

# Configurar un certificado SSL de OVH en la Release2 (Gentoo)

## 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 de pago adquirido en OVH con la distribución Release 2.

## Preparativos y pasos previos

### Requisitos

- Un nombre de dominio en OVH
- Un certificado SSL para este nombre de dominio o uno de los subdominios, adquirido en OVH (en el ejemplo **www.mi\_dominio.com**) : PedidoSsl
  
- Un servidor dedicado con la distribución OVH Release 2 (Gentoo)
- 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 con ayuda del OVHm como Alias.

Para ello siga las guías : IpFailover y NuevoAliasIp

## Configuración de Named

Si el dominio ya estaba configurado con la IP principal, deberá modificar la configuración para que apunte a la IP Fail-over.

Si está ya apuntando a la IP Fail-over definitiva, puede pasar a la etapa siguiente.

Edite el fichero `/var/bind/pri/mi_dominio.com.hosts` con ayuda del comando **nano**, indicando la IP Fail-over para el dominio o el subdominio de su certificado, en nuestro caso `www.mi_dominio.com` :

**Atención** : No olvide añadir el serial SOA al día de hoy: (**AAAAMMDD01**), en nuestro ejemplo 2007102901 (29 de octubre de 2007)

```
# nano /var/bind/pri/mi_dominio.com.hosts
```

Una vez modificado pulse :

- CTRL+O => para guardar
- CTRL+X => para salir

```
$ttl 86400
```

```
mi_dominio.com. IN SOA mi_dominio.com. webmaster.mi_dominio.com. (
```

```
2007103001
```

```
21600
```

```
3600
```

```
604800
86400 )
IN NS nsXXXXX.ovh.net.
IN NS sdns1.ovh.net.
IN MX 10 mail.mi_dominio.com.
IN A 213.xxx.xxx.xxx
www IN A 87.xx.xxx.xx
ftp IN A 213.xxx.xxx.xxx
mail IN A 213.xxx.xxx.xxx
```

A continuación reinicie el servidor de DNS (named) :

```
# /etc/init.d/named restart
```

Ahora debe esperar 24–48 horas a que se propaguen las modificaciones.

Cuando se propaguen los nuevos registros por el sistema de cachés de DNS, el dominio apuntará a la nueva IP y funcionará correctamente.

Verifique que el dominio funciona en :

- [http://www.mi\\_dominio.com](http://www.mi_dominio.com)

## Activar SSL en Apache

Primero verificamos si el Apache está funcionando en el puerto 443.

Para ello miramos si aparece la línea :

```
# grep ^Listen /etc/httpd/ssl.conf  
Listen 443
```

Si no aparece la línea **Listen 443**, significa que está comentada y el SSL está inactivo.

Para activarlo, edite el fichero y retire el carácter # de la línea :

```
# nano /etc/httpd/ssl.conf
```

Una vez modificada la línea y guardado el fichero, reiniciamos apache :

```
# /etc/init.d/apache restart
```

Por último, verifique que Apache está escuchando en el puerto 443 :

```
# netstat -tanpu | grep ":443"  
tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN 8965/httpd
```

## Descarga del certificado SSL

En un primer tiempo, el certificado tiene que estar en el directorio **/root/certificado/**.

Para ello, descargamos los .crt disponibles en el Manager v3 : MANAGER > Certificados SSL > Recuperar el certificado SSL y los situamos, junto con la clave privada en el directorio **/root/certificado/**.

El procedimiento nos arroja los tres ficheros del certificado :

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

## Activar el certificado

### Requisitos

- Suponemos que la clave privada, la cadena de certificación y el certificado, están situados en el directorio **/root/certificado/** de su servidor dedicado.
- El dominio ya está instalado sobre la IP Fail over correspondiente.
- El apache tiene SSL activado y funcionando en el puerto 443.

### Puesta en marcha del certificado SSL

Primero copiamos la clave privada del comando :

```
# cd /etc/httpd/ssl.key/  
# cp /root/certificado/private.key ./  
# pwd ; ll private.key
```

```
/etc/httpd/ssl.key  
-rw-r--r-- 1 root root 1743 oct 31 14:42 private.key
```

```
# chmod 400 private.key  
# pwd ; ll private.key
```

```
/etc/httpd/ssl.key  
-r----- 1 root root 1743 oct 31 14:42 private.key
```

```
#
```

Luego, para que Apache no nos pida la clave cada vez que inicia, añadimos la clave descriptada :

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

A partir de ahora, utilizaremos la clave descriptada **private-deprotect.key** en el resto de la guía.

Luego copiamos los certificados en el directorio de SSL de Apache :

```
# cd /etc/httpd/ssl.crt/
# cp /root/certificado/certificate* ./
# pwd ; ll certificate*

/etc/httpd/ssl.crt
-rw-r--r-- 1 root root 5637 oct 31 14:44 certificate-chain.crt
-rw-r--r-- 1 root root 1982 oct 31 14:44 certificate.crt

#
```

### **Puesta en marcha del Virtual Host**

A continuación, con ayuda del comando **nano**, modificamos el fichero **/etc/httpd/ssl.conf**.

```
# nano /etc/httpd/ssl.conf
```

Insertamos 3 elementos obligatorios :

- **La clave privada**
- **El certificado**
- **La cadena de certificación**

Añada las líneas siguientes, antes de `</IfDefine>` :

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

<VirtualHost 87.xx.xxx.xx:443>
ServerAdmin postmaster@mi_dominio.com
DocumentRoot /home/mi_login/www
SuexecUserGroup mi_login users
Servername www.mi_dominio.com
SSLEngine on
SSLCertificateFile /etc/httpd/ssl.crt/certificate.crt
SSLCertificateKeyFile /etc/httpd/ssl.key/private-deprotect.key
SSLCACertificateFile /etc/httpd/ssl.crt/certificate-chain.crt
```

Activar el certificado

```
Customlog logs/mi_login-acces_log combined
ScriptAlias /cgi-bin/ /home/mi_login/cgi-bin/
</VirtualHost>
```

**Atención : mi\_login** es el login de su espacio web /home/mi\_login/ del dominio correspondiente y deberá cambiarse en función de la configuración.

Ahora renicie Apache :

```
# /etc/init.d/apache restart
* Stopping apache2 ... [ ok ]
* Starting apache2 ... [ ok ]
```

En caso de error al iniciar Apache, consulte los ficheros de logs :

- /var/log/httpd/error\_log
- /var/log/httpd/error\_ssl\_log

Si no ha utilizado **private-deprotect.key**, le solicitará la contraseña al iniciar Apache :

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

Una vez iniciado correctamente Apache, el certificado está instalado.

Para verificarlo, realice el test de acceso a :

- [https://www.mi\\_dominio.com/](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