## 1.生成crt文件

在Nginx环境下配置ssl首先需要两个文件：通过openssl进行产生：example.key 文件和 example.csr

生成example.csr的命令：

openssl req -new -newkey rsa:2048 -sha256 -nodes -out example\_com.csr -keyout example\_com.key -subj "/C=CN/ST=ShenZhen/L=ShenZhen/O=Example Inc./OU=Web Security/CN=example.com"

C：Country 单位所在国家，为两位数的国家缩写，如： CN 就是中国

ST 字段： State/Province ，单位所在州或省

L 字段： Locality ，单位所在城市 / 或县区

O 字段： Organization ，此网站的单位名称;

OU 字段： Organization Unit，下属部门名称;也常常用于显示其他证书相关信息，如证书类型，证书产品名称或身份验证类型或验证内容等;

CN 字段： Common Name ，网站的域名;

生成 csr 文件后，提供给 CA 机构，签署成功后，就会得到一個 example.crt 证书文件，SSL 证书文件获得后，就可以在 Nginx 配置文件里配置 HTTPS 了。

## 2.复制上传

Crt文件与ssh文件复制到复制/usr/local/nginx/conf/ssl文件夹里面

## 3.nginx.conf

首先在/usr/local/nginx/conf文件夹里面使用vi命令用vi编辑器打开nginx.conf

server {

#ssl参数

listen 443 ssl;

server\_name example.com;

#证书文件

ssl\_certificate example.com.crt;

#私钥文件

ssl\_certificate\_key example.com.key;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_ciphers HIGH:!aNULL:!MD5;

#...

}