MozOut

Generated on 15/11/2026 00:39

KNOWLEDGE BASE · PUBLIC DOCUMENT

Running Docker on a VPS safely: the precautions that matter

Docker & Containers

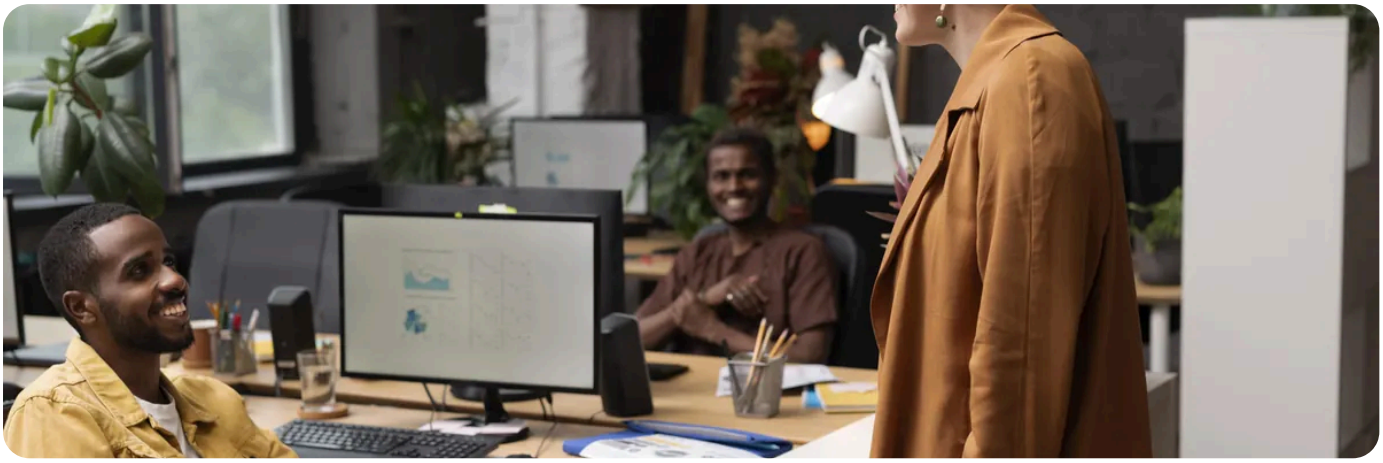
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-3456	v2026.10.10	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/3456

Running Docker on a VPS safely: the precautions that matter

Docker & Containers Created on **October 10, 2026** 3 min read



Docker makes it easy to get an application running, which is why it also makes it easy to get a poorly protected one running. **The short answer:** the security of a server with Docker is decided in six places: who can use `docker`, which ports stay open, which user each container runs as, which images they come from, where the secrets are, and how much each container may use. This article is for an unmanaged VPS, where all of this is yours.

The six precautions

Precaution	What to do	Why
Who uses `docker`	Give `docker` group access only to those who need it.	In practice, whoever has it is root on the server.
Published ports	Publish on `127.0.0.1` (`-p 127.0.0.1:8080:80`) whatever an HTTPS proxy should show; leave databases out.	Docker writes its own network rules and goes around ufw: **ports and firewall**.
The container's user	Use `USER` in the Dockerfile so the application does not run as root: **writing a Dockerfile**.	If someone compromises the application, they reach less.
Images	Prefer the official ones, pin the version instead of `latest`, and rebuild and update now and then.	An old image carries the known flaws of whatever it contains.
Secrets	In a `.env` file with `chmod 600`, outside the repository; never in the Dockerfile or the image.	What goes into an image stays there, and anyone who has it can read it: **environment variables and secrets**.
Limits	Set a memory limit and cap the logs (`max-size` and `max-file` in Compose).	A runaway container should not take the server with it or fill the disk.

Putting it into practice

1. **See what is exposed:**

```
docker ps
sudo ss -tlnp
```

In the ports column, any `0.0.0.0:port` is open to the world. If it should not be, republish it on `127.0.0.1`.

2. **See who is in the `docker` group:** `getent group docker`. Remove whoever does not need it.

3. **Limit a container's memory** when running it: `docker run --memory 512m ...` (the value is an example). Compose has an equivalent option: confirm it in the Compose documentation for your version.

4. **Update methodically:** **updating a Docker application without losing data**, and keep the server's system up to date: **the six VPS security measures**.

Never expose Docker's API to the Internet

(the daemon's TCP port, without authentication) and think twice before mounting `/var/run/docker.sock` inside a container: whoever controls that file controls the server. If a third-party program asks for it, understand why before agreeing.

Make backups before touching anything.

Security also means being able to recover: **backing up a VPS**. What runs on the VPS is yours to maintain, and our support does not install or repair third-party software: **how far our support goes**.

RECOMMENDED

Need a server of your own for your containers? Have a look at our VPS plans.

See the VPS servers →

SEE ALSO

- **Keeping your VPS or dedicated server secure: the six that matter** →
- **Ports and firewall on a VPS: why your app is not reachable** →

Writing a Dockerfile for a Node.js or Python app →

Mozout

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

RLX-INT-KB-3456 · v2026.10.10 · Generated on 15/11/2026 00:39

Online version of this document