

Configuración del Servidor de Correo “SendMail” para GNU/Linux

Tabla de Contenidos

8. Configuración del Servidor de Correo “SendMail” Para GNU/LINUX.....	2
8.1 Introducción.....	2
8.2 Preparativos.....	2
8.2.1 Verificando parámetros de red.....	3
8.2.2 Confirmando la instalación de Sendmail.....	4
8.3 Configurando Sendmail.....	5
8.4 Habilitando los servicios POP3 e IMAP.....	10
8.5 ¿Que hacer con el Spam?.....	11
8.6 El Servidor de Nombres (DNS).....	13
8.7 Configuración de los clientes de correo.....	16



8. Configuración del Servidor de Correo “SendMail” Para GNU/LINUX

8.1 Introducción

La mayoría de las distribuciones de GNU/Linux incluyen de manera predeterminada **Sendmail**, un poderoso servidor de correo electrónico ampliamente utilizado alrededor del mundo. Este requiere de una correcta configuración para su mejor aprovechamiento y poder disponer de un nivel de seguridad aceptable.

Es muy común que los administradores inexpertos no se molesten siquiera en establecer un nivel de seguridad apropiado en sus redes locales, y mucho menos en el servidor de correo, el cual ven como un servicio más. Es un error común el configurar Sendmail para que permita enviar correo como sea a cualquier costo. Usualmente este costo significa convertirse en Open Relay, y por lo tanto en un paraíso para personas que se dedican al envío masivo de correo comercial (Spam).

Tómese en consideración que, de ser posible, se debe utilizar la versión estable más reciente de todo el software que vaya a instalar al realizar los procedimientos descritos en este manual, a fin de contar con los parches de seguridad necesarios. Ninguna versión de sendmail anterior a la 8.11.6 se considera como apropiada debido a fallas de seguridad de gran importancia, y ningún administrador competente utilizaría una versión inferior a la 8.11.6. Por favor visite el sitio Web de su distribución predilecta para estar al tanto de cualquier aviso de actualizaciones de seguridad. Ejemplo: para Red Hat Linux 7.2, 7.3, 8.0 y 9 existen paquetes de actualización.

8.2 Preparativos

Lo primero será establecer que es lo que tenemos en la red local y que es lo que haremos con esto. Determine que máquinas de su red local, específicamente las direcciones IP, necesitan poder enviar y recibir correo electrónico y cuales NO deben hacerlo.

Determine como desea recuperar los mensajes de correo electrónico que arriben al servidor. POP3 o IMAP.

POP3: Es el protocolo de recuperación de correo electrónico más utilizado en la actualidad. Permite recuperar el correo pero este se almacenará localmente en el disco duro de las máquinas de los usuarios

IMAP: Este protocolo almacena el correo electrónico, y permite la creación de carpetas de usuario, en el servidor. De modo tal, los usuarios pueden acceder desde cualquier parte del mundo a su buzón de correo y carpetas personales. IMAP también facilita la utilización de webmails (servicios de correo basado sobre Web).

Determine el nombre de todos los posibles nombres o alias que tenga su servidor. Ejemplo: mi-dominio.org, mail.mi-dominio.org, servidor.mi-dominio.org, mi-red-local-org, mail.mi-red-local.org, etc.

Configure sus dos tarjetas de red, una para la red local con la IP interna y otra para la dirección IP real.

8.2.1 Verificando Parámetros De Red.

Debe de definirse el nombre de la máquina que funcionará como servidor de correo. Normalmente utilizaremos el esquema nombre_maquina.nombre_dominio. Un ejemplo del nombre de la máquina servidor sería linux.linuxparatodos.com o servidor.mi-dominio.org.com. Así que asegúrese de que esto se encuentra perfectamente definido en /etc/sysconfig/network y /etc/hosts:

Para /etc/sysconfig/network, es decir, el nombre que asignamos a la máquina, correspondería lo siguiente:

```
NETWORKING=yes
HOSTNAME=servidor.mi-dominio.org.com
GATEWAY=148.243.59.254
```



Para /etc/hosts, es decir, la información de los hosts y las direcciones IP, correspondería lo siguiente:

```
# Primero, verificamos que las direcciones IP del
# servidor estén asociadas correctamente a un nombre
# largo y uno corto. Los espacios son con tabuladores.
127.0.0.1 localhost.localdomain          localhost
148.243.59.1      servidor.mi-dominio.org.com      servidor
192.168.1.1       intranet.mi-red-local.org.com     intranet
#
# Opcionalmente aquí puede agregar también
# los nombres y direcciones IP de la máquinas
# de la red local.
192.168.1.2       maquina2.mi-red-local.org.com     maquina2
192.168.1.3       maquina3.mi-red-local.org.com     maquina3
192.168.1.4       maquina4.mi-red-local.org.com     maquina4
```

Además de configurar correctamente un DNS que defina bien los DNS o servidores de nombres de dominios correspondientes. Esto debe hacerlo en el archivo /etc/resolv.conf, de un modo similar al siguiente:

```
search mi-dominio.org.com
#
# El IP de la máquina que tiene el DNS de la red local.
nameserver 192.168.1.1
#
# Los DNS del proveedor de servicios.
nameserver 200.33.213.66
nameserver 200.33.209.66
```

Una cosa más antes de continuar...

No olvide que se requiere un DNS perfectamente configurado para que este resuelva su nombre de dominio utilizado por el servidor de correo. Recuerde que el correo proveniente de otros equipos no llega solo al servidor ni tampoco por arte de magia.

8.2.2 Confirmando La Instalación De Sendmail.

Es importante tener instalados los paquetes sendmail y sendmail-cf, ya que utilizaremos el servidor de correo Sendmail para el envío de nuestros mensajes y filtrado de correo masivo no solicitado -Spam-, y el paquete imap, mismo que nos permitirá utilizar el servicio de IMAP y POP3. Para asegurarse de esto, se puede utilizar la siguiente línea de comando:

```
rpm -q sendmail sendmail-cf imap
```

Esto debe devolvernos las versiones de sendmail, sendmail-cf e imap que se tienen instaladas. Si no fuese así, debemos cambiar a root, si aún no lo hemos hecho, y proceder a instalar estos paquetes. Introduzca el CDROM de su distribución y siga el siguiente procedimiento:

```
mount /mnt/cdrom
cd /mnt/cdrom/RedHat/RPMS
rpm -Uvh sendmail-* imap-*
cd $home
eject /mnt/cdrom
```

Debe instalar sendmail-cf o no le será posible compilar los archivos necesarios para configurar Sendmail. El paquete imap, el cual contiene el daemon para los protocolo POP3, es el que nos permitirá recuperar el correo desde el servidor en el resto de las máquinas que integren la red local con cualquier cliente de correo electrónico.

8.3 Configurando Sendmail.

Antes de continuar, debemos editar el fichero /etc/mail/local-host-names, en el cual deberemos de listar todos y cada uno de los alias que tenga el servidor que estamos configurando, así como los posibles sub-dominios. Es decir, todos los dominios para los cuales estaremos recibiendo correo en un momento dado.

```
# Incluya aquí todos los dominios para los que
# recibamos correo.
mi-dominio.org.com
servidor.mi-dominio.org.com
mail.mi-dominio.org.com
mi-red-local.org.com
intranet.mi-red-local.org.com
mail.mi-red-local.org.com
```

Procederemos entonces a modificar el archivo /etc/mail/sendmail.mc, con previo respaldo del original, a fin de

preparar la configuración del servidor de correo.

```
cp /etc/mail/sendmail.mc /etc/mail/etc/sendmail.mc.default
```

Por defecto Sendmail solo permitirá enviar correo solo desde la interfaz loopback (127.0.0.1), es decir, desde el mismo servidor. Si queremos poder enviar correo desde las máquinas de la red local comente la línea o bien, si tiene varias, añada las interfaces desde las cuales se quiere que escuche peticiones sendmail y omita las que no deben, como sería una red local secundaria con restricciones.

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

Si queremos filtrar Spam de manera eficiente, la mejor manera de empezar a hacerlo es rechazando correo proveniente de dominios NO RESUELTOS, es decir dominios que no están registrados en un DNS y que por lo tanto SON inválidos. Para tal fin, a menos que se requiera lo contrario, es necesario mantener comentada la siguiente línea:

```
dnl FEATURE(`accept_unresolvable_domains')dnl
```

Es necesario establecer que mi-dominio.org.com corresponderá a la máscara que utilizaremos para todo el correo que emitamos desde nuestro servidor. Debe, por tanto, añadirse una línea justo debajo de MAILER(procmail)dnl y que va del siguiente modo:

```
MASQUERADE_AS(mi-dominio.org.com)dnl
```



Todo en conjunto ya modificado y (muy importante) sin alterar el orden de las líneas de código, debería quedar como los scripts de configuración adjuntos al tema.



Se incluye el extracto del script de configuración para Red Hat Linux 7.x y Red Hat Linux 8.0 - 9 como documentación anexa al tema.

Luego se procesa con el siguiente comando para generar `/etc/sendmail.cf` (Red Hat Linux 7.x) o `/etc/mail/sendmail.cf` (Red Hat Linux 8.0 y 9):

Procedimiento en Red Hat Linux 7.x

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

Procedimiento en Red Hat Linux 8.0 y 9

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

Deben definirse los dominios para los cuales se estará permitiendo enviar correo electrónico. Esto se hace generando el fichero `/etc/mail/relay-domains`:

```
mi-dominio.org.com
servidor.mi-dominio.org.com
mi-red-local.org.com
intranet.mi-red-local.org.com
```

Abrimos ahora el archivo `/etc/mail/access` y agregamos algunas líneas para definir quienes podrán hacer uso de nuestro servidor de correo para poder enviar mensajes:



```
# Por defecto, solo se permite enviar correo desde localhost...
localhost.localdomain      RELAY
localhost                  RELAY
127.0.0.1                  RELAY
# Debemos añadir solo las direcciones IP
# que ahora tenga el servidor

192.168.1.1                RELAY
148.243.59.1              RELAY
#
# Agregue también las direcciones IP que integran su red local.
# Solo especifique aquellas máquinas que tendrán
# permitido enviar y recibir correo. No es buena idea
# especificar redes completas. Especifique máquinas
# individuales, aunque signifique ingresar manualmente un
# centenar de entradas. Es más seguro de este modo.
192.168.1.2                RELAY
192.168.1.3                RELAY
192.168.1.4                RELAY
# etc.
#
# Y también podemos agregar las direcciones de correo
# electrónico de aquellos a quienes consideremos
# "indeseables", o que queramos bloquear.
Spam@algun_Spamer.com      REJECT
info@otro_Spammer.com      REJECT
#
servidor.indeseable.com     REJECT
part.com.com                REJECT
newlad.com                  REJECT
dmc.com.com                 REJECT
propnewidea.com             REJECT
lapromocion.com             REJECT
hosting.com.com             REJECT
solopromos.com.com          REJECT
# etc.
```

En este archivo también puede agregar las direcciones de correo electrónico que desee bloquear, como son algunas de quienes envían correo masivo no solicitado -Spam-.

Al concluir, debemos también compilar este archivo para generar otro en formato de base de datos a fin de ser utilizado por Sendmail:

```
cd /etc/mail
make
```

O bien puede ejecutar lo siguiente:

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

Será de utilidad designar un alias a la cuenta de correo de root a fin de recibir los mensajes generados por el

sistema en una cuenta común de usuario. Abra el archivo `/etc/aliases`, en donde al final encontrará la siguientes líneas:

```
# Person who should get root's mail
root:                jperez
```

Esto corresponde a la cuenta de correo local hacia donde se re-direcciona el correo de root. Des-comente la última línea y asigne el nombre de la cuenta de usuario que utiliza normalmente:

```
# Person who should get root's mail
root:                jperez
```

A fin de que este nuevo alias surta efecto y pueda ser utilizado por Sendmail debe utilizar el comando `newaliases`:

```
/sbin/newaliases
```

Terminados los detalles de la configuración, reinicie sendmail del siguiente modo y tendrá listo un servidor de correo que podrá utilizar para enviar mensajes para toda su red local utilizando el servidor SMTP de su proveedor de servicios:

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

Generalmente Sendmail está incluido entre los servicios que de forma predeterminada se inician con el sistema. Si por alguna razón Sendmail no estuviese habilitado, ejecute lo siguiente a fin de habilitar sendmail en los niveles de ejecución 3, 4 y 5:

```
/sbin/chkconfig --level 345 sendmail on
```

Si está funcionando un contrafuegos o firewall, recuerde que debe de estar abierto el puerto 25, de otro modo el correo saldría pero no entraría. Añada o verifique que esté presente una línea en el guión de firewall similar a la siguiente:

```
#SMTP
/sbin/iptables -t filter -A INPUT -p tcp -s 0/0 -d 0/0 --dport 25 -j ACCEPT
```

8.4 Habilitando Los Servicios POP3 E IMAP

Si usted utiliza Red Hat Linux 7.x o versiones posteriores o equivalentes, debe saber que inetd ha sido sustituido por xinetd, y utiliza métodos de configuración muy distintos.

Puede habilitar los servicios ipop3 (POP3 tradicional, autenticación en texto plano), pop3s (POP3 seguro, autenticación con criptografía), imap (IMAP tradicional, autenticación en texto plano) e imaps (IMAP seguro, autenticación con criptografía). Utilice aquellos que considere como más apropiados para su red local de acuerdo a las capacidades de los clientes de correo electrónico utilizados. Tome en cuenta que la autenticación por medio de texto plano es definitivamente un método inseguro, y siempre serán mejor usar los servicios que permitan establecer conexiones seguras.

Puede habilitar los servicios de manera automática e inmediata ejecutando los siguientes comandos (solo habilite aquellos que realmente necesite):

```
/sbin/chkconfig ipop3 on
/sbin/chkconfig pop3s on
/sbin/chkconfig imap on
/sbin/chkconfig imaps on
```

También puede habilitarlos manualmente con un editor de texto, lo cual es sugerido a fin de habilitar opciones adicionales, como direcciones IP específicas a las cuales se les estaría permitido cierto servicio. Acceda a al directorio /etc/xinet.d/ y edite los fichero ipop3, pop3s, imap e imaps, según lo requiera. Estos requerirán edite una sola línea para habilitar el servicio:



```
service pop3
{
    socket_type      = stream
    wait             = no
    user             = root
    server           = /usr/sbin/ipop3d
    log_on_success   += USERID
    log_on_failure   += USERID
    disable          = no
    only_from        = 192.168.1.1 192.168.1.2 192.168.1.3 192.168.1.4 localhost
}
```

Lo mismo aplica para el protocolo IMAP e IMAPS.

Hecho lo anterior, es necesario reiniciar el daemon xinetd con la siguiente línea de comando:

```
/sbin/service xinet restart
```

8.5 ¿Que Hacer Con El Spam?

Sin duda alguna una de las cosas más molestas de Internet es el correo comercial no solicitado, comúnmente llamado Spam. Las empresas que incurren en esta forma de marketing no tienen el mínimo respeto por los demás, y saturan cientos de miles de buzones de correo a diario. Veamos pues un método civilizado para combatirlos.

No importa cuanto se queje uno, o cuantos mensajes con insultos y llamada telefónicas reclamo se hagan a las oficinas de las empresas que incurren en esta poco ética forma de promoción, estas gentes no les interesa la opinión de a quienes ellos perjudican haciendo malgastar el ancho de banda o bloqueando servidores de correo. Ellos compran y hacen uso sin autorización de discos con cientos de miles de direcciones correo electrónico con un solo objetivo: promocionar como sea productos y servicios, en su mayoría, inútiles.

El combate al Spam requiere de la colaboración de los administradores de las redes, quienes deben atender y dar seguimiento a las quejas y tomar las acciones ejemplares pertinentes. Los usuarios deben participar reportando incidentes a los administradores de las redes involucradas.

Empresas que, por alguna razón, y gracias a lagunas legales, recurren al envío de Spam, pueden ser bloqueadas por completo añadiendo una entrada que rechace correo generado por los servidores de empresas que incurran en Spam. esto se hace editando /etc/mail/access y generando /etc/mail/access.db. Ejemplo:

part.com.com	REJECT
newlad.com	REJECT
dmc.com.com	REJECT
propnewidea.com	REJECT
lapromocion.com	REJECT
hosting.com.com	REJECT
solopromos.com.com	REJECT

Acto seguido se ejecuta el siguiente comando:

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

Y se reinicia Sendmail. También pueden utilizarse listas de este tipo, como [la que mantenemos en Linux Para Todos](#). En adelante todo correo enviado desde los dominios anteriormente mencionados, será rechazado por completo para toda nuestra red.

Otra opción más del administrador es bloquear también el accesos a los dominios involucrados a través de IPChains o IPTables. Esto no impedirá que llegue correo, pero servirá para boicotear a las empresas que utilizan Spam para promocionarse, al no permitir el acceso a sus redes desde nuestras redes locales.

Para determinar la dirección IP de un dominio en particular, solo baste ejecutar el comando host, el cual devolverá la dirección IP y quizá algo de información adicional, como si se trata del alias de otro dominio.

```
host solopromos.com.com
solopromos.com.com. has address 200.57.146.18
```

Una vez determinadas las direcciones IP problemáticas, solo hay que añadir algunas líneas en el guión de Firewall que se este utilizando de modo tal que queden bloqueadas de manera permanente, por lo menos desde nuestra red local. Ejemplo:

```
/sbin/iptables -A INPUT -s 216.219.236.81 -d 0/0 -j DROP
/sbin/iptables -A INPUT -s 64.65.27.126 -d 0/0 -j DROP
/sbin/iptables -A INPUT -s 200.57.146.18 -d 0/0 -j DROP
```

Mientras más usuarios y administradores participen notificando y castigando el Spam, correspondientemente, esta molestia desaparecerá eventualmente, o al menos haremos saber a quienes se promocionan de este modo que NO NOS AGRADA lo que hacen.

8.6 El Servidor De Nombres (DNS)

Si el servidor DNS se localiza en otro servidor y es administrado por otras personas, solo bastará con informar al administrador de dicho servidor de nombres la existencia del nuevo servidor de correo electrónico, a fin de que se de de alta la entrada correspondiente en el DNS y a su vez a fin de que el NIC lo tome en cuenta en el siguiente ciclo de refresco.

Si desea configurar DNS propio, y dar éste de alta con el NIC, se necesitará tener instalados los siguientes paquetes: bind, bind-utils y caching-nameserver. Todos, seguramente, vienen incluidos en alguno de los CD de instalación. Note por favor que no es conveniente utilizar versiones anteriores a bind-9.1.3, debido a serias fallas de seguridad. Consulte en el sitio Web de su distribución para verificar si hay paquetes de actualización disponibles. ⁹

Los siguientes corresponderían a los contenidos para los ficheros de zona requeridos para la red local y por el NIC con el que se haya registrado el dominio. Note por favor que en las zonas de reenvío siempre se especifica al menos un Mail Exchanger (MX) y que se utilizan tabuladores (tecla TAB) en lugar de espacio. Solo necesitará sustituir nombres y direcciones IP, y quizá añadir nuevas entradas para complementar su red local.

```
Zona de reenvío red local
/var/named/mi-red-local.org.com.zone

$TTL 86400
@      IN      SOA      mi-red-local.org.com. jperez.mi-red-local.org.com. (
                        8 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )
@      IN      NS       dns
@      IN      MX       10      mail
@      IN      A        192.168.1.1
intranet IN      A        192.168.1.1
maquina2 IN      A        192.168.1.2
maquina3 IN      A        192.168.1.3
maquina4 IN      A        192.168.1.4
www     IN      CNAME    intranet
mail    IN      CNAME    intranet
ftp     IN      CNAME    intranet
dns     IN      CNAME    intranet
```

```
Zona de resolución inversa red local
/var/named/1.168.192.in-addr.arpa.zone
```

```
$TTL 86400
@      IN      SOA    mi-red-local.org.com.  jperez.mi-red-local.org.com. (
        6 ; serial
        28800 ; refresh
        7200 ; retry
        604800 ; expire
        86400 ; ttk
        )
@      IN      NS     dns.mi-red-local.org.com.
1      IN      PTR     intranet.mi-red-local.org.com.
2      IN      PTR     maquina2.mi-red-local.org.com.
3      IN      PTR     maquina3.mi-red-local.org.com.
4      IN      PTR     maquina4.mi-red-local.org.com.
```

Zona de reenvío del dominio

/var/named/mi-dominio.org.com.zone

```
$TTL 86400
@      IN      SOA    mi-dominio.org.com.  jperez.mi-dominio.org.com. (
        8 ; serial
        28800 ; refresh
        7200 ; retry
        604800 ; expire
        86400 ; ttl
        )
@      IN      NS     dns
@      IN      MX     10  mail
@      IN      A      148.243.59.1
servidor IN      A      148.243.59.1
www     IN      CNAME  servidor
mail    IN      CNAME  servidor
ftp     IN      CNAME  servidor
dns     IN      CNAME  servidor
```

Zona de resolución inversa del dominio

/var/named/1.243.148.in-addr.arpa.zone

```
$TTL 86400
@      IN      SOA    mi-dominio.org.com.  jperez.mi-dominio.org.com. (
        6 ; serial
        28800 ; refresh
        7200 ; retry
        604800 ; expire
        86400 ; ttk
        )
@      IN      NS     dns.mi-dominio.org.com.
1      IN      PTR     servidor.mi-dominio.org.com.
2      IN      PTR     maquina2.mi-dominio.org.com.
3      IN      PTR     maquina3.mi-dominio.org.com.
4      IN      PTR     maquina4.mi-dominio.org.com.
```

Recuerde que cada vez que haga algún cambio en algún fichero de zona, deberá cambiar el número de serie (serial) a fin de que tomen efecto los cambios de inmediato cuando se reinicie el daemon named, ya que de otro modo tendría que reiniciar el equipo, algo poco conveniente.

Fichero /etc/named.conf

```
options {
    directory "/var/named/";
};
zone "." {
    type hint;
    file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
    type master;
    file "0.0.127.in-addr.arpa.zone";
};
zone "localhost" {
    type master;
    file "localhost.zone";
};
zone "mi-dominio.org.com" {
    type master;
    file "mi-dominio.org.com.zone";
};
zone "1.243.148.in-addr.arpa" {
    type master;
    file "1.243.148.in-addr.arpa.zone";
};
zone "mi-red-local.org.com" {
    type master;
    file "mi-red-local.org.com.zone";
    allow-update { none; };
};
zone "1.168.192.in-addr.arpa" {
    type master;
    file "1.168.192.in-addr.arpa.zone";
    allow-update { none; };
};
```

Al terminar de editar todos los ficheros involucrados, solo bastará iniciar el servidor de nombres.

```
/sbin/service named start
```

Si queremos que el servidor de nombres quede añadido entre los servicios en el arranque del sistema, deberemos ejecutar lo siguiente a fin de habilitar named en los niveles de ejecución 3, 4 y 5:

```
/sbin/chkconfig --level 345 named on
```



8.7 Configuración De Los Clientes De Correo.

Considerando que tiene bien configurada su red local y que ha seguido este manual al pie de la letra, sea la PC que sea en su red local, puede configurar mail.mi-red-local.org.com o mail.mi-dominio.org.com como servidor de correo saliente o SMTP y servidor de correo entrante, POP3 o imap, en el cliente de correo que utilice.

