Mozout

Generated on 15/11/2026 00:40

KNOWLEDGE BASE · PUBLIC DOCUMENT

SELinux or AppArmor is blocking my service: how to tell, and what to do

Security & Access

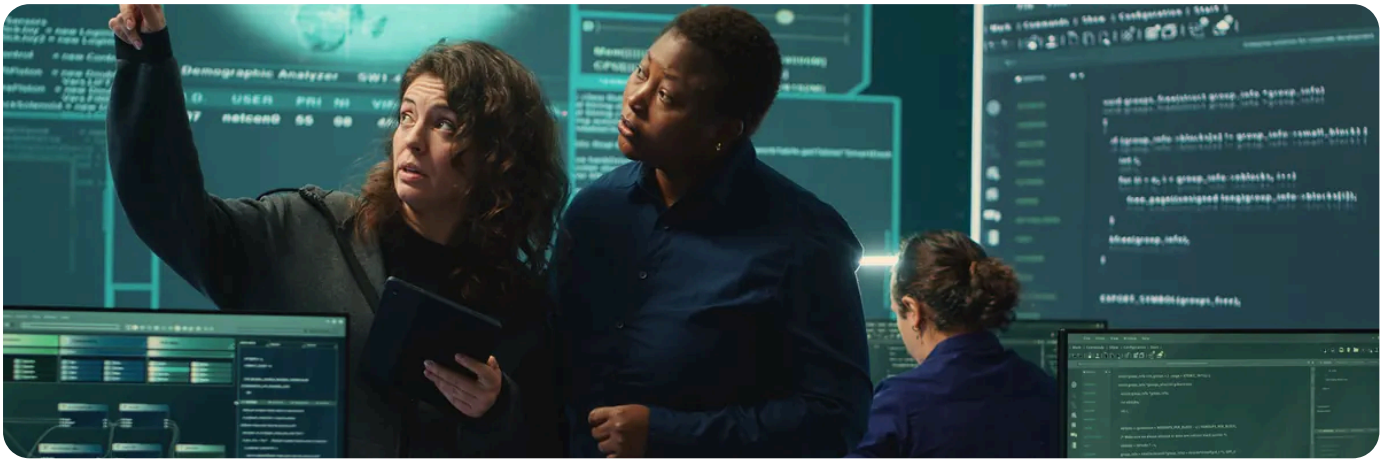
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-4296	v2026.10.10	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/4296

SELinux or AppArmor is blocking my service: how to tell, and what to do

Security & Access Created on **October 10, 2026** 3 min read



SELinux (AlmaLinux, Rocky and others in the Red Hat family) and AppArmor (Ubuntu and Debian) are security layers that **deny actions even to whoever has the right permissions**. If a service gets “Permission denied” and the owner and `chmod` are right, this is the suspect. You find out by switching the module to warning mode for a moment and reading what was denied; you fix it with the right rule, not by turning the protection off. On an unmanaged VPS this is yours to do.

Which one you have

	SELinux	AppArmor
Where it usually ships	AlmaLinux, Rocky, other Red Hat family	Ubuntu and Debian
See the state	`getenforce` or `sestatus`	`sudo aa-status`
See what was denied	`sudo ausearch -m avc -ts recent` (needs auditd) or the system log	The kernel log: `sudo journalctl -k | grep -i apparmor` look for “DENIED”
Rehearse without blocking	`sudo setenforce 0` (permissive mode, until the next boot)	`sudo aa-complain /path/to/profile` (from the apparmor-utils package)
Protect again	`sudo setenforce 1`	`sudo aa-enforce /path/to/profile`

Step by step

1. **Confirm it is this.** Put the module in warning mode (the “Rehearse” row). If the service starts working, the cause was SELinux or AppArmor. If it still fails, it is not this: go back to ordinary permissions (**file permissions**) and the service’s log (**reading systemctl status**).

2. **Switch the protection back on straight away.** `sudo setenforce 1` (SELinux) or `aa-enforce` (AppArmor). Permissive mode is for diagnosis, not a solution.

3. **Read what was denied.** The line names the program, the file or port, and the action. That tells you the rule that is missing.

4. **Apply the smallest rule** (see below), not an exception for everything.

5. **Test again** with the protection on.

The most common cases

Situation	Fix (SELinux)	Fix (AppArmor)
The web server will not read a folder outside /var/www	`sudo semanage fcontext -a -t httpd_sys_content_t "/srv/site(/.*)?"` and `sudo restorecon -Rv /srv/site` (`semanage` comes from the policycoreutils-python-utils package)	Edit the program’s profile in `/etc/apparmor.d/` to allow the folder and reload with `sudo systemctl reload apparmor`
The web server (as a proxy) cannot connect to the application	`sudo setsebool -P httpd_can_network_connect 1`	Rare; it is a specific profile.
A service wants to listen on a new port (for example SSH on another port)	`sudo semanage port -a -t ssh_port_t -p tcp 2222` (2222 is an example; for the web server, `http_port_t`)	Usually not needed.
Copied or moved files carry the wrong label	`sudo restorecon -Rv /folder`	Does not apply.

Turning SELinux off for good is the answer you regret.

`SELINUX=disabled` in `/etc/selinux/config` removes a protection that defends the server from a flaw in an application. The same goes for stopping AppArmor. Always prefer the smallest rule; use permissive mode only to diagnose, and briefly.

Changing a label or profile without understanding can open what should stay closed.

If you do not understand the denied line, copy it and look it up in the distribution's documentation before applying anything. Depending on your system, package and tool names may vary.

Before blaming SELinux or AppArmor,

check the basics: is the service running? is the port open in the firewall (**ports and firewall**)? does the file exist? Most "Permission denied" cases are plain permissions.

NEED A HAND?

Did the server become unreachable over SSH after touching these protections? The panel console gets you in without the network: tell us what you did.

Open a support ticket →

SEE ALSO

- File permissions on a Linux VPS →
- A service will not start: reading systemctl status →
- Changing the SSH port without locking yourself out →
- I have lost SSH access to my server →

Mozout

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-INT-KB-4296 · v2026.10.10 · Generated on 15/11/2026 00:40