FreeBSD Administration - Support #825

Using LetsEncrypt Certbot to Create SSL Certificates on FreeBSD

07/07/2016 05:28 PM - Daniel Curtis

Status:	Closed	**Start date:**	07/07/2016
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Web Server	**Estimated time:**	0.50 hour
Target version:	FreeBSD 9	**Spent time:**	2.00 hours

Description

This is a guide on setting up SSL key and certificates using the certbot tool on an nginx webserver running FreeBSD 9.

Prepare the Environment

- Make sure the system is up to date:

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

Install Certbot

- Install certbot:

```
pkg install py27-certbot
```

(Method 1) Standalone Server

This is useful for non-web servers like XMPP and mail servers.

- Use the certbot in standalone mode:

```
certbot certonly --standalone -d www.example.com
```

(Method 2) Nginx Site

- Create the acme-challenge directory:

```
mkdir /usr/local/www/www.example.com/.well-known/acme-challenge
```

- Edit the nginx server config for the site:

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

  - And add the following location block inside of the server block of the site:

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

    location '/.well-known/acme-challenge' {
      default_type "text/plain";
      root        /usr/local/www/www.example.com/.well-known/acme-challenge;
```

```
    }
```

- Restart nginx:

```
service nginx restart
```

- Obtain SSL certificate

```
certbot certonly --webroot -w /usr/local/www/www.example.com -d www.example.com
```

- Choose to Place the files in webroot directory (webroot)
- Enter an email address

(Method 3) Nginx Reverse Proxy

This is useful when a site or service is behind an nginx reverse proxy.

- Create the reverse proxy config on the nginx server:

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

  - And add the following to allow passing the well-known acme-challenge directory to the service requesting a letsencrypt certificate:

```
server {
    listen 80;
    server_name www.example.com;

    location '/.well-known/acme-challenge' {
      proxy_pass http://www.example.com:80;
    }
}
```

- Then restart nginx to apply the config:

```
service nginx restart
```

- Now on the site or server requesting the certificate, run the certbot in standalone mode:

```
certbot certonly --standalone -d www.example.com --standalone-supported-challenges http-01
```

Add SSL to Nginx

- Setup the Diffie-Hellman Key Exchange Parameters

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

- Edit the site server config:

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

- And add a SSL block for the site:

```
server {
  listen 443 ssl;
  server_name www.example.com;
  access_log  /var/log/www.example.com-access.log;
  error_log  /var/log/www.example.com-error.log;

  # 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 ORIGIN;
  add_header X-Content-Type-Options nosniff;

  root /usr/local/www/www.example.com;

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

  location '/.well-known/acme-challenge' {
    default_type "text/plain";
    root        /usr/local/www/www.example.com/.well-known/acme-challenge;
  }

  ## Disable .htaccess and other hidden files
  location  /. {
      return 404;
  }

 ## Allow a static html file to be shown first
  location / {
    index index.html index.php;
    try_files $uri $uri/;
    expires 30d;
  }
}
```

Resources

- https://github.com/certbot/certbot
- https://certbot.eff.org/docs/using.html#command-line-options
- https://wiki.archlinux.org/index.php/Let%E2%80%99s_Encrypt
- https://certbot.eff.org/all-instructions/#freebsd-nginx
- https://kristaps.bsd.lv/letskencrypt/
- https://community.letsencrypt.org/t/404-on-well-known-acme-challenge/15565/6

History

#1 - 07/07/2016 05:31 PM - Daniel Curtis

- Status changed from New to Resolved

- % Done changed from 0 to 100

#2 - 08/05/2016 08:57 PM - Daniel Curtis

- Status changed from Resolved to Closed

#3 - 08/07/2016 09:18 PM - Daniel Curtis

- Description updated

#4 - 08/07/2016 09:32 PM - Daniel Curtis

- Description updated

#5 - 08/07/2016 09:42 PM - Daniel Curtis

- Description updated