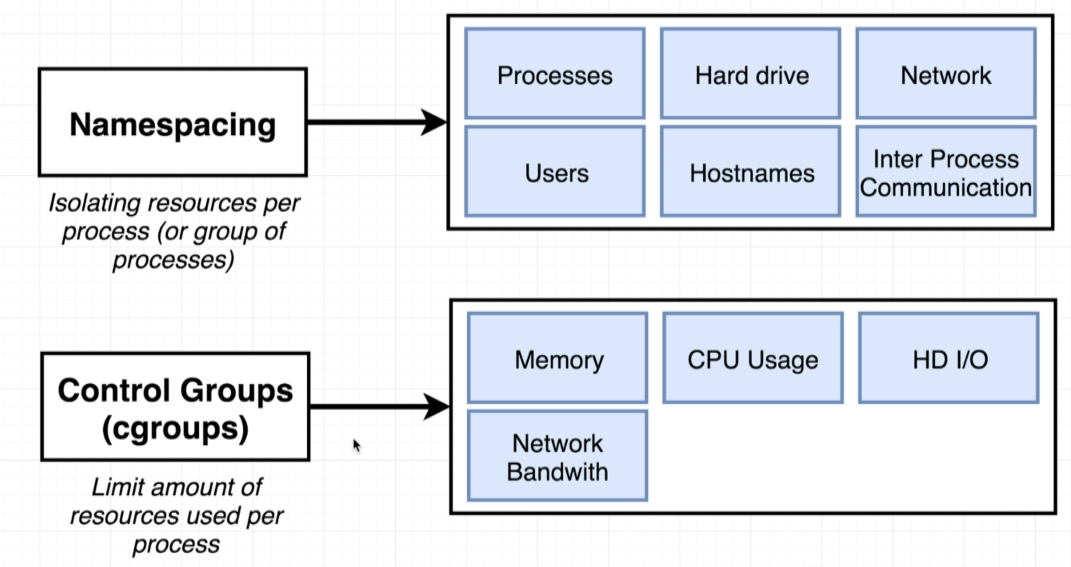


A **hypervisor** (or virtual machine monitor, VMM, virtualizer) is computer software, firmware or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources: for example, Linux, Windows, and macOS instances can all run on a single physical x86 machine. This contrasts with operating-system-level virtualization, where all instances (usually called containers) must share a single kernel, though the guest operating systems can differ in user space, such as different Linux distributions with the same kernel.

The term **hypervisor** is a variant of **supervisor**, a traditional term for the kernel of an operating system: the hypervisor is the supervisor of the supervisors, with hyper- used as a stronger variant of super-. The term dates to circa 1970;[2] in the earlier CP/CMS (1967) system, the term Control Program was used instead.

1. Namespaces and cgroups

Namespaces limit what you can see, CGroups limit what you can use.



* 1. Namespaces

Namespaces are features of the linux kernel, limit what other programs can see, but these programs are not even aware that they are limited. The application is not aware, that he is in a container. He thinks, he is the only app running on the os. You dont even need to change the app in order to put it into a container. Docker isolate containers so they dont communitace with each other and dont interfere with each others resources in any way.

Docker Engine uses the following namespaces on Linux:

* PID namespace for process isolation.
* NET namespace for managing network interfaces.
* IPC namespace for managing access to IPC resources.
* MNT namespace for managing filesystem mount points.
* UTS namespace for isolating kernel and version identifiers. You can use viamultiple containers multiple versions of the linux kernel.
* User namespaces: requires special configuration. Allows container processes to run as root inside the container while mapping that user to an unpriviliged user on the host. The container sees itself running as root, but in fact it is not.
  1. CGroups

**Control Groups** – limit the amount of resources that a particular process can use. So namespacing is for saying: Hey, this area of the harddrive is for this proess, a control group can be used to limit the amount of memory that a process can use, the amount of CPU, the amount of harddrive I/O and network bandwidth.

Docker Engine uses the following cgroups:

* Memory cgroup for managing accounting, limits and notifications.
* HugeTBL cgroup for accounting usage of huge pages by process group.
* CPU group for managing user / system CPU time and usage.
* CPUSet cgroup for binding a group to specific CPU. Useful for real time applications and NUMA systems with localized memory per CPU.
* BlkIO cgroup for measuring & limiting amount of blckIO by group.
* net\_cls and net\_prio cgroup for tagging the traffic control.
* Devices cgroup for reading / writing access devices.
* Freezer cgroup for freezing a group. Useful for cluster batch scheduling, process migration and debugging without affecting prtrace.

1. Dockerfile
2. FROM – specify the docker image what we want to use as base

FROM alpine

1. RUN – execute some commands while we are preparing our custom image

RUN apk add –update redis

1. CMD – what shuld be executed when our image is used to start up a brand new container

CMD [“redis-server”]

1. LABEL
2. MAINTAINER (deprecated)
3. EXPOSE

EXPOSE 3000 – to expose a given port

1. ENV
2. ADD
3. COPY

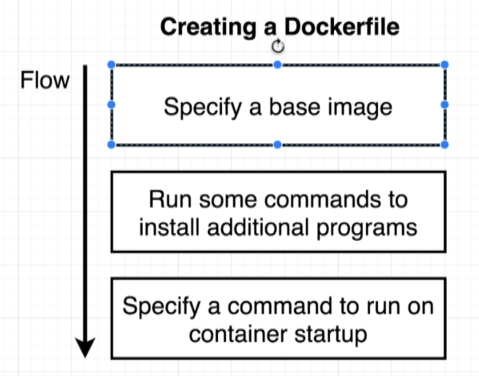
COPY ./ ./ or COPY <src> <dest> or COPY index.html /var/www/index.html

1. ENTRYPOINT
2. VOLUME
3. USER
4. WORKDIR

WORKDIR /path/to/workdir

The WORKDIR instruction sets the working directory for any RUN, CMD, ENTRYPOINT, COPY and ADD instructions that follow it in the Dockerfile. If the WORKDIR doesn’t exist, it will be created even if it’s not used in any subsequent Dockerfile instruction. Effects even the docker exec command.

1. ARG
2. ONBUILD
3. STOPSIGNAL
4. HEALTCHECK
5. SHELL



**Minimizing Cache Busting and Rebuilds**



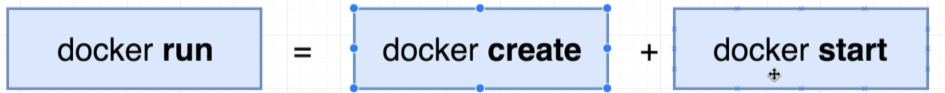
I moved the npm install command up. Now if you change the index.js the npm install does not need to rerun. Cache in the dockerfile works until the first change.

1. Docker commands

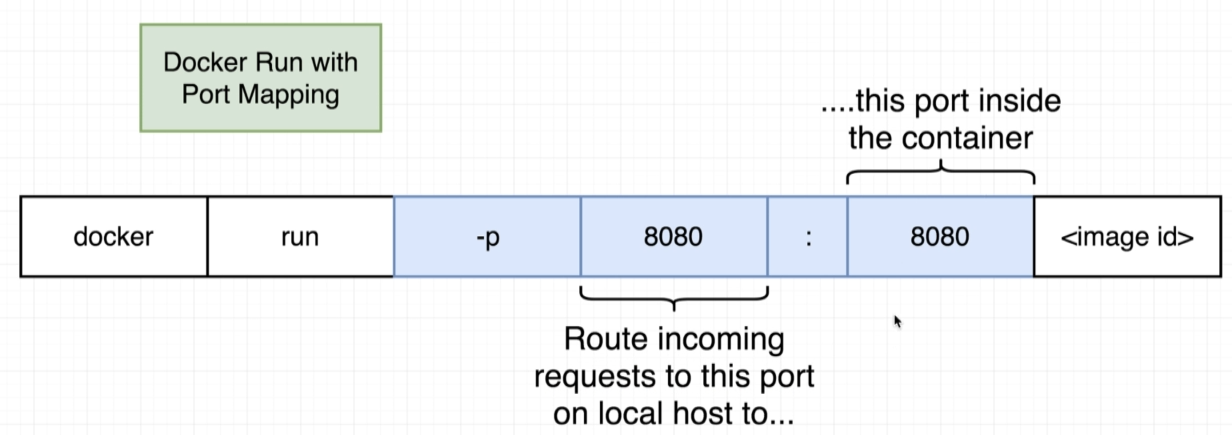
* cat /etc/\*-release – get your linux distribution

1. Docker run <image name> <override initial command>

Create a container out of an image.



The process of creating the container is where we kind of take the file system in here and kind of prep it for use in this new container when we create the container. To start we execute the startup program.



* These 2 ports do not have to be identical e.g. 5000:8080 -> localhost:5000 (we redirected it to 5000)

1. docker ps - to verify if docker is running? List containers (running)!
   1. Docker ps –a lists all of the images on the computer
2. docker images
3. docker rmi ImageID
4. sudo service doker start / stop / status
5. docker logs <container id> -> retrieve logs gen. by a given image
6. docker system prune (deletes even the cache) – delete the containers that are sitting around and eating up the space.
7. docker stop <container id> : a hardware signal is sent to the prim process of the container (SGITERM)
8. docker kill <container id> : SIGKILL
9. docker exec –it <container id> <command> (exec – run command in a running container)

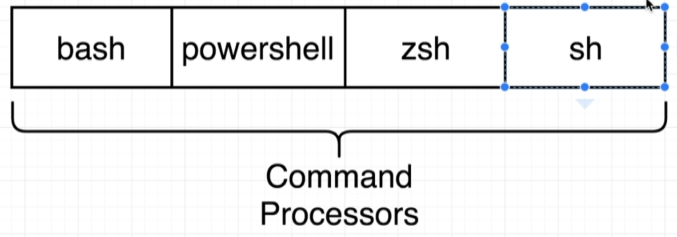
* -i standard in
* -t text formatting?

Open up a shell or a terminal in a context of your running container:

1. Docker exec –it <container id> sh

-a : attached? Give me any output coming from there

Sh is a command processor, something that allows us to type commands in and have them be executed inside that container.



1. Docker run –it <image name> sh
2. Docker build .
3. Docker build –t brt:latest .

How to log in into docker with one single command using env vars.

1. Echo “$DOCKER\_PASSWORD” | docker login –u $DOCKER\_ID –password\_stdin

Start up a new container and run shell. Give me access to that shell. Typical is to start with an initial process like web server and then attach to it the shell w docker exec.

* 1. Docker build

docker build [OPTIONS] PATH | URL | -

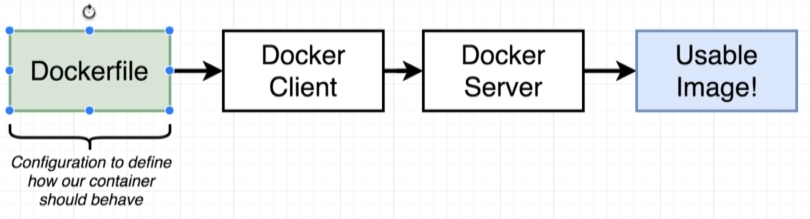
[OPTIONS]:

* –tag , -t
* --file , -f
* --no-cache

You can specify, path (where there is a dockerfile) url or pipe a docker file

docker build -f ctx/Dockerfile http://server/ctx.tar.gz

1. Working with Docker
   1. Creating a Docker Image

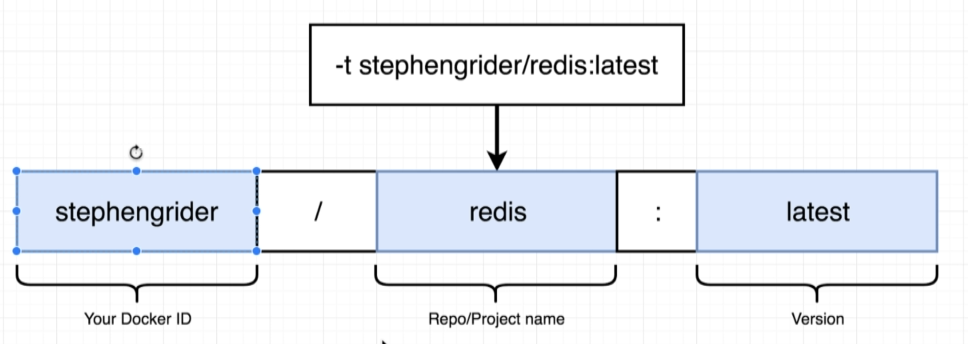


* Docker build .

(. – is the build context, set of files that belongs to our projects)

Docker Cache – if you want to change your Dockerfile you want the change to happen as far down as possible – the order matters when caching.

-t (tag the image, so we will not need to memorize / copy the image IDs )



Alpine and redis – these does not contain the docker ID because they are community images.

Whenever you want to create a custom image name it <docker id>/ …

* Docker commit –c ‘CMD [“redis-server”]’ <container id> (add a default command)

Pref Dockerfile because it is reusable. – fluid relation between containers and images.

1. Docker compose – communication between the containers.

FROM node:alpine

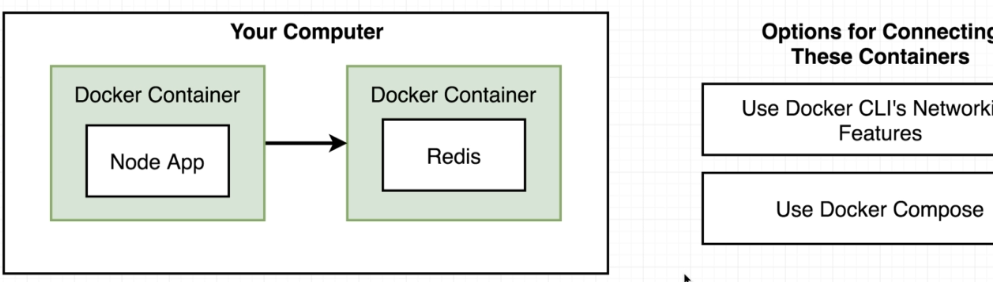
WORKDIR ‘/app’

COPY package.json .

RUN npm install

COPY . .

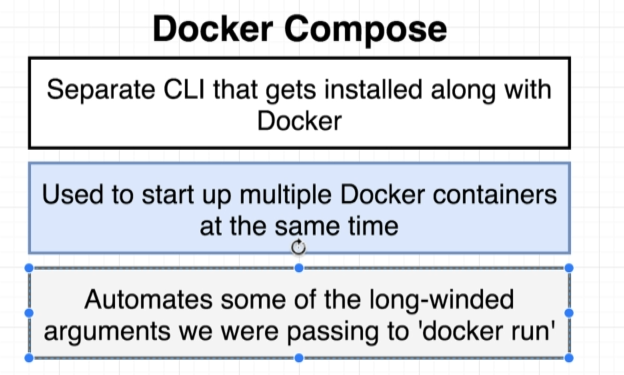
CMD [“npm”, “start”]



These 2 containers have no automatic communication between them. To allow the node app to be able to reach the Redis server and store some information we need to setup some networking infrastructure between them two.

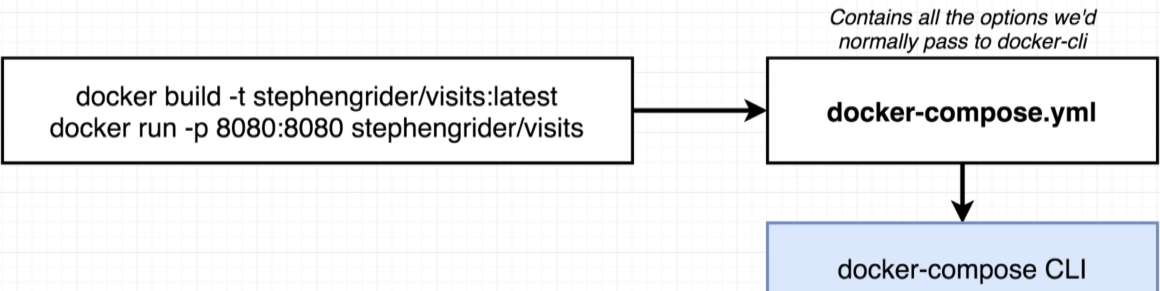
**Docker Swarm:** When you are trying to manage containers across multiple physical or virtual machines.

**Docker Compose**: When you are trying to define a multi container application. It’s a separate CLI, gets installed with the docker. Docker compose really exists to keep you from having to write out a tons of different repetitive commands with the docker cli.



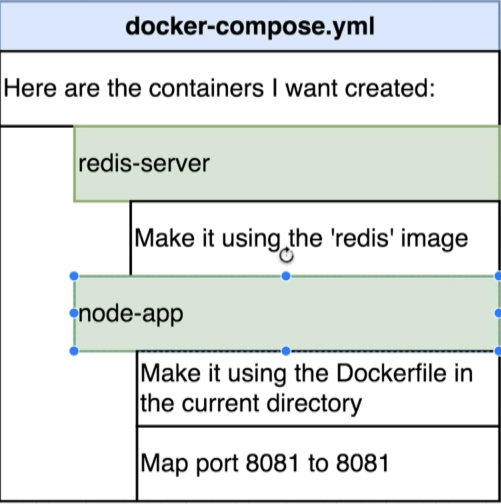
**Docker Networks**: rtfm.

* 1. docker-compose.yml

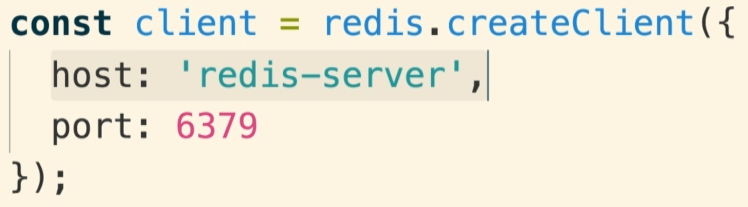


To make use of docker compose we’re going to use the same commands – docker build, docker run – but we will encode them into a very special file: **docker-compose.yml**. (w special syntax)

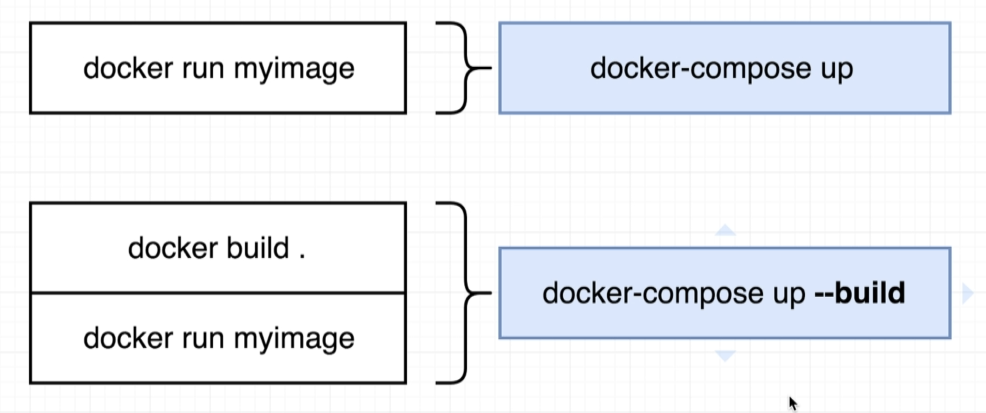
\*Map: map the port of the image to the local machine



To refer on the server from the node.js code:



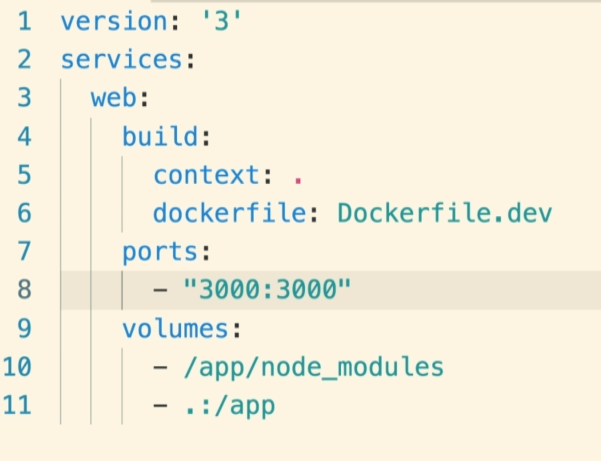
* 1. docker compose commands



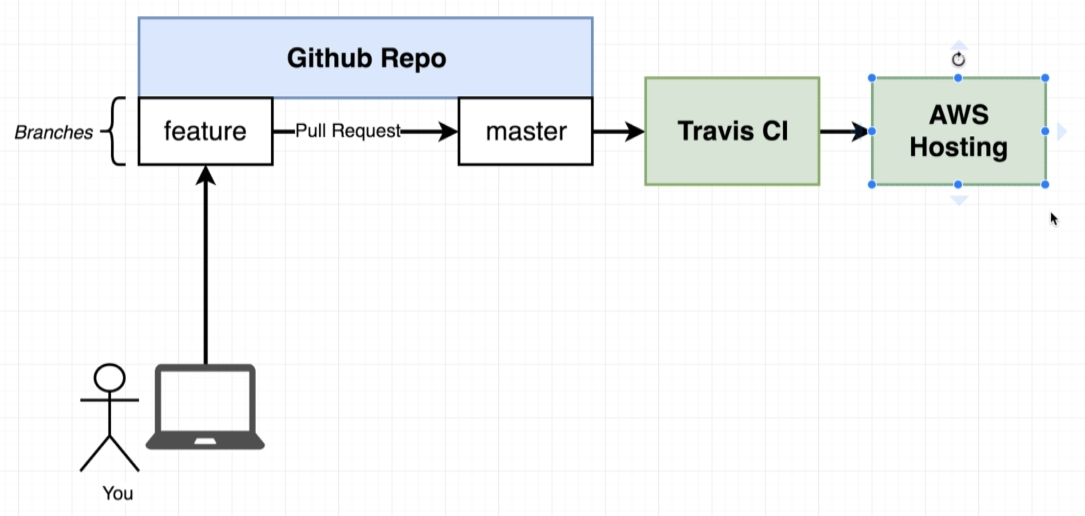
Remember: one of the main purpose of docker compose is to make docker run easier.

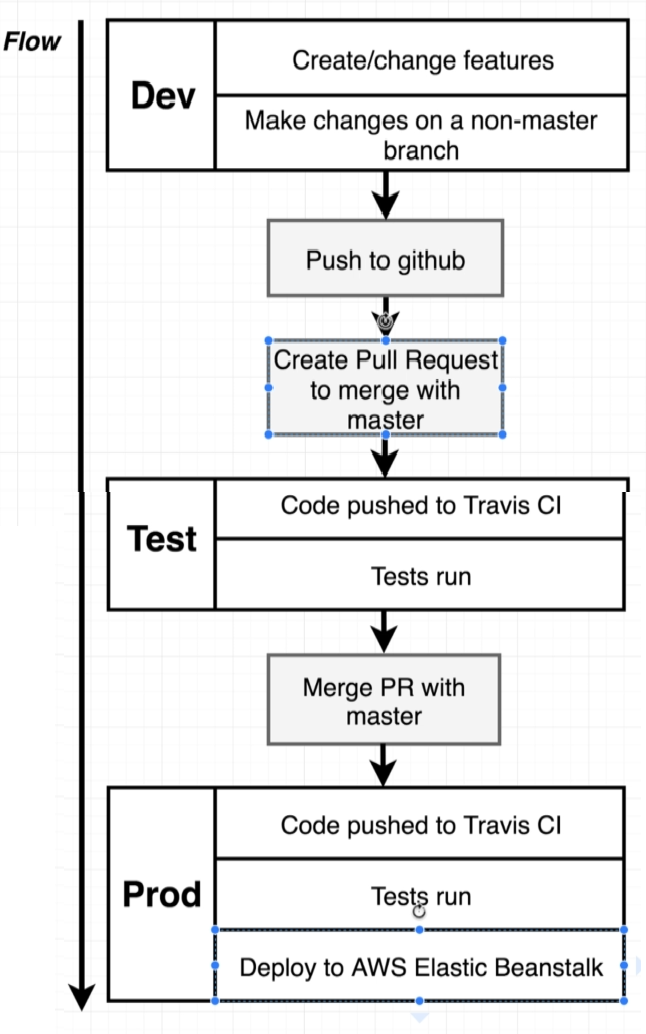
1. Docker-compose down

Next: Container Maintenance with Compose mp4



1. Deployment of docker application





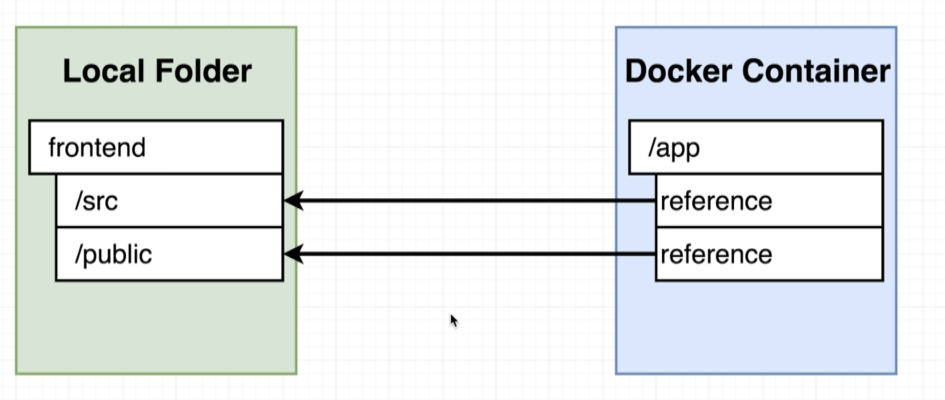
**Dockerfile.dev –** anytime we want to run docker build with custom dockerfile name:

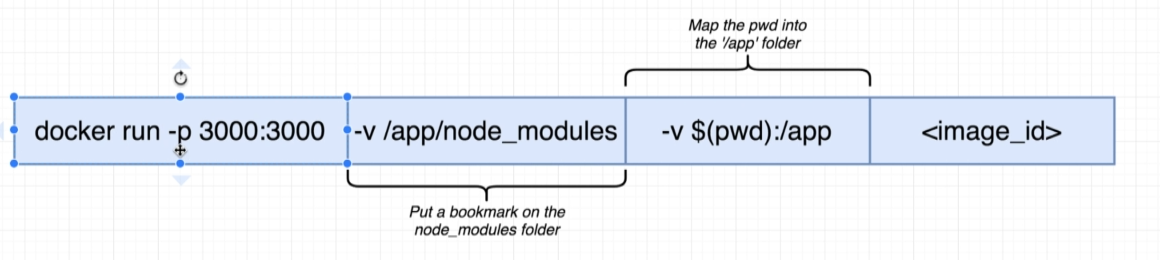
Docker build –f Dockerfile.dev

* 1. Docker volumes

**Get changes propagated to running container –** we do not want to rebuild the image. Image takes a snapshot of a source code so the changes will not be by default reflected.

Using volumes we will not copy the source to the image but use references.





**pwd** – **P**resent **W**orking **D**irectory

-v without the :/ - don’t try to map it up against

1. Using Docker behind the proxy

Create a systemd drop-in directory for the docker service:

$ sudo mkdir -p /etc/systemd/system/docker.service.d

Create a file called /etc/systemd/system/docker.service.d/http-proxy.conf that adds the HTTP\_PROXY environment variable:

[Service]

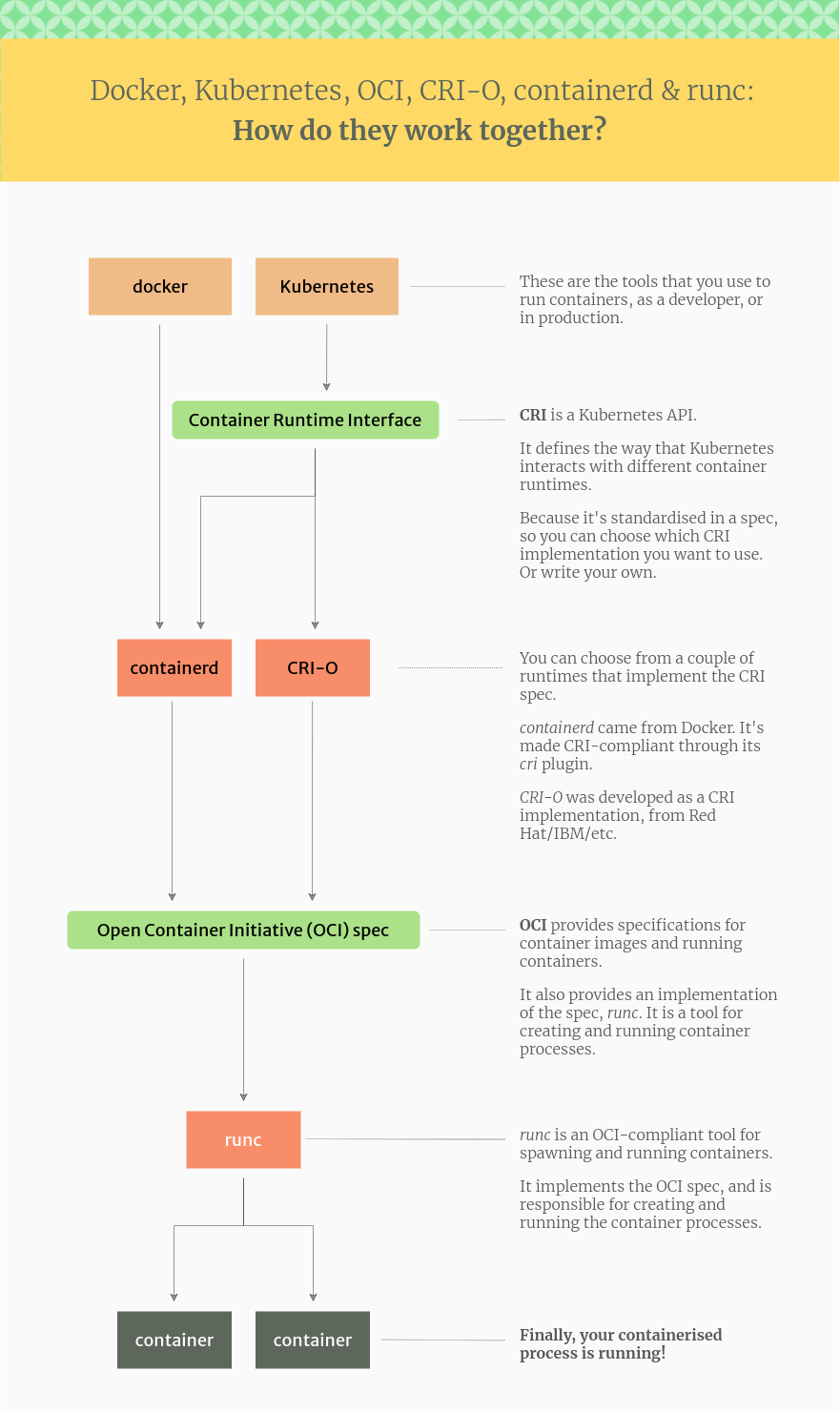
Environment="HTTP\_PROXY=http://proxy.example.com:80/"

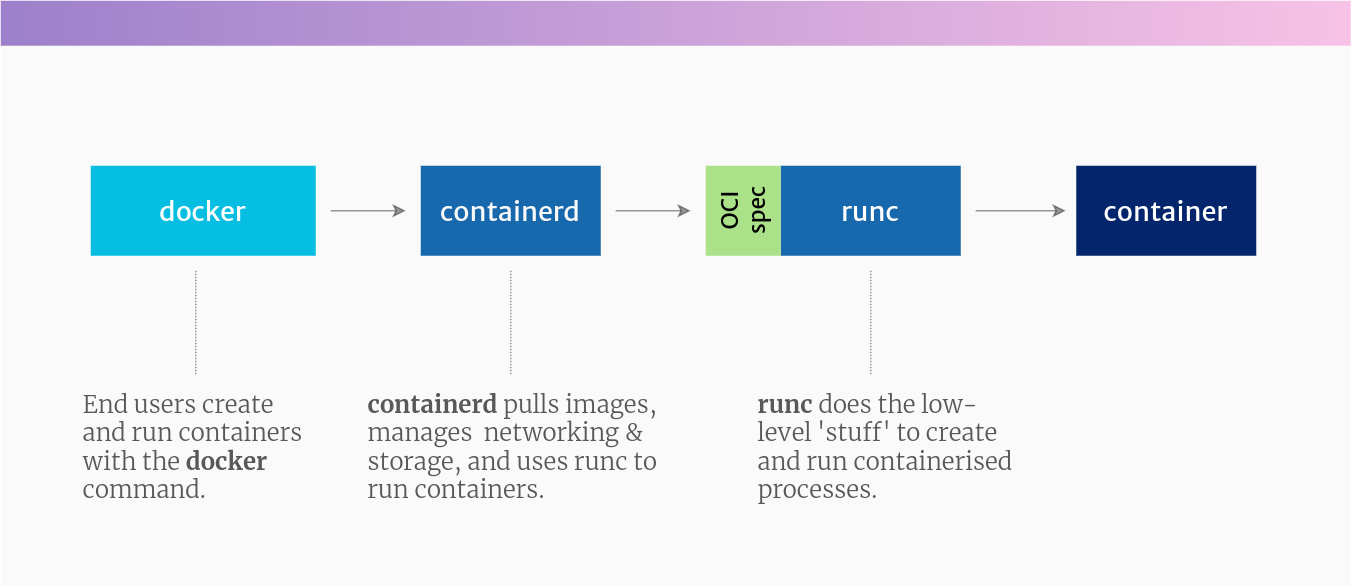
$ sudo systemctl daemon-reload

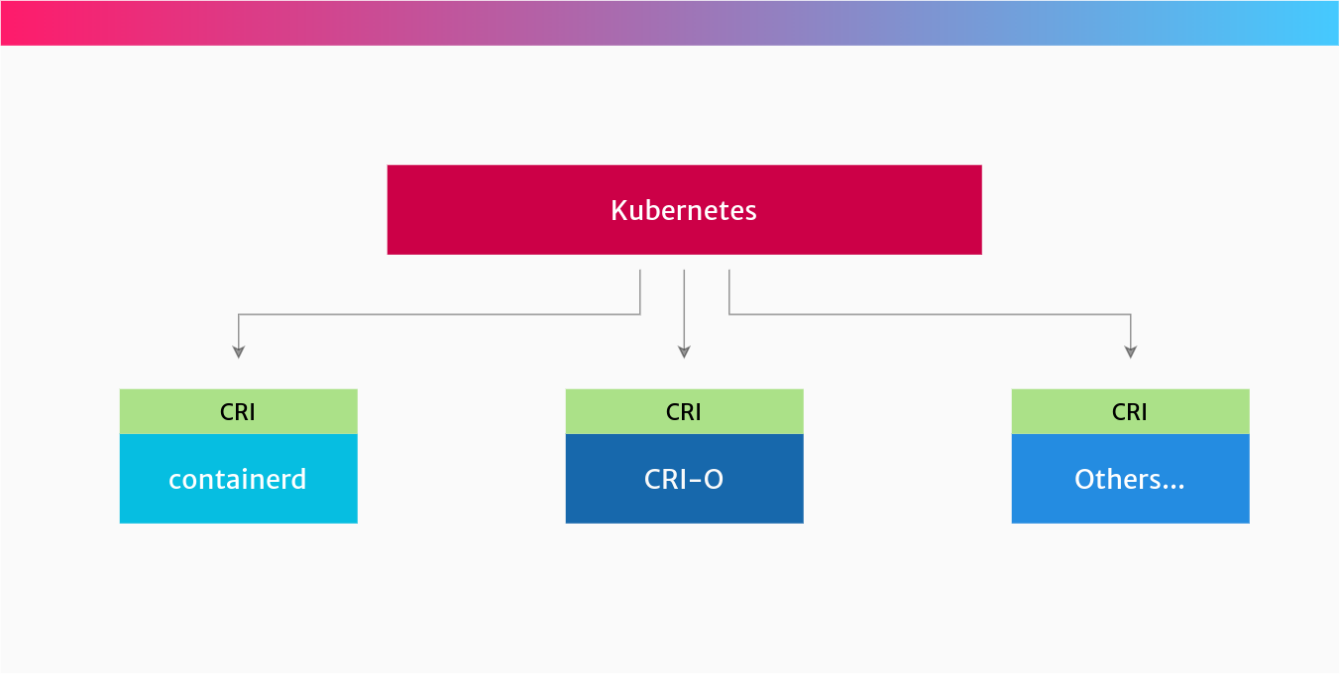
$ sudo systemctl restart docker

$ systemctl show --property=Environment docker

Environment=HTTP\_PROXY=http://proxy.example.com:80/

1. containerd





1. Docker Swarm

Swarm (raj)

* Cluster management integrated with Docker Engine

Docker CLI allows you to create a swarm of Docker Engine, where you can deploy your application. No additional software is needed.

* Declarative service model

Allows you to define the desired state of the various services in your application stack

* Scaling
* Desired state reconciliation
* Multi-host networking
* Service Discovery
* Load Balancing
* Security
* Rolling updates
  1. Swarm commands
* Docker swarm init
* Docker swarm join
* Docker node ls (works on master)
* Docker service (the task that is going to be executed by the manager and then pushed out to the worker nodes to actually implement it, central structure of the swarm system)
* Docker service create –replicas 2 –p 80:80 –name myweb nginx
* Docker service ls

1. Kubernetes

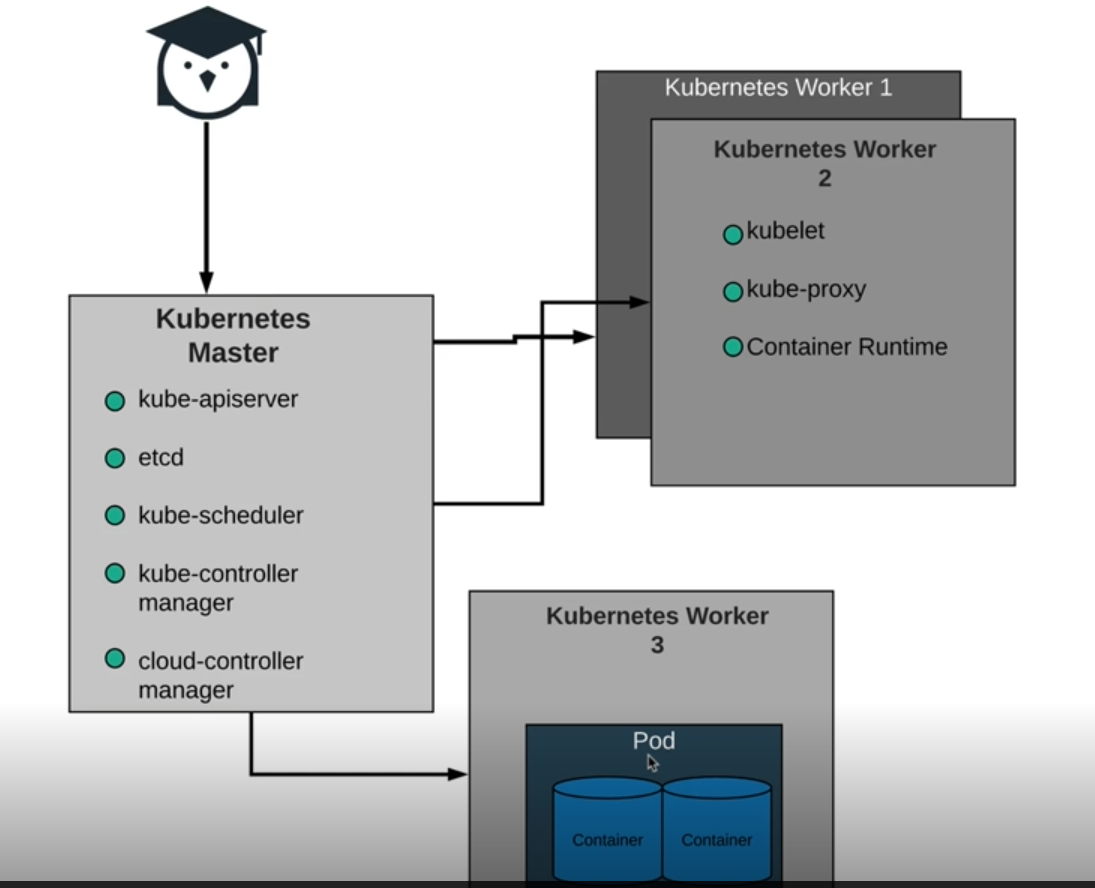
Container orchestration.

Others:

* Docker swarm
* Marathon (based on Apache Mesos)
* Amazon ECS
* Azure Container Service
* HashiCorp Nomad

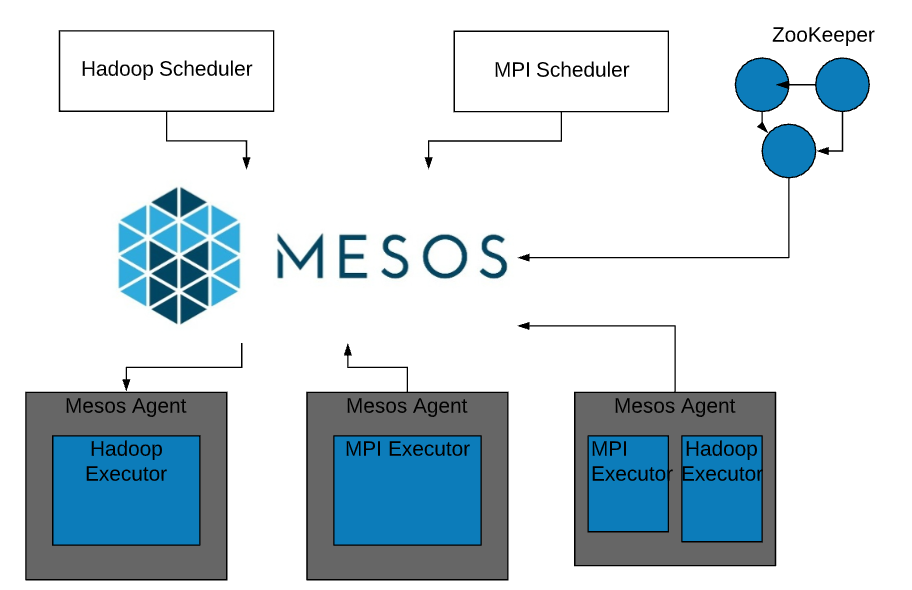
Container orchestration automates the deployment, management, scaling, and networking of containers.

Docker swarm vs Kubernetes: technically you could do the job with both of them, but one of them will be a better fit.



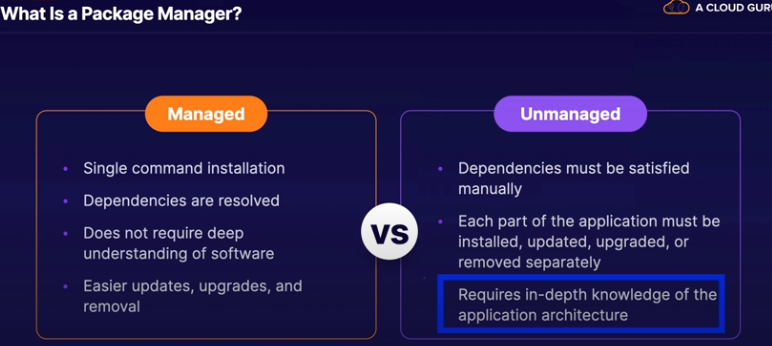
1. Mesos

Az on operating system for your datacenter. Elasticsearch, Hadoop, Kafka

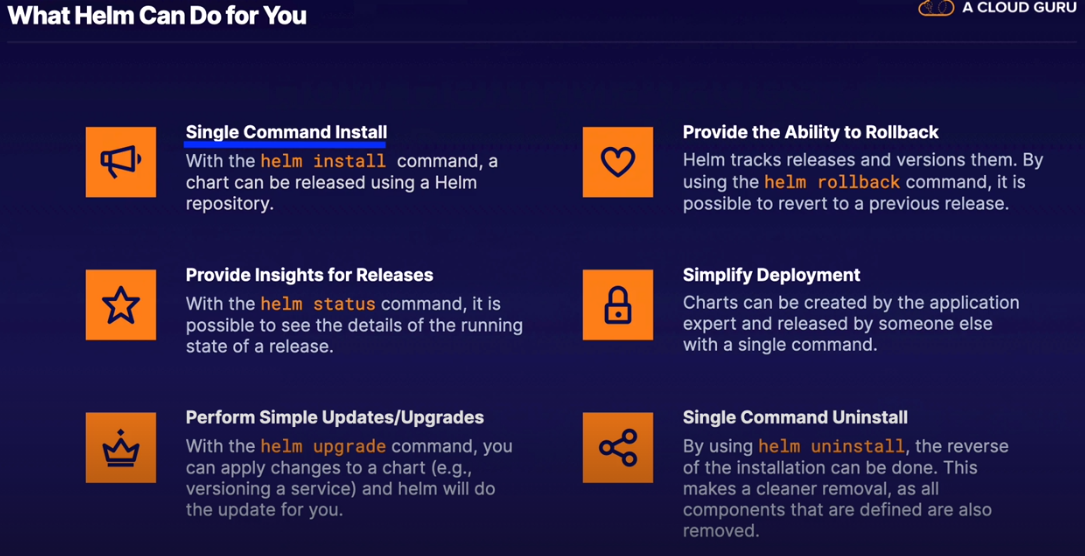


1. Helm

Helm is a package manager for Kubernetes







1. TODO

Helm ?