Certification

Documentation — Mise en place de Certbot avec Let's Encrypt

Présentation

Certbot est un client ACME permettant d'obtenir et de renouveler automatiquement des certificats SSL/TLS délivrés par **Let's Encrypt**, une autorité de certification gratuite et reconnue par tous les navigateurs modernes.

Certbot remplace avantageusement les certificats auto-signés (OpenSSL) en offrant une reconnaissance universelle sans avertissement de sécurité.

Prérequis

- Un serveur Linux (Debian/Ubuntu)
- Un nom de domaine pointant vers l'IP publique du serveur
- Le port **80 (HTTP) accessible depuis Internet** au moment de la génération du certificat
- Droits sudo sur le serveur

Installation

```
sudo apt update
sudo apt install certbot python3-certbot-apache -y
```

> Pour Nginx, remplacer `python3-certbot-apache` par `python3-certbot-nginx`.

Génération du certificat

Avec Apache (configuration automatique)

```
sudo certbot --apache -d mondomaine.fr
```

Avec Nginx (configuration automatique)

```
sudo certbot --nginx -d mondomaine.fr
```

Sans serveur web (autres services)

```
sudo certbot certonly --standalone -d mondomaine.fr
```

> Le port 80 doit être libre au moment de la commande.

Via validation DNS (serveur sans IP publique)

```
sudo certbot certonly --manual --preferred-challenges dns -d mondomaine.fr
```

> Certbot demandera d'ajouter un enregistrement TXT dans la zone DNS du domaine pour prouver sa propriété.

Fichiers générés

Les certificats sont stockés dans `/etc/letsencrypt/live/mondomaine.fr/` :

Fichier	Rôle
`fullchain.pem`	Certificat complet (à utiliser côté serveur)
`privkey.pem`	Clé privée associée

Ces fichiers peuvent être utilisés par n'importe quel service (Proxmox, Gitea, BookStack, etc.) en les référençant dans leur configuration respective.

Renouvellement

Les certificats Let's Encrypt ont une durée de validité de **90 jours**.

Certbot configure automatiquement un renouvellement périodique via un timer systemd. Pour vérifier que le renouvellement automatique fonctionne correctement :

```
sudo certbot renew --dry-run
```

Pour forcer un renouvellement manuel :

```
sudo certbot renew
```

Vérification

Après la génération, vérifier qu'Apache écoute bien sur le port 443 :

```
sudo ss -tlnp | grep 443
```

Vérifier également la date d'expiration du certificat :

```
sudo certbot certificates
```

Compatibilité

Certbot fonctionne sur tout type de machine Linux :

- Serveur dédié
- VPS
- Machine virtuelle (VM sous Proxmox, VMware, etc.)
- Conteneur (sous réserve d'accès réseau)

La seule contrainte reste la **validation du domaine** : Let's Encrypt doit pouvoir vérifier la propriété du domaine, soit via HTTP (port 80), soit via DNS.

Récapitulatif des commandes utiles

Action	Commande
Installer Certbot	`sudo apt install certbot python3-certbot-apache -y`
Générer un certificat (Apache)	`sudo certbot --apache -d mondomaine.fr`
Générer un certificat (standalone)	`sudo certbot certonly --standalone -d mondomaine.fr`
Tester le renouvellement auto	`sudo certbot renew --dry-run`
Lister les certificats	`sudo certbot certificates`
Renouveler manuellement	`sudo certbot renew`

Revision #1
Created 2026-04-30 16:42:21 UTC by Admin
Updated 2026-04-30 16:43:02 UTC by Admin