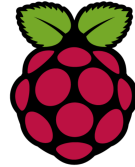


## Raspberry Pi https avec let's encrypt



### 1 let's Encrypt

**Let's Encrypt** est une autorité de certification lancée le 3 décembre 2015 . Cette autorité fournit des certificats gratuits X.509 pour le protocole cryptographique TLS au moyen d'un processus automatisé destiné à se passer du processus actuel impliquant la création manuelle, la validation, la signature, l'installation et le renouvellement des certificats.

### 2 Installation

En tant que super utilisateur (root) :

```
#cloner le repo
git clone https://github.com/letsencrypt/letsencrypt
# Push into the direcotry
pushd letsencrypt

# Run the automated installer (see wait times above)
time ./letsencrypt-auto
```

S'armer d'un peu de patience car le processus est lent (10 min sur une pi3).

Il vous faudra une adresse mail pour recevoir les invitations à renouveler le certificat. Et bien sûr un non de domaine actif. Ces informations vous seront demandées pendant le processus d'installation.

Si tout s'est bien passé, vous pouvez maintenant exécuter

```
tree /etc/letsencrypt/
```

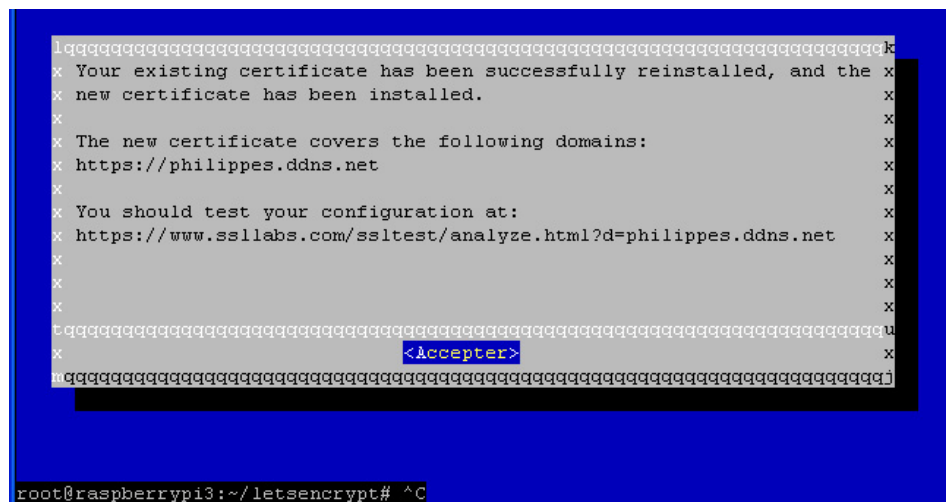
et vous pourrez voir tous les fichiers et clés d'enregistrement.

```
/etc/letsencrypt/
├── accounts
│   ├── acme-v01.api.letsencrypt.org
│   │   └── directory
│   │       ├── 44f78dcf1c0604a3ac5a9dc6f75399b9
│   │       ├── meta.json
│   │       ├── private_key.json
│   │       └── regr.json
├── archive
│   ├── philippes.ddns.net
│   │   ├── cert1.pem
│   │   ├── chain1.pem
│   │   ├── fullchain1.pem
│   │   └── privkey1.pem
├── csr
│   └── 0000_csr-certbot.pem
├── keys
│   └── 0000_key-certbot.pem
├── live
│   └── philippes.ddns.net
│       ├── cert.pem ->
│       │   ../../archive/philippes.ddns.net/cert1.pem
│       ├── chain.pem ->
│       │   ../../archive/philippes.ddns.net/chain1.pem
│       ├── fullchain.pem ->
│       │   ../../archive/philippes.ddns.net/fullchain1.pem
│       ├── privkey.pem ->
│       │   ../../archive/philippes.ddns.net/privkey1.pem
│       └── README
├── options-ssl-apache.conf
├── renewal
│   └── philippes.ddns.net.conf
```

### 3 Renouvellement du certificat

```
root@raspberrypi3:~/cd letsencrypt
root@raspberrypi3:~/letsencrypt# ./letsencrypt-auto
```

A la fin du processus vous devez obtenir l'écran suivant

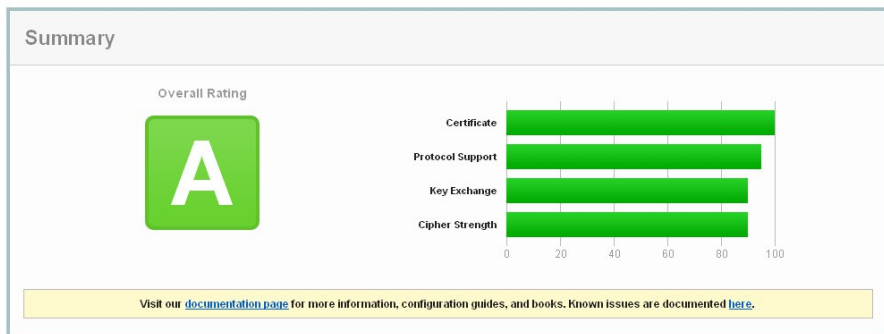


### 4 Test du certificat

<https://www.ssllabs.com/ssltest/analyze.html?d=philippes.ddns.net>

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > philippes.ddns.net  
**SSL Report: philippes.ddns.net (90.104.175.16)**  
Assessed on: Thu, 15 Sep 2016 16:43:10 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >](#)



### 5 Automatiser le Renouvellement du certificat

Let's Encrypt permet d'automatiser le renouvellement à l'aide de la commande suivante, à placer dans un cron mensuel :

```
root@raspberrypi3:~/ crontab -e
@monthly /root/letsencrypt/letsencrypt-auto -d
philippes.ddns.net --renew-by-default --no-redirect --text
```

@monthly (chaque mois)

Les paramètres sont les suivants :

- **-d** : une liste de domaines séparés par des virgules,
- **--renew-by-default** : on précise qu'on souhaite renouveler les domaines mentionnés précédemment,
- **--no-redirect** : pas besoin de remettre en place les redirections (surtout si vous les avez déjà ajoutées auparavant),
- **--text** : utilise le mode texte brut plutôt qu'une interface ncurses. Ça évite de se retrouver avec un écran final attendant que l'on valide un bouton « OK », ce qui fait un peu tâche dans un cron.

### 6 Mise en place des redirections

redirection du trafic HTTP vers l'adresse HTTPS

Si ce n'est pas déjà fait, activer le module rewrite d'Apache

```
root@raspberrypi3:~/ sudo a2enmod rewrite
```

puis éditer le fichier 000-default.conf

```
root@raspberrypi3:~/ cd /etc/apache2/sites-available/
root@raspberrypi3:~/ nano 000-default.conf
```

Pour l'accès HTTP, il doit ressembler à ça (pour le domaine philippes.ddns.net) :

Ajouter les lignes RewriteEngine et RewriteRule

```
<VirtualHost *:80>
    ServerName philippes.ddns.net
    ServerAdmin webmaster@philippes.ddns.net
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    RewriteEngine on
    RewriteRule ^ https://philippes.ddns.net%{REQUEST_URI}
[L,QSA,R=permanent]
</VirtualHost>
```