



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

Exim4 con antivirus (clamav) y spamassassin integrado (682 lectures)Per Ricardo Galli Granada, [gallir](http://mnm.uib.es/~gallir/) (<http://mnm.uib.es/~gallir/>)

Creat el 06/02/2004 03:08 modificat el 06/02/2004 03:08

*Como ya sabéis, vaya semanitas que hemos pasado otra vez. Saturados con gusanos del puñetero Microsoft, y aunque gente como yo hace años que no usa Windows, igual tenemos que seguir padeciendo saturación de líneas y servidores por esos p**** gusanos (y luego dicen que es nuestra comunidad las que los programa... en Windows). Así que me decidí a instalar el anti-virus libre Clamav, pero me llevó tiempo decir como los integraba con el Exim4 y el Spamassassin. Os cuento como lo hice con esos paquetes en una receta para que podáis poner todo en marcha en unos 10 minutos.*

Disclaimer: este artículo estaba en la "lista para hacer" desde hace semanas, así que me puse a hacerlo a la una de la mañana, directamente sobre el Quanta sin corrector (tengo el KDE 3.1 todavía) y con ganas de jugar el Enemy Territory, así que perdonadme los errores.

La introducción de rigor

Aunque todo lo explicado aquí está hecho sobre Debian Sid y Sarge, he visto que las configuraciones son similares en otros distros, especialmente SUSE, donde la configuración del amavisd-new es idéntica a la de Debian.

Estuve pensando varias semanas cómo integrar un antivirus en mis servidores de correo. Como expliqué anteriormente, uso [Exim4 y Spamassassin](#)⁽¹⁾, así que buscaba la solución que pudiera complementarse. Obviamente la solución anti-virus desde el primer momento era el [Clam AV](#)⁽²⁾, pero no tenía nada claro cómo integrarlo con el Exim y el Spamassassin.

Empecé a buscar la documentación y las opciones posibles. Hay mucha variedad, podéis comprobarlo con Google, pero no encontraba una que me convenza del todo. Finalmente me quedé con integrar el clamav y el spamassassin usando esa especie de "integradores" como son el MailScanner y el Amavis. Antes me aseguré que el clamav y spamassassin funcionase con ambos.

Luego de dar vueltas y leer una y otra vez la documentación (sí, soy muy perezoso a la hora de instalar software "de pruebas" sin tener idea ni cómo se instala, hay que hacer demasiadas pruebas y seguir un guión, pero soy muy desordenado), y otra vez, y volver a Google y leerme decenas de mensajes en listas de correos. Al final me decidí por usar el Amavis.

Pero... oh sorpresa! nuevamente. No hay una versión del Amavis, ni dos, hay tres:

1. [Amavis original](#)⁽³⁾
2. [Amavisd-ng \(next generation\)](#)⁽⁴⁾
3. [Amavisd-new](#)⁽⁵⁾

La verdad es que no entiendo todavía si hay diferencia entre la primera y la segunda, en todo caso los competidores finales eran el amavisd-ng y el amavisd-new. Finalmente [la decisión fue fácil](#)⁽⁶⁾: *me decidí por el amavisd-new*.

Instalación y configuración del Clamav

Para los que os preguntéis, sí, el clamav es totalmente libre y mantienen la base de datos actualizada. Por lo que he podido ver hasta ahora, no sólo es fiable sino que muy rápido y eficiente.

```
apt-get install clamav
```



Eso es todo lo que tuve que hacer, instala los paquetes adicionales clamav-base clamav-freshclam y libclamav1. También os recomiendo otros descompresores que suelen ser usados en algunos virus y también por el amavis para descomprimirlos. Los que yo he puesto son:

```
apt-get install unrar arj lha zoo lzop
```

Si esos paquetes están instalados, serán detectados automáticamente por el clamav y el amavis.

El clamav tiene dos paquetes importantes, el clamav-daemon que incluye lo que el título dice, o sea el demonio ;-), y el freshclam, que es otro demonio que se encarga de mantener la base de datos de "firmas" de virus actualizada. Ambos demonios deben estar siempre en marcha:

```
ponti:~# ps ax | grep clam
 2866 ?    S    0:06 /usr/bin/freshclam --daemon --checks 5
           --quiet --log /var/log/clamav-freshclam.log
           --datadir /var/lib/clamav/
11323 ?    S    0:00 /usr/sbin/clamd
```

De lo anterior ya se ha encargado el proceso de instalación y configuración de Debian. No recuerdo haber hecho nada en especial, salvo dar a todo "OK" y "Yes".

Instalación y configuración del amavisd-new

La instalación es directa, como todo en Debian. Se instalan muchos paquetes de Perl adicionales necesarios (el amavisd-new está programado en Perl, pero es muy eficiente). El amavisd-new ya tiene integrado las funciones de Perl para llamar al spamassassin, por lo que ya no hace falta ejecutar el spamd si es que pasan todos por el amavis (i.e. no se llama al spamassassin desde el Exim).

Para acabar de configurar al amavis sólo hay que hacer dos cosas: editar el fichero de configuración del amavis y luego configurar el exim para que se llame el amavis con los parámetros correctos.

Configurar el amavis

```
vi /etc/amavis/amavisd.conf
```

Ahora os mostraré las líneas que he cambiado y para que sirve cada una de ellas.

```
$mydomain = 'gallimedina.net'; # (no useful default)
```

Defino el nombre del dominio, no es importante para lo funcional, simplemente que los mensajes y cabeceras de correo adicionales llevarán este nombre. Por ejemplo:

```
X-Virus-Scanned: by amavisd-new-20030616-p5 (Debian) at gallimedina.net
```

```
$forward_method = 'smtp:127.0.0.1:10025'; # where to forward checked mail
$notify_method = $forward_method; # where to submit notifications
```

Las dos líneas de arriba indican la forma de comunicación que habrá entre el amavis y el exim. En mi caso es a través del loopback de red local en el puerto 10025. Ya veremos luego como se indica eso mismo en la configuración del Exim.

```
$DO_SYSLOG = 1; # (defaults to false)
```

Quiero hacer el log a través del syslogd (en mi caso, el defecto, irá a /var/log/syslog).

```
$log_level = 2;
```

Puse este nivel para que me salgan las estadísticas de tiempo. Ahora os mostraré una, esos datos son de mi viejo portátil, un Pentium 200, que me hace de servidor hogareño de wireless, cups, DNS, smtp, dhcp, etc.



```
Feb 6 01:59:12 ponti amavis[11217]: (11217-01) Checking: <gallir@origen> ->
<gallir@destino>
Feb 6 01:59:16 ponti amavis[11217]: (11217-01) spam_scan: hits=-4.25
tests=BAYES_00,PLING_PLING
Feb 6 01:59:16 ponti amavis[11217]: (11217-01) FWD via SMTP: [127.0.0.1:10025]
<gallir@origen> -> <gallir@destino>
Feb 6 01:59:16 ponti amavis[11217]: (11217-01) Passed, <gallir@origen> ->
<gallir@destino>, Message-ID: <200402060019.44177.switch;-)@tiscali.es>, Hits:
-4.25
Feb 6 01:59:16 ponti amavis[11217]: (11217-01) TIMING [total 5126 ms] - SMTP
EHLO: 30 (1%), SMTP pre-MAIL: 4 (0%), mkdir tempdir: 26 (1%), create email.txt:
6 (0%), SMTP pre-DATA-flush: 40 (1%), SMTP DATA: 30 (1%), body hash: 14 (0%),
mkdir parts: 11 (0%), mime_decode: 274 (5%), get-file-type: 203 (4%),
decompose_part: 11 (0%), parts: 0 (0%), AV-scan-1: 23 (0%), SA msg read: 25
(0%), SA parse: 49 (1%), SA check: 3705 (72%), fwd-connect: 113 (2%),
fwd-mail-from: 7 (0%), fwd-rcpt-to: 304 (6%), write-header: 111 (2%), fwd-data:
6 (0%), fwd-data-end: 71 (1%), fwd-rundown: 12 (0%), unlink-1-files: 45 (1%),
rundown: 4 (0%)
```

\$final_spam_destiny = D_PASS; # (defaults to D_REJECT)

Dejo pasar los spams, ya que tengo definidas reglas en mi .procmailrc. **Alerta**, si vuestros correos pasan antes por otro MX "cercano" o local (por ejemplo lo bajáis con el fetchmail) **no hagáis un REJECT**, que estaréis tirando piedras a vuestro propio tejado. Dejadlo pasad y luego lo descargaréis.

```
#$virus_admin = "gallir@$mydomain";
```

La línea está comentada, porque **no** quiero que avise a ningún "administrador" que se ha detectado un virus.

```
#$virus_quarantine_to = 'virus-quarantine';
```

También está comentada, **no** quiero dejar los mensajes con virus en cuarentena (sino los deja en /var/lib/amavis/virusmails).

```
#$spam_quarantine_to = 'spam-quarantine';
```

Idem a la anterior.

```
$sa_tag_level_deflt = 4.0; # add spam info headers if at, or above that level
```

```
$sa_tag2_level_deflt = 5.0; # add 'spam detected' headers at that level
```

El amavis usa funciones internas para el spamassassin. Si lo habilitáis, como en mi caso, tenéis que especificar esos dos parámetros indicados (no usa el local.conf el SA). La primera indica el puntaje mínimo que debe tener un mensaje para incluir las cabeceras de "tests" del spamassassin en el mensaje. La segunda es el puntaje mínimo para que sea considerado un spam (por defecto es 6.3).

```
#$sa_spam_subject_tag = '***SPAM***';
```

La línea de arriba está comentada porque no quiero que agregue esas palabras el subject, uso directamente las cabeceras para filtrarlas.

Ya está

Ahora lo podéis para y volver a arrancar y deberéis[*] ver líneas como las siguientes:

[*] La versión actual en Debian tiene un bug, ya lo reporté, en el restart que hace que falle. Haced primero un stop y luego el start.

```
amavis[11210]: starting.
```



```

    amavisd-new at ponti amavisd-new-20030616-p5, Unicode aware
amavis[11210]: Perl version          5.008003
amavis[11210]: Module Amavis::Conf  1.15
amavis[11210]: Module Archive::Tar   1.03
amavis[11210]: Module Archive::Zip   1.05
amavis[11210]: Module Compress::Zlib 1.16
amavis[11210]: Module Convert::TNEF  0.17
amavis[11210]: Module Convert::UULib 1.0
amavis[11210]: Module MIME::Entity   5.404
amavis[11210]: Module MIME::Parser   5.406
amavis[11210]: Module MIME::Tools    5.411
amavis[11210]: Module Mail::Header   1.59
amavis[11210]: Module Mail::Internet 1.59
amavis[11210]: Module Mail::SpamAssassin 2.63
amavis[11210]: Module Net::Cmd        2.24
amavis[11210]: Module Net::SMTP       2.26
amavis[11210]: Module Net::Server     0.85
amavis[11210]: Module Time::HiRes     1.52
amavis[11210]: Module Unix::Syslog    0.100
amavis[11210]: Found myself: /usr/sbin/amavisd-new -c /etc/amavis/amavisd.conf
amavis[11210]: Lookup::SQL code       NOT loaded
amavis[11210]: Lookup::LDAP code      NOT loaded
amavis[11210]: AMCL-in protocol code  NOT loaded
amavis[11210]: SMTP-in protocol code  loaded
amavis[11210]: ANTI-VIRUS code        loaded
amavis[11210]: ANTI-SPAM code         loaded
amavis[11211]: Net::Server: Process Backgrounded
amavis[11211]: Net::Server: 2004/02/06-01:39:23 Amavis
    (type Net::Server::PreForkSimple) starting! pid(11211)
amavis[11211]: Net::Server: Binding to TCP port 10024 on host 127.0.0.1
amavis[11211]: Net::Server: Setting gid to "107 107"
amavis[11211]: Net::Server: Setting uid to "104"
amavis[11211]: Net::Server: Couldn't POSIX::setuid to "104" []
amavis[11211]: Found $file            at /usr/bin/file
amavis[11211]: No $arc,                not using it
amavis[11211]: Found $gzip            at /bin/gzip
amavis[11211]: Found $bzip2           at /usr/bin/bzip2
amavis[11211]: Found $lzop           at /bin/lzop
amavis[11211]: Found $lha            at /usr/bin/lha
amavis[11211]: Found $unarj          at /usr/bin/arj
amavis[11211]: Found $uncompress     at /bin/uncompress
amavis[11211]: No $unfreeze,         not using it
amavis[11211]: Found $unrar          at /usr/bin/unrar
amavis[11211]: Found $zoo            at /usr/bin/zoo
amavis[11211]: Found $cpio           at /bin/cpio
amavis[11211]: Using internal av scanner code for (primary) Clam Antivirus-clamd
amavis[11211]: Found secondary av scanner Clam Antivirus - clamscan at /usr/bin/clamscan
amavis[11211]: SpamControl: initializing Mail::SpamAssassin

```

Si lo anterior os sale correctamente, ya podemos pasar a lo siguiente, configurar el Exim

Configurar el Exim

Los ficheros de configuración para el exim son similares al [explicado para el Spamassassin](#)⁽¹⁾. Sólo que en vez de llamar al spamassassin, llamaremos al amavis que ya debería estar bien configurado. Las pistas para la configuración las obtuve, como no, de `/usr/share/doc/amavisd-new/README.exim_v4`.

ALERTA: Recordad de quitar esos ficheros de configuración si llamáis al spamassassin desde el amavis. No es cuestión de estar haciendo dos veces el mismo trabajo [ineficiente].

Tampoco hace falta el exim4 "heavy", con el "light" es suficiente. Si os [funcionaba el spamassassin "corporativo"](#)⁽¹⁾, seguro que funcionará éste.

Los pasos que haremos serán, casi similares al del spamassassin:

1. Agregar la interfaz con el puerto 10025,



2. agregar un "router" y
3. agregar un transport.

Agregar el puerto 10025

En Debian es fácil, hay que agregar o modificar la variable `dc_local_interfaces` en `/etc/exim4/update-exim4.conf.conf`

```
dc_local_interfaces='0.0.0.0.25 : 127.0.0.1.10025'
```

En caso que tu distro no sea Debian, en el fichero de configuración debes agregar la siguiente línea:

```
local_interfaces = 0.0.0.0.25 : 127.0.0.1.10025
```

Agregar el router

```
# Fichero /etc/exim4/conf.d/router/199_amavis
amavis:
    driver = manualroute
    # No ejecutar si se recibe desde el 10025/tcp
    # o ya está analizado
    condition = "${if or {{eq {$interface_port}{10025}} \
        {eq {$received_protocol}{spam-scanned}} \
        {eq {$sender_address}{}} \
        }}{0}{1}"
    # Sólo escanea los entrantes para el local
    # y para los MX que se hace de relay
    # Si no haceis relay, podéis quitar +relay_to_domains
    domains = +local_domains : +relay_to_domains
    transport = amavis
    route_list = "* localhost byname"
    self = send
# Fin /etc/exim4/conf.d/router/199_amavis
```

Si tu distro no es Debian, puedes copiar y pegar las líneas anteriores en el fichero de configuración del Exim4 justo después de la línea "begin routers". El orden es importante.

Agregar el transport

```
# Fichero /etc/exim4/conf.d/transport/199_amavis
amavis:
    driver = smtp
    port = 10024
    allow_localhost
# Fin /etc/exim4/conf.d/transport/199_amavis
```

Si tu distro no es Debian, puedes copiar y pegar las líneas anteriores en el fichero de configuración del Exim4 después de la línea "begin transports". El orden no es importante.

Re-arrancar el exim

En Debian hay que ejecutar antes el comando `update-exim4.conf` para que genere el fichero definitivo (`/var/lib/exim4/config.autogenerated`) y ya podéis arrancarlo. Por supuesto tenéis que verificar que se arranque y luego enviaros un mensaje. Tenéis que ver en los logs las estadísticas tal como mostré antes y también la línea

```
X-Virus-Scanned: by amavisd-new-20030616-p5 (Debian) at gallimedina.net
```

en la cabecera del mensaje.

Nota final: los ficheros de base de datos Bayesianos del SA y otros ficheros adicionales se crean en el \$HOME del usuario amavis (que lo crea el instalador en Debian). En otras distros, mirad en el \$HOME del usuario del daemons del amavis.



Nada, ya está, son como las tres y media de la madrugada. A pesar que lo sabía casi de memoria me llevó dos horas y media escribir el artículo... y quién sabe los errores tipográficos horribles que tendrá, aunque he tenido mucho cuidado con los "tecnicos", de hecho hice la instalación completa un par de veces para verificar. De todas formas ya me enviaréis los parches seguramente :-).

Lista de enlaces de este artículo:

1. <http://bulma.net/body.phtml?nIdNoticia=1800>
 2. <http://www.clamav.net/>
 3. <http://www.amavis.org/>
 4. http://freshmeat.net/projects/amavis-ng/?topic_id=29
 5. <http://www.ijs.si/software/amavisd/>
 6. <http://www.googlefight.com/cgi-bin/compare.pl?q1=amavis-ng+exim>
-

E-mail del autor: gallir_ARROBA_uib.es

Podrás encontrar este artículo e información adicional en: <http://bulma.net/body.phtml?nIdNoticia=1973>