

# Portainer Privesc

If you find yourself in a Portainer with a user you can use this guide to privilege escalate.

- Setup a new Volume that maps the root folder ("/") to a bind type volume

portainer.io

Volumes > Add volume

### Create volume

Name: Dio

Driver configuration

Driver: local

Driver options

name	device	value	type
name	device	/	bind
name	type	n.g. /path/on/host	bind
n	n	bind	bind

Use NFS volume: ☐

Use CIFS volume: ☐

Access control

Enable access control: ☒

Private: I want to restrict this resource to be manageable by myself only

Restricted: I want any member of my team (Development) to be able to manage this resource

Actions

Create the volume

- Initiate a new container by re-using an existing image

portainer.io

Containers > Add container

### Create container

Name: Escape

Image configuration

Registry: Docker Hub (anonymous)

Image\*: docker.io/sha256:ca2b0f26964cf2e80ba3e084d5983da629310b87485dc6445f37bb8b9d7459

Advanced mode: ☒

Always pull the image: ☐

Network ports configuration

Publish all exposed network ports to random host ports: ☒

Manual network port publishing: Add a new network port

Access control

Enable access control: ☒

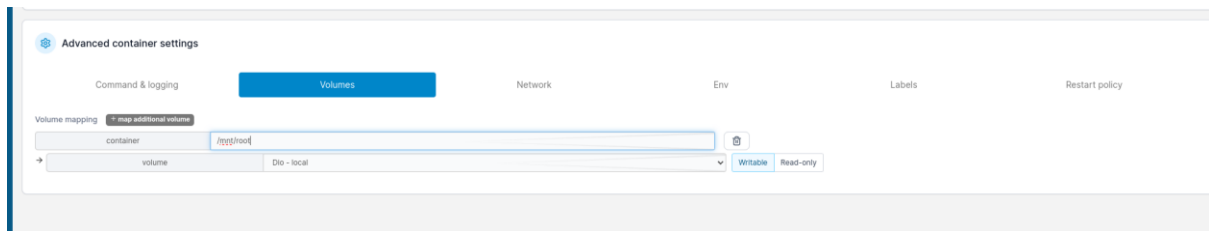
Actions

Auto-remove: ☒

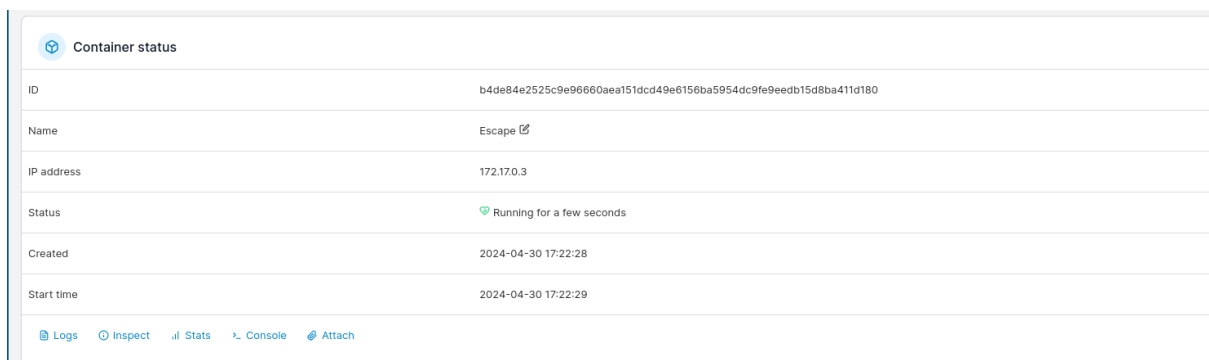
Create the container

- Allow the interactive TTY shell in the options.

- Map the new container to the volume just created before and choose /mnt/root as mounting point (this will be the path on the new container where the root will be mounted)



- Lastly deploy the container.
- Open the console on the container as root



- Now you should be able to map the root from the master machine in the docker container under /mnt/root/root and escape the docker env.

