
Redpill
Linpro

Redpill Linpro

About me

- Name: Olle Dencker
- Senior Consultant @Goteborg

Redpill Linpro

Improving container security

Running your containers rootless with podman

Redpill Linpro

Why do we like running containers with docker?

It's easy!

- Deployment
- Network
- Volumes
- Server-client architecture with Remote management API

Redpill Linpro

Why Docker just works

- Client <=> Server/service architecture
- The service is running as root
- To start a docker container, users either have to use sudo or they need to be added to the `docker` group.

```
olle@olle-ThinkPad-L480:~$ ps aux | grep dockerd
root      625302  0.0  0.1 1752820 46812 ?       Ssl  mai09   1:28 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
olle      972300  0.0  0.0  20740  2708 pts/2    S+   10:36   0:00 grep --color=auto dockerd
olle@olle-ThinkPad-L480:~$
```

Redpill Linpro

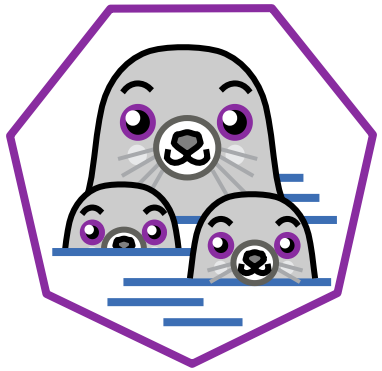
Whats the problem with rootfull containers?

As a regular user I can gain access to protected files.

```
docker run -it --rm \
    -v /etc/passwd:/files_to_edit/passwd \
    -v /etc/shadow:/files_to_edit/shadow \
    -v /etc/group:/files_to_edit/group \
    alpine /bin/ash
```

Redpill Linpro

Podman to the rescue



podman

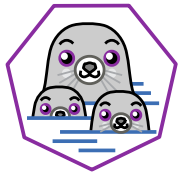
https://podman.io

Redpill Linpro

alias docker=podman

Redpill Linpro

All good things come in threes



podman

buildah

skopeo

Redpill Linpro

What's the catch with rootless containers?

Redpill Linpro

Network limitations

Can only publish ports above 1024 (unprivileged ports)

Redpill Linpro

File access

The container does not have access to "all" files (because your are not running it as root)

Redpill Linpro

Limitation workarounds

Challenge accepted!

Redpill Linpro

Networking

Redpill Linpro

Iptables portforwarding

- "Forward port 80 to localhost:8080"

Redpill Linpro

Run the one container that need access as root

- "its ok to run a container as root, if there is no other alternative."

Redpill Linpro

Reverse proxy/load balancer service

- Install a loadbalancer (haproxy) on server and route traffic to "correct" port.

Redpill Linpro

File/storage/dev access

Make shure the user has access to the file/folder

Redpill Linpro

But what about docker-compose?

`podman-compose` to the rescue!

- "An implementation of Compose Spec with Podman backend."
- Focus on running podman rootless and with no running deamon

```
$ pip3 install podman-compose
$ podman-compose up -d
```

Redpill Linpro

Podman has pods not just containers

Redpill Linpro

Podman kan generate YAML

Redpill Linpro

Alternative ways to start up containers?

What about systemd?

```
$ loginctl enable-linger olle
$ podman run -d --volume /home/olle/nginx/www:/usr/share/nginx/html:ro --name nginx -p 8080:80 nginx:latest
$ podman generate systemd --new --files --name nginx
$ mkdir -p $HOME/.config/systemd/user
$ cp container-nginx.service $HOME/.config/systemd/user/.
$ systemctl --user enable container-nginx.service
$ systemctl --user start container-nginx.service
```

Thank you!

Redpill Linpro

References

- https://podman.io
- https://github.com/containers/podman-compose
- https://developers.redhat.com/blog/2020/09/25/rootless-containers-with-podman-the-basics
- https://docs.docker.com/engine/security/rootless/
- https://github.com/rootless-containers/rootlesskit
- https://www.redhat.com/sysadmin/podman-run-pods-systemd-services
- `man podman-generate-systemd`