Distribution EOLE - Tâche #35976

Scénario # 35952 (Terminé (Sprint)): EOLE 2.10 : L'instance d'AmonEcole doit aller à son terme

Étude

10/06/2024 11:47 - Benjamin Bohard

Statut:	Fermé	**Début:**	01/10/2022
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Bohard	**% réalisé:**	100%
Version cible:	Livraison Cadoles - MEN 30/06/2024 (60+18)	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 10/06/2024 11:47 - Benjamin Bohard

- Statut changé de Nouveau à En cours

#2 - 10/06/2024 12:07 - Benjamin Bohard

La première erreur rapportée est un timeout qui existe aussi quand on exécute la commande hostnamectl à la main dans le conteneur.
La connexion au conteneur est par ailleurs très longue a aboutir.

Dans le même temps, dmseg enregistre l'activité suivante :

```
[ 6435.897758] audit: type=1400 audit(1718012376.097:1937): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-partage_</var/lib/lxc>" name="/dev/" pid=36502 comm="(sd-mkdc
reds)" flags="rw, rslave"
[ 6435.948892] audit: type=1400 audit(1718012376.148:1938): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-reseau_</var/lib/lxc>" name="/dev/" pid=36504 comm="(sd-mkdcr
eds)" flags="rw, rslave"
[ 6436.068802] audit: type=1400 audit(1718012376.268:1939): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-bdd_</var/lib/lxc>" name="/dev/" pid=36520 comm="(sd-mkdcreds
)" flags="rw, rslave"
[ 6436.146281] audit: type=1400 audit(1718012376.346:1940): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-partage_</var/lib/lxc>" name="/dev/" pid=36527 comm="(sd-mkdc
reds)" flags="rw, rslave"
[ 6436.226729] audit: type=1400 audit(1718012376.426:1941): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-bdd_</var/lib/lxc>" name="/dev/" pid=36529 comm="(sd-mkdcreds
)" flags="rw, rslave"
[ 6436.478778] audit: type=1400 audit(1718012376.678:1942): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-bdd_</var/lib/lxc>" name="/dev/" pid=36531 comm="(sd-mkdcreds
)" flags="rw, rslave"
[ 6436.724028] audit: type=1400 audit(1718012376.924:1943): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-bdd_</var/lib/lxc>" name="/dev/" pid=36533 comm="(sd-mkdcreds
)" flags="rw, rslave"
[ 6436.974419] audit: type=1400 audit(1718012377.174:1944): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-bdd_</var/lib/lxc>" name="/dev/" pid=36535 comm="(sd-mkdcreds
)" flags="rw, rslave"
[ 6437.313494] audit: type=1400 audit(1718012377.513:1945): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-addc_</var/lib/lxc>" name="/dev/" pid=36548 comm="(sd-mkdcred
s)" flags="rw, rslave"
[ 6437.565311] audit: type=1400 audit(1718012377.765:1946): apparmor="DENIED" operation="mount" class="mount"
info="failed perms check" error=-13 profile="lxc-addc_</var/lib/lxc>" name="/dev/" pid=36559 comm="(sd-mkdcred
s)" flags="rw, rslave"
```

Cela se traduit par une procédure d'instance très longue (plus d'une heure).
Après aa-teardown pour décharger les profils d'apparmor, la procédure d'instance est beaucoup plus rapide : 10 minutes.

#3 - 10/06/2024 12:12 - Benjamin Bohard

Les autres problèmes immédiatement visible lors de l'instance sont :
- l'exécution de quotacheck en pretemplate

```
quotacheck: Impossible de remonter le système de fichier monté sur / en lecture seule, les valeurs comptabilis
ées riquent d'être fausses.
Veuillez interrompre tous les programmes qui écrivent sur ce système de fichiers ou utilisez l'option -m pour
forcer la vérification.
```

- l'absence de nf_conntrack_helper (fait l'objet d'un autre scénario)
- la délégation à l'utilisateur eole-workstation-manager

```
run-parts: executing /usr/share/eole/postservice/30-eole-workstation-manager instance
Résolution du nom d'hôte "salt" en 10.3.2.5 : Record added successfully

Ajout du compte de jonction au domaine 'eole-workstation-manager'...
User 'eole-workstation-manager' added successfully
Mise en conformité de l'utilisateur 'eole-workstation-manager'...
Expiry for user 'eole-workstation-manager' disabled.
WARNING: Using passwords on command line is insecure. Installing the setproctitle python module will hide thes
e from shortly after program start.
Changed password OK
Délégation pour 'eole-workstation-manager' absentes sur CN=Computers
ERROR(<class 'ValueError'>): uncaught exception - Unable to parse SDDL
  File "/usr/lib/python3/dist-packages/samba/netcmd/__init__.py", line 279, in _run
    return self.run(*args, **kwargs)
           ^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/samba/netcmd/dsacl.py", line 148, in run
    self.add_ace(sd_helper, objectdn, new_ace)
  File "/usr/lib/python3/dist-packages/samba/netcmd/dsacl.py", line 103, in add_ace
    ai,ii = sd_helper.dacl_prepend_aces(object_dn, new_ace)
            ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/samba/sd_utils.py", line 171, in dacl_prepend_aces
    ace_sd = security.descriptor.from_sddl("D:" + aces, self.domain_sid)
             ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
Impossible de positionner la délégation pour 'eole-workstation-manager' sur CN=Computers
Ajout du compte de lecture 'eole-workstation-reader'...
User 'eole-workstation-reader' added successfully
```

- la version de Nextcloud incompatible avec la version de php du module.

```
This version of Nextcloud is not compatible with PHP>=8.2.<br/>You are currently running 8.3.6.
```

#4 - 10/06/2024 13:28 - Benjamin Bohard

Extrait de la configuration apparmor qui serait en cause :

```
  # currently blocked by apparmor bug
  mount -> /usr/lib*/*/lxc/{**,},
  mount -> /usr/lib*/lxc/{**,},
  mount -> /usr/lib/x86_64-linux-gnu/lxc/rootfs/{,**},
  mount fstype=devpts -> /dev/pts/,
  mount options=bind /dev/pts/ptmx/ -> /dev/ptmx/,
  mount options=bind /dev/pts/** -> /dev/**,
  mount options=(rw, make-slave) -> **,
  mount options=(rw, make-rslave) -> **,
  mount options=(rw, make-shared) -> **,
  mount options=(rw, make-rshared) -> **,
  mount fstype=debugfs,
  mount fstype=fuse.*,
```

#5 - 11/06/2024 10:15 - Benjamin Bohard

Le service en conteneur qui n'est pas compatible avec les règles de montage de Apparmor est systemd-logind (d'où la lenteur de connexion ssh, pam_systemd étant déclaré dans /etc/pam.d/common-session).
Il semble nécessaire de permettre le montage hors sandbox pour ce se soit fonctionnel.

Un problème similaire a déjà été rencontré par le passé :
https://wiki.debian.org/LXC/SystemdMountsAndAppArmor

Dans le contexte d'exécution sur EOLE, l'assouplissement des règles de contrôle semble acceptable.

#6 - 12/06/2024 09:39 - Benjamin Bohard

Il y a peut-être d'autres services systemd-* impactés en conteneur :
- systemd-hostnamed (fonctionne quand on arrête apparmor)
- d'autres services en échec mais peut-être pas en lien avec apparmor : systemd-networkd, systemd-resolved, systemd-sysctl, systemd-tmpfiles-setup-*

Les services systemd-* forment le gros des services en échec dans le conteneur addc.

#7 - 13/06/2024 08:48 - Benjamin Bohard

Rapport de bug qui semble lié : https://bugs.launchpad.net/ubuntu/+source/apparmor/+bug/2064144

#8 - 17/06/2024 15:35 - Benjamin Bohard

En jouant avec le profil apparmor chargé :

```
root@partage:~# systemctl list-units -t service --failed
  UNIT                                    LOAD   ACTIVE SUB    DESCRIPTION
● console-getty.service                   loaded failed failed Console Getty
● systemd-resolved.service                loaded failed failed Network Name Resolution
● systemd-sysctl.service                  loaded failed failed Apply Kernel Variables
● systemd-tmpfiles-setup-dev-early.service loaded failed failed Create Static Device Nodes in /dev gracefully
● systemd-tmpfiles-setup-dev.service      loaded failed failed Create Static Device Nodes in /dev
● systemd-tmpfiles-setup.service          loaded failed failed Create Volatile Files and Directories

Legend: LOAD   → Reflects whether the unit definition was properly loaded.
        ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
        SUB    → The low-level unit activation state, values depend on unit type.

6 loaded units listed.
root@partage:~# exit
déconnexion
root@amonecole:~# vim /var/lib/lxc/partage/config
root@amonecole:~# lxc-stop partage
root@amonecole:~# lxc-start partage
root@amonecole:~# ssh partage

EOLE est une distribution libre dérivée de la distribution Ubuntu.
Veuillez consulter les licences de chacun des produits dans
/usr/share/doc/*/copyright/.

Documentation EOLE : http://eole.ac-dijon.fr/documentations/
Last login: Mon Jun 17 14:51:02 2024 from 192.0.2.1
root@partage:~# systemctl list-units -t service --failed
  UNIT                     LOAD   ACTIVE SUB    DESCRIPTION
● systemd-resolved.service loaded failed failed Network Name Resolution
```

Avec comme différence (profil généré VS profil généré avec règles décommentées)

```
< #  mount options=(rw,make-slave) -> **,
< #  mount options=(rw,make-rslave) -> **,
< #  mount options=(rw,make-shared) -> **,
< #  mount options=(rw,make-rshared) -> **,
< #  mount options=(rw,make-private) -> **,
< #  mount options=(rw,make-rprivate) -> **,
< #  mount options=(rw,make-unbindable) -> **,
< #  mount options=(rw,make-runbindable) -> **,
---
>   mount options=(rw,make-slave) -> **,
>   mount options=(rw,make-rslave) -> **,
>   mount options=(rw,make-shared) -> **,
>   mount options=(rw,make-rshared) -> **,
>   mount options=(rw,make-private) -> **,
>   mount options=(rw,make-rprivate) -> **,
>   mount options=(rw,make-unbindable) -> **,
>   mount options=(rw,make-runbindable) -> **,
```

Le changement de syntaxe (*** devenant {,**/*}) ne semble pas indispensable (mais offre une meilleure protection ?).

La version générée du profil n'est, a priori, pas modifiable. Elle semble construite au moment de la compilation de lxc (la version du paquet liblxc-common sur oracular est corrigée).

Il reste toutefois des services en erreurs (variables selon les conteneurs).

#9 - 18/06/2024 09:53 - Benjamin Bohard

```
ssh addc "systemctl list-units -t service --failed"
  UNIT                                     LOAD   ACTIVE SUB    DESCRIPTION
● console-getty.service                    loaded failed failed Console Getty
● systemd-resolved.service                 loaded failed failed Network Name Resolution
● systemd-sysctl.service                   loaded failed failed Apply Kernel Variables
● systemd-tmpfiles-setup-dev-early.service loaded failed failed Create Static Device Nodes in /dev gracefully
● systemd-tmpfiles-setup-dev.service       loaded failed failed Create Static Device Nodes in /dev
● systemd-tmpfiles-setup.service           loaded failed failed Create Volatile Files and Directories
```

```
ssh reseau "systemctl list-units -t service --failed"
  UNIT                                     LOAD   ACTIVE SUB    DESCRIPTION
● console-getty.service                    loaded failed failed Console Getty
● courier-authdaemon.service               loaded failed failed Courier Authentification Daemon
● eoleapps.service                         loaded failed failed Eole flask server
● exim4.service                            loaded failed failed exim Mail Transport Agent
● spamd.service                            loaded failed failed Perl-based spam filter using text analysis
● systemd-resolved.service                 loaded failed failed Network Name Resolution
● systemd-sysctl.service                   loaded failed failed Apply Kernel Variables
● systemd-tmpfiles-setup-dev-early.service loaded failed failed Create Static Device Nodes in /dev gracefully
● systemd-tmpfiles-setup-dev.service       loaded failed failed Create Static Device Nodes in /dev
● systemd-tmpfiles-setup.service           loaded failed failed Create Volatile Files and Directories
```

```
ssh partage "systemctl list-units -t service --failed"
  UNIT                                     LOAD   ACTIVE SUB    DESCRIPTION
● console-getty.service                    loaded failed failed Console Getty
● systemd-resolved.service                 loaded failed failed Network Name Resolution
● systemd-sysctl.service                   loaded failed failed Apply Kernel Variables
● systemd-tmpfiles-setup-dev-early.service loaded failed failed Create Static Device Nodes in /dev gracefully
● systemd-tmpfiles-setup-dev.service       loaded failed failed Create Static Device Nodes in /dev
● systemd-tmpfiles-setup.service           loaded failed failed Create Volatile Files and Directories
```

```
ssh internet "systemctl list-units -t service --failed"
  UNIT                                     LOAD   ACTIVE SUB    DESCRIPTION
● console-getty.service                    loaded failed failed Console Getty
● systemd-resolved.service                 loaded failed failed Network Name Resolution
● systemd-sysctl.service                   loaded failed failed Apply Kernel Variables
● systemd-tmpfiles-setup-dev-early.service loaded failed failed Create Static Device Nodes in /dev gracefully
● systemd-tmpfiles-setup-dev.service       loaded failed failed Create Static Device Nodes in /dev
● systemd-tmpfiles-setup.service           loaded failed failed Create Volatile Files and Directories
```

```
ssh bdd "systemctl list-units -t service --failed"
  UNIT                                     LOAD   ACTIVE SUB    DESCRIPTION
● console-getty.service                    loaded failed failed Console Getty
● systemd-resolved.service                 loaded failed failed Network Name Resolution
● systemd-sysctl.service                   loaded failed failed Apply Kernel Variables
● systemd-tmpfiles-setup-dev-early.service loaded failed failed Create Static Device Nodes in /dev gracefully
● systemd-tmpfiles-setup-dev.service       loaded failed failed Create Static Device Nodes in /dev
● systemd-tmpfiles-setup.service           loaded failed failed Create Volatile Files and Directories
```

#10 - 18/06/2024 15:08 - Laurent Gourvenec

 courier-authdaemon.service loaded failed failed Courier Authentification Daemon
-> path /run/courier (/authdaemon?) manquant. Un lxc-destroy gen_conteneur semble résoudre le problème. -> problème à l'instance non lié à Apparmor ? En tout cas, sur une daily, Maj-Auto + instance n'a pas le problème.

#11 - 20/06/2024 10:50 - Benjamin Bohard

- Statut changé de En cours à À valider

#12 - 16/07/2024 16:27 - Laurent Gourvenec

- Statut changé de À valider à Résolu

#13 - 22/07/2024 15:59 - Joël Cuissinat

- Statut changé de Résolu à Fermé

- % réalisé changé de 0 à 100

- Restant à faire (heures) mis à 0.0