

1. Installation d'apache

apt-getinstall apache2

2. Activation du module ssl

Avant de commencer toute manipulation sur les fichiers de configuration apache, commençons par arrêter le serveur :

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

partie de apache, il suffit pour l'activer d'utiliser la commande a2enmod

```
# a2enmod ssl
```

3. Créer un hôte virtuel pour le site en https

il va falloir créer deux hôtes virtuels : un pour le port 80 et un pour le port 443.

Ajoutons un fichier *mondomaine.https* dans */etc/apache2/sites-available* contenant en plus des lignes habituelles les lignes suivantes :

```
NameVirtualHost *:443

<VirtualHost *:443>
    ...
    ...
    # add ssl protocol
    SSLEngine On
    SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
    SSLCertificateFile /etc/ssl/certs/server.crt
    SSLCertificateKeyFile /etc/ssl/private/server.pem
</VirtualHost>
```

Une fois terminé la configuration de l'hôte virtuel, on peut l'ajouter à la liste des sites à servir au démarrage de apache.

```
# a2ensite nom_du_site
```

Création du certificat serveur

Génération d'une clé privée pour le serveur

```
#openssl genrsa -out server.pem 1024
```

2. Génération d'une requête de création d'un certificat

A partir de votre clé, vous allez créer un fichier de demande de signature de certificat (CSR CertificateSigningRequest).

La demande de certificat est générée avec la commande suivante :

```
#openssl req -new -key server.pem -out server.csr
```

➤ Le fichier server.csr contient la clé publique à certifier.

3. Signature du certificat

Afin de signer le certificat deux possibilités sont offertes :

- Auto signer le certificat

- Signer le certificat par une autorité de certification (AC)

3.a. Auto signature d'un certificat

La commande suivante permet d'auto- signer votre certificat (le signer à l'aide de votre propre clé privée).

```
#openssl x509 -req -days 365 -in server.csr -signkey server.pem -out server.crt
```

Installation du certificat

Il vous reste plus qu'à installer votre certificat et votre clé privée dans le répertoire `/etc/ssl`

```
# cp server.crt /etc/ssl/certs
# cp server.pem /etc/ssl/private
```

Démarrage de apache

Et enfin à redémarrer votre serveur web :

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

Si vous avez protégé votre clé par un mot de passe, vous serez alors invité à saisir celui-ci.