eole-antivirus - Anomalie #12884

Problème droits sur /var/log/clamav suite a migration

10/09/2015 16:14 - Vincent Febvre

Statut:	Classée sans suite	**Début:**	10/09/2015
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	1.00 heure
Distribution:	EOLE 2.4		

Description

Test effectué sur un Amon 2.3 migré en 2.4.2

Avant Migration sur la version 2.3

```
root@amon:~# ll /var/log/clamav
total 56
drwxr-xr-x  2 clamav adm   4096 2015-09-10 14:23 ./
drwxr-xr-x 21 root   root  4096 2015-09-10 14:41 ../
-rw-r-----  1 clamav adm   9378 2015-09-10 14:41 clamav.log
-rw-r-----  1 clamav adm  31431 2015-09-10 14:40 freshclam.log
-rw-r--r--  1 clamav adm     60 2015-09-10 14:30 freshclam-status.log
```

Après Migration et redémarrage du serveur

```
root@amon:~# ll /var/log/clamav/
total 68
drwxr-xr-x  2 clamav adm   4096 sept. 10 14:23 ./
drwxr-xr-x 27 root   root  4096 sept. 10 15:42 ../
-rw-r-----  1 clamav adm  13921 sept. 10 15:42 clamav.log
-rw-r-----  1 root   adm  33054 sept. 10 15:42 freshclam.log
-rw-r--r--  1 clamav adm     60 sept. 10 14:30 freshclam-status.log
```

Les droits sur fresclam.log ne sont pas corrects.

Après instance

```
root@amon:~# ll /var/log/clamav/
total 72
drwxr-xr-x  2 root   clamav  4096 sept. 10 14:23 ./
drwxr-xr-x 27 root   root    4096 sept. 10 15:55 ../
-rw-r-----  1 root   clamav 18170 sept. 10 15:55 clamav.log
-rw-r-----  1 clamav clamav 35437 sept. 10 15:55 freshclam.log
-rw-r--r--  1 clamav clamav    53 sept. 10 15:49 freshclam-status.log
```

Les droits sur fresclam sont bons mais plus pour clamav.log
De plus les droits sur le dossiers clamav sont passés de clamav adm à root   clamav.

Si on regarde le fichier /etc/logrotate.d/clamav-daemon, on devrait avoir clamav adm :

```
/var/log/clamav/clamav.log {
     rotate 12
     weekly
     compress
     delaycompress
     create 640  clamav adm
     postrotate
     /etc/init.d/clamav-daemon reload-log > /dev/null
     endscript
     }
```

Demandes liées:

Lié à eole-antivirus - Scénario #14132: Clamav doit passer par le service rsy...	**Terminé (Sprint**	**23/11/2015**	**18/12/2015**

Historique

#1 - 10/09/2015 16:30 - Gérald Schwartzmann

J'ai reproduit le problème

#2 - 23/11/2015 12:11 - Emmanuel GARETTE

- Projet changé de creole à eole-antivirus

#3 - 07/12/2015 16:53 - Daniel Dehennin

Et d'après la configuration de **clamav**(1) il doit fonctionner en tant que **root**, contrairement à **freshclam**(2) :

```
root@scribe:~# lsof +D /var/log/clamav/
COMMAND    PID   USER   FD   TYPE DEVICE SIZE/OFF   NODE NAME
clamd     1455   root    3w   REG  252,2   108125 392246 /var/log/clamav/clamav.log
freshclam 1544 clamav    3w   REG  252,2   121094 392245 /var/log/clamav/freshclam.log
```

(1) source:tmpl/clamd.conf@74ea0ee#L155
(2) source:tmpl/freshclam.conf@74ea0ee#L32

#4 - 25/09/2019 17:12 - Joël Cuissinat

- Statut changé de Nouveau à Classée sans suite