amavisd-new / ClamAV / SpamAssassin
a Mac OS X HOWTO

1. - Introduction and Prerequisites

This article covers using amavisd to provide spam and virus controls to Postfix. This method will provide server-wide spam and virus filters for all incoming and outgoing mail. It's a very robust system and can be easily configured to provide a number of different site-specific options for your users. However, combating unwanted e-mail is an ongoing war and not just a single engagement. This article will describe a good beginning to a full-featured mail system, but you should not stop here.

This process works as a content filter for postfix. This means that Postfix will receive the e-mail and then pass it off, using an SMTP connection to port 1024 on the local machine, to amavisd before doing any actual processing of it. Amavisd will then run the mail through ClamAV, for virus detection, and then SpamAssassin, for spam detection. If the e-mail passes both sets of tests amavisd will then return the e-mail to Postfix by using an SMTP connection to port 1025 on the local machine. At this point Postfix will then deliver the mail to the POP/IMAP server that you are using.

If you are using OS X 10.2 you'll need to first upgrade your installation of Perl to 5.8 or higher.

If you don't want to build Perl from source, you can grab an installer from Aron Faby's site at:
http://www.serverlogistics.com/downloads-jag.php#perl.

Also note that if you have Perl support enabled in Apache under Mac OS X Server 10.2.x, you must disable it, as Faby’s Perl 5.8 is not compatible with Apple’s supplied Perl modules.

Download the Perl updater and double-click to install.

Examine the Macintosh.tar.gz tarball included with amavisd-new and ClamAV for updated files and installation instruction, these files will be updated to correspond with it's released version as required.

The files included in the Macintosh tarball provide a way to start the service without logging in as well as a way to manually start, stop and reload the service and include a 'log-rolling' option that is easy to implement.

Setting up the user/group. (10.3.x can use method a or b)

a).

```
% sudo dscl localhost -create /NetInfo/root/Groups/clamav

% sudo dscl localhost -create /NetInfo/root/Groups/clamav gid 30

% sudo dscl localhost -create /NetInfo/root/Users/clamav

% sudo dscl localhost -create /NetInfo/root/Users/clamav uid 30

% sudo dscl localhost -create /NetInfo/root/Users/clamav gid 30

% sudo dscl localhost -create /NetInfo/root/Users/clamav shell /bin/tcsh

% sudo dscl localhost -create /NetInfo/root/Users/clamav home /tmp

% sudo dscl localhost -create /NetInfo/root/Users/clamav passwd "*"
```

b). (10.2.x only)

```
% sudo niutil -create . /groups/clamav

% sudo niutil -createprop . /groups/clamav gid 30

% sudo niutil -create . /users/clamav

% sudo niutil -createprop . /users/clamav uid 30

% sudo niutil -createprop . /users/clamav gid 30

% sudo niutil -createprop . /users/clamav shell /bin/tcsh

% sudo niutil -createprop . /users/clamav home /tmp

% sudo niutil -createprop . /users/clamav passwd "*"
```

Setting up the folders.

```
% sudo mkdir /var/amavis

% sudo mkdir /var/amavis/tmp

% sudo mkdir /var/amavis/db

% sudo chown -R clamav:clamav /var/amavis

% sudo chmod -R 750 /var/amavis

% sudo mkdir /var/virusmails

% sudo chown clamav:clamav /var/virusmails

% sudo chmod 750 /var/virusmails

% sudo touch /var/amavis/whitelist_sender

% sudo mkdir /var/clamav

% sudo chown clamav:clamav /var/clamav

% sudo chmod 0750 /var/clamav

% sudo mkdir /var/log/clamav

% sudo touch /var/log/clamav/clamd.log

% sudo touch /var/log/clamav/freshclam.log

% sudo chmod 0644 /var/log/clamav/clamd.log

% sudo chmod 0644 /var/log/clamav/freshclam.log

% sudo chown clamav /var/log/clamav/clamd.log

% sudo chown clamav /var/log/clamav/freshclam.log
```

2. - Getting the archives

Download amavisd-new, ClamAV, db (BerkeleyDB), gmp.

The official URLs for these libraries are:

amavisd-new
http://www.ijs.si/software/amavisd/
ClamAV
http://sourceforge.net/projects/clamav/
BerkeleyDB
http://www.sleepycat.com/download/db/
gmp
ftp://ftp.gnu.org/gnu/gmp/

You can choose to download either Gzipped (.gz or .tgz extensions) or Bzipped (.bz2 extension) archives, since the latter are smaller. In any case, I advise to locally compute and compare MD5 checksums, if the distribution home lists them. You do that by executing:

```
% md5 <filename>
```

3. - Unpacking the archives

With all archives in the same directory, do:

```
% ls *.gz | xargs -n 1 tar zxvf
```

(I know, xargs is evil). If you downloaded any Bzipped archives, do:

```
% ls *.bz2 | xargs -n 1 tar jxvf
```

(when done it would be helpful to reduce the folder names without the version numbers)

ex.

```
% mv ./clamav-0.80 ./clamav
```

Now for a little cleanup.

```
% sudo rm -r *.gz
```

4. - Building BerkeleyDB

```
% cd ../db/build_unix

% ../dist/configure

% make; sudo make install

% cd ../
```

5. - Building gmp

```
% cd ../gmp

% ./configure --prefix=/usr --mandir=/usr/share/man --sysconfdir=/etc --
enable-devel

% make; sudo make install
```

6. - Building ClamAV

```
% cd ../clamav

% ./configure --prefix=/usr --mandir=/usr/share/man --sysconfdir=/etc

% make; sudo make install
```

Open `/etc/freshclam.conf` and make the following changes.
("Example" is an actual line to be deleted or commented out)

```
# Example

UpdateLogFile /var/log/clamav/freshclam.log

LogVerbose

PidFile /var/clamav/freshclam.pid

DatabaseOwner clamav

DNSDatabaseInfo current.cvd.clamav.net

DatabaseMirror database.clamav.net

MaxAttempts 5

Checks 24
```

Once these changes have been made you can save and close this file.

Open /etc/clamd.conf and make the following changes.
("Example" is an actual line to be deleted or commented out)

```
# Example

LogTime

LogFile /var/log/clamav/clamd.log

LogVerbose

PidFile /var/clamav/clamd.pid

LocalSocket /var/clamav/clamd.sock

MaxThreads 20

SelfCheck 1800

User clamav
```

Once these changes have been made you can save and close this file.

7. - Installing amavisd-new

```
% cd ../amavisd
```

Now we need to get some perl modules installed. CPAN makes this easy, but we will have to force one or two of them to go. I haven't come across any problems with this in testing, but do keep an eye on things. Also, when you are installing these perl modules you may run across dependencies that you don't have installed yet. Please respond in the affirmative when it asks you if you want them installed too.

```
% sudo perl -MCPAN -e shell
```

Now you are in the CPAN system. You will then type in the next four commands which will install the modules. Some of these modules may ask if you want to install the dependencies, say "yes" to this.

```
cpan> install Archive::Tar Archive::Zip BerkeleyDB Compress::Zlib Convert::
UUlib Digest::MD5

cpan> install IO::Stringy Mail::ClamAV Mail::Internet Mail::SpamAssassin
MIME::Base64 MIME::Parser

cpan> install Net::SMTP Net::Server Time::HiRes Unix::Syslog Digest::SHA1

cpan> force install Convert::TNEF Net::SMTP
```

Finally exit out of CPAN.

```
cpan> quit
```

You now need to edit your amavisd config file. This file contains a huge number of options that will pretty much determine your spam and virus policies for your server. You should familiarize yourself with this file so that you get the desired results from this system. It's rather well commented so you shouldn't need to mess with it too much.

In Section I you'll need to change

`$mydomain` to your main e-mail domain.

`$myhostname` to your FQDN.

`$daemon_user` should be set to "`clamav`"

`$daemon_group` should be set to "`clamav`"

`$pid_file` to "`/var/amavis/amavisd.pid`"

`$lock_file` to "`/var/amavis/amavisd.lock`"

Section II and III you can leave alone.

Section IV will require you to make some decisions. This section determines what happens when an e-mail is determined to be a spam or virus e-mail. Here you can specify the notification templates for what your bounce messages say. More importantly you an determine what you'll do with spam and virus e-mails.

The final destiny variables are what you are interested in here. By default amavisd will bounce all spam back to the sender. You may find that this clogs up your mail system attempting to be nice to spammers. If that's the case you can set this to `D_DISCARD` which will effectively delete the mail in question.

You will also want to set your `$virus_admin` and `$spam_admin` settings where the respective notifications will be sent.

The quarantine settings allow you to specify where the spam and virus e-mails will be stored. If you are interested in keeping the e-mails you can direct them to an e-mail address or folder, otherwise you can set these to "undef" which will delete the mails.

Section V sets up white and black lists for amavis. Use these to add in any domains that you know are good or bad.

Section VI you can leave alone.

Section VII is where you specify when e-mail is tagged as spam. The sa_tag levels determine when to quarantine spam mails and when to kill them. Also in this section you'll want to uncomment the clamd section here, which should look something like this:

```
['Clam Antivirus-clamd',
&ask_daemon, ["CONTSCAN {}n", "/var/clamav/clamd.pid"],
qr/bOK$/, qr/bFOUND$/,
qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

Next we need to move the files to their working locations.

```
% sudo cp amavisd.conf /etc/

% sudo chown root /etc/amavisd.conf

% sudo chmod 0644 /etc/amavisd.conf

% sudo cp amavisd /usr/bin/

% sudo chown root /usr/bin/amavisd

% sudo chmod 0755 /usr/bin/amavisd
```

Now we can edit the Postfix files, first you need to add the following lines to `/etc/postfix/main.cf` it will tell Postfix to run amavisd as a content filter before delivery.

```
#
# ==========================================================
# amavis-new/ClamAV
# ==========================================================
#
content_filter=smtp-amavis:[127.0.0.1]:10024
```

Now add the following to /etc/postfix/master.cf:

```
#
# ==========================================================
# amavis-new/ClamAV
# ==========================================================
#
smtp-amavis unix - - y - 2 smtp
-o smtp_data_done_timeout=1200
-o smtp_send_xforward_command=yes
-o disable_dns_lookups=yes
127.0.0.1:10025 inet n - y - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
-o smtpd_error_sleep_time=0
-o smtpd_soft_error_limit=1001
-o smtpd_hard_error_limit=1000
-o receive_override_options=no_header_body_checks
```

8. - Installing the Startup

Move the "AMAVISCLAMAV" folder to "/System/Library/StartupItems/".

```
% sudo mv AMAVISCLAMAV /System/Library/StartupItems/

% sudo chown root:admin /System/Library/StartupItems/AMAVISCLAMAV/*

% sudo chmod 0755 /System/Library/StartupItems/AMAVISCLAMAV/AMAVISCLAMAV
```

Note: You can also place the folder in /Library/StartupItems/

Open /etc/hostconfig with an editor and insert the following line:

```
"AMAVISCLAMAV=-YES-"
```

With the flag set to "-YES-", the service will be enabled at startup.

If you wish to disable auto startup at any time, set "AMAVISCLAMAV=-NO-" in /private/etc/hostconfig and it will disable this service and prevent manually starting it.

With the service enabled, you can start, stop and reload the service manually at any time from terminal with one of the following commands:

```
% sudo SystemStarter start "AMAVISCLAMAV"

% sudo SystemStarter stop "AMAVISCLAMAV"

% sudo SystemStarter restart "AMAVISCLAMAV"
```

A safety has been built in preventing you from starting the service if you have disabled it in the /private/etc/hostconfig file.

9. - (Optional) Installing the Log Rolling

First we move the clamav folder to the periodic folder and create some files.

```
% cd logroll

% sudo touch /var/log/clamav/amavis.log

% sudo chmod 0644 /var/log/clamav/amavis.log

% sudo chown clamav /var/log/clamav/amavis.log

% sudo mv ./clamav /etc/periodic/clamav

% chmod 0755 /etc/periodic/clamav

% chmod 0755 /etc/periodic/clamav/*

% chown root:wheel /etc/periodic/clamav

% chown root:wheel /etc/periodic/clamav/*
```

Using your favorite editor, edit `/etc/crontab` and add the following entry:

```
30   4    *    *    0    root periodic clamav
```

Next, we need to create a link to this file for periodic to access it with.

```
% cd /etc

% sudo ln -s periodic/clamav/500.clamav clamav

% sudotouch /var/log/clamav/amavis.log
```

Make the following changes to `amavisd.conf`:

```
$LOGFILE = "/var/log/clamav/amavis.log";

$DO_SYSLOG = 0; # log via syslogd (preferred)
```

Finally, we need to add our entry into the periodic config file located at `/etc/default/periodic.conf` using your favorite editor.

```
# clamav options
# These options are used by periodic(8) itself to determine what to do
# with the output of the sub-programs that are run, and where to send
# that output.
#
clamav_output="/var/log/clamav.out"  # user or /file
clamav_show_success="YES"   # scripts returning 0
clamav_show_info="YES" # scripts returning 1
clamav_show_badconfig="NO"  # scripts returning 2
```

This step is not required but I like to be able to see my available options so I have also edited `/usr/share/man/man8/periodic.8` and `/usr/share/man/cat8/periodic.8.gz` to include my added routines.

To edit the `periodic.8.gz` you must first unpack it, I recommend you use BBEdit to edit the file since it has an option to show invisible characters and this file is riddled with them.

After you have made your additions to this file, repack it (gz) and place it back in the `/usr/share/man/cat8` folder and your done.

(It will roll the logs once a week and retain the 8 previous weeks of the logs.)

The grand finally is to start the service and restart postfix.

```
% sudo SystemStarter start "AMAVISCLAMAV"

% sudo postfix reload
```