Setup of a ssl certificate with let’s encrypt

Clément Levallois

2017-04-09

Table of Contents

last modified: 2017-04-09

System

- I use Debian, version 8.7 (why?)
- Vi is used as a text editor in the following

Why SSL?

For users, no SSL shows as "http://" in front of a website address, and with SSL it shows as "https://"

"https" means that the connection between the user and the website is encrypted. It is useful for:

- human to machine communication: https keeps the email you write private on its way to gmail.com
- machine to machine communication: the api secret used by a machine to authenticate in a GET or PUT request is kept private.

Installing the Certbot by Let's Encrypt

Let's Encrypt is a product launched in 2015 by the Electronic Frontier Foundation (EFF) providing SSL certification for free, and made easy.

The "certbot" is the EFF's latest package to let your server use let's encrypt capabilities.

So, let's install the certbot:

```
vi /etc/apt/sources.list.d/sources.list
```

In this file, add a line `deb http://ftp.debian.org/debian jessie-backports main`

Then:

```
apt-update
```

```
sudo apt-get install certbot -t jessie-backports
```

- make sure your domain already points to the IP of your server (with a DNS record)
- make sure your firewall allows port 443 (with ufw: just do sudo ufw allow 443).

Then:

```
certbot certonly
```

→ in the interactive window, choose "standalone. Follow the instructions.

That's it. Certificates get installed at:

```
/etc/letsencrypt/live/yourdomainname.com
```

Automatic renewal of SSL certificates

Certificates expire after 90 days, so renewing them manually and regularly is a pain.

Thanks to certbot, they will renew themselves automatically, you don't need to add any script. Just check that it indeed works:

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

(this will not renew them, but just simulate the action)

This command is useful because you may realize that your port 443 needs to be open for the renewal to succeed. With Nginx or another reverse proxy running, 443 is already in use so the the renewal will fail.

Solution for nginx:

- with root privileges, edit a crontab:

  ```
  crontab -e
  ```

Add the following line:

@monthly certbot renew --pre-hook "service nginx stop" --post-hook "service nginx start"

This will test every month the need to renew certificates. Only when there is a need, nginx will be stopped before then restarted after the operation.

the end

Author of this tutorial: Clement Levallois

All resources on linux security: https://seinecle.github.io/linux-security-tutorials/