

LXC / contained

image not found

Description

A LXC container using nested virtualization responsible for running the majority of my services that run as docker containers.

Configuration

Resources

Hostname	CPU	Memory
contained	6 vCPU	24GB

Storage

Mount Point	Source	Mount Path	Size	Options
rootfs	local-zfs:subvol-100-disk-0	/	8GB	noatime
mp0	/storage/zpool10/downloads	/storage/downloads	-	noatime;nodev;noexec;nosuid
mp1	/storage/zpool10/downloads/incomplete	/storage/downloads/incomplete	-	noatime;nodev;noexec;nosuid
mp2	/storage/zpool10/media	/storage/media	-	noatime;nodev;noexec;nosuid
mp3	/storage/zpool10/services	/storage/services	-	
mp4	vpool-zfs:subvol-100-disk-1	/var/lib/docker	384GB	noatime

Networking

Interfaces

ID	Type	Name	Link	IPv4 Address	IPv6 Address	Description
net0	bridge	eth0	vmbr3	10.0.8.2/21	DHCPv6	DMZ
net1	bridge	eth2	vmbr4	-	-	WARP

Docker Networks

A brief overview of how I have my networking setup for Docker.

blackbox_containers

Type	Gateway	IP/Subnet	IP Range
bridge	-	-	-

Traefik binds to the host ports on [LXC / Contained](#) for HTTP(S) traffic that has been forwarded from [firewall](#) and proxies it to the appropriate container using this bridge network.

- Containers that are part of this network can directly access other containers in this network using their hostnames and/or container names.
- Using hostnames to network containers provides an IP agnostic way to communicate while reducing overhead of SSL.
- Containers in this network are not publically accessible, access is controlled with Traefik acting as a gatekeeper.

****NOTE**** All publically accessible containers should be part of the `blackbox_containers` network.

Creation Command

```
docker network create --driver bridge blackbox_containers
```

a_warp

Type	Gateway	IP/Subnet	IP Range
macvlan	10.0.9.1	10.0.9.2/24	10.0.9.128/25

All containers which need anonymity should be connected to this network so their traffic is automatically routed through a VPN. It is prefixed with `a_` because networks are added to containers alphabetically and this must be added first to be assigned as the default gateway.

****NOTE**** All containers that want to mask the location of their traffic should be part of the `a_warp` network.

Creation Command

```
docker network create --driver macvlan --subnet 10.0.9.2/24 --gateway 10.0.9.1 --ip-range 10.0.9.128/25 --opt parent=eth2 a_warp
```

Installed Software

- [Docker](#)
- [Netdata](#)

Revision #25

Created 29 December 2019 23:15:48 by Dustin Sweigart

Updated 12 April 2021 17:04:09 by dustin@swigg.net