# eole-antivirus - Anomalie #8002

## clamd ne se lance pas suite au reconfigure

04/16/2014 11:03 AM - équipe eole Academie d'Orléans-Tours

| | | | |
|---|---|---|---|
| **Status:** | Fermé | **Start date:** | |
| **Priority:** | Normal | **Due date:** | 05/16/2014 |
| **Assigned To:** | Joël Cuissinat | **% Done:** | 100% |
| **Category:** | | **Estimated time:** | 2.00 hours |
| **Target version:** | Mises à jour 2.3.13 | **Spent time:** | 1.00 hour |
| **Distribution:** | EOLE 2.3 | | |

**Description**

Un vieux signalement, http://dev-eole.ac-dijon.fr/issues/1711, a fait qu'au reconfigure un chmod sur /var/log/clamav/clamav.log est effectué, il appartient ensuite à root:adm

Mais cela ne plait pas à clamav-daemon :

```
root@amon23-0999999f:~# ll /var/log/clamav/clamav.log
-rw-r----- 1 root adm 2018 2014-04-16 09:51 /var/log/clamav/clamav.log
root@amon23-0999999f:~# service clamav-daemon restart
 * Stopping ClamAV daemon clamd     [ OK ]
 * Starting ClamAV daemon clamd
ERROR: Can't open /var/log/clamav/clamav.log in append mode (check permissions!).
ERROR: Can't initialize the internal logger
```

Un logorotate résoud le soucis :

```
 logrotate -f /etc/logrotate.conf
ll  /var/log/clamav/clamav.log
-rw-r----- 1 clamav adm 0 2014-04-09 15:21 /var/log/clamav/clamav.log
```

Mais c'est embetant de se retrouver avec un service inopérant suite à un reconfigure.
Par contre clamav-freshclam est bien fonctionnel, mais l'est tout autant avec les droits "-rw-r----- 1 clamav adm" apparement.

Du coup la ligne de http://dev-eole.ac-dijon.fr/issues/1711 ne doit t-elle pas être "chown -R clamav:adm /var/log/clamav" ?

Et finalement, le diagnose ne détecte pas ce soucis de lancement, il affiche :

```
*** Anti-virus
.                  Anti-virus => Ok
.              Service de maj => Ok
.                Dernière maj => Ok (08:01:35 04/16/14)
```

Alors que :

```
ps faux| grep clam
root      4488  0.0  0.0   3368   816 pts/0    S+   10:50   0:00          \_ grep --color clam
root      4035  2.6  0.0  17768  2092 ?        Ss   10:44   0:08 /usr/bin/freshclam -d --quiet
```

Le test de /usr/share/eole/diagnose/module/151-antivirus se base sur /etc/eole/clamd-reload.cnf qui dans le cas d'une install sans container retourne "ok" dans tous les cas.
Peut être ajouter un équivalent à 'TestPid "Service de maj" freshclam' pour clamd, comme : 'TestPid "Antivirus" clamd' ?

Ces tests sont effectués en 2.3.12 sur un Amon, mais les autres modules ont les mêmes soucis je pense, à vérifier.

**Related issues:**

| | | |
|---|---|---|
| Related to python-pyeole - Anomalie #8139: clamav-daemon désactivé alors qu'i... | **Fermé** | **06/20/2014** |

### Associated revisions

**Revision 24024dbd - 05/09/2014 11:05 AM - Joël Cuissinat**

Correction a minima des droits pour clamd

- posttemplate/00-antivirus : droits pour l'utilisateur clamav

Fixes #8002 @30m

### History

**#1 - 04/16/2014 11:11 AM - Joël Cuissinat**

*- Description updated*

*- Status changed from Nouveau to A étudier*

*- Target version set to Mises à jour 2.3.13*

*- Estimated time set to 2.00 h*

**#2 - 05/05/2014 02:59 PM - Joël Cuissinat**

*- Due date set to 05/16/2014*

**#3 - 05/06/2014 09:39 AM - Joël Cuissinat**

*- Assigned To set to Joël Cuissinat*

*- % Done changed from 0 to 10*

En réalité, cette situation apparaît lorsque clamav est activé mais qu'aucun des services EOLE pouvant l'utiliser (dansguardian, samba, proftpd, exim4) n'a jamais été configuré pour le faire.

Cela correspond bien à la configuration proposée par défaut sur Amon-2.3 (**activer_clam="oui"** mais **dansguardian_clam="non"**) dans laquelle le fichier **clamd.conf** n'est pas templatisé car jugé inutile.

En le templatisant une fois, l'erreur disparaît :

```
CreoleCat -o /etc/clamav/clamd.conf /usr/share/eole/creole/distrib/clamd.conf
```

En production, si la fonctionnalité "Activer l'anti-virus sur le proxy" n'est pas utilisée (et que le service clamav n'est pas utilisé par ailleurs) le plus simple est de désactiver totalement l'antivirus : **Activer l'anti-virus ClamAV ( activer_clam ) = "non"**

#### #4 - 05/09/2014 11:06 AM - Joël Cuissinat

*- Status changed from A étudier to Résolu*

*- % Done changed from 10 to 100*

Appliqué par commit conf-scribe:24024dbd213e332f16ff05427e16e69f1cc17b2e.

#### #5 - 05/09/2014 11:16 AM - Joël Cuissinat

**Corrigé à minima pour 2.3**

Sur Amon-2.4, le paquet eole-antivirus n'est plus préinstallé.
Si on l'installe, l'antivirus est par défaut :

- désactivé sur le proxy
- activé sur la messagerie

Si on installe le paquet et que l'on désactive les 2 (avant la 1ère instance), le service clamav-daemon n'est pas lancé à l'instance/reconfigure et est considéré comme désactivé :

```
*** Anti-virus
.                  Anti-virus => Désactivé
.              Service de maj => Ok
.                Dernière maj => Aucune information
```

#### #6 - 05/13/2014 11:25 AM - Daniel Dehennin

*- Status changed from Résolu to Fermé*

Après mise à jour et reconfigure:

```
root@amon:~# ls -ld /var/log/clamav/
drwxr-xr-x 2 clamav adm 4096 2014-05-13 11:11 /var/log/clamav/
```

```
*** Anti-virus
.                  Anti-virus => Ok
.              Service de maj => Ok
.                Dernière maj => Erreur : Impossible de recharger clamd (11:23:22 05/13/14)
```