

# SSL

## Créer un certificat pour un site web 101

1. Ajouter à votre fichier conf (de préférence vers l'entete de celui-ci):

```
include /etc/nginx/snippets/letsencrypt-acme-challenge.conf;
```

2. Utilisez la commande :

```
sudo certbot --authenticator webroot --install nginx
```

3. Lorsque demandé, spécifiez le webroot, il est le suivant :

```
/srv/www/letsencrypt
```

Si vous choisissez d'être redirigé automatiquement, vérifiez que les adresses ip automatiquement remplies par certbot soient bien indiquées et non sous la forme [::]:443

## Révoquer un certificat

```
certbot revoke --cert-path /PATH/TO/fullchain.pem --key-path /PATH/TO/privkey.pem
```

## Renouveler un certificat

```
#!/bin/bash
```

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

```
certbot renew >> /etc/letsencrypt/monthly.log 2>&1
```

```
service nginx restart
```

# Avec crontab

Mettre `PATH=$PATH:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin` au début du crontab (crontab -e)

## Http-101

/etc/nginx/snippets/letsencrypt-acme-challenge.conf :

```
#####  
#####  
  
#  
# This config enables to access /.well-known/acme-challenge/xxxxxxxxxx  
# on all our sites (HTTP), including all subdomains.  
# This is required by ACME Challenge (webroot authentication).  
# You can check that this location is working by placing ping.txt here:  
# /var/www/letsencrypt/.well-known/acme-challenge/ping.txt  
# And pointing your browser to:  
# http://xxx.domain.tld/.well-known/acme-challenge/ping.txt  
#  
# Sources:  
# https://community.letsencrypt.org/t/howto-easy-cert-generation-and-renewal-with-nginx/3491  
#  
#####  
#####  
  
# Rule for legitimate ACME Challenge requests (like /.well-known/acme-challenge/xxxxxxxxxx)  
# We use ^~ here, so that we don't check other regexes (for speed-up). We actually MUST cancel  
# other regex checks, because in our other config files have regex rule that denies access to files with dotted  
# names.  
location ^~ /.well-known/acme-challenge/ {  
  
    # Set correct content type. According to this:  
    # https://community.letsencrypt.org/t/using-the-webroot-domain-verification-method/1445/29  
    # Current specification requires "text/plain" or no content header at all.  
    # It seems that "text/plain" is a safe option.  
    default_type "text/plain";  
  
    # This directory must be the same as in /etc/letsencrypt/cli.ini  
    # as "webroot-path" parameter. Also don't forget to set "authenticator" parameter
```

```
# there to "webroot".  
# Do NOT use alias, use root! Target directory is located here:  
# /var/www/common/letsencrypt/.well-known/acme-challenge/  
root    /var/www/letsencrypt;  
}  
  
# Hide /acme-challenge subdirectory and return 404 on all requests.  
# It is somewhat more secure than letting Nginx return 403.  
# Ending slash is important!  
location = /.well-known/acme-challenge/ {  
    return 404;  
}
```

---

Révision #3

Créé 12 décembre 2020 11:50:19 par Admin

Mis à jour 1 janvier 2025 13:54:47 par tjiho