Let's Encrypt

Introduction

L'objectif de cette page est de générer et faire signer des certificats avec Let's Encrypt.
Cette méthode n'est pas la plus simple, mais elle permet de mettre en place DANE/TLSA et HPKP ainsi que d'avoir des certificats en ECC.

Pour cela, il faut juste le packet certbot/letsencrypt.

Cette méthode n'est pas éligible au renouvellement automatique de certbot, donc il faudra ajouter manuellement l'entrée en tache cron. La méthodologie, si suivie a la lettre, permet un gestion simple de ces certificats.

Génération des certificats

Pour chaque domaines, nous allons créer les dossiers où seront stocké les certificats et les clés:

```
# mkdir -p /etc/letsencrypt/wiki.virtit.fr/live
# mkdir -p /etc/letsencrypt/wiki.virtit.fr/archive
```

puis on génère le certificat :

```
# openssl ecparam -name prime256v1 -genkey -out
/etc/letsencrypt/wiki.virtit.fr/live/private.key
# openssl req -new -key virtit.pem -nodes -days 3650 -out
/etc/letsencrypt/wiki.virtit.fr/live/certificate.csr
```

Ces certificats seront unique mais pensez à les renouveler régulièrement  .

Signature du certificat

Pour signer votre certificat, il faut lancer la commande suivante :

```
 # certbot certonly --webroot -w /var/www/letsencrypt/ -d wiki.virtit.fr --
csr /etc/letsencrypt/wiki.virtit.fr/live/cert.csr --cert-path
/etc/letsencrypt/wiki.virtit.fr/live/cert.pem --chain-path
/etc/letsencrypt/wiki.virtit.fr/live/chain.pem --fullchain-path
/etc/letsencrypt/wiki.virtit.fr/live/fullchain.pem
```

Renouvellement du certificat

Pour renouveler le certificat, il faut déplacer le certificat, et les chaines de certificats.

Je vous conseil d'ajouter la tâche **cron** suivante :

```
0 2 * * * /bin/rm /etc/letsencrypt/wiki.virtit.fr/archive/* && /bin/mv
/etc/letsencrypt/wiki.virtit.fr/live/*.pem
/etc/letsencrypt/wiki.virtit.fr/archive/ && /usr/bin/certbot certonly --
webroot -w /var/www/letsencrypt/ -d wiki.virtit.fr --csr
/etc/letsencrypt/wiki.virtit.fr/live/cert.csr --cert-path
/etc/letsencrypt/wiki.virtit.fr/live/cert.pem --chain-path
/etc/letsencrypt/wiki.virtit.fr/live/chain.pem --fullchain-path
/etc/letsencrypt/wiki.virtit.fr/live/fullchain.pem --post-hook
'/bin/systemctl reload apache2'
```

Il faudra adapter la dite commande avec le bon domaine et les bons post-hook.

Installation de Let's Encrypt

Il faudra installer certbot qui est dans les dépôts backports

```
# apt install letsencrypt
```

Création d'un certificat SSL

il faudra stopper NginX, Apache ou toutes les applications utilisant le port 80 ou 443

```
# service apache2 stop
```

Création du certificat

```
# letsencrypt certonly --rsa-key-size 4096 -d wiki.virtit.fr
```

puis suivre les indications.

Renouvellement des certificats

il faudra stopper Nginx, Apache ou toutes les applications utilisant le port 80 ou 443

```
# service apache2 stop
```

Puis il suffira de lancer

```
# letsencrypt renew --force-renewal
```

Problèmes rencontrés

En cas de Reverse Proxy, Il faudra un peu plus s'acharné avec le script (qui ne prends pas en compte cette solution).

Il faudra s'orienter vers l'option “standalone” du script