

Configuración del certificado SSL de OVH en Plesk

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 en Plesk

Antes de poder activar/generar un certificado SSL, hace falta verificar que la opción está bien activada en su máquina.

En Plesk, 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 Plesk.

Requisitos

- Un nombre de dominio en OVH (en el ejemplo **www.mi_dominio.com**)
- Un certificado SSL para este nombre de dominio o uno de los subdominios, adquirido en OVH : PedidoSsl

- Un servidor dedicado con la distribución Plesk (acceso mediante admin)
- Acceso al servidor a través de SSH (mediante root) : SshSobreServidorDedicado

Preparativos y pasos previos

Antes de entrar en Plesk hay que realizar varias operaciones :

- Descarga del certificado SSL del Manager
- Desencriptar la clave SSL por SSH

- Añadir IP Fail-over en el Manager

Descarga del certificado SSL del Manager

En un primer tiempo, el certificado tiene que descargar el certificado a su ordenador.

Para ello, descargamos los ficheros del certificado, disponibles a través del Manager v3

Seleccione el certificado deseado, en la sección : **Certificado SSL**.

Haga clic en el icono *Recuperar el certificado SSL* de la sección **Acciones** :

Recuperar el certificado SSL

Desde esta página es posible descargar los siguientes ficheros del certificado :

- www.mi_dominio.com.cert
- www.mi_dominio.com.key
- www.mi_dominio.com.chain

Nota : En la mayoría de los casos la clave privada **mi_certificado.key** estará ya en su posesión y no será posible descargarla.

Necesita estos ficheros para añadir el certificado.

Descargamos estos ficheros y los situamos, junto con la clave privada en el directorio de su elección en su ordenador.

Desencriptar la clave SSL

Si ha utilizado un "passphrase", debe realizar una desprotección para obtener el fichero **private-deprotect.key** .

Nota : Necesitará la clave privada desencriptada : **private-deprotect.key** para poder cargarla en Plesk.

Esta operación se debe realizar a través de SSH en su servidor dedicado :

```
nsXXXXXX:~# openssl rsa -in private.key > private-deprotect.key
```

Para conectarse a SSH a su servidor, consulte la guía : [SshSobreServidorDedicado](#)

Añadir IP Fail-over en el Manager

Proceda a asignar la IP Fail-over asignada a la IP principal de su servidor desde el Manager v3

Seleccione el servidor que desea gestionar de la lista desplegable (nsXXXXXX.ovh.net).

Haga click en la sección *Servicios*

Servicios

Encontrará la opción *IP Failover* en la rúbrica **Servicios adicionales**

IP Failover

Para mover la IP inversa de una dirección IP de la lista pulse la opción *Mover*

Modificar

Configurar el certificado en Plesk

Una vez en Plesk bastan 2 simples operaciones para configurar el certificado :

- Añadir el certificado
- Añadir la IP Fail-over

Añadir el certificado

Diríjase al Plesk (<https://nsXXXXX.ovh.net:8443/>) y entre con su usuario admin.

Vaya a la sección *Servidores*

Servidores

Seleccione *Certificados*
Certificados

Haga clic en *Nuevo certificado*
Nuevo certificado

Aparecerá una pantalla para definir un certificado :

Crear un nuevo certificado SSL

Certificado

- Nombre del certificado* :

Preferencias

...

Enviar el fichero de un certificado

- Clave privada :
- Certificado :
- Certificado CA :

Enviar ficheros

Indique en la primera línea el nombre de su certificado (en nuestro ejemplo `www.mi_dominio.com`)

Rellene las últimas líneas (Cargar un certificado externo) con los ficheros de su certificado de OVH.

Rellene los campos y cargue los ficheros :

- la clave descriptada : **private-deprotect.key**
- el certificado : **www.mi_dominio.com.crt**
- la cadena de certificado CA : **www.mi_dominio.com.chain**

Por último haga clic en **Enviar ficheros**

Añadir IP Fail-over al Plesk

Una vez añadido el certificado, podemos añadir la nueva IP Fail-over.

Vaya a *Servidores*

Servidores

Seleccione *Dirección IP*

Dirección IP

Pluse *Nueva Dirección IP*

Nueva Dirección IP

Añada la nueva dirección IP Fail-over en eth0 con la máscara 255.255.255.255.

Selección **Compartida** y escoja el certificado que acaba de añadir **www.mi_dominio.com**

Activar el certificado

Atención : Esta manipulación modificará la zona DNS de su dominio para modificar la IP principal del dominio a la IP Fail-over.

Asignar IP Fail over al dominio

Para asignar la IP Fail over, diríjase al Plesk, en la sección *Dominios*

Dominios

Seleccione el dominio del certificado (en nuestro ejemplo *mi_dominio.com*).

Haga clic en *Configurar*

Configurar

Seleccione la IP Fail over definida previamente.

Marque la casilla **Soporte SSL**

Reiniciar el servicio Web

Finalmente, reinicie el servicio Web en Plesk.

Para ello, vaya a la sección *Servidor*
Servidor

Haga clic en Gestión de servicios

Gestión de servicios

Y por último haga clic en reiniciar [icono amarillo] para el **servidor WEB (Apache)**.

Compruebe el acceso en :

- `https://www.mi_dominio.com/`

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

Más información

: [ManualUtilizacionPlesk](#) :: [Manual Utilización Plesk](#)

: [PleskAvanzado](#) :: [Opciones avanzadas en Plesk](#)