检查OpenSSL

检查是否已经安装openssl：

openssl version

一般在CentOS7上，openssl已经默认安装好了。

生成自签名的SSL证书和私钥

第一步：生成私钥

mkdir 创建文件夹

cd 进入文件夹

新建/etc/ssl/certs/目录并进入，后执行命令：

openssl genrsa -des3 -out server.key 2048

输入一个4位以上的密码。

第二步：生成CSR(证书签名请求)

openssl req -new -key server.key -out server.csr -subj "/C=CN/ST=Fujian/L=Fuzhou/O=jiye/OU=jiye/CN=这里填域名或IP地址"

subj参数说明如下：

|  |  |  |
| --- | --- | --- |
| 字段 | 字段含义 | 示例 |
| /C= | Country 国家 | CN |
| /ST= | State or Province 省 | Fujian |
| /L= | Location or City城市 | Fuzhou |
| /O= | Organization 组织或企业 | jiye |
| /OU= | Organization Unit 部门 | jiye |
| /CN= | Common Name 域名或IP | 这里填域名或IP地址 |

第三步：去除私钥中的密码

在第1步创建私钥的过程中，由于必须要指定一个密码。而这个密码会带来一个副作用，那就是在每次启动Web服务器时，都会要求输入密码，

这显然非常不方便。要删除私钥中的密码，操作如下：

openssl rsa -in server.key -out server.key

第四步：生成自签名SSL证书

# -days 证书有效期-天

openssl x509 -req -days 3650 -in server.csr -signkey server.key -out server.crt