SSL证书更换

由于存在一定风险，请提前备份/usr/local/nginx/conf/nginx.conf，确认网站上没有重要的作业，且需要预先了解以下知识：

1. Nginx软件的常规操作；
2. centos系统基本操作；
3. 目前服务器的项目设置。

过程中出现任何问题，请联系陆昊宇，电话：13701415667，微信：luyu103713

用户https安全访问我们网站需要证书，考虑到经济性和我们网站的安全性，一般采用单域名SSL证书。

1 证书的申请

**免费申请：**

**腾讯云**，

登录并进入申请页面

<https://console.cloud.tencent.com/ssl>

目前教育网域名很难通过赛门铁克的安全验证，因此申请到概率不大，可以尝试几次，建议采用手动文件验证方式。在我们网站根目录（/home/web/public/htdocs/）下根据网站提示创建指定文件夹放入验证文件，修改ngnix设置如下：

*location ~ .well-known { #.well-known是验证的指定文件夹*

*allow all;*

*}*

一般一个工作日左右会验证结果，并把证书放在你的腾讯云里。

**购买证书（推荐方式）：**

1. 在腾讯云、阿里云等购买，2019年报价 约1500/年。
2. 淘宝购买，搜索“ssl证书注册”
3. 如果http可以访问我们网站，15元/年
4. 如果学校只开放https端口，需要购买企业级证书，50元-100元/年

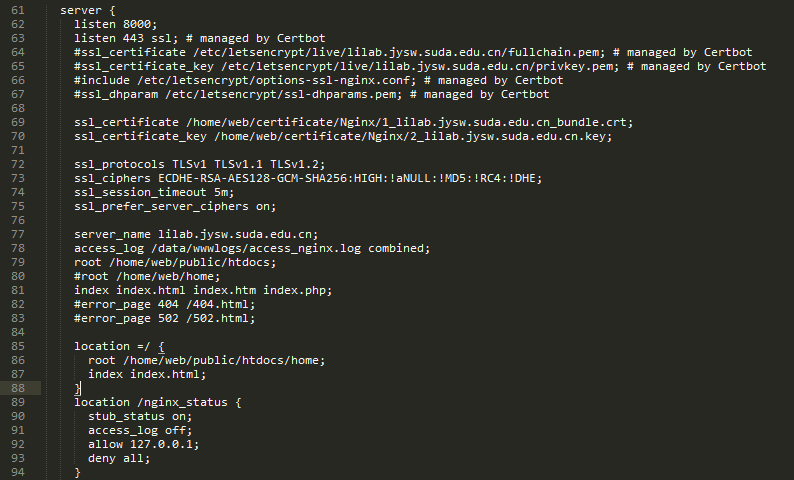
2020年的证书购买链接：（淘宝）

<https://shop266673846.taobao.com/shop/view_shop.htm?shop_id=266673846>

**证书验证：（验证域名的所有权利、需要root账户）**

1. 切换root打开nginx配置文件

**$***vi /usr/local/nginx/conf/nginx.conf*



88行光标位置后加入

*location ~ .well-known { #.well-known是验证的指定文件夹*

*allow all;*

*}*

保存后重启nginx：

**$***nginx -s quit*

**$***nginx -c /usr/local/nginx/conf/nginx.conf*

1. 在网站根目录*/home/web/public/htdocs/* 下创建验证用文件夹，放入验证文件，提醒卖家开始验证。并且要求卖家提供配置nginx/Apache/IIS三种web服务器的证书。验证成功后，会收到以下文件。Apache 
   [긺 Nginx 
   2020/1 /12 1425 
   2020/1 /12 1425 
   2020/1 /12 1425 
   호4수矣 
   호4수矣 
   호4수矣 

lilab-jysw-suda-edu-cn 
CAChai ns.crt 
lilab-jysw-suda-edu-cn.crt 
lilab-jysw-suda-edu-cn.key 
Apache 
2020/1/12 14:25 
2020/1/12 14:25 
2020/1/12 14:25 
Apac 
-*-e-iF 
KEY 

lilab-jysw-suda-edu-cn Nginx 
lilab-jysw-suda-edu-cn.key 
lilab-jysw-suda-edu-cn.pem 
2020/1/12 14:25 
2020/1/12 14:25 
KEY 
PEVI 
7 KB 

lilab-jysw-suda-edu-cn 
CAChains.crt 
lilab-jysw-suda-edu-cn.pfx 
2020/1/12 14:25 
2020/1/12 14:25 
Personal Inform... 

1. Window环境下可以双击打开.crt证书，确认红框内网站的域名和日期无误后，将之前设置的nginx配置删除：

**$***vi /usr/local/nginx/conf/nginx.conf*

删除以下行：

*location ~ .well-known {*

*allow all;*

*}*

保存后重启nginx，开始配置证书。



2 证书的配置

**a.**本地设置：

登录172切换root权限，把nginx证书上传到172服务器，

*/home/web/certificate/Nginx*  （我们2018年以来的证书备份也都在这里）

然后打开nginx配置文件

**$***vi /usr/local/nginx/conf/nginx.conf*

default 
server { 
listen 8øøø; 
listen 443 SSI; # managed by Certbot 
/etc/letsencrypt/live/lilab.jysw.suda.edu.cn/fullchain.pem; # managed by Certbot 
/etc/letsencrypt/live/lilab.jysw.suda.edu.cn/privkey.pem; # managed by Certbot 
#include / etc/ letsencrypt/options-ssl-nginx. conf; # managed by Certbot 
/etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot 
SSI 
SSI 
SSI 
SSI 
SSI 
SSI 
_ certificate 
_ certificate_key /home/web/certificate/Nginx/2_IiIab.jysw.suda.edu.cn.key; 
_ protocols TLSv1 TLSv1.1 TLSv1.2; 
_ ciphers ECDHE-RSA-AES128-Gcm-SHA256:HIGH 
session timeout 5m; 
_ on; 
: ! aNULL: !DHE; 

在红框位置

ssl\_certificate 后输入证书.crt或者.pem文件的路径

ssl\_certificate\_key 后输入证书.key文件路径

保存后重启nginx：

**$***nginx -s quit*

**$***nginx -c /usr/local/nginx/conf/nginx.conf*

b.学校对外服务器证书替换

由于我们使用的是学校内网，目前已经不再能对外网开放端口，需要写信给学校信息管理中心（80000@suda.edu.cn），让他们帮我们在学校服务器替换我们网站的证书，邮件模板如下：

 #################################################

收件人 :"80000"<80000@suda.edu.cn>;

主题：实验室网站证书需要更新

老师您好！

      我是我们学校医学部基础医学与生物科学学院的研究生###，学号：######，联系电话：########，我们实验室的网站 ：<https://lilab.jysw.suda.edu.cn/> 由于之前申请的SSL证书即将过期，需要替换，我已经申请好了新的证书，目前在实验室服务器的nginx端配置好了，请技术老师在学校服务器上替换下证书，需要的证书文件已经打包在附件，谢谢。

  #################################################

然后将所有证书打包放在附件内发送，一般发送后会有一个受理回信，很快可以替换好，如果进度比较慢，可以拨打65880000（校内短号80000）咨询。

等学校服务器替换后，清理浏览器缓存，查看证书替换是否完成。



如果浏览器没有安全提示，有安全标志，表明替换顺利完成。