Obtenir un certificat SSL avec Letsencrypt Certbot

Aperçu

Avant que letsencrypt ne génère et ne vous fournisse un certificat, il doit vérifier si vous contrôlez bien les enregistrements DNS de ce domaine. Pour ce faire, il vous demande de créer un enregistrement TXT qu'il peut vérifier via le système de noms de domaine. Vous utilisez donc certbot pour demander votre certificat. Il vous fournit les informations nécessaires dans l'enregistrement TXT. Vous créez l'enregistrement TXT via votre interface avec le service DNS que vous utilisez et, une fois le nouvel enregistrement propagé, vous cliquez sur « Continuer » pour permettre à certbot de terminer la tâche et d'enregistrer votre certificat.

Installer Certbot

```
sudo apt update
sudo apt install certbot
```

Demander le certificat

```
sudo certbot certonly --manual --preferred-challenges dns -d votresite.exemple.com

# À ce stage, un enregistrement TXT similaire à celui-ci vous sera
# demandé:
# nom :    _acme-challenge.votresite.exemple.com.
# valeur : Tv1E2PLJyIU1ePiLfW-bv8SdAq4wa3QDud76zfB7asU
# Vous serez invité à appuyer sur Enter pour continuer.
# Attendez la fin des étapes ci-dessous avant de continuer.
```

Ajouter l'enregistrement TXT

En utilisant votre interface Web à votre service DNS, ajoutez un enregistrement TXT comme celui-ci.

_acme-challenge.votresite TXT Tv1E2PLJyIU1ePiLfW-bv8SdAq4wa3QDud76zfB7asU

La propagation des enregistrements DNS prend du temps. Vous devez donc d'abord vous assurer que l'enregistrement a été propagé avant de cliquer sur "Continue" à l'invite de Certbot.

Vérifiez qu'il s'est propagé

Dans une autre fenêtre de terminal, tappez la commande suivante de temps à autre jusqu'à ce que votre enregistrement TXT apparaisse dans la section de réponse.

```
dig -t txt _acme-challenge.votresite.exemple.com
```

Continuer certbot dans la fenêtre de terminal d'origine

Appuyez sur "Enter". Vos fichiers de certificat se trouveront ici :

/etc/letsencrypt/live/votresite.exemple.com/

fullchain.pem:

> Contient le certificat SSL de votre domaine et les certificats intermédiaires nécessaires pour former une chaîne de confiance valide jusqu'au certificat racine Let's Encrypt.

privkey.pem:

> Votre clé privée, qui doit être gardée secrète pour sécuriser votre site.

cert.pem:

> Contient le certificat SSL spécifique de votre domaine.

chain.pem:

Contient le(s) certificat(s) intermédiaire(s) qui lient le certificat de votre domaine à l'autorité de certification racine.