

En cours !

```
su -  
cd /root  
wget http://belnet.dl.sourceforge.net/sourceforge/clamav/clamav-0.70.tar.gz  
tar xvfz clamav-0.70.tar.gz  
cd clamav-0.70  
/usr/sbin/groupadd clamav  
/usr/sbin/useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav  
./configure  
make  
make check  
make install  
cd ..
```

On test :

```
clamscan -r -l scan.txt clamav-0.70  
cat scan.txt  
root@adrien root# cat scan.txt  
Scan started: Sat May 15 16:59:32 2004
```

```
clamav-0.70/test/test1: Clamav-Test-Signature? FOUND  
clamav-0.70/test/test1.bz2: Clamav-Test-Signature? FOUND  
clamav-0.70/test/test2.zip: Clamav-Test-Signature? FOUND  
clamav-0.70/test/test3.rar: Clamav-Test-Signature? FOUND  
clamav-0.70/test/test2.badext: Clamav-Test-Signature? FOUND  
clamav-0.70/contrib/clamdwatc/clamdwatc.tar.gz: Eicar-Test-Signature? FOUND
```

--- summary ---

```
Known viruses: 21075  
Scanned directories: 48  
Scanned files: 514  
Infected files: 6  
Data scanned: 8.64 MB  
I/O buffer size: 131072 bytes  
Time: 7.492 sec (0 m 7 s)
```

Cool, marche :)

```
vi /usr/local/etc/clamav.conf  
Commenter la ligne #Example
```

```
Decommenter:  
LogFile? /var/log/clamav  
LogTime?  
PidFile? /var/run/clamd.pid  
TCPAddr 127.0.0.1
```

StreamSaveToDisk?

On lance le daemon :  
/usr/local/sbin/clamd

Mise a jour auto :

```
touch /var/log/clam-update.log
chmod 600 /var/log/clam-update.log
chown clamav /var/log/clam-update.log
vi /usr/local/etc/freshclam.conf
-> Il faut y trouver la ligne "#UpdateLogFile /var/log/freshclam.log" et la remplacer par "UpdateLogFile
/var/log/clam-update.log" (sans le diese).
```

On lance la mise a jour :

```
$ freshclam
Clamav update process started at Sat May 15 17:06:49 2004
Reading CVD header (main.cvd): OK
Downloading main.cvd *
main.cvd updated (version: 23, sigs: 21096, f-level: 2, builder: ddm)
Reading CVD header (daily.cvd): OK
Downloading daily.cvd *
daily.cvd updated (version: 317, sigs: 461, f-level: 2, builder: ccordes)
Database updated (21557 signatures) from database.clamav.net (212.31.160.239).
```

Il faut appliquer le patch qmail-queue :  
<http://www.qmail.org/qmailqueue-patch>

Il faut installer maildrop :

```
cd /root
wget http://belnet.dl.sourceforge.net/sourceforge/courier/maildrop-1.6.3.tar.bz2
tar xvfj maildrop-1.6.3.tar.bz2
cd maildrop-1.6.3
./configure
make
make install-strip
```

1. make install-man

Installer unzip pour pouvoir scanner les archives :

```
cd /root
wget ftp://ftp.info-zip.org/pub/infozip/UNIX/LINUX/unz550x-glibc.tar.gz
tar xvfz unz550x-glibc.tar.gz
cd unzip-5.50/
cp unzip /bin/
```

Installation de qmail-scanner :

```
cd /root
```

```
wget http://belnet.dl.sourceforge.net/sourceforge/qmail-scanner/qmail-scanner-1.22.tgz
tar xvzf qmail-scanner-1.22.tgz
cd qmail-scanner-1.22
/usr/sbin/groupadd qscand
/usr/sbin/useradd -c "Qmail-Scanner Account" -g qscand -s /bin/false qscand
$ ./configure --install
Entree
Entree
Après avoir lu...
Entree
Entree
```

Si vous avez cette erreur : " perl doesn't have Time::HiRes module – cannot continue.

Get it from CPAN:

<http://search.cpan.org/search?mode=modulehires>"

C'est qu'il manque le module HiRes?.

On va donc l'installer. Si vous ne l'avez pas déjà fait, installez et configurez la gestion des modules perl par CPAN via ce guide : [InstallCpan](#)

Pour installer le module HiRes? il suffit de taper ceci :

```
$ cpan
cpan> install Time::HiRes
cpan> quit
```

Et on recommence l'install :

```
$ ./configure --install
Entree
Entree
Après avoir lu...
Entree
Entree
```

```
$ su qmaild
```

```
qmaild@adrien qmail-scanner-1.20$ /var/qmail/bin/qmail-scanner-queue.pl -g
perlscanner: generate new DB file from /var/spool/qmailscan/quarantine-attachments.txt
perlscanner: total of 9 entries.
On retourne en root :
ctrl+d
```

Test:

```
$ contrib/test_installation.sh -doit
Ce test envoi 4 mails l'administrateur du serveur.
Le 1er n'a pas de virus.
Le 2nd contient le virus eicar
Le 3eme le virus eicar avec un nom modifie
Le dernier est un spam (il passera dans notre cas car nous n'avons pas installes d'anti spam).
```

On verifie les logs de clamav :

```
cat /var/log/clamav
Sat Feb 28 12:48:18 2004 -> /var/spool/qmailscan/tmp/adrien.ovh.net107796889846128025/sneaky.txt:
Eicar-Test-Signature? FOUND
Il nous en a trouve un ;)
```

On ajoute pour qmail :

```
$ vi /etc/tcp.smtp
:allow,QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
```

```
$ /usr/local/bin/tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
```

Les test :

Envoyer un mail sans virus.

Envoyer un mail avec ceci dans un fichier text et en meme temps taper tail -f /var/log/clamav.log :  
X5O!P% @AP[4PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*

Les headers :

Mail normal :

```
Received: from bacto@inter-chat.net by ns2.bacto.net by uid 503 with
qmail-scanner-1.22
(clamscan: 0.70. Clear:RC (interwiki):0(213.186.37.124):.
Processed in 0.236044 secs); 16 May 2004 11:40:12 -0000
```