ClamAV
a Mac OS X HOWTO

1. - Prerequisites

These instruction have been tested with the version it was released with.

Setting up the user/group.

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

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

% sudo niutil -create . /users/mailtransport

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

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

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

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

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

Setting up the folders.

```
% sudo mkdir /var/clamav

% sudo chown mailtransport:mailtransport /var/clamav

% sudo chmod 0750 /var/clamav

% sudo mkdir /var/log/mailtransport

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

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

% sudo chmod -R 0644 /var/log/mailtransport

% sudo chown -R mailtransport /var/log/mailtransport
```

2. - Getting the archives

Download ClamAV, gmp.

The official URLs for these libraries are:

ClamAV
http://sourceforge.net/projects/clamav/
gmp
ftp://ftp.gnu.org/gnu/gmp/

Download the Gzipped (.gz or .tgz extensions)
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
```

(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 gmp

```
% cd gmp
```

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

```
% make; sudo make install
```

5. - 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/mailtransport/freshclam.log

LogVerbose

PidFile /var/clamav/freshclam.pid

DatabaseOwner mailtransport

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/mailtransport/clamd.log

LogVerbose

PidFile /var/clamav/clamd.pid

LocalSocket /var/clamav/clamd.sock

MaxThreads 20

SelfCheck 1800

User mailtransport
```

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

6. - Installing the Startup Item

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

```
% sudo mv CLAMAV /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:

```
"CLAMAV=-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 "CLAMAV=-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 "CLAMAV"

% sudo SystemStarter stop "CLAMAV"

% sudo SystemStarter restart "CLAMAV"
```

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

7. - (Optional) Installing the Log Roll Item

First we move the 'mailtransport' folder to the periodic folder and set it's attributes.

```
% cd logroll

% sudo mv ./mailtransport /etc/periodic/

% chmod -R 0755 /etc/periodic/mailtransport

% chown -R root:wheel /etc/periodic/mailtransport
```

Using your favorite editor, edit /etc/periodic/mailtransport and change the following entry:

```
    SystemStarter restart "MAILTRANSPORT" | head -2;
```

To:

```
    SystemStarter restart "CLAMAV" | head -2;
```

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

```
30   4    *    *    0    root periodic mailtransport
```

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

```
% cd /etc

% sudo ln -s periodic/mailtransport/500.mailtransport mailtransport
```

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

```
# mailtransport 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.
#
mailtransport_output="/var/log/mailtransport.out"  # user or /file
mailtransport_show_success="YES" # scripts returning 0
mailtransport_show_info="YES"    # scripts returning 1
mailtransport_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 "CLAMAV"

% sudo postfix reload
```

Note: Additional patch files may be included in the Macintosh archive `'Macintosh.tar.gz'` for advanced/modified features, please see included `'README'` for related information.