
# UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

ESCUELA DE INGENIERÍA DE SISTEMAS

MONOGRAFÍA PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS

TEMA

"COMPARACIÓN TÉCNICA DE LAS CARACTERÍSTICAS ENTRE LOS MTA SENDMAIL Y POSTFIX"

AUTORES:

Xavier Esteban Idrovo Castañeda

José Benjamín Vélez Zhindón

DIRECTOR:

Ing. Oswaldo Merchán

Cuenca – Ecuador

2007

Las ideas, hechos y contenidos de esta monografía son de exclusiva responsabilidad de los autores.

Xavier Idrovo

CI: 0103418174

José Vélez

CI: 0103544854

DEDICATORIA

AGRADECIMIENTO

## Índice de Contenidos

**CAPITULO 4**

ARQUITECTURAS DE POSTFIX Y SENDMAIL



**CAPITULO 5**

INSTALACIÓN Y CONFIGURACIÓN



**CAPITULO 6**

CONFIGURACION DE UN ANTIVIRUS

## RESUMEN

El siguiente trabajo trata acerca de la instalación y configuración de dos Agentes de Transporte de Correo en la plataforma Linux y la comparación técnica entre ellos.

Un Agente de Transporte de Correo MTA (Mail Transfer Agent) es un programa que se encarga de transportar o encaminar el correo electrónico hacia un destinatario propio del dominio o hacia el Internet.

Los MTA que se configurarán son Sendmail y Postfix, cada uno se instalará en una maquina con el sistema operativo CentOS (Linux), en este documento consta la preparación del servidor de correo, una instalación básica del MTA con el cual se podrá enviar y recibir correo, y se agregara la capacidad de revisar si un correo tiene virus o si este es spam.

## ABSTRACT

The next project is about installation and configuration of two Mail Transfer Agents on Linux platform and a technical comparison between them.

A Mail Transfer Agent is a program which takes charge of transporting or sending an electronic mail to a recipient in the domain or towards Internet.

The MTAs which will be configured are Sendmail and Postfix. Each one are going to be installed in a machine with an operative system Cent Os (Linux). This document consists of the Mail Server preparation, a basic MTA installation which will be able to send and to receive mail. It will have the capacity to check if a mail whether has a virus or is spam.

# CAPITULO 1

# INTRODUCCION AL CORREO ELECTRÓNICO

## 1.1 Correo Electrónico

Correo electrónico, o en inglés e-mail, es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos. Esto lo hace muy útil comparado con el correo ordinario, pues es más barato y rápido. Junto con los mensajes también pueden ser enviados ficheros como paquetes adjuntos.

Sin embargo, el correo electrónico, en lugar de ser repartido a domicilio por un servicio postal, el correo electrónico se envía a través de una red computacional al ordenador que utiliza la persona a quien va dirigido.

## 1.2 Dirección de Correo Electrónico

Una dirección de Correo Electrónico es un conjunto de palabras siendo único e irrepetible que consta de dos partes nombre del usuario seguido del símbolo @ y luego nombre del dominio sin incluir espacios es blanco.

usuario@monografia.com.ec

A su vez el dominio se descompone en la siguientes partes, la primera el nombre del dominio en sí (monografía), seguido del tipo organización que presta este servicio (com) y luego el país en el que se encuentra (ec), siendo este último opcional.

Tipos de extensiones que utilizan los diferentes dominios.

| | **Significado** | **Ejemplos** |
|---|---|---|
| .com | Comerciales o compañías de negocios | ibm.com, att.com, ford.com |
| .net | Proveedores de Internet o Redes | webtv.net |
| .gov | Instituciones Gubernamentales | whitehouse.gov, nasa.gov |
| .edu | Instituciones relacionadas con la Educación | uiuc.edu, stanford.edu |
| .org | Instituciones sin fines de lucro | redcross.org, sfopera.org |
| .mil | Instituciones Militares | army.mil |
| .int | Instituciones Internacionales | itu.int |

| | **País** | **Ejemplo** |
|---|---|---|
| us | Estados Unidos | city.palo-alto.ca.us, washington.k12.ia.us |
| uk | Reino Unido | cam.ac.uk, tvr.co.uk |
| ec | Ecuador | uazuay.edu.ec, jaher.com.ec |
| de | Alemania | sgi.de |
| jp | Japón | www.hitachi.co.jp, www.nihon-u.ac.jp |

### 1.3 MUA (Mail User Agent, Agente de usuario de correo)

Un MUA (Mail User Agent, Agente de usuario de correo) es un programa que permite a un usuario, como mínimo, leer y escribir mensajes de correo electrónico. A un MUA se le denomina a menudo cliente de correo. Lógicamente, hay muchos programas MUA que ofrecen al usuario muchas más funciones, entre las que se incluyen la recuperación de mensajes mediante los protocolos POP3 e IMAP4, la configuración de buzones de correo para almacenar los mensajes o ayuda para presentar los mensajes nuevos a un programa MTA (Mail Transfer Agent, Agente de transferencia de correo) que los enviará al destino final.

Los programas MUA pueden ser gráficos, como Thunderbird, Outlook Express, o pueden tener una interfaz basada en texto sencilla, como Mutt o Pine.

### 1.4 MTA (Mail Transfer Agent, Agente de transferencia de correo)

Un programa MTA (Mail Transfer Agent, agente de transferencia de correo) transfiere los mensajes de correo electrónico entre máquinas que usan el protocolo SMTP.Un mensaje puede pasar por varios MTA hasta llegar al destino final. La mayoría de los usuarios desconocen la existencia de estos agentes, incluso si cada mensaje se envía a través de como mínimo un MTA.

Aunque el proceso de envío de mensajes entre las máquinas podría parecer directo, todo el proceso de decidir si un agente MTA concreto puede o debe aceptar un mensaje para entregarlo a un host remoto es relativamente complejo. Además, debido a los problemas de correo basura, el uso de un MTA concreto normalmente está limitado por la propia configuración del mismo o al acceso del sistema a la red en la cual se ejecuta.
La mayoría de sistemas operativos basados en UNIX utilizan Sendmail como agente MTA por defecto, aunque se pueden utilizar otros mas en su lugar.

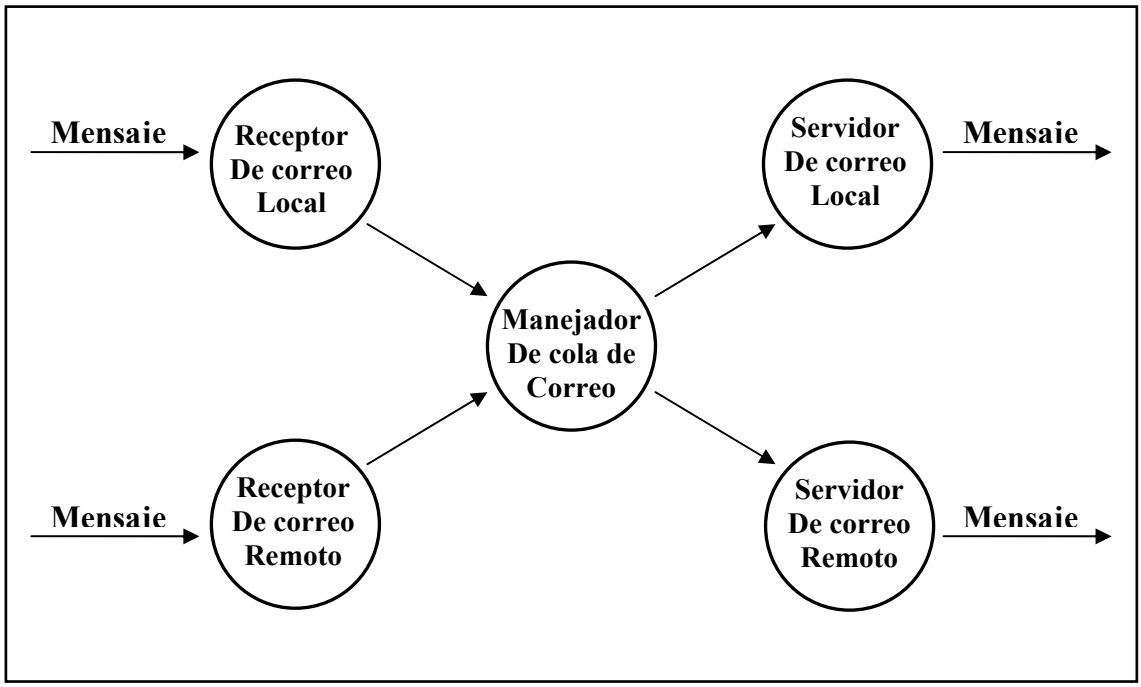


Figura 1 componentes de un MTA

### 1.5 MTA Funcionamiento Básico

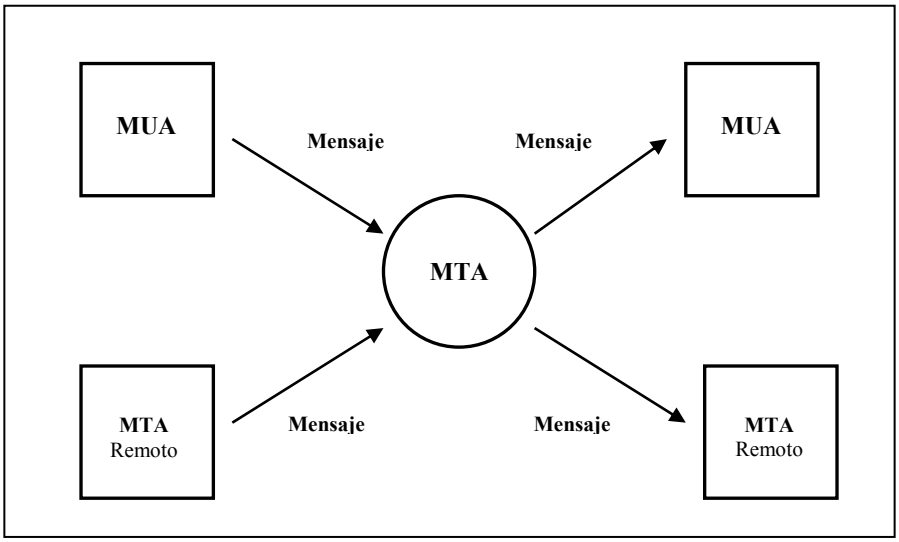


Figura 2 Funcionamiento básico de un MTA

En el siguiente ejemplo, Usuario A (a@monografia.com) envía un correo a Usuario B (b@tesis.com).

1. Usuario A escribe un correo electrónico en un cliente de correo cualquiera (p. ejm.: Outlook Express). Al enviar, el programa contacta con el servidor de correo usado por Usuario A (en este caso, sendmail.monografia.com). Se comunica usando un lenguaje conocido por el mismo, mediante el protocolo SMTP, se transfiere el correo y le da la orden de enviarlo.

2. El servidor SMTP busca el registro MX asociado a ese dominio ya que es un correo dirigido a alguien dentro del dominio tesis.com, se contacta con el servidor mx.tesis.com y transfiere el mensaje al servidor de destino y este lo ubica en la casilla de correo del usuario B.

3. Luego el Usuario B recibe el correo a través de su programa cliente de correo. Esto empieza una conexión, mediante el protocolo POP3 o IMAP4, al ordenador que está guardando los correos nuevos que le han llegado. Este ordenador (mx.tesis.com), se encarga tanto de recibir correos del exterior así como de entregárselos a sus usuarios. En el esquema, Usuario B se descarga el mensaje de Usuario A mediante el protocolo POP3.

# CAPITULO 2

# POSTFIX

## 2.1 Introducción a Postfix

Postfix es un programa informático para el enrutamiento y envío de correo electrónico, un MTA (Mail Transport Agent), de código abierto.

Postfix pretende ser rápido, fácil de administrar y seguro, y a la vez ser lo suficientemente compatible con Sendmail tanto para facilitar su configuración, administración y mantenimiento, como para asegurar transparencia ante los usuarios, siendo Postfix externamente parecido a Sendmail, pero en su interior completamente diferente.

Postfix utiliza un diseño modular para mejorar la seguridad, en el cual los subprocesos, con privilegios limitados, son lanzados por un demonio principal denominado master, éstos realizan tareas muy específicas relacionadas con las diferentes etapas de la entrega de correos y se ejecutan en un ambiente con privilegios de usuario de root, sin necesidad de serlo, para minimizar los posibles ataques.

## 2.2 Historia

Postfix fue escrito por Wietse Zweitse Venema para proveer una alternativa MTA para el estándar de servidores UNIX. Wietse Venema estaba de vacaciones del centro de IBM T. J. Watson Research Center cuando comenzó el desarrollo del proyecto de una alternativa mas rápida y segura que el afamado Sendmail.
Las pruebas de una Versión Alpha comenzaron en enero de 1998 y la versión Beta salio al público para diciembre del mismo año.
Inicialmente este MTA fue llamado VMailer. Charles Palmer, líder del proyecto, propuso el nombre de Postfix, el cual fue adoptado eventualmente.

Postfix ha alcanzado una gran difusión en los últimos tiempos debido a su versatilidad, llegando a convertirse incluso en el agente de transporte por omisión en nuevas distribuciones de Linux y en las dos últimas versiones del Mac OS X (Panther y Tiger).

## 2.3 El Proceso de Postfix

La instalación por defecto que tiene Postfix tiene tres procesos demonios corriendo: master, qmgr y pickup. Los cuales interactúan de la siguiente manera: receptan los mensajes, los coloca en cola y finalmente los despacha. Cada una de estas etapas es realizada por componentes diferentes de Postfix, lo que permite una configuración independiente en cada una de ellas. Después de que el mensaje es recibido y encolado, el administrador de la cola de mensajes invoca al agente de entrega adecuado para la fase final. El administrador de cola es el encargado de administrar la cola de mensajes y alertar a un componente cuando tiene una tarea por hacer.

Postfix basa su funcionamiento en cuatro colas: maildrop, incoming, active y deferred .

El correo que se genera de forma local se deposita en maildrop para su posterior proceso. El proceso pickup toma los mensajes que llegan a maildrop y los pasa a cleanup, que analiza las cabeceras de los mensajes y deposita éstos en la cola incoming.

En la cola active se encuentran aquellos mensajes que están en fase de encaminamiento, y en deferred los mensajes que por diversas causas no se pueden encaminar o están pendientes de reintentar su encaminamiento.
El proceso qmgr es el encargado de tratar los mensajes que llegan a la cola incoming, depositarlos en active y lanzar el proceso adecuado para su encaminamiento, como pueden ser local, smtp o pipe.

Pipe es un proceso demonio que se ejecuta para entregar correo a comandos o procesos externos.

El correo procedente de otros sistemas se atiende a través del proceso smtpd, utilizando el protocolo SMTP, pudiendo utilizar accesos a tablas internas para aplicar las políticas de acceso a cada mensaje entrante.

Existen además diferentes tablas que, creadas por el administrador, sirven a los diferentes procesos para concretar el tratamiento que debe darse a cada mensaje.

Se usan seis tablas: access, aliases, canonical, relocated, transport y virtual. Aunque no es obligatoria la existencia ni utilización de todas ellas.

La tabla access permite definir una relación explícita de sistemas a los que se les deben aceptar o rechazar sus mensajes. La utiliza el proceso smptd.

La tabla aliases, al igual que en Sendmail, define una serie de nombres alternativos a usuarios locales, y la consulta el proceso local.

El proceso cleanup, mediante la tabla canonical establece relaciones entre nombres alternativos y nombres reales, ya sean usuarios locales o no.

El proceso qmgr utiliza la tabla relocated para devolver los mensajes de usuarios que han cambiado de dirección: “User has moved to new-email”.

Con la tabla transport, que es utilizada por el proceso trivial-rewrite, se define la política de encaminamiento por dominios, subdominios e incluso por dirección concreta de usuario.

Para la gestión y soporte de dominios virtuales el proceso cleanup utiliza la tabla virtual. En ella se establecen las relaciones entre usuarios virtuales y reales, e incluso de dominios completos.

Todas estas tablas pueden usar alguno de los siguientes tipos de formato de base de datos:
- Fichero binario indexado (btree, hash, dbm, etc).
- Fichero de texto basado en expresiones regulares ( regexp).

- Sistema externo de base de datos (NIS, LDAP, MySQL, etc).

# CAPITULO 3

# SENDMAIL

## 3.1 Introducción a Sendmail

Sendmail es un conocido agente de transferencia de correo (MTA) usado en Internet, que maneja un amplio porcentaje de todos los correos encaminados en Internet a la vez que se traslada de un host a otro. Existen otros agentes de transferencia de correo, pero Sendmail es utilizado como MTA por su potencia, escalabilidad y compatibilidad con los estándares de Internet.

Sendmail es altamente configurable, permitiendo controlar cada aspecto de la gestión de correo y también, para la mayoría de la gente, increíblemente difícil de aprender y comprender. Sendmail se configuraba a través del fichero sendmai.cf lo cual representa una seria complejidad por su sintaxis, en lugar de esto se utiliza la herramienta de linux M4 la cual compila y transforma las instrucciones escritas en el archivo sendmail.mc para que sean utilizadas por el programa.

## 3.2 Historia

El programa Sendmail data antes de la evolución de la Internet, es el primer MTA ampliamente usado. Fue escrito por Eric Allman cuando el estaba en la Universidad de California en Berkeley. El escribió el precursor de Sendmail Delivermail este salio con la versión 4.0 y 4.1 de Unix BSD. Pero Delivermail no era lo suficientemente flexible para manejar los cambios en los requerimientos del ruteo de correo.

En 1980 ARPAnet comenzó a manejar TCP (Transmition Control Protocol). Este cambio incremento el número de hosts a más de un billón. Se desarrolló en SMTP para el transporte del correo con esto el Delivermail quedó obsoleto por que no soportaba los nuevos protocolos, Eric Allman evolucionó el Delivermail en Sendmail con lo que respondía a los cambios y requerimientos surgidos.

La primera versión de Sendmail salio con la versión 4.1c BSD que fue la primera versión de Unix en incluir TCP /IP

### 3.3 Proceso Sendmail

El programa Sendmail escucha a la red por correo entrante, y también envía mensajes de correo a otras máquinas. Además maneja el envío local entregando correo a través de procesos locales.

La entrega de correo vía SMTP puede ser en demanda de esta, sin embargo, Sendmail tiene que estar como proceso residente escuchando al puerto 25, admitiendo y realizando conexiones SMTP cuando sea necesario. Al recibir una petición de conexión, creará un proceso hijo que se encargará de ello, mientras el proceso padre seguirá escuchando el puerto 25, por esto sólo puede ser ejecutado en el modo de súper usuario del sistema.

El programa Sendmail adopta diferentes nombres para diferentes tareas que éste realiza. Por ejemplo el proceso de Sendmail que corre como demonio escuchando correo entrante se llama smtpd. También el proceso de Sendmail que imprime la cola de correo se llama mailq. Todos estos no son más que el mismo programa Sendmail corriendo bajo diferentes parámetros.

Procesos de sendmail que corren según el parámetro indicado.

| Nombre del parámetro | Descripción |
|---|---|
| **-bd** | **Corre como un Proceso Demonio (llamado smtpd)** |
| **-bi** | **Reconstruye la base de datos (newaliases)** |
| **-bp** | **Imprime la cola (llamado mailq)** |

Una vez que un correo ha sido procesado por sendmail, éste es ubicado en la casilla de correo, en el caso de que sea para un destinatario local, o enviado hacia otro MTA, en el caso de que sea un destinatario externo. Si el correo no puede ser enviado por cualquier motivo, este se queda en la cola el tiempo configurado por el administrador hasta que pueda ser enviado o desechado.

# CAPITULO 4

# ARQUITECTURAS DE POSTFIX Y SENDMAIL

## 4.1 Arquitectura de Postfix

Postfix se basa en una arquitectura modular, en este caso se desarrolla primero un módulo principal y se sirve de una serie de módulos que están al mismo nivel que éste.

Postfix se basa en programas, colas y tablas para el manejo de su configuración. El núcleo del programa de postfix es master, que corre en segundo plano todo el tiempo y este invoca procesos para examinar y procesar las colas según estos se requieran. El demonio master, obtiene las opciones de configuración de dos archivos: main.cf y master.cf al iniciarse.

Postfix tiene procesos que son semi-residentes, estos cooperan mutuamente y realizan una tarea específica para el proceso principal, sin tener ninguna relación padre - hijo, la mayoría de estos procesos se ejecutan como demonios.

## 4.2 Arquitectura de Sendmail

Sendmail tiene una arquitectura monolítica esto quiere decir que corre como un solo proceso de gran dimensión con privilegios de root, la diferencia radica en los parámetros con los que se ejecuta dependiendo del proceso a realizar.

Debido a que en Sendmail todos los componentes básicos de un MTA anteriormente citados, conforman una sola unidad; todos los procesos son ejecutados con los privilegios de superusuario, sean estos necesarios o no.

En base a los diversos procesos que Sendmail gestiona, se podría decir que sendmail es más que un solo programa.

Una parte importante de Sendmail es el archivo de configuración, el cual es muy complejo, en donde se define el lugar y el comportamiento de todas sus partes y las reglas de su comportamiento, otra parte importante es su cola de correo la cual le da fiabilidad a todo el proceso, esto es debido a que una vez que sendmail ha procesado el correo y este esta listo para enviarse el MTA se encarga, en un solo directorio de cola, que el mail llegue a su destinatario.

### 4.3 Conclusiones

El principal problema de sendmail es que se ejecuta como un solo proceso y éste tiene que ejecutarse con privilegios del usuario root para que realice ciertas tareas, esto puede producir algunos problemas de seguridad. En cambio Postfix debido a que utiliza varios procesos independientes entre sí, solo el proceso que lo requiera adoptaría los privilegios de root.

En algunas versiones de Sendmail, como la 8.11 o anteriores, tienen un fallo de seguridad que permite a un usuario local conseguir privilegios de súper usuario o root y así poder hacer cuanto cambio se le antoje en el servidor.

Por otra parte Postfix que fue diseñado en módulos es más flexible que sendmail. De esta manera el cambio de algún aspecto dentro de un modulo es totalmente transparente al resto por lo que le permite una fácil actualización y mantenimiento del programa en si, en cambio en sendmail por tener una arquitectura monolítica conlleva a que sea demasiado trabajoso mantenerlo y actualizarlo, por lo tanto nuevas versiones toman mucho mas tiempo en ser desarrolladas.

# CAPITULO 5

# INSTALACIÓN Y CONFIGURACIÓN

## 5.1 Servidor de resolución de nombres de dominios DNS

### 5.1.1 Que es un servidor DNS

Un servidor de DNS (Domain Name Server) es un servicio que resuelve los nombres de dominio de cada una de las máquinas que se encuentran en la red local, es decir tiene un registro que indica cual es la dirección ip de una máquina y con que nombre canónico se debe referenciar a ella.

Para que un servidor de correo electrónico funcione correctamente debe tener configurado un servidor de DNS para conocer las máquinas con las que se va a comunicar.

### 5.1.2 Configuración de un servidor DNS

El primer paso es asignar las direcciones de red que van a ser utilizadas

Dirección IP del servidor

192.168.119.3

Configuración en Linux

```
# ifconfig eth0 192.168.119.3 netmask 255.255.255.0 up
```

Dirección IP del cliente

192.168.119.1

Configuración en Windows XP

| | |
|---|---|
| IP | 192.168.119.1 |
| Mascara | 255.255.255.0 |
| DNS | 192.168.119.3 |

Para ingresar el nombre del servidor se debe especificar en un archivo cual va a ser su nombre y su dirección IP, esto se hace en el archivo /etc/hosts

192.168.119.3 monografia monografia.com

Debido a que se va utilizar un servicio de resolución de nombres se debe especificar la ubicación del mismo, eso se hace en el archivo /etc/resolv.conf

nameserver 192.168.119.3

Para hacer referencia al nombre de una máquina y este pueda resolver cual es la dirección ip de la misma para encontrarla dentro de la red se debe editar el archivo /etc/named.conf

Se indica que red va a utilizar el DNS

acl “lan” {127.0.0.1; 192.168.119.0/24};

Se configura la zona del dominio que vamos a utilizar para nuestro servicio de correo electrónico y su dominio inverso, esto sirve para que dado un nombre de maquina se pueda conocer su dirección ip y viceversa.

zone "monografia.com" {

```
        type master;
        file "monografia.com.hosts";
        };


zone "119.168.192.in-addr.arpa" {
        type master;
        file "119.168.192.in-addr.arpa";
        };
```

Se debe crear los archivos que contienen los nombres de maquina y sus direcciones ip respectivas, los nombres de archivo se definen en named.conf y estos deben almacenarse en el directorio /var/named/chroot/var/named.

Archivo monografia.com.hosts

```
$ttl 38400
monografia.com.     IN      SOA     monografia. root.monografia.com. (
                    1157674723      ; Serial Number
                    10800           ; Refresh (4 horas)
                    3600            ; Retry (2 horas)
                    604800          ; Expire (30 dias)
                    38400 )         ; Minimum TTL (8 horas)
 monografia.com.    IN      NS      monografia.
sendmail.monografia.com.    IN      A       192.168.119.3
cliente.monografia.com.     IN      A       192.168.119.1
sendmail.monografia.com.    IN  MX  10  192.168.119.3
```

MX Específica el servidor de correo para un dominio teniendo un número asociado como parámetro de prioridad.

NS Apunta a un servidor de nombres maestro de una zona

A Asocia direcciones IP con nombres

Archivo 119.168.192.in-addr.arpa

```
@       IN SOA  monografia.com. root.monografia.com. (
                1998022601              ; Serial Number
                14400                   ; Refresh (4 horas)
                7200                    ; Retry (2 horas)
                2592000                 ; Expire (30 dias)
                28800 )                 ; Minimum TTL (8 horas)

                IN NS   monografia.
3       IN PTR  sendmail.monografia.com.
1       IN PTR  cliente.monografia.com.
```

Para que la configuración funcione

```
# service named start .
```

Verificar su funcionamiento

```
# nslookup sendmail.monografia.com
se obtiene la dirección ip de la maquina
# 192.168.119.3
# nslookup 192.168.119.3
se obtiene el nombre de la maquina
# sendmail.monografia.com
```

**5.2 Configuración de POP3 o IMAP**

Para que un cliente se pueda conectar al servidor y revisar su correo se debe configurar el protocolo POP (Post office Protocol) o IMAP (Internet Message Access Protocol) estos protocolos permiten a los programas clientes de correo electrónico extraer los mensajes pendientes en las casillas del usuario, esto se hace configurando

el servicio Dovecot, para esto se configura en el archivo /etc/dovecot.conf la siguiente línea

protocols = imap imaps pop3 pop3s

Se inicia el servicio dovecot

#service dovecot start

### 5.3 Instalación y Configuración de Sendmail

#### 5.3.1 Instalación de Sendmail

El MTA Sendmail versión 8.13.1 viene instalado por defecto en la instalación completa de CentOS 4.3, para instalarlo manualmente se hace con la siguiente instrucción:

# rpm –ivh sendmail.x.y.z.rpm

#### 5.3.2 Configuración básica de Sendmail

El archivo en el cual se guarda la configuración del MTA es /etc/mail/sendmail.mc

Para que el servicio de transporte de correo funcione y simplemente tome el correo que le llega y envíe a su respectiva casilla o cola de correo se configura únicamente el dominio con el cual queramos que el correo salga y se indica al proceso que se puede enviar y recibir correo desde otra pc que no sea el servidor.

MASQUERADE_AS(`monografia.com')

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

Se debe compilar el archivo de configuración para que funcione con Sendmail

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

Configurar el archivo /etc/mail/access en donde se indica las redes que va a enviar mail desde este servidor, tambien se indica las que se pueden rechazar

```
localhost.localdomain      RELAY
localhost                  RELAY
127.0.0.1                  RELAY
192.168.119                RELAY
168.0                      REJECT
```

La opción RELAY indica que se puede aceptar el envió desde esta red, la opción REJECT que se rechazara el envió desde esta red.

Una vez ingresadas las redes se debe compilar este archivo

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

Se indica a Sendmail cual es el nombre del dominio del servidor en el que se esta configurando, esto se hace en el archivo /etc/mail/local-host-names

Contenido del archivo local-host-names

```
monografía.com
```

Indicar las ip's y los nombres de la red LAN en el archivo /etc/mail/hosts

```
127.0.0.1          localhost.localdomainlocalhost
192.168.119.3      monografia.com monografia
```

Se inicia el servicio de Sendmail

```
#service sendmail start
```

### 5.3.3 Configuración de seguridades controladas por Sendmail

En Sendmail se pueden configurar varios parámetros que lo hacen mas seguro para el servidor y el cliente, estos parámetros son líneas que se incluyen o modifican en el archivo /etc/mail/sendmail.mc.

(`confCONNECTION_RATE_THROTTLE', 3)

Define el número de conexiones que el servidor puede recibir por segundo en este caso tres son atendidas inmediatamente y otras tendrán que esperar hacer atendidas luego de un segundo.

define(`confMAX_HEADERS_LENGTH', `16384')

Tamaño de la cabecera, esto define un tamaño máximo de cabecera de 16 kb.
Algunos programas utilizados para enviar spam tratan de impedir que los MTA puedan registrar transacciones generando cabeceras muy grandes limitando el tamaño de la cabecera hace mas difícil que se exploten las vulnerabilidades.
La mayoría de las cabeceras tienen tamaños menores a 2 Kb (2048 bytes) Esta es una sección informativa que contiene datos relacionados a su envío, tales como el nombre y dirección electrónica del creador del mensaje, la lista de destinatarios, la fecha de envío, los servidores intermedios por donde el mensaje ha pasado, etc.

define(`confMAX_MESSAGE_SIZE', `3145728')

Aquí se especifica el tamaño máximo del mensaje, esto facilita al administrador a controlar que los clientes no envíen mensajes demasiado grandes, con esto se logra reducir la congestión en la red, en este ejemplo se configura un tamaño de mensaje de 3Mb

```
define(`confMAX_DAEMON_CHILDREN', 20)
```

Cada una de las conexiones que se crean el momento en el que un cliente envía correo electrónico se conoce como procesos hijo, este parámetro indica el máximo número de procesos hijo que se pueden producir. Por defecto, Sendmail no asigna un límite al número de procesos hijos. Si se coloca un límite y este es alcanzado, las conexiones siguientes son retrasadas.

```
define(`confMAX_RCPTS_PER_MESSAGE', `20')
```

Para evitar que un usuario envie correo a una cantidad demasiado grande de destinatarios lo cual puede conllevar a un congestionamiento en la red, se puede definir un valor máximo en este caso a 20 por mensaje.

```
define(`confSMTP_LOGIN_MSG',`$j ; $b')
```

Para que no se envíe la versión de Sendmail en el correo electrónico

## 5.4 Instalación y Configuración de Postfix

### 5.4.1 Instalación de Postfix

Para proceder a instalar Postfix primero se debe desinstalar el MTA que viene por defecto en una instalación común de CentOS 4.3.

Se elimina el servicio de Sendmail para que inicie al arrancar el sistema

```
#chkconfig sendmail off
```

Detenemos el servicio de Sendmail

```
#service sendmail stop
```

Desinstalamos Sendmail

```
#rpm –e --nodeps sendmail
```

Para instalar postfix utilizamos el paquete rpm que viene incluido en los cd's de instalación de CentOS, un paquete rpm es un instalador de cualquier programa que se puede utilizar en una plataforma linux.

```
#rpm –ivh postfix-2.1.5-4.2.RHEL4.i386.rpm
```

### 5.4.2 Configuración Básica

Para configurar Postfix se edita el archivo /etc/postfix/main.cf

Nombre del host

```
myhostname = postfix.monografia_postfix.com
```

Dominio

```
mydomain = monografía_postfix.com
```

El dominio con el que se va a enviar el correo electrónico

```
myorigin = $mydomain
```

Las redes que va a aceptar al enviar el correo electrónico

```
mynetworks = 192.168.119.0/24, 127.0.0.0/8
```

Los dominios que se va a aceptaral enviar mail

```
mydestination = $myhostname, localhost.$myadomain, localhost, monografia_postfix.com, postfix.monografia_postfix.com
```

Configurar el archivo /etc/mail/access en donde se indica las redes que va a enviar mail desde este servidor, también se indica las que se pueden rechazar

```
localhost.localdomain     RELAY
localhost                 RELAY
127.0.0.1                 RELAY
192.168.119               RELAY
168.0                     REJECT
```

La opción RELAY indica que se puede aceptar el envió desde esta red, la opción REJECT que se rechazara el envió desde esta red.

Una vez ingresadas las redes se debe compilar este archivo

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

Se indica a postfix cual es el nombre del dominio del servidor en el que se esta configurando, esto se hace en el archivo /etc/mail/local-host-names

Contenido del archivo local-host-names

```
Monografía_postfix.com
```

Indicar las ip's y los nombres de la red LAN en el archivo /etc/mail/hosts

```
127.0.0.1          localhost.localdomainlocalhost
192.168.119.3      monografia_postfix.com monografía_postfix
```

Se agrega el servicio de Postfix para que arranque igual con el sistema y se inicia el servicio de Postfix y este queda listo para transportar el correo electrónico de las redes configuradas

```
#chkconfig postfix on
#service postfix start
```

### 5.4.3 Configuraciones de seguridad controladas por Postfix

default_destination_recipient_limit = 20

Para evitar que un usuario envíe correo a una cantidad demasiado grande de destinatarios lo cual puede conllevar a un congestionamiento en la red, se puede definir un valor máximo en este caso a 20 por mensaje.

header_size_limit = 16384

Tamaño de la cabecera, esto define un tamaño máximo de cabecera de 16 kb.
Algunos programas utilizados para enviar spam tratan de impedir que los MTA puedan registrar transacciones generando cabeceras muy grandes limitando el tamaño de la cabecera hace mas difícil que se exploten las vulnerabilidades
La mayoría de las cabeceras tienen tamaños menores a 2 Kb (2048 bytes) Esta es una sección informativa que contiene datos relacionados a su envío, tales como el nombre y dirección electrónica del creador del mensaje, la lista de destinatarios, la fecha de envío, los servidores intermedios por donde el mensaje ha pasado, etc.

message_size_limit = 3145728

Aquí se especifica el tamaño máximo del mensaje, esto facilita al administrador a controlar que los clientes no envíen mensajes demasiado grandes, con esto se logra reducir la congestión en la red, en este ejemplo se configura un tamaño de mensaje de 3Mb

default_process_limit = 100

Cada una de las conexiones que se crean al momento de la llamada de un proceso se conoce como proceso hijo, este parámetro indica el máximo número de procesos hijo que se pueden producir. Por defecto, Postfix asigna un límite de máximo 100 procesos hijos. En Postfix se puede definir un limite máximo para cada tipo de proceso o servicio dado.

## 5.5 Conclusiones.

La instalación de Sendmail fue relativamente sencilla, en primera instancia porque este programa vienen instalado entre las herramientas de CentOS y lo único que se necesita para que funcione es configurar los parámetros del dominio y la red del servidor y arrancar el servicio correspondiente. Para instalar Postfix se tuvo que desinstalar primero Sendmail e instalar el paquete rpm directamente desde el CD de instalación de CentOS, lo cual no conlleva ninguna dificultad ya que lo único que se necesita es encontrar el paquete adecuado e instalarlo, con lo cual la instalación de cualquiera de los dos MTA no presenta ninguna dificultad.

Al configurar Sendmail se encontró suficiente información en Internet ya que este programa es uno de los mas antiguos y utilizados en el medio cosa que no sucedió con Postfix ya que este es relativamente nuevo (con respecto a Sendmail) y se tuvo un poco mas de dificultad el momento de encontrar cuales son los parámetros que se deben configurar para su funcionamiento.

Una ventaja de la configuración de Postfix es que los archivos de configuración no se tienen que compilar para que sean utilizados por el MTA sino los parámetros son escritos directamente en los mismos, en cambio en Sendmail se debe primero escribir las configuraciones en un archivo y compilar este para que sea entendido por programa.

En lo referente a los parámetros de seguridad manejados por Sendmail y Postfix se encontró que los limites y características que se pueden configurar en uno también se pudieron configurar en el otro, obteniéndose los mismos resultados, con lo cual no se tiene ninguna diferencia en este ámbito.

# CAPITULO 6

# CONFIGURACION DE UN ANTIVIRUS

## 6.1 Definiciones

Un Antivirus es un programa cuya función principal es proteger a los usuarios detectando y eliminando virus informáticos y de otros programas que pretendan causar cualquier daño en general.

Básicamente un Antivirus lo que hace es comparar código de los archivos con una base de datos de los códigos de los virus conocidos, por lo que siempre se pretende tener una base actualizada no muy antigua para poder evitar que virus nuevos no sean detectados.

Por lo general un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los Scripts y programas que pueden ejecutarse en un navegador Web.

## 6.2 ClamAV

ClamAV (Clam Antivirus) es un conjunto de herramientas antivirus para linux, una de las principales acciones que tiene es la de integrarse a un servidor de correo para escanear los archivos adjuntos, debido a la misma proliferación de este tipo de ejecutables, ClamAV consulta una base de datos (operada por sus mismos creadores) en la que se compara el contenido del mensaje ( attachment) con una lista de ejecutables malignos conocidos.

ClamAV también es un pre-procesador de correos que inspecciona el contenido antes de que el usuario descargue su correo a una PC.

La configuración de ClamAV se concentra en dos archivos: clamd.conf y freshclam.conf, ambos ubicados bajo el directorio /etc/. El primero de estos archivos contiene parámetros globales de ClamAV, como los serian generación de registros ("Logs") y limites de archivos a inspeccionar, mientras el segundo -- freshclam.conf -- incluye la configuración para consultar la Base de Datos ClamAV y así actualizar la información local referente a virus más recientes.

### 6.3 MailScanner

MailScanner es un completo sistema de seguridad diseñado para servidores de correo. Protege contra virus y spam detectado estos antes que el correo sea enviado a la cola de envío del MTA utilizado. Para esto MailScanner sirve como una interfaz entre el MTA y el antivirus.
MailScanner es de código abierto pero soporta varios antivirus comerciales como núcleo como son Sophos, McAfee, F-Prot, Command, Kaspersky, Inoculate, Inoculan, Nod32, F-Secure, Panda, RAV, eTrust, Antivir, ClamAV, and Vscan.
También puede detectar spam no deseado ya que soporta el SpamAssasin

### 6.4 Configuración de un antivirus en Sendmail

Para revisar si un correo contiene virus se configura el antivirus esto se realiza mediante la configuración de MailScanner el cual funciona en conjunto con Sendmail y el antivirus clamav.

#### 6.4.1 Instalación y Configuración de MailScanner en Sendmail

Se desempaqueta el archivo con el instalador

```
#tar -zxvf MailScanner-4.55.10-3.rpm.tar.gz
```

Ubicarse dentro de la carpeta desempaquetada y ejecutar el comando

#cd MailScanner-4.55.10-3
#./install.sh

Se edita el archivo /etc/MailScanner/MailScanner.conf para configurar el nombre de la empresa que utiliza el servidor de correo y cual va a ser el antivirus a usar.

Indicar el nombre de la empresa y su sitio web

%org-name% = Monografia
%org-long-name% = Monografia sendmail
%web-site% = http://www.monografia.com
%report-dir% = /etc/MailScanner/reports/es

Indicar cual va a ser el antivirus que se va a utilizar

Incoming Work User = clamav
Incoming Work Group = 0640
Virus Scanning = yes
Virus Scanners = clamav

Se indica la ubicación de las actualizaciones del antivirus

Monitors for ClamAV Updates = /var/lib/clamav/*.cvd

Acciones a tomar si se encuentra un virus

Almacenar los archivos infectados

Quarantine Infections = yes

Notificar a quien envió que su correo tiene virus

Notify Senders Of Viruses = yes

Mensajes que se envían al remitente

Virus Subject Text = {Virus Eliminado?}

Se indica un correo al cual se envía las notificaciones originadas por el antivirus

Notices To = xavier@monografia.com

Local Postmaster = xavier@monografia.com

### 6.4.2 Instalación y configuración de ClamAV

Instalamos el antivirus ClamAV de la siguiente manera

#rpm -ivh clamav-0.88.4-1.9.el4.lpt.i386.rpm

Una vez instalado y configurado el antivirus se inician los servicios de MailScanner y clamav.

Inicio de clamAV

chkconfig clamd on
chkconfig freshclam on
service clamd start
service freshclam start

Debido a que MailScanner utiliza el MTA Sendmail para transportar los correos antes de revisarlos se debe detener este servicio.

chkconfig sendmail off

service sendmail stop

chkconfig MailScanner on
service MailScanner start

### 6.5 Configuración del antivirus en Postfix

Para analizar el correo electrónico en busca de virus se utilizara MailScanner en conjunto con el antivirus ClamAV

#### 6.5.1 Instalación y Configuración de MailScanner

Para instalar Mailscanner se desempaqueta el archivo con el instalador

#tar -zxvf MailScanner-4.55.10-3.rpm.tar.gz

Ubicarse dentro de la carpeta desempaquetada y ejecutar el comando

#cd MailScanner-4.55.10-3
#./install.sh

Se edita el archivo /etc/MailScanner/MailScanner.conf para configurar el nombre de la empresa que utiliza el servidor de correo, cual va a ser el antivirus que se use.

Indicar el nombre de la empresa y su sitio web

%org-name% = Monografia
%org-long-name% = Monografia postfix
%web-site% = http://www.monografia_postfix.com
%report-dir% = /etc/MailScanner/reports/es

Usuario y grupo que maneja
Run as User = postfix

Run as Group = postfix

Indicar cuales van a ser las colas de ingreso y de revisión de correo

Incoming Queue Dir = /var/spool/postfix/hold

Outgoing Queue Dir = /var/spool/postfix/incoming

MTA que va a utilizar MailScanner

MTA = postfix

Ubicación del MTA

postfix = usr/sbin/postfix

Indicar cual va a ser el antivirus que se va a utilizar

Incoming Work User = clamav
Incoming Work Group = 0640
Virus Scanning = yes
Virus Scanners = clamav

Se indica la ubicación de las actualizaciones del antivirus

Monitors for ClamAV Updates = /var/lib/clamav/*.cvd

Acciones a tomar si se encuentra un virus

Almacenar los archivos infectados

Quarantine Infections = yes

Notificar a quien envió que su correo tiene virus

Notify Senders Of Viruses = yes

Mensajes que se envían al remitente

Virus Subject Text = {Virus Eliminado?}
Content Subject Text = {Contenido Peligroso?}
Disarmed Subject Text = {Revisado HTML}

Se indica un correo al cual se envía las notificaciones originadas por el antivirus

Notices To = xavier@monografia_postfix.com

Local Postmaster = xavier@monografia_postfix.com

### 6.5.2 Instalación y Configuración de ClamAV

Instalamos el antivirus ClamAV

#rpm –ivh clamav-0.88.4-1.9.el4.lpt.i386.rpm

Una vez instalado el antivirus se inician los servicios de MailScanner y clamav,

Inicio de clamAV

chkconfig clamd on
chkconfig freshclam on
service clamd start
service freshclam start

Debido a que MailScanner utiliza el MTA Postfix para transportar los correos antes de revisarlos se debe detener este servicio.

```
Chkconfig postfix off
service postfix stop

chkconfig MailScanner on
service MailScanner start
```

### 6.6 Conclusiones

Configurar el antivirus no tuvo ningún inconveniente, ya que para que el mismo funcione únicamente se tiene que instalar el paquete rpm e iniciar el servicio correspondiente, en cambio al configurar MailScanner se tuvo que tener en cuenta las acciones a tomar el momento de encontrar un virus y los parámetros que se deben modificar o agregar, esto puede ser un inconveniente al momento de decidir la configuración idónea para los clientes que utilicen el servidor.

La única diferencia que se encontró el momento de instalar el antivirus es que en Postfix se tiene que indicar la ubicación de las colas que va a manejar el MTA, mientras que en Sendmail utiliza los parámetros por defecto, esto es una ventaja para Sendmail ya que MailScanner está pensado para trabajar principalmente con Sendmail.

.

Utilizar un programa que sirva de interfaz entre el MTA y el antivirus es la configuración mas sencilla y mas utilizada el momento de configurar un servidor de correo, es por esta razón que se encuentra mucha información al respecto en el Internet.

# CAPITULO 7

# CONFIGURACION DE UN ANTISPAM

## 7.1 Spam en el Correo Electrónico

El medio mas utilizado para realizar spamming en la Internet es el correo electrónico o email, esto no es mas que enviar una serie de mensajes idénticos habitualmente de tipo publicitario, a un gran número de direcciones a diferencia de los servicios legítimos de correo, el spam es enviado sin permiso de los receptores y esto se ha convertido en una molestia para los usuarios de la red, ya que la mayoría de personas conectadas tienen una conexión pagada ya adicionalmente reciben un cobro por el buzón , lo cual causa cobros innecesarios y perdida de tiempo por parte del receptor sin contar que debido al tamaño de estos pueden colapsar servidores de correo y sobrecargar los buzones haciendo que la calidad del servicio sea mala.

## 7.2 SpamAssassin

SpamAssassin es una herramienta que se utiliza en servidores de correo electrónico para inspeccionar correos que permite determinar si se trata de mensajes basura, mejor conocido como SPAM.
Por esto se le conoce a Spamassassin como un pre- procesador de correo ya que la inspección es llevada acabo en el servidor de correos antes de que el usuario descargue su correo, así permitiendo una pre-clasificación de mensajes.
SpamAssassin utiliza varios criterios para determinar si un mensaje es SPAM:

Inspección de Cabeceras: Las cabeceras de mensaje contienen información importante acerca del mensaje, como lo son procedencia y rutas de servidor, SpamAssassin inspecciona esta información para fines de detección.

Análisis del Mensaje: El cuerpo y titulo del mensaje también son leídos por SpamAssassin, realizando búsquedas por palabras claves o estructuras que conforman un correo chatarra.

Listas Negras: Actualmente, existen listas que enumeran servidores de correo conocidos como generadores de SPAM ("Open-Relays"), SpamAssassin consulta estas listas negras entre las que se encuentran: http://www.mail-abuse.com/ , http://www.ordb.org/ y http://www.surbl.org/ .

Análisis probabilístico / bayesiano: Una vez definidas las reglas iniciales para detección, SpamAssassin utiliza análisis probabilístico para determinar similitudes entre mensajes entrantes y aquellos ya detectados como SPAM.

Listas Hash / Firmas de Correo: Debido a que un correo SPAM suele ser enviado a miles de personas a la vez, la estructura de cada mensaje es idéntica en todas sus instancias, así produciendo un "Hash" inequívoco. SpamAssasin consulta listas de "Hashes" sobre mensajes conocidos, como lo serian: Vipul's Razor , Pyzor y DCC .

### 7.3 Configuración de un Antispam en Sendmail

Para revisar si un correo es malicioso o spam se configura el antispam esto se realiza mediante la configuración de MailScanner el cual funciona en conjunto con Sendmail y spamassassin

Configuración de Mailscanner

Instalar MailScanner

Se desempaqueta el archivo con el instalador

```
#tar -zxvf MailScanner-4.55.10-3.rpm.tar.gz
```

Ubicarse dentro de la carpeta desempaquetada y ejecutar el comando

```
#cd MailScanner-4.55.10-3
#./install.sh
```

Se edita el archivo /etc/MailScanner/MailScanner.conf para configurar el nombre de la empresa que utiliza el servidor de correo, y el modo de resolver los problemas de spam.

Indicar el nombre de la empresa y su sitio web

%org-name% = Monografia
%org-long-name% = Monografia sendmail
%web-site% = http://www.monografia.com
%report-dir% = /etc/MailScanner/reports/es

Mensajes que se envían al remitente

Content Subject Text = {Contenido Peligroso?}
Disarmed Subject Text = {Revisado HTML}
Phishing Subject Text = {Posible intento de Fraude?}

Control de Spam

Se puede controlar el envió de spam a través de listas negras o a través de spamassassin

Listas negras son bases de datos publicadas y refrescadas con direcciones Ip de spammers o servidores desde donde se envía spam.

Se configura en el archivo /etc/MailScanner/MailScanner.conf

Spam List = ORDB-RBL SBL+XBL spamcop.net NJABL SORBS

Estas listas negras se pueden configurar en el archivo
/etc/MailScanner/spam.lists.conf

Configuración de Spamassassin

Instalación de spamassassin
Este software viene instalado por defecto en la instalación de CentOs 4.3

Se configura en el archivo /etc/MailScanner.conf

Indicarle que utilice spamassassin

Use SpamAssassin = yes

Para identificar el correo malicioso se le asigna un valor numérico a partir de 1 según cualquier característica que indique que este correo puede ser malicioso, si llega a un valor determinado (6 por defecto) este correo se lo marca como spam, y si sobrepasa otro valor establecido (10) se lo elimina directamente.

Valor que indica si un correo es spam

Required SpamAssassin Score = 6

Valor máximo que indica a spamassassin que lo puede eliminar

High SpamAssassin Score = 10

Se indica las acciones a tomar en el caso de que encuentre correo spam

Spam Actions = delete

Si se conoce de servidores que son tratados como generadores de spam y se sabe que no lo son se incluye esto dentro de una “lista blanca” que se encuentra en el archivo /etc/MailScanner/rules/spam.whitelist.rules en el cual se especifica con “yes” los servidores que no son maliciosos.

Una vez instalado y configurado se inician los servicios de MailScanner

Debido a que MailScanner utiliza el MTA Sendmail para transportar los correos antes de revisarlos se debe detener este servicio.

```
chkconfig sendmail off
service sendmail stop

chkconfig MailScanner on
service MailScanner start
```

### 7.4 Configuración del Antispam en Postfix

Para analizar el correo malicioso y spam se utilizara MailScanner en conjunto con spamassassin

Instalar MailScanner

Se desempaqueta el archivo con el instalador

```
#tar -zxvf MailScanner-4.55.10-3.rpm.tar.gz
```

Ubicarse dentro de la carpeta desempaquetada y ejecutar el commando

```
#cd MailScanner-4.55.10-3
#./install.sh
```

Se edita el archivo /etc/MailScanner/MailScanner.conf para configurar el nombre de la empresa que utiliza el servidor de correo, cual va a ser el antivirus que se use y el modo de resolver los problemas de spam.

Indicar el nombre de la empresa y su sitio web

%org-name% = Monografia
%org-long-name% = Monografia postfix
%web-site% = http://www.monografia_postfix.com
%report-dir% = /etc/MailScanner/reports/es

Usuario y grupo que maneja

Run as User = postfix
Run as Group = postfix

Indicar cuales van a ser las colas de ingreso y de revisión de correo

Incoming Queue Dir = /var/spool/postfix/hold

Outgoing Queue Dir = /var/spool/postfix/incoming

MTA que va a utilizar MailScanner

MTA = postfix

Ubicación del MTA

postfix = usr/sbin/postfix

Control de spam

Se puede controlar el envío de spam a través de listas negras o a través de spamassassin

Se configura en el archivo /etc/MailScanner/MailScanner.conf

Spam List = ORDB-RBL SBL+XBL spamcop.net NJABL SORBS

Estas listas negras se pueden configurar en el archivo
/etc/MailScanner/spam.lists.conf

Configuración de Spamassassin

Instalación de spamassassin
Este software viene instalado por defecto en la instalación de CentOs 4.3

Se configura en el archivo /etc/MailScanner.conf
Indicarle que utlice spamassassin

Use SpamAssassin = yes

Para identificar el correo malicioso se le asigna un valor numérico a partir de 1 según cualquier característica que indique que este correo puede ser malicioso, si llega a un valor determinado (6 por defecto) este correo se lo marca como spam, y si sobrepasa otro valor establecido (10) se lo elimina directamente.

Valor que indica si un correo es spam

Required SpamAssassin Score = 6

Valor máximo que indica a spamassassin que lo puede eliminar

High SpamAssassin Score = 10

Se indica las acciones a tomar en el caso de que encuentre correo spam

Spam Actions = delete

Si se conoce de servidores que son tratados como generadores de spam y se sabe que no lo son se incluye esto dentro de una “lista blanca” que se encuentra en el archivo /etc/MailScanner/rules/spam.whitelist.rules en el cual se especifica con “yes” los servidores que no son maliciosos.

Una vez instalado y configurado el antivirus se inician los servicios de MailScanner.

Debido a que MailScanner utiliza el MTA Postfix para transportar los correos antes de revisarlos se debe detener este servicio.

```
chkconfig postfix off
service postfix stop

chkconfig MailScanner on
service MailScanner start
```

### 7.5 Conclusiones

La instalación de spamassasin no tuvo ningún inconveniente ya que este se puede instalar como una de las herramientas que vienen con el sistema operativo CentOS, y la activación de este se lo hace por medio de MailScanner.

La única diferencia que se encontró el momento de configurar el antispam es que se tuvo que indicar a MailScanner cual es la ubicación de las colas para Postfix, mientras que en Sendmail utilizó los parámetros por defecto, esto es una ventaja para Sendmail ya que MailScanner está pensado para trabajar principalmente con Sendmail.

# CAPITULO 8

# COLAS DE CORREO

## 8.1 Colas de Correo

Las colas de correo son una parte muy importante dentro de un MTA ya que es aquí en donde se almacenan los correos cuando se transportan hacia un destinatario propio del dominio o hacia Internet, esto es necesario ya que al enviar un email o mensaje de correo y este no puede llegar a su destino porque no existe una conexión debido a que el host destino esta a pagado o saturado, este se mantiene en cola así que el email que se estaba por enviarse se tiene que almacenar temporalmente dentro del servidor, para luego tratar de enviarlo esperando completar la operación, según como este configurado el MTA este correo en espera podrá estar almacenado en el servidor hasta que sea enviado o eliminado del mismo.

## 8.2 Cola de Correo en Sendmail

### 8.2.1 Descripción de la cola de correo

Sendmail tiene una cola de correo que se encuentra en /var/spool/mqueue Cuando llega un correo para estar en cola dentro de este directorio se crean unos archivos temporales para cada email almacenado o encolado el formato de estos ficheros es el siguiente.

- df--------- Ficheros donde se guardan los cuerpos de los mensajes, sin las cabeceras
- qf--------- Ficheros donde se guardan la información necesaria para procesar los trabajos.
- tf--------- Ficheros temporales imagen de los ficheros qf cuando estos están siendo reconstruidos.
- xf--------- Fichero donde se almacena toda la información transmitida durante la apertura y cierre de una sesión).

Para hacer una visualización de los correo que esta en cola se usa el comando mailq que es un link simbólico a Sendmail –bp , esto visualizara una lista con los identificadores de los mensajes, su tamaño, la fecha en la que el mensaje entró en la cola, el remitente y el destinatario.

Para procesar la cola de correo (automática o manualmente), se utiliza el comando:

Sendmail -q<tiempo>

que procesa la cola de correo cada <tiempo> (solo pude ser ejecutado por el súper usuario, y normalmente se carga junto con el Sendmail en modo demonio en un script de inicio).

<tiempo> es un número seguido de caracteres, *s* para segundos, *m* para minutos, *h* para horas, *d* significa días y *w* significa semanas. Si se omite <tiempo>, Sendmail procesará la cola en ese momento.

Ejemplo:

Sendmail –q2h30m

Actualizará la cola de correo dos hora y media.

Si lo que queremos es procesar la cola en un instante, utilizaremos el comando:
Sendmail -q

Pueden utilizarse otros parámetros especiales para procesar la cola:

- qISubstr Procesará únicamente aquellos trabajos que tengan <Substr> como subcadena de los identificativos de mail.
- qRSubstr Procesará únicamente aquellos trabajos que tengan <Substr> como subcadena de los destinatarios.

- qSSubstr  Procesará únicamente aquellos trabajos que tengan <Substr> como subcadena de los remitentes.

### 8.2.2 Ubicación de las colas de correo electrónico en Sendmail con Mailscanner

Al configurar el MTA Sendmail con MailScanner los correos electrónicos que se van a transportar deben ubicarse en una cola temporal antes de ser analizados por el antivirus o el antispam.

Ubicación de la cola inicial

/var/spool/mqueue.in

Luego de ser revisados los correos son movidos a la cola de envío propia de Sendmail.

Cola de correo de Sendmail

/var/spool/mqueue

Los procesos de Sendmail se encargan de enviar el correo a su respectiva casilla o transportarlos en la red según el destinatario.

Ubicación de las casillas de correo de los usuarios propios del sistema

/var/spool/mail/usuario

En donde “usuario” es un archivo con el nombre de usuario del sistema en el cual están almacenados todos los correos electrónicos enviados al mismo.

### 8.2.3 Tiempo de permanencia en cola

Cuando un mensaje no puede ser enviado a un destinatario se mantiene en cola, pero este mensaje no puede permanecer almacenado en el servidor por siempre ya que se estaría desperdiciando espacio, para esto se tiene en Sendmail dos parámetros con los cuales se configura el tiempo en el que un usuario es notificado porque no se pudo entregar su correo y el tiempo en el que un correo es almacenado en el servidor antes de que este sea borrado.

dnl define(`confTO_QUEUEWARN',`4h')

Esta opción indica el tiempo que un mensaje permanece en cola antes de que envie un mensaje al remitente, el valor por defecto es de 4 horas.

dnl define(`confTO_QUEUERETURN',`5d')

Se establece el tiempo que el mensaje permanece en el sistema antes de ser borrado y envie un mensaje al remitente, este valor por defecto es de 5 días.

Por consistencia se debe configurar QUEWARN  menor que QUEUTURN de lo contrario el remitente no podrá saber nunca si un mensaje se envió o no.

Estos parámetros pueden ser cambiados para que los mensajes no enviados “reboten” mas rápido a sus remitentes.

### 8.2.4 Ordenamiento de los mensajes en cola

La opción QUEUE_SORT_ORDER indica como ordenar los correos en cola antes de ser enviados por defecto Sendmail ordena las colas por prioridad de envío, el problema de esto es que se tiene que ordenar todos los mensajes que se encuentren en cola antes de procesar la misma, con esto se gastan recursos que en la mayoría de los casos son innecesarios ya que los correos por lo general son enviados instantáneamente y no hay necesidad de ordenarlos por prioridad antes de enviarlos.

Otra opción comúnmente usada es ordenar los mensajes por host, ya que Sendmail pone en caché las conexiones de tal forma que si se acaba de enviar un mensaje a un dominio esta conexión permanece abierta por si se envía otro mail al mismo dominio esto es para evitar el proceso de reconexión, con esto primero se ordena los mensajes por host y se aprovecha al máximo las conexiones, pero esto no elimina el tener que indexar los mensajes y utilizar recursos del servidor.

Existen dos opciones mas con las que se puede configurar la cola el primero es tomar los mensajes y enviarlos a medida de que vayan llegando sin tener que ordenarlos, pero se tiene un inconveniente, si el mensaje que se esta enviando tiene un archivo que esta abierto o bloqueado por otro proceso se toma el siguiente correo que llegue y así hasta que encuentre un mensaje disponible, otra forma de hacer esto es randomizar los mensajes que se toman de la cola, con esto se disminuye la probabilidad de encontrarse con un mensaje que este bloqueado.

Formato del parámetro

dnl define(`confQUEUE_SORT_ORDER',`priority')

Opciones de ordenamiento en la cola

| | |
|---|---|
| priority. | Ordena por prioridad de envío |
| hosts | Ordena por Host de destino |
| filename | Envía los archivos a medida que llegan, si el archivo esta bloqueado por otro proceso continua con el siguiente |
| random | Randomiza los mensajes en la cola |

## 8.3 Colas de Correo en Postfix

### 8.3.1 Descripción de la cola de correo en Postfix

Una gran contribución a la estabilidad y velocidad del servidor Postfix es la forma inteligente en que su desarrollador implementó las colas de correo.
Postfix utiliza cuatro colas diferentes, cada una manejada de forma diferente:

La opción queue_directory que esta dentro del archivo /etc/postfix/mail.cf especifica el lugar de la cola de Postfix

queue_directory = /var/spool/postfix

### 8.3.2 Ubicación de las colas de correo en Postfix

Las colas de correo de Postfix se encuentran en /var/etc/postfix/ ahí se encuentran todas las colas que procesa Postfix al transportar un correo.

1. Maildrop queue:

/var/spool/postfix/maildrop

El correo que es entregado localmente en el sistema es aceptado por la cola Maildrop. El correo se chequea para formatearlo apropiadamente antes de ser entregado a la cola Incoming.

2. Hold queue:

/var/spool/postfix/hold

Aquí se almacenan los correos antes de ser procesados por MailScanner para revisar si tienen virus o si son spam

3. Incoming queue:

/var/spool/postfix/incoming

Esta cola recibe correo de otros hosts, clientes o de la cola Maildrop. Mientras sigue llegando correo y Postfix no puede manejarlo, en esta cola se quedan los e-mails.

4. Active queue:

/var/spool/postfix/active

Es la cola utilizada para entregar los mensajes. La Active queue tiene un tamaño limitado, y los mensajes solamente serán aceptado si hay espacio en ella. Esto quiere decir que las cola Incoming y Deferred tienen que esperar hasta que la cola Active pueda aceptar más mensajes.

5. Deferred queue:

/var/spool/postfix/deferred

En esta cola se encuentran los mensajes que por diversas causas no se pueden enviar o están pendientes de reintentar su encaminamiento.

### 8.3.3 Tiempo de permanencia en cola

Al enviar un mensaje y este no ha podido ser entregado, debido a cualquier motivo, ya sea un dominio saturado o apagado, los correos se quedan almacenados en la cola para intentar ser enviados posteriormente, estos correos no puedes permanecer almacenados por siempre para esto se configura un tiempo limite luego del cual el mensaje es eliminado y un mensaje es enviado al remitente.

bounce_queue_lifetime =5d

Este es el tiempo máximo en el que un mensaje permanece almacenado en cola antes de ser eliminado y un mensaje de aviso es entregado al remitente, este tiempo por defecto en Postfix es de 5 días, si este valor se lo pone en 0 se hará únicamente un intento de enviar el correo.

## 8.4 Conclusiones

La configuración de las colas en Sendmail y Postfix no presento ningún problema ya que los parámetros de su ubicación y manejo vienen configuradas por defecto el momento que se instala cada uno de los programas.

La diferencia en la configuración se basa principalmente en que en Sendmail se puede fijar el ordenamiento de la cola según la necesidad del administrador, en cambio en postifx es el mismo programa el encargado de manipular que mensaje tomar de la cola, aunque debido a que lo mas recomendado en Sendmail es randomizar los mensajes en cola y no utilizar los otros parámetros esto no se tomaría como una ventaja sobre el otro MTA.

Otro aspecto que se debe tomar en cuenta es que en Sendmail se tiene la posibilidad de configurar un parámetro para enviar un mensaje de aviso al remitente de que no se ha podido enviar el mensaje, y con otro parámetro fijar el tiempo de permanencia del mismo en el servidor, en cambio en Postfix se configura esto con un solo parámetro, es decir se elimina el mensaje y se envía la notificación.

# CAPITULO 9

# ALIAS

## 9.1 Alias de correo electrónico

Un alias de correo es una dirección especial o un nombre en tu dominio que redirige todos los mensajes que recibe hacia otra cuenta pudiendo estar esta también dentro de tu dominio o fuera de este, se puede también redirigir hacia mas de una cuenta en el caso que se requiera, esto es útil para enviar correo electrónico a una misma cuenta con otro nombre o dominio o para enviar correo por grupos de usuarios.

## 9.2 Creación de un alias en Sendmail

Para crear un alias se debe editar el archivo /etc/aliases

Se ingresa el nuevo alias con el formato:

<nombre_original>: <nuevo_nombre>

Por ejemplo para enviar un solo correo a varios usuarios se debe ingresar las siguientes líneas en el archivo

usuarios: xavier,pepe,juan

De esta forma se puede enviar un solo correo a usuarios@monografia.com y este llegará a todos los usuarios definidos en el alias.

Para que los cambios en un alias o la creación de uno nuevo tenga efecto en el MTA se debe correr la siguiente instrucción:

```
#newaliases
```

Luego se debe reiniciar los servicios del MTA.

```
#service sendmail restart
```

### 9.3 Creación de un alias en Postfix

La ubicación de los alias en Postfix esta definido en el archivo de configuración de postfix /etc/postfix/main.cf

```
alias_database = hash:/etc/aliases
```

Para crear un alias se debe editar el archivo de alias

Se ingresa el nuevo alias con el formato:

```
<nombre_original>: <nuevo_nombre>
```

Por ejemplo para enviar un solo correo a varios usuarios se debe ingresar las siguientes líneas en el archivo

```
usuarios:        xavier,pepe,juan
```

De esta forma se puede enviar un solo correo a usuarios@monografia.com y este llegará a todos los usuarios definidos en el alias.

Para que los cambios en un alias o la creación de uno nuevo tengan efecto en el MTA se debe correr la siguiente instrucción:

```
#newaliases
```

Luego se debe reiniciar los servicios del MTA.

```
#service postfix restart
```

### 9.4 Conclusiones

La configuración de los alias tanto en Sendmail como en Postfix se hace editando el mismo archivo y utilizando el mismo comando para que los cambios tengan efecto, es por esto que para hacer uso de los alias no se presentó ninguna diferencia entre ambos.

# CAPITULO 10

# MILTERS

## 10.1 Definición de Milter

Milter es un termino utilizado en el dialecto de los usuarios de Sendmail que proviene de las palabras en ingles Mail y Filter, estos son un conjunto de librerías e interfaces usadas para crear extensiones (add-ons) del programa Sendmail, las cuales son utilizadas por terceros, tales como antivirus o programas de antispam, durante la cadena de proceso de correo electrónico.
Estos milters también pueden ser utilizados en Postfix en su versión 2.3 con compatibilidad para milters

## 10.2 Milters Soportados por sendmail y postfix

Los milters son filtros de correo pensados para funcionar con Sendmail, sin embargo Postfix a partir de la versión 2.3 fue desarrollado con compatibilidad para estos milters.

A continuación se detalla los milter que se conoce son soportados por ambos programas en sus versiones Sendmail 8.13 y Postfix 2.3, a pesar de que postfix tiene soporte para los milter, todos estos no son totalmente compatibles con el MTA debido principalmente a que son programas diseñados y desarrollados para sendmail.

**ClamAV-Milter Versión: 0.88.7**

Provee una interfase con el antivirus Clamav, En el caso de que se llegue un mensaje de correo que contenga virus este milter lo rechaza antes que el servidor lo procese.

**Milter-link Versión: 0.3.15**

Extrae el URL del mensaje de correo y compara con uno o más direcciones en Listas Negras, también puede verificar si el link tiene errores.

**Milter-ahead Versión: 1.6.125**

Este milter sirve para cuando Spammers envían una serie de emails o correos hacia un dominio sin tener una dirección exacta sino usando un diccionario, el cual busca nombres de usuarios más comúnmente usados, esto provoca que varios mensajes en el cual el usuario o destinatario de dicho dominio no existe sean rechazados. Este milter verifica antes de aceptar el mensaje de correo si el destinatario existe en el dominio antes que el servidor acepte dicho correo.

## 10.3 Ejemplo de la instalación de un milter en sendmail y postfix

En el siguiente punto se detalla un ejemplo de la instalación de un milter en sendmail y postfix, en esta caso se instalará clamav-milter el cual sirve para revisar si un correo electrónico tiene virus.

### 10.3.1 Instalación y configuración de un milter en sendmail

La instalación del milter se realizo en la versión 8.13 de sendmail, para saber si sendmail lo soporta se utiliza el siguiente comando y sin importar mucho lo que salga se debe obtener la palabra MILTER en la línea de salida.

```
# sendmail -d0 < /dev/null | grep MILTER
Compiled with: DNSMAP LOG MAP_REGEX MATCHGECOS MILTER
MIME7TO8 MIME8TO7
```

Se debe tener la librería de milter instalada, para verificar esto se ejecuta el siguiente comando:

```
# locate libmilter | grep /usr/local
/usr/local/include/sendmail/libmilter
/usr/local/include/sendmail/libmilter/mfapi.h
/usr/local/include/sendmail/libmilter/mfdef.h
/usr/local/include/sendmail/libmilter/milter.h
/usr/local/lib/libmilter.a
```

En caso de no tener estos archivos instalados se ejecuta el siguiente comando, dentro de la carpeta /libmilter del código fuente de sendmail

```
# cd libmilter
# ./Build install
```

Se inserta la siguiente línea en el archivo de configuración /sendmail.mc para indicarle que se va a utilizar un milter y que milter se va a utilizar.

```
INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav-milter.sock, F=T, T=S:4m;R:4m')
```

Esta línea se debe insertar antes de la línea que tiene la palabra MAILER dentro del archivo, aquí se indica que se va a utilizar un socket para el milter y que proceso hace referencia al mismo.

Se recompila el archivo de configuración de sendmail.

```
#m4 sendmail.mc > sendmail.cf
```

El milter que se va a configurar es utilizado con el antivirus ClamAV 0.88.7 para lo cual el momento de instalar se debe habilitar el soporte para el milter.

```
#./configure --enable-milter
```

Con esto se instala clamav-milter el cual es usado por sendmail y ClamAV para que se revisen los correos en busca de virus.

Esto se debe hacer antes de instalarlo.

Se van a necesitar dos carpetas de destino para el uso del milter, las cuales deben ser utilizadas por el usuario clamav, el cual es utilizado por el antivirus.

```
# mkdir /var/run/clamav
# chown clamav:clamav /var/run/clamav
# chmod 750 /var/run/clamav
# mkdir /var/run/clamav/quarantine
# chown clamav:clamav /var/run/clamav/quarantine
# chmod 700 /var/run/clamav/quarantine
```

En el archivo de configuración de clamav se deben tener los siguientes parámetros habilitados para que funcione en conjunto con el milter.

```
LocalSocket /var/run/clamav.sock
LogSyslog
FixStaleSocket
User clamav
ScanMail
ScanArchive
```

Estos parámetros indica a clamav que escuche el socket que se crea el momento que arranca el milter, además le indica las acciones que debe hacer, tales como revisar el correo (ScanMail), y que revise los archivos adjuntos al correo (ScanArchive).

Se tiene que iniciar el servicio de clamav

```
#service clamd Start
```

Para que el milter funcione se lo debe iniciar esto se hace con el siguiente comando.

#/usr/local/sbin/clamav-milter -olb local:/var/run/clamav-milter.sock

Aquí se indica al milter que envíe una notificación al remitente y que revise los mensajes de la red lan, además se indica la ubicación del socket la cual debe coincidir con la configurada en sendmail.

Una vez realizado todo esto se debe reiniciar el servicio de sendmail para que los cambios tengan efecto

#service sendmail restart

### 10.3.2 Instalación y Configuración de un milter en Postfix

Postfix a partir de la versión 2.3 tiene soporte de la librería de milter que utiliza sendmail, para esto se debe tener instalado sendmail y luego postfix, obviamente el único servicio que se debe activar es el de postfix.

#### 10.3.2.1 Configuración previa de sendmail

La instalación del milter se realizo en la versión 8.13 de sendmail, para saber si sendmail lo soporta se utiliza el siguiente comando y sin importar mucho lo que salga se debe obtener la palabra MILTER en la línea de salida.

# sendmail -d0 < /dev/null | grep MILTER
Compiled with: DNSMAP LOG MAP_REGEX MATCHGECOS MILTER MIME7TO8 MIME8TO7

Se debe tener la librería de milter instalada, para verificar esto se ejecuta el siguiente comando:

# locate libmilter | grep /usr/local

/usr/local/include/sendmail/libmilter
/usr/local/include/sendmail/libmilter/mfapi.h
/usr/local/include/sendmail/libmilter/mfdef.h
/usr/local/include/sendmail/libmilter/milter.h
/usr/local/lib/libmilter.a

En caso de no tener estos archivos instalados se ejecuta el siguiente comando, dentro de la carpeta /libmilter del código fuente de sendmail

# cd libmilter
# ./Build install

Se inserta la siguiente línea en el archivo de configuración /sendmail.mc para indicarle que se va a utilizar un milter y que milter se va a utilizar.

INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav-milter.sock, F=T, T=S:4m;R:4m')

Esta línea se debe insertar antes de la línea que tiene la palabra MAILER dentro del archivo, aquí se indica que se va a utilizar un socket para el milter y que proceso hace referencia al mismo.

Se recompila el archivo de configuración de sendmail.

#m4 sendmail.mc > sendmail.cf

El milter que se va a configurar es utilizado con el antivirus ClamAV 0.88.7 para lo cual el momento de instalar se debe habilitar el soporte para el milter.

#./configure --enable-milter

Con esto se instala clamav-milter el cual es usado por sendmail y ClamAV para que se revisen los correos en busca de virus.

Esto se debe hacer antes de instalarlo.

En el archivo de configuración de clamav se deben tener los siguientes parámetros habilitados para que funcione en conjunto con el milter.

LocalSocket /var/run/clamav.sock
LogSyslog
FixStaleSocket
User clamav
ScanMail
ScanArchive

Estos parámetros indica a clamav que escuche el socket que se crea el momento que arranca el milter, además le indica las acciones que debe hacer, tales como revisar el correo (ScanMail), y que revise los archivos adjuntos al correo (ScanArchive).

Se tiene que iniciar el servicio de clamav

#service clamd Start

**10.3.2.2 Configuración en Postfix**

Lo primero que se necesita son dos carpetas de destino que va a utilizar el milter para su funcionamiento.

# mkdir /var/run/clamav
# chown clamav:postfix /var/run/clamav
# chmod 750 /var/run/clamav
# mkdir /var/run/clamav/quarantine
# chown clamav:clamav /var/run/clamav/quarantine
# chmod 700 /var/run/clamav/quarantine

Esto sirve para que el usuario postfix tenga acceso a el socket del milter.

Se configura el archivo /etc/postfix/main.cf indicando cual va ser la ubicación del milter que se va a usar.

```
smtpd_milters = unix:/var/run/clamav/clamav-milter
milter_default_action = accept
```

Para que el milter funcione con postfix es necesario la creación de un script de inicialización, el cual le indica a postfix en donde esta la ubicación del archivo de configuración de sendmail y cual va a ser el milter a utilizar, el contenido del script es el siguiente y el nombre de este puede ser milter-postfix

```
#ubicacion del archivo de configuración de sendmail
sm_conf="/etc/mail/sendmail.cf"

clamav_milter_flags="--sendmail-cf=$sm_conf --headers --force-scan \
 --max-children=2 --timeout=0 --pidfile=/var/run/clamav/clamav-milter.pid \
 --quarantine-dir=/var/run/clamav/quarantine"

milter_socket="/var/run/clamav/clamav-milter"


mailsystem_start() {
 if [ -x /usr/local/sbin/clamav-milter ]; then
  rm -f $milter_socket
  echo "Starting clamav-milter: "
  echo "  /usr/local/sbin/clamav-milter $clamav_milter_flags $milter_socket"
  /usr/local/sbin/clamav-milter $clamav_milter_flags $milter_socket
  echo "  waiting for ClamAv milter socket to be created..."
  for second in 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 20 ; do
   if [ -r $milter_socket ]; then
    break;
   fi
   sleep 1
```

```
    done
    if [ "$second" = "20" ]; then
      echo "WARNING: Gave up waiting for socket to appear!"
    fi
    chmod 777 $milter_socket 1> /dev/null 2> /dev/null
  fi;
  /usr/local/sbin/postfix start
}


mailsystem_stop() {
  /usr/local/sbin/postfix stop
  killall clamav-milter
}

case "$1" in
'start')
  mailsystem_start
  ;;
'stop')
  mailsystem_stop
 ;;
*)
  echo "usage: $0 start|stop"
esac
```

Para que el milter funcione se debe ejecutar el script, el cual inicializa postfix y utiliza clamav para revisar los virus.

./milter-postfix

## 10.4 Conclusiones

Debido a que la utilización de los milter no es muy común entre los servidores de correos se tuvo un poco de problemas para encontrar la información necesaria para su instalación y configuración, y aun mas debido a que para la revisión de virus dentro del correo electrónico la herramienta mas utilizada es MailScanner no se pudo obtener la documentación necesaria fácilmente, y además se ha encontrado en algunos foros de discusión en Internet que no es muy conveniente utilizar un milter ya que por lo general no son herramientas bien probadas, debido a que su uso es relativamente reciente sobre todo en postfix, y en lo que respecta a revisión de virus se utilice MailScanner.

Una desventaja de postfix en el uso de milters es que se debe tener instalado previamente sendmail para que estos funcionen, y además se necesita de un script de inicialización para que este funcione mientras que en sendmail simplemente se indica el milter en el archivo de configuración.

# CAPITULO 11
# CONCLUSIONES Y RECOMENDACIONES

## 11.1Conclusiones

Como se ha podido observar a lo largo del trabajo la instalación tanto de postfix como de sendmail ha cumplido con el objetivo final, el cual es transportar el correo desde su remitente hasta su destinatario final, siempre que el destinatario tenga un dominio válido y que el usuario exista.

La principal diferencia que se encontró entre los dos MTA es el manejo de los procesos internos de cada programa, y esto es debido a que postfix utiliza diferentes procesos para cada una de las acciones que realiza, con lo cual se tiene una sola instancia de postfix, el cual es el proceso master, y varios procesos que se ejecutan según lo que se esté realizando con el correo, sin embargo sendmail crea una instancia o proceso de si mismo por cada conexión que se realice, con lo cual se utilizan mas recursos del sistema en el que esté funcionando. Otra diferencia que tienen estos programas es que los privilegios que utiliza postfix para recibir y procesar correo son únicamente de su usuario, y utiliza privilegios de root únicamente para lo absolutamente necesario; en cambio sendmail, como se ejecuta como un solo proceso con diferentes parámetros, todo lo hace con privilegios de root lo cual deja abierta la posibilidad de intrusiones o vulnerabilidades en la seguridad del sistema.

La instalación del antivirus y antispam fue prácticamente igual en ambos programas, así como su funcionamiento, es decir en ambos casos se obtuvieron los resultados requeridos, y no se tuvo ningún inconveniente en la configuración de los mismos.

Una alternativa para la revisión de virus es la instalación de un milter, en este trabajo se realizo la instalación de clamav-milter, el cual hace la revisión del correo antes de que el MTA lo ingrese en la cola, en contraste con MailScanner que primero lo encola para revisarlo. Un inconveniente que tiene postfix en la instalación de un milter es que necesita de los archivos de sendmail para que funcione.

**Recomendaciones**

Debido al mejor desempeño de Postfix y sus mejores prestaciones en cuanto rendimiento, administración y capacidad de personalización, se convierte en la mejor opción al momento de instalar un servidor de gestión de correo empresarial, ya que en síntesis lo que requiere una empresa es una mayor seguridad, confiabilidad, flexibilidad y sobre todo con una inversión mínima en cuanto a hardware se refiere.

Si bien se ha tomado el tema de seguridad como punto a favor sobre Postfix, Sendmail sigue siendo el MTA de preferencia a nivel de Internet, esto debido a su facilidad de administración, compatibilidad y estandarización, lo cual lo hace atractivo principalmente para proveedores de Internet los cuales ofrecen cuentas de correo como parte de su servicio.

**GLOSARIO**

IP Protocolo de Internet (Internet Protocol)

POP Protocolo de Correo (Post Office Protocol)

IMAP Protocolo de acceso a mensajería en Internet (Internet Message Access Protocol)

SMPT Protocolo de transporte de mensajes simple (Simple Message Protocol Transfer)

DNS Servidor de Nombres de Dominio (Domain Name Server)

TTL Tiempo de vida o de Validez (Time to life)

MTA Agente de Trasnferecia de correo (Mail Transfer Agent)

MUA Agente de usuario de correo (Mail User Agent)

**BIBLIOGRAFIA**

Universidad del Azuay Curso de linux Disponible en la web:
<httpd://www.uazuay.edu.ec/linux/ >
[Fecha de ingreso: 04/12/2006]

Microsoft Corporation, Disponible en la web :
<http://www.microsoft.com/spain/empresas/tecnologia/uso_correo_competitivo.msp
x>
[Fecha de ingreso: 04/12/2006]

Red Hat, Inc Manual oficial de referencia de Red Hat Linux, Disponible en la web:
<http://www.europe.redhat.com/documentation/rhl8.0/rhl-rg-es-8.0/s1-email-
types.php3>
[Ref. Del 4 de diciembre del 2006]

Servicio de informática - Universidad de Valencia, Disponible en la web:
<http://www.uv.es/ciuv/cas/correo/email.html>
[Ref. Del 4 de diciembre del 2006]

Red Hut Documentation Agentes de transporte de correo, Disponible en la web:
<http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/es/ref-guide/s1-
email-mta.html>
[Ref. Del 4 de diciembre del 2006]

Red Hat, Inc. Introducción a Sendmail, Disponible en la web :
<http://www.europe.redhat.com/documentation/rhl7.1/rhl-rg-es-7.1/ch-
sendmail.php3>
[Ref. Del 4 de diciembre del 2006]

Enciclopedia Wikipedia. Correo electrónico - Wikipedia, la enciclopedia libre Disponible en la web: < http://es.wikipedia.org/wiki/Correo_electrónico>
[Ref. Del 17 de enero del 2007].

World Wide Webfoot Press, A Beginner's Guide to Effective Email
Domain Names Disponible en la web:
<http://webfoot.com/advice/email.domain.html>
[Ref. Del 17 de enero del 2007].

SnertSoft Milter solutions Disponible en la web:
<http://www.snertsoft.com/solutions.php>
[Ref. Del 17 de enero del 2007].

Security Architecture of mail Transfer Agents por Munawar Hafiz
Disponible en la Web:
<Https://netfiles.uiuc.edu/mhafiz/www/ResearchandPublications/mastersthesis/thesis.pdf>[Ref. Del 17 de enero del 2007].

Curso de Linux Avanzado por Fernando Ferrer Arquitectura de Postfix
Disponible en la web:
< http://fferrer.dsic.upv.es/cursos/Linux/Avanzado/HTML/ch07s03.html>
[Ref. Del 19 de enero del 2007].

Universidad Nacional Autónoma de México Departamento de cómputo
Disponible en la web:
< http://www.seguridad.unam.mx/doc/?ap=tutorial&id=182>
[Ref. Del 19 de enero del 2007].

El valle del Viento Helado Sendmail y filtrado: milter Disponible en la web:
<http://icewinddale.blogspot.com/2006/10/sendmail-y-filtrado-milter.html>
[Ref. Del 19 de enero del 2007].

Tutorial de Sendmail por David Rubert Viana Disponible en la web:
< http://www.marquezetelecom.com/LuCAS/Universitarios/tutorial-sendmail.html>
[Ref. Del 19 de enero del 2007].

Tutorial de Postfix por Fernando Limón Disponible en la web:
<http://panoramix.fi.upm.es/~flimon/Tutorial2.pdf>
[Ref. Del 21 de enero del 2007].

Tutorial de Sendmail por Diego Bravo Estrada
Disponible en la web:
< http://www.redes-linux.com/manuales/Servidor_correo/tutorial-sendmail.pdf>
[Ref. Del 21 de enero del 2007].

Spam Wikipedia , la enciclopedia libre Disponible en la web:
< http://es.wikipedia.org/wiki/Spam >
[Ref. Del 22 de enero del 2007].

Que es el Spam? Disponible en la web:
<http://www.geocities.com/SiliconValley/Way/4302/spam.html>
[Ref. Del 22 de enero del 2007].

Universidad de Cordoba Postfix: La nueva generación, por Luis Mendez
Disponible en la web:
<http://www.uco.es/ccc/sistemas/postfix/intro.html>
[Ref. Del 22 de enero del 2007].

SpamAssassin, Wikipedia, la enciclopedia libre Disponible en la web:
< http://en.wikipedia.org/wiki/SpamAssassin>
[Ref. Del 25 de enero del 2007].

Antivirus, Wikipedia, la enciclopedia libre Disponible en la web:
< http://es.wikipedia.org/wiki/Antivirus >
[Ref. Del 25 de enero del 2007].

Kriptolopis Clamav Disponible en la web:
<http://www.kriptopolis.org/node/1069>
[Ref. Del 25 de enero del 2007].

Osmosis Latina Configuración de Clamav Disponible en la web:
<http://www.osmosislatina.com/spamvirus/configuracionclamav.htm>
[Ref. Del 25 de enero del 2007].

Osmosis Latina Configuración de SpamAssasin Disponible en la web:
<http://www.osmosislatina.com/spamvirus/configuracionspamassassin.htm>
[Ref. Del 25 de enero del 2007].

Osmosis Que es spamassassin? que hace? que es clamav ? que hace? Disponible en la web: <http://www.osmosislatina.com/spamvirus/basico.htm>
[Ref. Del 25 de enero del 2007].

Postfix Organization Postfix Architecture Disponible en la web:
<http://www.porcupine.org/postfix/architecture.html>
[Ref. Del 26 de enero del 2007].

Postfix Organization Postfix Architecture Disponible en la web:
<http://www.postfix.org/architecture.html>
[Ref. Del 26 de enero del 2007].

The Postfix mail server as a secure programming example, Wietse Venema
IBM T.J. Watson Research Center Hawthorne, USA Disponible en la web:
<http://www.nycbsdcon.org/slides/postfix-key.ppt>
[Ref. Del 26 de enero del 2007].

Sendmail Inc. Open source milter solutions Disponible en la Web:
<http://www.sendmail.com/partners/milter/milter.detail/>
[Ref. Del 26 de enero del 2007].

Linux Dada Recursos informáticos Apéndice: Opciones avanzadas de seguridad para Sendmail Disponible en la Web:
< http://www.linuxdata.com.ar/index.php?idmanual=segsendmail.htm&manuale=1>
[Ref. Del 1 de febrero del 2007].

Sendmail Inc. Open source milter solutions Disponible en la Web:
<http://www.sendmail.com/partners/milter/milter.detail/>
[Ref. Del 1 de febrero del 2007].

MailScanner Installation Guide – Postfix Disponible en la web.
<http://www.mailscanner.info/install/postfix.shtml>
[Ref. Del 13 de Enero del 2007].

Tux_cl como implementar postfix + mailscanner + fprot Disponible en la Web:
<http://www.tux.cl/articulos:correo:como_implementar_postfix_mailscanner_f-prot>
[Ref. Del 13 de Enero del 2007].

Filtering Mail with Sendmail Disponible en la web:
<http://www.sendmail.org/doc/sendmail-current/libmilter/docs/ >
[Ref. Del 13 de Enero del 2007].

Postfix before-queue Milter support Disponible en la web:
<http://www.postfix.org/MILTER_README.html>
[Ref. Del 14 de Enero del 2007].

Antivirus para Sendmail con clam y milter Disponible en la Web:
<http://www.opensource.apple.com/darwinsource/Current/SpamAssassin-124.5/clamav/docs/Spanish/sendmail-Clam.html>
[Ref. Del 24 de Enero del 2007].

TestingInstallation - Spamassassin Wiki Disponible en la Web:
<http://wiki.apache.org/spamassassin/TestingInstallation>
[Ref. Del 24 de Enero del 2007].

SendMail (II) Configuración y manejo de Sendmail Disponible en la Web:
<http://es.tldp.org/Articulos-periodisticos/jantonio/sendmail/sendmail2.html>
[Ref. Del 25 de Enero del 2007].

Tux_cl - v4 configuracion de postfix Disponible en la Web:
<http://www.tux.cl/articulos:correo:postfix_-_guia_de_configuracion>
[Ref. Del 29 de Enero del 2007].

MailScanner - Wikipedia, the free enciclopedia Disponible en la Web:
<http://en.wikipedia.org/wiki/MailScanner>
[Ref. Del 30 de Enero del 2007].

What is MailScanner and what does it do Disponible en la web:
<http://www.bynari.net/esupport/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=104&nav=0,52>
[Ref. Del 30 de Enero del 2007].

IT Services Spam filtering Disponible en la Web:
<http://www.buckingham.ac.uk/its/spam/mailscanner.html>
[Ref. Del 30 de Enero del 2007].

Postfix Queue Management Disponible en la Web:
<http://www.porcupine.org/postfix/queueing.html>
[Ref. Del 30 de Enero del 2007].

Postfix Architecture Overview Disponible en la Web:
<http://www.postfix.org/OVERVIEW.html>
[Ref. Del 30 de Enero del 2007].

Postfix manual - qmgr(8) Disponible en la Web:
<http://www.postfix.org/qmgr.8.html>
[Ref. Del 30 de Enero del 2007].