Installing and configuring ClamAV

ANTIVIRUS ON LINUX

Protecting Windows clients from the big bad Internet.

BY KURT SEIFRIED

My first thought was why bother writing a column about antivirus for Linux? In all my years I actually haven't encountered a Linux box that was infected with a virus in the wild (as opposed to machines that were compromised through a worm or a direct attack). So why bother writing about this? More often than not people run Windows on their client systems and Linux on their servers which got me thinking "why not protect those Windows machines with the Linux servers." So I checked a little: I knew you could easily scan incoming email with ClamAV [1], and you can configure the Squid web proxy to use ClamAV, but did you know you can configure Samba to use ClamAV to scan files when they are accessed? One important note: Using ClamAV on your servers to sanitize oncoming data to filter email and HTTP traffic won't make you completely safe; if you run Windows, you need to run a local antivirus scanner. Unfortunately I won't be able to give step-by-step details; they vary a lot from Linux vendor to Linux vendor (different package layouts, configuration file locations, etc.), and the amount of instructions needed to get this working simply won't fit in two pages. So instead, I'll cheat and call this a survey article.

Installing and Using ClamAV

Installing ClamAV is pretty simple because most vendors ship ClamAV as a standard set of packages. Some notable exceptions to this are Red Hat Enterprise 5 and CentOS 5. If you run these systems, the easiest way to get RPMs is from Dag [2]. Other vendors, such as Debian and Red Hat Fedora, have split ClamAV into many packages; for example, Fedora 12 has clamav, clamav-data, clamav-data-empty, clamav-devel, clamav-filesystem, clamav-lib, clamav-milter, clamav-milter-sysvinit, clamav-milter-upstart, clamav-scanner, clamav-scanner-sysvinit, clamav-scanner-upstart, clamav-server, clamav-server-sysvinit, clamav-update, and exim-clamav (Debian has a mere dozen packages).

ClamAV can be run locally to scan specific files, directories, and so on like a regular antivirus scanner. However, ClamAV also supports a server mode, making it available to other systems on the network. This means that you can, for example have one centralized machine running ClamAV that is kept up to date and has a lot of horsepower that is used by other machines, such as email servers, to scan content for viruses without bogging down the email servers. This also makes adding antivirus capabilities to a program or a service easy: Just fire the content off to a ClamAV server and get a response – no need to integrated libraries or anything complicated. Simply install the clamav-scanner-sysvinit package on Fedora or clamav-daemon on Debian and configure it to start automatically. Also, you need to edit your *clamd.conf* file (*/etc/clamd.d/scan.conf* on Fedora) and uncomment the *TCPSocket* and *TCPAddr* lines:

```
TCPSocket 3310
TCPAddr 127.0.0.1
```

Keeping ClamAV Up To Date

If you have to get one thing right for any of this to work, updating your antivirus signatures is it. The majority of antivirus scanners rely on signatures to detect viruses; very few antivirus scanners implement heuristic or behavior-based monitoring. To update your ClamAV signatures, you'll want the clamav-update package on Fedora or clamav-freshclam on Debian installed. This package includes a binary called *freshclam*,

which downloads the updates and integrates them into your existing antivirus signatures. To configure *freshclam* to run, you'll need to edit the *freshclam.conf* file. The only lines you typically need to change are commenting out the "Example" line at the top (which will cause an error and prevent *freshclam* from running) and changing the *DatabaseMirror* line to point to your country's ClamAV mirrors at a bare minimum:

```
# Uncomment the following line
   and replace XY with your country
# code. See http://www.iana.org/cctld/
   cctld-whois.htm for the full list.
DatabaseMirror db.ca.clamav.net
```

Then you can add *freshclam* to the system crontab files in */etc* or into root's crontab so that it is run regularly and notifies you of the results. Or, you can use the *OnUpdateExecute* command in *freshclam.conf* to run a script to notify you:

```
0 * * * * /usr/bin/freshclam |
   mail -s "freshclam update info"
   admin@example.org
```

One critical note: If you are running the clamd server, it will have outdated signatures because it loads them when first executed. To make sure clamd has the most recent signatures, you need to configure freshclam to send a "RELOAD" command to it. To do this, change the *NotifyClamd* parameter in *freshclam.conf* so that it points to the configuration file for clamd (e.g., on Fedora):

```
NotifyClamd /etc/clamd.d/scan.conf
```

ClamAV and Sendmail

Many years ago if you wanted to have Sendmail filter email with the use of an external program, you had to delve into *sendmail.mc* – you know, the file that looked like line noise and was really no fun to deal with. Luckily, Sendmail implemented Milter (Mail Filter), which allows you to reject and modify connections, messages, and recipients; add or delete headers; rewrite message bodies; and so on. Postfix has also implemented Milter, so if your program provides a Milter interface, you can use it easily with either Sendmail or Postfix. When scanning email with ClamAV, you can communicate with ClamAV via a local Unix socket or TCP (either on the local server or on another machine). TCP is very easy to set up, once you have clamd up and running (assuming you use the default port 3310). All you need to do is add the following line to *sendmail.mc*:

```
INPUT_MAIL_FILTER
   (`clamav', `S=inet:3310@127.0.0.1,
    F=, T=S:4m;R:4m')dnl
```

Then you simply rebuild *sendmail.mc*, restart Sendmail, and you are done. Postfix is slightly more complicated – you have to edit two files – but details are available online [3]. Additionally, if you don't want to or cannot integrate ClamAV with your mail agent, you can use ClamSMTP to act as a proxy [4] and filter email.

ClamAV and Squid

Now I'm getting into something interesting. It appears that one of the most popular techniques for creating botnets is via "drive-by" downloads. Simply put, an attacker inserts malicious content into a web page or an ad server and then infects several hundred or even thousand Windows clients that are then compromised and taken over. So how can you add antivirus scanning to your web proxy? Squid 3.0 has client support for ICAP (Internet Content Adaptation Protocol) [5], which is much like Milter for Sendmail, in that it allows you to offload processing (such as antivirus scanning) to a different server. To enable an ICAP client in Squid, you simply use the *--enable-icap-client* option when you compile it:

```
./configure --enable-icap-client
```

But this is only half the battle. Then you need to get an ICAP server for ClamAV: Currently, there appears to be only one: c-icap. But the good news is that it runs on Linux and should work on BSD systems. For details on installing c-icap and configuring Squid to use it, the c-icap website has an install page that covers all the details [6]. It should be noted that if you're in the market for a commercial antivirus solution for Linux, you should make sure it has a working ICAP server if you want to use it with your web proxy.

ClamAV and Samba

So, you've locked up your email and web browsing, but what happens when someone brings in removable media with a virus onboard, and it copies itself onto the file server in the hopes of infecting other systems? In most cases, the virus runs rampant, unless, of course, your file server has antivirus capabilities. The samba-vscan [7] module adds on-access scanning capabilities to Samba. The minute a file with a virus is accessed, it should be detected and access blocked to the file (that's the idea, anyway). Details on installation are covered in detail in the *INSTALL* file.

For the Lazy: Copfilter

If you can dedicate a separate machine (or VM image) to your network antivirus scanning, I would recommend going with Copfilter [8], and if you want a turnkey solution, get IPCop, which includes it as a package [9]. ■

INFO

[1] ClamAV: *http://www.clamav.net/*

[2] Dag Wiers ClamAV packages: *http://dag.wieers.com/rpm/packages/clamav/*

[3] Virus Filtering with Postfix and ClamAV: *http://www.debian-administration.org/articles/259*

[4] ClamSMTP: *http://memberwebs.com/stef/software/clamsmtp/*

[5] ICAP: *http://en.wikipedia.org/wiki/Internet_Content_Adaptation_Protocol*

[6] c-icap Server: *http://c-icap.sourceforge.net/install.html*

[7] Open Antivirus: *http://www.openantivirus.org/projects.php*

[8] Copfilter: *http://www.copfilter.org/*

[9] IPCop: *http://sourceforge.net/apps/trac/ipcop/wiki*

THE AUTHOR

Kurt Seifried is an Information Security Consultant specializing in Linux and networks since 1996. He often wonders how it is that technology works on a large scale but often fails on a small scale.