Certbot SSL Certificates

Its important to encrypt your web traffic to keep you and anyone who passes information through your website secure.

To install Certbot and generate an SSL certificate, run the below commands.

```
curl -o- https://raw.githubusercontent.com/vinyll/certbot-install/master/install.sh | bash
# Generate a certificate, but don't do any automatic NGINX configuration
sudo certbot certonly --nginx -d domain.com -d www.domain.com
```

Since we passed the `certonly` argument to `certbot`, there will not be any automatic configuration of our NGINX server to use SSL. In my experience using this automatic configuration tool on an NGINX server that has already been modified from the default settings doesn't work very well, so I'll explain the required changes to `nginx.conf` later on this page.

There are a few benefits to using Certbot. Your certificates will automatically be renewed when nearing expiration, and it can configure several different web servers to use the new SSL certificate automatically. I personally do the configuring manually, but on a new server the automatic configuration might be a useful feature to you!

To check on the time left until certbot renews -

```
sudo systemctl status certbot.timer
```

Dry run renew with your current configuration -

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

Check installed certificates on this system -

```
sudo certbot certificates
Saving debug log to /var/log/letsencrypt/letsencrypt.log
OCSP check failed for /etc/letsencrypt/live/domain.com/cert.pem (are we offline?)

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Found the following certs:
  Certificate Name: domain.com
    Domains: domain.com www.domain.com
    Expiry Date: 2020-08-18 03:00:10+00:00 (INVALID: EXPIRED)
```

```
    Certificate Path: /etc/letsencrypt/live/domain.com/fullchain.pem
    Private Key Path: /etc/letsencrypt/live/domain.com/privkey.pem
  Certificate Name: other-domain.com
    Domains: other-domain.com www.other-domain.com
    Expiry Date: 2020-08-24 22:16:30+00:00 (VALID: 6 days)
    Certificate Path: /etc/letsencrypt/live/other-domain.com/fullchain.pem
    Private Key Path: /etc/letsencrypt/live/other-domain.com/privkey.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

NGINX SSL Setup

Now we need a webserver to redirect traffic over https. The below nginx configuration is verified to be working on Ubuntu 20.04 using certbot certificates to decrypt the traffic on default port 80, then passing it to a container hosted locally on a specific port. See the NGINX Book for more details on configuring nginx.

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events { }

http {
  include mime.types;

  # Redirect root domains
  server {
    listen 80;
    server_name domain.com www.domain.com;
    return 301 https://www.domain.com$request_uri;
  }



  # SSL - domain.com
  server {
    server_name domain.com www.domain.com;
    server_tokens off;
    listen 443 ssl;
```

```
    ssl_certificate /etc/letsencrypt/live/domain.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/domain.com/privkey.pem;

    # Pass to container
    location / {
      include proxy_params;
      proxy_pass http://localhost:1234/;
    }
  }

}
```

Errors

Sometimes, if your webserver is running already, you may see the following error

```
Attempting to renew cert (domain.com) from /etc/letsencrypt/renewal/domain.com.conf produced an unexpected error: Problem binding to port 80: Could not bind to IPv4 or IPv6.. Skipping.
```

To fix this, we can use certbot's `--pre-hook` and `--post-hook` options

```
sudo certbot renew --dry-run --pre-hook 'service nginx stop' --post-hook 'service nginx start'
```

You can also add executables to the `/etc/letsencrypt/renewal-hooks/pre` and `/etc/letsencrypt/renewal-hooks/post` directories and certbot will automatically handle executing them on a request to renew certificates, removing the need to specify these arguments each time.

See Official Certbot Documentation for more info. An important point made there can be seen in the quote below

> These hooks are run in alphabetical order and are not run for other subcommands. (The order the hooks are run is determined by the byte value of the characters in their filenames and is not dependent on your locale.)
>
> Hooks specified in the command line, configuration file, or renewal configuration files are run as usual after running all hooks in these directories.

More help can be found within a termianl with `sudo certbot --help renew`

Revision #9
Created 2019-05-24 14:27:49 UTC by Shaun Reed
Updated 2022-03-15 20:59:14 UTC by Shaun Reed