[Nginx 配置SSL实现HTTPS访问（Windows）](https://www.cnblogs.com/yuan-liu/p/16540934.html" \o "发布于 2022-08-01 17:14)

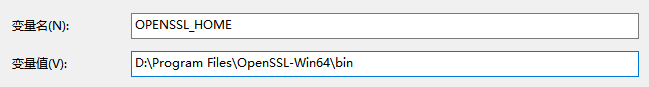
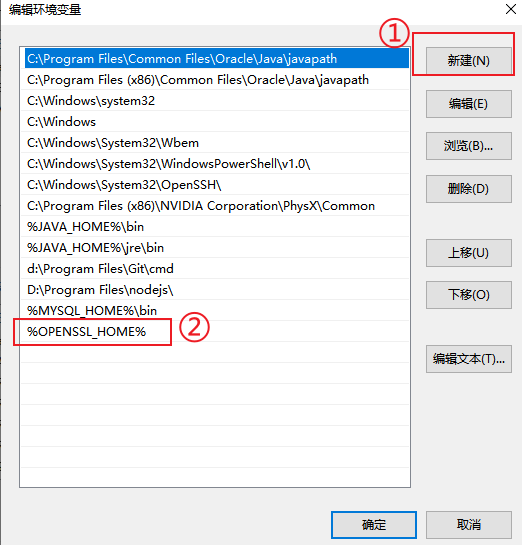
**windows**

**环境装备**

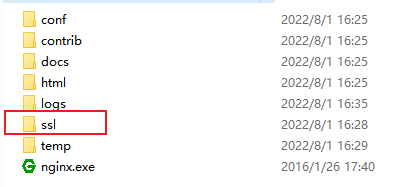
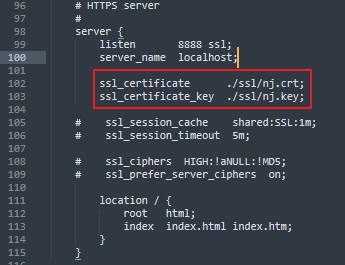
openSSL 需要安装并配置环境变量  
nginx 下载解压即可

* 官网地址
  + openSSL: [http://slproweb.com/products/Win32OpenSSL.html](http://slproweb.com/products/Win32OpenSSL.html" \t "_blank)
  + nginx: <http://nginx.org/en/download.html>
* 阿里云盘
  + openSSL: <https://www.aliyundrive.com/s/1Ru1WAjwK3e>
  + 

**openSSL 环境变量配置**

* 新增系统变量：变量名 OPENSSL\_HOME 变量值 D:\Program Files\OpenSSL-Win64\bin(以自己实际安装路径为准)  
  
* 在path变量内新增内容 %OPENSSL\_HOME%  
  

**nginx 配置**

* 在nginx安装目录下创建文件夹 ssl  
  
* 在 ssl 文件夹下执行命令行操作
* 本文详细介绍了如何生成和使用X509证书，包括私钥key、证书请求文件csr和证书crt的生成步骤。通过openssl命令行工具，演示了从创建RSA私钥到生成自签名SSL证书的全过程，涉及des3加密算法和证书有效期设置。此外，还解释了CSR文件中各项信息的重要性，尤其是commonname与域名的匹配对于HTTPS申请的必要性。
* x509证书一般会用到三类文，key，csr，crt。
* Key是私用密钥openssl格，通常是rsa算法。
* Csr是证书请求文件，用于申请证书。在制作csr文件的时，必须使用自己的私钥来签署申，还可以设定一个密钥。
* crt是CA认证后的证书文，（windows下面的，其实是crt），签署人用自己的key给你签署的凭证。
* 1.key的生成
* **openssl genrsa -des3 -out server.key 2048**
* 这样是生成rsa私钥，des3算法，openssl格式，2048位强度。server.key是密钥文件名。为了生成这样的密钥，需要一个至少四位的密码。可以通过以下方法生成没有密码的key:
* openssl rsa -in server.key -out server.key
* server.key就是没有密码的版本了。
* 2.生成CA的crt
* **openssl req -new -x509 -key server.key -out ca.crt -days 3650**
* 生成的ca.crt文件是用来签署下面的server.csr文件。
* 3. csr的生成方法
* **openssl req -new -key server.key -out server.csr**
* 需要依次输入国家，地区，组织，email。最重要的是有一个common name，可以写你的名字或者域名。如果为了https申请，这个必须和域名吻合，否则会引发浏览器警报。生成的csr文件交给CA签名后形成服务端自己的证书。
* 4. crt生成方法
* CSR文件必须有CA的签名才可形成证书，可将此文件发送到verisign等地方由它验证，要交一大笔钱，何不自己做CA呢。
* **openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey server.key -CAcreateserial -out server.crt**
* 输入key的密钥后，完成证书生成。-CA选项指明用于被签名的csr证书，-CAkey选项指明用于签名的密钥，-CAserial指明序列号文件，而-CAcreateserial指明文件不存在时自动生成。
* 最后生成了私用密钥：server.key和自己认证的SSL证书：server.crt
  1. 证书路径最好采用相对路径  
     

**最终结果**



**linux**

本文主要介绍的是项目如何部署成https访问，当然前提是你们服务器使用的是nginx进行代理的。

**1.去腾讯云或阿里云申请ssl证书**

**2.当签发了证书之后下载证书，**

我使用的是nginx，所以这里下载的是nginx证书,如图：

**3.查看nginx是否安装了with-http\_ssl\_module**

进入到你的nginx安装目录下面，我的目录是在（/usr/local/nginx），进入到目录的sbin目录下，输入

#注意这里是大写的V，小写的只显示版本号

./nginx -V

如果出现 (configure arguments: --with-http\_ssl\_module), 则已安装。

一般情况下都是不存在ssl模块的，接下来进入到你的解压缩后的nginx目录，注意这里不是nginx安装目录，是解压缩后的目录，我的是在（/usr/local/nginx-1.14.2），进入目录后，输入

./configure --prefix=/usr/local/nginx --with-http\_stub\_status\_module --with-http\_ssl\_module

接下来执行make,切记不要执行make install，否则会重新安装nginx

make

上述操作执行完成以后，你的目录下会出现objs文件夹，文件夹内存在nginx文件，如图：

接下来使用新的nginx文件替换掉之前安装目录sbin下的nginx，注意这里的替换的时候可以先将之前的文件备份下，停掉nginx服务

./nginx -s stop #停止nginx服务

#替换之前的nginx

cp /usr/local/nginx-1.14.2/objs/nginx /usr/local/nginx/sbin

成功之后，进入到nginx安装目录下，查看ssl是否成功

#注意这里是大写的V，小写的只显示版本号

./nginx -V

#可以看到这里出现了configure arguments: --with-http\_ssl\_module 证明已经安装成功

**4.配置ssl证书**

将下载的证书解压上传至服务器，（只需pem文件和key文件），我将它放在nginx目录下，创建cert文件夹

mkdir cert

**5.修改nginx.conf配置**

解释

server {

listen 443 ssl;

#你的域名

server\_name xxx.com;

#上传的证书

ssl\_certificate ../cert/xxxx.pem;

ssl\_certificate\_key ../cert/xxxx.key;

ssl\_session\_cache shared:SSL:1m;

ssl\_session\_timeout 5m;

ssl\_ciphers HIGH:!aNULL:!MD5;

ssl\_prefer\_server\_ciphers on;

location / {

root /usr/local/blog/vue-blog/https/dist;

index index.html index.htm;

try\_files $uri $uri/ /index.html;

}

location /shiyi{

proxy\_pass http://127.0.0.1:8800/shiyi;

proxy\_set\_header Host $host;

proxy\_set\_header X-Real-IP $remote\_addr;

proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

proxy\_http\_version 1.1;

proxy\_read\_timeout 3600s;

proxy\_set\_header Upgrade $http\_upgrade;

proxy\_set\_header Connection "upgrade";

}

location /admin{

alias /usr/local/blog/admin-blog/dist;

index index.html index.htm;

try\_files $uri $uri/ /index.html ;

}

error\_page 404 /404.html;

location = /404.html {

}

error\_page 500 502 503 504 /50x.html;

location = /50x.html {

}

}

server {

listen 80;

server\_name xxx.com;

#将请求转成https

rewrite ^(.\*)$ https://$host$1 permanent;

}

**6.重启nginx**

./nginx -s reload

然后就可以通过https访问你的网站了，如果能够正常访问则说明配置成功，当然如使用了七牛云对象存储等第三方的就需要也去配置七牛云的https，否则就会出现https访问http的错误异常。