**Content**

[1. Introduction 2](#_Toc48470801)

[1. Virtualization vs Containerization 7](#_Toc48470802)

[2. Dockerfile 8](#_Toc48470803)

[1. Creating a Docker Image 9](#_Toc48470804)

[3. Docker commands 11](#_Toc48470805)

[4. Docker compose – communication between the containers. 13](#_Toc48470806)

[1. docker-compose.yml 14](#_Toc48470807)

[2. docker compose commands 15](#_Toc48470808)

[5. Deployment of docker application 16](#_Toc48470809)

[1. Docker volumes 17](#_Toc48470810)

[6. Using Docker behind the proxy 18](#_Toc48470811)

[7. Docker on AWS 19](#_Toc48470812)

[1. ECS 19](#_Toc48470813)

[7.1.1. ECS – Task definition 19](#_Toc48470814)

[7.1.2. ECS – Service definition 20](#_Toc48470815)

[2. Elastic Beanstalk 20](#_Toc48470816)

[7.2.1. Dockerrun.aws.json 21](#_Toc48470817)

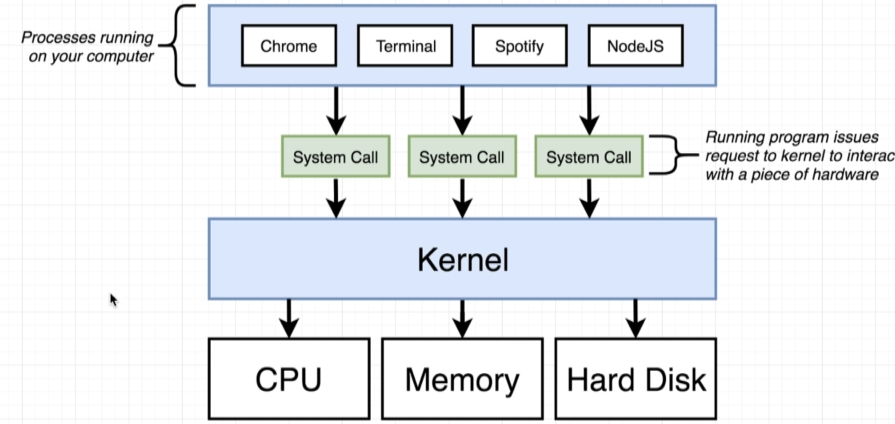
1. Introduction

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.

**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.



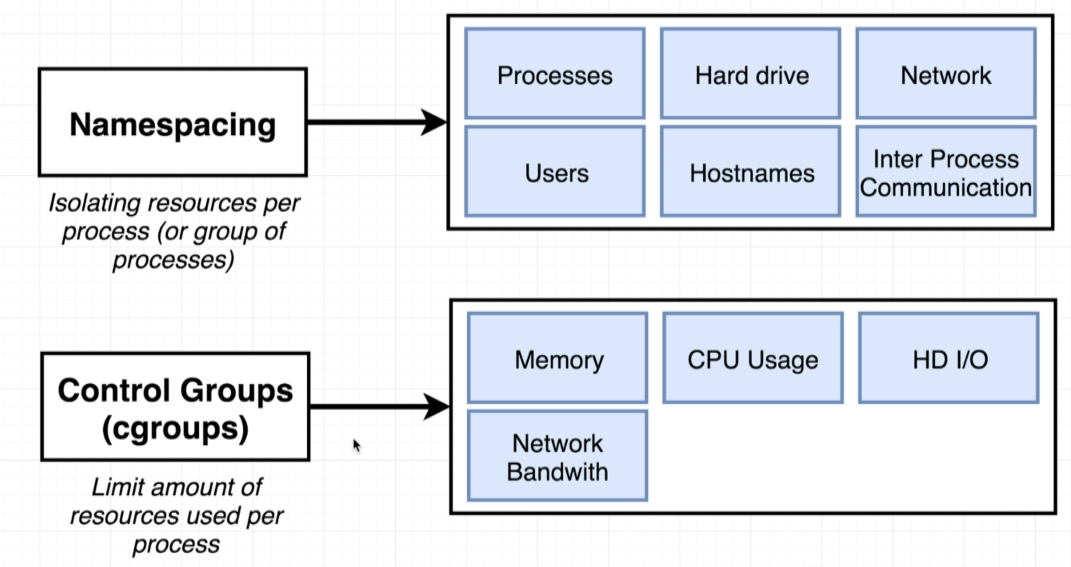
**CentOS** (Community Enterprise Operating System) is a Linux distribution that provides a free, enterprise-class, community-supported computing platform functionally compatible with its upstream source, Red Hat Enterprise Linux (RHEL).[5][6] In January 2014, CentOS announced the official joining with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

**Docker Hub** is a registry service on the cloud that allows you to download Docker images that are built by other communities. You can also upload your own Docker built images to Docker hub. In this chapter, we will see how to download and the use the Jenkins Docker image from Docker hub.

I**solate processes:**

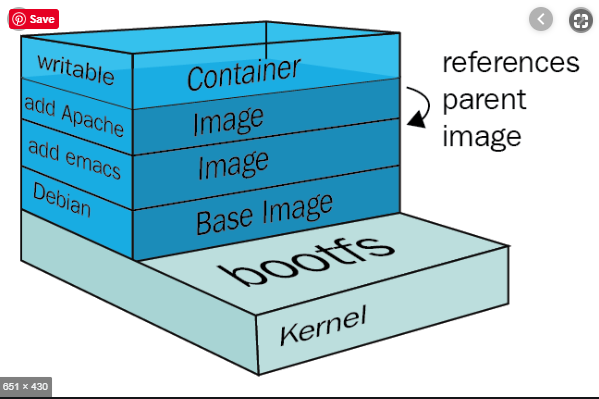
**Namespaces** are named program regions used to limit the scope of variables inside the program. They are used in many programming languages to create a separate region for a group of variables, functions, classes, etc. With namespacing we are allowed to allocate resources as per a process or a group of processes and we essentially saying that anytime a particular process ask for a resource, we’re going to direct it to this one little specific area of the given piece of the hardware. But namespacing can be used even for software elements as well. We can namespace a process to restrict the area of a hard drive that is available for, or the network devices that are available or the ability to talk to other process. “redirect request for resource”

**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.

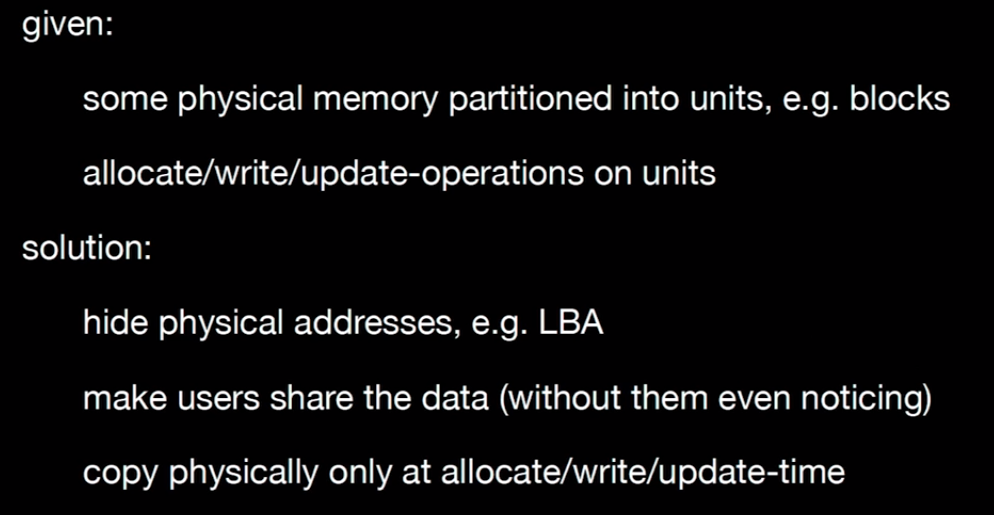


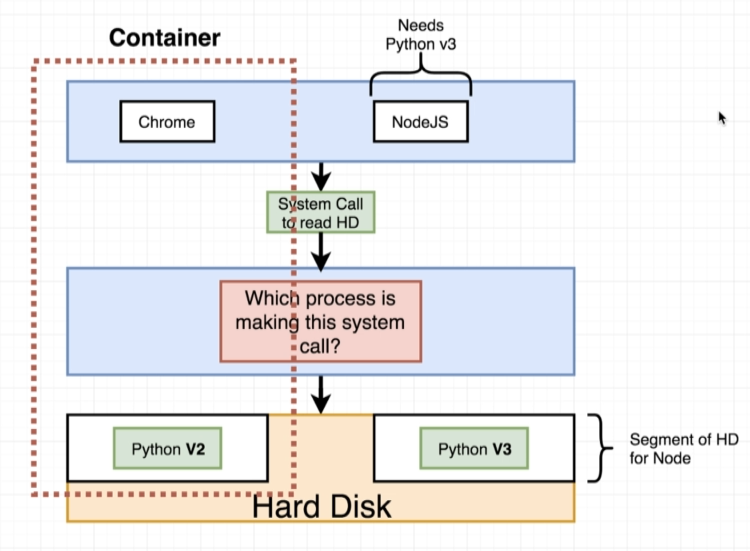
Namespaces limit what you can see, CGroups limit what you can use.

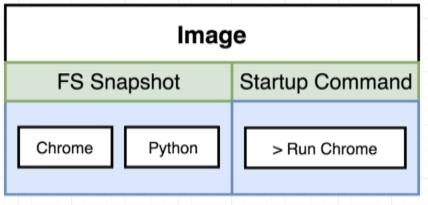
Union Capable File System – Union Mounting – a way of combining multiple directories into one that appears to contain their combined contents.



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.

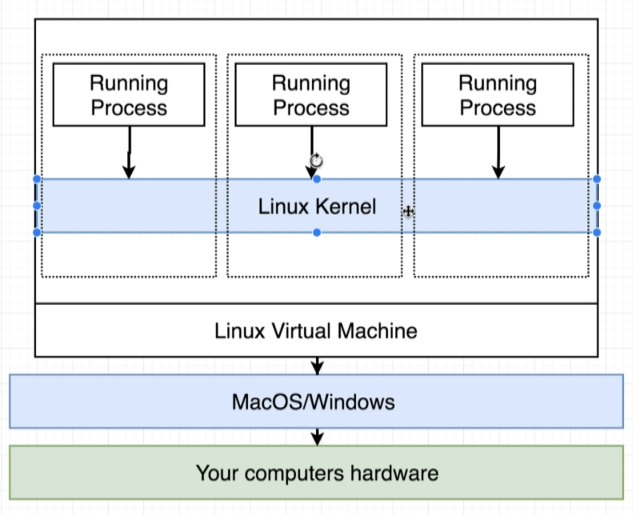






Container is a running process along with a subset of physical resources on your there are allocated to that process specifically.

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.

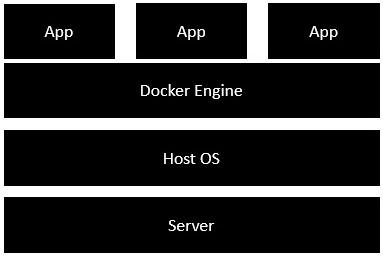
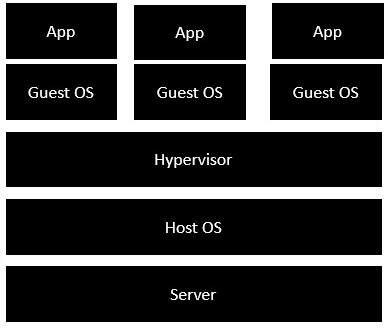


**Alpine**

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. 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
4. ENV
5. ADD
6. COPY

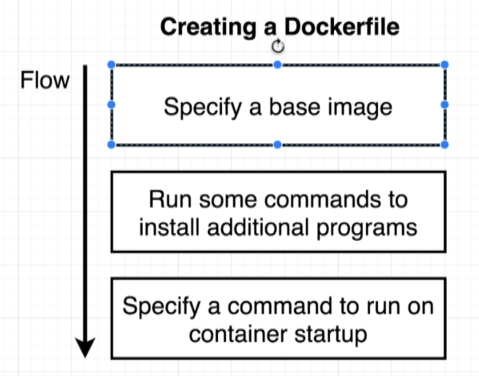
COPY ./ ./ ------------ COPY <src> <dest>

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

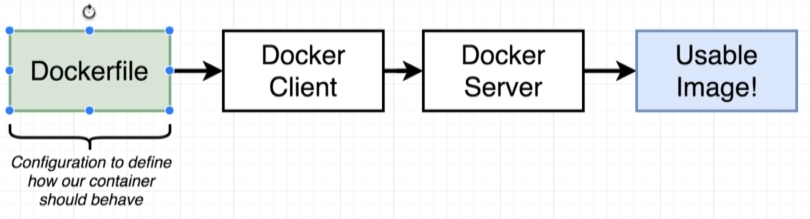


**Minimizing Cache Busting and Rebuilds**



e.g. now if you change the index.js the npm install does not need to rerun. Cache works until the first change.

* 1. Creating a Docker Image

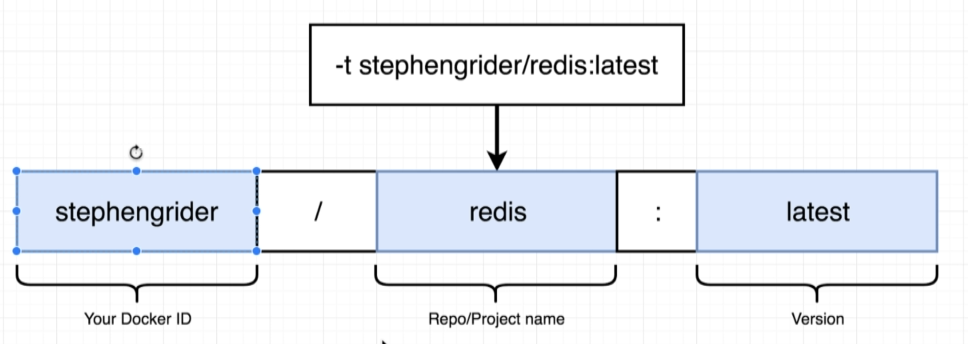


* Docker build .

(. – 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.

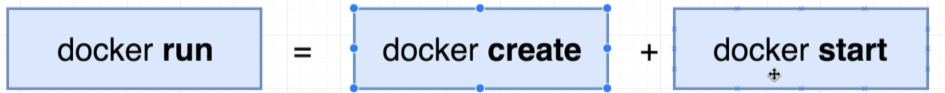
1. Docker commands

Bonus:

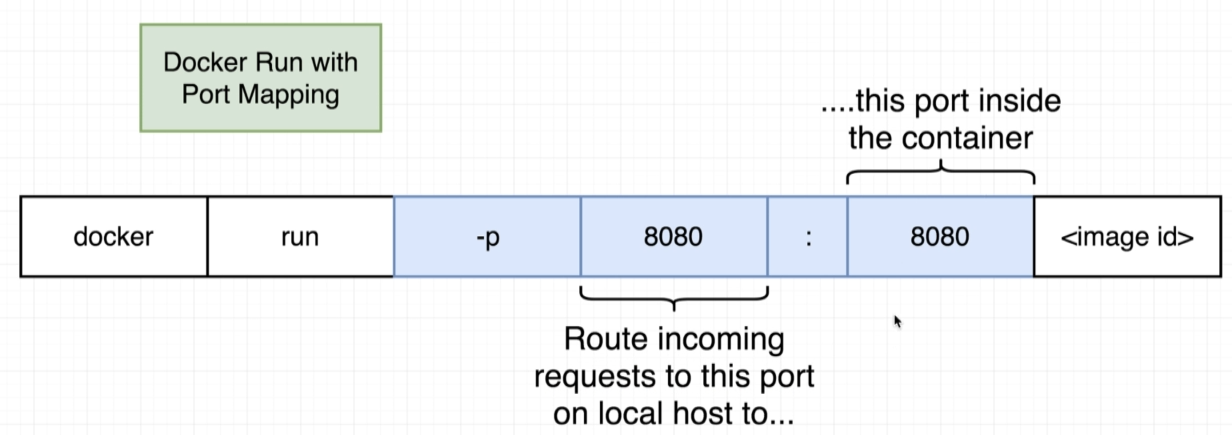
cat /etc/\*-release – get your linux distribution

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)

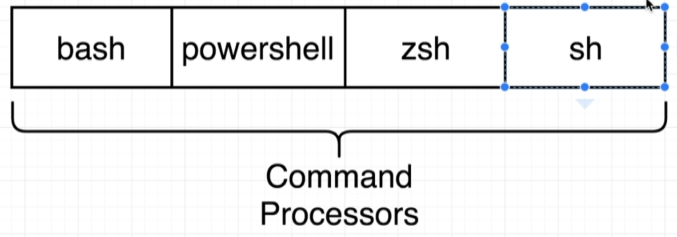
* -i standard in
* -t text formatting?

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 compose – communication between the containers.

FROM node:alpine

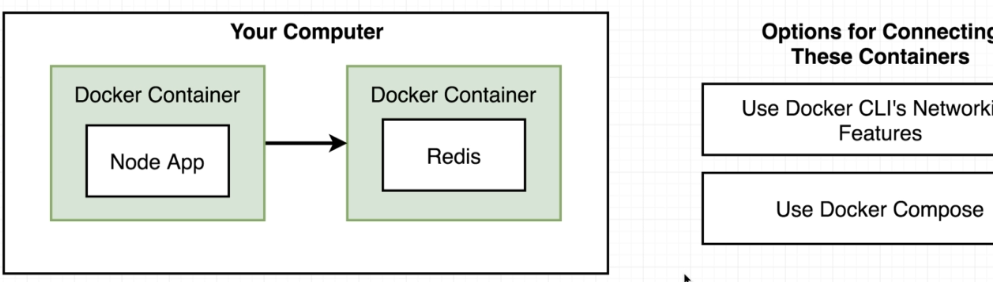
WORKDIR ‘/app’

COPY package.json .

RUN npm install

COPY . .

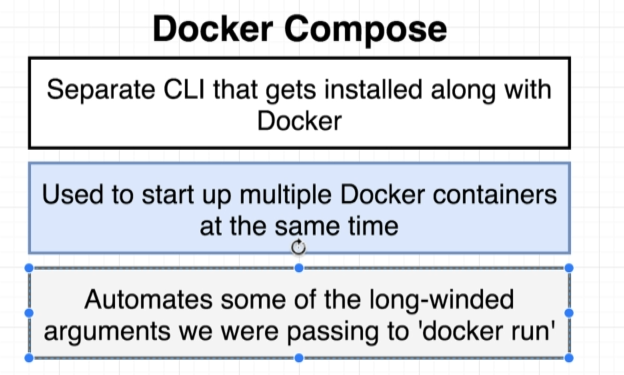
CMD [“npm”, “start”]



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.

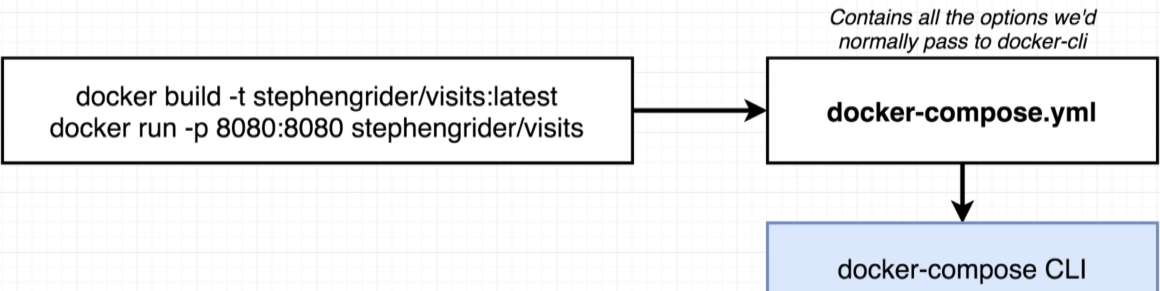
**Docker Swarm:** When you are trying to manage containers across multiple physical or virtual machines.

**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.



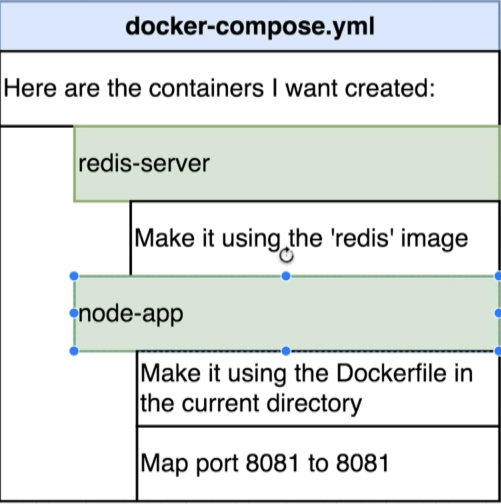
**Docker Networks**: rtfm.

* 1. docker-compose.yml

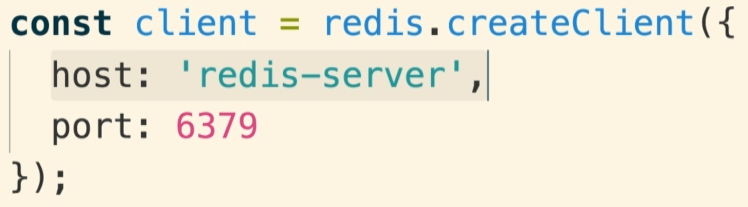


To make use of docker compose we’re going to use the same commands – docker build, docker run – but we will encode them into a very special file: **docker-compose.yml**. (w special syntax)

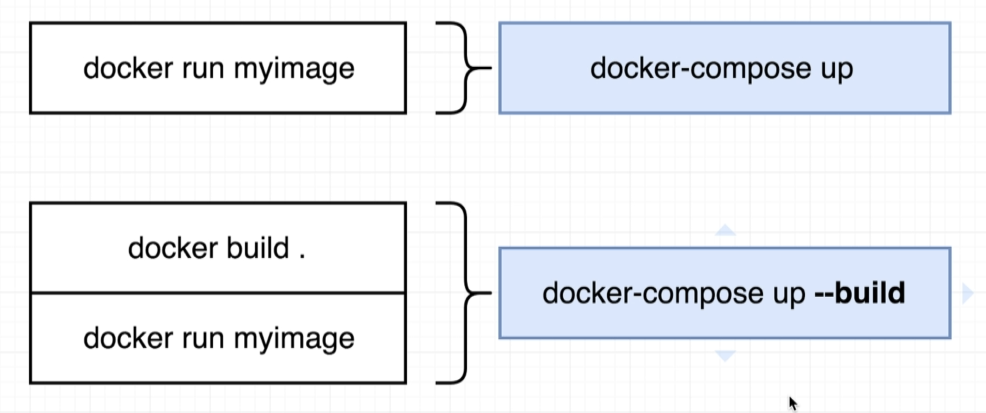
\*Map: map the port of the image to the local machine



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



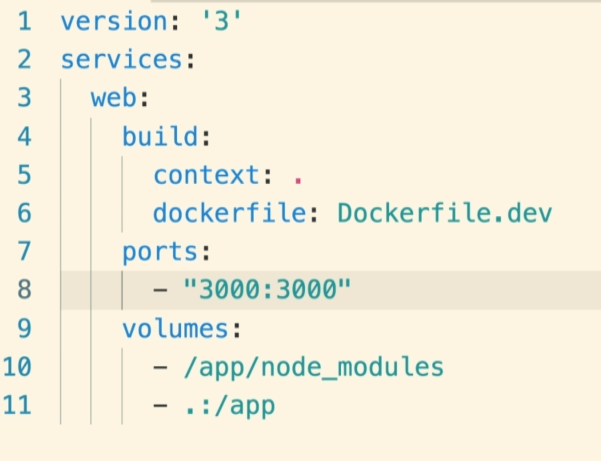
* 1. docker compose commands



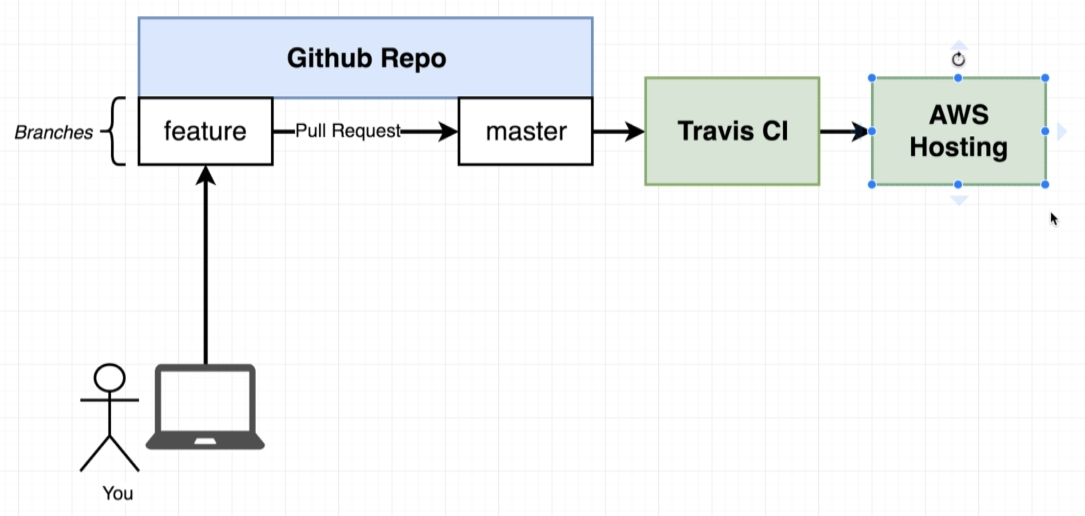
Remember: one of the main purpose of docker compose is to make docker run easier.

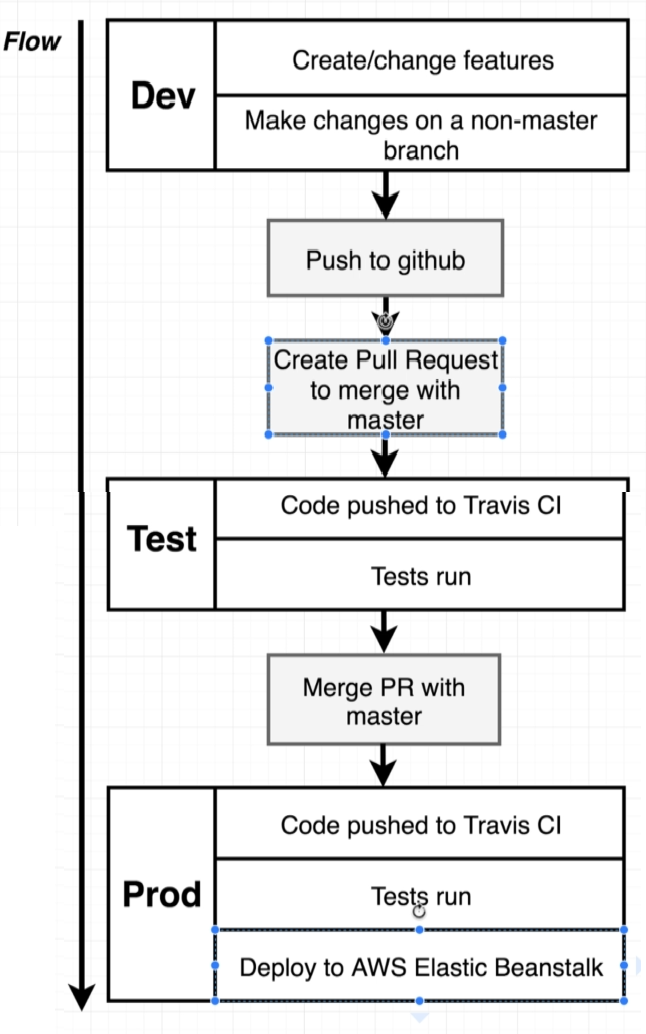
1. Docker-compose down

Next: Container Maintenance with Compose mp4



1. Deployment of docker application





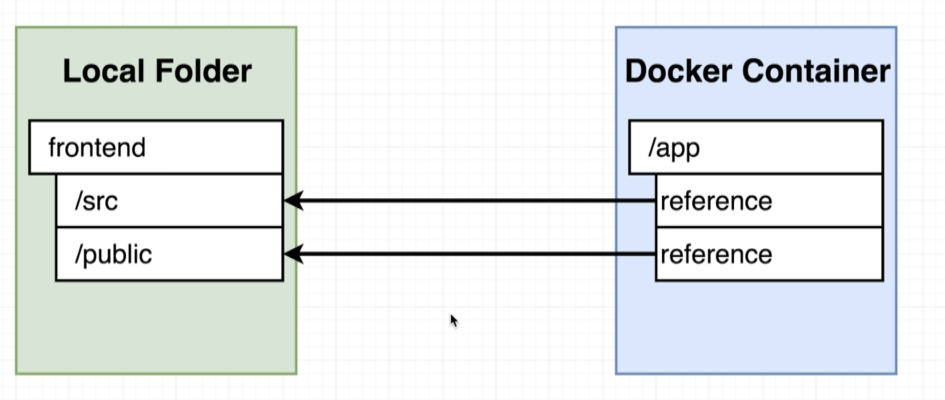
**Dockerfile.dev –** anytime we want to run docker build with custom dockerfile name:

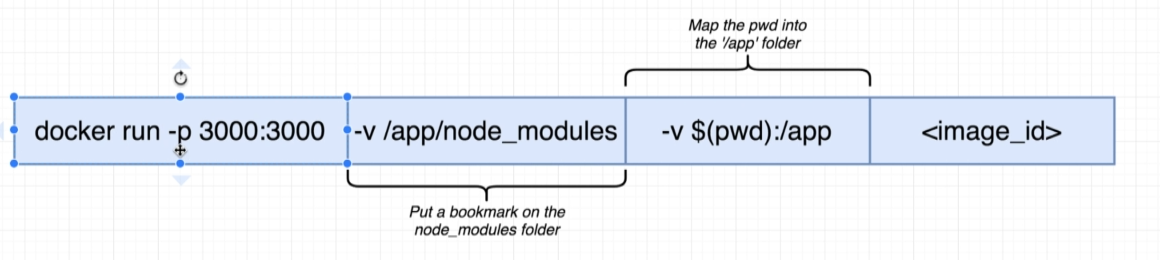
Docker build –f Dockerfile.dev

* 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. Docker on AWS

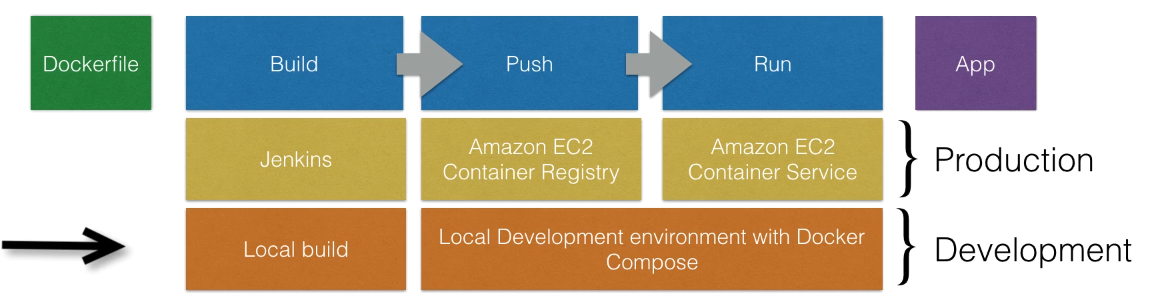
To manage containers we need a container management platform:

* ECS – Amazon’s own platform
* Fargate: Amazon’s own serverless platform
* EKS – Amazons’ managed Kuernetes (open source)

Just like **packer builds AMIs,** you can use docker to build docker images.

Those images can then be run on any Linux host with Docker Engine.

**Docker Engine installed in the Vagrant DevOps box?**



Docker build ca be executed manually or by Jenkins.

You can run the docker app by executing “docker run” locally. Instead we can push it to Amazon and run this app on AWS.

* Push this locally build image to Amazon ECR – where docker images can be stored in.
* Set up a docker cluster (ECS) to run our Docker applications.
* [Optional] the creation of the registry can be done using terraform.

(terraform to create aws resource, build, login to the ecr, push using the url , so easy )

* 1. ECS

*The cluster is just a group of EC2 instances with this agent installed on.*

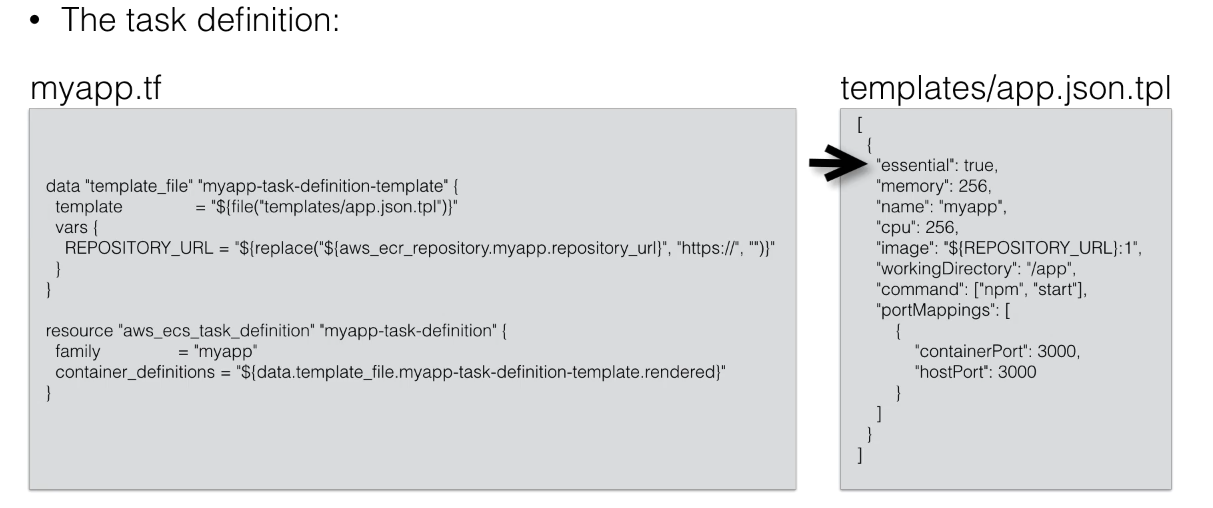
You need to start an autoscaling group with a custom AMI. The custom AMI contains the ECS agent. Once the ECS cluster is online, tasks and services can be started on the cluster.

* + 1. ECS – Task definition

Before docker app can be launched, a task definition needs to be provided. The task definition describes what docker container to be run on the cluster. JSON form, to tell EC2 how to run the container (it does not runs it itself).

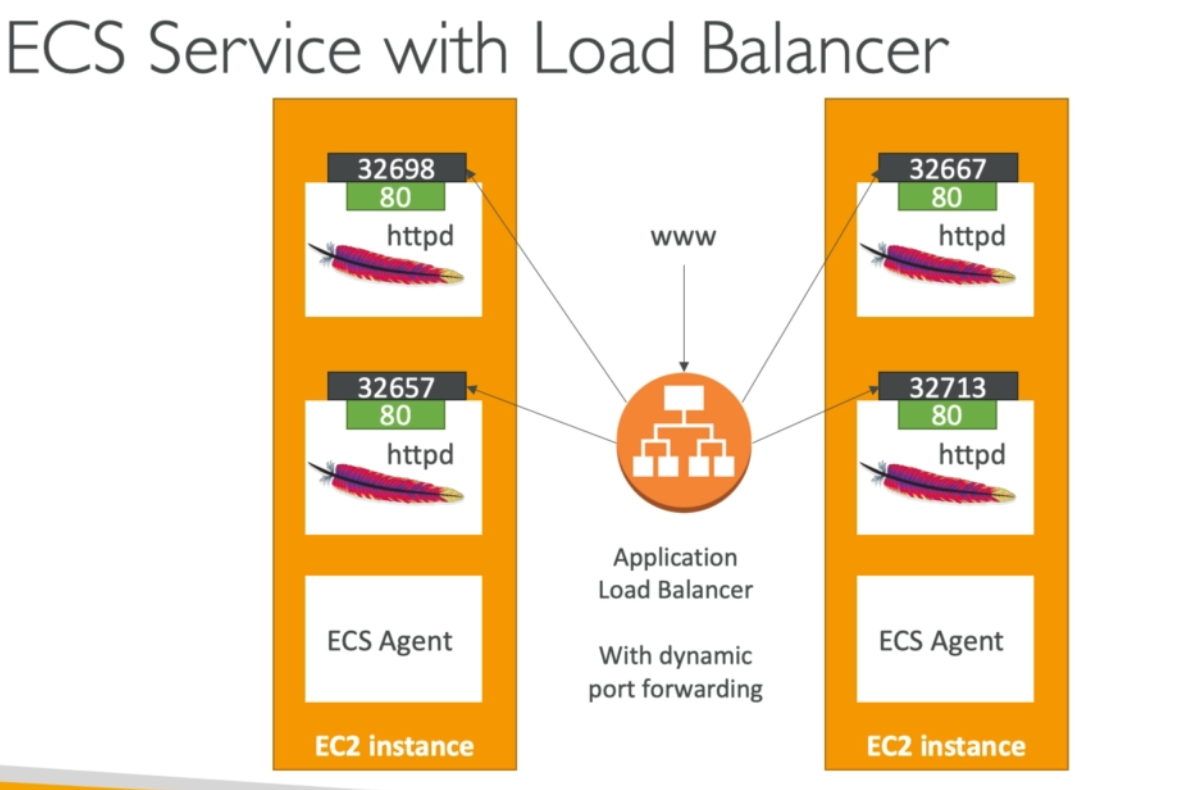
* Specifies Docker image (the docker image in ECR)
* Max CPU usage, max memory usage
* Wether containers should be linked (e.g. link app container w DB container)
* Env vars. (credentials)
* Port binding
* Networking information
* Any other container specific info

The task definition needs an IAM role. So if it cannot do something first thing is to check the permissions.

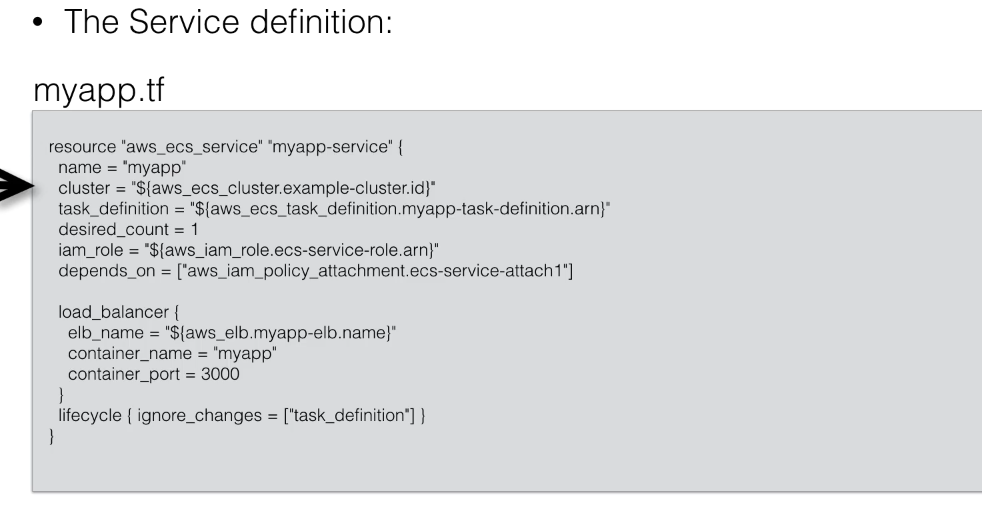


* + 1. ECS – Service definition

It is going to run a specific amount of containers based on the task definition. You can scale. A service is always running, if the container stops it will be restarted, can be scaled, you can run 1 instance of a container or multiple. You can put an ELB in front of a service. Typically run multiple instances of a container, spread over AZs. If one container fails, your LBs stops sending traffic to it. Running multiple instances w an ELB / ALB allows you to have HA.



If we do not set static mapping, aws will generate random port to map the task. Load Balancer is able to figure out these random ports and distribute traffic using dynamic port forwarding.



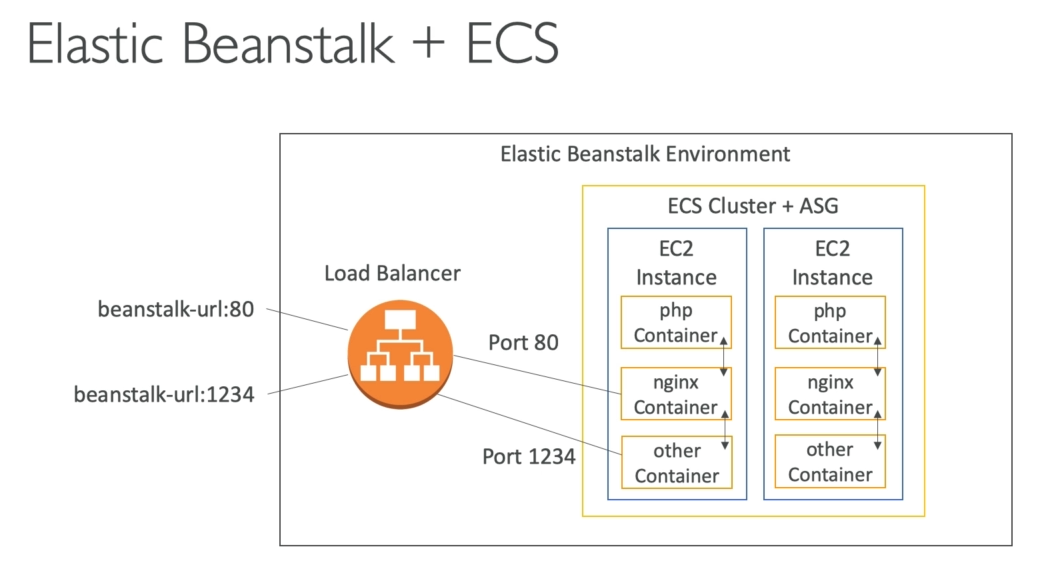
* 1. Fargate
  2. Elastic Beanstalk

Difference between single container deployment and multi-container. If there are e.g. 3 packages and all of them has its own dockerfile then EB will need a little bit of help.

The multi container mode will create for you the:

* ECS Cluster
* EC2 instances, configured to use the ECS Cluster
* Load Balancers (in high availability mode)
* Task definitions and executions

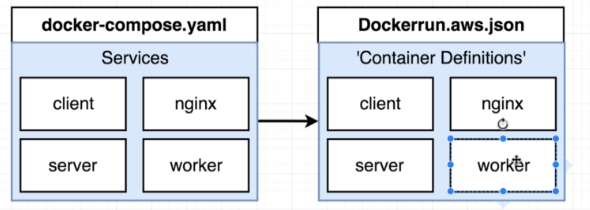
Docker images must be pre-built (stored in ECR for example) and Dockerrun.aws.json must be provided at the root of the source code.



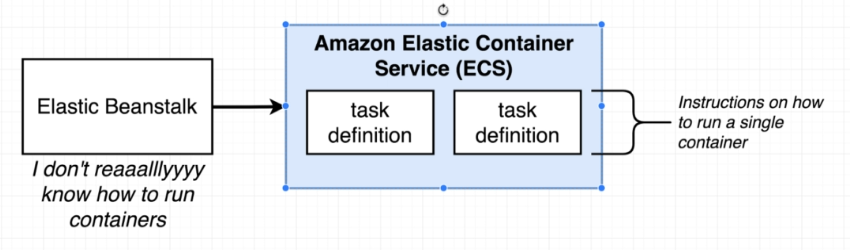
* + 1. Dockerrun.aws.json

That file is going to tell EB exactly where to pull all of our images from, what resources to allocate each one, how to setup some port mappings and some associated information. It will remind you how docker-compose.yml is setup.

Docker-compose.yml is primarly meant to use in development, environments, and you can kind of think of it as a single file that encodes a lot of directions that would normally be passed to docker run.



The biggest difference that in docker-compose.yml we define how to build the image but in Dockerrun.aws.json we already have the image, just need to pull it from DockerHub using an ID.







Tip: use json validator (jsonlint.com? )s