Crear un VirtualHost con https en Apache

Para poder utilizar el protocolo seguro, debemos tener instalado el módulo que maneja la capa de conexión segura o *SSL*:

```
sudo a2enmod ssl
service apache2 restart
```

Por otro lado, tenemos que asegurarnos de que *Apache* es capaz de “escuchar” por el puerto 443, que es el que utiliza por defecto este protocolo. Tendremos que editar el archivo */etc/apache2/ports.conf* y confirmar que tiene una línea tal como esta:

```
Listen 443
```

Que normalmente se activará a condición de que *Apache* tenga activado el módulo correspondiente.

Ahora tenemos que encargarnos de crear el *Host Virtual* activando el *site default-ssl*:

```
sudo a2ensite default-ssl
```

Tenemos ahora que editar el archivo de configuración de este *Host Virtual*, señalando donde se encuentran el archivo del certificado y el archivo de la clave del certificado:

```
sudo gedit /etc/apache2/sites-available/default-ssl.conf
```

Y editamos las líneas antes mencionadas:

```
SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

Y finalizamos reiniciando apache:

```
sudo service apache2 restart
```

Si queremos ver el funcionamiento de nuestro servidor *https*, ponemos la siguiente *URL* en nuestro navegador:

```
https://localhost
```

Crear un certificado autofirmado

En los pasos previos hemos creado un servidor web mediante *https* utilizando los archivos de certificado que incluye por defecto el *SSL*. Si queremos crear nuestro propio certificado autofirmado tendremos que seguir los siguientes pasos:

1. Generar la clave:

```
sudo openssl genrsa -out miclave.key 2048
```

2. Crear la petición de certificado. Esto nos pedirá a continuación una serie de datos:

```
sudo openssl req -new -key miclave.key -out mipeticion.csr
```

3. Obtener el certificado autofirmado:

```
sudo openssl x509 -req -days 365 -in mipeticion.csr -signkey miclave.key -out micertificado.crt
```

4. Mover los archivos a sus directorios correspondientes de *SSL*:

```
sudo mv miclave.key /etc/ssl/private/
sudo mv micertificado.crt /etc/ssl/certs/
```

5. Editar las siguientes líneas del archivo de configuración del host:

```
SSLCertificateFile /etc/ssl/certs/micertificado.crt
SSLCertificateKeyFile /etc/ssl/miclave.key
```

6. Reiniciar *Apache*:

```
sudo service apache2 restart
```

Por último añadir que si quisiéramos crear un servicio https en un Host Virtual podríamos hacerlo modificando los parámetros ya sabidos ServerName y DocumentRoot en el archivo de configuración.