
AppArmor: control d'accés obligatori a Linux

Índex

Introducció	1
1. Conceptes bàsics	1
1.1. Perfils	1
1.2. Modes de funcionament	1
2. Eines bàsiques	2
2.1. Instal·lació	2
2.2. Veure l'estat general	2
2.3. Canviar el mode d'un perfil	3
2.4. Recarregar un perfil després d'editar-lo	3
3. Anatomia d'un perfil	3
3.1. Permisos de fitxers	4
3.2. Comodins (wildcards)	4
3.3. Capabilities	4
3.4. Xarxa	4
4. Depurar denegacions (DENIED)	5
4.1. Generar regles automàticament amb aa-logprof	5
5. Fitxers “local” (overrides sense tocar el perfil original)	6
6. Cas pràctic: BIND9 + zones dinàmiques (DDNS)	6
7. Cas pràctic: Kea DHCP-DDNS (D2)	7
8. Desactivar AppArmor per a un servei (només per depurar!)	7
9. Ordres de referència ràpida	8
10. Resum	8

Introducció

AppArmor (Application Armor) és un sistema de **control d'accés obligatori** (*Mandatory Access Control*, MAC) integrat al kernel de Linux mitjançant el mòdul de seguretat **LSM** (*Linux Security Modules*). A diferència dels permisos tradicionals Unix (propietari/grup/altres), AppArmor limita **què pot fer un programa concret**, independentment de l'usuari que l'executi.

És el sistema MAC per defecte a **Ubuntu** i **Debian**, mentre que **SELinux** ho és a la família Red Hat (RHEL, Fedora, CentOS).

NOTA

AppArmor treballa amb **rutes de fitxers** (path-based), no amb etiquetes com SELinux. Això el fa més senzill d'entendre i configurar, encara que una mica menys flexible en alguns escenaris.

1. Conceptes bàsics

1.1. Perfils

Un **perfil** és un fitxer de text que descriu els permisos d'un binari concret: quins fitxers pot llegir/escriure/executar, quines capacitats del kernel pot fer servir, i quins recursos de xarxa pot accedir.

Els perfils es guarden a:

```
/etc/apparmor.d/
```

El nom del fitxer normalment és la ruta del binari amb els / substituïts per . :

```
/usr/sbin/named      → /etc/apparmor.d/usr.sbin.named
/usr/sbin/mysqld     → /etc/apparmor.d/usr.sbin.mysqld
/usr/sbin/kea-dhcp-ddns → /etc/apparmor.d/usr.sbin.kea-dhcp-ddns
```

1.2. Modes de funcionament

Mode	Descripció
enforce	Bloqueja activament les accions no permeses i les registra
complain	Només registra les violacions (mode "queixa"), sense bloquejar res
disabled	El perfil no s'aplica
unconfined	El procés no té cap perfil carregat

El mode **complain** és molt útil quan estàs **desenvolupant o depurant** un perfil nou, perquè et deixa veure què faria falta permetre sense trencar el servei.

2. Eines bàsiques

2.1. Instal·lació

A Ubuntu/Debian sol venir instal·lat per defecte. Si no:

```
sudo apt update
sudo apt install apparmor apparmor-utils apparmor-profiles
```

- apparmor-utils: eines de gestió (aa-status, aa-complain, aa-enforce, aa-genprof...)
- apparmor-profiles: perfils predefinits per a molts serveis comuns

2.2. Veure l'estat general

```
sudo aa-status
```

Exemple de sortida:

```
apparmor module is loaded.
15 profiles are loaded.
12 profiles are in enforce mode.
  /usr/sbin/named
  /usr/sbin/mysqld
  /usr/sbin/tcpdump
  ...
3 profiles are in complain mode.
  /usr/sbin/kea-dhcp-ddns
  ...
2 processes have profiles defined.
2 processes are in enforce mode.
  /usr/sbin/named (1234)
```

Alternativa més curta:

```
sudo apparmor_status
```

2.3. Canviar el mode d'un perfil

```
# Passar a mode complain (només registra, no bloqueja)
sudo aa-complain /etc/apparmor.d/usr.sbin.named

# Tornar a mode enforce (bloqueja)
sudo aa-enforce /etc/apparmor.d/usr.sbin.named

# Desactivar completament un perfil
sudo ln -s /etc/apparmor.d/usr.sbin.named /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/usr.sbin.named
```

2.4. Recarregar un perfil després d'editar-lo

```
sudo systemctl reload apparmor
```

O bé, per a un perfil concret:

```
sudo apparmor_parser -r /etc/apparmor.d/usr.sbin.named
```

3. Anatomia d'un perfil

Estructura bàsica d'un perfil:

```
#include <tunables/global>

/usr/sbin/named {
    #include <abstractions/base>
    #include <abstractions/nameservice>

    capability net_bind_service,
    capability setgid,
    capability setuid,

    network inet stream,
    network inet dgram,

    /usr/sbin/named mr,
    /etc/bind/** r,
    /var/cache/bind/** rw,
    /var/log/named/** rw,
    /run/named/** rw,

    # Denegar explícitament l'accés a dades sensibles
    deny /etc/shadow r,
}
```

3.1. Permisos de fitxers

Símbol	Significat
r	lectura
w	escriptura
a	append (afegir, subconjunt de w)
l	crear enllaços (link)
k	lock
m	mmap executable
x	execució
ix	execució heretant el mateix perfil
Px	execució amb un altre perfil, netejant l'entorn
Ux	execució sense confinar (unconfined)

3.2. Comodins (wildcards)

```
/var/cache/bind/*      → fitxers directes dins el directori
/var/cache/bind/**     → fitxers a qualsevol profunditat
/etc/bind/named.conf.? → un sol caràcter comodí
```

3.3. Capabilities

Corresponen a les *capabilities* del kernel Linux (man 7 capabilities):

```
capability net_bind_service,    # obrir ports < 1024
capability setuid,
capability setgid,
capability dac_override,        # saltar-se permisos DAC
```

3.4. Xarxa

```
network inet stream,    # TCP
network inet dgram,     # UDP
network inet6 stream,
```

4. Depurar denegacions (DENIED)

Quan AppArmor bloqueja alguna cosa, ho registra al log del sistema.

```
# journalctl (systemd)
sudo journalctl -xe | grep -i apparmor

# o directament al syslog
sudo grep -i apparmor /var/log/syslog
sudo grep -i "type=AVC" /var/log/audit/audit.log # si audit està
↪ actiu
```

Exemple d'entrada de log:

```
audit: type=1400 audit(1719999999.123:45): apparmor="DENIED"
↪ operation="open"
profile="/usr/sbin/named" name="/etc/bind/zones/thos.local.db.jnl"
pid=1234 comm="named" requested_mask="w" denied_mask="w" fsuid=101
↪ ouid=101
```

Informació clau del missatge:

- **profile**: quin perfil ha fet el bloqueig
- **name**: la ruta a la qual s'intentava accedir
- **requested_mask / denied_mask**: quin permís faltava (aquí, w d'escriptura)
- **comm**: el procés implicat

CONSELL

Per al cas típic amb **BIND9**: si mous el directori de zones fora de `/var/lib/bind/` (per exemple a `/etc/bind/zones/`), el perfil per defecte no ho permetrà i veuràs **DENIED** en intentar escriure els fitxers `.jnl` de les zones dinàmiques (DDNS). Cal afegir una regla al perfil o bé a un fitxer *local override*.

4.1. Generar regles automàticament amb aa-logprof

Una manera còmoda d'“aprendre” un perfil és:

1. Posa el perfil en mode complain
2. Fes servir el servei normalment (deixa que falli el que hagi de fallar)
3. Executa aa-logprof, que llegeix el log i et proposa regles noves

```
sudo aa-complain /etc/apparmor.d/usr.sbin.named
sudo systemctl restart bind9
# ... provoca l'ús normal del servei (transferències, DDNS, etc.) ...
sudo aa-logprof
```

aa-logprof et mostrarà cada accés denegat i et preguntarà si vols **Allow**, **Deny**, **Glob** (generalitzar amb comodins) o **Ignore**. Al final, torna el perfil a enforce:

```
sudo aa-enforce /etc/apparmor.d/usr.sbin.named
```

5. Fitxers “local” (overrides sense tocar el perfil original)

Els paquets Debian/Ubuntu solen incloure una línia com aquesta al final del perfil:

```
#include <local/usr.sbin.named>
```

Això permet afegir regles pròpies sense modificar el fitxer original del paquet (que es pot sobre escriure en una actualització):

```
sudo nano /etc/apparmor.d/local/usr.sbin.named
```

Contingut d'exemple, per permetre un directori de zones personalitzat:

```
/etc/bind/zones/** rw,  
/etc/bind/zones/*.jnl rw,
```

Després, recarrega:

```
sudo apparmor_parser -r /etc/apparmor.d/usr.sbin.named
```

6. Cas pràctic: BIND9 + zones dinàmiques (DDNS)

Escenari habitual en un laboratori amb named i actualitzacions dinàmiques (Kea DHCP-DDNS):

1. **Síntoma:** el servidor DHCP envia actualitzacions DDNS, però la zona no s'actualitza; als logs de named no hi ha error clar.

2. **Comprovació:**

```
sudo journalctl -u apparmor -f  
sudo tail -f /var/log/syslog | grep DENIED
```

3. **Causa típica:** named no té permís d'escriptura al directori on hi ha els fitxers de zona (.db) o els fitxers de diari (.jnl), perquè s'ha canviat la ubicació per defecte (/var/lib/bind/).

4. **Solució:**

- Afegir el directori concret al perfil local:

```
/etc/bind/zones/** rw,
```

- Recarregar el perfil.

- Verificar propietari i permisos Unix (AppArmor **no substitueix** els permisos DAC, els complementa):

```
sudo chown bind:bind /etc/bind/zones/*
```

7. Cas pràctic: Kea DHCP-DDNS (D2)

El dimoni kea-dhcp-ddns també pot necessitar permisos d'escriptura per als seus fitxers de lease, sockets Unix de control, o certificats TLS si Stork hi connecta per gRPC.

```
sudo aa-status | grep kea
```

Si el perfil existeix i està en enforce, comprova denegacions igual que amb BIND9:

```
sudo journalctl -xe | grep -i "kea.*DENIED"
```

Regles habituals a revisar/afegir en un override local:

```
/var/lib/kea/** rw,  
/run/kea/** rw,  
/etc/kea/** r,
```

8. Desactivar AppArmor per a un servei (només per depurar!)

AVÍS

Desactivar AppArmor **redueix la seguretat** del sistema. Fes-ho només temporalment per aïllar un problema, mai com a solució definitiva en producció.

```
# Posar en complain (no bloqueja, però registra)  
sudo aa-complain /etc/apparmor.d/usr.sbin.named  
  
# Desactivar completament el perfil  
sudo ln -s /etc/apparmor.d/usr.sbin.named /etc/apparmor.d/disable/  
sudo apparmor_parser -R /etc/apparmor.d/usr.sbin.named
```

Per tornar-lo a activar:

```
sudo rm /etc/apparmor.d/disable/usr.sbin.named  
sudo apparmor_parser -r /etc/apparmor.d/usr.sbin.named
```

9. Ordres de referència ràpida

```
sudo aa-status                # estat general
sudo aa-enabled               # comprova si AppArmor està
    ⇨ actiu al kernel
sudo aa-complain <perfil>     # mode complain
sudo aa-enforce <perfil>      # mode enforce
sudo aa-disable <perfil>      # desactivar un perfil
sudo apparmor_parser -r <fitxer_perfil> # recarregar un perfil
sudo aa-logprof               # generar regles a partir del log
sudo aa-genprof <binari>      # crear un perfil nou des de
    ⇨ zero
journalctl -xe | grep -i apparmor # veure denegacions recents
```

10. Resum

- AppArmor confina programes concrets segons **rutes de fitxers**, no usuaris.
- Els perfils viuen a `/etc/apparmor.d/` i tenen mode `enforce` o `complain`.
- Les denegacions es veuen amb `journalctl` o `/var/log/syslog`, amb el camp `DENIED`.
- Per a serveis com **BIND9** o **Kea DHCP-DDNS** amb rutes no estàndard, cal afegir regles a un fitxer local i recarregar el perfil.
- `aa-logprof` automatitza la creació de regles a partir dels logs generats en mode `complain`.
- AppArmor complementa els permisos Unix (DAC); no els substitueix --- cal que tots dos siguin correctes.

Versions d'aquest document

- [HTML](#)
- [PDF](#)
- [ODT](#)
- [MD](#)

[Domini Públic \(CC0\)](#)