中国互联网络信息中心
China Internet Network Information Center

最后更新时间：2010年12月22日

软 件 版 本 号： linux
Nginx0.7稳定版 openssl-0.9.8
ActivePerl-5.12.2 VC++6.0

服务器证书安装配置指南系列之

Nginx 服务器证书安装配置指南

www.cnnic.cn

中国互联网络信息中心(CNNIC)

地址： 北京中关村南四街四号中国科学院软件园1号楼一层
7*24小时客户服务咨询电话：86-10-58813000
传真：86-10-58812666
邮政地址：北京349信箱6分箱 CNNIC
邮政编码：100190

目录

图表目录

1. 应用环境

系统环境：
windows xp sp3 ； Nginx； openssl-0.9.8； Perl-5.12.2； vc++6.0.

证书类型：
可信服务器证书，申请地址：http://www.cnnic.cn/jczyfw/wzws/

2. 关于 openssl

1）openssl 简介

openssl 是一个 Linux/windows 平台下、开放源代码的实现了 SSL 及相关加密技术的软件包。

2）openssl 下载及安装配置

配置 OPENSSL_CONF 的变量环境，值为 openssl 里 apps 目录下的 openssl.cnf 文件。

安装 perl 和 vc6，注册环境变量。

然后运行 cmd 进入到 Openssl 根目录，输入 perl Configure VC-WIN32,回车输入 ms\do_ms,然后 cd 到 microsoft visual studio\vc98\bin 目录下执行 vcvars32.bat,最后回到 openssl 目录下执行 nmake –f ms\ntdll.mak 成功之后在 openssl 安装目录下多了几个文件夹并且文件夹下有相关文件。需要把得到的 out32dll 文件夹路径添加到变量环境 path 里。

以上是配置 openssl。

3. 申请服务器证书

本手册以 m1.cnnic.cn 为例，以下命令请使用 开始-运行-cmd 进入 DOS 环境进行

1）生成私钥

命令格式：**openssl genrsa -des3 -out cnnic.key 2048**

注：[]中的内容为需要输入的参数

- keystore_name：表示证书密钥库的文件名，扩展名一般为 key

如下图所示：

```
E:\openssl\openssl-0.9.8>openssl genrsa -des3 -out m1.cnnic.cn.key 2048 Gener
ng RSA private key, 2048 bit long modulus
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.........................................+++
.....................+++
e is 65537 (0x10001)
Enter pass phrase for m1.cnnic.cn.key:
Verifying - Enter pass phrase for m1.cnnic.cn.key:

E:\openssl\openssl-0.9.8>_
```

图表一 生成密钥命令行

如上图所示，行命令运后会提示输入两次私钥的密码，结果生成 2048 位的 RSA 私钥，私钥文件名为： m1.cnnic.cn.key。

〈注：CNNIC 可信服务器证书要求域名证书密钥对最少为 2048 位〉

2）生成 CSR 证书请求文件

命令格式：**openssl req -new -key ssl.key -out cnnic.csr**

注：[]中的内容为需要输入的参数

- csr_name：表示生成的证书请求文件的文件名

- keystore_name：表示证书密钥库的文件名，扩展名一般为 key

如下图所示：

```
E:\openssl\openssl-0.9.8>openssl req -new -key m1.cnnic.cn.key -out m1.cnnic.
csr
Enter pass phrase for m1.cnnic.cn.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:beijing
Locality Name (eg, city) []:beijing
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cnnic
Organizational Unit Name (eg, section) []:cnnic
Common Name (eg, YOUR name) []:m1.cnnic.cn
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

E:\openssl\openssl-0.9.8>
```

图表二　生成 csr 请求文件

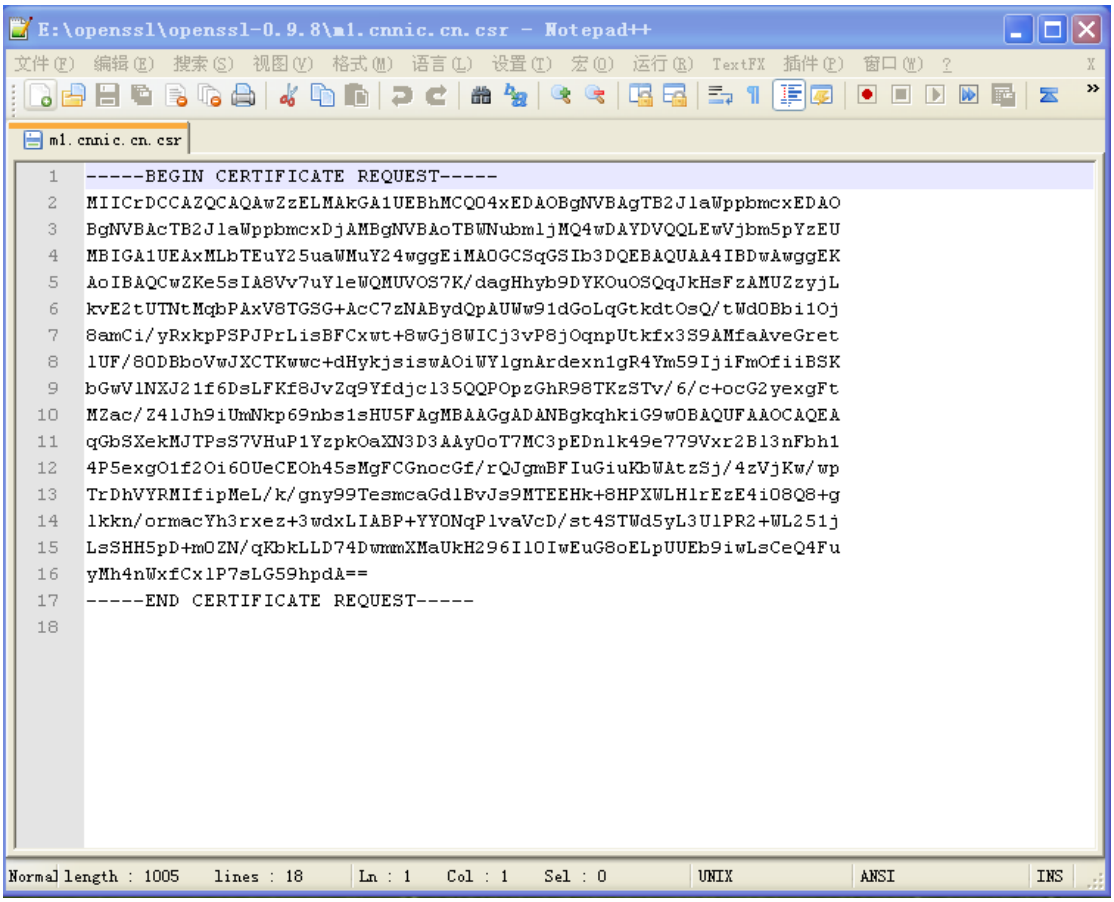
上述命令运行后，系统提示输入第一步骤中输入的私钥密码，然后输入 X.509 证书所要求的字段信息，包括国家(中国添 CN)、省份、所在城市、单位名称、单位部门名称(可以不填直接回车)。请注意： 除国家缩写必须填 CN 外，其余都可以是英文或中文。

Common Name 项请输入您要申请域名证书的域名，例如：如果需要为 www.domain.cn 申请域名证书就必须输入 www.domain.cn 而不能输入 domain.cn。通配域名证书请填写通配域名；多域名证书仅需要填写第一个域名名称即可。

请不要输入 Email、口令(challenge password)和可选的公司名称，直接打回车即可。

现在已经成功生成了私钥文件：m1.cnnic.cn.key 保存在您的服务器中。生成的 csr 文件为文本文件，可以使用记事本等文本查看工具打开刚刚生成的证书

请求文件，如下图所示：



图表三　查看 csr 文件

4. 下载服务器证书

1) 准备下载证书所需信息

参考号与授权码：参考号与授权码是下载证书的密码凭证。当申请的证书通过审核时，用户将接收到由 CNNIC 发送的通过审批的电子邮件通知，该邮件中含有 16 位的参考号与授权码信息，其中参考号与授权码的前 13 位为明文显示，后 3 位为密文显示。审核员会以邮件通知的方式发送后三位的明文显示。

2) 下载证书

登录 CNNIC 可信网络服务中心网页面

http://www.cnnic.cn/jczyfw/wzws/xz/201010/t20101027_16322.html，

点击页面中部的“可信服务器证书下载”链接进入到证书下载页面，如下图所示：

图表四　可信服务器证书下载页面

根据网页上的提示输入“参考号”和“授权码”，将证书请求文件中除去头尾“-----BEGIN NEW CERTIFICATE REQUEST-----”和“-----END NEW CERTIFICATE REQUEST-----”的中间部分内容复制到 CSR 文本框中。结果如下所示：

图表五　填入收到的参考号和授权码以及生成的 csr

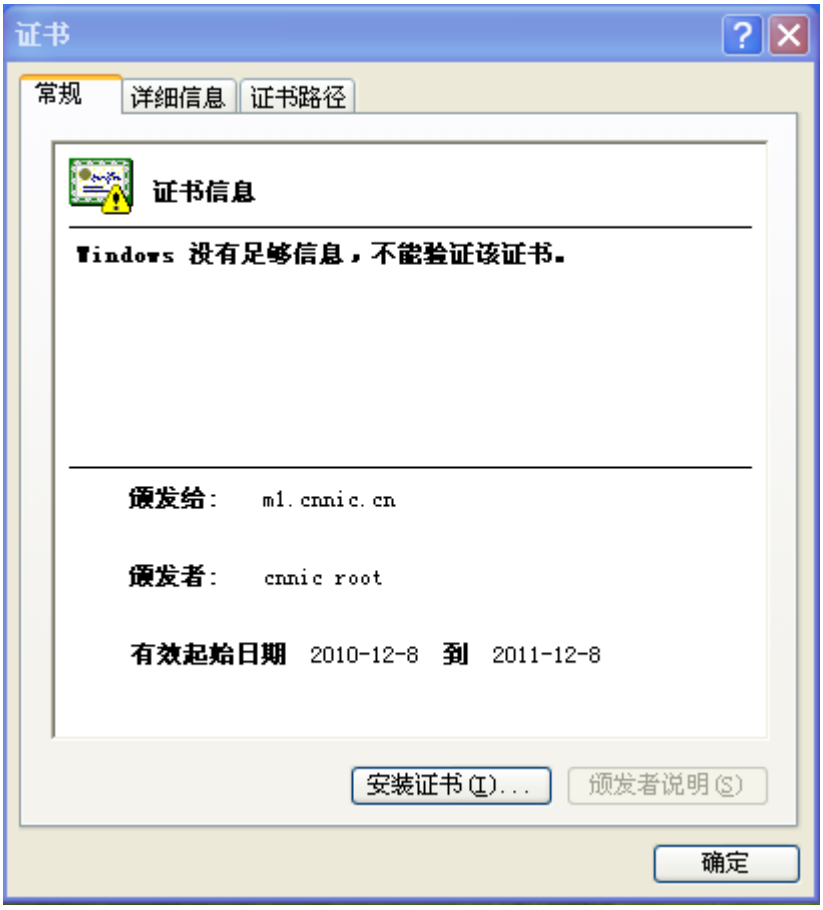
点击“提交”，如果参考号、授权码和 CSR 均无问题，则显示页面如下所示：

图表六　生成证书

请按页面提示保存，文件名保存为 m1.cnnic.cn.cer。该文件即为申请的证书，如果该证书丢失，就必须进行证书补办。

注意：关于证书的格式转换

从 CNNIC 获得的证书格式为 X509 格式。该将证书文件的扩展名由 txt 改为 cer 或 crt 后，可在 windows 中双击打开查看证书的相关信息。显示信息类 似下图所示：

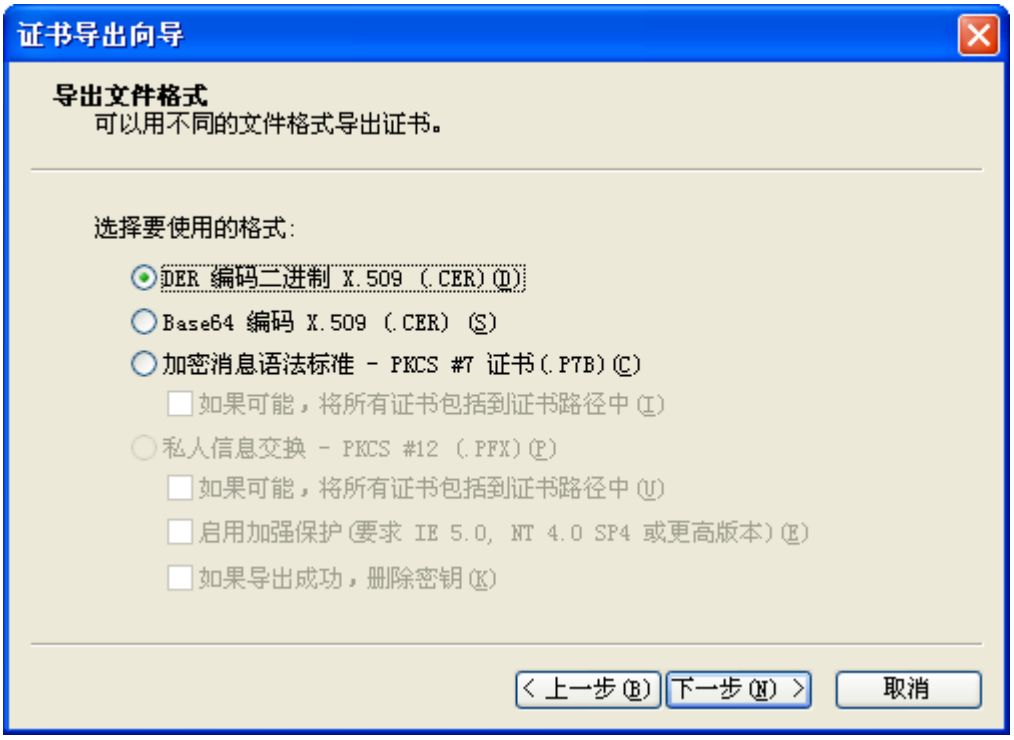


图表七　格式转换

X509 格式的证书利用 windows 提供的图形界面操作工具可以另存为以下两种编码格式：

- BASE64 编码格式：该格式的证书可以用记事本打开
- DER 编码格式：二进制格式

在上图中，点击“详细信息”->“复制到文件”后，即可以根据提示点击“下一步”利用证书导出向导导出需要格式的证书，如下图所示：



图表八　证书导出向导（A）

5. 安装根证书和服务器证书

1） 下载根证书及CNNIC中级根证书

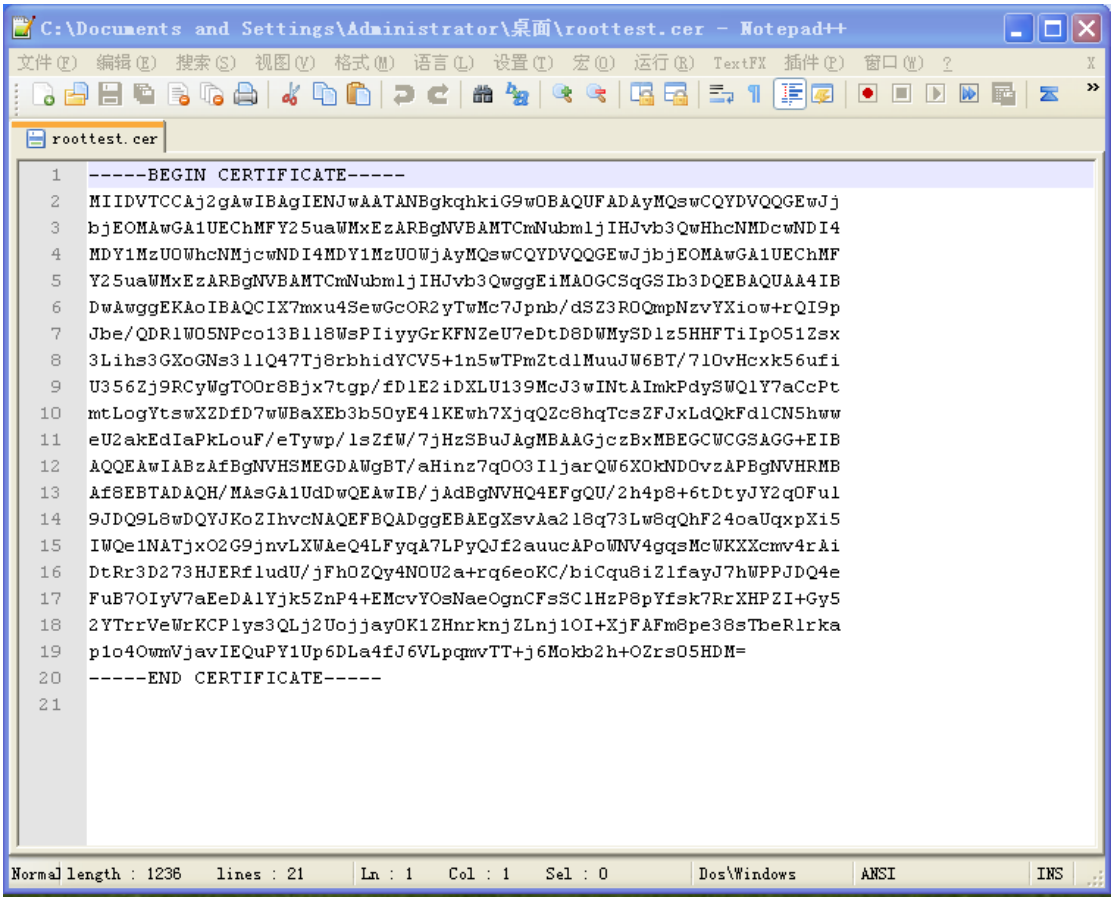
下载地址：

快速证书：http://www.cnnic.cn/jczyfw/wzws/ksym/ksxz/201105/t20110524_21055.html

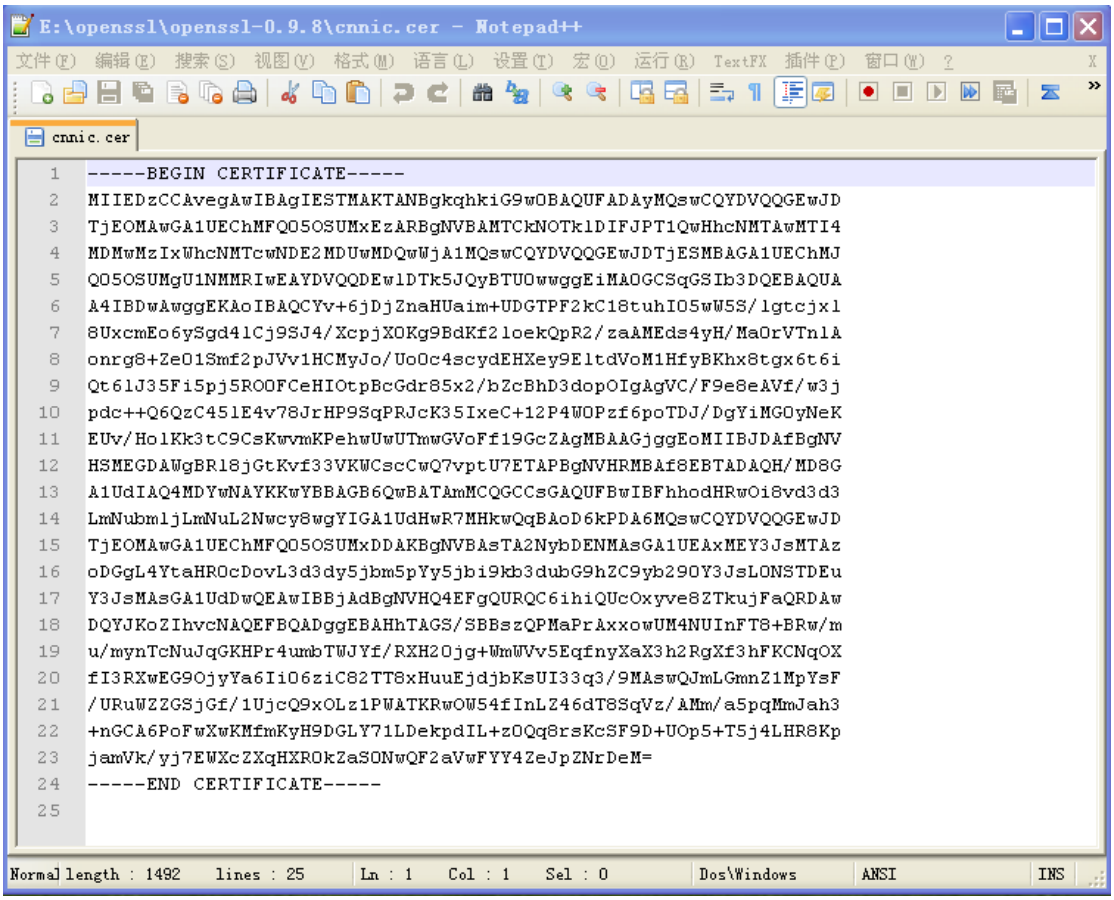
标准证书：http://www.cnnic.cn/jczyfw/wzws/bzkx/xz/201010/t20101027_16322.html

EV证书： http://www.cnnic.cn/jczyfw/wzws/kxEV/xz/

将 CNNIC 中级根证书文件名保存为“CNNIC.cer”，将根证书文件名保存为“root.cer”。

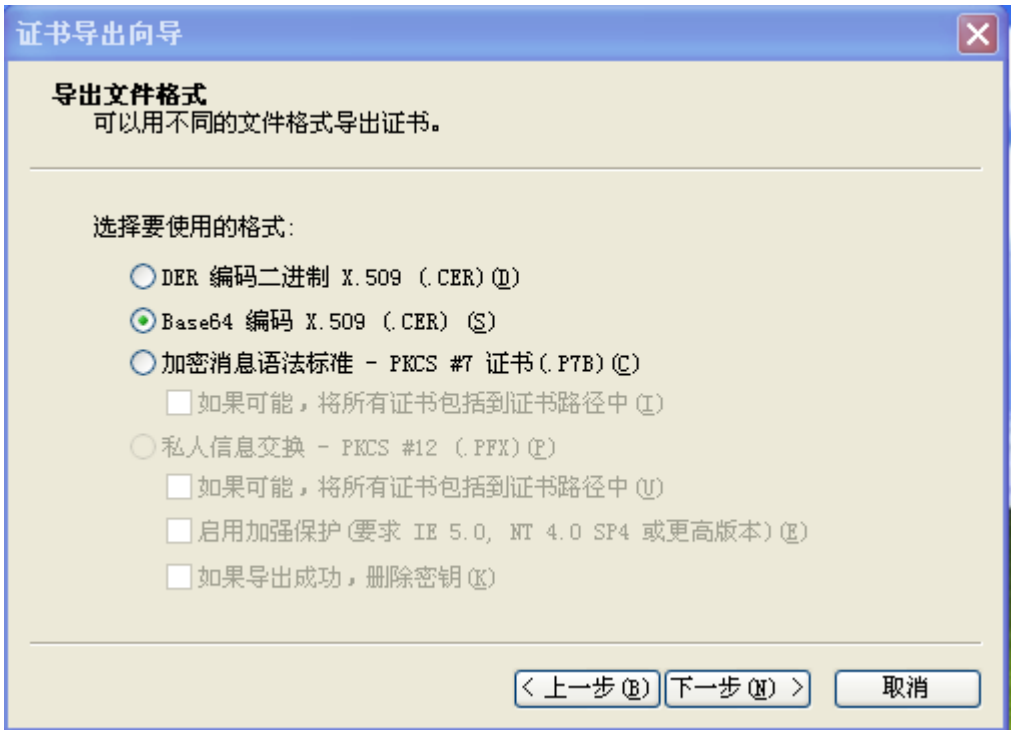


图表九　查看根证书 roottest.cer



图表十　查看中级根证书 cnnic.cer

注意：在用 notepad 打开 roottes.cer 的时候可能会出现乱码，这样我们就先直接打开 roottest.cer --详细信息--复制到文本，选择 Base64 编码 X.509,如下图：



图表十一　证书导出向导（B）

下一步，替换之前的 roottest.cer 文件即可。

复制 m1.cnnic.cn.key 及 m1.cnnic.cn.cer 文件到 Nginx 安装目录下的 conf 目录。

6. 修改配置文件

1)　修改Nginx　SSL配置模块

```
server {

listen 443;

server_name www.domain.com;



ssl on;

ssl_certificate /etc/ssl/m1.cnnic.cer;     //公钥文件(cnnic 颁发的证书)
```

```
ssl_certificate_key /etc/ssl/m1.cnnic.key;        //私钥文件

ssl_client_certificate /etc/ssl/cnnic.cer;    //中级证书



ssl_session_timeout 5m;

ssl_protocols SSLv2 SSLv3 TLSv1;

ssl_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;

ssl_prefer_server_ciphers on;

location / {

root html;

index index.html index.htm;

}

}
```

按照以上的步骤配置完成后，重新启动 nginx（如果有设置 server.key 私钥密码，这时会提示输入） 后就可以使用 https://m1.cnni.cn 来访问了。

7. 备份服务器证书

只需备份好服务器证书文件 m1.cnnic.cn.cer

私钥保存文件 m1.cnnic.cn.key 即可。