# Renouvellement automatique de certificat Let's Encrypt

## Introduction

- *Let's Encrypt* est un service de PKI gratuit
- Les certificats *Let's Encrypt* sont reconnus par les navigateurs
- Un certificat *Let's Encrypt* peut contenir plusieurs *hostnames*
- La validation des certificats est automatisée grâce au protocole ACME
- Nous utiliserons l'implémentation «certbot»
- Le script est prévu pour le serveur web *Nginx*
- Lien ⇒ https://certbot.eff.org/

## Installation

- Installer *Let's Encrypt*:

```
cd /root
wget https://dl.eff.org/certbot-auto
chmod +x certbot-auto
./certbot-auto
```

- Installer le script de renouvellement de certificat:

```
wget -O /usr/local/sbin/renew-cert-letsencrypt
"https://www.ilard.fr/dokuwiki/doku.php?do=export_code&id=public:renouvellem
ent_automatique_de_certificat_let_s_encrypt&codeblock=2"
chmod +x /usr/local/sbin/renew-cert-letsencrypt
```

/usr/local/sbin/renew-cert-letsencrypt

```
#!/bin/bash

########################################################################
######################

. /usr/local/etc/renew-cert-letsencrypt.cf || exit 1

########################################################################
######################

ARGS=$(echo ${ARGS})

# Récupérer l'âge du certificat
age=$(($(date +%s)-$(date -r /etc/nginx/privkey.pem +%s)))
age=$((${age}/86400))
```

```
echo -n "* Certificat renouvelé il y a ${age} jours => renouvellement "
if [ ${age} -ge ${AGEMAX} ] ; then
        echo "nécessaire"
else
        if [ "${1}" = "-f" ] ; then
                echo "forcé"
        else
                echo "pas nécessaire"
                exit 0
        fi
fi
echo

cd ${REP}
echo -e "* Commande à exécuter:\n\n${PROG} ${ARGS}\n"

service nginx stop

${PROG} ${ARGS}
echo

# Récupérer le nom du dossier qui contient le certificat le plus récent
rep=$(ls -l --time-style long-iso /etc/letsencrypt/live/*/privkey.pem
|awk '{print $6" "$7" "$8}' |sort |tail -1 |cut -d"/" -f5)
echo -n "* Certificat le plus récent: /etc/letsencrypt/live/${rep} => "

# Comparer le certificat le plus récent et le certificat installé
diff /etc/letsencrypt/live/${rep}/privkey.pem /etc/nginx/privkey.pem >
/dev/null

if [ $? -eq 1 ] ; then
        echo "renouvelé"

        echo "* Installation certificat pour Nginx"
        cp /etc/letsencrypt/live/${rep}/fullchain.pem /etc/nginx/
        cp /etc/letsencrypt/live/${rep}/privkey.pem /etc/nginx/

        if [ -f /usr/local/etc/certs-letsencrypt_post_ok.sh ] ; then
                . /usr/local/etc/certs-letsencrypt_post_ok.sh
        fi

else
        echo "PAS renouvelé"
fi

service nginx start
echo
```

# Configuration

- Installer et éditer le fichier de configuration:

```
wget -O /usr/local/etc/renew-cert-letsencrypt.cf
"https://www.ilard.fr/dokuwiki/doku.php?do=export_code&id=public:renouvellem
ent_automatique_de_certificat_let_s_encrypt&codeblock=4"
```

/usr/local/etc/renew-cert-letsencrypt.cf

```
AGEMAX=60

REP=/root
PROG="./certbot-auto"

ARGS="
certonly
 --renew-by-default
 --standalone
 --rsa-key-size 4096
 -m contact@mondomaine.fr
 -t
 -d mondomaine.fr
 -d autredomaine.net
 -d www.mondomaine.fr
 -d mail.mondomaine.fr
 -d www.autredomaine.net
"
```

- **Facultatif** ⇒ installer et éditer le script à exécuter **après** un renouvellement réussi de certificat:

```
wget -O /usr/local/etc/renew-cert-letsencrypt_post_ok.sh
"https://www.ilard.fr/dokuwiki/doku.php?do=export_code&id=public:renouvellem
ent_automatique_de_certificat_let_s_encrypt&codeblock=6"
```

/usr/local/etc/renew-cert-letsencrypt_post_ok.sh

```
echo "* Installation certificat pour Cyrus-Imap et Postfix"
scp -q /etc/letsencrypt/live/${rep}/*.pem 192.168.50.123:/etc/ssl
ssh 192.168.50.123 'service cyrus-imapd restart ; service postfix
restart'
```

- Planifier le renouvellement dans *CRON*:

```
ln -s /usr/local/sbin/renew-cert-letsencrypt /etc/cron.daily
```

- Forcer la création / renouvellement de certificat:

```
renew-cert-letsencrypt -f
```