Mozout

Gerado a 15/11/2026 02:03

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Manter o seu VPS ou servidor dedicado seguro: as seis que contam

Segurança e acesso

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1002	v2026.09.28	Angola · Português

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

https://www.my.mozout.com/knowledgebase/1002

Manter o seu VPS ou servidor dedicado seguro: as seis que contam

Segurança e acesso Criado em **10 de setembro de 2026** Atualizado em **28 de setembro de 2026** 6 min de leitura



Num plano de hospedagem compartilhada, a máquina é nossa e somos nós que a mantemos fechada. Num VPS ou servidor dedicado, **a máquina é sua** - e com ela vem a parte que ninguém menciona no dia da compra: manter a porta trancada é trabalho seu. Onde passa exactamente a linha está em **VPS gerido ou não gerido: quem faz o quê**.

Este artigo é a lista curta. Não é um curso de administração de sistemas - são as seis coisas que, feitas, evitam praticamente tudo o que vemos acontecer.

1. O sistema operativo é a decisão que mais pesa

Um sistema que já não recebe actualizações de segurança não se protege com mais nada: as falhas descobertas depois do fim de vida **nunca serão corrigidas**. Nenhuma firewall tapa isso.

> **Atenção ao escolher na encomenda.**
> A lista de sistemas disponíveis ainda inclui versões que **chegaram ao fim de vida** - CentOS 7, Fedora 37 e 38, Ubuntu 21.04 e 23.04, Windows Server 2008 R2 e 2012 R2. Estão lá por razões históricas e continuam a poder ser instaladas; **não as escolha para um servidor novo**. Se já tem uma delas, fale connosco antes de reinstalar - ver **reinstalar ou mudar o sistema operativo do VPS**.

Para um servidor novo	Escolha
Linux, com painel cPanel/WHM	**AlmaLinux 9** ou **Rocky Linux 9**. São as duas que o cPanel suporta melhor hoje.
Linux, sem painel	**Debian 12** ou **Ubuntu 22.04 LTS**. As versões LTS são as que têm anos de actualizações pela frente.
Windows	**Windows Server 2022**. As anteriores já não recebem correcções.

A escolha completa, com o que cada um serve, está em **que sistema operativo escolher para o seu VPS ou servidor**.

2. As primeiras duas horas do servidor

Um servidor novo começa a ser procurado por varredores automáticos **minutos** depois de ficar no ar. Não é exagero: é o que se vê nos registos. Faça isto antes de instalar o que quer que seja.

1. **Actualize tudo.** Em AlmaLinux ou Rocky: `dnf update -y`. Em Debian ou Ubuntu: `apt update && apt upgrade -y`. A imagem com que o servidor nasce tem sempre semanas ou meses de atraso.

2. **Mude a senha inicial** que lhe foi entregue, e escolha uma longa. Uma frase de cinco palavras vale mais do que oito caracteres com símbolos.

3. **Crie um utilizador normal para si** e use-o no dia a dia, subindo a administrador só quando precisa. Entrar sempre como *root* significa que qualquer erro seu - ou de um programa - tem poderes totais.

4. **Ligue a firewall** e feche tudo o que não usa. É o passo 4 e não o 1 porque de nada serve fechar portas num sistema por actualizar.

3. O SSH é a porta mais atacada. Trate-a assim

A esmagadora maioria das tentativas que um servidor recebe são de adivinhação de senha no SSH, dia e noite, vindas do mundo inteiro. Três mudanças no ficheiro `/etc/ssh/sshd_config` acabam com o problema:

```
PermitRootLogin no
PasswordAuthentication no
Port 2222
```

A linha	O que faz
PermitRootLogin no	Ninguém entra directamente como *root*. Entra-se com o seu utilizador e sobe-se depois. Corta metade dos ataques automáticos de uma vez.
PasswordAuthentication no	Só se entra com **chave**. Uma chave não se adivinha - e uma senha, com tempo suficiente, adivinha-se sempre.
Port 2222	Muda a porta. Não é segurança a sério, mas tira do caminho o ruído dos varredores que só procuram a 22 - e deixa os registos legíveis.

Não feche a sessão antes de testar. É o erro clássico.
Depois de `systemctl restart sshd`, **deixe a sessão actual aberta** e abra uma segunda para testar a entrada. Se a nova falhar, ainda tem a primeira para desfazer. Fechar a única sessão que tinha e só depois descobrir que a chave estava mal é como se perde o acesso a um servidor - ver **perdi o acesso SSH ao meu servidor**.

Antes de desligar a senha, ponha a chave a funcionar.
Gere a chave no **seu** computador com `ssh-keygen -t ed25519`, copie-a com `ssh-copy-id utilizador@o-seu-ip`, e só quando entrar sem senha é que mete o `PasswordAuthentication no`. Por esta ordem, nunca fica fechado de fora.

4. Firewall: feche tudo e abra o que usa

A regra é a mesma em qualquer sistema: negar por omissão e abrir caso a caso. Estas são as portas que um servidor de sites costuma precisar - e mais nenhuma:

Porta	Para quê
80 e 443	O site. A 443 é a cifrada e é a que interessa; a 80 fica aberta só para redireccionar para ela.
22 (ou a que escolheu)	O SSH. Se conseguir, limite-a ao endereço de onde trabalha.
25, 465, 587, 993	Correio. Só se o servidor tratar mesmo de e-mail. Se não trata, deixe fechadas.
2087 e 2083	WHM e cPanel, se tiver painel. São portas de administração - merecem o mesmo cuidado que o SSH.

Junte-lhe um bloqueador de tentativas repetidas - o *CSF* nos servidores com cPanel, ou o *fail2ban* nos outros. É o que trava quem está a adivinhar senhas antes de ele acertar. Sobre o outro lado da mesma moeda, quando é *você* que fica bloqueado, ver **porque é que o seu IP é bloqueado pela firewall**.

5. Cópias de segurança: num VPS, não são automáticas

Isto é o que mais surpreende.
Os planos de VPS vendem a máquina - processador, memória, disco e ligação. **Não incluem cópias de segurança** como a hospedagem compartilhada inclui. Se não contratou um plano gerido nem configurou cópias, **não há nenhuma**. Confirme hoje, e não no dia em que precisar - ver **VPS gerido ou não gerido**.

Uma cópia só conta se estiver **fora da máquina**. Uma cópia guardada no próprio servidor desaparece com ele - e desaparece exactamente nos dois casos em que faz falta: o disco falhar, ou alguém entrar e cifrar tudo. Se o seu plano tem **JetBackup** disponível, confirme que está ligado e que sabe repor.

6. Saber ver que já entraram

Um servidor comprometido raramente dá erro. Ele continua a servir o site - enquanto faz outra coisa por baixo. Estes são os sinais, por ordem de frequência:

Sinal	O que costuma ser
Processador a 100% sem motivo	Mineração de criptomoeda. É hoje o uso mais comum de um servidor invadido.
O IP entrou numa lista de bloqueio	O servidor está a disparar spam. Ver **IP do servidor em lista de bloqueio**
Ficheiros novos com datas de madrugada	Alguém deixou lá qualquer coisa. Compare com uma cópia anterior.
Contas ou chaves SSH que não criou	A porta ficou aberta para voltarem. Verifique */etc/passwd* e os ficheiros *authorized_keys*.

Se desconfia, não limpe primeiro.
Apagar o ficheiro que encontrou não resolve nada se a porta de entrada continua aberta - e destrói a prova de como entraram. Avise-nos, mantenha o servidor como está, e trate a reposição a partir de uma cópia anterior à data suspeita.

O que fica connosco

A rede, o equipamento físico e a disponibilidade da máquina são nossos. O sistema dentro dela é seu - a menos que tenha um plano gerido. Isso não quer dizer que fique sozinho: se tiver dúvidas numa destas mudanças, pergunte antes de mexer. É muito mais barato do que reparar depois. Se o servidor é novo, comece por **primeiros passos com o seu VPS**; se alguma coisa já está a correr mal, **erros comuns de VPS e Cloud**.

PRECISA DE AJUDA?

Quer que revejamos consigo a configuração do seu servidor?

Falar connosco →

Mozout

MozOut 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@mozout.com · +244 942 011 191 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-AO-KB-1002 · v2026.09.28 · Gerado a 15/11/2026 02:03