amavisd-new
a Mac OS X HOWTO

1. - Introduction and Prerequisites

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.

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.

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
```

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/

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
```

Now for a little cleanup.

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

4. - Installing amavisd-new with SpamAssassin

```
% 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

$MYHOME to "/var/amavis"

$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"

$pid_file to "$MYHOME/amavisd.pid"

$lock_file to "$MYHOME/amavisd.lock"

$unix_socketname to "$MYHOME/amavisd.sock"

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. For example, if your using clamd (part of ClamAV), you'll want to uncomment the clamd section and change the path to point to the socket file, it should look something like this:

```
['Clam Antivirus-clamd',
&ask_daemon, ["CONTSCAN {}n", "/var/clamav/clamd.sock"],
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 644 /etc/amavisd.conf

% sudo cp amavisd /usr/bin/

% sudo chown root /usr/bin/amavisd

% sudo chmod 755 /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
```

5. - Installing the Startup

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

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

```
% sudo chown root:admin /System/Library/StartupItems/CLAMAV/*
```

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

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

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

```
"AMAVIS=-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 "AMAVIS=-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 "AMAVIS"
```

```
% sudo SystemStarter stop "AMAVIS"
```

```
% sudo SystemStarter restart "AMAVIS"
```

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

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

```
% sudo SystemStarter start "AMAVIS"
```