

Servidores de correo electrónico con Postfix



Marco Antonio Manzo
amnesiac@perl.org.mx

<http://www.unixmonkeys.com/amnesiac/>

16-Jun-2005



Una pequeña vista previa

+ ¿Qué es un MTA?

- El cartero (*postino*)

+ ¿Qué nos ofrece?

- Paz con los vecinos
- Excelente seguridad 24/7
- Muy ordenado para trabajar
- Si no lo pelan se pone mas violento
- Entorno seguro, es decir me pueden encerrar (*chroot*)
- Sencilla instalación
- Se acopla de manera sencilla al trabajo en grupo (*filosofía UNIX*)



Y un poco mas en serio...

➤ Ahora si... ¿Qué nos ofrece realmente?

- Completa compatibilidad con sendmail
 - * alias
 - * /var/[spool]/mail
 - * NIS
 - * .forward
 - * user.lock files
- Excelente desempeño en servidores de alta carga
- Flexibilidad y robustez (viene de IBM por ahí)
- Una manera muy peculiar de entregar los correos
- *Chrooting/Sandboxing* o *Defensive mailing*
- Sencilla instalación (mailbox/Maildir)
- Soporte para trabajo en conjunto nativamente con procmail, diverso software AV, SpamAssassin, entre otros.
- VDA (*Virtual Delivery Agent*)
 - * Dominios virtuales
 - * Usuarios virtuales
 - * Quotas virtuales
 - * Todo esto también de manera nativa...
- Soporte para SASL/TLS
- y claro... LDAP



¿Seguridad?

- Sus procesos (demonios) corren utilizando un mínimo de privilegios e incluso (o sumándole) puede estar en un *sandbox*.
- Debido a su diseño, cualquier vulnerabilidad encontrada, no puede ser explotada sobre la red.
- Sigue 100% la filosofía UNIX, procesos separados y aislados para cada tarea. Y el sistema solo corre los procesos que necesita.
- Procesos no corren bajo privilegios de usuario, por lo tanto explotarlo por uso de archivos/señales entre padre e hijo, etc es imposible (muy poco probable).
- Confía o declínalo, su filosofía.
- No hay programas setuid, no hay variables de entorno, no hay programas de shell.



Algunas consideraciones

- ✚ Conocer mi dominio
 - Nombre a utilizar para la salida de correo (*FQDN*)
 - Dominios/hosts/usuarios locales a recibir mensajes.
 - A quién le vamos a permitir tener salida de correo (*relay*)
 - Y claro... conocer nuestra red
- ✚ Módulos externos corren por su cuenta
- ✚ Ganas de leer... les suena conocido esto? :P



Instalación básica

+ Necesitamos un grupo “maildrop”

+ Necesitamos un usuario “postfix”

+ ¿Qué pasará con sendmail?

Nada... le diremos al SO que utilice postfix como sendmail (*mailfer.conf*):

```
sendmail /usr/libexec/postfix/sendmail  
send-mail /usr/libexec/postfix/sendmail  
mailq /usr/libexec/postfix/sendmail  
newaliases /usr/libexec/postfix/sendmail
```

+ Nuestros archivos:

- main.cf
- master.cf
- aliases
- virtual



Instalación básica (cont...)

main.cf

```
command_directory = /usr/local/sbin
```

```
daemon_directory = /usr/local/libexec/postfix
```

```
mail_owner = postfix
```

```
myhostname = amnesiac.unixmonkeys.com
```

```
mydomain = unixmonkeys.net
```

```
myorigin = $myhostname
```

```
myorigin = $mydomain
```

```
#inet_interfaces = all
```

```
#inet_interfaces = $myhostname
```

```
#inet_interfaces = $myhostname, localhost
```

```
#mydestination = $myhostname, localhost.$mydomain
```

```
#mydestination = $myhostname, localhost.$mydomain $mydomain
```

```
#mydestination = $myhostname, localhost.$mydomain, $mydomain,
```

```
mail.$mydomain, www.$mydomain, ftp.$mydomain
```

```
my destination = $myhostname, localhost.$mydomain, unix-power.net
```



Instalación básica (cont...)

```
# mynetworks_style = class
# mynetworks_style = subnet
# mynetworks_style = host
# mynetworks = 192.168.0.0/24, 127.0.0.0/8
# mynetworks = $config_directory/mynetworks
#relay_domains = $mydestination, unix-power.net, otrodominio.com
#alias_maps = dbm:/etc/aliases
alias_maps = hash:/etc/aliases
#alias_maps = hash:/etc/aliases, nis:mail.aliases
#alias_maps = netinfo:/aliases
#alias_database = dbm:/etc/aliases
#alias_database = dbm:/etc/aliases
alias_database = hash:/etc/aliases (4.4BSD, LINUX)
#alias_database = hash:/etc/aliases, hash:/opt/majordomo/aliases
#home_mailbox = Mailbox
home_mailbox = Maildir/
mail_spool_directory = /var/mail
# mail_spool_directory = /var/spool/mail
```



Instalación básica (cont...)

```
#mailbox_command = /some/where/procmail

#mailbox_command = /some/where/procmail -a
"$EXTENSION"

#smtpd_banner = $myhostname ESMTP $mail_name

#smtpd_banner = $myhostname ESMTP $mail_name
($mail_version)

debug_peer_level = 2

@ Otras opciones

# user_relay = $user@other.host

# user_relay = $local@other.host

# user_relay = admin+$local

masquerade_domains = $mydomain

masquerade_exceptions = root
```



Instalación básica (cont...)

virtual

Dominios virtuales tipo sendmail:

user1@virtual.domain address1

user2@virtual.domain address2,address3

Nota: Este estilo requiere que el virtual.domain este listado en el apartado de mydestination en main.cf

Dominios virtuales tipo postfix:

virtual.domain anything

admin@virtual.domain admin

user1@virtual.domain address1

user2@virtual.domain address2

Nota: no requiere que virtual.domain este en mydestination.

Email forwarding

virtual.domain anything

admin@virtual.domain admin


user1@virtual.domain address1


user2@virtual.domain address2



Instalación básica (cont...)

Virtual Delivery Agent (VDA)

 Archivos necesarios:
main.cf
vmailbox

 Archivos necesarios:
main.cf
vmailbox

 main.cf
main.cf
vmailbox

```
virtual_mailbox_base = /var/vhosts
```

```
virtual_mailbox_maps =  
hash:/etc/postfix/vmailbox
```

```
virtual_minimum_uid = 1000
```

```
virtual_uid_maps = static:4000
```

```
virtual_gid_maps = static:4000
```

```
virtual_mailbox_limit = 100000000
```

```
virtual_maildir_extended = yes
```

```
virtual_mailbox_limit_inbox = yes
```

```
virtual_maildir_suffix = Maildir/
```

```
#transport_maps =  
hash:/etc/postfix/transport
```



Instalación básica (cont...)

vmailbox

micasita.com anything

user1@micasita.com /var/vhosts/user1/

user2@micasita.com /var/vhosts/user2/

user3@micasita.com /var/vhosts/user3

user4@micasita.com /var/vhosts/user4

transport en el caso de utilizar dominios virtuales

virtual1.domain virtual

virtual2.domain virtual

- *Ejemplo:*

virtual1.domain *(esto se pone para prevenir errores de acceso denegado para relay)*

virtual2.domain

test1@virtual1.domain test1

test2@virtual2.domain test2/



¿Qué faltó?

Iniciar postfix claro...

- postfix start
- postfix stop
- postfix reload

SASL o TLS

Y lo mas importante...



EDUCAR AL PATUX



GRACIAS!