在软件工程课中配置SSL证书

作者：橘子 邮箱：1372722289@qq.com

1. 什么是SSL证书

在软件工程课中，对项目的安全性没有很高要求。但是只需要几个小步骤，就可以提高自己的网站/APP的安全性。尤其是微信小程序，要求后端服务必须有域名且支持TLS加密。

SSL的全称是Secure socket layer，它是在五层网络抽象（在计算机网络课上会学到）中加了“半层”，将TCP传输进行了加密。1994年，NetScape公司设计了SSL协议，1999年互联网标准化组织ISOC接替了NetScape公司，发布了SSL的升级版TLS。由于历史原因，两个缩写指代的可能都是安全套接字，这里本文就不加区分了。

1.1 SSL证书有什么用？

不妨做一个小实验，打开http://info.tsinghua.edu.cn, 你会发现浏览器在该网址左侧标注了不安全。这是因为信息门户没有使用SSL证书。接着，再打开http://www.baidu.com/，你会发现网址自动做了重定向，指向https://www.baidu.com/， 并且浏览器上改网址左侧有一把小锁（不同浏览器可能显示不同），表示该网站有SSL加密。

简而言之，SSL证书使得网站变得更加安全，其具体实现方法请参考计算机网络课程，本文会教你如何动手为自己的项目配置SSL证书。

1.2 为什么不自己生成SSL证书

SSL的基石是公钥-私钥加密体系。公钥被放在证书中，私钥被服务器保存。为了防止有人篡改证书，公钥又要被CA（Certification Authorities）加密（这都是计算机网络课程的内容）。而我们要做的就是向CA申请一个**免费**的SSL证书，有效期一般是一年。

2. 准备事项

1. 有一台配有公网ip的服务器。

   软工课应该每个人都会发一个，19届用的是腾讯云的。

2. 有域名DNS解析，但是二级域名**不属于**自己。

   由于域名的购买不仅需要经费，而且需要一定周期，软工课不需要同学自己购买域名。19届课上，助教提供二级域名，并且给同学们下发三级域名。

   > 例如，tool.sample.com中，com是一级域名，sample是二级域名，tool是三级域名。tool.sample.com和info.sample.com可以解析出不同ip，分别分配证书。助教购买了域名sample.com之后，可以发配stu1.sample.com, stu2.sample.com, ... 等多个域名给同学们使用，但是分别指向不同ip的服务器，所以需要同学们自己申请证书。

   注： 如果自己购买了域名，可以参照教程《如何合法的、安全的发布自己的网站》中的引导用更便捷的方式获得SSL证书。

3. 本教程使用腾讯云做示例。
4. 会用简单的docker指令。（软工课会讲的，不会也没关系，下文有简要介绍）

3. 申请SSL证书

3.1 简要介绍SSL证书的认证方式

既然SSL证书要由CA验证，那么如何让CA知道你确确实实地拥有该域名呢？有两种常见方式：

1. **文件验证**。CA告诉申请人一串密码字符串，申请人配置服务器的网页服务；接着CA访问该网页，发现能够获取该密码字符串，那么就能确定网站归属权。
2. **DNS验证**。CA告诉申请人一串密码字符串，申请人配置DNS解析；接着CA做DNS解析，发现能够获取该密码字符串，那么就能确定网站归属权。

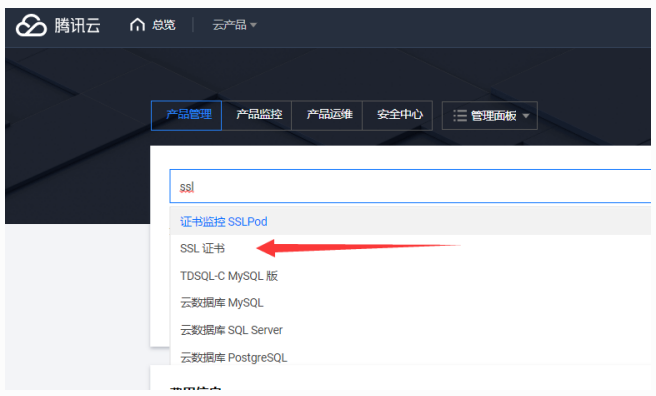
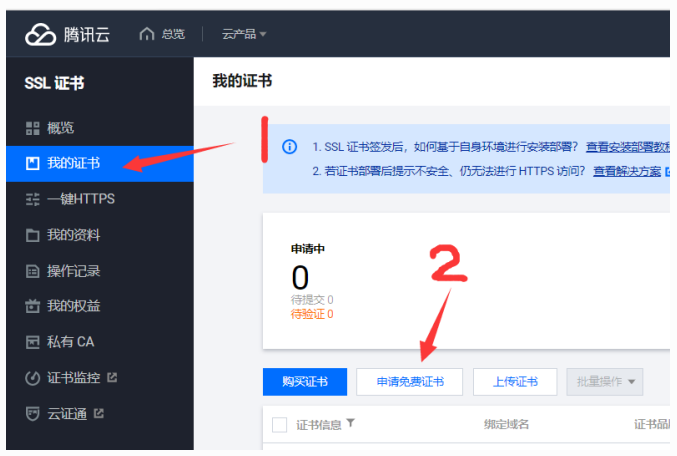
本文采用**第一种**方式，但实际上第二种方式更简单。那为什么用第一种呢？还记得前置条件吗？二级域名**不属于**自己，所以你无法控制DNS解析（或者你联系助教帮你做，就太麻烦助教了吧）。

3.2 具体实现

接下来是具体的申请步骤

3.2.1 在腾讯云申请SSL证书

腾讯云不是CA，但是可以做证书代购。进入网站https://cloud.tencent.com/， **不要**在主页直接搜索“SSL证书”，那里购买页面的整数都非常贵，而我们的目的是免费申请。选择右上角的控制台（图1），接着在控制台中搜索SSL证书（图2）；然后点击申请免费证书（图3），选择一个免费证书。

图1	图2	图3
		

接下来，填写必要的信息，密码留空表示自动生成（图4）。此处域名应该填写完整，比如助教的二级域名是`sample.com`，而你分到的是`tool.sample.com`，就请填写`tool.sample.com`. 验证方式选择**文件验证**（图5）。然后来到了验证界面（图6），把这些信息记录下来。如果忘记了，也可以通过”申请中的SSL证书“入口查看订单。

图4	图5	图6
		

3.2.2 在服务器上部署文件

接下来要把指定的`.txt`文件放在服务器的对应位置。为了部署方便，适配多种服务器机型，这里使用docker部署。

目录结构：

```
|-Dockerfile
|-docker-compose.yml
|-.well-known
   |-pki-validation
       |-fileauth.txt
|-config
   |-nginx
       |-nginx.conf
```

其中`Dockerfile`和`docker-compose.yml`指定了docker容器的构建。

1. `fileauth.txt`中填入图6中的**文件内容**，把`fileauth.txt`的文件名**重命名**为指定的文件名。
2. `Dockerfile`中填入：

```
#指定基础镜像，在其上进行定制
FROM nginx:latest

#复制同级路径下的dist文件夹中的所有文件到容器里
#dist文件为vue打包后上传到服务器的解压包
ADD ./.well-known/pki-validation/ /home/wwwroot/default/auth/.well-known/pki-validation/
#复制nginx配置文件，替换nginx容器中的默认配置
ADD config/nginx/nginx.conf /etc/nginx/conf.d/default.conf
```

3. `docker-compose.yml` 中填入：

```
version: "3.4"
services: #指定服务名称
  front: #前端服务
    container_name: tencent_test
    image: nginx:latest #nginx镜像
    ports: #避免出现端口映射错误，建议采用字符串格式
      - "80:80"
    volumes:
      #挂载nginx配置文件到容器中，替换nginx容器中的默认配置
      - ./config/nginx:/etc/nginx/conf.d
      - ./.well-known/pki-validation/:/home/wwwroot/default/auth/.well-known/pki-validation/
    restart: always
```

4. `nginx.conf` 中填入如下内容，**注意域名替换**：

```
server {
    listen       80;
    server_name  www.example.com; # 填写你的域名

    #charset koi8-r;
    access_log  /var/log/nginx/host.access.log  main;

    location / {
        root   /usr/share/nginx/html;
        # ;index  index.html index.htm;
    }

#http://域名/.well-known/pki-validation/fileauth.txt
    location /.well-known/pki-validation/ {
        root   /home/wwwroot/default/auth/;
        #alias   /home/wwwroot/default/.well-known/pki-validation/;
        index  index.html index.htm;
    }
}
```

5. 运行docker容器。可以在本目录下使用 `docker-compose up` 命令来启动，如果想挂载在后台，则使用 `docker-compose up -d` . 如果想停止，使用 `docker-compose down` .

3.2.3 等待验证完成

回到验证页（图6）点击“查看验证状态”按钮可以刷新验证情况。然后会显示验证成功。

4. 可能遇到的问题与解决情况

1. Q: 我找到的SSL证书需要花钱购买?

   A: 找错地方了！直接搜索SSL证书的话，会进入到购买页面，应该从控制台入口进入，申请免费SSL证书。

2. Q: 今年软工课，助教没有提供域名了，要自己准备?

   A: 请参考另一篇教程《如何合法的、安全的发布自己的网站》

3. Q: 我已经按照步骤完成了配置，但是验证失败了?

A: 在图6中，会显示验证网址。你可以自己在浏览器中打开这个网址，看看内容。如果是网页不可访问，请检查**防火墙80端口是否开启**。如果是`Nginx 502 bad gateway`，请检查`nginx.conf`的配置。如果正常显示出字符串，请检查内容是否正确，文件名称是否修改。

5. 参考

在SSL 证书 文件验证-域名验证-文档中心-腾讯云 (tencent.com)有简单的教程，但是并不详细，而且没有示例代码。

示例代码可以在此处下载：

https://github.com/citrusreticulata/ssl-tencet-auth-sample