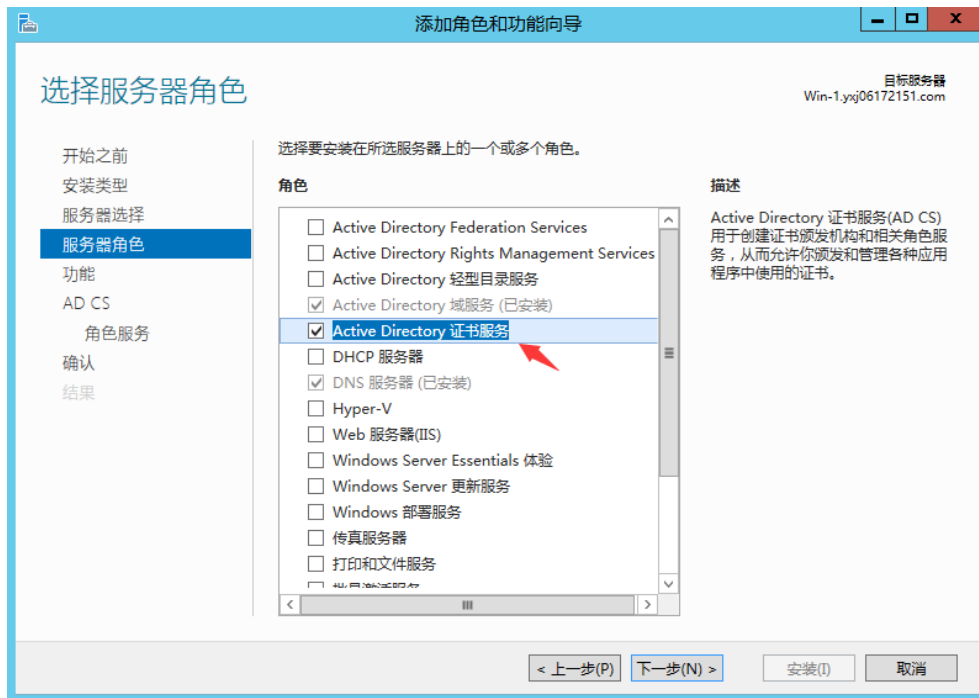


0x01 证书服务安装

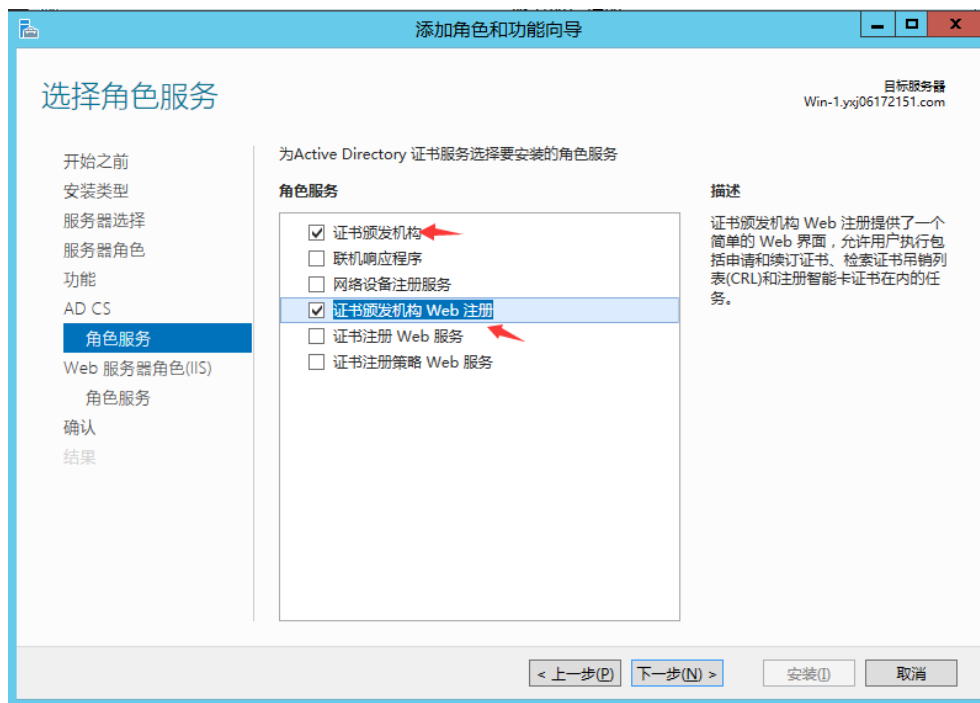
(1) 选择“添加角色和功能”：



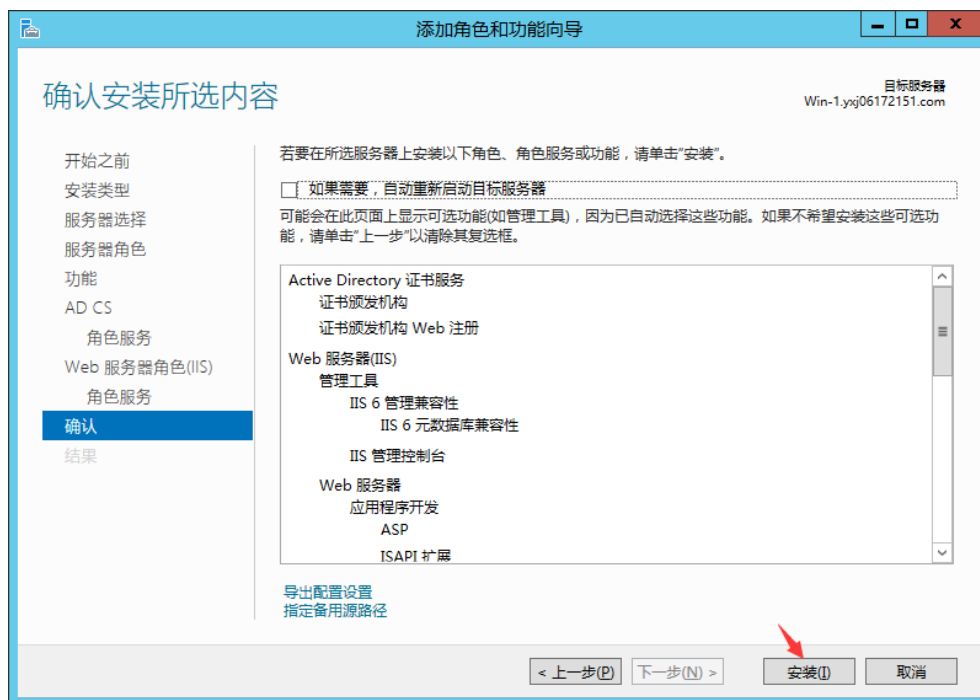
(2) 这一步勾选上“证书服务”，其他步骤默认选项即可：



(3) 选择“证书颁发机构”和“证书颁发机构 Web 注册”：



(4) 后续默认选项即可，点击“下一步”直至安装：

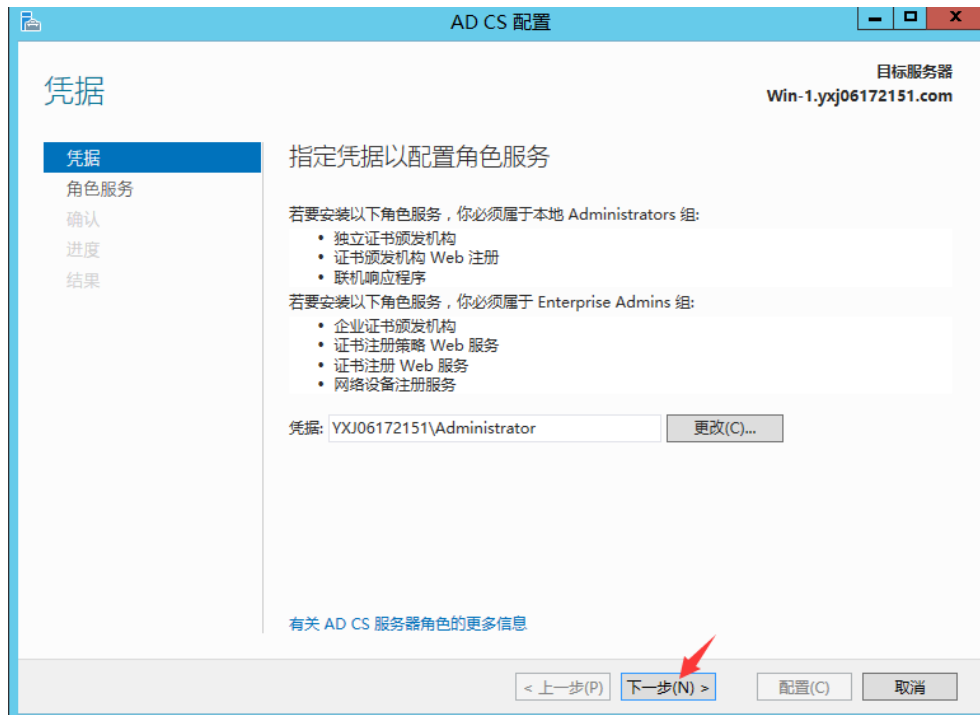


0x02 配置证书服务

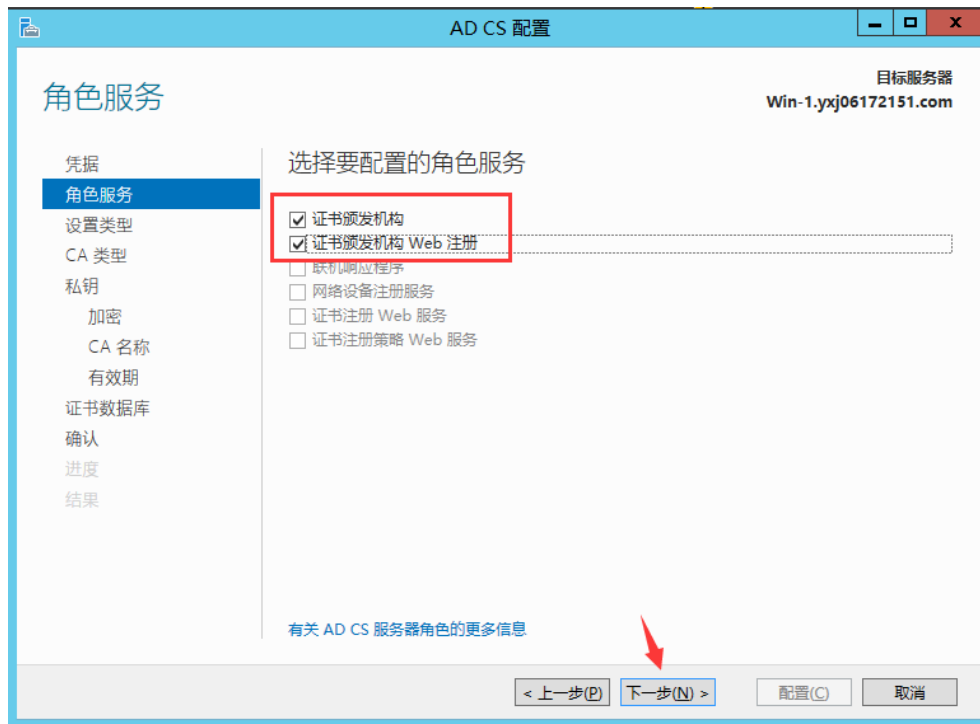
(1) 选择配置证书服务



默认即可：

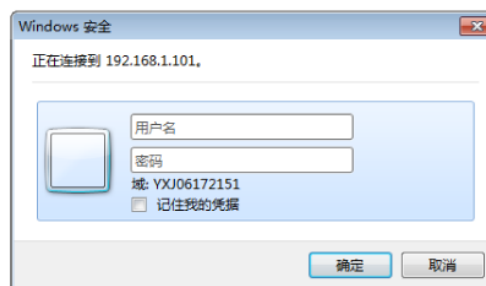
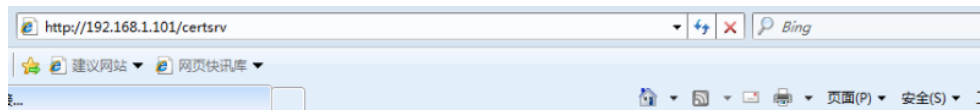


(2) 选择“证书颁发机构”、“证书颁发机构 Web 注册”，此步骤之后均使用默认选项即可：

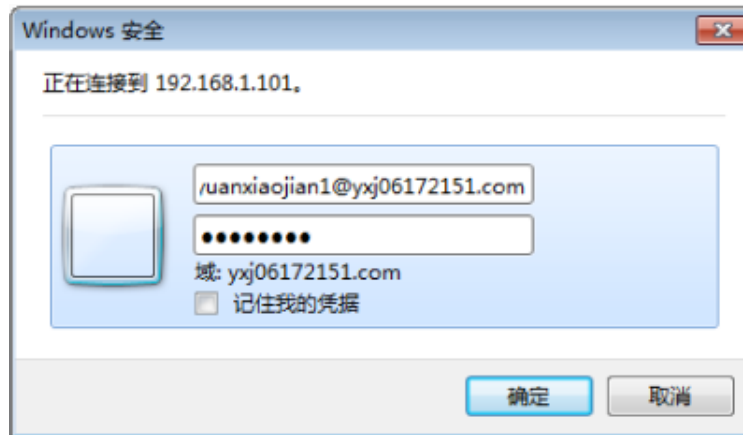


0x03 申请证书

(1) 在客户机上访问顶域的 <http://192.168.1.101/certsrv>



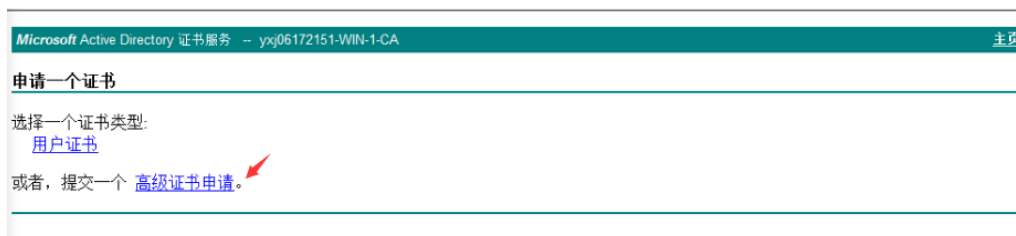
(2) 以一个域用户身份登录:



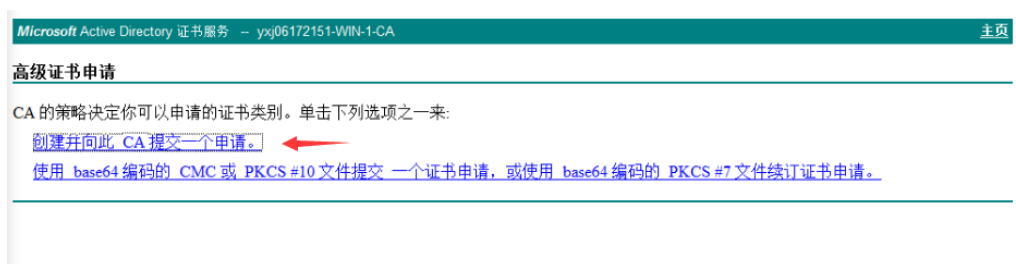
(3) 登陆后选择“申请证书”:



(4) 再选择“高级证书申请”:



(5) 选择向 CA 提交一个申请:



(6) 这里我们申请一个 EFS 恢复代理的证书，并填一个好记的名称：

高级证书申请

证书模板：
EFS 恢复代理

密钥选项：
☒ 创建新密钥集 ☐ 使用现存的密钥集
CSP: Microsoft Enhanced Cryptographic Provider v1.0
密钥用法: ☒ 交换
密钥大小: 1024 (最小值: 384 (一般密钥大小: 112 1024 2048 4096 8192 16384))
☒ 自动密钥容器名称 ☐ 用户指定的密钥容器名称
☒ 标记密钥为可导出
☐ 启用强私钥保护

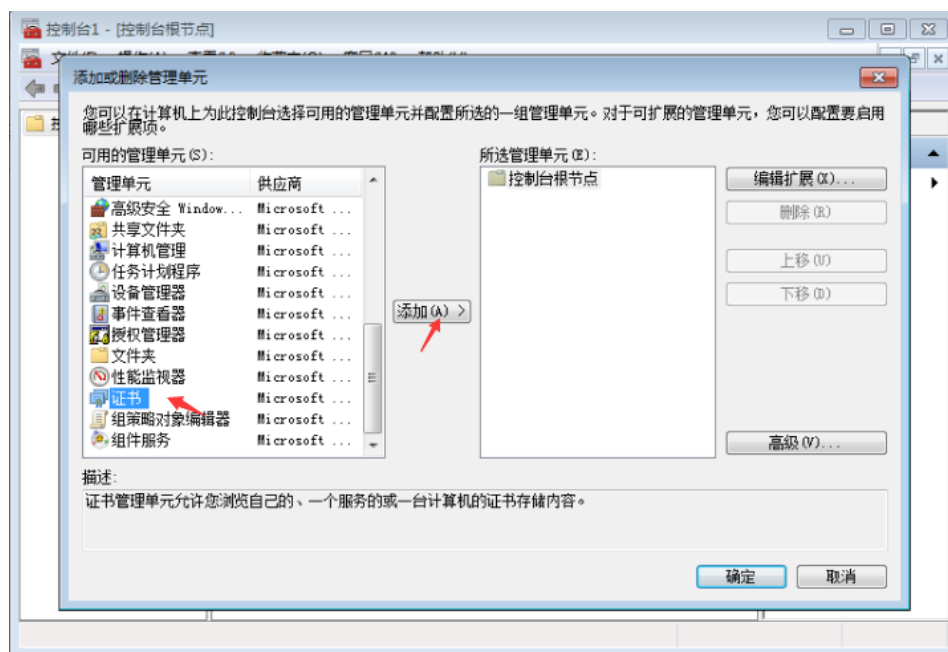
其他选项：
申请格式: ☒ CMC ☐ PKCS10
哈希算法: sha1 (仅用于申请签名)
☐ 保存申请
属性:
好记的名称: yuanyaojian

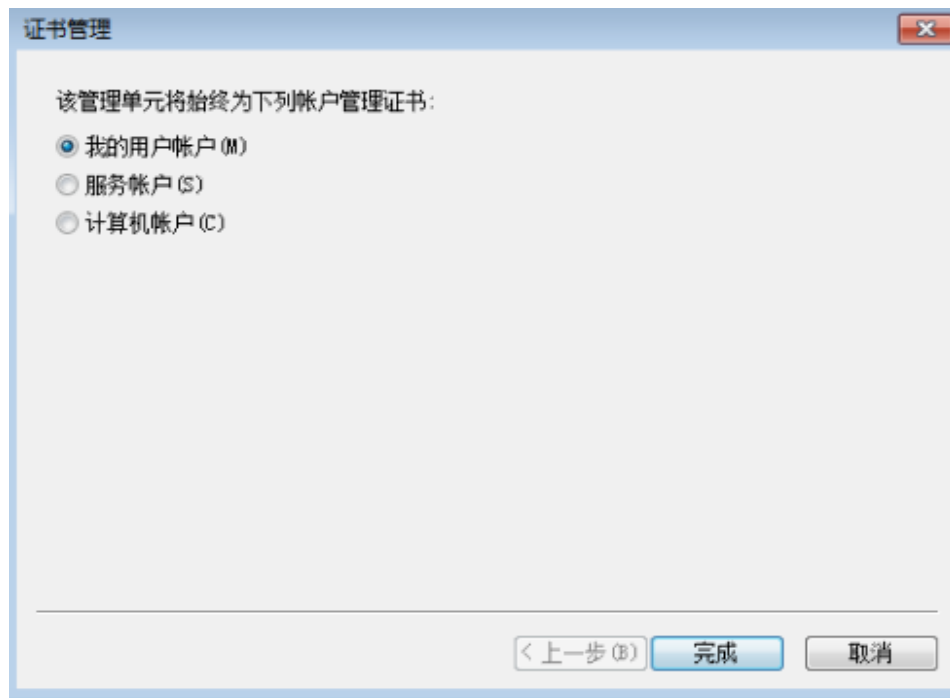
提交 >

(7) 提交后，选择“安装此证书”：



(8) 然后打开 mmc 控制台并添加证书管理单元：



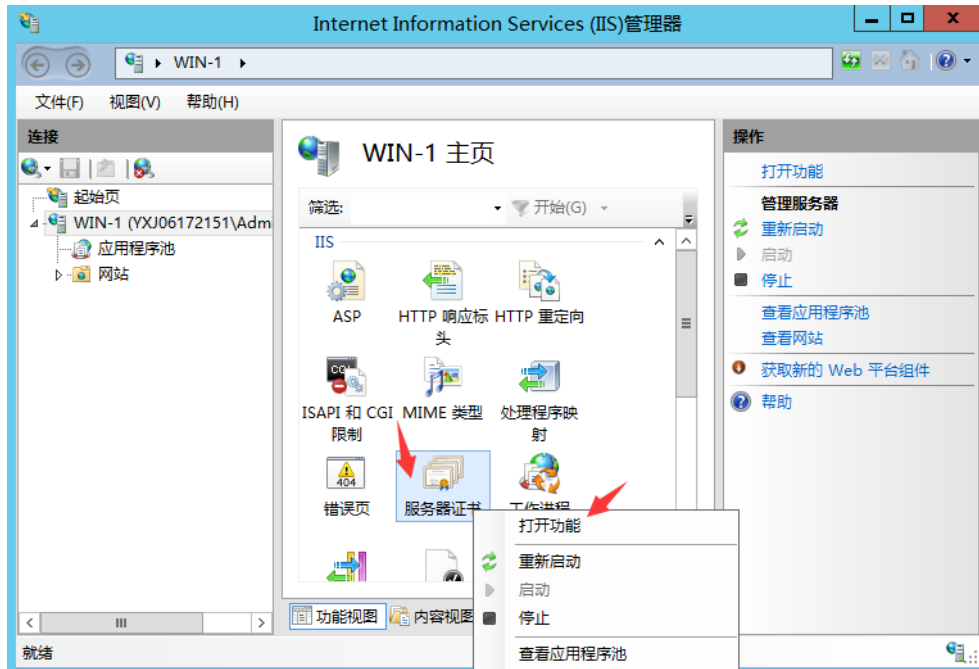


(9) 在证书管理单元中可以看到我们刚才申请的证书：

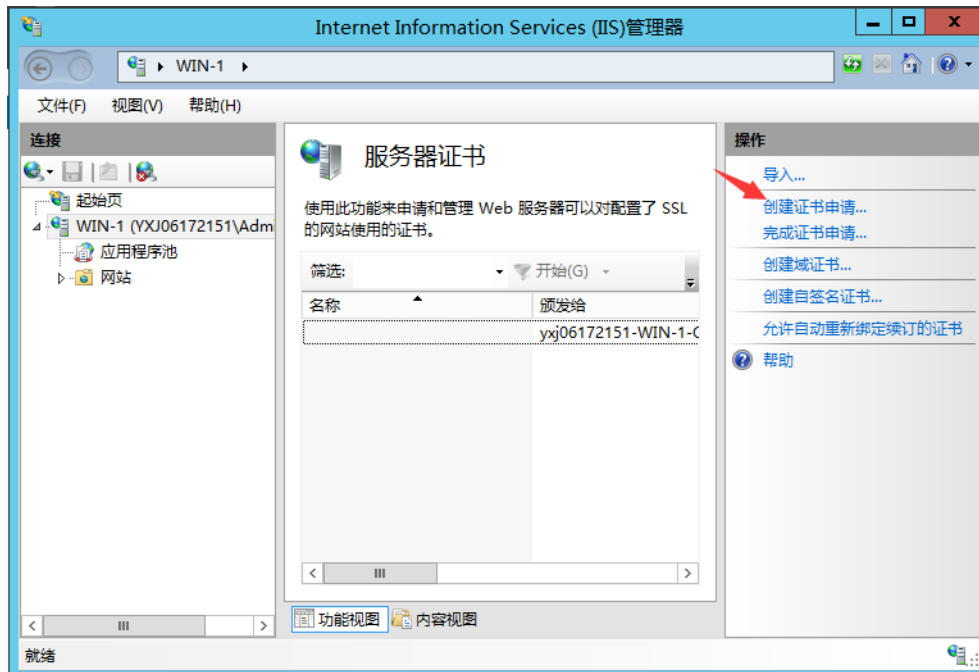


0x04 使用证书进行 https 通信

(1) 打开 IIS 服务器，并选择服务器证书：



(2) 选择“创建证书申请”：



(3) 填写相应信息:

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): yxj06172151

组织(O): CUMT

组织单位(U): CUMT

城市/地点(L): 徐州

省/市/自治区(S): 江苏

国家/地区(R): CN

上一页(P) 下一步(N) 完成(F) 取消

(4) 默认即可，下一步:

申请证书

加密服务提供程序属性

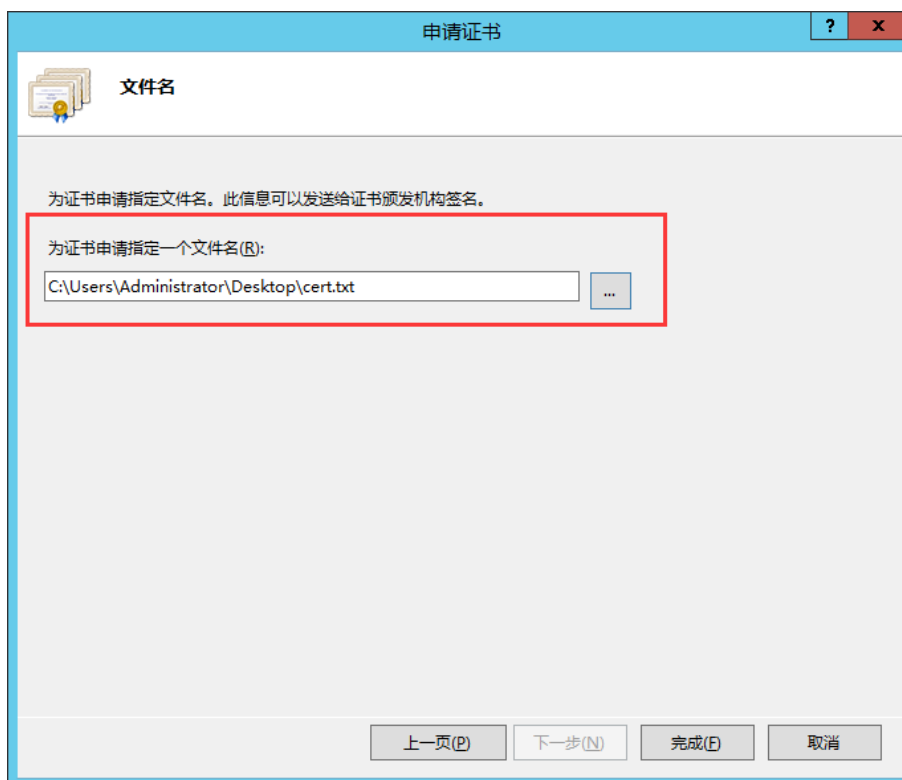
选择加密服务提供程序和位长。加密密钥的位长决定了证书的加密强度。位长越大，安全性越强，但较大的位长可能会降低性能。

加密服务提供程序(S): Microsoft RSA SChannel Cryptographic Provider

位长(B): 1024

上一页(P) 下一步(N) 完成(F) 取消

(5) 输入文件名:



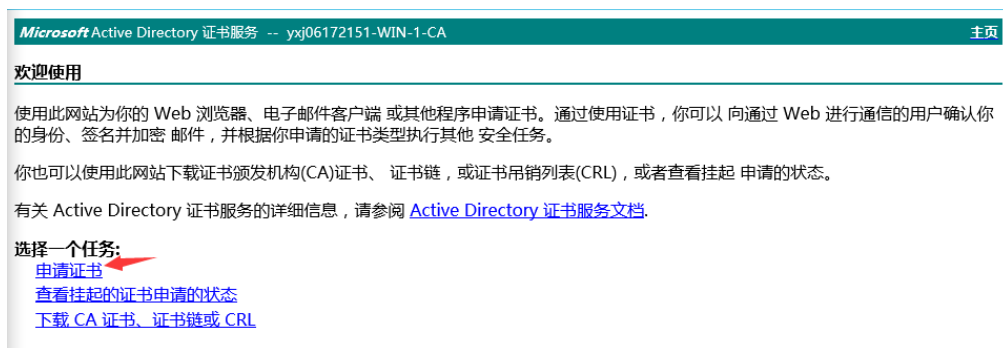
(6) 打开申请的证书，复制文件内容:



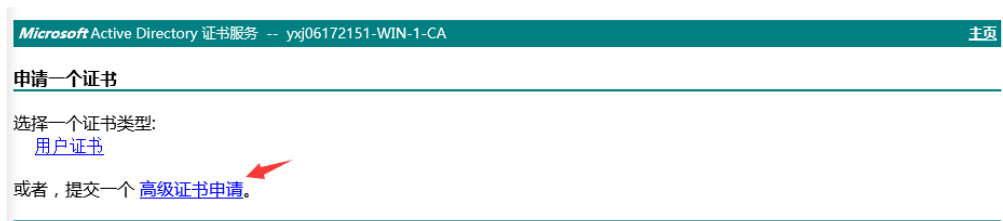
(7) 访问 <http://192.168.1.101/certsrv>，并以一个域用户身份登录：



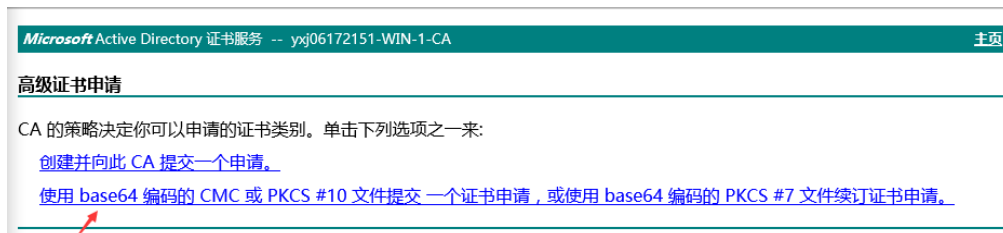
(8) 登陆后选择“申请证书”：



(9) 再选择“高级证书申请”：



(10) 然后使用 base64 编码申请：



(11) 将前面步骤复制的证书内容粘贴进来，证书模板可以选择 Web 服务器:

Microsoft Active Directory 证书服务 -- yxj06172151-WIN-1-CA 主页

提交一个证书申请或续订申请

要提交一个保存的申请到 CA，在“保存的申请”框中粘贴一个由外部源(如 Web 服务器)生成的 base-64 编码的 CMC 或 PKCS #10 证书申请或 PKCS #7 续订申请。

保存的申请:

Base-64 编码的证书申请 (CMC 或 PKCS #10 或 PKCS #7):

```
MAeGcWCGSAFlAwQBLTALBg1ghkgBZQMEASQIwCwYJ
MAeGCCqGSIb3DQMHMB0GA1UdDgQWBBSMScnQR1IB
hkiG9w0BAQUFAAOBgQBop51Etprn7uOx9QX+LGVe
E8mq554bQBYW1e0oW7Rp7NQe7jL1C9Ybdl161V3g
jMjVTvLy2pqF2N0ie6zJazI112WgCxBHNBklQ5p30\
-----END NEW CERTIFICATE REQUEST-----
```

证书模板:

Web 服务器

附加属性:

属性:

[提交 >](#)

(12) 提交后，选择下载证书将证书下载到本地:

Microsoft Active Directory 证书服务 -- yxj06172151-WIN-1-CA 主页

证书已颁发

你申请的证书已颁发给你。

☒ DER 编码 或 ☐ Base 64 编码

[下载证书](#) [下载证书链](#)

(13) 然后再打开 IIS 管理器，完成证书申请:

文件(F) 视图(V) 帮助(H)

服务器证书

使用此功能来申请和管理 Web 服务器可以对配置了 SSL 的网站使用的证书。

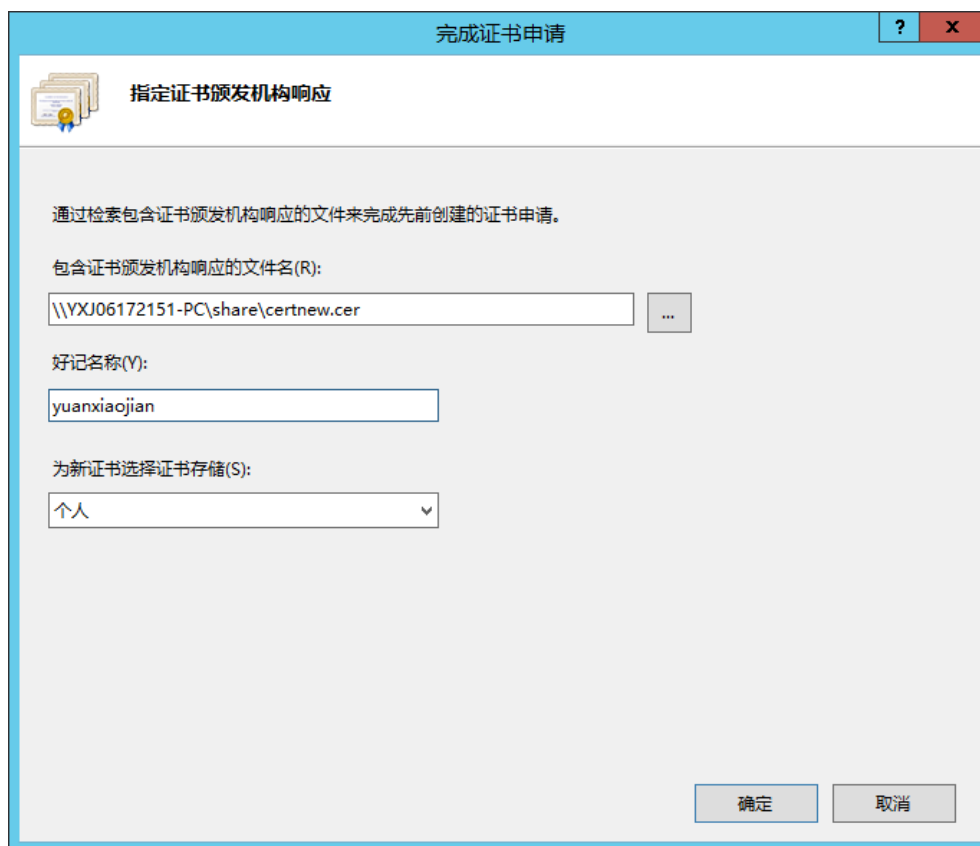
筛选: 开始(G) 全部显示(A) 分组依据:

名称	颁发给	颁发者
	Win-1.yxj06172151.com	yxj06172151-WIN-1-CA
	yxj06172151-WIN-1-CA	yxj06172151-WIN-1-CA

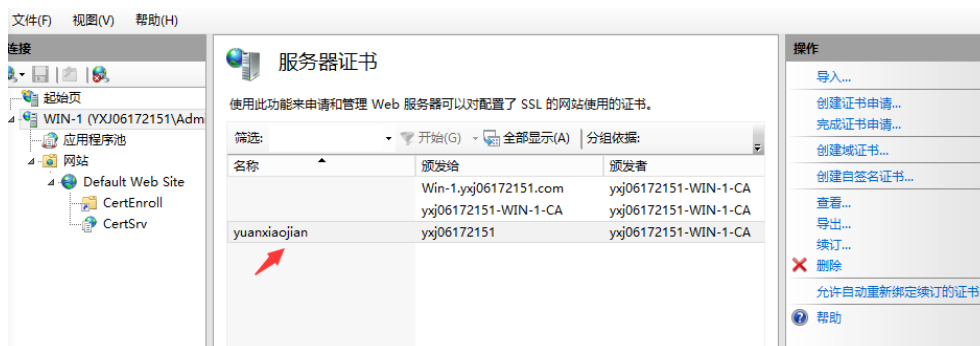
操作

- 导入...
- 创建证书申请...
- 完成证书申请...
- 创建域证书...
- 创建自签名证书...
- 允许自动重新绑定续订的证书
- 帮助

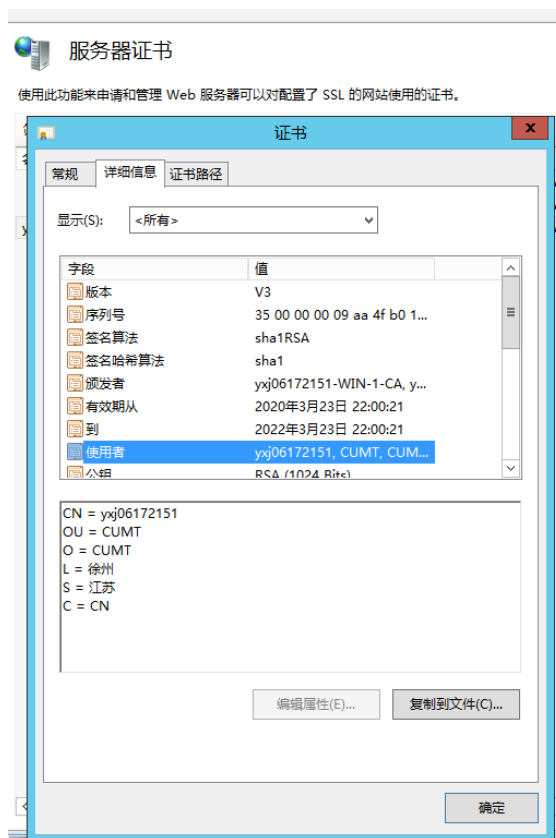
(14) 导入刚才下载下来的证书:



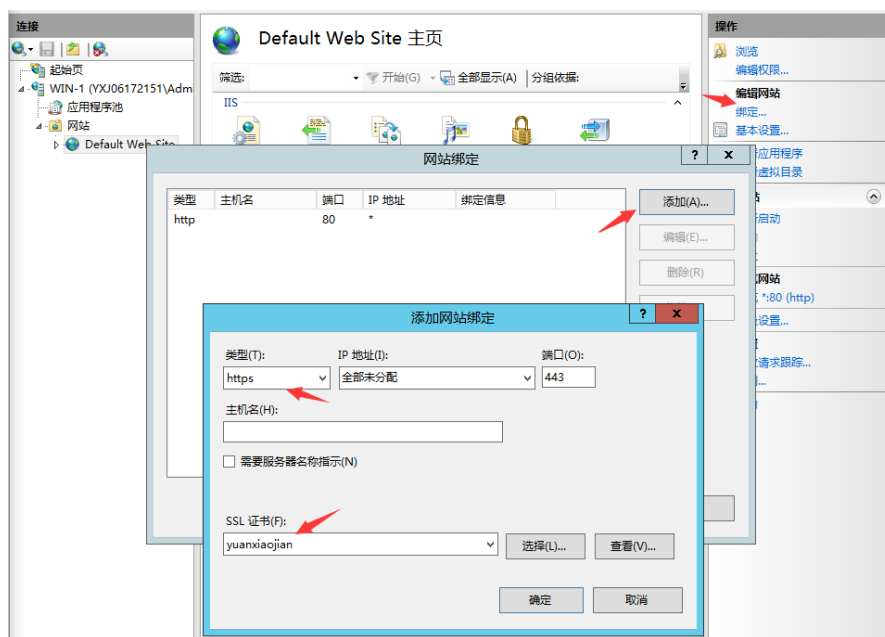
(15) 确定后可以看到证书服务器中多了一个证书:



(16) 查看该证书为刚才创建的证书：



(17) 然后选择“绑定”，然后“添加”，选择 https 类型，并将 SSL 证书选择为我们刚才创建的证书：



(18) 然后我们尝试访问 https://localhost 如下：



(19) 可以看到使用的证书即为我们刚才创建的证书：

