Manual de instalación de pasarela de correo en Fedora Core 2

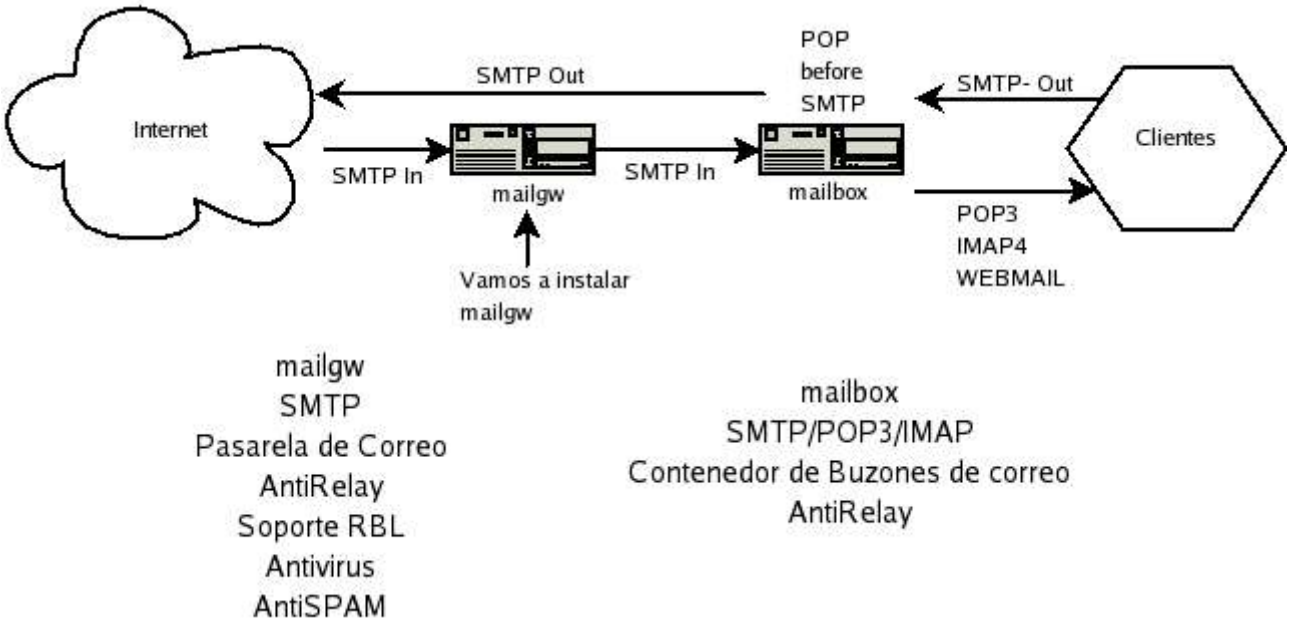
Antivirus + AntiSPAM + AntiRBL + SPF con qmail

Toni de la Fuente Diaz
toni@blyx.com
17/Marzo/2005

El presente documento muestra como configurar una pasarela de correo (SMTP) con soporte Antivirus, AntiSPAM, AntiRBL, SPF y SSL. También instalaremos Awstats, Isoqlog, MRTG-qmail y qmailstats para gestión de estadísticas y generar informes sobre el servicio de correo.

En este servidor no existirá configuración de usuarios ni buzones, simplemente será el servidor que reciba el correo de los dominios especificados y lo reenviará al servidor (backend) con los buzones de los usuarios. Esta pasarela debe ser el MX primario de los dominios que se quieran proteger.

En el siguiente esquema se muestra como quedará nuestra arquitectura de correo:



Basado en la documentación de http://www.qmailrocks.org/

A lo largo del documento se hará uso de la utilidad de gestión de paquetes **apt** para instalarla y configurarla puedes visitar

http://www.blyx.com/comments.php?id=P25_0_1_0_C o
http://dag.wieers.com/apt/

Implementación de la pasarela de correo Antivirus y AntiSPAM:

Inconvenientes:

1. Comprar un servidor (mailgw.blyx.com)
2. Sistema Operativo (Linux Fedora Core 2 = Libre y gratuito)
3. Software de correo (qmail: Libre y gratuito)
4. Satisfacción de los clientes: la migración es transparente para ellos.
5. Tiempo de parada para pase a producción:

-Servicios de correo en mailgw.blyx.com: 10 Minuto

Ventajas:

1. Aumento de la capacidad de entrade de correo (mínimo 10,000 mensajes por hora).
2. Incrementa la protección contra SPAM (reducirá SPAM en un 90%)
3. Más rápido y más estable para los clientes.
4. Redundancia automática de correo (necesario cambios en DNS).

Instalación:

La instalación de las aplicaciones se hacen sobre Fedora Core 2 instalación mínima.

```
# mkdir /root/paquetes
# cd /root/paquetes/
```

Instalación de dependencias:

```
# apt-get install gcc openssl openssl-devel patch patchutils curl libidn gcc-c++
```

Instalamos varios módulos de perl que vamos a necesitar:

```
# apt-get install perl-Digest-HMAC perl-Digest-SHA1 perl-Net-DNS perl-Time-HiRes perl-HTML-Tagset
perl-HTML-Parser
```

Preparamos la descarga de parte del software que necesitamos:

```
# mkdir /downloads
# cd /downloads/
# wget http://www.qmailrocks.org/downloads/qmailrocks.tar.gz
# tar zxvf qmailrocks.tar.gz
# /downloads/qmailrocks/scripts/install/qmr_install_linux-s1.script
Creating initial qmail directories...
Done!
Creating all needed users and groups...
Done!
Unpacking qmail, ucspi-tcp and daemontools...
[...]
All steps completed!
```

```
# /downloads/qmailrocks/scripts/util/qmail_big_patches.script
Applying John Simpson's all in one qmail patch...
[...]
All done!
```

Instalmos y preconfiguramos qmail:

```
# cd /usr/src/qmail/qmail-1.03
# make man && make setup check
# ./config-fast mailgw.blyx.com
# make cert
Country Name (2 letter code) [GB]:ES
State or Province Name (full name) [Berkshire]:GRANADA
Locality Name (eg, city) [Newbury]:GRANADA
Organization Name (eg, company) [My Company Ltd]:Blyx
Organizational Unit Name (eg, section) []:Blyx
Common Name (eg, your name or your server's hostname) []:mailgw.Blyx.com
Email Address []:soporte@Blyx.es
chmod 640 /var/qmail/control/servercert.pem
chown qmaild.qmail /var/qmail/control/servercert.pem
ln -s /var/qmail/control/servercert.pem /var/qmail/control/clientcert.pem

# chown -R vpopmail:qmail /var/qmail/control/clientcert.pem /var/qmail/control/servercert.pem

# cd /usr/src/qmail/ucspi-tcp-0.88/
# patch < /downloads/qmailrocks/patches/ucspi-tcp-0.88.errno.patch
# make && make setup check

# cd /package/admin/daemontools-0.76/src
# patch < /downloads/qmailrocks/patches/daemontools-0.76.errno.patch
# cd /package/admin/daemontools-0.76
# package/install

# ps aux|grep svscanboot
root     29268  0.0  0.0  3852 1000 ?        S    17:03   0:00 /bin/sh /command/svscanboot
```

Todo OK!!! Sigamos!!!

Tenemos que hacer unas modificaciones, para ello creamos el siguiente script para finalizar la instalación:

```
# cd /root/paquetes
# vi finalize_linux.script
#!/bin/sh

echo "This scripts will perform 3 functions:\n

1. Copy all supervise scripts to their proper locations.\n

2. Copy the qmail rc and qmailctl scripts to their proper locations and create needed symlinks.\n

3. Set all needed permisions on all supervise scripts.\n"

echo
echo "Press ENTER to proceeed"
read

echo
sleep 2

echo "Copying supervise scripts to their correct locations..."
echo
sleep 2

cp /downloads/qmailrocks/scripts/finalize/linux/smtpd_run /var/qmail/supervise/qmail-smtpd/run

cp /downloads/qmailrocks/scripts/finalize/linux/smtpd_log /var/qmail/supervise/qmail-smtpd/log/run

cp /downloads/qmailrocks/scripts/finalize/linux/send_run /var/qmail/supervise/qmail-send/run

cp /downloads/qmailrocks/scripts/finalize/linux/send_log /var/qmail/supervise/qmail-send/log/run

echo Done!
echo
sleep 2

echo "Copying rc and qmailctl scripts to proper locations..."
```

```
echo
sleep 2

cp /downloads/qmailrocks/scripts/finalize/rc /var/qmail/

cp /downloads/qmailrocks/scripts/finalize/qmailctl /var/qmail/bin/

echo Done!
echo
sleep 2

echo "Setting needed permisions..."
echo
sleep 2

chmod 755 /var/qmail/rc /var/qmail/bin/qmailctl

chmod 751 /var/qmail/supervise/qmail-smtpd/run
chmod 751 /var/qmail/supervise/qmail-smtpd/log/run

chmod 751 /var/qmail/supervise/qmail-send/run
chmod 751 /var/qmail/supervise/qmail-send/log/run

echo ./Maildir > /var/qmail/control/defaultdelivery

echo 255 > /var/qmail/control/concurrencyremote

chmod 644 /var/qmail/control/concurrencyremote

echo 30 > /var/qmail/control/concurrencyincoming

chmod 644 /var/qmail/control/concurrencyincoming

ln -s /var/qmail/bin/qmailctl /usr/bin

ln -s /var/qmail/supervise/qmail-send /var/qmail/supervise/qmail-smtpd /service

echo "Done!"
echo
sleep 2

echo "Script Complete!"
echo
```

```
# chmod +x finalize_linux.script

# ./finalize_linux.script
This scripts will perform 3 functions:\n

1. Copy all supervise scripts to their proper locations.\n

2. Copy the qmail rc and qmailctl scripts to their proper locations and create needed symlinks.\n

3. Set all needed permisions on all supervise scripts.\n

Press ENTER to proceeed


Copying supervise scripts to their correct locations...

Done!

Copying rc and qmailctl scripts to proper locations...

Done!

Setting needed permisions...

Done!

Script Complete!
```

Comentar las siguientes lineas en /usr/bin/qmailctl

```
##if svok /service/qmail-pop3d ; then
##svc -u /service/qmail-pop3d /service/qmail-pop3d/log
##echo "Starting qmail-pop3d"
##else
##echo "qmail-pop3d supervise not running"
##fi
##echo " qmail-pop3d"
##svc -d /service/qmail-pop3d /service/qmail-pop3d/log
```

```
##svstat /service/qmail-pop3d
##svstat /service/qmail-pop3d/log
##echo "Pausing qmail-pop3d"
##svc -p /service/qmail-pop3d
##echo "Continuing qmail-pop3d"
##svc -c /service/qmail-pop3d
##echo "* Sending qmail-pop3d SIGTERM and restarting."
##svc -t /service/qmail-pop3d /service/qmail-pop3d/log
```

Desabilitamos todo lo referente a pop ya que no vamos a usar ese servicio en la pasarela.

```
# vi /var/qmail/supervise/qmail-smtpd/run
```

En la penúltima linea hay que modificar "mail.example.com" por mailgw.blyx.com

```
# qmailctl stop
Stopping qmail...

 qmail-smtpd
 qmail-send
```

Preparamos el archivo de relays, en este caso permitimos envío de correo desde localhost, la red 192.168.1.0/24 y la IP pública 80.35.159.58:

```
# echo '127.:allow,RELAYCLIENT="" ' >> /etc/tcp.smtp
# echo '192.168.1..:allow,RELAYCLIENT="" ' >> /etc/tcp.smtp
# echo '80.35.159.58:allow,RELAYCLIENT="" ' >> /etc/tcp.smtp
```

Actualizamos el archivo de relays:

```
# qmailctl cdb
Reloaded /etc/tcp.smtp.
```

Creamos los aliases:

```
# echo postmaster@blyx.com > /var/qmail/alias/.qmail-root
# echo postmaster@blyx.com > /var/qmail/alias/.qmail-postmaster
# echo postmaster@blyx.com > /var/qmail/alias/.qmail-mailer-daemon
# echo postmaster@blyx.com > /var/qmail/alias/.qmail-anonymous

# chmod 644 /var/qmail/alias/.qmail*
```

Deshabilitamos sendmail:

```
# /etc/init.d/sendmail stop
# chkconfig sendmail off
# mv /usr/lib/sendmail /usr/lib/sendmail.orig
# mv /usr/sbin/sendmail /usr/sbin/sendmail.orig
# ln -s /var/qmail/bin/sendmail /usr/lib/sendmail
# ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
```

Chequeamos la instalación:

```
# vi /downloads/qmailrocks/scripts/util/qmr_inst_check
CHECKPOP=n


# /downloads/qmailrocks/scripts/util/qmr_inst_check
Congratulations, your Qmailrocks.org Qmail installation looks good!



# qmailctl stop
Stopping qmail...

 qmail-smtpd
 qmail-send

# qmailctl start
Starting qmail...

Starting qmail-send
Starting qmail-smtpd
```

```
# qmailctl stat
/service/qmail-send: up (pid 29587) 3 seconds
/service/qmail-send/log: up (pid 29588) 3 seconds
/service/qmail-smtpd: up (pid 29589) 3 seconds
/service/qmail-smtpd/log: up (pid 29590) 3 seconds
messages in queue: 0
messages in queue but not yet preprocessed: 0

# ln -s /usr/bin/qmailctl /etc/init.d/qmailctl
# chkconfig qmailctl on
# rmdir /var/log/qmail/qmail-pop3d/
```

Comprobamos que todo está correcto:

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mailgw.blyx.com ESMTP
ehlo localhost
250-mailgw.blyx.com
250-AUTH LOGIN CRAM-MD5 PLAIN
250-AUTH=LOGIN CRAM-MD5 PLAIN
250-STARTTLS
250-PIPELINING
250 8BITMIME
starttls
220 ready for tls
quit
quit
Connection closed by foreign host.
```

Instalamos maildrop, lo necesitaremos posteriormente para poder usar antivirus y antispam:

```
# cd /downloads/qmailrocks
# tar zxvf maildrop-1.6.3.tar.gz
# cd maildrop-1.6.3
# ./configure --prefix=/usr/local --exec-prefix=/usr/local --enable-maildrop-uid=root --enable-
maildrop-gid=vchkpw --enable-maildirquota

# make && make install-strip && make install-man
```

Instalación de Antivirus ClamAV y los módulos necesarios

```
# apt-get install perl-suidperl spamassassin

# cd /downloads/qmailrocks/perlmods/source
# tar zxvf Parse-Syslog-1.03.tar.gz
# cd Parse-Syslog-1.03
# perl Makefile.PL
# make
# make install

# cd /downloads/qmailrocks/perlmods/source
# tar zxvf Statistics-Distributions-1.02.tar.gz
# cd Statistics-Distributions-1.02
# perl Makefile.PL
# make
# make install
```

Comprobamos que tenemos todos los módulos de perl necesarios instalados:

```
# /downloads/qmailrocks/scripts/util/check_perlmods.script


QMR check_perlmods v1.1

Checking for the existence of needed perl modules...

checking for Time::HiRes...
/usr/lib/perl5/vendor_perl/5.8.3/i386-linux-thread-multi/Time/HiRes.pm

checking for Net::DNS...
/usr/lib/perl5/vendor_perl/5.8.3/i386-linux-thread-multi/Net/DNS.pm
```

```
checking for Digest::SHA1...
/usr/lib/perl5/vendor_perl/5.8.3/i386-linux-thread-multi/Digest/SHA1.pm

checking for Digest::HMAC...
/usr/lib/perl5/vendor_perl/5.8.3/Digest/HMAC.pm

checking for HTML::Tagset...
/usr/lib/perl5/vendor_perl/5.8.3/HTML/Tagset.pm

checking for HTML::Parser...
/usr/lib/perl5/vendor_perl/5.8.3/i386-linux-thread-multi/HTML/Parser.pm

checking for Mail::SpamAssassin...
/usr/lib/perl5/vendor_perl/5.8.3/Mail/SpamAssassin.pm

checking for Pod::Usage...
/usr/lib/perl5/5.8.3/Pod/Usage.pm

checking for Parse::Syslog...
/usr/lib/perl5/site_perl/5.8.3/Parse/Syslog.pm

checking for Statistics::Distributions...
/usr/lib/perl5/site_perl/5.8.3/Statistics/Distributions.pm

Check Complete.
```

```
# apt-get install clamav clamav-devel clamd
```

Editar /etc/clamd.conf y modificar el atributo User clamav a User **qscand**.

```
# useradd -c "Qmail-Scanner Account" -s /bin/false qscand

# /etc/init.d/clamd start
Starting Clam AntiVirus Daemon:                            [  OK  ]
```

Actualizamos el antivirus:

```
# /usr/bin/freshclam -l /var/log/clamav/clam-update.log
ClamAV update process started at Wed Mar 16 18:57:59 2005
main.cvd is up to date (version: 30, sigs: 31086, f-level: 4, builder: tkojm)
daily.cvd is up to date (version: 762, sigs: 520, f-level: 4, builder: ccordes)

# crontab -e
# Actualizamos el antivirus todos los dias a las 1:25h AM
25 1 * * * /usr/bin/freshclam --quiet -l /var/log/clamav/freshclam.log

# chkconfig clamd on
```

Instalación de Spamassassin

```
# groupadd spamd
# useradd -g spamd -s /home/spamd spamd

# vi /etc/sysconfig/spamassassin
# Options to spamd
SPAMDOPTIONS="-x -u spamd -H /home/spamd -d"

# vi /etc/mail/spamassassin/local.cf
```

Comprueba la directiva:

```
required_hits 5

# /etc/rc.d/init.d/spamassassin start
# ps axuwf|grep spamd
spamd    31250  2.2  2.0 26636 21212 ?       S    09:24   0:00 /usr/bin/spamd -x -u spamd -H /
home/spamd -d

# chkconfig spamassassin on
```

Integración ClamAV con spamassassin para qmail:

```
# cd /downloads/qmailrocks
# tar zxvf qmail-scanner-1.25.tgz
# tar zxvf qms-analog-0.4.2.tar.gz
# cd qms-analog-0.4.2
# make all
# cp qmail-scanner-1.25-st-qms-20050219.patch /downloads/qmailrocks/qmail-scanner-1.25
# cd /downloads/qmailrocks/qmail-scanner-1.25
# patch -p1 < qmail-scanner-1.25-st-qms-20050219.patch
```

Modificar las siguientes lineas de qms-config:

```
# vi qms-config
 --domain blyx.com \
 --local-domains "blyx.com" \

# chmod +x qms-config

# ./qms-config

Building Qmail-Scanner 1.25-st-qms...


                ***** NOTE ******

Qmail-Scanner doesn't have language translations for es_ES.UTF-8,
- so defaulting to english...

[Hit <RETURN> to continue]



This script will search your system for the virus scanners it knows
about, and will ensure that all external programs
qmail-scanner-queue.pl uses are explicitly pathed for performance
reasons.


It will then generate qmail-scanner-queue.pl - it is up to you to install it
correctly.

Continue? ([Y]/N)
Y
Searching ..............................qms-monitor = no

===============================================================
The following binaries and scanners were found on your system:
===============================================================


mimeunpacker=/usr/local/bin/reformime

Content/Virus Scanners installed on your System

clamdscan=/usr/bin/clamdscan (which means clamscan won't be used as clamdscan is better)
fast_spamassassin=/usr/bin/spamc

Qmail-Scanner details.

qms-log=yes
log-details=syslog
log-crypto=0
fix-mime=2
ignore-eol-check=1
debug=0
notify=admin
redundant-scanning=yes
block-password-protected=0
virus-admin=postmaster@Blyx.com
local-domains='Blyx.com'
silent-
viruses='klez','bugbear','hybris','yaha','braid','nimda','tanatos','sobig','winevar','palyh','fizzer
','gibe','cailont','lovelorn','swen','dumaru','sober','hawawi','hawaii','holar-
i','mimail','poffer','bagle','worm.galil','mydoom','worm.sco','tanx','novarg','\@mm','cissy','cissi'
,'qizy','bugler','dloade','netsky','spam'
scanners="clamdscan_scanner","fast_spamassassin"

-------------------------------------
```

```
st: configuration options for  1.25st
-------------------------------------
admin-fromname='System Anti-Virus Administrator'
minidebug=1
scanners-per-domain=0
dscr-hdrs-text='X-Antivirus-MYDOMAIN'

sa-subject=":SPAM:"

sa-delta  =0
sa-alt    =1
sa-debug  =0    (only valid if sa-alt is enabled)
sa-report =0    (only valid if sa-alt and sa-debug are enabled)

Spamassasin Required_Hits=5.0
sa-quarantine=0         (no mail will be quarantined)
sa-delete    =0         (no mail will be deleted/rejected)
sa-reject    =0
---------------------------------------------------------------------------

If that looks correct, I will now generate qmail-scanner-queue.pl
for your system...
Continue? ([Y]/N)
Y
Testing suid nature of /usr/bin/perl...
Looks OK...

Finished. Please read README(.html) and then go over the script to
check paths/etc, and then install as you see fit.

Remember to copy quarantine-attachments.txt to /var/spool/qmailscan and then
run "qmail-scanner-queue.pl -g" to generate DB version.



              ****** FINAL TEST ******

Please log into an unpriviledged account and run
/var/qmail/bin/qmail-scanner-queue.pl -g

If you see the error "Can't do setuid", or "Permission denied", then
refer to the FAQ.

(e.g.  "setuidgid qmaild /var/qmail/bin/qmail-scanner-queue.pl -g")


That's it! To report success:

   % (echo 'First M. Last'; cat SYSDEF)|mail jhaar-s4vstats@crom.trimble.co.nz
Replace First M. Last with your name.



# ./qms-config install

Building Qmail-Scanner 1.25-st-qms...


                ***** NOTE ******

Qmail-Scanner doesn't have language translations for es_ES.UTF-8,
- so defaulting to english...

[Hit <RETURN> to continue]



This script will search your system for the virus scanners it knows
about, and will ensure that all external programs
qmail-scanner-queue.pl uses are explicitly pathed for performance
reasons.

Continue? ([Y]/N)
Y
Searching ..............................qms-monitor = no

==============================================================
The following binaries and scanners were found on your system:
==============================================================


mimeunpacker=/usr/local/bin/reformime

Content/Virus Scanners installed on your System
```

```
clamdscan=/usr/bin/clamdscan (which means clamscan won't be used as clamdscan is better)
fast_spamassassin=/usr/bin/spamc

Qmail-Scanner details.

qms-log=yes
log-details=syslog
log-crypto=0
fix-mime=2
ignore-eol-check=1
debug=0
notify=admin
redundant-scanning=yes
block-password-protected=0
virus-admin=postmaster@Blyx.com
local-domains='Blyx.com'
silent-
viruses='klez','bugbear','hybris','yaha','braid','nimda','tanatos','sobig','winevar','palyh','fizzer
','gibe','cailont','lovelorn','swen','dumaru','sober','hawawi','hawaii','holar-
i','mimail','poffer','bagle','worm.galil','mydoom','worm.sco','tanx','novarg','\@mm','cissy','cissi'
,'qizy','bugler','dloade','netsky','spam'
scanners="clamdscan_scanner","fast_spamassassin"

-------------------------------------
st: configuration options for  1.25st
-------------------------------------
admin-fromname='System Anti-Virus Administrator'
minidebug=1
scanners-per-domain=0
dscr-hdrs-text='X-Antivirus-MYDOMAIN'

sa-subject=":SPAM:"

sa-delta  =0
sa-alt    =1
sa-debug  =0    (only valid if sa-alt is enabled)
sa-report =0    (only valid if sa-alt and sa-debug are enabled)

Spamassasin Required_Hits=5.0
sa-quarantine=0         (no mail will be quarantined)
sa-delete    =0         (no mail will be deleted/rejected)
sa-reject    =0
---------------------------------------------------------------------------

If that looks correct, I will now generate qmail-scanner-queue.pl
for your system...
Continue? ([Y]/N)
Y
Testing suid nature of /usr/bin/perl...
Looks OK...
Hit RETURN to create initial directory structure under /var/spool/qmailscan,
and install qmail-scanner-queue.pl under /var/qmail/bin:
perlscanner: generate new DB file from /var/spool/qmailscan/quarantine-attachments.txt
perlscanner: total of 81 entries.

Finished installation of initial directory structure for Qmail-Scanner
under /var/spool/qmailscan and qmail-scanner-queue.pl under /var/qmail/bin.

Finished. Please read README(.html) and then go over the script
(/var/qmail/bin/qmail-scanner-queue.pl) to check paths/etc.

"/var/qmail/bin/qmail-scanner-queue.pl -r" should return some well-known virus
definitions to show that the internal perlscanner component is working.

If you're upgrading, remember that your previous quarantine-attachments.txt file
has not been changed, maybe it's a good idea to have a look at the file
coming with this distribution.

That's it!


              ****** FINAL TEST ******

Please log into an unpriviledged account and run
/var/qmail/bin/qmail-scanner-queue.pl -g

If you see the error "Can't do setuid", or "Permission denied", then
refer to the FAQ.

(e.g.  "setuidgid qmaild /var/qmail/bin/qmail-scanner-queue.pl -g")
```

```
That's it! To report success:

   % (echo 'First M. Last'; cat SYSDEF)|mail jhaar-s4vstats@crom.trimble.co.nz
Replace First M. Last with your name.
```

Para probar la instalación de qmail-scanner ejecuta el comando siguiente y no deberías recibir ninguna salida:

```
# setuidgid qscand /var/qmail/bin/qmail-scanner-queue.pl -z

# setuidgid qscand /var/qmail/bin/qmail-scanner-queue.pl -g
perlscanner: generate new DB file from /var/spool/qmailscan/quarantine-attachments.txt
perlscanner: total of 81 entries.
```

```
# chown -R qscand:qscand /var/spool/qmailscan
```

Añade/modifica los valores en negrita:

```
# cat /var/qmail/supervise/qmail-smtpd/run
#!/bin/sh
QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl" export QMAILQUEUE
QMAILDUID=`id -u vpopmail`
NOFILESGID=`id -g vpopmail`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
LOCAL=`head -1 /var/qmail/control/me`
if [ -z "$QMAILDUID" -o -z "$NOFILESGID" -o -z "$MAXSMTPD" -o -z "$LOCAL" ]; then
echo QMAILDUID, NOFILESGID, MAXSMTPD, or LOCAL is unset in
echo /var/qmail/supervise/qmail-smtpd/run
exit 1
fi
if [ ! -f /var/qmail/control/rcpthosts ]; then
echo "No /var/qmail/control/rcpthosts!"
echo "Refusing to start SMTP listener because it'll create an open relay"
exit 1
fi
exec /usr/local/bin/softlimit -m 40000000 \
/usr/local/bin/tcpserver -v -R -l "$LOCAL" -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" \
-u "$QMAILDUID" -g "$NOFILESGID" 0 smtp \
/var/qmail/bin/qmail-smtpd mailgw.blyx.com \
/home/vpopmail/bin/vchkpw /usr/bin/true 2>&1
```

```
# qmailctl stop
# qmailctl start
# qmailctl stat

# cd /downloads/qmailrocks/qmail-scanner-1.25/contrib
# chmod +x test_installation.sh
# ./test_installation.sh -doit
QMAILQUEUE was not set, defaulting to /var/qmail/bin/qmail-scanner-queue.pl for this test...

Sending standard test message - no viruses...
done!

Sending eicar test virus - should be caught by perlscanner module...
done!

Sending eicar test virus with altered filename - should only be caught by commercial anti-virus
modules (if you have any)...

Sending bad spam message for anti-spam testing - In case you are using SpamAssassin...
Done!

Finished test. Now go and check Email for postmaster@Blyx.com
```

Revisa el correo de postmaster@blyx.com para ver los mails enviados, deberías haber recibido dos correos.

En el directorio `/var/spool/qmailscan/quarantine/new/` debería haber otros dos correos.

Personalizar el escaneo de archivos (cabeceras de correos)

```
# vi /var/qmail/bin/qmail-scanner-queue.pl
```

```
##my $V_HEADER="X-Antivirus-MYDOMAIN";
my $V_HEADER="X-Antivirus-Blyx";

##my $V_FROMNAME="System Anti-Virus Administrator";
my $V_FROMNAME="Administrador del Sistema Anti-Virus/Anti-SPAM";

my $spamc_subject=":::SPAM:::";

$sa_delete='1.0';
```

Explicación de $sa_delete:

Ahora substituye el ' 0 ' por un número que represente los "required_hits" de SpamAssassin que indica cuando qmail-scanner elimina los mensajes. Por ejemplo, si la variable “required_hits” de SpamAssassin fuese "5" y usted fijara a la variable "sa_delete" el valor "1.0", entonces cualquier mensaje que tenga un valor de Spam que excediera de 1.0 a la marca "5" sería suprimido. Es decir cualquier correo con una cuenta de 6 o más sería borrado automáticamente.

Gestión de logs e informes:

```
# cd /downloads/qmailrocks
# tar zxvf qmailanalog-0.70.tar.gz
# cd qmailanalog-0.70
# patch < /downloads/qmailrocks/patches/0.70-errno.patch
# make && make setup check

# cd /downloads/qmailrocks/
# tar zxvf qlogtools-3.1.tar.gz
# cd qlogtools-3.1
# patch < /downloads/qmailrocks/patches/qlogtools_errno.patch
# make
# ./installer

# cp /downloads/qmailrocks/qms-analog-0.4.2/qmailstats /var/qmail/bin

# vi /var/qmail/bin/qmailstats
cat /var/log/qmail/qmail-send/* /var/log/qmail/qmail-smtpd/* | tai64n2tai | awk '{$1=substr
($1,1,index($1,".")+6);print}' | matchup > $QMAILSTATS 5>/dev/null
echo "To: sistemas@Blyx.es" > $EMAILMSG
echo "From: postmaster@Blyx.com" >> $EMAILMSG
echo "Subject: Estadisticas de Qmail en mailgw.blyx.com $DATE" >> $EMAILMSG

# chmod 750 /var/qmail/bin/qmailstats
```

Vamos a aplicar un parche que hemos hecho para añadir en el informe que nos envía diariamente un Top-50-Virus-Found, es decir los 50 virus más “famosillos” y las veces que han sido detectados por el servidor.

Descargamos el parche:

```
# cd /root/paquetes/
# wget http://blyx.com/public/pasarelamail/qmailstats-top-virus.patch

# cd /var/qmail/bin/
# patch -p0 < /root/paquetes/qmailstats-top-virus.patch
patching file qmailstats
```

Ejecutamos el script y miramos el correo:

```
# /var/qmail/bin/qmailstats
```

Añadimos la siguiente entrada en el crontab de root:

```
# crontab -e
# Generamos y enviamos el informe del servidor a las 3:00h AM
0 3 * * * /var/qmail/bin/qmailstats 1>/dev/null 2>/dev/null
```

Configuración de SPF:

```
# cd /var/qmail/control
# echo 3 > spfbehavior

# cat <<EOF> spfexp
> 550 Ha enviado su correo a traves de un servidor no autorizado, visite
http://spf.pobox.com/why.html?sender=%{S}&ip=%{I}&receiver=%{xR}.
> 550 Your mail has been sent trought not allow server, see http://spf.pobox.com/why.html?sender=%
{S}&ip=%{I}&receiver=%{xR}.
> EOF
```

Recuerda añadir el registro SPF en la zona de tu dominio, más info en http://www.blyx.com/comments.php?id=P60_0_1_0 y en http://www.blyx.com/comments.php?id=P59_0_1_0

Configuración de RBL:

```
# vi /var/qmail/supervise/qmail-smtpd/run
#!/bin/sh
QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl" export QMAILQUEUE
QMAILDUID=`id -u vpopmail`
NOFILESGID=`id -g vpopmail`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
LOCAL=`head -1 /var/qmail/control/me`
if [ -z "$QMAILDUID" -o -z "$NOFILESGID" -o -z "$MAXSMTPD" -o -z "$LOCAL" ]; then
echo QMAILDUID, NOFILESGID, MAXSMTPD, or LOCAL is unset in
echo /var/qmail/supervise/qmail-smtpd/run
exit 1
fi
if [ ! -f /var/qmail/control/rcpthosts ]; then
echo "No /var/qmail/control/rcpthosts!"
echo "Refusing to start SMTP listener because it'll create an open relay"
exit 1
fi
exec /usr/local/bin/softlimit -m 40000000 \
/usr/local/bin/tcpserver -v -R -l "$LOCAL" -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" \
-u "$QMAILDUID" -g "$NOFILESGID" 0 smtp \
/usr/local/bin/rblsmtpd -r relays.ordb.org \
/var/qmail/bin/qmail-smtpd mailgw.blyx.com \
/home/vpopmail/bin/vchkpw /usr/bin/true 2>&1
```

Mantenimiento de la cola de correo:

```
# cd /root/paquetes/
# wget http://www.enfocados.net/public/practica2/qmqtool-current.tgz
# tar zxvf qmqtool-current.tgz
# cd qmqtool-1.03/
# vi qmqtool
#!/usr/bin/perl
# cp qmqtool /var/qmail/bin/
# chmod +x /var/qmail/bin/qmqtool

# /var/qmail/bin/qmqtool -s
Messages in local queue: 0
Messages in remote queue: 0
Messages in todo queue: 0
```

Esta aplicación tiene muchas opciones muy útiles, ejecutala sin parámetros para ver la capacidad de esta utilidad.

Estadísticas:

AWSTATS

```
# apt-get install httpd mod_ssl awstats
# chkconfig httpd on

# vi /etc/httpd/conf.d/awstats.conf
Alias /awstats/icon/ /var/www/awstats/icon/

ScriptAlias /awstats/ /var/www/awstats/
<Directory /var/www/awstats/>
        DirectoryIndex awstats.pl
        Options ExecCGI
        order allow, deny
        allow from all
</Directory>

#Alias /css/ /var/www/awstats/css/
#Alias /js/ /var/www/awstats/js/




# /etc/init.d/httpd start

# cp /etc/awstats/awstats.model.conf /etc/awstats/awstats.mailgw.blyx.com.conf

# cd /var/www/awstats/

# vi /etc/awstats/awstats.mailgw.blyx.com.conf
LogFile="/usr/local/bin/tai64nlocal < /var/log/qmail/qmail-send/current | /usr/bin/maillogconvert.pl
standard |"
LogType=M
LogFormat="%time2 %email %email_r %host %host_r %method %url %code %bytesd"
DirData="/var/www/awstats"
DirCgi="/awstats"
DirIcons="/awstats/icon"
SiteDomain=mailgw.blyx.com
HostAliases="localhost 127.0.0.1 mailgw.blyx.com"
LevelForBrowsersDetection=0=0
LevelForOSDetection=0
LevelForRefererAnalyze=0
LevelForRobotsDetection=0
LevelForWormsDetection=0
LevelForSearchEnginesDetection=0
LevelForFileTypesDetection=0
ShowMenu=1
ShowMonthStats=HB
ShowDaysOfMonthStats=HB
ShowDaysOfWeekStats=HB
ShowHoursStats=HB
ShowDomainsStats=0
ShowHostsStats=HBL
ShowAuthenticatedUsers=0
ShowRobotsStats=0
ShowEMailSenders=HBML
ShowEMailReceivers=HBML
ShowSessionsStats=0
ShowPagesStats=0
ShowFileTypesStats=0
ShowFileSizesStats=0
ShowBrowsersStats=0
ShowOSStats=0
ShowOriginStats=0
ShowKeyphrasesStats=0
ShowKeywordsStats=0
ShowMiscStats=0
ShowHTTPErrorsStats=0
ShowSMTPErrorsStats=1

# ./awstats.pl config=mailgw.blyx.com update
Update for config "/etc/awstats/awstats.mailgw.blyx.com.conf"
With data in log file "/usr/local/bin/tai64nlocal < /var/log/qmail/qmail-send/current | /
usr/bin/maillogconvert.pl standard |"...
Phase 1 : First bypass old records, searching new record...
Searching new records from beginning of log file...
Phase 2 : Now process new records (Flush history on disk after 20000 hosts)...
Jumped lines in file: 0
Parsed lines in file: 8
 Found 0 dropped records,
 Found 0 corrupted records,
 Found 0 old records,
 Found 8 new qualified records.
```

https://mailgw.blyx.com/awstats/awstats.pl

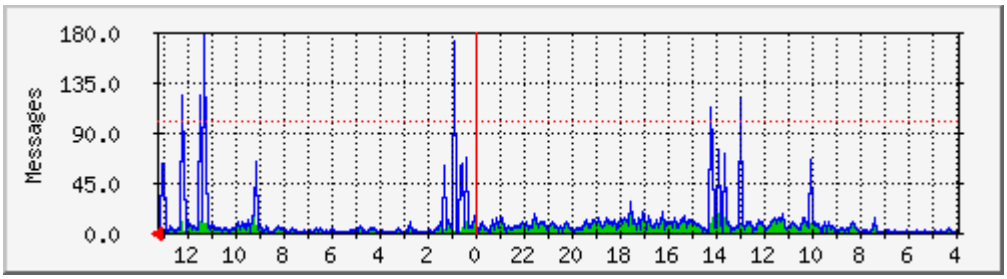
ISOQLOG

```
# wget http://www.enderunix.org/isoqlog/isoqlog-2.2.tar.gz

# tar zxvf isoqlog-2.2.tar.gz
# cd isoqlog-2.2
# ./configure
# make
# make install
# make clean

# mkdir /var/www/html/isoqlog
# cp -pr isoqlog/htmltemp/images isoqlog/htmltemp/library /var/www/html/isoqlog/

#
# vi /usr/local/etc/isoqlog.conf
#isoqlog Configuration file

logtype     = "qmail-multilog"                          # log type qmai-multilog, qmail-syslog,
sendmail, postfix
logstore    = "/var/log/qmail/qmail-send"                                   #
domainsfile = "/usr/local/etc/isoqlog.domains"          #
outputdir   = "/var/www/html/isoqlog"                   # html output directory
htmldir     = "/usr/local/share/isoqlog/htmltemp"
langfile    = "/usr/local/share/isoqlog/lang/spanish"
hostname    = "mailgw.blyx.com"
maxsender   = 100
maxreceiver = 100
maxtotal    = 100
maxbyte     = 100

# cp /usr/local/etc/isoqlog.domains-dist /usr/local/etc/isoqlog.domains
# cat /var/qmail/control/rcpthosts > /usr/local/etc/isoqlog.domains


# vi /etc/cron.hourly/01isoqlog
#!/bin/bash
/usr/local/bin/isoqlog

# chmod +x /etc/cron.hourly/01isoqlog
```

https://mailgw.blyx.com/isoqlog/

MRTG-QMAIL

Generación de gráficas de estado de nuestro servidor. Ejemplo sobre los mensages recibidos diariamente:



cd /root/paquetes
wget http://x42.com/qmail/mrtg/qmail-mrtg-0.1.tar.gz
apt-get install mrtg
/etc/init.d/httpd restart

mkdir /var/www/html/qmailmrtg
cd /var/www/html/qmailmrtg/
tar zxvf /root/paquetes/qmail-mrtg-0.1.tar.gz
cp /var/www/mrtg/*.gif .

Modificamos el archivo de configuración mrtg.cfg que hay en el directorio donde nos encontramos para que refleje el nombre de nuestro dominio principal, con vi se hace así:

```
# vi mrtg.cfg
:1,$s/example.com/blyx.com/g
```

En negrita las modificaciones que debes hacer en el fichero:

```
WorkDir: /var/www/html/qmailmrtg
##############################################################

Title[messages]: blyx.com - qmail message throughput
MaxBytes[messages]: 100
AbsMax[messages]: 10000
Options[messages]: gauge
Target[messages]: `/usr/local/bin/qmail-mrtg-mess /var/log/qmail/qmail-send`
PageTop[messages]: <H1>blyxcom - qmail message throughput</H1>
ShortLegend[messages]: Messages
YLegend[messages]: Messages
Legend1[messages]: Total messages
LegendI[messages]:  Deliveries:
LegendO[messages]:  Attempts:
WithPeak[messages]: ymwd

#-------------------------------------------------------------------

Title[queue-size]: blyx.com - qmail queue size
MaxBytes[queue-size]: 1000
AbsMax[queue-size]: 10000
Options[queue-size]: gauge
Target[queue-size]: `/usr/local/bin/qmail-mrtg-queue`
PageTop[queue-size]: <H1>blyx.com - qmail queue size</H1>
ShortLegend[queue-size]: Messages
YLegend[queue-size]: Messages
Legend1[queue-size]: Messages
LegendI[queue-size]:  Messages:
LegendO[queue-size]:  Unprocessed Messages:
WithPeak[queue-size]: ymwd

#-------------------------------------------------------------------

Title[concurrency]: blyx.com - qmail concurrency
MaxBytes[concurrency]: 1000
AbsMax[concurrency]: 10000
Options[concurrency]: gauge
Target[concurrency]: `/usr/local/bin/qmail-mrtg-concurrency /var/log/qmail/qmail-send`
PageTop[concurrency]: <H1>blyx.com - qmail concurrency</H1>
ShortLegend[concurrency]: Concurrency
YLegend[concurrency]: Concurrency
Legend1[concurrency]: Concurrency
LegendI[concurrency]:  Local:
LegendO[concurrency]:  Remote:
WithPeak[concurrency]: ymwd

#-------------------------------------------------------------------
```

```
# cp qmail-mrtg-* /usr/local/bin/
```

Para probarlo ejecutamos:

```
# env LANG=C /usr/bin/mrtg /var/www/html/qmailmrtg/mrtg.cfg
```

Probablemente recibas errores y avisos (warnings) pero no son preocupantes, son relacionados con la poca cantidad de logs que tenemos al principio.

Ajustamos el crontab de root para que se ejecute cada 5 minutos:

```
# crontab -e
# Generacion de graficas mrtg cada 5 minutos:
0,5,10,15,20,25,30,35,40,45,50,55 * * * * env LANG=C /usr/bin/mrtg /var/www/html/qmailmrtg/mrtg.cfg
```

Creamos en index.html para nuestras estadísticas:

```
# indexmaker --output=index.html –title=mailgw.blyx.com mrtg.cfg
```

Ya podemos ver nuestras estadísticas de correo en la siguiente URL:
https://mailgw.blyx.com/qmailmrtg/

Anotaciones:

Los correos con virus se encuentran en /var/spool/qmailscan/quarantine/new

Los logs del Antivirus se encuentran en /var/log/clamav/clamd.log
Los logs de qmail (correo saliente) /var/log/qmail/qmail-send/current
Los logs de qmail (correo entrante) /var/log/qmail/qmail-smtpd/current

Recuerda abrir en el firewall local para la entrada de tráfico a través de los puertos 25TCP qmail, 783TCP spamassassin, 80TCP http y 443TCP https.

En el firewall perimetral (si lo tienes) debes abrir 25TCP qmail y 783TCP spamassassin. Los puertos 80 y 443 TCP para las IP o redes de gestión nunca para todo Internet.

Creación de las rutas de correo:

Para que el servidor reenvíe el correo entrante al servidor con los buzones mailbox.blyx.com debemos especificarlo de la siguiente forma:

```
# cd /var/qmail/control/
# vi smtproutes
blyx.com:mailbox.blyx.com
miotrodominio.com:mailbox.blyx.com
otrodominio.net:mailbox1.nostracom.com
```

Recueda añadir esos dominios al archivo rcpthosts:

```
# vi rcpthosts
mailgw.blyx.com
blyx.com
miotrodominio.com
otrodominio.net

# qmailctl reload
Sending HUP signal to qmail-send.
```

Probando el sistema de correo:

```
# telnet mailgw.blyx.com 25
Trying 192.168.1.227...
Connected to mailgw.blyx.com.
Escape character is '^]'.
220 mailgw.blyx.com ESMTP
ehlo blyx.com
250-mailgw.blyx.com
250-AUTH LOGIN CRAM-MD5 PLAIN
250-AUTH=LOGIN CRAM-MD5 PLAIN
```

```
250-STARTTLS
250-PIPELINING
250 8BITMIME
mail from: unacuenta@yahoo.com
250 ok
rcpt to: toni@blyx.es
250 ok
data
354 go ahead
Esto es una prueba de correo

.
250 ok 1111059688 qp 31731
quit
221 mailgw.blyx.com
Connection closed by foreign host.
```

Deberemos recibir un correo que aparentemente está en blanco pero si pinchamos en “ver cabeceras completas” podemos ver los siguiente:

```
Return-Path: <toniblyx@gmail.com>
Delivered-To: Blyx.es-toni@Blyx.es
Received: (qmail 9317 invoked by uid 508); 17 Mar 2005 11:40:01 -0000
Received: from unknown (HELO mailgw.blyx.com) (212.163.145.131) by
mailbox1.Blyx.com with SMTP; 17 Mar 2005 11:40:01 -0000
Received: (qmail 31739 invoked by uid 509); 17 Mar 2005 12:41:28 +0100
Received: from 192.168.1.227 by mailgw.blyx.com (envelope-from
<toniblyx@gmail.com>, uid 508) with qmail-scanner-1.25-st-qms (clamdscan:
0.83/764. spamassassin: 2.64. perlscan: 1.25-st-qms.
Clear:RC:0(192.168.1.227):SA:0(2.9/5.0):. Processed in 2.748286 secs); 17
Mar 2005 11:41:28 -0000
X-Spam-Status: No, hits=2.9 required=5.0
X-Spam-Level: ++
X-Antivirus-Blyx-Mail-From: unacuenta@yahoo.com via mailgw.blyx.com
X-Antivirus-Blyx: 1.25-st-qms
(Clear:RC:0(192.168.1.227):SA:0(2.9/5.0):. Processed in 2.748286 secs
Process 31731)
Received: from unknown (HELO Blyx.com) (192.168.1.227) by
mailgw.blyx.com with SMTP; 17 Mar 2005 12:41:25 +0100
Received-SPF: pass (mailgw.blyx.com: local policy designates
192.168.1.227 as permitted sender)
X-Antivirus-Blyx-Message-ID: <1111059687107231731@mailgw.blyx.com>
X-Evolution-Source: pop://afuente%40Blyx.es@pop.Blyx.com/
From:
Date: Thu, 17 Mar 2005 12:42:36 +0100
Subject: No Subject
Message-Id: <1111059756.6938.175.camel@flame.Blyx.com>
Mime-Version: 1.0
```

Apendice: (1/Abril/2005)

Instalación de Razor, utilidad para filtrar spam:

```
# apt-get install perl-Razor-Agent razor-agents
```

Creamos el directorio de configuración y los archivos de configuración:

```
# razor-client
# razor-admin -d -create -home=/etc/razor
```

Deberíamos ver muchas líneas ya que está actualizandose y por último una linea como la siguiente:

```
razor-admin finished successfully.
```

Instalación de DCC:

```
# cd /root/paquetes
# wget http://www.rhyolite.com/anti-spam/dcc/source/dcc.tar.Z
# tar zxvf dcc.tar.Z
# cd dcc-1.2.74/
# ./configure && make && make install
# cdcc 'info'
```

Activamos estas aplicaciones en spamassassin:

```
# vi /etc/mail/spamassassin/local.cf
use_razor2 1
use_dcc 1
dcc_add_header 1
use_bayes 1
bayes_auto_learn 1

# /etc/init.d/spamassassin restart
```

Podremos ver archivos referentes a los filtros bayesianos y a razor en el home del usuario spamd /home/spamd, directorios .spamassassin y .razor

Y eso es todo amigos!!! ;P

Este documento puedes copiarlo, modificarlo, ampliarlo y mejorarlo, incluso lo puedes traducir a otros idiomas si quieres, pero recuerda que debes poner una reseña a Toni de la Fuente Diaz y a blyx.com.

Toni de la Fuente Diaz
toni@blyx.com
05/Mayo/2005