

## El Día a Día del Administrador de Sistemas: ClamFS

# GUSTOS DE GOURMET

Se dice que demasiados cocineros estropean la sopa, aunque perfectamente podría ser culpa de un ingrediente que no formara parte de la receta. Si no puedes reducir el número de cocineros, tendrás que seguir otros pasos para que la sopa sea comestible. **POR CHARLY KÜHNAST**

```
File Edit View Terminal Help
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
```

Figura 1: ClamFS monitoriza los accesos de escritura y llama a ClamAV.

Cuando la gente comienza a hablar de antivirus en servidores de ficheros, con frecuencia se oye que no es muy importante, ya que los servidores Linux no son realmente vulnerables. Esto me hace recordar el debate sobre la vacunación contra la gripe porcina. Existen tantos argumentos a favor como en contra, pero hay algo que realmente me impresiona: si ha sido vacunado, no propagará la enfermedad y, por ello, de forma pasiva protegerá a otras personas al mismo tiempo que se estará protegiendo usted mismo. La gente como yo, que tiene problemas con su sistema inmunológico, apreciará siempre este beneficio.

El argumento a favor de los antivirus en los servidores de ficheros es similar. Cuanto más usuarios accedan a los datos, más importante debe ser la protección. Una vez dicho esto, los antivirus a menudo están configurados para realizar un análisis de forma cíclica, digamos cada hora. Sería preferible poseer un antivirus que se dispare cada vez que se produzca un acceso de escritura.

ClamFS [1] proporciona la premisa básica que implementa mi solución. Para ello crea un FUSE (Sistema de ficheros en el espacio del usuario) que intercepta los

accesos de escritura y tiene a ClamAV [2] para analizar los datos antes de que se escriban en el disco.

Una caché impide que el antivirus investigue los mismos ficheros múltiples veces. El rendimiento no es precisamente excitante, pero es lo suficientemente rápido como para tenerlo en un almacén de datos en el que las operaciones de escritura son ocasionales.

## Hermético

ClamFS se incluye en la mayoría de las distribuciones populares; además harán falta las utilidades Fuse. Tras concluir la instalación, debería encontrar una configuración de ejemplo en el directorio *docs* con una gran cantidad de ajustes potenciales. Sólo tuve que ajustar tres parámetros para la primera prueba de uso. El primer paso es indicarle a ClamFS dónde está el socket de ClamAV:

```
<clamd socket= ↵
"/var/run/clamav/clamd.ct1" ↵
check="yes" />
```

A continuación, definí la ruta que quería que Clam investigara en el sistema de ficheros (*root*) y dónde quería que Linux montara FUSE:

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



studio\_busse/yankushiev\_123RF

Guardé el fichero de configuración en */etc/clamfs/*. Si necesita múltiples puntos de montaje para ClamFS, necesitará un fichero de configuración independiente para cada uno de ellos. Todo comienza con */usr/bin/clamfs/ruta/clamfs.xml*. Ahora no importará cuántos cocineros haya alrededor de mi puchero, ya que ClamFS quitará de en medio todos los ingredientes que no sean apropiados (Figura 1).

## RECURSOS

- [1] ClamFS: <http://clamfs.sourceforge.net>
- [2] ClamAV: <http://www.clamav.net>

## SYSADMIN

**Administrador de Acceso SUMO .....62**

Accesos web restringidos con el administrador de accesos SUMO.

**Monitorización con Shinken .....67**

Un nuevo fork de Nagios que ofrece prometedoras funcionalidades.

## EL AUTOR

Charly Kühnast es Gerente de Sistemas Unix en el centro de datos de Moers, Alemania, cerca del conocido Rhin. Entre sus labores se



incluye la seguridad del cortafuegos, la disponibilidad y el cuidado de la DMZ (zona desmilitarizada). Divide su tiempo libre entre el calor, la humedad y oriente, donde se divierte cocinando, visitando acuarios y aprendiendo japonés respectivamente.