# LetsEncrypt SSL 证书签发 (Nginx)

作者：ixiaozhi
原文链接：https://ld246.com/article/1501949183701
来源网站：链滴

# 概述

官方文档参考: let's encrypt getting started

域名认证过程有自动认证与手动认证，自动认证会启动一个监听 80 端口的程序来完成自动认证。手认证使用参数 --webroot 来进行使用网站访问手动认证，认证时，会访问网址 /.well-known/acme-hallenge/xxxxxxxx。

每次签发的证书有 90 天的有效期，所以我们还得在每个月去重新签发一个新的证书。

本文的操作是基于系统 CentOS 6.7 操作进行。

# 准备工作

在取得官方代码前，得先查看系统环境中是否安装全所需要的工具软件。

- Git

```
yum -y install git
```

- python 2.7 检查

```
/usr/bin/python -V #查看版本
```

- 安装编译需要的工具

```
yum install zlib-devel bzip2-devel openssl-devel xz-libs wget xz
```

- 安装 Python2.7.8

```
wget http://www.python.org/ftp/python/2.7.8/Python-2.7.8.tar.xz
xz -d Python-2.7.8.tar #下载源码
tar -xvf Python-2.7.8.tar #解压
cd Python-2.7.8 #进入目录
./configure --prefix=/usr/local #运行配置
make
make altinstall #编译及安装
python2.7 -V #检查版本
export PATH="/usr/local/bin:$PATH"
cd ../
```

- 安装 pip 及 virtualenv

```
wget --no-check-certificate https://pypi.python.org/packages/source/s/setuptools/setuptools
1.4.2.tar.gz #下载源码
tar -xvf setuptools-1.4.2.tar.gz #解压
cd setuptools-1.4.2
python2.7 setup.py install #用 Python2.7.8安装setuptools
cd ../

curl https://bootstrap.pypa.io/get-pip.py | python2.7 -   #安装pip
pip2.7 install virtualenv   #安装virtualenv
```

# 域名认证并生成证书

- 从官方 Git 库中取得代码。

```
git clone https://github.com/letsencrypt/letsencrypt
cd letsencrypt
```

- 自动认证 standalone 模式

运行认证程序。

```
service nginx stop #停止 Nginx 服务器
./letsencrypt-auto certonly --standalone -d ixiaozhi.com -d www.ixiaozhi.com
```

letsencrypt-auto 按照提示输入 E-mail 和域名即可。在运行认证程序前，要先停用 nginx，因为接来的环节需要占用80等端口。之后证书会生成到 /etc/letsencrypt/live/ixiaozhi.com/ 下，其中的 ixiaozhi.com 改为自己的域名。

- 手动认证 webroot 模式

Nginx 添加目录访问：

```
location /.well-known/acme-challenge/ {
    default_type text/plain;
    root /home/ixiaozhi/acme-challenge/;
}
```

添加目录，并重启服务：

```
cd /home/ixiaozhi/
mkdir acme-challenge
service nginx restart
```

进行认证并生成证书：

```
service nginx reload

./letsencrypt-auto certonly --webroot -w /home/ixiaozhi/acme-challenge -d ixiaozhi.com -d
ww.ixiaozhi.com
```

认真阅读输出信息，输入邮箱且同意协议后，成功后会输出：

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/ixiaozhi.com/fullchain.pem. Your cert will
   expire on 2016-05-29. To obtain a new version of the certificate in
   the future, simply run Let's Encrypt again.
 - If you like Let's Encrypt, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

看到 Congratulations 我们就放心了。之后证书会生成到 /etc/letsencrypt/live/ixiaozhi.com/ 下。

# 配置 Nginx

修改 Nginx 的 nginx.conf，添加配置 ssl。

```
listen 80;
listen 443 ssl;
ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
server_name ixiaozhi.com;

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

重启 nginx 即可。

# 定时任务定时签发证书

我们可以先测试一个 renew 证书是否可以成功。

```
./letsencrypt-auto renew --email admin@ixiaozhi.com --dry-run --agree-tos
```

当看到 Congratulations, all renewals succeeded. The following certs have been renewed 时，试就是通过的。使用 --dry-run 参数来测试并不会保存任何证书。

如果需要自动更新，先使用“crontab -e”，选择编辑器后，在最底部加入

```
0 0 1 * * ./letsencrypt-auto renew --email admin@ixiaozhi.com --agree-tos --force-renewal
```

crontab 的时间格式为：

```
*     *     *     *     *      command
分    时    日    月    周     命令
```

添加成功后，可以使用 crontab -l 查看当前用户的定时任务，确认是否已经生效。

# 转发设置

如果希望访问 http 都跳转至 https 进行访问，可以通过两种方法进行转发。（如果是使用 --webroot 进行认证的，在 nginx 设置中要把 /.well-known/acme-challenge/ 例外不进行转发）

一个是直接利用 nginx 进行转发。

```
server {
    listen 80;
    server_name ixiaozhi.com;
    return https://ixiaozhi.com$request_uri;

...
```

一个是设置HSTS。

```
server {
    add_header Strict-Transport-Security "max-age=63072000;includeSubdomains; preload";
    #添加一行
```

...

别忘了上述设置都需要重启 Nginx。

# 参考资料

- let's encrypt getting started
- let's encrypt github
- Nginx 安装 Let's Encrypt 免费 SSL 证书
- 免费 SSL 证书 Let’ s Encrypt 安装使用教程
- Ghost Blog 启用 HTTPS 使用 Let's Encrypt SSL 证书
- Let's Encrypt 花三分钟免费接入 SSL 证书