

Créer une Autorité de certification

Dans cette procédure je vais vous expliquer comment créer une autorité de certification et un certificat hôte pour Apache2. Pour réaliser l'autorité de certification nous allons utiliser Openssl et une machine Debian.



Prérequis :

- Une machine sous Debian
- Openssl

Créer une Autorité de certification :

D'abord, nous allons créer un répertoire pour notre autorité de certification :

```
mkdir -p /etc/ssl/certificats/CA
```

Ensuite nous allons créer la clé privée de l'autorité de certification :

```
openssl genrsa -des3 -out /etc/ssl/certificats/CA/CA.key 2048
```

Saisir une passphrase qui sera utilisée pour signer les certificats (Donc à ne pas perdre).

Puis nous allons générer le certificat *root* (racine) de l'autorité de certification au format .pem :

```
openssl req -x509 -new -nodes -key /etc/ssl/certificats/CA/CA.key -sha256 -days 10000 -out  
/etc/ssl/certificats/CA/CA.pem
```

Une liste de questions va vous être demandée.

Ensuite nous allons générer le certificat root (racine) au format .crt :

```
openssl x509 -in /etc/ssl/certificats/CA/CA.pem -inform PEM -out /etc/ssl/certificats/CA/CA.crt
```

Installer l'autorité de certification sur une machine :

Nous avons créer 3 fichiers dans le répertoire /etc/ssl/certificats

Intallation version web :

Le fichier CA.crt est a importé dans votre navigateur Web :

- Firefox => saisir dans l'url : about:preferences#privacy => Se rendre dans **Certificats** => **Afficher les certificats** => **Importer** => Choisir le fichier .crt
- Chrome => saisir dans l'url : chrome://settings/security => Se rendre dans **Gérer les certificats** => **Importer** => Choisir le fichier .crt

Installation au niveau de l'OS :

Windows :

Récupérer le fichier CA.crt et double cliquer dessus => Choisir l'emplacement : « Autorité de certification racine de confiance »

Ou en ligne de commande :

```
certutil.exe -addstore root CA.crt
```

Pour Firefox, il faut autoriser l'utilisation des autorités de certifications de confiances de Windows. Donc il faut créer un fichier dans le répertoire suivant C:\Program Files (x86)\Mozilla Firefox\Defaults\Pref\defaults\pref\ ou C:\Program Files\Mozilla Firefox\Defaults\Pref\defaults\pref\ :

Créer un fichier enableroot.js

Ajoutez y le contenu suivant :

```
pref("security.enterprise_roots.enabled", true);
```

Linux :

D'abord, on va copier le fichier CA.crt dans le répertoire des autorités (**/usr/local/share/ca-certificates/**) :

```
cp CA.crt /usr/local/share/ca-certificates/
```

Ensuite mettre à jour les autorités :

```
update-ca-certificates
```

Créer un certificat hôte :

D'abord nous allons créer un répertoire pour notre hôte :

```
mkdir -p /etc/ssl/certificats/hote
```

Ensuite nous allons créer la clé privée de l'hôte :

```
openssl genrsa -out /etc/ssl/certificats/hote/hote.key 2048
```

Puis on génère la demande de signature de certificat (fichier au format .csr) :

```
openssl req -new -key /etc/ssl/certificats/hote/hote.key -out /etc/ssl/certificats/hote/hote.csr
```

Dans les questions qui sont demandées, il faut mettre le DNS du serveur pour le Common Name.

Signer le certificat hôte par l'autorité de certification :

D'abord on va créer un fichier de configuration :

```
nano /etc/ssl/certificats/hote/hote.ext
```

Avec le contenu suivant :

```
authorityKeyIdentifier=keyid,issuer  
basicConstraints=CA:FALSE
```

```
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = hote
```

Pour signer le certificat de l'hôte par l'autorité de certification précédemment créée nous allons exécuter la commande suivante :

```
openssl x509 -req -in /etc/ssl/certificats/hote/hote.csr -CA /etc/ssl/certificats/CA/CA.pem -CAkey /etc/ssl/certificats/CA/CA.key -out /etc/ssl/certificats/hote/hote.crt
```

Enfin on renseigne la passphrase de l'autorité de certification.

Intégré le certificat signé avec Apache2 :

Pour intégrer le certificat dans Apache2, on doit éditer le Virtual Host qui est utilisé dans le répertoire **/etc/apache2/sites-available** :

```
nano /etc/apache2/sites-available/000-default.conf
```

Voici un exemple de configuration :

```
<VirtualHost *:80>
    ServerName hote

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    Redirect permanent / https://hote/
</VirtualHost>
<VirtualHost *:443>
    ServerName hote

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

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

    SSLEngine on
```

```
SSLCertificateFile /etc/ssl/certificats/hote/hote.crt
SSLCertificateKeyFile /etc/ssl/certificats/hote/hote.key
</VirtualHost>
```

Cette configuration permet d'automatiquement rediriger les connexions http en https et d'utiliser les fichiers du certificat et de la clé de l'hôte.

Ensuite on va activer le SSL sur Apache2 :

```
a2enmod ssl
```

Puis on redémarrer le service Apache2 :

```
systemctl restart apache2
```

Revision #2

Created 12 December 2024 18:32:10 by Nicolas

Updated 13 February 2025 21:17:14 by Nicolas