interweb

Gerado a 15/11/2026 00:28

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Instalar o fail2ban num VPS para travar quem tenta adivinhar a senha do SSH

Segurança e acesso

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1350	v2026.10.28	Angola · Português

Interweb Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/1350

Instalar o fail2ban num VPS para travar quem tenta adivinhar a senha do SSH

Segurança e acesso Criado em **10 de outubro de 2026** Atualizado em **28 de outubro de 2026** 2 min de leitura



Um servidor com SSH aberto recebe, **dia e noite, tentativas automáticas de senha** vindas de todo o mundo. O **fail2ban** lê os registos, vê os endereços que falham vezes demais e bloqueia-os durante um tempo. Não substitui a chave SSH, mas limpa o ruído e trava quem insiste. Os comandos são seus, num servidor seu: o suporte não os instala nem repara (ver **até onde vai o nosso suporte**).

Instalar

1. **Debian e Ubuntu:** `sudo apt update` e `sudo apt install fail2ban`.
2. **AlmaLinux e Rocky:** o pacote vem de um repositório extra: `sudo dnf install epel-release` e depois `sudo dnf install fail2ban`.
3. **Ligue o serviço e faça-o arrancar com o servidor:** `sudo systemctl enable --now fail2ban`.

Configurar sem estragar

Não edite o ficheiro `/etc/fail2ban/jail.conf`: uma actualização do pacote pode substituí-lo. Crie o seu, `/etc/fail2ban/jail.local`, só com o que quer mudar:

```
[DEFAULT]
ignoreip = 127.0.0.1/8 ::1 O.SEU.ENDERECO
bantime = 1h
findtime = 10m
maxretry = 5

[sshd]
enabled = true
```

Linha	O que faz
ignoreip	Endereços que nunca são bloqueados. Ponha aí o seu, para não se bloquear a si. Separe-os por espaços.
maxretry	Quantas falhas, dentro do tempo de findtime, antes de bloquear. Os valores deste exemplo (5, 10 minutos, 1 hora) são só um ponto de partida.
findtime	A janela em que as falhas são contadas.
bantime	Durante quanto tempo o endereço fica bloqueado.
port	Se o seu SSH usa outra porta, acrescente em [sshd] a linha `port = 2222`, com o número da sua.

1. **Reinicie para aplicar:** `sudo systemctl restart fail2ban`. Pode testar a configuração antes com `sudo fail2ban-client -t`.

2. **Veja o estado geral:** `sudo fail2ban-client status` lista as "jails" activas, que devem incluir a `sshd`.

3. **Veja quem está bloqueado:** `sudo fail2ban-client status sshd`.

4. **Desbloqueie um endereço** (o seu, se se enganou várias vezes): `sudo fail2ban-client set sshd unbanip O.ENDERECO`.

Pode bloquear-se a si.
Falhar a senha cinco vezes seguidas é o suficiente. Por isso o `ignoreip` e uma chave SSH que funcione. Se acontecer, entre por outra rede (dados móveis, por exemplo) e desbloqueie, ou use o console do painel: ver **perdi o acesso SSH ao servidor**, que tem este caso como a terceira causa.

Se o registo do SSH não existe,
o fail2ban não tem o que ler. Em sistemas mais recentes, que guardam os registos no journal, acrescente `backend = systemd` na secção `[sshd]`. Onde os registos ficam está em **os registos num VPS Linux**. A firewall faz o resto do trabalho com o fail2ban: ver **configurar a firewall ufw**.

PRECISA DE AJUDA?

O fail2ban bloqueou-o e não consegue entrar? Diga-nos o endereço do VPS e de onde se liga.

Abrir um pedido de suporte →

VEJA TAMBÉM

- Configurar a firewall ufw sem ficar de fora
- Criar uma chave SSH e entrar sem senha
- Perdi o acesso SSH ao servidor
- Manter o VPS seguro: as seis coisas que contam

interweb

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao · +244 942 011 191 · www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-AO-KB-1350 · v2026.10.28 · Gerado a 15/11/2026 00:28

Versão online deste documento