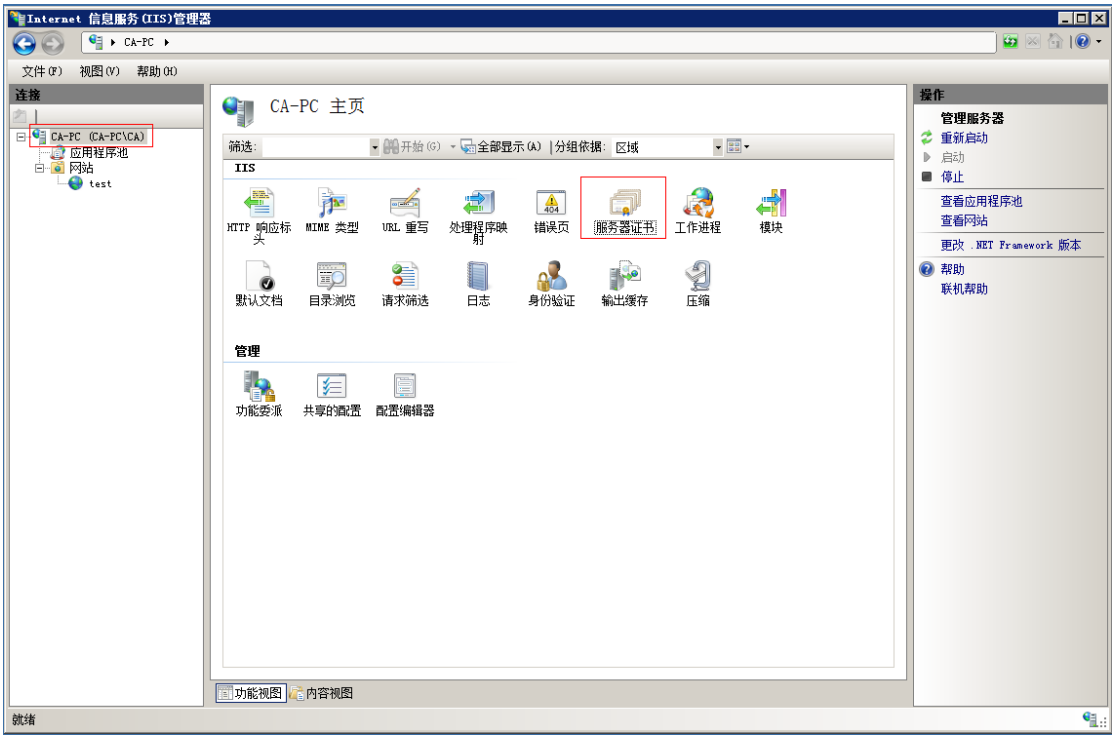
目录

一、 生成证书请求

1. 打开 IIS 控制台

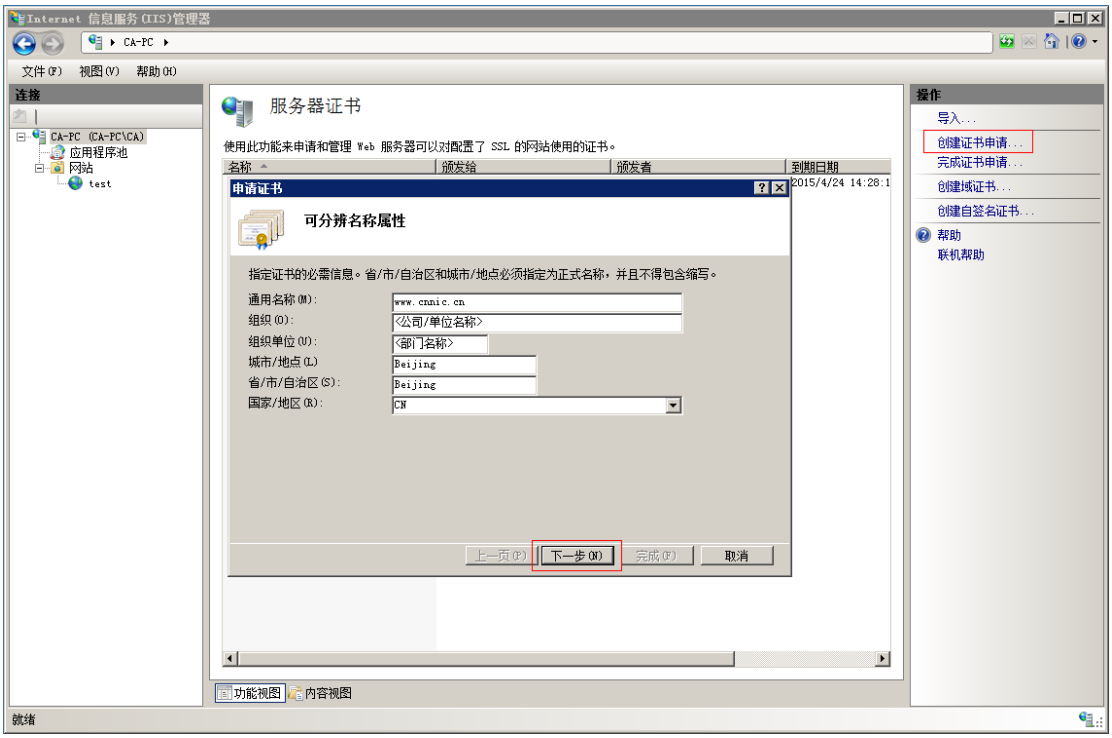
进入 IIS 控制台，并选择服务器的服务器证书设置选项。



图表一　进入 IIS 控制台找到服务器证书项

2. 创建证书申请

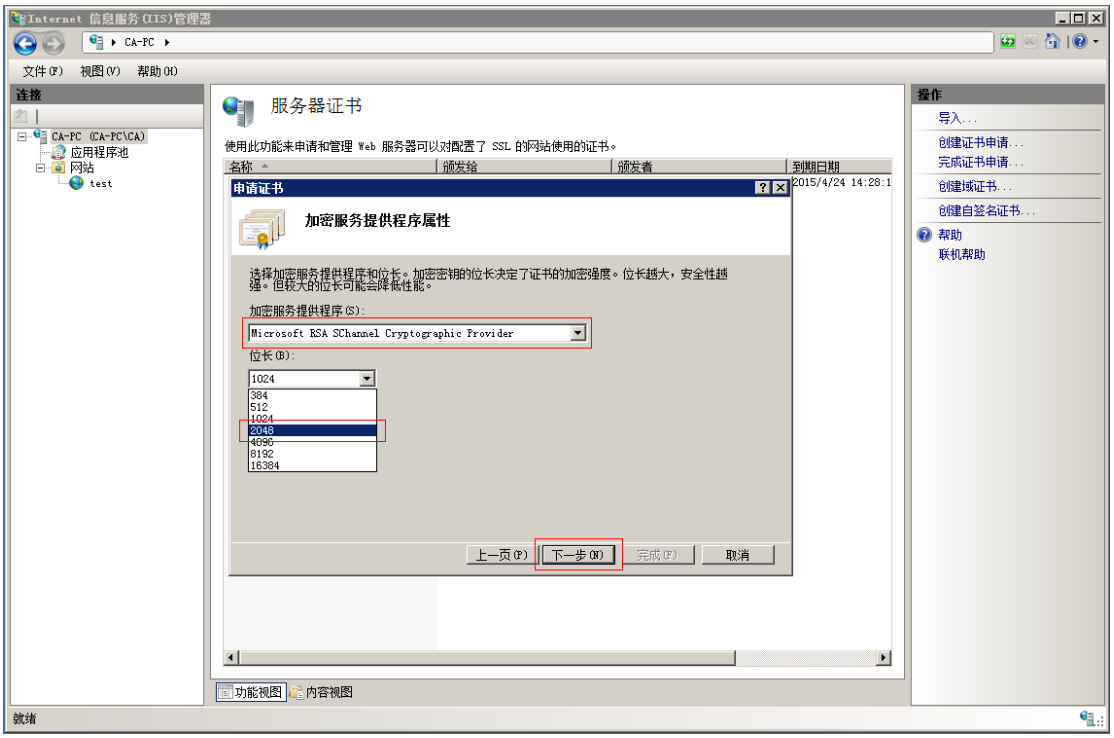
进入服务器证书配置页面，并选择“创建证书申请”



图表二　创建证书申请并填写相关信息

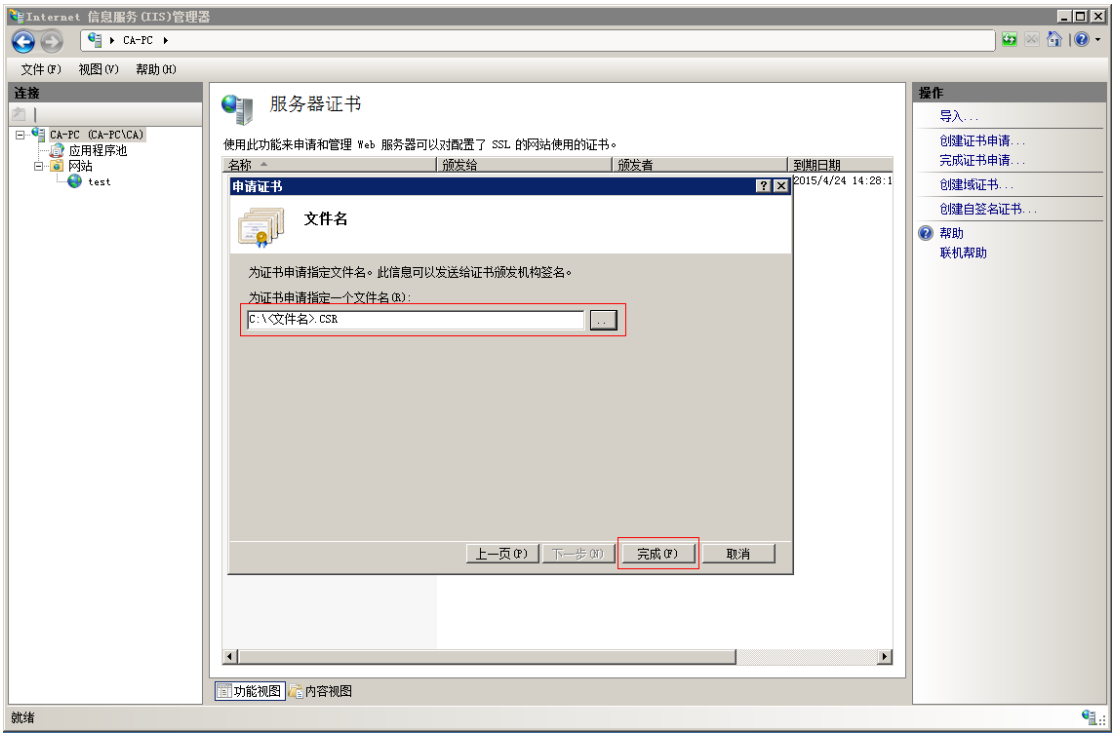
3. 设置证书密钥长度

按下图所示选择正确的加密服务提供程序，接下来设置证书密钥长度，需要注意的是，CNNIC 服务器证书要求 2048 位密钥长度。



图表三　选择密钥长度

4. 生成证书请求文件并保存



图表四　保存证书请求文件

5. 查看证书请求文件

生成的证书请求文件可使用记事本工具打开，所显示内容如下图所示：

图表五　请求文件内容

二、 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 官网，进入 CNNIC 服务器证书下载中心页面：

http://www.cnnic.net.cn/jczyfw/fwqzs/fwqzsxzzx/

点击相应的链接进入到证书下载页面，如下图所示：

图表六　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：

图表七　填入收到的参考号和授权码以及生成的 CSR

点击“下载”，如果参考号、授权码和证书请求文件均无问题，则显示页面如下所示。

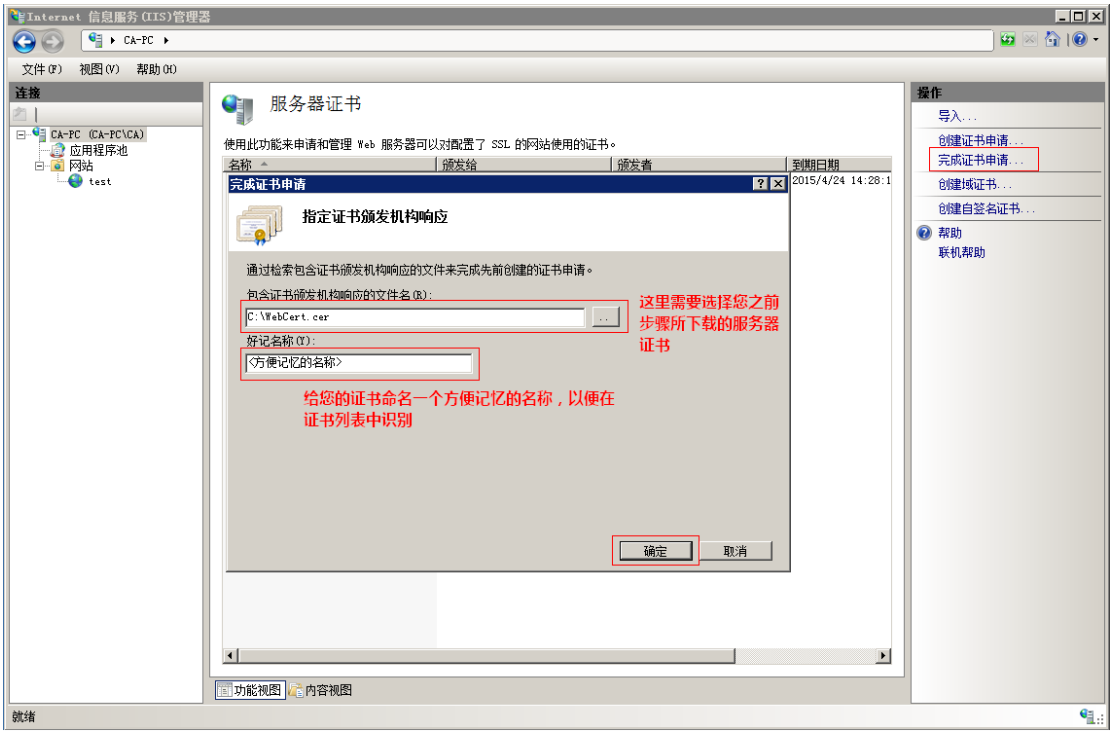
图表八　生成证书

请按页面提示将文本框中的内容拷贝下来，粘贴到一个文本文档中保存，为文件起一个方便记忆的名字，以.cer 为后缀。您也可以直接点击保存，自动下载一个名为 WebCert.cer 的文件，该文件即为申请的证书。请妥善保存该文件，如果该证书丢失，就必须进行证书补发操作，此操作可能会有相应费用产生。

三、 安装服务器证书

1. 完成证书申请

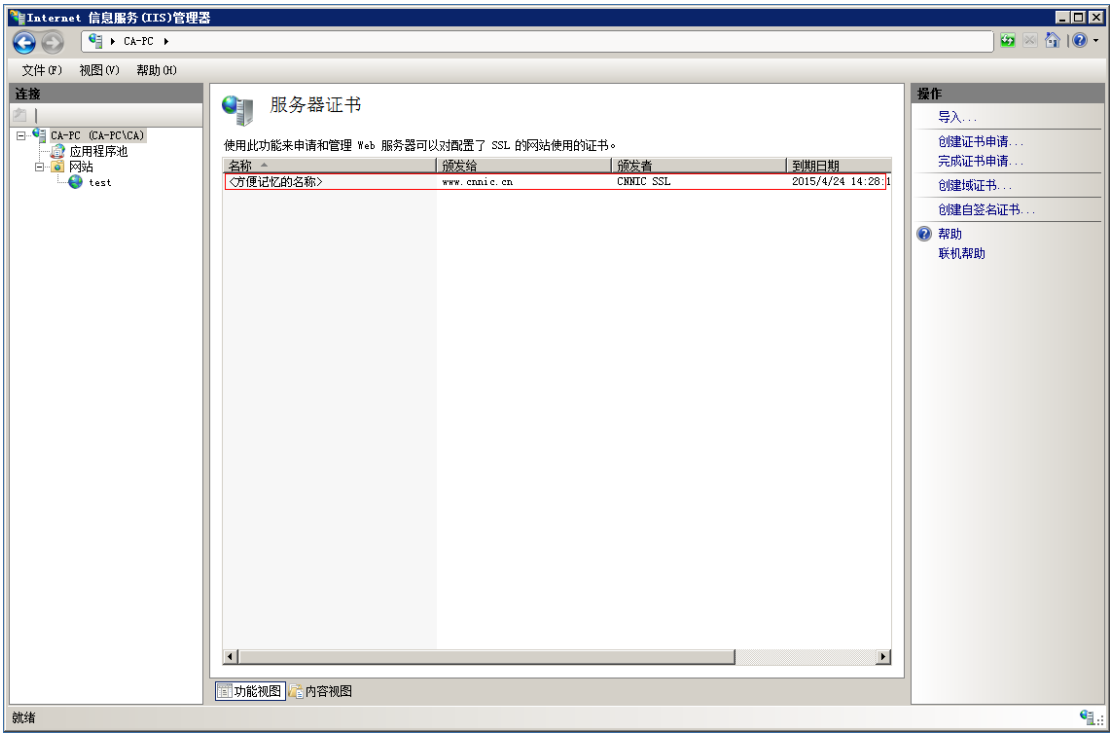
打开 IIS 控制台界面，点击右侧边栏“完成证书申请”选项，按照下图进行配置。



图表九　完成证书申请

2. 查看证书列表

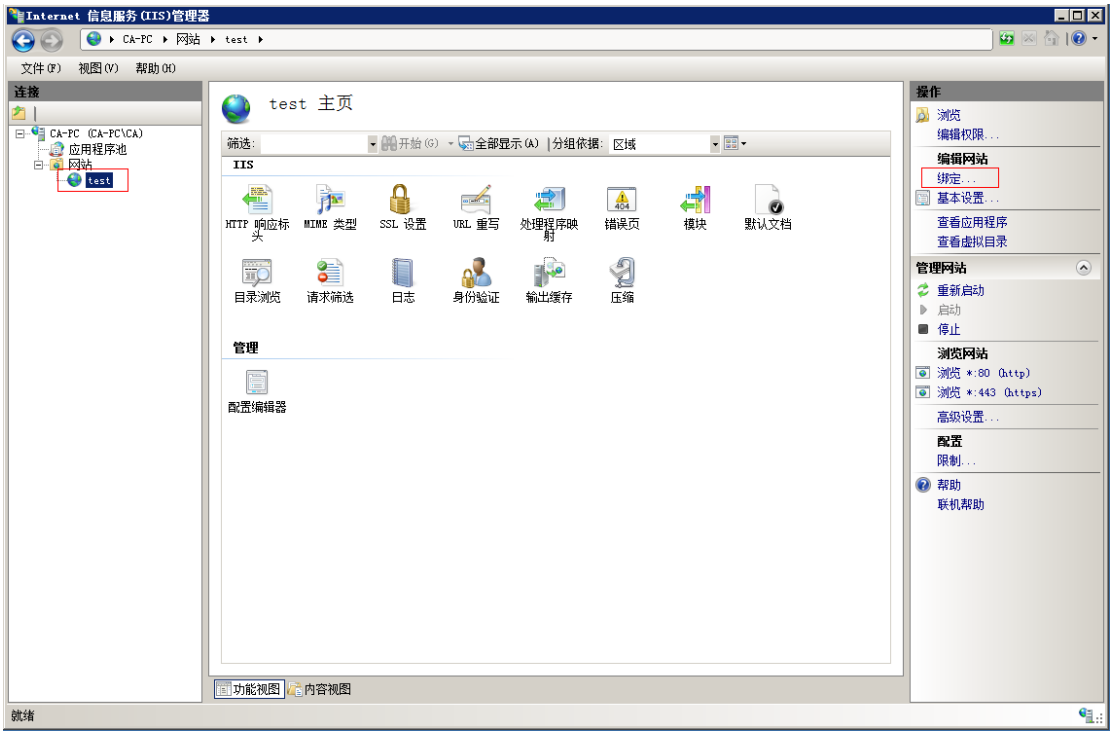
完成证书申请后，该证书会在服务器证书列表中出现，以<方便记忆的名称>标识，如下图所示：



图表十　服务器证书列表

3. 配置服务器证书

选中需要配置证书的站点，并选择右侧“编辑站点”下的“绑定”



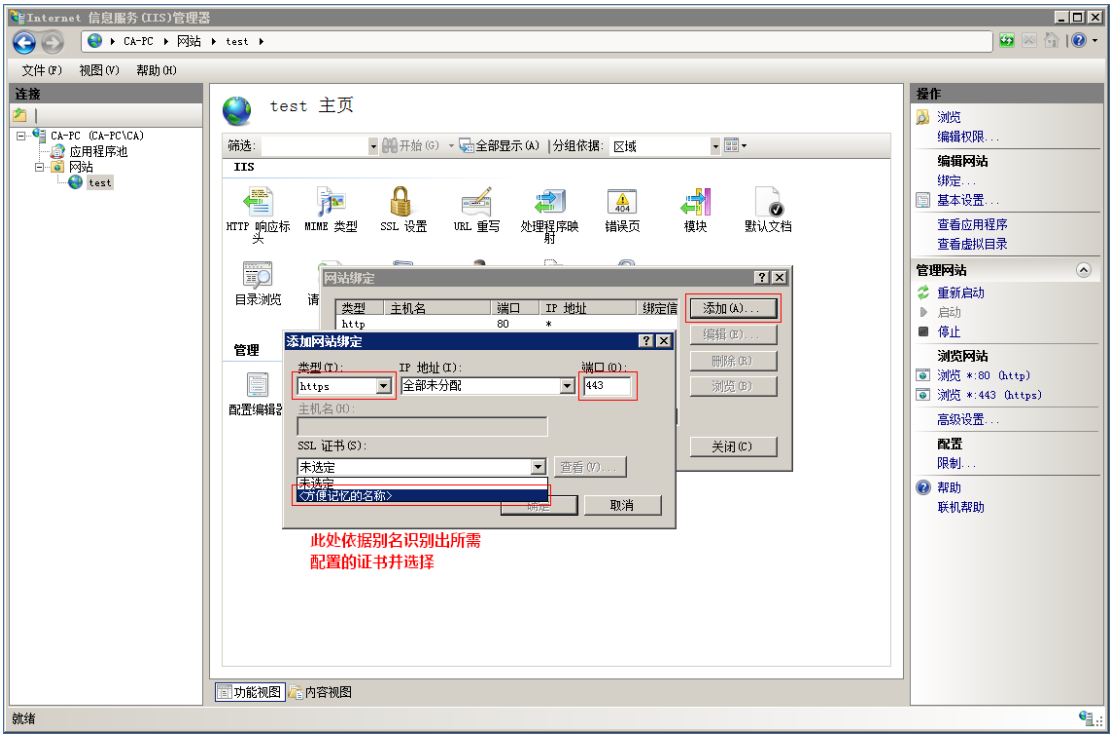
图表十一　选择对应网站进行绑定

选择“添加”并设定：

类型：https

端口：443

指派站点证书，点击“确定”



图表十二　绑定 https 端口

4. 安装中级根证书

通过以上步骤已经安装成功网站的域名证书，还需要通过“证书管理器”安装对应的中级根证书。

在 MMC 中添加证书管理器：

a. 从“开始”菜单，单击“运行”；

b. 在“打开”框中，键入以下内容：mmc；

c. 单击“确定”；

d. 在“文件”菜单上，单击“添加/删除管理单元”；

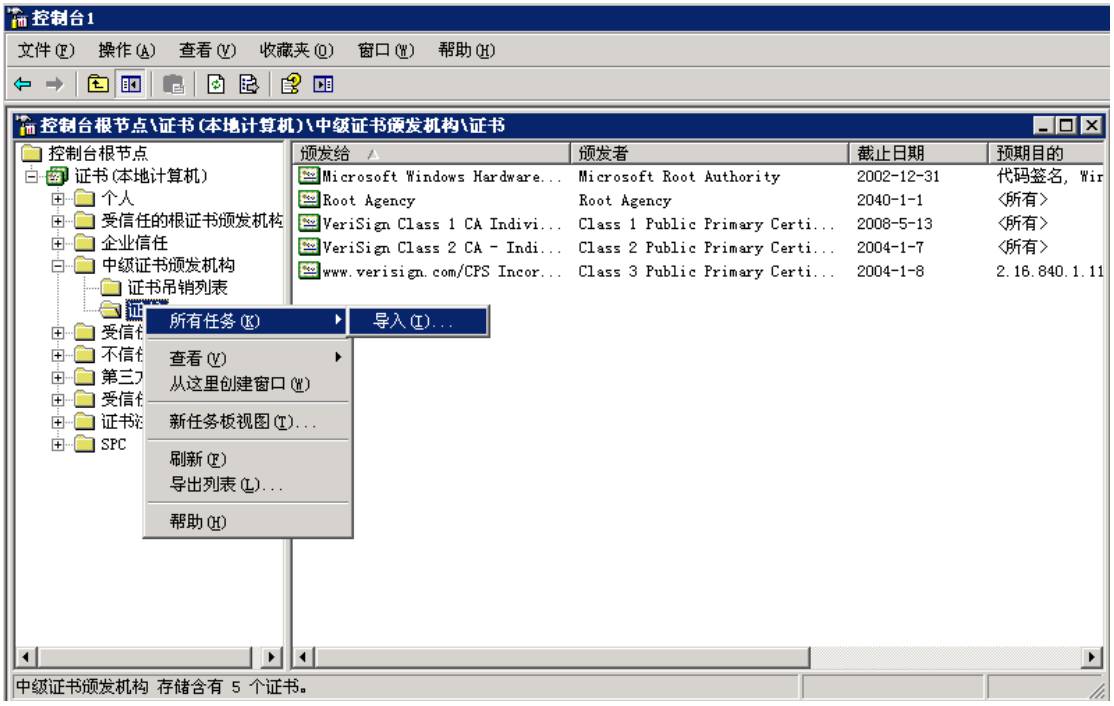
e. 在“添加/删除管理单元”对话框中，单击“添加”；

f. 在“可用的独立管理单元”列表中，单击“证书”，然后单击“添加”；

g. 在“证书管理单元”框中，单击“计算机帐户”，然后单击“下一步”；

h. 在“选择计算机”框中，单击“本地计算机”，然后单击“完成”。

运行 MMC 管理证书，右击“中级证书颁发机构”-“证书”后的“所有任务”中的“导入”，选择已下载的 CNNIC 中级根证书，即可安装成功。



图表十三　导入中级根证书

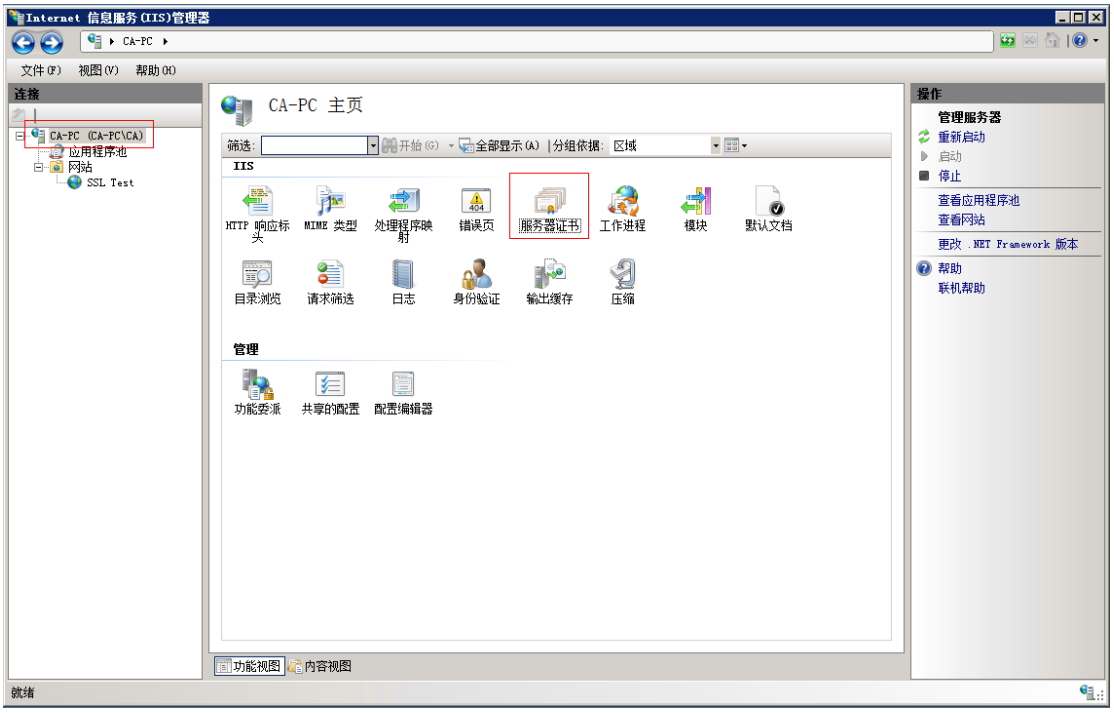
5. 测试是否安装成功

重新启动您的 IIS 应用后，在浏览器地址栏输入：https://<申请证书的域名>测试您的 SSL 证书是否安装成功，如果成功，则浏览器下方会显示一个安全锁标志。双击安全锁，可查看网站的域名证书。

四、 备份服务器证书

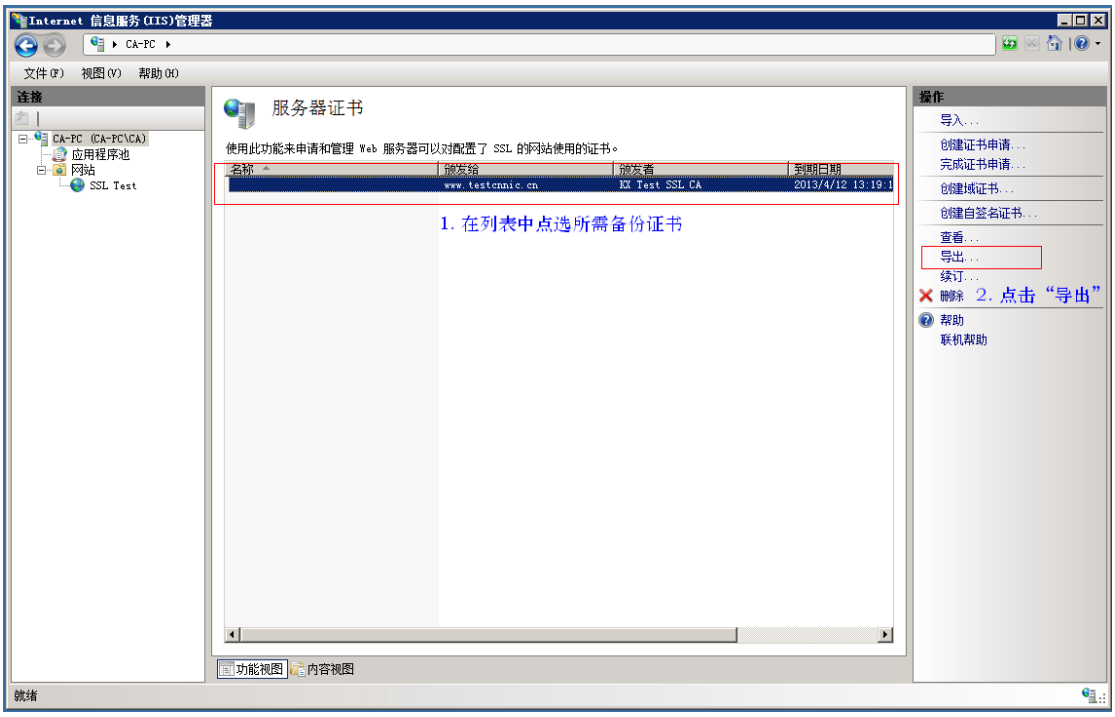
当您完成服务器证书在 IIS 中的首次部署，应当对服务器证书的公钥及私钥进行备份，具体步骤如下：

1) 打开 IIS 管理界面，在最顶层菜单中双击“服务器证书”图标，如下图所示：



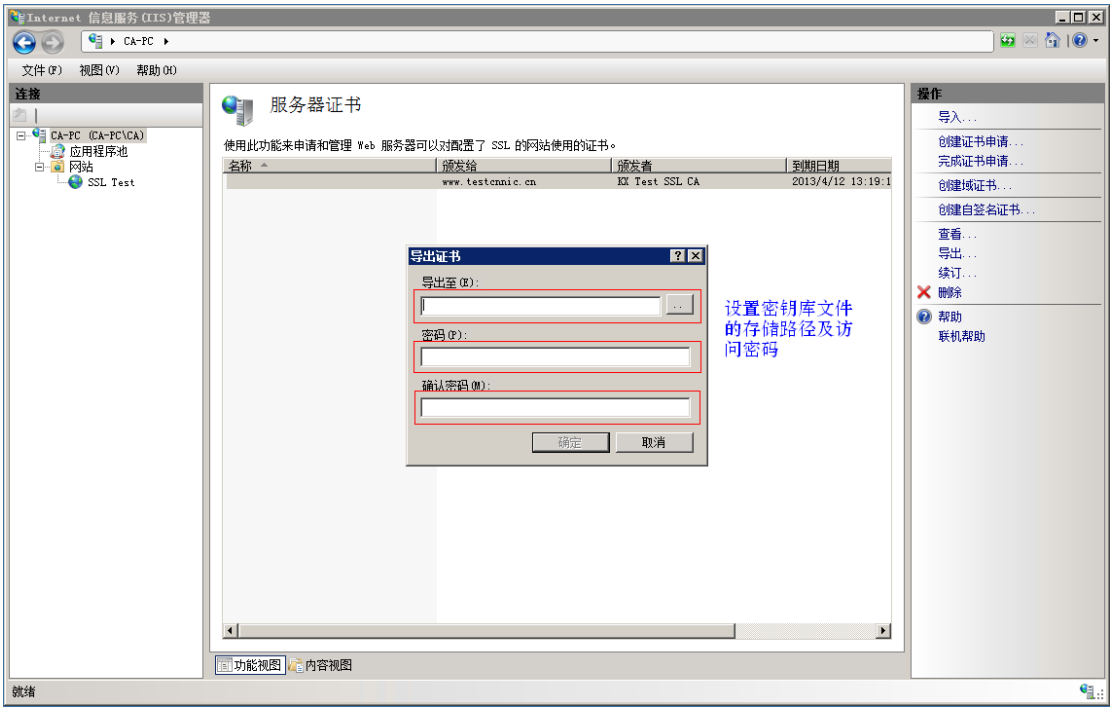
图表十四

2) 进入“服务器证书”功能模块后可以看到当前服务器中所安装的所有证书，点选所要备份的证书后，右侧便可看到“导出”选项，如下图：



图表十五

3) 点击“导出”后将弹出如下图所示对话框，设置密钥库存储路径及访问密码后点击“确定”便可完成证书导出，进入导出时设置的存储路径，手动复制***.pfx 文件至安全的地方即可完成备份。两点需要强调：1、请牢记导出时设置的访问密码，是再次导入证书时所必需的；2、所备份的密钥库文件中包含 a.证书私钥、b.服务器证书（公钥）、c.全部证书链。



图表十六

PS：所需备份的密钥库文件应如下图所示，后缀为 pfx 的文件：