Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Poner clamav configurando sólo procmail (22978 lectures)

Per **Carles Pina i Estany**, ***cpina*** (http://pinux.info)

Creado el 13/02/2004 22:50 modificado el 13/02/2004 22:50

En este breve truco veremos como podemos poner clamav (un antivirus libre) a cualquier servidor de correo, a través de procmail.

De esa forma no necesitaremos a amavis ni tendremos que modificar la configuración del servidor de correo si ya estaba entregando los mensajes a través de procmail.

El antivirus que usaremos será el clamav(1). Es GPL, es muy bueno y actualizado frecuentemente.

Para empezar, tendremos que instalar el antivirus. Si estamos usando Debian Wooody añadiremos en el `/etc/apt/sources.list` esta línea:

```
deb http://www.backports.org/debian stable clamav
```

para tener a clamav como paquete (sinó lo podriamos bajar, compilar, etc. desde http://www.clamav.net(1))

En Debian Sarge o Sid podemos hacer directamente:

```
apt-get install clamav clamav-freshclam clamav-daemon
```

(podriamos instalar el `clamav-data` en lugar del `clamav-freshclam` si no queremos que se actualice la base de datos de virus por Internet)

Cuando estemos instalando el `clamav-freshclam` nos preguntará en qué interfaz estamos conectados a Internet y un servidor (ya viene por defecto) donde bajarse las actualizaciones.

Suponemos que tenemos nuestro servidor de correo (MTA) funcionando correctamente, y que además está entregando los mails locales mediante postfix(2).

Por ejemplo, en postfix tenemos que tener una línea como esta:

```
mailbox_command = /usr/bin/procmail -a "$EXTENSION"
```

En el `/etc/postfix/main.cf`
Si no usamos postfix miraremos como es en nuestro servidor (es posible que ya venga por defecto, y sinó poco le faltará para hacerlo)

Un correo electrónico que tenga que ser entregado localmente pasará a `procmail`, que hará las reglas de filtrado de `/etc/procmailrc` (y después las de `$HOME/.procmailrc`, para cada usuario) y lo dejará, típicamente en `/var/mail/usuario`.

En el fichero `/etc/procmailrc` añadiremos esas líneas:

```
SHELL=/bin/sh


AV_REPORT=`clamdscan --stdout --disable-summary - | cut -d: -f 2`
VIRUS=`if [ "$AV_REPORT" != " OK" ]; then echo Yes; else echo No;fi`
```

```
:0fw
| formail -i "X-Virus: $VIRUS"

:0fw
* ^X-Virus: Yes
| formail -i "Virus: $AV_REPORT" -i "Subject: MENSAJE CON VIRUS: $AV_REPORT"
```

La línea de `SHELL=/bin/sh` la pongo porqué yo tengo algunos usuarios que no tienen shell en el `/etc/passwd` por lo que no se ejecutaba los que hay entre las comillas invertidas.

En la línea del **AV_REPORT** guardamos " OK" si no tiene ningún virus o bien el nombre del virus.

En la siguiente línea, en la variable **VIRUS** ponemos "Yes" si tiene algun virus. Si no tiene ningún virus ponemos "No".

En la primera regla de filtrado, añadimos la cabecera `X-Virus` con "Yes" o "No" (así el usuario final lo puede filtrar fácilmente, y nos sirve a nosotros para saber que ha sido escaneado, etc.)

Y en la segunda línea, si ha venido con un virus ponemos una cabecera llamada "Virus" que contiene el reporte de Clamav. Y además, modificamos el Subject que tuviera y ponemos el nombre del virus.
En lugar de modificar el Subject y añadir una cabecera más lo podriamos eliminar directamente.

Como curiosidad, después del control de virus yo tengo:

```
:0fw
| spamc -f -s 100000 -u $LOGNAME
```

Para pasarlo por el Spamassassin. Nunca había sido tan fácil tener un sistema de correo con antivirus y antispam.

En algun usuario nos puede interesar tener su `~/.procmailrc` algo como:

```
DEFAULT=$MAIL
LOGFILE=$HOME/.procmailrc.log

:0
* ^X-Virus: Yes
/dev/null   #o bien guardarlo en otro fichero, etc.

:0
* ^X-Spam-Status: Yes
/dev/null   #o bien guardarlo en otro fichero, etc.
```

He hecho el "truco" con el `clamdscan`. Eso nos obliga a tener el demonio `clamav-daemon` ejecutándose (por defecto no abre ningún puerto sinó que sólo crea un fichero tipo fifo para comunicarse con el cliente).
Si no nos gusta tener un demonio para esto, podemos no instalar el clamav-daemon y usar en el `procmailrc` el clamscan, que no usa ningún demonio sinó que él mismo escanea el correo y ya está.

Para probar que funcione, podemos ir a http://www.eicar.org/download/eicar.com.txt[3] y mandarnos esa línea por e-mail. Es un test para saber si el antivirus que usemos está activado. De esa forma veremos si lo está detectando bien o no.

También nos tenemos que fijar que todos los correos nuevos que nos lleguen tengan la nueva cabecera de `X-Virus:`

Espero que esa manera simple (pero efectiva) sea útil a alguien.

Lista de enlaces de este artículo:

1. http://www.clamav.net
2. http://www.postfix.org
3. http://www.eicar.org/download/eicar.com.txt

E-mail del autor: carles _ARROBA_ pinux.info
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=1978