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-tos --renew-by-default --rsa-key-size 4096 --
server https://acme-v01.api.letsencrypt.org/directory certonly -d Le.Domaine
```

`–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-tos --renew-by-default --rsa-key-size 4096 --
server https://acme-v01.api.letsencrypt.org/directory certonly --webroot -w
Dossier/Du/Site -d Le.Domaine
```

Les ajouts de cette commande permet de lancer Let's Encrypt avec le plugin **webroot**. Ce plugin indique qu'il existe déjà un serveur web sur notre machine et que nous souhaitons l'utiliser. Il prend un paramètre **-w** suivit du chemin vers la racine du site.

Tel que, Let's Encrypt nous obtiendra un certificat pour le domaine indiquer avec le paramètre `-d` du

site stocké dans le répertoire indiqué par le paramètre `-w`.
On peut indiquer plusieurs domaine avec plusieurs paramètre `-d`. Si le site se trouve dans un autre répertoire, il faudra précédé `-d` par `-w Dossier/Du/Site`.

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/Le.Domaine/

Renouveler le certificat

Pour effectuer le renouvellement de manière automatisé, nous utiliserons le paramètre `renew`. Nous placerons la commande en tache cron est effectuons la vérification de manière hebdomadaire (ici tout les mardis à 14h et sauvegarderons la sortie de la commande vers un fichier créer pour l'occasion) :

```
mkdir -p /var/log/letsencrypt
touch /var/log/letsencrypt/renew.log
crontab -e
```

```
0 14 * * 2 /opt/letsencrypt/letsencrypt-auto renew >>
/var/log/letsencrypt/renew.log
```

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
```