Updating ClamAV
on
Mac OS X 10.5.5 or greater

1. – Introduction

2. – What is installed as part of OS X Server

3. – Requirements

4. – Getting and installing the latest version of ClamAV

5. – Caveats – READ this chapter!

1. - Introduction

The purpose of this document is to provide instructions on how to update the version of ClamAV included with OS X 10.5.5 Server or greater. DO NOT USE this document to update ClamAV on 10.4.x Tiger Server. Another version of this tutorial is available for 10.4.x.

It will guide you through updating to the latest stable version of ClamAV without breaking Server Admin functionality. The new version will be installed alongside Apple's. Thus, it will not be overwritten by Apple SW updates.

Although the Apple included version of ClamAV is suitable for most users, there are situations where one might need to update. A common reason is to take advantage of the latest security fixes.

This document will require you to use the command line. If you do not feel comfortable with using the command line, you should look for a ready made installer package or for somebody to assist you.

This document is written for Mac OS X 10.5.5 or greater.

DISCLAIMER: Whatever you do based on this document, you do it at your own risk! Just in case you haven't understood: Whatever you do based on this document, you do it at your own risk!

This tutorial has been tested on a standard Mac OS X 10.5.5 Server installation. If you have already tinkered with your system, be aware that things might differ. It is impossible for me to foresee all changes that one might have applied to a server.

This tutorial contains step-by-step instructions for the terminal. Although you could just type them line by line, it is recommended you have a basic understanding of the terminal.

2. - What is installed as part of OS X Server

In order to better understand the process it is useful to have a
basic knowledge of the basic installation.

As of 10.5.5 and the latest security updates, Apple includes
ClamAV 0.94 with its server operating system.
As of 10.5.8 and the latest security updates, Apple includes
ClamAV 0.95.3 with its server operating system.
These can be safely updated to the latest stable version of
ClamAV 0.96.x

3. - Requirements

Before you get started, you need to make sure some basic
requirements are met:

- You have made a backup of your system.
- You have the latest version of Apple's Developer Tools
  (Xcode 3.1.2 or higher for Leopard) installed.
  Dev Tools are available on your Server DVD and as a free
  download from Apple's Developer Connection.
- You do have a backup
- You are running 10.5.5 or greater
- You have not manually updated anything related to ClamAV
  so far (if you have, you must know how to adapt
  these instructions to the changes you made).

- Not a requirement, but it is recommended you subscribe to our
  newsletter(s) to be informed when updated versions of this
  tutorial become available:
  http://osx.topicdesk.com/newsletter/

4. - Getting and installing the latest version of ClamAV

This chapter will guide you through replacing your current version of ClamAV with the latest stable version available. It will not add any visible functionality compared to the Apple installed version. It will however update the ClamAV engine to the latest internal virus scanning functionality. It will also give you the peace of mind to have the latest version with the most recent security fixes. Please be aware that instructions apply only to the 0.96.x branches of ClamAV.

So let's get going:
Make sure you are logged in as root or issue "sudo -s" first.

Get and install the latest version of ClamAV by issuing the following commands (*in oblique type*). Issue them one after the other making sure you do not miss any dots or slashes. Also note that the download URL given may change in the future. In that case just replace the URL in this document with the current one. The URL used at the time this document was written refers to ClamAV 0.96. If you want to install a different version, adjust accordingly. Lines wrapping without line spacing are a single command.

mkdir -p /SourceCache

cd /SourceCache

curl -O http://sunet.dl.sourceforge.net/project/clamav/ clamav/0.96.1/clamav-0.96.1.tar.gz

tar xzf clamav-0.96.1.tar.gz

cd clamav-0.96.1

Then continue with the following configure string.

./configure --prefix=/usr/local --mandir=/usr/local/share/man --sysconfdir=/private/etc/spam/clamav/new --enable-bigstack --with-user=_clamav --enable-static --with-group=_clamav --with-dbdir=/var/clamav --datadir=/var/clamav

make

make install

If everything went well, you have just installed an updated version of ClamAV.

Since we installed this alongside Apple's original install, there are a few more things we need to do:

NOTE: If you have already updated ClamAV following this tutorial in the past, you only need to restart it (unload and load the launchd property lists). You do not need to re-do the following procedures.
If this is the first time you update ClamAV by using this tutorial, read on.

To simplify things for you, I have prepared a set of ready made and OS X Server compliant configuration files for you. To get and install them issue:

cd /SourceCache

curl -O http://downloads.topicdesk.com/docextras/ clamav_extras_105_096.tar.gz

tar xzf clamav_extras_105_096.tar.gz

cd clamav_extras_105_096

chown root:wheel /SourceCache/clamav_extras_105_096/*

mkdir -p /private/etc/spam/clamav/new

cp *.conf /private/etc/spam/clamav/new

cp *.plist /System/Library/LaunchDaemons

On some servers it seems that one of the necessary directories is not created automatically. So let's do this now

mkdir -p /var/clamav/tmp

chown _amavisd:_amavisd /var/clamav/tmp

Now everything is ready. All we need to do is to switch over from the Apple supplied version of ClamAV to the one we just installed. To do so issue:

sudo /bin/launchctl unload -w /System/Library/ LaunchDaemons/org.clamav.freshclam.plist

sudo /bin/launchctl load -w /System/Library/ LaunchDaemons/net.clamav.freshclam.plist

sudo /bin/launchctl unload -w /System/Library/ LaunchDaemons/org.clamav.clamd.plist

sudo /bin/launchctl load -w /System/Library/ LaunchDaemons/net.clamav.clamd.plist

sudo /bin/launchctl unload /System/Library/ LaunchDaemons/org.amavis.amavisd.plist

sudo /bin/launchctl load /System/Library/LaunchDaemons/ org.amavis.amavisd.plist

Now you MUST reboot! (There are ways around it, but because of the database format change in ClamAV, it is safer to reboot)

Check your /var/log/freshclam.log. You should see the new version updating. You should now be all set and have an "Apple compliant" version of ClamAV on your server. Server Admin will still work as before.

Note: If things go wrong you can try and fall back to the original Apple installation of ClamAV which we left untouched.

To do so, issue the following:

*sudo /bin/launchctl unload -w /System/Library/
LaunchDaemons/net.clamav.freshclam.plist*

*sudo /bin/launchctl load -w /System/Library/
LaunchDaemons/org.clamav.freshclam.plist*

*sudo /bin/launchctl unload -w /System/Library/
LaunchDaemons/net.clamav.clamd.plist*

*sudo /bin/launchctl load -w /System/Library/
LaunchDaemons/org.clamav.clamd.plist*

*sudo /bin/launchctl unload /System/Library/
LaunchDaemons/org.amavis.amavisd.plist*

*sudo /bin/launchctl load /System/Library/LaunchDaemons/
org.amavis.amavisd.plist*

5. - Caveats

This tutorial has been tested on a standard Mac OS X 10.5.5 or greater Server installation. If you have already tinkered with your system, be aware that things might differ. It is impossible for me to foresee all changes that one might have applied to a server.

That's all folks.
Hope this helps.
Have fun,
Alex

Doc. Version 1.4.0, 20.5.2010
Athanasios Alexandrides
Lugano, Switzerland
tutorials -at- topicdesk.com