



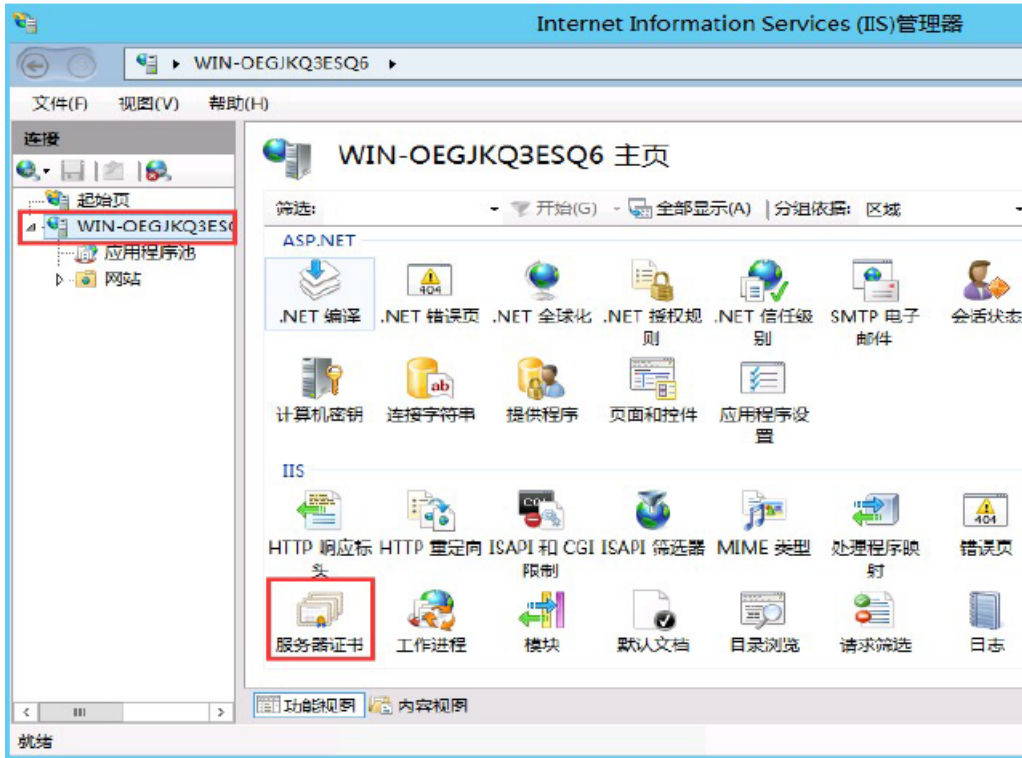
服务器证书安装配置指南

IIS8

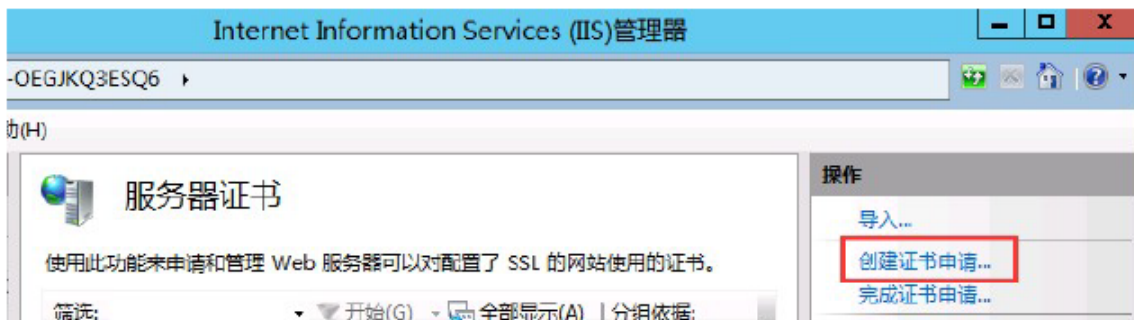
二〇二一年一月

第一步：生成证书签名请求文件(CSR)

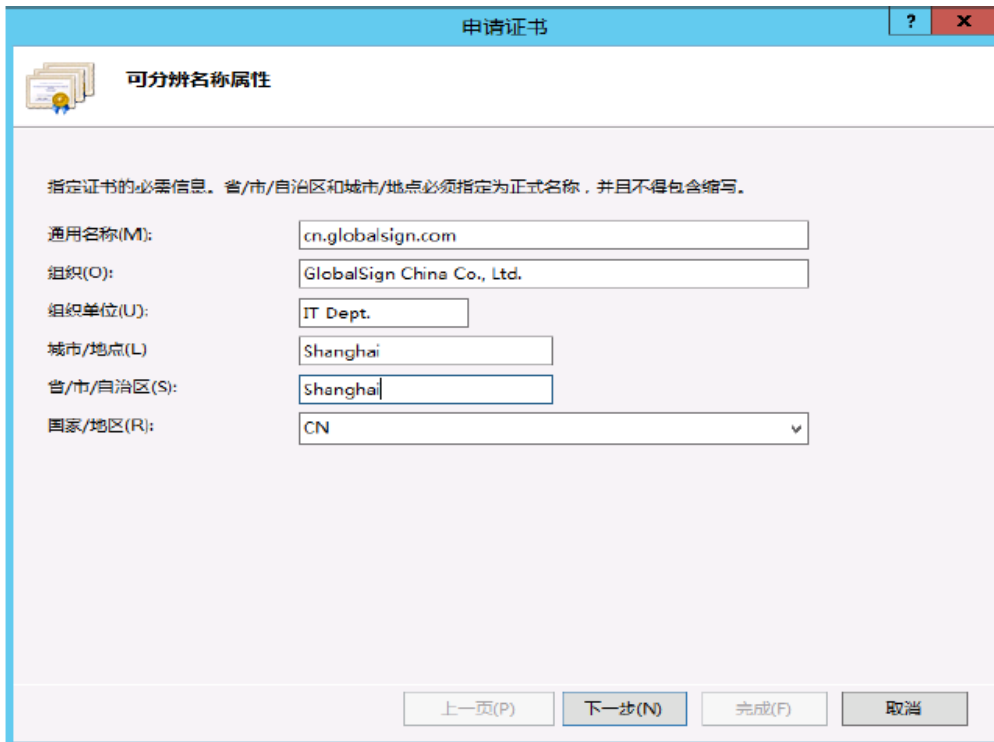
打开 IIS 服务管理器，点击计算机名称，双击打开右侧的“服务器证书”图标



双击打开服务器证书后，点击右侧的“创建证书申请”



输入申请证书信息，点击下一步



申请证书

可分辨名称属性

指定证书的必需信息。省/市/自治区和城市/地点必须指定为正式名称，并且不得包含缩写。

通用名称(M):

组织(O):

组织单位(U):

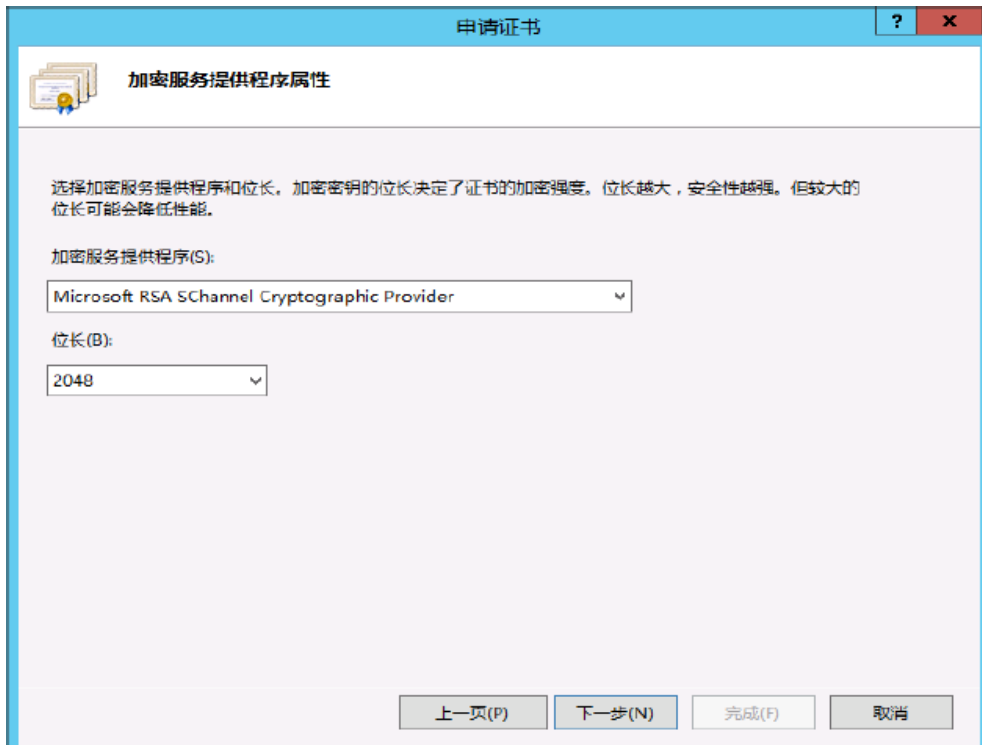
城市/地点(L):

省/市/自治区(S):

国家/地区(R):

上一页(P) 下一步(N) 完成(F) 取消

选择加密服务提供程序和加密长度，建议默认，点击“下一步”



申请证书

加密服务提供程序属性

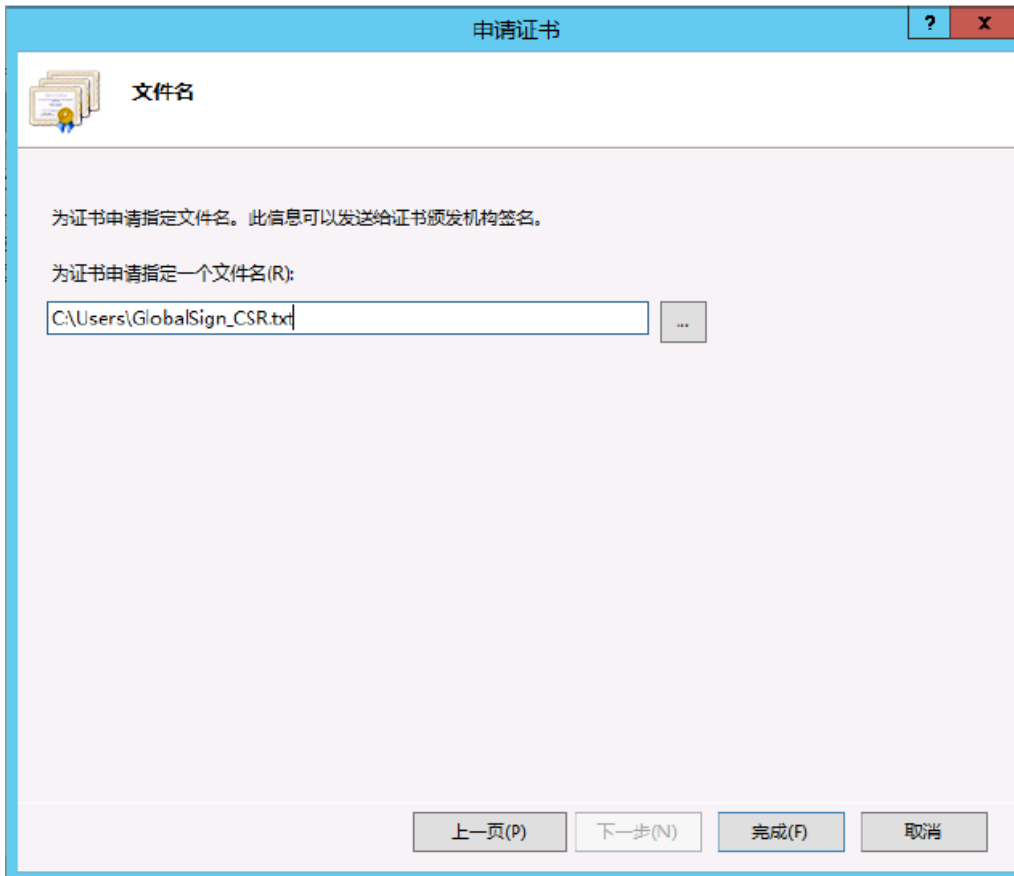
选择加密服务提供程序和位长。加密密钥的位长决定了证书的加密强度。位长越大，安全性越强。但较大的位长可能会降低性能。

加密服务提供程序(S):

位长(B):

上一页(P) 下一步(N) 完成(F) 取消

选择证书签名请求 (CSR) 文件保存的路径和文件名，点击“完成”



第二步：提交 CSR，申请证书

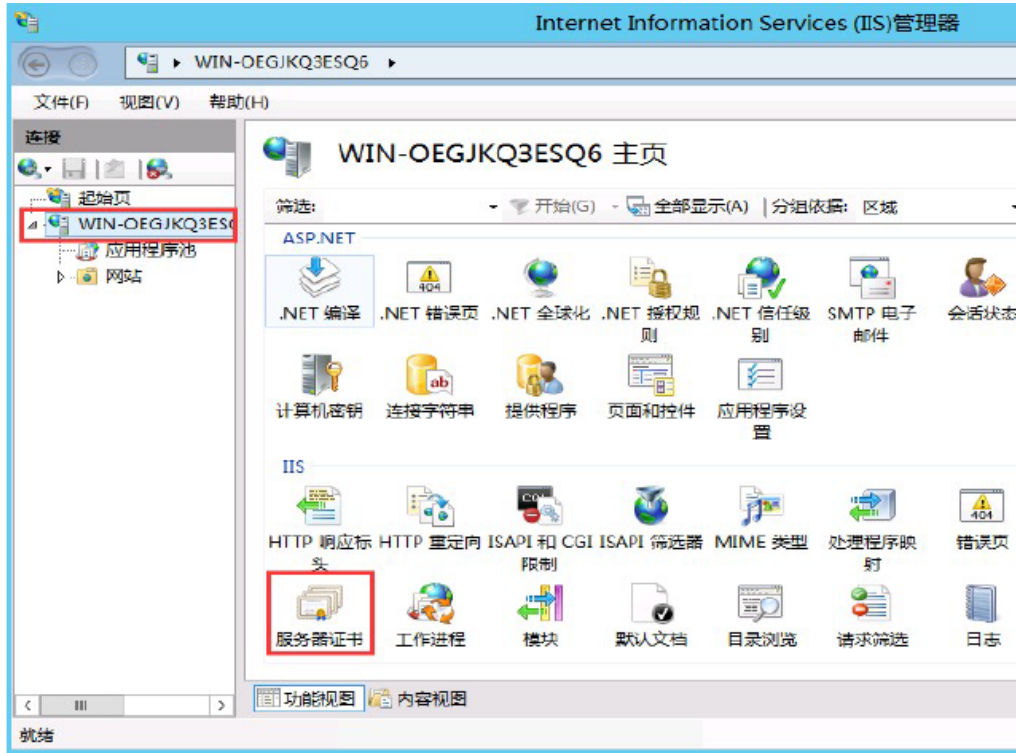
递交证书申请表及相关资料，并把证书请求文件 (CSR) 提交给我们。我们确认资料齐全后，三个工作日内完成证书颁发。

第三步：获取服务器证书

将证书签发邮件中的从BEGIN 到 END 结束的服务器证书内容 (包括 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----”) 粘贴到记事本等文本编辑器中，并修改文件扩展名，保存为server.cer 文件。

第四步：安装服务器证书

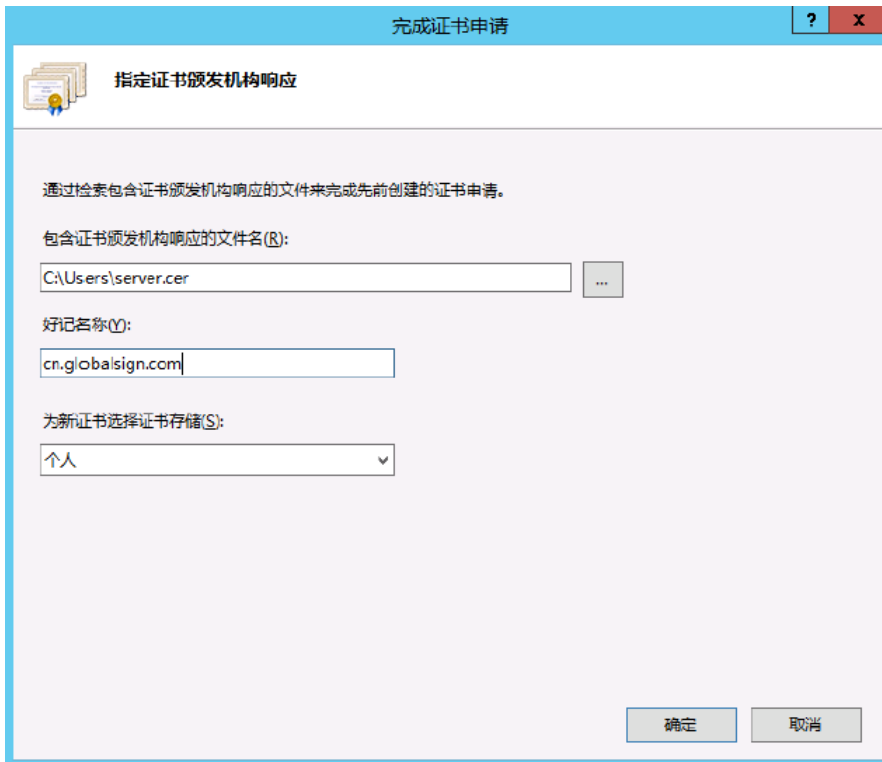
打开 IIS 服务管理器，点击计算机名称，双击打开右侧的服务器证书图标



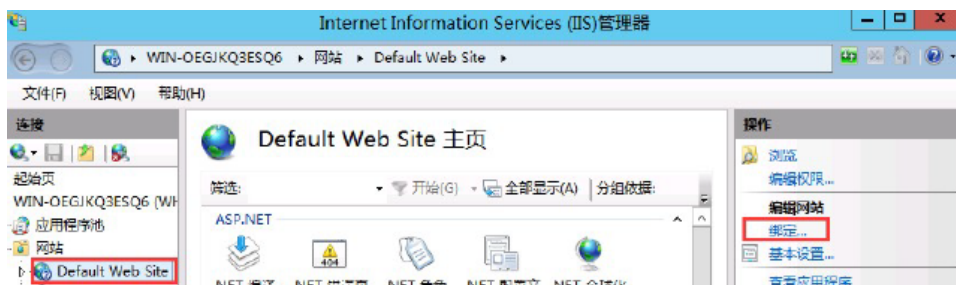
双击打开服务器证书后，点击右侧的“完成证书申请”



选择GlobalSign 颁发的服务器证书文件，并指定一个好记的名称（可选），点击确定

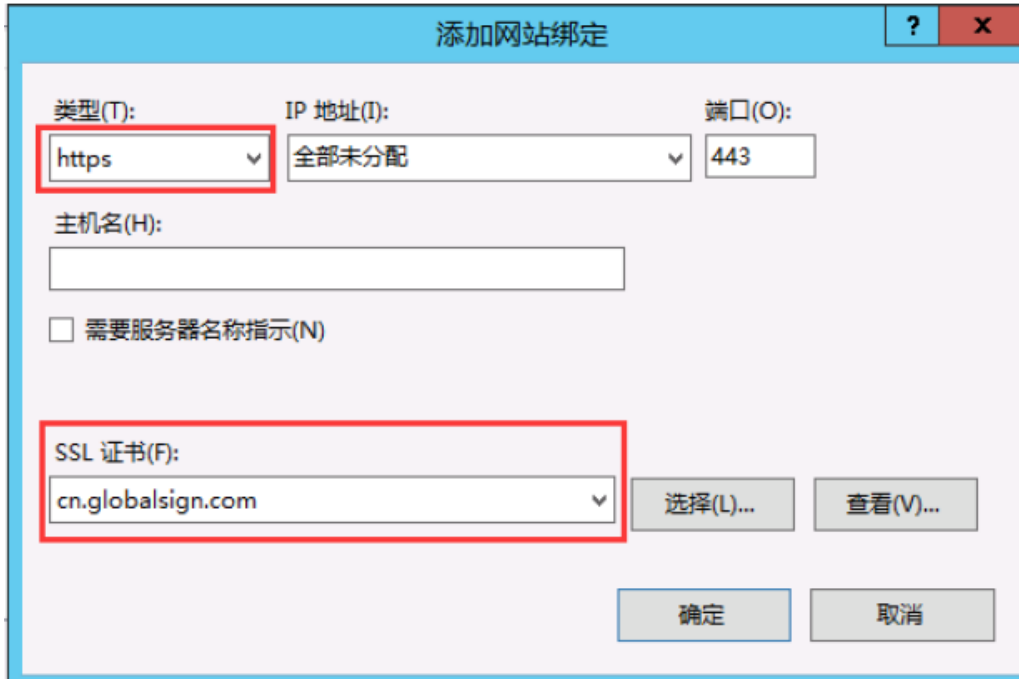


点击网站下的站点名称，点击右侧的“绑定”



打开网站绑定界面后，点击“添加”





添加网站绑定

类型(T): **https** IP 地址(I): 全部未分配 端口(O): 443

主机名(H):

需要服务器名称指示(N)

SSL 证书(F): **cn.globalsign.com** 选择(L)... 查看(V)...

确定 取消

添加网站绑定内容：选择类型为 https，端口 443 和指定对应的 SSL 证书，点击确定

添加完成后，网站绑定界面将会看到刚刚添加的内容



网站绑定

类型	主机名	端口	IP 地址	绑定信息
http		80	*	
https		443	*	

添加(A)...
编辑(E)...
删除(R)
浏览(B)
关闭(C)

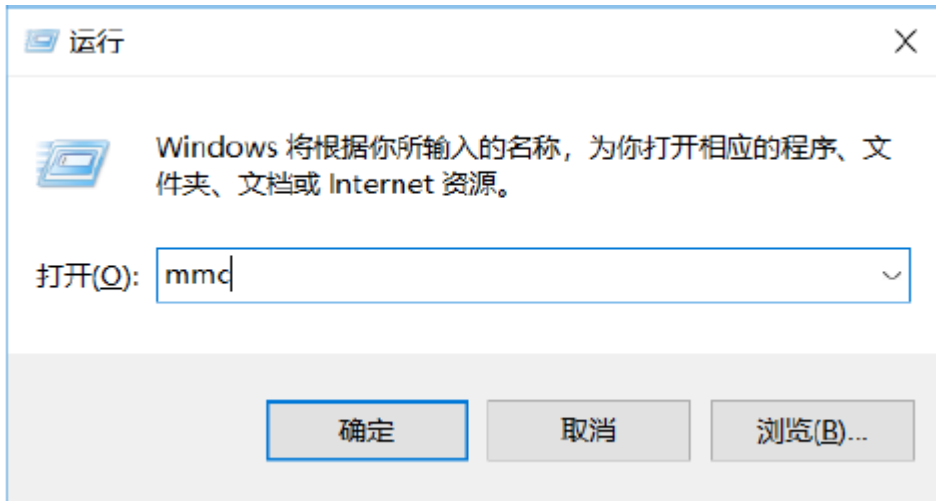
第五步：配置中级 CA 证书

为保障服务器证书在IE7 以下客户端的兼容性，服务器证书需要安装两张中级CA证书（即中级证书和交叉证书）。从邮件中获取中级证书和交叉证书：将证书签发邮件中的从BEGIN 到 END 结束的两张中级CA 证书内容（包括 “-----BEGIN CERTIFICATE-----” 和 “-----END CERTIFICATE-----” ）分别粘

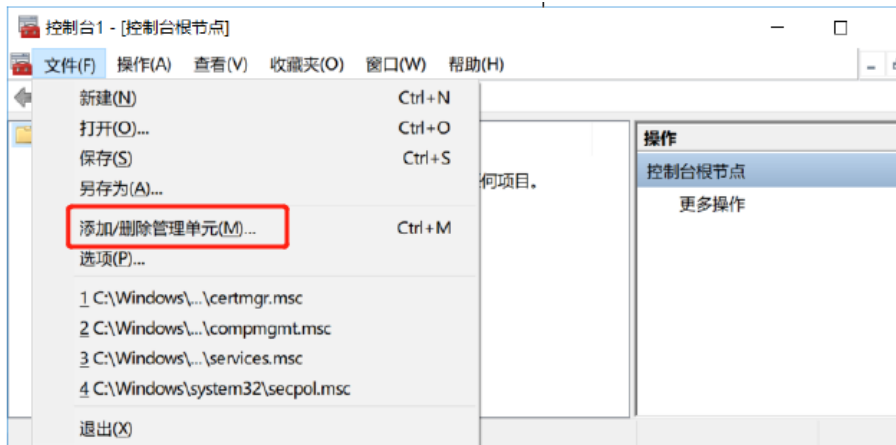
贴到记事本等文本编辑器中，并修改文件扩展名，保存为intermediate1.cer 和intermediate2.cer文件。

第六步：安装中级 CA 证书

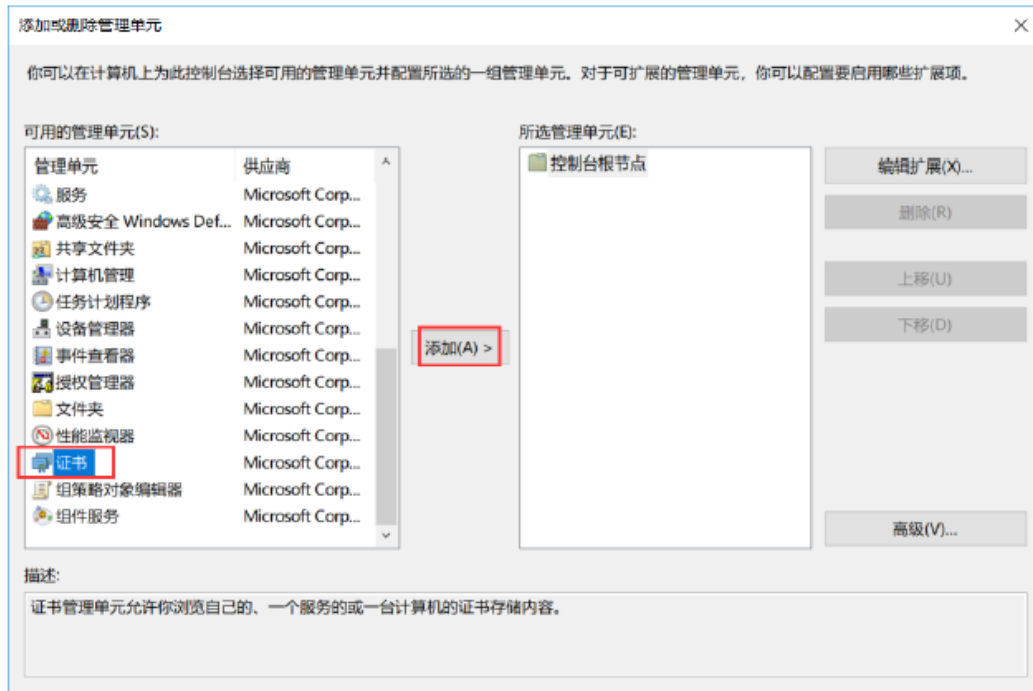
点击“开始”“运行”“mmc”



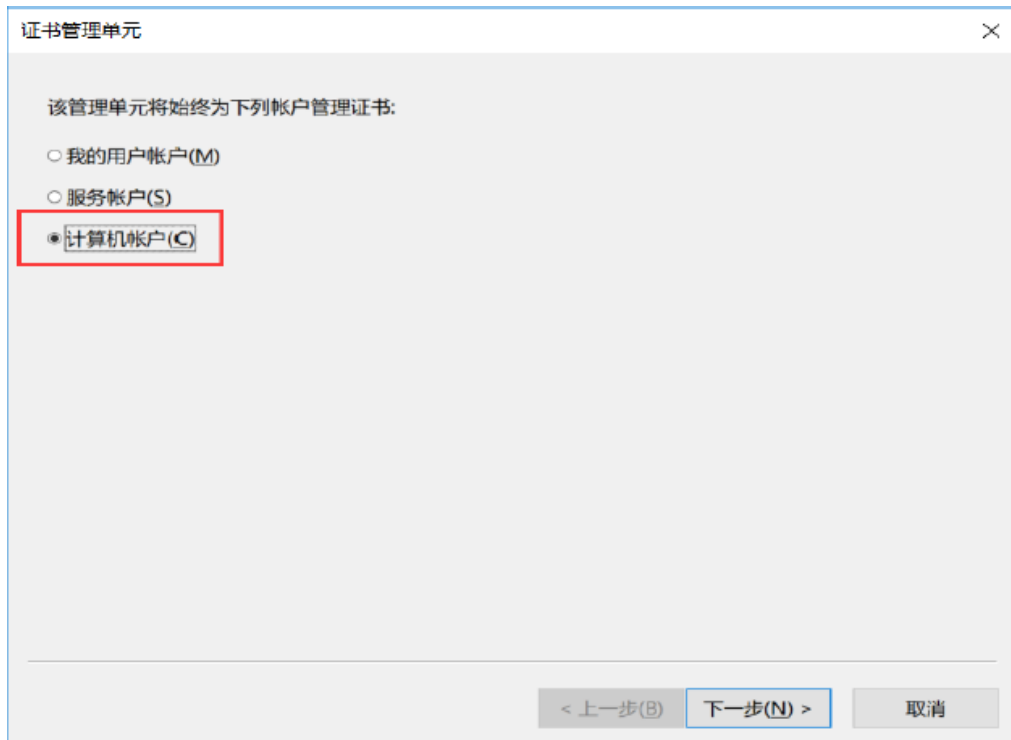
打开控制台，点击“文件”“添加/删除管理单元”



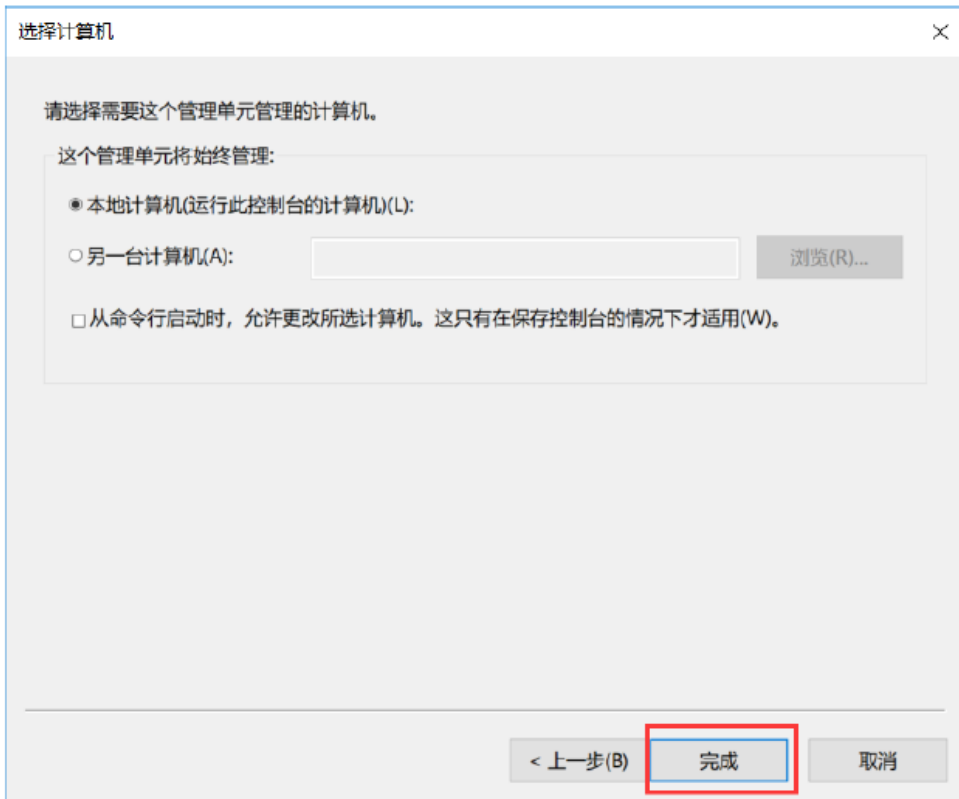
找到“证书” 点击“添加”



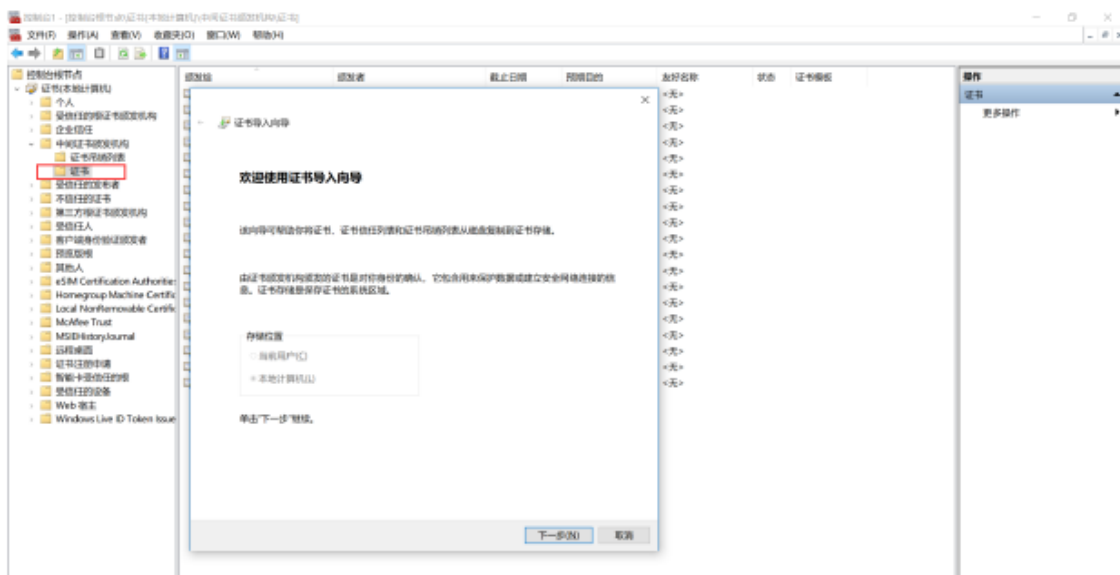
选择“计算机帐户”，点击“下一步”



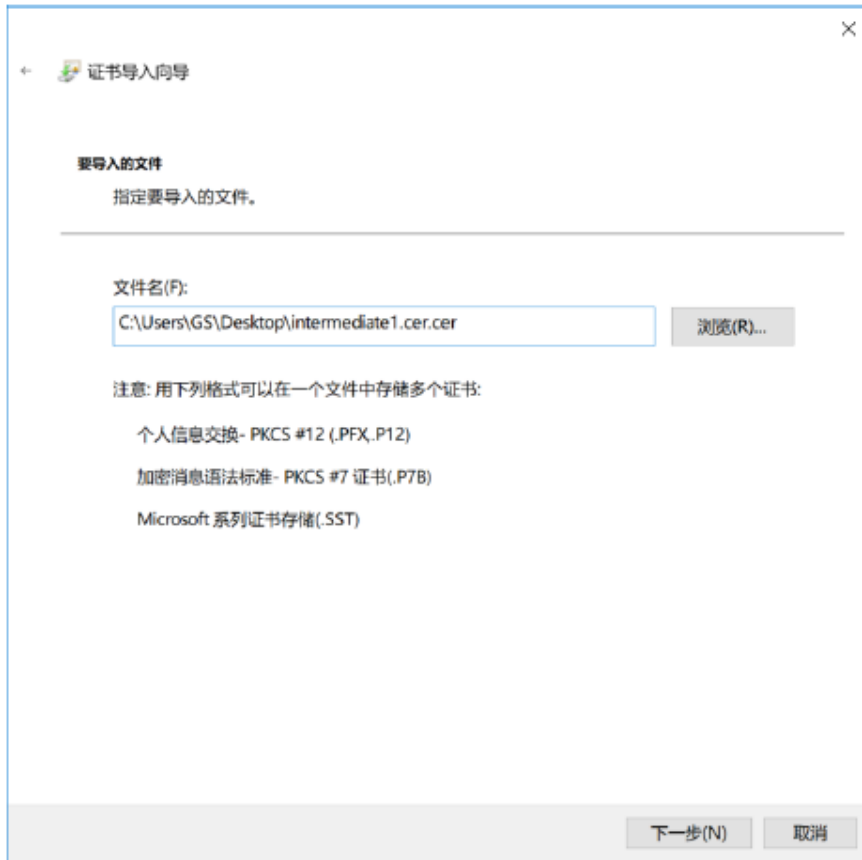
点击“完成”



点击“证书(本地计算机)”，选择“中级证书颁发机构”“证书”，在空白处点击右键，选择“所有任务”“导入”。



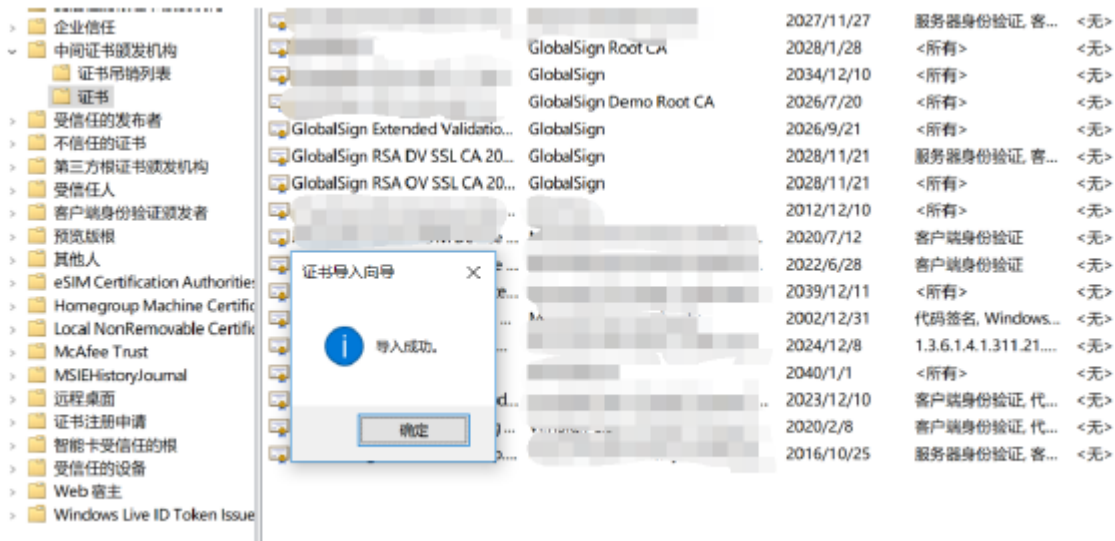
通过证书向导分别导入中级 CA 证书 intermediate1.cer、intermediate2.cer



选择“将所有的证书放入下列存储”，点击“下一步”，点击“完成”



导入中级 CA 证书完成。



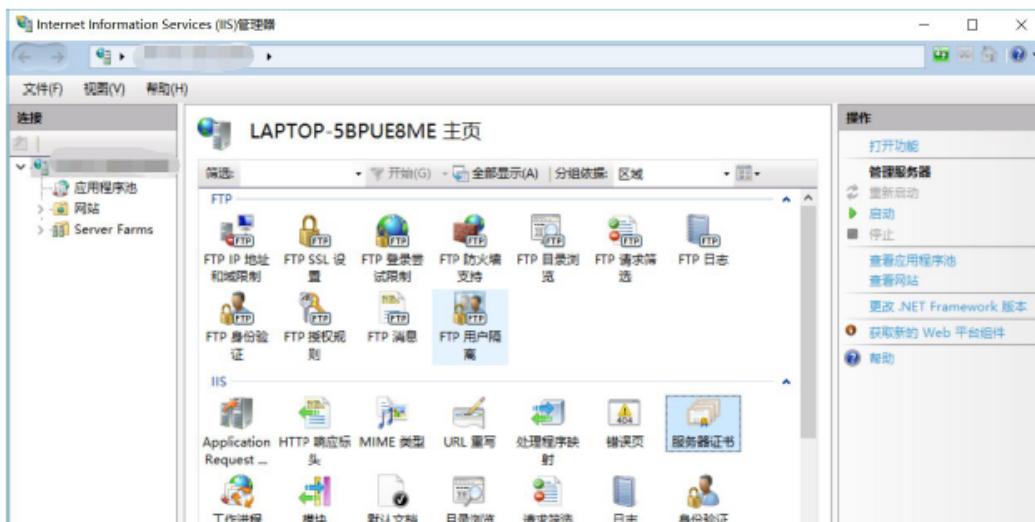
按照以上的步骤配置完成，重启IIS服务后，就可以使用 <https://www.domain.com>访问了。

第七步：服务器证书的备份及恢复

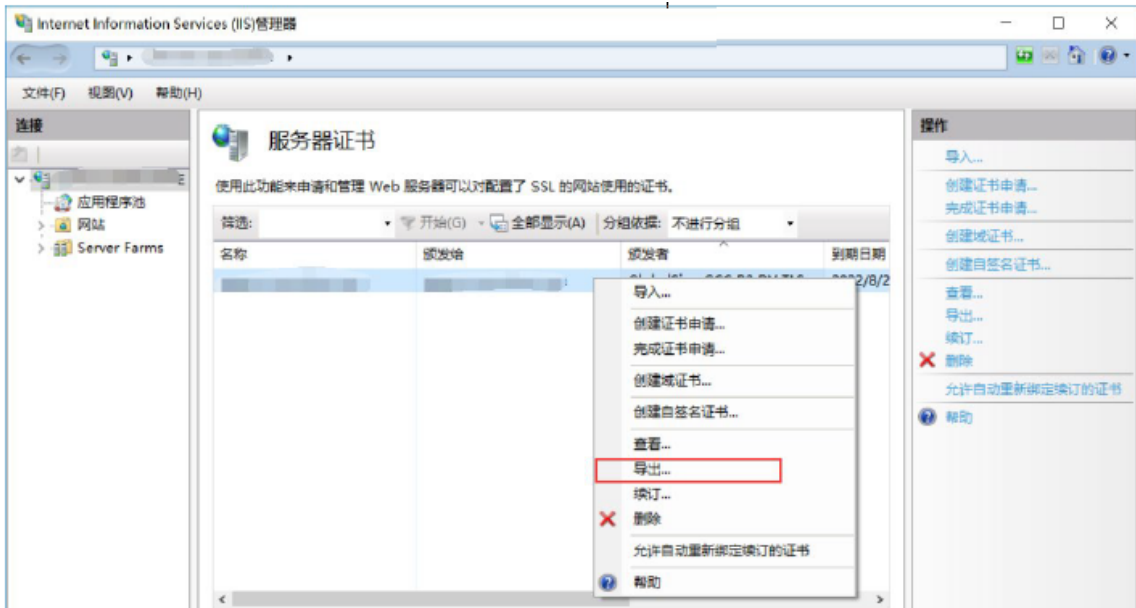
在您成功安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您带来不便。

(1) 服务器证书的备份

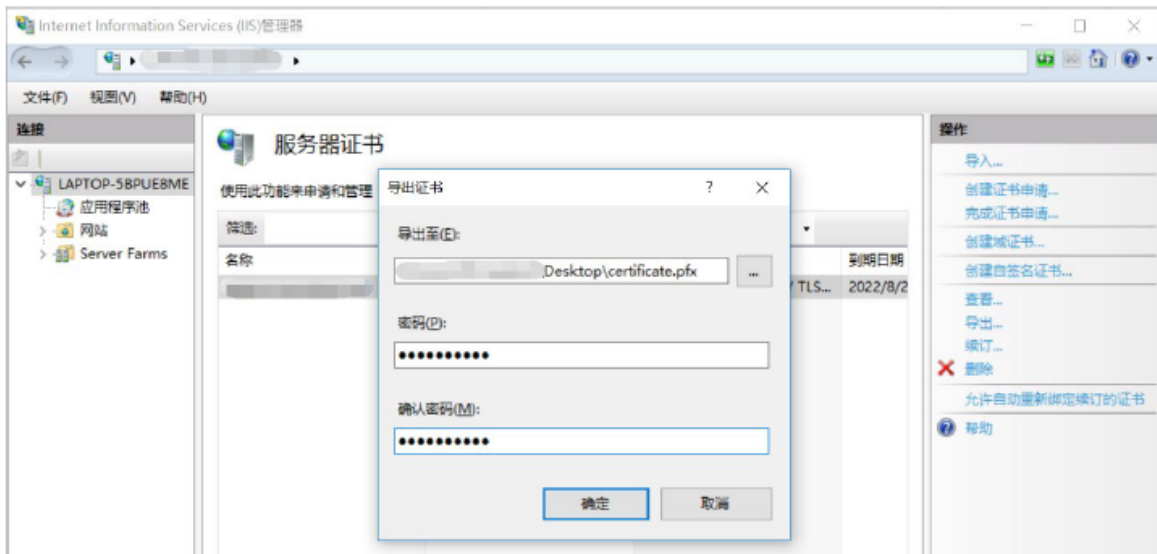
进入 IIS 管理控制台，并选择“服务器证书”



选中您的服务器证书项目，并右键选择“导出”



输入导出的密钥文件名、存储路径，并为导出的 pfx 格式证书备份文件设置保护密码。

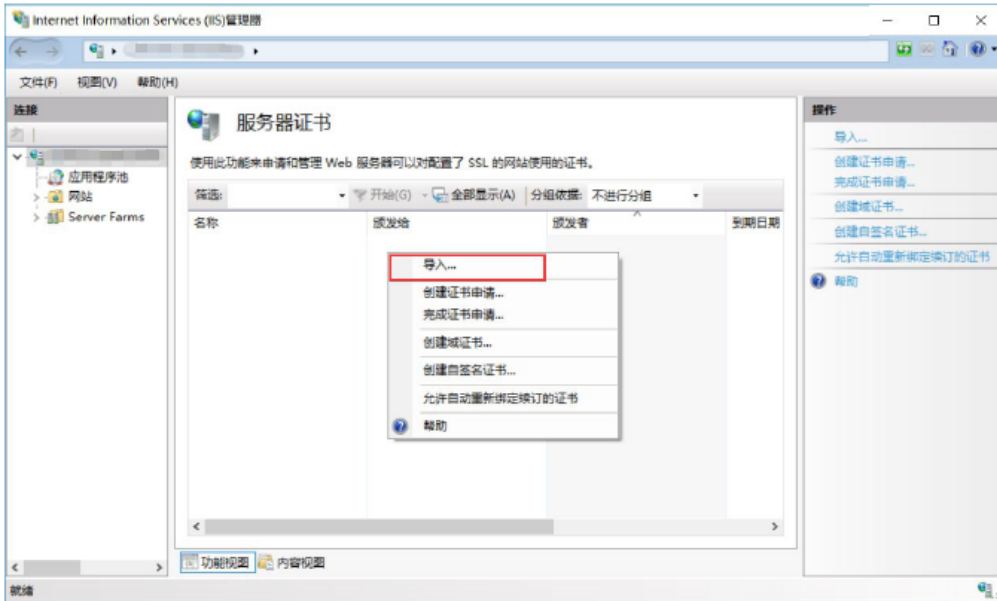


保

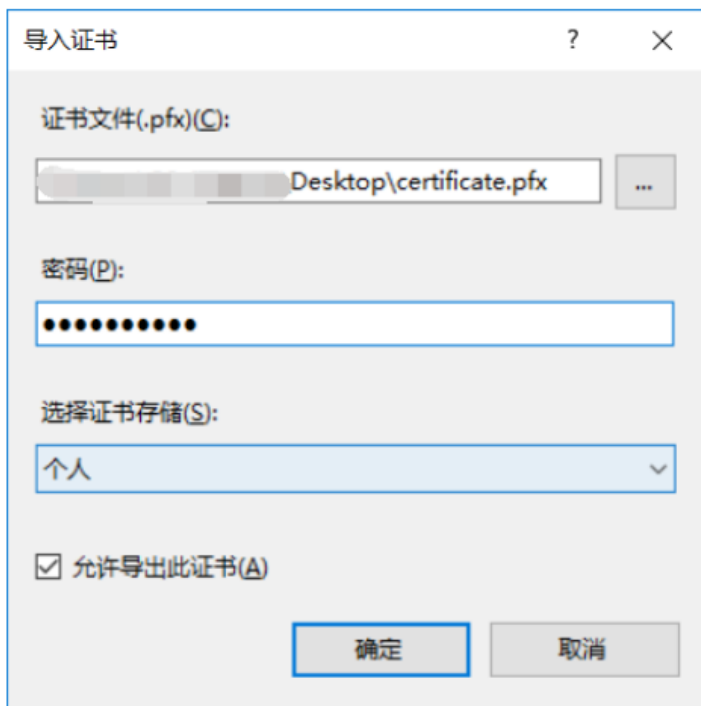
存好备份的 pfx 文件即可完成备份操作。

(2) 服务器证书的恢复

进入 IIS 管理控制台的服务器证书管理页面，右键选择“导入”



选择您的证书备份文件，并输入文件保护密码。



如果选中“标志此密钥为可导出”则您稍后可以将私钥从该服务器导出。不选中此选项时，密钥将无法从当前服务器中导出。参考服务器证书安装部分内容，恢复对导入的证书配置操作。

请注意，此文档会不定期更新！

GlobalSign China Co., Ltd

环玺信息科技（上海）有限公司

2021年 1 月