Distribution EOLE - Tâche #37581

Scénario # 37403 (Nouveau): Porter Scribe en 2.11

Profil apparmor trop restrictif

11/08/2026 09:34 - Benjamin Bohard

Statut:	À valider	**Début:**	30/06/2026
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Bohard	**% réalisé:**	0%
Version cible:	Carnet Cadoles - MEN	**Temps estimé:**	0.00 heure

Description

Un certain nombre de services est en erreur dans le conteneur du fait d'accès à des ressources interdit par apparmor

Révisions associées

Révision 704ce635 - 11/08/2026 09:54 - Benjamin Bohard

Règles supplémentaires pour le profil apparmor du conteneur addc

Ref #37581

Historique

#1 - 11/08/2026 09:34 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#2 - 11/08/2026 09:53 - Benjamin Bohard

```
root@addc:~# systemctl list-units --failed
  UNIT                                LOAD   ACTIVE SUB    DESCRIPTION
● chrony.service                      loaded failed failed chrony, an NTP client/server
● container-getty@1.service           loaded failed failed Container Getty on /dev/pts/1
● container-getty@2.service           loaded failed failed Container Getty on /dev/pts/2
● container-getty@3.service           loaded failed failed Container Getty on /dev/pts/3
● container-getty@4.service           loaded failed failed Container Getty on /dev/pts/4
● netplan-configure.service           loaded failed failed Netplan Backend Configuration
● systemd-journal-flush.service       loaded failed failed Flush Journal to Persistent Storage
● systemd-journald.service            loaded failed failed Journal Service
● systemd-udev-load-credentials.service loaded failed failed Load udev Rules from Credentials
● systemd-journald-dev-log.socket     loaded failed failed Journal Socket (/dev/log)
● systemd-journald.socket             loaded failed failed Journal Sockets
```

Tous ces services, exceptés chrony et netplan-configure, échouent avec un code d'erreur 243/CREDENTIALS.

Le cas de chrony est plus complexe.

Installation de plusieurs outils pour permettre de trouver les bonne adaptations à faire :
- apparmor-utils (pour avoir l'outil aa-logprof)
- auditd (parce que l'outil aa-logprof ne tire pas parti des journaux de journald)

Les règles suivantes sont proposées :

```
mount options=(rw,move) -> /run/credentials/**,
mount options=(bind, nodev, noexec, nosuid, remount, rw) -> /run/systemd/mount-rootfs/proc/,
mount fstype=proc options=(nodev, noexec, nosuid, rw) proc -> /run/systemd/namespace-*/,
mount options=(rbind,rw) / -> /run/systemd/mount-rootfs/,
pivot_root /run/systemd/mount-rootfs/,
```

Ces règles peuvent être intégrées au profil généré automatiquement pour les conteneurs (lxc.apparmor.profile = generated) en les ajoutant à leur configuration via l'option lxc.apparmor.raw (une ligne par règle ?).

#3 - 11/08/2026 09:58 - Benjamin Bohard

- Statut changé de En cours à À valider