eole-antivir - Tâche #30913

Scénario # 30912 (Terminé (Sprint)): comportement clamav

les logs remontent une erreur de socket

27/10/2020 16:19 - Thierry Bertrand

Statut:	Fermé	**Début:**	26/10/2020
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	100%
Version cible:	MTES - prestation cadoles 43-46	**Temps estimé:**	0.00 heure
		Temps passé:	0.00 heure

Description

Historique

#1 - 27/10/2020 16:22 - Thierry Bertrand

que ce soit par cron ou par un lancement manuel, l'erreur suivante est remontée :

```
ERROR: Could not connect to clamd on LocalSocket /var/run/clamav/clamd.ctl: No such file or directory
```

```
root@set-ente-59ens1:/home# /usr/bin/clamdscan -l /var/log/clamav/clamav.log -v -m --fdpass liste_postes_fa201
9-2020.pdf
WARNING: Ignoring deprecated option DetectBrokenExecutables at /etc/clamav/clamd.conf:206
--------------------------------------
ERROR: Could not connect to clamd on LocalSocket /var/run/clamav/clamd.ctl: No such file or directory

----------- SCAN SUMMARY -----------
Infected files: 0
Time: 0.000 sec (0 m 0 s)
```

#2 - 27/10/2020 16:52 - Thierry Bertrand

configuration du seth 2.7.1 :

```
oot@set-ente-59ens1:/home# CreoleGet --list|grep clam
activer_clam="oui"
clam_broken_exe="no"
clam_checks="24"
clam_connect_timeout="300"
clam_detect_pua="no"
clam_dns_database_info="current.cvd.clamav.net"
```

```
clam_exit_on_oom="no"
clam_forcer_daemon="oui"
clam_forcer_mirror_database="oui"
clam_max_attempts="5"
clam_max_directory_recursion="15"
clam_max_file_size="10"
clam_max_files="5000"
clam_max_recursion="16"
clam_max_scan_size="50"
clam_mirror_database="clamav.depot.ac.centre-serveur.i2"
clam_mirror_type="PrivateMirror"
clam_receive_timeout="300"
clam_scan_elf="no"
clam_scan_mail="no"
clam_scan_pdf="yes"
exim_clamav="non"
serveurs_clamav_nationaux_ip=""
serveurs_clamav_nationaux_netmask=""
```

#3 - 16/11/2020 10:18 - Emmanuel GARETTE

Moi je n'ai pas d'erreur.

La socket existe et est bien utilisé par clamd :

```
root@scribe:~# ls -alh /var/run/clamav/clamd.ctl
srw-rw-rw- 1 root root 0 nov.  16 10:11 /var/run/clamav/clamd.ctl
root@scribe:~# lsof |grep clamd.ctl
clamd     26684                 root    4u     unix 0xffff9a34b64b9c00      0t0    1036229 /var/run/clamav/cl
amd.ctl type=STREAM
clamd     26684 28487           root    4u     unix 0xffff9a34b64b9c00      0t0    1036229 /var/run/clamav/cl
amd.ctl type=STREAM
```

#4 - 16/11/2020 11:49 - Emmanuel GARETTE

Il semble que parfois clamav-daemon s'arrête, ce qui provoque cette erreur.

Lors d'un défaillance il faudrait au moins récupérer les logs du daemon :

```
journalctl -fu clamav-daemon.service
```

#5 - 16/11/2020 16:55 - Philippe Carre

avscan lancé à 16h13 :
13 16 * * * /usr/share/eole/sbin/avscan -s
avec mode debug pour clamd

/home/data/bureautique/dossiers: OK
ERROR: Could not connect to clamd on LocalSocket /var/run/clamav/clamd.ctl: Connection refused
ERROR: Could not connect to clamd on LocalSocket /var/run/clamav/clamd.ctl: Connection refused
ERROR: Could not connect to clamd on LocalSocket /var/run/clamav/clamd.ctl: Connection refused

---------- SCAN SUMMARY ----------
Infected files: 0
Total errors: 3
Time: 671.564 sec (11 m 11 s)

journalctl clamd :

```
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_find_and_parse_objs_in_objstm: Found object
7269 0 in object stream at offset: 9467
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_parseobj: Parsing object 7269 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_parseobj: 7269 0 obj flags: 02
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_find_and_parse_objs_in_objstm: Found object
7270 0 in object stream at offset: 9680
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_parseobj: Parsing object 7270 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_parseobj: 7270 0 obj flags: 02
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_decodestream_internal: pdf_find_and_parse_ob
js_in_objstm found 31 new objects.
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: -------------EXPERIMENTAL-------------
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: extracted 9808 bytes 7216 0 obj
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj:         ... to /var/lib/clamav/
clamav-2aa02a6656ac64bac334d1a7d918cec2.tmp/pdf02
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: in cli_magic_scandesc (reclevel: 1/16)
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Recognized ASCII text
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: cache_check: c978d560ed9aeb56c928723be36b5fce is
 negative
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: matcher_run: performing regex matching on full m
ap: 0+9808(9808) >= 9808
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: hashtab: Freeing hashset, elements: 0, capacity:
 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: in cli_scanscript()
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: matcher_run: performing regex matching on full m
ap: 0+9808(9808) >= 9808
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: hashtab: Freeing hashset, elements: 0, capacity:
 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: cli_magic_scandesc: returning 0  at line 3202
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: cache_add: c978d560ed9aeb56c928723be36b5fce (lev
el 0)
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode executing hook id 258 (2 hooks)
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode 3: executing in JIT mode
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: bytecode finished in 5 us
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode 3 returned 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode 43: executing in JIT mode
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: bytecode finished in 0 us
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode 43 returned 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode: executed 2 bytecodes for this hook
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: obj 7217 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: dumping obj 7217 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: parsing a stream in obj 7217 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: -------------EXPERIMENTAL-------------
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_getdict: /DecodeParms not found in dict
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_getdict: /DP not found in dict
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_getdict: /Type/ObjStm not found in dict
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_decodestream: detected 1 applied filters
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_decodestream_internal: decoding [5] => FLATE
DECODE
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: cli_pdf: inflated 459 bytes from 276 total bytes
 (0 bytes remaining)
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: -------------EXPERIMENTAL-------------
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: extracted 459 bytes 7217 0 obj
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj:         ... to /var/lib/clamav/
clamav-2aa02a6656ac64bac334d1a7d918cec2.tmp/pdf03
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: in cli_magic_scandesc (reclevel: 1/16)
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Recognized ASCII text
```

```
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: cache_check: ebed4903ae7d57a5cf794bc807d4ba68 is
 positive
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: cli_magic_scandesc: returning 0  at line 3439 (n
o post, no cache)
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode executing hook id 258 (2 hooks)
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode 3: executing in JIT mode
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: bytecode finished in 3 us
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode 3 returned 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode 43: executing in JIT mode
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: bytecode finished in 0 us
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode 43 returned 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: Bytecode: executed 2 bytecodes for this hook
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: obj 7218 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: dumping obj 7218 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: parsing a stream in obj 7218 0
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: -------------EXPERIMENTAL-------------
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_getdict: /DecodeParms not found in dict
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_getdict: /DP not found in dict
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_getdict: /Type/ObjStm not found in dict
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_decodestream: detected 1 applied filters
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_decodestream_internal: decoding [5] => FLATE
DECODE
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: cli_pdf: inflated 1823 bytes from 773 total byte
s (0 bytes remaining)
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: -------------EXPERIMENTAL-------------
nov. 16 16:24:02 set-ente-59ens1 clamd[929]: LibClamAV debug: pdf_extract_obj: extracted 1823 bytes 7218 0 obj
nov. 16 16:24:13 set-ente-59ens1 systemd[1]: Stopping Clam AntiVirus userspace daemon...
nov. 16 16:24:13 set-ente-59ens1 clamd[929]: Shutdown closed fd 5
nov. 16 16:24:13 set-ente-59ens1 clamd[929]: Waiting for all threads to finish
nov. 16 16:24:13 set-ente-59ens1 clamd[929]: Received POLLIN|POLLHUP on fd 7
nov. 16 16:24:13 set-ente-59ens1 clamd[929]: Shutdown: closed fd 4
nov. 16 16:24:13 set-ente-59ens1 clamd[929]: Shutdown: closed fd 7
nov. 16 16:24:13 set-ente-59ens1 clamd[929]: Syncpipe write failed
nov. 16 16:24:14 set-ente-59ens1 clamd[929]: Client disconnected while scanjob was active
nov. 16 16:24:14 set-ente-59ens1 clamd[929]: Finished scanthread
nov. 16 16:24:14 set-ente-59ens1 clamd[929]: Scanthread: connection shut down (FD 9)
nov. 16 16:24:14 set-ente-59ens1 clamd[929]: THRMGR: queue (single) crossed low threshold -> signaling
nov. 16 16:24:14 set-ente-59ens1 clamd[929]: THRMGR: queue (bulk) crossed low threshold -> signaling
nov. 16 16:24:16 set-ente-59ens1 clamd[929]: Shutting down the main socket.
nov. 16 16:24:16 set-ente-59ens1 clamd[929]: Closing the main socket.
nov. 16 16:24:16 set-ente-59ens1 systemd[1]: Stopped Clam AntiVirus userspace daemon.
nov. 16 16:24:16 set-ente-59ens1 systemd[1]: Starting Clam AntiVirus userspace daemon...
nov. 16 16:24:16 set-ente-59ens1 systemd[1]: Started Clam AntiVirus userspace daemon.
nov. 16 16:24:30 set-ente-59ens1 clamd[2564]: Limits: Core-dump limit is 0.
nov. 16 16:24:30 set-ente-59ens1 clamd[2564]: Listening daemon: PID: 2564
nov. 16 16:24:30 set-ente-59ens1 clamd[2564]: MaxQueue set to: 100
nov. 16 16:24:30 set-ente-59ens1 clamd[2564]: fds_poll_recv: timeout after 600 seconds
```

cat kernel.notice.log :

2020-11-16T16:24:16.122989+01:00 set-ente-59ens1.ente-ens.ad.e2.rie.gouv.fr kernel: [2207908.566453] audit: type=1400 audit(1605540256.117:178): apparmor="DENIED" operation="connect" profile="/usr/sbin/clamd" name="/run/samba/winbindd/pipe" pid=2564 comm="clamd" requested_mask="wr" denied_mask="wr" fsuid=0 ouid=0

dmesg :
[2207908.566453] audit: type=1400 audit(1605540256.117:178): apparmor="DENIED" operation="connect" profile="/usr/sbin/clamd" name="/run/samba/winbindd/pipe" pid=2564 comm="clamd" requested_mask="wr" denied_mask="wr" fsuid=0 ouid=0

#6 - 17/11/2020 16:54 - Emmanuel GARETTE

Les messages de dmesg sont "normaux" au démarrage du service.

Ce que je ne comprends pas c'est :

```
nov. 16 16:24:13 set-ente-59ens1 systemd[1]: Stopping Clam AntiVirus userspace daemon...
```

Je ne sais pas pourquoi le service semble s'arrêté en plein milieu du scan antivirus ...

Je constate par contre qu'au redémarrage du service il faut attendre environ 20 seconds avant que la socket redémarre.

Je ne vois rien dans la configuration de systemd qui expliquerait cet arrêt.

Je ne vois rien non plus du côté de freshclam.

Il faudrait peut etre regarder tous les logs au moment de l'arrêt du service pour voir si on sait pourquoi ce service est arrêté.

#7 - 20/11/2020 15:41 - Emmanuel GARETTE

- Statut changé de Nouveau à En cours

#8 - 11/03/2021 11:23 - Philippe Carre

- Statut changé de En cours à Résolu

- % réalisé changé de 0 à 100

- Temps estimé mis à 0.00 h

- Restant à faire (heures) mis à 0.0

Ok, le pb a été détecté : c'est notre supervision qui stoppe le process clam qd la charge CPU est > à 90% pendant un certain temps ...
Le script nagios a été corrigé.
Fin de l'affaire!

#9 - 02/08/2021 17:45 - Philippe Carre

- Statut changé de Résolu à Fermé