Cómo configurar Sendmail y Dovecot con soporte SSL/TLS.

Autor: *Joel Barrios Dueñas*
Correo electrónico: *darkshram en gmail punto com*
Sitio de Red: *http://www.alcancelibre.org/*
Jabber ID: *darkshram@jabber.org*

Introducción.

Este documento requiere la lectura y comprensión previa de los siguientes temas:

- Configuración básica de Sendmail (Parte I).
- Configuración básica de Sendmail (Parte II).

Acerca de DSA.

DSA (**D**igital **S**ignature **A**lgorithm o Algoritmo de Firma digital) es un algoritmo creado por el NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology o Instituto Nacional de Normas y Tecnología de EE.UU.), publicado el 30 de agosto de 1991, como propuesta para el proceso de firmas digitales. Se utiliza para firmar información, más no para cifrar ésta.
URL: http://es.wikipedia.org/wiki/DSA

Acerca de RSA.

RSA, acrónimo de los apellidos de sus autores, Ron **R**ivest, Adi **S**hamir y Len **A**dleman, es un algoritmo para el ciframiento de claves públicas que fue publicado en 1977, patentado en EE.UU. en 1983 por el el Instituto Tecnológico de Michigan (**MIT**). **RSA** es utilizado ampliamente en todo el mundo para los protocolos destinados para el comercio electrónico.

URL: http://es.wikipedia.org/wiki/RSA

Acerca de X.509.

X.509 es un estándar **ITU-T** (estandarización de **T**elecomunicaciones de la **I**nternational **T**elecommunication **U**nion) para infraestructura de claves públicas (**PKI**, o **P**ublic **K**ey **I**nfrastructure). Entre otras cosas, establece los estándares para certificados de claves públicas y un algoritmo para validación de ruta de certificación. Este último se encarga de verificar que la ruta de un certificado sea válida bajo una infraestructura de clave pública determinada. Es decir, desde el certificado inicial, pasando por certificados intermedios, hasta el certificado de confianza emitido por una Autoridad Certificadora (**CA**, o **C**ertification **A**uthority).

URL: http://es.wikipedia.org/wiki/X.509

Acerca de OpenSSL.

OpenSSL es una implementación libre, de código abierto, de los protocolos **SSL** (**S**ecure **S**ockets **L**ayer o Nivel de Zócalo Seguro) y **TLS** (**T**ransport **L**ayer **S**ecurity, o Seguridad para Nivel de Transporte). Está basado sobre el extinto proyecto **SSLeay**, iniciado por Eric Young y Tim Hudson, hasta que éstos comenzaron a trabajar para la división de seguridad de EMC Corporation.

URL: http://www.openssl.org/

Procedimientos.

Entretenimiento (87/0)
Equipamiento lógico (Software) (272/0)
Humor (49/0)
Internet (164/0)
Juegos (59/0)
Manuales y documentos (99/0)
Música (17/0)
Negocios y empresas (214/0)
Noticias Generales (788/0)
Nuestro idioma (8/0)
Opiniones (95/0)
Programación y desarrollo (56/0)
Seguridad (119/0)
Sustento Físico (Hardware) (71/0)
Tiras cómicas (17/0)
Ubunteando (33/0)

Están en línea...

Registrados: 6
darth_tradd
fuentes_adrian
josech
robokick
woly1980
yasmany
Invitados: 568
Últimos registrados:
EsseleDrugs
inickmickat
aluctuack
TRAREEEVOTT
attineapilt
Total registrados: 1532

Foro de soporte

Índice Foro
Miembros del sitio
Temas populares

Participan...

Noticias
joelbarrios (1871)
bartoloco (133)
Koalasoft (115)
capotes (88)
bakara (59)
Flaquita (49)
The One (47)
gomezbjesus (45)
domingov (43)
aLb3rT (37)
ValeriaBueno (30)
adrianpazr (21)
varisti (21)
yucleto (16)
linuxfrog (14)

Comentarios
joelbarrios (235)
Koalasoft (180)
aLb3rT (137)
gomezbjesus (83)
The One (61)
Oscar Hernández (53)
juanroberto (47)
Cause (39)

Acceda al sistema como el usuario **root**.

Se debe crear el directorio donde se almacenarán los certificados para todos los sitios SSL. El directorio, **por motivos de seguridad**, debe ser solamente accesible para el usuario **root**.

```
mkdir -m 0700 /etc/ssl
```

A fin de mantener cierta organización, es conveniente crear un directorio específico para almacenar el certificado del servidor. Igualmente, **por motivos de seguridad**, debe ser solamente accesible para el usuario **root**.

```
mkdir -m 0700 /etc/ssl/midominio.org
```

Acceder al directorio que se acaba de crear.

```
cd /etc/ssl/midominio.org
```

Sendmail.

Generando clave y certificado.

Sendmail requiere una llave creada con algoritmo **DSA** de 1024 octetos. Para tal fin, se crea primero un fichero de parámetros **DSA**:

```
openssl dsaparam 1024 -out dsa1024.pem
```

A continuación, se utiliza este fichero de parámetros **DSA** para crear una llave con algoritmo **DSA** y estructura **x509**, así como también el correspondiente certificado. En el ejemplo a continuación, se establece una validez por 730 días (dos años) para el certificado creado.

```
openssl req -x509 -nodes -newkey dsa:dsa1024.pem
-days 730 -out sendmail.crt -keyout sendmail.key
```

Lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.

La salida devuelta sería similar a la siguiente:

```
Generating a 1024 bit DSA private key
writing new private key to 'sendmail.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:
Mi empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:
midominio.org
Email Address []:webmaster@midominio.org
```

El certificado solo será válido cuando el servidor de correo electrónico sea invocado con el nombre definido en el campo **Common Name**. Es decir, solo podrá utilizarlo cuando se defina **midominio.org** como servidor **SMTP** con soporte **TLS**. No funcionará si se invoca al servidor como, por mencionar un ejemplo, **mail.midominio.org**.

Al terminar, ya no será necesario conservar el fichero **dsa1024.pem**, mismo que puede eliminarse con plena seguridad.

```
rm -f dsa1024.pem
```

Es indispensable que todos los ficheros de claves y certificados tengan permisos de acceso de solo lectura para el usuario **root**:

```
chmod 400 /etc/ssl/midominio.org/sendmail.*
```

Parámetros de /etc/mail/sendmail.mc.

Es necesario configurar los siguiente parámetros en el fichero

/etc/mail/sendmail.mc a fin de que Sendmail utilice la clave y certificado recién creados:

```
define(`confCACERT_PATH',`/etc/ssl/midominio.org')
define(`confCACERT',`/etc/ssl/midominio.org/sendmail.crt')
define(`confSERVER_CERT',`/etc/ssl/midominio.org/sendmail.crt')
define(`confSERVER_KEY',`/etc/ssl/midominio.org/sendmail.key')
```

Solo resta activar el puerto que será utilizado para SMTPS (465 por TCP).

```
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTA, M=s')dnl
```

El acceso cifrado con TLS es opcional si se realizan conexiones a través del puerto 25, y obligatorio si se hacen a través del puerto 465. El puerto 587 (submission), puede ser también utilizado para envío de correo electrónico. Por estándar se utiliza como puerto alternativo en los casos donde un cortafuegos impide a los usuarios acceder hacia servidores de correo trabajando por puerto 25. MS Outlook Express no tiene soporte para usar TLS a través del puerto 587, pero el resto de los clientes de correo electrónico con soporte TLS si.

```
DAEMON_OPTIONS(`Port=submission, Name=MSA, M=Ea')dnl
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio sendmail.

```
service sendmail restart
```

Comprobación.

Realice una conexión con **telnet** al puerto 25 del sistema. Ingrese el mandato **EHLO**. La salida deberá devolver, entre todas las funciones del servidor, una línea que indica **STARTTLS**. La salida puede ser similar a la siguiente:

```
telnet 127.0.0.1 25
EHLO midominio.org

Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 midominio.org ESMTP Sendmail 8.13.1/8.13.1; Mon, 2 Oct 2006
13:18:02 -0500
ehlo midominio.org
250-midominio.org Hello localhost.localdomain [127.0.0.1], pleased to
meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH LOGIN PLAIN
250-STARTTLS
250-DELIVERBY
250 HELP
```

Al realizar la configuración del cliente de correo electrónico, deberá especificarse conexión por TLS. Tras aceptar el certificado, deberá ser posible autenticar, con nombre de usuario y clave de acceso, y enviar correo electrónico.

Dovecot.

Generando clave y certificado.

La creación de la llave y certificado para **Dovecot** es más simple, pero requiere utilizar una clave con algoritmo **RSA** de 1024 octetos, con estructura **X.509**. En el ejemplo a continuación, se establece una validez por 730 días (dos años) para el certificado creado.

```
openssl req -x509 -nodes -newkey rsa:1024
-days 730 -out dovecot.crt -keyout dovecot.key
```

De forma similar a como ocurrió con **Sendmail**, lo anterior solicitará se ingresen varios datos:

- Código de dos letras para el país.
- Estado o provincia.
- Ciudad.
- Nombre de la empresa o razón social.
- Unidad o sección.
- Nombre del anfitrión.
- Dirección de correo.

La salida devuelta sería similar a la siguiente:

```
Generating a 1024 bit RSA private key
................++++++
.++++++
writing new private key to 'dovecot.key'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name
or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:MX
State or Province Name (full name) [Berkshire]:Distrito Federal
Locality Name (eg, city) [Newbury]:Mexico
Organization Name (eg, company) [My Company Ltd]:
Mi empresa, S.A. de C.V.
Organizational Unit Name (eg, section) []:Direccion Comercial
Common Name (eg, your name or your server's hostname) []:
midominio.org
Email Address []:webmaster@midominio.org
```

El certificado solo será válido cuando el servidor de correo electrónico sea invocado con el nombre definido en el campo **Common Name**. Es decir, solo podrá utilizarlo cuando se defina **midominio.org** como servidor **POP3** o **IMAP** con soporte **TLS**. No funcionará si se invoca al servidor como, por mencionar un ejemplo, **mail.midominio.org**.

Es indispensable que todos los ficheros de claves y certificados tengan permisos de acceso de solo lectura para el usuario **root**:

```
chmod 400 /etc/ssl/midominio.org/dovecot.*
```

Parámetros de /etc/dovecot.conf.

En el parámetro **protocols**, se activan todos los servicios (imap, imaps, pop3 y pop3s).

```
protocols = imap imaps pop3 pop3s
```

De modo predeterminado, el soporte SSL de **Dovecot** está activo. Verifique que el parámetro **ssl_disable** tenga el valor **no**, o bien solo esté comentado.

```
#ssl_disable = no
```

Y se especifican las rutas del certificado y clave a través de los parámetros **ssl_cert_file** y **ssl_key_file**, del siguiente modo:

```
ssl_cert_file = /etc/ssl/midominio.org/dovecot.crt
ssl_key_file = /etc/ssl/midominio.org/dovecot.key
```

A fin de que surtan efecto los cambios, es necesario reiniciar el servicio **dovecot**.

```
service dovecot restart
```

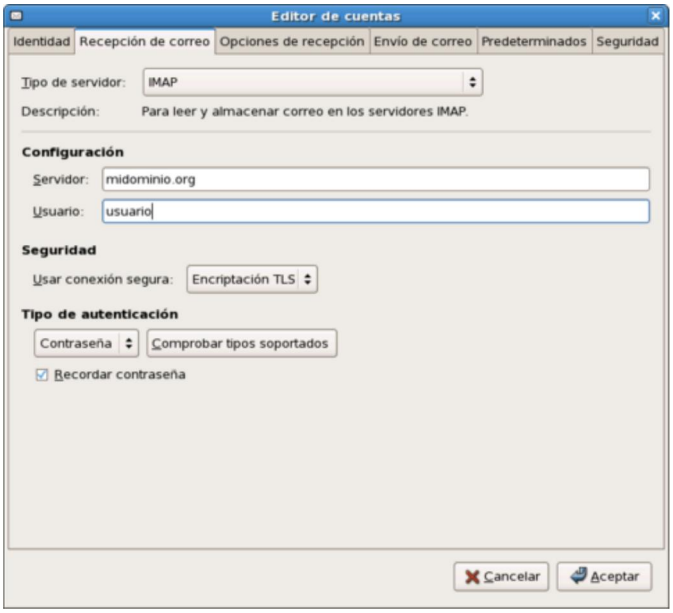
Comprobación.

Utilice cualquier cliente de correo electrónico con soporte para TLS y configure éste para conectarse hacia el sistema a través de **IMAPS** (puerto 993) o bien **POP3S** (puerto 995). Tras aceptar el certificado del servidor, el sistema deberá permitir autenticar, con nombre de usuario y clave de acceso, y realizar la lectura del correo electrónico.

Configuración de GNOME Evolution.

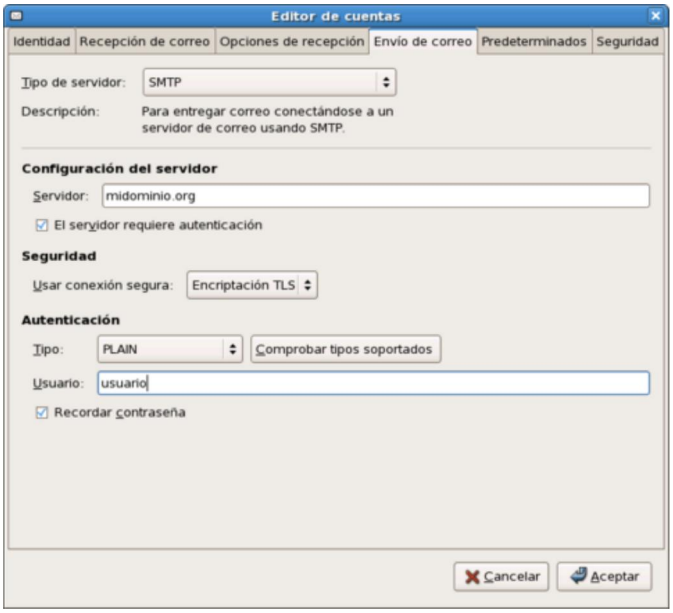
Configuración GNOME Evolution.

Para GNOME Evolution, la configuración de IMAP o POP3 se realiza selecionando el tipo de servidor, definiendo el nombre del servidor utilizado para crear el certificado, nombre de usuario, y usar encriptación segura TLS.



Configuración IMAP, en GNOME Evolution.

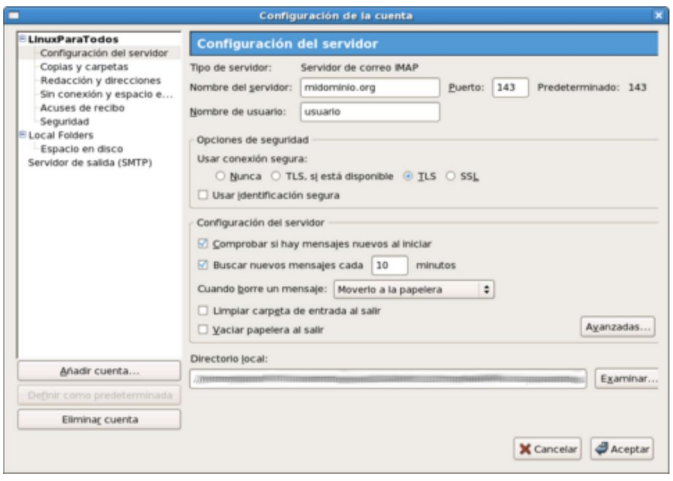
Se hace lo mismo para SMTP.



Configuración SMTP, GNOME Evolution.

Configuración Mozilla Thunderbird.

Para Mozilla Thunderbird, se define el nombre del servidor utilizado para crear el certificado, usuario y usar conexión segura TLS.



Configuración IMAP, Mozilla Thunderbird.

Se hace lo mismo para SMTP.

Configuración SMTP, Mozilla Thunderbird.

Modificaciones necesarias en el muro cortafuegos.

Si se utiliza un cortafuegos con políticas estrictas, como por ejemplo **Shorewall**, es necesario abrir, además de los puertos 25, 110, 143 y 587 por TCP (**SMTP**, **POP3**, **IMAP** y **Submission**, respectivamente), los puertos 465, 993 y 995 por TCP (**SMTPS**, **IMAP** y **POP3S**, respectivamente).

Las reglas para el fichero **/etc/shorewall/rules** de **Shorewall** correspondería a algo similar a lo siguiente:

```
#ACTION SOURCE  DEST    PROTO   DEST            SOURCE
#                               PORT            PORT(S)1
ACCEPT  net     fw      tcp     25,110,143,465,587,993,995
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Última Edición lunes 17 de marzo de 2008 @ 02:45 CST | 7,840 Hits

Noticias Recientes

- Jim Zemelin: Se necesita un esfuerzo concertado de Linux en ultra-portátiles para derrotar a Microsoft.
- Genesys presenta su principal evento mundial: G-Force 2009
- ZENworks Application Virtualization 7 de Novell asegura una implementación de aplicaciones fácil y segura
- ¿10 razones por las cuales GNOME es mejor que KDE 4?
- SegInf amplia sus horizontes hacia el noreste de México.
- Google Earth reveló ubicación de base nuclear británica.
- Primera actualización de Altiris desde que fue adquirido por Symantec.
- Hay fuertes rumores del lanzamiento de ultra-portátil de Apple.
- FFmpeg finalmente publica la versión 0.5.
- Microsoft intenta manipular la Unión Europea.

Comentarios Recientes

- ¿10 razones por l... [+2]
- >
- Cómo recabar info... [+2]
- ¿Necesitas una ca... [+5]
- Más información a...
- Desventajas de us... [+3]
- Dreamweaver tiene... [+3]
- ¿Cómo escribir un... [+2]
- ¿Has oido de la A... [+2]
- Demanda de Micros...

Enlaces Recientes

- GatoLinux
- Re-Vapaus
- RadioEQUIS
- Blog de Cesar Rodas
- Hosting Santiago
- Tuxsoul
- Gruslic
- Empleos TI - Bolsa de trabajo de Sistemas e Informatica
- Fedora Live USB
- Webmin