Get SSL Certificate Using Letsencrypt Certbot

Overview

Before letsencrypt will generate and deliver a certificate for you it must test whether you indeed control the DNS RECORDS for that domain. It does that by asking you to create a TXT record that it can check through the domain name system. So you use certbot to request your certificate. It supplies you with what it wants in the TXT record. You create the txt record using your interface to the DNS service you are using and when the new record has propagated, you press continue allowing certbot to complete the task and save your certificate.

Install Certbot

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

Request the certificate

```
sudo certbot certonly --manual --preferred-challenges dns -d yoursite.example.com
# At this point You will be asked for a TXT record similar to this:
# name:  _acme-challenge.yoursite.example.com.
# value: Tv1E2PLJyIU1ePiLfW-bv8SdAq4wa3QDud76zfB7asU
# And prompted to press enter to continue.
# Wait until the steps below are done before continuing.
```

Add the TXT record

Using your web interface to your DNS service add a TXT record like this.

_acme-challenge.yoursite TXT Tv1E2PLJyIU1ePiLfW-bv8SdAq4wa3QDud76zfB7asU

DNS records take time to propagate, so you must first make sure that the record has propagated before you press continue on the certbot prompt.

Verify that it has propagated

In anoter terminal window type the following command once in a while until your TXT record appears in the answer section.

```
dig -t txt _acme-challenge.yoursite.example.com
```

Continue certbot in the original terminal window

Press Enter. Your certificate files will be here: /etc/letsencrypt/live/yoursite.example.com/

fullchain.pem:

Contains your domain's SSL certificate and the necessary intermediate certificates to form a valid chain of trust back to the Let's Encrypt root certificate.

privkey.pem:

Your private key, which must be kept secret to secure your website.

cert.pem:

Contains your domain's specific SSL certificate.

chain.pem:

Contains the intermediate certificate(s) that link your domain's certificate to the root CA.