Let’s Encrypt TLS/SSL Certificate with Nginx on Arch Linux Server

Last Updated: April 6th, 2017 Xiao Guoan (Admin) 0 Comment Nginx

In this tutorial, we’re going to look at how to obtain and install a free Let’s Encrypt TLS/SSL certificate with Nginx on Arch Linux server.

Obtain a Free Let’s Encrypt TLS/SSL Certificate

First we need to install the letsencrypt client which is available in Arch Linux community repository. So run this command to install it.

```
sudo pacman -S certbot
```

There are two plugins we can use to obtain a certificate for Nginx Web server: standalone and Webroot. I recommend using the Webroot plugin. It has the following two advantages over the standalone plugin when obtaining and renewing your certificates.

- The standalone plugin needs to start a temporary standalone Web server which requires you to stop Nginx. Using the Webroot plugin, you don’t have to stop Nginx.
- Domain validation used by the standalone plugin requires you to point your domain name to the IP address of your origin server. This means if you are using a CDN service like CloudFlare, then you must expose your origin server to the world during the obtaining and renewing process. You don’t have to do so with the Webroot plugin.

The Webroot plugin validates you by placing a temporary file under `your-web-root/.well-known/acme-challenge/`.

To obtain a certificate with the Webroot plugin, run the following command.

```
sudo cerrbot certonly --webroot --email <your-email-address> -d www.example.com -d example.com -w /usr/share/nginx/example.com/
```

The subcommmand `certonly` tells letsencrypt client to obtain a certificate, but do not install it because letsencrypt client doesn't support auto-configuration for Nginx at time of writing.

`--webroot` flag tells letsencrypt client to use the Webroot plugin.

Replace <your-email-address> with your real email address. Replace www.example.com and example.com with your real domain name. You can include up to 100 domain names, just add another `-d` flag followed by your domain name.

`-w` is short for `--webroot-path`. `/usr/share/nginx/example.com` is a common Nginx Web root.

Within a few seconds, you should see a congrats message like below.

```
Congratulations! Your certificate and chain have been saved at
/etc/letsencrypt/live/www.example.com/fullchain.pem. Your cert
will expire on 2016-08-23. To obtain a new version of the
certificate in the future, simply run Let's Encrypt again.
```

If you see a 403 forbidden error after running the above command, that's probably because your Nginx configurations doesn't allow access to hidden files. To enable access to `your-web-root/.well-known/acme-challenge`, add the following directive to your Nginx config file.

```
location ~ /.well-known/acme-challenge {
    allow all;
}
```

Then reload Nginx configuration.

```
sudo systemctl reload nginx
```

And run the letsencrypt command again to obtain your certificate.

Install the Certificate

Edit your Nginx config file.

```
sudo nano /etc/nginx/conf.d/your-site.conf
```

Change the contents in this file like blow.

```
server {
  listen 80;
  server_name www.example.com;
  return 301 https://www.example.com$request_uri;
}
server {
  listen 443 ssl;
  server_name www.example.com;

  ssl_protocols TLSv1.1 TLSv1.2;
  ssl_certificate /etc/letsencrypt/live/www.example.com/fullchain.pem;
  ssl_certificate_key /etc/letsencrypt/live/www.example.com/privkey.pem;

  access_log /var/log/nginx/www.example.com.log;
  root /var/www/html;
....
}
```

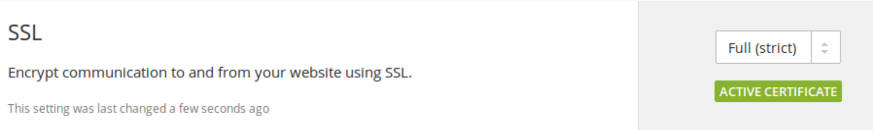
Save and close the file. Then test and reload Nginx configuration.

```
sudo nginx -t

sudo systemctl reload nginx
```

Now visit your Web site, you should see a green padlock in the address bar.

If you are using a CDN service like CloudFlare, you may need to enable SSL in your CDN control panel.



SSL

Encrypt communication to and from your website using SSL.

This setting was last changed a few seconds ago

Full (strict)

ACTIVE CERTIFICATE

Auto Renew Your Certificate

Let’s Encrypt certificates last for 90 days. To renew your certificate, simply run the same command again. To automatically renew the certificate, your can edit root user’s crontab.

```
sudo crontab -e
```

Then add a monthly cron job like below. Again, replace the email address and domain name.

```
@monthly certbot renew --quiet
```

The command will run at 00:00 on 1st day of every month.

Rate this tutorial

☆☆☆☆☆ [Total: 0 Average: 0]

Arch Linux server   Let's Encrypt   Nginx   SSL Certificate