

Installing Clamav 0.95.2 on Leopard 10.5.6

Doc version 0.1

One of the many programs running on my server is Clamav. It is an open source virus checker. I don't use it because I think I might get a virus (like that would ever happen). I have it because it makes for a more complete mail server. I may not be affected by viruses, but others are and if I ever get an IT job I should know how to setup and run a proper mail server, including a virus checker.

Previously I followed the tutorial available at <http://amadain.net/2007/11/03/postfix-amavis-spamassassin-dspam-and-clamav-working-together-mac-osx-leopard> and then modified it with the tutorial from <http://osx.topicdesk.com/content/view/139/41/>. However, while this did get Clamav installed, it just didn't work like I wanted it to. There were permissions problems and service setup problems.

I wrote a "from scratch" tutorial for installing Clamav 0.95.2 on Leopard.

I am assuming you have XCode installed. We will also be using the terminal exclusively.

This is a copy and paste tutorial. if you don't feel like reading you could just cut and paste the commands in order to end up with an installed and (as far as I know) running virus scanner.

Firstly we have to get the Clamav sourcecode.

```
curl -O http://jaist.dl.sourceforge.net/sourceforge/clamav/clamav-0.95.2.tar.gz
```

Then we need to expand the archive and configure it. This configuration will install clamav in the /usr/local default locations.

```
tar -xvf clamav-0.95.2.tar.gz
cd clamav-0.95.2
./configure --with-user=_clamav --with-group=_clamav
```

Now we build and then install clamav.

```
make
sudo make install
cd ..
```

That should have installed without any problems. Now we need to setup a few things before we start running it.

First, lets setup the logfiles for Clamav and it's update agent freshclam.

```
sudo touch /var/log/freshclam.log
sudo touch /var/log/clamd.log
sudo chown _clamav /var/log/freshclam.log
sudo chown _clamav /var/log/clamd.log
```

We also need to create the path for the virus database and set permissions.

```
sudo mkdir /var/lib/clamav
sudo chown _clamav:_clamav /var/lib/clamav
sudo chmod 0644 /var/lib/clamav
```

We add the `_clamav` user to the daemon group to allow it to save its PID file in the same place as other programs. (for tidyness).

```
sudo dscl . -append /Groups/daemon GroupMembership _clamav
```

Now we need should edit the config files for clamav and freshclam.

We are going to use the terminal to create the config files we need.

First we will create `clamd.conf`. Simply copy and paste the following to your terminal window. Be sure to press return afterwards.

```
echo LogFile /var/log/clamd.log >> clamd.conf
echo LogFileSize 2M >> clamd.conf
echo LogTime yes >> clamd.conf
echo LogSyslog yes >> clamd.conf
echo LogFacility LOG_MAIL >> clamd.conf
echo PidFile /var/run/clamd.pid >> clamd.conf
echo TemporaryDirectory /var/tmp >> clamd.conf
echo DatabaseDirectory /var/lib/clamav >> clamd.conf
echo LocalSocket /tmp/clamd.socket >> clamd.conf
echo FixStaleSocket yes >> clamd.conf
echo ReadTimeout 300 >> clamd.conf
echo IdleTimeout 60 >> clamd.conf
echo MaxDirectoryRecursion 20 >> clamd.conf
echo SelfCheck 600 >> clamd.conf
echo User _clamav >> clamd.conf
echo AllowSupplementaryGroups yes >> clamd.conf
echo Foreground yes >> clamd.conf
echo DetectPUA yes >> clamd.conf
echo AlgorithmicDetection yes >> clamd.conf
echo ScanPE yes >> clamd.conf
echo ScanELF yes >> clamd.conf
echo DetectBrokenExecutables yes >> clamd.conf
echo ScanOLE2 yes >> clamd.conf
echo ScanPDF yes >> clamd.conf
echo ScanMail yes >> clamd.conf
echo PhishingSignatures yes >> clamd.conf
echo ScanHTML yes >> clamd.conf
echo ScanArchive yes >> clamd.conf
```

Now you have created a file called `clamd.conf` in your current directory. We need to modify it a little and move it before we can use it.

```
sudo chmod 0644 clamd.conf
sudo chown _clamav:wheel clamd.conf
sudo mv clamd.conf /usr/local/etc/
```

Easy.

Next we will create the config file for freshclam.

```
echo DatabaseDirectory /var/lib/clamav >> freshclam.conf
echo UpdateLogFile /var/log/freshclam.log >> freshclam.conf
echo LogFileSize 2M >> freshclam.conf
echo LogTime yes >> freshclam.conf
echo LogSyslog yes >> freshclam.conf
echo PidFile /var/run/freshclam.pid >> freshclam.conf
echo DatabaseOwner _clamav >> freshclam.conf
echo AllowSupplementaryGroups yes >> freshclam.conf
```

```
echo DatabaseMirror database.clamav.net >> freshclam.conf
echo MaxAttempts 2 >> freshclam.conf
echo Checks 2 >> freshclam.conf
echo Foreground yes >> freshclam.conf
```

As with the clamd config file we need to modify it and move it.

```
sudo chmod 0644 freshclam.conf
sudo chown _clamav:wheel freshclam.conf
sudo mv freshclam.conf /usr/local/etc/
```

You now have a fully functional installation of clamav. However, you should run freshclam once as root once to get your virus patterns and to setup the database for clamav to use.

```
sudo freshclam
```

Once it is finished, you should then set permission on one more file, then your good to go.

```
sudo chown _clamav /var/lib/clamav/mirrors.dat
```

You can now use clamav to scan your files. This is a great setup for interfacing with postfix to scan all mails arriving to your server.

If you are going to run a server with clamav as the virus checker, then you should have clamav start up in daemon mode when your computer boots, and also have the freshclam updater run automatically. To do this you will need to create 2 more files. We need to create 2 .plist files in the /System/Library/LaunchDaemons/ folder.

Even if your not going to run a mail server, it is a good idea to set up freshclam to update the virus patterns automatically. To do this we will create a file that we will call net.clamav.freshclam.plist and we will use settings to load freshclam at boot, and have it update twice a day.

Just copy and paste the following into your terminal window to create the file.

```
echo "<?xml version="1.0" encoding="UTF-8"?> " >> net.clamav.freshclam.plist
echo '<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">' >> net.clamav.freshclam.plist
echo "<plist version="1.0">" >> net.clamav.freshclam.plist
echo "<dict>" >> net.clamav.freshclam.plist
echo " <key>KeepAlive</key>" >> net.clamav.freshclam.plist
echo " <true/>" >> net.clamav.freshclam.plist
echo " <key>Label</key>" >> net.clamav.freshclam.plist
echo " <string>org.clamav.freshclam</string>" >> net.clamav.freshclam.plist
echo " <key>OnDemand</key>" >> net.clamav.freshclam.plist
echo " <false/>" >> net.clamav.freshclam.plist
echo " <key>Program</key>" >> net.clamav.freshclam.plist
echo " <string>/usr/local/bin/freshclam</string>" >> net.clamav.freshclam.plist
echo " <key>ProgramArguments</key>" >> net.clamav.freshclam.plist
echo " <array>" >> net.clamav.freshclam.plist
echo " <string>/usr/local/bin/freshclam</string>" >> net.clamav.freshclam.plist
echo " <string>-d</string>" >> net.clamav.freshclam.plist
echo " <string>-c</string>" >> net.clamav.freshclam.plist
echo " <string>2</string>" >> net.clamav.freshclam.plist
echo " </array>" >> net.clamav.freshclam.plist
echo " <key>RunAtLoad</key>" >> net.clamav.freshclam.plist
echo " <false/>" >> net.clamav.freshclam.plist
echo " <key>ServiceIPC</key>" >> net.clamav.freshclam.plist
echo " <false/>" >> net.clamav.freshclam.plist
```

```
echo " <key>UserName</key>" >> net.clamav.freshclam.plist
echo " <string>_clamav</string>" >> net.clamav.freshclam.plist
echo "</dict>" >> net.clamav.freshclam.plist
echo "</plist>" >> net.clamav.freshclam.plist
```

Now you have the file, it needs, like the others, to be modified then installed.

```
sudo chmod 664 net.clamav.freshclam.plist
sudo chown root:wheel net.clamav.freshclam.plist
sudo mv net.clamav.freshclam.plist /System/Library/LaunchDaemons/
```

This will now load at your next reboot. If you like me however, and you never turn off your machine or reboot, then you should enter the following to start the service.

```
sudo launchctl /System/Library/LaunchDaemons/net.clamav.freshclam.plist
```

For those of you who wish to have clamav start at boot time (especially for integration with postfix or some other MTA), I have provided the appropriate plist below. Just cut and paste into the terminal.

```
echo "<?xml version='1.0' encoding='UTF-8'?>" >> net.clamav.clamd.plist
echo '<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">' >> net.clamav.clamd.plist
echo "<plist version='1.0'>" >> net.clamav.clamd.plist
echo "<dict>" >> net.clamav.clamd.plist
echo " <key>Label</key> " >> net.clamav.clamd.plist
echo " <string>net.clamav.clamd</string>" >> net.clamav.clamd.plist
echo " <key>OnDemand</key>" >> net.clamav.clamd.plist
echo " <false/>" >> net.clamav.clamd.plist
echo " <key>Program</key>" >> net.clamav.clamd.plist
echo " <string>/usr/local/sbin/clamd</string>" >> net.clamav.clamd.plist
echo " <key>ProgramArguments</key>" >> net.clamav.clamd.plist
echo " <array>" >> net.clamav.clamd.plist
echo " <string>clamd</string>" >> net.clamav.clamd.plist
echo " </array>" >> net.clamav.clamd.plist
echo " <key>ServiceIPC</key>" >> net.clamav.clamd.plist
echo " <false/>" >> net.clamav.clamd.plist
echo " <key>UserName</key>" >> net.clamav.clamd.plist
echo " <string>_amavisd</string>" >> net.clamav.clamd.plist
echo "</dict>" >> net.clamav.clamd.plist
echo "</plist>" >> net.clamav.clamd.plist
```

Once created, the file needs to be modified and moved before it is usable.

```
sudo chmod 664 net.clamav.clamd.plist
sudo chown root:wheel net.clamav.clamd.plist
sudo mv net.clamav.clamd.plist /System/Library/LaunchDaemons/
```

This will now load at your next reboot. If you like me however, and you never turn off your machine or reboot, then you should enter the following to start the service.

```
sudo launchctl load /System/Library/LaunchDaemons/net.clamav.clamd.plist
```

Congratulations, you now have a fully installed virus checker and startup scripts for Clamav 0.95.2 on OS X 10.5.6