Disusun oleh wawan bahtiar (a.k.a masterpop3)
Kenapa saya mengangkat judul "menginstall Antivirus Clamav di Redhat" ? karena semua OS yg ada tidak luput dari serangan virus yg ada, apalagi computer anda terhubung langsung ke internet selama 24 jam sehari. Dan kenapa mesti **Clamav** untuk Antivirusnya ?

Karena Clamav termasuk **GPL** anti-virus toolkit untuk linux yang artinya semua orang boleh memakainya gratis tanpa melanggar undang-undang pembajakan Software, virus update yg selalu ditambah setiap hari, dan kelebihan clamav yg lainnya yaitu :

command-line scanner
fast, multi-threaded daemon
milter interface for sendmail
database updater with support for digital signatures
virus scanner C library
on-access scanning (Linux and FreeBSD)
detection of over 20000 viruses, worms and trojans
built-in support for RAR (2.0), Zip, Gzip, Bzip2, Tar, MS OLE2, MS Cabinet files, MS CHM (Compressed HTML), MS SZDD
built-in support for mbox, Maildir and raw mail files
support for built-in support Portable Executable files compressed with UPX, FSG, and Petite

Kenapa mesti install Clamav di Redhat ? Sebenarnya clamav dapat di install selain dari Redhat bisa juga di install di OS yg berbasis :
GNU/Linux
Solaris
FreeBSD
OpenBSD 2
AIX 4.1/4.2/4.3/5.1
HPUX 11.0
SCO UNIX
IRIX 6.5.20f
Mac OS X
BeOS
Cobalt MIPS boxes
Cygwin
Windows Services for Unix 3.5 (Interix)

Penulis memilih Redhat untuk menginstall clamav, karena RedHat OS yg popular dan banyak digunakan oleh orang , jika anda pengguna OS selain RedHat mohon ikuti dan samakan saja prosedurnya.

A. INSTALLASI
Paket-paket Yang dibutuhkan :
Paket2 yg dibutuhkan untuk meng-compile Clamav yaitu :
zlib and zlib-devel packages

gcc compiler suite (both 2.9x and 3.x are supported)

Paket lainnya yg sangat disarankan untuk compile Clamav :
bzip2 and bzip2-devel library
GNU MP 3

Download Paket Clamav :
Untuk Redhat, ambil paket RPM (paket binary/RPM) atau SRPM

Shell> mkdir /download
Shell> cd /download
Shell> wget http://crash.fce.vutbr.cz/crash-hat/2/clamav/clamav-0.80-2.src.rpm

Installasi Clamav :

Compile SRPM clamav :

Shell> rpmbuild -rebuild clamav-0.80-2.src.rpm

Untuk installasi baru paket clamav, coba jalankan perintah di bawah ini :

Shell> rpm -ivh /usr/src/redhat/RPMS/i386/clamav-0.80-1.i386.rpm
Shell> rpm -ivh /usr/src/redhat/RPMS/i386/clamav-devel-0.80-1.i386.rpm
Shell> rpm -ivh /usr/src/redhat/RPMS/i386/clamav-milter-0.80-1.i386.rpm

Jika anda sudah menginstall clamav sebelumnya, maka anda update dengan perintah berikut ini :

Shell> rpm -Uvh -replacepkgs -replacefiles /usr/src/redhat/RPMS/i386/clamav-0.80-1.i386.rpm
Shell> rpm -Uvh -replacepkgs -replacefiles
/usr/src/redhat/RPMS/i386/clamav-devel-0.80-1.i386.rpm
Shell> rpm -Uvh -replacepkgs -replacefiles
/usr/src/redhat/RPMS/i386/clamav-milter-0.80-1.i386.rpm

Tahap installasi sudah selesai, system Redhat anda sudah terpasang system Antivirus Clamav versi 0.8 yg terbaru saat ini (5 November 2004).

B. KONFIGURASI

Clamd
Jika anda ingin menjalankan Clamav sebagai daemon yg hidden di memory, anda harus edit file konfigurasi clamd.conf
Shell> clamd
ERROR: Please edit the example config file /etc/clamd.conf.

Ini menunjukan lokasi file konfigurasi clamd.conf yg belum anda edit untuk keperluan clamav

daemon.

Setting Konfigurasi clamd.conf
Shell> vi /etc/clamd.conf

Di bawah ini adalah konfigurasi yg ada pada computer penulis :

LogFile /var/log/clamav/clamd.log
LogFileMaxSize 0
LogTime
LogSyslog
LogVerbose
PidFile /var/run/clamav/clamd.pid
TemporaryDirectory /tmp
DatabaseDirectory /var/lib/clamav
LocalSocket /var/run/clamav/clamd.sock
FixStaleSocket
MaxConnectionQueueLength 30
MaxThreads 50
ReadTimeout 300
User clamav
AllowSupplementaryGroups
ScanPE
DetectBrokenExecutables
ScanOLE2
ScanMail
ScanHTML
ArchiveMaxCompressionRatio 300
ArchiveBlockEncrypted
ArchiveBlockMax

Running Clamd
Unutuk Redhat sys-V tinggal menjalankan script :
Shell> /sbin/chkconfig -level 2345 clamd on
Shell> /etc/init.d/clamd start

TESTING
Untuk mengetes kemampuan clamav anda yg sudah di install coba jalankan perintah berikut ini :
Shell> clamscan

Contoh :
Shell> clamscan /usr/share/doc/clamav-0.80/test/clam.exe
/usr/share/doc/clamav-0.80/test/clam.exe: OK

---------- SCAN SUMMARY ----------

Known viruses: 26254
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
I/O buffer size: 131072 bytes
Time: 0.505 sec (0 m 0 s)

Ini menunjukan clamav anda sudah bekerja dengan baik. SELAMAT!!!

Freshclam (setting auto Update)
Freshclam adalah program auto update bawaan dari clamav. Freshclam dapat bekerja dalam 2 modus :
interactive - from command line, verbosely
daemon - alone, silently

Setting konfigurasi freshclam.conf
Di bawah ini adalah konfigurasi freshclam.conf dari computer penulis :

DatabaseDirectory /var/lib/clamav
UpdateLogFile /var/log/clamav/freshclam.log
LogVerbose
PidFile /var/run/clamav/freshclam.pid
DatabaseOwner clamav
DNSDatabaseInfo current.cvd.clamav.net
DatabaseMirror database.clamav.net
Checks 1 #--untuk check update 1x sehari
NotifyClamd /etc/clamd.conf

Running freshclam
Anda dapat menjadwalkan untuk update berkala dengan menjalankan script-V di redhat :

Shell> /sbin/chkconfig -level 2345 freshclam on
Shell> /etc/init.d/freshclam start

Online Access Scanner

Jika anda ingin system RedHat anda terlindung dari serangan virus yg masuk lewat hardisk anda maka anda harus melakukan perubahan di clamd.conf dan freshclam.conf.

Freshclam.conf
DatabaseOwner root ##sebelumnya ## DatabaseOwner clamav

Clamd.conf
User root ##sebelumnya ## User clamav
ClamukoScanOnAccess

ClamukoScanOnOpen
ClamukoScanOnClose
ClamukoScanOnExec
ClamukoIncludePath /
ClamukoExcludePath /dev
ClamukoExcludePath /proc
ClamukoMaxFileSize 10M

Sebelumnya anda edit startup clamd dan install dan compile dazuko.
Shell> vi /etc/init.d/clamd
...
...
start() {
echo -n $"Starting Clam AV daemon: "
/sbin/insmod dazuko ##Tambahkan baris ini, sebelumnya tidak ada
daemon /usr/sbin/clamd
RETVAL=$?
echo
[$RETVAL -eq 0] && touch /var/lock/subsys/clamd
return $RETVAL
}
stop() {
echo -n $"Stopping Clam AV daemon: "
killproc clamd
RETVAL=$?
/sbin/rmmod dazuko ##Tambahkan baris ini, sebelumnya tidak ada
echo
[$RETVAL -eq 0] && rm -f /var/run/clamav/clamd.pid /var/lock/subsys/clamd
return $RETVAL
}
...
...

Compile dan Install Dazuko
Shell> cd /download
Shell> wget http://dazuko.org/files/dazuko-2.0.4.tar.gz
Shell> tar xzf dazuko-2.0.4.tar.gz
Shell> cd dazuko-2.0.4
Shell> ./configure
Shell> make
Shell> /sbin/insmod dazuko.o
Shell> mknod -m 600 /dev/dazuko c 254 0
Shell> chown root:root /dev/dazuko
Shell> cp dazuko.o /lib/modules/2.4.18-14/kernel/lib/
Shell> /sbin/rmmod dazuko

Restart Clamd & freshclam

Shell> /etc/init.d/clamd restart
Shell> /etc/init.d/freshclam restart

HEBAT SUDAH SYSTEM KEKEBALAN SUDAH TERINSTALL DI SYSTEM REDHAT ANDA. SELAMAT MENIKMATI..sementara FAQ nya belum dibuat nih...

wawan.bahtiar