Mettre en place un anti-virus sur son serveur de mail

Baptiste SIMON (aka BeTa)

e-glop.net

Vous apprendrez dans ce document comment mettre en place un filtrage de vos mails par un antivirus. Ce guide (howto) explique la marche à suivre pour postfix (le serveur SMTP), amavisd-new (le lien) et clamav (l'antivirus à proprement parler).

1. Introduisons les concepts

Afin de mieux vous faire comprendre la façon dont fonctionnera votre système de messagerie, nous allons décrire le cheminement d'un mail au sein de celui-ci :

Un hote distant se connecte sur votre SMTP local. Celui-ci effectue son travail de premiers filtrages (vérifier si la boîte aux lettres existe, si l'hôte distant répond bien aux normes que l'on a définies, etc...). Si le message passe les tests, il est "envoyé" à amavisd-new.

amavisd-new reçoit le message, effectue un premier filtrage succint et "contacte" clamav.

clamav étudie le mail de manière à détecter du code suspicieux, décompresse au besoin les archives jointes... en somme, effectue toutes les actions permettant de qualifier un antivirus d'antivirus.

2. Passons aux choses sérieuses

2.1. Installation des logiciels

Comme nous l'avons dis dans le résumé de l'article, nous considérons que vous utilisez déjà un postfix fonctionnel et maîtrisé.

2.1.1. Pré-requis Debian woody

Préparation de la distribution

```
# cat >> /etc/apt/sources.list <<EOF
deb http://people.debian.org/~hmh/woody/ hmh/amavisd-new/
```

```
deb http://people.debian.org/~hmh/woody/ hmh/misc/
EOF
# apt-get update
```

2.1.2. Amavisd-new

L'installation de amavisd-new ne pose désormais plus de problème. Tout se passe comme avec n'importe quel paquet

```
# apt-get install amavisd-new
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
  amavisd-new
0 packages upgraded, 1 newly installed, 0 to remove and 5  not upgraded.
Need to get 0B/601kB of archives. After unpacking 1929kB will be used.
Do you want to continue? [Y/n] y
Preconfiguring packages ...
```

2.1.3. clamav

De la même manière que amavisd-new, autant avant l'ajout de nouvelles sources clamav était introuvable avec un apt-cache search, autant maintenant il vous suffit de taper les commandes suivantes pour l'installer tout simplement

```
# apt-get install clamav-daemon clamav-testfiles
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  clamav clamav-freshclam libclamav1
The following NEW packages will be installed:
  amavisd-new clamav clamav-daemon clamav-freshclam clamav-testfiles libclamav1
0 packages upgraded, 5 newly installed, 0 to remove and 5  not upgraded.
Need to get 0B/601kB of archives. After unpacking 1929kB will be used.
Do you want to continue? [Y/n] y
Preconfiguring packages ...
```

2.2. Configurations diverses

2.2.1. Postfix

Les deux fichiers de configuration main.cf et master.cf sont à mettre à jour de la manière suivante

```
# cat >> /etc/postfix/main.cf <<EOF

#
# Mail virus filtering
```

```
#
content_filter = smtp-amavis:[127.0.0.1]:10024
EOF
[enter]
# cat >> /etc/postfix/master.cf <<EOF

#
# Amavisd-new
#
smtp-amavis unix - - y - 2 smtp
    -o smtp_data_done_timeout=1200
    -o disable_dns_lookups=yes

127.0.0.1:10025 inet n - n - - smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o smtpd_helo_restrictions=
    -o smtpd_client_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o mynetworks=127.0.0.0/8
EOF
[enter]
#
```

N'hésitez pas à remplacer *[127.0.0.1]:10024* par des paramètres différents au besoin. A vos risques et périls.

2.2.2. Amavisd-new

Nous n'avons aucune méthode empirique à vous proposer... Éditez *simplement* le fichier /etc/amavis/amavisd.conf et parcourez le en quête d'une option à modifier.

2.2.3. Clamav

Le fichier de configuration de clamav est relativement explicite. Je vous invite à modifier directement les option que vous trouverez ci-dessous en fonction de vos besoins et de votre distribution

```
# cat > /etc/clamav.conf <<EOF
ScanMail
ScanArchive
StreamSaveToDisk
StreamMaxLength 1000M
ArchiveMaxRecursion 5
ArchiveMaxFiles 1000
ArchiveMaxFileSize 20M
ThreadTimeout 180
MaxThreads 5
MaxConnectionQueueLength 15
LogSyslog
PidFile /var/run/clamd.pid
DataDirectory /var/lib/clamav/
SelfCheck 3600
```

À noter que sous Debian, l'outil de configuration "assisté" est de très bonne facture. Pour l'utiliser, il suffit de taper la commande

```
# dpkg-reconfigure clamav-daemon
```

nb: clamav-daemon doit aussi pouvoir être capable d'être utilisé en tant qu'antivirus de systèmes de fichiers (par exemple pour des partages SaMBa).

3. Conclusion

Pour être sûrs que tout c'est bien passé lors de la configuration de nos services, redémarrons les tous

```
# /etc/init.d/postfix restart
Stopping mail transport agent: Postfix.
Starting mail transport agent: Postfix.

# /etc/init.d/amavis restart
Stopping amavisd: amavisd-new.
Waiting for complete shutdown...
Starting amavisd: amavisd-new.

# /etc/init.d/clamav-daemon restart
Restarting clam daemon: clamd.
```

Voilà, votre système de messagerie embarque maintenant un scanner de virus pour mails. Rien de tel pour rassurer un décideur pressé... sous Windows(tm).

Si vous constatez une quelconque erreur, si vous souhaitez améliorer certains passages, certains points, n'hésitez pas à me contacter par mail (mailto:beta@e-glop.net) pour me soumettre vos "patches" ou vos remarques. De même, si vous vous sentez capable d'écrire un tutoriel de ce genre sous licence Libre, pour la mise en place d'un antivirus de systèmes de fichiers... ;c)

4. Annexes

4.1. L'auteur

Baptiste SIMON (http://doc.gentoofr.org/Members/BeTa) <baptiste.simon@e-glop.net (mailto:baptiste.simon@e-glop.net)>

Administrateur système GNU/Linux

Responsable de la section "Intégration" chez Code Lutin (http://www.codelutin.com/)

Toujours *à la recherche d'aventures*, dans le cadre de son emploi en cours ;c)

4.2. Aperçu des divers formats de ce document

Ce document a été rédigé au format RST (http://docutils.sourceforge.net/) avec KWrite puis converti aux formats DN-XML et Docbook avec dn2dbk.xsl (http://membres.lycos.fr/ebellot/dn2dbk/).

Les versions XHTML, HTML et XSL-FO a été réalisée avec les feuilles XSLT officielles de docbook [1]. Les version PDF, postscript, RTF et texte ont été créées grâce à Jade (http://openjade.sourceforge.net).

Retrouvez toutes ces version ici :

- XHTML (antivirus-mail.xhtml)
- HTML (antivirus-mail.html)
- PDF (antivirus-mail.pdf)
- postcript (antivirus-mail.ps)
- Texte brut (antivirus-mail.txt)
- RTF (antivirus-mail.rtf)
- reStructuredText (antivirus-mail.rst)
- DocBook - XML (antivirus-mail.db-xml)
- DN-XML (antivirus-mail.dn-xml)
- XSL-FO (antivirus-mail.fo)

4.3. Licence de publication

Notes

1. paquet app-text/docbook-xsl-stylesheets (http://www.oasis-open.org/docbook) sur Gentoo Linux