interweb

Gerado a 21/10/2026 11:47

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Redis aberto à internet: feche-o com bind, modo protegido, senha e firewall

Segurança

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-2252	v2026.10.21	Angola · Português

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

https://www.meu.interweb.ao/knowledgebase/2252

Para quem tem um VPS ou um servidor dedicado com acesso root. A resposta curta: o Redis foi feito para falar só com aplicações de confiança, na mesma máquina ou numa rede privada. Se responde na porta **6379** a qualquer endereço da internet, qualquer pessoa pode ler e apagar os dados, e há ataques automáticos que usam um Redis aberto para escrever ficheiros no servidor e entrar nele. É por isso que uma equipa nacional de resposta a incidentes (CERT) o reporta e o nosso fornecedor de rede nos envia o aviso, que reencaminhamos para si (**o que é um aviso de abuso**). Fecha-se em quatro camadas: **bind** só no endereço local, **modo protegido**, **palavra-passe** e **firewall**.

Porque é que o Redis ficou aberto

O que encontra	Causa mais provável
`bind 0.0.0.0` **no redis.conf, ou a linha bind comentada**	Alguém abriu o Redis para ligar de outra máquina, ou seguiu um guia que mandava fazê-lo.
Redis num contentor Docker publicado com `-p 6379:6379`	O Docker publica a porta em todos os endereços e passa à frente da ufw: a firewall diz que está fechada e a porta responde na mesma. Veja **usar o Docker num VPS em segurança**.
`protected-mode no`	Foi desligado para «resolver» um erro de ligação. Sem ele e sem palavra-passe, o Redis aceita qualquer um.
Firewall desligada, ou com uma regra que deixa passar a 6379	A regra ficou de um teste e ninguém a apagou.
O `dir` **do Redis a apontar para** `/root/.ssh`**,** `/etc/cron.d` **ou** `/var/spool/cron`**, ou chaves que não criou**	Sinal de que alguém já usou o Redis aberto para escrever ficheiros: trate o servidor como invadido (**o meu VPS foi invadido?**).

Como fechar o Redis sem partir as aplicações

1 **Veja o que está a ouvir:** `sudo ss -tlnp | grep 6379`
`redis-cli CONFIG GET bind`
`redis-cli CONFIG GET protected-mode`
`redis-cli CONFIG GET dir` Se aparece `0.0.0.0:6379`, `[::]:6379` ou o processo `docker-proxy`, está aberto. Se o Redis já tem palavra-passe, use `redis-cli --askpass`.

2 **Antes de fechar, veja quem o usa:** `sudo ss -tnp state established '( sport = :6379 )'`
`redis-cli CLIENT LIST` As aplicações da mesma máquina ligam de 127.0.0.1 e não são afectadas. Se aparece o IP de outro servidor seu, anote-o: vai precisar dele na firewall ou num túnel.

3 **Feche no ficheiro de configuração** (em Debian e Ubuntu costuma ser `/etc/redis/redis.conf`; noutras distribuições pode ser `/etc/redis.conf`). Faça uma cópia do ficheiro e deixe estas linhas:
`bind 127.0.0.1`
`protected-mode yes`
`requirepass UMA-PALAVRA-PASSE-LONGA` Reinicie com `sudo systemctl restart redis-server` (em algumas distribuições o serviço chama-se `redis`).

4 **Se o Redis corre no Docker,** no `docker-compose.yml` troque `"6379:6379"` por `"127.0.0.1:6379:6379"`, ou retire a secção `ports` se só outros contentores o usam (falam pela rede interna do compose). Depois `docker compose up -d`.

5 **Ponha a palavra-passe nova nas aplicações** que usam o Redis (cache de objectos do WordPress, filas, sessões): **cache de objectos com Redis** e **onde cada aplicação guarda os dados de ligação**.

6 **Feche também na firewall:** `sudo ufw status numbered`
`sudo ufw delete N`
`sudo ufw allow from 203.0.113.10 to any port 6379 proto tcp` O `N` é o número da regra da 6379. A última linha só serve se outro servidor seu precisa mesmo do Redis: troque o IP de exemplo pelo dele. Guia completo em **configurar a ufw sem ficar de fora**.

7 **Teste a partir de outra máquina** (não do próprio servidor): `redis-cli -h IP_DO_SERVIDOR ping` ou `nc -zv IP_DO_SERVIDOR 6379`. Tem de falhar ou esgotar o tempo. Se responde PONG, ou NOAUTH, a porta continua aberta à internet.

8 **Responda ao pedido de suporte** no Meu Interweb, dentro do prazo do aviso (curto, muitas vezes de um dia), com um relatório curto: a causa, o que mudou e como confirmou que a porta já não responde de fora. Há um modelo em **responder a um aviso de abuso**. Sem resposta, ou se o problema continuar, o servidor pode ser desligado para proteger a rede, com os dados intactos: **porque o servidor é desligado e como o voltar a ligar**.

Não reinicie o Redis com bind e palavra-passe novos sem saber quem o usa: as aplicações que ligam de outra máquina, ou sem palavra-passe, deixam de funcionar no momento. Confirme no passo 2 e actualize-as no passo 5. Se encontrar sinais de que alguém já entrou, fechar a porta não chega: o mais seguro é **reinstalar o servidor e repor uma cópia limpa** (**que cópia restaurar**). A limpeza no sítio é para quem sabe o que está a fazer.

Se só um servidor seu precisa do Redis, um túnel SSH ou uma VPN (**WireGuard num VPS**) é mais seguro do que abrir a porta, mesmo a um único IP. Num VPS o acesso root é seu: nós não entramos no servidor nem mudamos a firewall que está lá dentro. Se ficar sem SSH, diga-nos no pedido de suporte.

Recebeu um aviso de Redis aberto? Responda no pedido de suporte com o resultado dos comandos do passo 1 e o que mudou.

Abrir pedido de suporte

VEJA TAMBÉM

Um aviso de abuso sobre o seu servidor: o que significa, o prazo e o que precisamos de si

Responder a um aviso de abuso: a causa, o que removeu e como não se vai repetir

O meu VPS foi invadido? Verificar processos, cron, utilizadores, chaves SSH e pastas temporárias

Configurar a firewall ufw no Ubuntu sem ficar de fora do servidor

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

Cache de objetos com Redis no WordPress, num VPS: o que acelera e como instalar

interweb

Versão online deste documento

A Interweb é uma empresa líder em serviços de internet, com a missão de ajudar negócios a nascerem e prosperarem por meio da tecnologia.

2020
FUNDADA

37 mil+
CLIENTES

130+
INSCRIÇÕES POR DIA

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-2252 · v2026.10.21 · Gerado a 21/10/2026 11:47