

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

MySQL, MariaDB ou PostgreSQL acessíveis da internet: fechar a porta sem partir as aplicações

Segurança

CÓDIGO

RLX-MZ-KB-2258

VERSÃO

v2026.10.21

PAÍS · IDIOMA

Moçambique · Português

Interweb Moçambique

RLX Holdings, S.A. · Grupo RLX Holdings

NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

<https://www.meu.interweb.co.mz/knowledgebase/2258>

MySQL, MariaDB ou PostgreSQL acessíveis da internet: fechar a porta sem partir as aplicações

🔒 Segurança 📅 Criado em 21 de outubro de 2026 ⌚ 5 min de leitura



Para quem tem um VPS ou um servidor dedicado com acesso root. A resposta curta: uma base de dados que responde à internet (MySQL ou MariaDB na porta **3306**, PostgreSQL na **5432**) recebe tentativas de entrada a toda a hora, e uma equipa nacional de resposta a incidentes (CERT) reporta-a ao nosso fornecedor de rede. Quase nunca é preciso: as aplicações no mesmo servidor ligam por localhost. Fecha-se em três passos: **ver quem liga de fora**, pôr a base a **ouvir só por dentro**, e deixar passar na firewall só os IPs que precisam, ou usar um **túnel SSH**. Antes de fechar, atenção aos dois casos que partem: aplicações noutro servidor e aplicações em contentores Docker.

🔍 Quem é afectado quando fecha a porta

Quem liga à base	O que acontece
Uma aplicação no mesmo servidor, com host <code>localhost</code> ou <code>127.0.0.1</code>	Nada: continua a funcionar.
Uma aplicação num contentor Docker que liga à base do próprio servidor (por <code>172.17.0.1</code> ou <code>host.docker.internal</code>)	Deixa de ligar se a base ouvir só em 127.0.0.1. Ponha a base na mesma rede do compose, ou faça-a ouvir também no endereço da ponte do Docker e limite essa porta na firewall.
A base num contentor publicado com <code>-p 3306:3306</code> ou <code>-p 5432:5432</code>	O Docker publica-a em todos os endereços e passa à frente da ufw. Troque por <code>127.0.0.1:3306:3306</code> , ou retire a publicação.
Outro servidor seu, um escritório, uma ferramenta de relatórios	Deixa de ligar. Abra só para esse IP, ou use um túnel SSH.
Você, com o Workbench ou o DBeaver	Use um túnel SSH: não precisa de porta aberta. Túnel SSH, passo a passo.

➔ Como fechar a porta, pela ordem certa

1 **Veja se a base ouve para fora:** `sudo ss -tlnp | grep -E ':(3306|5432) ' 0.0.0.0 , [::]` ou o IP público: aberta. `127.0.0.1` : só por dentro. `docker-proxy` : publicada por um contentor.

2 **Veja quem liga hoje, antes de mudar nada:** `sudo ss -tnp state established '( sport = :3306 or sport = :5432 )'` No MySQL ou MariaDB: `SELECT user, host FROM mysql.user; SHOW PROCESSLIST;` (contas com host `%` aceitam ligações de qualquer lado). No PostgreSQL: `SELECT client_addr, username, datname FROM pg_stat_activity;` Anote os IPs que não sejam `127.0.0.1` e descubra que aplicação é cada um.

3 **MySQL ou MariaDB, se ninguém de fora precisa:** faça uma cópia do ficheiro de configuração e, na secção `[mysqld]`, deixe `[mysqld]`
`bind-address = 127.0.0.1` O ficheiro varia: Ubuntu com MySQL, `/etc/mysql/mysql.conf.d/mysqld.cnf`; Debian e Ubuntu com MariaDB, `/etc/mysql/mariadb.conf.d/50-server.cnf`; noutros sistemas, `/etc/my.cnf` ou `/etc/my.cnf.d/`. Reinicie (`sudo systemctl restart mysql`, ou `mariadb`, ou `mysqld`) e confirme com `sudo mysql -e "SHOW VARIABLES LIKE 'bind_address';"`.

4 **PostgreSQL, se ninguém de fora precisa:** encontre os ficheiros com `sudo -u postgres psql -c 'SHOW config_file;'`
`sudo -u postgres psql -c 'SHOW hba_file;'` No primeiro deixe `listen_addresses = 'localhost'`; no segundo retire as linhas `host` com `0.0.0.0/0` ou `:::/0`. Depois `sudo systemctl restart postgresql`. Mais em **ligações remotas ao PostgreSQL**.

5 **Se uma aplicação de fora tem mesmo de ligar directamente,** a base continua a ouvir no endereço público e quem decide é a firewall: só o IP dessa aplicação. `sudo ufw status numbered`
`sudo ufw delete N`
`sudo ufw allow from 203.0.113.10 to any port 3306 proto tcp` (`N` é o número da regra aberta a todos; troque o IP de exemplo pelo da aplicação, e a 3306 pela 5432 no PostgreSQL). Prefira o túnel SSH ou uma VPN (**WireGuard**).

6 **Se a base corre no Docker,** troque a publicação para `"127.0.0.1:3306:3306"` (ou retire-a) e `docker compose up -d`: **Docker num VPS em segurança**.

7 **Teste de fora e troque as palavras-passe:** a partir de outra máquina, `nc -zv IP_DO_SERVIDOR 3306` tem de falhar. Depois mude as palavras-passe das contas da base que estiveram expostas, apague as contas com host `%` que não fazem falta, e actualize as aplicações: **onde cada aplicação guarda os dados de ligação**.

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**.



Uma base que esteve aberta pode já ter sido visitada.

Sinais: bases ou tabelas novas com um pedido de resgate, tabelas vazias, contas que não criou. Não pague: não há garantia nenhuma de que os dados voltem. 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. Veja também **o meu VPS foi invadido?**.



Para trabalhar na base a partir de casa não precisa de porta aberta:

O túnel SSH leva o Workbench ou o DBeaver até ao 127.0.0.1 do servidor, e para quem não tem a sua chave SSH a porta não existe. 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.

PRECISA DE AJUDA?

Não sabe que aplicação liga à base a partir de fora? Envie-nos no pedido de suporte o resultado do passo 2.

 **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



Chegar ao MySQL ou ao PostgreSQL por um túnel SSH, passo a passo



Permitir ligações remotas ao PostgreSQL num VPS, com segurança



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

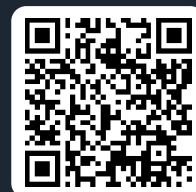


Onde cada aplicação guarda os dados de ligação à base de dados



interweb**Interweb Moçambique****RLX Holdings, S.A. · Grupo RLX Holdings**

NUIT	401 191 607
NUEL	105 045 974
CAE	62022
SEDE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Moçambique
CONTACTOS	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste
documento

RLX-MZ-KB-2258 · v2026.10.21 · Gerado a 21/10/2026 17:37