

Configurar un certificado SSL en un servidor Debian

Introducción

El protocolo SSL (Secure Socket Layer) está destinado a encriptar de manera segura los datos intercambiados entre dos máquinas. En su servidor dedicado, puede ser útil utilizar SSL con el fin de proteger datos sensibles.

Encontrará más información sobre el funcionamiento de SSL en esta página.

Procedimiento

Antes de poder activar/generar un certificado SSL, hace falta verificar que la opción está bien activada en su máquina. En la Release, Apache ha sido compilado por defecto con SSL; basta con indicarle dónde debe adquirir el certificado al iniciarse.

Esta guía le ayudará a configurar el SSL con la distribución Debian.

Preparativos y pasos previos

Requisitos

- Un nombre de dominio
 - Un certificado SSL para este nombre de dominio o uno de los subdominios
 - Suponemos que la clave privada, la cadena de certificación y el certificado han sido colocados en el directorio `/root/` de su servidor dedicado.
-
- Un servidor dedicado con la distribución Debian
 - Acceso al servidor a través de SSH (mediante root) : `SshSobreServidorDedicado`

Añadir IP Fail-over

Cada certificado está unido a una única IP. Para no utilizar la IP principal, en este ejemplo añadimos una IP Fail-over y la configuramos como Alias.

Para ello siga las guías : IpFailover y NuevoAliasIp

Instalar los paquetes

Actualice las fuentes y a continuación instale **apache2** y **openssl** :

```
debian:~# apt-get update
```

```
debian:~# apt-get install apache2 openssl
```

Configuración de Apache

Edite el fichero **/etc/apache2/ports.conf** con ayuda del comando **nano** y añada la línea **Listen 443** a continuación de **Listen 80** :

Acerca del editor **nano** : CTRL+O => para guardar – CTRL+X => para salir

```
ns3773:~# cat /etc/apache2/ports.conf
Listen 80
Listen 443
```

Cree ahora los enlaces simbólicos siguientes para cargar el módulo SSL en Apache 2 :

```
debian:~# ln -s /etc/apache2/mods-available/ssl.load /etc/apache2/mods-enabled/ssl.load
```

```
debian:~# ln -s /etc/apache2/mods-available/ssl.conf /etc/apache2/mods-enabled/ssl.conf
```

Puesta en marcha del certificado SSL

Descargue los **ficheros del certificado** disponibles en su proveedor :

- private.key
- certificate-chain.crt
- certificate.crt

Suponemos que la clave privada, la cadena de certificación y el certificado han sido colocados en el directorio /root/ de su servidor dedicado.

```

debian:~# mkdir /etc/apache2/ssl.crt/
debian:~# cd /etc/apache2/ssl.crt/
debian:~# cp /root/private.key ./
debian:~# cp /root/certificate-chain.crt ./
debian:~# cp /root/certificate.crt ./
debian:~# chmod 400 private.key
debian:/etc/apache2/ssl.crt# ll
total 24
drwxr-xr-x 2 root root 4096 2007-11-02 18:00 .
drwxr-xr-x 8 root root 4096 2007-11-02 18:02 ..
-rw-r--r-- 1 root root 5637 2007-11-02 18:00 certificate-chain.crt
-rw-r--r-- 1 root root 1982 2007-11-02 18:00 certificate.crt
-r----- 1 root root 1743 2007-11-02 18:00 private.key

```

Para que Apache no solicite la passphrase de la clave privada cada vez que se inicie, es recomendable desencriptar la clave previamente:

```
# openssl rsa -in private.key > private-deprotect.key
```

Si desea hacerlo, reemplace private.key por private-deprotect.key a lo largo de la guía.

Puesta en marcha del Virtual host

Con ayuda de un editor de texto como **pico**, edite el fichero **/etc/apache2/mods-enabled/ssl.conf**

Añada las líneas siguiente antes del identificador </IfModule> :

```
NameVirtualHost 87.xx.xxx.xx:443

<VirtualHost 87.xx.xxx.xx:443>
ServerAdmin postmaster@mi_dominio.com
DocumentRoot /home/mi_login/www
Servername www.mi_dominio.com
SSLEngine on
SSLCertificateFile /etc/apache2/ssl.crt/certificate.crt
SSLCertificateKeyFile /etc/apache2/ssl.crt/private.key
SSLCACertificateFile /etc/apache2/ssl.crt/certificate-chain.crt
ScriptAlias /cgi-bin/ /home/mondamai/cgi-bin/
</VirtualHost>
```

El login de su espacio en este caso es **mi_login** y el espacio web está en **/home/mi_login/www**. Esto puede cambiar en función de su configuración.

Finalización

Reinicie Apache para leer la nueva configuración:

```
debian:~# /etc/init.d/apache2 restart
debian::/etc/apache2/ssl.crt#/etc/init.d/apache2 restart
Forcing reload of web server (apache2)... waiting Apache/2.2.3 mod_ssl/2.2.3 (Pass Phrase Dialog)
```

Si no ha descriptado la clave privada, indique su contraseña passphrase solicitada – es aquella que ha indicado durante la creación de la llave privada **private.key**):

Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

```
Server www.mi_dominio.com:443 (RSA)
Enter pass phrase:
```

```
OK: Pass Phrase Dialog successful.
```

En caso de error, revise el fichero de LOG **/var/log/apache2/error.log**

Verifique que Apache funciona bien en el puerto 443 :

```
debian:~# netstat -tanpu | grep ":443"
```

```
tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN 11015/apache2
```

Haga la prueba en https://www.mi_dominio.com/

Volver a las guías sobre SSL en OVH : [GuiaSSL](#)

Más información

: [RecupSSL](#) :: Gestión del certificado SSL de OVH

: [ServidorSSL](#) :: Certificados SSL en un servidor dedicado Release 1

: [ServidorCertificados](#) :: Certificados SSL en un servidor dedicado Release 2

: [PleskCertificadosSSL](#) :: Certificados SSL en un servidor dedicado Plesk