Gerado a 17/10/2026 11:51

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

A renovação do certbot falhou ou o certificado expirou: como descobrir porquê

VPS e Servidores

CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-MZ-KB-4230	v2026.10.10	Moçambique · Português

MozOut Moçambique
RLX Holdings, S.A. · Grupo RLX Holdings
NUIT 401 191 607 · NUEL 105 045 974 · CAE 62022

https://www.my.mozout.com/knowledgebase/4230

Se o navegador avisa que o certificado expirou num VPS com certbot, a renovação automática **não correu** ou **correu e falhou**. Abra o terminal e faça, por esta ordem: `sudo certbot certificates` para ver as datas, `sudo certbot renew --dry-run` para provar a renovação sem gastar nada, e leia a mensagem de erro. Quase sempre é a porta 80, a DNS ou o servidor web. Num VPS não gerido não há AutoSSL: o certificado e a renovação são seus.

Passo a passo

1. **Veja o estado.** `sudo certbot certificates` mostra cada certificado, os nomes que cobre e os dias que faltam; ao lado de um expirado aparece “INVALID: EXPIRED”.

2. **Provoque o erro com um ensaio.** `sudo certbot renew --dry-run` faz o mesmo que a renovação real contra o ambiente de ensaio. A mensagem que vier no fim é a pista. Use sempre o `--dry-run` enquanto procura a causa: repetir pedidos reais falhados pode esbarrar nos limites do Let’s Encrypt.

3. **Leia o registo completo.** `sudo tail -n 60 /var/log/letsencrypt/letsencrypt.log` tem o pedido, a resposta e o nome que falhou.

4 **Confira se a renovação automática está agendada.** `systemctl list-timers | grep -i certbot`. Se nada aparece, ou o certbot veio de outra forma de instalação (pacote do sistema ou snap), o temporizador pode ter outro nome ou nunca ter sido ligado; veja o que o site do certbot recomenda para o seu sistema.

5 **Resolva a causa, renove e recarregue.** `sudo certbot renew` e, se o servidor web não for recarregado sozinho, `sudo systemctl reload nginx` (ou `apache2` / `httpd`).

6 **Confirme de fora.** `echo | openssl s_client -connect seudominio.tld:443 -servername seudominio.tld 2>/dev/null | openssl x509 -noout -dates` mostra as datas do certificado que os visitantes recebem de facto.

As causas, por ordem de frequência

A mensagem diz…	O que costuma ser
Timeout during connect / Connection refused	A porta 80 está fechada na firewall, ou o servidor web está parado. A validação é por HTTP na porta 80, mesmo que o site viva em 443.
Invalid response / 404 em /.well-known/acme-challenge/	O pedido de validação chega a outro site ou a uma regra de redireccionamento ou de `location` que o apanha. Veja que bloco responde a esse nome.
DNS problem / NXDOMAIN / o IP não é este	O domínio já não aponta para este servidor, ou tem um registo AAAA (IPv6) que aponta para outro lado. Veja **os registos DNS**.
Could not bind to port 80	O certbot em modo autónomo (`--standalone`) quer a porta que o nginx ou o Apache já tem. Mude para o módulo do servidor web (`--nginx` ou `--apache`) ou para `--webroot` .
too many failed authorizations / rate limit	Demasiadas tentativas falhadas. Pare, corrija a causa e espere o tempo que o Let's Encrypt indica antes de tentar de novo.
CAA record prevents issuance	Um registo CAA do domínio não deixa esta autoridade emitir: **registos CAA**.
Renovou com sucesso, mas o navegador mostra o antigo	O servidor web não foi recarregado e continua a servir o certificado em memória. Recarregue-o.

Não fique a repetir o pedido real. Cada tentativa falhada conta para os limites de validação. Se não alterou nada entre dois ensaios, o resultado vai ser o mesmo. Corrija, depois tente.

Mudou o site de servidor ou de IP? O certificado vive no servidor antigo. No novo, tem de o pedir outra vez, e a DNS tem de apontar para o novo antes de a validação passar.

Acrescente um aviso antes de expirar. Uma verificação externa ao certificado (muitos serviços de monitorização gratuitos fazem-no) manda-lhe um e-mail semanas antes, em vez de saber pelo cliente. E guarde o e-mail de contacto que deu ao certbot: é para lá que o Let's Encrypt avisa.

O domínio é nosso e a DNS parece certa mas a validação continua a falhar? Diga-nos o nome e o IP do servidor e confirmamos a zona.

Abrir um pedido de suporte

VEJA TAMBÉM

HTTPS para um contentor: certificado e domínio

Redirecionar para HTTPS e para o domínio simples

Sem cadeado no site: as causas, por ordem

O que é um certificado SSL e porque importa

Versão online deste documento

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

2020	37 mil+	130+
FUNDADA	CLIENTES	INSCRIÇÕES POR DIA

MozOut 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@mozout.com · +258 84 635 1111 · +258 86 635 1111 · www.mozout.com
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

RLX-MZ-KB-4230 · v2026.10.10 · Gerado a 17/10/2026 11:51