CLAMAV

- Objet : Clamav, Installation, Utilisation
- Niveau requis :
  débutant, avisé
- Commentaires : *logiciel antivirus pour UNIX*
- Débutant, à savoir : Utiliser GNU/Linux en ligne de commande, tout commence là !
- Suivi :
  à-tester
    - Création par smolski le 02/07/2009
    - Testé par cemoi le 10/02/2018
- Commentaires sur le forum : C'est ici[1)]

Introduction

Quoi? *un anti virus sous Linux?* !
Certains crieront que cela ne sert à rien alors que d'autres soutiendront que nous ne sommes jamais assez prudent...

- Les virus par le détail

Il est totalement faux de croire qu'un antivirus ne se met que sur un dual-boot ou sur un serveur de fichiers.
Personnellement, j'envoie des documents à des clients sous Windows et je ne peux pas me permettre de les contaminer.
Également, il existe des virus sous Linux (si, si !) et même si les dépôts sont tenus par des gens dignes de confiance, nous ne sommes pas à l'abri d'un paquet contenant un virus.

Les avantages de Linux par rapport à Windows sur ce point :

1. Moins connus + politique de liberté du code
2. Un virus ne peut pas s'installer sans l'accord (direct ou indirect) de l'admin du système.

Autrement dit :
Un bon admin sous linux ne prendra jamais de virus, un bon admin sous M$ si !

M'enfin, petite introduction faite, rentrons dans le vif du sujet...voici donc mon petit pense-bête concernant clamav !

Installation

Pour commencer une petite installation[2)]

```
apt-get update && apt-get install clamav
```

Sans plus de soucis...

Mise à jour

La commande pour la mise à jour:

```
freshclam
```

Mais cela donnera:

retour de la commande

```
The following error messages came up:

ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile =
/var/log/clamav/freshclam.log)
```

C'est par ce que le demon fonctionne, il faut donc l'arréter

```
service clamav-freshclam stop
```

Puis de lancer la mise à jour comme précédemment:

```
freshclam
```

retour de la commande

```
ClamAV update process started at Thu Nov 24 17:41:13 2011
main.cvd is up to date (version: 54, sigs: 1044387, f-level: 60,
builder: sven)
connect_error: getsockopt(SO_ERROR): fd=4 error=111: Connection refused
Can't connect to port 80 of host db.local.clamav.net (IP:
195.190.27.134)
Trying host db.local.clamav.net (193.218.105.9)...
Downloading daily-13986.cdiff [100%]
daily.cld updated (version: 13986, sigs: 31881, f-level: 60, builder:
ccordes)
bytecode.cld is up to date (version: 154, sigs: 38, f-level: 60,
builder: edwin)
Database updated (1076306 signatures) from db.local.clamav.net (IP:
193.218.105.9)
```

Votre **clamav** est maintenant à jour et prêt à inspecter les recoins de votre pc pour ne pas contaminer vos amis windowsiens, qui, soit dit en passant, pourront quand même vous remercier de vous soucier de leurs p'tites santés

N'oubliez pas de relancer le demon sans quoi les maj virale ne se feront plus automatiquement!

Pour relancer le demon:

```
service clamav-freshclam start
```

En revanche quand vous voyez ce message d'erreur :

```
      LibClamAV Warning: ************************************************
      LibClamAV Warning: ***  The virus database is older than 7 days.  ***
      LibClamAV Warning: ***        Please update it IMMEDIATELY!       ***
      LibClamAV Warning: ************************************************
```

Ça c'est juste un message qui vous dit que vous n'avez pas la dernière version de clamav

Pourtant il me semblait bien avoir mis à jour clamav avec freshclam o_O'

C'est en faisant quelques recherches que j'ai fait la connaissance de **stable-updates**[3)]

Debian stable-updates

Pour résumer vite fait, stable-updates (*stable* car comme ce sont les mêmes virus, pas la peine d'en faire un pour chaque branche) est un dépôt qui va permettre à clamav, par exemple d'avoir sa base de définition de virus à jour

Voir le tuto des sources.list ici :
Le fichier des sources en détail

- Voir : Les Outils APT pour la gestion des logiciels debian...

Dualboot :
On met un antivirus pour faire une détection de virus sur nos partitions mais aussi sur la partition Ntfs tandis que le système Windows n'est pas actif, et donc si un virus est présent il ne peut pas se déployer et activer un système de défense destiné à le cacher.

Lancements du scan

Scanner le répertoire courant :

```
clamscan
```

Scanner tout le système :

```
clamscan -r /
```

Affichage des fichiers infectés

Scanner un répertoire et ses sous-répertoires en n'affichant que les fichiers infectés :

```
clamscan -r -i /chemin/du/répertoire
```

Se débarrasser ensuite du virus :

```
clamscan --remove /le/chemin/du/fichier/infecté
```

Scanner tout le système et logger :

```
ionice -c3 -n15 nice -n 19 clamscan --infected -r / 2>/dev/null >>
/var/log/clamav/analyse.log
```

On ionice et **nice**
le scan pour éviter de surcharger notre système, sinon les accès disque augmenteront la charge et le processus clamav va “plomber” notre système.
De plus, on affiche que les fichiers infectés !

Automatisation

Le daemon a besoin de tourner pour mettre la base automatiquement à jour :

```
invoke-rc.d clamav-freshclam restart
```

Les fichiers de la base de données de virus sont stockés ici :

```
/var/lib/clamav/daily.cld
/var/lib/clamav/main.cvd
```

Quelques commandes en vrac :

- **Scanner** intégralement sont /home:

```
clamscan -r /home/votre_home
```

- Pour **supprimer** un éventuel fichier infecté:

```
clamscan --remove /le/chemin/du/fichier/infecté
```

- **Biper** sur les virus:

```
clamscan -r --bell /chemin/scan
```

- **Scanner** le disque complet:

```
clamscan -r /
```

Compléments

clamassassin

Adaptateur de filtre de virus dans des courriels pour ClamAV

```
apt-get install clamassassin
```

http://packages.debian.org/search?keywords=clamassassin&searchon=names&suite=stable&section=all

clamsmtp

Mandataire SMTP qui vérifie la présence de virus

```
apt-get install clamsmtp
```

https://packages.debian.org/search?keywords=clamsmtp&searchon=names&suite=stable&section=all

clamtk

Interface graphique pour ClamAV

```
apt-get install clamtk
```

http://packages.debian.org/search?keywords=clamtk&searchon=names&suite=stable&section=all

Liste complète des paquets Clamav

Une liste complète de tous les paquets associés à Clamav ici :

- http://packages.debian.org/search?keywords=Clamav&searchon=all&suite=all&section=all

Liens divers

- Les malwares - Généralités
- Les logiciels malveillants sous Linux

1)

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

2)

Les outils apt

3)

Les dépôts en détail