https免费证书配置

背景

1、http 和 https 是什么？ 简单来说，http 是一个传输网页内容的协议，比如你看到的 http 开头的网站 http://www.163.com，其网页上的文字、图片、 CSS 、 JS 等文件都是通过 http 协议传输到我们的浏览器，然后被我们看到。 而 https 可以理解为“ HTTP over SSL/TLS ”，好端端的 http 为什么需要“ over SSL/TLS ”呢，因为 http 是明文传输的，通过 http 协议传输的内容很容易被偷看和篡改，为了安全（你肯定不想被人偷看或者篡改网页内容吧，比如网站银行密码什么的。）就为 http 协议再加上了一层 SSL/TLS 安全协议，所以就有了 https 。

2、SSL/TLS 是什么?

“ HTTP over SSL/TLS ”字面意思就是带“安全套接层”的 http 协议，其中 SSL 是“ Secure Sockets Layer ” 的缩写，是“安全套接层”的意思。 TLS 是 “Transport Layer Security” 的缩写，是 ” 传输层安全协议 ” 的意思。 SSL 和 TLS 是同一个东西的不同阶段，理解为同一个东西也行，都是安全协议就对了。

3、为什么要部署 https?

说到底，就是 https 更安全。甚至为了安全，一个专业可靠的网站， https 是必须的。 Firefox 和 Chrome 都计划将没有配置 SSL 加密的 http 网站标记为不安全（貌似 Firefox 50 已经这么干了），目前它们也正在联合其他相关的基金会与公司推动整个互联网 https 化，现在大家访问的一些主要的网站。如 Google 多年前就已经全部启用 https ，国内的淘宝、搜狗、知乎、百度等等也全面 https 了。甚至 Google 的搜索结果也正在给予 https 的网站更高的排名和优先收录权。

4、怎么部署 https 呢?

你只需要有一张被信任的 CA （ Certificate Authority ）也就是证书授权中心颁发的 SSL 安全证书，并且将它部署到你的网站服务器上。一旦部署成功后，当用户访问你的网站时，浏览器会在显示的网址前加一把小绿锁，表明这个网站是安全的，当然同时你也会看到网址前的前缀变成了 https ，不再是 http 了。

5、怎么获得 SSL 安全证书呢?

理论上，我们自己也可以签发 SSL 安全证书，但是我们自己签发的安全证书不会被主流的浏览器信任，所以我们需要被信任的证书授权中心（ CA ）签发的安全证书。而一般的 SSL 安全证书签发服务都比较贵，比如 Godaddy 、 GlobalSign 等机构签发的证书一般都需要20美金一年甚至更贵，不过为了加快推广 https 的普及， EEF 电子前哨基金会、 Mozilla 基金会和美国密歇根大学成立了一个公益组织叫 ISRG （ Internet Security Research Group ），这个组织从 2015 年开始推出了 Let’s Encrypt 免费证书。这个免费证书不仅免费，而且还相当好用，所以我们就可以利用 Let’s Encrypt 提供的免费证书部署 https 了。那么怎么获得 Let’s Encrypt 安全证书，并且将它部署在自己的网站服务器上呢？接下来进行详细介绍。

♦ Let’s Encrypt 及 Certbot 简介 前面已经介绍过， Let’s Encrypt 是 一个叫 ISRG （ Internet Security

Research Group ， 互联网安全研究小组）的组织推出的免费安全证书计划。参与这个计划的组织和公司可以说是互联网顶顶重要的先驱，除了前文提到的三个牛气哄哄的发起单位外，后来又有思科（全球网络设备制造商执牛耳者）、 Akamai 加入，甚至连 Linux 基金会也加入了合作，这些大牌组织的加入保证了这个项目的可信度和可持续性。

后来 ISRG 的发起者 EFF （电子前哨基金会）为 Let's Encrypt 项目发布了一个官方的客户端 Certbot ，利用它可以完全自动化的获取、部署和更新安全证书。这真是非常容易、方便呀，所以我们就可以直接使用官方客户端，不需要再使用第三方的工具了。虽然第三方工具也可以使用，但是官方工具更权威，风险也更小，而且遇到问题也更容易解决，毕竟有官方的支持。何况 Certbot 确实非常方便，也比所有的第三方工具都更方便，何乐而不用呢?

♦官方客户端 Certbot 使用方法 Certbot 的官方网站是 https://certbot.eff.org/ ，打开这个链接选择自己使用的 web server 和操作系统，EFF 官方会给出详细的使用方法，如下图，不过我觉得这样还是太复杂，太麻烦，所以建议读者朋友可以不用看这个网站，按照我的方法走一遍即可。以下以网站（ bitop.io ）举例。

配置

> 当前工作目录为root

1.获取certbot客户端

```
wget https://dl.eff.org/certbot-auto
chmod a+x certbot-auto
```

2.停止nginx

```
service nginx stop
```

> 注意:在生成证书前要将web服务器nginx或者apache关闭，否certbot一旦检测到80和443端口被占用，将会报错，无法生成证书。

3.生成证书(如果后期生成报错,先删除原有certbot-auto,按第一步重新下载certbot即可)

```
#使用-d追加多个域名
./certbot-auto certonly --standalone --email support@bitop.io --agree-tos -d bitop
.io -d www.bitop.io
 在证书生成之后，我们会在 “/etc/letsencrypt/live/dgtlinux.xin/” 域名目录下有4个文件就是生成的密钥证书文件。

cert.pem  - Apache服务器端证书
chain.pem  - Apache根证书和中继证书
fullchain.pem  - Nginx所需要ssl_certificate文件
privkey.pem - 安全证书KEY文件
```

4.查看生成的证书

```
ls /etc/letsencrypt/live/bitop.io/
```

5.在nginx中配置证书

```
 ssl on;
 ssl_certificate      /etc/letsencrypt/live/bitop.io/fullchain.pem;
 ssl_certificate_key  /etc/letsencrypt/live/bitop.io/privkey.pem;
 ssl_session_timeout 5m;
 ssl_protocols TLSv1;
 ssl_ciphers HIGH:!RC4:!MD5:!aNULL:!eNULL:!NULL:!DH:!EDH:!EXP:+MEDIUM;
 ssl_prefer_server_ciphers on;
```

apache中配置证书

```
vim /etc/httpd/conf/httpd.conf
SSLCertificateFile /etc/letsencrypt/live/bitop.io/cert.pem;
SSLCertificateKeyFile /etc/letsencrypt/live/bitop.io/chain.pem;
```

6.启动nginx

```
service nginx start
```

编写更新脚本renew-cert.sh

```
#!/bin/bash
# 停止nginx
service nginx stop

# 续签
# --force-renew 强制更新
/root/certbot-auto renew --force-renew

# 启动nginx
service nginx start
```

> Let’s Encrypt 生成的免费证书为3个月时间，但是我们可以无限次续签证书