Mozout

Gerado a 15/11/2026 01:46

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Usar o Docker num VPS em segurança: as precauções que importam

Docker e contentores

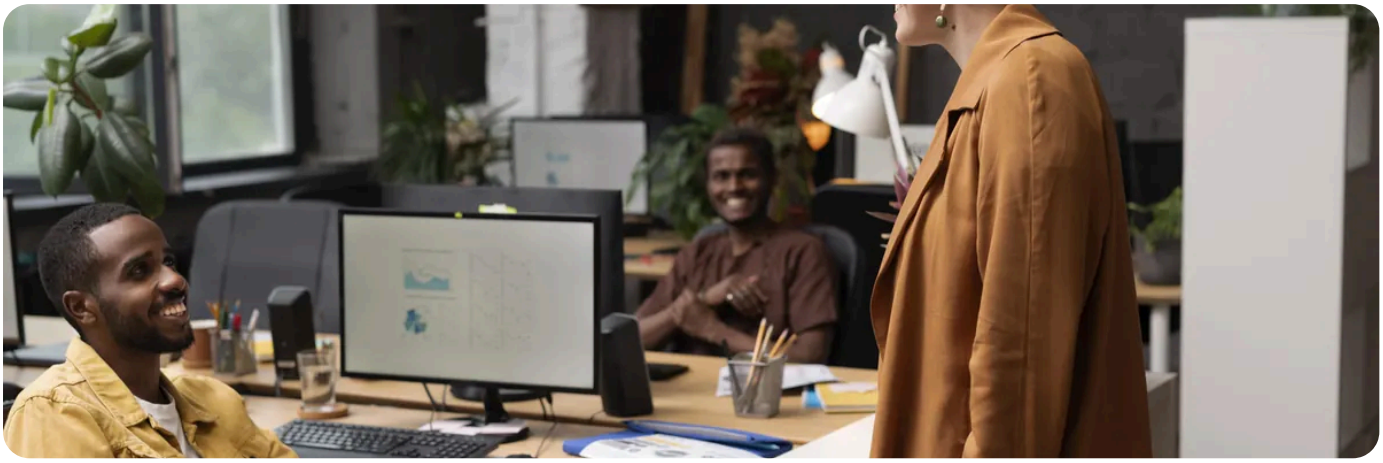
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-PT-KB-3456	v2026.10.10	Portugal · Português

MozOut Portugal
RLX Holdings (Pty) Ltd. · Grupo RLX Holdings
N.º fiscal (SARS) 943 907 6234 · N.º de registo (CIPC) 2025/667953/07

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

Usar o Docker num VPS em segurança: as precauções que importam

Docker e contentores Criado em **10 de outubro de 2026** 3 min de leitura



O Docker facilita pôr uma aplicação a correr, e é por isso que também facilita pôr uma aplicação mal protegida a correr. **A resposta curta:** a segurança de um servidor com Docker joga-se em seis sítios: quem pode usar o `docker`, que portas ficam abertas, com que utilizador corre cada contentor, de que imagens vêm, onde estão os segredos e quanto cada contentor pode gastar. Este artigo é para um VPS não gerido, em que tudo isto é seu.

As seis precauções

Precaução	O que fazer	Porquê
Quem usa o `docker`	Dê acesso ao grupo `docker` só a quem precisa.	Na prática, quem o tem equivale a root no servidor.
Portas publicadas	Publique em `127.0.0.1` (`-p 127.0.0.1:8080:80`) tudo o que um proxy com HTTPS deve mostrar; deixe de fora as bases de dados.	O Docker escreve as suas próprias regras de rede e contorna o ufw: **portas e firewall**.
O utilizador do contentor	Use `USER` no Dockerfile para a aplicação não correr como root: **escrever um Dockerfile**.	Se alguém comprometer a aplicação, alcança menos.
As imagens	Prefira as oficiais, fixe a versão em vez de `latest`, e reconstrua e actualize de vez em quando.	Uma imagem velha leva consigo as falhas conhecidas do que tinha dentro.
Os segredos	Num ficheiro `.env` com `chmod 600`, fora do repositório; nunca no Dockerfile nem na imagem.	O que entra numa imagem fica lá, e quem a tiver lê-o: **variáveis de ambiente e segredos**.
Os limites	Ponha um limite de memória e limite os registos (`max-size` e `max-file` no Compose).	Um contentor descontrolado não deve levar o servidor consigo nem encher o disco.

Passos para pôr isto em prática

1 **Veja o que está exposto:**

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

Na coluna das portas, qualquer `0.0.0.0:porta` está aberto ao mundo. Se não devia estar, republique em `127.0.0.1`.

2 **Veja quem está no grupo `docker`:** `getent group docker`. Tire quem não precisa.

3 **Limite a memória** de um contentor, ao correr: `docker run --memory 512m ...` (o valor é um exemplo). No Compose existe uma opção equivalente: confirme-a na documentação do Compose da sua versão.

4 **Actualize com método:** **actualizar uma aplicação Docker sem perder dados**, e mantenha o sistema do servidor em dia: **as seis medidas de segurança do VPS**.

Nunca exponha a API do Docker à Internet

(a porta TCP do daemon, sem autenticação) e pense duas vezes antes de montar o `/var/run/docker.sock` dentro de um contentor: quem controla esse ficheiro controla o servidor. Se um programa de terceiros pede isso, perceba porquê antes de aceitar.

Faça cópias antes de mexer.

Segurança também é conseguir recuperar: **cópias de um VPS**. O que corre no VPS é seu de manter, e o nosso suporte não instala nem repara software de terceiros: **até onde vai o nosso suporte**.

RECOMENDADO

Precisa de um servidor seu para os contentores? Veja os VPS.

Ver os servidores VPS →

VEJA TAMBÉM

- **Manter o seu VPS ou servidor dedicado seguro: as seis que importam** →
- **Portas e firewall num VPS: porque a aplicação não é alcançável** →

Escrever um Dockerfile para uma aplicação Node.js ou Python

Mozout

MozOut Portugal

RLX Holdings (Pty) Ltd. · Grupo RLX Holdings

N.º FISCAL (SARS)	943 907 6234
N.º DE REGISTO (CIPC)	2025/667953/07
SEDE	72 York Road, Kensington Joanesburgo 2094, Gauteng, África do Sul
CONTACTOS	info@mozout.com · +27 78 823 3325 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-PT-KB-3456 · v2026.10.10 · Gerado a 15/11/2026 01:46

Versão online deste documento