Généralités

Clam AntiVirus (ClamAV), est un logiciel antivirus très utilisé sous UNIX. Il est généralement utilisé avec les serveurs de courriels pour filtrer les courriers comportant des virus. Les virus ciblés sont très majoritairement des virus s'attaquant au système d'exploitation Microsoft Windows et non pas aux systèmes sur lesquels ClamAV s'installe, qui sont peu menacés par les virus.

Installation

Se rendre sur l'excellent site dag-wieers qui regroupe les paquetages des différentes versions Red Hat : http://dag.wieers.com/rpm/packages.php

Récupérer le rpm de clamd, clamav, clamav-db en fonction de l'architecture du système et la version de la Red Hat. Ex : wget http://dag.wieers.com/rpm/packages/clamav/clamav-……el4.rf.i386.rpm

L'installer avec la commande suivante : rpm –ivh clamav……el4.rpm

Je n'ai pas eu de dépendances à installer avec une installation de base de RHEL4.6. Si il y en a les obtenir sur le même site et les installer avec la même commande avant d'installer le paquetage que l'on désire.

Configuration

Documentation

- Site officiel : http://www.clamav.net/lang-pref/fr/
- Questions concernant les messages dans les logs : http://www.clamav.net/support/faq

Configuration générale

Emplacement	Fonction
/etc/clamd.conf	Fichier de configuration de clamav.
/etc/freshclam.conf	Fichier de configuration de l'utilitaire de mise à jour de clamav nommé freshclam.

`clamd.conf`, voici les directives à modifier.

```
LocalSocket /tmp/clamd.socket # la valeur peut etre différentes (juste
clamd) mais ce n'est pas grave.


AllowSupplementaryGroups no
```

```
ClamukoScanOnAccess yes
ClamukoScanOnExec yes

# ajout des volumes à inclure et exclure. L'adapter en fonction des volumes
du serveur
ClamukoIncludePath /data
ClamukoExcludePath /proc
ClamukoExcludePath /tmp
ClamukoExcludePath /dev
ClamukoExcludePath /var
ClamukoExcludePath /etc
ClamukoExcludePath /usr/local/jakarta-tomcat/temp
ClamukoExcludePath /data/Sites/Logs
```

Redémarrer le service avec un `service clamd restart`. La mise à jour est réalisée via cron tout les jours à l'heure indiquée dans `/etc/crontab` qui est 4h02 du matin. Le fichier qui réalise les mise à jour est `/etc/cron.daily/freshclam`.

Freshclam.conf

```
# configuration proxy
HTTPProxyServer proxy.domaine.local
HTTPProxyPort 8080
HTTPProxyUsername loginproxy
HTTPProxyPassword motdepasse

OnUpdateExecute /bin/touch /var/clamav/UpdateSuccess.lock # creation du
fichier après mise à jour reussie.
```

Mettre les droits sur le fichier `/etc/freshclam.conf` à 700 sinon les mises à jour ne s'effectuent pas.

```
chmod 700 /etc/freshclam.conf
```

On peut lancer les mises à jour en commande et vérifier les éventuelles messages avec un `freshclam –v`.

Si Monit est utilisé, dans `/etc/monit.d/clamav` est réalisé la vérification de la présence du fichier créé lors d'une mise à jour des patterns avec succès (`/var/clamav/UpdateSuccess.lock`).

Au bout d'un moment, monit doit trouver le fichier et mettre le pattern_file à l'état : accessible

Vérifier que clamd est au démarrage avec `chkconfig –list | grep clamd`. C'est le cas par défaut. Si non, le mettre au démarrage du système avec `chkconfig clamd on`. Freshclam n'est pas lancé en tant que daemon. Il n'est donc pas dans la liste des processus lancé. Il est seulement exécuté lors de la mise à jour.