Qmail−Scanner and ClamAV HowTo

Steve Peace

Gregory L. Porter −

version 1.0 Edition

Edited by

Todd Hawley

09/19/2004

Revision History

Revision 1.0	09/19/2004	Revised by: glp
Initial Release, reviewed by TLDP		
Revision 0.9	08/01/2004	Revised by: glp
Converted to DocBook		
Revision 0.4	07/01/2004	Revised by: srp
First public draft in html		

This HOWTO describes how to integrate ClamAV, an anti−virus attachment scanner and Qmail−Scanner, an anti−virus message content scanner, with an existing installation of a qmail email server.

Table of Contents

Table of Contents

Chapter 1. Introduction

1.1. What This Document Is:

This document started out as a way for me to document the procedure and required readings for re−creating the deployment of Qmail−Scanner and ClamAV for my employer's email system. I am not a writer, or a programmer. I am a lowly little systems administrator that got frustrated looking online for all of the information to make Qmail−Scanner work with ClamAV. This HOWTO will document the steps that I took to get Qmail−Scanner and ClamAV to work together. Is this the right way to do it? Who knows, it worked for me. There are plenty of snippets of information that I *"liberated"* from many sources. Please see the Acknowledgments. The most current version of this document can be found at *http://stevepeace.no−ip.org*.

1.2. What This Document Is Not:

This document is not a comprehensive source of information for ClamAV, Qmail−Scanner, qmail, daemontools, Linux, Un*x, FreeBSD, Perl, etc. I do not pretend to know everything about everything. Like I said before, this worked for me it may not work for you. If you don't know how to use a particular OS, tool, or piece of software, THIS HOWTO WILL NOT HELP YOU! I am a firm believer in RTFM. So please make sure that you check out Appendix A, and the Disclaimer before following this HOWTO.

1.3. Acknowledgments

I would like to acknowledge the following people and groups:

Jason Haar (for Qmail−Scanner)
Jesse D. Guardiani (original clamd+daemontools HOWTO)
The entire ClamAV group (for ClamAV)
Dan Bernstein (for qmail and daemontools)
Dave Sill (for lfwq)
Bruce Guenter (qmailqueue patch)
Mark Simpson (TNEF unpacker)
Double Precision Inc. (maildrop)
CPAN.org (Perl modules)

1.4. Copyright

warranty; without even the implied warranty of merchantability or fitness for a particular purpose.

1.5. Disclaimer

I disavow any potential liability for the contents of this document. Use of the concepts, examples, and/or any other information or content of this document is entirely at your own risk.

All copyrights are owned by their owners, unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

You are strongly recommended to take a backup of your system before major installation and backups at regular intervals.

1.6. News

The document home page can be found at *http://stevepeace.no−ip.org*. Check here for the most current versions.

Chapter 2. Prerequisites

You should already have a working qmail server with daemontools installed. Your server will also need:

ClamAV Prerequisites:

Zlib and zlib−devel packages
Gcc compiler (2.9x or 3.x)
Bzip2 library (recommended)

Qmail−Scanner Prerequisites:

qmail 1.03
Reformmime from Maildrop 1.3.8+
Perl 5.005_03+
Perl module Time::HiRes
Perl module DB_File
Perl module Sys::Syslog
Mark Simpson's TNEF Unpacker
Bruce Guenter's QMAILQUEUE patch

Chapter 3. ClamAV

3.1. What is ClamAV?

From the ClamAV website:

"Clam AntiVirus is a *GPL* anti−virus toolkit for UNIX. The main purpose of this software is the integration with mail servers (attachment scanning). The package provides a flexible and scalable multi−threaded daemon, a command line scanner, and a tool for automatic updating via Internet. The programs are based on a shared library distributed with the Clam AntiVirus package, which you can use with your own software. Most importantly, the virus database is *kept up to date*."

3.2. Installing ClamAV

Download the ClamAV source at *http://www.clamav.net*. As of the writing of this HOWTO, the latest version is 0.65.

```
#tar −xvzf clamav−0.65.tar.gz
#cd clamav−0.65 #groupadd clamav
#useradd clamav −g clamav −c "Clam AntiVirus" −s /nonexistent .
#/configure
#make
#make install
#cd ..
```

3.3. Testing

As long as make and make install have finished without errors, you are now ready to test your installation (If you did experience errors, please review the ClamAV documentation that was included in the tar ball. You may also try the ClamAV website for some helpful tips). To test your installation type:

```
#clamscan −r −l scan.txt clamav−0.65
```

Clamscan should find a test virus (This is NOT a real virus) in the clamav−0.65/test directory and log it to the scan.txt log file.

Now you need to configure the ClamAV daemon, clamd, for testing.

```
#vi /usr/local/etc/clamav.conf
```

Comment out "Example" line in clamav.conf and save.

```
#clamdscan −l scan.txt clamav−0.65
```

This should provide output that is similar to the clamscan command you entered above.

3.4. Updating Defs

Now we need to update our virus definitions. Clamscan includes a utility, freshclam, to take care of this. Freshclam automatically changes from root to the clamav user that you created during the installation. First, create a log file that freshclam can log to.

```
#touch /var/log/clam-update.log
#chmod 600 /var/log/clamupdate.log
#chown clamav /var/log/clamupdate.log
```

Now start freshclam:

```
#freshclam -d -c 6 -l /var/log/clam-update.log
```

This checks for a new virus definition database six (6) times a day. Check the /var/log/clam−update.log file. It should look something like this:

```
-----------------------------------------------------------------------------------------------------
ClamAV update process started at Wed Jan 28 17:49:48 2004
main.cvd is up to date (version: 19, sigs: 19987, f-level: 1, builder: ddm)
daily.cvd updated (version: 111, sigs: 597, f-level: 1, builder: tomek)
Database updated (20584 signatures) from database.clamav.net (81.4.91.185).
-----------------------------------------------------------------------------------------------------
```

Now add the freshclam −d −c 6 −l /var/log/clam−update.log to your startup scripts.

You can also setup a cronjob to update the Defs every 6 hours, if you like.

```
#vi /etc/crontab
```

```
0 6 * * * root /usr/local/bin/clamscan
```

3.5. Setting up Clamd and Using With Daemontools

Edit /etc/clamd.conf and make the following changes.

```
#vi /etc/clamd.conf
```

Uncomment "LogSyslog"
Uncomment "StreamSaveToDisk"
Uncomment "MaxThreads" and change value to "30"
Uncomment "User" and change value to "qscand"
Uncomment "Foreground"
Uncomment "ScanMail"

Create the clamav directory.

```
#mkdir −p /usr/local/clamav/bin
```

Now create a startup/shutdown script for clamd. Copy and paste the script shown below. This script was written by Jesse D. Guardiani.

```
#vi /usr/local/clamav/bin/clamdctl

#!/bin/sh

# For Red Hat chkconfig
# chkconfig: − 80 30
# description: the ClamAV clamd daemon

PATH=/usr/local/clamav/bin:/bin:/usr/bin:/usr/local/bin:/usr/local/sbin
export PATH

case "$1" in
  start)
    echo "Starting clamd"
    if svok /service/clamd ; then
      svc −u /service/clamd
    else
      echo clamd supervise not running
    fi
    if [ −d /var/lock/subsys ]; then
      touch /var/lock/subsys/clamd
    fi
    ;;
  stop)
    echo "Stopping clamd..."
    echo "  clamd"
    svc −d /service/clamd
    if [ −f /var/lock/subsys/clamd ]; then
      rm /var/lock/subsys/clamd
    fi
    ;;
  stat)
    svstat /service/clamd
    svstat /service/clamd/log
    ;;
  restart)
    echo "Restarting clamd:"
    echo "* Stopping clamd."
    svc −d /service/clamd
    echo "* Sending clamd SIGTERM and restarting."
    svc −t /service/clamd
    echo "* Restarting clamd."
    svc −u /service/clamd
    ;;
  hup)
    echo "Sending HUP signal to clamd."
    svc −h /service/clamd
    ;;
  help)
    cat <<HELP
   stop −− stops clamd service (smtp connections refused, nothing goes out)
  start −− starts clamd service (smtp connection accepted, mail can go out)
   stat −− displays status of clamd service
restart −− stops and restarts the clamd service
    hup −− same as reload
HELP
```

```
    ;;
  *)
    echo "Usage: $0 {start|stop|stat|restart|hup|help}"
    exit 1
    ;;
esac

exit 0
```

Make clamdctl an executable and link to path:

```
#chmod 755 /usr/local/clamav/bin/clamdctl
```

```
#chown clamav /usr/local/clamav/bin/clamdctl
```

```
#ln −s /usr/local/clamav/bin/clamdctl /usr/local/bin
```

Create the supervise directories for the clamd service:

```
#mkdir −p /usr/local/clamav/supervise/clamd/log
```

Now you must create the /usr/local/clamav/supervise/clamd/run file, or just copy and paste the script shown below. This script was also created by Jesse D. Guardiani:

```
vi /usr/local/clamav/supervise/clamd/run

#!/bin/sh
#
# −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
# run
#
# Purpose     − Start the clamd daemon/service.
#
# Author      − Jesse D. Guardiani
# Created     − 09/10/03
# Modified    − 09/25/03
# −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
# This script is designed to be run under DJB's
# daemontools package.
#
#  ChangeLog
#  −−−−−−−−−
#
#  09/25/03 − JDG
#  −−−−−−−−−−−−−−
#  − Changed clamd user to qscand in compliance with
#    the change to qmail−scanner−1.20rc3
#
#  09/10/03 − JDG
#  −−−−−−−−−−−−−−
#  − Created
# −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
# Copyright (C) 2003 WingNET Internet Services
# Contact: Jesse D. Guardiani (jesse at wingnet dot net)
# −−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
```

```
lockfile="/tmp/clamd"   # Location of clamd lock file
path_to_clamd="/usr/local/sbin/clamd"
                        # Location of the clamd binary
BAD_EXIT_CODE=1         # The exit code we use to announce that something bad has happened

# The following pipeline is designed to return the pid of each
# clamd process currently running.
get_clam_pids_pipeline=`ps -ax | grep -E "${path_to_clamd}\$" | grep -v grep | awk '{print $1}'`


# ---------------------------------------------------
# Generic helper functions
# ---------------------------------------------------

# Basic return code error message function
die_rcode() {
        EXIT_CODE=$1
        ERROR_MSG=$2

        if [ $EXIT_CODE -ne '0' ]; then
                echo "$ERROR_MSG" 1>&2
                echo "Exiting!" 1>&2
                exit "$BAD_EXIT_CODE"
        fi
}


# ---------------------------------------------------
# Main
# ---------------------------------------------------

ps_clamd=""
ps_clamd="$get_clam_pids_pipeline"

if [ -n "$ps_clamd" ]; then
        pid_count="0"
        for pid in $ps_clamd
        do
                pid_count=`expr $pid_count + 1`
        done

        die_rcode $BAD_EXIT_CODE "Error: $pid_count clamd process(es) already running!"

fi

if [ -e "$lockfile" ]; then
        rm "$lockfile"
        exit_code="$?"
        die_rcode $exit_code "Error: 'rm $lockfile' call failed."
fi

exec /usr/local/bin/setuidgid qscand $path_to_clamd

# --
# END /usr/local/clamav/supervise/clamd/run file.
# --

Create the /usr/local/clamav/supervise/clamd/log/run file:

#vi /usr/local/clamav/supervise/clamd/log/run
```

```
#!/bin/sh
exec /usr/local/bin/setuidgid qscand /usr/local/bin/multilog t /var/log/clamd
```

Make the run files executable:

```
#chmod 755 /usr/local/clamav/supervise/clamd/run
```

```
#chmod 755 /usr/local/clamav/supervise/clamd/log/run
```

Now set up the log directories:

```
#mkdir −p /var/log/clamd
```

```
chown qscand /var/log/clamd
```

Finally, link the supervise directory into /service:

```
#ln −s /usr/local/clamav/supervise/clamd /service
```

* Note: The clamd script will start automatically shortly after these links are created. If you don't want it running, do the following:

```
#clamdctl stop
```

To start clamd backup, do the following

```
#clamdctl start
```

Chapter 4. Qmail−Scanner

4.1. What Is Qmail−Scanner?

From the Qmail−Scanner website: "Qmail−Scanner is an addon that enables a qmail email server to scan all gateway−ed email for certain characteristics (i.e. a content scanner). It is typically used for its anti−virus protection functions, in which case it is used in conjunction with commercial virus scanners, but also enables a site (at a server/site level) to react to email that contains specific strings in particular headers, or particular attachment filenames or types (e.g. *.VBS attachments). It also can be used as an archiving tool for auditing or backup purposes. Qmail−Scanner is integrated into the mail server at a lower level than some other Unix−based virus scanners, resulting in better performance. It is capable of scanning not only locally sent/received email, but also email that crosses the server in a relay capacity."

4.2. Installing Qmail−Scanner Prerequisites

4.2.1. Maildrop

What is Maildrop:

From the maildrop web site:

"*maildrop* is the mail filter/mail delivery agent that's used by the *Courier Mail Server*."

You will not be using Maildrop or the Courier Mail Server for this installation. However, Qmail−Scanner requires reformmime, which is included in Maildrop. This is the only reason Maildrop is mentioned in this HOWTO.

Download and unpack the latest version of Maildrop. Please read the INSTALL file included in the tar ball.

```
#./configure
```

```
#make
```

```
#make install−strip
```

```
#make install−man
```

4.2.2. Perl Modules

Time::HiRes Perl module:

From the README file in the tar ball:

Time::HiRes module: High resolution time, sleep, and alarm. "Implement usleep, ualarm, and gettimeofday for Perl, as well as wrappers to implement time, sleep, and alarm that know about non−integral seconds."

DB_File Perl module:

From the README file in the tar ball:

"DB_File is a module which allows Perl programs to make use of the facilities provided by Berkeley DB version 1. (DB_File can be built version 2, 3 or 4 of Berkeley DB, but it will only support the 1.x features),"

Download Time::HiRes and DB_File Perl Modules. The modules can be obtained at *www.cpan.org* (See Appendix C). There is a HOWTO there as well that will explain the installation procedure of Perl modules. Once again, please read the instructions included in the tar balls and review the README information before installing.

4.2.3. Mark Simpson's TNEF Unpacker

What is TNEF Unpacker:

This utility unpacks ms−tnef type MIME attachments. For a better explanation of MIME type attachments, please review *http://www.ietf.org/rfc/rfc1521.txt?number=1521* .

Download the package, and uncompress the tar ball. As with the Maildrop install, you should read the INSTALL file included in the tar ball.

```
#./configure
```

```
#./make check
```

```
#./make install
```

4.2.4. Patching qmail

If you have not already done so, please install Bruce Guenter?s QMAILQUEUE patch.

To patch qmail, download the patch to your qmail source directory.

```
#patch −p1<qmailqueue.patch
```

```
#./make setup check
```

4.3. Installing Qmail−Scanner

We are now ready to install Qmail−Scanner. Download the latest source of Qmail−Scanner. As of the writing of this HOWTO, it is 1.20.

Create a user for Qmail−Scanner to run as.

```
#groupadd qscand
```

```
#useradd qscand −g qscand −c "qmail scanner" −s /nonexistent
```

Unpack the tar ball and change to the Qmail−Scanner directory.

```
#tar -zxvf qmail-scanner-1.20.tar.gz
```

```
#cd qmail-scanner-1.20
```

Run Configure to autodetect what software is installed on your system. Review the output to make sure it is correct. It should look similar to this:

```
#./configure

This script will search your system for the virus scanners it knows
about, and will ensure that all external programs
qmail-scanner-queue.pl uses are explicitly pathed for performance
reasons.

It will then generate qmail-scanner-queue.pl - it is up to you to install it
correctly.

Continue? ([Y]/N) <PRESS ENTER>

Found tnef on your system! That means we'll be able to decode stupid
M$ attachments :-)


The following binaries and scanners were found on your system:

mimeunpacker=/usr/local/bin/reformime
unzip=/usr/bin/unzip
tnef=/usr/local/bin/tnef

Content/Virus Scanners installed on your System

clamuko=/usr/local/bin/clamdscan (which means clamscan won't be used as clamdscan is better)

Qmail-Scanner details.

log-details=0
fix-mime=1
debug=1
notify=sender,admin
redundant-scanning=no
virus-admin=root@mail  --substitute you domain here
local-domains='mail' --substitute your domain here
silent-viruses='klez','bugbear','hybris','yaha','braid','nimda','tanatos','sobig','winevar','palyh','fizzer','gibe','
cailont','lovelorn','swen','dumaru','sober','hawaii','holar-i'
scanners="clamuko_scanner"

If that looks correct, I will now generate qmail-scanner-queue.pl
for your system...
Continue? ([Y]/N)<PRESS ENTER>
```

Now type:

```
# ./configure ?install
```

This installs qmail−scanner−queue.pl and creates the necessary directory structures. You should see similar messages as before. Once again, read the output of the script to make sure everything is correct. If it is press

ENTER to install Qmail−scanner.

If qmail has been installed successfully, qmail−scanner−queue.pl should now be installed. You should see qmail−scanner−queue.pl in /var/qmail/bin.

```
#ls /var/qmail/bin
```

```
/var/qmail/bin/qmail-scanner-queue.pl
```

If you do not see qmail−scanner−queue.pl in /var/qmail/bin, then execute the configure script again. Please pay attention to the output of the script and verify that all of the settings are correct. You can also visit the Qmail−scanner mail−archives at *http://lists.sourceforge.net/mailman/listinfo/qmail−scanner−general* .

4.4. Ownership

In order for Qmail−Scanner to be able to use ClamAV, some of the ClamAV ownerships must be changed. If you recall, we made a clamav user to run ClamAV, and then changed the permissions so only the clamav user could run it. Now we need to provide the qscand user privledges to use ClamAV First, change the ownership of the clamd supervise directories.

```
#chown -R qscand /usr/local/clamav/supervise
```

Now change the ownership of the ClamAV log file:

```
#chown -R qscand /var/log/clamd
```

4.5. Testing

Now test Qmail−Scanner:

```
#./contrib./test_instaltion.sh -doit
```

```
Sending standard test message - no viruses...done!
```

```
Sending eicar test virus - should be caught by perlscanner module...
                                done!
```

```
Sending eicar test virus with altered filename - should only be caught
                                by commercial anti-virus modules (if you have any)...
```

```
Sending bad spam message for anti-spam testing - In case you are using
                                SpamAssassin... Done!
```

Now check the e−mail for your postmaster alias account.

You should now have 4 email messages in your postmaster?s mailbox

If you do not have the 4 messages in the postmaster's mailbox, then: Verify that you are checking the proper mailbox.

Re−execute the configure script for qmail−scanner−queue.pl. Verify that the 'virus−admin' from the script output is the same as your qmail postmaster alias.

Check qmail to see if the messages are in the queue. If they are try issuing a 'qmailctl' flush command to force delivery.

If all else fails check the Qmail−Scanner mailing list archives at *http://lists.sourceforge.net/mailman/listinfo/qmail−scanner−general*.

Chapter 5. Configuring qmail to Use qmail−scanner−queue.pl

5.1. Changing Your Tcp Rules

Once everything is installed, configured, and successfully tested, configure qmail to utilize Qmail−Scanner and ClamAV. If you have followed the instructions found in Dave Sills Life With qmail (see Appendix A: Reading Resources), you should have a tcp.smtp file in your /etc directory. You must edit tcp.smtp file to include the QMAILQUEUE variable.

```
#vi /etc/tcp.smtp

127.:allow,RELAYCLIENT="",QMAILQUEUE="/var/qmail/bin/qmail-queue"
10.:allow,RELAYCLIENT="",QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
:allow.QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
```

As you can see, we use qmail−queue for all local deliveries by setting the QMAILQUEUE variable to be the original qmail−queue. We then changed the local subnet mail deliveries to use qmail−scanner−queue.pl. This causes all local subnet SMTP traffic to be scanned by Qmail−Scanner and ClamAV. The last line of this file scans all inbound emails.

After adding the QMAILQUEUE variables, you must rebuild the cdb file for Qmail.

```
#qmailctl cdb
```

5.2. Increasing Your Softlimit

If you try to send an email message, you will most likely receive an error from your client. The error message will say something that includes this:

```
451 qq temporary problem (#4.3.0)
```

If you followed Life with qmail, you then have a memory limit set in the /var/qmail/supervise/qmail−smtpd/run file. Look for the line that contains softlimit. It should look similar to this:

```
exec /usr/local/bin/softlimit -m 2000000 \
```

This example sets the memory limit for qmail−smtpd to 2M. After all of your changes qmail−smtpd is now running the entire Perl interpreter, and ClamAV. 2M will never be enough.

Each system is different, and has different requirements. It will take some experimenting on your part to find the correct value for your system's softlimit. Do not set softlimit to some high value! You are asking for trouble if you do this. To find the minimal value for your system, I recommend the following steps:

- Increase softlimit by 1M
- #qmailctl restart
- Send a message

* Repeat until you can successfully send an email

Once you have found the minimum, I recommend increasing that by 1.5M, just for times that your email server has a heavy load.

After that just create a daily cronjob that runs /var/qmail/bin/qmail−scan−queue.pl −z to cleanup any dropped SMTP sessions that may be lying around in /var/spool/qmailscan.

Chapter 6. Conclusion

After following the instructions in this HOWTO, now you can feel confident about your email messages being more secure. By implementing Qmail−Scanner and clamav, you have successfully added another layer of security to your email system and overall anti−virus protection. Of course, there is no such thing as 100% secure email messages. Nor will this installation replace sound anti−virus practices, but it should make those practices a little easier to implement and manage.

Appendix A. Recommended Reading and Other Resources

Life with qmail written by Dave Sills *http://www.lifewithqmail.org*

qmail FAQ Written by D.J. Bernstein *http://cr.yp.to/qmail/faq*

SMTP: Simple Mail Transfer Protocol written by Dan Bernstein *http://cr.yp.to/smtp.html*

Daemontools FAQ written by D.J. Bernstein *http://cr.yp.to/daemontools/faq*

ClamAV FAQ *http://www.clamav.net/faq.html#pagestart*

ClamAV User Manual Written by Thomasz Kojm *http://www.clamav.net/doc*

Qmail−Scanner: Content Scanner for qmail written by Jason Haar *http://qmail−scanner.sourceforge.net*

Qmail−Scanner FAQ *http://qmail−scanner.sourceforge.net/FAQ.php*

Clamd+daemontools howto written by Jesse D. Guardiani *http://clamav.elektrapro.com/doc/clamd_supervised/clamd−daemontools−guide.txt*

qmail mailing list archive *http://www−archive.ornl.gov:8000/*

Qmail−Scanner list archive *http://sourceforge.net/mailarchive/forum.php?forum=qmail−scanner−general*

ClamAV users list archive *http://news.gmane.org/gmane.comp.security.virus.clamav.user*

ClamAV Virus DB list archive *http://news.gmane.org/gmane.comp.security.virus.clamav.virusdb*

Maildrop *http://www.flounder.net/~mrsam/maildrop/*

Perl module installation HOWTO *http://www.cpan.org/modules/INSTALL.html*

Mime type RFC *http://www.ietf.org/rfc/rfc1521.txt?number=1521*

Appendix B. Scripts

These are the scripts contained in this HOWTO. They were created by Jesse D. Guardiani, and can be found in his clamd+daemontools HOWTO.

Clamdctl

```
#!/bin/sh

# For Red Hat chkconfig
# chkconfig: - 80 30
# description: the ClamAV clamd daemon

PATH=/usr/local/clamav/bin:/bin:/usr/bin:/usr/local/bin:/usr/local/sbin
export PATH

case "$1" in
  start)
    echo "Starting clamd"
    if svok /service/clamd ; then
      svc -u /service/clamd
    else
      echo clamd supervise not running
    fi
    if [ -d /var/lock/subsys ]; then
      touch /var/lock/subsys/clamd
    fi
    ;;
  stop)
    echo "Stopping clamd..."
    echo "  clamd"
    svc -d /service/clamd
    if [ -f /var/lock/subsys/clamd ]; then
      rm /var/lock/subsys/clamd
    fi
    ;;
  stat)
    svstat /service/clamd
    svstat /service/clamd/log
    ;;
  restart)
    echo "Restarting clamd:"
    echo "* Stopping clamd."
    svc -d /service/clamd
    echo "* Sending clamd SIGTERM and restarting."
    svc -t /service/clamd
    echo "* Restarting clamd."
    svc -u /service/clamd
    ;;
  hup)
    echo "Sending HUP signal to clamd."
    svc -h /service/clamd
    ;;
  help)
    cat <<HELP
   stop -- stops clamd service (smtp connections refused, nothing goes out)
  start -- starts clamd service (smtp connection accepted, mail can go out)
   stat -- displays status of clamd service
restart -- stops and restarts the clamd service
```

```
    hup -- same as reload
HELP
    ;;
  *)
    echo "Usage: $0 {start|stop|stat|restart|hup|help}"
    exit 1
    ;;
esac

exit 0
```

/usr/local/clamav/supervise/clamd/run

```
vi /usr/local/clamav/supervise/clamd/run

#!/bin/sh
#
# ---------------------------------------------------
# run
#
# Purpose     - Start the clamd daemon/service.
#
# Author      - Jesse D. Guardiani
# Created     - 09/10/03
# Modified    - 09/25/03
# ---------------------------------------------------
# This script is designed to be run under DJB's
# daemontools package.
#
#  ChangeLog
#  ---------
#
#  09/25/03 - JDG
#  --------------
#  - Changed clamd user to qscand in compliance with
#    the change to qmail-scanner-1.20rc3
#
#  09/10/03 - JDG
#  --------------
#  - Created
# ---------------------------------------------------
# Copyright (C) 2003 WingNET Internet Services
# Contact: Jesse D. Guardiani (jesse at wingnet dot net)
# ---------------------------------------------------

lockfile="/tmp/clamd"   # Location of clamd lock file
path_to_clamd="/usr/local/sbin/clamd"
                        # Location of the clamd binary
BAD_EXIT_CODE=1         # The exit code we use to announce that something bad has happened

# The following pipeline is designed to return the pid of each
# clamd process currently running.
get_clam_pids_pipeline=`ps -ax | grep -E "${path_to_clamd}\$" | grep -v grep | awk '{print $1}'`


# ---------------------------------------------------
# Generic helper functions
# ---------------------------------------------------

# Basic return code error message function
die_rcode() {
```

```
        EXIT_CODE=$1
        ERROR_MSG=$2

        if [ $EXIT_CODE -ne '0' ]; then
                echo "$ERROR_MSG" 1>&2
                echo "Exiting!" 1>&2
                exit "$BAD_EXIT_CODE"
        fi
}


# ---------------------------------------------------
# Main
# ---------------------------------------------------

ps_clamd=""
ps_clamd="$get_clam_pids_pipeline"

if [ -n "$ps_clamd" ]; then
        pid_count="0"
        for pid in $ps_clamd
        do
                pid_count=`expr $pid_count + 1`
        done

        die_rcode $BAD_EXIT_CODE "Error: $pid_count clamd process(es) already running!"

fi

if [ -e "$lockfile" ]; then
        rm "$lockfile"
        exit_code="$?"
        die_rcode $exit_code "Error: 'rm $lockfile' call failed."
fi

exec /usr/local/bin/setuidgid qscand $path_to_clamd

# --
# END /usr/local/clamav/supervise/clamd/run file.
# --

Create the /usr/local/clamav/supervise/clamd/log/run file:

#vi /usr/local/clamav/supervise/clamd/log/run

#!/bin/sh
exec /usr/local/bin/setuidgid qscand /usr/local/bin/multilog t /var/log/clamd
```

/usr/local/clamav/supervise/clamd/log/run

```
#!/bin/sh
exec /usr/local/bin/setuidgid qscand /usr/local/bin/multilog t /var/log/clamd
```

Appendix C. Software

qmail– *http://www.qmail.org/netqmail−1.05.tar.gz*
Daemontools– *ftp://cr.yp.to/daemontools/daemontools−0.76.tar.gz*
ClamAV– *http://prodownloads.sourceforge.net/clamav/clamav−0.65.tar.gz*
QMAILQUEUE Patch– *http://www.qmail.org/top.html#qmailqueue*
MailDrop– *http://download.sourceforge.net/courier*
Time::HiRes – *http://search.cpan.org/search?module=Time::HiRes*
DB_File– *http://search.cpan.org/search?module=DB_File*
TNEF unpacker– *http://sourcforge.net/projects/tnef*
Qmail−Scanner– *http://prodownloads.sourceforge.net/qmail−scanner/qmail−scanner−1.20.tgz?download*
MIME type RFC– *http://www.ietf.org/rfc/rfc1521.txt?number=1521*

Appendix D. GNU Free Documentation License

Version 1.2, November 2002

D.1. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

D.2. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world−wide, royalty−free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front−matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of

Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front−Cover Texts or Back−Cover Texts, in the notice that says that the Document is released under this License. A Front−Cover Text may be at most 5 words, and a Back−Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine−readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard−conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine−generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

D.3. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

D.4. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front−Cover Texts on the front cover, and Back−Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine−readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer−network location from which the general network−using public has access to download using public−standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

D.5. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

GNU FDL Modification Conditions

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice giving the public permission to use

the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front−matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties−−for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front−Cover Text, and a passage of up to 25 words as a Back−Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front−Cover Text and one of Back−Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

D.6. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

D.7. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

D.8. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

D.9. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

D.10. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

D.11. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

D.12. ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> **Sample Invariant Sections list**
>
> Copyright (c) YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front−Cover Texts, and no Back−Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front−Cover Texts and Back−Cover Texts, replace the "with...Texts." line with this:

> **Sample Invariant Sections list**
>
> with the Invariant Sections being LIST THEIR TITLES, with the Front−Cover Texts being LIST, and with the Back−Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.