

# Letencrypt : création de certificats

Comment créer des certificat officiel pour son site ?



## Let's Encrypt

- ⇒ [Certificat avec letsencrypt](#)
  - ⇒ [Prérequis Système](#)
  - ⇒ [Prérequis réseaux](#)
    - ⇒ [Installation](#)
      - ⇒ [Sous Debian/Ubuntu](#)
      - ⇒ [Sous CentOS](#)
    - ⇒ [Créer les certificats](#)
    - ⇒ [Emplacement : Certificat et privkey](#)
    - ⇒ [Renouvellement des certificats](#)

## 1) Certificat avec letsencrypt

### 1.1) Prérequis Système

Disposer de: \* git \* virtualenv

### 1.2) Prérequis réseaux

Disposer d'un nom de domaine, ainsi que les enregistrements **DNS** correspondant aux différent sous domaine que vous voulez certifier.

Par exemple, les services web que je souhaite mettre en production sont auto\_hebergé, j'indique donc l'IP public de destination:

rtfm	3600	IN	A	<IP_DEST>
virtualdomain	3600	IN	A	<IP_DEST>
gitlab	3600	IN	A	<IP_DEST>
grafana	3600	IN	A	<IP_DEST>

#### 1.2.1) Installation

##### 1.2.1.1) Sous Debian/Ubuntu

- ⇒ `sudo apt update && sudo apt upgrade`
- ⇒ `sudo apt install git`
- ⇒ `pip install virtualenv`

##### 1.2.1.2) Sous CentOS

- ⇒ `sudo yum update && sudo yum upgrade`
- ⇒ `sudo yum install git`
- ⇒ `pip install virtualenv`

Cloner le dépôt letsencrypt dans /opt

- ⇒ `sudo git clone https://github.com/letsencrypt/letsencrypt`  
`/opt/letsencrypt` ### Créer les certificats Se déplacer dans  
`/opt/letsencrypt`

Saisir cette commande, chaque domaine est signalé par -d

```
sudo -H ./letsencrypt-auto certonly --standalone -d nom.domaine.com -d  
ww.nom.domaine.com
```

```
[sudo] password for ordinatous:
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for nom.domaine.com
http-01 challenge for www.nom.domaine.com
Waiting for verification...
Cleaning up challenges
```

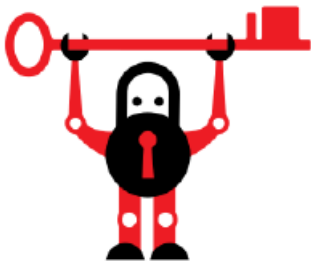
IMPORTANT NOTES:

- Congratulations! Your certificate **and** chain have been saved at:  
/etc/letsencrypt/live/nom.domaine.com/fullchain.pem  
Your key file has been saved at:  
/etc/letsencrypt/live/nom.domaine.com/privkey.pem  
Your cert will expire on 2018-10-08. To obtain a new **or** tweaked version of this certificate **in** the future, simply run letsencrypt-auto again. To non-interactively renew \*all\* of your certificates, run "letsencrypt-auto renew"
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: <https://letsencrypt.org/donate>  
Donating to EFF: <https://eff.org/donate-le>

Note: la procédure est un peu différente si l'on souhaite produire un certificat pour un serveur Apache2.

### 1.2.2) Emplacement : Certificat et privkey



Logo Certbot

La commande `certbot` permet de vérifier la présence des certificats: `* ./certbot-auto certificates`

```
./certbot-auto certificates
Requesting to rerun ./certbot-auto with root privileges...
Saving debug log to /var/log/letsencrypt/letsencrypt.log
```

```
-----
---
```

Found the following certs:

```
Certificate Name: rtfm.ordinatous.com
  Domains: rtfm.ordinatous.com www.rtfm.ordinatous.com
  Expiry Date: 2018-10-09 09:34:12+00:00 (VALID: 89 days)
  Certificate Path: /etc/letsencrypt/live/rtfm.ordinatous.com/fullchain.pem
  Private Key Path: /etc/letsencrypt/live/rtfm.ordinatous.com/privkey.pem
Certificate Name: dotfiles.ordinatous.com
  Domains: dotfiles.ordinatous.com gitlab.ordinatous.com
grafana.ordinatous.com www.dotfiles.ordinatous.com www.gitlab.ordinatous.com
www.grafana.ordinatous.com
  Expiry Date: 2018-10-08 07:38:19+00:00 (VALID: 88 days)
  Certificate Path:
/etc/letsencrypt/live/dotfiles.ordinatous.com/fullchain.pem
  Private Key Path: /etc/letsencrypt/live/dotfiles.ordinatous.com/privkey.pem
Certificate Name: gitlab.ordinatous.com
  Domains: gitlab.ordinatous.com www.gitlab.ordinatous.com
  Expiry Date: 2018-10-08 07:39:53+00:00 (VALID: 88 days)
  Certificate Path: /etc/letsencrypt/live/gitlab.ordinatous.com/fullchain.pem
  Private Key Path: /etc/letsencrypt/live/gitlab.ordinatous.com/privkey.pem
Certificate Name: virtualdomain.ordinatous.com
  Domains: virtualdomain.ordinatous.com www.virtualdomain.ordinatous.com
  Expiry Date: 2018-10-09 09:42:39+00:00 (VALID: 89 days)
  Certificate Path:
/etc/letsencrypt/live/virtualdomain.ordinatous.com/fullchain.pem
  Private Key Path:
/etc/letsencrypt/live/virtualdomain.ordinatous.com/privkey.pem
```

```
Le certificat et la clé privé sont rangés ici: *
/etc/letsencrypt/live/nom.domaine.com/fullchain.pem *
/etc/letsencrypt/live/nom.domaine.com/privkey.pem
```

Il s'agit en réalité d'un lien qui pointe vers un répertoire du même niveau que /etc/letsencrypt/live nommé archive.

### 1.2.3) Renouvellement des certificats

Il est indiqué dans les *Importants Notes* qu'un script est à notre disposition afin de renouveler l'ensemble des certificats `letsencrypt-auto renew`.

Nous verrons dans le mémo **crontab** comment mettre en place l'automatisation. L'informaticien n'aime pas les choses répétitives...