Let’s Encrypt

Objectif

L'objectif de cette documentation est la mise en place des outils nécessaire à la création de certificats via l'autorité de certification Let's Encrypt.

Installation

Pour le moment, il n'existe pas de dépôts pour effectuer l'installation. Il faudra donc cloner depuis le dépôt Git :

```
git clone https://github.com/letsencrypt/letsencrypt
```

Utilisation

Parmi les commandes les plus importantes nous trouvons celles permettant d'obtenir un certificat, le renouveler ou encore le révoquer.

Obtenir un certificat

L’obtention d'un certificat s'obtient simplement via la commande suivante :

```
./letsencrypt-auto --agree-dev-preview --agree-tos --renew-by-default --rsa-key-size 4096 --server https://acme-v01.api.letsencrypt.org/directory certonly
```

–`agree-dev-preview` permet d'indiquer que nous avons bien compris qu'il s'agit d'une version en cours de développement qui n'est pas faite pour être utiliser dans un environnement de production pour le moment ;
–`agree-tos` signifie que nous acceptons les conditions d'utilisation ;
–`renew-by-default` permet d'activer le renouvellement du/des certificat(s) que l'on va obtenir ;
–`rsa-key-size` indique que l'on souhaite modifier la taille du hash du certificat, ici 4096 ;
–`server` permet de modifier le serveur que l'on va interroger.

Cependant, Let's Encrypt nécessite d'avoir le port 80 de disponible, ce qui n'est pas possible dans un environnement de production. Il existe cependant une solution :

```
./letsencrypt-auto --agree-dev-preview --agree-tos --renew-by-default --rsa-key-size 4096 --standalone --standalone-supported-challenges http-01 --http-01-port 1337 --server https://acme-v01.api.letsencrypt.org/directory certonly
```

Les ajouts de cette commande permet de lancer le service en *standalone* et de le faire écouter sur un port de notre choix, défini ici à **1337**.
Il faudra cependant faire en sorte que la communication contenant la réponse à la requête du service arrive jusqu'à ce dernier. Nous configurerons donc notre **nginx** comme suit (il s'agit d'une configuration minimale) :

```
server {
    listen 80;
    listen [::]:80;

    server_name votre.domaine.a.certifie;

    location /.well-known/acme-challenge/ {
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host $http_host;
        proxy_pass http://127.0.0.1:1337/.well-known/acme-challenge/;
        proxy_redirect off;
    }
}
```

Tel que, Let's Encrypt ouvrira une interface pour demander le(s) domaine(s)/sous-domaine(s) pour le(s)quel(s) on souhaite obtenir un certificat. on pourra utiliser le switch `-d` pour le préciser dans la commande directement. Chaque domaine/sous-domaine nécessite l'utilisation de ce switch.

Une fois le certificat obtenu, nous pourrons utiliser le générateur de Mozilla pour obtenir une configuration pour son serveur Web : https://mozilla.github.io/server-side-tls/ssl-config-generator/

Les certificats générés seront enregistrer dans le répertoire suivant :
/etc/letsencrypt/live/votre.domaine/

Renouveler le certificat

Malgré le renouvellement automatique, nous pouvons demander pour en obtenir un manuellement en utilisant les même valeurs que lorsque nous avons généré le certificat.

Révoquer du certificat

En cas d'erreur, de disparition du site, d'une attaque ou pour tout autre raison, on peut demander la révocation de notre certificat grâce à la commande :

```
./letsencrypt-auto revoke --cert-path certificat.pem
```