

Apéndice: Resumen Configuración básica de Sendmail.

Autor: Joel Barrios Dueñas

Correo electrónico: [joelbarrios arroba linuxparatodos punto net](mailto:joelbarrios@linuxparatodos.punto.net)

Sitio de Red: <http://www.linuxparatodos.net/>

Jabber ID: darkshram@jabber.org

Usted puede contribuir financiando la elaboración de más documentos como éste haciendo aportaciones voluntarias y anónimas en:

HSBC (México)
Cuenta: 4007112287, Sucursal 00643
A nombre de: Joel Barrios Dueñas.

Creative Commons [Reconocimiento-NoComercial-CompartirIgual 2.1](#)

© 1999-2005 Linux Para Todos. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes: a) Debe reconocer y citar al autor original. b) No puede utilizar esta obra para fines comerciales. c) Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en [castellano](#). La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.

Este documento asume que el lector ya ha aplicado todos los parches de seguridad correspondientes para cyrus-sasl, sendmail e imap. Los procedimientos aplican para las versiones 3.0 y 4.0 de Red Hat Enterprise Linux, White Box Enterprise Linux y CentOS.

Software requerido.

- sendmail
- sendmail-cf
- dovecot (o bien imap si se utilizan derivados de Enterprise Linux 3.0 y anteriores)
- m4
- make
- cyrus-sasl
- cyrus-sasl-md5

- cyrus-sasl-plain

Procedimientos.

Instalación a través de yum.

Si se utiliza de CentOS 4.0 o White Box Enterprise Linux 4.0, el paquete `imap` es reemplazado por el paquete **dovecot**. De tal modo que se ejecuta lo siguiente:

```
yum -y install sendmail sendmail-cf dovecot m4 make cyrus-sasl  
cyrus-sasl-md5 cyrus-sasl-plain
```

Si se utiliza de CentOS 3.0 o White Box Enterprise Linux 3.0, el paquete `imap` es reemplazado por el paquete **dovecot**. De tal modo que se ejecuta lo siguiente:

```
yum -y install sendmail sendmail-cf imap m4 make cyrus-sasl cyrus-  
sasl-md5 cyrus-sasl-plain
```

Si acaso estuviese instalado, elimine el paquete `cyrus-sasl-gssapi`, ya que este utiliza el método de autenticación GSSAPI, mismo que requeriría de la base de datos de cuentas de usuario de un servidor Kerberos:

```
yum -y remove cyrus-sasl-gssapi
```

Instalación a través de Up2date

Si se utiliza de Red Hat Enterprise Linux 4.0, el paquete `imap` es reemplazado por el paquete **dovecot**. De tal modo que se ejecuta lo siguiente:

```
up2date -i sendmail sendmail-cf dovecot m4 make cyrus-sasl cyrus-  
sasl-md5 cyrus-sasl-plain
```

Si se utiliza de Red Hat Enterprise Linux 3.0, el paquete `imap` es reemplazado por el paquete **dovecot**. De tal modo que se ejecuta lo siguiente:

```
up2date -i sendmail sendmail-cf imap m4 make cyrus-sasl cyrus-sasl-  
md5 cyrus-sasl-plain
```

Si acaso estuviese instalado, elimine el paquete `cyrus-sasl-gssapi`, ya que este utiliza el método de autenticación GSSAPI, mismo que requeriría de la base de datos de cuentas de usuario de un servidor Kerberos:

```
rpm -e cyrus-sasl-gssapi
```

Alta de cuentas.

El alta de usuarios a través de este método será diferente a la manera tradicional, debido a que para utilizar el método de autenticación para SMTP, sendmail utilizará SASL. Por tal motivo, el alta de cuentas de usuario de correo deberá de seguir el siguiente procedimiento:

- Alta de la cuenta del usuario en el sistema, la cual se sugiere no deberá tener acceso a interprete de mandato alguno:

```
useradd -s /sbin/nologin fulano
```

- Asignación de contraseña en el sistema para permitir autenticar a través de POP3 o IMAP:

```
passwd fulano
```

- Si utiliza una versión de sendmail compilada contra SASL-2 (Red Hat Enterprise Linux 4.0, CentOS 4.0 o White Box Enterprise Linux 4.0), utilice el siguiente mandato:

```
saslpasswd2 fulano
```

- Si utiliza una versión de sendmail compilada contra SASL-1 (Red Hat Enterprise Linux 3.0, CentOS 3.0 o White Box Enterprise Linux 3.0), utilice el siguiente mandato:

```
saslpasswd fulano
```

Si va a utilizar autenticación, habilite e inicie el servicio de **saslauthd** del siguiente modo:

```
chkconfig saslauthd on  
service saslauthd start
```

Dominios.

Establecer dominios a administrar en:

```
/etc/mail/local-host-names
```

Ejemplo:

```
mi-dominio.com  
mail.mi-dominio.com  
mi-otro-dominio.com  
mail.mi-otro-dominio.com
```

Establecer dominios permitidos para poder enviar correo en:

```
/etc/mail/relay-domains
```

Por defecto, no existe dicho fichero, hay que generarlo. Para fines generales tiene el mismo contenido de `/etc/mail/local-host-names` a menos que se desee excluir algún dominio en particular.

Control de acceso

Definir lista de control de acceso en:

```
/etc/mail/access
```

Incluir solo las IPs locales del servidor, y la lista negra de direcciones de correo, dominios e IPs denegadas. Considere que cualquier IP que vaya acompañada de RELAY se le permitirá enviar correo sin necesidad de autenticar, lo cual puede ser útil si se utiliza un Webmail en otro servidor. Ejemplo:

```
localhost.localdomain      RELAY
localhost                   RELAY
127.0.0.1                   RELAY
192.168.1.254               RELAY
# Otros servidores de correo en la LAN
192.168.1.253               RELAY
192.168.1.252               RELAY
#
# Lista negra
usuario@molesto.com         REJECT
productoinutil.com.mx      REJECT
10.4.5.6                    REJECT
#
# Bloques de Asia Pacific Networks, ISP desde el cual se emite la
mayor
# parte del Spam del mundo.
# Las redes involucradas abarcan Australia, Japón, China, Korea,
Taiwan,
# Hong Kong e India por lo que bloquear el correo de dichas redes
significa
# cortar comunicación con estos países, pero acaba con entre el 60%
y 80%
# del Spam.
222                          REJECT
221                          REJECT
220                          REJECT
219                          REJECT
218                          REJECT
212                          REJECT
211                          REJECT
210                          REJECT
203                          REJECT
```

```
202 REJECT
140.109 REJECT
133 REJECT
61 REJECT
60 REJECT
59 REJECT
58 REJECT
```

Alias de la cuenta de root.

No es conveniente estar autenticando la cuenta de root a través de la red para revisar los mensajes originados por el sistema. Se debe definir alias para la cuenta de root a donde re-direccionar el correo en:

```
/etc/aliases
```

Ejemplo:

```
root: fulano
```

Configuración de funciones de Sendmail.

Editar `/etc/mail/sendmail.mc` y deshabilitar/habilitar funciones:

- I. Si se utiliza la siguiente línea, habilitada por defecto, se permitirá realizar autenticación a través del puerto 25 por cualquier método, incluyendo PLAIN, el cual se realiza en texto simple. Esto implica cierto riesgo de seguridad.

```
define(`confAUTH_OPTIONS', `A')dnl
```

Si comenta la anterior línea con `dnl`, y se utiliza en cambio la siguiente línea, se deshabilita la autenticación por de texto simple en conexiones no seguras (TLS), de modo tal que solo se podrá autenticar a través de métodos que utilicen ciframiento, como sería CRAM-MD5 y DIGEST-MD5.

```
define(`confAUTH_OPTIONS', `A p')dnl
```

- II. Si se desea utilizar SMTP autenticado para equipos no incluidos dentro de `/etc/mail/access`, se requieren des-comentar las siguientes dos líneas, eliminando el `'dnl'` que les precede:

```
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-
MD5 LOGIN PLAIN')dnl
```

- III. Deshabilitar las funciones que definen trabajar sobre la interfaz 127.0.0.1 y recibir correo de dominios inexistentes precediendo con `'dnl'` en las siguientes líneas:

```
dn1 DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dn1
```

```
dn1 FEATURE(`accept_unresolvable_domains')dn1
```

IV. Habilitar las siguientes líneas y adaptar valores para definir la máscara que utilizará el servidor:

```
MASQUERADE_AS(`mi-dominio.com')dn1
```

```
FEATURE(masquerade_envelope)dn1
```

```
FEATURE(masquerade_entire_domain)dn1
```

Si va a administrar múltiples dominios, no utilice los parámetros anteriores.

V. Añadir al final de `sendmail.mc` un parámetro que defina que `mi-dominio.com` se trata de un dominio local. Note que no debe haber espacios entre `Cw` y `mi-dominio.com`, y que `Cw` lleva `C` mayúscula.

```
Cwmi-dominio.com
```

Control del Spam a través de DNSBLs.

Si se desea cargar *listas negras* para mitigar el Spam, pueden añadirse las siguientes líneas justo arriba de `MAILER(smtp)dn1`:

```
FEATURE(dnsbl, `relays.ordb.org', `Rejected - see http://relays.ordb.org/')dn1
```

```
FEATURE(dnsbl, `bl.spamcop.net', `Rejected - see: http://spamcop.net/')dn1
```

```
FEATURE(dnsbl, `sbl-xbl.spamhaus.org', `Rejected - see http://www.spamhaus.org/XBL/')dn1
```

```
FEATURE(dnsbl, `dnsbl.njabl.org', `Rejected - see http://dnsbl.njabl.org')dn1
```

```
FEATURE(dnsbl, `dnsbl.sorbs.net', `Rejected - see http://dnsbl.sorbs.net')dn1
```

Protocolos para acceder hacia el correo.

Habilitar protocolos de lectura de correo:

Si utiliza Red Hat Enterprise Linux 4.0, CentOS 4.0 o White Box Enterprise Linux 4.0, el paquete `imap` es reemplazado por `dovecot`, el cual funciona como otros servicios. Se debe editar el fichero `/etc/dovecot.conf` y habilitar los servicios de `imap` y/o `pop3` del siguiente modo (de modo predefinido solo está habilitado `imap`):

```
protocols = imap pop3
```

El servicio se agrega al arranque del sistema y se inicializa del siguiente modo:

```
/sbin/chkconfig dovecot on  
/sbin/service dovecot start
```

Si utiliza Red Hat Enterprise Linux 3.0, CentOS 3.0 o White Box Enterprise Linux 3.0, el procedimiento utilizará el paquete imap, el cual solo requiere un simple mandato para activar el servicio.

```
/sbin/chkconfig imap on  
/sbin/chkconfig ipop3 on
```

Reiniciando servicio.

Para reiniciar servicio de Sendmail solo bastará ejecutar:

```
/sbin/service sendmail restart
```

Probar servidor enviando/recibiendo mensajes con CUALQUIER cliente estándar de correo electrónico con soporte para POP3/IMAP/SMTP con soporte para autenticar a través de SMTP utilizando los métodos DIGEST-MD5 o CRAM-MD5.

Para depurar posibles errores, se puede examinar el contenido de la bitácora de correo del sistema en `/var/log/maillog` del siguiente modo:

```
tail -f /var/log/maillog
```

Linux Para Todos

<http://www.linuxparatodos.net/geeklog/staticpages/index.php?page=15-como-sendmail-apendice-01>