Louise ISABEL

2SLAM

Rédiger un document expliquant comment on peut obtenir un certificat et reconfigurer un serveur APACHE

Un certificat SSL (Secure Sockets Layer) permet de sécuriser les échanges de données sur internet en chiffrant les informations entre le serveur et le client. Le protocole SSL est aujourd'hui remplacé par TLS (Transport Layer Security), mais le terme SSL est encore couramment utilisé pour désigner les certificats de sécurité. Ce rapport va expliquer comment obtenir un certificat SSL gratuit et configurer votre serveur Apache.

Étape 1 : Obtenir un certificat SSL gratuit

Il existe plusieurs moyens pour obtenir un certificat SSL, mais l'une des méthodes les plus courantes et gratuites est d'utiliser **Let's Encrypt**. Let's Encrypt est une autorité de certification gratuite qui permet d'obtenir un certificat SSL facilement. Voici les étapes pour obtenir un certificat avec Let's Encrypt :

1.1 Installer Certbot

Certbot est un outil gratuit qui permet d'automatiser la demande et le renouvellement des certificats SSL Let's Encrypt. Pour l'installer, suivez les étapes ci-dessous en fonction de votre système d'exploitation.

Debian :

```
sudo apt update
sudo apt install certbot python3-certbot-apache
```

1.2 Obtenir le certificat SSL

Une fois Certbot installé, vous pouvez obtenir le certificat SSL en utilisant la commande suivante :

```
sudo certbot --apache
```

Certbot va automatiquement vérifier votre serveur, générer le certificat et le configurer pour Apache. Vous devrez spécifier votre adresse e-mail et accepter les conditions d'utilisation.

1.3 Vérification de la configuration

Une fois le certificat installé, Certbot configure généralement Apache pour qu'il utilise automatiquement le certificat SSL. Vous pouvez vérifier que votre site est bien sécurisé en visitant `https://votre-domaine` et en vous assurant qu'il affiche un cadenas vert dans la barre d'adresse.

Étape 2 : Configurer Apache pour utiliser le certificat SSL

Si vous n'avez pas utilisé Certbot ou que vous souhaitez configurer manuellement votre serveur Apache, voici les étapes pour ajouter un certificat SSL à votre serveur Apache.

2.1 Localiser les fichiers du certificat SSL

Après avoir obtenu le certificat SSL, vous devez localiser les fichiers du certificat. Let's Encrypt les place généralement dans le répertoire `/etc/letsencrypt/live/nom-de-domaine/` :

- **Certificat public** : `/etc/letsencrypt/live/nom-de-domaine/cert.pem`
- **Clé privée** : `/etc/letsencrypt/live/nom-de-domaine/privkey.pem`
- **Chaîne de certificats** : `/etc/letsencrypt/live/nom-de-domaine/chain.pem`

Si vous avez un autre fournisseur de certificat SSL, vous devriez recevoir ces fichiers après avoir demandé votre certificat.

2.2 Modifier le fichier de configuration d'Apache

Ouvrez le fichier de configuration d'Apache pour votre site, généralement situé dans le répertoire `/etc/apache2/sites-available/` ou `/etc/httpd/sites-available/`. Le fichier peut s'appeler `000-default.conf`, `default-ssl.conf` ou le nom de votre site.

Voici un exemple de configuration pour activer SSL sur Apache :

```
<VirtualHost *:443>
    ServerAdmin webmaster@votre-domaine.com
    ServerName votre-domaine.com
    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/letsencrypt/live/votre-domaine/cert.pem
    SSLCertificateKeyFile
/etc/letsencrypt/live/votre-domaine/privkey.pem
    SSLCertificateChainFile
/etc/letsencrypt/live/votre-domaine/chain.pem
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
</VirtualHost>
```

2.3 Activer SSL dans Apache

Si vous n'avez pas encore activé le module SSL d'Apache, vous devez le faire. Exécutez la commande suivante pour activer le module SSL et le site SSL par défaut :

```
sudo a2enmod ssl
sudo a2ensite default-ssl.conf
```

Ensuite, redémarrez Apache pour appliquer les changements :

```
sudo systemctl restart apache2
```

Screen de notre site certifié avec Let’s Encrypt comme indiqué :

(nous utilisons un domaine à mon nom que j’avais déjà, pour le marieteam, étant cheffe de projet)

Général | Détails

Émis pour

Nom commun (CN)	marieteam.louiseisabel.fr
Organisation (O)	<Ne fait pas partie du certificat>
Unité d'organisation (OU)	<Ne fait pas partie du certificat>

Émis par

Nom commun (CN)	R10
Organisation (O)	Let's Encrypt
Unité d'organisation (OU)	<Ne fait pas partie du certificat>

Durée de validité

Émis le	mercredi 15 janvier 2025 à 08:15:43
Expire le	mardi 15 avril 2025 à 09:15:42

Empreintes SHA-256

Certificat	71ed4ea2db2fc7985489126b0aed0e1578d6c0ad49429b79fdd3f78fef731ad3
Clé publique	6a6fde738a27cbc504d79af6bfce82d1af022702bf37cdbd5546decae321d78e