Gerado a 21/10/2026 13:26

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Permitir conexões remotas ao PostgreSQL num VPS, com segurança

Bancos de Dados

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-BR-KB-2400	v2026.10.10	Brasil · Português (Brasil)

MozOut Brasil
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/2400

Permitir conexões remotas ao PostgreSQL num VPS, com segurança

Bancos de Dados Criado em **10 de outubro de 2026** 3 min de leitura



Por padrão o PostgreSQL só escuta em `127.0.0.1`. Para aceitar conexões de fora, são **três ajustes**: dizer-lhe em que endereço escutar (`listen_addresses`), dizer-lhe **quem** pode entrar (`pg_hba.conf`) e abrir a porta 5432 **só para esse endereço** na firewall. Pressupõe um VPS com root, de preferência com Ubuntu 22.04 LTS, e a configuração e a segurança são suas.

Antes de abrir seja o que for,
pergunte-se se um **túnel SSH** não chega. Com o túnel não se abre porta nenhuma e a base continua invisível para a internet. Veja **o túnel SSH**. Só siga os passos abaixo se uma aplicação em outro servidor tem mesmo de falar diretamente com a base.

Passo a passo

1. **Escutar em outro endereço.** Edite `/etc/postgresql/<versão>/main/postgresql.conf` e mude `listen_addresses = 'localhost'` para `listen_addresses = 'localhost,<IP-do-VPS>'`. Não use `'*'` se puder evitá-lo.

2. **Dizer quem entra.** No `pg_hba.conf`, acrescente uma linha só para o **endereço exato** da aplicação, com senha criptografada:

```
host nome_da_base usuário 203.0.113.10/32 scram-sha-256
```

O `/32` quer dizer «apenas este endereço». O 203.0.113.10 é só um exemplo.

3. **Abrir a porta só para ele.** Com o `ufw`: `ufw allow from 203.0.113.10 to any port 5432 proto tcp`.

4. **Reiniciar.** `systemctl restart postgresql`.

5 **Confirmar.** No VPS, `ss -ltn | grep 5432` mostra os endereços em que escuta. Do outro servidor, `psql -h <IP-do-VPS> -U usuário -d nome_da_base`.

Linha do pg_hba.conf	Quer dizer
`host base usuário IP/32 scram-sha-256`	**Bom.** Uma base, um usuário, um endereço, senha criptografada.
`host all all 0.0.0.0/0 scram-sha-256`	**Mau.** Qualquer pessoa no mundo pode tentar entrar em qualquer base.
`host all all 0.0.0.0/0 trust`	**Desastre.** Entra-se sem senha.

O que costuma dar errado:
Mudar o `postgresql.conf` e esquecer o `pg_hba.conf` (o erro é *no pg_hba.conf entry*); abrir a porta na firewall do servidor mas não em outra firewall que esteja à frente; e deixar uma senha fraca. Bots varrem a porta 5432 o dia todo. Veja **portas e firewall num VPS**.

Como mexer sem se trancar de fora

Antes de editar, faça uma cópia dos dois arquivos (por exemplo, `cp pg_hba.conf pg_hba.conf.antes`). Mexa numa coisa de cada vez e teste. Uma diferença útil: alterações ao `pg_hba.conf` aplicam-se com `systemctl reload postgresql`, mas o `listen_addresses` só muda com `systemctl restart postgresql`. Na firewall, **garanta primeiro a regra da porta do seu SSH** antes de a ligar: se o ligar sem ela, fica sem acesso ao servidor. Se mesmo assim se trancar de fora, veja **as quatro causas habituais**.

Cifre a conexão.
Uma base acessível pela internet, sem TLS, envia a senha e os dados em claro. Se a aplicação suporta, use SSL na conexão. Em alternativa, um túnel SSH dá-lhe a criptografia sem configurar nada no PostgreSQL. Veja **manter o VPS seguro**.

PRECISA DE AJUDA?

Perdeu o acesso ao VPS depois de mexer na firewall? Escreva-nos com o nome do servidor e a hora da alteração.

Abrir um pedido de suporte →

VEJA TAMBÉM

- Ligar ao MySQL ou ao PostgreSQL por túnel SSH
- Portas e firewall num VPS
- Manter o VPS seguro: as seis coisas que contam

MozOut Brasil
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-BR-KB-2400 · v2026.10.10 · Gerado a 21/10/2026 13:26

Versão online deste documento