**背景：**

当前许多网站系统在访问时，都已支持https安全访问，保障用户数据传输的安全性。

首先，需申请一张SSL证书，将SSL证书部署到服务器端，开启443端口，然后即可实现HTTPS访问。

获取SSL的途径：

1) 到CA机构申请，支持部署跨浏览器的SSL证书。 （安全性好，但要按年收费.）

2）自签名SSL证书。 (使用者需导入证书至各浏览器受信任根目录，安全性稍差，但免费、便捷测试.)

**OpenSSL 简介**

它是一个密码库工具，用于支持传输层安全性（TLS/SSL）协议的实现。 功能也包括了主要的密码算法、常用密钥和证书封装管理等。 安装完成后，会包含openssl 组件，是一个多用途的命令行工具。

openssl的默认安装路径： /usr/local/ssl 查看版本号 : openssl version

**使用流程：** (一键生成key和 证书)

一、首先确保服务器上已安装了OpenSSL，并配置了环境变量。

二、在服务器上任意位置新建一目录，执行如下命令：

openssl req \

-newkey rsa:2048 \

-x509 \

-nodes \

-keyout server.key \

-new \

-out server.crt \

-subj /CN=cpl.weibo.com \

-reqexts SAN \

-extensions SAN \

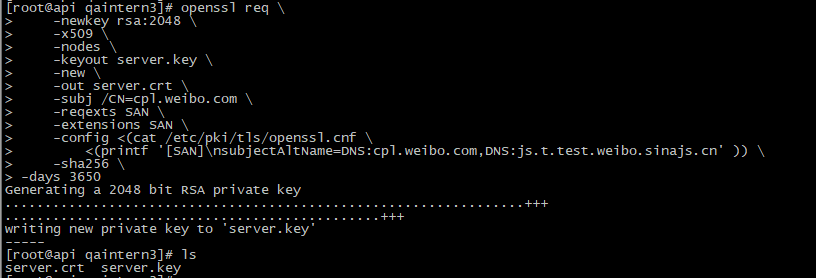
-config <(cat /etc/pki/tls/openssl.cnf \

<(printf '[SAN]\nsubjectAltName=DNS:cpl.weibo.com,DNS:js.t.test.weibo.sinajs.cn' )) \

-sha256 \

-days 3650

运行示例:



目录中生成了 server.crt server.key 两个文件.

key 是**服务器上的私钥文件**，用于对发送给客户端数据的加密，以及对从客户端接收到数据的解密。

crt 是自签名证书， 包含：证书持有人的信息，**持有人的公钥**，以及签署者的签名等信息。

#参数说明

1）openssl req 证书签发请求命令.

2）-newkey rsa:2048 表示自动生成RSA私钥，2048位.

（RSA 是非对称加密算法，使用两套密钥：公钥和私钥.

使用私钥加密的内容，只能通过公钥来解密； 使用公钥加密的内容，只能通过私钥来解密.）

3）-x509 使用本参数，则表示直接输出一个X.509自签名数字安全证书.

4）-nodes 表示私钥不加密，若不带参数将提示设置/输入密码；

5）-keyout server.key 指定 2) 中生成的私钥名称并输出.

6）-new 生成证书的请求.

7）-out server.crt 指定输出证书的名字并输出.

8）-subj /CN=cpl.weibo.com 附加的一些信息，这些信息将会添加到证书里面； CN——申请证书的组织名.

9）-reqexts SAN \ -extensions SAN \ 指定扩展的section名字.

10）-config <(cat /etc/pki/tls/openssl.cnf \ req命令的配置参数文件.

<(printf '[SAN]\nsubjectAltName=DNS:cpl.weibo.com,DNS:js.t.test.weibo.sinajs.cn' ))

在生成证书的【使用者备用域名】中写入备用域名. (可扩展多个DNS域名)

11) -sha256 使用sha256签名hash算法.

12) -days 3650 证书的有效时间， (一般设置为365\*10， 10年)

三. 将生成的证书&服务器私钥 ( .crt .key ) 配置nginx， 同时启动 ssl on; (若前后端工程分离，则需配置2个nginx)

ssl on;

ssl\_certificate /usr/local/adinf/adweb-1.2/ngx\_openresty/1.9.3.2/nginx/conf/ca/https\_cert\_cpl/server.crt;

ssl\_certificate\_key /usr/local/adinf/adweb-1.2/ngx\_openresty/1.9.3.2/nginx/conf/ca/https\_cert\_cpl/server.key;

#配置完成，重启nginx

四. 将 .crt 证书 从服务器 sz下载， 导入到对应浏览器受信任根目录中。

( 关闭浏览器，再打开； https自制签名证书 才生效. )

五. 查看证书信息， 是否是对应的域名/dns.





#六. 若多个机器上搭建有同一套测试环境。 可通过主服务器生成的  **server.key server.crt**， sz下载 —> rz上传至新服务器的某一目录中， 重新配置/重启nginx。 (浏览器中不用再导入证书， 只需导入一次即可.)