Apache2 - Configuration HTTPS

Difficulté : Intermédiaire

Notions : Chiffrement, Certificats, HTTPS

I. Introduction

Afin de sécuriser les flux vers le serveur web et garantir l'authenticité de la communication avec le partenaire, il est nécessaire de passer à la version sécurisée du protocole HTTP. Qui est le HTTPS.

Cette procédure vise à mettre en place la configuration nécessaire sur le serveur apache2.

> **Prérequis** : Un serveur apache2 doit être installé et fonctionnel.

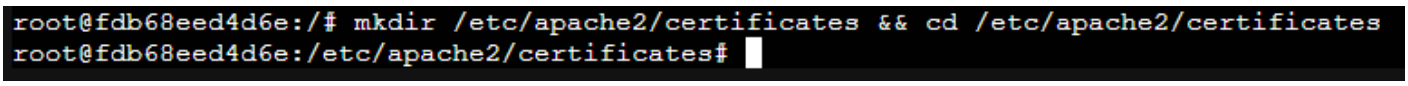
II. Génération des certificats

2.1 Cas du certificat auto-signé

> **Attention**: cette méthode chiffre les communications mais ne garantit pas forcément l'identité du serveur. En effet, pour que cela soit le cas, il faudra faire signer sa requête par une autorité de certification reconnue.

Créer dans le répertoire "***/etc/apache2/*** " un répertoire "***certificates***".

```
mkdir /etc/apache2/certificates && cd /etc/apache2/certificates
```



Avec openssl, il va falloir faire 3 choses :

- Créer une clé privée.

```
openssl genrsa -out private.key 2048
```

ici, ***2048*** est la longueur de la clé de chiffrement. ***private.key*** est le nom du fichier.

> ***Bonne pratique*** *: Il est préférable de protéger la clé avec un chiffrement. Ainsi, un mot de passe sera demandé lors de toute lecture de la clé. Pour cela ajouter l'opérande '**-aes-256**' après genrsa lors de la génération.*

- Générer une requête (demande de certificat) signée par la clé privée.

```
openssl req -new -key private.key -out server.csr
```

ici, ***private.key*** est le nom du fichier de la clé avec laquelle la demande sera signée. ***server.csr*** *est le nom du fichier de la requête.*

Il va falloir alors répondre à quelques questions :

```
root@fdb68eed4d6e:/etc/apache2/certificates# openssl req -new -key private.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Isère
Locality Name (eg, city) []:Saint-Egrève
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MFR St Egrève
Organizational Unit Name (eg, section) []:IT Dept.
Common Name (e.g. server FQDN or YOUR name) []:ste-lab-dmi01.mfrstegreve.fr
Email Address []:contact-it@mfrstegreve.fr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@fdb68eed4d6e:/etc/apache2/certificates#
```

Le champ ***challenge password*** sert à protéger le csr contre l'altération. Il sera en effet demandé lors de la modification ou la révocation de celle-ci. il est optionnel.

On a donc le csr suivant :

```
root@fdb68eed4d6e:/etc/apache2/certificates# cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
M                                                                Y
M                                                                C
q                                                                t
Z                                                                n
c                                                                c
l                                                                L
l                                                                s
I                                                                J
9                                                                Q
N                                                                O
t                                                                q
p                                                                v
U                                                                l
h                                                                0
n                                                                q
M                                                                B
GHHW
-----END CERTIFICATE REQUEST-----
root@fdb68eed4d6e:/etc/apache2/certificates#
```

- Signer la requête pour générer le certificat.

```
openssl x509 -req -days 365 -in server.csr -signkey private.key -out certificate.crt
```

ici, ***x509*** est le format du certificat voulu.

365 est le nombre de jour de validité de certificat (celui-ci expirera dans 365 jours et devra être renouvelé).

-in : la demande que l'on souhaite signer

-signkey *:* la clé qui servira à signer la demande

- out : le fichier de sortie --> le certificat.

```
root@fdb68eed4d6e:/etc/apache2/certificates# openssl x509 -req -days 365 -in server.csr -signkey private.key -out certificate.crt
Certificate request self-signature ok
subject=C = FR, ST = Is\C3\83\C2\A8re, L = Saint-Egr\C3\83\C2\A8ve, O = MFR St Egr\C3\83\C2\A8ve, OU = IT Dept., CN = ste-lab-dmi
mfrstegreve.fr
root@fdb68eed4d6e:/etc/apache2/certificates#
```

On a donc le certificat suivant :

```
root@fdb68eed4d6e:/etc/apache2/certificates# cat certificate.crt
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
root@fdb68eed4d6e:/etc/apache2/certificates#
```

> **Astuce** : il est possible de réaliser les trois actions ci-dessus en une seule commande.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out
/etc/apache2/certificates/certificate.crt -keyout /etc/apache2/certificates/private.key
```

2.2 Cas du certificat signé par une CA

Pour garantir l'authenticité de la communication, il est nécessaire de faire valider le certificat par une autorité tierce.

> **Info** : par exemple Let's Encrypt

Il faudra alors effectuer les deux premières étapes, à savoir :

- Génération de la clé privée
- Génération de la requête (csr)

Mais au lieu de la signer, le csr sera envoyé à la CA, qui s'assurera d'abord de la légitimité de la requête et nous renverra le certificat signé.

Il faudra alors le déposer dans le dossier des certificats précédemment créé.

III. Configuration apache 2

> **Bonne pratique** : Il est préférable à ce stade de sécuriser l'accès à la clé privée en limitant son accès. En effet, si un pirate récupère la clé, il pourra lui-même générer un certificat pour usurper l'identité du serveur.

```
chown -r root:www-data /etc/apache2/certificates
chmod 440 /etc/apache2/certificates/private.key
```

3.1 Activation des modules

Activer le module apache pour le HTTPS.

```
a2enmod ssl
```

```
root@fdb68eed4d6e:/# a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Module socache_shmcb already enabled
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
root@fdb68eed4d6e:/#
```

Redémarrer apache2.

```
service apache2 restart
```

```
root@fdb68eed4d6e:/etc/apache2/sites-available# service apache2 restart
 * Restarting Apache httpd web server apache2
AH00558: apache2: Could not reliably determine the server's fully qualifie
```

3.2 Configuration apache

Aller dans : "***/etc/apache2/sites-available/***" et éditer le fichier de configuration SSL "***default-ssl.conf***".

Modifier les deux lignes suivantes pour qu'elles reflètent la configuration voulue.

```
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/apache2/certificates/certificate.crt
SSLCertificateKeyFile   /etc/apache2/certificates/private.key
```

Enregistrer et quitter.

Activer le site avec la commande :

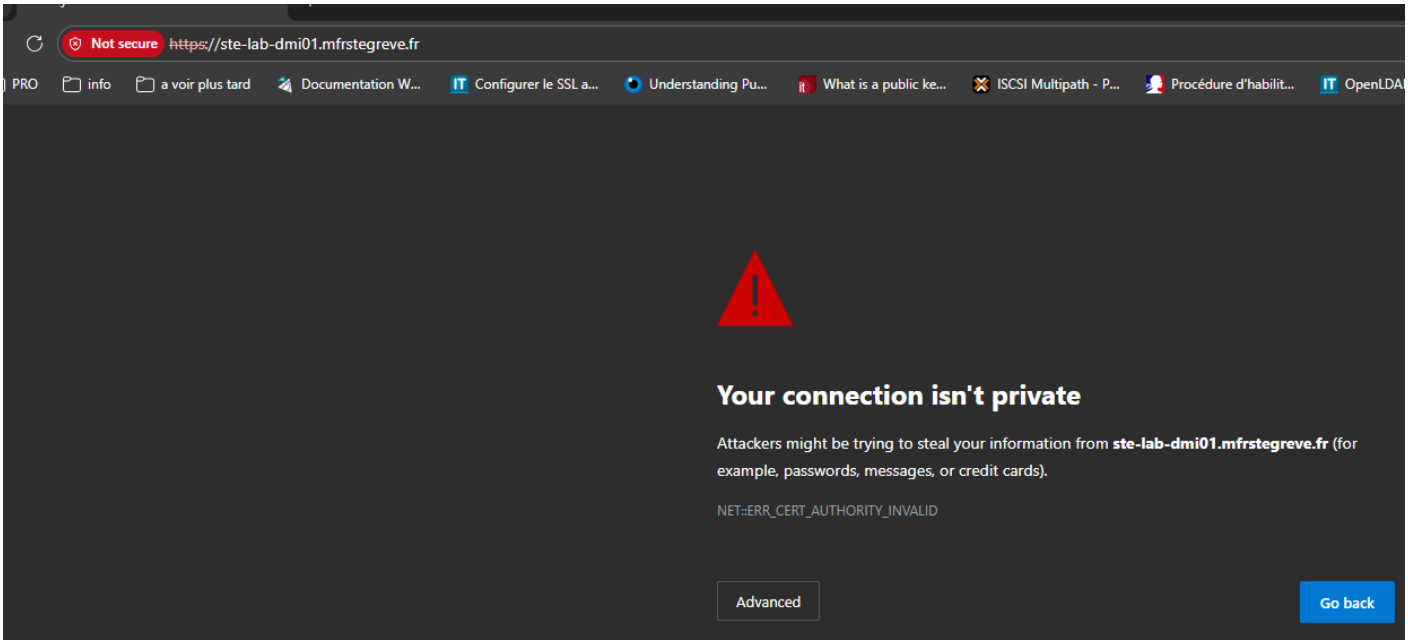
```
a2ensite default-ssl.conf
```

```
root@fdb68eed4d6e:/etc/apache2/sites-available# a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
root@fdb68eed4d6e:/etc/apache2/sites-available#
```

Recharger le service apache2 pour appliquer toutes les configurations de sites.

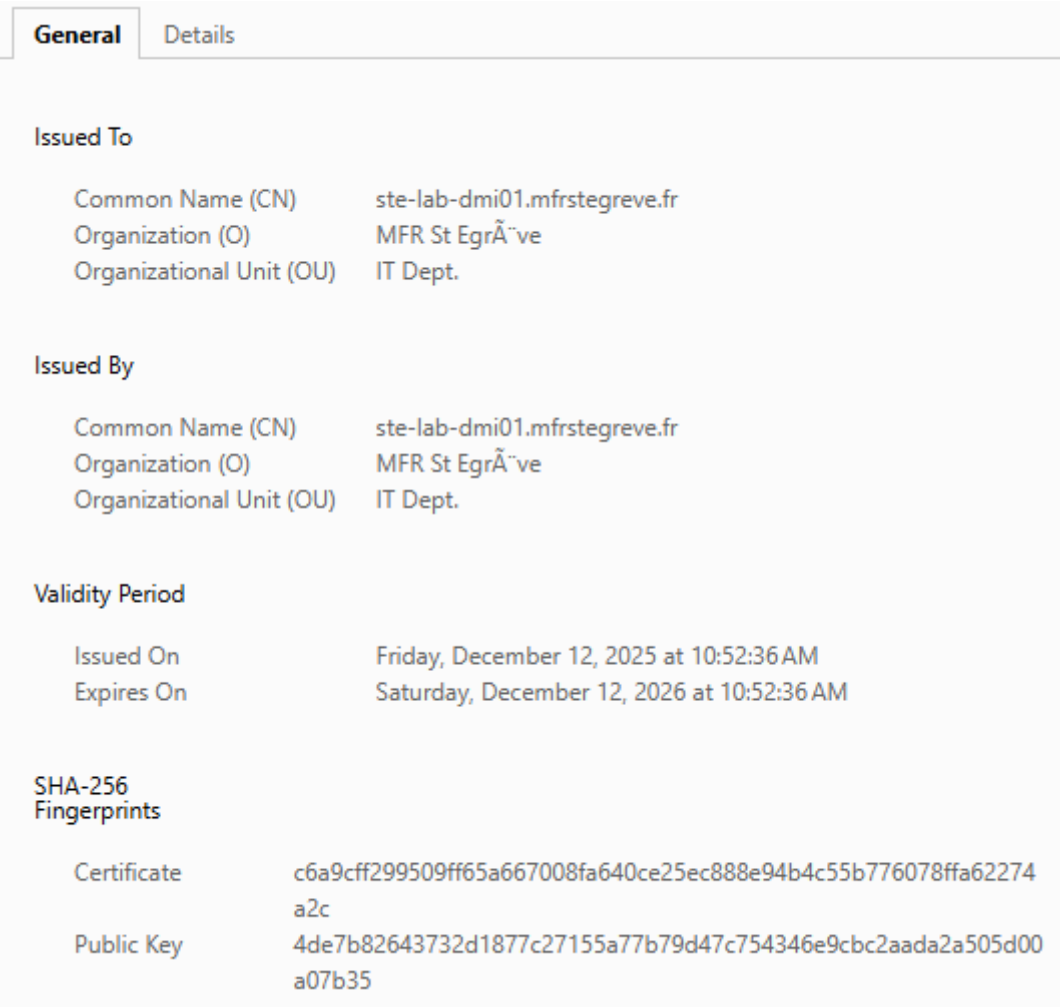
```
service apache2 reload
```

Le site est désormais accessible en https :



> **Info** : l'erreur de confidentialité viens du fait que le certificat est auto-signé.

Si l'on affiche le certificat :



Facultatif - optimisation de sécurité

Ajouter également dans le fichier "***default-ssl.conf***" les lignes suivantes pour corriger les failles du protocole SSL :

```
SSLProtocol -ALL +TLSv1 +TLSv1.1 +TLSv1.2
SSLHonorCipherOrder On
SSLCipherSuite ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
SSLCompression off
```

IV. Redirection HTTP vers HTTPS

Pour terminer la configuration, trois solutions sont possibles.

1. Laisser tel quel et offrir la possibilité de choisir entre le http et le https.
2. Couper le service http si l'on ne l'estime plus nécessaire.
3. Rediriger l'utilisateur vers le https automatiquement si il tente une connexion en http.

Dans le premiers cas rien de plus n'est à faire. Sinon :

Désativer HTTP

Désactiver le site HTTP par défaut :

```
a2dissite 000-default.conf
```

Couper le port d'écoute 80 en éditant le fichier "***/etc/apache2/ports.conf***" et en commentant la ligne suivante :

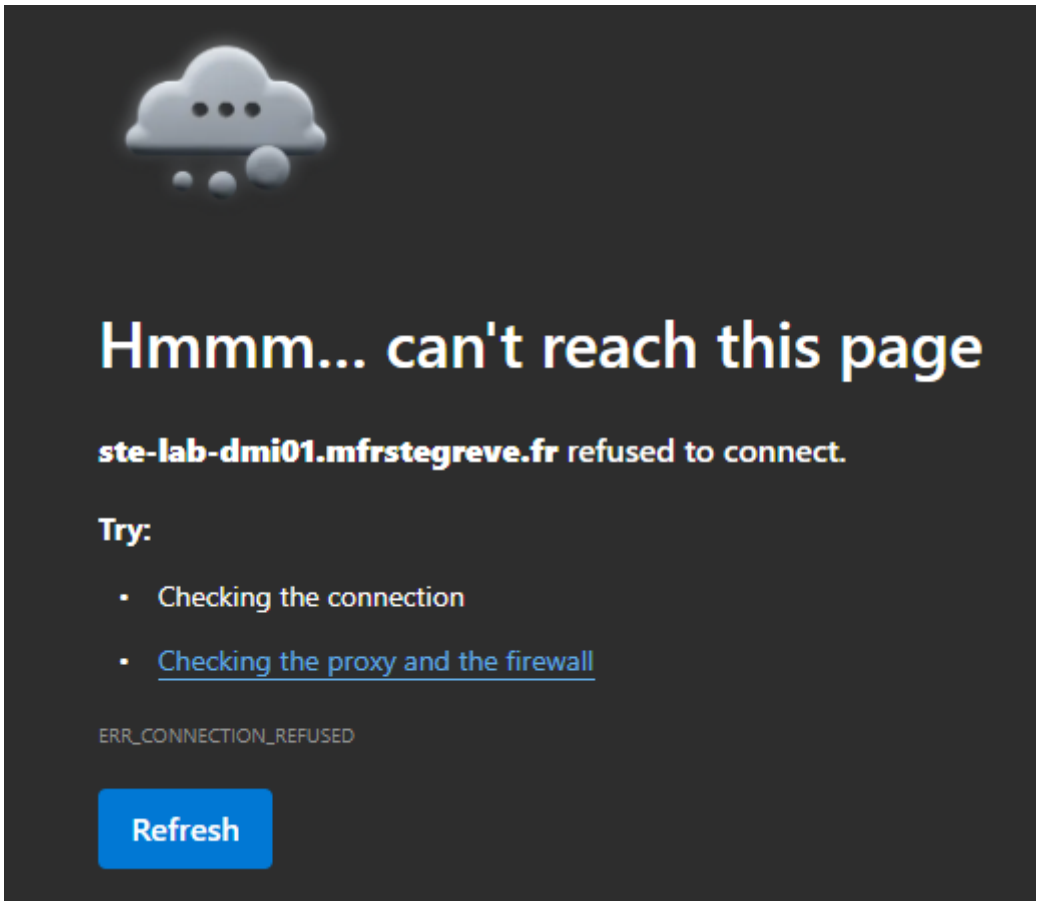
```
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

#Listen 80

<IfModule ssl_module>
        Listen 443
</IfModule>

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

Sauvegarder, quitter.

Puis relancer le service apache.

```
service apache2 restart
```

Le serveur web n'écoute plus les communications sur le port 80.



Rediriger HTTP --> HTTPS

Activer le module url rewriting (celui-ci permet au serveur de réécrire les url).

```
a2enmod rewrite
```

```
root@fdb68eed4d6e:/etc/apache2/sites-available# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  service apache2 restart
root@fdb68eed4d6e:/etc/apache2/sites-available#
```

Désactiver le site HTTP par défaut :

```
a2dissite 000-default.conf
```

Remplacer le fichier "***000-default.conf***" par un autre fichier appelé par exemple "***default-http.conf***"

```
cd /etc/apache2/sites-available/
mv 000-default.conf 000-default.conf.bkp && touch default-http.conf
```

Editer le fichier créé "***default-http.conf***" et écrire ce qui suit :

```
<VirtualHost *:80>
ServerName ste-lab-dmi01.mfrstegreve.fr
ServerAlias ste-lab-dmi01.mfrstegreve.fr

RewriteEngine On

Redirect permanent / https://ste-lab-dmi01.mfrstegreve.fr?

</VirtualHost>
```

Revision #2
Created 2026-07-30 07:34:05 UTC by Olivier
Updated 2026-07-30 07:34:41 UTC by Olivier