链滴

使用 acme-tiny 工具生成 Let'"'"'s Encrypt 的免费 SSL 证书

作者：aqjun

原文链接：https://ld246.com/article/1487899289204

来源网站：链滴

下载acme-tiny

下载地址：https://github.com/diafygi/acme-tiny

创建用户私钥和域名私钥 "创建用户私钥和域名私钥")创建用户私钥域名私钥

```
mkdir -p /etc/ssl/letsencrypt/
cd /etc/ssl/letsencrypt/

openssl genrsa 4096 > account.key
openssl genrsa 4096 > domain.key
```

生成域名csr文件 "生成域名csr文件")生成域名csr文件

单域名

```
openssl req -new -sha256 -key domain.key -subj "/CN=www.yoursite.com" > domain.csr
```

多域名

```
ln -s /etc/pki/tls/openssl.cnf /etc/ssl/openssl.cnf


openssl req -new -sha256 -key domain.key -subj "/" -reqexts SAN -config <(cat /etc/ssl/open
sl.cnf <(printf "[SAN]\nsubjectAltName=DNS:yoursite.com,DNS:www.yoursite.com")) > domai
.csr
```

配置web站点的challenge文件 "配置web站点的challenge文件")置web站点的challenge文件

```
mkdir -p /var/www/challenges/

#example for nginx
server {
 listen 80;
 server_name yoursite.com www.yoursite.com;

 location /.well-known/acme-challenge/ {
 alias /var/www/challenges/;
 try_files $uri =404;
 }

 ...the rest of your config
}
```

生成signed文件 "生成signed文件")生成signed文件

```
wget -c https://raw.githubusercontent.com/yangphere/acme-tiny/master/acme_tiny.py --no-
heck-certificate
python acme_tiny.py --account-key /etc/ssl/letsencrypt/account.key --csr /etc/ssl/letsencrypt
```

原文链接：使用 acme-tiny 工具生成 Let'"'"'s Encrypt 的免费 SSL 证书

```
domain.csr --acme-dir /var/www/challenges/ > /etc/ssl/letsencrypt/signed.crt
```

生成证书链 "生成证书链")生成证书链

v1版，兼容性差点

```
wget -O - https://letsencrypt.org/certs/lets-encrypt-x1-cross-signed.pem > /etc/ssl/letsencry
t/intermediate.pem
cat /etc/ssl/letsencrypt/signed.crt /etc/ssl/letsencrypt/intermediate.pem > /etc/ssl/letsencrypt
chained.pem
```

建议使用v3版

```
wget -O - https://letsencrypt.org/certs/lets-encrypt-x3-cross-signed.pem > /etc/ssl/letsencry
t/intermediate.pem
cat /etc/ssl/letsencrypt/signed.crt /etc/ssl/letsencrypt/intermediate.pem > /etc/ssl/letsencrypt
chained.pem
```

生成dh证书 "生成dh证书")生成dh证书

```
openssl dhparam -out dhparam.pem 2048
```

配置nginx使SSL证书生效 "配置nginx使SSL证书生效")配置nginx SSL证书生效

```
server {
 listen 443;
 server_name yoursite.com, www.yoursite.com;

 ssl on;
 ssl_certificate /etc/ssl/letsencrypt/chained.pem;
 ssl_certificate_key /etc/ssl/letsencrypt/domain.key;
 ssl_session_timeout 5m;
 ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
 ssl_ciphers ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-
ES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-RSA-
ES256-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA;
 ssl_session_cache shared:SSL:50m;
 ssl_dhparam /etc/ssl/letsencrypt/dhparam.pem;
 ssl_prefer_server_ciphers on;

 ...the rest of your config
}

server {
 listen 80;
 server_name yoursite.com, www.yoursite.com;

 location /.well-known/acme-challenge/ {
 alias /var/www/challenges/;
 try_files $uri =404;
 }
```

```
 ...the rest of your config
}
```

重启nginx服务 "重启nginx服务")重启nginx服务

```
service nginx reload
```

自动生成SSL证书 "自动生成SSL证书")自动生成SSL证书

由于Let’ s Encrypt的证书只有90天的有效期，需要使用系统每个月生成一次。编辑**renew_cert.sh**件

以下是v1版，兼容性差点

```
#!/usr/bin/sh
python /etc/ssl/letsencrypt/acme_tiny.py --account-key /etc/ssl/letsencrypt/account.key --csr
etc/ssl/letsencrypt/domain.csr --acme-dir /var/www/challenges/ > /etc/ssl/letsencrypt/signed
crt || exit
wget -O - https://letsencrypt.org/certs/lets-encrypt-x1-cross-signed.pem > /etc/ssl/letsencry
t/intermediate.pem
cat /etc/ssl/letsencrypt/signed.crt /etc/ssl/letsencrypt/intermediate.pem > /etc/ssl/letsencrypt
chained.pem
service nginx reload
```

建议使用v3版

```
#!/usr/bin/sh
python /etc/ssl/letsencrypt/acme_tiny.py --account-key /etc/ssl/letsencrypt/account.key --csr
etc/ssl/letsencrypt/domain.csr --acme-dir /var/www/challenges/ > /etc/ssl/letsencrypt/signed
crt || exit
wget -O - https://letsencrypt.org/certs/lets-encrypt-x3-cross-signed.pem > /etc/ssl/letsencry
t/intermediate.pem
cat /etc/ssl/letsencrypt/signed.crt /etc/ssl/letsencrypt/intermediate.pem > /etc/ssl/letsencrypt
chained.pem
service nginx reload
```

添加可执行权限

```
chmod +x renew_cert.sh
```

编辑crontab文件

```
crontab -e
```

加入如下内容

```
0 0 1 * * /etc/ssl/letsencrypt/renew_cert.sh 2>> /var/log/acme_tiny.log
```

重启crontab服务

```
service crond restart
```

测试一下SSL质量 "测试一下SSL质量")测试一下SSL质量

网址：https://www.ssllabs.com/ssltest/