Table des matières :

Introduction

Un serveur web permet d'héberger et de diffuser des sites internet ou des applications web. En entreprise, il est essentiel pour la communication, le partage d'informations (intranet) et la mise en place de services en ligne.

Apache est l'un des serveurs web les plus utilisés pour sa fiabilité, sa flexibilité et sa compatibilité avec de nombreux systèmes. Il permet d'héberger des sites sécurisés grâce au protocole HTTPS, qui chiffre les échanges pour garantir la confidentialité et l'intégrité des données. L'utilisation d'une autorité de certification (PKI) permet de générer des certificats SSL/TLS et d'assurer une sécurité renforcée pour les utilisateurs et les services web.

Prérequis

Pour installer notre serveur apache nous utilisons ici une machine Debian 12. Il faut préalablement installer un serveur Windows en PKI (autorité de certification) pour certifier et sécuriser notre serveur web.

Installation

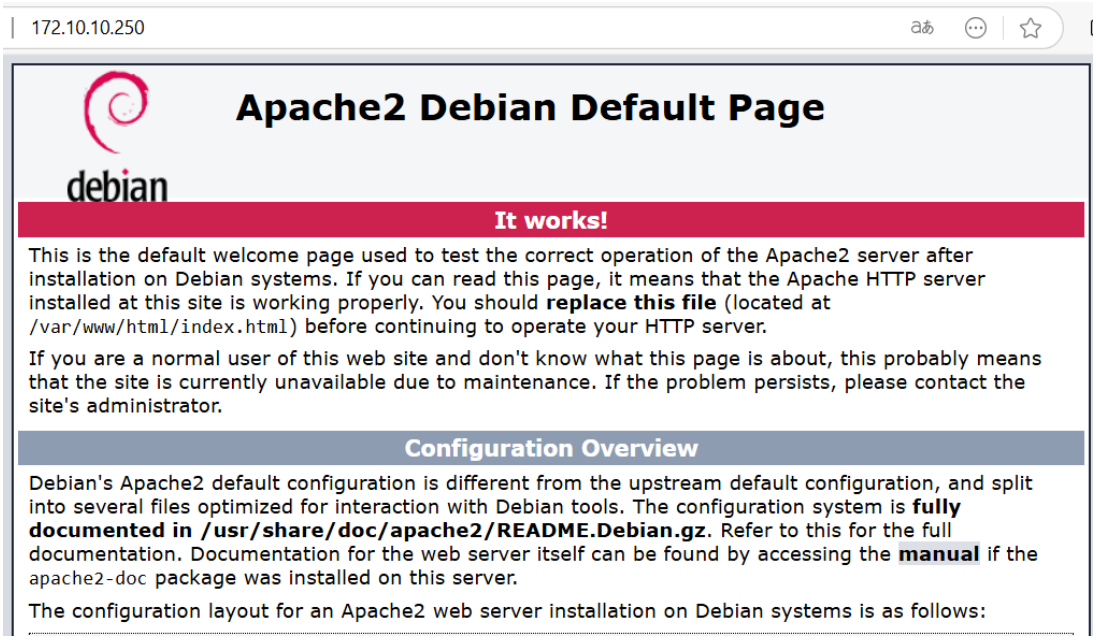
Installons apache2 :

```
apt install apache2
```

Pour s'assurer qu'apache s'est bien installé, testons à l'adresse ip du serveur sur un client :

```
http://IP_SERVEUR_WEB
```

Si tout s'est bien passé cette page doit apparaitre :



Configuration

Déplaçons-nous dans le dossier /etc/apache2/sites-available puis copions le fichier 000-default.conf pour créer notre site :

```
cd /etc/ apache2/sites-available

cp 000-default.conf  www.algara.at.conf
```

```
root@srv-web:/etc/apache2/sites-available# cp 000-default.conf www.algara.at.conf
root@srv-web:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf  www.algara.at.conf
```

Modifions le fichier de configuration www.algara.at.conf :

```
nano www.algara.at.conf
```

```
 GNU nano 7.2                                  /etc/apache2/sites-available/www.algara.at.conf

        ServerName www.algara.at
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/www.algara.at

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        SSLEngine on
        SSLCertificateFile      /etc/ssl/www.algara.at/www.algara.at.cer
        SSLCertificateKeyFile   /etc/ssl/www.algara.at/www.algara.at.key

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

Créons le dossier /var/www/www.algara.at/ :

```
mkdir /var/www/www.algara.at
```

Créons le fichier du code de notre site web :

```
nano  /var/www/www.algara.at/index.html
```

```
  GNU nano 7.2                                  /var/www/www.algara.at/index.html
<body>

        <h1>Bonjour bienvenu sur mon site</h1>

</body>
```

Création d'un certificat ssl

Passons à la création du certificat.

Créons le dossier ou sera stocké notre clé ssl, notre demande de certificat et notre certificat mkdir /etc/ssl/intra.rouliere.eni :

```
mkdir /etc/ssl/www.algara.at
```

Déplaçons-nous dans ce dossier et créons notre clé :

```
cd /etc/ssl/www.algara.at

openssl genrsa -out www.algara.at.key 2048
```

```
root@srv-web:/etc/apache2/sites-available# mkdir /etc/ssl/www.algara.at
root@srv-web:/etc/apache2/sites-available# cd /etc/ssl/www.algara.at
root@srv-web:/etc/ssl/www.algara.at# openssl genrsa -out www.algara.at.key 2048
root@srv-web:/etc/ssl/www.algara.at# ls
www.algara.at.key
root@srv-web:/etc/ssl/www.algara.at# cat www.algara.at.key
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDY4ryMC/BLi/je
yko3nQ1zl0DsSrwBs+Y/Cr3XRI/jBHGKvGjFsDLLQWa9qXOGhQiXCNCblqQSGTlv
eZ3Cyn8K5eysnEdQ115TIcnQz9o3Rf1KUPZ4p/2/75jAPVPFNSCAk/hkeH7EPjQy
```

Créons le fichier de configuration permettant de créer la demande de certificat :

```
nano /etc/ssl/www.algara.at/fic.txt
```

```
  GNU nano 7.2
[ req ]
default_bits = 2048
distinguished_name = dn
prompt = no
default_md = sha256
req_extensions = req_ext

[ dn ]
C=FR
L=Angers
O=algara
CN=www.algara.at

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = www.algara.at
```

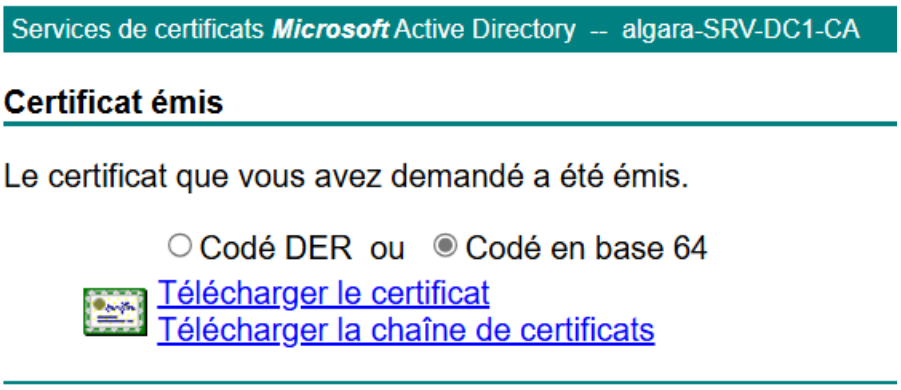
Créons notre demande de certificat :

```
openssl req -new -key www.algara.at.key -out www.algara.at.pem -config fic.txt
```

```
root@srv-web:/etc/ssl/www.algara.at# ls
fic.txt  www.algara.at.key  www.algara.at.pem
root@srv-web:/etc/ssl/www.algara.at# cat www.algara.at.pem
-----BEGIN CERTIFICATE REQUEST-----
MIICzzCCAbcCAQAwRzELMAkGA1UEBhMCRlIxDzANBgNVBAcMBkFuZ2VyczEPMA0G
A1UECgwGYWxnYXJhMRYwFAYDVQQDDA13d3cuYWxnYXJhLmF0MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2OK8jAvwS4v43spKN50Nc5dA7Eq8AbPmPwq9
10SP4wRxirxoxbAyy0FmvalzhoUIlwjQm5akEhk5b3mdwsp/CuXsrJxHUNdeUyHJ
```

Il faut maintenant copier notre demande de certificat et la coller dans notre serveur PKI :

Télécharger le certificat :



L'envoyer sur le serveur web via scp :

```
scp .\www.algara.at.cer thomas@srv-web:/tmp
```

```
C:\Users\administrateur\Downloads>scp .\www.algara.at.cer thomas@srv-web:/tmp
thomas@srv-web's password:
www.algara.at.cer                                     100% 1652     1.6KB/s   00:00
```

Sur le serveur web, le mettre dans le bon dossier :

```
mv /tmp/www.algara.at.cer /etc/ssl/www.algara.at/www.algara.at.cer
```

Activons le module ssl de apache :

```
a2enmod ssl
```

Vérifions notre configuration :

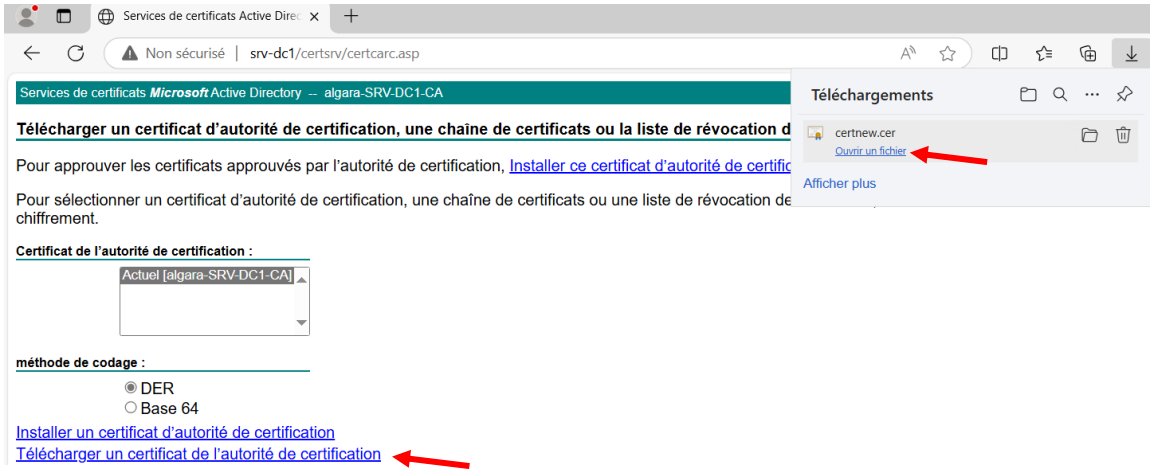
```
apachectl configtest
```

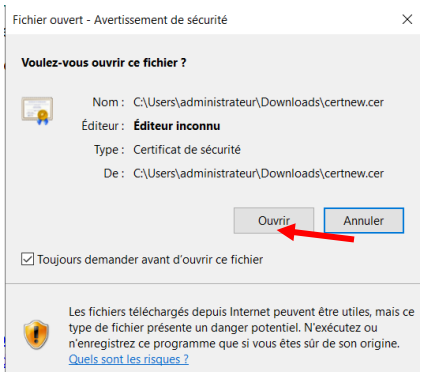
```
root@srv-web:/etc/ssl/www.algara.at# apachectl configtest
Syntax OK
```

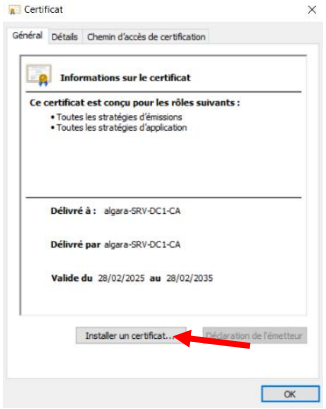
Enfin publions notre site :

```
a2ensite www.algara.at.conf
```

Sur un client téléchargeons puis installons le certificat :







Une fois les enregistrement DNS effectués, testons notre site :

Notre site est bien certifié, et notre connexion est bien sécurisée.