

Servidor de eMail Courier-MTA - Parte 1

Me la paso recomendando Courier-MTA en todos lados. Hoy me llegó la hora: dejo de amenazar, y les presento esta maravillosa pieza de software... y comentarios de su autor.

El paquete Courier-MTA es un completo sistema de correo: provee servicio de ESMTP, POP3, IMAP, Webmail y panel administrativo y configuración via Web. Adicionalmente, soporta TLS y SSL para SMTP, POP3 e IMAP. Tiene un excelente soporte de usuarios y dominios virtuales, muy facil de utilizar, y las cuentas de usuarios se pueden almacenar en MySQL, PostgreSQL y OpenLDAP. ¿Les interesa probarlo?

Ante todo, es bueno saber de que si no queremos usar dominios virtuales, o sea, solamente vamos a "hostear" correo del dominio de nuestro servidor, entonces no es necesario utilizar un "backend" SQL o LDAP.

Adicionalmente, Courier-MTA posee un agente de distribución de correo(MDA - Mail Delivery Agent) llamado "maildrop" que a su vez incluye un lenguaje para armar avanzadas reglas de correo, que veremos en una próxima entrega, muy superiores a las ofrecidas por "procmail", y con un mejor manejo de recursos.

Adicionalmente, soporta los llamados "mailfilters", que permiten aplicar filtros muy complejos tanto al eMail entrante **como al saliente**. Trae un filtro de ejemplo escrito en Perl, llamado graciosamente "perlfiler". Siguiendo el ejemplo, un programador podria desarrollar los filtros en el lenguaje que desee.

En este artículo voy a suponer que ustedes están instalando un MTA desde cero, y no que están haciendo una migración de un sistema existente basado en otro MTA como Sendmail, Postfix, Exim o Qmail. Ya habrá tiempo más adelante, si les interesa, de tratar el tema en nuestras páginas. Por otra parte, voy a suponer que desean utilizar PostgreSQL para almacenar la configuración de usuarios, lo cual es mucho mas interesante que una configuración PAM, o sea, usando usuarios del sistema, y mucho más fucional y útil para futuros administradores de sistemas. La instalación y configuración de PostgreSQL corre por cuenta de ustedes, pero, obviamente, encontrarán en estas páginas las sentencias SQL necesarias para crear base de datos, tablas y usuarios.

Descarga

La última versión estable disponible al redactar este artículo es la 0.46. En el recuadro encontrarán la dirección directa de descarga de Courier-MTA y otros componentes. Vale destacar que Courier-IMAP y Maildrop vienen incluidos en el paquete Courier-MTA, no así el resto de los paquetes disponibles para descarga.

En Septiembre el autor liberó la primer herramienta de análisis de los logs de Courier, courier-analog, y me ha resultado de gran utilidad. Pueden descargarla desde la misma página.

MUY IMPORTANTE!

**Courier debe ser desempaquetado y compilado por un usuario que NO SEA ROOT!
Esto no es opcional, es OBLIGATORIO.**

Una vez descargado y desempaquetado encontraremos un archivo "INSTALL". Les recomiendo fervientemente que lo lean completo al menos antes de hacer nada. Courier es complejo, completo y muy seguro. Muchos de los pasos de la instalación son opcionales si es que solo deseamos una instalación simple, pero si deseamos alias en LDAP, carpetas compartidas en IMAP o envío y recepción de faxes... no nos quedará más remedio que prestarle mucha atención a esas secciones opcionales.

Atencion: si usan Gentoo, tan solo "emerge courier" será necesario. Recuerden agregar el servicio FAM - File Alteration Monitor y el courier al inicio del sistema:

```
rc-update add famd default
rc-update add courier default
```

Si desearan hilar fino en la instalación de paquetes adicionales usados por Courier, con *emerge -pv courier* podrán ver que banderas de USE pueden eliminar al emergear, por ejemplo, para remover el soporte MySQL, dejando PostgreSQL:

```
USE="-mysql postgres" emerge courier
```

Pasos Necesarios Antes de Compilar

Antes de compilar el código, es necesario crear un usuario y grupo **courier**:

```
groupadd courier
useradd -g courier courier
```

Si no lo hicieran el script configure de courier intentará usar "daemon" o algún usuario/grupo similar, pero siempre es buena práctica de seguridad separar los tantos.

Los usuarios que deseen cambiar en que directorio debe ir cada componente de courier (manpages, archivos de /etc, binarios, queue, etc) pueden hacerlo con switches del script configure que pueden obtener con:

```
./configure --help
```

desde el directorio creado al desempaquetar el tar de courier. Por defecto todo se instala por debajo de /usr/lib/courier, pero podríamos elegir guardar la configuración solamente en /etc/courier, esto lo haríamos con:

```
./configure --sysconfdir=/etc/courier
```

O tal vez, si deseamos cambiar el path /usr/lib/courier, deseemos usar el parámetro --prefix:

```
./configure --prefix=/algun/otro/directorio
```

Para ahorrar un poco de tiempo, podemos elegir deshabilitar todos los módulos de autenticación que no vamos a utilizar, agregando los siguientes parámetros a la línea de comandos de ./configure:

```
--without-authpam
--without-authldap
--without-authpwd
--without-authmysql
--without-authshadow
--without-authuserdb
--without-authvchkpw
```

ATENCIÓN:

Muchos paquetes de software permiten utilizar parámetros de configure para cambiar directorios y habilitar/deshabilitar funciones, etc. Revisen detalladamente la salida del comando `./configure --help | less` para conocerlos todos.

Compilación

Una vez ejecutado `./configure`, con o sin parámetros especiales, la compilación de courier sigue, casi, los pasos comunes que ya todos conocen. Desde el directorio raíz de la distribución de Courier-MTA, ingresen los siguientes comandos.

```
make
make check
```

El "make check" es opcional, pero no está de más, ya que realiza pruebas de los módulos compilados y otros aspectos del sistema en relación al MTA. Si llegara a fallar, lo más probable es que puedan solucionar el problema aplicando algunos parámetros del script `./configure`. Va más allá del propósito de este artículo analizar las causas posibles de fallo.

Si todo sale bien, ahora deberán hacer "su" al usuario root. En este caso usamos "su" a secas, y no "su -", para no cambiar el directorio actual. Recuerden que el desempaquetado y `./configure` lo hicieron con un usuario diferente.

Una vez con root, cambien su umask al valor 022 (lo que implica "por defecto tomar permisos 755 para directorios, y 644 para archivos"). Esto lo logran con el siguiente comando:

```
umask 022
```

Ahora, con los siguientes comandos, se copiará Courier-MTA a `/usr/lib/courier`, si es que no modificamos el default, ni el `sysconfdir`. Nótese que usamos "install-strip" en vez del común "install". El `install-strip` remueve los símbolos de depuración de los binarios que se instalen, haciéndolos más pequeños. Por supuesto, podríamos usar "make install" si quisieramos mantener los símbolos de depuración:

```
make install-strip
make install-configure > upgrade.log
```

El "make install-configure" permite actualizar la configuración de un Courier que ya se encontrara instalado, pero solo a partir de la versión 0.30. (Ver `INSTALL` para detalles), manteniendo la configuración previa, y agregando las diferencias de la nueva versión. No

es un paso opcional, debemos aunque no tengamos una version anterior de Courier. En el ejemplo, redireccionamos su salida al archivo upgrade.log, que sería interesante revisáramos posteriormente.

Configurando Courier-MTA

Una vez realizado el `make install-configure`, podemos cambiar al directorio definido como `sysconfdir`. Por defecto, este será `/usr/lib/courier/etc`. Desde allí editaremos varios archivos. Debemos utilizar un editor de texto plano (`joe`, `nano`, `vi`, `jed`, `emacs`). A continuación, un listado de los archivos a editar, y un detalle de los parámetros MINIMOS a modificar. Los archivos de configuración están muy bien comentados, y las páginas del manual en `/usr/lib/courier/man` son excelentes y pueden ser vistas con el Midnight Commander.

* **authdaemonrc** En la línea 27 aproximadamente, definir `authmodulelist` con el valor `"authpgsql"`, correspondiente a PostgreSQL.

* **authmodulelist** Tan solo debe contener una línea, la cadena `"authdaemon"`.

* **bofh** Ingresar `BOFHBADMIME=accept` para evitar que los emails enviados por clientes que hagan uso incorrecto de MIME (Ciertas versiones de Outlook) no sean descartados.

* **courierd** Línea 79 aproximadamente, `DEFAULTDELIVERY=./Maildir`. Línea 97 aprox., `ESMTP_CORK=1`.

* **esmtpd** Línea 41 aproximadamente, `BOFHCHECKDNS=1`

Línea 47 aproximadamente, `BOFHNOEXPN=1`

Línea 53 aproximadamente, `BOFHNOVRFY=1`

Línea 264 aproximadamente, `TCPDOPTS="-nodnslookup -noidentlookup"`

Línea 277 aproximadamente, `AUTHMODULES="authdaemon"`

Línea 297 aproximadamente, `ESMTPAUTH="LOGIN CRAM-MD5"`

Línea 326, al final, `ESMTPDSTART=YES`

* **locals** La primera línea será `"localhost"`, y la segunda, el contenido del archivo `/etc/HOSTNAME`. Por ejemplo, `murray.buanzo.com.ar`. No se refiere a un dominio de mail (lo posterior a la arroba).

* **me** Contendrá una única línea, y será el dominio de email local, por ejemplo `buanzo.com.ar`

* **pop3d** Línea 45, aproximadamente, `AUTHMODULES="authdaemon"`

Línea 123, aproximadamente, `TCPDOPTS="-nodnslookup -noidentlookup"`

Línea 142, al final, `POP3DSTART=YES`. Este archivo configura los parámetros del demonio POP3.

* **aliases/system** En la línea 22 aproximadamente, definir el alias `postmaster`. Ejecutar `../sbin/makealiases`. Este archivo permite armar aliases y redireccionamientos tanto a direcciones de email múltiples como a programas.

* **smtpaccess/default** Este archivo configura quienes pueden enviar email (hacer relay) utilizando nuestro servidor. Por defecto se le da permiso a todas las redes privadas y al loopback, 127.x.x.x. Ejecutar ../sbin/makesmtpaccess

Iniciando el Servicio

Por supuesto, aún falta definir direcciones de eMail, pueden esperar al próximo número, o hacerlo como tarea para el hogar. Los invito a bajar el script de inicio de Courier (ver recuadro). El archivo se llama couriermta. Ubiquenlo en el directorio /etc/init.d, /etc/rc.d/init.d o similar de su distribución, y vincúlenlo al inicio del sistema. Con Gentoo, ya vimos como hacerlo, y no necesitan este archivo. Con otras distribuciones que tengan chkconfig, pueden usar el siguiente comando:

```
cp couriermta /etc/init.d
chmod +x /etc/init.d/couriermta
chkconfig -a couriermta
```

Si dicho comando no funcionara, intenten con:

```
chkconfig --add couriermta ; chkconfig --level 235 couriermta on
```

En la segunda parte de esta nota, todo lo referente a PostgreSQL en combinación con Courier-MTA y algunos detalles de seguridad. Disfruten la entrevista a Sam Varshavchik, autor de Courier-MTA!

Entrevista a Sam Varshavchik, Autor de Courier.

USERS - Contanos un poco acerca de vos.

Soy programador para varias compañías financieras de la ciudad de Nueva York. Nací en Rusia, y a los 11 emigré a los Estados Unidos. Terminé la Licenciatura en Ciencias de la Computación, y desde entonces trabajo por aquí.

USERS - ¿Qué es lo que más te gusta de Courier-MTA?

Hace lo que necesito. Desarrollé Courier después de haber probado casi todo MTA existente, pero no encontré ninguno que hiciera todo lo que yo hubiera querido. Por lo tanto, reinventando un poco, hice uno.

USERS - Si tuvieras que convencer a nuestros lectores de probarlo... ¿Qué les dirías?

Pregunta complicada. Francamente, Courier no es para principiantes. Aunque muchas personas pudieron tomar e instalarlo sin muchas complicaciones. creo que es mejor tener una cierta experiencia de administración y mantenimiento de servidores de correo, y un moderado conocimiento de las tecnologías vinculadas al correo electrónico. Courier es complejo, eso se ve por el contenido del archivo INSTALL. Esperen dedicarle algo de tiempo para tenerlo instalado y funcionando.

USERS - ¿Han existido vulnerabilidades, de cualquier clase, en Courier-MTA?

Han habido vulnerabilidades propias, creo yo, de las de cualquier software de este nivel de complejidad, pero nada serio. Las vulnerabilidades eran mayormente en partes de Courier raramente usadas, o no habilitadas por default en lo más mínimo. Por ejemplo, al principio de este año hubo un error XSS (Cross-Site Scripting, posibilidad de inyectar código JavaScript o similar en una página para que sea ejecutado desde otra) en el Webmail, pero solo si utilizabas el comando "Ver Cabeceras Completas". Muy poca gente ve las cabeceras de los mails. El año pasado hubo algunos bugs en las funciones de conversión de un juego de caracteres de Asia Oriental, que no es compilado por default. Hubo una vulnerabilidad de SQL Injection (N. del T. Ver recuadro) en el driver MySQL, y una de agotamiento de CPU en el servicio IMAP, causado por correos corruptos. También hubo una hace unos meses en las funciones de depuración de logs, que no se habilitan por default.

USERS - ¿Qué funcionalidad pensás agregar a largo plazo?

Pienso trabajar en funcionalidad vinculada al trabajo en grupo (N.del T. "groupware"), y en todo lo que se me vaya cruzando por la cabeza.

USERS - ¿Cómo es la relación entre Courier-MTA, sus usuarios y vos?

Hay un par de listas de correo. La principal, courier-users, es bastante grande, con varios miles de suscriptores. Courier tiene sus fans y detractores, como cualquier otro paquete

Open Source. Mi personalidad me lleva a participar activamente en las listas y en grupos de USENET. (N.del T. Es muy raro que Sam no responda consultas.)

USERS - ¿Qué funcionalidad Anti-Spam provee Courier?

Courier tiene varias APIs internas de filtrado. Podrían ser mejoradas, y planeo hacerlo en el futuro proximo. Puede utilizar listas negras basadas en DNS (DNSBLS) como cualquier otro servidor de mail, pero la próxima versión traerá soporte para SPF - Sender Policy Framework (N. del T. Ver recuadro). Se pueden configurar que tan permisivo el Courier-MTA en relación a las RFC, MIME, etc. Un montón de Spam es generado por aplicaciones que no respetan dichos estándares, y podemos usar eso. Desafortunadamente, tambien hay clientes de correo que no los respetan.

USERS - ¿Algo que quieras agregar?

Si! Mucha gente olvida que Courier trae un módulo de configuración basado en web, muy completo. Por otra parte, la proxima versión de Courier traerá incorporado un analizador de logs, courier-analog, con reportes de uso de IMAP, POP3 y SMTP.

Websites de referencia:

- **Courier-MTA** : <http://www.courier-mta.org/>
- **Download** : <http://www.courier-mta.org/download.php>
- **Script de Inicio**: <http://www.buanzo.com.ar/couriermta>
- **SQL Injection**:
<http://www.hernanracciatti.com.ar/document/sql.pdf>
- **SPF** : <http://www.argo.es/~jcea/antispam/spf.htm>

©Arturo A. Busleiman 2004

e-mail: buanzo@buanzo.com.ar

Este artículo es de distribución y modificación libres; el autor mantiene el derecho de copia.