> 技术要点：HTTPS、Certbot

前言

Nginx 部署完毕可通过 http://yangzw.vip 访问自己的个人官网。打开个人官网，有强迫症的同学可能很快会注意到浏览器地址栏左边显示一个不安全的标记。

HTTP报文 以明文形式传输，若网站只支持 HTTP协议 ，就有可能遭受到安全攻击。使用 Chrome 打开 HTTP协议 的个人官网，自然就会在浏览器地址栏左边显示该标记。若不加以处理，轻则挂满垃圾广告，重则被不法分子盗用。本章将带领你**不花一分钱部署HTTPS证书**，把自己域名中所有网站升级为 HTTPS协议 ，通过 HTTPS 为 HTTP报文 提供一个加密传输通道，这样攻击者就无法窃听或篡改传输内容了。

背景：有免费HTTPS证书却不用

要启用 HTTPS ，必须向一个可信任机构申请一个 HTTPS证书 。发现很多公司都会寻求阿里云、腾讯云、百度云、华为云等第三方平台提供免费或付费的 HTTPS证书 ，像阿里云会提供一年的免费的 HTTPS证书 ，但一年有何用，又不是一直免费，到期续费还要 2000 多一年，要你有何用?

专业的 HTTPS证书 申请需收费，不过对于个人官网来说可用免费的 HTTPS证书 ，推荐一个免费好用的 HTTPS证书 服务商Letsencrypt。

Letsencrypt作为一个公共且提供免费 SSL 的项目逐渐被广大用户传播与使用。它由 Mozilla 、 Cisco 、 Akamai 、 IdenTrust 、 EFF 等组织发起，主要目的是为了推进网站从 HTTP 向 HTTPS 过渡的进程，目前已有越来越多的商家加入与赞助支持。相信在未来，所有 HTTPS证书 都能让你白嫖。

Letsencrypt 不仅提供免费的 HTTPS证书 申请服务且申请过程很简单，关键是能与第7章学习的 Nginx 完美契合，可谓一劳永逸。

方案：不花一分钱部署HTTPS证书

Letsencrypt 提供一个称为 certbot 的工具，它可快速生成或刷新 HTTPS证书 。不过 CentOS8 的 yum 中未包括 certbot源 ，所以无法使用 yum 安装。当然可用 dnf 代替 yum 安装 certbot ， CentOS8 已内置 dnf ，它也是一个**Shell软件包管理器**。

安装

打开 CMD工具 ，登录服务器。执行 dnf --version ，输出版本表示软件可用。通过以下方式安装 certbot 。

> 增加epel源

```
dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

> 更新dnf仓库

```
dnf upgrade
```

> 安装snap

certbot官网也推荐使用 snap 安装 certbot 。

```
dnf install snapd -y
```

> 设置开机自启

```
systemctl enable --now snapd.socket
```

> 设置软链接

可通过 snapd 快速调用命令。

```
ln -s /var/lib/snapd/snap /snap
```

> 更新快照

```
snap install core
snap refresh core
```

> 安装certbot

因为文件体积较大，安装有点慢，请耐心等待。

```
snap install --classic certbot
```

> 设置软链接

可通过 `certbot` 快速调用命令。

```
ln -s /snap/bin/certbot /usr/bin/certbot
```

相比 `CentOS7` ， `CentOS8` 安装 `certbot` 复杂很多，一定要根据上述命令逐条执行完毕。若安装失败，请从第一步重新开始。

配置

`certbot` 安装完毕执行 `certbot --version` ，输出版本表示安装成功。

执行 `certbot --nginx` 扫描 `Nginx` 所有配置，输出以下信息。

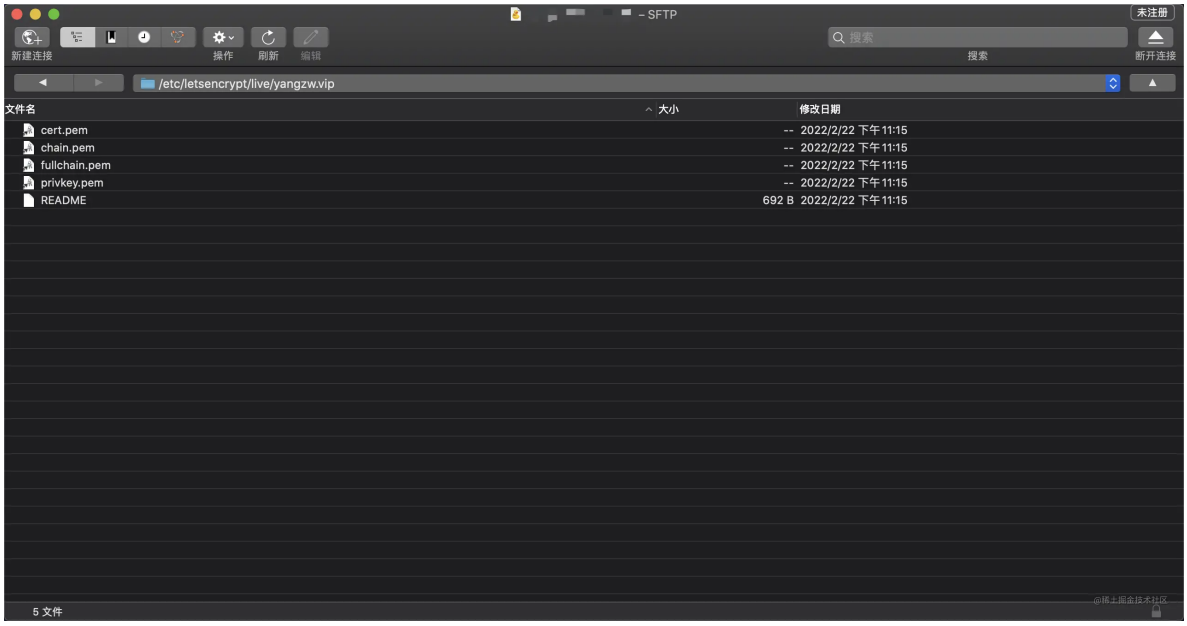
```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
 (Enter 'c' to cancel): young.joway@aliyun.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

```
(Y)es/(N)o: y

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(Y)es/(N)o: n
Account registered.

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: yangzw.vip
2: www.yangzw.vip
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 1,2
Requesting a certificate for yangzw.vip and www.yangzw.vip

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/yangzw.vip/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/yangzw.vip/privkey.pem
This certificate expires on 2022-05-23.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the backg

Deploying certificate
Successfully deployed certificate for yangzw.vip to /etc/nginx/conf.d/yangzw.vip.conf
Successfully deployed certificate for www.yangzw.vip to /etc/nginx/conf.d/yangzw.vip.cor
Congratulations! You have successfully enabled HTTPS on https://yangzw.vip and https://w
```

翻译上述英文，跟随我填写。

- 输入电子邮箱：输入 邮箱 ，用于 紧急续签 与 安全通知
- 是否同意服务条款：输入 y 同意
- 是否接受新闻邮件：输入 n 不同意
- 注册账户成功：自动处理，请耐心等待
- 选择需激活 HTTPS协议 的域名：根据列表输入 数字 ，以 空格 或 英文逗号 分隔
- 申请证书服务：自动处理，请耐心等待

HTTPS证书 最终生成到 /etc/letsencrypt/live/yangzw.vip 目录中。打开 FTP工具 ，进入到该目录，以下文件就是通过 certbot 自动签发的 HTTPS证书 。



HTTPS证书 的有效期为三个月，三个月后不续签就会自动失效。因为 certbot 已设置开机自启，所以 certbot 会一直在后台运行，这些文件将在 HTTPS证书 续订时自动更新，以达到一直免费使用的效果。

解读：Nginx配置文件改动哪些内容

签发 HTTPS证书 会自动修改对应 Nginx配置文件 。看看 certbot 对 Nginx 的配置文件做了哪些改动。还记得第7章个人官网的 yangzw.vip.conf 的内容吗?

```
server {
        listen 80;
        server_name yangzw.vip www.yangzw.vip;
        location / {
                root /www/client/yangzw;
                index index.html;
        }
}
```

执行 vim /etc/nginx/conf.d/yangzw.vip.conf ，发现变成以下内容。凡是后方有这段注释 # managed by Certbot 的代码都是由 certbot 生成。

```
server {
        server_name yangzw.vip www.yangzw.vip;
        location / {
                root /www/client/yangzw;
                index index.html;
        }
        listen 443 ssl; # managed by Certbot
```

```
        include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
        ssl_certificate /etc/letsencrypt/live/yangzw.vip/fullchain.pem; # managed by Cer
        ssl_certificate_key /etc/letsencrypt/live/yangzw.vip/privkey.pem; # managed by C
        ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}
server {
        if ($host = www.yangzw.vip) {
                return 301 https://$host$request_uri;
        } # managed by Certbot
        if ($host = yangzw.vip) {
                return 301 https://$host$request_uri;
        } # managed by Certbot
        listen 80;
        server_name yangzw.vip www.yangzw.vip;
        return 404; # managed by Certbot
}
```

修改端口

端口从原来的 80 改成 443 并从第一个 server块 移动到第二个 server块 中，第二个 server块 也是由 certbot 生成。

导入证书

加入以下核心代码，告知 Nginx 要使用 HTTPS协议 ，通过绝对路径导入 证书文件 。这些文件在上述已通过 FTP工具 展示出来了。

```
ssl_certificate /etc/letsencrypt/live/yangzw.vip/fullchain.pem;
ssl_certificate_key /etc/letsencrypt/live/yangzw.vip/privkey.pem;
```

重定向

加入两个 `if ($host = xyz) {}` 的判断，当使用非 HTTPS协议 访问域名时，直接 301 重定向到 `https://$host$request_uri` 。若出现其他情况则 404 。

---

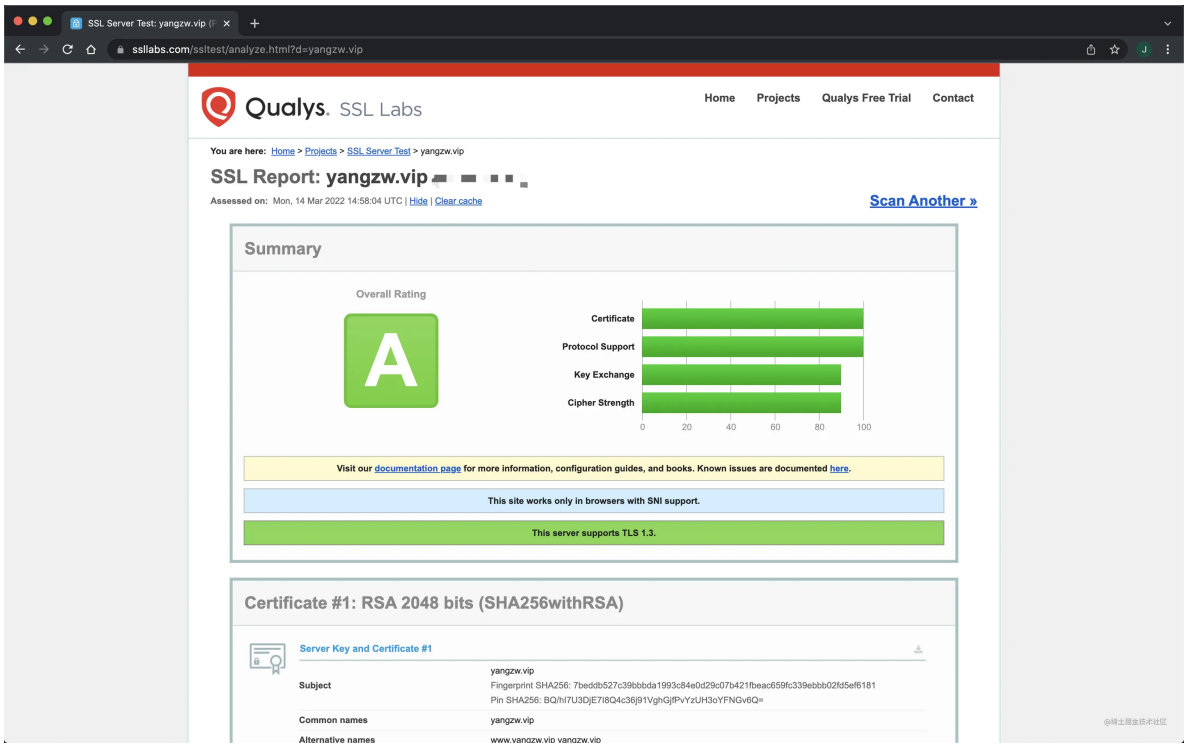
certbot 会根据选择的域名自动匹配出对应 Nginx配置文件 并对其做上述三部分改动，所以每次增加一个网站都需单独创建 xyz.yangzw.conf 文件到 conf.d 文件夹

中，目的是为了隔离每个网站的 Nginx配置 。

在浏览器地址栏中输入 https://yangzw.vip ，发现网页 404 。每次新开端口都需在服务器中配置安全组，可回看第7章的 个人官网-安全组配置 。这次增加 443 端口，在安全组中配置一个 443 端口。再次输入 https://yangzw.vip 就可正常访问了。

在浏览器地址栏中输入 http://yangzw.vip ，发现其重定向到 https://yangzw.vip ，后续所有网站都可通过该方案升级为 HTTPS协议 的网站了。

打开SslTest或SslChecker，输入域名就可检查证书是否有效。



总结

得益于 certbot 才能无限期使用免费的 HTTPS证书 ，更应响应号召，通过上述方案把所有 HTTP协议 网站升级 HTTPS协议 网站。当然也不要再花钱购买那些厂商的 HTTPS证书 了，简直是亏大发。

其实 Nginx 的功能很强大，后续章节会继续结合其他应用场景聊聊 Nginx 在实际开发中的应用。

本章内容到此为止，希望能对你有所启发，欢迎你把自己的学习心得打到评论区！

- [x] 示例项目：fe-engineering
- [x] 正式项目：bruce

留言

输入评论（Enter换行，Ctrl + Enter发送）

发表评论

全部评论（5）

C-ra-ZY JY.3 2月前

snapd安装遇到好多坑,大佬能不能给个装好的docker镜像

点赞 回复

努力的矿工 LV.3 JY.4 web前端工程师 2月前

老厉害了!!

点赞 回复

NewName LV.4 JY.5 前端CV 2月前

安装snapd 不好使，根据命令行提示 使用 dnf install snapd -y --nobest 好使

点赞 回复

王star丶 JY.5 前端小菜鸡 2月前

点赞 回复

Damon 风 LV.2 JY.3 3月前

厉害哦

1 回复