Certificat Autosigné

- Génération du certificat autosigné
- Mise an place du certificat autosigné

Génération du certificat autosigné

Génération d'un certificat auto-signé pour *.megaproduction.local

Ce guide vous permet de générer une autorité de certification (CA) auto-signée, puis un certificat wildcard pour `\*.megaproduction.local` signé par cette CA.

Étape 1 : Créer une autorité de certification (CA)

```
mkdir -p ~/certs &amp;amp;&amp;amp; cd ~/certs

# Générer la clé privée de la CA
openssl genrsa -out megaproduction-rootCA.key 4096

# Générer le certificat de la CA (valide 10 ans)
openssl req -x509 -new -nodes -key megaproduction-rootCA.key -sha256 -days 3650 -out
megaproduction-rootCA.pem \\
 -subj "/C=FR/ST=IDF/L=Paris/O=MegaProduction/OU=IT/CN=MegaProduction Root CA"
```

Étape 2 : Générer un certificat wildcard pour *.megaproduction.local

2.1 Générer une clé privée pour le certificat

```
openssl genrsa -out megaproduction.local.key 2048
```

2.2 Créer un fichier de configuration OpenSSL (megaproduction.ext)

Créer un fichier `megaproduction.ext` avec le contenu suivant :

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
subjectAltName = @alt\_names

\[alt\_names\]
DNS.1 = \*.megaproduction.local
DNS.2 = megaproduction.local
```

2.3 Créer une CSR (Certificate Signing Request)

```
openssl req -new -key megaproduction.local.key -out megaproduction.local.csr \\
 -subj "/C=FR/ST=IDF/L=Paris/O=MegaProduction/OU=IT/CN=\*.megaproduction.local"
```

2.4 Signer le certificat avec la CA

```
openssl x509 -req -in megaproduction.local.csr -CA megaproduction-rootCA.pem -CAkey
megaproduction-rootCA.key \\
 -CAcreateserial -out megaproduction.local.crt -days 825 -sha256 -extfile megaproduction.ext
```

Résultat

- `megaproduction.local.key` : clé privée du certificat
- `megaproduction.local.crt` : certificat wildcard
- `megaproduction-rootCA.pem` : certificat de l'autorité de certification à importer dans Firefox

Mise an place du certificat autosigné

Mise en place d’un certificat autosigné `*.megaproduction.local`

Certificat : `megaproduction.local.crt`
Clé : `megaproduction.local.key`
Fichier de configuration : `megaproduction.local.ext`

Apache

1. Copier les fichiers dans `/etc/ssl/megaproduction.local/` :

   ```
   sudo mkdir -p /etc/ssl/megaproduction.local
   sudo cp megaproduction.local.crt megaproduction.local.key
   /etc/ssl/megaproduction.local/
   ```

2. Modifier le virtualhost :

   ```
   <VirtualHost *:443>
       ServerName megaproduction.local
       ServerAlias *.megaproduction.local

       SSLEngine on
       SSLCertificateFile /etc/ssl/megaproduction.local/megaproduction.local.crt
       SSLCertificateKeyFile /etc/ssl/megaproduction.local/megaproduction.local.key
   ```

```
    DocumentRoot /var/www/megaproduction.local
</VirtualHost>
```

3. Activer SSL :

```
sudo a2enmod ssl
sudo systemctl reload apache2
```

Nginx

1. Copier les fichiers dans `/etc/ssl/megaproduction.local/` :

```
sudo mkdir -p /etc/ssl/megaproduction.local
sudo cp megaproduction.local.crt megaproduction.local.key
/etc/ssl/megaproduction.local/
```

2. Modifier la configuration :

```
server {
    listen 443 ssl;
    server_name *.megaproduction.local;

    ssl_certificate /etc/ssl/megaproduction.local/megaproduction.local.crt;
    ssl_certificate_key /etc/ssl/megaproduction.local/megaproduction.local.key;

    root /var/www/megaproduction.local;
}
```

3. Redémarrer Nginx :

```
sudo systemctl reload nginx
```

HAProxy

1. Fusionner les certificats :

```
cat megaproduction.local.crt megaproduction.local.key >
/etc/ssl/megaproduction.local.pem
```

2. Modifier `/etc/haproxy/haproxy.cfg` :

```
frontend https-in
    bind *:443 ssl crt /etc/ssl/megaproduction.local.pem
    mode http
    default_backend servers

backend servers
    server web1 127.0.0.1:8080
```

3. Redémarrer HAProxy :

```
sudo systemctl reload haproxy
```

Astuce Firefox

Pour éviter l’avertissement de certificat autosigné, importe le certificat racine dans Firefox via : `Paramètres > Confidentialité et sécurité > Certificats > Afficher les certificats > Importer`