Actualización de los servicios de red en el OAN

P. de Vicente

Informe Técnico IT-OAN 2004-x

Índice

1. Introducción

Este informe describe la actualización de algunos servicios de la red del OAN desde Debian 3.0 a Debian 3.1. En el momento de la redacción de este informe la distribución 3.1 estaba en pruebas y se esperaba su congelación en breve. Los Se han modificado el servicio de correo y el DNS (resolución de nombres). También se ha instalado un servidor HTTP seguro y un servidor Twiki.

2. Filosofía del filtrado de mensajes

Debian 3.1 incluye la versión 4 de *Exim*. *Exim* es un MTA (Mail Transport Agent), es decir una estafeta de correo electrónico que permite integrar con facilidad el filtrado de correo basura y de mensajes que contengan virus.

Existen dos modos de explorar los mensajes que llegan a un MTA:

- Aceptar todos los mensajes, filtrarlos y, admitirlos o rechazarlos según su contenido.
- Explorar los mensajes según llegan y rechazarlos durante la negociación SMTP si contienen correo basura o virus.

El primero método se suele utilizar para integrar *Spamassassin* en *Exim 3*. *Exim* recibe los mensajes, los almacena en la cola, se los entrega a sí mismo y los procesa en el filtro del transporte. Este filtro pasa el mensaje por una tubería que dirige el mensaje a *Spamassassin* y nuevamente de vuelta a *Exim* utilizando BSMTP (Batch SMTP). Al recibir de nuevo el mensaje lo encola, pero esta vez ya lleva la etiqueta que indica que ha sido revisado por *Spamassassin* de modo que entrega el mensaje por segunda vez pero sin volver a ejecutar *Spamassassin*. Este procedimiento implica que *Exim* procesa dos veces cada mensaje y realiza una exploración en busca de correo basura por cada destinatario.

La segunda opción es posible gracias al nuevo diseño de *Exim 4*. Una vez que el servidor remoto se conecta con el MTA y entrega la cabecera y el cuerpo del mensaje, *Exim 4* explora el mensaje completo y toma la decisión de rechazarlo o entregarlo ante de enviar la confirmación SMTP final. Si decide rechazarlo envía una instrucción SMTP de rechazo y devuelve el mensaje al remitente incluyendo información adicional. La ventaja de este método es que sólo procesa una vez cada mensaje y lo hace independientemente del número de destinatarios que haya. Es necesario advertir que esta política puede generar más tráfico con nuestro servidor y con la red en general aunque si todos los MTAs en Internet empleasen la misma política se reduciría el tráfico global de spam. Es posible que esta opción suponga una mayor carga a la CPU por lo costoso del proceso.

Existen dos paquetes que permiten integrar en *Exim* el filtrado de mensajes:

- *ExiScan-ACL*. Se trata de una modificación a *Exim* que permite explorar virus, correo basura y otros tipos de información. Es sencillo de configurar y no permite ajustes muy complicados.

- *SA-Exim*. Permite explorar sólo correo basura y realizar una configuración más detallada que en el caso anterior. Por ejemplo SA-Exim permite almacenar el correo basura en un archivo.

Ambas soluciones pueden coexistir sin problemas. Por ejemplo se puede emplear la primera para explorar virus y la segunda para correo basura. En la solución que se describe en este informe se ha utilizado *Exiscan-ACL* tanto para filtrar correo basura como virus.

3. Spamassassin

Spamassassin es un filtro de correo que se utiliza para identificar correo basura (conocido habitualmente como spam), desarrollado por el grupo que desarrolla el servidor web Apache. En la actualidad existen diferentes aplicaciones para filtrar correo basura, como *bogofilter*, *spamprobe*, *crm114*, pero de todas ellas la más conocida es *Spamassassin*. Dado que en el OAN ya disponemos de una experiencia de 2 años en su uso se ha seguido utilizando. Para disponer de él en Debian se deben instalar los siguientes paquetes:

- *spamassassin*. Perl-based spam filter using text analysis
- *spamc*. Client for perl-based spam filtering daemon
- *razor*. spam-catcher using a collaborative filtering network

El primer paquete contiene *Spamassassin* y el segundo una versión de esa misma aplicación que funciona como demonio y, por tanto, se ejecuta desconectada de los terminales y de los usuarios. Esta opción es recomendable cuando se emplea en estafetas de correo electrónico.

El comportamiento de *Spamassassin* se puede mejorar instalando el paquete Debian *Razor* que hace una consulta a una base de datos donde se mantiene información proporcionada por usuarios de toda la red de mensajes de correo basura recientes. No es necesario cambiar la configuración de *Spamassassin* ni de *Razor* para que ambos funcionen conjuntamente.

La configuración de *Spamassassin* se hace en dos archivos diferentes:

- `/etc/spamassassin/local.cnf`. Este archivo contiene instrucciones para el uso de *Spamassassin*. Habitualmente las opciones predefinidas son las adecuadas por lo que apenas deberemos añadir nuevas opciones. Nuestra configuración es la siguiente:

```
report_safe 0
bayes_path /var/mail/.spamassassin/bayes
bayes_file_mode 0664
# Fuera los mensajes que no estén en inglés, francés o español
# italiano, alemán o catalán
ok_languages en es fr ca it de
# Con 4 de puntuación los mensajes son considerados spam
required_hits 4.0
```

`report_safe 1` indica que el cuerpo del mensaje original se adjuntará como archivo y el cuerpo nuevo contendrá el informe de Spamassassin. En este caso lo ponemos a 0 porque *Exiscan-ACL* no soporta esta opción. Las opciones relacionadas con las reglas bayesianas sirven para indicar el lugar donde se encuentra la base de datos con los mensajes aprendidos. La opción:

```
bayes\_path /var/mail/.spamassassin/bayes
```

indica que los archivos se encuentran en el directorio `/var/mail/.spamassassin` y comienzan por `bayes`.

- `/etc/default/spamassassin`. Contiene instrucciones con información para ejecutar el demonio spamd. Aquí se pueden especificar las opciones de lanzamiento del demonio. Por ejemplo una de las opciones más útiles es la que activa el modo de depuración. Se consigue añadiendo la opción `-D`. La información de depuración se escribe en `/var/log/mail.info` y permite analizar los pasos que sigue spamassassin para clasificar y puntuar mensajes. Una vez hayamos conseguido nuestro objetivo es conveniente eliminar esta opción para evitar un crecimiento desmesurado de los archivos de registro. Las opciones que se emplean en el OAN son las siguientes:

```
# Change to one to enable spamd
#PdV
ENABLED=1

# Options
# See man spamd for possible options. The -d option is
# automatically added.
OPTIONS="-c -m 10 -a -H"

# Set nice level of spamd
#NICE="--nicelevel 15"
```

Spamassassin se puede poner en marcha, detener o reiniciar con el siguiente comando:

```
/etc/init.d/spamassassin start|stop|restart
```

donde las opciones separadas por "|" son incompatibles entre sí. Es decir se elegirá la opción `start` o `stop` o `restart`. Al ejecutar `start` se pondrá en marcha un demonio que escucha en el puerto TCP 783 a través del cual se comunicará con *Exim 4*. El demonio es propiedad de 'root'. Este detalle es importante porque si activamos el aprendizaje con reglas bayesianas es necesario que el propietario del proceso tenga acceso al directorio donde colocamos la base de datos con mensajes basura (spam) y mensajes válidos (ham).

Para poner en marcha los filtros bayesianos es necesario crear un directorio que aloje la información con la base de datos y colocar los permisos adecuados. En este caso el directorio

debería pertenecer al usuario 'Debian-exim' porque *Exim* lanza a *Spamassassin* (esto no está claro porque el demonio va por su cuenta). ¿Hay que lanzar el demonio como usuario Debian-exim?

El comportamiento de *Spamassassin* se puede mejorar instalando el paquete Debian *Razor* que hace una consulta a una base de datos donde se mantiene información procedente de muchos usuarios de Internet que informan de los mensajes de correo que consideran basura. No es necesario cambiar la configuración de *Spamassassin* ni de *Razor* para que ambos funcionen adecuadamente. Si queremos informar al centro de recogida de spam de *Razor* es necesario registrarse previamente empleando la instrucción:

```
razor-register
```

Para dar parte de la existencia de spam se emplea la instrucción:

```
razor-report
```

La integración de *Spamassassin* en *Exim 4* se realiza gracias a *Exiscan-ACL* y su filosofía se ha descrito en la sección anterior.

4. Antivirus: clamav

Exiscan-ACL soporta directamente varios exploradores de virus y permite, indirectamente, utilizar otros más a través de la configuración de exploración en línea. Los antivirus más comunes, que se implementan cargando un demonio en memoria son *Clam Antivirus*, *Sophos Antivirus*, *Kaspersky Antivirus* y *ScannerDaemon*. En nuestro caso emplearemos la primera solución ya que es software libre y para la que existen paquetes Debian.

La primera operación consiste en instalar los siguientes paquetes:

- *clamav*. Antivirus scanner for Unix
- *clamav-base*. Base package for clamav, an anti-virus utility for U
- *clamav-freshclam*. Downloads clamav virus databases from the Internet
- *clamav-daemon*. Powerful Antivirus scanner daemon

El paquete *clamav-freshclam* instala un demonio que obtiene de modo regular a través de Internet (cada hora) una base de datos de virus nuevos. La configuración de este paquete se hace en el proceso de postinstalación, y las respuestas más adecuadas son las predefinidas. Al igual que todos los paquetes se puede reconfigurar a posteriori empleando *dpkg-reconfigure*. El archivo de configuración se guarda en `/etc/clamv/freshclam.conf` y la base de datos de antivirus en `/var/lib/clamav/`.

El demonio se pone en marcha introduciendo la instrucción:

```
/etc/init.d/clamav-freshclam start
```

El archivo de configuración actual para `clamav-freshclam` está en `/etc/clamav/freshclam.conf` y contiene las siguientes opciones:

```
# Automatically created by the clamav-freshclam postinst
# Comments will get lost when you reconfigure the
# clamav-freshclam package

DatabaseOwner clamav
UpdateLogFile /var/log/clamav/freshclam.log
LogFileMaxSize 0
MaxAttempts 5
# Check for new database 24 times a day
Checks 24
DatabaseMirror db.es.clamav.net
DatabaseMirror database.clamav.net
DatabaseDirectory /var/lib/clamav/
NotifyClamd
DNSDatabaseInfo current.cvd.clamav.net
```

Como se puede observar la base de datos se actualiza cada hora contra una réplica española del servidor central. El explorador de virus deja traza de su proceso en el directorio `/var/log/clamav/freshclam.log`

Para facilitar la operación con Exim4 es conveniente instalar un demonio preparado para ejecutarse permanentemente y capaz de atender varias peticiones de análisis de virus. El paquete *clamav-daemon* requiere una configuración más detallada, aunque la configuración predefinida es adecuada. En nuestro caso la configuración es la siguiente:

```
TCPSocket 3310
TCPAddr 127.0.0.1
User clamav
AllowSupplementaryGroups
ScanMail
ScanArchive
ArchiveMaxRecursion 5
ArchiveMaxFiles 1000
ArchiveMaxFileSize 10M
ReadTimeout 300
MaxThreads 20
MaxConnectionQueueLength 30
StreamMaxLength 20M
LogFile /var/log/clamd.log
LogTime
LogFileMaxSize 2M
PidFile /var/run/clamav/clamd.pid
DatabaseDirectory /var/lib/clamav
TemporaryDirectory /var/tmp
SelfCheck 3600
```

Para poner en marcha el demonio es necesario introducir:

```
/etc/init.d/clamav-daemon start
```

Cuando reiniciemos ”clamav-daemon” es muy importante verificar que realmente el demonio ha sido detenido y luego arrancado. Durante la instalación esto no suele ocurrir y a veces es necesario matar el proceso manualmente empleando:

```
killall clamd
```

Es posible emplear sockets Unix en lugar de sockets TCP para la comunicación entre *Exim 4* y *Clamav*. En ese caso el archivo de configuración debería disponer de una entrada de este tipo:

```
LocalSocket /var/spool/exim4/clamd.sock
User Debian-exim
```

y en `/etc/exim4/exim4.conf.template` hay que añadir:

```
av_scanner = clamd:/var/spool/exim/clamd.sock
```

La traza con la información sobre los virus encontrados junto con la marca temporal de la detección del virus se guarda en el archivo de registro `/var/log/clamd.log`.

5. Actualización de Exim.

Exim es el MTA (Mail Transport Agent) que se ha venido utilizando en el OAN desde hace varios años. La instalación de Debian 3.1 permite la posibilidad de instalar *Exim 3* o *Exim 4*. En el OAN se optó por pasar a *Exim 4* porque permite un filtrado más sencillo de los mensajes e integra mucho mejor antivirus y detectores de correo basura. *Exim 4* introduce una directiva denominada ACL (Access Control List) que deja obsoletas algunas directivas antiguas y por tanto el archivo de configuración de *Exim 3* no es válido para *Exim 4*.

La instalación de *Exim 4* requiere la instalación de los siguientes paquetes:

- *exim4* An MTA (Mail Transport Agent)
- *exim4-base* EXperimental Internal Mailer – a Mail Transport Age
- *exim4-config* Debian configuration for exim4
- *exim4-daemon-heavy* Exim (v4) with extended features, including exiscan-ACL
- *exim4-doc-html* Documentation for Exim v4 in html format
- *eximon4* X monitor for the Exim (v4) mail transport agent

Al instalarse estos paquetes, si *Exim 3* estuviera previamente instalado se desinstalaría, ya que ambas versiones son incompatibles.

Existen dos paquetes que proporcionan el demonio de *Exim 4*, `exim4-daemon-heavy` y `exim4-daemon-light`. El primero de ellos es el que necesitamos para las estafetas de correo ya que integra soporte para LDAP, PostgreSQL y MySQL, así como autentificación SPA para SMTP y un intérprete integrado de Perl. También incluye el parche *Exiscan-ACL* que

permite integrar *Spamassassin* y los detectores de antivirus. En el resto de los ordenadores se instalará el paquete `exim4-daemon-light`

Durante la instalación se deben seleccionar las opciones más adecuadas para cada equipo. En el OAN la configuración difiere si los equipos son:

- las estafetas de correo, en cuyo caso elegimos la opción *el ordenador está conectado directamente a Internet*
- ordenadores normales, en cuyo caso elegimos *el ordenador envía mensajes empleando un smarthost*. El ”smarthost” en ese caso es una de las estafetas de correo electrónico del OAN.

En caso de error durante la instalación de los paquetes de *Exim 4* se pueden reajustar las preferencias ejecutando:

```
dpkg-reconfigure exim4-config
```

Las principales diferencias a tener en cuenta entre *Exim 3* y *Exim 4* son las siguientes:

- El directorio de configuración de *Exim 4* es `/etc/exim4`
- El directorio de registro de *Exim 4* es `/var/log/exim4`
- El directorio de almacenaje de mensajes por entregar es `/var/spool/exim4`
- El usuario que gestiona *Exim 4* es “Debian-exim”.
- La ejecución de *Exim 4* se realiza por omisión empleando un demonio exclusivo en lugar de ejecutarlo desde “inetd”. En este caso cada cambio en los archivos de configuración, incluido `/etc/aliases` requiere reiniciar el demonio con la instrucción:

  ```
  /etc/init.d/exim4 restart
  ```

5.1. Configuración de Exim 4

La configuración de *Exim 4* en Debian también es diferente respecto de *Exim 3*. Las opciones de configuración elegidas duante el proceso de instalación son las siguientes:

```
dc_eximconfig_configtype='internet'
dc_other_hostnames='hercules.oan.es'
dc_local_interfaces=''
dc_readhost=''
dc_relay_domains=''
dc_minimaldns='false'
dc_relay_nets='193.146.252.0/16'
dc_smarthost=''
CFILEMODE='644'
dc_use_split_config='false'
dc_hide_mailname='false'
```

Estas opciones se guardan en el archivo `/etc/exim4/exim4.conf.conf`.
El ajuste fino de la configuración se realiza en otros archivos.

- Si la opción `dc_use_split_config='true'` el resto de la configuración se hace empleando unos 40 archivos situados en el directorio `/etc/exim4/conf.d`.
- Si la opción `dc_use_split_config='false'` el resto de la configuración se hace en el archivo `/etc/exim4/exim4.template`. En el OAN se eligió la segunda opción por ser más compacta.

El archivo `/etc/exim4/exim4.template` contiene en su parte inicial una serie de opciones "rodeadas" por el prefijo y sufijo `DEBCONF`, que sirven para indicar que los valores de esas variables se tomarán del fichero `/etc/exim4/exim4.conf.conf`. El resto de las variables se editan manualmente y algunas de ellas se describen a continuación. *Exim 4* interpreta adecuadamente algunas de estas opciones gracias al *Exiscan-ACL*. Si no estuviese instalado se generaría un error. Las opciones añadidas son las siguientes:

- En la parte final de la sección 03 y antes de la sección de ACL, introduciremos las siguientes dos opciones:

```
#########################################################
### end main/03_exim4-config_tlsoptions
#########################################################

# Spamassassin
spamd_address=127.0.0.1 783

# Clam Antivirus
av_scanner = clamd:127.0.0.1 3310
```

  Con ellas indicamos a *Exim 4* qué ordenador ('127.0.0.1' indica que es el propio servidor) y en qué puerto escuchan las aplicaciones de detección de correo basura y antivirus. El demonio de *Spamassassin* escucha en el puerto 783 y el antivirus *clamav* en el puerto 3310.

- En la sección '40_exim4-config_check_data' incluimos una opción para rechazar archivos MIME incorrectos:

```
# MIMEs incorrectos
# referencia: http://www.timj.co.uk/linux/Exim-SpamAndVirusScanning.pdf
deny message = This message contains malformed MIME ($demime_reason)
     demime = *
     condition = ${if > {$demime_errorlevel}{2}{1}{0}}
```

  La anterior opción indica que si el error supera el nivel 2 el mensaje es rechazado con el mensaje que se indica al comienzo.

- En la misma sección, y a continuación, incluimos una opción para rechazar los mensajes que lleven archivos adjuntos del tipo: bat, com, exe, pif, prf, scr o vbs.

```
# Bloqueo de adjuntos con las siguientes extensiones
deny message = Blacklisted file extension detected (.$found_extension)
     demime = bat:com:exe:pif:prf:scr:vbs
```

- En la misma sección, más abajo, incluimos las siguientes opciones para rechazar los mensajes de spam:

```
# Los que superen la puntuación de 7.0 (7 * 10) los rechazamos.
deny message = This message scored $spam_score spam points.
     spam = nobody:true
     condition = ${if > {$spam_score_int}{70}{1}{0}}

# Todos los mensajes son marcados con puntuación, al ponerle :true
warn message = X-Spam-Score: $spam_score
     spam = nobody:true

# Solo los mensajes que dan positivo en spamassassin se les pone
# el flag a Yes y se adjunta el informe.
warn message = X-Spam-Flag: YES
     spam = nobody
warn message = X-Spam-Report: $spam_report
     spam = nobody
```

  La primera regla indica que si la puntuación del mensaje supera los 7 puntos el mensaje se rechaza enviando un mensaje que es el que se indica en la parte superior.

  La segunda regla indica que todos los mensajes van a llevar en la cabecera un campo con la puntuación que le ha dado *Spamassassin*.

  La tercera regla indica que sólo los mensajes que Spamassassin considera spam llevarán en la cabecera la etiqueta: `X-Spam-Flag: YES` y el informe producido por *Spamassassin*.

  La opción `spam=nobody` indica que *Spamassassin* va a explorar los mensajes de todos los usuarios y que el resultado puede ser verdadero (true) o falso (false) y que sólo en caso de que sea verdadero se incluye un mensaje de advertencia.

  La opción `spam=nobody:true` indica que *Spamassassin* va a explorar los mensajes de todos los usuarios y que el resultado es siempre verdadero y por tanto se incluirá siempre un mensaje de advertencia con el resultado de la puntuación.

- En la misma sección y a continuación incluimos la siguiente opción para rechazar los mensajes que contienen virus:

```
#Antivirus
deny message = This message contains a virus or other harmful content ($mal
     demime = *
     malware = *
```

- Finalmente en la sección de reescritura (`rewrite/31_exim4-config_rewriting`) incluimos una directiva para que todos aquellos mensajes que lleven como dominio de remitente ”*oan.es” sean sustituidos por ”oan.es”. Esto impide que el remitente del mensaje sea del tipo: `usuario@maquina.oan.es` y lo transforma automáticamente en `usuario@oan.es`. Esta opción es necesaria porque los mensajes del primer tipo tienen una alta probabilidad de ser rechazados al no poder comprobar el MTA del destinatario el nombre del dominio ”maquina.oan.es”.

```
# Reescribimos la dirección de remite
*@*oan.es       $1@oan.es  frFs
```

Para que todas las opciones sean leidas por *Exim 4* es necesario ejecutar el programa

```
update-exim4.conf
```

- Si la opción `dc_use_split_config='false'` entonces `update-exim4.conf` lee el archivo `/etc/exim4/update-exim4.conf.conf` y `exim4.conf.template`.
- Si la opción `dc_use_split_config='false'` entonces `update-exim4.conf` lee los archivos en el directorio `/etc/exim4/conf.d` y `exim4.conf.template`.

La configuración final se escribe en el archivo `/var/lib/exim4/config.autogenerated`, que es el archivo que el demonio de *Exim 4* utiliza realmente para su operación.

5.2. Mantenimiento de Exim 4

Para forzar el arranque de la cola se debe ejecutar:

```
exim -qf
```

Si algún tipo de mensaje se bloquea es posible ejecutar *Exim 4* manualmente pasando la dirección del destinatario con el que se produce el problema y obtener información de depuración:

```
exim -bt -d usuario@maquina.com
```

6. Servidores POP3 e IMAP

Con Debian 3.1 se han dejado de utilizar los antiguos paquetes *ipopd* e *imap* porque las contraseñas de los usuarios se transmitían en claro y se encontraron algunos problemas de acceso desde los clientes de correo.

En su lugar hemos instalado un conjunto de paquetes del grupo ”Courier”. Se han instalado los siguientes paquetes en las estafetas de correo electrónico:

- *courier-authdaemon* Courier Mail Server - Authentication daemon
- *courier-base* Courier Mail Server - Base system

- *courier-imap* Courier Mail Server - IMAP server
- *courier-imap-ssl* Courier Mail Server - IMAP over SSL
- *courier-pop* Courier Mail Server - POP3 server
- *courier-pop-ssl* Courier Mail Server - POP3 over SSL
- *courier-ssl* Courier Mail Server - SSL/TLS Support
- *courier-webadmin* Courier Mail Server - Web-based administration front

Durante el proceso de instalación se genera un certificado X509 para poder utilizar comunicaciones cifradas SSL entre el servidor y el cliente empleando POP e IMAP. Este certificado se hace empleando las opciones que se introducen durante la instalación. Si deseamos cambiar el certificado es necesario ejecutar:

```
/usr/sbin/mkpop3dcert
```

o bien

```
/usr/sbin/mkimap3dcert
```

empleando las opciones que se encuentran en el fichero `/etc/pop3d.cnf` y `/etc/imap.cnf`. Este certificado está autofirmado y el procedimiento ortodoxo es que una autoridad reconocida vise dicho certificado.

El modo de trabajo de los servidores POP e IMAP difiere de los antiguos servidores POP e IMAP. La principal diferencia radica en el lugar de almacenamiento de los mensajes recien llegados. Con las aplicaciones servidoras anteriores los mensajes se escribían en formato ”mbox” en el directorio `/var/spool/mail/` y se generaba un fichero por cada usuario con el nombre de dicho usuario. Con el nuevo sistema los mensajes se almacenan en el directorio `/home/usuario/Maildir` y se genera un fichero por mensaje. El directorio `/home/usuario/Maildir` dispone de tres subdirectorios: `new`, `cur` y `tmp`. En `new` se almacenan los archivos recién llegados y en `cur` los archivos leídos. Este formato se conoce como ”Maildir”.

Esta estructura, si no existe, se crea automáticamente al recibir el usuario un nuevo mensaje. Es posible hacer que los nuevos usuarios dispongan de esta estructura modificando del siguiente modo el archivo `/etc/skel....`

Para que los clientes de correo encuentren los mensajes en los directorios donde se depositan es necesario realizar las siguientes modificaciones:

- Archivo: `/etc/pam.d/ssh`

```
#PdV
session    optional     pam_mail.so standard noenv dir=~Maildir
```

- Archivo `/etc/pam.d/login`

```
#PdV
session    optional   pam_mail.so standard noenv dir=~Maildir
```

- Archivo `/etc/login.defs`

```
QMAIL_DIR      Maildir/
#MAIL_DIR        /var/mail
MAIL_FILE      .mail
```

Tras estas modificaciones los clientes de correo que empleen POP encontrarán los nuevos mensajes en los subdirectorios `Maildir` de cada usuario. Una excepción a este comportamiento se produce si los usuarios disponen de un fichero `.procmail` o `.procmailrc` en el directorio principal.

Si los usuarios disponen de un archivo `.procmailrc` *Exim 4* entrega el mensaje a *procmail* que lo procesa de acuerdo con las instrucciones que figuren en dicho archivo. En ese caso puede ocurrir que los mensajes se guarden en `/var/spool/mail` o vayan a parar a `home/usuario/Maildir`.

7. Servidor seguro Apache

En la siguiente sección se describe la instalación y configuración de webmail, un interfaz web de correo. Para que este servidor funcione con la mayor seguridad es necesario instalar un servidor web que permita la transferencia de las contraseñas cifradas entre el cliente y el servidor, usando SSL.

La instalación del servidor apache seguro se realiza instalando los paquetes:

- *apache-ssl*. Versatile, high-performance HTTP server with SSL support
- *ssl-cert*. Simple debconf wrapper for openssl

Durante la instalación se solicita información para generar un certificado autofirmado que permita la negociación entre los navegadores y el servidor web.

El servidor Apache seguro escucha en el puerto 443. Esta información es muy importante porque permite abrir el puerto 443 en el router para un cierto ordenador manteniendo cerrado el puerto 80 (HTTP) para ese mismo ordenador.

Si se encontrara algún tipo de errro en la configuración de Apache podemos ejecutar:

```
apache-sslctl configtest
```

para depurar dicha configuración.

8. Webmail

Para facilitar la consulta de mensajes de correo desde el exterior por el personal del OAN se ha instalado un interfaz que permite gestionar el correo desde un navegador. En esta sección describimos el procedimiento para instalar y configurar *sqwebmail* una aplicación del grupo de paquetes *courier*.

En primer lugar es necesario instalar el paquete:

- *sqwebmail*. Courier Mail Server - Webmail server

Durante la instalación se nos solicitará saber si deseamos copiar, enlazar o crear manualmente un directorio de plantillas web; elegir copiar, si bien la configuración de *sqwebmail* está mal planificada y tendremos que modificar manualmente esta configuración después. El resto de las preguntas se pueden contestar dejando la opción predefinida.

Para configurar correctamente ”sqwebmail” se deben seguir los siguientes pasos:

- Añadir la siguiente directiva en el archivo `/etc/apache-ssl/httpd.conf`

  ```
  <Directory /var/www/webmail>
  SetEnv SQWEBMAIL_TEMPLATEDIR /var/www/webmailTempl
  ```

  Donde `var/www/webmail` es el directorio raíz del servidor HTTPS.

- Añadir los siguientes módulos en el archivo `/etc/apache-ssl/modules.conf`:

  ```
  LoadModule env_module /usr/lib/apache/1.3/mod_env.so
  LoadModule auth_module /usr/lib/apache/1.3/mod_auth_ssl.so
  ```

  El primer módulo permite que Apache comprenda la opción `SetEnv` anterior. El segundo módulo permite el uso de formularios en los que se envían usuarios y contraseñas de estos.

- Reiniciar el servidor apache:

  ```
  /etc/init.d/apache-sslctl restart
  ```

- Modificar el permiso de ejecución del script `/usr/lib/cgi-bin/sqwebmail` poniendo SUID:

  ```
  chmod a+s /usr/lib/cgi-bin/sqwebmail
  ```

- Crear los directorios siguientes, modificar el propietario y copiar los archivos con las plantillas al directorio de destino:

  ```
  mkdir /var/www/webmailTempl
  mkdir /var/www/webmailTempl/en-us
  cd /var/www/webmailTempl
  ln -s en-us en
  ln -s en-us es
  cp /usr/lib/courier/sqwebmail/html/en-us/* en-us/
  chown -R www-data.www-data /var/www/webmailTempl
  ```

  Podemos modificar las plantillas una vez copiadads, traduciendolas, por ejemplo al español. También debemos cambiar el propietario del directorio al que solemos usar para todo el contenido de la web.

- Mover el directorio `sqwebmail` al directorio raíz del servidor HTTPS, que en nuestro caso es `var/www/webmail/`, porque en el residen todas las imágenes que necesita la aplicación servidora *sqwebmail*, y es allí donde se buscan.
- Finalmente para poder acceder al servicio apuntar el navegador a la dirección `https://conga.oan.es`

Como el correo se recibe en las estafetas es necesario que los servidores web estén en cada una de las tres estafetas de correo. Para que los usuarios del OAN puedan acceder a sus cuentas de correo utilizando el navegador se ha preparado una página común `https://webmail.oan.es` que reenvia a los usuarios a cada una de las máquinas correspondientes:

- http://conga.oan.es/cgi-bin/sqwebmail.cgi
- http://zeus.oan.es/cgi-bin/sqwebmail.cgi
- http://mercurio.oan.es/cgi-bin/sqwebmail.cgi

9. DNS

Se ha modificado el servicio de nombres dividiendo en dos áreas el dominio del oan. Para ello se ha utilizado la opción `view`. La configuración en `/etc/bind/named.conf` es la siguiente:

```
view "internal" {// This should match our internal networks.
match-clients { 193.146.252.0/8; };
// Provide recursive service to internal clients only.
recursion yes;


// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};
```

```
zone "0.in-addr.arpa" {
         type master;
         file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
         type master;
         file "/etc/bind/db.255";
};

zone "oan.es" {
        type master;
        file "/etc/bind/db.oan-private";
};

zone "252.146.193.in-addr.arpa" {
        type master;
        file "/etc/bind/db.252.146.193-private";
};

};

view "external" {
match-clients { any; };
// Refuse recursive service to external clients.
recursion no;
zone "oan.es" {
        type master;
        file "/etc/bind/db.oan";
};

zone "252.146.193.in-addr.arpa" {
        type master;
        file "/etc/bind/db.252.146.193";
};
};
```

La parte pública del OAN se guarda en la sección “external” y la parte privada en la “internal. Como se puede apreciar los archivos con la asignación de números IP en función de los nombres son diferentes para cada sección:

- Parte pública: Direcciones directas: `/etc/bind/db.oan`, direcciones reversas: `/etc/bind/db.252`
- Parte privada: Direcciones directas: `/etc/bind/db.oan-private`, direcciones reversas: `/etc/bind/db.252.146.193-private`.

10. Twiki

Referencias

[1] http://dman.ddts.net/ dman/config_docs/exim4_spamassassin.html

[2] http://dman13.dyndns.org/ dman/config_docs/exim-spamassassin/node1.html

[3] http://www.timj.co.uk/linux/Exim-SpamAndVirusScanning.pdf

[4] http://duncanthrax.net/exiscan-acl/

[5] http://spamassassin.apache.org/