

Servidor de correo en GNU/Linux con Postfix

Alberto Molina Coballes <alberto.molina@hispalinux.es>
José Domingo Muñoz Rodríguez <josedom24@gmail.com>
IES Gonzalo Nazareno. Dos Hermanas (Sevilla)

12 de enero de 2009

Resumen

En este documento se describe la instalación y configuración de un servidor de correo en GNU/Linux con postfix, dovecot y squirrelmail. Todo el desarrollo que se presenta se ha realizado utilizando la distribución Debian GNU/Linux (lenny).

Este documento se elaboró para el curso *Introducción a los servicios en GNU/Linux* organizado por el [CEP de Lora del Río](#) (Sevilla) durante el curso 2008/2009.

©Alberto Molina Coballes y José Domingo Muñoz Rodríguez. Algunos Derechos reservados.

Esta obra está bajo una licencia Attribution-ShareAlike 2.5 de Creative Commons. Para ver una copia de esta licencia, visite:

<http://creativecommons.org/licenses/by-sa/2.5/>

Índice

1. Introducción	3
2. Conceptos generales	3
2.1. Componentes de un servidor de correo	3
2.2. DNS	4
2.3. Retransmisión de correo (<i>relay</i>)	4
2.4. Listas de bloqueo	5
3. Instalación y configuración de Postfix en un equipo con dirección IP pública estática	5
3.1. Parámetros de configuración	5
3.2. Instalación de postfix	6
3.3. Pruebas de funcionamiento	7
3.3.1. Destinatario local y remitente local	7
3.3.2. Destinatario local y remitente exterior	8
3.3.3. Destinatario exterior y remitente local	8
4. Configuración de Postfix a través de un <i>relay host</i> autenticado	8
4.1. Características de la conexión	9
4.2. Configuración de <code>main.cf</code>	9
4.3. Datos de autenticación	10
4.4. Utilización del certificado adecuado	10
4.5. Prueba de funcionamiento	10
5. Dovecot IMAP	11
6. Dovecot POP	11
6.1. Configuración segura	12
7. Squirrelmail	12

1. Introducción

El correo electrónico es sin duda de una de las aplicaciones más utilizadas en Internet y es muy interesante conocer sus principales características y configurar un servidor de correo. Sin embargo, la instalación de un servidor de correo electrónico tiene cierta complicación, en parte por el propio mecanismo de envío y recepción de correo electrónico, como últimamente por el problema del envío masivo de correo no deseado (*spam*), que obliga a entender con más detalle lo que se está haciendo y configurar los servidores de correo de forma más precisa.

En la siguiente sección se presentan las características generales del servicio de correo electrónico así como las consideraciones previas que hay que hacer para montarlo. En el resto de las secciones se irán configurando los diferentes componentes de un servidor de correo básico: mta, servidores pop e imap y webmail.

2. Conceptos generales

Para configurar adecuadamente un servidor de correo es necesario conocer bien sus componentes y el proceso de envío y recepción de correo, que se explican en los siguientes apartados.

2.1. Componentes de un servidor de correo

El proceso de envío y recepción de un mensaje de correo electrónico se representa en la figura 1 y se podría describir brevemente de la siguiente manera:

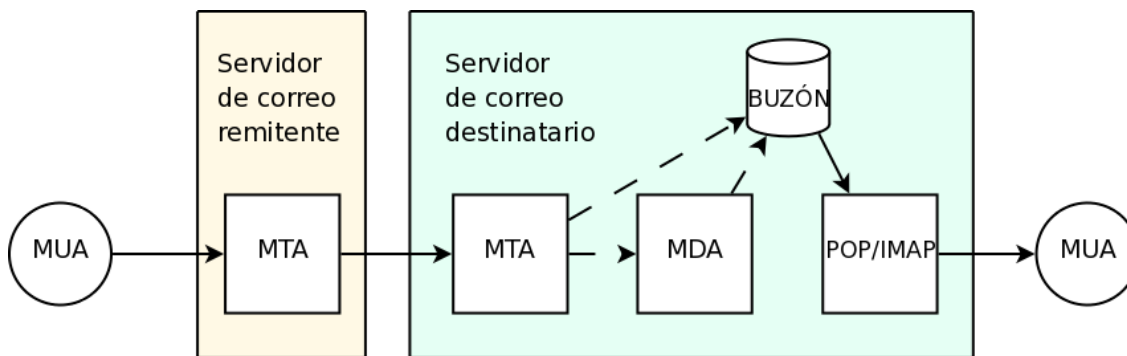


Figura 1: Componentes básicos que intervienen en el envío y recepción de un mensaje de correo electrónico

- El usuario que actúa como remitente utiliza un cliente de correo electrónico o *Mail User Agent* (MUA) y envía un mensaje de correo a su servidor de correo electrónico o *Mail Transfer Agent* (MTA) utilizando el protocolo SMTP.
- El MTA recibe el correo y lo coloca en la cola de mensajes para enviar, llegado el momento, envía el mensaje de correo al servidor de correo electrónico del destinatario utilizando el protocolo SMTP.
- El MTA del destinatario acepta el mensaje y lo almacena en el buzón correspondiente, función que en algunos casos realiza un programa específico que se denomina

Mail Delivery Agent o MDA.

- El mensaje de correo permanece en el buzón hasta que el usuario que actúa como destinatario, utiliza su MUA y accede a su buzón a través de alguno de los distintos mecanismos posibles, siendo los más habituales los protocolos POP o IMAP.

Por tanto, un servidor de correos tiene un componente imprescindible que es el MTA, término que en muchas ocasiones se utiliza como sinónimo de servidor de correo, y una serie de componentes adicionales, que además de los mencionados pueden incluir también bases de datos relacionales o directorios para almacenar información de los usuarios, sistemas de filtrado de correo para eliminar spam o virus, sistemas de autenticación de usuarios y un largo etcétera.

Otro aspecto importante a destacar es que un MTA puede funcionar como cliente SMTP —cuando envía mensajes de correo— o como servidor SMTP —cuando recibe mensajes de correo—.

2.2. DNS

Para que un equipo pueda recibir correo de cualquier otro servidor de correo de Internet, es necesario que esté configurado su servidor DNS de alguna de estas dos formas:

- Que el FQHN del equipo aparezca en un registro tipo ADDRESS del servidor DNS. En ese caso cuando se pregunte por la dirección IP de, por ejemplo, mortadelo.tia.com el servidor DNS responderá con la dirección IP pública correspondiente al equipo y de esa manera el servidor de correo de mortadelo.tia.com podrá recibir correo del tipo <usuario@mortadelo.tia.com>.
- Que además del registro ADDRESS anterior, exista un registro MX (*Mail eXchange*) que redirija todo el correo del dominio al equipo donde está el servidor de correo, por ejemplo, que envíe todo el correo del dominio tia.com al equipo mortadelo.tia.com, por lo que el servidor de correo de mortadelo.tia.com podrá recibir correo del tipo <usuario@tia.com>.

2.3. Retransmisión de correo (*relay*)

La mayoría de los usuarios de un servidor de correo no lo son del propio sistema sino que son usuarios de otros equipos, por lo que un MTA tiene que ser capaz de *retransmitir* los mensajes de usuarios que provengan de otros equipos. Un MTA que retransmita correo de cualquiera se dice que está configurado como *open relay*, por lo que será utilizado masivamente por *spammers*. Algunos MTA vienen por defecto configurados como *open relay*, pero no es el caso de postfix, que por defecto sólo permite el envío de correo desde el propio equipo.

Para permitir la retransmisión de correo de otros equipos se utilizan principalmente dos métodos:

- Autenticar los usuarios, tarea que debe realizarse mediante un mecanismo externo, ya que SMTP no provee ningún método de autenticación (SASL es el más utilizado).
- Permitir la retransmisión de determinadas direcciones IP o segmentos de red.

2.4. Listas de bloqueo

Cuando se establece una conexión SMTP entre dos MTA, muchos servidores de correo en Internet contrastan la dirección IP del remitente en listas de direcciones IP utilizadas por *spammers*, si la dirección IP del remitente aparece en esas listas, no se aceptan los mensajes de correo y se cierra la conexión¹.

Si instalamos un servidor de correo en un equipo que accede a Internet con una dirección IP estática y ésta aparece en alguna lista negra, tendremos que seguir una serie de pasos en la configuración para conseguir que saquen nuestra dirección IP de tales listas. Si por el contrario, instalamos un servidor de correo en un equipo con una dirección IP dinámica, esta labor se hace imposible, por lo que hoy día **no se puede instalar un servidor de correo que envíe directamente correo en un equipo con dirección IP dinámica**.

3. Instalación y configuración de Postfix en un equipo con dirección IP pública estática

Vamos a configurar postfix para que envíe correo directamente a Internet desde un equipo con una dirección IP pública estática, con el nombre de correo saliente *mortadelo.tia.com* y que acepte correo para ese dominio y *localhost*.

3.1. Parámetros de configuración

Antes de empezar con la instalación del MTA propiamente, hay que aclarar algunos parámetros que se van a utilizar.

Nombre del equipo Asociado a la variable `myhostname` y en el que se especifica el nombre largo del equipo (FQHN). Por ejemplo:

```
mortadelo.tia.com
```

Nombre de dominio para el correo saliente Lo que aparecerá como domino (a la derecha de la @) en el correo que envíe el equipo. En postfix se define este parámetro en la variable `myorigin` y por defecto se asocia `myhostname`:

```
myorigin = $myhostname
```

Dominios para los que se recibe correo Dominios que se aceptan como correo entrante, porque se reparta localmente (*local delivery*) o se envíe a otro equipo (*forward*). Este parámetro viene definido por `mydestination` y no tiene por qué coincidir con `myorigin`, los valores por defecto son:

```
mydestination = $myhostname localhost.localdomain localhost
```

Direcciones para las que se retransmite correo Es habitual que un servidor smtp permita a diferentes clientes retransmitir correo a través de él. Se pueden definir direcciones IP o redes con la variable `mynetworks`, por ejemplo:

¹Ver por ejemplo <http://openrbl.org/>

```
mynetworks = 127.0.0.0/8 192.168.1.0/24
```

Para que se permita enviar correo al propio equipo (127.0.0.0/8) y a los de la red 192.168.1.0/24.

Dominios para los que se recibe correo De forma complementaria a lo anterior, el servidor de correo puede aceptar correo entrante para diferentes destinos. Mediante el parámetro `relay_domains` se define este parámetro, que por defecto es:

```
relay_domains = $mydestination
```

Método de envío Si se trata de un servidor de correo que envía directamente el correo a Internet o tiene que enviarlo a través de otro servidor (lo que se conoce como *Smarthost*). Esto se define en la variable `relayhost`, que por defecto no toma ningún valor.

3.2. Instalación de postfix

Para instalar el MTA postfix en una máquina escribimos:

```
aptitude install postfix
```

Durante la instalación *debconf* hace una serie de preguntas con idea de dejar el MTA configurado al final, siendo los puntos más importantes:

- Configuraremos la máquina como *Internet site*
- Como nombre de correo pondremos `mortadelo.tia.com`

El fichero de configuración de postfix es `/etc/postfix/main.cf`, que queda:

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
```

```
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
```

```
#myorigin = /etc/mailname
```

```
smtpd_banner = $myhostname ESMTPEX $mail_name (Debian/GNU)
```

```
biff = no
```

```
# appending .domain is the MUA's job.
```

```
append_dot_mydomain = no
```

```
# Uncomment the next line to generate "delayed mail" warnings
```

```
#delay_warning_time = 4h
```

```
readme_directory = no
```

```
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

myhostname = mortadelo.tia.com
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, localhost, localhost.localdomain
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
```

3.3. Pruebas de funcionamiento

Instalamos el programa *mail*, que se incluye en el paquete `bsd-mailx` y realizamos diferentes pruebas de envío y recepción de correo.

3.3.1. Destinatario local y remitente local

Desde una terminal cualquiera:

```
mortadelo:~# mail usuario
Subject: Asunto
Prueba de envío local
[CTRL-D]
Cc:
```

Abrimos el fichero de registros de correo `/var/log/mail.log`² y extraemos las líneas que informan de la recepción correcta del mensaje y envío al buzón adecuado (las `\` representan continuación de líneas):

```
postfix/pickup[7199]: E8B8C34675: uid=0 from=<root>
postfix/cleanup[7295]: E8B8C34675: message-id=<20081125104513.E8B8C34675@m\
ortadelo>
postfix/qmgr[7201]: E8B8C34675: from=<root@mortadelo.tia.com>, size=315, n\
rcpt=1 (queue active)
postfix/local[7297]: E8B8C34675: to=<usuario@mortadelo.tia.com>, orig_to=<\
```

²Es recomendable hacerlo de forma continua con la instrucción `tail -f`

```
usuario>, relay=local, delay=0.12, delays=0.04/0.02/0/0.06, dsn=2.0.0, sta\
tus=sent (delivered to command: procmail -a "$EXTENSION")
postfix/qmgr[7201]: E8B8C34675: removed
```

El nuevo mensaje se almacenará en el fichero `/var/mail/usuario` y podemos abrirlo con cualquier MUA, en particular si escribimos *mail* aparecerá:

```
N 1 root@localhost      Thu Nov 25 11:45   14/479   Asunto
```

3.3.2. Destinatario local y remitente exterior

Si el DNS está configurado correctamente, podemos enviar correo desde una cuenta de correo cualquiera a un usuario de nuestro equipo y comprobar el mensaje que ha llegado en los registros de correo:

```
postfix/smtpd[7402]: connect from mail-bw0-f20.google.com[209.85.218.20]
postfix/smtpd[7402]: F037834676: client=mail-bw0-f20.google.com[209.85.218\
.20]
postfix/cleanup[7407]: F037834676:message-id=<d752a77a0812250308s15414d9ve\
cc61628ed4fed03@mail.gmail.com>
postfix/qmgr[7201]: F037834676: from=<unacuenta@gmail.com>, size=2136, nrc\
pt=1 (queue active)
postfix/local[7408]: F037834676: to=<usuario@mortadelo.tia.com>, relay=loc\
al, delay=0.42, delays=0.36/0.01/0/0.05, dsn=2.0.0, status=sent (delivered\
to command: procmail -a "$EXTENSION")
postfix/qmgr[7201]: F037834676: removed
```

3.3.3. Destinatario exterior y remitente local

Enviamos un mensaje a una cuenta de correo externa (en este caso a gmail) y comprobamos de nuevo en los registros de correo las líneas que aparecen:

```
postfix/pickup[5933]: 7539434680: uid=1000 from=<alberto>
postfix/cleanup[5940]: 7539434680: message-id=<20081231121556.7539434680@m\
ortadelo>
postfix/qmgr[5935]: 7539434680: from=<alberto@mortadelo.tia.com>, size=306\
, nrcpt=1 (queue active)
postfix/smtp[5942]: 7539434680: to=<unacuenta@gmail.com>, delay=3.1, delay\
s=0.04/0.06/1.7/1.3, dsn=2.0.0, status=sent (250 2.0.0 OK 12307259715sm255\
1300eyf.47)
postfix/qmgr[5935]: 7539434680: removed
```

4. Configuración de Postfix a través de un *relay host* autenticado

Como ya se explicó en el apartado 2.4 no es posible configurar un servidor de correo en un equipo que acceda a Internet con una dirección IP pública dinámica, porque con toda

probabilidad aparecerá en una lista de bloqueo y no podremos enviar correo a determinados dominios. Una forma de comprobar esto sería instalar postfix siguiendo los pasos del apartado anterior, pero en un equipo con dirección IP dinámica, en ese caso al enviar un mensaje a cuentas de correo de determinados dominios (hotmail por ejemplo) aparecerían registros como los siguientes:

```
postfix/pickup[6804]: 09B0634680: uid=1000 from=<alberto>
postfix/cleanup[6810]: 09B0634680:message-id=<20081231154700.09B0634680@m\
ortadelo>
postfix/qmgr[6802]: 09B0634680: from=<alberto@mortadelo.tia.com>, size=30\
7, nrcpt=1 (queue active)
postfix/smtp[6812]: 09B0634680: to=<una@hotmail.com>,relay=mx2.hotmail.co\
m[65.54.244.40]:25, delay=1.3, delays=0.03/0.04/0.92/0.3, dsn=5.0.0, stat\
us=bounced (host mx2.hotmail.com[65.54.244.40] said: 550 DY-001 Mail reje\
cted by Windows Live Hotmail for policy reasons. We generally do not acce\
pt email from dynamic IP's as they are not typically used to deliver unau\
thenticated SMTP e-mail to an Internet mail server. http://www.spamhaus.o\
rg maintains lists of dynamic and residential IP addresses. If you are no\
t an email/network admin please contact your E-mail/Internet Service Prov\
ider for help. Email/network admins, please visit http://postmaster.live.\
com for email delivery information and support (in reply to MAIL FROM com\
mand))
postfix/smtp[6812]: 09B0634680: lost connection with mx2.hotmail.com[65.5\
4.244.40] while sending RCPT TO
```

Para evitar esto podemos utilizar otro MTA para que retransmita el correo de nuestro servidor, para lo que debemos tener una cuenta de correo en dicho MTA. Explicaremos a continuación los pasos que hay que dar para hacer eso con el servidor de correo de GMail (smtp.gmail.com).

4.1. Características de la conexión

Para enviar correo utilizando el servidor SMTP de Gmail la conexión tiene que estar cifrada con TLS (nueva denominación de SSL), para lo que debemos añadir la Autoridad Certificadora adecuada (en este caso Thawte) y autenticada, para lo que utilizaremos un nombre de usuario (dirección de correo) y contraseña del servicio.

4.2. Configuración de main.cf

Tenemos que editar el fichero y añadir las siguientes líneas:

```
relayhost = [smtp.gmail.com]:587
```

Donde indicamos el nombre del equipo que retransmitirá nuestro mensajes (los corchetes ([]) son para que no haga la resolución MX) y el puerto de la conexión es el que se utiliza para la conexión entre un cliente y un servidor SMTP (587/TCP *message submission*)³.

³El puerto 25/TCP se reserva para comunicación entre dos servidores de correo y aquí estamos actuando como un cliente de correo.

```
smtp_use_tls = yes
smtp_tls_CAfile = /etc/postfix/cacert.pem
```

Para que utilice TLS y confíe en las autoridades certificadoras que se añadan al fichero `cacert.pem`

```
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous
```

donde le decimos a postfix que debe autenticarse mediante SASL y especificamos la ubicación del fichero con la información del nombre de usuario y contraseña.

4.3. Datos de autenticación

Creamos el fichero `/etc/postfix/sasl/passwd` con el siguiente contenido:

```
[smtp.gmail.com]:587      unacuenta@gmail.com:unacontraseña
```

Y lo protegemos adecuadamente con:

```
chmod 600 /etc/postfix/sasl/passwd
```

El fichero de configuración hay que transformarlo a un fichero indexado de tipo hash mediante la instrucción:

```
postmap /etc/postfix/sasl/passwd
```

que creará el fichero `/etc/postfix/sasl/passwd.db`

4.4. Utilización del certificado adecuado

Para añadir la autoridad certificadora *Thawte* al fichero de certificados que utilizará postfix, hacemos:

```
cat /etc/ssl/certs/Thawte_Premium_Server_CA.pem >> /etc/postfix/cacert.pem
```

si no existiesen los ficheros de certificados SSL, debemos instalar el paquete `ca-certificates`.

4.5. Prueba de funcionamiento

Para comprobar que todo está funcionando correctamente, enviamos un mensaje a una cuenta cualquiera de correo y miramos de nuevo los registros:

```
postfix/pickup[6703]: 6AFF534680: uid=1000 from=<alberto>
postfix/cleanup[6786]: 6AFF534680: message-id=<20081231154524.6AFF534680@m\
ortadelo>
postfix/qmgr[5935]: 6AFF534680: from=<alberto@mortadelo.tia.com>, size=310\
, nrcpt=1 (queue active)
postfix/smtp[6788]: 6AFF534680:to=<unacuenta@hotmail.com>,relay=smtp.gmail\
.com[66.249.93.111]:587, delay=2.8, delays=0.04/0.02/1.2/1.6, dsn=2.0.0, s\
tatus=sent (250 2.0.0 OK 1230738538 34sm19633915ugh.10)
postfix/qmgr[5935]: 6AFF534680: removed
```

5. Dovecot IMAP

Dovecot se encarga del reparto del correo a los usuarios a través de los protocolos más conocidos para ello *pop3* e *imap* y sus versiones cifradas *pop3s* e *imaps*. Para instalar el servidor dovecot imap hay que hacer:

```
aptitude install dovecot-imapd
```

que instala por dependencias el paquete `dovecot-common`.

Una vez instalado el servicio se pone en marcha y abre los puertos 143/tcp y 993/tcp, correspondientes respectivamente a los protocolos IMAP e IMAPs y que podemos ver con la instrucción:

```
# netstat -putan|grep dovecot
tcp      0      0 0.0.0.0:993      0.0.0.0:*        LISTEN   4396/dovecot
tcp      0      0 0.0.0.0:143     0.0.0.0:*        LISTEN   4396/dovecot
```

Ahora podemos configurar una cuenta del servidor de correo en un cliente de correo y establecer la conexión, para los que nos pedirá el nombre de usuario y la contraseña.

Si la conexión se realiza por IMAP (tcp/143) será no cifrada y aparecerá el siguiente registro en el fichero `/var/log/mail.log`:

```
dovecot: imap-login: Login: user=<usuario>, method=PLAIN, rip=127.0.0.1, 1\
ip=127.0.0.1, secured
```

Si por el contrario la conexión se realiza por IMAPs (tcp/993) será cifrada y aparecerá el siguiente registro:

```
dovecot: imap-login: Login: user=<usuario>, method=PLAIN, rip=127.0.0.1, 1\
ip=127.0.0.1, TLS
```

Y podemos ver la conexión establecida con `netstat`:

```
tcp      0      0 127.0.0.1:56049  127.0.0.1:993     ESTABLISHED 3443/evolution
```

6. Dovecot POP

Instalamos el paquete mediante:

```
aptitude install dovecot-pop3d
```

Se inicia el demonio de forma automática y abre los puertos 110/tcp y 995/tcp correspondientes a los servicios POP3 y POP3s, como podemos ver de nuevo con `netstat`:

```
# netstat -putan |grep dovecot
tcp      0      0 0.0.0.0:993     0.0.0.0:*        LISTEN   4210/dovecot
tcp      0      0 0.0.0.0:995     0.0.0.0:*        LISTEN   4210/dovecot
tcp      0      0 0.0.0.0:110     0.0.0.0:*        LISTEN   4210/dovecot
tcp      0      0 0.0.0.0:143     0.0.0.0:*        LISTEN   4210/dovecot
```

Ahora tendremos que configurar de nuevo el cliente de correo, pudiéndose conectar ahora tanto a un servidor POP3 como IMAP.

6.1. Configuración segura

La utilización de un mecanismo de conexión cifrado se recomienda siempre, para no sufrir ataques de suplantación de identidad por contraseñas “esnifadas” en la red, por lo que es recomendable editar el fichero `/etc/dovecot/dovecot.conf` y modificar la línea actual:

```
protocols = imap imaps pop3 pop3s
```

por:

```
protocols = imaps pop3s
```

para que sólo se permitan conexiones cifradas entre dovecot y los clientes de correo de los usuarios.

7. Squirrelmail

Para que nuestros usuarios puedan enviar y recibir correo vamos a instalar un “webmail”, en particular squirrelmail. Para ello hacemos como es habitual:

```
apt-get install squirrelmail
```

que si no tenemos instalado apache2 o php4 nos los instalará, además de algún otro paquete adicional.

Squirrelmail no es más que una aplicación en PHP que valida a los usuarios de forma local y que utiliza el servidor IMAP del sistema para la recepción y clasificación de los mensajes y el servidor SMTP en modo local para el envío de los mismos.

En caso de utilizar apache2, no es necesario modificar el fichero de configuración del servidor web, para incluir soporte para php4, ya que viene incluido de forma automática.

La única modificación que tendremos que hacer en el fichero:

```
/etc/apache2/apache2.conf
```

es incluir la línea:

```
Alias /webmail/ /usr/share/squirrelmail/
```

donde *webmail/* es el directorio sobre el directorio raíz del servidor web donde estará la aplicación en php.

Para que los cambios se apliquen, reiniciamos el servidor web mediante:

```
/etc/init.d/apache2 restart
```

Para acceder al webmail, abrimos nuestro navegador y escribimos:

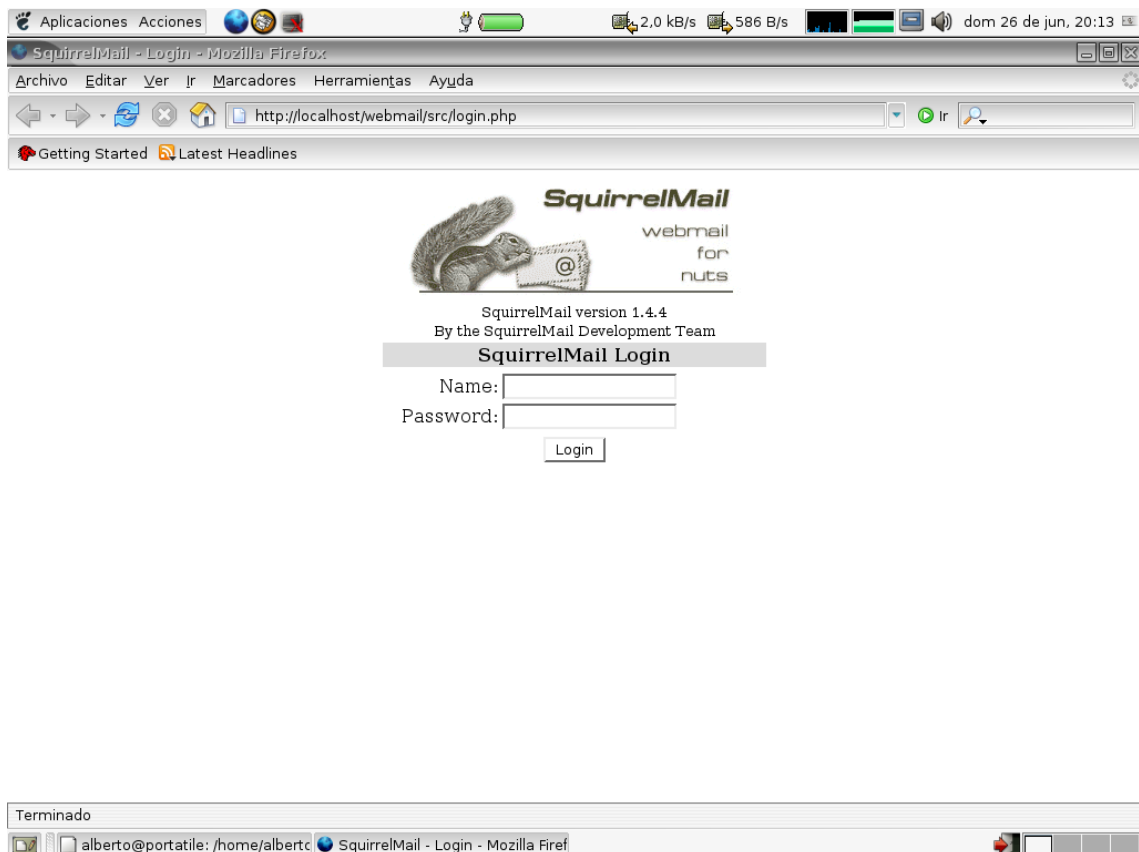


Figura 2: Página de ingreso de squirrelmail

`http://nuestra_ip/webmail/`

con lo accederemos a la pantalla que se observa en la figura 2.

Si queremos modificar la configuración de squirrelmail, podemos hacerlo a través del programa:

`/etc/squirrelmail/conf.pl`