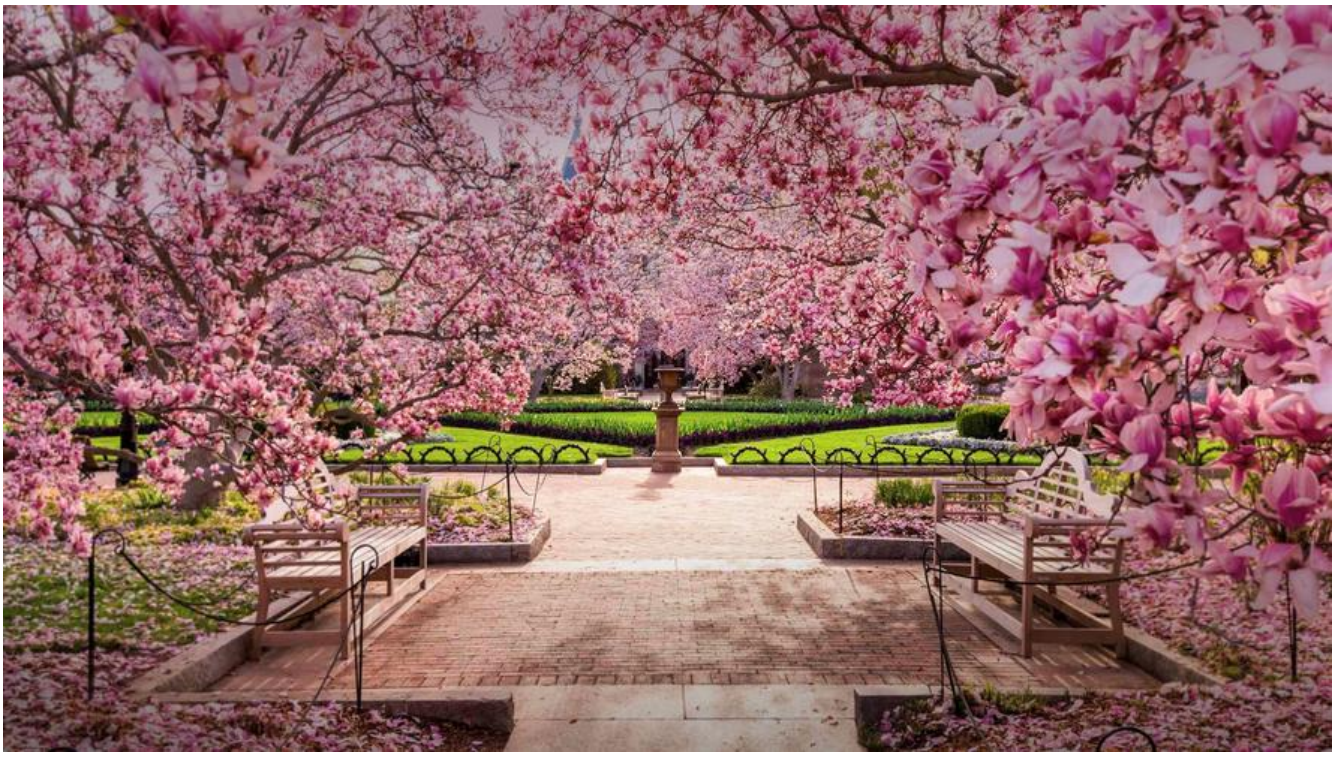
# Nginx 配置 Https 反向代理

作者：someone33881
原文链接：https://ld246.com/article/1544347718158
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)



    本文主要是记录配置ng
nx反向代理https过程中的一些记录！

一、Nginx添加SSL模块

nginx默认缺少SSL模块支持，需要手动编译安装！由于本文之前已经编译安装过nginx，因此本文将在原有基础之上编译安装添加SSL模块

```
cd /root/app/nginx-1.14.0
/usr/local/nginx/sbin/nginx -V  #查看nginx旧的编译参数
./configure [.....旧的编译参数仍然保持不变] --prefix=/usr/local/nginx --with-http_ssl_module
在原有旧的编译参数基础之上添加新的模块--with-http_ssl_module
make  #注意：千万不能执行make install，否则原来nginx的一堆配置文件将被覆盖
cp /usr/local/nginx/sbin/nginx ~/   #备份原来的nginx可执行程序
cp objs/nginx /usr/local/nginx/sbin/  #将新编译的nginx可执行程序objs/nginx复制覆盖原nginx
行程序
#覆盖之后，重新启动nginx即为新的nginx
```

二、免费获取SSL证书

```
#https://freessl.cn/  #注册freessl账号
#输入域名以及域名注册的邮箱地址，生成SSL证书
#到域名所在服务商位置，设置TXT解析以进行域名验证，如下
```


#在freessl控制台进行域名验证，验证通过之后可以下载证书压缩文件解压之后传输到nginx所在服务上（full_chain.pem和private.key两个文件）

三、配置nginx

vim /usr/local/nginx/conf/nginx.conf

```
#修改配置付下
server {
    listen 80;
    server_name caizhaoke.cn,www.caizhaoke.cn;
    rewrite ^(.*)$ https://www.caizhaoke.cn;
}
server {
    listen 443 ssl;
    server_name caizhaoke.cn,www.caizhaoke.cn;
    ssl on;
    #SSL-START SSL相关配置，请勿删除或修改下一行带注释的404规则
    ssl_certificate /root/data/cert/full_chain.pem;
    ssl_certificate_key /root/data/cert/private.key;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;
    ssl_prefer_server_ciphers on;
    ssl_session_timeout 10m;
    #SSL-END
```

原文链接：Nginx 配置 Https 反向代理

```
    index index.jsp index.html;

    location / {
        add_header Content-Security-Policy upgrade-insecure-requests; # for 解决 https 之后静
资源http mixed content问题

        proxy_pass http://pipe$request_uri;
        proxy_set_header Host $host:$server_port;
        proxy_set_header X-Real-IP $remote_addr;
        client_max_body_size 10m;
    }
}

/usr/local/nginx/sbin/nginx -t #检测nginx配置文件是否有错误
/usr/local/nginx/sbin/nginx -s reload #重启nginx

#保证服务器以及云服务商的防火墙开启443端口之后，浏览器中访问https即可验证成功
```