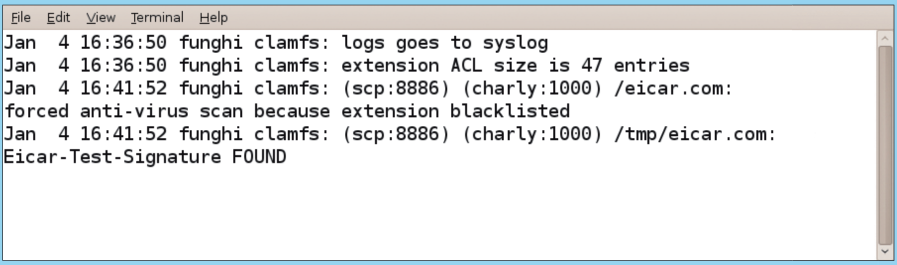
The sys admin's daily grind: ClamFS

GOURMET TEMPLE

Too many cooks spoil the broth, they say, but it could just as easily be an ingredient that isn't part of the recipe. If you can't reduce the number of cooks, you have to take other steps to make your broth more edible.

BY CHARLY KÜHNAST



```
Jan  4 16:36:50 funghi clamfs: logs goes to syslog
Jan  4 16:36:50 funghi clamfs: extension ACL size is 47 entries
Jan  4 16:41:52 funghi clamfs: (scp:8886) (charly:1000) /eicar.com:
forced anti-virus scan because extension blacklisted
Jan  4 16:41:52 funghi clamfs: (scp:8886) (charly:1000) /tmp/eicar.com:
Eicar-Test-Signature FOUND
```

Figure 1: ClamFS monitors write access and triggers ClamAV.

studio_busse yankushev, 123RF

When people start talking about anti-virus scanners on file servers, you often hear them say they're not that important because Linux servers are not really vulnerable anyway. This reminds me about the debate on swine flu vaccination. There are many arguments for and against, but there is one thing that really impressed me: If you have been vaccinated, you won't spread the illness and will thus passively protect other people whether you actually benefit from the vaccination yourself. People like me, who have problems with their immune systems, will always appreciate this benefit.

The argument in favor of anti-virus scanners on file servers is similar. The more users that access a data pool, the more important protection is. Having said this, scanners are often configured to scan cyclically, say once an hour. It would be preferable to have a scanner that triggers whenever write access occurs.

ClamFS [1] provides the basic premise to implement my solution. To do this, it creates a FUSE (Filesystem in User Space) that intercepts write access and has ClamAV [2] check it before the data are written out to disc.

A cache prevents the scanner from investigating the same file multiple times. The performance isn't exactly thrilling, but it's definitely fast enough for a data bucket with very occasional write operations.

Airtight

ClamFS is included in many popular distributions; you will additionally need Fuse-utils. After completing the installation, you should find a sample configuration in the *docs* directory with plenty of potential for tweaking. I only needed to adjust three parameters for the first function test. The first step is to tell ClamFS where the ClamAV socket is:

```
<clamd socket=➘
   "/var/run/clamav/clamd.ctl" ➘
   check="yes" />
```

Next, I defined the path I wanted Clam to investigate on the filesystem (*root*) and where I wanted Linux to mount the FUSE:

```
<filesystem root=➘
   "/home/charly/clamfs" ➘
   mountpoint="/home/charly/myfiles" ➘
   public="yes" />
```

I saved the configuration file in */etc/clamfs/*. If you need multiple ClamFS mountpoints, you will need a separate configuration file for each one. The whole thing starts with */usr/bin/clamfs /path/clamfs.xml*. Now it really doesn't matter how many cooks work on my brand of broth, because ClamFS will reliably remove any inappropriate ingredients (see Figure 1). ■

INFO

[1] ClamFS: *http://clamfs.sourceforge.net*

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

THE AUTHOR

Charly Kühnast is a Unix operating system administrator at the Data Center in Moers, Germany. His tasks include firewall and DMZ security and availability. He divides his leisure time into hot, wet, and eastern sectors, where he enjoys cooking, freshwater aquariums, and learning Japanese, respectively.