

0.1 ClamAV

Clamav est pour le moment le seul antivirus libre et gratuit disponible sous linux. Il permet de protéger votre système des virus, troyens et divers malware pouvant nuire. Et conjointement à des plugins ou des configuration particulières, il s'associe aux logiciels de courriels thunderbird, Kmail et Evolution pour filtrer vos messages.

Le bon fonctionnement de l'utilisation des mises à jour des bases de données de signatures virales dépend de la mise à jour des versions du logiciel. Dans les distributions Linux, vous disposez certainement d'une possibilité d'installation de Clamav à partir de votre gestionnaire de paquets. Or, dans la plus part des cas, la versions proposées est périmée et ne vous donnera la meilleure fiabilité lors de l'utilisation des bases de données de signatures virales.

Nous vous recommandons donc d'installer le logiciel à partir de ses sources. Dans tout ce tutoriel, nous allons présenter les manipulations à faire sur une machine Debian Etch. Elles sont très simples et généralisables ou adaptables aux autres distributions.

Nous prendrons le cas simple de la protection d'un poste bureautique classique, qu'il soit branché sur l'internet par l'intermédiaire d'une connection directe ou en réseau ne change rien aux installations et configurations : le logiciel sera configuré de façon à pouvoir scanner ce qui se passe sur le système de fichier monté de la machine, y compris les éventuelles partitions Windows présentes en double boot.

- le site officiel¹
- le téléchargement des sources²

0.1.1 1. Installation

1.1 Dépendances

Vérifiez bien la présence de ces dépendances qui sont indispensables :

- zlib
- zlib-devel
- gcc compiler suite
- bzip2 bzip2-devel
- GNU MP3 : il permet à fresclam de vérifier que les signatures digitales des bases de virus sont à jour.

Si freshclam a été compilé sans GNU MP3 on obtient un message "SECURITY WARNING : NO SUPPORT FOR DIGITAL SIGNATURES3" à chaque update. GNU MP3 est téléchargeable à <http://gmplib.org/>

- check
- Téléchargez les sources à cette adresse : <http://www.clamav.net/download/sources>

Vous allez copier en root cette archive dans le répertoire /usr/src/

```
$su
#cp ~/clamav-x.y.z.tar.gz /usr/src/clamav-x.y.z.tar.gz
```

Puis vous allez extraire l'archive dans ce même dossier ce qui créera un nouveau dossier

```
#tar -xzvf clamav-x.y.z.tar.gz
```

déplacez vous alors dans ce nouveau dossier :

¹<http://www.clamav.net/lang-pref/fr/>

²<http://www.clamav.net/download/sources>

#cd ./clamav-x.y.z

et vérifiez en le contenu :

aclocal.m4
AUTHORS
BUGS
ChangeLog
clamav-config
clamav-config.h
clamav-config.h.in
clamav-config.in
clamav-milter
clamconf
clamd
clamdscan
clamscan
config
config.log
config.status
configure
contrib
configure.in
COPYING
COPYING.BSD
COPYING.bzip2
COPYING.file
COPYING.LGPL
COPYING.lzma
COPYING.unrar
COPYING.zlib
database
docs
etc
examples
FAQ
freshclam
INSTALL
libclamav
libclamav.pc
libclamav.pc.in
libclamunrar
libclamunrar_iface
libtool

```
m4
Makefile
Makefile.am
Makefile.in
NEWS
README
shared
sigtool
stamp-h1
target.h
test
unit_tests
UPGRADE
```

Nous vous recommandons de lire précautionneusement le fichier INSTALL qui donne d'éventuelles particularités d'installation pour la version téléchargée.

1.2 Ajouter d'un nouveau groupe et usager système

Si vous insatallez Clamav pour la première fois il faut ajouter un nouveau groupe et usager.*enroot*)

```
$su
# groupadd clamav
# useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav
```

Ne pas oublier de fermer l'accès au compte.

Le mieux est donc de mettre l'umask à 700 et de restreindre ainsi l'accès à ce compte.

1.3 Nous proposons ici une installation standard.

Le logiciel va être installé dans `/usr/local/`, c'est à dire que la commande se trouvera dans `/usr/local/bin` et les autres fichiers exécutables dans `/usr/local/include`. Les fichiers de configurations seront dans `/usr/local/etc/` (et non pas dans `/etc`).

La première étape est donc de lancer le plus simplement du monde la configuration :

```
./configure
```

En supposant que l'on veuille installer les fichiers de configuration dans `/etc` il faut configurer et construire comme suit :

```
./configure --sysconfdir=/etc
```

Eventuellement contrôle de cette configuration :

```
$make check
```

Puis

```
$make
```

et enfin

```
#make install
```

Le logiciel est installé mais il faut encore le configurer, automatiser son lancement et enfin le faire reconnaître par les logiciels de courriel.

Le daemon est installé dans `/usr/local/sbin/clamd` pour le vérifiez faites :

```
$whereis clamd
```

ce qui donne quelque chose comme :

```
clamd : /usr/src/clamav-0.94.1/clamd /usr/local/sbin/clamd /usr/local/etc/clamd.conf  
/usr/local/etc/clamd.conf~
```

0.1.2 2. Configuration.

Il y a deux fichiers à éditer et à compléter :

- `/usr/local/etc/clamd.conf`
- `/usr/local/etc/freshclam.conf`

Pour plus d'explications détaillées sur chacun de ces fichiers de configuration nous donnons en annexe les traductions en français de ces fichiers exemples livrés lors de l'installation.

Nous indiquons ici ce que nous proposons une configuration standard.

Pour `/usr/local/etc/clamd.conf`

```
LogFile /tmp/clamd.log  
LogFileUnlock yes  
#Chemin à un fichier de socket local sur lequel le  
daemon écoutera.  
#Par défaut il est désactivé mais doit être spécifié  
par l'utilisateur dans #certains cas, notamment  
l'utilisation de plugins de scanner de mail pour  
des #logiciels de courriels.  
LocalSocket /tmp/clamd.socket  
TCPSocket 3310  
StreamMaxLength 20M  
StreamMinPort 30000  
StreamMaxPort 32000
```

```
VirusEvent /usr/local/bin/send_sms 123456789 "VIRUS
  ALERT : %v"
User clamav
AllowSupplementaryGroups yes
DetectPUA yes
AlgorithmicDetection yes
ScanPE yes
ScanELF yes
DetectBrokenExecutables yes
ScanOLE2 yes
ScanPDF yes
ScanMail yes
MailFollowURLs yes
PhishingSignatures yes
PhishingScanURLs yes
ScanHTML yes
ScanArchive yes
ArchiveMaxFileSize 0
ArchiveMaxRecursion 0
ArchiveMaxFiles 0
```

Pour /etc/freshclam.conf

```
DatabaseOwner clamav
AllowSupplementaryGroups yes
DatabaseMirror db.fr.clamav.net
DatabaseMirror database.clamav.net
```

Ces deux exemples montrent que l'on ne change pas grand chose aux valeurs proposées par défaut surtout dans le cas de freshclam.

Le logiciels est configuré et prêt à tourner. mais il n'est pas encore lancé en tant que daemon et nous n'avons pas encore téléchargé les mises à jours antivirales.

Pour le lancer faites(en root) :

```
#clamd
```

Il devrait être lancé.

Pour faire la mise à jour de la base de données de signatures, toujours en root, faites :

```
#freshclam
```

Si vous avez tout installé, surtout en commençant la vérification des dépendances et l'installation de GNU MP3 comme demandé vous devriez voir les messages de recherche puis de téléchargements apparaître sans erreurs.

Test rapide : lancer freshclam en root sans mettre de paramètre et contrôler les sorties. si tout est OK vous avez à créer le fichier journal in /var/log (possédé par clamav ou un autre utilisateur par qui freshclam est lancé :

```
$touch /var/log/freshclam.log
$chmod 600 /var/log/freshclam.log
$chown clamav /var/log/freshclam.log
```

Si vous installez Clamav dans le cas d'une mise à jour du logiciel, il est possible que vous obteniez un message de ce type :

```
clamd : error while loading shared libraries : libclamav.so.5 : cannot open
shared object file : no such file or directory
```

Consultez alors le fichier journal de clamav en général dans /tmp/clamd.log (en root) faites :

```
#cat /tmp/clamd.log
```

puis cherchez quelques chose du type :

```
/usr/local/bin/freshclam : error while loading shared libraries :
libclamav.so.5 : cannot open shared object file : No such file or directory
Stopping clamd : [FAILED]
Starting clamd : /usr/local/sbin/clamd : error while loading shared libra-
ries :
libclamav.so.5 : cannot open shared object file : No such file or directory
[FAILED]
```

Si vous trouvez ces erreurs alors toujours en root faites :

```
#ldconfig
```

Puis relancez clamd avec la commande :

```
#clamd restart
```

0.1.3 3. Lancement automatique au boot de clamd

Il faut mettre un script de lancement dans /etc/init.d ou dans le dossier où sont rangés tous les scripts de lancement de daemon sur votre distribution. Il faut donc vous renseigner sur les particularités de votre distribution en matière de mise à jour des dossiers rc.d.

L'explication que nous donnons ici est la procédure à suivre pour les distribution Debian ou issues de Debian.

Le script que nous proposons est tiré de celui présenté sur cette page extérieur à notre site³.

Créez donc ce fichier en l'appellant par exemple clamavstarter.sh puis en root :

```
#cp ~/clamavstarter.sh /etc/init.d/clamavstarter.sh
#chmod a+x /etc/init.d/clamavstarter.sh
```

Ensuite il faut passer à la mise à jour des fichiers rc.d sous Debian la commande à utiliser est update-rc.d comme suit en root

```
#update-rc.d -f clamavstarter.sh defaults
```

3.1 Le fichier starter de clamav

```
#! /bin/bash
#
# crond Start/Stop the clam antivirus daemon.
#
# chkconfig : 2345 70 41
# description : clamd is a standard Linux/UNIX program
#               that scans for Viruses.
# processname : clamd
# config : /usr/local/etc/clamd.conf
# pidfile : /var/lock/subsys/clamd
# Source function library.
#. /etc/init.d/functions
. /lib/lsb/init-functions
RETVAL=0
TMPDIR=/tmp
export TMPDIR
# See how we were called.
prog="/usr/local/sbin/clamd"
start() {
echo -n "$Starting $prog : "
start-stop-daemon -start -quiet -oknodo -exec $prog
```

³<http://www.funix.org/fr/linux/main-linux.php?ref=filtrermail\&page=menu>

```
RETVAL=$?
echo
[ $RETVAL -eq 0 ] && touch /var/lock/clamd
return $RETVAL
}
stop() {
echo -n $"Stopping $prog : "
# Would be better to send QUIT first, then killproc
  if that fails
start-stop-daemon -stop -quiet -oknodo -exec $prog
RETVAL=$?
echo
[ $RETVAL -eq 0 ] && rm -f /var/lock/clamd
return $RETVAL
}
status() {
clamd status
}
restart() {
stop
start
}
reload() {
echo -n $"Reloading clam daemon configuration : "
start-stop-daemon -stop -quiet -oknodo -exec clamd
  -HUP
retval=$?
echo
return $RETVAL
}
case "$1" in
start)
start
;;
stop)
stop
;;
restart)
restart
;;
reload)
reload
```

```
;;
status)
status
;;
condrestart)
[ -f /var/lock/clamd ] && restart || :
;;
*)
echo $"Usage : $0 {start|stop|status|reload|restart|condrestart}"
exit 1
esac
exit $?
#fin du fichier
```

Maintenant, vérifiez que votre configuration est opérationnelle : redémarrez votre machine. Puis, retournez dans une console. Passez en root :

```
$su
```

Puis lancez

```
#clamd status
```

normalement ça doit marcher. Si vous voulez modifier alors votre fichier de configuration (dans une console root faites) :

```
#gedit /usr/local/etc/clamd.conf &
```

faites vos modifications sauvegardez le fichiers. Puis faites toujours dans la même console :

```
#clamd reload
```

0.1.4 4. Utilisation.

4.1 Scanne de dossiers et fichiers.

L'utilisation première de clamav est en ligne de console de façon très simple.

Il faut avoir une bonne connaissance de votre système de fichier.

L'exemple initial est toujours le scanne antivirus de votre dossier d'utilisateur, par exemple /home/user/. Faites un dossier /home/user/virus/ libre en écriture pour l'utilisateur clamav de sorte que clamav puisse y écrire les fichiers infectés et que vous puissiez le consulter en root.

Puis en console faites :

```
$clamscan -r -i --remove=/home/user/virus/ /home/user/
```

Clamav va alors scanner récursivement tous les dossiers et déplacer les fichiers infectés dans le dossier indiqué.

De la même façon, vous pouvez faire régulièrement un contrôle sur le dossier caché de boîte mail de votre logiciel de courriel.

4.2 Scanne en lien avec les logiciels de courriels.

Nous donnerons ici les procédures à suivre pour les logiciels **Kmail** et **Thunderbird**.

[h4]4.2.1 Dans Kmail[/h4]

Il faut aller dans le menu /outils/assistant de gestion des virus

Là vous aurez une fenêtre qui vous permettra de vérifier que **kamail** reconnaît bien **clamav** puis vous aurez à indiquer que faire en cas de détection de virus.

[h4]4.2.2 Pour thunderbird[/h4]

- Il faut installer le plugin **clamrib**.
- Il est disponible en allant le télécharger sur cette page⁴.
- Il faut sur cette page créer un compte d'utilisateur pour pouvoir le télécharger et l'installer.
- Allez dans le menu de thunderbird /outils/modules complémentaires.
- Puis allez sur l'adresse en bas à droite de la petite fenêtre "obtenir des extensions". Cela lance le navigateur et vous tombez sur la page indiquées précédemment.
- Vous cherchez dans vie privée et sécurité l'extension clamrip. vous faites votre compte utilisateur comme demandé. et vous téléchargez : l'installation suit.
- Si tout se passe bien, pour chaque mail sur lequel vous cliquez, doit apparaître en entête la mention "scanne in progress" puis "clean" ou autre si un virus est détecté (pour l'instant ça ne m'est jamais arrivé !).

0.1.5 5. Annexes

5.1 Traduction française de clamd.conf

Cette traduction vous donnera toute les explications concernant les nombreuses options de ce fichier.

```
##  
## Example config file for the Clam AV daemon  
Exemple de fichier de configuration pour le daemon  
clam AV  
## Please read the clamd.conf(5) manual before editing  
this file.
```

⁴<https://addons.mozilla.org/fr/thunderbird/>

```
##veuillez lire le manuel clamd.conf(5) avant d'éditer
ce fichier.
# Comment or remove the line below.
commentez ou effacez la ligne suivante.
#Example
# Uncomment this option to enable logging.
décommentez cette option pour activer le logging.
# LogFile must be writable for the user running daemon.
LogFile doit être libre en écriture pour l'utilisateur
qui lance le daemon.
# A full path is required.
Un chemin complet est requis.
# Default : disabled
LogFile /tmp/clamd.log
# By default the log file is locked for writing -
the lock protects against
# running clamd multiple times (if want to run another
clamd, please
# copy the configuration file, change the LogFile
variable, and run
# the daemon with -config-file option).
Par défaut le log file est fermé en écriture - la
fermeture protège contre le lancement de clamd
un nombre mutiple de fois. (si l'on veut lancer
un autre clamd, il faut copier le fichier de configuration,
changer les variables du LogFile et lancer le daemon
avec l'option -config-file).
# This option disables log file locking.
Cette option désactive la fermeture du log file (fichier
journal)
# Default : no
LogFileUnlock yes
# Maximum size of the log file.
Taille maximum du log file.
# Value of 0 disables the limit.
La valeur 0 désactive la limite.
# You may use 'M' or 'm' for megabytes (1M = 1m =
1048576 bytes)
# and 'K' or 'k' for kilobytes (1K = 1k = 1024 bytes).
To specify the size
# in bytes just don't use modifiers.
Vous devez utiliser 'M' ou 'm' pour megabytes (1M
= 1m = 1048576 bytes) et 'K' ou 'k' pour kilobytes
(1K = 1k = 1024 bytes)
```

Pour spécifier la taille ne pas utiliser seulement de modifications.

```
# Default : 1M
#LogFileMaxSize 2M
# Log time with each message.
Indiquer l'heure avec chaque message.
# Default : no
#LogTime yes
# Also log clean files. Useful in debugging but drastically
  increases the
Aussi Fichiers nettoyés. Pratique dans le cas de debugging
  mais accroît considérablement la taille du fichier
  journal.
# log size.
# Default : no
#LogClean yes
# Use system logger (can work together with LogFile).
Utiliser le logger system (peut fonctionner en même
  temps avec le LogFile).
# Default : no
#LogSyslog yes
# Specify the type of syslog messages - please refer
  to 'man syslog'
# for facility names.
Spécifier le type de message syslog - veuillez vous
  référer à 'man syslog' pour l'usage des noms.
# Default : LOG_LOCAL6
#LogFacility LOG_MAIL
# Enable verbose logging.
Activation du mode verbeux du logging.
# Default : no
#LogVerbose yes
# This option allows you to save a process identifier
  of the listening
# daemon (main thread).
Cette option permet de sauvegarder l'identifiant de
  processus du daemon en écoute (main thread) (fil
  principal)
# Default : disabled
#PidFile /var/run/clamd.pid
# Optional path to the global temporary directory.
Chemin optionel pour le fichier global temporaire.
# Default : system specific (usually /tmp or /var/tmp).
```

Par défaut : spécifique au système (ordinairement /tmp ou /var/tmp).

```
#TemporaryDirectory /var/tmp
```

Path to the database directory.
Chemin vers le dossier de base de donnée.

```
# Default : hardcoded (depends on installation options)
```

Par défaut il est codé dans le logiciel et dépend des options d'installation.

```
#DatabaseDirectory /var/lib/clamav
```

The daemon works in a local OR a network mode. Due to security reasons we
recommend the local mode.

Le daemon travaille dans un mode local ou réseau.
Pour des raisons de sécurité nous recommandons le mode local.

```
# Path to a local socket file the daemon will listen on.
```

Chemin à un fichier de socket local sur lequel le daemon écoutera.

```
# Default : disabled (must be specified by a user)
```

Par défaut il est désactivé mais doit être spécifié par l'utilisateur dans certains cas notamment l'utilisation de plugins de scanner de mail pour des logiciels de courriels.

```
LocalSocket /tmp/clamd.socket
```

Remove stale socket after unclean shutdown.
Effacement du socket usagé après un arrêt incomplet.

```
# Default : yes
```

```
#FixStaleSocket yes
```

TCP port address.
Adresse de port TCP
Indispensable dans le cas de scanne plugins pour logiciels de courriels.

```
# Default : no
```

```
TCPSocket 3310
```

TCP address.
Adresse TCP.

```
# By default we bind to INADDR_ANY, probably not wise.
```

Par défaut nous lions à INADDR_ANY, probablement pas prudent.

```
# Enable the following to provide some degree of protection
```

```
# from the outside world.
```

Activez l'option suivante pour donner quelque degrés de sécurité à l'encontre du monde extérieur.

```
# Default : no
#TCPAddr 127.0.0.1
# Maximum length the queue of pending connections
  may grow to.
Longueur maximum de queue de connection en instance
  à atteindre.
# Default : 15
#MaxConnectionQueueLength 30
# Clamd uses FTP-like protocol to receive data from
  remote clients.
Clamd utilise les protocoles de type FTP pour recevoir
  les données de clients éloignés.
# If you are using clamav-milter to balance load between
  remote clamd daemons
# on firewall servers you may need to tune the options
  below.
Si vous utilisez clamav-milter pour partager les chargements
  entre le daemon clamd éloigné sur un serveur parefeu
  vous devez utiliser les options suivantes.
# Close the connection when the data size limit is
  exceeded.
Fermer la connection quand la taille des données atteint
  une certaine limite.
# The value should match your MTA's limit for a maximum
  attachment size.
La valeur doit rejoindre votre limite de MTA pour
  une taille d'attachement maximum.
# Default : 10M
StreamMaxLength 20M
# Limit port range.
Limite de champ de port.
# Default : 1024
StreamMinPort 30000
# Default : 2048
StreamMaxPort 32000
# Maximum number of threads running at the same time.
Nombre maximum de pistes tournant en même temps.
# Default : 10
#MaxThreads 20
# Waiting for data from a client socket will timeout
  after this time (seconds).
l'attente de données depuis un socket client s'arrêtera
  après une limite en secondes.
# Value of 0 disables the timeout.
```

```
la valeur 0 désactive la limite d'attente.
# Default : 120
#ReadTimeout 300
# Waiting for a new job will timeout after this time
  (seconds).
L'attente pour un nouveau travail s'arrêtera après
  un certain temps en secondes
# Default : 30
#IdleTimeout 60
# Maximum depth directories are scanned at.
Profondeur d'emboîtement maximale de dossiers à scanner.
# Default : 15
#MaxDirectoryRecursion 20
# Follow directory symlinks.
Suivre les liens vers des dossiers.
# Default : no
#FollowDirectorySymlinks yes
# Follow regular file symlinks.
Suivre les liens vers des fichiers réguliers.
# Default : no
#FollowFileSymlinks yes
# Perform a database check.
Faire un contrôle de la base de données.
# Default : 1800 (30 min)
#SelfCheck 600
# Execute a command when virus is found. In the command
  string %v will
# be replaced with the virus name.
Exécuter une commande quand un virus est trouvé. Dans
  le libellé de la commande %v sera remplacé par
  le nom du virus.
# Default : no
VirusEvent /usr/local/bin/send_sms 123456789 "VIRUS
  ALERT : %v"
# Run as another user (clamd must be started by root
  for this option to work)
Lancement en tant qu'autre utilisateur (clamd doit
  être démarré par root pour que cette option fonctionne.).
# Default : don't drop privileges
Par défaut ne laisser tomber les privilèges.
User clamav
# Initialize supplementary group access (clamd must
  be started by root).
```

```
Initier l'accès d'autres groupes (clamd doit être
    lancé par root).
# Default : no
AllowSupplementaryGroups yes
# Stop daemon when libclamav reports out of memory
    condition.
Arrêter le daemon quand libclamav sort des conditions
    de mémoire.
#ExitOnOOM yes
# Don't fork into background.
Ne pas bifurquer dans l'arrière fond.
# Default : no
#Foreground yes
# Enable debug messages in libclamav.
Activer les messages de debuggage dans libclamav.
# Default : no
#Debug yes
# Do not remove temporary files (for debug purposes).
Ne pas effacer les fichiers temporaires pour des raisons
    de debuggage.
# Default : no
#LeaveTemporaryFiles yes
# Detect Possibly Unwanted Applications.
Detecter les applications non désirées éventuelles.
# Default : no
DetectPUA yes
# In some cases (eg. complex malware, exploits in
    graphic files, and others),
# ClamAV uses special algorithms to provide accurate
    detection. This option
# controls the algorithmic detection.
Dans certains cas, par exemple malware complexes,
    exploits dans des fichiers graphiques et autres,
    Clamav utilise des algorithmes speciaux pour donner
    une détection accrue. Cette option contrôle la
    détection algorithme.
# Default : yes
AlgorithmicDetection yes
##
## Executable files
##Fichiers exécutables.
# PE stands for Portable Executable - it's an executable
    file format used
```

```
# in all 32 and 64-bit versions of Windows operating
  systems. This option allows
# ClamAV to perform a deeper analysis of executable
  files and it's also
# required for decompression of popular executable
  packers such as UPX, FSG,
# and Petite.
PE veut dire Exécutables Portables c'est un format
  de fichier exécutable utilisé dans tous les systèmes
  windows 32 et 64 bits. Cette option permet aussi
  à Clamav de faire une analyse plus profonde des
  fichiers exécutables et est aussi requise pour
  la décompression des exécutables enpackageurs communs
  comme UPX FSG et Petite.
# Default : yes
ScanPE yes
# Executable and Linking Format is a standard format
  for UN*X executables.
Exécutable et format liés est un standard pour les
  exécutables un*x.
# This option allows you to control the scanning of
  ELF files.
Cette option permet de contrôler le scannage des fichiers
  ELF.
# Default : yes
ScanELF yes
# With this option clamav will try to detect broken
  executables (both PE and
# ELF) and mark them as Broken.Executable.
Avec cette option clamav essaiera de détecter les exécutables
  cassés (à la fois PE etELF) et les indiquera comme
  exécutables cassés.
# Default : no
DetectBrokenExecutables yes
##
## Documents
##Documents
# This option enables scanning of OLE2 files, such
  as Microsoft Office
# documents and .msi files.
Cette option active le scane des fichiers OLE2 comme
  Microsoft Office et fichiers .msi
# Default : yes
ScanOLE2 yes
```

```
# This option enables scanning within PDF files.
Cette option active le scanne dans les fichiers pdf.
# Default : no
ScanPDF yes
##
## Mail files
##fichiers mails
# Enable internal e-mail scanner.
Active le scanner interne d'email.
# Default : yes
ScanMail yes
# If an email contains URLs ClamAV can download and
  scan them.
# WARNING : This option may open your system to a
  DoS attack.
# Never use it on loaded servers.
Si un email contient une URL clamav peut télécharger
  et la scanner.
Attention : cette option peut ouvrir votre système
  à une attaque dos.
Ne jamais l'utiliser sur un seueur chargé.
# Default : no
MailFollowURLs yes
# Recursion level limit for the mail scanner.
Limite de niveau de récursivité pour le scanner de
  mail.
# Default : 64
#MailMaxRecursion 128
# With this option enabled ClamAV will try to detect
  phishing attempts by using
# signatures.
Avec cette option activée clamav essaiera de détecter
  les atteintes ameçonnage en utilisant des signatures.
# Default : yes
PhishingSignatures yes
# Scan URLs found in mails for phishing attempts using
  heuristics.
Scanner les URL prouvées dans les maisl pour les ameçonnage
  en utilisant les heuristiques.
# Default : yes
PhishingScanURLs yes
# Use phishing detection only for domains listed in
  the .pdb database. It is
```

```
# not recommended to have this option turned off,
  because scanning of all
# domains may lead to many false positives!
Utiliser la détection d'ameçonnage uniquement pour
  les domaines indiqués dans la base de données .pdb.
  Ce n'est pas recommandé d'avoir cette option désactivée
  car scanner tous les domaines peut mener à de nombreuses
  fausses indications d'ameçonnage.
# Default : yes
#PhishingRestrictedScan yes
# Always block SSL mismatches in URLs, even if the
  URL isn't in the database.
# This can lead to false positives.
#Toujours bloquer les mauvaises connections à SSL
  dans les URL même si l'URL n'est pas dans la base
  de donnée.
L'option peut conduire à de fausses détections.
# Default : no
#PhishingAlwaysBlockSSLMismatch no
# Always block cloaked URLs, even if URL isn't in
  database.
# This can lead to false positives.
#Toujours bloquer les URL couvertes même si l'URL
  n'est pas dans la base de données.
L'option peut conduire à de fausses détections.
# Default : no
#PhishingAlwaysBlockCloak no
##
## HTML
##
# Perform HTML normalisation and decryption of MS
  Script Encoder code.
Faire la normalisation HTML et le décryptage des codes
  MS Script Encoder.
# Default : yes
ScanHTML yes
##
## Archives
##
# ClamAV can scan within archives and compressed files.
Clamav peut scanner dans les archives et fichiers
  compressés.
# Default : yes
ScanArchive yes
```

```
# The options below protect your system against Denial
  of Service attacks
#using archive bombs.
Cette option protège votre système contre les attaques
  déni de service en utilisant des bombes archives.
# Files in archives larger than this limit won't be
  scanned.
Les fichiers de plus d'une certaine taille ne seront
  pas scannés.
# Value of 0 disables the limit.
La valeur 0 désactive la limite.
# Default : 10M
ArchiveMaxFileSize 15M
# Nested archives are scanned recursively, e.g. if
  a Zip archive contains a RAR
# file, all files within it will also be scanned.
  This options specifies how
# deeply the process should be continued.
Les archives emboîtées sont scannées récursivement,
  c'est à dire que si une archive zip contient une
  archive rar, tous les fichiers internes seront
  aussi scannés. Cette option spécifie jusqu'à quelle
  profondeur d'emboitement le scanne continue.
# Value of 0 disables the limit.
# Default : 8
ArchiveMaxRecursion 10
# Number of files to be scanned within an archive.
Nombre de fichiers à scanner dans une archive.
# Value of 0 disables the limit.
La valeur 0 désactive la limite.
# Default : 1000
ArchiveMaxFiles 1500
# If a file in an archive is compressed more than
  ArchiveMaxCompressionRatio
# times it will be marked as a virus (Oversized.ArchiveType,
  e.g. Oversized.Zip)
Si un fichier dans une archive est compressé au delà
  d'un certain taux de compression il sera marqué
  comme virus. (Oversized.ArchiveType par exemple
  Oversized.Zip)
# Value of 0 disables the limit.
La valeur 0 désactive la limite.
# Default : 250
ArchiveMaxCompressionRatio 300
```

```
# Use slower but memory efficient decompression algorithm.
# only affects the bzip2 decompressor.
Utiliser le plus lent mais efficace algorithme de
  décompression. Cela n'affecte que la décompression
  bzip2.
# Default : no
#ArchiveLimitMemoryUsage yes
# Mark encrypted archives as viruses (Encrypted.Zip,
  Encrypted.RAR).
Marquer les archives cryptées comme virus (Encrypted.zip
  Encrypted.RAR)
# Default : no
#ArchiveBlockEncrypted no
# Mark archives as viruses (e.g. RAR.ExceededFileSize,
  Zip.ExceededFilesLimit)
# if ArchiveMaxFiles, ArchiveMaxFileSize, or ArchiveMaxRecursion
  limit is
# reached.
Marquer certaines archives comme virus (par exemple
  RAR.ExceededFileSize) si une limite de taille est
  atteinte ArchiveMaxFiles, ArchiveMaxFileSize, ou
  ArchiveMaxRecursion.
# Default : no
#ArchiveBlockMax no
##
## Clamuko settings
Paramétrage de Clamuko.
## WARNING : This is experimental software. It is
  very likely it will hang
## up your system!!!
Attention : c'est un logiciel expérimental. Il est
  très possible qu'il prenne en main votre système!!!
##
# Enable Clamuko. Dazuko (/dev/dazuko) must be configured
  and running.
Activer Clamuko. Dazuko (/dev/dazuko) doit être configuré
  et tourner.
# Default : no
#ClamukoScanOnAccess yes
# Set access mask for Clamuko.
Paramétrage du masque d'accès pour Clamuko.
# Default : no
#ClamukoScanOnOpen yes
#ClamukoScanOnClose yes
```

```
#ClamukoScanOnExec yes
# Set the include paths (all files inside them will
  be scanned). You can have
# multiple ClamukoIncludePath directives but each
  directory must be added
Paramétrer les chemins inclus (tous les fichiers contenus
  dedans seront scannés). Vous pouvez avoir de multiples
  directives ClamukoIncludePath mais chaque dossier
  doit être ajouté dans une ligne séparée.
# Default : disabled
#ClamukoIncludePath /home
#ClamukoIncludePath /students
# Set the exclude paths. All subdirectories are also
  excluded.
Paramétrage des chemins exclus. Tous les sousdossiers
  sont aussi exclus.
# Default : disabled
#ClamukoExcludePath /home/bofh
# Don't scan files larger than ClamukoMaxFileSize
Ne pas scanner les fichiers plus gros que la limite
  ClamukoMaxFileSize
# Value of 0 disables the limit.
La valeur 0 désactive la limite.
# Default : 5M
#ClamukoMaxFileSize 10M
```

5.2 Traduction française de freshclam.conf

Cette traduction vous donnera toute les explications concernant les nombreuses options de ce fichier.

```
##
## Example config file for freshclam
Exemple de fichier de configuration pour fresclam
## Please read the freshclam.conf(5) manual before
  editing this file.
veuillez lire le manuel freshclam.conf(5) avant d'éditer
  ce fichier.
##
# Comment or remove the line below.
Commentez ou effacez la ligne suivante.
#Example
# Path to the database directory.
Chemin vers le dossier de la base de données.
```

```
# WARNING : It must match clamd.conf's directive!  
Attention : cela doit rejoindre les directives de  
    clamd.conf!  
# Default : hardcoded (depends on installation options)  
Par défaut : codé dans le logiciel, dépend des options  
    d'installation.  
# Path to the log file (make sure it has proper permissions)  
Chemin d'accès au fichier journal, vérifiez qu'il  
    ait les permissions requises.  
# Default : disabled  
Par défaut : désactivé.  
#UpdateLogFile /var/log/freshclam.log  
# Maximum size of the log file.  
Taille maximum pour le fichier journal.  
# Value of 0 disables the limit.  
La valeur 0 désactive la limite.  
# You may use 'M' or 'm' for megabytes (1M = 1m =  
    1048576 bytes)  
Vous devez utiliser 'M' ou 'm' pour megabytes (1M  
    = 1m = 1048576 bytes)  
# and 'K' or 'k' for kilobytes (1K = 1k = 1024 bytes).  
et 'K' ou 'k' pour kilobytes (1K = 1k = 1024 bytes).  
# in bytes just don't use modifiers.  
en bytes n'utilisez pas de modificateurs.  
# Default : 1M  
#LogFileMaxSize 2M  
# Log time with each message.  
Indique l'heure de chaque message.  
# Default : no  
#LogTime yes  
# Enable verbose logging.  
Active le mode verbeux de logging.  
# Default : no  
#LogVerbose yes  
# Use system logger (can work together with UpdateLogFile).  
Utilise le logger système (peut fonctionner avec EupdateLogFile).  
# Default : no  
#LogSyslog yes  
# Specify the type of syslog messages - please refer  
    to 'man syslog'  
Spécifie le type de messages syslog - veuillez vous  
    référer à 'man syslog' pour les usages de noms.  
# for facility names.
```

```
# Default : LOG_LOCAL6
#LogFacility LOG_MAIL
# This option allows you to save the process identifier
  of the daemon
Cette option vous permet de sauvegarder l'identificateur
  du processus du daemon.
# Default : disabled
#PidFile /var/run/freshclam.pid
# By default when started freshclam drops privileges
  and switches to the
# "clamav" user. This directive allows you to change
  the database owner.
Par défaut quand freshclam démarre, laisse tomber
  les privilèges et passe sur l'utilisateur "clamav".
# Default : clamav (may depend on installation options)
DatabaseOwner clamav
# Initialize supplementary group access (freshclam
  must be started by root).
Initialise l'autorisation d'accès pour d'autres groupes.
  (freshclam doit être démarré par root.)
# Default : no
AllowSupplementaryGroups yes
# Use DNS to verify virus database version. Freshclam
  uses DNS TXT records
# to verify database and software versions. With this
  directive you can change
# the database verification domain.
Utilise le DNS pour vérifier la version de la base
  de données. Freshclam utilise les enregistrements
  DNS TXT pour vérifier les versions de la base de
  données et du logiciel. Avec cette directive vous
  pouvez changer le domaine de vérification de la
  base de données.
# WARNING : Do not touch it unless you're configuring
  freshclam to use your
# own database verification domain.
Attention : Ne pas modifier cette directive sauf si
  vous configurez freshclam pour utiliser votre propre
  domaine de vérification de la base de données.
# Default : current.cvd.clamav.net
#DNSDatabaseInfo current.cvd.clamav.net
# Uncomment the following line and replace XY with
  your country
# code. See http ://www.iana.org/cctld/cctld-whois.htm
  for the full list.
```

Décommentez les lignes suivantes et remplacez XY avec votre code de pays. Voyez <http://www.iana.org/cctld/cctld-whois.htm> pour avoir la liste complète des codes de pays.

```
#DatabaseMirror db.fr.clamav.net
# database.clamav.net is a round-robin record which
# points to our most
# reliable mirrors. It's used as a fall back in case
# db.XY.clamav.net is
# not working. DO NOT TOUCH the following line unless
# you know what you
# are doing.
database.clamav.net est un point de raliement à tous
# les miroirs liés. Il est utilisé en retour dans
# le cas où db.XY.clamav.net ne fonctionne pas. Ne
# modifiez pas la ligne suivante sauf si vous savez
# vraiment ce que vous faites.
DatabaseMirror database.clamav.net
# How many attempts to make before giving up.
# Combien d'essais à faire avant de changer.
# Default : 3 (per mirror)
#MaxAttempts 5
# With this option you can control scripted updates.
# It's highly recommended
# to keep it enabled.
# Avec cette option vous pouvez contrôler les scripts
# de mise à jour. Il est hautement recommandé de
# conserver cette option activée.
#ScriptedUpdates yes
# Number of database checks per day.
# Nombre de contrôles de la base de données par jours.
# Default : 12 (every two hours)
#Checks 24
# Proxy settings
# paramétrage du proxy
# Default : disabled
#HTTPProxyServer myproxy.com
#HTTPProxyPort 1234
#HTTPProxyUsername myusername
#HTTPProxyPassword mypass
# If your servers are behind a firewall/proxy which
# applies User-Agent
# filtering you can use this option to force the use
# of a different
# User-Agent header.
```

Si votre serveur est derrière un proxy/parefeu qui applique un filtrage suivant les usager-agents vous pouvez utiliser cette option pour forcer l'utilisation d'un autre entête d'utilisateur-agent.

Default : clamav/version_number

#HTTPUserAgent SomeUserAgentIdString

Use aaa.bbb.ccc.ddd as client address for downloading databases. Useful for

multi-homed systems.

Utiliser aaa.bbb.ccc.ddd comme adresse de client pour télécharger la base de données. Utile pour les systèmes multidomicilés.

Default : Use OS'es default outgoing IP address.

Par défaut utilise l'adresse IP de sortie du système d'exploitation.

#LocalIPAddress aaa.bbb.ccc.ddd

Send the RELOAD command to clamd.

Envoie la commande reload à clamd.

Default : no

#NotifyClamd /path/to/clamd.conf

Run command after successful database update.

Lancer une commande après une mise à jours réussie de la base de données.

Default : disabled

#OnUpdateExecute command

Run command when database update process fails.

Lancer une commande quand la mise à jour de la base de données a échoué.

Default : disabled

#OnErrorExecute command

Run command when freshclam reports outdated version.

In the command string %v will be replaced by the new version number.

Lancer une commande quand freshclam renvoie une version périmée.

Default : disabled

#OnOutdatedExecute command

Don't fork into background.

Ne pas bifurquer dans l'arrière fond.

Default : no

#Foreground yes

Enable debug messages in libclamav.

Activation des messages de debuggage dans libclamav.

```
# Default : no
#Debug yes
# Timeout in seconds when connecting to database server.
Limite de temps de connection au serveur de base de
  données.
# Default : 30
#ConnectTimeout 60
# Timeout in seconds when reading from database server.
Limite de temps de connection lors de la lecture depuis
  le serveur de la base de données.
# Default : 30
#ReceiveTimeout 60
```