Sistema de correo con Postfix, OpenLDAP, Courier ((POP3&&IMAP) + SSL), SASL, Spamassassin, Amavis-new y SquirrelMail

Sergio González González
Instituto Politécnico de Bragrança (http://www.ipb.pt/), Portugal

sergio.gonzalez@hispalinux.es

Sistema de correo con Postfix, OpenLDAP, Courier ((POP3&&IMAP) + SSL), SASL, Spamassassin, Amavis-new y SquirrelMail
por Sergio González González

Trabajo realizado para la asignatura *Comunicações por Computador 2* perteneciente a la carrera *Ingeniería Informática* impartida en la Escola Superior de Tecnologia e de Gestão de Bragança (http://www.estig.ipb.pt/) del Instituto Politécnico de Bragrança (http://www.ipb.pt/), Portugal.

Esta documentación muestra la forma de montar un sistema de correo con las siguientes características: servidor SMTP con autentificación para el envío de correos; servidor POP3 e IMAP para la recepción de correos; así como servicio de webmail, antivirus y control de SPAM. Este conjunto de herramientas ha de funcionar sobre LDAP.

Historial de revisiones
Revisión 0.1 3-06-2004 Revisado por: sgg

Tabla de contenidos

Lista de figuras

Lista de ejemplos

I. Introducción

Introducción

Esta documentación muestra la forma de instalar y configurar un sistema SMTP con autentificación; para lo cual se utilizará el servidor Postfix como servidor SMTP y SASL (Simple Authentication and Security Layer) como sistema de autentificación.

Todo el correo que pase a través del servidor SMTP será revisado en busca de virus y SPAM. Para llevar a cabo esta tarea se utilizará AMaViSd-new como interfaz entre el servidor de correo SMTP y las aplicaciones Clamav y Spamassassin, las cuales analizarán el correo en busca de virus y SPAM respectivamente.

El sistema de correo final dispondrá de un servidor POP3 e IMAP, para lo cual se hará uso del software *Courier*.

Otra de las funcionalidades a implementar será el correo a través de la web, o webmail. SquirrelMail ha sido el software elegido para dar este servicio.

Todos los servicios han de funcionar con LDAP. Esta documentación supondrá que se tiene un directorio LDAP correctamente instalado y configurado. La herramienta de administración del directorio LDAP será phpLDAPadmin, que también se supondrá instalada, así como las herramientas de administración que provee OpenLDAP.

Se hace notar que la instalación de todos los servicios va a tener lugar en un sistema Debian GNU/Linux, en su versión en desarrollo (aka Sid).

> **Nota:** Los servicios SMTP, POP3 e IMAP tendrán activada la opción de encriptación, es decir, podrán hacer uso del protocolo SSL o TLS para la transferencia de información.

II. Postfix

Capítulo 1. Instalación

Introducción

Esta sección está dedicada a la instalación de Postfix, en su versión 2.1.1. (versión que viene con la distribución en desarrollo de Debian GNU/Linux - aka Sid -).

Se van a utilizar las características de integración con LDAP y SASL que posee Postfix. En las siguientes secciones se verá el proceso de instalación y configuración de Postfix.

Selección e instalación de paquetes

Para dar el servicio SMTP con Postfix, se han de instalar los siguientes paquetes: postfix, postfix-ldap y postfix-tls. El primero de ellos es el servidor SMTP en sí; *postfix-ldap* y *postfix-tls* son librerías que permiten a Postfix hacer uso de un directorio LDAP así como permitir la autentificación por TLS y SASL, respectivamente.

La descripción de los paquetes se puede ver en el siguiente ejemplo:

Ejemplo 1-1. Descripción de los paquetes *postfix*, *postfix-ldap* y *postfix-tls*

```
# /usr/bin/apt-cache show postfix postfix-ldap postfix-tls
Package: postfix
Priority: extra
Section: mail
Installed-Size: 1908
Maintainer: LaMont Jones <lamont@debian.org>
Architecture: i386
Version: 2.1.1-3
Replaces: postfix-doc (<< 1.1.7-0), postfix-tls
Provides: mail-transport-agent
Depends: libc6 (>= 2.3.2.ds1-4), libdb4.2, debconf (>= 0.5), netbase,
adduser (>= 3.48), dpkg (>= 1.8.3), debconf
Recommends: mail-reader, resolvconf
Suggests: procmail, postfix-mysql, postfix-pgsql, postfix-ldap, postfix-pcre
Conflicts: mail-transport-agent, smail, libnss-db (<< 2.2-3), postfix-tls (<< 1.1.0+tls0.7.15-0)
Filename: pool/main/p/postfix/postfix_2.1.1-3_i386.deb
Size: 764672
MD5sum: f0025b1bdaef4be6622ee94850c86236
Description: A high-performance mail transport agent
 Postfix is Wietse Venema's mail transport agent that started life as an
 alternative to the widely-used Sendmail program.  Postfix attempts to
 be fast, easy to administer, and secure, while at the same time being
 sendmail compatible enough to not upset existing users. Thus, the outside
 has a sendmail-ish flavor, but the inside is completely different.
 .
 This package does not have SASL or TLS support.  For SASL and TLS support,
 install postfix-tls.

Package: postfix-ldap
Priority: extra
Section: mail
Installed-Size: 100
Maintainer: LaMont Jones <lamont@debian.org>
```

```
Architecture: i386
Source: postfix
Version: 2.1.1-3
Depends: libc6 (>= 2.3.2.ds1-4), libldap2 (>= 2.1.17-1), postfix, postfix (= 2.1.1-3)
Filename: pool/main/p/postfix/postfix-ldap_2.1.1-3_i386.deb
Size: 32884
MD5sum: 1e4255ba410226e7c514e8c8ba107049
Description: LDAP map support for Postfix
 Postfix is Wietse Venema's mail transport agent that started life as an
 alternative to the widely-used Sendmail program.  Postfix attempts to
 be fast, easy to administer, and secure, while at the same time being
 sendmail compatible enough to not upset existing users. Thus, the outside
 has a sendmail-ish flavor, but the inside is completely different.
 .
 This provides support for LDAP maps in Postfix.  If you plan to use LDAP maps
 with Postfix, you need this.

Package: postfix-tls
Priority: extra
Section: mail
Installed-Size: 384
Maintainer: LaMont Jones <lamont@debian.org>
Architecture: i386
Source: postfix
Version: 2.1.1-3
Depends: libc6 (>= 2.3.2.ds1-4), libdb4.2, libsasl2 (>= 2.1.15), libssl0.9.7, postfix,
postfix (= 2.1.1-3)
Recommends: mail-reader
Conflicts: postfix-snap-tls
Filename: pool/main/p/postfix/postfix-tls_2.1.1-3_i386.deb
Size: 136668
MD5sum: 9dc114c346ab462e6c38d2198dcd3538
Description: TLS and SASL support for Postfix
 Postfix is Wietse Venema's mail transport agent that started life as an
 alternative to the widely-used Sendmail program.  Postfix attempts to
 be fast, easy to administer, and secure, while at the same time being
 sendmail compatible enough to not upset existing users. Thus, the outside
 has a sendmail-ish flavor, but the inside is completely different.
 .
 This package adds support for TLS (see RFC 2487) and SASL (see RFC 2554) to
 Postfix.
```

El proceso de instalación de estos paquetes se muestra a continuación:

Ejemplo 1-2. Instalación de *postfix*, *postfix-ldap* y *postfix-tls*

```
# /usr/bin/apt-get install postfix postfix-ldap postfix-tls
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  postfix postfix-ldap postfix-tls
0 actualizados, 3 se instalarán, 0 reinstalados, 0 para eliminar y 0 no actualizados.
Se necesita descargar 0B/934kB de archivos.
Se utilizarán 496kB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n]
Preconfiguring packages ...
```

```
(Leyendo la base de datos ...
273428 ficheros y directorios instalados actualmente.)
Desempaquetando postfix (de .../postfix_2.1.1-3_i386.deb) ...
Desempaquetando postfix-ldap (de .../postfix-ldap_2.1.1-3_i386.deb) ...
Desempaquetando postfix-tls (de .../postfix-tls_2.1.1-3_i386.deb) ...
Addign `diversion of /usr/share/man/man8/smtpd.8.gz to /usr/share/man/man8/smtpd.real.8.gz by postfix'
Adding `diversion of /usr/lib/postfix/lmtp to /usr/lib/postfix/lmtp.postfix by postfix-tls'
Adding `diversion of /usr/lib/postfix/smtp to /usr/lib/postfix/smtp.postfix by postfix-tls'
Adding `diversion of /usr/lib/postfix/smtpd to /usr/lib/postfix/smtpd.postfix by postfix-tls'
Configurando postfix (2.1.1-3) ...

Postfix configuration was not changed.  If you need to make changes, edit
/etc/postfix/main.cf (and others) as needed.  To view Postfix configuration
values, see postconf(1).

After modifying main.cf, be sure to run '/etc/init.d/postfix reload'.

Running newaliases
Starting mail transport agent: Postfix.

Configurando postfix-ldap (2.1.1-3) ...
Adding ldap map entry to /etc/postfix/dynamicmaps.cf

Configurando postfix-tls (2.1.1-3) ...
Adding sdbm map entry to /etc/postfix/dynamicmaps.cf
```

Importante: Normalmente el proceso de instalación de Postfix realizará una serie de preguntas antes de proceder con la ejecución de los demonios que lo integran. Debido a que Postfix ya estaba instalado en el sistema en el que se han realizado las pruebas, dicha configuración preliminar ya se había realizado en otro momento. En la la sección de nombre *Forzando la configuración preliminar de Postfix* se forzará la configuración preliminar de Postfix, de esta forma se mostrará el proceso de configuración inicial.

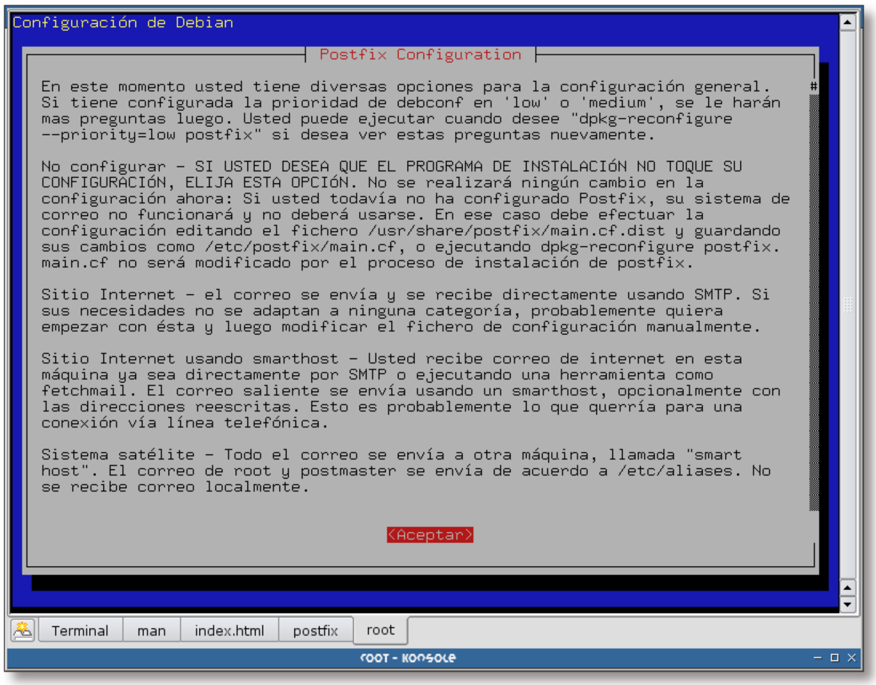
Forzando la configuración preliminar de Postfix

La forma de forzar la configuración de un paquete se realiza con el comando **dpkg-reconfigure**, de esta forma, para reconfigurar Postfix se ha de teclear:

Ejemplo 1-3. Reconfiguración de Postfix (primera parte)

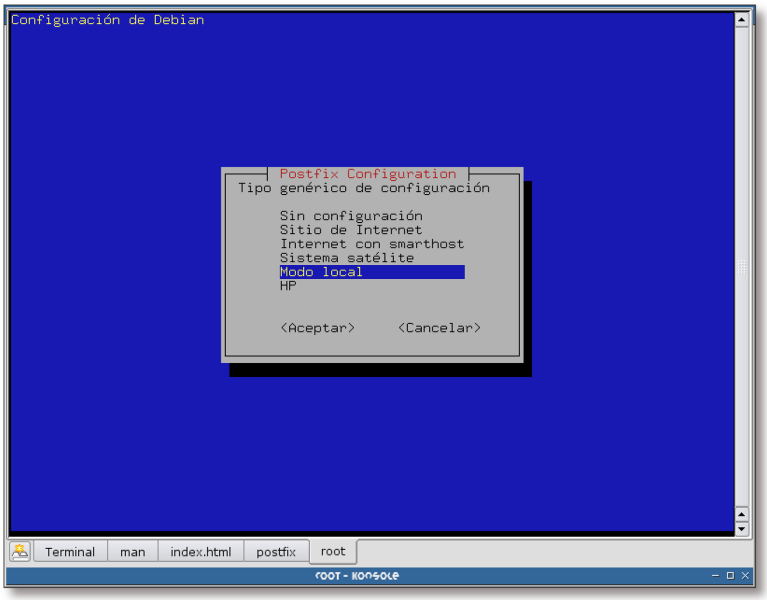
```
# /usr/bin/dpkg-reconfigure postfix

Stopping mail transport agent: Postfix.
```

Figura 1-1. Información sobre las opciones de configuración general



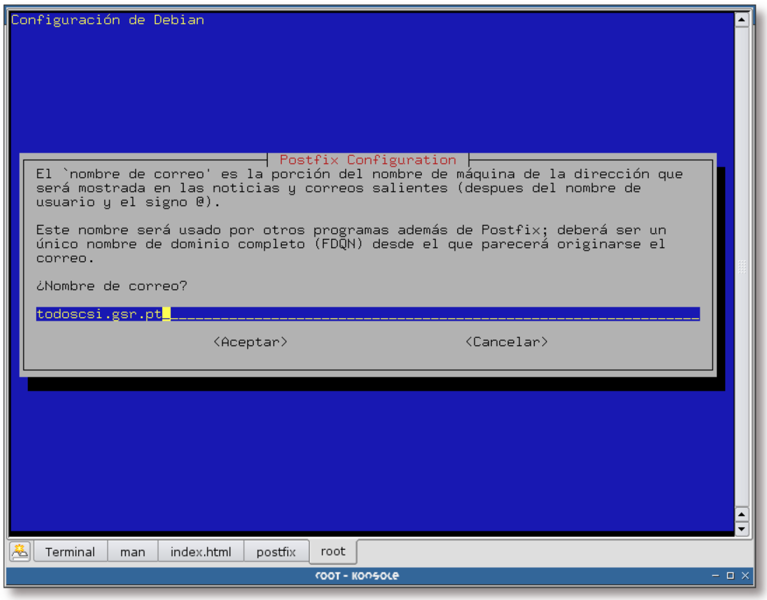
Esta pantalla muestra información sobre las distintas opciones de configuración que tiene Postfix. Lea con detenimiento cada una de ellas para saber cual se adapta a sus necesidades.

Figura 1-2. Tipo genérico de configuración



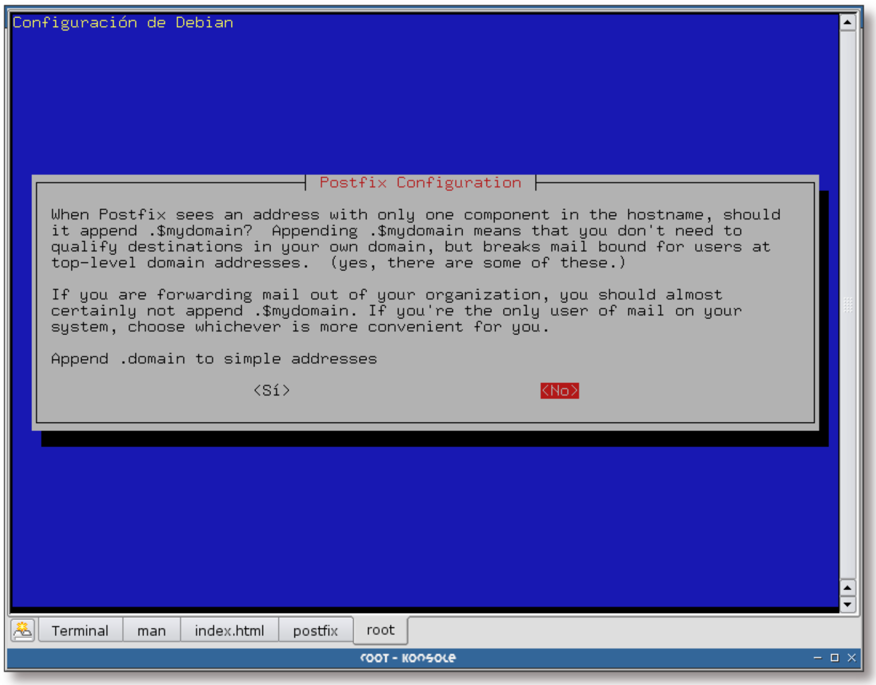
Elección del tipo genérico de configuración, en este caso se va a elegir el *Modo local*, pero lo más normal será elegir el modo *Sitio de Internet* o *Internet con smarthost*. De todas formas, esto no es muy importante en principio, ya que la configuración se puede cambiar en cualquier momento.

Figura 1-3. “Nombre de correo”



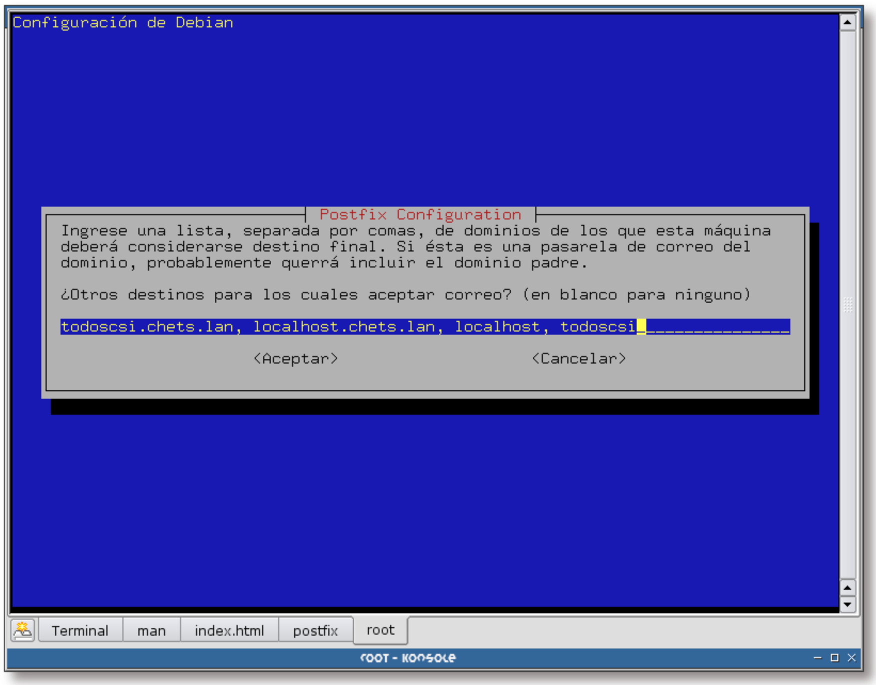
Aquí se indica la parte de la dirección de correo electrónico que va seguida de la @, es decir, si las cuentas de correo electrónico que piensa administrar son de tipo “usuario@dominio.pt”, en esta pantalla ha de teclear el “dominio.pt”.

Figura 1-4. ¿Añadir el dominio a las direcciones simples?



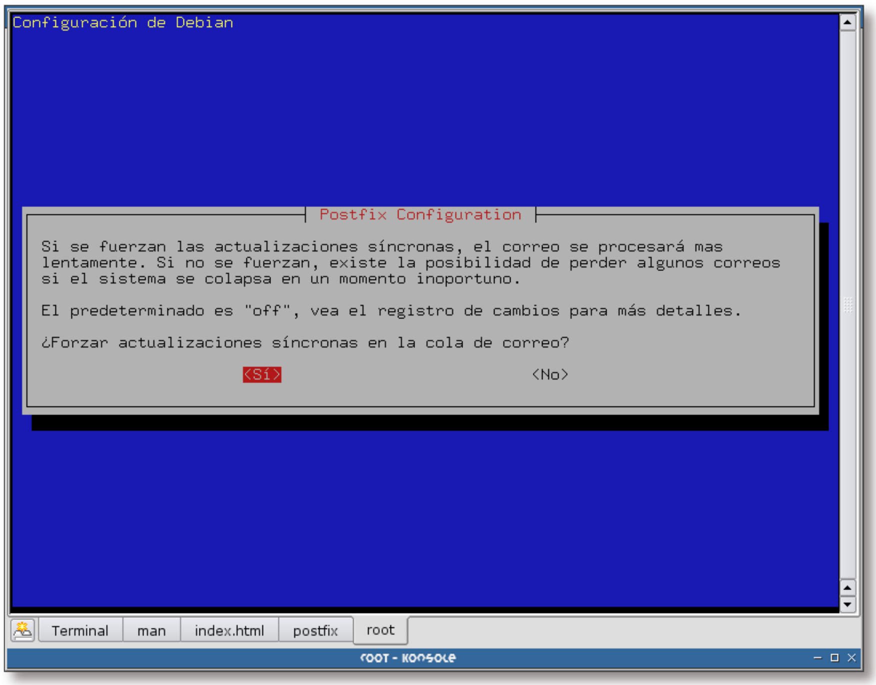
La respuesta a esta pregunta será *No*.

Figura 1-5. Lista de dominios locales



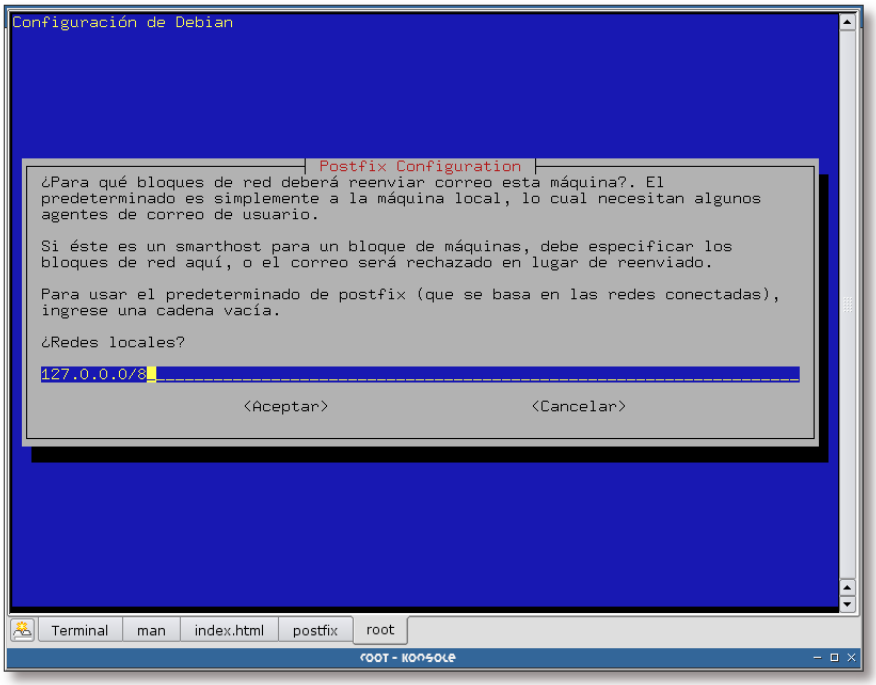
Complete en esta pantalla la lista de dominios para los cuales su servidor SMTP será la máquina final.

Figura 1-6. Actualizaciones síncronas en la cola de correo



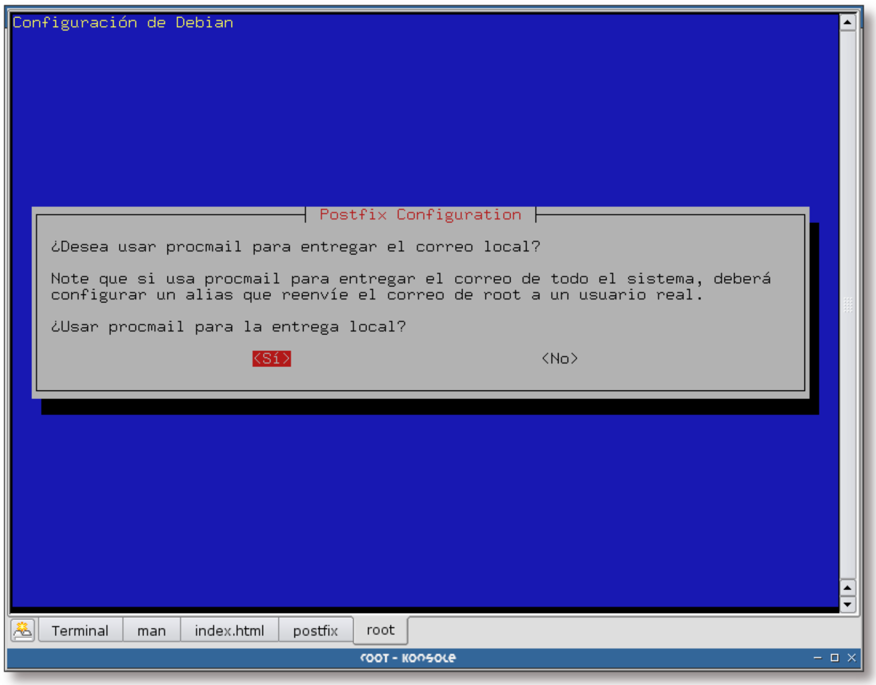
Se responde afirmativamente a esta pregunta, para asegurarse de un correcto manipulado de los mensajes. Tenga en cuenta la carga de su servidor de correo para la respuesta a esta pregunta, si la carga es elevada, tal vez fuese buena idea responder que *No* a esta cuestión.

Figura 1-7. Redes a las que se les permite el *relay*



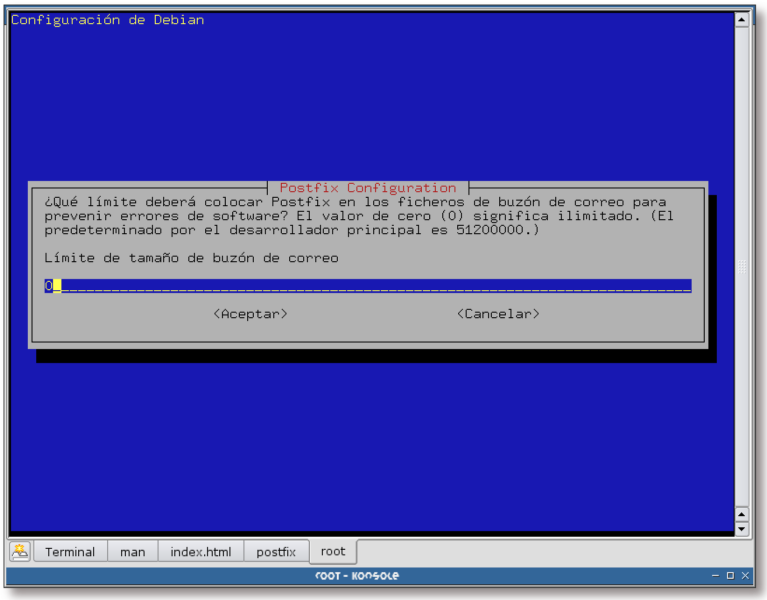
Complete el recuadro que se muestra en esta pantalla con todas aquellas redes para las cuales el servidor SMTP va a permitir el reenvío de correo.

Figura 1-8. Uso de procmail



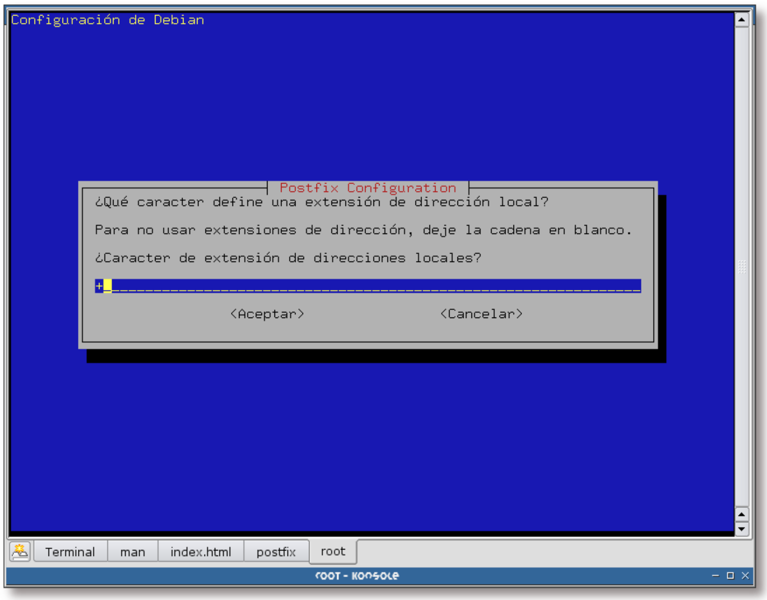
Se va a hacer uso de procmail para el reparto local de correos, por lo que se responde afirmativamente a esta pregunta.

Figura 1-9. Quota del buzón de correo



En principio no se establecerán quotas para las cuentas de correo. Si su sitema necesita establecer una quota, establézcala aquí.

Figura 1-10. Extensión de la dirección local



Se deja la respuesta por defecto en esta pantalla.

Ejemplo 1-4. Reconfiguración de Postfix (segunda parte)

```
setting synchronous mail queue updates: true
changing /etc/mailname
setting myorigin
setting destinations: todoscsi.chets.lan, localhost.chets.lan, localhost, todoscsi
setting append_dot_mydomain: no
setting relayhost:
setting mynetworks: 127.0.0.0/8
setting mailbox_command
setting mailbox_size_limit: 0
setting recipient_delimiter: +

Postfix is now set up with the changes above.  If you need to make changes, edit
/etc/postfix/main.cf (and others) as needed.  To view Postfix configuration
values, see postconf(1).

After modifying main.cf, be sure to run '/etc/init.d/postfix reload'.

Running newaliases
Starting mail transport agent: Postfix.
```

Capítulo 2. Configuración del soporte LDAP en Postfix

Introducción

En esta sección se preparará, tanto al sistema como a Postfix, para que este último tenga soporte LDAP.

> **Nota:** Esta sección se ha basado en la entrada bibliográfica Roncero01.

Esquema para el directorio LDAP

El esquema que se utilizará para el directorio LDAP será un árbol cuya la raíz será: *dc=gsr,dc=pt*, de la cual colgarán tres *organizationalUnit* que almacenarán toda la información necesaria:

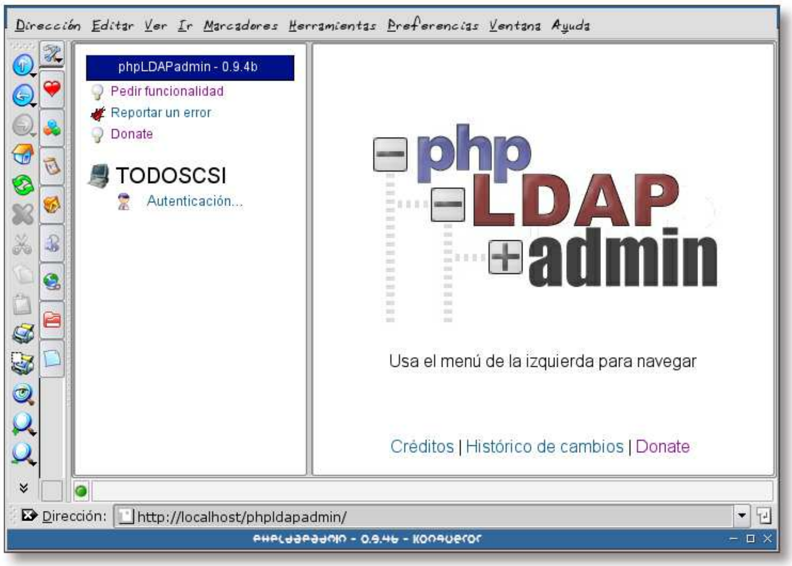
- Rama "people": la cual contendrá información sobre las cuentas de usuario. Aquí se almacenarán todos los datos obligatorios de las cuentas: direcciones de correo electrónico, directorio Maildir, etc.
- Rama "groups": almacenará la información relativa a grupos de usuarios.
- Rama "postfix": que contendrá la información necesaria para Postfix. En esta rama se creará una rama hija para el almacén de los alias de correo, de manera que se puedan tener varias direcciones que apunten a una misma cuenta o a otra cuenta externa.

> **Nota:** En la siguiente sección se mostrará el proceso a seguir para añadir una *organizationalUnit* desde phpLDAPadmin, las unidades organizacionales que falten deberá añadirlas de la misma forma.

Añadiendo las ramas "postfix" y "alias"

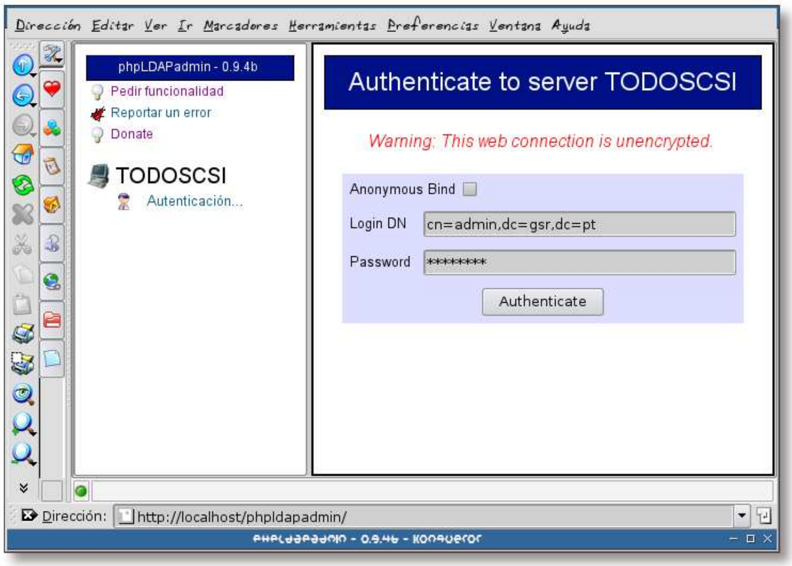
A continuación se muestra la forma de añadir la rama postfix y la rama hija de esta, *alias*, al directorio LDAP:

Figura 2-1. Acceso a phpLDAPadmin



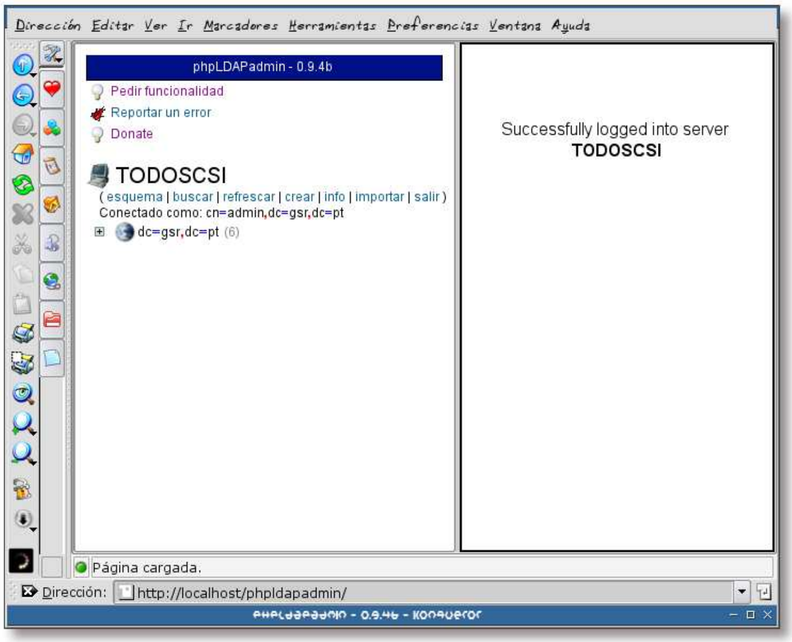
Teclee en su navegador favorito la URL donde se encuentre instalado phpLDAPadmin y pulse sobre el enlace "Autenticación...", si así lo requiere la herramienta (dependerá de la configuración de phpLDAPadmin).

Figura 2-2. Autentificación



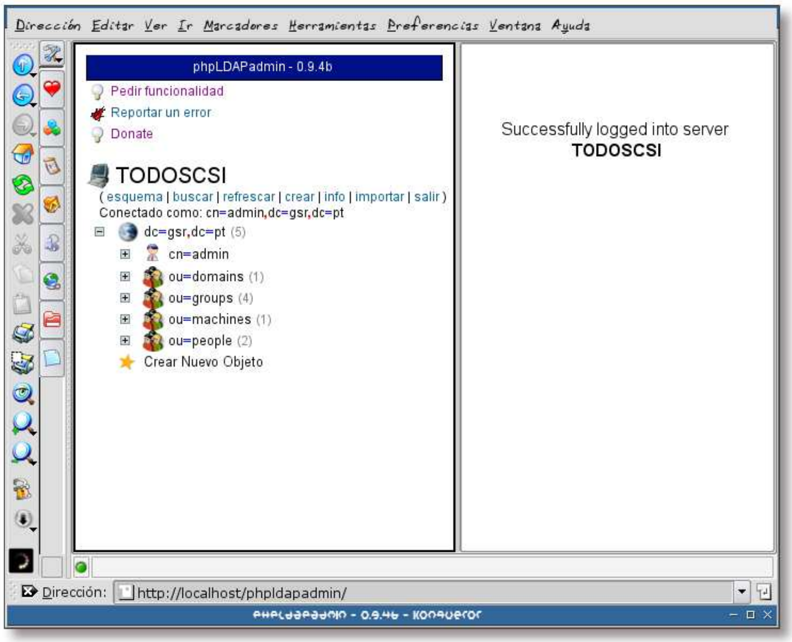
Teclee el DN del administrador de su directorio LDAP y la clave. Luego pulse sobre "Authenticate".

Figura 2-3. Autentificación correcta



Si todo ha ido bien, se habrá autentificado correctamente en el directorio LDAP. Pulse ahora sobre el signo + que aparece al lado de *dc=gsr,dc=pt* para ver la estructura del directorio.

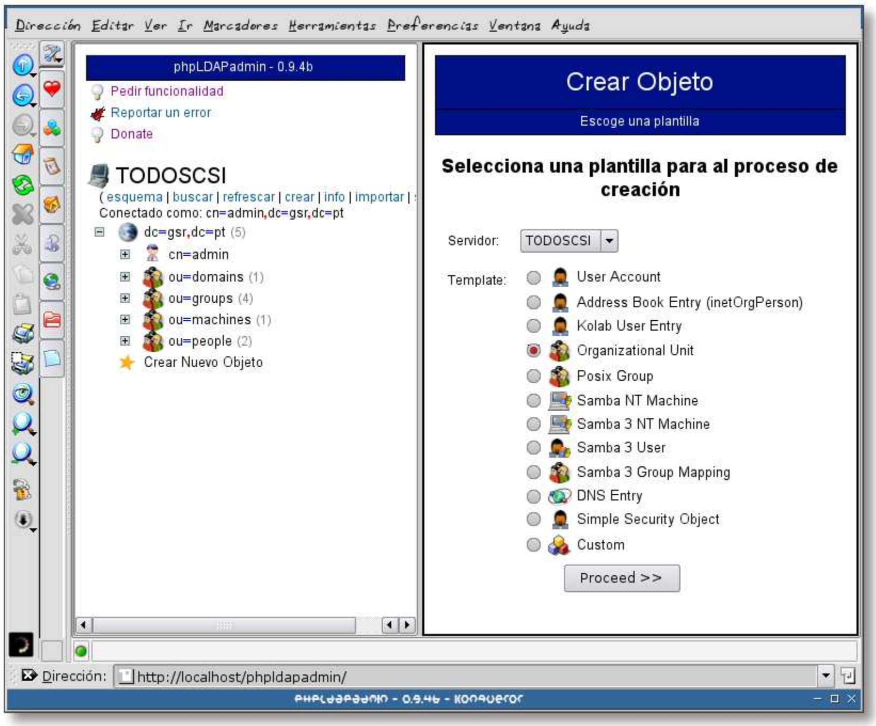
Figura 2-4. Estructura del directorio



Esta pantalla muestra la estructura actual del directorio LDAP sobre el que se va a trabajar. Las únicas ramas que van a interesar, de momento, para esta documentación son la rama *people* y la rama *groups*.

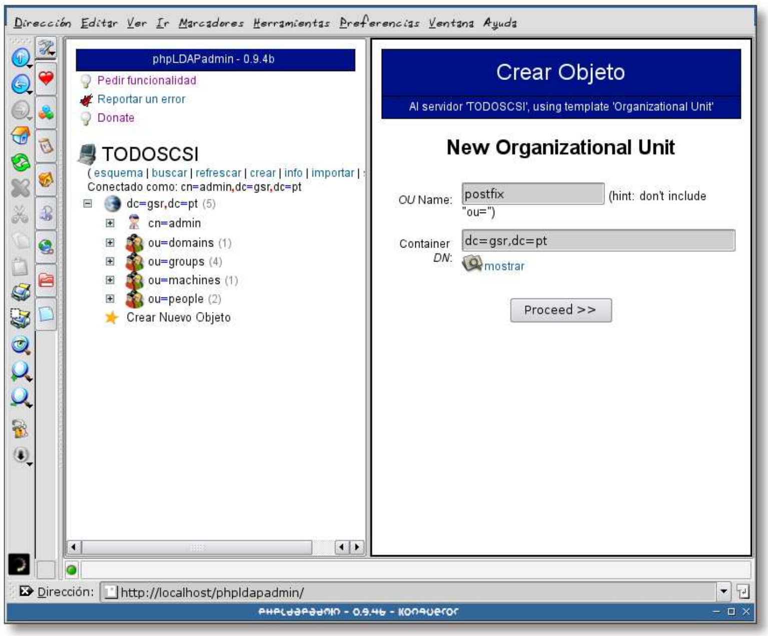
Pulse ahora sobre “Crear Nuevo Objeto”, para crear la rama *postfix*.

Figura 2-5. Creando la unidad organizacional *postfix*



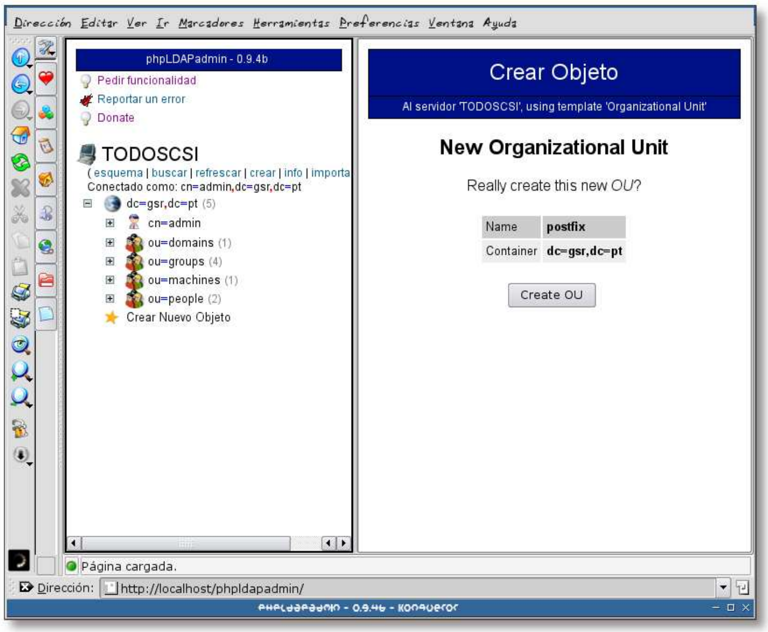
Seleccione la opción “Organizational Unit” y pulse sobre el botón *Proceed >>* para continuar.

Figura 2-6. Creando la unidad organizacional *postfix*, selección del nombre



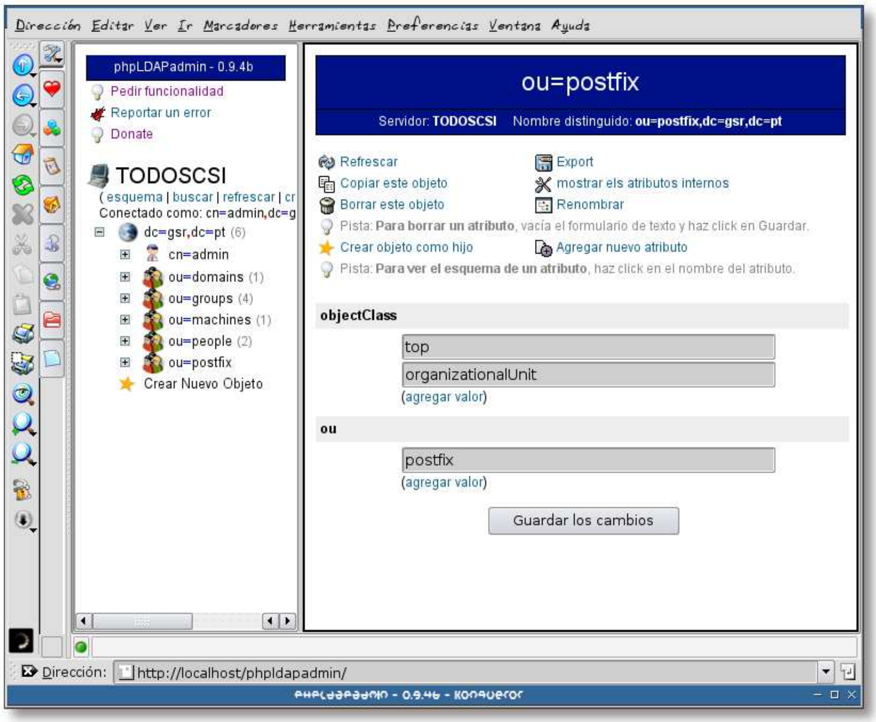
Teclee el nombre que va a tener la nueva unidad organizacional, en este caso se va a denominar: *postfix*. Pulse sobre el botón *Proceed >>* para continuar.

Figura 2-7. Creando la unidad organizacional *postfix*, creación de la unidad



Finalmente pulse sobre el botón "Create OU" para finalizar con el proceso de creación de la unidad organizacional *postfix*.

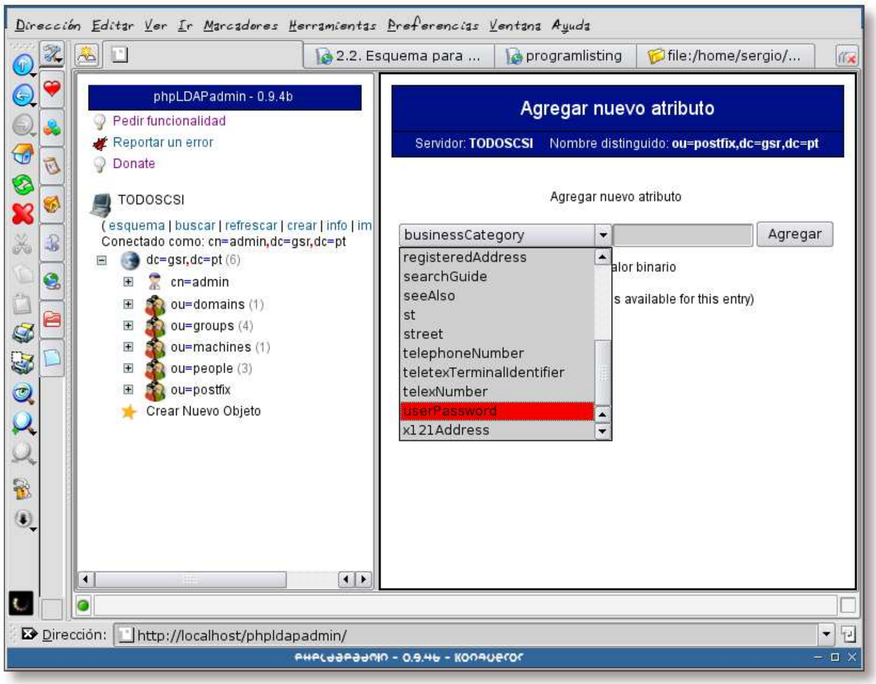
Figura 2-8. Creando la unidad organizacional *postfix*, información sobre la unidad



Una vez creada la unidad organizacional, se mostrará la información sobre la misma.

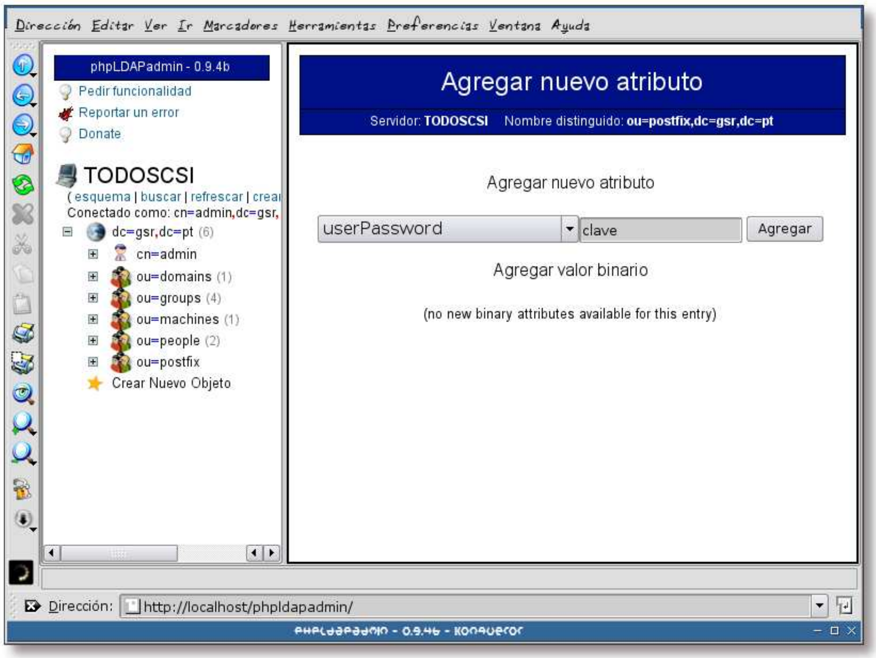
Ahora se va a asignar una clave a la unidad organizacional *postfix*, para ello pulse sobre el enlace “Agregar nuevo atributo”.

Figura 2-9. Creando la unidad organizacional *postfix*, estableciendo una clave I



Seleccione el atributo *userPassword*

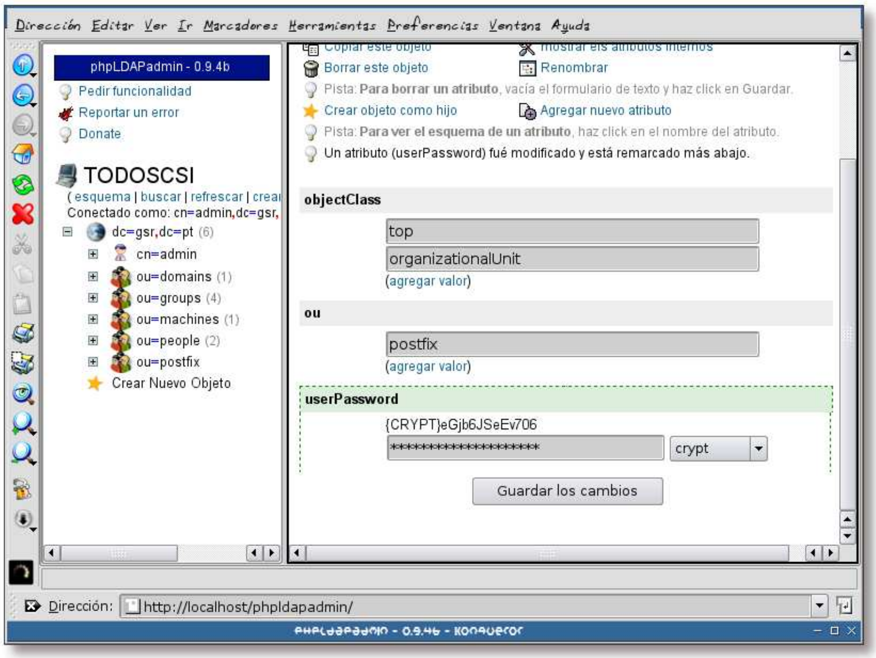
Figura 2-10. Creando la unidad organizacional *postfix*, estableciendo una clave II



Teclee la clave que quiera asignar al usuario y pulse sobre el botón *Agregar*.

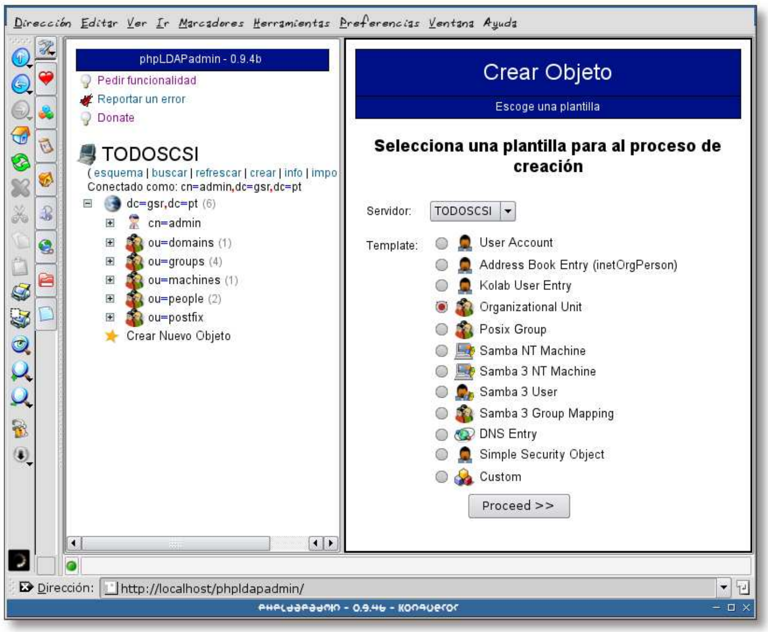
Nota: phpLDAPadmin la encriptará con el algoritmo de hash definido en su archivo de configuración (`/etc/phpldapadmin/config.php`); siendo en este caso el algoritmo *crypt*.

Figura 2-11. Creando la unidad organizacional *postfix*, estableciendo una clave III



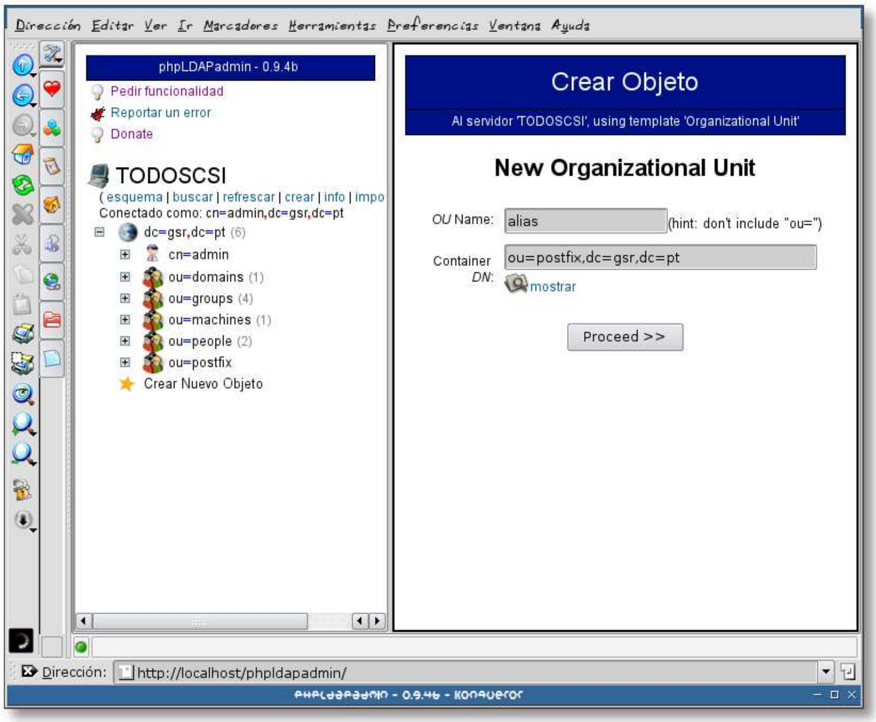
Como se puede observar en la imagen, la unidad organizacional *postfix* posee un nuevo atributo (userPassword). Para continuar, pulse sobre el enlace *Crear objeto como hijo*.

Figura 2-12. Creando la unidad organizacional *alias*



Seleccione la opción “Organizational Unit” y pulse sobre el botón *Proceed >>* para continuar.

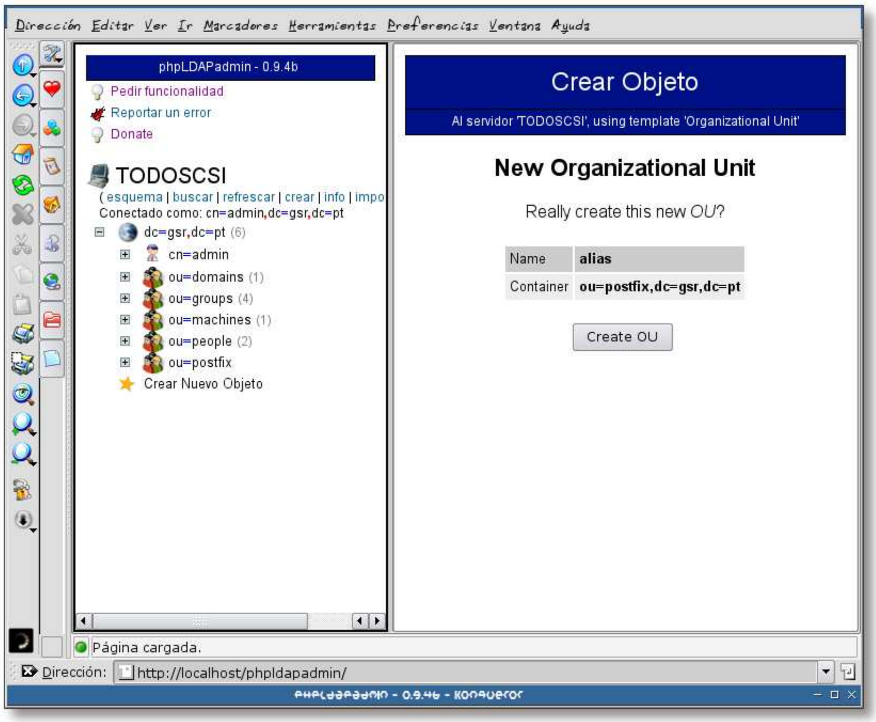
Figura 2-13. Creando la unidad organizacional *alias*, selección del nombre



Teclee el nombre que va a tener la nueva unidad organizacional, en este caso se va a denominar: *alias*. Pulse sobre el botón *Proceed >>* para continuar.

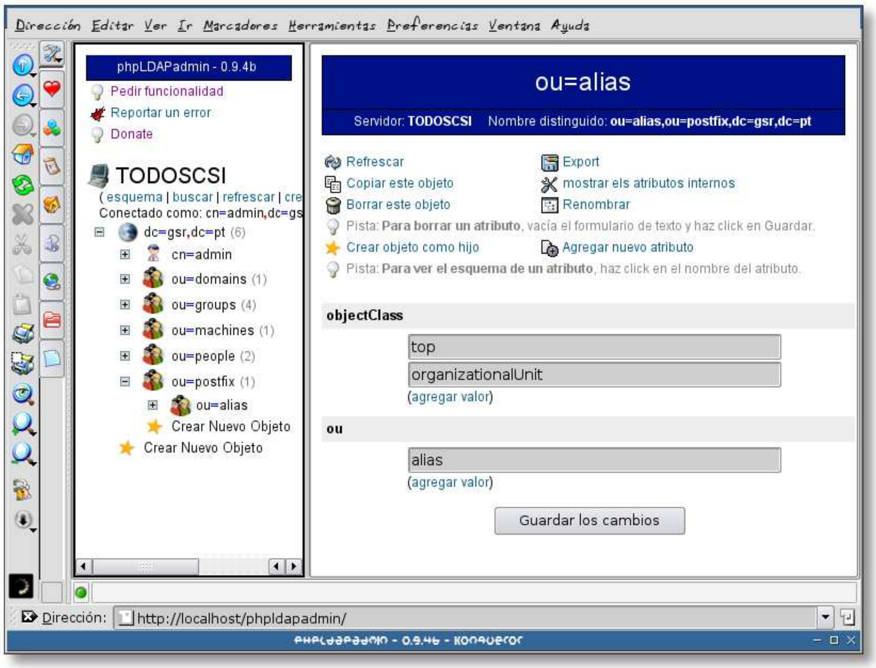
Importante: Tenga en cuenta que la unidad organizacional *alias* ha se ser hija de la unidad *postfix*, por lo que asegúrese de que la ruta seleccionada en el recuadro “Container DN:” es: *ou=postfix,dc=gsr,dc=pt*.

Figura 2-14. Creando la unidad organizacional *alias*, creación



Finalmente pulse sobre el botón “Create OU” para finalizar con el proceso de creación de la unidad organizacional *alias*.

Figura 2-15. Creando la unidad organizacional *alias*, información final



Como puede verse en la imagen, la unidad organizacional *alias* aparece bajo la unidad *postfix*, que era el objetivo final.

Plantilla *LDIF* para las unidades organizacionales

Otra forma de añadir información en un directorio LDAP, es hacer uso de plantillas *LDIF*. A continuación se mostrará una plantilla que podría haberse empleado para la generación de las unidades organizacionales descritas anteriormente:

Ejemplo 2-1. Plantilla *LDIF* para la creación de las unidades organizacionales: postfix, alias, people y groups

```
# Entry 1: ou=people,dc=gsr,dc=pt
dn:ou=people,dc=gsr,dc=pt
objectClass: organizationalunit
ou: people

# Entry 2: ou=groups,dc=gsr,dc=pt
dn:ou=groups,dc=gsr,dc=pt
objectClass: organizationalunit
ou: groups

# Entry 3: ou=postfix,dc=gsr,dc=pt
dn:ou=postfix,dc=gsr,dc=pt
ou: postfix
objectClass: top
objectClass: organizationalUnit
userPassword: {CRYPT}***************
```

```
# Entry 4: ou=alias,ou=postfix,dc=gsr,dc=pt
dn:ou=alias,ou=postfix,dc=gsr,dc=pt
ou: alias
objectClass: top
objectClass: organizationalUnit
```

Para añadir la plantilla al directorio LDAP, puede utilizar phpLDAPadmin. Simplemente guarde la plantilla en un archivo y haga uso del enlace “importar” de la herramienta.

También se puede emplear el comando **ldapadd**, como se muestra a continuación:

Ejemplo 2-2. Añadiendo una plantilla *LDIF* con ldapadd

```
$ /usr/bin/ldapadd -x -D "cn=admin,dc=gsr,dc=pt" -W -h gsr.pt \
                   -f organizationalunits.ldif
Enter LDAP Password: [clave]
adding new entry "ou=people,dc=gsr,dc=pt"

adding new entry "ou=groups,dc=gsr,dc=pt"

adding new entry "ou=postfix,dc=gsr,dc=pt"

adding new entry "ou=alias,ou=postfix,dc=gsr,dc=pt"
```

Directorio para el almacén de correos

Las cuentas de correo tendrán su buzón de correo bajo el directorio `/home/vmail/$user/Maildir`, donde “$user” se sustituirá por el nombre del usuario.

Todos los usuarios de correo pertenecerán al grupo *vmail*, por lo que si este grupo no existe en su sitema, tendrá que crearlo. A continuación se presenta la plantilla *LDIF* necesaria para añadir el grupo “vmail” al directorio LDAP:

Ejemplo 2-3. Plantilla *LDIF* para el grupo “vmail”

```
# Entry 1: cn=vmail,ou=groups,dc=gsr,dc=pt
dn:cn=vmail,ou=groups,dc=gsr,dc=pt
cn: vmail
gidNumber: 10004 ❶
objectClass: top
objectClass: posixGroup
```

❶ Elija el GID del grupo de acuerdo a la configuración de su sistema.

El siguiente paso es la creación del directorio que almacenará los buzones de correo de los nuevos usuarios:

Ejemplo 2-4. Creación del directorio para los usuarios de correo

```
# /bin/mkdir -vp -m 2755 /home/vmail
mkdir: se ha creado el directorio ‘/home/vmail’
# /bin/chown -v root.vmail /home/vmail/
cambiado el propietario de ‘/home/vmail/’ a root:vmail
```

Como los usuarios de correo van a ser usuarios del sistema, pero sin acceso a la shell, en principio, tienen asociado un directorio *home*, cuyo path será: `/home/vmail/$user` ($user se corresponde con el nombre del usuario). Por este motivo, se va a añadir al directorio `/etc/skel/` un archivo de recursos para procmail (programa encargado del repardo de correos de los usuarios) y el directorio bajo el cual se van a almacenar los correos de los usuarios en formato Maildir. El siguiente ejemplo muestra como hacerlo:

Ejemplo 2-5. Preparando el directorio `/etc/skel/`

```
# /bin/echo -ne "PATH=/usr/bin:/bin:/usr/local/bin:.\n\
MAILDIR=\$HOME/Maildir\nDEFAULT=\$MAILDIR/" > /etc/skel/.procmailrc ❶
# /usr/bin/maildirmake /etc/skel/Maildir
```

❶ En esta línea se define la localización del directorio donde procmail va a almacenar los correos de los usuarios en formato Maildir.

Ahora el sistema ya se encuentra preparado para la correcta creación del home de los usuarios de correo.

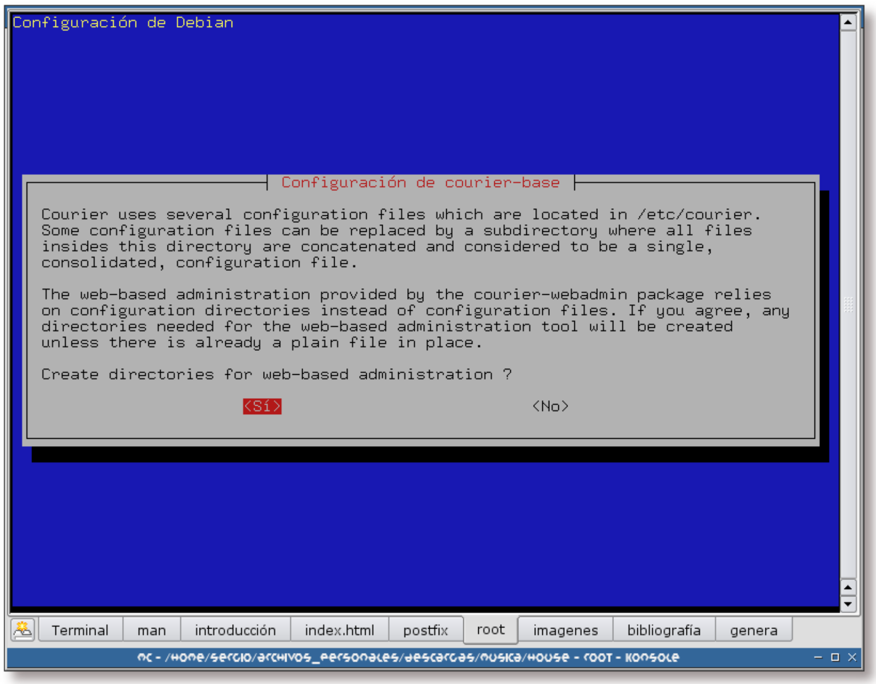
Preparando OpenLDAP para el soporte de correo

OpenLDAP necesita un esquema específico para poder manejar información acerca del correo electrónico, este esquema se encuentra en el paquete *courier-ldap*, por lo que se procederá a su instalación:

Ejemplo 2-6. Instalación del paquete *courier-ldap* (primera parte)

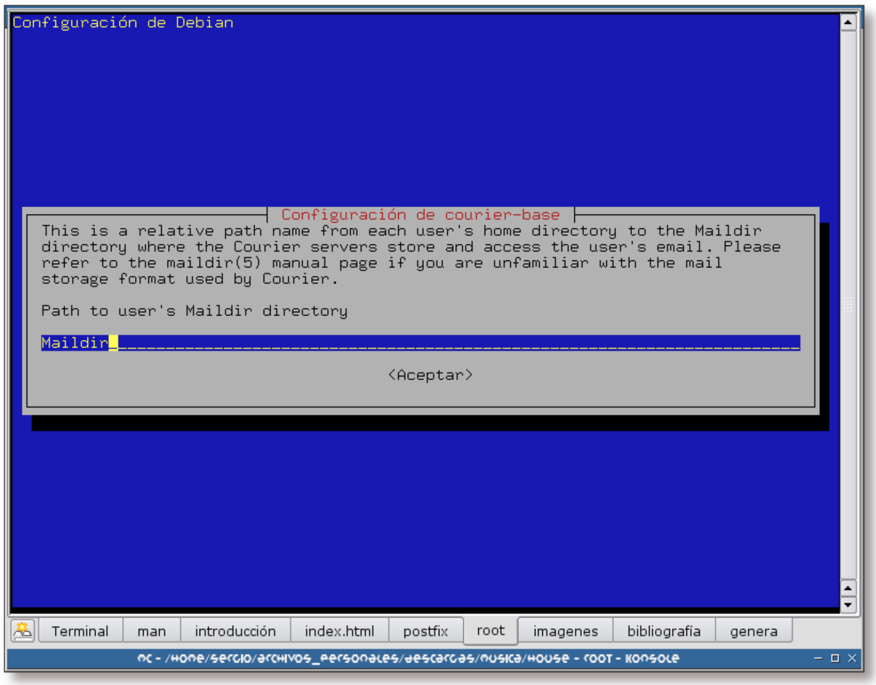
```
# /usr/bin/apt-get install courier-ldap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  courier-authdaemon courier-base
Se instalarán los siguientes paquetes NUEVOS:
  courier-authdaemon courier-base courier-ldap
0 actualizados, 3 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/344kB de archivos.
Se utilizarán 1114kB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n]
Preconfiguring packages ...
```

Figura 2-16. ¿Crear directorios para la administración vía web?



Se responde afirmativamente a esta pregunta, de forma que se creen los directorios necesarios para poder administrar la aplicación por una interfaz web (con el paquete *courier-webadmin*).

Figura 2-17. Nombre del directorio para el almacén de los correos en formato *Maildir*



Directorio, bajo el home del usuario, donde se almacenarán los correos en formato *Maildir*.

Ejemplo 2-7. Instalación del paquete *courier-ldap* (segunda parte)

```
--------------------- Sourcerer Apt Watcher ---------------------
Configure: courier-base
-----------------------------------------------------------------
(Leyendo la base de datos ...
273464 ficheros y directorios instalados actualmente.)
Desempaquetando courier-base (de .../courier-base_0.45.4-1_i386.deb) ...
Desempaquetando courier-authdaemon (de .../courier-authdaemon_0.45.4-1_i386.deb) ...
Desempaquetando courier-ldap (de .../courier-ldap_0.45.4-1_i386.deb) ...
Configurando courier-base (0.45.4-1) ...

Configurando courier-authdaemon (0.45.4-1) ...
Starting Courier authdaemon: done.

Configurando courier-ldap (0.45.4-1) ...
Starting Courier LDAP alias daemon: done.
```

El siguiente ejemplo muestra una descripción del paquete que se acaba de instalar en el sistema, así como sus dependencias más directas:

Ejemplo 2-8. Información sobre los paquetes *courier-ldap*, *courier-authdaemon* y *courier-base*

```
# /usr/bin/apt-cache show courier-ldap courier-authdaemon courier-base
Package: courier-ldap
Priority: optional
Section: mail
Installed-Size: 260
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
Architecture: i386
Source: courier
Version: 0.45.4-1
Replaces: courier-imap-authldap
Depends: libc6 (>= 2.3.2.ds1-4), libgdbm3, libldap2 (>= 2.1.17-1), libpam0g (>= 0.76),
courier-base (>= 0.45.4), courier-authdaemon (>= 0.45.4)
Conflicts: courier-imap-authldap
Filename: pool/main/c/courier/courier-ldap_0.45.4-1_i386.deb
Size: 62014
MD5sum: 205b66ece1774ccbf354038e05b2e8f5
Description: Courier Mail Server - LDAP support
 This package contains support for LDAP authentication and
 LDAP-based mail aliasing.

Package: courier-authdaemon
Priority: optional
Section: mail
Installed-Size: 208
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
Architecture: i386
Source: courier
Version: 0.45.4-1
Depends: libc6 (>= 2.3.2.ds1-4), libgdbm3, libpam0g (>= 0.76), courier-base (>= 0.45.4)
Filename: pool/main/c/courier/courier-authdaemon_0.45.4-1_i386.deb
Size: 51486
```

```
MD5sum: da101bf6c9b839d2462e3da4bec49eeb
Description: Courier Mail Server - Authentication daemon
 This package contains the authentication daemon for the
 Courier Mail Server.

Package: courier-base
Priority: optional
Section: mail
Installed-Size: 620
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
Architecture: i386
Source: courier
Version: 0.45.4-1
Replaces: courier-debug (<< 0.44.2)
Depends: libc6 (>= 2.3.2.ds1-4), libfam0c102, libgdbm3, perl, debconf (>= 0.5.00)
Conflicts: courier-imap (<= 1.3.3), courier-debug (<< 0.44.2)
Filename: pool/main/c/courier/courier-base_0.45.4-1_i386.deb
Size: 230866
MD5sum: 6cfa4f6dc8ac2e3feba5d50022700b6b
Description: Courier Mail Server - Base system
 The Courier mail transfer agent (MTA) is an integrated mail/groupware
 server based on open commodity protocols, such as ESMTP, IMAP, POP3, LDAP,
 SSL, and HTTP. Courier provides ESMTP, IMAP, POP3, webmail, and mailing list
 services within a single, consistent, framework.
 .
 This package provides the functionality needed by all Debian courier packages
 like some configuration files, helper programs and the Courier TCP server
 daemon.
```

Ahora que ya se encuentra instalado el paquete *courier-ldap*, se procederá a copiar el esquema necesario para dar soporte de correo al directorio LDAP al directorio de esquemas de OpenLDAP, como se muestra a continuación:

Ejemplo 2-9. Copiando el esquema `authldap.schema` al directorio de esquemas de OpenLDAP

```
# /bin/cp -v /usr/share/doc/courier-ldap/authldap.schema /etc/ldap/schema/
'/usr/share/doc/courier-ldap/authldap.schema' -> '/etc/ldap/schema/authldap.schema'
# /bin/chown -v slapd.slapd /etc/ldap/schema/authldap.schema
cambiado el propietario de '/etc/ldap/schema/authldap.schema' a slapd:slapd
# /bin/chmod -v 640 /etc/ldap/schema/authldap.schema
el modo de '/etc/ldap/schema/authldap.schema' cambia a 0640 (rw-r-----)
```

Por último se ha de añadir el nuevo esquema al archivo de configuración del demonio slapd y reiniciar el demonio. Para ello, añada la siguiente línea en la sección de definiciones de *objectClass* y *Schemas*:

```
include         /etc/ldap/schema/authldap.schema
```

Una vez hecho esto, reinicie el servidor slapd:

```
# /etc/init.d/slapd restart
Stopping OpenLDAP: slapd.
Starting OpenLDAP: slapd.
```

A partir de este momento, OpenLDAP ya tiene soporte para almacenar información relativa a sistemas de correo. En la siguiente sección se verá como añadir nuevos usuarios de correo al directorio LDAP.

Adición de un usuario de correo

En esta sección se verá como añadir un usuario de correo al directorio LDAP. En esta ocasión se hará uso de las herramientas de consola que provee el paquete *ldap-utils*. Para ello, se creará un archivo ldif con la siguiente estructura:

```
dn:uid=user,ou=people,dc=gsr,dc=pt
uid: user
cn: Nombre
sn: Apellidos
userPassword: {CRYPT}******** ❶
loginShell: /bin/false ❷
uidNumber: 10001
gidNumber: 10004 ❸
homeDirectory: /home/vmail/user ❹
shadowMin: -1
shadowMax: 999999
shadowWarning: 7
shadowInactive: -1
shadowExpire: -1
shadowFlag: 0
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
objectClass: CourierMailAccount ❺
mail: usuario@dominio.com ❻
mailbox: Maildir/ ❼
quota: 0 ❽
```

❶ Clave del usuario encriptada con el algoritmo de hash CRYPT. La elección del algoritmo es crítica para el funcionamiento global del sistema. Si no se escoge este algoritmo, no se podrá autentificar más tarde en los servicios POP3 e IMAP.

❷ La shell para los usuarios destinados al correo será una shell nula, es decir, no tendrán acceso al sistema; sólo podrán obtener y enviar su correo del mismo. Si en el futuro se quisiese dotar a este usuario con acceso shell, sólo habría que cambiar este atributo por una shell válida.

❸ GID del grupo principal del usuario de correo. Este ha de ser el GID del grupo *vmail* (eche un vistazo al valor introducido en GID del grupo vmail).

❹ Directorio home del usuario.

❺ *objectClass* que especifica los atributos relacionados con el correo.

❻ Correo electrónico del usuario.

❽ Atributo que controla la quota del usuario. Como de momento no se va a hacer uso de este parámetro, se utilizará para controlar si una cuenta se encuentra desactivada (valor -1) o no (cualquier otro valor).

❼ Ruta relativa al buzón de correo donde se almacenarán los mensajes. Se han de tener en cuenta los siguientes puntos: el directorio almacén será de la forma *dominio.com/usuario/*; el directorio se ha de crear antes de ser utilizado; el directorio ha de finalizar en "/" para indicar que se está trabajando con el formato Maildir.

A continuación se mostrará un ejemplo sobre como añadir un nuevo usuario al sistema. Para ello se creará un archivo con el siguiente contenido:

```
# Entry 1: uid=severa,ou=people,dc=gsr,dc=pt
dn:uid=severa,ou=people,dc=gsr,dc=pt
```

```
uid: severa
cn: Severa
sn: Sanches Lopes
userPassword: {CRYPT}************ ❶
loginShell: /bin/false
uidNumber: 10001
gidNumber: 10004 ❷
homeDirectory: /home/vmail/severa
shadowMin: -1
shadowMax: 999999
shadowWarning: 7
shadowInactive: -1
shadowExpire: -1
shadowFlag: 0
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: shadowAccount
objectClass: CourierMailAccount
mail: severa@gsr.pt
mailbox: Maildir/
quota: 0
```

❶ Para encriptar la clave con el algoritmo de hash CRYPT, se ha utilizado la herramienta *slappasswd* que provee el paquete *ldap-utisl*. El proceso de generación ha sido el siguiente:

Ejemplo 2-10. Obtención de una clave encriptada con CRYPT

```
# /usr/sbin/slappasswd -v -u -h {CRYPT}
New password: [clave]
Re-enter new password: [clave]
{CRYPT}u8.2mAF.3QmIQ
```

❷ El número que aparece en esta línea se corresponde con el gid del grupo *vmail* añadido en el Ejemplo 2-3.

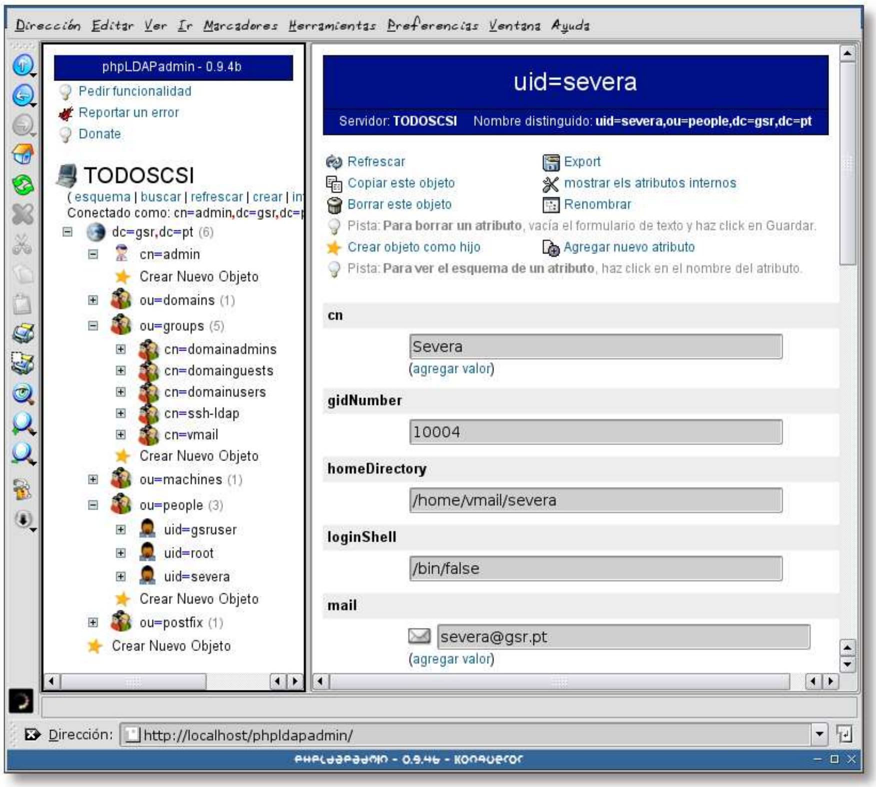
Suponiendo que el archivo donde se ha almacenado la información de la captura LDIF para Severa se denomina `severa.ldif`, ha de ejecutar el siguiente comando para añadir la información al directorio LDAP:

Ejemplo 2-11. Adición de un usuario con el comando ldapadd

```
$ /usr/bin/ldapadd -x -D "cn=admin,dc=gsr,dc=pt" -W -h  gsr.pt -f severa.ldif
Enter LDAP Password: [clave]
adding new entry "uid=severa,ou=people,dc=gsr,dc=pt"
```

La siguiente imagen muestra de forma gráfica, gracias a phpLDAPadmin, el nuevo usuario añadido al directorio LDAP:

Figura 2-18. Nuevo usuario: Severa



Esta captura muestra la nueva entrada bajo la unidad organizacional *people*: *severa*, usuario añadido en el Ejemplo 2-11.

Creación del directorio *HOME* para los nuevos usuarios

Es imprescindible que los buzones de correo existan antes de su uso. Por este motivo, cada vez que se añada un usuario de correo, se ha de crear su directorio *HOME* y el buzón de correo asociado, así como el archivo de recursos para procmail.

Para automatizar esta operación se ha creado el siguiente script:

```
#!/bin/sh
#
# Copyright (C) 2004 Sergio González González <sergio.gonzalez@hispalinux.es>
#
# Depends on:
#               - ldapsearch
#               - maildirmake ( from courier )
#
# Based on http://jeroen.protheus.com/postfix-courier-ldap-howto.html
# (c) J.Vriesman
#
# and
#
# Based on http://bulma.net/body.phtml?nIdNoticia=2013
```

```
# (c) Jesús Roncero Franco
#
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
#


# Password to bind to ldap server
systempass="1"
# Bind dn
binddn="ou=postfix,dc=gsr,dc=pt"
# Acount leave
accountleave="ou=people,dc=gsr,dc=pt"
# ldap host
ldaphost="gsr.pt"
# Maildir name
maildir="Maildir/"
# Mail users home name
homedir="/home/vmail"
# Mail user's group
group="vmail"


usernames=`ldapsearch -h $ldaphost -x -w $systempass -D "$binddn" \
                      -b "$accountleave" "(!(quota=-1))" uid  \
                      | grep "^[^#]" | grep "^[^dn]" | grep uid | awk '{ print $2 }'`


# create personal mailfolders

for username in $usernames
do
  homedirectory=`ldapsearch -h $ldaphost -x -w $systempass -D "$binddn" \
                            -b "$accountleave" "(uid=$username)" homeDirectory \
                            | grep "^[^#]" | grep homeDirectory | grep "$homedir" \
                            | awk '{ print $2 }'`

  if [ ! -d $homedirectory/$maildir ] && [ ! -z $homedirectory ]
  then

    mkdir -p -m 2750 $homedirectory
    maildirmake $homedirectory/$maildir

    if [ ! -f $homedirectory/.procmailrc ]
    then
```

```
      echo -ne "PATH=/usr/bin:/bin:/usr/local/bin:.\nMAILDIR=\$HOME/Maildir\n\
                DEFAULT=\$MAILDIR/" > $homedirectory/.procmailrc

    fi

    chown -R $username.$group $homedirectory
  fi

done
```

El script anterior creará el *HOME* de los usuarios de correo que no lo tuviesen ya creado, el directorio `Maildir` en el que se almacenarán los correos enviados al usuario y el archivo `.procmailrc`, que se encargará de decirle a procmail como se ha de comportar.

> **Nota:** Para la correcta ejecución del script se necesita la herramienta maildirmake. Esta herramienta, utilizada para crear un directorio tipo Maildir, viene junto al paquete *courier-base*.

> **Importante:** Recuerde que cada vez que se añada un usuario al sistema, se ha de ejecutar este script como *root*.

Creación de un alias de correo

Para crear un alias de correo, se ha de crear un elemento bajo la hoja *ou=alias,ou=postfix,dc=gsr,dc=pt* e indicar que hacer cuando llegue un correo a esta cuenta.

En este caso, la plantilla a utilizar es la siguiente:

```
dn: mail=alias@dominio.com,ou=alias,ou=postfix,dc=gsr,dc=pt ❶
cn: Nombre
mail: alias@dominio.com ❷
maildrop: direccion@destino.com ❸
sn: Apellidos
objectClass: couriermailalias ❹
objectClass: inetOrgPerson
objectClass: Person
```

❶ Se utilizará como *dn* el atributo mail.

❷ Se corresponde con el alias de uno de los dominios virtuales que se poseen.

❸ Dirección de destino. Se puede corresponder con una dirección virtual de alguno de los dominios virtuales en su poder o una en otro dominio. Si existe más de una línea con el atributo *maildrop*, el mensaje que llegue a la cuenta mail se enviará a todas las direcciones especificadas.

❹ *objectClass que especifica que la cuenta es de tipo alias.*

Un ejemplo podía ser el siguiente:

```
dn: mail=liviana@gsr1.pt,ou=alias,ou=postfix,dc=gsr,dc=pt
cn: Liviana
mail: liviana@gsr1.pt
maildrop: severa@gsr.pt
```

```
sn: Sanches
objectClass: couriermailalias
objectClass: inetOrgPerson
objectClass: Person
```

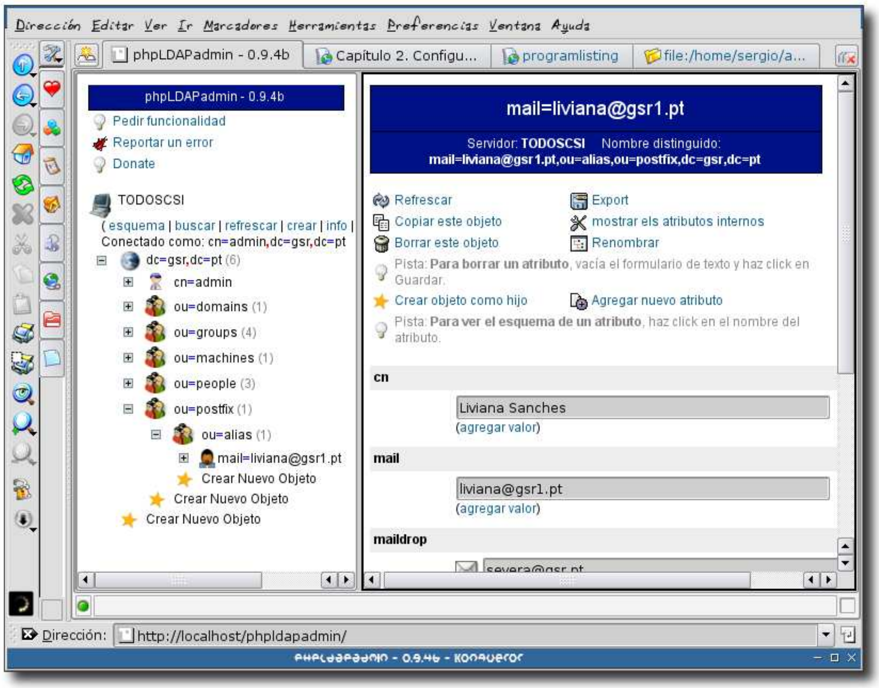
Suponiendo que el archivo donde se ha almacenado la información de la captura LDIF para Liviana se denomina `liviana.ldif`, ha de ejecutar el siguiente comando para añadir la información al directorio LDAP:

Ejemplo 2-12. Adición de un alias con el comando ldapadd

```
$ /usr/bin/ldapadd -x -D "cn=admin,dc=gsr,dc=pt" -W -h  gsr.pt -f liviana.ldif
Enter LDAP Password: [clave]
adding new entry "mail=liviana@gsr1.pt,ou=alias,ou=postfix,dc=gsr,dc=pt"
```

La siguiente imagen muestra de forma gráfica, gracias a phpLDAPadmin, el nuevo alias añadido al directorio LDAP:

Figura 2-19. Nuevo alias: liviana



Esta captura muestra la nueva entrada bajo la unidad organizacional *postfix -> alias* a *liviana@gsr1.pt*, alias añadido en el Ejemplo 2-12.

Modificación de la configuración de Postfix

Introducción

En esta sección se mostrarán los aspectos de configuración de Postfix más importantes para hacer uso de un directorio LDAP, entre otras cosas.

> **Sugerencia:** Durante todo el proceso de configuración de Postfix sería recomendable tener una consola de monitorización de los logs de este programa. Puede ejecutar el siguiente comando en la consola destinada a la monitorización:
>
> ```
> # /usr/bin/tail -f /var/log/mail.log | colorize
> ```
>
> El programa *colorize* se encuentra en el paquete “colorize”, por lo que puede utilizar el comando **/usr/bin/apt-get install colorize** para instalarlo.

Configuración de los alias de correo

Como los alias de correo están almacenados en el directorio LDAP hay que decirle a Postfix donde y como ha de realizar las búsquedas. Cuando se especifica: *ldap:nombre*, *nombre* va a ser el prefijo que se va a utilizar en una serie de variables de Postfix para especificar la configuración e interrogación de LDAP. De esta forma, para la sentencia *ldap:nombre*, se deberán definir las siguientes opciones:

- *nombre_server_host*: servidor LDAP
- *nombre_search_base*: base de las búsquedas en LDAP
- *nombre_query_filter*: filtro para la búsqueda
- *nombre_result_attribute*: atributos que se quieren leer de los resultados de la búsqueda
- *nombre_bind*: ¿es precisa la autentificación?. En este caso no es precisa, ya que la parte a consultar en el directorio LDAP es accesible anónimamente

De esta forma, por ejemplo, para la configuración de los alias de correo, se tendría una configuración como:

```
#Alias virtuales
virtual_maps = ldap:valiases
valiases_server_host = gsr.pt
valiases_search_base = ou=alias,ou=postfix,dc=gsr,dc=pt
valiases_query_filter = (&(mail=%s)(objectClass=CourierMailAlias))
valiases_result_attribute = maildrop
valiases_bind = no
```

> **Nota:** En este caso, la búsqueda se realizaría en la rama *ou=alias,ou=postfix,dc=gsr,dc=pt*, devolviendo como resultado aquellos elementos cuyo atributo *mail* sea igual a la dirección de correo electrónico que se está buscando, siempre y cuando el *objectClass* sea *CourierMailAlias*

> **Nota:** *_query_filter* utiliza notación prefija, como se puede observar en (&(condición)(condición)). Otros ejemplos podrían ser:

- (|(condición)(condición))
- (&(|(condición)(condición))(condición))

Configuración de Postfix para la entrega local

También se desea que el correo local sea administrado por Postfix, de forma que hay que indicárselo en su archivo de configuración. A continuación se verá la forma de hacer esto:

```
local_transport = local
mydestination = $myhostname $localhost.$mydomain localhost.gsr.pt
local_recipient_maps = unix:passwd.byname $alias_maps
```

Esto sería suficiente para la realización de la entrega local.

Configuración preliminar para Postfix

En la la sección de nombre *Modificación de la configuración de Postfix* se mostraron las opciones necesarias para utilizar el servidor de correo Postfix con LDAP y alias de correo, entre otros. A continuación se verá un archivo de configuración completo, integrando todas las opciones vistas en la la sección de nombre *Modificación de la configuración de Postfix*:

```
# see /usr/share/postfix/main.cf.dist for a commented, fuller
# version of this file.

# Do not change these directory settings - they are critical to Postfix
# operation.
command_directory = /usr/sbin
daemon_directory = /usr/lib/postfix
program_directory = /usr/lib/postfix
setgid_group = postdrop

# appending .domain is the MUA's job.
append_dot_mydomain = no

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no

# Uncomment the next line to generate delayed mail warnings
#delay_warning_time = 4h

myhostname = todoscsi.gsr.pt
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mynetworks = 127.0.0.0/8

#Alias virtuales
virtual_maps = ldap:valiases
valiases_server_host = gsr.pt
valiases_search_base = ou=alias,ou=postfix,dc=gsr,dc=pt
```

```
valiases_query_filter = (&(mail=%s)(objectClass=CourierMailAlias))
valiases_result_attribute = maildrop
valiases_bind = no

# Todos los dominios y los usuarios entragados por el agente de entrega local
# local_recipient_maps es usado por el servidor SMTP para rechazar el correo
# de los usuarios no conocidos
local_transport = local
mydestination = $myhostname $localhost.$mydomain localhost.gsr.pt
local_recipient_maps = unix:passwd.byname $alias_maps

mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
```

Una vez modificado el archivo de configuración de Postfix, este ha de releer su configuración, para ello teclee:

Ejemplo 2-13. Releyendo la configuración de Postfix

```
# /etc/init.d/postfix reload
Reloading Postfix configuration...done.
```

Ahora se puede probar el envío de un correo para la cuenta <liviana@gsr.pt>:

Ejemplo 2-14. Envío de un correo a <liviana@gsr.pt>

```
$ /usr/bin/mail liviana@gsr1.pt
Subject: Prueba
Cuerpo del mensaje
.
Cc: [enter]
```

Si tras ejecutar el Ejemplo 2-14 se mira en el archivo de log `/var/log/mail.log` se verá una entrada parecida a:

Ejemplo 2-15. Entrada en el log indicando el envío de un correo

```
Jun  4 11:29:06 todoscsi postfix/pickup[4799]: 89FC13A: uid=1000 from=<sergio>
Jun  4 11:29:06 todoscsi postfix/cleanup[4807]: 89FC13A: \
                                  message-id=<20040604102906.89FC13A@todoscsi.gsr.pt>
Jun  4 11:29:06 todoscsi postfix/qmgr[4800]: 89FC13A: from=<sergio@todoscsi.gsr.pt>, \
                                                      size=328, nrcpt=1 (queue active)
Jun  4 11:29:06 todoscsi postfix/local[4809]: 89FC13A: to=<severa@gsr.pt>, \
                     orig_to=<liviana@gsr1.pt>, relay=local, delay=0, status=sent \
                     (delivered to command: procmail -a "$EXTENSION")
Jun  4 11:29:06 todoscsi postfix/qmgr[4800]: 89FC13A: removed
Jun  4 11:29:40 todoscsi postfix/smtpd[4738]: disconnect from gsr.pt[x.x.x.x]
```

Como se puede comprobar, el correo ha sido enviado a la dirección *severa@gsr.pt*, ya que *liviana@gsr1.pt* es un alias para esa cuenta.

Con esto quedaría finalizada la parte de la configuración de Postfix con soporte de LDAP.

III. Courier

Capítulo 3. Instalación y configuración de Courier

Introducción

En el Ejemplo 2-6 se instalaron los paquetes courier-authdaemon, courier-base y courier-ldap. En este capítulo se van a configurar de la manera apropiada y se van a instalar aquellos paquetes que faltan para dar servicio POP3 e IMAP a los usuarios.

> **Nota:** Esta sección se ha basado en la entrada bibliográfica Roncero01.

Configuración del servicio de autentificación

Courier utiliza un servicio de autentificación para todos sus servicios. Este servicio se puede configurar de varias formas, de manera que haga la autentificación desde varias fuentes (PAM, LDAP, MySQL, et.). Esto significa que una vez configurado este servicio, los demás servicios de courier (POP3, POP3s, IMAP, etc) harán uso de este para la autentificación.

El servicio de autentificación está formado por un demonio llamado authdaemon, cuyo fichero de configuración es `/etc/courier/authdaemonrc`. Por defecto viene configurado para la autentificación vía PAM. A parte de este método, en esta documentación se hará uso de LDAP, por lo que modifique el archivo `/etc/courier/authdaemonrc` y añada este método de autentificación a la variable *authmodulelist*, como se muestra a continuación:

```
authmodulelist="authpam authldap"
```

> **Nota:** En el Apéndice C posee un archivo de configuración completo para este demonio.

Configuración de la autentificación por LDAP

Como se ha elegido el método de autentificación por LDAP, se ha de configurar el archivo `/etc/courier/authldaprc` para adaptarlo a las necesidades del sistema.

Las opciones más importantes que ha de modificar son:

```
LDAP_SERVER             gsr.pt
LDAP_PORT               389
LDAP_BASEDN             ou=people,dc=gsr,dc=pt
LDAP_BINDDN             ou=postfix,dc=gsr,dc=pt
LDAP_BINDPW             ********
LDAP_TIMEOUT            15
LDAP_AUTHBIND           1
LDAP_MAIL               mail
LDAP_FILTER             (!(quota=-1))
LDAP_UID                uidNumber
LDAP_GID                gidNumber
LDAP_HOMEDIR            homeDirectory
LDAP_MAILDIR            mailbox
```

```
LDAP_FULLNAME           cn
LDAP_CRYPTPW            userPassword
LDAP_DEREF              never
LDAP_TLS                0
```

Nota: En el Apéndice D posee un archivo de configuración completo.

Instalación del servicio POP3

El servicio POP3 lo aporta el paquete *courier-pop*, por lo que ha de instalarse en el sistema:

Ejemplo 3-1. Instalación del paquete *courier-pop*

```
# /usr/bin/apt-get install courier-pop
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  courier-pop
0 actualizados, 1 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/46,6kB de archivos.
Se utilizarán 221kB de espacio de disco adicional después de desempaquetar.
--------------------- Sourcerer Apt Watcher ---------------------
Configure: courier-pop
-----------------------------------------------------------------
(Leyendo la base de datos ...
273580 ficheros y directorios instalados actualmente.)
Desempaquetando courier-pop (de .../courier-pop_0.45.4-1_i386.deb) ...
Configurando courier-pop (0.45.4-1) ...
Starting Courier POP3 server: pop3d.
```

La descripción del paquete que se acaba de instalar es la siguiente:

Ejemplo 3-2. Descripción del paquete *courier-pop*

```
# /usr/bin/apt-cache show courier-pop
Package: courier-pop
Priority: extra
Section: mail
Installed-Size: 216
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
Architecture: i386
Source: courier
Version: 0.45.4-1
Replaces: pop3-server
Provides: pop3-server
Depends: libc6 (>= 2.3.2.ds1-4), exim4 | mail-transport-agent, courier-base (>= 0.45.4),
courier-authdaemon (>= 0.45.4)
Suggests: mail-reader, courier-pop-ssl
Conflicts: pop3-server
Filename: pool/main/c/courier/courier-pop_0.45.4-1_i386.deb
```

```
Size: 46614
MD5sum: 962e9728f57c2524f8c4d466796119e3
Description: Courier Mail Server - POP3 server
 The POP3 daemon from the Courier Mail Server supports only email
 stored in the maildir format.
```

La configuración del demonio pop3d se realiza desde el archivo `/etc/courier/pop3d`, de todas formas, la configuración por defecto es suficiente en este caso.

> **Nota:** En el Apéndice E tiene un archivo de configuración completo para el demonio *pop3d*.

Instalación del servicio IMAP

El servicio IMAP lo aporta el paquete *courier-imap*, por lo que ha de instalarse en el sistema:

Ejemplo 3-3. Instalación del paquete *courier-imap*

```
# /usr/bin/apt-get install courier-imap
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  courier-imap
0 actualizados, 1 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/553kB de archivos.
Se utilizarán 1602kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...
--------------------- Sourcerer Apt Watcher ---------------------
Configure: courier-imap
-----------------------------------------------------------------
(Leyendo la base de datos ...
273596 ficheros y directorios instalados actualmente.)
Desempaquetando courier-imap (de .../courier-imap_3.0.3-1_i386.deb) ...
Configurando courier-imap (3.0.3-1) ...
Starting Courier IMAP server: imapd.
```

A continuación se muestra la descripción del paquete:

Ejemplo 3-4. Descripción del paquete *courier-imap*

```
# /usr/bin/apt-cache show courier-imap
Package: courier-imap
Priority: extra
Section: mail
Installed-Size: 1564
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
Architecture: i386
Source: courier (0.45.4-1)
Version: 3.0.3-1
Replaces: imap-server
Provides: imap-server
Depends: libc6 (>= 2.3.2.ds1-4), libfam0c102, libgdbm3, exim4 | mail-transport-agent,
```

```
courier-base (>= 0.45.4), courier-authdaemon (>= 0.45.4)
Suggests: imap-client, courier-imap-ssl
Conflicts: imap-server
Filename: pool/main/c/courier/courier-imap_3.0.3-1_i386.deb
Size: 552608
MD5sum: c9780ad4a859427c7a755b45bdb0d29d
Description: Courier Mail Server - IMAP server
 The Courier IMAP server provides access to email stored in Maildirs.
 This server has an extremely small footprint, provides shared and
 virtual shared folders.
```

La configuración del demonio imapd se realiza desde el archivo `/etc/courier/imapd`, de todas formas, la configuración por defecto es suficiente en este caso.

> **Nota:** En el Apéndice G tiene un archivo de configuración completo para el demonio *impad*.

Uso del frontend *webadmin* de Courier

Instalación del paquete *courier-webadmin*

Courier dispone de un frontend para la administración de los servicios vía web. La interfaz de administración la provee el paquete *courier-webadmin*. La descripción del paquete es la siguiente:

Ejemplo 3-5. Descripción del paquete *courier-webadmin*

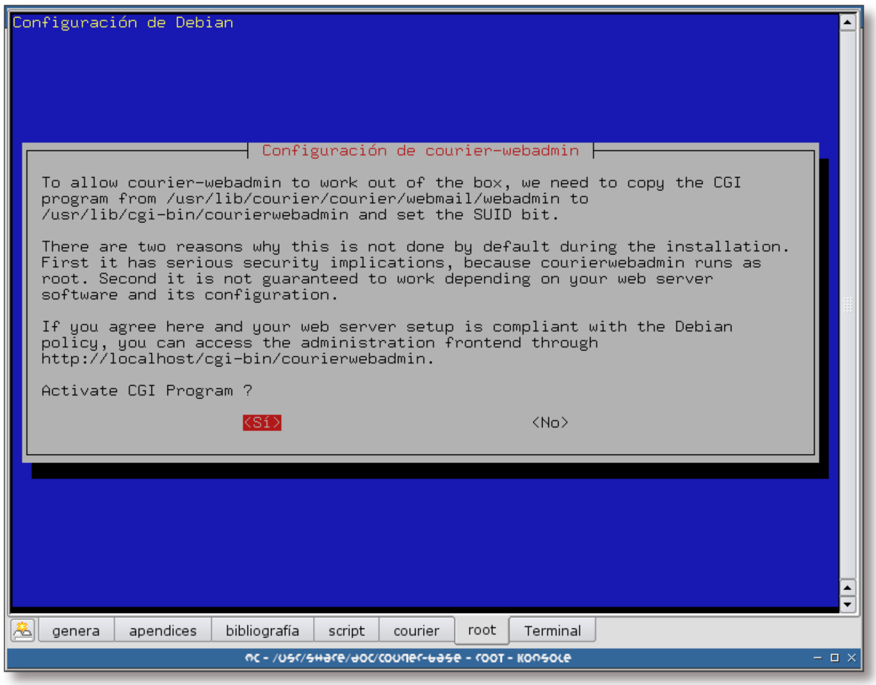
```
# /usr/bin/apt-cache show courier-webadmin
Package: courier-webadmin
Priority: optional
Section: mail
Installed-Size: 200
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
Architecture: i386
Source: courier
Version: 0.45.4-1
Depends: courier-base (>= 0.45.4), apache | httpd
Filename: pool/main/c/courier/courier-webadmin_0.45.4-1_i386.deb
Size: 32060
MD5sum: 8250af24eeaaaaeec4eefeb2ec8cf703
Description: Courier Mail Server - Web-based administration frontend
 The web-based administration and configuration tool for the Courier
 Mail Server is capable of changing the settings of the MTA, IMAP, POP
 and Webmail servers and the LDAP, MySQL and PostgreSQL authentication
 modules. Only the installed parts of the Courier Mail Server show up
 in the administration frontend.
```

El proceso de instación es muy parecido al que se ha venido realizando hasta este momento:

Ejemplo 3-6. Instalación del paquete *courier-webadmin* (primera parte)

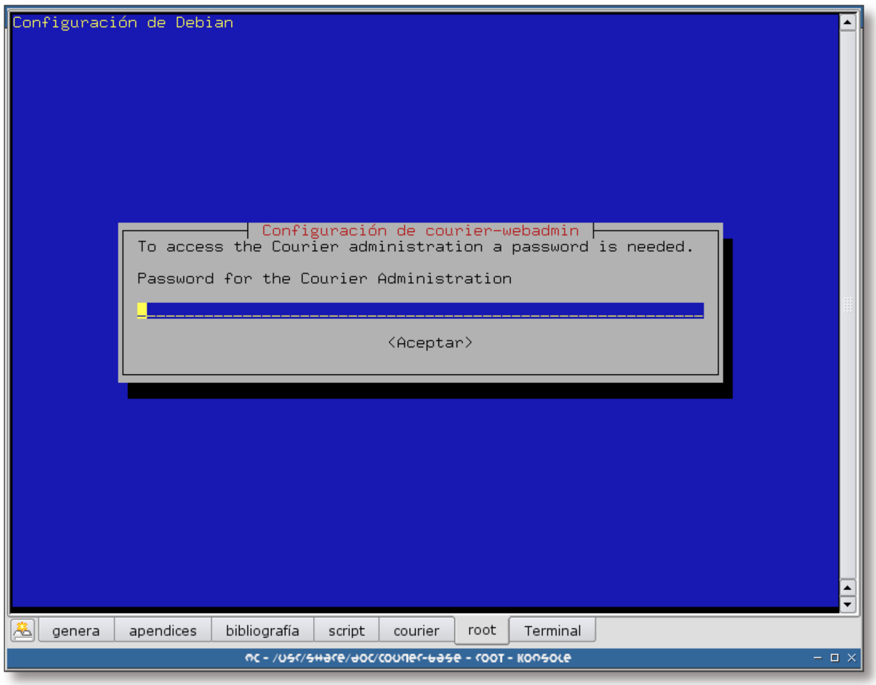
```
# /usr/bin/apt-get install courier-webadmin
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  courier-webadmin
0 actualizados, 1 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/32,1kB de archivos.
Se utilizarán 205kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...

--------------------- Sourcerer Apt Watcher ---------------------
Configure: courier-webadmin
-----------------------------------------------------------------
Seleccionando el paquete courier-webadmin previamente no seleccionado.
(Leyendo la base de datos ...
274038 ficheros y directorios instalados actualmente.)
Desempaquetando courier-webadmin (de .../courier-webadmin_0.45.4-1_i386.deb) ...
Configurando courier-webadmin (0.45.4-1) ...
```

Figura 3-1. Activación del programa CGI



Se responde afirmativamente a esta pregunta, para poder hacer uso de la interfaz web de administración.

Figura 3-2. Clave de administración



Teclee una clave para acceder al frontend de administración *webadmin* de Courier.

Ejemplo 3-7. Instalación del paquete *courier-webadmin* (segunda parte)

```
--------------------- Sourcerer Apt Watcher ---------------------
Configure: courier-webadmin
------------------------------------------------------------------
Seleccionando el paquete courier-webadmin previamente no seleccionado.
(Leyendo la base de datos ...
274038 ficheros y directorios instalados actualmente.)
Desempaquetando courier-webadmin (de .../courier-webadmin_0.45.4-1_i386.deb) ...
Configurando courier-webadmin (0.45.4-1) ...
```

Uso del frontend

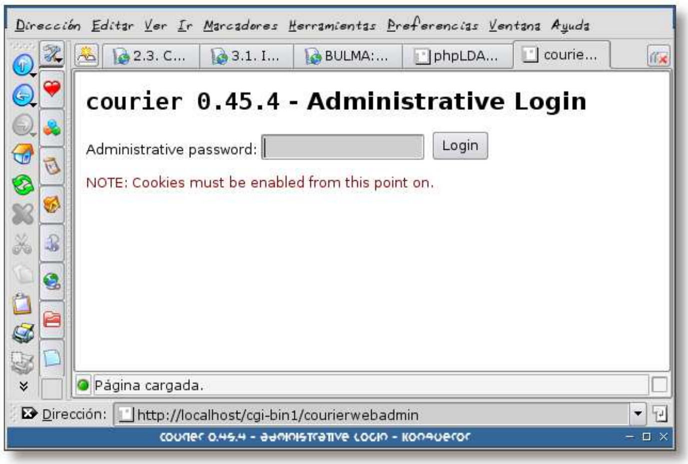
Una vez finalizada la instalación de *courier-webadmin*, se ha de acceder al mismo con el navegador web. Para ello, teclee la URL de su servidor web, seguida del directorio donde tiene almacenados los programas CGI y del nombre del frontend para la configuración de Courier, courierwebadmin.

Las siguientes secciones mostrarán algunos ejemplos de uso de este frontend.

Módulos de autentificación

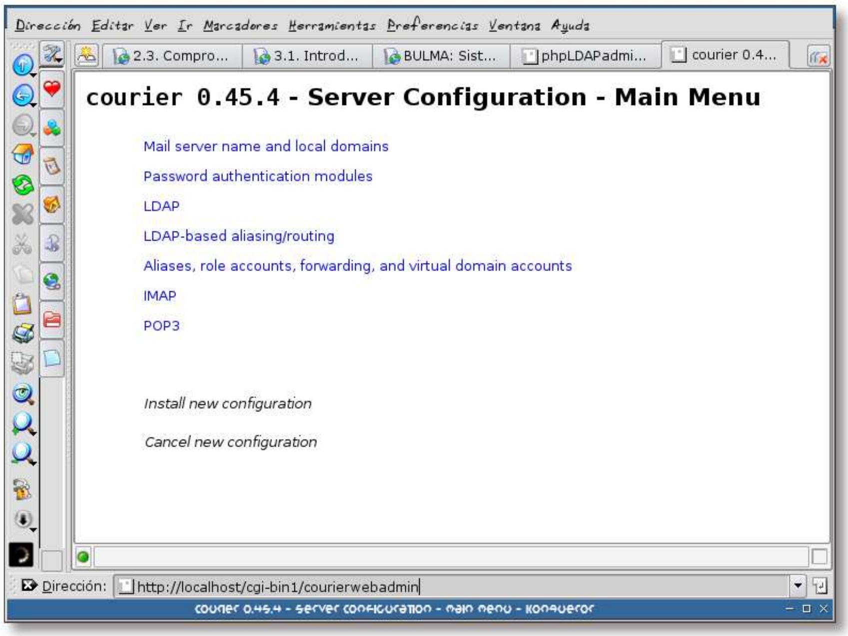
Sección dedicada a la configuración de los módulos utilizados por el demonio *authdaemon* para la autentificación de usuarios.

Figura 3-3. Clave de acceso



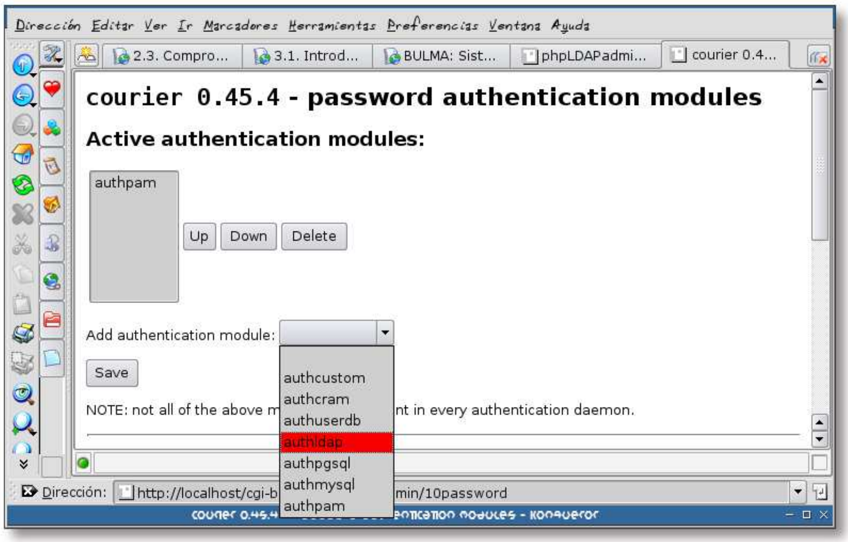
Teclee la clave de administración (esta clave es la misma que la que se ha tecleado en el proceso de instalación del frontend *courier-webadmin*: Figura 3-2).

Figura 3-4. Menú principal



Esta captura muestra el menú principal de la herramienta de configuración. Pulse sobre el enlace: *Password authentication modules*.

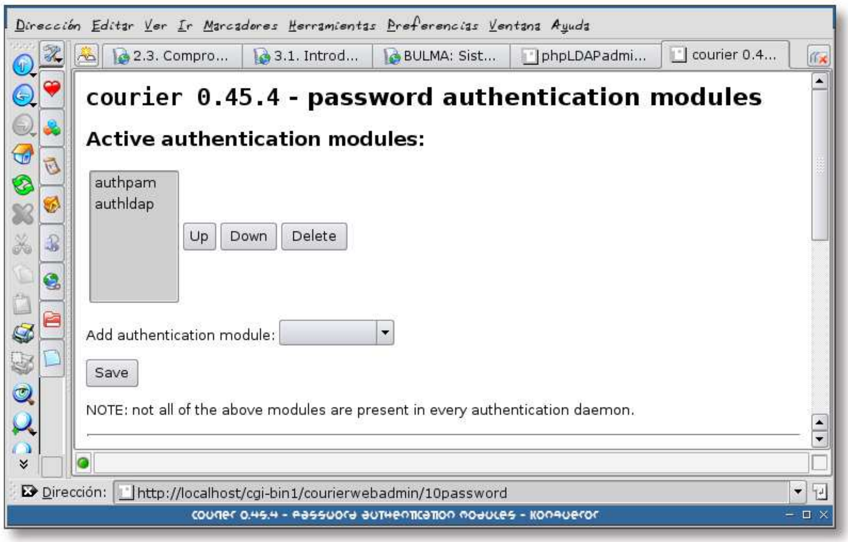
Figura 3-5. Módulos de authentificación, elección



Pulse sobre el menú desplegable *Add authentication module:* y seleccione el módulo que desee añadir, en este caso: “authldap”.

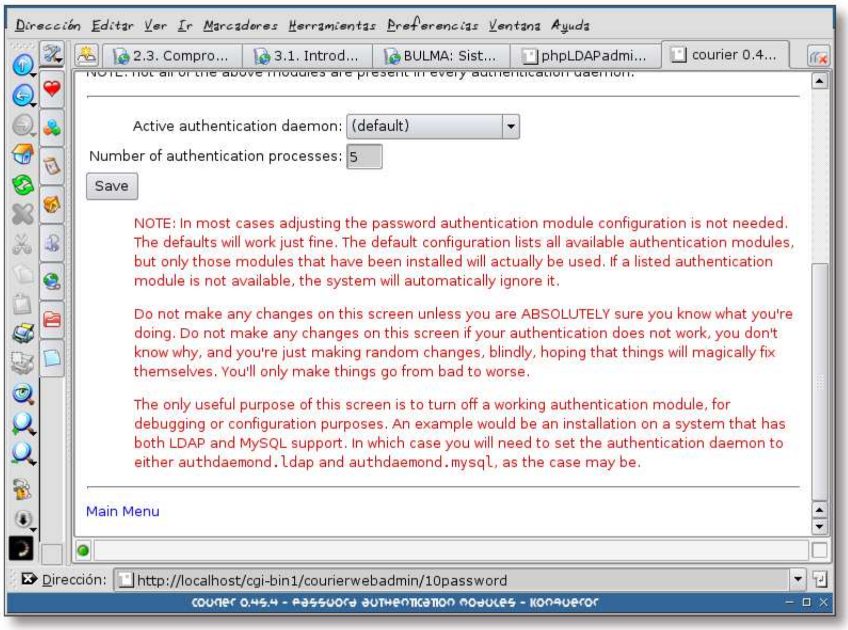
Una vez seleccionado, pulse sobre el botón “Save”.

Figura 3-6. Módulos de authentificación, módulo seleccionado



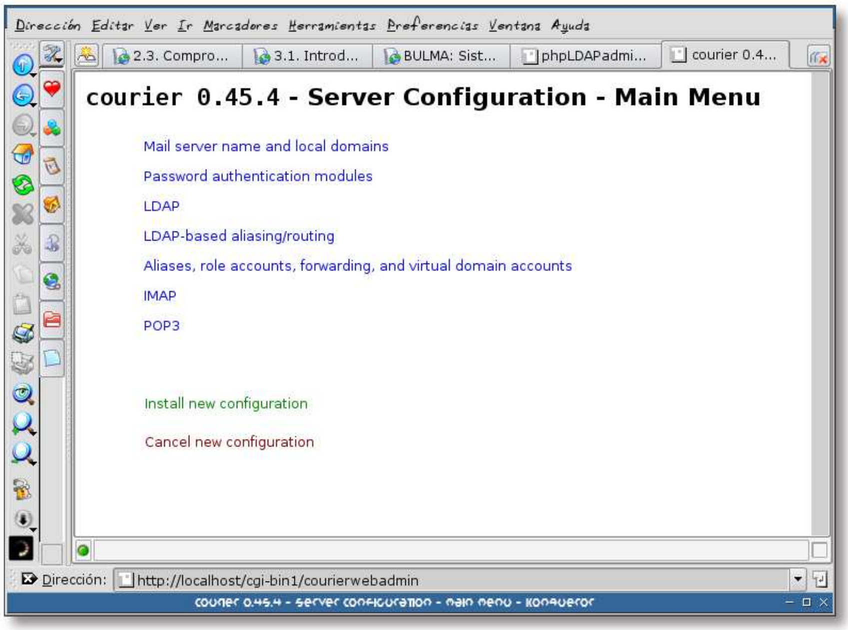
Se puede comprobar que en la lista de módulos de authentificación aparece uno nuevo: *authldap*.

Figura 3-7. Módulos de authentificación, volviendo al menú principal



Una vez que haya finalizado con esta sección, vaya al final de la página y pulse sobre el enlace: "Main menu" para regresar al menú principal.

Figura 3-8. Menú principal

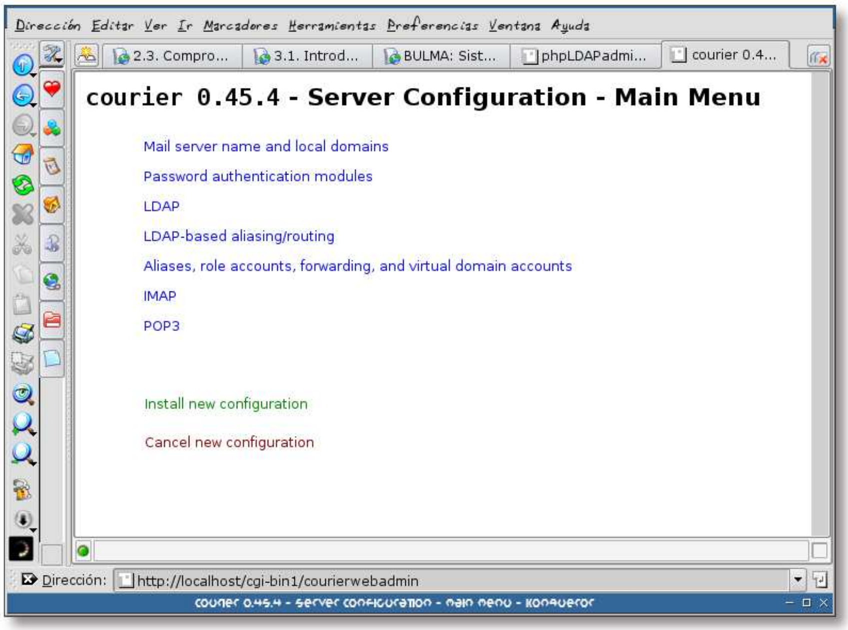


Si se fija, ahora aparecen dos nuevos enlaces en esta pantalla: *Install new configuration* y *Cancel new configuration*. Estos dos enlaces sirven para aplicar las modificaciones realizadas o no, respectivamente. De momento se va a continuar con la configuración, por lo que no se presiona sobre ninguno de ellos.

Configuración del soporte de LDAP

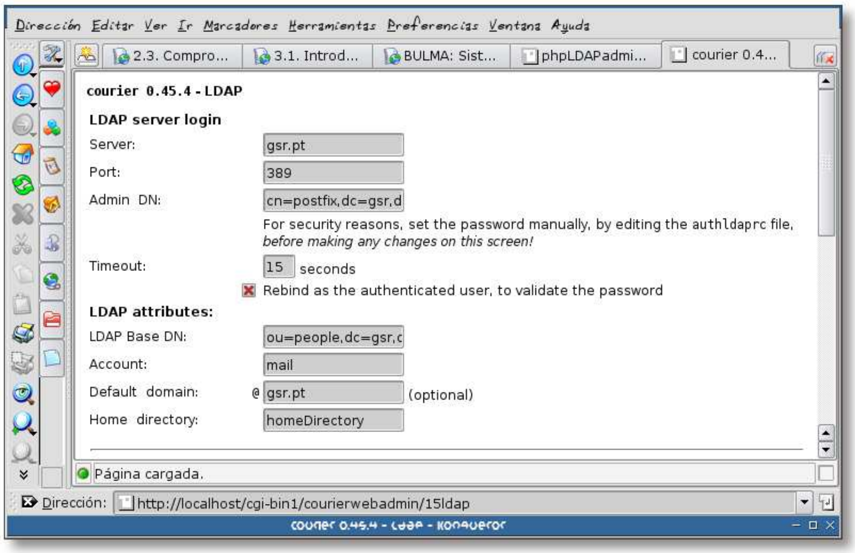
Como la autentificación de usuarios también se va a realizar a partir de un servidor LDAP, se han de configurar una serie de parámetros, para que el módulo *authdaemon* de Courier sepa como obtener la información del directorio LDAP:

Figura 3-9. Menú principal



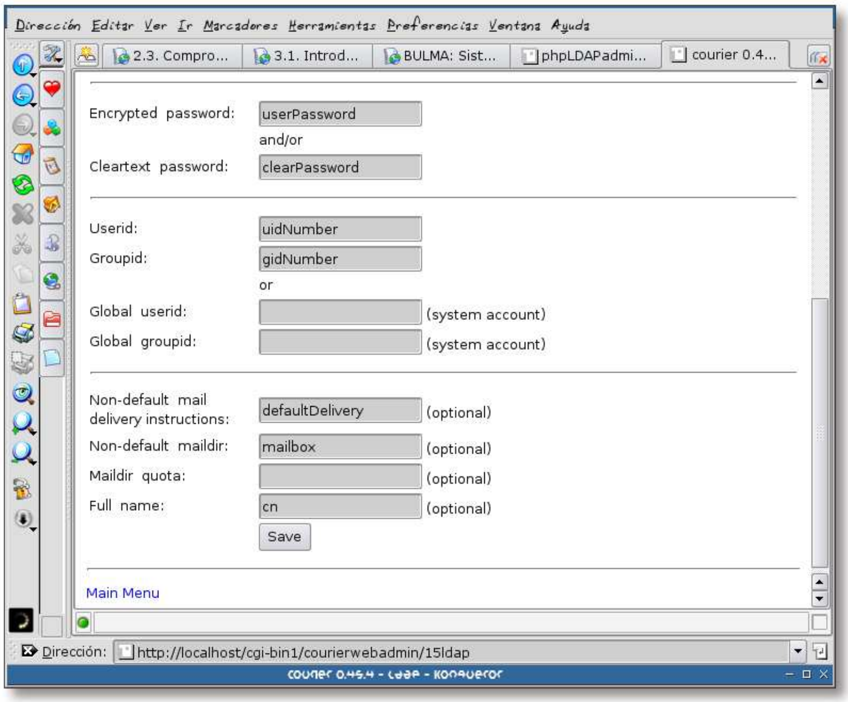
Pulse sobre el enlace *LDAP*.

Figura 3-10. Opciones de LDAP I



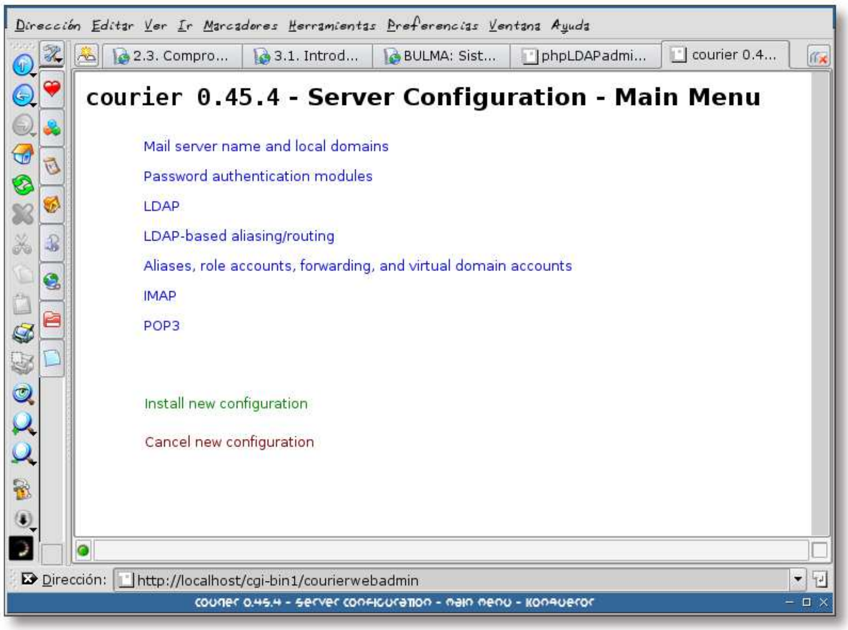
Complete la información con las características de su servidor LDAP. Tenga en cuenta, que tendrá que añadir *a mano* la clave del usuario con el que se vaya a autentificar en el servidor LDAP.

Figura 3-11. Opciones de LDAP II



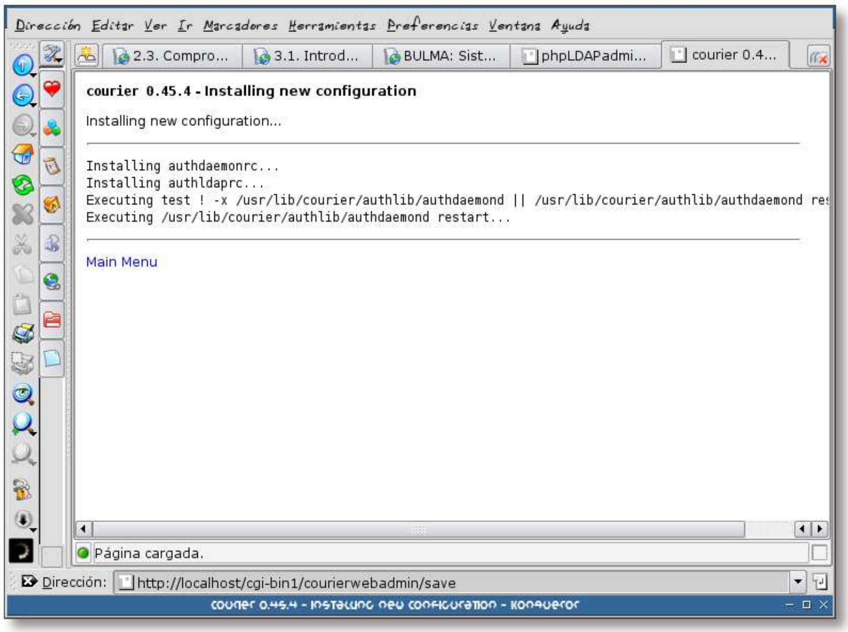
Una vez terminada la configuración de este apartado, pulse sobre el enlace “Main menu”, para regresar al menú principal.

Figura 3-12. Menú principal



En este momento se van a aplicar los cambios realizados, para ello, pulse sobre el enlace: "Install new configuration".

Figura 3-13. Aplicando la nueva configuración



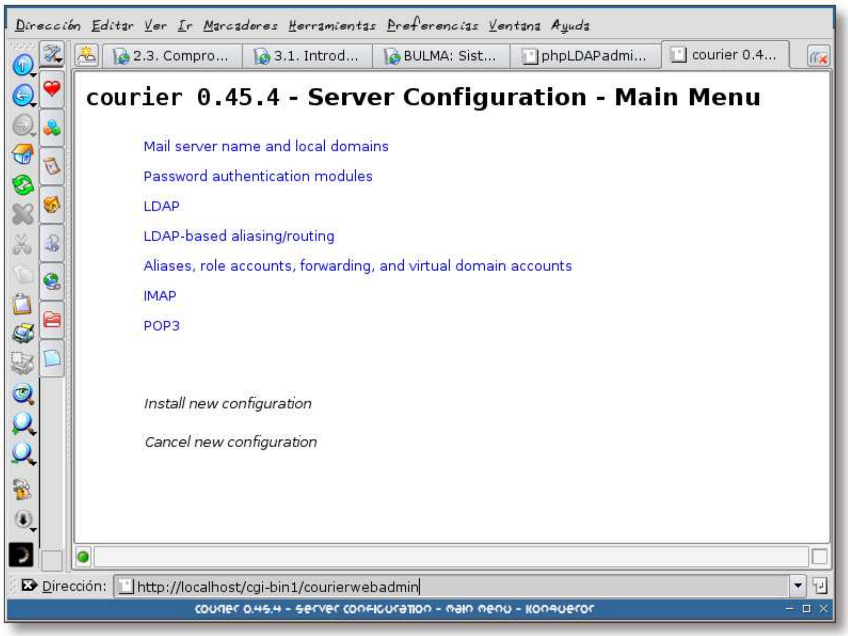
El frontend de administración, aplica los cambios a los archivos oportunos y reinicia el servidor *authdaemon*, que ha sido el servidor afectado por los cambios, en este caso.

Una vez se ha finalizado el proceso de instalación, pulse sobre el enlace "Main menu".

Opciones POP3

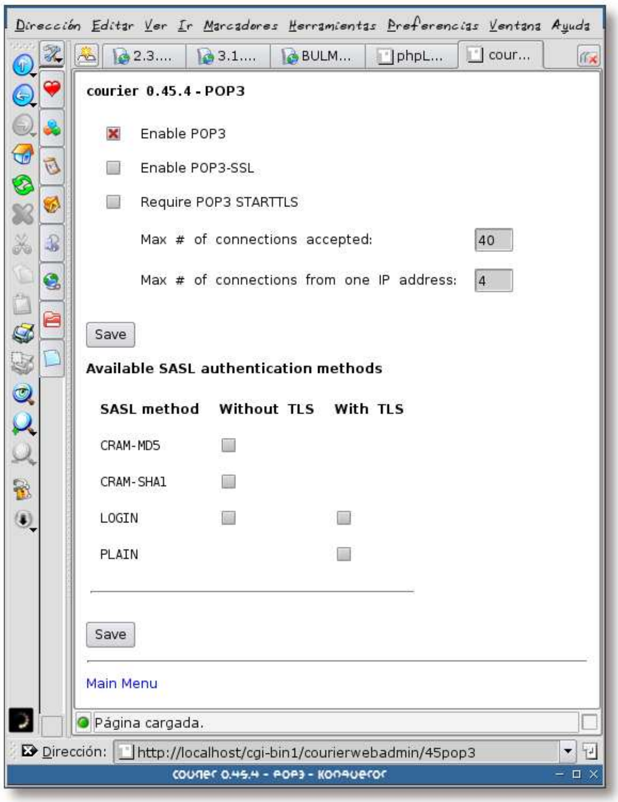
Esta sección es meramente informativa, no se va a realizar ningún cambio en el servidor POP3.

Figura 3-14. Menú principal



Pulse sobre el enlace “POP3” para acceder a las opciones de configuración de este servidor.

Figura 3-15. Opciones del servidor “POP3”

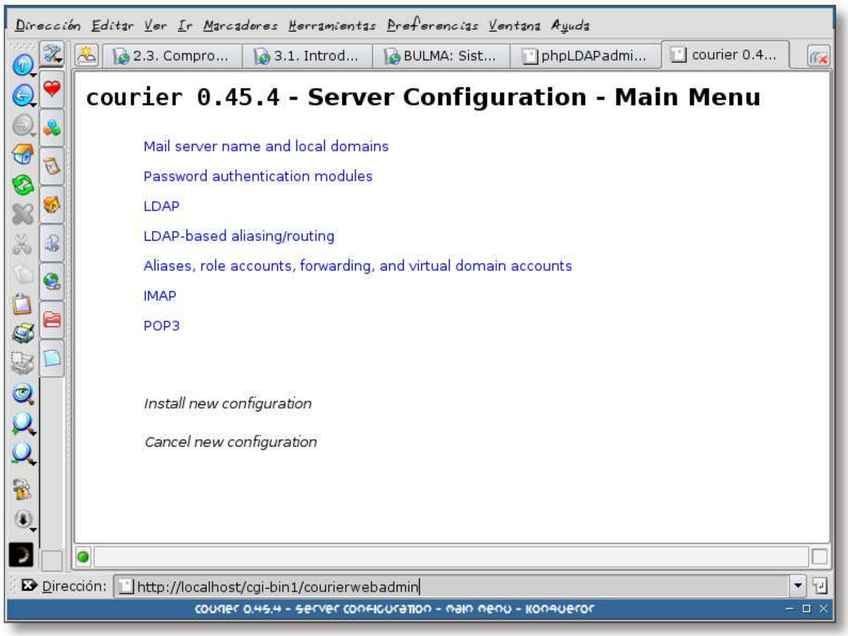


En esta pantalla se muestran las distintas opciones que se pueden seleccionar para establecer la configuración del servidor “POP3”. Una vez adecuadas a sus necesidades, pulse sobre el enlace “Main menu”.

Opciones IMAP

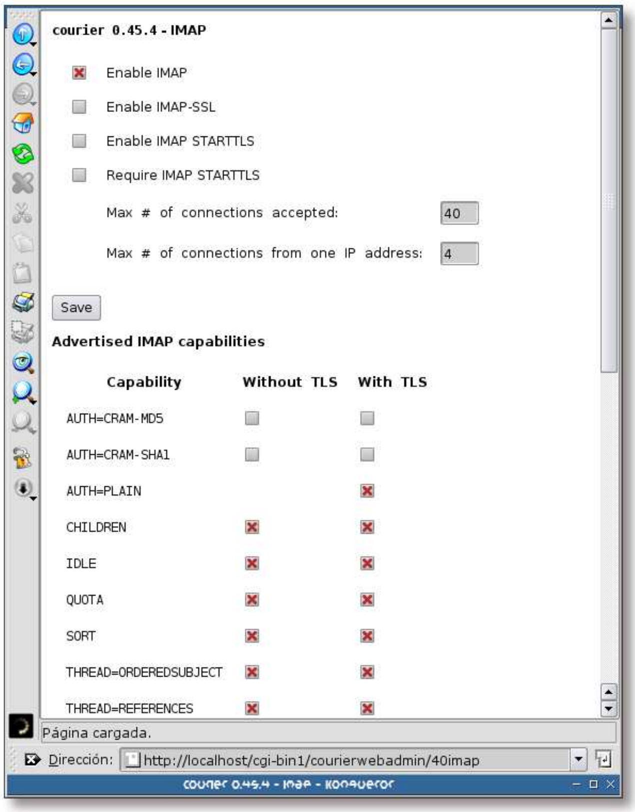
Esta sección es meramente informativa, no se va a realizar ningún cambio en el servidor IMAP3.

Figura 3-16. Menú principal



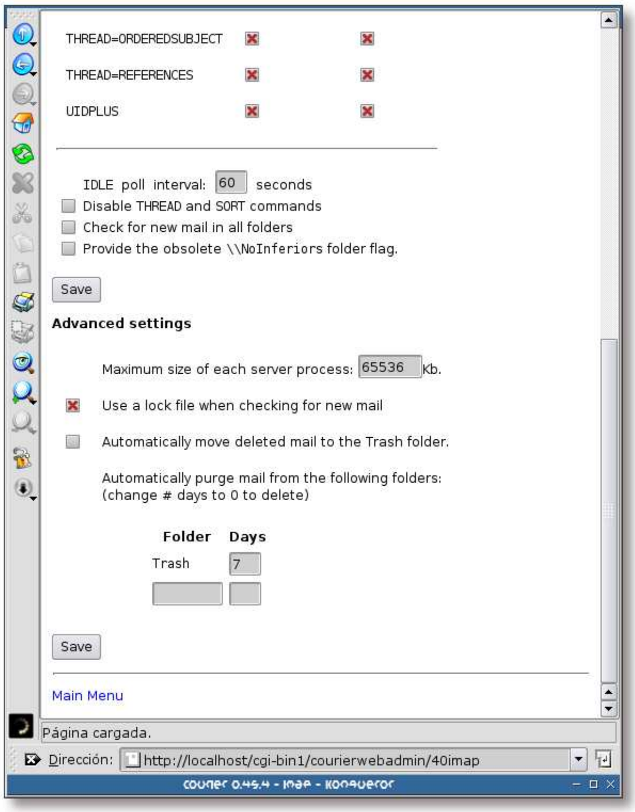
Pulse sobre el enlace "IMAP" para acceder a las opciones de configuración de este servidor.

Figura 3-17. Opciones del servidor IMAP I



Primeras opciones relativas al servidor IMAP.

Figura 3-18. Opciones del servidor IMAP II



Opciones finales del servidor IMAP. Cuando haya finalizado las modificaciones pertinentes, pulse sobre el enlace “Main menu”. Una vez en este, si es necesario, pulse sobre el enlace “Install new configuration”.

Capítulo 4. Pruebas de funcionamiento

Servidor POP3

Para verificar que el servidor POP3 está funcionando, se va a conectar al mismo con el comando **telnet**, realizando la autentificación. El ejemplo siguiente muestra como hacerlo:

> **Nota:** Las letras en negrita son los comandos que ha tecleado el usuario.

Ejemplo 4-1. Conexión al servidor POP3 con telnet

```
$ /usr/bin/telnet gsr.pt 110
Trying x.x.x.x...
Connected to gsr.pt.
Escape character is '^]'.
+OK Hello there.
user severa ❶
+OK Password required.
pass ******** ❷
+OK logged in. ❸
list ❹
+OK POP3 clients that break here, they violate STD53.
1 413
2 412
3 406
4 406
.
retr 1 ❺
+OK 413 octets follow.
Return-Path: <sergio@todoscsi.gsr.pt>
X-Original-To: severa
Delivered-To: severa@todoscsi.gsr.pt
Received: by todoscsi.gsr.pt (Postfix, from userid 1000)
        id 248A03C; Sat,  5 Jun 2004 21:20:41 +0100 (WEST)
To: severa@todoscsi.gsr.pt
Subject: hola
Message-Id: <20040605202041.248A03C@todoscsi.gsr.pt>
Date: Sat,  5 Jun 2004 21:20:41 +0100 (WEST)
From: sergio@todoscsi.gsr.pt (Sergio González González)

.
quit ❻
+OK Bye-bye.
Connection closed by foreign host.
```

❶ Se indica el usuario con el cual se quiere conectar al servidor.

❷ Se teclea la clave del usuario.

❸ Se ha entrado al servidor POP3 satisfactoriamente.

❹ Se listan los correos disponibles en el buzón del usuario.

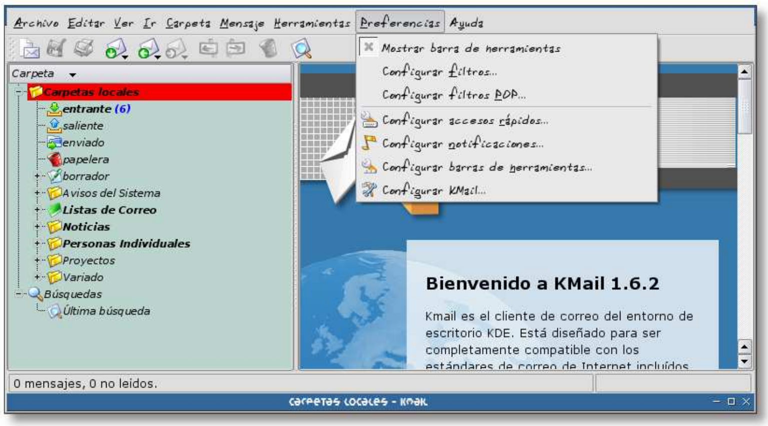
❺ Se obtiene el primer correo de la lista.

❻ Se abandona el servidor POP3.

Servidor IMAP

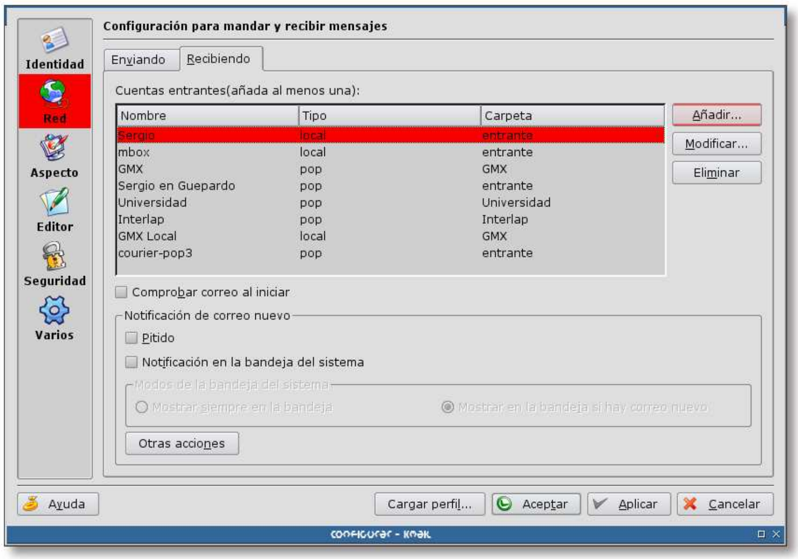
Las pruebas con el servidor IMAP se van a realizar desde el gestor de correo kmail. Las siguientes capturas mostrarán la forma de acceso al dicho servidor:

Figura 4-1. Ejecución de Kmail



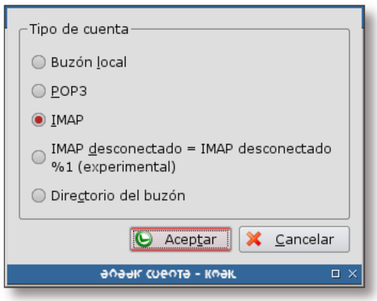
Se ejecuta Kmail y una vez arrancado, se pulsa sobre el menú *Preferencias -> Configurar Kmail...* para añadir la cuenta IMAP.

Figura 4-2. Añadiendo una cuenta IMAP



Se accede a: *Red -> Recibiendo* y se pulsa en el botón “Añadir”.

Figura 4-3. Selección de una cuenta IMAP



Seleccione el tipo de cuenta IMAP y pulse sobre “Aceptar”.

Figura 4-4. Datos de la cuenta

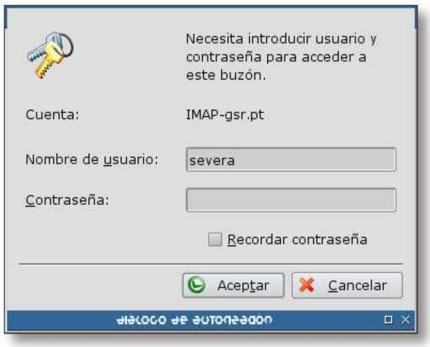
Complete la información necesaria en la pestaña *General* y pulse sobre la pestaña “Seguridad”.

Figura 4-5. Opciones de seguridad

Pulse sobre el botón "Comprobar qué soporta el servidor"; despues de un momento de espera, debería aparecer una pantalla como la que se muestra en esta imagen: de momento el servidor no soporta ningún tipo de cifrado ni de método de autentificación alternativo.

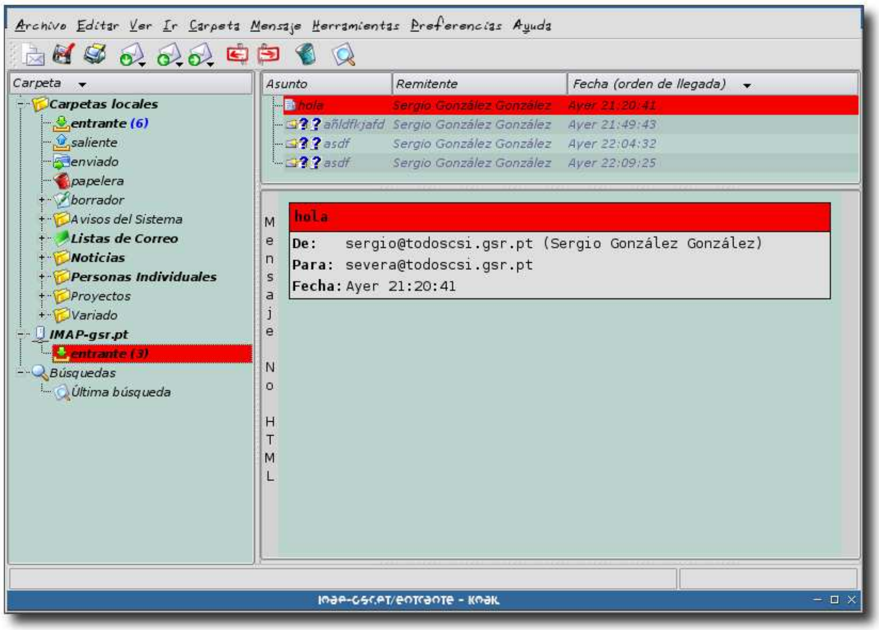
Cuando finalice, pulse sobre el botón "Aceptar".

Figura 4-6. Clave del usuario



Inmediatamente después de pulsar sobre el botón "Aceptar" de la pantalla anterior, se pedirá la clave para la nueva cuenta que se acaba de añadir (siempre y cuando no se haya introducido en el campo correspondiente de la pantalla de configuración). Tecléela y pulse sobre "Aceptar".

Figura 4-7. Acceso a la cuenta IMAP



Una vez se ha finalizado la creación de la cuenta, se puede observar que en la lista de carpetas de Kmail, ha aparecido una nueva carpeta denominada: *IMAP-gsr.pt*. Si accedemos a la subcarpeta *entrante* veremos el correo para el usuario “severa”, ya que ha sido el usuario para el cual se ha configurado la cuenta IMAP.

IV. Squirrelmail

Capítulo 5. Instalación y configuración de squirrelmail

Instalación

La forma de instalar squirrelmail se muestra en el siguiente ejemplo:

Ejemplo 5-1. Instalación del paquete *squirrelmail*

```
# /usr/bin/apt-get install squirrelmail
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  squirrelmail
0 actualizados, 1 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/675kB de archivos.
Se utilizarán 3957kB de espacio de disco adicional después de desempaquetar.
--------------------- Sourcerer Apt Watcher ---------------------
Configure: squirrelmail
-----------------------------------------------------------------
(Leyendo la base de datos ...
273612 ficheros y directorios instalados actualmente.)
Desempaquetando squirrelmail (de .../squirrelmail_1%3a1.5.0-1_all.deb) ...
Configurando squirrelmail (1.5.0-1) ...
Installing default squirrelmail config.
Run /usr/sbin/squirrelmail-configure as root to configure/upgrade config. ❶
```

❶ Para configurar squirrelmail se ha de ejecutar este script. Debido a la facilidad de configuración que ofrece dicho script, no se va a mostrar el proceso de configuración en esta documentación, se insta al lector a que lo ejecute y adapte las opciones a sus necesidades.

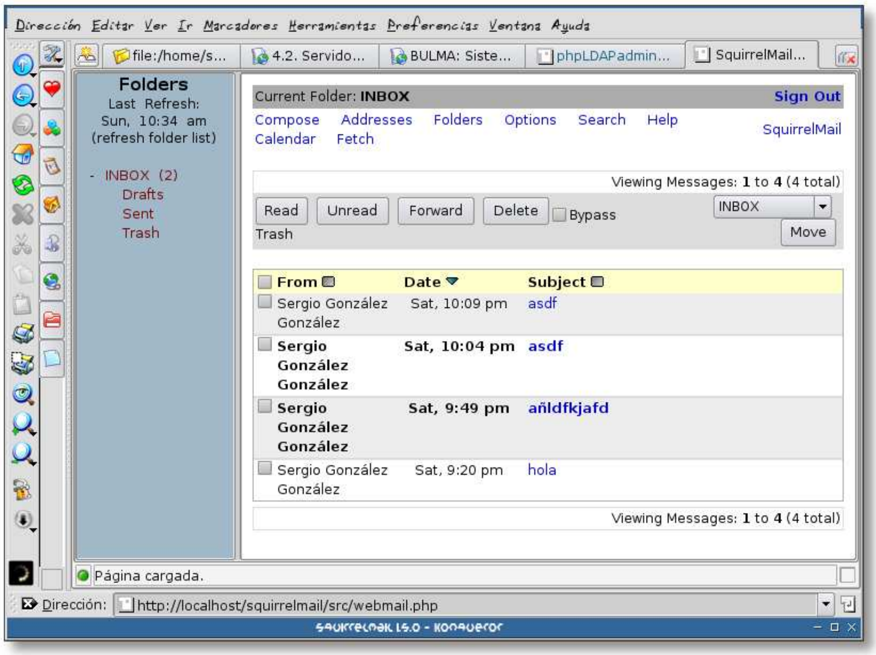
Acceso a la herramienta

Lectura y envío de correos

Figura 5-1. Ingreso en la aplicación

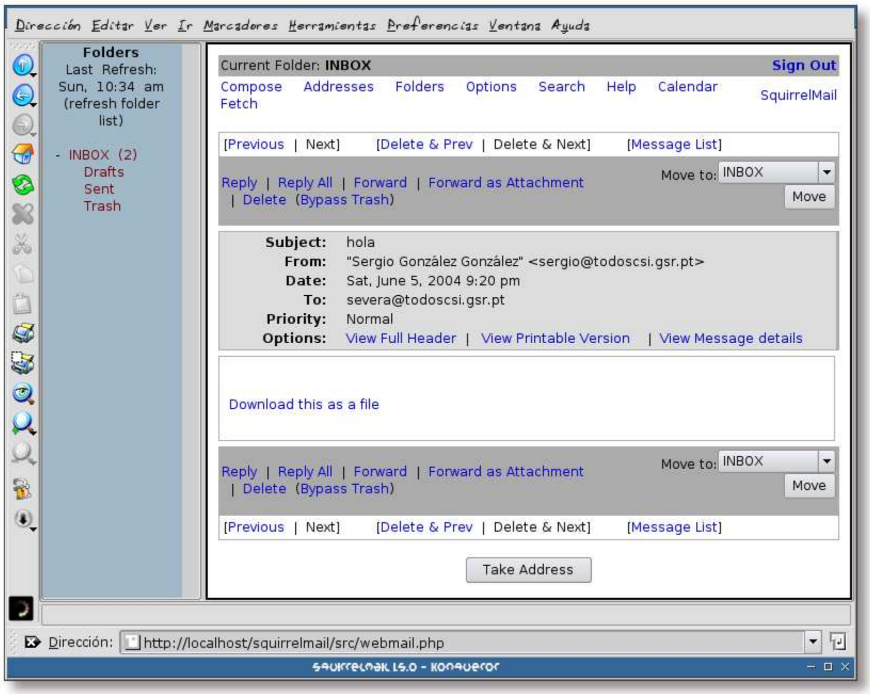
Teclee el nombre y clave de la cuenta a utilizar y pulse sobre el botón “Login”.

Figura 5-2. Lista de mensajes



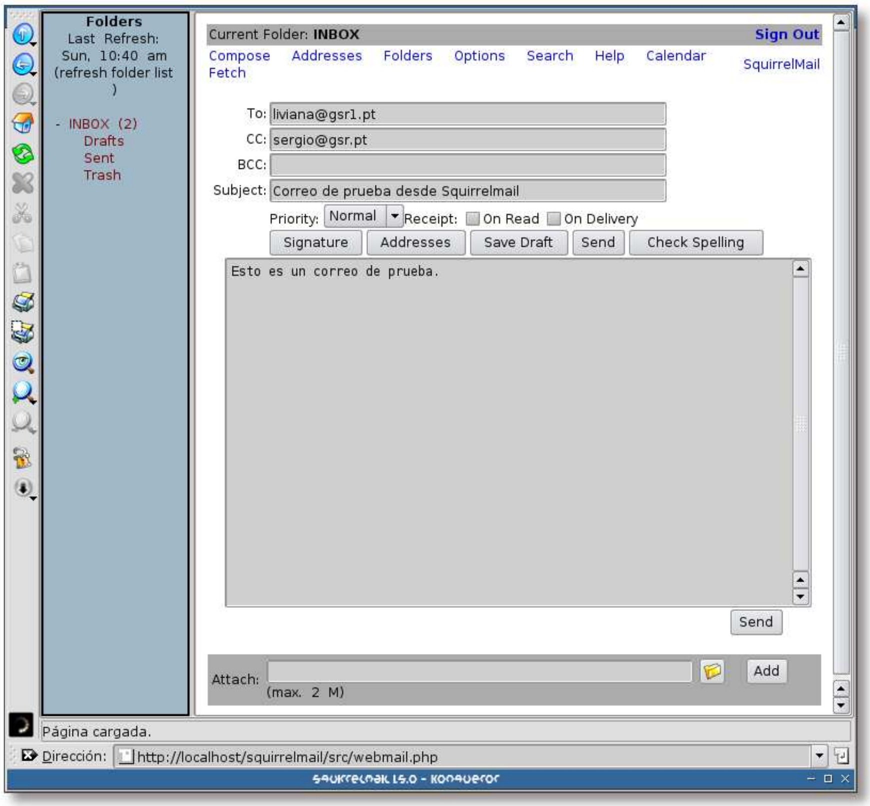
La primera pantalla, tras el ingreso, es la lista de correos existentes en la carpeta *INBOX*. Si se pulsa sobre el asunto de un correo, se procederá a mostrar su contenido.

Figura 5-3. Mostrando el contenido de un correo



Esta pantalla muestra el contenido de un correo. Este correo no posee ninguna información en el cuerpo del mismo.

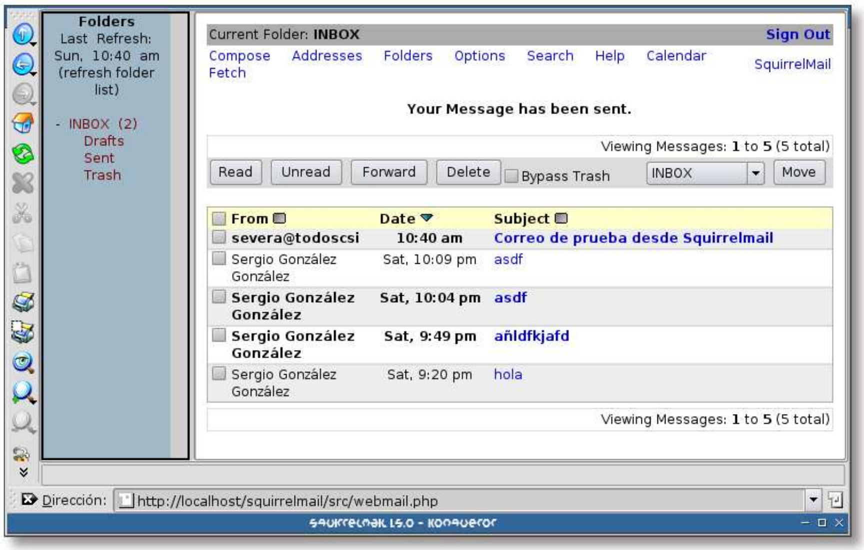
Figura 5-4. Creando un nuevo correo



La creación de un nuevo correo se hace gracias al enlace "Compose" que aparece en el menú superior de la aplicación. Al pulsar sobre el mismo, aparecerá una pantalla similar a la que se muestra en la figura.

Cuando se ha terminado de escribir el correo, se ha de pulsar sobre el botón "Send".

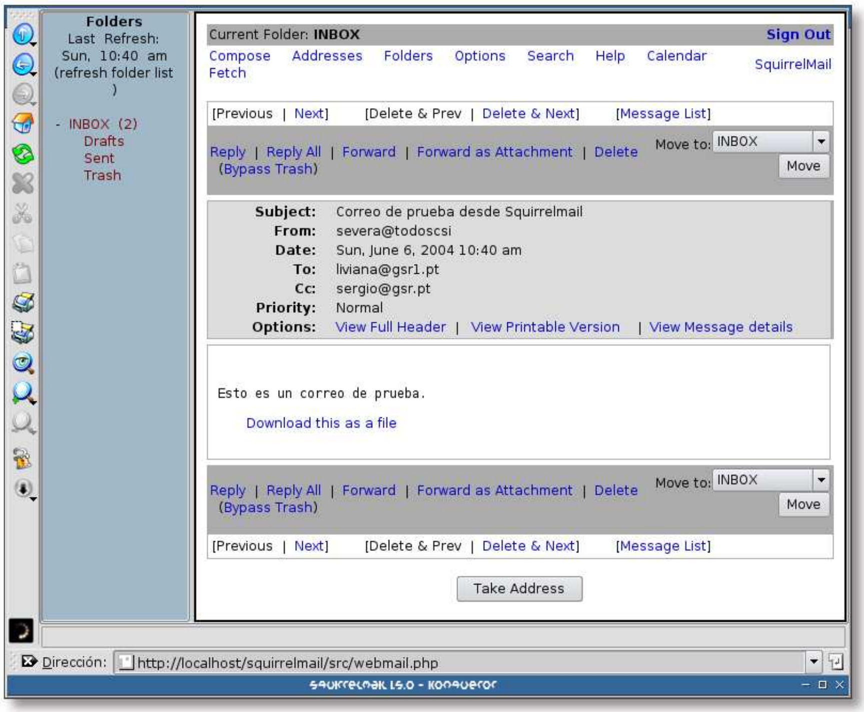
Figura 5-5. Recibiendo mensajes



Cuando se ha enviado un mensaje, Squirrelmail informa con el texto: *Your Message has been sent.*, como se puede apreciar en esta pantalla.

Como el mensaje iba dirigido a la cuenta desde la cual se escribió, ya aparece en la lista de correos.

Figura 5-6. Lectura de un correo

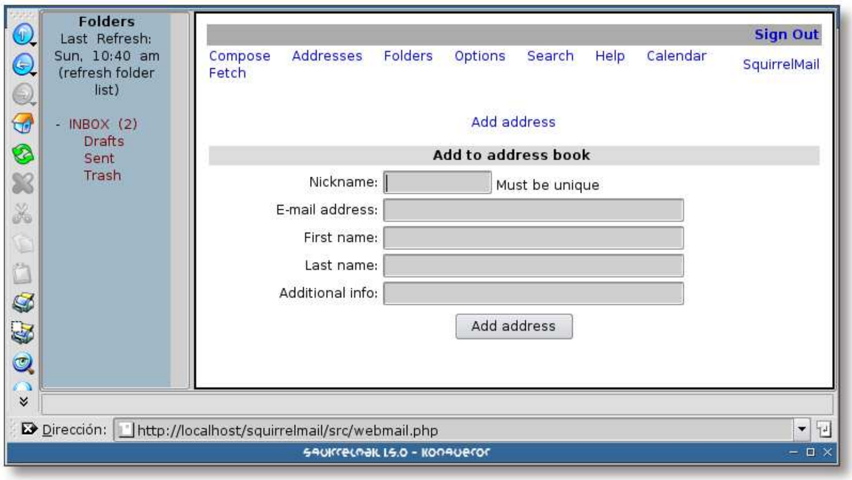


Al pulsar sobre el asunto del correo que acaba de llegar, accederemos a su contenido, como ya se ha visto anteriormente.

Características de Squirrelmail

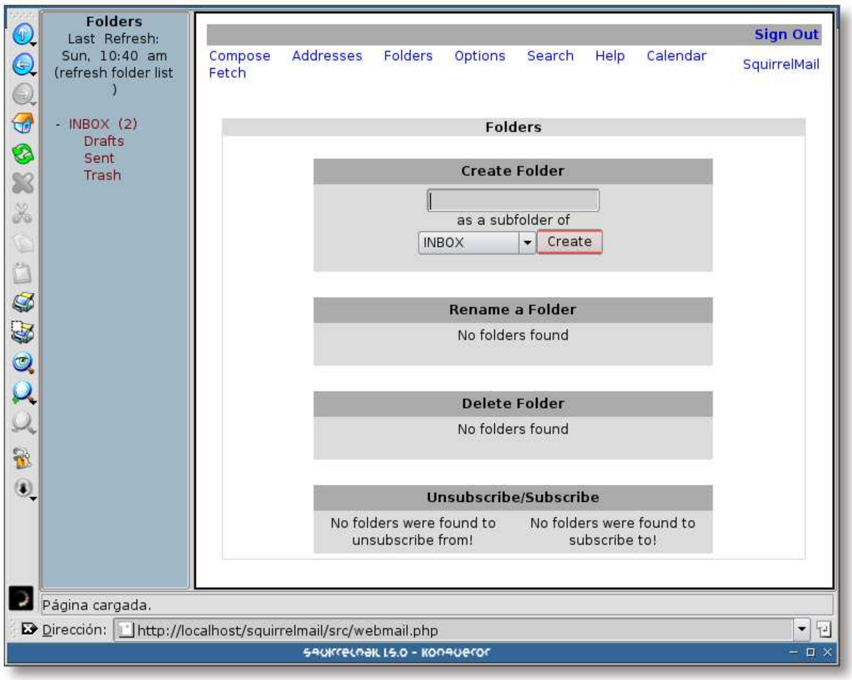
Squirrelmail, a parte de ser un gestor de correo vía web, incorpora una serie de funcionalidades, como las que se listarán en las siguientes capturas:

Figura 5-7. Libreta de direcciones



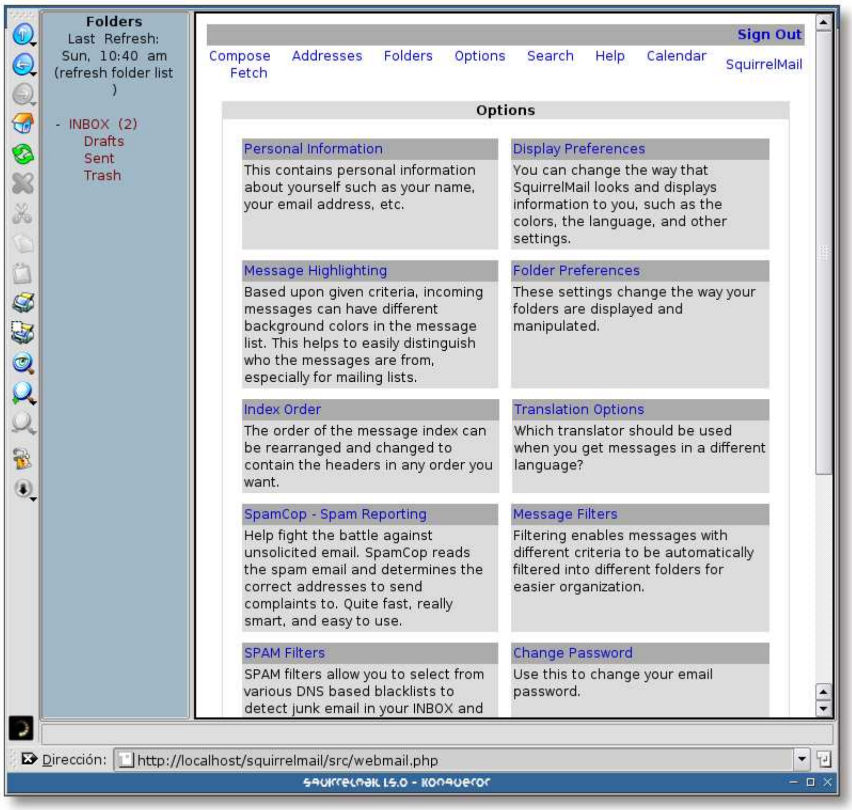
Desde Squirrelmail se puede mantener una libreta de direcciones de correo. El interfaz para gestionarla se muestra en esta captura.

Figura 5-8. Creación de nuevas carpetas



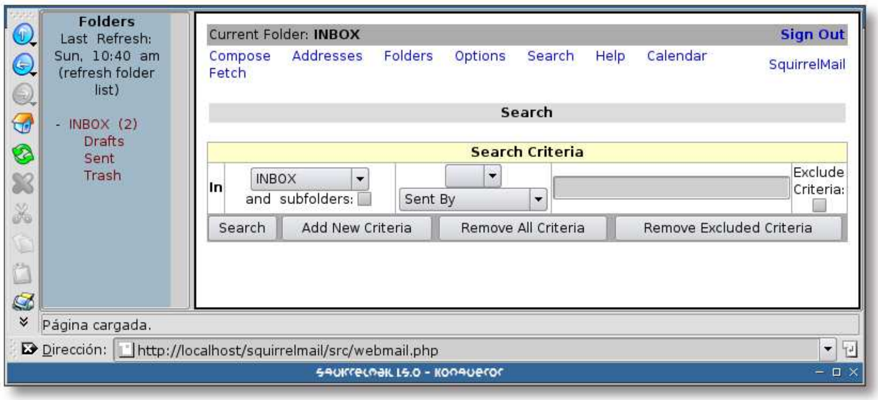
Para mantener el correo organizado, normalmente se hace uso de carpetas clasificatorias. Por este motivo, Squirrelmail dispone de una sección dedicada a la gestión de carpetas.

Figura 5-9. Lista de opciones



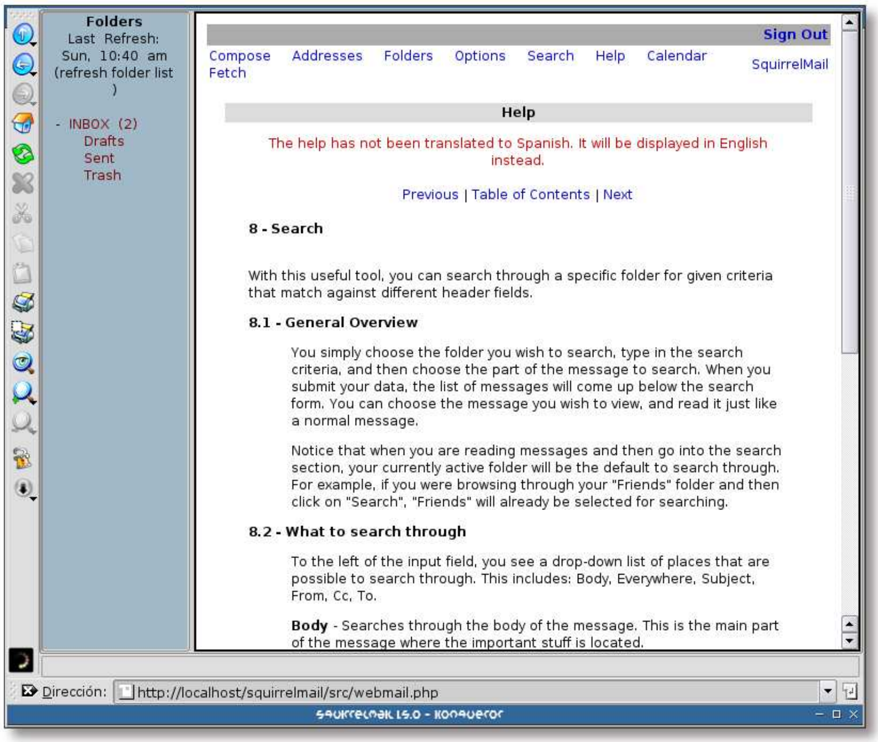
Desde esta pantalla se puede personalizar la configuración de Squirrelmail y de la cuenta IMAP que se está usando.

Figura 5-10. Búsquedas



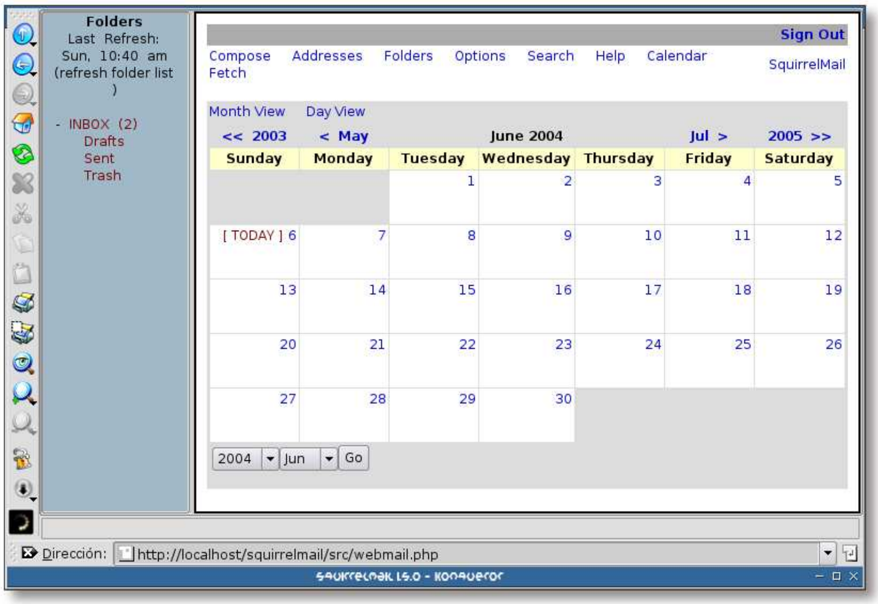
Squirrelmail dispone de un apartado dedicado a las búsquedas, siendo especialmente útil para encontrar correos con determinadas características.

Figura 5-11. Ayuda



Si en cualquier momento se encuentra perdido y necesita ayuda sobre una funcionalidad de Squirrelmail, puede pulsar sobre el enlace “Help” para obtenerla.

Figura 5-12. Calendario



Squirrelmail también dispone de un calendario de actividades, desde el cual se pueden mantener las tareas pendientes.

Figura 5-13. Recogida de correo desde cuentas POP

Otra de las opciones que posee este gestor de correo, es la posibilidad de obtener mensajes de correo desde buzones POP.

Saliendo de la aplicación

Figura 5-14. Saliendo de Squirrelmail

En cualquier momento se puede pulsar sobre el enlace "Sign Out" para cerrar la sesión. Una vez pulsado sobre el mismo, aparecerá esta pantalla.

V. Filtrado de mensajes con Clamav y Spamassassin

Capítulo 6. Instalación

Introducción

Este capítulo se va a encargar del proceso de instalación de las herramientas de filtrado destinadas al control de SPAM y virus desde Postfix.

Como se va a hacer uso de amavisd-new, que posee interfaces para las aplicaciones spamassassin y clamav, el proceso de instalación y configuración de estas herramientas está muy interligado.

> **Nota:** Este capítulo se ha basado en la entrada bibliográfica Pereda01.

Instalación del software necesario

El proceso de instalación de las aplicaciones va a comenzar por la herramienta *amavisd-new*, a partir de la cual, se procederá a la instalación de las herramientas restantes. Se pondrá especial atención en las sugerencias y recomendaciones de los paquetes sugetos a instalación.

Instalación del paquete *amavisd-new*

Ejemplo 6-1. Instalación del paquete *amavisd-new*

```
# /usr/bin/apt-get install amavisd-new
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  libarchive-tar-perl libarchive-zip-perl libconvert-tnef-perl libconvert-uulib-perl libio-multiplex-perl
  libio-zlib-perl libnet-perl libnet-server-perl libunix-syslog-perl
Paquetes sugeridos:
  spamassassin clamav clamav-daemon lha zoo ❶
Paquetes recomendados
  libnet-ph-perl libnet-snpp-perl libnet-telnet-perl ❷
Se instalarán los siguientes paquetes NUEVOS:
  amavisd-new libarchive-tar-perl libarchive-zip-perl libconvert-tnef-perl libconvert-uulib-perl
  libio-multiplex-perl libio-zlib-perl libnet-perl libnet-server-perl libunix-syslog-perl
0 actualizados, 10 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/828kB de archivos.
Se utilizarán 2613kB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n]
Preconfiguring packages ...
--------------------- Sourcerer Apt Watcher ---------------------
Configure: libio-zlib-perl
-----------------------------------------------------------------
(Leyendo la base de datos ...
274080 ficheros y directorios instalados actualmente.)
Desempaquetando libio-zlib-perl (de .../libio-zlib-perl_1.01-2_all.deb) ...
Desempaquetando libarchive-tar-perl (de .../libarchive-tar-perl_1.08-1_all.deb) ...
Desempaquetando libarchive-zip-perl (de .../libarchive-zip-perl_1.05-1_all.deb) ...
```

```
Desempaquetando libconvert-tnef-perl (de .../libconvert-tnef-perl_0.17-3_all.deb) ...
Desempaquetando libconvert-uulib-perl (de .../libconvert-uulib-perl_1.0.1-1_i386.deb) ...
Seleccionando el paquete libio-multiplex-perl previamente no seleccionado.
Desempaquetando libio-multiplex-perl (de .../libio-multiplex-perl_1.04-1_all.deb) ...
Seleccionando el paquete libnet-perl previamente no seleccionado.
Desempaquetando libnet-perl (de .../libnet-perl_1%3a1.18-2_all.deb) ...
Seleccionando el paquete libnet-server-perl previamente no seleccionado.
Desempaquetando libnet-server-perl (de .../libnet-server-perl_0.85-3_all.deb) ...
Seleccionando el paquete libunix-syslog-perl previamente no seleccionado.
Desempaquetando libunix-syslog-perl (de .../libunix-syslog-perl_0.100-2_i386.deb) ...
Seleccionando el paquete amavisd-new previamente no seleccionado.
Desempaquetando amavisd-new (de .../amavisd-new_20030616p7-3_all.deb) ...
Configurando libio-zlib-perl (1.01-2) ...
Configurando libarchive-tar-perl (1.08-1) ...
Configurando libarchive-zip-perl (1.05-1) ...
Configurando libconvert-tnef-perl (0.17-3) ...
Configurando libconvert-uulib-perl (1.0.1-1) ...
Configurando libio-multiplex-perl (1.04-1) ...
Configurando libnet-perl (1.18-2) ...

Configurando libnet-server-perl (0.85-3) ...
Configurando libunix-syslog-perl (0.100-2) ...
Configurando amavisd-new (20030616p7-3) ...
Creating/updating amavis user account...
Añadiendo el grupo amavis (136)...
Hecho.
Añadiendo usuario del sistema amavis...
Añadiendo nuevo usuario amavis (129) con grupo amavis.
Starting amavisd: amavisd-new.
```

❶ Lista de paquetes que *amavisd-new* sugiere instalar. Entre ellos se encuentran los programas de antivirus y control de SPAM que se van a emplear. También se sugiere la instación de una serie de programas de manipulado de archivos comprimidos.

❷ Lista de paquetes recomendados por *amavisd-new*. Bajo esta lista se encuentran librerías de Perl dedicadas a proveer funciones de conexión a distintos protocolos de red.

Instalación del paquete *spamassassin*

Ejemplo 6-2. Instalación del paquete *spamassassin*

```
# /usr/bin/apt-get install spamassassin
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  spamc
Paquetes sugeridos:
  razor pyzor libnet-ident-perl ❶
Paquetes recomendados ❷
  libmail-spf-query-perl
Se instalarán los siguientes paquetes NUEVOS:
  spamassassin spamc
0 actualizados, 2 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/664kB de archivos.
```

```
Se utilizarán 2019kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...
--------------------- Sourcerer Apt Watcher ---------------------
Configure: spamc
-----------------------------------------------------------------
Seleccionando el paquete spamc previamente no seleccionado.
(Leyendo la base de datos ...
274315 ficheros y directorios instalados actualmente.)
Desempaquetando spamc (de .../archives/spamc_2.63-1_i386.deb) ...
Seleccionando el paquete spamassassin previamente no seleccionado.
Desempaquetando spamassassin (de .../spamassassin_2.63-1_all.deb) ...
Configurando spamc (2.63-1) ...
Configurando spamassassin (2.63-1) ...
```

❶ Lista de paquetes que *spamassassin* sugiere instalar. Entre ellos se encuentran programas dedicados a la actualización desde Internet, de la lista de filtros dedicados a la detección de SPAM.

❷ Lista de paquetes recomendados por *spamassassin*.

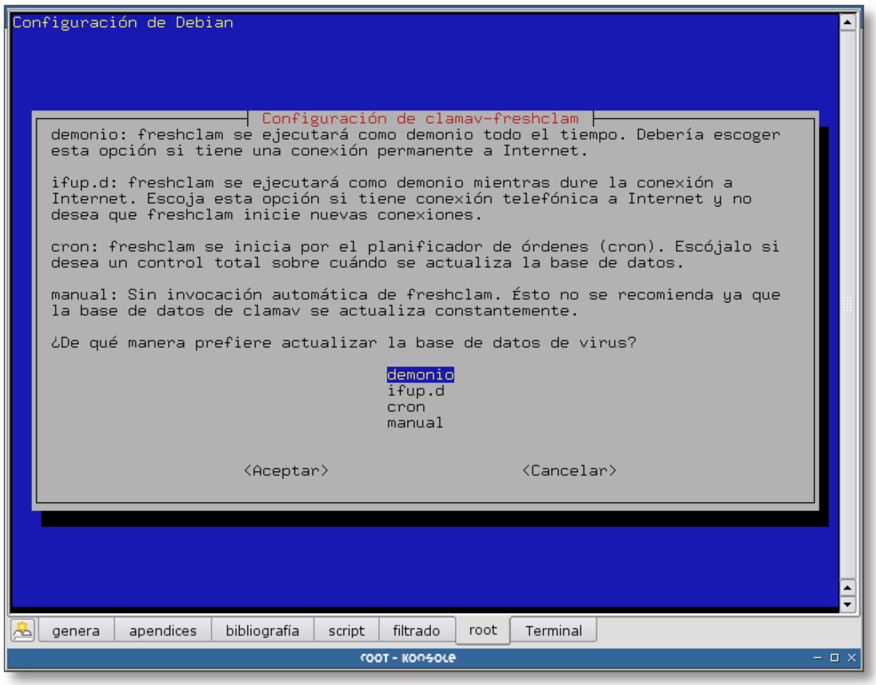
Instalación de *Clamav*

Ejemplo 6-3. Instalación de *Clamav* (primera parte)

```
# apt-get install clamav
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... 50%
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  clamav-base clamav-freshclam libclamav1
Paquetes sugeridos: ❶
  lha
Se instalarán los siguientes paquetes NUEVOS:
  clamav clamav-base clamav-freshclam libclamav1
0 actualizados, 4 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/2194kB de archivos.
Se utilizarán 3490kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...
```

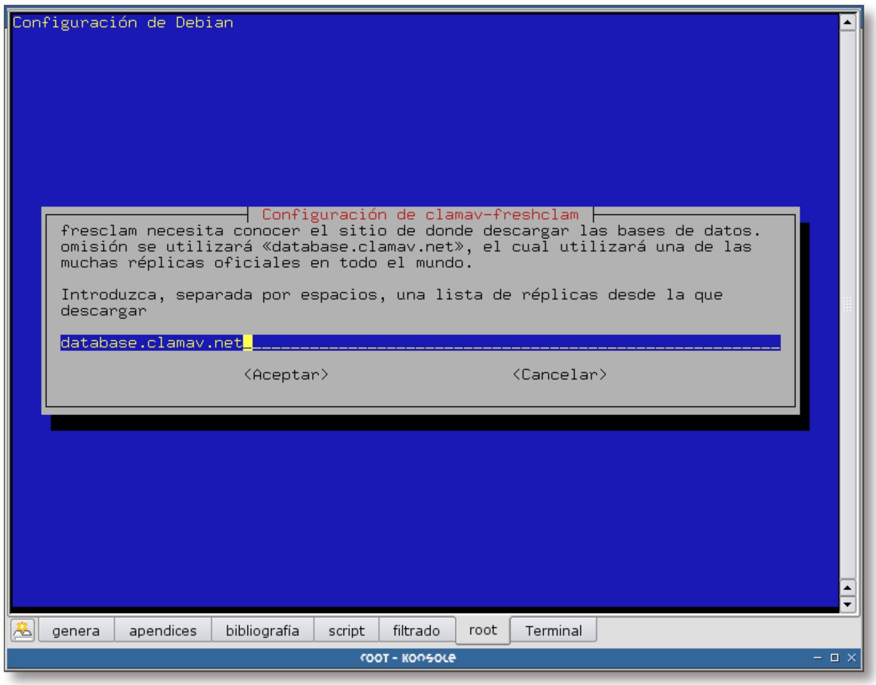
❶ *clamav* sugiere instalar el paquete *lha*, paquete ya recomendado en el Ejemplo 6-1.

Figura 6-1. Modo de actualización de la base de datos



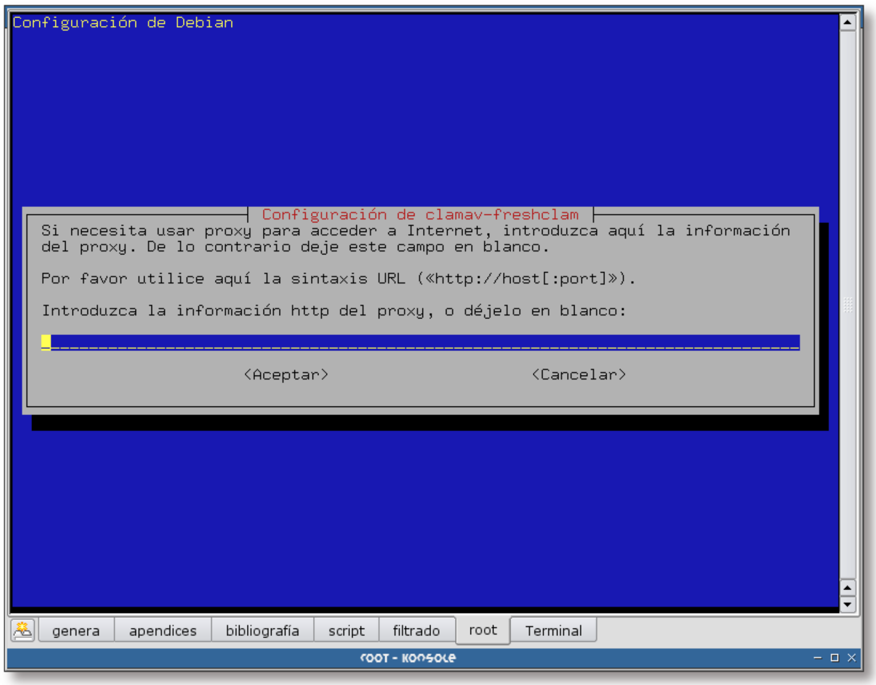
El paquete *clamav-freshclam* permite actualizar la base de datos de virus desde Internet. Esta herramienta se puede ejecutar de varias formas, detalladas en la captura de pantalla. La forma elegida en esta documentación ha sido el modo *demonio*.

Figura 6-2. Servidor para descargar la base de datos



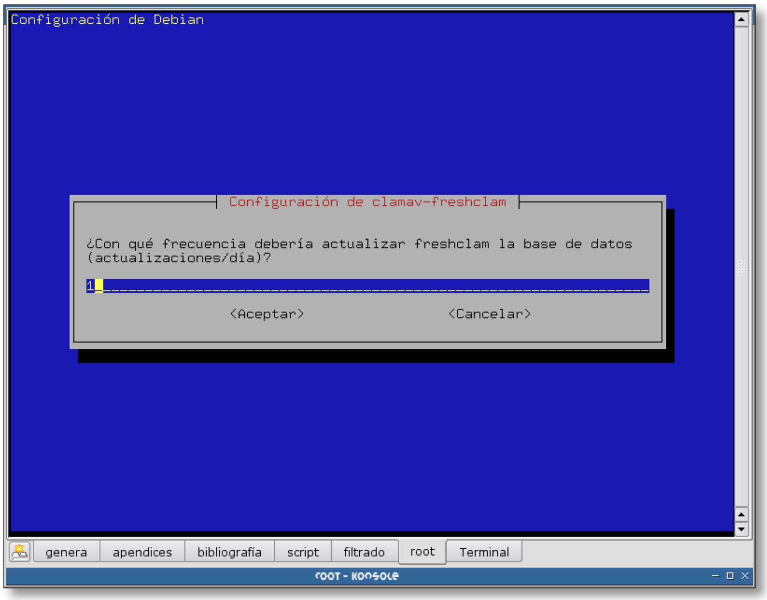
Aquí se indica el servidor desde donde se ha de actualizar la base de datos. En este caso se deja la opción por defecto.

Figura 6-3. Información sobre el proxy



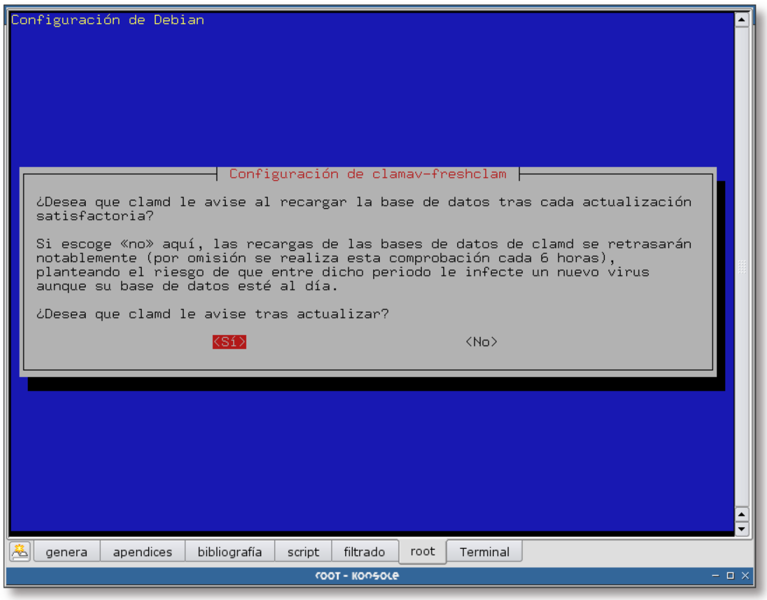
Si dispone de un proxy para el acceso a Internet, aquí debería completar la información sobre el mismo.

Figura 6-4. Frecuencia de actualización de la base de datos



Seleccione aquí la frecuencia con la que se debería actualizar la base de datos de virus. En este caso se ha decidido actualizarla una vez al día.

Figura 6-5. Aviso de actualización



Respondemos afirmativamente a esta pregunta.

Ejemplo 6-4. Instalación de *Clamav* (segunda parte)

```
--------------------- Sourcerer Apt Watcher ---------------------
Configure: libclamav1
-----------------------------------------------------------------
Seleccionando el paquete libclamav1 previamente no seleccionado.
(Leyendo la base de datos ...
274441 ficheros y directorios instalados actualmente.)
Desempaquetando libclamav1 (de .../libclamav1_0.71-3_i386.deb) ...
Seleccionando el paquete clamav-base previamente no seleccionado.
Desempaquetando clamav-base (de .../clamav-base_0.71-3_all.deb) ...
Seleccionando el paquete clamav-freshclam previamente no seleccionado.
Desempaquetando clamav-freshclam (de .../clamav-freshclam_0.71-3_i386.deb) ...
Seleccionando el paquete clamav previamente no seleccionado.
Desempaquetando clamav (de .../clamav_0.71-3_i386.deb) ...
Configurando libclamav1 (0.71-3) ...

Configurando clamav-base (0.71-3) ...
Añadiendo usuario del sistema clamav...
Añadiendo nuevo grupo clamav (137).
Añadiendo nuevo usuario clamav (137) con grupo clamav.
No se crea el directorio home.

Configurando clamav-freshclam (0.71-3) ...
Starting clamav virus database updater: freshclam.
```

```
Configurando clamav (0.71-3) ...
```

> **Importante:** Si no posee conexión a Internet desde su equipo, sería buena idea instalar el paquete *clamav-data*, paquete que provee la base de datos de virus. La instalación de este paquete no es recomendable, ya que normalmente se encontrará muy desactualizado.

Ejemplo 6-5. Instalación de *Clamav-daemon*

```
# /usr/bin/apt-get install clamav-daemon
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  clamav-daemon
0 actualizados, 1 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/111kB de archivos.
Se utilizarán 315kB de espacio de disco adicional después de desempaquetar.
Preconfiguring packages ...
--------------------- Sourcerer Apt Watcher ---------------------
Configure: clamav-daemon
-----------------------------------------------------------------
Seleccionando el paquete clamav-daemon previamente no seleccionado.
(Leyendo la base de datos ...
274608 ficheros y directorios instalados actualmente.)
Desempaquetando clamav-daemon (de .../clamav-daemon_0.71-3_i386.deb) ...
Configurando clamav-daemon (0.71-3) ...
Starting clamav daemon: clamd.
```

Instalación de paquetes sugeridos y recomendados

Para finalizar con la instalación, se recomienda revisar la lista de paquetes recomendados y sugeridos en la instalación de los paquetes anteriores y seleccionar aquellos que considere importantes. En este caso se han instalado los paquetes: *zoo* y *lha*.

Capítulo 7. Configuración

Introducción

Este capítulo tratará la configuración de *amavis-new*, *clamav* y *spamassassin* junto con Postfix. De forma que, cada correo que pase a través de Postfix sea analizado en busca de virus y puntuado de acuerdo al nivel de SPAM detectado.

> **Nota:** Este capítulo se ha basado en la entrada bibliográfica Pereda01.

Configuración de *amavis-new*

La configuración del *amavis-new* se realiza a partir del archivo `/etc/amavis/amavisd.conf`. Edítelo y modifique las siguientes variables, de acuerdo a la configuración de su sistema.

> **Nota:** En el Apéndice I se encuentra un archivo de configuración completo.

```
$mydomain = 'gsr.pt';
$forward_method = 'smtp:127.0.0.1:10025'; ❶
$notify_method = $forward_method;
$final_spam_destiny       = D_PASS; ❷
$sa_tag_level_deflt  = 4.0;
$sa_tag2_level_deflt = 6.3; ❸
$sa_kill_level_deflt = $sa_tag2_level_deflt; ❹
```

❶ Esta opción indica la vía que *amavisd-new* utilizará para reinyectar el mensaje de correo en Postfix. En este caso se ha configurado de forma que haga uso del servicio SMTP que esté escuchando en la interfaz *localhost* por el puerto 10025.

❷ Esta opción indica qué se hace con los correos calificados como SPAM. Por defecto los rechaza (D_REJECT), pero se ha cambiado la opción por el valor "D_PASS", de esta forma no será rechazados, pudiendo analizarlos para detectar falsos positivos (correos marcados como SPAM, pero que no lo son).

❸❹ Estas dos opciones indican el nivel en el cual un correo es considerado como SPAM.

> **Aviso**
>
> Para que *amavisd-new* haga uso de *Spamassassin*, en el archivo de configuración de *amavisd-new* se ha de comentar la línea:
>
> ```
> @bypass_spam_checks_acl  = qw( . );
> ```

Una vez realizadas estas modificaciones, *amavisd-new* ya se encontraría listo. La siguiente sección mostrará la forma de configurar Postfix para que haga uso de *amavisd-new*.

Configuración de *Postfix*

A continuación se verá la forma de configurar *Postfix*. La idea es hacer que en los puertos por defecto (25 y 465 - en caso de tener configurado Postfix en modo SSL), *Postfix* pase todos los correos electrónicos por *amavisd-new*. Luego se creará un proceso SMTP que únicamente se ejecute en la interfaz *loopback* (127.0.0.1) en el puerto 10025; dicho proceso pasará el correo a los usuarios sin hacer uso de *amavisd-new*. Esto es necesario para evitar que los mensajes entren en un bucle sin fin.

Para conseguir esto, se ha de añadir la siguiente línea al archivo `/etc/postfix/main.cf`:

```
content_filter=smtp-amavis:[localhost]:10024
```

Y en `/etc/postfix/master.cf`:

```
smtp-amavis unix - - y - 2 smtp ❶
 -o smtp_data_done_timeout=1200
 -o disable_dns_lookups=yes
127.0.0.1:10025 inet n - y - - smtpd ❷
 -o content_filter=
 -o local_recipient_maps=
 -o relay_recipient_maps=
 -o smtpd_restriction_classes=
 -o smtpd_client_restrictions=
 -o smtpd_helo_restrictions=
 -o smtpd_sender_restrictions=
 -o smtpd_recipient_restrictions=permit_mynetworks,reject
 -o mynetworks=127.0.0.0/8
 -o strict_rfc821_envelopes=yes
```

❶ Línea que indica el filtro para *AMaVis*

❷ Línea que crea el servidor SMTP local, por el pasarán los correos sin ser filtrados

> **Importante:** Cuando añada las líneas al archivo `/etc/postfix/master.cf`, asegúrese de que al final de las líneas no existan espacios en blanco.

Ahora sólo queda reiniciar los demonios postfix, amavisd-new, clamd, clamav-freshclan y spamassassin y comprobar que todo funciona. Las pruebas de funcionamiento se realizarán en el siguiente capítulo (Capítulo 8).

Capítulo 8. Pruebas de funcionamiento

Introducción

Ahora que ya están todos los servicios correctamente configurados, ha de reiniciarlos para que relean su configuración. Una vez se han reiniciado los servicios, se van a enviar un par de mensajes para comprobar el comportamiento del filtrado.

El primero de los mensajes va a ser un texto simple, sin ninguna complicación, para comprobar el análisis antivirus. El segundo correo llevará el contenido del archivo `/usr/share/doc/spamc/sample-spam.txt` para comprobar el funcionamiento de *Spamassassin*.

Comprobando el antivirus

A continuación se va a enviar un correo y se van a analizar las cabeceras del correo resultante en el buzón del usuario a quien ha sido enviado, para ver si ha sido analizado por el antivirus:

Ejemplo 8-1. Envío de un correo

```
$ /usr/bin/mail severa@gsr.pt
Subject: Prueba para el antivirus

   Este correo no es más que una prueba ;-)
.
Cc: [enter]
```

Ahora se muestra el correo recibido por el usuario *severa*:

```
Return-Path: <sergio@todoscsi.gsr.pt>
X-Original-To: severa@gsr.pt
Delivered-To: severa@gsr.pt
Received: from localhost (localhost [127.0.0.1])
        by todoscsi.gsr.pt (Postfix) with ESMTP id 634A748 ❶
        for <severa@gsr.pt>; Sun,  6 Jun 2004 15:50:19 +0100 (WEST)
Received: from todoscsi.gsr.pt ([127.0.0.1])
        by localhost (todoscsi [127.0.0.1]) (amavisd-new, port 10024) ❷
        with ESMTP id 05067-03 for <severa@gsr.pt>;
        Sun, 6 Jun 2004 15:50:15 +0100 (WEST)
Received: by todoscsi.gsr.pt (Postfix, from userid 1000) ❸
        id 3FB5F4B; Sun,  6 Jun 2004 15:50:15 +0100 (WEST)
To: severa@gsr.pt
Subject: Prueba para el antivirus
Message-Id: <20040606145015.3FB5F4B@todoscsi.gsr.pt>
Date: Sun,  6 Jun 2004 15:50:15 +0100 (WEST)
From: sergio@todoscsi.gsr.pt (Sergio González González)
X-Virus-Scanned: by amavisd-new-20030616-p7 (Debian) at gsr.pt ❹
X-Amavis-Alert: BAD HEADER Non-encoded 8-bit data (char E1 hex) in message header 'From'
        From: sergio@todoscsi.gsr.pt (Sergio Gonz\341lez Gonz\341lez)\n ^


   Este correo no es más que una prueba ;-)
```

❶ Esta línea indica que el correo ha sido recogido por el servidor Postfix.

❷ El servidor Postfix le ha pasado el correo al servidor *amavis-new* por el puerto 10024.

❸ Finalmente, *amavis-new* ha entregado el correo ya analizado a Postfix, esta vez por el puerto 10025.

❹ Esta cabecera indica que el presente correo ha sido analizado por el software *amavisd-new-20030616-p7*

Comprobando el control de SPAM

En esta sección se va a enviar un correo con el contenido del archivo `/usr/share/doc/spamc/sample-spam.txt` para comprobar que *Spamassassin* está funcionando y lo hace de la forma correcta:

Ejemplo 8-2. Envío de un correo

```
$ /usr/bin/mail severa@gsr.pt
Subject: Prueba para el control antispam
This is the GTUBE, the
        Generic
        Test for
        Unsolicited
        Bulk
        Email

If your spam filter supports it, the GTUBE provides a test by which you
can verify that the filter is installed correctly and is detecting incoming
spam. You can send yourself a test mail containing the following string of
characters (in upper case and with no white spaces and line breaks):

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

You should send this test mail from an account outside of your network.
.
Cc: [enter]
```

Ahora se muestra el correo recibido por el usuario *severa*:

```
Return-Path: <sergio@todoscsi.gsr.pt>
X-Original-To: severa@gsr.pt
Delivered-To: severa@gsr.pt
Received: from localhost (localhost [127.0.0.1])
        by todoscsi.gsr.pt (Postfix) with ESMTP id 82F0548
        for <severa@gsr.pt>; Sun,  6 Jun 2004 16:01:41 +0100 (WEST)
Received: from todoscsi.gsr.pt ([127.0.0.1])
        by localhost (todoscsi [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id 05068-03 for <severa@gsr.pt>;
        Sun, 6 Jun 2004 16:01:37 +0100 (WEST)
Received: by todoscsi.gsr.pt (Postfix, from userid 1000)
        id 4B5D04B; Sun,  6 Jun 2004 16:01:37 +0100 (WEST)
To: severa@gsr.pt
Subject: ***SPAM*** Prueba para el control antispam ❶
Message-Id: <20040606150137.4B5D04B@todoscsi.gsr.pt>
Date: Sun,  6 Jun 2004 16:01:37 +0100 (WEST)
From: sergio@todoscsi.gsr.pt (Sergio González González)
X-Virus-Scanned: by amavisd-new-20030616-p7 (Debian) at gsr.pt
```

```
X-Amavis-Alert: BAD HEADER Non-encoded 8-bit data (char E1 hex) in message header 'From'
        From: sergio@todoscsi.gsr.pt (Sergio Gonz\341lez Gonz\341lez)\n ^
X-Spam-Status: Yes, hits=1000.0 tagged_above=4.0 required=6.3 tests=GTUBE  ❷
X-Spam-Level: ****************************************************************  ❸
X-Spam-Flag: YES  ❹

This is the GTUBE, the
        Generic
        Test for
        Unsolicited
        Bulk
        Email

If your spam filter supports it, the GTUBE provides a test by which you
can verify that the filter is installed correctly and is detecting incoming
spam. You can send yourself a test mail containing the following string of
characters (in upper case and with no white spaces and line breaks):

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

You should send this test mail from an account outside of your network.
```

❶ Se puede comprobar que el asunto del correo ha sido modificado por *Spamassassin*; este ha considerado que el correo es SPAM y así lo marca en el asunto del correo.

❷ El análisis del correo ha dado un valor de 1000.0, y como se puede comprobar, sólo hace falta un valor de 6.3 para considerar un correo como SPAM.

❸ Dependiendo del nivel de SPAM, esta línea será más larga o más corta.

❹ Esta cabecera indica que el correo es SPAM, por lo que puede ser utilizada para clasificar los correos desde su aplicación favorita.

VI. Habilitando la encriptación en los distintos servicios

Capítulo 9. Postfix

Configuración

> **Nota:** Esta sección se ha basado en la entrada bibliográfica Pereda01.

Postfix permite hacer uso de de encriptación SSL, para ello hay que instalar el paquete *postfix-tls*. Este paquete se instaló en el Capítulo 9, por lo tanto ahora sólo queda habilitar el soporte SSL.

Edite el archivo `/etc/postfix/main.cf` y añada al final del mismo las siguientes líneas:

```
## TLS/SSL
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls = yes
smtpd_tls_note_starttls = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd-key.pem
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.pem
smtpd_tls_loglevel = 1
```

El siguiente paso es la generación del certificado y la clave. Vea la forma de hacerlo en el siguiente ejemplo:

> **Importante:** Ha de crear el directorio `/etc/postfix/ssl/` antes de proceder con la generación del certificado y la clave.

Ejemplo 9-1. Generación de un certificado y una clave para el servidor Postfix

```
# /usr/bin/openssl req -config /etc/ssl/openssl.cnf -new -x509 -nodes -out \
/etc/postfix/ssl/smtpd.pem -keyout /etc/postfix/ssl/smtpd-key.pem -days 999999
```

> **Nota:** Tras la ejecución del comando del Ejemplo 9-1, se le harán una serie de preguntas, contéstelas adecuando las respuestas a su sistema.

El último paso es descomentar tres líneas del archivo `/etc/postfix/master.cf`:

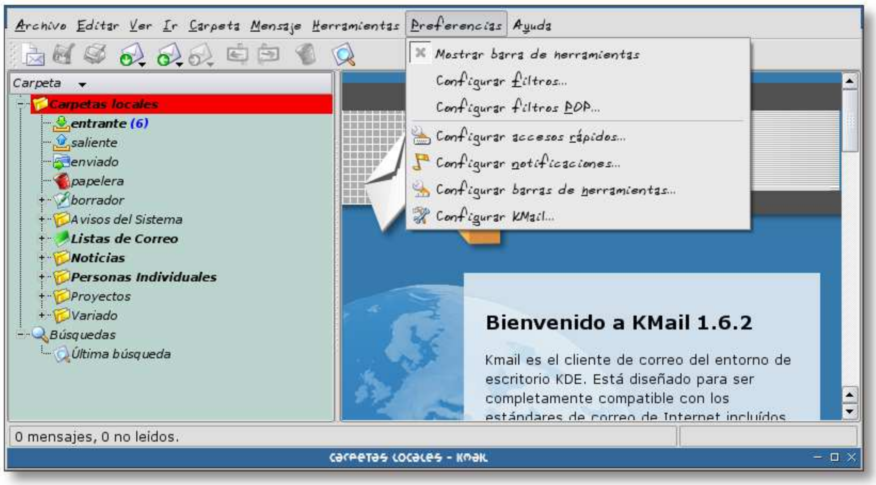
```
# only used by postfix-tls
tlsmgr fifo -   -  n 300 1   tlsmgr
smtps  inet n   -  n -   -   smtpd -o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
587    inet n   -  n -   -   smtpd -o smtpd_enforce_tls=yes -o smtpd_sasl_auth_enable=yes
```

Ahora sólo queda que el servidor de correo relea su configuración. Vea el Ejemplo 2-13 para saber como hacerlo.

Prueba de funcionamiento

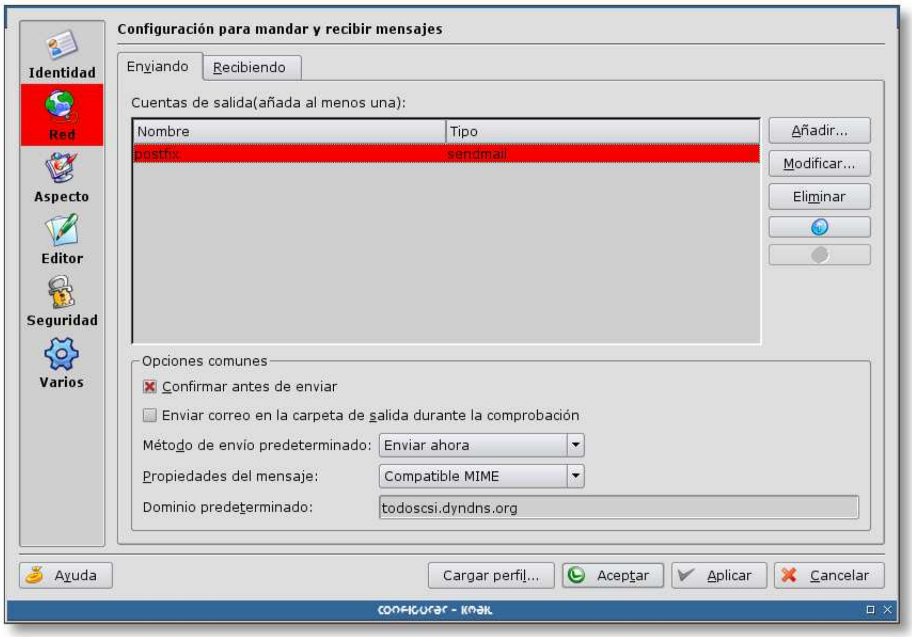
A continuación se probará el funcionamiento de Postfix mediante el protocolo TLS. Se hará uso de Kmail para comprobar su funcionamiento, como se muestra en las siguientes capturas:

Figura 9-1. Configuración de Kmail



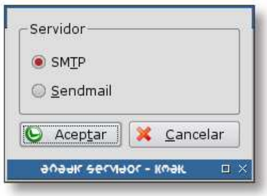
Ejecute Kmail y acceda al menú *Preferencias -> Configurar Kmail...*.

Figura 9-2. Nuevo servidor SMTP I



Acceda a la pestaña *Enviando* de la opción *Red* y pulse sobre el botón "Añadir..."

Figura 9-3. Nuevo servidor SMTP II

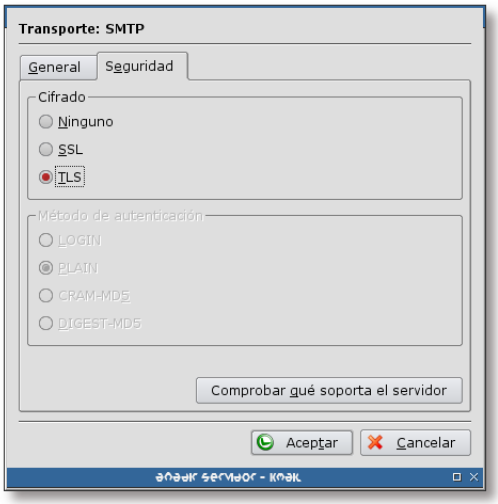


Seleccione la opción SMTP y pulse sobre "Aceptar".

Figura 9-4. Nuevo servidor SMTP III

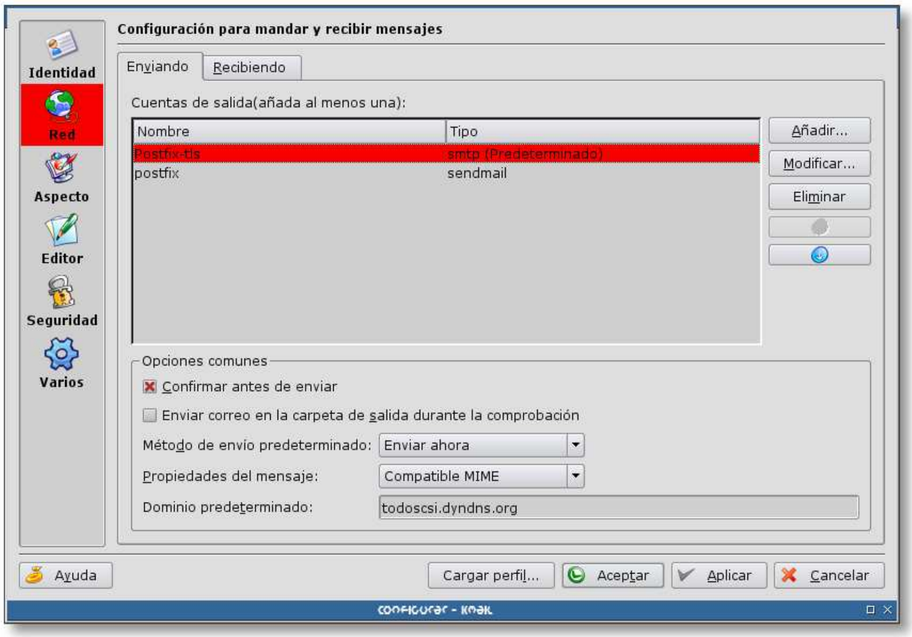
Complete las opciones necesarias con la configuración de su servidor SMTP y pulse sobre la pestaña *Seguridad*.

Figura 9-5. Nuevo servidor SMTP IV



Pulse sobre el botón “Comprobar qué soporta el servidor”. Tras un instante, nos permitirá elegir entre tres opciones de cifrado: Ninguno, SSL y TLS, seleccione este último y pulse sobre “Aceptar”.

Figura 9-6. Nuevo servidor SMTP V



Establezca el nuevo servidor SMTP como el predeterminado y pulse sobre el botón “Aceptar”.

Ahora ya se tiene un nuevo servidor SMTP para el envío de correos. Para el envío de correos a través de este servidor se utilizará el protocolo TLS. Para comprobar que realmente se utiliza, genere un nuevo mensaje y envíelo con el nuevo servidor.

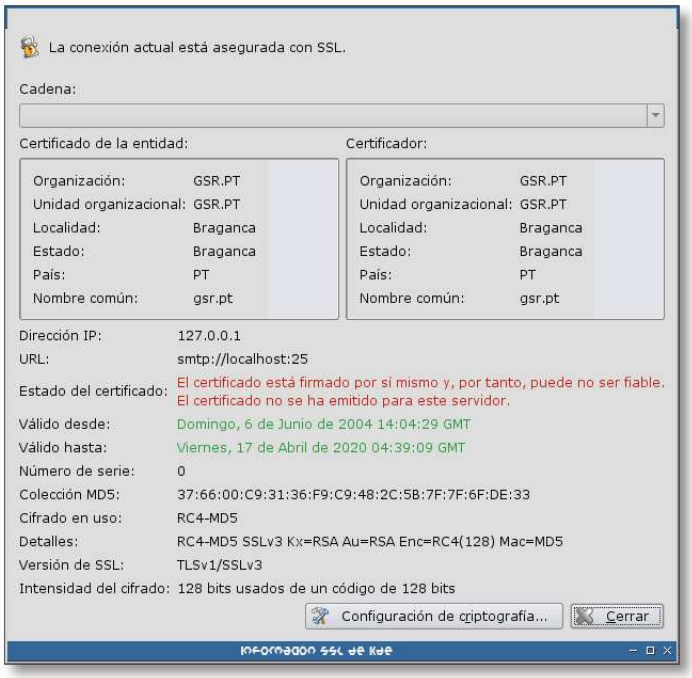
Al pulsar sobre el botón de enviar mensaje, le aparecerá la siguiente pantalla:

Figura 9-7. Certificado no válido

Al conectarse al servidor de correo y tratar de verificar la autenticidad del certificado, Kmail detecta que el certificado está firmado por si mismo y por lo tanto no lo considera válido, nada de qué preocuparse.

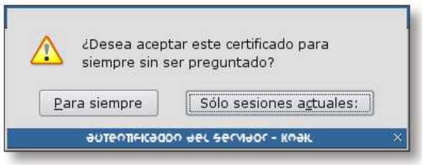
Pulse sobre el botón “Detalles” para ver la información sobre el certificado.

Figura 9-8. Información sobre el certificado



Esta pantalla muestra la información del certificado del servidor de correo. Tras analizarlo, pulse sobre el botón "Cerrar" y a continuación sobre el botón "Continuar".

Figura 9-9. Hasta cuando aceptar el certificado



La última pregunta que nos realizará Kmail antes de enviar el correo, será hasta cuando se acepta el certificado. Elija la opción que más le guste.

Si tras enviar el correo por medio del nuevo servidor SMTP echamos un vistazo a los logs, se verá una entrada similar a la siguiente:

```
Jun  6 16:32:34 todoscsi postfix/smtpd[5690]: connect from localhost[127.0.0.1]
Jun  6 16:32:35 todoscsi postfix/smtpd[5690]: setting up TLS connection from localhost[127.0.0.1]
Jun  6 16:32:35 todoscsi postfix/smtpd[5690]: TLS connection established from \
                                   localhost[127.0.0.1]: TLSv1 with cipher RC4-MD5 (128/128 bits)
```

Si se analizan detenidamente las líneas anteriores, se puede comprobar que se ha establecido una conexión TLS entre el cliente y el servidor, haciendo uso del algoritmo de encriptación *RC4-MD5*.

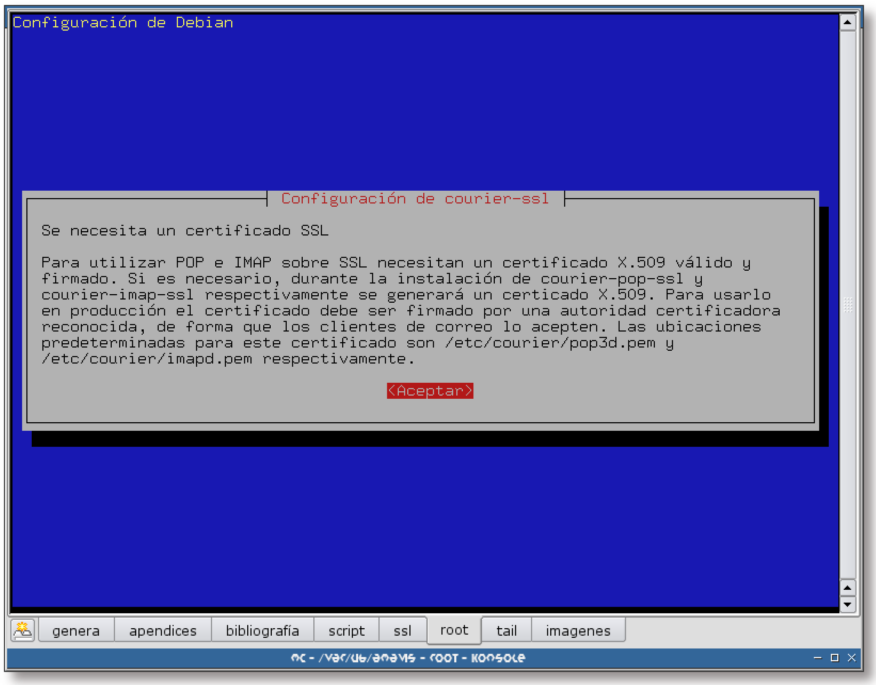
Capítulo 10. Servidor Courier POP3

Para dar soporte SSL al servidor POP3, se ha de instalar el paquete *courier-pop-ssl*. El siguiente ejemplo muestra como hacerlo:

Ejemplo 10-1. Instalación del paquete *courier-pop-ssl* (primera parte)

```
# /usr/bin/apt-get install courier-pop-ssl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  courier-ssl
Se instalarán los siguientes paquetes NUEVOS:
  courier-pop-ssl courier-ssl
0 actualizados, 2 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/207kB de archivos.
Se utilizarán 836kB de espacio de disco adicional después de desempaquetar.
¿Desea continuar? [S/n] [enter]
Preconfiguring packages ...
```

Figura 10-1. Necesidad de un certificado X.509



El proceso de instalación informa que hace falta un certificado X.509 para poder realizar las conexiones por SSL. También informa que durante el proceso de instalación se creará un certificado de ejemplo.

Ejemplo 10-2. Instalación del paquete *courier-pop-ssl* (segunda parte)

```
--------------------- Sourcerer Apt Watcher ---------------------
```

```
Configure: courier-ssl
-----------------------------------------------------------------
(Leyendo la base de datos ...
274623 ficheros y directorios instalados actualmente.)
Desempaquetando courier-ssl (de .../courier-ssl_0.45.4-1_i386.deb) ...
Desempaquetando courier-pop-ssl (de .../courier-pop-ssl_0.45.4-1_i386.deb) ...
Configurando courier-ssl (0.45.4-1) ...

Configurando courier-pop-ssl (0.45.4-1) ...
Generating a 1024 bit RSA private key
...................++++++
.++++++
writing new private key to '/usr/lib/courier/pop3d.pem'
-----
1024 semi-random bytes loaded
Generating DH parameters, 512 bit long safe prime, generator 2
This is going to take a long time
...+.+.......+......................+........+.........++*++*++*++*++*++*
subject= /C=US/ST=NY/L=New York/O=Courier Mail Server/OU=Automatically-generated POP3
SSL key/CN=localhost/emailAddress=postmaster@example.com
notBefore=Jun  6 16:19:45 2004 GMT
notAfter=Jun  6 16:19:45 2005 GMT
MD5 Fingerprint=78:24:5F:04:32:5F:92:37:F0:72:20:89:42:59:DA:53
Starting Courier POP3-SSL server: pop3d-ssl.
```

> **Nota:** El proceso de instalación ha generado un certificado de ejemplo. Se utilizará este certificado para hacer las pruebas.

A continuación se muestra la descripción de los paquetes que se acaban de instalar:

Ejemplo 10-3. Descripción de los paquetes *courier-pop-ssl* y *courier-ssl*

```
# /usr/bin/apt-cache shoe courier-pop-ssl courier-ssl
Package: courier-pop-ssl
Priority: optional
Section: mail
Installed-Size: 124
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
Architecture: i386
Source: courier
Version: 0.45.4-1
Depends: courier-pop, courier-ssl (>= 0.45.4)
Filename: pool/main/c/courier/courier-pop-ssl_0.45.4-1_i386.deb
Size: 18320
MD5sum: f9c9f2b3b90bb13eac17e52a377ccfa7
Description: Courier Mail Server - POP3 over SSL
 POP3 over SSL is handled by the regular POP3 daemon from courier-pop
 in conjunction with the SSL/TLS wrapper supplied by courier-ssl.

Package: courier-ssl
Priority: optional
Section: mail
Installed-Size: 692
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
```

```
Architecture: i386
Source: courier
Version: 0.45.4-1
Depends: libc6 (>= 2.3.2.ds1-4), libssl0.9.7, courier-base (>= 0.45.4), openssl
Filename: pool/main/c/courier/courier-ssl_0.45.4-1_i386.deb
Size: 188422
MD5sum: 4ff16dc86d7a02eb494a69706b50f331
Description: Courier Mail Server - SSL/TLS Support
 The Courier Mail Server employs the SSL/TLS wrapper application
 couriertls instead of equipping the different applications with
 SSL/TLS support. Additionally, this package contains a default set
 of trusted X.509 root CA certs.
```

Tras la instalación, el sistema dispone de un nuevo demonio que escucha en el puerto 995 (pop3s); si ahora su gestor de correo se conecta a este puerto para bajarse los correos por el protocolo POP3, lo hará utilizando encriptación en la transferencia.

> **Sugerencia:** Sería interesante forzar el uso de TLS, para ello asigne el valor “1” a la variable *POP3_TLS_REQUIRED* del archivo de configuración del demonio *courier-pop-ssl*: `/etc/courier/pop3d-ssl`.

Capítulo 11. Servidor Courier IMAP

Para dar soporte SSL al servidor IMAP, se ha de instalar el paquete *courier-imap-ssl*. El siguiente ejemplo muestra como hacerlo:

Ejemplo 11-1. Instalación del paquete *courier-imap-ssl*

```
# /usr/bin/apt-get install courier-imap-ssl
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  courier-imap-ssl
0 actualizados, 1 se instalarán, 0 para eliminar y 9 no actualizados.
Se necesita descargar 0B/18,5kB de archivos.
Se utilizarán 127kB de espacio de disco adicional después de desempaquetar.
--------------------- Sourcerer Apt Watcher ---------------------
Configure: courier-imap-ssl
-----------------------------------------------------------------
(Leyendo la base de datos ...
274822 ficheros y directorios instalados actualmente.)
Desempaquetando courier-imap-ssl (de .../courier-imap-ssl_3.0.3-1_i386.deb) ...
Configurando courier-imap-ssl (3.0.3-1) ...
Generating a 1024 bit RSA private key
..........++++++
.................................................++++++
writing new private key to '/usr/lib/courier/imapd.pem'
-----
1024 semi-random bytes loaded
Generating DH parameters, 512 bit long safe prime, generator 2
This is going to take a long time
..........................................++*++*++*++*++*++*
subject= /C=US/ST=NY/L=New York/O=Courier Mail Server/OU=Automatically-generated IMAP
SSL key/CN=localhost/emailAddress=postmaster@example.com
notBefore=Jun  6 16:35:58 2004 GMT
notAfter=Jun  6 16:35:58 2005 GMT
MD5 Fingerprint=59:94:B8:E5:54:6B:DE:4D:33:08:F9:90:74:81:1F:0B
Starting Courier IMAP-SSL server: imapd-ssl.
```

> **Nota:** El proceso de instalación ha generado un certificado de ejemplo. Se utilizará este certificado para hacer las pruebas.

A continuación se muestra la descripción de los paquetes que se acaban de instalar:

Ejemplo 11-2. Descripción del paquete *courier-imap-ssl*

```
# /usr/bin/apt-cache shoe courier-imap-ssl
Package: courier-imap-ssl
Priority: extra
Section: mail
Installed-Size: 124
Maintainer: Stefan Hornburg (Racke) <racke@linuxia.de>
Architecture: i386
```

```
Source: courier (0.45.4-1)
Version: 3.0.3-1
Depends: courier-imap (>= 1.3.7-3), courier-ssl (>= 0.45.4), openssl
Suggests: imap-client
Filename: pool/main/c/courier/courier-imap-ssl_3.0.3-1_i386.deb
Size: 18514
MD5sum: 4af6baf8397602608b4a19035db6b7c3
Description: Courier Mail Server - IMAP over SSL
 IMAP over SSL is handled by the regular IMAP daemon from courier-imap
 in conjunction with the SSL/TLS wrapper supplied by courier-ssl.
```

Tras la instalación, el sistema dispone de un nuevo demonio que escucha en el puerto 993 (imaps); si ahora su gestor de correo se conecta a este puerto para bajarse los correos por el protocolo IMAP, lo hará utilizando encriptación en la transferencia.

> **Sugerencia:** Sería interesante forzar el uso de TLS, para ello asigne el valor "1" a la variable *IMAP_TLS_REQUIRED* del archivo de configuración del demonio *courier-imap-ssl*: `/etc/courier/imap-ssl`.

VII. Archivos de configuración

Apéndice A. Archivo de configuración `/etc/postfix/main.cf`

```
# see /usr/share/postfix/main.cf.dist for a commented, fuller
# version of this file.

# NOMBRE, DOMINIO(S) y RED(ES)
myhostname = todoscsi
mydomain   = gsr.pt
myorigin   = /etc/mailname
#relay     =


# DIRECCION QUE APARECE EN EL FROM
#myorigin = $myhostname
#myorigin = $mydomain


# CONFIGURACION TLS
smtp_use_tls            = yes
smtpd_use_tls           = yes
smtp_tls_note_starttls  = yes
smtpd_tls_note_starttls = yes
smtpd_tls_key_file      = /etc/postfix/ssl/smtpd-key.pem
smtpd_tls_cert_file     = /etc/postfix/ssl/smtpd.pem
smtpd_tls_loglevel      = 1


## CONFIGURACION SASL
#broken_sasl_auth_clients  = yes
#smtpd_sasl_local_domain   = $myhostname
#smtpd_sasl_auth_enable    = yes
#smtpd_sasl_security_options = noanonymous


# UBICACION DE DIRECTORIOS
#
# Do not change these directory settings - they are critical to Postfix
# operation.
command_directory = /usr/sbin
daemon_directory  = /usr/lib/postfix
program_directory = /usr/lib/postfix


# PROPIETARIO DE COLAS Y PROCESOS
mail_owner   = postfix
setgid_group = postdrop


# TRATAMIENTO DE ALIAS
alias_maps     = hash:/etc/aliases
alias_database = hash:/etc/aliases

# Alias virtuales
virtual_maps          = ldap:valiases
```

```
valiases_server_host  = gsr.pt
valiases_search_base  = ou=alias,ou=postfix,dc=gsr,dc=pt
valiases_query_filter = (&(mail=%s)(objectClass=CourierMailAlias))
valiases_result_attribute = maildrop
valiases_bind         = no


# IDENTIFICACION DE USUARIOS LOCALES
local_recipient_maps = unix:passwd.byname $alias_maps


# ENVIO EN PARALELO A UN MISMO DESTINO
local_destination_concurrency_limit   = 2
default_destination_concurrency_limit = 10


# OTROS PARAMETROS DE CONFIGURACION
notify_classes       = resource, software, policy
disable_vrfy_command = yes
disable_dns_lookups  = no
#relayhost           = [$relay]
message_size_limit   = 10485760
mailbox_size_limit   = 0
maximal_queue_lifetime = 5d
recipient_delimiter  = +
append_dot_mydomain  = no
biff                 = no

# CONTROL DE CORREO ENTRANTE / SALIENTE
mynetworks    = 127.0.0.0/8 192.168.2.0/24
mydestination = todoscsi.gsr.pt localhost.gsr.pt gsr.pt todoscsi.chets.lan, \
                localhost.chets.lan, localhost, todoscsi
#relay_domains       =
#smtpd_client_restrictions = reject_rbl_client relays.ordb.org \
#                    reject_rhsbl_client relays.ordb.org reject_unknown_client
#smtpd_helo_required       = yes
#smtpd_helo_restrictions   = reject_invalid_hostname reject_unknown_hostname \
#                            reject_non_fqdn_hostname
##smtpd_recipient_restrictions = permit_sasl_authenticated permit_mynetworks \
#                                reject_unauth_destination
##smtpd_data_restrictions    = reject_unauth_pipelining
##header_checks              = regexp:/etc/postfix/header_checks
##body_checks                = regexp:/etc/postfix/body_checks
local_transport = local
mailbox_command = procmail -a "$EXTENSION"
content_filter  = smtp-amavis:[localhost]:10024

# VERSION
mail_name = Postfix
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
```

Apéndice B. Archivo de configuración `/etc/postfix/master.cf`

```
#
# Postfix master process configuration file.  Each logical line
# describes how a Postfix daemon program should be run.
#
# A logical line starts with non-whitespace, non-comment text.
# Empty lines and whitespace-only lines are ignored, as are comment
# lines whose first non-whitespace character is a `#'.
# A line that starts with whitespace continues a logical line.
#
# The fields that make up each line are described below. A "-" field
# value requests that a default value be used for that field.
#
# Service: any name that is valid for the specified transport type
# (the next field).  With INET transports, a service is specified as
# host:port.  The host part (and colon) may be omitted. Either host
# or port may be given in symbolic form or in numeric form. Examples
# for the SMTP server:  localhost:smtp receives mail via the loopback
# interface only; 10025 receives mail on port 10025.
#
# Transport type: "inet" for Internet sockets, "unix" for UNIX-domain
# sockets, "fifo" for named pipes.
#
# Private: whether or not access is restricted to the mail system.
# Default is private service.  Internet (inet) sockets can't be private.
#
# Unprivileged: whether the service runs with root privileges or as
# the owner of the Postfix system (the owner name is controlled by the
# mail_owner configuration variable in the main.cf file). Only the
# pipe, virtual and local delivery daemons require privileges.
#
# Chroot: whether or not the service runs chrooted to the mail queue
# directory (pathname is controlled by the queue_directory configuration
# variable in the main.cf file). Presently, all Postfix daemons can run
# chrooted, except for the pipe, virtual and local delivery daemons.
# The proxymap server can run chrooted, but doing so defeats most of
# the purpose of having that service in the first place.
# The files in the examples/chroot-setup subdirectory describe how
# to set up a Postfix chroot environment for your type of machine.
#
# Wakeup time: automatically wake up the named service after the
# specified number of seconds. A ? at the end of the wakeup time
# field requests that wake up events be sent only to services that
# are actually being used.  Specify 0 for no wakeup. Presently, only
# the pickup, queue manager and flush daemons need a wakeup timer.
#
# Max procs: the maximum number of processes that may execute this
# service simultaneously. Default is to use a globally configurable
# limit (the default_process_limit configuration parameter in main.cf).
# Specify 0 for no process count limit.
#
# Command + args: the command to be executed. The command name is
# relative to the Postfix program directory (pathname is controlled by
```

```
# the daemon_directory configuration variable). Adding one or more
# -v options turns on verbose logging for that service; adding a -D
# option enables symbolic debugging (see the debugger_command variable
# in the main.cf configuration file). See individual command man pages
# for specific command-line options, if any.
#
# General main.cf options can be overridden for specific services.
# To override one or more main.cf options, specify them as arguments
# below, preceding each option by "-o".  There must be no whitespace
# in the option itself (separate multiple values for an option by
# commas).
#
# In order to use the "uucp" message tranport below, set up entries
# in the transport table.
#
# In order to use the "cyrus" message transport below, configure it
# in main.cf as the mailbox_transport.
#
# SPECIFY ONLY PROGRAMS THAT ARE WRITTEN TO RUN AS POSTFIX DAEMONS.
# ALL DAEMONS SPECIFIED HERE MUST SPEAK A POSTFIX-INTERNAL PROTOCOL.
#
# DO NOT SHARE THE POSTFIX QUEUE BETWEEN MULTIPLE POSTFIX INSTANCES.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       -       -       -       smtpd
#submission inet n      -       -       -       -       smtpd
# -o smtpd_etrn_restrictions=reject
#628      inet  n       -       -       -       -       qmqpd
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       -       300     1       qmgr
#qmgr     fifo  n       -       -       300     1       oqmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
smtp      unix  -       -       -       -       -       smtp
relay     unix  -       -       -       -       -       smtp
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       -       -       -       showq
error     unix  -       -       -       -       -       error
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       n       -       1       anvil
#
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
#
# maildrop. See the Postfix MAILDROP_README file for details.
#
```

```
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${recipient}
#
# The Cyrus deliver program has changed incompatibly, multiple times.
cyrus     unix  -   n   n   -   -   pipe
  flags=R user=cyrus argv=/usr/sbin/cyrdeliver -e -m "${extension}" ${user}
#CYRUS## Cyrus 2.1.5 (Amos Gouaux)
#CYRUS## Also specify in main.cf: cyrus_destination_recipient_limit=1
#CYRUS#cyrus     unix  -       n       n       -       -       pipe
#CYRUS#  user=cyrus argv=/usr/sbin/deliver -e -r ${sender} -m ${extension} \
#                                                                      ${user}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail \
                                                               ($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -d -t$nexthop -f$sender \
                                                                   $recipient
scalemail-backend unix  -   n   n   -   2   pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store \
                                               ${nexthop} ${user} ${extension}
# only used by postfix-tls
tlsmgr    fifo  -   -   n   300 1   tlsmgr
smtps     inet  n   -   n   -   -   smtpd -o smtpd_tls_wrappermode=yes \
                                               -o smtpd_sasl_auth_enable=yes
587   inet  n   -   n   -   -   smtpd -o smtpd_enforce_tls=yes \
                                               -o smtpd_sasl_auth_enable=yes

smtp-amavis unix    -   -   y   -   2   smtp
    -o smtp_data_done_timeout=1200
    -o disable_dns_lookups=yes
127.0.0.1:10025 inet    n   -   y   -   -   smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_client_restrictions=
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o mynetworks=127.0.0.0/8
    -o strict_rfc821_envelopes=yes
```

Apéndice C. Archivo de configuración /etc/courier/authdaemonrc

```
#
#VERSION: $Id: courier-authdaemonrc.xml,v 1.1 2004/06/29 20:33:32 sergio Exp $
#
# Copyright 2000-2001 Double Precision, Inc.  See COPYING for
# distribution information.
#
# authdaemonrc created from authdaemonrc.dist by sysconftool
#
# Do not alter lines that begin with ##, they are used when upgrading
# this configuration.
#
# This file configures authdaemond, the resident authentication daemon.
#
# Comments in this file are ignored.  Although this file is intended to
# be sourced as a shell script, authdaemond parses it manually, so
# the acceptable syntax is a bit limited.  Multiline variable contents,
# with the \ continuation character, are not allowed.  Everything must
# fit on one line.  Do not use any additional whitespace for indentation,
# or anything else.

##NAME: authmodulelist:0
#
# The authentication modules that are linked into authdaemond.  The
# default list is installed.  You may selectively disable modules simply
# by removing them from the following list.  The available modules you
# can use are: authcustom authcram authuserdb authldap authpgsql authmysql
# authpam

authmodulelist="authpam authldap"

##NAME: authmodulelistorig:1
#
# This setting is used by Courier's webadmin module, and should be left
# alone

authmodulelistorig="authcustom authcram authuserdb authldap authpgsql \
                    authmysql authpam"

##NAME: daemons:0
#
# The number of daemon processes that are started.  authdaemon is typically
# installed where authentication modules are relatively expensive: such
# as authldap, or authmysql, so it's better to have a number of them running.
# PLEASE NOTE:  Some platforms may experience a problem if there's more than
# one daemon.  Specifically, SystemV derived platforms that use TLI with
# socket emulation.  I'm suspicious of TLI's ability to handle multiple
# processes accepting connections on the same filesystem domain socket.
#
# You may need to increase daemons if as your system load increases.  Symptoms
# include sporadic authentication failures.  If you start getting
# authentication failures, increase daemons.  However, the default of 5
# SHOULD be sufficient.  Bumping up daemon count is only a short-term
```

```
# solution.  The permanent solution is to add more resources: RAM, faster
# disks, faster CPUs...

daemons=5

##NAME: version:0
#
# When you have multiple versions of authdaemond.* installed, authdaemond
# just picks the first one it finds.  Set "version" to override that.
# For example:  version=authdaemond.plain

version=""

##NAME: authdaemonvar:0
#
# authdaemonvar is here, but is not used directly by authdaemond.  It’s
# used by various configuration and build scripts, so don’t touch it!

authdaemonvar=/var/run/courier/authdaemon
```

Apéndice D. Archivo de configuración /etc/courier/authldaprc

```
#
#VERSION: $Id: courier-authldaprc.xml,v 1.1 2004/06/29 20:33:32 sergio Exp $
#
# Copyright 2000-2004 Double Precision, Inc.  See COPYING for
# distribution information.
#
# Do not alter lines that begin with ##, they are used when upgrading
# this configuration.
#
# authldaprc created from authldaprc.dist by sysconftool
#
# DO NOT INSTALL THIS FILE with world read permissions.  This file
# might contain the LDAP admin password!
#
# This configuration file specifies LDAP authentication parameters
#
# The format of this file must be as follows:
#
# field[spaces|tabs]value
#
# That is, the name of the field, followed by spaces or tabs, followed by
# field value.  No trailing spaces.
#
# Here are the fields:

##NAME: LOCATION:0
#
# Location of your LDAP server:

LDAP_SERVER gsr.pt
LDAP_PORT 389

##NAME: LDAP_BASEDN:0
#
# Look for authentication here:

LDAP_BASEDN ou=people,dc=gsr,dc=pt

##NAME: LDAP_BINDDN:0
#
# You may or may not need to specify the following.  Because you've got
# a password here, authldaprc should not be world-readable!!!

LDAP_BINDDN cn=postfix,dc=gsr,dc=pt
LDAP_BINDPW ********

##NAME: LDAP_TIMEOUT:0
#
# Timeout for LDAP search

LDAP_TIMEOUT 15
```

```
##NAME: LDAP_AUTHBIND:0
#
# Define this to have the ldap server authenticate passwords.  If LDAP_AUTHBIND
# the password is validated by rebinding with the supplied userid and password.
# If rebind succeeds, this is considered to be an authenticated request.  This
# does not support CRAM-MD5 authentication, which requires userPassword.

LDAP_AUTHBIND 1

##NAME: LDAP_MAIL:0
#
# Here's the field on which we query

LDAP_MAIL mail

##NAME: LDAP_FILTER:0
#
# This LDAP filter will be ANDed with the query for the field defined above
# in LDAP_MAIL.  So if you are querying for mail, and you have LDAP_FILTER
# defined to be "(objectClass=CourierMailAccount)" the query that is performed
# will be "(&(objectClass=CourierMailAccount)(mail=<someAccount>))"

LDAP_FILTER (!(quota=-1))


##NAME: LDAP_DOMAIN:0
#
# The following default domain will be appended, if not explicitly specified.

LDAP_DOMAIN gsr.pt

##NAME: LDAP_GLOB_IDS:0
#
# The following two variables can be used to set everybody's uid and gid.
# This is convenient if your LDAP specifies a bunch of virtual mail accounts
# The values can be usernames or userids:



##NAME: LDAP_HOMEDIR:0
#
# We will retrieve the following attributes
#
# The HOMEDIR attribute MUST exist, and we MUST be able to chdir to it

LDAP_HOMEDIR homeDirectory

##NAME: LDAP_MAILROOT:0
#
# If homeDirectory is not an absolute path, define the root of the
# relative paths in LDAP_MAILROOT



##NAME: LDAP_MAILDIR:0
#
# The MAILDIR attribute is OPTIONAL, and specifies the location of the
```

```
# mail directory.  If not specified, ./Maildir will be used

LDAP_MAILDIR mailbox

##NAME: LDAP_DEFAULTDELIVERY:0
#
# Courier mail server only: optional attribute specifies custom mail delivery
# instructions for this account (if defined) -- essentially overrides
# DEFAULTDELIVERY from ${sysconfdir}/courierd

LDAP_DEFAULTDELIVERY defaultDelivery

##NAME: LDAP_MAILDIRQUOTA:0
#
# The following variable, if defined, specifies the field containing the
# maildir quota, see README.maildirquota for more information
#
# LDAP_MAILDIRQUOTA quota



##NAME: LDAP_FULLNAME:0
#
# FULLNAME is optional, specifies the user's full name

LDAP_FULLNAME cn

##NAME: LDAP_PW:0
#
# CLEARPW is the clear text password.  CRYPT is the crypted password.
# ONE OF THESE TWO ATTRIBUTES IS REQUIRED.  If CLEARPW is provided, and
# libhmac.a is available, CRAM authentication will be possible!

LDAP_CLEARPW clearPassword
LDAP_CRYPTPW userPassword

##NAME: LDAP_IDS:0
#
# Uncomment the following, and modify as appropriate, if your LDAP database
# stores individual userids and groupids.  Otherwise, you must uncomment
# LDAP_GLOB_UID and LDAP_GLOB_GID above.  LDAP_GLOB_UID and LDAP_GLOB_GID
# specify a uid/gid for everyone.  Otherwise, LDAP_UID and LDAP_GID must
# be defined as attributes for everyone.
#
LDAP_UID  uidNumber
LDAP_GID  gidNumber

##NAME: LDAP_AUXOPTIONS:0
#
# Auxiliary options.  The LDAP_AUXOPTIONS setting should contain a list of
# comma-separated "ATTRIBUTE=NAME" pairs.  These names are additional
# attributes that define various per-account "options", as given in
# INSTALL's description of the OPTIONS setting.
#
# Each ATTRIBUTE specifies an LDAP attribute name.  If it is present,
# the attribute value gets placed in the OPTIONS variable, with the name
# NAME.  For example:
```

```
#
#    LDAP_AUXOPTIONS shared=sharedgroup,allowimap=allowimap
#
# Then, if an LDAP record contains the following attributes:
#
#     shared: domain1
#     allowimap: 0
#
# Then authldap will initialize OPTIONS to "sharedgroup=domain1,allowimap=0"
#
# NOTE: ** no spaces in this setting **, the above example has exactly
# one tab character after LDAP_AUXOPTIONS



##NAME: LDAP_DEREF:0
#
# Determines how aliases are handled during a search.  This option is available
# only with OpenLDAP 2.0
#
# LDAP_DEREF can be one of the following values:
# never, searching, finding, always. If not specified, aliases are
# never dereferenced.

LDAP_DEREF never


##NAME: LDAP_TLS:0
#
# Set LDAP_TLS to 1 to enable LDAP over SSL/TLS.  Experimental setting.
# Requires OpenLDAP 2.0
#

LDAP_TLS 0


##NAME: LDAP_EMAILMAP:0
#
# The following optional settings, if enabled, result in an extra LDAP
# lookup to first locate a handle for an E-mail address, then a second lookup
# on that handle to get the actual authentication record.  You'll need
# to uncomment these settings to enable an email handle lookup.
#
# The E-mail address must be of the form user@realm, and this is plugged
# into the following search string.  "@user@" and "@realm@" are placeholders
# for the user and the realm portions of the login ID.
#
# LDAP_EMAILMAP  (&(userid=@user@)(realm=@realm@))



##NAME: LDAP_EMAILMAP_BASEDN:0
#
# Specify the basedn for the email lookup.  The default is LDAP_BASEDN.
#
# LDAP_EMAILMAP_BASEDN o=emailmap, c=com
```

```
##NAME: LDAP_EMAILMAP_ATTRIBUTE:0
#
# The attribute which holds the handle.  The contents of this attribute
# are then plugged into the regular authentication lookup, and you must set
# LDAP_EMAILMAP_MAIL to the name of this attribute in the authentication
# records (which may be the same as LDAP_MAIL).
# You MUST also leave LDAP_DOMAIN undefined.  This enables authenticating
# by handles only.
#
# Here's an example:
#
# dn: userid=john, realm=example.com, o=emailmap, c=com # LDAP_EMAILMAP_BASEDN
# userid: john          # LDAP_EMAILMAP search
# realm: example.com    # LDAP_EMAILMAP search
# handle: cc223344      # LDAP_EMAILMAP_ATTRIBUTE
#
#
# dn: controlHandle=cc223344, o=example, c=com      # LDAP_BASEDN
# controlHandle: cc223344         # LDAP_EMAILMAP_MAIL set to "controlHandle"
# uid: ...
# gid: ...
# [ etc... ]
#
# LDAP_EMAILMAP_ATTRIBUTE handle



##NAME: LDAP_EMAILMAP_MAIL:0
#
# After reading LDAP_EMAIL_ATTRIBUTE, the second query will go against
# LDAP_BASEDN, but will key against LDAP_EMAILMAP_MAIL instead of LDAP_MAIL.
#
# LDAP_EMAILMAP_MAIL mail
```

Apéndice E. Archivo de configuración `/etc/courier/pop3d`

```
#
#VERSION: $Id: courier-pop3d.xml,v 1.1 2004/06/29 20:33:33 sergio Exp $
#
# pop3d created from pop3d.dist by sysconftool
#
# Do not alter lines that begin with ##, they are used when upgrading
# this configuration.
#
#  Copyright 1998 - 2002 Double Precision, Inc.  See COPYING for
#  distribution information.
#
#  Courier POP3 daemon configuration
#
##NAME: PIDFILE:0
#

PIDFILE=/var/run/courier/pop3d.pid

##NAME: MAXDAEMONS:0
#
#  Maximum number of POP3 servers started
#

MAXDAEMONS="40"

##NAME: MAXPERIP:4
#
#  Maximum number of connections to accept from the same IP address

MAXPERIP="4"

##NAME: AUTHMODULES:0
#
#########################################################################
##
## Authentication modules which attempt to validate userid/password
## combinations.  See authpam(8) for more information.  The default set
## is installed at configuration time.  You may have to edit the following
## to remove unnecessary authentication modules.  In particular, if
## authpam is included in the list below, you will have to remove authpwd
## and authshadow, since their functionality is included in the authpam
## module.
##
#########################################################################
#
# If this is currently set to AUTHMODULES="authdaemon", DO NOT CHANGE IT.
# Instead, change the parameter authmodulelist in authdaemonrc.

AUTHMODULES="authdaemon"


##NAME: AUTHMODULES_ORIG:0
```

```
#
# This setting is for use with webadmin

AUTHMODULES_ORIG="authdaemon"

##NAME: DEBUG_LOGIN:0
#
# Dump additional login diagnostics to syslog
#
# DEBUG_LOGIN=0   - turn off login debugging
# DEBUG_LOGIN=1   - turn on login debugging
# DEBUG_LOGIN=2   - turn on login debugging + log passwords too

DEBUG_LOGIN=0

##NAME: POP3AUTH:1
#
# To advertise the SASL capability, per RFC 2449, uncomment the POP3AUTH
# variable:
#
# POP3AUTH="LOGIN"
#
# If you have configured the CRAM-MD5 or CRAM-SHA1, set POP3AUTH to something
# like this:
#
# POP3AUTH="LOGIN CRAM-MD5 CRAM-SHA1"

POP3AUTH=""

##NAME: POP3AUTH_ORIG:0
#
# For use by webadmin

POP3AUTH_ORIG="LOGIN CRAM-MD5 CRAM-SHA1"

##NAME: POP3AUTH_TLS:1
#
# To also advertise SASL PLAIN if SSL is enabled, uncomment the
# POP3AUTH_TLS environment variable:
#
# POP3AUTH_TLS="LOGIN PLAIN"

POP3AUTH_TLS=""

##NAME: POP3AUTH_TLS_ORIG:0
#
# For use by webadmin

POP3AUTH_TLS_ORIG="LOGIN PLAIN"

##NAME: PORT:1
#
# Port to listen on for connections.  The default is port 110.
#
#  Multiple port numbers can be separated by commas.  When multiple port
#  numbers are used it is possibly to select a specific IP address for a
#  given port as "ip.port".  For example, "127.0.0.1.900,192.68.0.1.900"
```

```
#  accepts connections on port 900 on IP addresses 127.0.0.1 and 192.68.0.1
#  The ADDRESS setting is a default for ports that do not have a specified
#  IP address.

PORT=110

##NAME: ADDRESS:0
#
# IP address to listen on.  0 means all IP addresses.

ADDRESS=0

##NAME: TCPDOPTS:0
#
# Other couriertcpd(1) options.  The following defaults should be fine.
#

TCPDOPTS="-nodnslookup -noidentlookup"

##NAME: POP3DSTART:0
#
# POP3DSTART is not referenced anywhere in the standard Courier programs
# or scripts.  Rather, this is a convenient flag to be read by your system
# startup script in /etc/rc.d, like this:
#
#  . /etc/courier/pop3d
#  case x$POP3DSTART in
#  x[yY]*)
#        /usr/lib/courier/pop3d.rc start
#        ;;
#  esac
#
# The default setting is going to be NO, until Courier is shipped by default
# with enough platforms so that people get annoyed with having to flip it to
# YES every time.

POP3DSTART="YES"

##NAME: MAILDIRPATH:0
#
# MAILDIRPATH - directory name of the maildir directory.
#
MAILDIRPATH=Maildir
```

Apéndice F. Archivo de configuración `/etc/courier/pop3d-ssl`

```
#
#VERSION: $Id: courier-pop3d-ssl.xml,v 1.1 2004/06/29 20:33:32 sergio Exp $
#
# pop3d-ssl created from pop3d-ssl.dist by sysconftool
#
# Do not alter lines that begin with ##, they are used when upgrading
# this configuration.
#
#  Copyright 2000-2002 Double Precision, Inc.  See COPYING for
#  distribution information.
#
#  This configuration file sets various options for the Courier-IMAP server
#  when used to handle SSL POP3 connections.
#
#  SSL and non-SSL connections are handled by a dedicated instance of the
#  couriertcpd daemon.  If you are accepting both SSL and non-SSL POP3
#  connections, you will start two instances of couriertcpd, one on the
#  POP3 port 110, and another one on the POP3-SSL port 995.
#
#  Download OpenSSL from http://www.openssl.org/
#
##NAME: SSLPORT:0
#
#  Options in the pop3d-ssl configuration file AUGMENT the options in the
#  pop3d configuration file.  First the pop3d configuration file is read,
#  then the pop3d-ssl configuration file, so we do not have to redefine
#  anything.
#
#  However, some things do have to be redefined.  The port number is
#  specified by SSLPORT, instead of PORT.  The default port is port 995.
#
#  Multiple port numbers can be separated by commas.  When multiple port
#  numbers are used it is possibly to select a specific IP address for a
#  given port as "ip.port".  For example, "127.0.0.1.900,192.68.0.1.900"
#  accepts connections on port 900 on IP addresses 127.0.0.1 and 192.68.0.1
#  The SSLADDRESS setting is a default for ports that do not have
#  a specified IP address.

SSLPORT=995

##NAME: SSLADDRESS:0
#
#  Address to listen on, can be set to a single IP address.
#
# SSLADDRESS=127.0.0.1

SSLADDRESS=0

##NAME: SSLPIDFILE:0
#
# You can also redefine AUTHMODULES, although I can't
# think of why you'd want to do that.
```

```
#
#

SSLPIDFILE=/var/run/courier/pop3d-ssl.pid

##NAME: POP3DSSLSTART:0
#
#  Whether or not to start POP3 over SSL on spop3 port:

POP3DSSLSTART="YES"

##NAME: POP3_STARTTLS:0
#
# Whether or not to implement the POP3 STLS extension:

POP3_STARTTLS=YES

##NAME: POP3_TLS_REQUIRED:1
#
# Set POP3_TLS_REQUIRED to 1 if you REQUIRE STARTTLS for everyone.
# (this option advertises the LOGINDISABLED POP3 capability, until STARTTLS
# is issued).

POP3_TLS_REQUIRED="1"

##NAME: COURIERTLS:0
#
# The following variables configure POP3 over SSL.  If OpenSSL is available
# during configuration, the couriertls helper gets compiled, and upon
# installation a dummy TLS_CERTFILE gets generated.  courieresmtpd will
# automatically advertise the ESMTP STARTTLS extension if both TLS_CERTFILE
# and COURIERTLS exist.
#
# WARNING: Peer certificate verification has NOT yet been tested.  Proceed
# at your own risk.  Only the basic SSL/TLS functionality is known to be
# working. Keep this in mind as you play with the following variables.

COURIERTLS=/usr/bin/couriertls

##NAME: TLS_PROTOCOL:0
#
# TLS_PROTOCOL sets the protocol version.  The possible versions are:
#
# SSL2 - SSLv2
# SSL3 - SSLv3
# TLS1 - TLS1

TLS_PROTOCOL=SSL3

##NAME: TLS_STARTTLS_PROTOCOL:0
#
# TLS_STARTTLS_PROTOCOL is used instead of TLS_PROTOCOL for the POP3 STARTTLS
# extension, as opposed to POP3 over SSL on port 995.
#

TLS_STARTTLS_PROTOCOL=TLS1
```

```
##NAME: TLS_CIPHER_LIST:0
#
# TLS_CIPHER_LIST optionally sets the list of ciphers to be used by the
# OpenSSL library.  In most situations you can leave TLS_CIPHER_LIST
# undefined
#
# TLS_CIPHER_LIST="ALL:!ADH:RC4+RSA:+SSLv2:@STRENGTH"

##NAME: TLS_TIMEOUT:0
# TLS_TIMEOUT is currently not implemented, and reserved for future use.
# This is supposed to be an inactivity timeout, but its not yet implemented.
#

##NAME: TLS_DHCERTFILE:0
#
# TLS_DHCERTFILE - PEM file that stores our Diffie-Hellman cipher pair.
# When OpenSSL is compiled to use Diffie-Hellman ciphers instead of RSA
# you must generate a DH pair that will be used.  In most situations the
# DH pair is to be treated as confidential, and the file specified by
# TLS_DHCERTFILE must not be world-readable.
#
# TLS_DHCERTFILE=

##NAME: TLS_CERTFILE:0
#
# TLS_CERTFILE - certificate to use.  TLS_CERTFILE is required for SSL/TLS
# servers, and is optional for SSL/TLS clients.  TLS_CERTFILE is usually
# treated as confidential, and must not be world-readable.
#
TLS_CERTFILE=/etc/courier/pop3d.pem

##NAME: TLS_TRUSTCERTS:0
#
# TLS_TRUSTCERTS=pathname - load trusted certificates from pathname.
# pathname can be a file or a directory. If a file, the file should
# contain a list of trusted certificates, in PEM format. If a
# directory, the directory should contain the trusted certificates,
# in PEM format, one per file and hashed using OpenSSL's c_rehash
# script. TLS_TRUSTCERTS is used by SSL/TLS clients (by specifying
# the -domain option) and by SSL/TLS servers (TLS_VERIFYPEER is set
# to PEER or REQUIREPEER).
#
#
# TLS_TRUSTCERTS=

##NAME: TLS_VERIFYPEER:0
#
# TLS_VERIFYPEER - how to verify client certificates.  The possible values of
# this setting are:
#
# NONE - do not verify anything
#
# PEER - verify the client certificate, if one's presented
#
# REQUIREPEER - require a client certificate, fail if one's not presented
#
#
```

```
TLS_VERIFYPEER=NONE

##NAME: TLS_CACHE:0
#
# A TLS/SSL session cache may slightly improve response for long-running
# POP3 clients. TLS_CACHEFILE will be automatically created, TLS_CACHESIZE
# bytes long, and used as a cache buffer.
#
# This is an experimental feature and should be disabled if it causes
# problems with SSL clients.  Disable SSL caching by commenting out the
# following settings:

TLS_CACHEFILE=/var/lib/courier/couriersslcache
TLS_CACHESIZE=524288
```

Apéndice G. Archivo de configuración /etc/courier/imapd

```
#
#VERSION: $Id: courier-imapd.xml,v 1.1 2004/06/29 20:33:32 sergio Exp $
#
# imapd created from imapd.dist by sysconftool
#
# Do not alter lines that begin with ##, they are used when upgrading
# this configuration.
#
#  Copyright 1998 - 2004 Double Precision, Inc.  See COPYING for
#  distribution information.
#
#  This configuration file sets various options for the Courier-IMAP server
#  when used with the couriertcpd server.
#  A lot of the stuff here is documented in the manual page for couriertcpd.
#
#  NOTE - do not use \ to split long variable contents on multiple lines.
#  This will break the default imapd.rc script, which parses this file.
#
##NAME: ADDRESS:0
#
#  Address to listen on, can be set to a single IP address.
#
# ADDRESS=127.0.0.1

ADDRESS=0

##NAME: PORT:1
#
#  Port numbers that connections are accepted on.  The default is 143,
#  the standard IMAP port.
#
#  Multiple port numbers can be separated by commas.  When multiple port
#  numbers are used it is possible to select a specific IP address for a
#  given port as "ip.port".  For example, "127.0.0.1.900,192.68.0.1.900"
#  accepts connections on port 900 on IP addresses 127.0.0.1 and 192.68.0.1
#  The previous ADDRESS setting is a default for ports that do not have
#  a specified IP address.

PORT=143

##NAME: AUTHSERVICE:0
#
#  It’s possible to authenticate using a different ’service’ parameter
#  depending on the connection’s port.  This only works with authentication
#  modules that use the ’service’ parameter, such as PAM.  Example:
#
#  AUTHSERVICE143=imap
#  AUTHSERVICE993=imaps

##NAME: MAXDAEMONS:0
#
#  Maximum number of IMAP servers started
```

```
#

MAXDAEMONS="40"

##NAME: MAXPERIP:0
#
#  Maximum number of connections to accept from the same IP address

MAXPERIP="4"

##NAME: PIDFILE:0
#
#  File where couriertcpd will save its process ID
#

PIDFILE=/var/run/courier/imapd.pid

##NAME: TCPDOPTS:0
#
# Miscellaneous couriertcpd options that shouldn't be changed.
#

TCPDOPTS="-nodnslookup -noidentlookup"

##NAME: AUTHMODULES:0
#
# Authentication modules.  Here's the default list:
#
#    authdaemon
#
# The default is set during the initial configuration.
#
# If this is currently set to AUTHMODULES="authdaemon", DO NOT CHANGE IT.
# Instead, change the parameter authmodulelist in authdaemonrc.

AUTHMODULES="authdaemon"

##NAME: AUTHMODULES_ORIG:0
#
# For use by webadmin

AUTHMODULES_ORIG="authdaemon"

##NAME: DEBUG_LOGIN:0
#
# Dump additional login diagnostics to syslog
#
# DEBUG_LOGIN=0   - turn off login debugging
# DEBUG_LOGIN=1   - turn on login debugging
# DEBUG_LOGIN=2   - turn on login debugging + log passwords too

DEBUG_LOGIN=0

##NAME: IMAP_CAPABILITY:1
#
# IMAP_CAPABILITY specifies what most of the response should be to the
# CAPABILITY command.
```

```
#
# If you have properly configured Courier to use CRAM-MD5 or CRAM-SHA1
# authentication (see INSTALL), set IMAP_CAPABILITY as follows:
#
# IMAP_CAPABILITY="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT \
#             THREAD=REFERENCES SORT QUOTA AUTH=CRAM-MD5 AUTH=CRAM-SHA1 IDLE"
#

IMAP_CAPABILITY="IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT \
                 THREAD=REFERENCES SORT QUOTA IDLE"

##NAME: KEYWORDS_CAPABILITY:0
#
# IMAP_KEYWORDS=1 enables custom IMAP keywords.  Set this option to 0 to
# disable custom keywords.

IMAP_KEYWORDS=1

##NAME: SMAP1_CAPABILITY:0
#
# EXPERIMENTAL
#
# To enable the experimental "Simple Mail Access Protocol" extensions,
# uncomment the following setting.
#
# SMAP_CAPABILITY=SMAP1

##NAME: IMAP_CAPABILITY_ORIG:1
#
# For use by webadmin

IMAP_CAPABILITY_ORIG="IMAP4rev1 UIDPLUS CHILDREN \
                      NAMESPACE THREAD=ORDEREDSUBJECT \
                      THREAD=REFERENCES SORT QUOTA AUTH=CRAM-MD5 AUTH=CRAM-SHA1
IDLE"

##NAME: IMAP_IDLE_TIMEOUT:0
#
# This setting controls how often
# the server polls for changes to the folder, in IDLE mode (in seconds).

IMAP_IDLE_TIMEOUT=60

##NAME: IMAP_CAPABILITY_TLS:0
#
# The following setting will advertise SASL PLAIN authentication after
# STARTTLS is established.  If you want to allow SASL PLAIN authentication
# with or without TLS then just comment this out, and add AUTH=PLAIN to
# IMAP_CAPABILITY

IMAP_CAPABILITY_TLS="$IMAP_CAPABILITY AUTH=PLAIN"

##NAME: IMAP_TLS_ORIG:0
#
# For use by webadmin

IMAP_CAPABILITY_TLS_ORIG="$IMAP_CAPABILITY_ORIG AUTH=PLAIN"
```

```
##NAME: IMAP_DISABLETHREADSORT:0
#
# Set IMAP_DISABLETHREADSORT to disable the THREAD and SORT commands -
# server side sorting and threading.
#
# Those capabilities will still be advertised, but the server will reject
# them.  Set this option if you want to disable all the extra load from
# server-side threading and sorting.  Not advertising those capabilities
# will simply result in the clients reading the entire folder, and sorting
# it on the client side.  That will still put some load on the server.
# advertising these capabilities, but rejecting the commands, will stop this
# silliness.
#

IMAP_DISABLETHREADSORT=0

##NAME: IMAP_CHECK_ALL_FOLDERS:0
#
# Set IMAP_CHECK_ALL_FOLDERS to 1 if you want the server to check for new
# mail in every folder.  Not all IMAP clients use the IMAP's new mail
# indicator, but some do.  Normally new mail is checked only in INBOX,
# because it is a comparatively time consuming operation, and it would be
# a complete waste of time unless mail filters are used to deliver
# mail directly to folders.
#
# When IMAP clients are used which support new mail indication, and when
# mail filters are used to sort incoming mail into folders, setting
# IMAP_CHECK_ALL_FOLDERS to 1 will allow IMAP clients to announce new
# mail in folders.  Note that this will result in slightly more load on the
# server.
#

IMAP_CHECK_ALL_FOLDERS=0

##NAME: IMAP_OBSOLETE_CLIENT:0
#
# Set IMAP_OBSOLETE_CLIENT if your IMAP client expects \\NoInferiors to mean
# what \\HasNoChildren really means.

IMAP_OBSOLETE_CLIENT=0

##NAME: IMAP_ULIMITD:0
#
# IMAP_ULIMITD sets the maximum size of the data segment of the server
# process.  The value of IMAP_ULIMITD is simply passed to the "ulimit -d"
# command (or ulimit -v).  The argument to ulimi sets the upper limit on the
# size of the data segment of the server process, in kilobytes.  The default
# value of 65536 sets a very generous limit of 64 megabytes, which should
# be more than plenty for anyone.
#
# This feature is used as an additional safety check that should stop
# any potential denial-of-service attacks that exploit any kind of
# a memory leak to exhaust all the available memory on the server.
# It is theoretically possible that obscenely huge folders will also
# result in the server running out of memory when doing server-side
# sorting (by my calculations you have to have at least 100,000 messages
```

```
# in a single folder, for that to happen).

IMAP_ULIMITD=65536

##NAME: IMAP_USELOCKS:0
#
# Setting IMAP_USELOCKS to 1 will use dot-locking to support concurrent
# multiple access to the same folder.  This incurs slight additional
# overhead.  Concurrent multiple access will still work without this setting,
# however occasionally a minor race condition may result in an IMAP client
# downloading the same message twice, or a keyword update will fail.
#
# IMAP_USELOCKS=1 is strongly recommended when shared folders are used.

IMAP_USELOCKS=1

##NAME: IMAP_SHAREDINDEXFILE:0
#
# The index of all accessible folders.  Do not change this setting unless
# you know what you're doing.  See README.sharedfolders for additional
# information.

IMAP_SHAREDINDEXFILE=/etc/courier/shared/index

##NAME: IMAP_ENHANCEDIDLE:0
#
# If Courier was compiled with the File Alteration Monitor, setting
# IMAP_ENHANCEDIDLE to 1 enables enhanced IDLE mode, where multiple
# clients may open the same folder concurrently, and receive updates to
# folder contents in realtime.  See the imapd(8) man page for additional
# information.
#
# IMPORTANT: IMAP_USELOCKS *MUST* also be set to 1, and IDLE must be included
# in the IMAP_CAPABILITY list.
#

IMAP_ENHANCEDIDLE=0

##NAME: IMAP_TRASHFOLDERNAME:0
#
# The name of the magic trash Folder.  For MSOE compatibility,
# you can set IMAP_TRASHFOLDERNAME="Deleted Items".
#
# IMPORTANT:  If you change this, you must also change IMAP_EMPTYTRASH

IMAP_TRASHFOLDERNAME=Trash

##NAME: IMAP_EMPTYTRASH:0
#
# The following setting is optional, and causes messages from the given
# folder to be automatically deleted after the given number of days.
# IMAP_EMPTYTRASH is a comma-separated list of folder:days.  The default
# setting, below, purges 7 day old messages from the Trash folder.
# Another useful setting would be:
#
# IMAP_EMPTYTRASH=Trash:7,Sent:30
#
```

```
# This would also delete messages from the Sent folder (presumably copies
# of sent mail) after 30 days.  This is a global setting that is applied to
# every mail account, and is probably useful in a controlled, corporate
# environment.
#
# Important: the purging is controlled by CTIME, not MTIME (the file time
# as shown by ls).  It is perfectly ordinary to see stuff in Trash that's
# a year old.  That's the file modification time, MTIME, that's displayed.
# This is generally when the message was originally delivered to this
# mailbox.  Purging is controlled by a different timestamp, CTIME, which is
# changed when the file is moved to the Trash folder (and at other times too).
#
# You might want to disable this setting in certain situations - it results
# in a stat() of every file in each folder, at login and logout.
#

IMAP_EMPTYTRASH=Trash:7

##NAME: IMAP_MOVE_EXPUNGE_TO_TRASH:0
#
# Set IMAP_MOVE_EXPUNGE_TO_TRASH to move expunged messages to Trash.  This
# effectively allows an undo of message deletion by fishing the deleted
# mail from trash.  Trash can be manually expunged as usually, and mail
# will get automatically expunged from Trash according to IMAP_EMPTYTRASH.
#
# NOTE: shared folders are still expunged as usual.  Shared folders are
# not affected.
#

IMAP_MOVE_EXPUNGE_TO_TRASH=0


##NAME: OUTBOX:0
#
# The next set of options deal with the "Outbox" enhancement.
# Uncomment the following setting to create a special folder, named
# INBOX.Outbox
#
# OUTBOX=.Outbox

##NAME: SENDMAIL:0
#
# If OUTBOX is defined, mail can be sent via the IMAP connection by copying
# a message to the INBOX.Outbox folder.  For all practical matters,
# INBOX.Outbox looks and behaves just like any other IMAP folder.  If this
# folder doesn't exist it must be created by the IMAP mail client, just
# like any other IMAP folder.  The kicker: any message copied or moved to
# this folder is will be E-mailed by the Courier-IMAP server, by running
# the SENDMAIL program.  Therefore, messages copied or moved to this
# folder must be well-formed RFC-2822 messages, with the recipient list
# specified in the To:, Cc:, and Bcc: headers.  Courier-IMAP relies on
# SENDMAIL to read the recipient list from these headers (and delete the Bcc:
# header) by running the command "$SENDMAIL -oi -t -f $SENDER", with the
# message piped on standard input.  $SENDER will be the return address
# of the message, which is set by the authentication module.
#
# DO NOT MODIFY SENDMAIL, below, unless you know what you're doing.
```

```
#

SENDMAIL=/usr/sbin/sendmail

##NAME: HEADERFROM:0
#
# For administrative and oversight purposes, the return address, $SENDER
# will also be saved in the X-IMAP-Sender mail header.  This header gets
# added to the sent E-mail (but it doesn't get saved in the copy of the
# message that's saved in the folder)
#
# WARNING - By enabling OUTBOX above, *every* IMAP mail client will receive
# the magic OUTBOX treatment.  Therefore advance LARTing is in order for
# _all_ of your lusers, until every one of them is aware of this.  Otherwise if
# OUTBOX is left at its default setting - a folder name that might be used
# accidentally - some people may be in for a rude surprise.  You can redefine
# the name of the magic folder by changing OUTBOX, above.  You should do that
# and pick a less-obvious name.  Perhaps brand it with your organizational
# name ( OUTBOX=.WidgetsAndSonsOutbox )

HEADERFROM=X-IMAP-Sender

##NAME: IMAPDSTART:0
#
# IMAPDSTART is not used directly.  Rather, this is a convenient flag to
# be read by your system startup script in /etc/rc.d, like this:
#
#  . /etc/courier/imapd
#
#  case x$IMAPDSTART in
#  x[yY]*)
#        /usr/lib/courier/imapd.rc start
#        ;;
#  esac
#
# The default setting is going to be NO, so you'll have to manually flip
# it to yes.

IMAPDSTART="YES"

##NAME: MAILDIRPATH:0
#
# MAILDIRPATH - directory name of the maildir directory.
#
MAILDIRPATH=Maildir
```

Apéndice H. Archivo de configuración `/etc/courier/imapd-ssl`

```
#
#VERSION: $Id: courier-imapd-ssl.xml,v 1.1 2004/06/29 20:33:32 sergio Exp $
#
# imapd-ssl created from imapd-ssl.dist by sysconftool
#
# Do not alter lines that begin with ##, they are used when upgrading
# this configuration.
#
#  Copyright 2000 - 2002 Double Precision, Inc.  See COPYING for
#  distribution information.
#
#  This configuration file sets various options for the Courier-IMAP server
#  when used to handle SSL IMAP connections.
#
#  SSL and non-SSL connections are handled by a dedicated instance of the
#  couriertcpd daemon.  If you are accepting both SSL and non-SSL IMAP
#  connections, you will start two instances of couriertcpd, one on the
#  IMAP port 143, and another one on the IMAP-SSL port 993.
#
#  Download OpenSSL from http://www.openssl.org/
#
##NAME: SSLPORT:1
#
#  Options in the imapd-ssl configuration file AUGMENT the options in the
#  imapd configuration file.  First the imapd configuration file is read,
#  then the imapd-ssl configuration file, so we do not have to redefine
#  anything.
#
#  However, some things do have to be redefined.  The port number is
#  specified by SSLPORT, instead of PORT.  The default port is port 993.
#
#  Multiple port numbers can be separated by commas.  When multiple port
#  numbers are used it is possibly to select a specific IP address for a
#  given port as "ip.port".  For example, "127.0.0.1.900,192.68.0.1.900"
#  accepts connections on port 900 on IP addresses 127.0.0.1 and 192.68.0.1
#  The SSLADDRESS setting is a default for ports that do not have
#  a specified IP address.

SSLPORT=993

##NAME: SSLADDRESS:0
#
#  Address to listen on, can be set to a single IP address.
#
# SSLADDRESS=127.0.0.1

SSLADDRESS=0

##NAME: SSLPIDFILE:0
#
# That’s the SSL IMAP port we’ll listen on.
# Feel free to redefine MAXDAEMONS, TCPDOPTS, and MAXPERIP.
```

```
SSLPIDFILE=/var/run/courier/imapd-ssl.pid

##NAME: IMAPDSSLSTART:0
#
# Different pid files, so that both instances of couriertcpd can coexist
# happily.
#
# You can also redefine AUTHMODULES and IMAP_CAPABILITY, although I can't
# think of why you'd want to do that.
#
#
# Ok, the following settings are new to imapd-ssl:
#
#  Whether or not to start IMAP over SSL on simap port:

IMAPDSSLSTART="YES"

##NAME: IMAPDSTARTTLS:0
#
#  Whether or not to implement IMAP STARTTLS extension instead:

IMAPDSTARTTLS="YES"

##NAME: IMAP_TLS_REQUIRED:1
#
# Set IMAP_TLS_REQUIRED to 1 if you REQUIRE STARTTLS for everyone.
# (this option advertises the LOGINDISABLED IMAP capability, until STARTTLS
# is issued).

IMAP_TLS_REQUIRED="1"


#########################################################################
#
# The following variables configure IMAP over SSL.  If OpenSSL is available
# during configuration, the couriertls helper gets compiled, and upon
# installation a dummy TLS_CERTFILE gets generated.  courieresmtpd will
# automatically advertise the ESMTP STARTTLS extension if both TLS_CERTFILE
# and COURIERTLS exist.
#
# WARNING: Peer certificate verification has NOT yet been tested.  Proceed
# at your own risk.  Only the basic SSL/TLS functionality is known to be
# working. Keep this in mind as you play with the following variables.
#
##NAME: COURIERTLS:0
#

COURIERTLS=/usr/bin/couriertls

##NAME: TLS_PROTOCOL:0
#
# TLS_PROTOCOL sets the protocol version.  The possible versions are:
#
# SSL2 - SSLv2
# SSL3 - SSLv3
# TLS1 - TLS1
```

```
TLS_PROTOCOL=SSL3

##NAME: TLS_STARTTLS_PROTOCOL:0
#
# TLS_STARTTLS_PROTOCOL is used instead of TLS_PROTOCOL for the IMAP STARTTLS
# extension, as opposed to IMAP over SSL on port 993.
#

TLS_STARTTLS_PROTOCOL=TLS1

##NAME: TLS_CIPHER_LIST:0
#
# TLS_CIPHER_LIST optionally sets the list of ciphers to be used by the
# OpenSSL library.  In most situations you can leave TLS_CIPHER_LIST
# undefined
#
# TLS_CIPHER_LIST="ALL:!ADH:RC4+RSA:+SSLv2:@STRENGTH"

##NAME: TLS_TIMEOUT:0
# TLS_TIMEOUT is currently not implemented, and reserved for future use.
# This is supposed to be an inactivity timeout, but its not yet implemented.
#

##NAME: TLS_DHCERTFILE:0
#
# TLS_DHCERTFILE - PEM file that stores our Diffie-Hellman cipher pair.
# When OpenSSL is compiled to use Diffie-Hellman ciphers instead of RSA
# you must generate a DH pair that will be used.  In most situations the
# DH pair is to be treated as confidential, and the file specified by
# TLS_DHCERTFILE must not be world-readable.
#
# TLS_DHCERTFILE=

##NAME: TLS_CERTFILE:0
#
# TLS_CERTFILE - certificate to use.  TLS_CERTFILE is required for SSL/TLS
# servers, and is optional for SSL/TLS clients.  TLS_CERTFILE is usually
# treated as confidential, and must not be world-readable.
#
TLS_CERTFILE=/etc/courier/imapd.pem

##NAME: TLS_TRUSTCERTS:0
#
# TLS_TRUSTCERTS=pathname - load trusted certificates from pathname.
# pathname can be a file or a directory. If a file, the file should
# contain a list of trusted certificates, in PEM format. If a
# directory, the directory should contain the trusted certificates,
# in PEM format, one per file and hashed using OpenSSL's c_rehash
# script. TLS_TRUSTCERTS is used by SSL/TLS clients (by specifying
# the -domain option) and by SSL/TLS servers (TLS_VERIFYPEER is set
# to PEER or REQUIREPEER).
#
#
# TLS_TRUSTCERTS=

##NAME: TLS_VERIFYPEER:0
```

```
#
# TLS_VERIFYPEER - how to verify client certificates.  The possible values of
# this setting are:
#
# NONE - do not verify anything
#
# PEER - verify the client certificate, if one's presented
#
# REQUIREPEER - require a client certificate, fail if one's not presented
#
#
TLS_VERIFYPEER=NONE

##NAME: TLS_CACHE:0
#
# A TLS/SSL session cache may slightly improve response for IMAP clients
# that open multiple SSL sessions to the server.  TLS_CACHEFILE will be
# automatically created, TLS_CACHESIZE bytes long, and used as a cache
# buffer.
#
# This is an experimental feature and should be disabled if it causes
# problems with SSL clients.  Disable SSL caching by commenting out the
# following settings:

TLS_CACHEFILE=/var/lib/courier/couriersslcache
TLS_CACHESIZE=524288
```

Apéndice I. Archivo de configuración `/etc/amavis/amavisd.conf`

```
use strict;

# Configuration file for amavisd-new
# Defaults modified for the Debian amavisd-new package
# $Id: amavisd-amavisd.conf.xml,v 1.1 2004/06/29 20:33:32 sergio Exp $
#
# This software is licensed under the GNU General Public License (GPL).
# See comments at the start of amavisd-new for the whole license text.

#Sections:
# Section I    - Essential daemon and MTA settings
# Section II   - MTA specific
# Section III  - Logging
# Section IV   - Notifications/DSN, BOUNCE/REJECT/DROP/PASS destiny, quarantine
# Section V    - Per-recipient and per-sender handling, whitelisting, etc.
# Section VI   - Resource limits
# Section VII  - External programs, virus scanners, SpamAssassin
# Section VIII - Debugging

#GENERAL NOTES:
#  This file is a normal Perl code, interpreted by Perl itself.
#  - make sure this file (or directory where it resides) is NOT WRITABLE
#    by mere mortals, otherwise it represents a severe security risk!
#  - for values which are interpreted as booleans, it is recommended
#    to use 1 for true, and 0 or undef or ” for false.
#    THIS IS DIFFERENT FROM OLDER AMAVIS VERSIONS where "no" also meant false,
#    now it means true, like any nonempty string does!
#  - Perl syntax applies. Most notably: strings in "" may include variables
#    (which start with $ or @); to include characters @ and $ in double
#    quoted strings, precede them by a backslash; in single-quoted strings
#    the $ and @ lose their special meaning, so it is usually easier to use
#    single quoted strings. Still, in both cases backslash needs to be doubled.
#  - variables with names starting with a ’@’ are lists, the values assigned
#    to them should be lists as well, e.g. (’one@foo’, $mydomain, "three");
#    note the comma-separation and parenthesis. If strings in the list
#    do not contain spaces nor variables, a Perl operator qw() may be used
#    as a shorthand to split its argument on whitespace and produce a list
#    of strings, e.g. qw( one@foo example.com three );  Note that the argument
#    to qw is quoted implicitly and no variable interpretation is done within
#    (no ’$’ variable evaluations). The #-initiated comments can not be used
#    within the string. In other words, $ and # lose their special meaning
#    within a qw argument, just like within ’...’ strings.
#  - all e-mail addresses in this file and as used internally by the daemon
#    are in their raw (rfc2821-unquoted and nonbracketed) form, i.e.
#    Bob "Funny" Dude@example.com, not: "Bob \"Funny\" Dude"@example.com
#    and not <"Bob \"Funny\" Dude"@example.com>; also: ” and not ’<>’.


#
# Section I - Essential daemon and MTA settings
#
```

```
# $MYHOME serves as a quick default for some other configuration settings.
# More refined control is available with each individual setting further down.
# $MYHOME is not used directly by the program. No trailing slash!
$MYHOME = '/var/lib/amavis';   # (default is '/var/amavis')

# $mydomain serves as a quick default for some other configuration settings.
# More refined control is available with each individual setting further down.
# $mydomain is never used directly by the program.
$mydomain = 'gsr.pt';      # (no useful default)

# Set the user and group to which the daemon will change if started as root
# (otherwise just keeps the UID unchanged, and these settings have no effect):
$daemon_user  = 'amavis'; # (no default (undef))
$daemon_group = 'amavis'; # (no default (undef))

# Runtime working directory (cwd), and a place where
# temporary directories for unpacking mail are created.
# if you change this, you might want to modify the cleanup()
# function in /etc/init.d/amavisd-new
# (no trailing slash, may be a scratch file system)
$TEMPBASE = $MYHOME;           # (must be set if other config vars use is)
#$TEMPBASE = "$MYHOME/tmp";     # prefer to keep home dir /var/amavis clean?

# $helpers_home sets environment variable HOME, and is passed as option
# 'home_dir_for_helpers' to Mail::SpamAssassin::new. It should be a directory
# on a normal persistent file system, not a scratch or temporary file system
#$helpers_home = $MYHOME;      # (defaults to $MYHOME)

# Run the daemon in the specified chroot jail if nonempty:
#$daemon_chroot_dir = $MYHOME;  # (default is undef, meaning: do not chroot)

$pid_file  = "/var/run/amavis/amavisd.pid";  # (default: "$MYHOME/amavisd.pid")
$lock_file = "/var/run/amavis/amavisd.lock"; # (default: "$MYHOME/amavisd.lock")

# set environment variables if you want (no defaults):
$ENV{TMPDIR} = $TEMPBASE;       # wise, but usually not necessary
#...


# MTA SETTINGS, UNCOMMENT AS APPROPRIATE,
# both $forward_method and $notify_method default to 'smtp:127.0.0.1:10025'

# POSTFIX, or SENDMAIL in dual-MTA setup, or EXIM V4
# (set host and port number as required; host can be specified
# as IP address or DNS name (A or CNAME, but MX is ignored)
$forward_method = 'smtp:127.0.0.1:10025';  # where to forward checked mail
$notify_method = $forward_method;          # where to submit notifications

# NOTE: The defaults (above) are good for Postfix or dual-sendmail. You MUST
#       uncomment the appropriate settings below if using other setups!

# SENDMAIL MILTER, using amavis-milter.c helper program:
# SEE amavisd-new-milter package docs FOR DEBIAN INSTRUCTIONS
#$forward_method = undef;  # no explicit forwarding, sendmail does it by itself
# milter; option -odd is needed to avoid deadlocks
#$notify_method = 'pipe:flags=q argv=/usr/sbin/sendmail -Ac -i -odd \
#                                                  -f ${sender} -- ${recipient}';
```

```
# just a thought: can we use use -Am instead of -odd ?

# SENDMAIL (old non-milter setup, as relay):
#$forward_method = 'pipe:flags=q argv=/usr/sbin/sendmail \
#                       -C/etc/sendmail.orig.cf -i -f ${sender} -- ${recipient}';
#$notify_method = $forward_method;

# SENDMAIL (old non-milter setup, amavis.c calls local delivery agent):
#$forward_method = undef;  # no explicit forwarding, amavis.c will call LDA
#$notify_method = 'pipe:flags=q argv=/usr/sbin/sendmail -Ac -i \
#                                                  -f ${sender} -- ${recipient}';

# EXIM v3 (not recommended with v4 or later, which can use SMTP setup instead):
#$forward_method = 'pipe:flags=q argv=/usr/sbin/exim -oMr scanned-ok -i \
#                                          -f ${sender} -- ${recipient}';
#$notify_method = $forward_method;

# prefer to collect mail for forwarding as BSMTP files?
#$forward_method = "bsmtp:$MYHOME/out-%i-%n.bsmtp";
#$notify_method = $forward_method;


# Net::Server pre-forking settings
# You may want $max_servers to match the width of your MTA pipe
# feeding amavisd, e.g. with Postfix the 'Max procs' field in the
# master.cf file, like the '2' in the:  smtp-amavis unix - - n - 2 smtp
#
$max_servers  =  2;   # number of pre-forked children          (default 2)
$max_requests = 10;   # retire a child after that many accepts (default 10)

$child_timeout=5*60;  # abort child if it does not complete each task in n sec
                      # (default: 8*60 seconds)

# Check also the settings of @av_scanners at the end if you want to use
# virus scanners. If not, you may want to delete the whole long assignment
# to the variable @av_scanners, which will also remove the virus checking
# code (e.g. if you only want to do spam scanning).

# Here is a QUICK WAY to completely DISABLE some sections of code
# that WE DO NOT WANT (it won't even be compiled-in).
# For more refined controls leave the following two lines commented out,
# and see further down what these two lookup lists really mean.
#
# @bypass_virus_checks_acl = qw( . );  # uncomment to DISABLE anti-virus code
# @bypass_spam_checks_acl  = qw( . );  # uncomment to DISABLE anti-spam code
#
# Any setting can be changed with a new assignment, so make sure
# you do not unintentionally override these settings further down!
#@bypass_spam_checks_acl  = qw( . );    # No default dependency on spamassassin

# Lookup list of local domains (see README.lookups for syntax details)
#
# NOTE:
#   For backwards compatibility the variable names @local_domains (old) and
#   @local_domains_acl (new) are synonyms. For consistency with other lookups
#   the name @local_domains_acl is now preferred. It also makes it more
#   obviously distinct from the new %local_domains hash lookup table.
```

```
#
# local_domains* lookup tables are used in deciding whether a recipient
# is local or not, or in other words, if the message is outgoing or not.
# This affects inserting spam-related headers for local recipients,
# limiting recipient virus notifications (if enabled) to local recipients,
# in deciding if address extension may be appended, and in SQL lookups
# for non-fqdn addresses. Set it up correctly if you need features
# that rely on this setting (or just leave empty otherwise).
#
# With Postfix (2.0) a quick reminder on what local domains normally are:
# a union of domains specified in: $mydestination, $virtual_alias_domains,
# $virtual_mailbox_domains, and $relay_domains.
#
@local_domains_acl = ( ".$mydomain" );  # $mydomain and its subdomains
# @local_domains_acl = ( ".$mydomain", "my.other.domain" );
# @local_domains_acl = qw();  # default is empty, no recipient treated as local
# @local_domains_acl = qw( .example.com );
#@local_domains_acl = qw( .example.com !host.sub.example.net .sub.example.net);

# or alternatively(A), using a Perl hash lookup table, which may be assigned
# directly, or read from a file, one domain per line; comments and empty lines
# are ignored, a dot before a domain name implies its subdomains:
#
#read_hash(\%local_domains, '/etc/amavis/local_domains');

#or alternatively(B), using a list of regular expressions:
# $local_domains_re = new_RE( qr'[@.]example\.com$'i );
#
# see README.lookups for syntax and semantics


#
# Section II - MTA specific (defaults should be ok)
#

# if $relayhost_is_client is true, the IP address in $notify_method and
# $forward_method is dynamically overridden with SMTP client peer address
# (if available), which makes it possible for several hosts to share one
# daemon.  The static port number is also overridden, and is dynamically
# calculated  as being one above the incoming SMTP/LMTP session port number.
#
# These are logged at level 3, so enable logging until you know you got it
# right.
$relayhost_is_client = 0;         # (defaults to false)

$insert_received_line = 1;        # behave like MTA: insert 'Received:' header
             # (does not apply to sendmail/milter)
             # (default is true (1) )

# AMAVIS-CLIENT PROTOCOL INPUT SETTINGS (e.g. with sendmail milter)
#   (used with amavis helper clients like amavis-milter.c and amavis.c,
#   NOT needed for Postfix and Exim  or dual-sendmail - keep it undefined.)
#$unix_socketname = "/var/lib/amavis/amavisd.sock"; # amavis helper protocol
                                                    # socket
$unix_socketname = undef;         # disable listening on a unix socket
                                  # (default is undef, i.e. disabled)
```

```
# Do we receive quoted or raw addresses from the helper program?
# (does not apply to SMTP;  defaults to true)
#$gets_addr_in_quoted_form = 1;   # "Bob \"Funny\" Dude"@example.com
#$gets_addr_in_quoted_form = 0;   # Bob "Funny" Dude@example.com



# SMTP SERVER (INPUT) PROTOCOL SETTINGS (e.g. with Postfix, Exim v4, ...)
#   (used when MTA is configured to pass mail to amavisd via SMTP or LMTP)
$inet_socket_port = 10024;        # accept SMTP on this local TCP port
                                  # (default is undef, i.e. disabled)
# multiple ports may be provided: $inet_socket_port = [10024, 10026, 10028];

# SMTP SERVER (INPUT) access control
# - do not allow free access to the amavisd SMTP port !!!
#
# when MTA is at the same host, use the following (one or the other or both):
$inet_socket_bind = '127.0.0.1';  # limit socket bind to loopback interface
                                  # (default is '127.0.0.1')
@inet_acl = qw( 127.0.0.1 );      # allow SMTP access only from localhost IP
                                  # (default is qw( 127.0.0.1 ) )

# when MTA (one or more) is on a different host, use the following:
# @inet_acl = qw(127/8 10.1.0.1 10.1.0.2);  # adjust the list as appropriate
# $inet_socket_bind = undef;      # bind to all IP interfaces if undef
#
# Example1:
# @inet_acl = qw( 127/8 10/8 172.16/12 192.168/16 );
# permit only SMTP access from loopback and rfc1918 private address space
#
# Example2:
# @inet_acl = qw( !192.168.1.12 172.16.3.3 !172.16.3/255.255.255.0
#    127.0.0.1 10/8 172.16/12 192.168/16 );
# matches loopback and rfc1918 private address space except host 192.168.1.12
# and net 172.16.3/24 (but host 172.16.3.3 within 172.16.3/24 still matches)
#
# Example3:
# @inet_acl = qw( 127/8
#    !172.16.3.0   !172.16.3.127 172.16.3.0/25
#    !172.16.3.128 !172.16.3.255 172.16.3.128/25 );
# matches loopback and both halves of the 172.16.3/24 C-class,
# split into two subnets, except all four broadcast addresses
# for these subnets
#
# See README.lookups for details on specifying access control lists.


#
# Section III - Logging
#

# true (e.g. 1) => syslog;  false (e.g. 0) => logging to file
$DO_SYSLOG = 1;                 # (defaults to false)
#$SYSLOG_LEVEL = 'user.info';   # (defaults to 'mail.info')

# Log file (if not using syslog)
$LOGFILE = "/var/log/amavis.log";  # (defaults to empty, no log)
```

```
#NOTE: levels are not strictly observed and are somewhat arbitrary
# 0: startup/exit/failure messages, viruses detected
# 1: args passed from client, some more interesting messages
# 2: virus scanner output, timing
# 3: server, client
# 4: decompose parts
# 5: more debug details
#$log_level = 2;  # (defaults to 0)

# Customizable template for the most interesting log file entry (e.g. with
# $log_level=0) (take care to properly quote Perl special characters like '\')
# For a list of available macros see README.customize .

# only log infected messages (useful with log level 0):
# $log_templ = '[? %#V |[? %#F ||banned filename ([%F|,])]|infected ([%V|,])]#
# [? %#V |[? %#F ||, from=[?%o|(?)|<%o>], to=[<%R>|,][? %i ||, quarantine %i]]#
# |, from=[?%o|(?)|<%o>], to=[<%R>|,][? %i ||, quarantine %i]]';

# log both infected and noninfected messages (default):
$log_templ = '[? %#V |[? %#F |[?%#D|Not-Delivered|Passed]|BANNED name/type \
                                                    (%F)] |INFECTED (%V)], #
[?%o|(?)|<%o>] -> [<%R>|,][? %i ||, quarantine %i], Message-ID: %m, Hits: %c';


#
# Section IV - Notifications/DSN, BOUNCE/REJECT/DROP/PASS destiny, quarantine
#

# Select notifications text encoding when Unicode-aware Perl is converting
# text from internal character representation to external encoding (charset
# in MIME terminology). Used as argument to Perl Encode::encode subroutine.
#
#   to be used in RFC 2047-encoded header field bodies, e.g. in Subject:
#$hdr_encoding = 'iso-8859-1';  # (default: 'iso-8859-1')
#
#   to be used in notification body text: its encoding and Content-type.charset
#$bdy_encoding = 'iso-8859-1';  # (default: 'iso-8859-1')

# Default template texts for notifications may be overruled by directly
# assigning new text to template variables, or by reading template text
# from files. A second argument may be specified in a call to read_text(),
# specifying character encoding layer to be used when reading from the
# external file, e.g. 'utf8', 'iso-8859-1', or often just $bdy_encoding.
# Text will be converted to internal character representation by Perl 5.8.0
# or later; second argument is ignored otherwise. See PerlIO::encoding,
# Encode::PerlIO and perluniintro man pages.
#
# $notify_sender_templ      = read_text('/var/amavis/notify_sender.txt');
# $notify_virus_sender_templ= read_text('/var/amavis/notify_virus_sender.txt');
# $notify_virus_admin_templ = read_text('/var/amavis/notify_virus_admin.txt');
# $notify_virus_recips_templ= read_text('/var/amavis/notify_virus_recips.txt');
# $notify_spam_sender_templ = read_text('/var/amavis/notify_spam_sender.txt');
# $notify_spam_admin_templ  = read_text('/var/amavis/notify_spam_admin.txt');

# If notification template files are collectively available in some directory,
# use read_l10n_templates which calls read_text for each known template.
```

```
#
#   read_l10n_templates('/etc/amavis/en_US');
#
# Debian available locales: en_US, pt_BR
read_l10n_templates('en_US', '/etc/amavis');


# Here is an overall picture (sequence of events) of how pieces fit together
# (only virus controls are shown, spam controls work the same way):
#
#   bypass_virus_checks? ==> PASS
#   no viruses?   ==> PASS
#   log virus     if $log_templ is nonempty
#   quarantine    if $virus_quarantine_to is nonempty
#   notify admin  if $virus_admin (lookup) nonempty
#   notify recips if $warnvirusrecip and (recipient is local or $warn_offsite)
#   add address extensions if adding extensions is enabled and virus will pass
#   send (non-)delivery notifications
#      to sender if DSN needed (BOUNCE or ($warn_virus_sender and D_PASS))
#   virus_lovers or final_destiny==D_PASS  ==> PASS
#   DISCARD (2xx) or REJECT (5xx) (depending on final_*_destiny)
#
# Equivalent flow diagram applies for spam checks.
# If a virus is detected, spam checking is skipped entirely.

# The following symbolic constants can be used in *destiny settings:
#
# D_PASS     mail will pass to recipients, regardless of bad contents;
#
# D_DISCARD  mail will not be delivered to its recipients, sender will NOT be
#            notified. Effectively we lose mail (but will be quarantined
#            unless disabled). Losing mail is not decent for a mailer,
#            but might be desired.
#
# D_BOUNCE   mail will not be delivered to its recipients, a non-delivery
#            notification (bounce) will be sent to the sender by amavisd-new;
#            Exception: bounce (DSN) will not be sent if a virus name matches
#            $viruses_that_fake_sender_re, or to messages from mailing lists
#            (Precedence: bulk|list|junk);
#
# D_REJECT   mail will not be delivered to its recipients, sender should
#            preferably get a reject, e.g. SMTP permanent reject response
#            (e.g. with milter), or non-delivery notification from MTA
#            (e.g. Postfix). If this is not possible (e.g. different recipients
#            have different tolerances to bad mail contents and not using LMTP)
#            amavisd-new sends a bounce by itself (same as D_BOUNCE).
#
# Notes:
#   D_REJECT and D_BOUNCE are similar, the difference is in who is responsible
#            for informing the sender about non-delivery, and how informative
#            the notification can be (amavisd-new knows more than MTA);
#   With D_REJECT, MTA may reject original SMTP, or send DSN (delivery status
#            notification, colloquially called 'bounce') - depending on MTA;
#            Best suited for sendmail milter, especially for spam.
#   With D_BOUNCE, amavisd-new (not MTA) sends DSN (can better explain the
#            reason for mail non-delivery, but unable to reject the original
#            SMTP session). Best suited to reporting viruses, and for Postfix
```

```
#            and other dual-MTA setups, which can't reject original client SMTP
#            session, as the mail has already been enqueued.

$final_virus_destiny      = D_DISCARD; # (defaults to D_BOUNCE)
$final_banned_destiny     = D_BOUNCE;  # (defaults to D_BOUNCE)
$final_spam_destiny       = D_PASS;  # (defaults to D_REJECT)
$final_bad_header_destiny = D_PASS;  # (defaults to D_PASS), D_BOUNCE suggested

# Alternatives to consider for spam:
# - use D_PASS if clients will do filtering based on inserted mail headers;
# - use D_DISCARD, if kill_level is set safely high;
# - use D_BOUNCE instead of D_REJECT if not using milter;
#
# D_BOUNCE is preferred for viruses, but consider:
# - use D_DISCARD to avoid bothering the rest of the network, it is hopeless
#   to try to keep up with the viruses that faker the envelope sender anyway,
#   and bouncing only increases the network cost of viruses for everyone
# - use D_PASS (or virus_lovers) and $warnvirussender=1 to deliver viruses;
# - use D_REJECT instead of D_BOUNCE if using milter and under heavy
#   virus storm;
#
# Don't bother to set both D_DISCARD and $warn*sender=1, it will get mapped
# to D_BOUNCE.
#
# The separation of *_destiny values into D_BOUNCE, D_REJECT, D_DISCARD
# and D_PASS made settings $warnvirussender and $warnspamsender only still
# useful with D_PASS.

# The following $warn*sender settings are ONLY used when mail is
# actually passed to recipients ($final_*_destiny=D_PASS, or *_lovers*).
# Bounces or rejects produce non-delivery status notification anyway.

# Notify virus sender?
#$warnvirussender = 1; # (defaults to false (undef))

# Notify spam sender?
#$warnspamsender = 1; # (defaults to false (undef))

# Notify sender of banned files?
#$warnbannedsender = 1; # (defaults to false (undef))

# Notify sender of syntactically invalid header containing non-ASCII characters?
#$warnbadhsender = 1; # (defaults to false (undef))

# Notify virus (or banned files) RECIPIENT?
#  (not very useful, but some policies demand it)
#$warnvirusrecip = 1; # (defaults to false (undef))
#$warnbannedrecip = 1; # (defaults to false (undef))

# Notify also non-local virus/banned recipients if $warn*recip is true?
#  (including those not matching local_domains*)
#$warn_offsite = 1;    # (defaults to false (undef), i.e. only notify locals)


# Treat envelope sender address as unreliable and don't send sender
# notification / bounces if name(s) of detected virus(es) match the list.
# Note that virus names are supplied by external virus scanner(s) and are
```

```
# not standardized, so virus names may need to be adjusted.
# See README.lookups for syntax.
#
$viruses_that_fake_sender_re = new_RE(
  qr'nimda|hybris|klez|bugbear|yaha|braid|sobig|fizzer|palyh|peido|holar'i,
  qr'tanatos|lentin|bridex|mimail|trojan\.dropper|dumaru|parite|spaces'i,
  qr'dloader|galil|gibe|swen|netwatch|bics|sbrowse'i,
  [qr'^(EICAR\.COM|Joke\.|Junk\.)'i           => 0],
  [qr'^(WM97|OF97|W95/CIH-|JS/Fort)'i         => 0],
  # [qr/.*/ => 1],   # true by default?
);

# where to send ADMIN VIRUS NOTIFICATIONS (should be a fully qualified address)
# - the administrator address may be a simple fixed e-mail address (a scalar),
#   or may depend on the SENDER address (e.g. its domain), in which case
#   a ref to a hash table can be specified (specify lower-cased keys,
#   dot is a catchall, see README.lookups).
#
#   Empty or undef lookup disables virus admin notifications.

# $virus_admin = undef;   # do not send virus admin notifications (default)
# $virus_admin = {'not.example.com' => '', '.' => 'virusalert@example.com'};
# $virus_admin = 'virus-admin@example.com';
$virus_admin = "postmaster\@$mydomain";  # due to D_DISCARD default

# equivalent to $virus_admin, but for spam admin notifications:
# $spam_admin = "spamalert\@$mydomain";
# $spam_admin = undef;    # do not send spam admin notifications (default)
# $spam_admin = {'not.example.com' => '', '.' => 'spamalert@example.com'};

#advanced example, using a hash lookup table:
#$virus_admin = {
# 'baduser@sub1.example.com' => 'HisBoss@sub1.example.com',
# '.sub1.example.com'  => 'virusalert@sub1.example.com',
# '.sub2.example.com'  => '',                  # don't send admin notifications
# 'a.sub3.example.com' => 'abuse@sub3.example.com',
# '.sub3.example.com'  => 'virusalert@sub3.example.com',
# '.example.com'       => 'noc@example.com',   # catchall for our virus senders
# '.'                  => 'virusalert@hq.example.com',  # catchall for the rest
#};


# whom notification reports are sent from (ENVELOPE SENDER);
# may be a null reverse path, or a fully qualified address:
#   (admin and recip sender addresses default to $mailfrom
#   for compatibility, which in turn defaults to undef (empty) )
#   If using strings in double quotes, don't forget to quote @, i.e. \@
#
#$mailfrom_notify_admin     = "virusalert\@$mydomain";
#$mailfrom_notify_recip     = "virusalert\@$mydomain";
#$mailfrom_notify_spamadmin = "spam.police\@$mydomain";

# 'From' HEADER FIELD for sender and admin notifications.
# This should be a replyable address, see rfc1894. Not to be confused
# with $mailfrom_notify_sender, which is the envelope return address
# and should be empty (null reverse path) according to rfc2821.
#
```

```
# The syntax of the 'From' header field is specified in rfc2822, section
# '3.4. Address Specification'. Note in particular that display-name must be
# a quoted-string if it contains any special characters like spaces and dots.
#
# $hdrfrom_notify_sender = "amavisd-new <postmaster\@$mydomain>";
# $hdrfrom_notify_sender = 'amavisd-new <postmaster@example.com>';
# $hdrfrom_notify_sender = '"Content-Filter Master" <postmaster@example.com>';
#   (defaults to: "amavisd-new <postmaster\@$myhostname>")
# $hdrfrom_notify_admin = $mailfrom_notify_admin;
#   (defaults to: $mailfrom_notify_admin)
# $hdrfrom_notify_spamadmin = $mailfrom_notify_spamadmin;
#   (defaults to: $mailfrom_notify_spamadmin)

# whom quarantined messages appear to be sent from (envelope sender)
$mailfrom_to_quarantine = undef; # original sender if undef, or set explicitly
                                 # (default is undef)


# Location to put infected mail into: (applies to 'local:' quarantine method)
#   empty for not quarantining, may be a file (mailbox),
#   or a directory (no trailing slash)
#   (the default value is undef, meaning no quarantine)
#
$QUARANTINEDIR = '/var/lib/amavis/virusmails';

#$virus_quarantine_method = "local:virus-%i-%n";    # default
#$spam_quarantine_method  = "local:spam-%b-%i-%n";  # default
#
#use the new 'bsmtp:' method as an alternative to the default 'local:'
#$virus_quarantine_method = "bsmtp:$QUARANTINEDIR/virus-%i-%n.bsmtp";
#$spam_quarantine_method  = "bsmtp:$QUARANTINEDIR/spam-%b-%i-%n.bsmtp";

# When using the 'local:' quarantine method (default), the following applies:
#
# A finer control of quarantining is available through variable
# $virus_quarantine_to/$spam_quarantine_to. It may be a simple scalar string,
# or a ref to a hash lookup table, or a regexp lookup table object,
# which makes possible to set up per-recipient quarantine addresses.
#
# The value of scalar $virus_quarantine_to/$spam_quarantine_to (or a
# per-recipient lookup result from the hash table %$virus_quarantine_to)
# is/are interpreted as follows:
#
# VARIANT 1:
#   empty or undef disables quarantine;
#
# VARIANT 2:
#   a string NOT containing an '@';
# amavisd will behave as a local delivery agent (LDA) and will quarantine
# viruses to local files according to hash %local_delivery_aliases (pseudo
# aliases map) - see subroutine mail_to_local_mailbox() for details.
# Some of the predefined aliases are 'virus-quarantine' and 'spam-quarantine'.
# Setting $virus_quarantine_to ($spam_quarantine_to) to this string will:
#
# * if $QUARANTINEDIR is a directory, each quarantined virus will go
#   to a separate file in the $QUARANTINEDIR directory (traditional
#   amavis style, similar to maildir mailbox format);
```

```
#
# * otherwise $QUARANTINEDIR is treated as a file name of a Unix-style
#   mailbox. All quarantined messages will be appended to this file.
#   Amavisd child process must obtain an exclusive lock on the file during
#   delivery, so this may be less efficient than using individual files
#   or forwarding to MTA, and it may not work across NFS or other non-local
#   file systems (but may be handy for pickup of quarantined files via IMAP
#   for example);
#
# VARIANT 3:
#   any email address (must contain '@').
# The e-mail messages to be quarantined will be handed to MTA
# for delivery to the specified address. If a recipient address local to MTA
# is desired, you may leave the domain part empty, e.g. 'infected@', but the
# '@' character must nevertheless be included to distinguish it from variant 2.
#
# This method enables more refined delivery control made available by MTA
# (e.g. its aliases file, other local delivery agents, dealing with
# privileges and file locking when delivering to user's mailbox, nonlocal
# delivery and forwarding, fan-out lists). Make sure the mail-to-be-quarantined
# will not be handed back to amavisd for checking, as this will cause a loop
# (hopefully broken at some stage)! If this can be assured, notifications
# will benefit too from not being unnecessarily virus-scanned.
#
# By default this is safe to do with Postfix and Exim v4 and dual-sendmail
# setup, but probably not safe with sendmail milter interface without
# precaution.

# (the default value is undef, meaning no quarantine)

$virus_quarantine_to  = 'virus-quarantine';    # traditional local quarantine
#$virus_quarantine_to = 'infected@';           # forward to MTA for delivery
#$virus_quarantine_to = "virus-quarantine\@$mydomain";   # similar
#$virus_quarantine_to = 'virus-quarantine@example.com';  # similar
#$virus_quarantine_to = undef;                 # no quarantine
#
#$virus_quarantine_to = new_RE(                # per-recip multiple quarantines
#  [qr'^user@example\.com$'i => 'infected@'],
#  [qr'^(.*)@example\.com$'i => 'virus-${1}@example.com'],
#  [qr'^(.*)(@[^@])?$'i      => 'virus-${1}${2}'],
#  [qr/.*/                   => 'virus-quarantine'] );

# similar for spam
# (the default value is undef, meaning no quarantine)
#
$spam_quarantine_to = 'spam-quarantine';
#$spam_quarantine_to = "spam-quarantine\@$mydomain";
#$spam_quarantine_to = new_RE(                 # per-recip multiple quarantines
#  [qr'^(.*)@example\.com$'i => 'spam-${1}@example.com'],
#  [qr/.*/                   => 'spam-quarantine'] );

# In addition to per-recip quarantine, a by-sender lookup is possible. It is
# similar to $spam_quarantine_to, but the lookup key is the sender address:
#$spam_quarantine_bysender_to = undef;   # dflt: no by-sender spam quarantine


# Add X-Virus-Scanned header field to mail?
```

```
$X_HEADER_TAG = 'X-Virus-Scanned'; # (default: undef)
# Leave empty to add no header  # (default: undef)
$X_HEADER_LINE = "by $myversion (Debian) at $mydomain";

$remove_existing_x_scanned_headers = 0; # leave existing X-Virus-Scanned alone
#$remove_existing_x_scanned_headers= 1; # remove existing headers
     # (defaults to false)
#$remove_existing_spam_headers = 0;     # leave existing X-Spam* headers alone
$remove_existing_spam_headers  = 1;     # remove existing spam headers if
     # spam scanning is enabled (default)

# set $bypass_decode_parts to true if you only do spam scanning, or if you
# have a good virus scanner that can deal with compression and recursively
# unpacking archives by itself, and save amavisd the trouble.
# Disabling decoding also causes banned_files checking to only see
# MIME names and MIME content types, not the content classification types
# as provided by the file(1) utility.
# It is a double-edged sword, make sure you know what you are doing!
#
#$bypass_decode_parts = 1;  # (defaults to false)

# don't trust this file type or corresponding unpacker for this file type,
# keep both the original and the unpacked file for a virus checker to see
# (lookup key is what file(1) utility returned):
#
$keep_decoded_original_re = new_RE(
  qr'^MAIL$',    # retain full original message for virus checking
  qr'^(ASCII(?! cpio)|text|uuencoded|xxencoded|binhex)'i,
);


# Checking for banned MIME types and names. If any mail part matches,
# the whole mail is rejected, much like the way viruses are handled.
# A list in object $banned_filename_re can be defined to provide a list
# of Perl regular expressions to be matched against each part's:
#
#  * Content-Type value (both declared and effective mime-type),
#    including the possible security risk content types
#    message/partial and message/external-body, as specified by rfc2046;
#
#  * declared (i.e. recommended) file names as specified by MIME subfields
#    Content-Disposition.filename and Content-Type.name, both in their
#    raw (encoded) form and in rfc2047-decoded form if applicable;
#
#  * file content type as guessed by 'file' utility, both the raw
#    result from 'file', as well as short type name, classified
#    into names such as .asc, .txt, .html, .doc, .jpg, .pdf,
#    .zip, .exe, ... - see subroutine determine_file_types().
#    This step is done only if $bypass_decode_parts is not true.
#
#  * leave $banned_filename_re undefined to disable these checks
#    (giving an empty list to new_RE() will also always return false)

$banned_filename_re = new_RE(
   qr'\.[a-zA-Z][a-zA-Z0-9]{0,3}\.(vbs|pif|scr|bat|com|exe|dll)$'i, # double
                                                                  # extension
   qr'.\.(exe|vbs|pif|scr|bat|com)$'i,               # banned extension - basic
```

```
#  qr'.\.(ade|adp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|
#         jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shs|shb|vb|
#         vbe|vbs|wsc|wsf|wsh)$'ix,                  # banned extension - long
#  qr'^\.(exe|zip|lha|tnef)$'i,                      # banned file(1) types
#  qr'^application/x-msdownload$'i,                  # banned MIME types
   qr'^message/partial$'i, qr'^message/external-body$'i, # rfc2046
);
# See http://support.microsoft.com/default.aspx?scid=kb;EN-US;q262631
# and http://www.cknow.com/vtutor/vtextensions.htm

# A little trick: a pattern qr'\.exe$' matches both a short type name '.exe',
# as well as any file name which happens to end with .exe. If only matching
# a file name is desired, but not the short name, a pattern qr'.\.exe$'i
# or similar may be used, which requires that at least one character precedes
# the '.exe', and so it will never match short file types, which always start
# with a dot.


#
# Section V - Per-recipient and per-sender handling, whitelisting, etc.
#

# %virus_lovers, @virus_lovers_acl and $virus_lovers_re lookup tables:
#   (these should be considered policy options, they do not disable checks,
#   see bypass*checks for that!)
#
# Exclude certain RECIPIENTS from virus filtering by adding their lower-cased
# envelope e-mail address (or domain only) to the hash %virus_lovers, or to
# the access list @virus_lovers_acl - see README.lookups and examples.
# Make sure the appropriate form (e.g. external/internal) of address
# is used in case of virtual domains, or when mapping external to internal
# addresses, etc. - this is MTA-specific.
#
# Notifications would still be generated however (see the overall
# picture above), and infected mail (if passed) gets additional header:
#   X-AMaViS-Alert: INFECTED, message contains virus: ...
# (header not inserted with milter interface!)
#
# NOTE (milter interface only): in case of multiple recipients,
# it is only possible to drop or accept the message in its entirety - for all
# recipients. If all of them are virus lovers, we'll accept mail, but if
# at least one recipient is not a virus lover, we'll discard the message.


# %bypass_virus_checks, @bypass_virus_checks_acl and $bypass_virus_checks_re
# lookup tables:
#   (this is mainly a time-saving option, unlike virus_lovers* !)
#
# Similar in concept to %virus_lovers, a hash %bypass_virus_checks,
# access list @bypass_virus_checks_acl and regexp list $bypass_virus_checks_re
# are used to skip entirely the decoding, unpacking and virus checking,
# but only if ALL recipients match the lookup.
#
# %bypass_virus_checks/@bypass_virus_checks_acl/$bypass_virus_checks_re
# do NOT GUARANTEE the message will NOT be checked for viruses - this may
# still happen when there is more than one recipient for a message, and
# not all of them match these lookup tables. To guarantee virus delivery,
```

```
# a recipient must also match %virus_lovers/@virus_lovers_acl lookups
# (but see milter limitations above),

# NOTE: it would not be clever to base virus checks on SENDER address,
# since there are no guarantees that it is genuine. Many viruses
# and spam messages fake sender address. To achieve selective filtering
# based on the source of the mail (e.g. IP address, MTA port number, ...),
# use mechanisms provided by MTA if available.


# Similar to lookup tables controlling virus checking, there exist
# spam scanning, banned names/types, and headers_checks control counterparts:
#   %spam_lovers, @spam_lovers_acl, $spam_lovers_re
#   %banned_files_lovers, @banned_files_lovers_acl, $banned_files_lovers_re
#   %bad_header_lovers, @bad_header_lovers_acl, $bad_header_lovers_re
# and:
#   %bypass_spam_checks/@bypass_spam_checks_acl/$bypass_spam_checks_re
#   %bypass_banned_checks/@bypass_banned_checks_acl/$bypass_banned_checks_re
#   %bypass_header_checks/@bypass_header_checks_acl/$bypass_header_checks_re
# See README.lookups for details about the syntax.

# The following example disables spam checking altogether,
# since it matches any recipient e-mail address (any address
# is a subdomain of the top-level root DNS domain):
#   @bypass_spam_checks_acl = qw( . );

#   @bypass_header_checks_acl = qw( user@example.com );
#   @bad_header_lovers_acl    = qw( user@example.com );


# See README.lookups for further detail, and examples below.

# $virus_lovers{lc("postmaster\@$mydomain")} = 1;
# $virus_lovers{lc('postmaster@example.com')} = 1;
# $virus_lovers{lc('abuse@example.com')} = 1;
# $virus_lovers{lc('some.user@')} = 1;  # this recipient, regardless of domain
# $virus_lovers{lc('boss@example.com')} = 0; # never, even if domain matches
# $virus_lovers{lc('example.com')} = 1; # this domain, but not its subdomains
# $virus_lovers{lc('.example.com')}= 1; # this domain, including its subdomains
#or:
# @virus_lovers_acl = qw( me@lab.xxx.com !lab.xxx.com .xxx.com yyy.org );
#
# $bypass_virus_checks{lc('some.user2@butnot.example.com')} = 1;
# @bypass_virus_checks_acl = qw( some.ddd !butnot.example.com .example.com );

# @virus_lovers_acl = qw( postmaster@example.com );
# $virus_lovers_re = new_RE( qr'^(helpdesk|postmaster)@example\.com$'i );

# $spam_lovers{lc("postmaster\@$mydomain")} = 1;
# $spam_lovers{lc('postmaster@example.com')} = 1;
# $spam_lovers{lc('abuse@example.com')} = 1;
# @spam_lovers_acl = qw( !.example.com );
# $spam_lovers_re = new_RE( qr'^user@example\.com$'i );


# don't run spam check for these RECIPIENT domains:
#   @bypass_spam_checks_acl = qw( d1.com .d2.com a.d3.com );
```

```
# or the other way around (bypass check for all BUT these):
#   @bypass_spam_checks_acl = qw( !d1.com !.d2.com !a.d3.com . );
# a practical application: don't check outgoing mail for spam:
#   @bypass_spam_checks_acl = ( "!.$mydomain", "." );
# (a downside of which is that such mail will not count as ham in SA bayes db)


# Where to find SQL server(s) and database to support SQL lookups?
# A list of triples: (dsn,user,passw).   (dsn = data source name)
# More than one entry may be specified for multiple (backup) SQL servers.
# See 'man DBI', 'man DBD::mysql', 'man DBD::Pg', ... for details.
# When chroot-ed, accessing SQL server over inet socket may be more convenient.
#
# @lookup_sql_dsn =
#   ( ['DBI:mysql:database=mail;host=127.0.0.1;port=3306', 'user1', 'passwd1'],
#     ['DBI:mysql:database=mail;host=host2', 'username2', 'password2'] );
#
# ('mail' in the example is the database name, choose what you like)
# With PostgreSQL the dsn (first element of the triple) may look like:
#      'DBI:Pg:host=host1;dbname=mail'

# The SQL select clause to fetch per-recipient policy settings.
# The %k will be replaced by a comma-separated list of query addresses
# (e.g. full address, domain only, catchall).  Use ORDER, if there
# is a chance that multiple records will match - the first match wins.
# If field names are not unique (e.g. 'id'), the later field overwrites the
# earlier in a hash returned by lookup, which is why we use '*,users.id'.
# $sql_select_policy = 'SELECT *,users.id FROM users,policy'.
#   ' WHERE (users.policy_id=policy.id) AND (users.email IN (%k))'.
#   ' ORDER BY users.priority DESC';
#
# The SQL select clause to check sender in per-recipient whitelist/blacklist
# The first SELECT argument '?' will be users.id from recipient SQL lookup,
# the %k will be sender addresses (e.g. full address, domain only, catchall).
# $sql_select_white_black_list = 'SELECT wb FROM wblist,mailaddr'.
#     ' WHERE (wblist.rid=?) AND (wblist.sid=mailaddr.id)'.
#     '   AND (mailaddr.email IN (%k))'.
#   ' ORDER BY mailaddr.priority DESC';

$sql_select_white_black_list = undef;  # undef disables SQL white/blacklisting


# If you decide to pass viruses (or spam) to certain recipients using the
# above lookup tables or using $final_virus_destiny=D_PASS, you can set
# the variable $addr_extension_virus ($addr_extension_spam) to some
# string, and the recipient address will have this string appended
# as an address extension to the local-part of the address. This extension
# can be used by final local delivery agent to place such mail in different
# folders. Leave these two variables undefined or empty strings to prevent
# appending address extensions. Setting has no effect on recipient which will
# not be receiving viruses/spam. Recipients who do not match lookup tables
# local_domains* are not affected.
#
# LDAs usually default to stripping away address extension if no special
# handling is specified, so having this option enabled normally does no harm,
# provided the $recipients_delimiter matches the setting on the final
# MTA's LDA.
```

```
# $addr_extension_virus  = 'virus'; # (default is undef, same as empty)
# $addr_extension_spam   = 'spam'; # (default is undef, same as empty)
# $addr_extension_banned = 'banned'; # (default is undef, same as empty)


# Delimiter between local part of the recipient address and address extension
# (which can optionally be added, see variables $addr_extension_virus and
# $addr_extension_spam). E.g. recipient address <user@example.com> gets changed
# to <user+virus@example.com>.
#
# Delimiter should match equivalent (final) MTA delimiter setting.
# (e.g. for Postfix add 'recipient_delimiter = +' to main.cf)
# Setting it to an empty string or to undef disables this feature
# regardless of $addr_extension_virus and $addr_extension_spam settings.

$recipient_delimiter = '+';  # (default is '+')

# true: replace extension;  false: append extension
$replace_existing_extension = 1; # (default is false)

# Affects matching of localpart of e-mail addresses (left of '@')
# in lookups: true = case sensitive, false = case insensitive
$localpart_is_case_sensitive = 0; # (default is false)


# ENVELOPE SENDER WHITELISTING / BLACKLISTING  - GLOBAL (RECIPIENT-INDEPENDENT)
# (affects spam checking only, has no effect on virus and other checks)

# WHITELISTING: use ENVELOPE SENDER lookups to ENSURE DELIVERY from whitelisted
# senders even if the message is recognized as spam. Effectively, for the
# specified senders, message RECIPIENTS temporarily become 'spam_lovers', with
# further processing being the same as otherwise specified for spam lovers.
# It does not turn off inserting spam-related headers, if they are enabled.
#
# BLACKLISTING: messages from specified SENDERS are DECLARED SPAM.
# Effectively, for messages from blacklisted senders, spam level
# is artificially pushed high, and the normal spam processing applies,
# resulting in 'X-Spam-Flag: YES', high 'X-Spam-Level' bar and other usual
# reactions to spam, including possible rejection. If the message nevertheless
# still passes (e.g. for spam loving recipients), it is tagged as BLACKLISTED
# in the 'X-Spam-Status' header field, but the reported spam value and
# set of tests in this report header field (if available from SpamAssassin,
# which may have not been called) is not adjusted.
#
# A sender may be both white- and blacklisted at the same time,
# settings are independent. For example, being both white- and blacklisted,
# message is delivered to recipients, but is tagged as spam.
#
# If ALL recipients of the message either white- or blacklist the sender,
# spam scanning (calling the SpamAssassin) is bypassed, saving on time.
#
# The following variables (lookup tables) are available, with the semantics
# and syntax as specified in README.lookups:
#
# %whitelist_sender, @whitelist_sender_acl, $whitelist_sender_re
# %blacklist_sender, @blacklist_sender_acl, $blacklist_sender_re
```

```
# SOME EXAMPLES:
#
#ACL:
# @whitelist_sender_acl = qw( .example.com );
#
# @whitelist_sender_acl = ( ".$mydomain" );  # $mydomain and its subdomains
# NOTE: This is not a reliable way of turning off spam checks for
#       locally-originating mail, as sender address can easily be faked.
#       To reliably avoid spam-scanning outgoing mail,
#       use @bypass_spam_checks_acl .

#RE:
# $whitelist_sender_re = new_RE(
#   qr'^postmaster@.*\bexample\.com$'i,
#   qr'owner-[^@]*@'i,  qr'-request@'i,
#   qr'\.example\.com$'i );
#
$blacklist_sender_re = new_RE(
    qr'^(bulkmail|offers|cheapbenefits|earnmoney|foryou|greatcasino)@'i,
    qr'^(investments|lose_weight_today|market.alert|money2you|MyGreenCard)@'i,
    qr'^(new\.tld\.registry|opt-out|opt-in|optin|saveonl|smoking2002k)@'i,
    qr'^(specialoffer|specialoffers|stockalert|stopsnoring|wantsome)@'i,
    qr'^(workathome|yesitsfree|your_friend|greatoffers)@'i,
    qr'^(inkjetplanet|marketopt|MakeMoney)\d*@'i,
);

#HASH lookup variant:
# NOTE: Perl operator qw splits its argument string by whitespace
# and produces a list. This means that addresses can not contain
# whitespace, and there is no provision for comments within the string.
# You can use the normal Perl list syntax if you have special requirements,
# e.g. map {...} ('one user@bla', '.second.com'), or use read_hash to read
# addresses from a file.
#

# a hash lookup table can be read from a file,
# one address per line, comments and empty lines are permitted:
#
# read_hash(\%whitelist_sender, '/var/amavis/whitelist_sender');

# ... or set directly:
map { $whitelist_sender{lc($_)}=1 } (qw(
  cert-advisory-owner@cert.org
  owner-alert@iss.net
  slashdot@slashdot.org
  bugtraq@securityfocus.com
  NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM
  security-alerts@linuxsecurity.com
  amavis-user-admin@lists.sourceforge.net
  razor-users-admin@lists.sourceforge.net
  notification-return@lists.sophos.com
  mailman-announce-admin@python.org
  zope-announce-admin@zope.org
  owner-postfix-users@postfix.org
  owner-postfix-announce@postfix.org
  owner-sendmail-announce@Lists.Sendmail.ORG
```

```
  owner-technews@postel.ACM.ORG
  lvs-users-admin@LinuxVirtualServer.org
  ietf-123-owner@loki.ietf.org
  cvs-commits-list-admin@gnome.org
  rt-users-admin@lists.fsck.com
  owner-announce@mnogosearch.org
  owner-hackers@ntp.org
  owner-bugs@ntp.org
  clp-request@comp.nus.edu.sg
  surveys-errors@lists.nua.ie
  emailNews@genomeweb.com
  owner-textbreakingnews@CNNIMAIL12.CNN.COM
  spamassassin-talk-admin@lists.sourceforge.net
  yahoo-dev-null@yahoo-inc.com
));


# ENVELOPE SENDER WHITELISTING / BLACKLISTING - PER-RECIPIENT

# The same semantics as for global white/blacklisting applies, but this
# time each recipient (or its domain, or subdomain, ...) can be given
# an individual lookup table for matching senders. The per-recipient lookups
# override the global lookups, which serve as a fallback default.

# Specify a two-level lookup table: the key for the outer table is recipient,
# and the result should be an inner lookup table (hash or ACL or RE),
# where the key used will be the sender.
#
#$per_recip_blacklist_sender_lookup_tables = {
# 'user1@my.example.com'=>new_RE(qr'^(inkjetplanet|marketopt|MakeMoney)\d*@'i),
# 'user2@my.example.com'=>[qw( spammer@d1.example,org .d2.example,org )],
#};
#$per_recip_whitelist_sender_lookup_tables = {
# 'user@my.example.com' => [qw( friend@example.org .other.example.org )],
# '.my1.example.com'    => [qw( !foe.other.example,org .other.example,org )],
# '.my2.example.com'    => read_hash('/var/amavis/my2-wl.dat'),
# 'abuse@' => { 'postmaster@'=>1,
#               'cert-advisory-owner@cert.org'=>1, 'owner-alert@iss.net'=>1 },
#};



#
# Section VI - Resource limits
#

# Sanity limit to the number of allowed recipients per SMTP transaction
# $smtpd_recipient_limit = 1000;  # (default is 1000)


# Resource limits to protect unpackers, decompressors and virus scanners
# against mail bombs (e.g. 42.zip)

# Maximum recursion level for extraction/decoding (0 or undef disables limit)
$MAXLEVELS = 14;  # (default is undef, no limit)

# Maximum number of extracted files (0 or undef disables the limit)
$MAXFILES = 1500;  # (default is undef, no limit)
```

```
# For the cumulative total of all decoded mail parts we set max storage size
# to defend against mail bombs. Even though parts may be deleted (replaced
# by decoded text) during decoding, the size they occupied is _not_ returned
# to the quota pool.
#
# Parameters to storage quota formula for unpacking/decoding/decompressing
#   Formula:
#     quota = max($MIN_EXPANSION_QUOTA,
#                 $mail_size*$MIN_EXPANSION_FACTOR,
#                 min($MAX_EXPANSION_QUOTA, $mail_size*$MAX_EXPANSION_FACTOR))
#   In plain words (later condition overrules previous ones):
#     allow MAX_EXPANSION_FACTOR times initial mail size,
#     but not more than MAX_EXPANSION_QUOTA,
#     but not less than MIN_EXPANSION_FACTOR times initial mail size,
#     but never less than MIN_EXPANSION_QUOTA
#
$MIN_EXPANSION_QUOTA =      100*1024;  # bytes  (default undef, not enforced)
$MAX_EXPANSION_QUOTA = 300*1024*1024;  # bytes  (default undef, not enforced)
$MIN_EXPANSION_FACTOR =   5;  # times original mail size  (must be specified)
$MAX_EXPANSION_FACTOR = 500;  # times original mail size  (must be specified)


#
# Section VII - External programs, virus scanners
#

# Specify a path string, which is a colon-separated string of directories
# (no trailing slashes!) to be assigned to the environment variable PATH
# and to serve for locating external programs below.

# NOTE: if $daemon_chroot_dir is nonempty, the directories will be
#       relative to the chroot directory specified;

$path = '/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';

# Specify one string or a search list of strings (first match wins).
# The string (or: each string in a list) may be an absolute path,
# or just a program name, to be located via $path;
# Empty string or undef (=default) disables the use of that external program.
# Optionally command arguments may be specified - only the first substring
# up to the whitespace is used for file searching.

$file   = 'file';   # file(1) utility; use 3.41 or later to avoid vulnerability

$gzip   = 'gzip';
$bzip2  = 'bzip2';
$lzop   = 'lzop';
$uncompress = ['uncompress', 'gzip -d', 'zcat'];
$unfreeze   = ['unfreeze', 'freeze -d', 'melt', 'fcat'];
$arc        = ['nomarch', 'arc'];
$unarj      = ['arj', 'unarj'];  # both can extract, same options
$unrar      = ['rar', 'unrar'];  # both can extract, same options
$zoo    = 'zoo';
$lha    = 'lha';
$cpio   = 'cpio';   # comment out if cpio does not support GNU options
```

```
# SpamAssassin settings

# Timout for SpamAssassin. This is only used if spamassassin does NOT
# override it (which it often does if sa_local_tests_only is not true)
$sa_timeout = 300;    # default is 120 seconds

# $sa_local_tests_only = 1; # defaults to false

# AWL (auto whitelisting), requires spamassassin 2.44 or better
# $sa_auto_whitelist = 1;   # defaults to undef

$sa_mail_body_size_limit = 150*1024;  # don't waste time on SA is mail is larger
       # (less than 1% of spam is > 64k)
       # default: undef, no limitations

# default values, can be overridden by more specific lookups, e.g. SQL
$sa_tag_level_deflt  = 4.0; # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 6.3; # add 'spam detected' headers at that level
$sa_kill_level_deflt = $sa_tag2_level_deflt; # triggers spam evasive actions
                           # at or above that level: bounce/reject/drop,
                           # quarantine, and adding mail address extension
#
# The $sa_tag_level_deflt, $sa_tag2_level_deflt and $sa_kill_level_deflt
# may also be hashrefs to hash lookup tables, to make static per-recipient
# settings possible without having to resort to SQL or LDAP lookups.

# a quick reference:
#   tag_level  controls adding the X-Spam-Status and X-Spam-Level headers,
#   tag2_level controls adding 'X-Spam-Flag: YES', and editing Subject,
#   kill_level controls 'evasive actions' (reject, quarantine, extensions);
# it only makes sense to maintain the relationship:
# tag_level <= tag2_level <= kill_level

# string to prepend to Subject header field when message exceeds tag2 level
$sa_spam_subject_tag = '***SPAM*** '; # (defaults to undef, disables)
        # (only seen when spam is not to be rejected
        # and recipient is in local_domains*)

#$sa_spam_modifies_subj = 1; # may be a ref to a lookup table, default is true
# Example: modify Subject for all local recipients except user@example.com
#$sa_spam_modifies_subj = [qw( !user@example.com . )];


# @av_scanners is a list of n-tuples, where fields semantics is:
#  1. av scanner plain name, to be used in log and reports;
#  2. scanner program name; this string will be submitted to subroutine
#     find_external_programs(), which will try to find the full program
#     path name; if program is not found, this scanner is disabled.
#     Besides a simple string (full program path name or just the basename
#     to be looked for in PATH), this may be an array ref of alternative
#     program names or full paths - the first match in the list will be used;
#     As a special case for more complex scanners, this field may be
#     a subroutine reference, and the whole n-tuple is passed to it as args.
#  3. command arguments to be given to the scanner program;
#     a substring {} will be replaced by the directory name to be scanned,
#     i.e. "$tempdir/parts", a "*" will be replaced by file names of parts;
```

```
#  4. an array ref of av scanner exit status values, or a regexp (to be
#     matched against scanner output), indicating NO VIRUSES found;
#  5. an array ref of av scanner exit status values, or a regexp (to be
#     matched against scanner output), indicating VIRUSES WERE FOUND;
#     Note: the virus match prevails over a 'not found' match, so it is safe
#     even if the no. 4. matches for viruses too;
#  6. a regexp (to be matched against scanner output), returning a list
#     of virus names found.
#  7. and 8.: (optional) subroutines to be executed before and after scanner
#     (e.g. to set environment or current directory);
#     see examples for these at KasperskyLab AVP and Sophos sweep.

# NOTES:
#
# - NOT DEFINING @av_scanners (e.g. setting it to empty list, or deleting the
#   whole assignment) TURNS OFF LOADING AND COMPILING OF THE ANTIVIRUS CODE
#   (which can be handy if all you want to do is spam scanning);
#
# - the order matters: although _all_ available entries from the list are
#   always tried regardless of their verdict, scanners are run in the order
#   specified: the report from the first one detecting a virus will be used
#   (providing virus names and scanner output); REARRANGE THE ORDER TO WILL;
#
# - it doesn't hurt to keep an unused command line scanner entry in the list
#   if the program can not be found; the path search is only performed once
#   during the program startup;
#
#   COROLLARY: to disable a scanner that _does_ exist on your system,
#   comment out its entry or use undef or '' as its program name/path
#   (second parameter). An example where this is almost a must: disable
#   Sophos 'sweep' if you have its daemonized version Sophie or SAVI-Perl
#   (same for Trophie/vscan, and clamd/clamscan), or if another unrelated
#   program happens to have a name matching one of the entries ('sweep'
#   again comes to mind);
#
# - it DOES HURT to keep unwanted entries which use INTERNAL SUBROUTINES
#   for interfacing (where the second parameter starts with \&).
#   Keeping such entry and not having a corresponding virus scanner daemon
#   causes an unnecessary connection attempt (which eventually times out,
#   but it wastes precious time). For this reason the daemonized entries
#   are commented in the distribution - just remove the '#' where needed.


@av_scanners = (

# ### http://www.vanja.com/tools/sophie/
# ['Sophie',
#   \&ask_daemon, ["{}/\n", '/var/run/sophie'],
#   qr/(?x)^ 0+ ( : | [\000\r\n]* $)/,  qr/(?x)^ 1 ( : | [\000\r\n]* $)/,
#   qr/(?x)^ [-+]? \d+ : (.*?) [\000\r\n]* $/ ],

# ### http://www.csupomona.edu/~henson/www/projects/SAVI-Perl/
# ['Sophos SAVI', \&sophos_savi ],

### http://clamav.elektrapro.com/
  ['Clam Antivirus-clamd',
    \&ask_daemon, ["CONTSCAN {}\n", '/var/run/clamav/clamd.ctl'],
```

```
    qr/\bOK$/, qr/\bFOUND$/,
    qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],

# ### http://www.openantivirus.org/
# ['OpenAntiVirus ScannerDaemon (OAV)',
#   \&ask_daemon, ["SCAN {}\n", '127.0.0.1:8127'],
#   qr/^OK/, qr/^FOUND: /, qr/^FOUND: (.+)/ ],

# ### http://www.vanja.com/tools/trophie/
# ['Trophie',
#   \&ask_daemon, ["{}/\n", '/var/run/trophie'],
#   qr/(?x)^ 0+ ( : | [\000\r\n]* $)/,  qr/(?x)^ 1 ( : | [\000\r\n]* $)/,
#   qr/(?x)^ [-+]? \d+ : (.*?) [\000\r\n]* $/ ],

# ### http://www.grisoft.com/
# ['AVG Anti-Virus',
#   \&ask_daemon, ["SCAN {}\n", '127.0.0.1:55555'],
#   qr/^200/, qr/^403/, qr/^403 .*?: (.+)/ ],

# ### http://www.f-prot.com/
# ['FRISK F-Prot Daemon',
#   \&ask_daemon,
#   ["GET {}/*?-dumb%20-archive%20-packed HTTP/1.0\r\n\r\n",
#     ['127.0.0.1:10200','127.0.0.1:10201','127.0.0.1:10202',
#      '127.0.0.1:10203','127.0.0.1:10204'] ],
#   qr/(?i)<summary[^>]*>clean<\/summary>/,
#   qr/(?i)<summary[^>]*>infected<\/summary>/,
#   qr/(?i)<name>(.+)<\/name>/ ],

  ['KasperskyLab AVP - aveclient', ['/opt/kav/bin/aveclient','aveclient'],
    '-p /var/run/aveserver -s {}/*', [0,3,6,8], [2,4],
    qr/LINFECTED (.+)/,
  ],

  ['KasperskyLab AntiViral Toolkit Pro (AVP)', ['avp'],
    '-* -P -B -Y -O- {}', [0,3,6,8], [2,4],    # any use for -A -K   ?
    qr/infected: (.+)/,
    sub {chdir('/opt/AVP') or die "Can't chdir to AVP: $!"},
    sub {chdir($TEMPBASE) or die "Can't chdir back to $TEMPBASE $!"},
  ],

  ### The kavdaemon and AVPDaemonClient have been removed from Kasperky
  ### products and replaced by aveserver and aveclient
  ['KasperskyLab AVPDaemonClient',
    [ '/opt/AVP/kavdaemon',       'kavdaemon',
      '/opt/AVP/AvpDaemonClient', 'AvpDaemonClient',
      '/opt/AVP/AvpTeamDream',    'AvpTeamDream',
      '/opt/AVP/avpdc', 'avpdc' ],
    "-f=$TEMPBASE {}", [0,8], [3,4,5,6], qr/infected: ([^\r\n]+)/ ],
    # change the startup-script in /etc/init.d/kavd to:
    #   DPARMS="-* -Y -dl -f=/var/amavis /var/amavis"
    #   (or perhaps:   DPARMS="-I0 -Y -* /var/amavis" )
    # adjusting /var/amavis above to match your $TEMPBASE.
    # The '-f=/var/amavis' is needed if not running it as root, so it
    # can find, read, and write its pid file, etc., see 'man kavdaemon'.
    # defUnix.prf: there must be an entry "*/var/amavis" (or whatever
    #   directory $TEMPBASE specifies) in the 'Names=' section.
```

```
    # cd /opt/AVP/DaemonClients; configure; cd Sample; make
    # cp AvpDaemonClient /opt/AVP/
    # su - vscan -c "${PREFIX}/kavdaemon ${DPARMS}"

  ### http://www.hbedv.com/ or http://www.centralcommand.com/
  ['H+BEDV AntiVir or CentralCommand Vexira Antivirus',
    ['antivir','vexira'],
    '--allfiles -noboot -nombr -rs -s -z {}', [0], qr/ALERT:|VIRUS:/,
    qr/(?x)^\s* (?: ALERT: \s* (?: \[ | [^']* ' ) |
         (?i) VIRUS:\ .*?\ virus\ '?) ( [^\]\s']+ )/ ],
    # NOTE: remove the -z if you only have a demo version

  ### http://www.commandsoftware.com/
  ['Command AntiVirus for Linux', 'csav',
    '-all -archive -packed {}', [50], [51,52,53],
    qr/Infection: (.+)/ ],

  ### http://www.symantec.com/
  ['Symantec CarrierScan via Symantec CommandLineScanner',
    'cscmdline', '-a scan -i 1 -v -s 127.0.0.1:7777 {}',
    qr/^Files Infected:\s+0$/, qr/^Infected\b/,
    qr/^(?:Info|Virus Name):\s+(.+)/ ],

  ### http://www.symantec.com/
  ['Symantec AntiVirus Scan Engine',
    'savsecls', '-server 127.0.0.1:7777 -mode scanrepair -details -verbose {}',
    [0], qr/^Infected\b/,
    qr/^(?:Info|Virus Name):\s+(.+)/ ],
    # NOTE: check options and patterns to see which entry better applies

  ### http://drweb.imshop.de/
  ['Dr.Web Antivirus for Linux/FreeBSD/Solaris', 'drweb',
    '-al -ar -fm -go -ha -ml -ni -ot -sd -up {}',
    [0], [1], sub {('no-name')} ],

# ['Dr.Web Daemon', \&ask_daemon,
#   [pack('N',1).  # DRWEBD_SCAN_CMD - 1
#    pack('N',1).  # DRWEBD_RETURN_VIRUSES
#    pack('N',     # path length
#      length("$TEMPBASE/amavis-yyyymmddTHHMMSS-xxxxx/parts/part-xxxxx")).
#    '{}/*'.       # path
#    pack('N',0) . pack('N',0),
#    '/usr/local/drweb/run/drwebd.sock'],
#   qr/^\x00(\x00|\x01)\x00\x00/,
#   qr/^\x00(\x00|\x01)\x00(\x20|\x40|\x80)/,
#   qr/infected with ([^\x00]+)\x00\z/
# ],

  ### http://www.f-secure.com/products/anti-virus/
  ['F-Secure Antivirus', 'fsav',
    '--dumb --archive {}', [0], [3,8],
    qr/infection: (.+)/ ],

  ['CAI InoculateIT', 'inocucmd',
    '-sec -nex {}', [0], [100],
    qr/was infected by virus (.+)/ ],
```

```
  ['MkS_Vir for Linux (beta)', ['mks32','mks'],
    '-s {}/*', [0], [1,2],    # any use for options: -a -c  ?
    qr/--[ \t]*(.+)/ ],

  ### http://www.nod32.com/
  ['ESET Software NOD32', 'nod32',
    '-all -subdir+ {}', [0], [1,2],
    qr/^.+? - (.+?)\s*(?:backdoor|joke|trojan|virus|worm)/ ],

  ### http://www.nod32.com/
  ['ESET Software NOD32 - Client/Server Version', 'nod32cli',
    '-a -r -d recurse --heur standard {}', [0], [10,11],
    qr/^\S+\s+infected:\s+(.+)/ ],

  ### http://www.norman.com/products_nvc.shtml
  ['Norman Virus Control v5 / Linux', 'nvccmd',
    '-c -l:0 -s -u {}', [0], [1],
    qr/(?i).* virus in .* -> \'(.+)\'/ ],

  ### http://www.pandasoftware.com/
  ['Panda Antivirus for Linux', ['pavcl'],
    '-aut -aex -heu -cmp -nbr -nor -nso -eng {}',
    qr/Number of files infected[ \.]*: 0(?!\d)/,
    qr/Number of files infected[ \.]*: 0*[1-9]/,
    qr/Found virus :\s*(\S+)/ ],

# GeCAD AV technology is acquired by Microsoft; RAV has been discontinued.
# Check your RAV license terms before fiddling with the following two lines!
# ['GeCAD RAV AntiVirus 8', 'ravav',
#   '--all --archive --mail {}', [1], [2,3,4,5], qr/Infected: (.+)/ ],
# # NOTE: the command line switches changed with scan engine 8.5 !
# # (btw, assigning stdin to /dev/null causes RAV to fail)

  ### http://www.nai.com/
  ['NAI McAfee AntiVirus (uvscan)', 'uvscan',
    '--secure -rv --summary --noboot - {}', [0], [13],
    qr/(?x) Found (?:
        \ the\ (.+)\ (?:virus|trojan)  |
        \ (?:virus|trojan)\ or\ variant\ ([^ ]+)  |
        :\ (.+)\ NOT\ a\ virus)/,
  # sub {$ENV{LD_PRELOAD}='/lib/libc.so.6'},
  # sub {delete $ENV{LD_PRELOAD}},
  ],
  # NOTE with RH9: force the dynamic linker to look at /lib/libc.so.6 before
  # anything else by setting environment variable LD_PRELOAD=/lib/libc.so.6
  # and then clear it when finished to avoid confusing anything else

  ### http://www.virusbuster.hu/en/
  ['VirusBuster', ['vbuster', 'vbengcl'],
    # VirusBuster Ltd. does not support the daemon version for the workstation
    # engine (vbuster-eng-1.12-linux-i386-libc6.tgz) any longer. The names of
    # binaries, some parameters AND return codes (from 3 to 1) changed.
    "{} -ss -i '*' -log=$MYHOME/vbuster.log", [0], [1],
    qr/: '(.*)' - Virus/ ],

# ### http://www.virusbuster.hu/en/
# ['VirusBuster (Client + Daemon)', 'vbengd',
```

```
#   # HINT: for an infected file it returns always 3,
#   # although the man-page tells a different story
#   '-f -log scandir {}', [0], [3],
#   qr/Virus found = (.*);/ ],

  ### http://www.cyber.com/
  ['CyberSoft VFind', 'vfind',
    '--vexit {}/*', [0], [23], qr/##==>>>> VIRUS ID: CVDL (.+)/,
  # sub {$ENV{VSTK_HOME}='/usr/lib/vstk'},
  ],

  ### http://www.ikarus-software.com/
  ['Ikarus AntiVirus for Linux', 'ikarus',
    '{}', [0], [40], qr/Signature (.+) found/ ],

  ### http://www.bitdefender.com/
  ['BitDefender', 'bdc',
    '--all --arc {}', qr/^Infected files *:0(?!\d)/,
    qr/^(?:Infected files|Identified viruses|Suspect files) *:0*[1-9]/,
    qr/(?:suspected|infected): (.*)\033/ ],
);

# If no virus scanners from the @av_scanners list produce 'clean' nor
# 'infected' status (e.g. they all fail to run or the list is empty),
# then _all_ scanners from the @av_scanners_backup list are tried.
# When there are both daemonized and command-line scanners available,
# it is customary to place slower command-line scanners in the
# @av_scanners_backup list. The default choice is somewhat arbitrary,
# move entries from one list to another as desired.

@av_scanners_backup = (

  ### http://clamav.elektrapro.com/
  ['Clam Antivirus - clamscan', 'clamscan',
    '--stdout --disable-summary -r {}', [0], [1],
    qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],

  ### http://www.f-prot.com/
  ['FRISK F-Prot Antivirus', ['f-prot','f-prot.sh'],
    '-dumb -archive -packed {}', [0,8], [3,6],
    qr/Infection: (.+)/ ],

  ### http://www.trendmicro.com/
  ['Trend Micro FileScanner', ['/etc/iscan/vscan','vscan'],
    '-a {}', [0], qr/Found virus/, qr/Found virus (.+) in/ ],

  ['KasperskyLab kavscanner', ['/opt/kav/bin/kavscanner','kavscanner'],
    '-i1 -xp {}', [0,10,15], [5,20,21,25],
    qr/(?:CURED|INFECTED|CUREFAILED|WARNING|SUSPICION) (.*)/ ,
    sub {chdir('/opt/kav/bin') or die "Can't chdir to kav: $!"},
    sub {chdir($TEMPBASE) or die "Can't chdir back to $TEMPBASE $!"},
  ],

# Commented out because the name 'sweep' clashes with the Debian package of
# the same name. Make sure the correct sweep is found in the path when enabling
#
# ### http://www.sophos.com/
```

```
# ['Sophos Anti Virus (sweep)', 'sweep',
#   '-nb -f -all -rec -ss -sc -archive {}',
#   [0,2], qr/Virus .*? found/,
#   qr/^>>> Virus(?:(?: fragment)? '?(.+?)'? found)/,
# # sub {$ENV{SAV_IDE}='/usr/local/sav'},
# ],


# always succeeds (uncomment to avoid mail requeue if all other scanners fail)
# ['always-clean', sub {0}],

);


#
# Section VIII - Debugging
#

# The most useful debugging tool is to run amavisd-new non-detached
# from a terminal window:
# amavisd debug

# Some more refined approaches:

# If sender matches ACL, turn debugging fully up, just for this one message
#@debug_sender_acl = ( "test-sender\@$mydomain" );
#@debug_sender_acl = qw( debug@example.com );

# May be useful along with @debug_sender_acl:
# Prevent all decoded originals being deleted (replaced by decoded part)
#$keep_decoded_original_re = new_RE( qr/.*/ );

# Turn on SpamAssassin debugging (output to STDERR, use with 'amavisd debug')
#$sa_debug = 1;            # defaults to false

#-------------
1;  # insure a defined return
```

VIII. Licencias

Apéndice J. GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other written document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you".

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (For example, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, whose contents can be viewed and edited directly and straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup has been designed to thwart or discourage subsequent modification by readers is not Transparent. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML designed for human modification. Opaque formats include PostScript, PDF, proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies of the Document numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a publicly-accessible computer-network location containing a complete Transparent copy of the Document, free of added material, which the general network-using public has access to download anonymously at no charge using public-standard network protocols. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has less than five).

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section entitled "History", and its title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. In any section entitled "Acknowledgements" or "Dedications", preserve the section's title, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section as "Endorsements" or to conflict in title with any Invariant Section.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections entitled "History" in the various original documents, forming one section entitled "History"; likewise combine any sections entitled "Acknowledgements", and any sections entitled "Dedications". You must delete all sections entitled "Endorsements."

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, does not as a whole count as a Modified Version of the Document, provided no compilation copyright is claimed for the compilation. Such a compilation is called an "aggregate", and this License does not apply to the other self-contained works thus compiled with the Document, on account of their being thus compiled, if they are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one quarter of the entire aggregate, the Document's Cover Texts may be placed on covers that surround only the Document within the aggregate. Otherwise they must appear on covers around the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License provided that you also include the original English version of this License. In case of a disagreement between the translation and the original English version of this License, the original English version will prevail.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/..

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

IX. bibliografía

Bibliografía

Documentación

[Limón01] *Postfix (versión 2.0) [Tutorial] (http://laurel.datsi.fi.upm.es/postfix/Tutorial2.pdf), Fernando Limón Martínez, Enero 2003, 2003.*

[Lombraña01] *Cómo montar un potente sistema de correo (II) (http://bulma.net/body.phtml?nIdNoticia=1938), Daniel Lombraña González, 10/12/2003, 2003.*

[Lombraña02] *Como Montar un Servidor Imap de manera rápida (http://bulma.net/body.phtml?nIdNoticia=1857), Daniel Lombraña González, 25/08/2003, 2003.*

[Meléndez01] *Controles de acceso en Postfix (http://www.uco.es/ccc/sistemas/postfix/restricciones.html), Luis Meléndez Aganzo, septiembre 2002, 2002.*

[Pereda01] *Filtrando correo en postfix (antivirus y spam) (http://bulma.net/body.phtml?nIdNoticia=1977), Fernando J. Pereda, 10/02/2004, 2004.*

[Polo01] *Cómo montar un potente sistema de correo con postfix (http://bulma.net/body.phtml?nIdNoticia=1621), Javi Polo, 12/12/2002, 2002.*

[Polo02] *Filtrando mensajes con Postfix (http://bulma.net/body.phtml?nIdNoticia=878), Javi Polo, 01/10/2001, 2001.*

[Roncero01] *Sistema de cuentas de correo virtuales con PostFix, OpenLDAP y Courier (http://bulma.net/body.phtml?nIdNoticia=2013), Jesús Roncero Franco, 17/04/2004 02:40, 2004.*

[Ros01] *Ensalada de correo: Courier-imap, Exim, Fetchmail, Procmail, Spamassassin, Kmail, Evolution, Thunderbird y Squirrelmail (http://bulma.net/body.phtml?nIdNoticia=1869), Paco Ros, 07/09/2003, 2003.*

[Teijeiro01] *Postfix+Cyrus Imap+sasl+tls (http://cernicalo.escomposlinux.org/~emeteo/imap), Mario Teijeiro Otero, 10/11/2003, 2003.*

SPAM

[Galli01] *Asesinando spams (http://bulma.net/body.phtml?nIdNoticia=1389), Ricardo Galli Granada, 24/06/2002, 2002.*

[Galli02] *Bogofilter mata mejor (http://bulma.net/body.phtml?nIdNoticia=1537), Ricardo Galli Granada, 07/10/2002, 2002.*

[Sort01] *Control antispam con Postfix+SpamAssassin (http://bulma.net/body.phtml?nIdNoticia=1799), Josep Sort, 22/06/2003, 2003.*

Antivirus

[Pina01] *Poner clamav configurando sólo procmail (http://bulma.net/body.phtml?nIdNoticia=1978), Carles Pina i Estany, 13/02/2004, 2004.*

SASL

[Ballester01] *Cómo utilizar SASL con Postfix., Guillermo Ballester Valor.*

[Ben01] *Postfix SMTP AUTH (and TLS) HOWTO for RedHat Linux < Version 8.0 and Cyrus-SASL < 1.5.28 (http://postfix.state-of-mind.de/patrick.koetter/smtpauth/), Patrick Ben Koetter, 04/04/2004, 2004.*

[Danen01] *Enabling SASL support in Postfix (http://www.mandrakesecure.net/en/docs/postfix-sasl.php), Vicent Danen, 08/03/2002, 2002.*

Listas de correo

[Fuentes01] *Autenficar Postfix mediante SASL (http://llistes.bulma.net/pipermail/bulmailing/Week-of-Mon-20021202/008535.html), Manuel Fuentes, 03/12/2002.*

Software relacionado y utilizado

[AMaViSd-new] *AMaViSd-new (http://www.ijs.si/software/amavisd/).*

[Clamav] *Clamav (http://www.clamav.net/).*

[Courier] *Courier (http://courier.sourceforge.net/).*

[OpenLDAP] *OpenLDAP (http://www.openldap.org/)* .

[phpLDAPadmin] *phpLDAPadmin (http://phpldapadmin.sourceforge.net/).*

[Postfix] *Postfix (http://www.postfix.org/).*

[SASL] *SASL (http://asg.web.cmu.edu/sasl/).*

[Spamassassin] *Spamassassin (http://www.spamassassin.org/).*

[SquirrelMail] *SquirrelMail (http://www.squirrelmail.org/).*

[TheGimp] *The Gimp! (http://www.gimp.org/)* .

Sistemas Operativos empleados

[DebianGNULinux] *Debian GNU/Linux (http://www.debian.org/)* .

Núcleos implicados

[Linux] *Linux (http://www.kernel.org/)* .