Mise en place d'un certificat SSL sur Apache 2

Emetteur(s) : Saviard Matthieu

Destinataire(s) : Jury BTS SIO

Date : 25/02/2024

Objet : Certificat SSL sur un serveur Apache2

1. Contexte

Les certificats SSL sont essentiels pour le référencement et la confiance des utilisateurs sur un site web. En chiffrant les données échangées entre le navigateur et le serveur, ils garantissent la sécurité des informations sensibles, ce qui est pris en compte par les moteurs de recherche dans le classement des pages.

L'utilisation du protocole HTTPS, rendu possible par les certificats SSL, est également un critère de référencement positif. Les navigateurs signalent la présence de certificats SSL, renforçant la confiance des utilisateurs grâce à des indicateurs visuels de sécurité.

En réduisant les risques de piratage et en assurant la conformité aux normes de sécurité, les certificats SSL contribuent à une expérience utilisateur positive, ce qui est devenu un facteur crucial tant pour le référencement que pour la fidélisation des visiteurs.

2. Mise en place du service SSL

On commence par installer notre service SSL sur notre machine avec la commande suivante →

```
root@debian:~# apt install openssl -y
```

On va ensuite générer notre certificat SSL avec la commande suivante →

openssl: C'est la commande principale pour interagir avec OpenSSL, une bibliothèque open-source pour la mise en œuvre des protocoles de sécurité SSL/TLS.

req: Indique que l'action à effectuer concerne les certificats de requête (request).

-x509: Spécifie que le certificat généré sera auto-signé au lieu d'être signé par une autorité de certification externe.

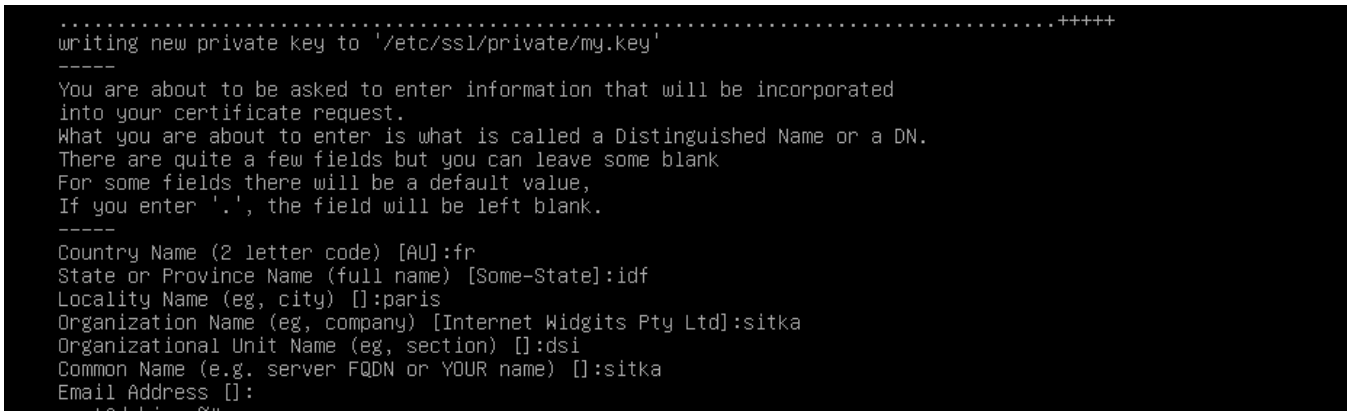
-days 365: Définit la durée de validité du certificat en jours, dans cet exemple, le certificat sera valide pendant 365 jours.

-newkey rsa:2048: Génère une nouvelle paire de clés RSA de 2048 bits, avec une clé privée et une clé publique. La clé privée sera sauvegardée dans le fichier spécifié par l'option -keyout et la clé publique sera utilisée pour générer le certificat.

-keyout /etc/ssl/private/my.key: Indique le chemin où la clé privée générée doit être sauvegardée. Dans cet exemple, la clé privée sera enregistrée dans le fichier /etc/ssl/private/my.key.

-out /etc/ssl/certs/my.crt: Indique le chemin où le certificat auto-signé généré doit être sauvegardé. Dans cet exemple, le certificat sera enregistré dans le fichier /etc/ssl/certs/my.crt.

Ensuite on rentre nos infos sur le certificat SSL qui nous enregistrera →



On va ensuite créer un répertoire mine dans /var/www/mine

```
Email Address []:
root@debian:~# mkdir /var/www/mine
root@debian:~#
```

On créé dedans un fichier index.html, qui sera l'outil pour vérifier que notre site fonctionne bien →

```
root@debian:~# nano /var/www/mine/index.html_
```

On met une petite phrase →

```
  GNU nano 5.4
welcome to sitka.local
```

On donne le full access au compte de service www-data à notre index.html créé

```
root@debian:~# chown -R www-data.www-data /var/www/mine/_
```

Ainsi que pour notre repertoire /mine

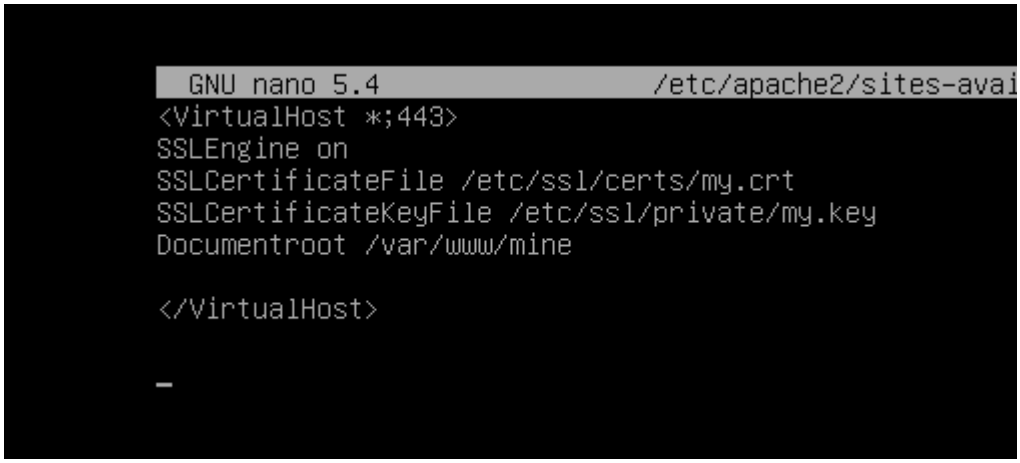
```
root@debian:~# chown -R www-data.www-data /var/www/mine/
root@debian:~# chmod -R 775 /var/www/mine/
root@debian:~#
```

On va ensuite créer notre fichier de configuration SSL dans /etc/apache2/sites-available

```
root@debian:~# nano /etc/apache2/sites-available/mine-ssl.conf_
```

On remplit toutes les lignes suivantes →

- SSLEngine on : autorise le chiffrement SSL
- SSLCertificateFile /etc/ssl/certs/my.crt : c'est le chemin de notre certificat
- SSLCertificateKeyFile : c'est le chemin de notre clé SSL
- Documentroot : le chemin de notre dossier racine
- Port 443 → c'est le port HTTPS



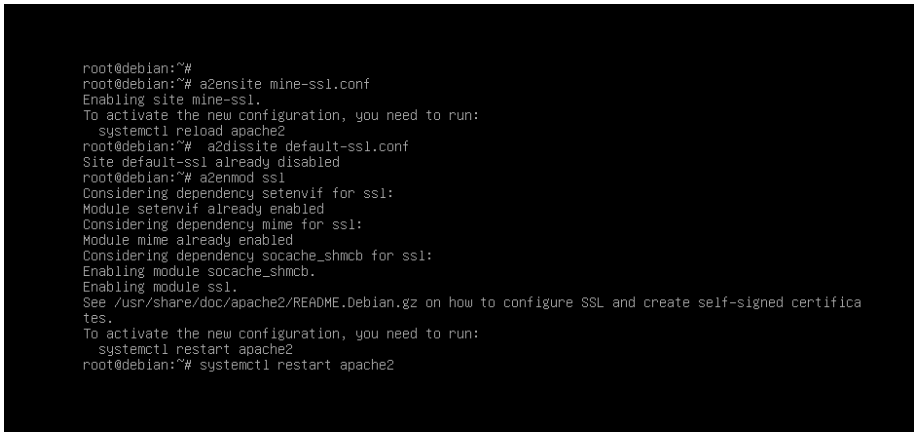
Ensuite on exécute les commandes suivantes →
On va tout d'abord activer notre fichier de conf SSL et désactiver celui par défaut, activer le SSL et relancer le service →

A2ensite mine-ssl.conf

A2dissite default-ssl.conf

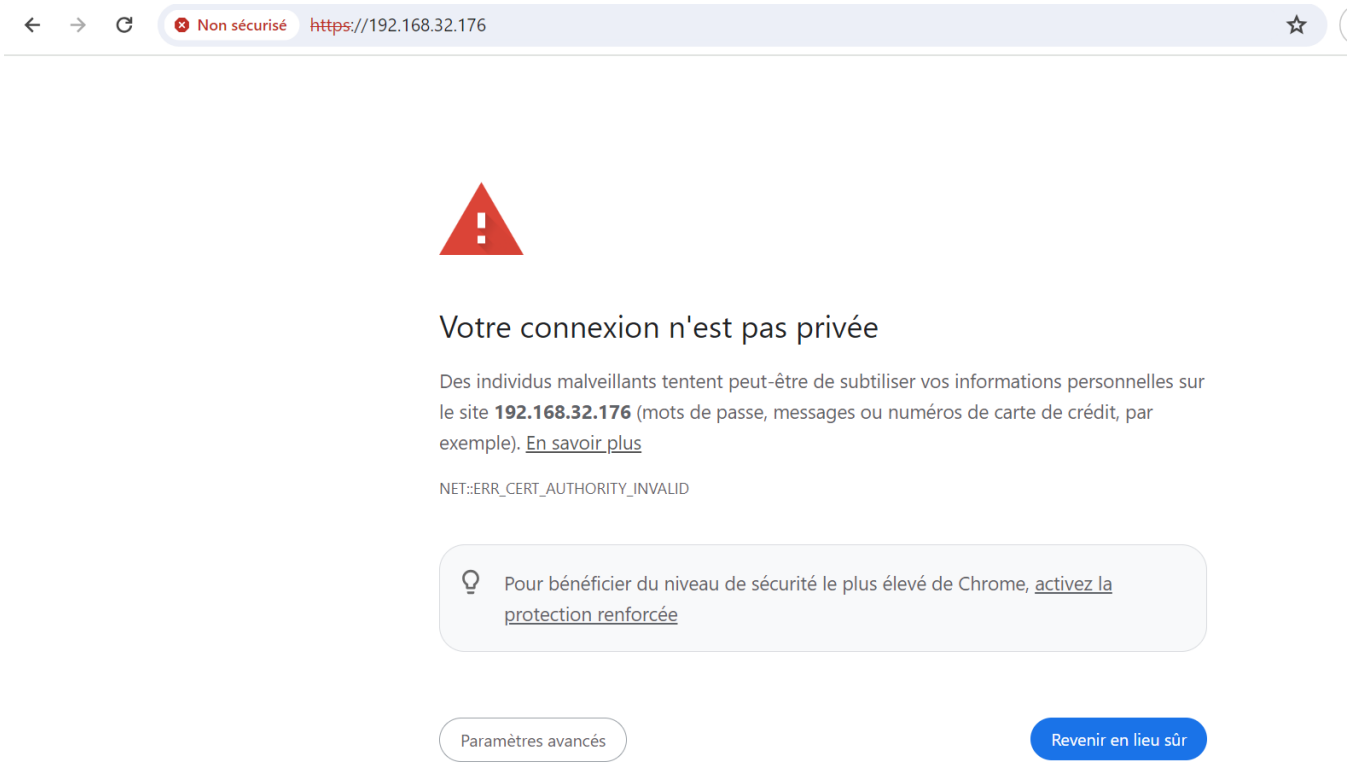
A2enmod ssl

Systemctl reload apache2

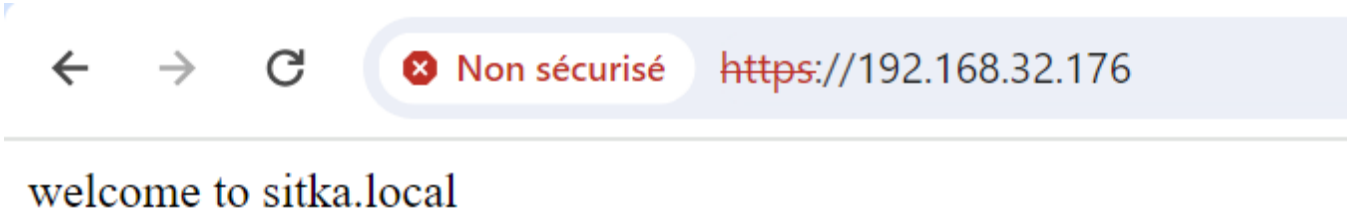


Une fois dans le navigateur on tape https://192.168.32.176

Faire « Paramètres avancés »→ « Continuer vers le site 192.168.32.176 (dangereux) »



Et on a bien notre page web →



Le contenu affiche que le site est malveillant car notre certificat SSL est auto signée, dans le cadre de production, il faudra un certificat valide et vérifié. En tout cas, notre connexion elle est sécurisée sur le port 443 et accessible en HTTPS.

3. Conclusion

Notre site est donc accessible :

- Sur le port 443 de HTTPS
- On a un chiffrement avec le SSL

Notre site sera donc mieux référencé, et nous auront ainsi une meilleure visibilité sur Internet.

Cependant il est important de noter que même si un site est en HTTPS, cela ne veut pas dire qu'il n'est pas frauduleux