

## Servidor de correo en GNU/Linux con Postfix

Alberto Molina Coballes, José Domingo Muñoz Rodríguez y José Luis Rodríguez Rodríguez.

25 de abril de 2011

En este documento se describe la instalación y configuración de un servidor de correo en GNU/Linux con postfix como MTA, dovecot como servidor POP/IMAP y squirrelmail como webmail. Este documento se elaboró para el curso *Servicios en GNU/Linux (Nivel Intermedio)* organizado por el [CEP de Lora del Río](#) (Sevilla) en 2011, por lo que no es un documento que describa de forma exhaustiva la configuración de un servidor de correo completo. Todo el desarrollo que se presenta se ha realizado utilizando la distribución Debian GNU/Linux (lenny), aunque la mayoría de aspectos son comunes a todas las distribuciones.



Usted es libre de copiar, distribuir y modificar este documento de acuerdo con las condiciones de la licencia Attribution-ShareAlike 3.0 de Creative Commons. Puede ver una copia de ésta en:

<http://creativecommons.org/licenses/by-sa/3.0/es/>



<b>Índice</b>	<b>2</b>
<b>1. Introducción</b>	<b>4</b>
<b>2. Conceptos generales</b>	<b>4</b>
2.1. Componentes de un servidor de correo . . . . .	4
2.2. DNS . . . . .	5
2.3. Retransmisión de correo o <i>relay</i> . . . . .	5
2.4. Listas de bloqueo . . . . .	5
<b>3. Configuración previa</b>	<b>6</b>
3.1. Gestión DNS externo . . . . .	6
3.2. Configuración del router: DNAT o port forwarding . . . . .	7
<b>4. Instalación y configuración de Postfix en un equipo con dirección IP pública estática</b>	<b>7</b>
4.1. Parámetros de configuración . . . . .	7
4.2. Instalación de postfix . . . . .	8
4.3. Estructura de ficheros . . . . .	9
4.4. Pruebas de funcionamiento . . . . .	9
4.4.1. Destinatario local y remitente local . . . . .	10
4.4.2. Destinatario local y remitente exterior . . . . .	10
4.4.3. Destinatario exterior y remitente local . . . . .	11
4.5. Avatar como servidor de correo de los clientes de nuestra red . . . . .	12
4.5.1. Envío desde cliente a usuarios de avatar . . . . .	12
4.5.2. Envío desde cliente a direcciones de Internet . . . . .	13
<b>5. Configuración de Postfix a través de un <i>relay host</i> autenticado</b>	<b>14</b>
5.1. Características de la conexión . . . . .	14
5.2. Configuración de <code>main.cf</code> . . . . .	15
5.3. Datos de autenticación . . . . .	15
5.4. Utilización del certificado adecuado . . . . .	15
5.5. Prueba de funcionamiento . . . . .	16
<b>6. Dovecot POP e IMAP</b>	<b>16</b>
6.1. Instalación de dovecot IMAP . . . . .	17
6.2. Pruebas de funcionamiento . . . . .	17
6.3. Dovecot POP . . . . .	18
<b>7. Squirrelmail</b>	<b>19</b>
<b>8. Anexo: SMTP. Protocolos y comandos</b>	<b>21</b>



8.1. Esquema general . . . . .	3 21
8.2. Fases en el envío de un mensaje de correo . . . . .	21



# 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

### 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:

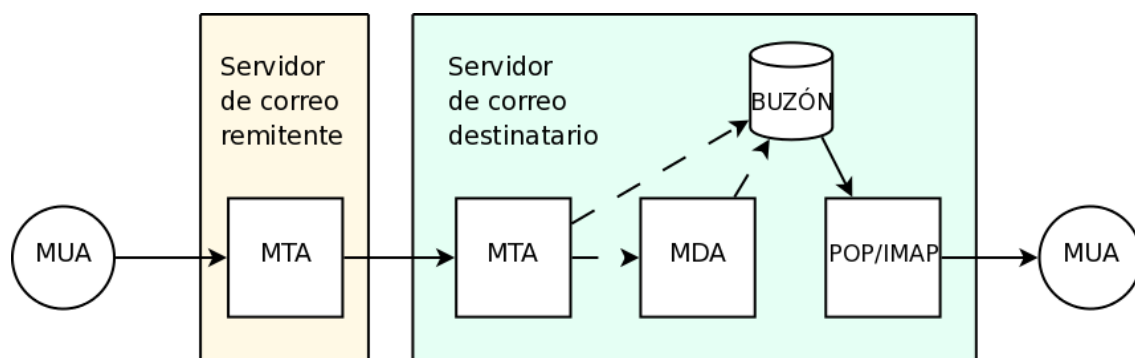


Figura 1: Componentes básicos que intervienen en el envío y recepción de un mensaje de correo electrónico

- 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 LDAP 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 funciona como cliente SMTP cuando envía mensajes de correo o como servidor SMTP cuando los recibe.

## 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, avatar.doesntexist.org el servidor DNS responderá con la dirección IP pública correspondiente al equipo y de esa manera el servidor de correo de avatar.doesntexist.org podrá recibir correo del tipo <usuario@avatar.doesntexist.org>.
- 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 dynalias.com al equipo avatar.doesntexist.org, por lo que el equipo avatar.doesntexist.org recibiría correo del tipo <usuario@dynalias.com><sup>1</sup>.

## 2.3. Retransmisión de correo o relay

Es bastante habitual que un servidor de correo se utilice como *pasarela* para enviar o recibir correo de otros sistemas, es decir que no sólo reciba y envíe correo de sus usuarios sino también de los usuarios de otros equipos. Esta característica se conoce como retransmisión de correo o *relay* en inglés. Un MTA debe estar configurado para permitir el *relay* sólo de ciertos equipos o usuarios, no de cualquiera, un MTA que retransmita correo de cualquiera se dice que está configurado como *open relay* y 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

Quando 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 conexión<sup>2</sup>.

<sup>1</sup> En nuestro caso, puesto que no somos propietarios del dominio dynalias.com sólo podemos utilizar la primera opción.

<sup>2</sup> Ver por ejemplo <http://openrbl.org/>



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. Configuración previa

Antes de instalar el MTA en avatar, debemos tener un DNS asociado a nuestra dirección IP y hacer accesible el puerto 25/tcp de avatar desde Internet.

#### 3.1. Gestión DNS externo

El servicio de correo electrónico no funciona con direcciones IP, es decir no podemos enviar un mensaje de correo a usuario@88.88.66.66, por tanto debemos tener un DNS asociado a nuestra dirección IP externa. La forma más sencilla de hacer este es utilizar alguno de los servicios gratuitos de DNS que hay disponibles (dyndns.com, no-ip.com, ...).

Podemos encontrarnos diferentes situaciones:

- Tenemos dirección IP pública estática y un nombre de dominio ya registrado y apuntando a nuestra dirección IP pública: Este es el caso ideal y no necesitaríamos configurar nada.
- Tenemos dirección IP pública estática y no tenemos un nombre de dominio registrado: Recomendamos utilizar dyndns.com o cualquier servicio similar que nos permita gestionar un registro DNS gratuito.
- Tenemos una dirección IP dinámica y un nombre de dominio registrado: Utilizamos la aplicación que nos proporcione la empresa en la que tenemos registrado el dominio para actualizar el registro DNS cada vez que cambie la dirección IP.
- Tenemos dirección IP dinámica y no tenemos registrado un nombre de dominio: Seguramente el caso más habitual, entonces recomendamos utilizar dyndns.com, que es un servicio gratuito de gestión de nombres de dominios, aunque puede utilizarse cualquier otro si así se prefiere.

En <http://www.loracep.org/moodle/mod/resource/view.php?id=1651> se explica con detalle los pasos que hay que dar para asociar nuestra dirección IP pública a un nombre DNS en el servicio dyndns.com. En ese enlace se explica que es necesario instalar la aplicación ddclient en avatar para que se actualice el registro DNS cuando cambie nuestra dirección IP externa, hay que notar que hoy en día muchos routers domésticos incluyen su propio cliente de dyndns, por lo que sería totalmente equivalente configurar esta opción del router a instalar y configurar ddclient.

En el resto de temas del curso, el equipo avatar utilizaba el nombre de dominio example.com, que es un nombre de dominio DNS reservado para realizar documentación y pruebas, pero que no se puede utilizar en Internet. En este tema habrá que cambiar la configuración de avatar, para que esté asociado al nombre que tengamos registrado en el DNS externo (avatar.dynalias.com, avatar.dyndns.com, avatar.doesntexist.com, etc.), este documento se ha realizado utilizando el nombre avatar.doesntexist.org.



### 3.2. Configuración del router: DNAT o port forwarding

Para que el puerto 25/tcp de avatar sea accesible desde el exterior, debemos configurar el dispositivo que tengamos de acceso a Internet (supondremos un router ADSL) para que todas las peticiones que vengan al puerto 25/tcp de la dirección pública, se "pasen" a avatar, cambiando la dirección pública del router por la dirección privada de avatar, esto se denomina Destination NAT o port forwarding y en <http://www.loracep.org/moodle/mod/resource/view.php?id=1653> aparecen diversos enlaces en los que se explica la forma de hacerlo en distintos dispositivos domésticos de acceso a Internet.

De forma totalmente equivalente al protocolo SMTP, habrá que realizar las mismas modificaciones para poder acceder a los servicios POP o IMAP desde Internet.

## 4. 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 *avatar.doesntexist.org* y que acepte correo para ese dominio y *localhost*.

### 4.1. 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:

```
avatar.doesntexist.org
```

**Nombre de dominio para el correo saliente** Lo que aparecerá como dominio (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 locales para los que se recibe correo** Dominios que se aceptan como correo entrante y que se reparte localmente (*local delivery*). Este parámetro viene definido por `mydestination` y no tiene por qué coincidir con `myorigin`, los valores por defecto son:

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

Observa que en la directiva `mydestination` se indican los dominios que serán propios del servidor, es decir, el correo recibido con destino a alguno de estos dominios está dirigido a usuarios del propio servidor en Avatar. Si el usuario existe, el mensaje será almacenado, sino el servidor devolverá un mensaje de error.

**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:

```
mynetworks = 127.0.0.0/8 192.168.2.0/24
```



Para que se permita enviar correo al propio equipo (127.0.0.0/8) y a los de la red 192.168.2.0/24.

**Dominios para los que se recibe correo** Dominios que se aceptan como correo entrante y que se reparte tanto localmente (*local delivery*) o se reenvían a otro equipo (*forward*). Se utiliza el parámetro `relay_domains` que por defecto tiene el valor:

```
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.

## 4.2. Instalación de postfix

Para instalar el MTA postfix en una máquina escribimos:

```
avatar:~# 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 `avatar.doesntexist.org`

El fichero de configuración principal de postfix queda:

/etc/postfix/main.cf

```

1 # See /usr/share/postfix/main.cf.dist for a commented, more complete\
2 version
3
4
5 # Debian specific:  Specifying a file name will cause the first
6 # line of that file to be used as the name.  The Debian default
7 # is /etc/mailname.
8 #myorigin = /etc/mailname
9
10 smtpd_banner = $myhostname ESMTPEX $mail_name (Debian/GNU)
11 biff = no
12
13 # appending .domain is the MUA's job.
14 append_dot_mydomain = no
15
16 # Uncomment the next line to generate "delayed mail" warnings
17 #delay_warning_time = 4h
18
19 readme_directory = no
20
21 # TLS parameters
22 smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
23 smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
24 smtpd_use_tls=yes
25 smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_\
26 scache
27 smtpd_tls_session_cache_database = btree:${data_directory}/smtp_scache

```





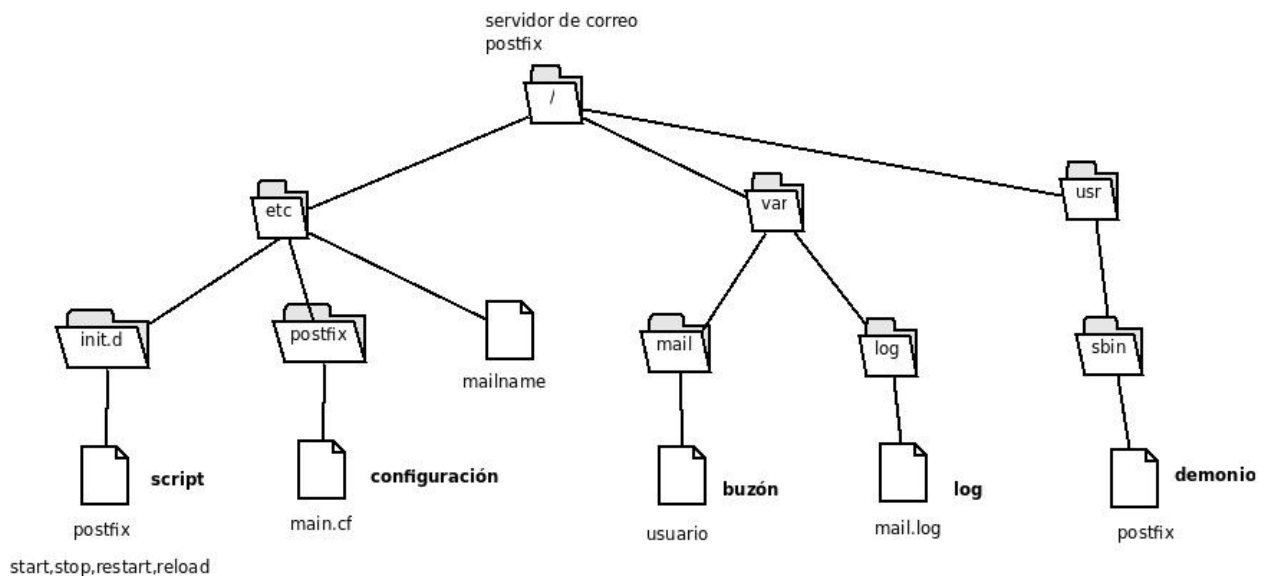
```

28
29 # See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package
30 # for information on enabling SSL in the smtp client.
31
32 myhostname = avatar.doesntexist.org
33 alias_maps = hash:/etc/aliases
34 alias_database = hash:/etc/aliases
35 myorigin = /etc/mailname
36 mydestination = $myhostname, localhost, localhost.localdomain
37 relayhost =
38 mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
39 mailbox_command = procmail -a "$EXTENSION"
40 mailbox_size_limit = 0
41 recipient_delimiter = +
42 inet_interfaces = all

```

### 4.3. Estructura de ficheros

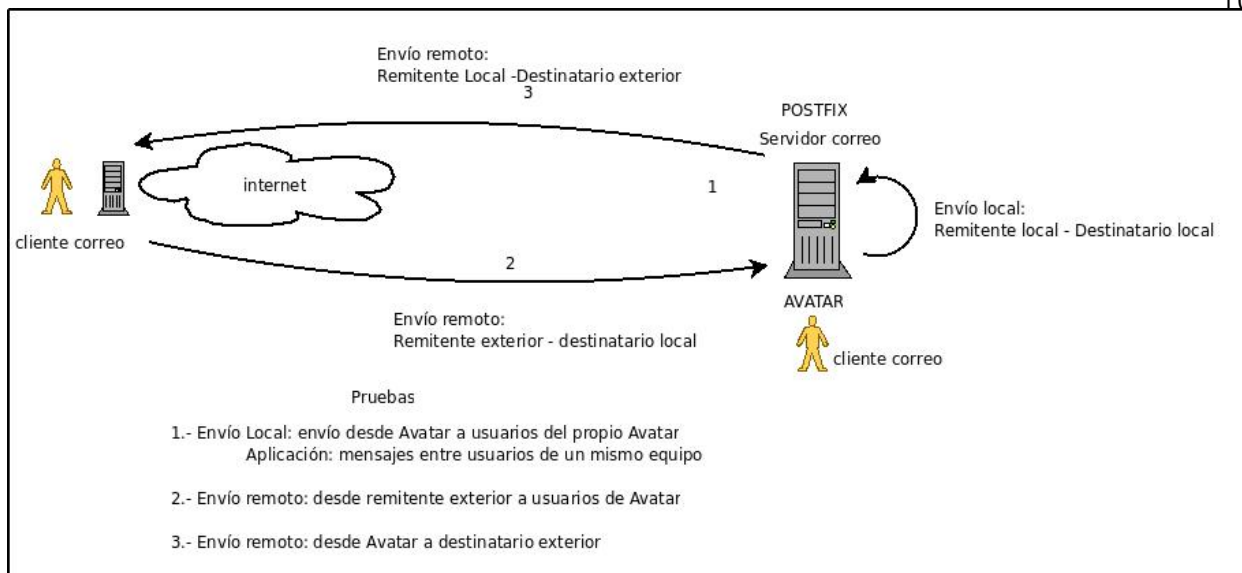
Use el siguiente árbol para localizar los ficheros de Postfix:



### 4.4. Pruebas de funcionamiento

Vamos a realizar diferentes pruebas de funcionamiento para comprobar la configuración correcta de avatar como cliente y como servidor SMTP. En primer lugar es necesario comprobar que está instalado el programa *mail*, que se incluye en el paquete *bsd-mailx*, este programa es un sencillo cliente de correo, que nos permite enviar correo mediante el protocolo SMTP y leer los buzones locales.





#### 4.4.1. Destinatario local y remitente local

Desde una terminal cualquiera de avatar enviamos un correo a un usuario local (si no se especifica ... se envía al propio equipo):

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

Abrimos el fichero de registros de correo `/var/log/mail.log3` 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.E8B8C34\
675@avatar>
postfix/qmgr[7201]: E8B8C34675: from=<root@avatar.doesntexist.org>, s\
ize=315, nrcpt=1 (queue active)
postfix/local[7297]: E8B8C34675: to=<usuario@avatar.doesntexist.org>,\
orig_to=<usuario>, relay=local, delay=0.12, delays=0.04/0.02/0/0.06,\
dsn=2.0.0, status=sent (delivered to command: procmail -a "$EXTENSIO\
N")
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      Fri Apr 15 11:45    14/479    Asunto
```

#### 4.4.2. 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:







<sup>3</sup>Es recomendable hacerlo de forma continua con la instrucción `tail -f`

**To:** <alumno@avatar.doesntexist.org>

[Add Cc](#) | [Add Bcc](#)

**Subject:** Caso 2: enviar correo desde un cliente en Internet a usuarios del propio servidor

 [Attach a file](#) Insert: [Invitation](#)

**B** *I* U ~~F~~ ~~rT~~ ~~T~~                        [« Plain Text](#)

Envío de correo desde gmail.

```
postfix/smtpd[7402]: connect from mail-bw0-f20.google.com[209.85.218.\
20]
postfix/smtpd[7402]: F037834676: client=mail-bw0-f20.google.com[209.8\
5.218.20]
postfix/cleanup[7407]: F037834676:message-id=<d752a77a0812250308s1541\
4d9vecc61628ed4fed03@mail.gmail.com>
postfix/qmgr[7201]: F037834676: from=<unacuenta@gmail.com>, size=2136\
, nrcpt=1 (queue active)
postfix/local[7408]: F037834676: to=<alumno@avatar.doesntexist.org>, \
relay=local, 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
```

#### 4.4.3. 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=<usuario>
postfix/cleanup[5940]: 7539434680: message-id=<20081231121556.753943\
4680@avatar>
postfix/qmgr[5935]: 7539434680: from=<usuario@avatar.doesntexist.org\
>, size=306, nrcpt=1 (queue active)
postfix/smtp[5942]: 7539434680: to=<unacuenta@gmail.com>, delay=3.1,\
delays=0.04/0.06/1.7/1.3, dsn=2.0.0, status=sent (250 2.0.0 OK 1230\
7259715sm2551300eyf.47)
postfix/qmgr[5935]: 7539434680: removed
```

En el caso de que tuviéramos una dirección IP dinámica, al enviar un mensaje a determinados servidores de correo (hotmail por ejemplo), aparecerían registros como los siguientes:

```
postfix/pickup[6804]: 09B0634680: uid=1000 from=<usuario>
postfix/cleanup[6810]: 09B0634680:message-id=<20081231154700.09B0634\
680@avatar>
postfix/qmgr[6802]: 09B0634680: from=<usuario@avatar.doesntexist.org\
>, size=307, nrcpt=1 (queue active)
postfix/smtp[6812]: 09B0634680: to=<una@hotmail.com>,relay=mx2.hotma\
il.com[65.54.244.40]:25, delay=1.3, delays=0.03/0.04/0.92/0.3, dsn=5\
.0.0, status=bounced (host mx2.hotmail.com[65.54.244.40] said: 550 D\
Y-001 Mail rejected by Windows Live Hotmail for policy reasons. We g\
enerally do not accept email from dynamic IP's as they are not typic\
ally used to deliver unauthenticated SMTP e-mail to an Internet mail\
server. http://www.spamhaus.org maintains lists of dynamic and resi\
dential IP addresses. If you are not an email/network admin please c\
```

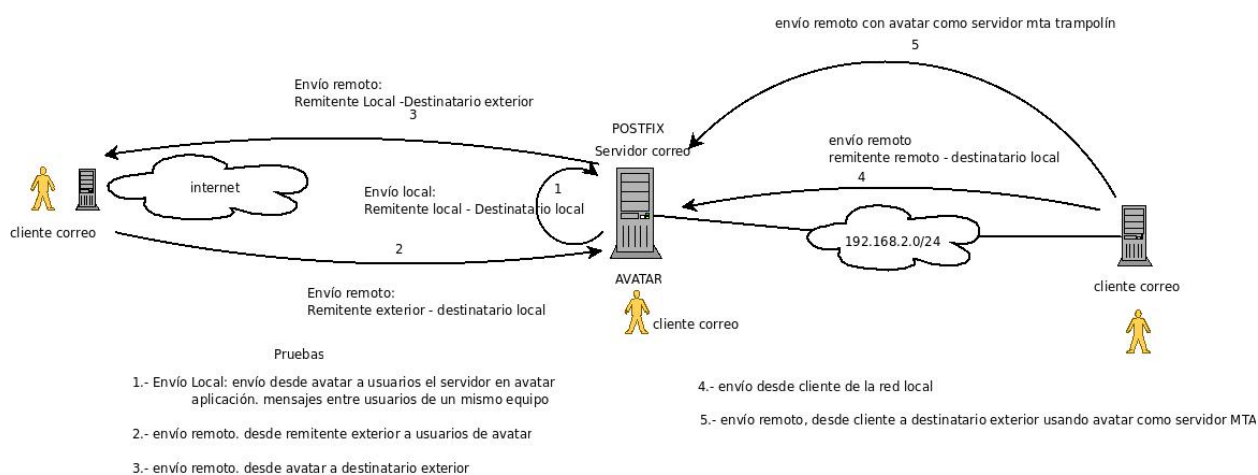


```
ontact your E-mail/Internet Service Provider for help. Email/network\
admins, please visit http://postmaster.live.com for email delivery \
information and support (in reply to MAIL FROM command))
postfix/smtp[6812]: 09B0634680: lost connection with mx2.hotmail.com\
[65.54.244.40] while sending RCPT TO
```

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, en este caso una solución es utilizar como smarthost un servidor SMTP en el que tengamos una cuenta, en la sección 5 se explica con detalle la forma de hacerlo con el servidor smtp.gmail.com.

## 4.5. Avatar como servidor de correo de los clientes de nuestra red

A la figura anterior le añadimos dos situaciones más:



El objetivo de este apartado es la configuración en equipos cliente de nuestra red para posibilitar el envío de correo a los usuarios.

### 4.5.1. Envío desde cliente a usuarios de avatar

Usaremos como cliente, en primer lugar, una conexión telnet (poco vistosa y nada usada por los usuarios, pero muy interesante para entender los pasos que sigue el protocolo SMTP (y otros) y para un administrador de redes):



```

u1-ubuntu-profe@ubuntu-profe:~$ telnet avatar.doesntexist.org 25
Trying 192.168.2.1...
Connected to avatar.
Escape character is '^]'.
220 hola avatar.doesntexist.org ESMTP Postfix (Debian/GNU)
ehlo ClientUbuntu
250-avatar.doesntexist.org
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: usuario-x@avatar.doesntexist.org
250 2.1.0 Ok
rcpt to: alumno@avatar.doesntexist.org
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
subject: Envío desde cliente a través de comandos
date: 17 Abril 2010
Este correo es un ejemplo enviado desde un equipo de la MZ a un usuario
del dominio avatar.doesntexist.org
.
250 2.0.0 Ok: queued as 6C4A26975

```

En la figura anterior observa los pasos del protocolo SMTP, para conocer más detalles puedes leer el anexo 8.

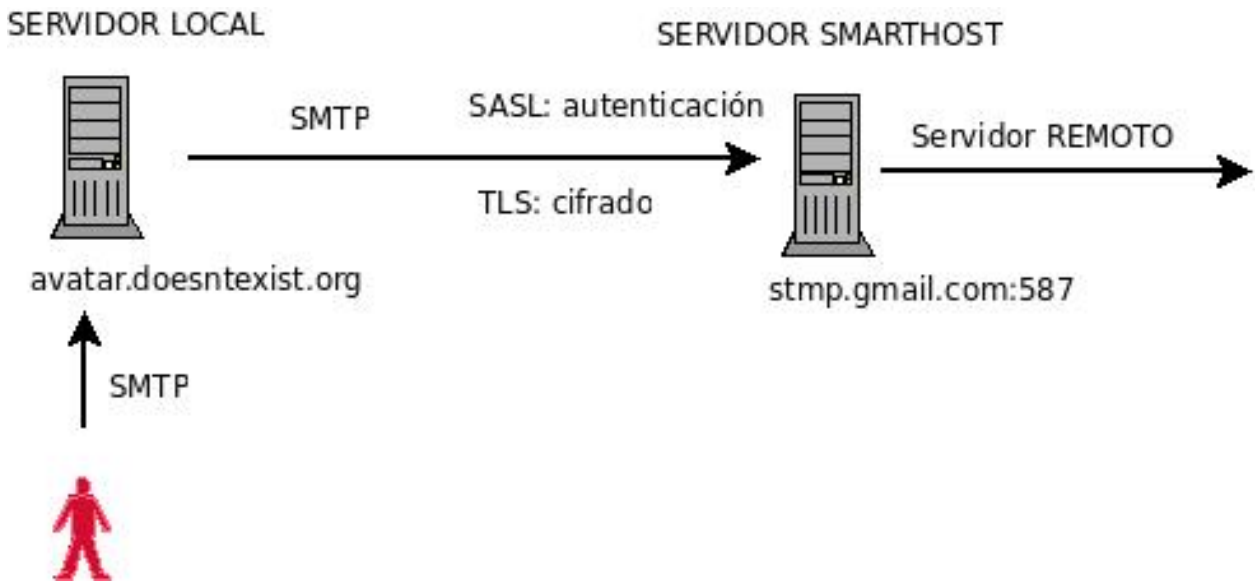
De forma totalmente equivalente se puede hacer configurando un cliente gráfico en cliente, en nuestro caso utilizaremos Evolution, en el que creamos una nueva cuenta:

The image shows two screenshots of the 'Editor de cuentas' (Account Editor) dialog box in Evolution. The left screenshot shows the 'Identidad' (Identity) tab, where the user enters the email address 'alumno@avatar.doesntexist.org', the full name 'u1-ubuntu-profe', and the email address 'alumno@avatar.doesntexist.org'. The right screenshot shows the 'Envío de correo' (Outgoing Mail) tab, where the server type is set to 'SMTP', the server address is '192.168.2.1', and the security is set to 'Sin cifrado' (No encryption). The authentication type is set to 'PLAIN'.

#### 4.5.2. Envío desde cliente a direcciones de Internet

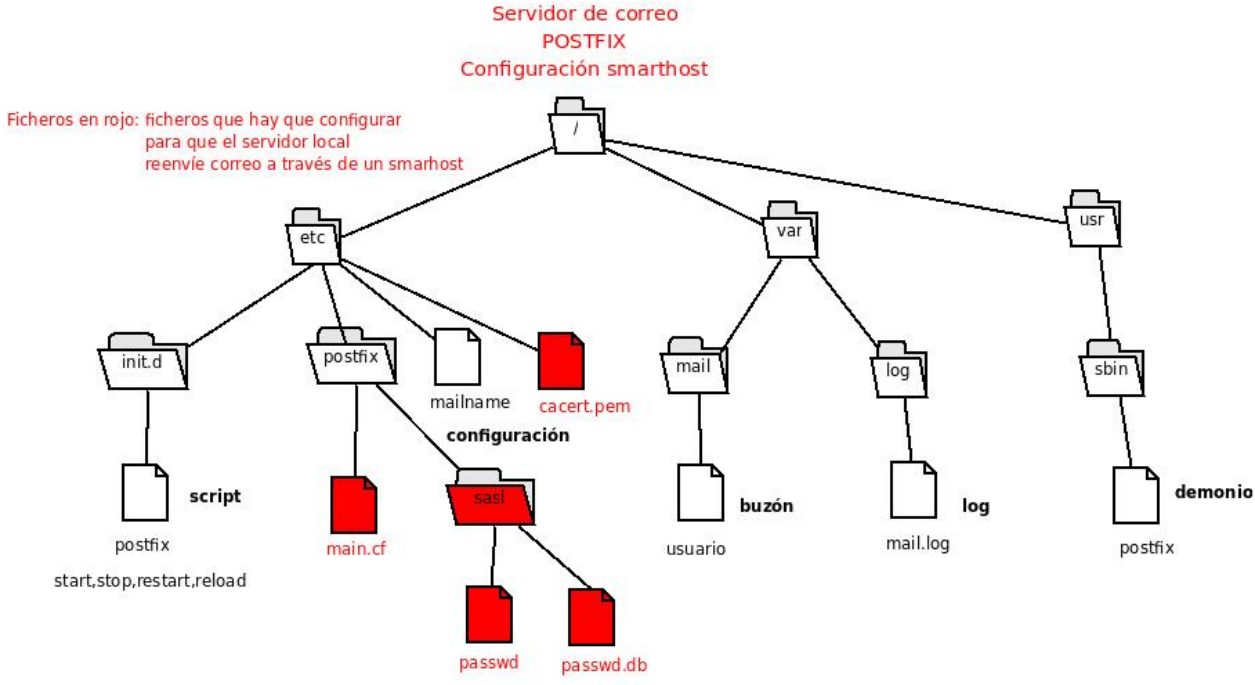
Para poder enviar correo a través de avatar, hay que abrir la retransmisión en avatar, en este caso especificando la dirección IP de los equipos a los que se permite enviar correo mediante la directiva mynetworks, a la que habrá que añadir la dirección de la red, 192.168.2.0/24.

# 5. Configuración de Postfix a través de un *relay host* autenticado



En la figura anterior se observa que el usuario envía correo vía SMTP usando Avatar como servidor de correo local. En nuestro caso, utilizaremos gmail como smarthost, pero puede utilizarse cualquier servidor SMTP externo al que se tenga acceso, en el caso de gmail la conexión debe ser autenticada mediante SASL y cifrada con TLS.

Para tener una visión global de los ficheros a configurar, usa esta figura, destacándose en rojo aquellos que serán objeto de modificaciones:



## 5.1. 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 Equifax) y autenticada, para lo que utilizaremos un nombre de usuario (dirección de correo) y contraseña del servicio.



## 5.2. Configuración de main.cf

Tenemos que editar el fichero y añadir las siguientes líneas:

```

                                     /etc/postfix/main.cf
35 relayhost = [smtp.gmail.com]:587

```

Donde indicamos el nombre del equipo que retransmitirá nuestros 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*)<sup>4</sup>.

```
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.

## 5.3. Datos de autenticación

Creemos el fichero /etc/postfix/sasl/passwd con el siguiente contenido:

```

                                     /etc/postfix/sasl/passwd
1 [smtp.gmail.com]:587 unacuenta@gmail.com:unacontraseña

```

Y lo protegemos adecuadamente con:

```
avatar:~# chmod 600 /etc/postfix/sasl/passwd
```

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

```
avatar:~# postmap /etc/postfix/sasl/passwd
```

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

## 5.4. Utilización del certificado adecuado

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

```
avatar:~# cat /etc/ssl/certs/Equifax_Secure_CA.pem >> /etc/postfix/cacert.pem
```

si no existiese el fichero con el certificado de Equifax o de otras autoridades certificadoras, deberemos instalar previamente el paquete ca-certificates.

<sup>4</sup>El puerto 25/TCP se reserva para comunicación entre dos servidores de correo y aquí estamos actuando como un cliente de correo.



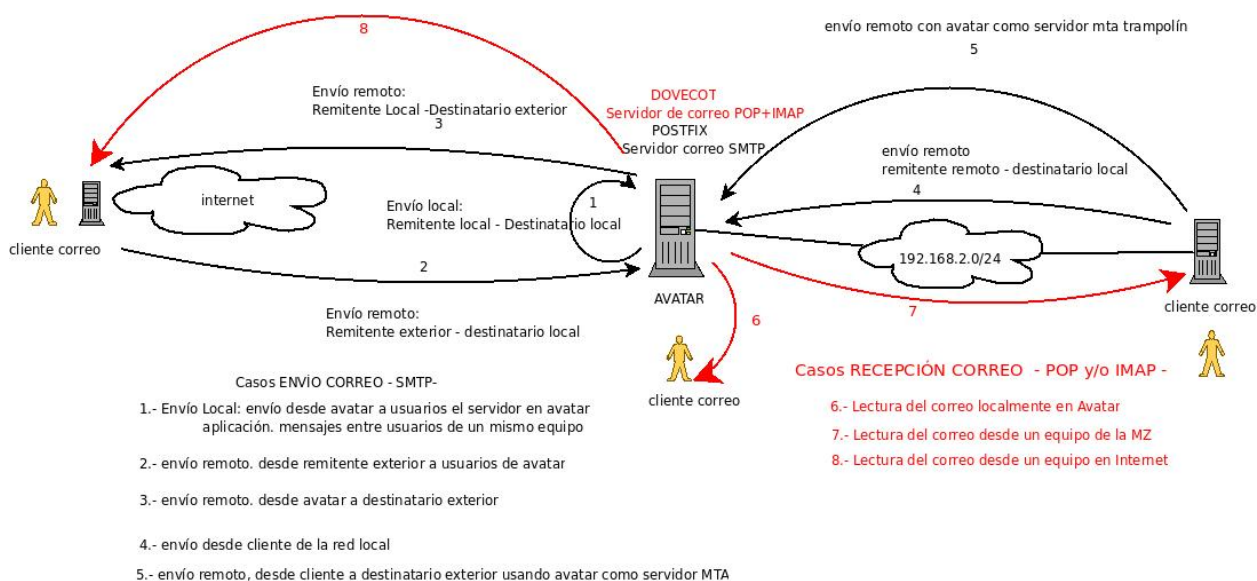
## 5.5. Prueba de funcionamiento

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=<usuario>
postfix/cleanup [6786]: 6AFF534680: message-id=<20081231154524.6AFF5346\
80@avatar>
postfix/qmgr [5935]: 6AFF534680: from=<usuario@avatar.doesntexist.org>,\
size=310, nrcpt=1 (queue active)
postfix/smtp [6788]: 6AFF534680: to=<unacuenta@hotmail.com>, relay=smtp.g\
mail.com [66.249.93.111]:587, delay=2.8, delays=0.04/0.02/1.2/1.6, dsn=\
2.0.0, status=sent (250 2.0.0 OK 1230738538 34sm19633915ugh.10)
postfix/qmgr [5935]: 6AFF534680: removed
```

## 6. Dovecot POP e IMAP

Una vez conseguido el envío de correo a usuarios de nuestro dominio local (casos 1, 2 y 4) y a usuarios de otros dominios (casos 3 y 5 con ayuda del smarthost), nos queda pendiente la recepción del correo dirigido a usuarios de nuestro dominio avatar.doesntexist.org (o avatar.example.com).

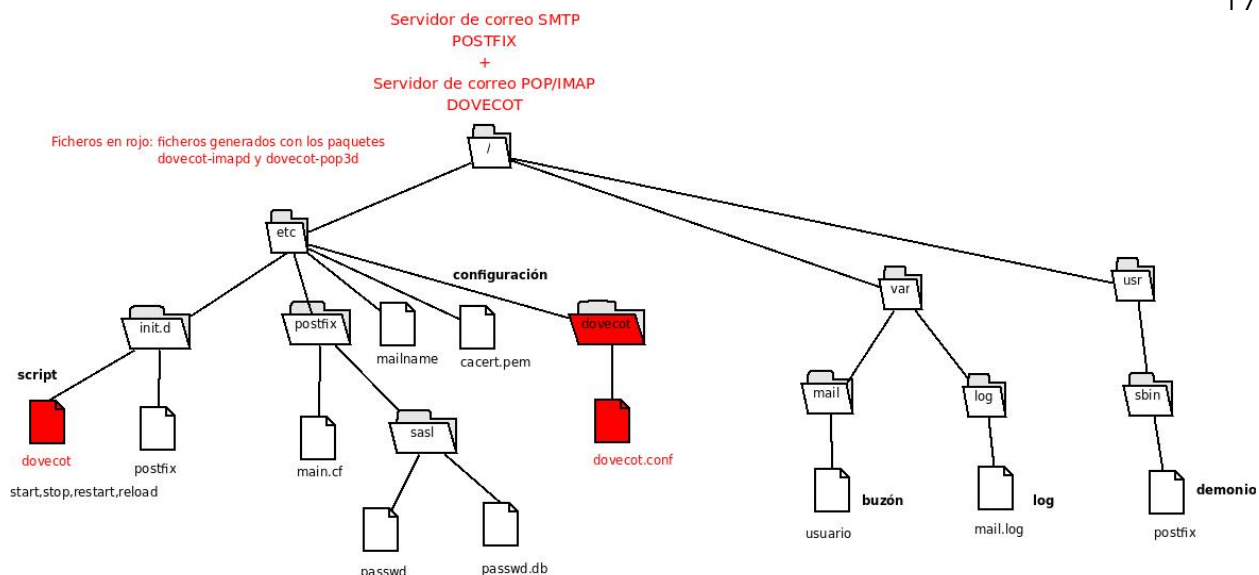


Leeremos el correo desde el propio servidor Avatar, siendo éste el caso 6 de la figura anterior, a continuación haremos la lectura desde los equipos clientes de nuestra red (caso 7), y por último leeremos el correo desde fuera de nuestra red, desde Internet (caso 8). En definitiva, cuando se envíe un correo a un usuario de avatar.doesntexist.org, éste podrá acceder a su correo desde la propia red local (sentado frente a Avatar o en cualquier equipo de la red), e incluso desde otro puesto en Internet.

Los protocolos de lectura de correo a configurar son POP3 e IMAP. Conseguiremos este objetivo gracias a Dovecot, que además puede configurarse para un acceso cifrado, POP3s y IMAPs.







## 6.1. Instalación de dovecot IMAP

Para instalar el servidor dovecot imap hay que hacer:

```
avatar:~# 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:

```
avatar:~# 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

La instalación básica de dovecot incluye la creación de un certificado para la conexión cifrada con TLS, este certificado autofirmado se ubica en /etc/ssl/private/dovecot.pem, pero se puede sustituir de forma trivial por cualquier otro certificado que se disponga para el servidor.

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

Es habitual que los usuarios del servicio de correo no sean usuarios locales, sino que se encuentren en un directorio LDAP o en una base de datos relaciones, sin embargo, en este documento por simplificar vamos a utilizar usuarios locales, por lo que deberemos modificar la siguiente línea del fichero de configuración de dovecot:

```
/etc/dovecot/dovecot.conf
```

```
230 mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

para que busque el correo en el directorio /var/mail y lo almacene posteriormente en formato mbox en la cuenta del usuario.

## 6.2. Pruebas de funcionamiento

Utilizamos de nuevo el cliente de correo evolution y configuramos el apartado de recepción de correo con los parámetros adecuados (en la imagen se ve que se ha seleccionado cifrado

con TLS, pero podemos probar de las dos formas):

Si la conexión se realiza sin cifrar aparecerá el siguiente registro en el fichero `/var/log/mail.log`:

```
dovecot: imap-login: Login: user=<usuario>, method=PLAIN, rip=192.168.\
2.2, lip=192.268.2.1, secured
```

Si por el contrario la conexión se realiza utilizando una conexión cifrada con TLS, en el cliente de correo habrá que aceptar el certificado autofirmado de dovecot y aparecerá el siguiente registro en `/var/log/mail.log`:

```
dovecot: imap-login: Login: user=<usuario>, method=PLAIN, rip=192.168.\
2.2, lip=192.168.2.1, TLS
```

### 6.3. Dovecot POP

Instalamos el paquete mediante:

```
avatar:~# 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`:

```
avatar:~# 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 y no es necesario realizar ninguna nueva modificación en dovecot.

En cualquier caso, puesto que el siguiente paso es configurar un webmail, es importante tener activo el protocolo IMAP, ya que un webmail no es más que un cliente IMAP local que ofrece una interfaz web al usuario.



Figura 2: Página de ingreso de squirrelmail

## 7. Squirrelmail

La consulta de correo desde un equipo exterior está solucionada con la instalación de los servidores POP e IMAP, pero para que nuestros usuarios puedan enviar correo a través del servidor postfix (que postfix retransmita sus mensajes) deberíamos configurar la autenticación de usuarios, por ejemplo con SASL y TLS, pero sería algo más complicado y no tiene cabida en un documento como éste. Existe una solución alternativa que es la instalación de un webmail, ya que si se instala en el mismo equipo que el mta o en un equipo con dirección IP conocida, se puede garantizar la retransmisión de correo sin perder seguridad.

Hay varios webmail libres que podemos instalar (squirrelmail, roundcube, bluemamba, ilohamail, horde, openwebmail, ...), aquí presentamos la instalación de uno de los más sencillos, squirrelmail:

```
avatar:~# apt-get install squirrelmail
```

que si no tenemos instalado apache2 o php5 nos los instalará, además de algún otro paquete adicional.

Squirrelmail no es más que un cliente IMAP/SMTP escrito en PHP y que se ejecuta normalmente en el mismo equipo que está el MTA, por lo que el envío de correo por SMTP está garantizado sin necesidad de incluir ninguna configuración extra.

El paquete squirrelmail incluye el fichero `/texttt/etc/squirrelmail/apache.conf` que habrá que añadir al fichero de configuración de apache que tengamos y luego reiniciar el servicio:

```
avatar:~# /etc/init.d/apache2 restart
```

Para acceder al webmail, abrimos nuestro navegador y escribimos:

```
http://avatar.example.com/squirrelmail/
```

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

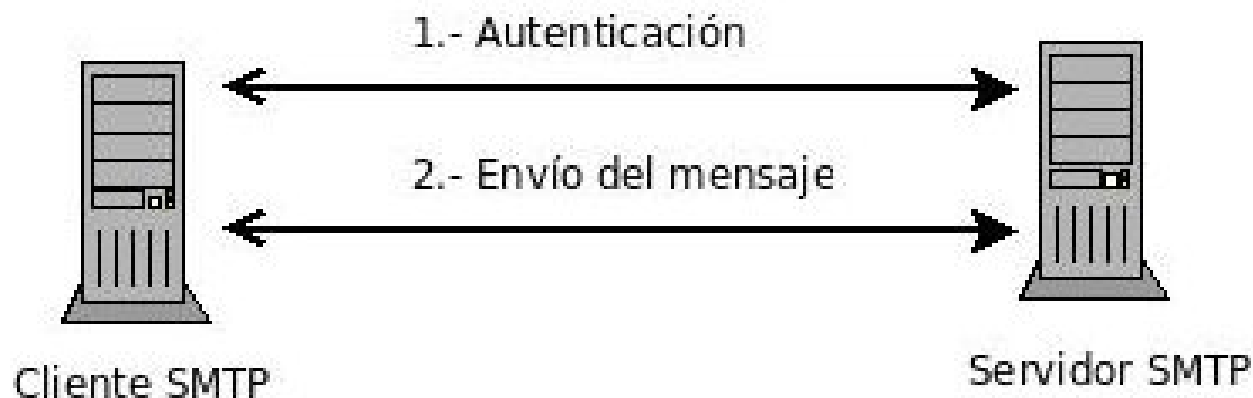
Si queremos modificar la configuración de squirrelmail, podemos hacerlo a través del programa:

```
avatar:~# /etc/squirrelmail/conf.pl
```



## 8. Anexo: SMTP. Protocolos y comandos

### 8.1. Esquema general



### 8.2. Fases en el envío de un mensaje de correo

- Fase de autenticación (puede haber otra si la sesión es cifrada). El cliente lanza los comandos siguientes para indicar qué usuario envía el correo, y a quién va dirigido. En nuestro ejemplo el cliente no llega a autenticarse al no estar configurado el servidor de correo para ello, tan sólo se intercambian estos mensajes.

- EHLO o HELO "cadena presentándose el cliente ante el servidor"
- MAIL FROM: "dirección de correo del remitente"
- RCPT TO: "dirección de correo del destinatario"

Una vez autenticado hay que componer el mensaje y enviar

- Fase de envío del mensaje. El cliente lanza la orden DATA y el servidor responde indicando "354 End data with <CR> <LF>. <CR> <LF>", lo que quiere decir que cuando el cliente finalice el mensaje y desee enviarlo debe escribir un punto y dar un retorno de carro, es decir, una vez a la tecla intro.

A continuación el cliente lanza las cadenas:

- From: "dirección del remitente" + SALTO DE LÍNEA (ie intro)
- To: "dirección del destinatario" + SALTO DE LÍNEA (ie intro)
- Cc: "dirección del destinatario" para tener una copia + SALTO DE LÍNEA (ie intro)
- Bcc: "dirección del destinatario" para tener una copia ciega
- Date: "fecha" + SALTO DE LÍNEA (ie intro)
- Subject: "asunto" + SALTO DE LÍNEA (ie intro)
- MIME-Versión: "valor de la versión de MIME usada" + SALTO DE LÍNEA (ie intro)
- Otras cabeceras + SALTO DE LÍNEA (ie intro)
- DOS SALTOS DE LÍNEAS
- Escribe el mensaje en varias líneas
- DOS SALTOS DE LÍNEAS, y en el segundo escribe "." para finalizar el mensaje, y el cliente lo envía al servidor

