AppArmor : confinement et diagnostic

Formation : BTS SIO — Option SISR

1. Rôle et fonctionnement

AppArmor limite les ressources accessibles à un programme selon un profil. Un fichier peut donc être accessible avec les permissions Linux classiques tout en restant interdit au service par son profil AppArmor.

Dans le cas d'Unbound, le problème concerne la journalisation : le service doit pouvoir écrire dans le chemin prévu et son profil doit autoriser cette opération.

2. Diagnostic

```
sudo aa-status
sudo journalctl -k -b | grep -i apparmor
sudo journalctl -u unbound -b --no-pager
ls -ld /var/log/unbound
ls -l /var/log/unbound
```

Comparer le chemin refusé, le programme concerné et l'opération demandée. Vérifier également le propriétaire et les droits du répertoire parent.

3. Correction ciblée

Identifier le profil chargé et son éventuel fichier local d'extension. Ajouter uniquement l'autorisation nécessaire au chemin de journalisation, selon la syntaxe du profil. Recharger ensuite le profil concerné :

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

Cette commande suppose que ce fichier est bien le profil utilisé sur la machine. Vérifier son existence et son contenu avant exécution.

4. Vérification et dépannage

Relancer le service, générer une requête DNS et vérifier que le journal reçoit un événement sans nouveau refus AppArmor. Le mode complain peut aider ponctuellement au diagnostic, mais il ne doit pas être confondu avec le mode enforce attendu pour le confinement.

La désactivation globale d'AppArmor masque la cause et affaiblit tous les services protégés. Conserver la correction dans l'historique de configuration avec etckeeper.

5. Références

- Debian — apparmor_parser

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=cyber:apparmor

Last update: **2026/10/18 01:23**