FreeBSD Administration - Support #843

LetsEncrypt Auto Renewal for Nginx on FreeBSD

08/21/2016 09:49 PM - Daniel Curtis

Status:	Closed	**Start date:**	08/21/2016
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Web Server	**Estimated time:**	1.00 hour
Target version:	FreeBSD 10	**Spent time:**	6.50 hours

Description

This is a guide for setting up auto-renewal for a LetsEncrypt certificate used on an nginx site on FreeBSD 10.

Prepare the Environment

- Make sure the system is up to date:

```
pkg update && pkg upgrade
```

Nginx Config

- Create a configuration directory to make managing individual server blocks easier

```
mkdir /usr/local/etc/nginx/conf.d
```

- Edit the main nginx config file:

```
vi /usr/local/etc/nginx/nginx.conf
```

  - And strip down the config file and add the include statement at the end to make it easier to handle various server blocks:

```
worker_processes  1;
error_log  /var/log/nginx-error.log;

events {
    worker_connections  1024;
}

http {
    include       mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;

    # Load config files from the /etc/nginx/conf.d directory
    include /usr/local/etc/nginx/conf.d/*.conf;
}
```

- Create the default site folder:

```
mkdir -p /usr/local/www/sites/www.example.com
```

- Setup the default site configuration:

```
vi /usr/local/etc/nginx/conf.d/www.example.com.conf
```

- Then add or modify the configuration to look similar to the following:

```
server {
    listen 80;
#    listen 443 default ssl;
    server_name www.example.com;

    # Turn on ans set SSL key/cert
#    ssl on;
#    ssl_certificate /usr/local/etc/letsencrypt/live/www.example.com/fullchain.pem;
#    ssl_certificate_key /usr/local/etc/letsencrypt/live/www.example.com/privkey.pem;

    # Strong SSL configuration
#    ssl_ciphers 'AES128+EECDH:AES128+EDH:!aNULL';
#    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
#    ssl_session_cache  builtin:1000  shared:SSL:10m;
#    ssl_stapling on;
#    ssl_stapling_verify on;
#    ssl_prefer_server_ciphers on;
#    ssl_dhparam /usr/local/etc/nginx/dhparam.pem;
#    add_header Strict-Transport-Security max-age=63072000;
#    add_header X-Frame-Options SAMEORIGIN;
#    add_header X-Content-Type-Options nosniff;

    root /usr/local/www/sites/www.example.com;
    index index.html index.htm;
    autoindex on;

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

- Restart nginx to load the new website config:

```
service nginx restart
```

LetsEncrypt

- Install the LetsEncrypt certbot:

```
pkg install py27-certbot
```

- Create the letsencrypt config directory:

```
mkdir -p /usr/local/etc/letsencrypt/configs
```

- Then create the initial letsencrypt domain config:

```
vi /usr/local/etc/letsencrypt/config/www.example.com.conf
```

- And add the following:

```
# the domain we want to get the cert for;
domains = www.example.com

# increase key size
rsa-key-size = 4096

# the current closed beta (as of 2015-Nov-07) is using this server
server = https://acme-v01.api.letsencrypt.org/directory

# this address will receive renewal reminders, IIRC
email = bob@example.com

# turn off the ncurses UI, we want this to be run as a cronjob
text = True

# agree to the terms of service
agree-tos

# authenticate by placing a file in the webroot and then letting LE fetch it
authenticator = webroot
webroot-path = /usr/local/www/sites/www.example.com
```

- Generate the first certificate:

```
certbot certonly --config /usr/local/etc/letsencrypt/config/www.example.com.conf
```

Automatic Renewal

- Test automatic renewal for your certificates by running this command:

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

- If that appears to be working correctly, you can arrange for automatic renewal by adding a cron or systemd job which runs the following:

```
certbot renew --quiet
```

- Edit the root cron table:

```
crontab -e
```

  - And add the following to the end of the file:

```
# LetEncrypt monthly renewal
30 2 * * 1 /usr/local/bin/certbot renew --quiet >> /var/log/le-renew.log

# Reload nginx after LetsEncrypt renewal
40 2 * * 1 /usr/local/etc/rc.d/nginx reload
```

Nginx SSL

- Generate the dhparam file:

```
openssl dhparam -out /usr/local/etc/nginx/dhparam.pem 4096
```

- Edit the default site configuration:

```
vi /usr/local/etc/nginx/conf.d/www.example.com.conf
```

  - Uncomment the SSL configuration options to enable SSL:

```
server {
    listen 80;
    listen 443 default ssl;
    server_name www.example.com;

    # Turn on ans set SSL key/cert
    ssl on;
    ssl_certificate /usr/local/etc/letsencrypt/live/www.example.com/fullchain.pem;
    ssl_certificate_key /usr/local/etc/letsencrypt/live/www.example.com/privkey.pem;

    # Strong SSL configuration
    ssl_ciphers 'AES128+EECDH:AES128+EDH:!aNULL';
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_session_cache  builtin:1000  shared:SSL:10m;
    ssl_stapling on;
    ssl_stapling_verify on;
    ssl_prefer_server_ciphers on;
    ssl_dhparam /usr/local/etc/nginx/dhparam.pem;
    add_header Strict-Transport-Security max-age=63072000;
    add_header X-Frame-Options SAMEORIGIN;
    add_header X-Content-Type-Options nosniff;

    root /usr/local/www/sites/www.example.com;
    index index.html index.htm;
    autoindex on;

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

Resources

- https://wiki.freebsd.org/BernardSpil/LetsEncrypt
- https://gist.github.com/xrstf/581981008b6be0d2224f
- https://laracasts.com/discuss/channels/general-discussion/installing-letsencrypt-certificate-and-auto-renewal
- https://www.digitalocean.com/community/tutorials/how-to-secure-nginx-with-let-s-encrypt-on-ubuntu-14-04#step-4-%E2%80%94-set-up-auto-renewal
- https://certbot.eff.org/all-instructions/#freebsd-none-of-the-above

History

#1 - 08/22/2016 02:35 PM - Daniel Curtis

- Description updated

- Status changed from New to In Progress

- % Done changed from 0 to 30

#2 - 08/22/2016 09:08 PM - Daniel Curtis

- Tracker changed from Bug to Support

- Description updated

- Status changed from In Progress to Resolved

- % Done changed from 30 to 100

#3 - 09/12/2016 07:29 PM - Daniel Curtis

- Status changed from Resolved to Closed

#4 - 09/27/2016 08:04 AM - Daniel Curtis

- Description updated

#5 - 09/30/2016 11:00 PM - Daniel Curtis

- Description updated