r/selfhosted • 1 yr. ago
sofakng

Best practice for accessing lots of Docker containers? (re: macvlan vs reverse proxy)

Docker Management

What is the best practice (or what is everybody using) for accessing many different containers on their network?

I've been using Docker with macvlan and assigning each container a dedicated ip address on my network. Each container is then accessible from my other computers using their ip address and I also configure each container's web interface to use port 80.

However, I've been asking on the LinuxServer Discord and they recommend using SWAG or another reverse proxy. They didn't say it's a bad idea to use macvlan but it sounds like treating containers as VMs (like I'm doing?) isn't recommended.

What is everybody doing to access their containers?

clintkev251 • 1y ago
Top 1% Commenter

Reverse proxy absolutely. Assigning IPs to every single container will just get really messy and you also loose out on all the advantages of routing everything through a proxy (SSL, SSO, etc.)

1 Reply ...

4 more replies

[deleted] • 1y ago • Edited 1y ago

> I've been using Docker with macvlan and assigning each container a dedicated ip address on my network. Each container is then accessible from my other computers using their ip address and I also configure each container's web interface to use port 80.

That is so much extra work, why do any of this? Youre making things so much harder on yourself without any real gain.

You do not need a IP in your network for every single container. Do not treat containers as VMs, they are not.

Switch to using a reverse proxy with DNS names, can be something like a local Pihole.

Then you can turn your nightmare of IPs into basic domains for each service, like `portainer.example.home` or `portainer.home`.

If you also want to use valid (trusted) SSL certs, you can do that too with most reverse proxies, but the domains you use must be valid public ones (doesnt mean you need to open any ports tho). So `portainer.example.home` wouldnt work, but `portainer.example.duckdns.org` would work.

Tons of threads here exist about this already, simply search.

15 Reply ...

sofakng OP • 1y ago

Thanks! Do you recommend subdomains or paths? (ie. sabnzbd.home.mydomain.com or proxy.home.mydomain.com/sabnzbd)

Also, what reverse proxy do you recommend?

1 Reply ...

14 more replies

sk1nT7 • 1y ago

Top 1% Commenter

Furthermore, you likely expose many network services that must not be exposed such as database ports etc.

The recommended way would be to use Docker bridge networks (a unique one per container stack) and then joining a reverse proxy to the networks. The reverse proxy will expose TCP/80 and TCP/443 and proxy to your docker containers. You won't even map any container ports to your docker host server anymore. Only 80 and 443 of the reverse proxy. Everything else happens within Docker networks.

So the reverse proxy can directly talk to your other container services as they both remain in the same docker bridge networks. Docker also handles name resolution, so you can just tell the reverse proxy to proxy to 'nginx', which may be the name of your nginx container. No need to define internal Docker IPs or remember those.

If you have a valid domain name, you can even opt for obtaining valid SSL certificates for all your services. Even when you do not plan to expose anything, you can use dns challenge and obtain valid lets encrypt certificates. Then just use subdomain names for your services like plesk.example.com, cloud.example.com, which all point to the IP address of your reverse proxy (in this case the IP address of your server). May use an internal DNS server to resolve your domain properly (split brain dns).

4 Reply ...

sofakng OP • 1y ago

> The recommended way would be to use Docker bridge networks (a unique one per container stack)

Are you saying to have separate networks for each container or having all containers share a bridge network and then having the reverse proxy on two networks (macvlan [?] and the bridge network).

If you are saying to use a different bridge network for every container, isn't that a bit overkill and would also prevent containers from communicating with each other? (sonarr to sabnzbd, etc)

1 Reply ...

14 more replies

1 more reply

container from each other, but I don't see that paying off. With a reverse proxy you can still give them different names, all you need to worry about is they don't have a conflicting port on the same host. The proxy configuration is easy to maintain and can be trivially reloaded anytime with zero downtime to the underlying services.

The only drawback I can thing off is your proxy needs to have access to all your containers, so generally they will all share the same network, not a biggie at all to me.

2 Reply ···

PaulEngineer-89 • 1y ago

One advantage of Macvlans is with Tailscale. With Tailscale you get to choose only the host name. Your domain name is always host.net name.ts.net or else use /application or very limited ports. So with a Macvlan you can assign each container a separate name. With Cloudflare or without tunnels then reverse proxy makes more sense.

2 Reply ···

joecool42069 • 1y ago

imho, most people using macvlans are trying to treat containers like VMs. macvlans, again imho.. should rarely, if ever be used, and only for very specific reason.

1 Reply ···

ithilelda • 1y ago

you are using macvlans wrong... it is intended for special cases where you absolutely need the container to appear physically connected to your nic, like they need to monitor traffic or such. IT IS not designed to be anything more secure than the default bridge driver...

what exactly is your concern of security? are you trying to isolate each container so that they can't communicate with each other? then just put each container in its own bridge network. are you trying to hide insecure endpoints from the public, so that it is only accessible through secure connections like tls? then use a reverse proxy. in any of those cases, macvlan does not play a role.

1 Reply ···

r/selfhosted • 10 mo. ago

What are some lesser known docker containers you use?

397 upvotes · 288 comments

r/selfhosted • 2 mo. ago

Using Traefik reverse proxy with Docker - guide

51 upvotes · 13 comments

r/selfhosted • 4 mo. ago

So whats the best way to run a reverse proxy?

62 upvotes · 60 comments

r/selfhosted • 6 mo. ago

Do you run your reverse proxy in Docker or directly on the host?

32 upvotes · 76 comments

r/selfhosted • 1 mo. ago

Best way to backup docker containers?

18 upvotes · 34 comments

r/unRAID • 1 mo. ago

Better Docker container management options?

33 upvotes · 38 comments

r/selfhosted • 7 mo. ago

How do most people configure a reverse proxy?

92 upvotes · 117 comments

r/selfhosted • 2 mo. ago

Is there a way to backup and restore Docker Containers and Volumes?

14 upvotes · 16 comments

163 upvotes · 101 comments

r/selfhosted • 1 mo. ago

Looking for an overview of Docker containers with newer tags available 👀

8 upvotes · 10 comments

r/selfhosted • 23 days ago

Anyone else psychotically keep ALL docker containers on one LXC?

278 upvotes · 145 comments

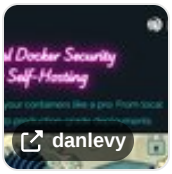
r/selfhosted • 10 mo. ago

Best Practices for Docker Networking with VLANs and Firewall Rules?

3 upvotes · 2 comments

r/selfhosted • 2 mo. ago

Essential Docker Security Tips for Self-Hosting



321 upvotes · 76 comments

r/selfhosted • 5 mo. ago

PSA: A reverse proxy does not automatically increase your security

191 upvotes · 85 comments

r/selfhosted • 10 mo. ago

How do you guys backup your servers especially with docker?

61 upvotes · 79 comments

r/selfhosted • 2 mo. ago

Migrating away from Docker Swarm

6 upvotes · 28 comments

r/selfhosted • 2 mo. ago

How do you back up your Docker Compose / container setup

136 upvotes · 189 comments

217 upvotes · 43 comments

r/selfhosted • 2 mo. ago

Rsync over other backup solutions

21 upvotes · 52 comments

r/selfhosted • 1 mo. ago

Docker Security - How much should I question the software I get from places like LinuxserverIO?

88 upvotes · 61 comments

r/selfhosted • 4 mo. ago

Migrating to rootless docker

87 upvotes · 36 comments

r/selfhosted • 5 mo. ago

A reminder to prune your docker images every so often :)

975 upvotes · 101 comments

r/selfhosted • 9 mo. ago

Pros/cons of having a reverse proxy on the same physical server vs separate?

1 upvote · 25 comments

r/selfhosted • 1 mo. ago

What would be the best way to run a small home server that replaces dropbox/google drive?

4 upvotes · 8 comments

r/selfhosted • 2 mo. ago

Do you have a single reverse proxy?

8 upvotes · 64 comments

TOP POSTS

Reddit