interweb

Gerado a 15/11/2026 00:28

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

O SELinux ou o AppArmor está a bloquear o meu serviço: como saber e o que fazer

Segurança e acesso

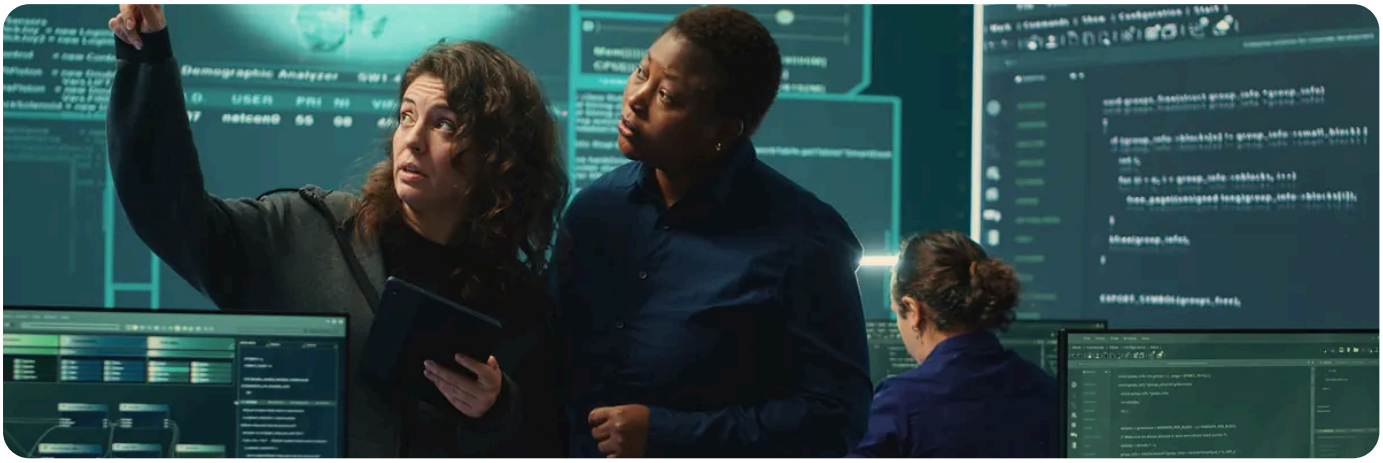
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-1386	v2026.10.10	Angola · Português

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

https://www.meu.interweb.ao/knowledgebase/1386

O SELinux ou o AppArmor está a bloquear o meu serviço: como saber e o que fazer

Segurança e acesso Criado em **10 de outubro de 2026** 3 min de leitura



O SELinux (AlmaLinux, Rocky e outros da família Red Hat) e o AppArmor (Ubuntu e Debian) são camadas de segurança que **negam acções mesmo a quem tem as permissões certas**. Se um serviço dá “Permission denied” e o dono e o `chmod` estão certos, é este o suspeito. Descobre-se pondo o módulo em modo de aviso por um momento e lendo o que foi negado; resolve-se com a regra certa, e não desligando a protecção. Num VPS não gerido, isto é consigo.

Qual é o seu

	SELinux	AppArmor
Onde costuma vir	AlmaLinux, Rocky, outros Red Hat	Ubuntu e Debian
Ver o estado	`getenforce` ou `sestatus`	`sudo aa-status`
Ver o que foi negado	`sudo ausearch -m avc -ts recent` (precisa do auditd) ou o registo do sistema	O registo do núcleo: `sudo journalctl -k | grep -i apparmor` procure “DENIED”
Ensaio sem bloquear	`sudo setenforce 0` (modo permissivo, até ao próximo arranque)	`sudo aa-complain /caminho/do/perfil` (do pacote apparmor-utils)
Voltar a proteger	`sudo setenforce 1`	`sudo aa-enforce /caminho/do/perfil`

Passo a passo

1. **Confirme que é isto.** Ponha o módulo em modo de aviso (linha “Ensaio” da tabela). Se o serviço passa a funcionar, a causa era o SELinux ou o AppArmor. Se continua a falhar, não é isto: volte às permissões normais (**permissões de ficheiros**) e ao registo do serviço (**ler o systemctl status**).

2. **Volte a ligar a protecção logo a seguir.** `sudo setenforce 1` (SELinux) ou `aa-enforce` (AppArmor). O modo permissivo serve de diagnóstico e não de solução.

3. **Leia o que foi negado.** A linha diz o programa, o ficheiro ou a porta, e a acção. Isso diz a regra que falta.

4. **Aplique a regra mínima** (ver abaixo), não uma excepção para tudo.

5. **Teste outra vez** com a protecção ligada.

Os casos mais comuns

Situação	Solução (SELinux)	Solução (AppArmor)
O servidor web não lê uma pasta fora de /var/www	`sudo semanage fcontext -a -t httpd_sys_content_t "/srv/site(/.*)?"` e `sudo restorecon -Rv /srv/site` (`semanage` vem do pacote policycoreutils-python-utils)	Edite o perfil do programa em `/etc/apparmor.d/` para permitir a pasta e recarregue com `sudo systemctl reload apparmor`
O servidor web (como proxy) não consegue ligar-se à aplicação	`sudo setsebool -P httpd_can_network_connect 1`	Raro; é um perfil específico.
Um serviço quer escutar numa porta nova (por exemplo o SSH noutra porta)	`sudo semanage port -a -t ssh_port_t -p tcp 2222` (2222 é um exemplo; para o servidor web, `http_port_t`)	Normalmente não é preciso.
Ficheiros copiados ou movidos ficam com a etiqueta errada	`sudo restorecon -Rv /pasta`	Não se aplica.

Desligar o SELinux de vez é a resposta de que se arrepende. `SELINUX=disabled` em `/etc/selinux/config` tira uma protecção que defende o servidor de uma falha numa aplicação. O mesmo para parar o AppArmor. Prefira sempre a regra mínima; use o modo permissivo só para diagnosticar, e por pouco tempo.

Mudar a etiqueta ou o perfil sem perceber pode abrir o que devia estar fechado.
Se não percebe a linha negada, copie-a e procure-a na documentação da distribuição antes de aplicar. Segundo o seu sistema, os nomes de pacotes e ferramentas podem variar.

Antes de culpar o SELinux ou o AppArmor,
confira o básico: o serviço está a correr? a porta está aberta na firewall (**portas e firewall**)? o ficheiro existe? A maioria dos “Permission denied” são permissões normais.

PRECISA DE AJUDA?

O servidor ficou inacessível por SSH depois de mexer nestas protecções? A consola do painel entra sem passar pela rede: diga-nos o que fez.

Abrir um pedido de suporte →

VEJA TAMBÉM

- Permissões de ficheiros num VPS Linux →
- Um serviço não arranca: ler o systemctl status →
- Mudar a porta do SSH sem se trancar fora →
- Perdi o acesso SSH ao servidor →

interweb

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

Versão online deste documento

RLX-AO-KB-1386 · v2026.10.10 · Gerado a 15/11/2026 00:28