eole-antivirus - Anomalie #8102

on peut envoyer de mail avec des virus

04/29/2014 04:48 PM - Emmanuel GARETTE

Status:	Fermé	**Start date:**	
Priority:	Haut	**Due date:**	
Assigned To:	Emmanuel GARETTE	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	Eole 2.4 Stable	**Spent time:**	2.75 hours
Distribution:	EOLE 2.4		

Description

Sur Scribe il n'y a pas de vérification de la présence de virus quand on envoi un mail.

J'ai pu envoyer le fichier joint à une liste du Scribe et a une adresse extérieur à l'établissement.

Le fichier est pourtant bien vu comme un virus par clamdscan :

```
root@scribe:~# clamdscan test.txt
/root/test.txt: Eicar-Test-Signature FOUND

----------- SCAN SUMMARY -----------
Infected files: 1
Time: 5.217 sec (0 m 5 s)
```

L'antivirus est bien activé :

```
root@scribe:~# CreoleGet exim_clamav
oui
```

Related issues:

Related to conf-scribe - Evolution #3735: Mise à niveau du fichier clamd.conf...	**Fermé**	**06/25/2012**	**06/07/2013**
Related to conf-scribe - Anomalie #8104: vérifier le fonctionnement de l'anti...	**Pas un bug**	**05/05/2014**	**05/16/2014**

Associated revisions

Revision d53669c2 - 04/30/2014 09:20 AM - Emmanuel GARETTE

ne pas proposer l'option clam_scan_mail (de eole-antirus) si exim_clamav est à oui (ref #8102 @1h)

Revision ee4682f0 - 04/30/2014 09:23 AM - Emmanuel GARETTE

si exim_clamav existe et est à oui, forcer l'option ScanMail (fixes #8102)

History

#1 - 04/29/2014 04:48 PM - Emmanuel GARETTE

- File test.txt added

#2 - 04/29/2014 05:05 PM - Emmanuel GARETTE

Ajout du test SCRIBE-T03-001 test 4

#3 - 04/29/2014 05:35 PM - Daniel Dehennin

- Project changed from eole-exim to eole-antivirus

Le problème vient de la configuration de clamav.

Par défaut, clamav est configuré pour ne pas prendre en compte les fichiers de type mail sauf à changer la variable **clam_scan_mail** (eole-antivirus:source:tmpl/clamd.conf@cdaac368#L234)

Exim interagit avec clamd de la façon suivante :

```
Tue Apr 29 17:26:25 2014 -> Received POLLIN|POLLHUP on fd 4
Tue Apr 29 17:26:25 2014 -> Got new connection, FD 9
Tue Apr 29 17:26:25 2014 -> Received POLLIN|POLLHUP on fd 5
Tue Apr 29 17:26:25 2014 -> fds_poll_recv: timeout after 5 seconds
Tue Apr 29 17:26:25 2014 -> Received POLLIN|POLLHUP on fd 9
Tue Apr 29 17:26:25 2014 -> got command SCAN /var/spool/exim4/scan/1Wf9vF-0008Gz-DQ/1Wf9vF-0008Gz-DQ.eml (64,
5), argument: /var/spool/exim4/scan/1Wf9vF-0008Gz-DQ/1Wf9vF-0008Gz-DQ.eml
Tue Apr 29 17:26:25 2014 -> mode -> MODE_WAITREPLY
Tue Apr 29 17:26:25 2014 -> Breaking command loop, mode is no longer MODE_COMMAND
Tue Apr 29 17:26:25 2014 -> Consumed entire command
Tue Apr 29 17:26:25 2014 -> Number of file descriptors polled: 1 fds
Tue Apr 29 17:26:25 2014 -> fds_poll_recv: timeout after 600 seconds
Tue Apr 29 17:26:25 2014 -> THRMGR: queue (single) crossed low threshold -> signaling
Tue Apr 29 17:26:25 2014 -> THRMGR: queue (bulk) crossed low threshold -> signaling
Tue Apr 29 17:26:25 2014 -> Finished scanthread
Tue Apr 29 17:26:25 2014 -> Scanthread: connection shut down (FD 9)
Tue Apr 29 17:26:25 2014 -> THRMGR: queue (single) crossed low threshold -> signaling
Tue Apr 29 17:26:25 2014 -> THRMGR: queue (bulk) crossed low threshold -> signaling
```

Exim écrit donc le mail sur le système de fichier et demande à clamd de le scanner.

Il faudrait donc que la variable **clamd_scan_mail** change en fonction de la valeur de **exim_clamav**.

#4 - 04/30/2014 09:23 AM - Emmanuel GARETTE

- Status changed from Nouveau to Résolu

- % Done changed from 0 to 100

Appliqué par commit ee4682f0d495914ca5f6c9a854a42f683ab3a5dd.

#5 - 04/30/2014 11:09 AM - Philippe Caseiro

Ok sur un scribe 2.4.0 stable.

Le webmail nous renvois l'erreur : Erreur SMTP: [550] This message contains malware (Eicar-Test-Signature)

#6 - 04/30/2014 11:09 AM - Philippe Caseiro

- Status changed from Résolu to Fermé

#7 - 05/07/2014 09:24 AM - Daniel Dehennin

- Assigned To set to Emmanuel GARETTE

Files

test.txt	69 Bytes	04/29/2014	Emmanuel GARETTE