

Installation du service HTTPS



Sommaire.

- 1 Installation d'OpenSSL
- 2 Sécuriser d'OpenSSL

1- Installation d'OpenSSL.

Pour sécuriser les données transférées entre le serveur et le client, il faut crypter ces échanges.

Pour cela il faut installer et créer un certificat ssl , puis configurer le serveur Apache.

Pour installer OpenSSL, saisir :

```
root# apt-get install openssl
```

2- Création d'un certificat.

Pour créer le certificat, il faut créer un répertoire pour le stocker.

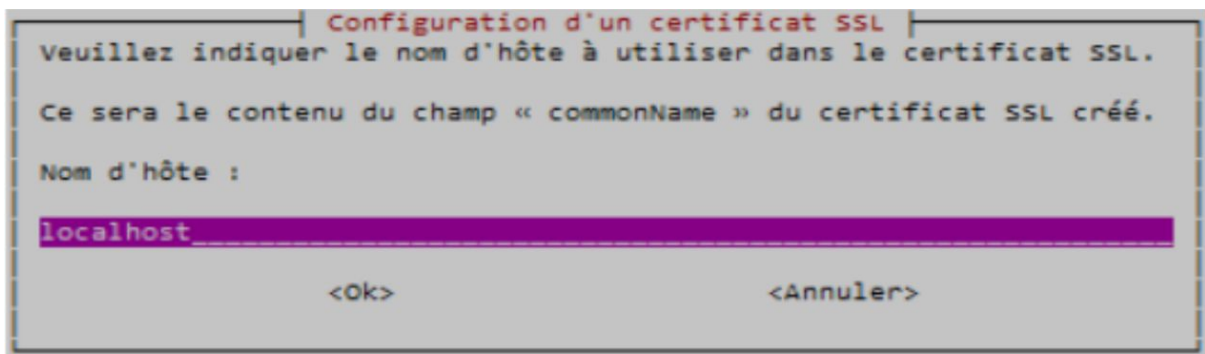
Saisir :

```
root# mkdir /etc/apache2/ssl
```

Ensuite, nous allons créer le certificat avec la commande :

```
root#/usr/sbin/make-ssl-cert /usr/share/ssl-cert/ssleay.cnf  
/etc/apache2/ssl/apache.pem
```

Ensuite, une interface apparaît.



Configuration d'un certificat SSL

Veuillez indiquer le nom d'hôte à utiliser dans le certificat SSL.
Ce sera le contenu du champ « commonName » du certificat SSL créé.

Nom d'hôte :

localhost

<Ok> <Annuler>

Saisir : « ok » . Laisser vide et saisir : « ok »

3- Configuration d'Apache.

Vérifier que le serveur Apache soit maintenant écouter sur le port 443 (port pour le HTTPS). :

```
root#nano /etc/apache2/ports.conf
```

```
<IfModule ssl_module>  
    Listen 443  
</IfModule>  
  
<IfModule mod_gnutls.c>  
    Listen 443  
</IfModule>
```

4- Activation du module.

Pour activer le module ssl :

```
root#a2enmod ssl
```

Pour activer le virtualhost ssl

```
root#a2ensite default-ssl
```

Redémarrer ensuite le service Apache

```
root #/etc/init.d/apache2 restart
```

5 Test du protocole https.

Se rendre sur un navigateur et saisir dans la barre de recherche :



Vérifier dans l'url de la page que *https* soit présent. Comme ceci.



Il existe différents types de certificats ssl qui permettent de vérifier certains éléments sur la valeur du site web et de l'entreprise qui le gère. Pour cela je vous propose de suivre ce lien qui explique les différences entre ceux-ci.

<https://www.globesign.fr/fr/centre-information-ssl/types-certificats-ssl/>