Configuración de un servidor de Correo

Funcionamiento general de un servidor de Correo Electrónico
Un servidor de correo electrónico funciona de forma similar a un enrutador, sólo que en lugar de paquetes, se ocupa exclusivamente del tráfico SMTP (*Simple Mail Transfer)*

- Acepta un mensaje entrante.
- Comprueba las direcciones del mensaje.
- Si son direcciones locales, almacena el mensaje para recuperarlo.
- Si son direcciones remotas, envía el mensaje.
- Si encuentra que el mensaje no se puede enviar (la cuenta ha excedido su cuota o el usuario ya no existe), devuelve un mensaje de error al remitente que explica el problema.

Protocolos

SMTP
El Simple Message Transfer Protocol se emplea para enviar mensajes de correo electrónico entre servidores. En muchos casos, el programa cliente de correo electrónico remite un nuevo mensaje al servidor usando también SMTP.
POP
El Post Office Protocol permite a los programas clientes de correo electrónico extraer los mensajes pendientes en las casillas de correo del usuario para que éste los pueda visualizar.
IMAP
El Internet Message Access Protocol, al igual que POP, permite a los programas clientes de correo electrónico extraer los mensajes pendientes en las casillas de correo del usuario para que éste los pueda visualizar. Tiene características adicionales a las proporcionadas por POP

DNS
El Domain Name System permite que los mensajes de correo electrónico sean dirigidos al servidor correspondiente en el Internet. En particular, a partir de una dirección de correo electrónico de destino en un mensaje, se puede encontrar la dirección IP del computador que debe recibir dicho mensaje.

Aplicaciones necesarias para el funcionamiento del servicio de correo electrónico
Los sistemas de correo electrónico se componen de varias partes denominadas agentes. Cada agente se responsabiliza de una porción lógica del sistema. Existen cinco agentes:
MUA (*Mail User Agent*, Agente de Usuario de Correo),
MTA (*Mail Transfer Agent*, Agente de Transferencia de Correo),
MDA (*Mail Delivery Agent*, Agente de Entrega de Correo),
MSA (*Mail Submission Agent*, Agente de Registro de Correo),
MAA (Mail Access Agent, Agente de Acceso al Correo).

MUA
El MUA o cliente de correo, es el programa que le va a permitir a un usuario (como mínimo) leer y escribir mensajes de correo electrónico. Típicamente, esto se hace a través de una interfaz que puede ser gráfica (Ximina Evolution, Outlook, Webmail, etc) o en texto (Pine, Mutt, etc). Debe tener funcionalidades de agente de acceso a correo para permitir la recuperación de correo a través

de POP o IMAP y debe tener funcionalidad MIME (*Multipurpose Internet Mail Extensions*, Extensiones de Correo de Internet Multipropósito).
La funcionalidad MIME es la habilidad para leer o incluir texto no ASCII (texto plano) en el cuerpo de un mensaje. MIME especifica formas de incluir otra clase de documentos incluyendo imágenes y otros archivos binarios. Esta habilidad depende tanto del MUA como de la existencia de otras aplicaciones capaces de entender el formato del archivo y que puedan ser llamadas o cargadas por el MUA para su visualización.

MTA
El MTA se encarga de la transferencia de los mensajes de correo electrónico entre las máquinas que usan el protocolo SMTP. Un mensaje puede pasar por varios MTA hasta llegar al destino final. Los MTA escuchan en los puertos 25 y 587. Típicamente se contactan el uno al otro usando el puerto 25. Los agentes de registro usan el puerto 587. A la transferencia de correo electrónico para un cliente se denomina reenvío (o envío). Sendmail es un MTA

MDA
Los agentes MTA utilizan programas MDA (*Mail Delivery Agent*, Agente de Entrega de Correo) para entregar el correo electrónico al buzón de un usuario concreto. En muchos casos, el agente MDA es realmente un LDA (*Local Delivery Agent*, Agente de entrega local), como bin/mail o Procmail. Cualquier programa que gestione realmente un mensaje para entregarlo al punto donde lo leerá un agente MUA se puede considerar un agente MDA. Los agentes MDA no transportan mensajes entre sistemas ni actúan como interfaz para el usuario final.
Muchos usuarios no utilizan directamente agentes MDA, porque sólo se necesitan agentes MTA y MUA para enviar y recibir correo. Sin embargo, algunos agentes MDA se pueden utilizar para ordenar los mensajes antes de que los lea el usuario, lo cual es de gran ayuda si recibe una gran cantidad de correo.

MSA
El MSA o Agente de Registro de Correo es un agente nuevo que divide la carga de trabajo del MTA en servicios con muchos usuarios y mejora el desempeño. La idea es que el agente de servicio se preocupe de las tareas relativas al direccionamiento, tomando cierta parte de la carga de trabajo del MTA primario. Éste simplemente puede confiar la validez de las direcciones cuando recibe un correo de agentes de registro conocidos. El MSA corrige direcciones, y arregla y reescribe encabezados. Procesa el correo de su propia cola y lo envía a un agente de transferencia local.

MAA
El MAA o Agente de Acceso al Correo es usado para recuperar el buzón de mensajes de un servidor de correo electrónico. Ejemplos de MAAs son el protocolo IMAP y POP.

Sendmail

Configuración

En el directorio `/etc/mail` se encuentran los archivos principales de configuración de sendmail. El archivo `sendmail.cf` contiene la configuración del servidor que atiende conexiones en el puerto 25, este archivo no se edita directamente, en su lugar se edita el archivo `sendmail.mc` y se crea la configuración de este mediante la macro: **m4**

Archivo /etc/mail/sendmail.mc

`sendmail.mc` es el archivo de configuración para sendmail.cf

```
divert(-1)dnl
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
VERSIONID(`setup for Red Hat Linux')dnl
OSTYPE(`linux')dnl
define(`confLOG_LEVEL’,`15’)
dnl define(`SMART_HOST',`smtp:your.provider.com')
define(`confDEF_USER_ID',``8:12'')dnl
define(`confTRUSTED_USER', `smmsp')dnl
dnl define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT', `1m')dnl
define(`confTRY_NULL_MX_LIST',true)dnl
define(`confDONT_PROBE_INTERFACES',true)dnl
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
define(`UUCP_MAILER_MAX', `2000000')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn, restrictqrun')
dnl
define(`confAUTH_OPTIONS', `A')dnl
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN
PLAIN')dnl
define(`confTO_IDENT', `0')dnl
FEATURE(`no_default_msa',`dnl')dnl
FEATURE(`smrsh',`/usr/sbin/smrsh')dnl
FEATURE(`mailertable',`hash -o /etc/mail/mailertable.db')dnl
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
FEATURE(local_procmail,`',`procmail -t -Y -a $h -d $u')dnl
FEATURE(`access_db',`hash -T<TMPF> -o /etc/mail/access.db')dnl
FEATURE(`blacklist_recipients')dnl
EXPOSED_USER(`root')dnl
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
FEATURE(`relay_based_on_MX’)
```

```
LOCAL_DOMAIN(`localhost.localdomain')dnl
MASQUERADE_AS(`dominio.com.uy')dnl
FEATURE(masquerade_envelope)dnl
FEATURE(dnsbl, `blackholes.mail-abuse.org', `Rejected - see www.mail-
abuse.org/rbl/')dnl
FEATURE(dnsbl, `dialups.mail-abuse.org', `Rejected - see www.mail-
abuse.org/dul/')dnl
FEATURE(dnsbl, `relays.mail-abuse.org', `Rejected - see work-rss.mail-
abuse.org/rss/')dnl
FEATURE(`delay_checks')dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
```

Opción de log

```
define(`confLOG_LEVEL',`13')
```

Los logs se anotan en `/var/log/maillog`, el número indica el nivel de anotación, cuanto mas grande, mas debug se anotara.

Para depurar la configuración es conveniente ejecutar en una terminal:

```
tail –f /var/log/maillog
```

Puerto SMTP

En sendmail viene por defecto configurado para aceptar sólo conexiones locales; es decir, no recibirá ningún mensaje que llegue desde el exterior por tanto hay que comentar la línea ingresando al principio de la línea la palabra dnl.

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

Nombre del dominio

```
MASQUERADE_AS(`dominio.com.uy')dnl
```

Opciones de autenticación

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.

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

Si comenta la anterior línea con dnl, y se utiliza en cambio la siguiente línea, se deshabilitará 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
```

Si se desea utilizar SMTP autenticado para equipos no incluidos dentro de /etc/mail/access, se requieren descomentar 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
```

Evitar el spam

Si se desea cargar listas negras para mitigar el Spam, pueden añadirse las siguientes líneas:

```
FEATURE(dnsbl, `blackholes.mail-abuse.org', `Rejected - see www.mail-
abuse.org/rbl/')dnl
FEATURE(dnsbl, `dialups.mail-abuse.org', `Rejected - see www.mail-
abuse.org/dul/')dnl
FEATURE(dnsbl, `relays.mail-abuse.org', `Rejected - see work-rss.mail-
```

```
abuse.org/rss/')dnl
```

Macro m4

Regenerar la configuración de sendmail.cf con la macro m4:

```
cd /etc/mail
m4 sendmail.mc > sendmail.cf
```

Una vez modificada la configuración hay que reiniciar el servicio.

```
service sendmail restart
```

Archivo /etc/hosts

Asegurémonos de que existan las siguientes líneas, y que tengan un contenido como este:

```
127.0.0.1 localhost
1.2.3.4 correo.dominio.com.uy  correo
```

Archivo local-host-names

Este archivo debe contener todos los nombres con los cuales se conoce al host servidor.
Como las direcciones son del estilo "`usuario@dominio.com.uy`", nuestro servidor debe asumir como suyos todos los mensajes dirigidos a "`@dominio.com.uy`".
Esto se consigue escribiendo "` dominio.com.uy`" en el archivo `/etc/mail/local-host-names`:

```
dominio.com.uy
```

Para que se utilice este archivo debe existir la siguiente línea en sendmail.mc

```
FEATURE(use_cw_file)dnl
```

Archivo /etc/mail/access

Permitir el relay a nuestros clientes

Asumiremos que las estaciones de nuestra organización están contenidas en la subset "1.2.3.0". En ese caso, añadiremos la siguiente línea al archivo aceptando con **RELAY** y negando con **REJECT**

```
20.20.128.              RELAY     #toda la subred
20.20.139.231           RELAY #UN HOST
usuario@molesto.com     REJECT
productoinutil.com.mx   REJECT
10.4.5.6                REJECT
```

Luego generaremos la versión indexada generando el archivo access.db:

```
cd /etc/mail
```

```
make
```

En sistemas distintos a RedHat habrá que usar (en vez de "make") el comando "makemap" con las opciones correspondientes:

```
cd /etc/mail
makemap hash access.db < access
```

Esta funcionalidad viene activada normalmente en la configuración proporcionada por RedHat.
Línea correspondiente en el archivo sendmail.mc

```
FEATURE(`access_db',`hash -T<TMPF> -o /etc/mail/access.db')dnl
```

En Fedora la orden make se ejecuta al iniciar el servicio sendmail.

Archivo /etc/mail/relay-domains

Contiene los dominios validos para enviar correo, este archivo no existe de forma predeterminada.

```
dominio.com.uy RELAY
```

Archivo /etc/sysconfig/network

El nombre del computador donde se ejecuta Sendmail debe corresponder a lo configurado en el DNS y el archivo hosts. Lamentablemente, la configuración de este parámetro varía de sistema en sistema. Por ejemplo, en RedHat, la configuración del hostname se efectúa en el archivo /etc/sysconfig/network en la variable HOSTNAME.

```
cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=correo.dominio.edu.uy
GATEWAY=172.192.12.1
```

Archivo /etc/aliases

Contiene los alias por los cuales se puede conocer a los usuarios. Una vez modificado este archivo se debe ejecutar el comando newaliases, para regenar los datos. Formato:

```
# Basic system aliases -- these MUST be present.
MAILER-DAEMON: postmaster
postmaster:    root
```

Archivo .forward

Al igual que el archivo de aliases, existe un archivo -opcional- por cada usuario. Si éste tiene un archivo `.forward` en su `${HOME}` sendmail interpreta éste como un fichero alias particular y lo procesa.

Archivo /etc/mail/submit.mc

En las últimas versiones de sendmail (8.12 o superiores) es usual que se configure el servidor para que se ejecute "dividido" en dos programas complementarios a fin de elevar la seguridad del sistema.
En este caso, el segundo proceso (client queue runner) es controlado mediante otro archivo : `/etc/mail/submit.cf` que tiene la configuración del sendmail que se usa para mandar mails de la propia máquina.

/etc/mail/submit.cf

```
divert(0)dnl
include(`/usr/share/sendmail-cf/m4/cf.m4')
VERSIONID(`linux setup for Red Hat Linux')dnl
define(`confCF_VERSION', `Submit')dnl
define(`__OSTYPE__',`')dnl
define(`_USE_DECNET_SYNTAX_', `1')dnl support DECnet
define(`confTIME_ZONE', `USE_TZ')dnl
define(`confDONT_INIT_GROUPS', `True')dnl
define(`confPID_FILE', `/var/run/sm-client.pid')dnl
define(`confDIRECT_SUBMISSION_MODIFIERS',`C')
FEATURE(`use_ct_file')dnl
FEATURE(`msp')
```

Configurar DNS

Configurar el DNS incluyen el registro para el servidor de correo:

```
correo    IN   A         20.20.142.104
@         IN   MX   10    correo
```

Consultar por el servidor de correo, para chequear la configuración.

nslookup -q=mx *dominio.com.uy*

Autentificación

El método de autentificación se basa en el software de `cyrus-sasl`, el demonio **`saslauthd`** debe estar corriendo, y para que certifique a los usuarios se debe existir el archivo `Sendmail.conf` en los directorios `/usr/lib/sasl2 y/usr/lib/sasl` con el siguiente contenido:

`pwcheck_method:saslauthd`

Iniciar sendmail

`service sendmail start`

`service saslauthd start`

Es conveniente automatizar el inicio de los servicios al inicio del sistema, para que cada uno se levante en el orden correspondiente.

```
chkconfig –-level 345 sendmail on
chkconfig –-level 345 saslauthd on
```

Usuarios de Sendmail

Los usuarios del sistema automáticamente son usuarios de sendmail.

Configurar servicios POP / IMAP

Primero hay que diferenciar entre un servidor SMTP y un servidor de POP3. Así a grandes rasgos podríamos decir que un servidor SMTP es el que se utiliza para que nosotros enviemos correo. Y un servidor POP3 es el que utilizamos para recoger el correo que nos han enviado. El servidor SMTP y POP3 podrían no estar en la misma máquina físicamente e incluso no estar incluidos en la misma aplicación.

Configuración para Centos RedHat

En Fedora Core 2 t RedHat AS 4 dependen del demonio cyrus-imapd, se deben instalar los paquetes **cyrus***.rpm.

Usuarios de Cyrus

Los usuarios no son los usuarios del sistema, se deben crear los usuarios y posteriormente sus buzones.

Comando saslpasswd2

El comando saslpaswd2 permite ingresar nuevos usuarios al servidor cyrus-imap, a diferencia de sendmail no son por defecto los usuarios del sistema.
En el momento de creación del usuario se solicita la contraseña.

SINTANXIS SASLPASSWD2 [–C|D] USER

Opciones	descripción
-c	nuevo usuario
-d	elimina usuario

Ejemplo

```
saslpasswd2 –c usr1
PASSWORD:
AGAIN (FOR VERIFICATION)
```

Comando sasldblistusers2

Listado de los usuarios ingresados.

Comando testsaslauthd

Permite testear la configuración

```
testsaslauthd -u usr1 -p contras -s pop3d
0: OK "Success."
```

Utilidad cyradm

Esta utilidad permite crear los buzones de los usuarios, debe ser invocada por un usuario administrador. El usuario administrador se define en el archivo

/etc/imapd.conf

```
configdirectory: /var/lib/imap
partition-default: /var/spool/imap
admins: cyrus root
sievedir: /var/lib/imap/sieve
sendmail: /usr/sbin/sendmail
hashimapspool: true
sasl_pwcheck_method: saslauthd
sasl_mech_list: PLAIN
tls_cert_file: /etc/pki/cyrus-imapd/cyrus-imapd.pem
tls_key_file: /etc/pki/cyrus-imapd/cyrus-imapd.pem
tls_ca_file: /etc/pki/tls/certs/ca-bundle.crt
```

```
cyradm --user usuario.administrador.cyrus  nombre.host
```

Ejemplo

```
cyradm --user root  correo
```

Orden para crear un buzón

```
correo.dominio.com.uy> cm user.usr3
```

Orden para consultar

```
correo.dominio.com.uy> lam user.usr1
usr1 lrswipcda
correo.dominio.com.uy> lam user.usr2
```

USR2 LRSWIPCDA

```
correo.dominio.com.uy>
```

Para terminar digite quit en el prompt

Levantar el servicio

```
service curys-imapd start
```

Se recomienda que este servicio se levante automáticamente al inicio del sistema.

```
chkconfig –-level 345 curys-imapd on
```

Comprobar POP3

Los servidores POP3 de correo escuchan el puerto 110 de TCP. Se puede comprobar el funcionamiento del correo en el servidor POP3 del proveedor desde una sesión 'telnet'.
Ejemplo:

```
telnet host104.univeritario.com.uy 110
Trying 20.20.142.104...
Connected to host104.
```

```
Escape character is '^]'.
+OK POP3 host104.univeritario.com.uy v2001.78rh server ready
```

Configuración de sendmail

Se debe configurar el archivo `/etc/mail/sendmail.mc` para que sendmail trabaje con cyrus. Ejemplo

```
divert(-1)dnl
include(`/usr/share/sendmail-cf/m4/cf.m4')dnl
VERSIONID(`setup for Red Hat Linux')dnl
OSTYPE(`linux')dnl
define(`confLOG_LEVEL', `29')dnl
dnl #
dnl define(`SMART_HOST',`smtp.your.provider')
dnl #
define(`confDEF_USER_ID',``8:12'')dnl
dnl define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT', `1m')dnl
define(`confTRY_NULL_MX_LIST',true)dnl
define(`confDONT_PROBE_INTERFACES',true)dnl
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
define(`STATUS_FILE', `/var/log/mail/statistics')dnl
define(`UUCP_MAILER_MAX', `2000000')dnl
define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confAUTH_OPTIONS', `A')dnl
dnl #
TRUST_AUTH_MECH(`EXTERNAL DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `EXTERNAL GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN
PLAIN')dnl
dnl #
define(`confLOCAL_MAILER',`cyrus')
define(`confTO_IDENT', `0')dnl
FEATURE(`no_default_msa',`dnl')dnl
FEATURE(`smrsh',`/usr/sbin/smrsh')dnl
FEATURE(`mailertable',`hash -o /etc/mail/mailertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
FEATURE(local_procmail,`',`procmail -t -Y -a $h -d $u')dnl
FEATURE(`access_db',`hash -T<TMPF> -o /etc/mail/access.db')dnl
FEATURE(`blacklist_recipients')dnl
EXPOSED_USER(`root')dnl
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')dnl
dnl FEATURE(`accept_unresolvable_domains')dnl
```

```
FEATURE(`relay_based_on_MX')dnl
LOCAL_DOMAIN(`linux.dominio.edu.uy')dnl
MASQUERADE_AS(`linux.dominio.edu.uy')dnl
FEATURE(masquerade_envelope)dnl
dnl MASQUERADE_DOMAIN(localhost)dnl
dnl MASQUERADE_DOMAIN(localhost.localdomain)dnl
dnl MASQUERADE_DOMAIN(mydomainalias.com)dnl
dnl MASQUERADE_DOMAIN(mydomain.lan)dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
MAILER(cyrus)dnl
```

SERVICIOS

Para tener funcionando en un host el servicio de mail deben estar ejecutándose simultáneamente los siguientes servicios:

```
saslauthd
sendmail
cyrus-imapd
```

Para configurar que estos servicios arranquen al inicio del sistema se debe configurar:

```
chkconfig --level 2345 sendmail on
chkconfig --level 2345 saslauthd on
chkconfig --level 2345 cyrus-imapd on
```