25/7/2017

Docker hub is a docker registry which is user to keep track/store docker images posted on cloud.

Registry:

Can configure security exceptions

Hub:

Location setup in cloud used to handle docker images.

Docker search – search an image in dicker hub

Nomenclature for pushing image

Username,org name/repository:tag

Resource limitation:-

Docker run -it –name cont-name –memory 128m image

Goto sys/fs/cgroup/memory/docker/cont-name/ - cat memory.limit\_in\_bytes

Dockerd – to talk to docker daemon

First service shld be stopped for that

Service docker stop

Docker run –name cont-name -p 1000:80 image

Docker run –name cont-name -P

Flag small p is used to specify explicitly against which port it has to be run.

P -random port

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*888

Docker networking:

Ifconfig is run on host machine:

Docker 0 appears – it acts as a bridgeto provide ip addresses to containers

3 types based on n/w driver:

1.bridge[default]

2.host-container behaves as if it is a vm[only one container can behave as host,suitable for single-vm arch]

3.none[no n/w required when no data containers are shared]

--net is used to define type

Intra -host comm is facilitated using overlay.

n/w creation:

docker network create –driver bridge –subnet 10.0.0.1/25 first

**Docker file:**

**Docker build -t dockerfile/1 .**

**ADD - COPIES THE URL ALSO**

**COPY – CAN COPY ONLY THE FILES**

**All the commands in docker file shld be in non interactive mode.**

BEST PRACTICES:

Try to minimize the layers

CMD – used to pass a command during runtime

ENTRYPOINT: message from entrypoint can never be overridden[highest priority]

WORKDIR : commands after this are exected on the path specified.

ONBUILD : do the operation while the second buid happens

26/7/2017 – Wednesday

Clustering- Docker machine

Way of running containers into individual machines[more like type-2 hypervisor]

Adv:

Seamless interact with any cloud providers

Docker for windows:

Initializes VE which installs linux kernel

2 ways:

Docker toolbox for windows[type 2 hypervisor] like oracle virtualbox/vmware

Docker windows[hyper v]

DTW- to manage vms ,we use docker machine

In order to establish comm b/w contains created using docker-machine,we moved to docker-swarm

Swarm itself is a container[Any machine connecting to sworm shld have a specific token]

DOCKER SWARM:

SWARM1: CONTROLLED BY DOCKER CLIENT RUNNING OUTSIDE

SWARM 2:CONTOLLED BY THE MANAGER ITSELF

Docker pull swarm

Docker run swarm

$sid = $(docker run swarm create)

Echo $sid

Docker ps

Docker-machine create –driver virtualbox –swarm –swarm-master –swarm-discovery token://$sid master

Docker-machine create –driver virtualbox –swarm –swarm –swarm-discovery token://$sid node1

Every docker compose is linked with a project

Docker-compose config -to check if the yaml is in correct format

Docker-compose up -d

Docker-compose scale cont-name=no.of containers

27/7/2017 – Thursday

COW[COPY ON WRITE]

Starts processes by making a copy of them

They make sure the underlying containers share the same data layers

Data layers are not controlled by the storage driver[but by host file system]

Supported file systems:aufs,btrfs,overlay

In aufs, each binary is treated as a file, even if a small change is made, the entire file is copied.

Service docker stop

28/7/2017

DOCKER UCP[UNIVERSAL CONTROL PLANE]

Nodes,volumes and networks can be managed from a single place

DOCKRE TRUSTED REGISTRY

When ucp is deployed,it deploys a service called ucp-agent. It is used to manage ucp services according to whether a node is manager/worker.

Hostname ucp.local

Echo ucp/local>/etc/hostname

Exec bash

Do the same for dtr.local

ucp:

Nano etc/hosts/

Add ip address to host

Go to /etc/network

Nano interfaces

Iface eth1 inet static

Address 192.168.99.100

Netmask 255.255.255.0

Gateway 192.168.99.1

Do the same for dtr[docker trusted registry]

Ucp:

Docker pull docker/ucp:2.1.5

docker run --rm -it \

-v /var/run/docker.sock:/var/run/docker.sock \

--name ucp docker/ucp install -i \

--swarm-port 3376 --host-address $(docker-machine ip node1)

Docker pull docker/dtr:2.2.7

DOCKER CONTENT TRUST

USED TO VERIFY THE PUBLISHER OF DOCKER IMAGES

2 TAGS:

OFFLINE KEY:ROOT OF TRUST.DIFF REPOSITORIES CAN USE THE SAME OFFLINE KEY

TAGGING KEY: TAGGING KEY IS GENERATED EACH TIME THE USER PUSHES REPOSITORY.[repo specific]

Set env variable to download only signed trusted images.

EXPORT DOCKER\_CONTENT\_TRUST=1

/docker/trust/private

Damages can be done by:

Processes

Root

Docker daemon

Cgroups

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Apparmour contains predefined style for defining profiles

AppArmor (Application Armor) is a Linux security module that protects an operating system and its applications from security threats

2 modes in which profiles are run:

Enforced – whatever policies defined will be enforced in the container.

Complain – monitored and logged

Can specify allow/deny access - apparmor

https://docs.docker.com/engine/security/apparmor

sclinux and sccom

himashu3894@gmail.com