Issue and renew a web server certificate from letsencrypt on AWS EC2

Author : Tobias Hofmann

Date : June 19, 2020

I'll show how to obtain a valid letsencrypt certificate for Apache on AWS EC2 Linux AMI and Namecheap as DNS provider.

Running a private web server on AWS EC2 is easy. Managing it is not so easy. Having a valid TLS web server certificate from letsencrypt is one of the managing jobs that could be easier. I was told that this part is easier on Azure, maybe I should take a look at that option. Letsencrypt for an AWS Linux AMI isn't as easy as it normally is to manage your web certificates with letsencrypt as the standard letsencrypt client certbot is not fully working and supported. It works, but you have to run it in debug mode, and sometimes it won't work. See google for how many people got into problems because certbot stopped working on AMI Linux.

As letsencrypt is following a protocol for issuing a certificate (ACME), you can choose from a wide range of alternatives. One that is working with the AWS Linux AMI is acme.sh. It supports ACME v2. This is important when you want to have wildcard certificates and still getting normal certificates, as the v1 protocol is EOL. Acme.sh can do everything automatically once configured, making it really easy to always have a valid certificate.

> **Note**
>
> My setup is an exception from the rule. My DNS is hosted by Namecheap. They do not allow to script the DNS configuration if you are not a meeting some minimum requirements. As the ACME protocol validates if you are the owner of a DNS by setting a TXT entry: I have to do this manually (thanks for nothing Namecheap). Therefore, my setup is a little bit different.

Installation

Follow the installation detailed at the acme.sh wiki.

```
curl https://get.acme.sh | sh
```

Get certificate for given FQDN

You run the program and inform the fqdn (parameter -d) and the document root of your web server (parameter -w). Acme.sh takes care of the rest.

```
./acme.sh --issue -d www.itsfullofstars.de -w /var/www/wordpress/
```

Activate certificate

Above step obtained the certificate from letsencrypt CA. To activate them, you have to copy them to Apache directory and restart the http server.

```
./acme.sh --install-cert -d www.itsfullofstars.de --cert-file /etc/letsencrypt
/live/www.itsfullofstars.de/cert.pem --key-file /etc/letsencrypt/live/www.itsf
ullofstars.de/privkey.pem --fullchain-
file /etc/letsencrypt/live/www.itsfullofstars.de/fullchain.pem
```

Get wildcard certificate

In case you want a wildcard certificate, the procedure is a little bit different. Normally acme.sh can handle the extra validation work needed for a wildcard certificate. With namecheap, you have to do set the DNS

entries to validate that you are the owner of the domain manually. The wildcard process contains of two steps:

1. Get a TXT challenge that you add to your DNS and
2. Validate the TXT challenge and get the certificate

Run program to get the TXT challenge

```
./acme.sh --issue -d itsfullofstars.de -d '*.itsfullofstars.de' -w /var/www/wo
rdpress/ --force --dns --yes-I-know-dns-manual-mode-enough-go-ahead-please
```

In the output you can see that you have to create a TXT record for _acme-challenge.. and assign the provided text value to it. Letsencrypt will check for that value to validate that you are the owner of the domain. If you can change the DNS entry, you are the owner. Make sure to know how add a TXT record to your DNS.

Set DNS value.

```
Domain: '_acme-challenge.itsfullofstars.de' TXT value: 'DvHx946wm_jdipMIA88hll
3Z11JM62kp7nWpKQiYhZQ'
```

Check if new TXT value is available.

```
dig -t txt _acme-challenge.itsfullofstars.de
```

Only if this command shows that the TXT value is updated, you can continue with the next step!

Validate the TXT challenge and get the certificate

When the new TXT record is available, the wildcard certificate can be requested. Run the same command as before, but use –renew instead of –issue.

```
./acme.sh --renew -d itsfullofstars.de -d '*.itsfullofstars.de' -w /var/www/wo
rdpress/ --force --dns --yes-I-know-dns-manual-mode-enough-go-ahead-please
```

To activate the new certificate, you have to restart the httpd server.