

SSL证书更换最终版

2020年1月13日 8:59

网站https访问需要证书才能安全访问，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（购买）

★ 免费申请途径：

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nginx设置如下：

```
location ~ .well-known {    #.well-known是验证的指定文件夹
    allow all;
}
```

如果是新注册帐号，验证期间腾讯的客服很有可能会给你打电话咨询你的用途和网站规模等，建议表现得我们很有可能使用他们的产品，增加授权通过概率。

一般一个工作日左右会验证结果，（如果通过）并把证书放在你的腾讯云里。

Certbot

172已经安装了Certbot，建议使用手动模式获取证书，需要我们网站能够http访问（联系信息处），但是证书时常只有三个月，不推荐。

★ 购买证书（推荐）

大厂的一般比较贵，1500元年以上，建议淘宝搜索ssl证书注册，如果http可以访问验证我们网站，15元/年左右，如果学校还是只开放https端口，需要购买企业级证书，50元-100元/年。

2020-2021年的证书在这里购买的：（淘宝）

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

验证方式也是

设置nginx

```
location ~ .well-known {    #.well-known是验证的指定文件夹
    allow all;
}
```

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

一般是




/home/web/public/htdocs/.well-known/pki-validation/




或者



/home/web/public/htdocs/.well-known/acme-challenge/

下面放入指定文件，通过验证后，店家会把证书打包后邮件发给你。

特别提醒店家，说需要nginx/Apache/IIS都配置（因为学校可能用到），一般的，会得到一下文件

	Apache	2020/1/12 14:25	文件夹	
	IIS	2020/1/12 14:25	文件夹	
	Nginx	2020/1/12 14:25	文件夹	

电脑 > 下载 > lilab-jysw-suda-edu-cn > Apache				
名称	修改日期	类型	大小	
	CAChains.crt	2020/1/12 14:25	安全证书	5 KB
	lilab-jysw-suda-edu-cn.crt	2020/1/12 14:25	安全证书	3 KB
	lilab-jysw-suda-edu-cn.key	2020/1/12 14:25	KEY 文件	2 KB

电脑 > 下载 > lilab-jysw-suda-edu-cn > Nginx				
名称	修改日期	类型	大小	
	lilab-jysw-suda-edu-cn.key	2020/1/12 14:25	KEY 文件	2 KB
	lilab-jysw-suda-edu-cn.pem	2020/1/12 14:25	PEM 文件	7 KB

电脑 > 下载 > lilab-jysw-suda-edu-cn > IIS				
名称	修改日期	类型	大小	
CAChains.crt	2020/1/12 14:25	安全证书	5 KB	
lilab-jysw-suda-edu-cn.pfx	2020/1/12 14:25	Personal Inform...	5 KB	

2 证书的配置:

a.本地设置:

登录172切换root权限, 把nginx证书上传到服务器, 推荐文件夹:

/home/web/certificate/Nginx (我们从2018年的证书备份也都在这里)

然后打开nginx配置文件

(目前在 /usr/local/nginx/conf/nginx.conf)

```
##### default #####
server {
    listen 8000;
    listen 443 ssl; # managed by Certbot
    #ssl_certificate /etc/letsencrypt/live/lilab.jysw.suda.edu.cn/fullchain.pem; # managed by Certbot
    #ssl_certificate_key /etc/letsencrypt/live/lilab.jysw.suda.edu.cn/privkey.pem; # managed by Certbot
    #include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    #ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

    ssl_certificate /home/web/certificate/Nginx/1_lilab.jysw.suda.edu.cn_bundle.crt;
    ssl_certificate_key /home/web/certificate/Nginx/2_lilab.jysw.suda.edu.cn.key;

    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:HIGH:!aNULL:!MD5:!RC4:!DHE;
    ssl_session_timeout 5m;
    ssl_prefer_server_ciphers on;
}
```

写入替换.crt或者.pem文件路径

这里替换对应的key路径

完成后重启nginx, 如果没有报错就成功了。

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了, 需要写信给学校信息管理中心, 让他们帮我们替换我们网站的证书, 外网访问才能使用新的证书, 推荐的邮件内容:

Send to: "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, 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, 就可以看到证书替换好了。