Installation de Samba-Vscan avec l'antivirus libre CLAMAV

Samba-Vscan

Site où récupérer tout ce qu'il faut :
http://sourceforge.net/projects/openantivirus/

- Récupérer sur SourceForge la dernière version de samba-vscan

- **bunzip2** samba-vscan-0.3.4.tar.bz2

- **tar -xf** samba-vscan-0.3.4.tar

- L'installation nécessite les sources de samba et particulièrement le fichier : config.h (une fois le "configure" lancé dans les sources de samba)

- Copier (ça n'est pas obligatoire, voir plus bas) tout le répertoire obtenu dans /usr/local/src/samba-3.0.0/examples/VFS/
  On a donc **/usr/local/src/samba-3.0.0/examples/VFS/samba-vscan-0.3.4**

- Sous ce répertoire, lancer **./configure**

- Si le répertoire samba-vscan-0.3.4 n'a pas été copié dans /usr/local/src/samba-3.0.0/examples/VFS/, il faut rajouter l'option suivante : **./configure --with-samba-source=/usr/local/src/samba/source.**

- Lancer make
  Samba-vscan est livré avec plusieurs modules permettant d'utiliser différents moteurs anti-virus (f-prot; sophos....clamav)

Le choix se portera sur ClamAv (libre)
  Lancer make tout seul permet de compiler tous les modules, ici, seul le module pour ClamAv nous intéresse :
  make clamav pour ne compiler que le module clamav

- Un **make install** copiera tous les modules compilés dans /usr/local/samba/lib/vfs

le make install ne copie pas les fichiers de conf de chaque module, il faut les copier à la main dans /usr/local/samba/lib (par exemple).

On reparle de ce fichier de configuration un peu plus bas (il s'agit du fichier de configuration du module de vscan pour le moteur ClamAv)

- Le **smb.conf** ressemblera à ça :
  vfs object = vscan-clamav
  vscan-clamav: config-file = /usr/local/samba/lib/vscan-clamav.conf

Dans la doc ils mettent : vfs object = vscan-clamav.so.....ça ne marche pas, il ne faut pas mettre l'extension.

On fait le point :
- Le fichier vscan-clamav.so doit être dans /usr/local/samba/lib/vfs
- Le fichier vscan-clamav.conf doit être dans /usr/local/samba/lib
- Le smb.conf contient les bonnes lignes

ClamaV

Récupérer les sources sur le site qui va bien

Le moteur
http://prdownloads.sourceforge.net/clamav/clamav-0.60.tar.gz

Les derniers fichiers de signatures
http://clamav.sourceforge.net/database/viruses.db
http://clamav.sourceforge.net/database/viruses.db2.gz

Installation du moteur

- Créer un **utilisateur clamav** appartenant au **group clamav** (c'est important dixit la doc)

- Créer un répertoire /home/clam_40 pour mettre en quarantaine les fichiers contenant un virus (du moins c'est ce que j'ai fait) appartenant à "clamav".

- **Tar** -xzf clamav-0.60.tar.gz

- Le triplé gagnant : **./configure** puis **make** puis **make install**

- Par défaut, tout sera installé dans /usr/local/bin; /usr/local/man; /usr/local/etc; /usr/local/include; /usr/local/lib; /usr/local/ ..

- Le fichier de configuration de l'anti-virus clamav se trouve dans /usr/local/etc **(clamav.conf)**

- Le daemon de clamav se trouve dans /usr/local/sbin **(clamd)**

- Les deux fichiers de signatures se trouvent dans /usr/local/share/clamav **(virus.db; virus.db2)**
C'est ici que l'on copie les deux fichiers de signatures téléchargées précédemment

- Concernant le fichier de configuration, la seule manip effectuée pour l'instant est de commenter la ligne 8 "Example".

- Le socket se trouve par défaut dans /tmp

- Modification du fichier de configuration du module clamav (modifs basiques effectuées)
vscan-clamav.conf (on ne touche pas pour l'instant à clamav.conf)

```
; where to put infected files - you really want to change this!
; it has to be on the same physical device as the share!
  quarantine directory  = /home/clam_40
; prefix for files in quarantine
  quarantine prefix = vir-

; socket name of clamd (default: /var/run/clamd)
  clamd socket name = /tmp/clamd
```

Petit script (qui mange pas de pain) pour le démarrage de clamd, (peut être mis dans /etc/rc.d/init.d/

```
#!/bin/sh
#
#Demarrage du socket clamav.
#
# Source function library.
. /etc/rc.d/init.d/functions

case "$1" in
  start)
        echo -n "Starting clamd "
        /usr/local/sbin/clamd
        echo
        ;;
  stop)
        echo -n "Shutting clamd "
        killproc clamd
        echo
        ;;
  status)
        status clamd
        echo
        ;;
  restart|reload)
        $0 stop
        $0 start
        ;;
  *)
        echo "Usage: clamav {start|stop|status|restart}"
        exit 1
esac
```

Tests

J'ai effectué les tests avec le fichier eicar.com, qui est un fichier test pour les anti-virus

http://www.eicar.org/download/eicar.com.txt

Il faut juste supprimer l'extension txt, il sera ensuite détecté par clamav.
Un petit tail –n 1 – f /var/log/messages permet de voir tout ce qui se passe en temps réel.