



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

## Exim 3 con MailScanner y ClamAV (402 lectures)

Per Pablo Iranzo Gómez, [iranzop](http://www.uv.es/~iranzop/) (<http://www.uv.es/~iranzop/>)

Creado el 06/02/2004 11:49 modificado el 06/02/2004 11:49

*Pues el lanzamiento de este artículo se lo debo a Ricardo... la verdad es que tenía desde hace mucho tiempo funcionando servidor con antispam y antivirus, primero fue con el sendmail y cuando migré a Debian pues lo monté con el exim... Así que este es el recetario :)*

## Previos:

Para hacerlo funcionar, vamos a tener que hacer unas cosillas...

Debemos tener instalados:

- MailScanner
- Exim
- Clamav (con clamav-freshclam)

Recomendables: razor, unrar, lha, unzoo, arj

El funcionamiento es muy sencillo, a partir de la configuración, dispondremos de dos colas de correo, una para recibir y otra para enviar.

El correo que recibamos será almacenado por exim en sus carpetas, cada cierto tiempo MailScanner comprobará que hay o no correo nuevo, y en ese caso, lo analizará mediante su sistema antispam (sí, el spamassassin) y junto con razor (red colaborativa para notificación de spam), con el antivirus, y al final de todo, si el mensaje supera todos los criterios, lo moverá a la cola de salida, y exim, lo enviará como toque (a la cuenta local del usuario, a un equipo remoto, etc).

**mailscanner:** es un programa que vengo usando desde hace mucho, su archivo de configuración está bien documentado y permite configurarlo para que los mensajes de email enviados al administrador, al usuario o a la persona que mandó el archivo que estaba infectado lleguen en castellano. Soporta muchos antivirus, reglas de configuración, listas de emails a no comprobar, listas de email a prohibir, etc

**exim:** Sólo puedo decir que todo el mundo se mete con el ;) Es pequeñito, rápido y por defecto, se ejecuta a cada correo recibido en lugar de estar como demonio... (pero para lo que quiero me vale).

**clamav:** antes gastaba el fprot (los scripts que venían con el mailscanner servían para actualizarlo, etc. Clamav además de libre, se actualiza el solito ;) (por eso lo del freshclam y que os pregunte que cuál es la interfaz que se conecta a internet, para saber cuando estais conectados y en base a eso hacer las actualizaciones).

**razor:** es una red colaborativa de detección/notificación de spam. Si yo recibo un tipo de spam nuevo, informo a esa red de ese mensaje (cat mensaje.spam | razor-report) y a partir de ese momento, gente que reciba ese mismo mensaje y utilice razor, lo detectará también como spam sin tener que configurar nada...

---

## Configuración:

Bueno, vamos allá con la configuración.

El clamav lo único que tenemos que hacer es configurarlo durante la instalación para decirle en que interfaz escuchar, si no se pone ninguna, es que siempre estamos conectados..

Tal y como indica el Readme.Debian del paquete MailScanner (bueno, acabo de darme cuenta que nanai, han quitado el documento de montarlo con exim3, así que lo haré en base al que tengo yo ya puesto :))

## Exim:

El caso es que una vez tenemos una configuración válida de exim (en /etc/exim/exim.conf), tenemos que hacer lo siguiente:

```
cd /etc/exim
mv exim.conf exim_original.conf
cp exim_original.conf exim_incoming.conf
cp exim_original.conf exim_outgoing.conf
ln -s exim_incoming.conf exim.conf
```

Tendremos que crear ahora también unos directorios copia de los que ya tenemos para el exim normal pero llamados exim\_incoming (misma estructura, mismo propietario, mismos permisos)

Y ahora, empezamos a editar archivos...

Lo primero es cambiar la configuración del `exim_incoming.conf` y añadimos al principio del archivo de configuración, tras los comentarios lo siguiente:

```
# mailscanner config
spool_directory = /var/spool/exim_incoming
queue_only = true
```

De este modo `exim_incoming` sólo almacenará los correos en la carpeta indicada, pero sin intentar su entrega. Luego al principio de la parte `DIRECTORS`, justo tras los comentarios del encabezamiento añadimos:

```
#mailscanner config
defer_director:
driver = smartuser
new_address = :defer: All deliveries are deferred
```

Y luego justo tras el encabezamiento de la sección `ROUTERS`

```
#mailscanner config
defer_router:
driver = domainlist
self = defer
route_list = "* 127.0.0.1 byname"
```

Acabado con el `exim_incoming.conf`, ahora vamos a retocar el `exim_outgoing.conf` y lo habeis adivinado... no hay que tocar nada :) Hemos de crear el `/etc/cron.d/exim` con el siguiente contenido:

```
# /etc/cron.d/exim: crontab fragment for exim

# Run queue every 15 minutes
08,23,38,53 * * * * mail if [ -x /usr/sbin/exim -a -f /etc/exim/exim_outgoing.conf -q ; fi

# Tidy databases
13 6 * * * mail if [ -x /usr/sbin/exim_tidydb ]; then /usr/sbin/exim_tidydb /var/spool/exim retry >/dev/null; fi
17 6 * * * mail if [ -x /usr/sbin/exim_tidydb ]; then /usr/sbin/exim_tidydb /var/spool/exim wait-remote_smtp >/dev/null; fi
```

(las dos anteriores, van en la misma línea)

Con esta entrada en el cron, nos aseguramos que se envíen los correos de salida cada 15 minutos.

---

## MailScanner:

Vamos a pasar a configurar el MailScanner editando el `/etc/MailScanner/MailScanner.conf`

Como es un archivo grande, las opciones que voy a poner, están puestas por orden, pero sería conveniente buscar el ejemplo o explicación asociado a cada una y poner los valores propuestos en lugar de los ya establecidos o bajo su explicación.

Yo recomendaría cambiar:

```
%report-dir% = /etc/MailScanner/reports/es
```

Para configurar los mensajes en español

```
%org-name% = Merak
```

Para poner el de la máquina donde ejecutamos (que así aparecerá en los correos salientes, mensajes de error, etc)

```
Queue Scan Interval = 5
```

para indicar cada cuantos segundos debe controlarse la cola y comenzar a procesar correos

```
Incoming Queue Dir = /var/spool/exim_incoming/input
Outgoing Queue Dir = /var/spool/exim/input
```

Para indicar de dónde se recoge el correo y dónde se ubica tras los controles pertinentes

```
MTA = exim
Sendmail2 = /usr/sbin/exim -C /etc/exim/exim_outgoing.conf
```

Para configurar nuestro demonio de correo, y el comando necesario para realizar la entrega final

```
Virus Scanning = yes
Virus Scanners = clamav
```

A partir de aquí vienen unas opciones interesantes (os podeis leer el archivo de configuración para entenderlas), pero para destacar, por ejemplo permite quitar los IFRAMES para así evitar muchos de los virus que se propagan hoy en día... puede que clamav no los detectase, pero como mailscanner puede eliminar esos tags, esos archivos serían inofensivos (además, permite bloqueos automáticos de .scr, .pif, etc), incluso bloquear formularios en mails... y lo mejor: convertir esas órdenes o incluso el mensaje entero de HTML a texto ;)

```
Spam Checks = yes
Use SpamAssassin = yes
```

Por si acaso no lo sabeis, SpamAssassin incorpora un sistema bayesiano que os permitirá tanto detectar los mensajes en base a reglas como en base a análisis tipo bogofilter... con la ventaja según muchos usuarios de que al incorporar reglas, no "diverge" con el uso como por lo visto pasa con otros sistemas.

Una vez todo configurado, deberemos editar el /etc/default/mailscanner y cambiarlo a:

```
run_mailscanner=1
```

Con esto, ya tendremos todo el sistema operativo, y ¿qué mejor prueba que mandarnos un virus?

Vamos a <http://www.eicar.com><sup>(1)</sup> y descargamos el virus que lleva de prueba y nos lo enviamos a nuestra propia cuenta de correo...

Este esquema al utilizar directamente el sistema de correo, permite que si por ejemplo utilizamos fetchmail, los correos que recibamos, también "sufran" este pequeño análisis, pudiendo así tener nuestro correo también limpio.

Claro, ahora tendremos que iniciar MailScanner: /etc/init.d/mailscanner start y tras un momento, habrá iniciado el proceso y podremos hacer las pruebas...

Espero que os haya resultado útil

Saludos

---

#### Lista de enlaces de este artículo:

1. <http://www.eicar.com>

---

E-mail del autor: Pablo.Iranzo \_ARROBA\_ uv.es

Podrás encontrar este artículo e información adicional en: <http://bulma.net/body.phtml?nIdNoticia=1974>