Aruba 集成 Windows NPS 实现 802.1X 认证

北京力尊信通科技股份有限公司

lilei@holyzone.com.cn 李磊

目　　录

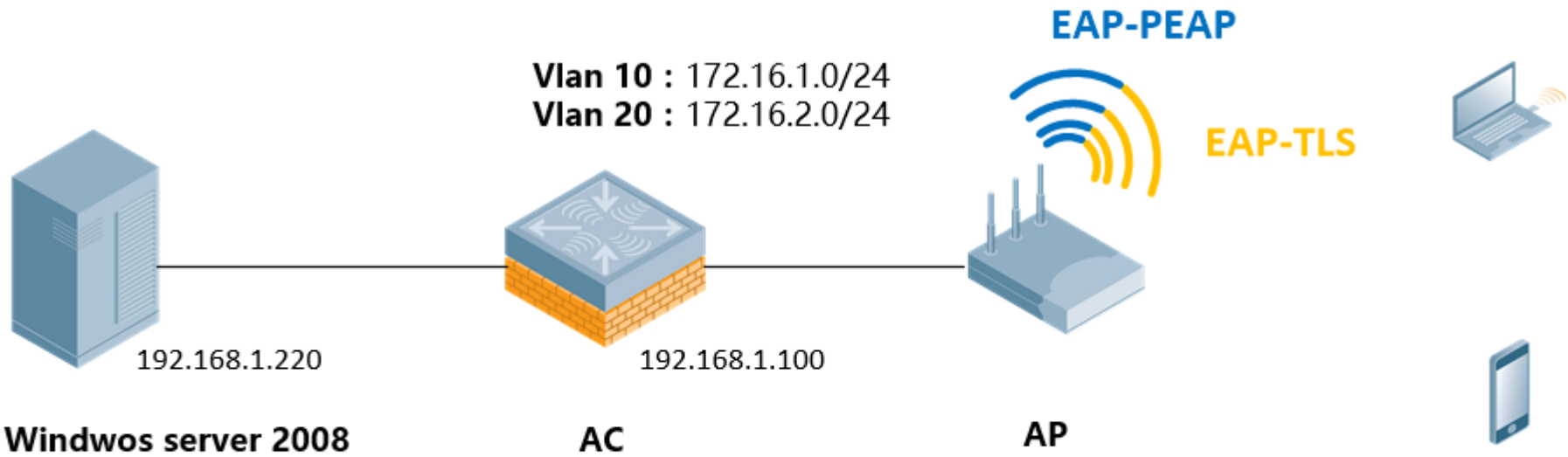
802.1X 认证是企业在部署无线网络时首选的无线认证方式，部署 802.1X 认证必须要有 RAIDUS 服务器，如果企业中没有 RAIDUS 服务器，可以选择购买 Aruba ClearPass 产品，也可以选择 Windows NPS 作为 RADIUS 服务器，使用企业员工的 AD 账号来进行认证。

本文章将详细讲解如何一步一步配置 Aruba 无线控制器集成 Windows NPS 来实现 802.1X 认证。

802.1X 认证的 EAP 类型有多种，通常在企业中最常见的就两种类型：

- **EAP-PEAPv0（PEAP-MSCHAPv2）：**使用用户名/密码方式认证无线客户端
- **EAP-TLS：**使用用户证书认证无线客户端

本手册基于的网络拓扑环境如下：



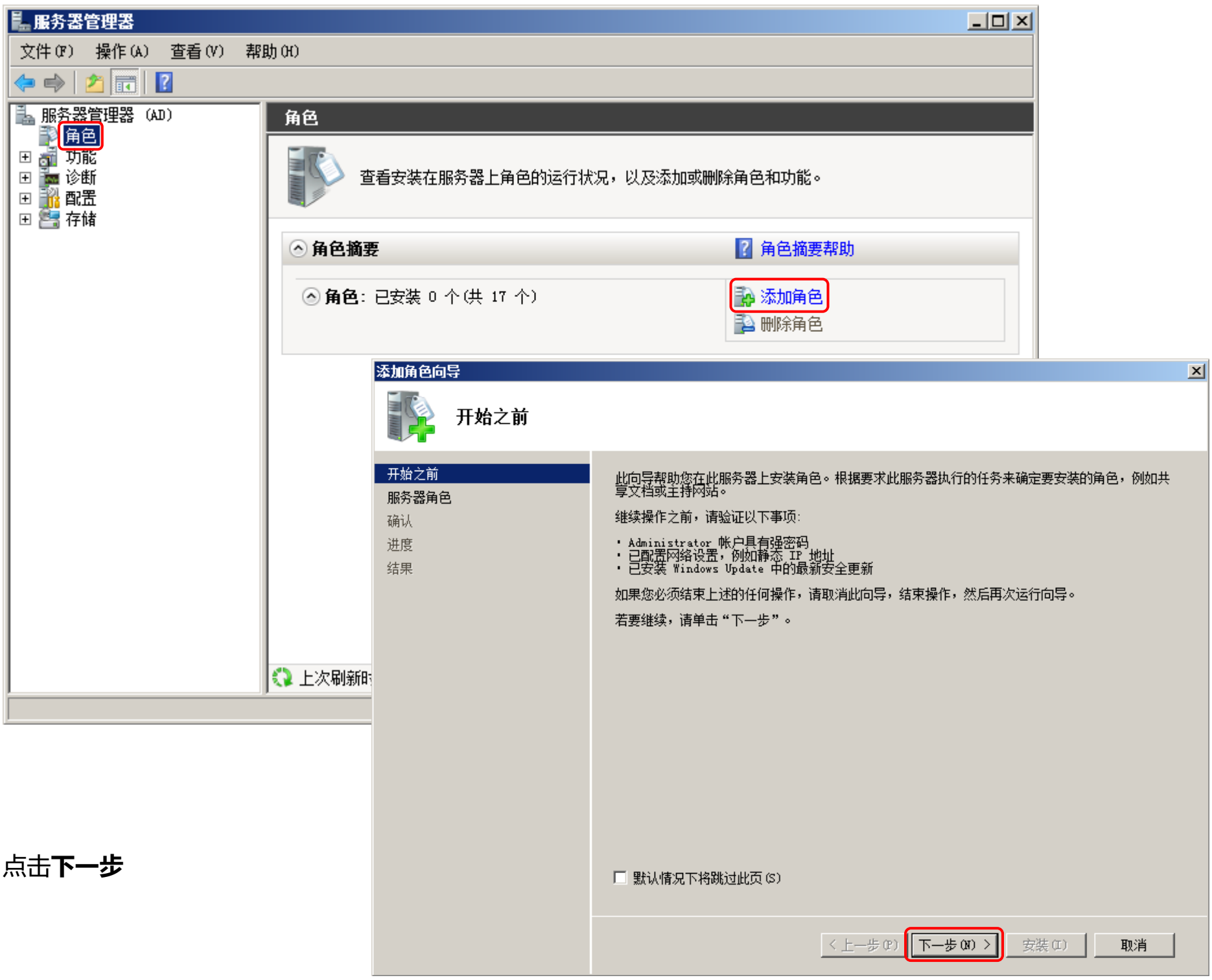
1. 配置 Windows Server 2008

Windows Server 2008 执行以下功能：

- **Domain Controller（DC）**：域控制器；
- **Active Directory（AD）**：存储用户账号，作为认证的用户数据库；
- **DNS**：安装域控制器必须安装 DNS 服务器；
- **Certificate Services**：安装证书服务在服务器上，服务器作为根 CA，为服务器颁发计算机证书，为无线客户端颁发用户证书；
- **IIS**：Web 服务器，无线客户端可以通过浏览器申请用户证书；
- **NPS**：RADIUS 服务器，网络接入策略；

1.1 安装 AD+DC+DNS

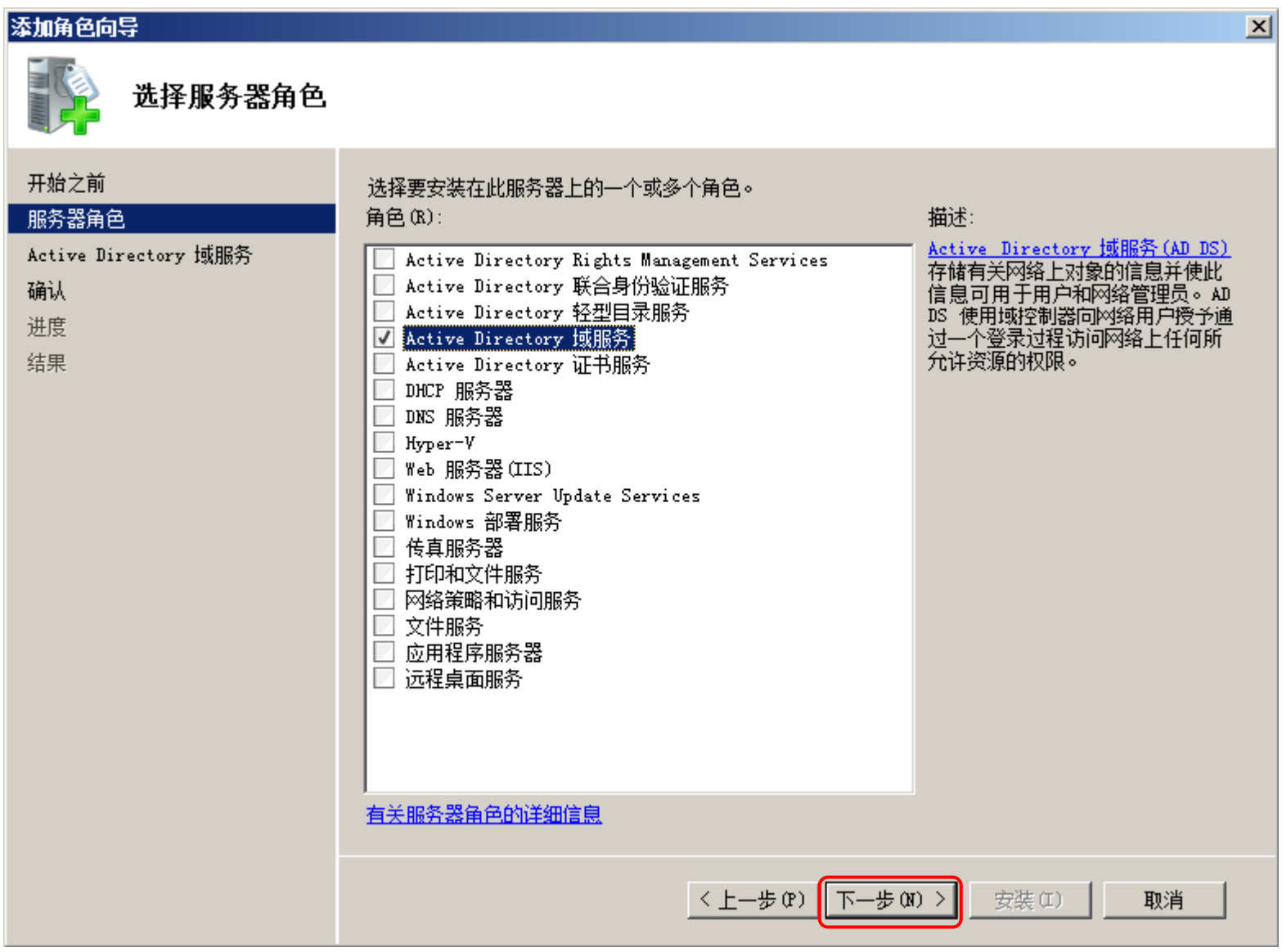
点击**服务器管理器** > **角色** > **添加角色**



点击**下一步**

选中 **Active Directory 域服务**，点击**添加必需的功能**

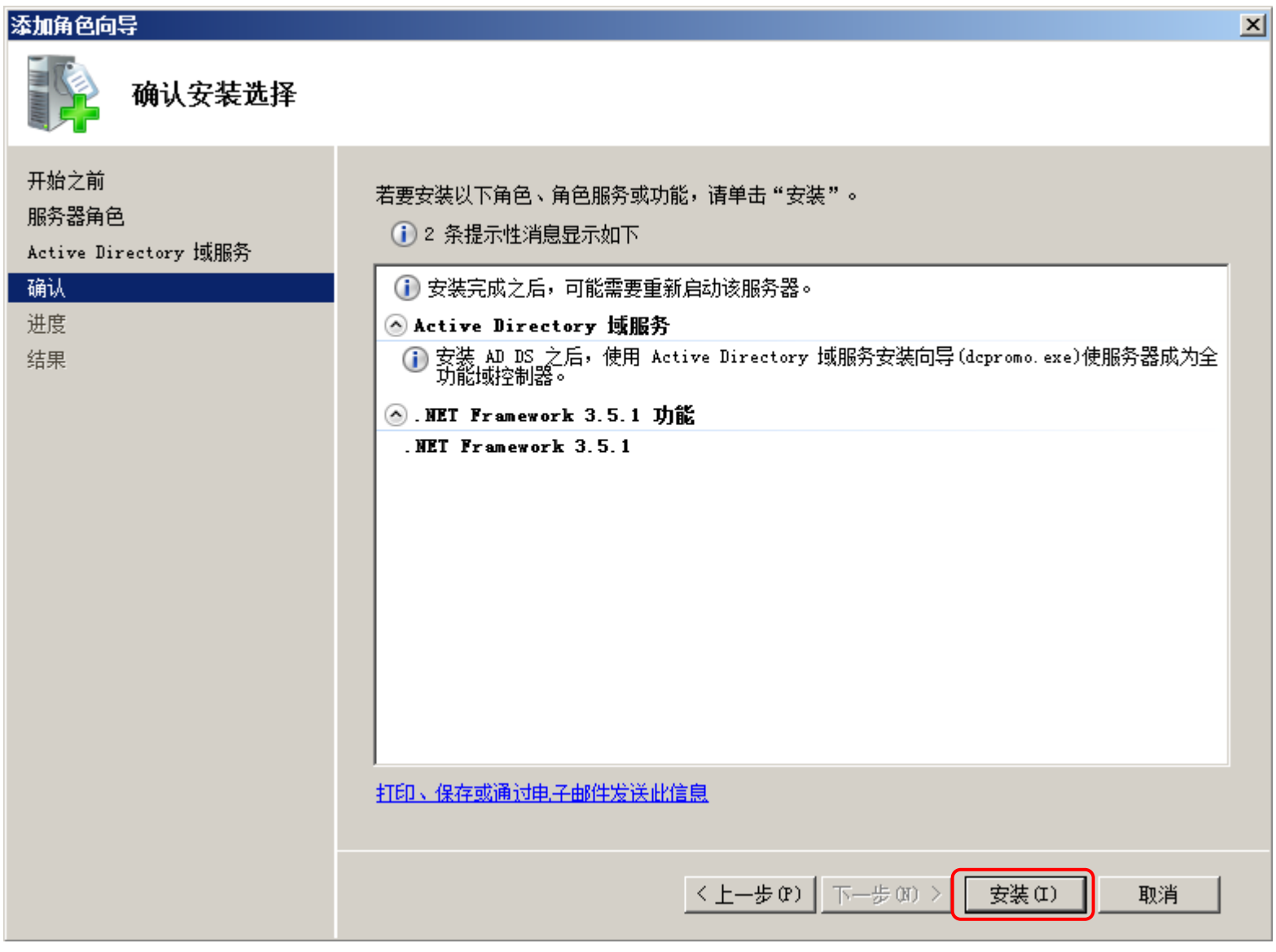
点击**下一步**



点击**下一步**

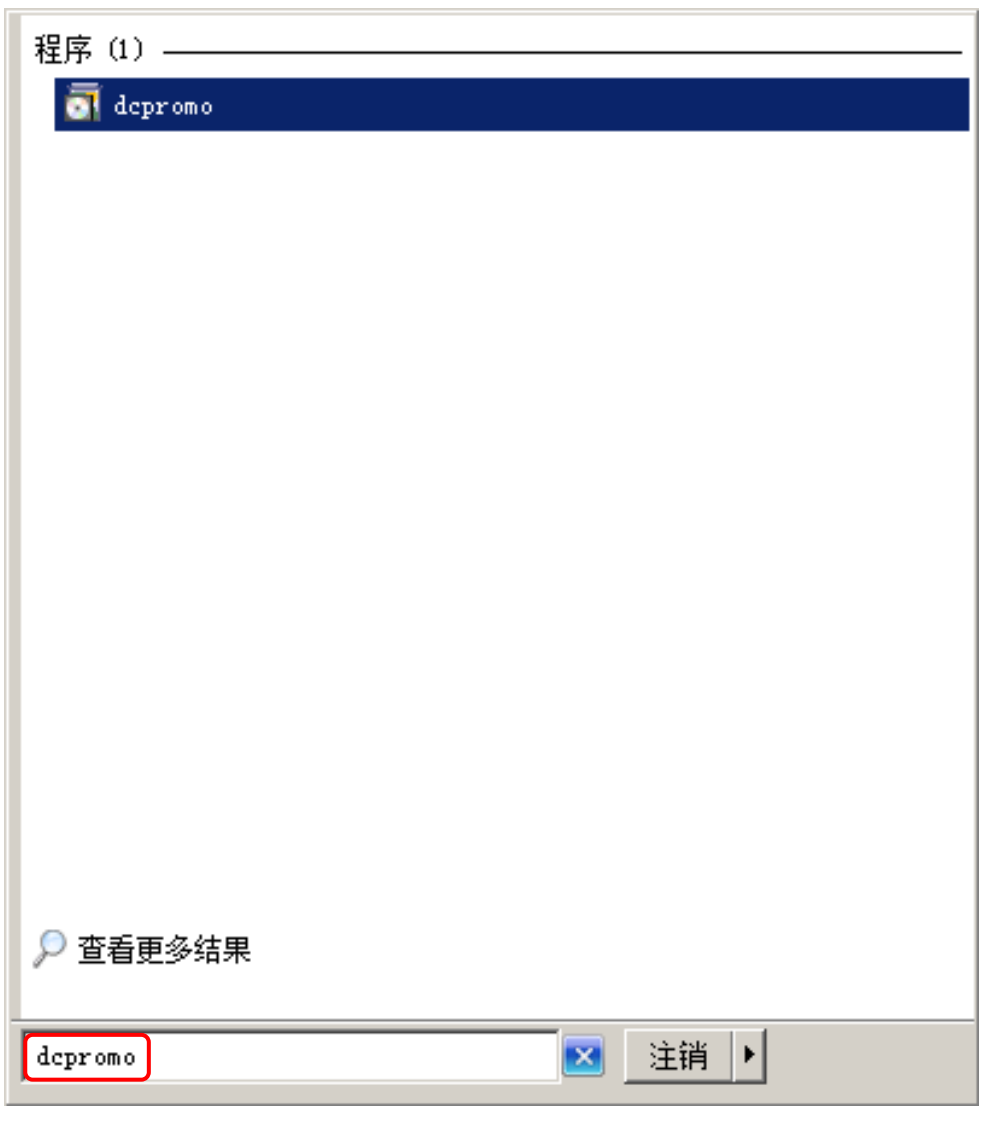

添加角色向导
Active Directory 域服务
开始之前
服务器角色
Active Directory 域服务
确认
进度
结果
Active Directory 域服务简介
Active Directory 域服务(AD DS)存储有关网络上的用户、计算机和其他设备的信息。AD DS 有助于管理员安全地管理该信息，并有助于用户间的资源共享和协作。启用目录的应用程序(例如 Microsoft Exchange Server)和其他 Windows 服务器技术(例如组策略)也需要 AD DS。
注意事项
若要有助于确保在某台服务器中断的情况下用户仍然可以登录到网络，请至少为域安装两个域控制器。
AD DS 要求将 DNS 服务器安装在网络上。如果未安装 DNS，系统会提示您在该服务器上安装 DNS 服务器角色。
安装 AD DS 之后，使用 Active Directory 域服务安装向导(dcpromo.exe)使服务器成为全功能域控制器。
安装 AD DS 将会同时安装目录服务所需的 DFS 命名空间、DFS 复制和文件复制服务。
其他信息
AD DS 概述
安装 AD DS
AD DS 的常见配置
< 上一步(P)
下一步(N) >
安装(I)
取消

点击**安装**

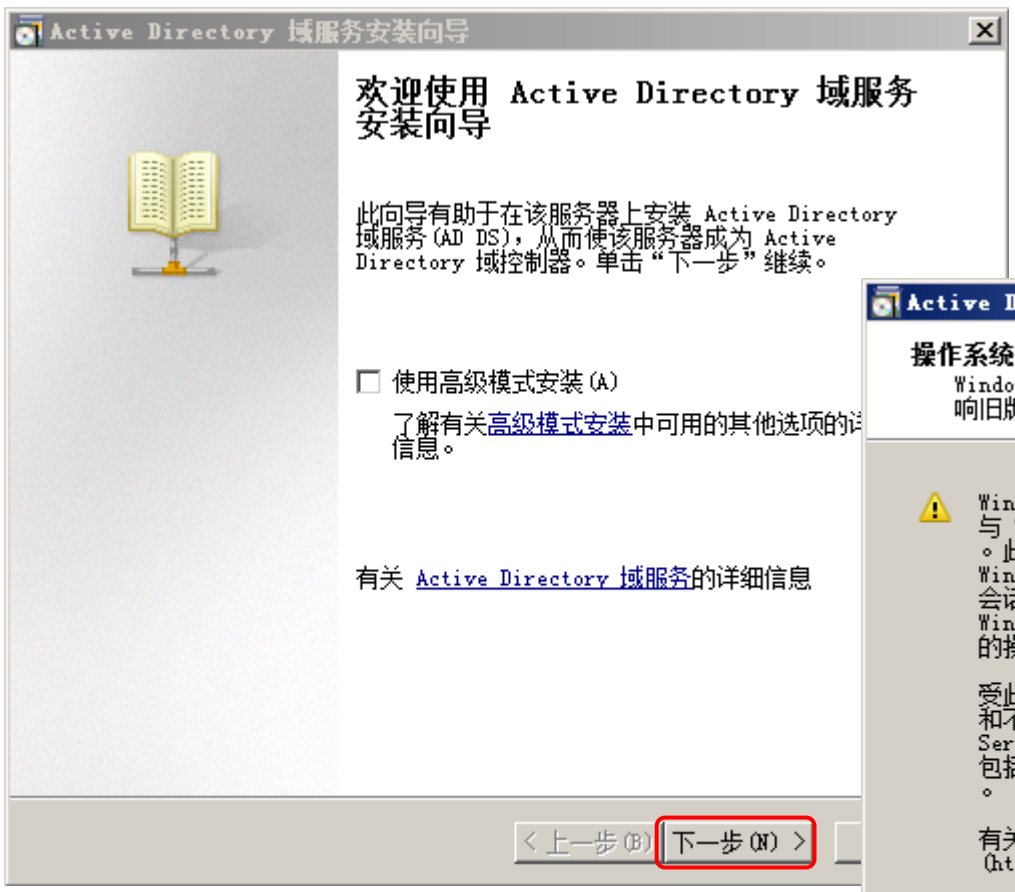

添加角色向导
确认安装选择
开始之前
服务器角色
Active Directory 域服务
确认
进度
结果
若要安装以下角色、角色服务或功能，请单击“安装”。
2 条提示性消息显示如下
安装完成之后，可能需要重新启动该服务器。
Active Directory 域服务
安装 AD DS 之后，使用 Active Directory 域服务安装向导(dcpromo.exe)使服务器成为全功能域控制器。
.NET Framework 3.5.1 功能
.NET Framework 3.5.1
打印、保存或通过电子邮件发送此信息
< 上一步(P)
下一步(N) >
安装(I)
取消

点击**关闭**，Active Directory 域服务安装完成

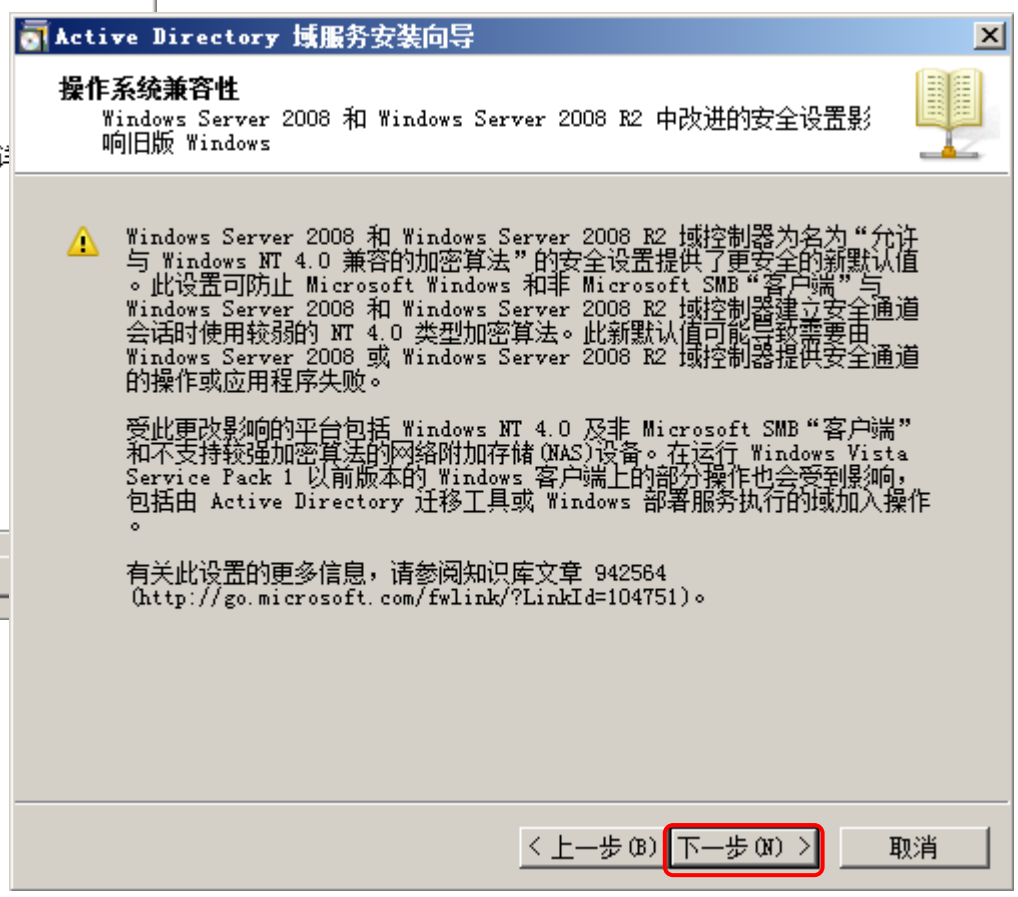
Active Directory 域服务安装完成之后，创建一个新的域，点击**开始** > 输入 **dcpromo**



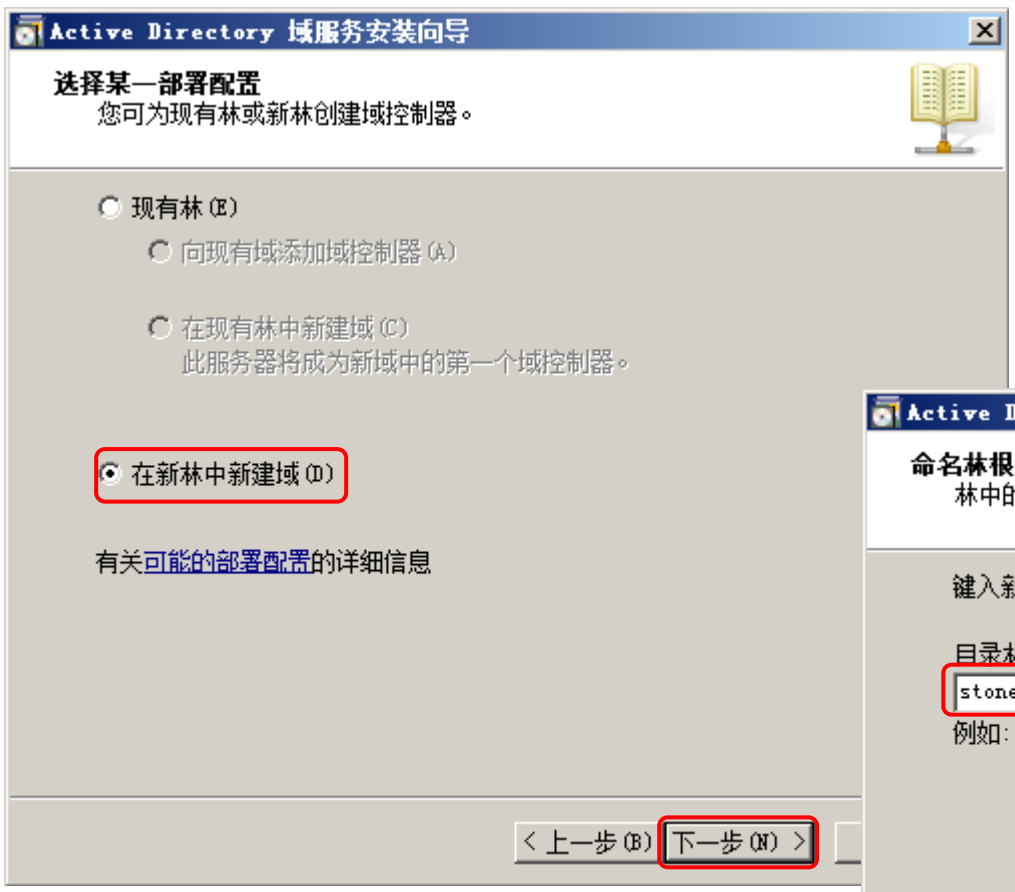
点击**下一步**



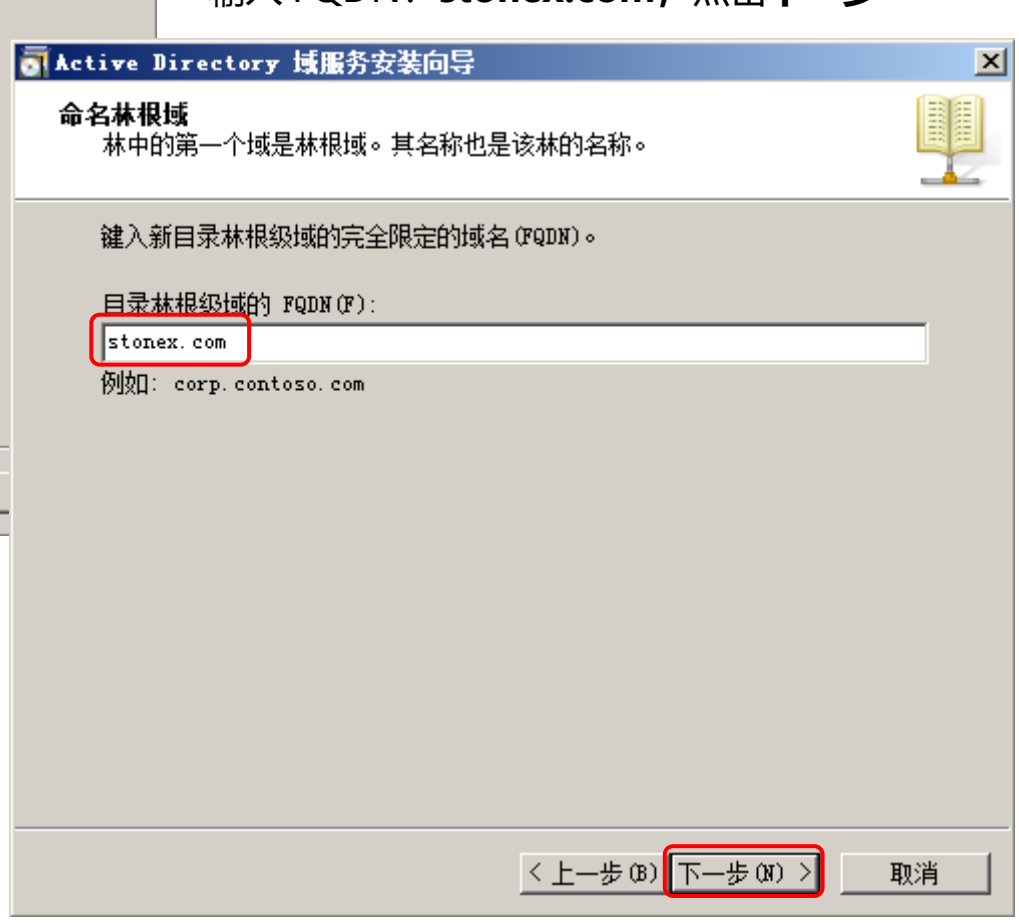
点击**下一步**



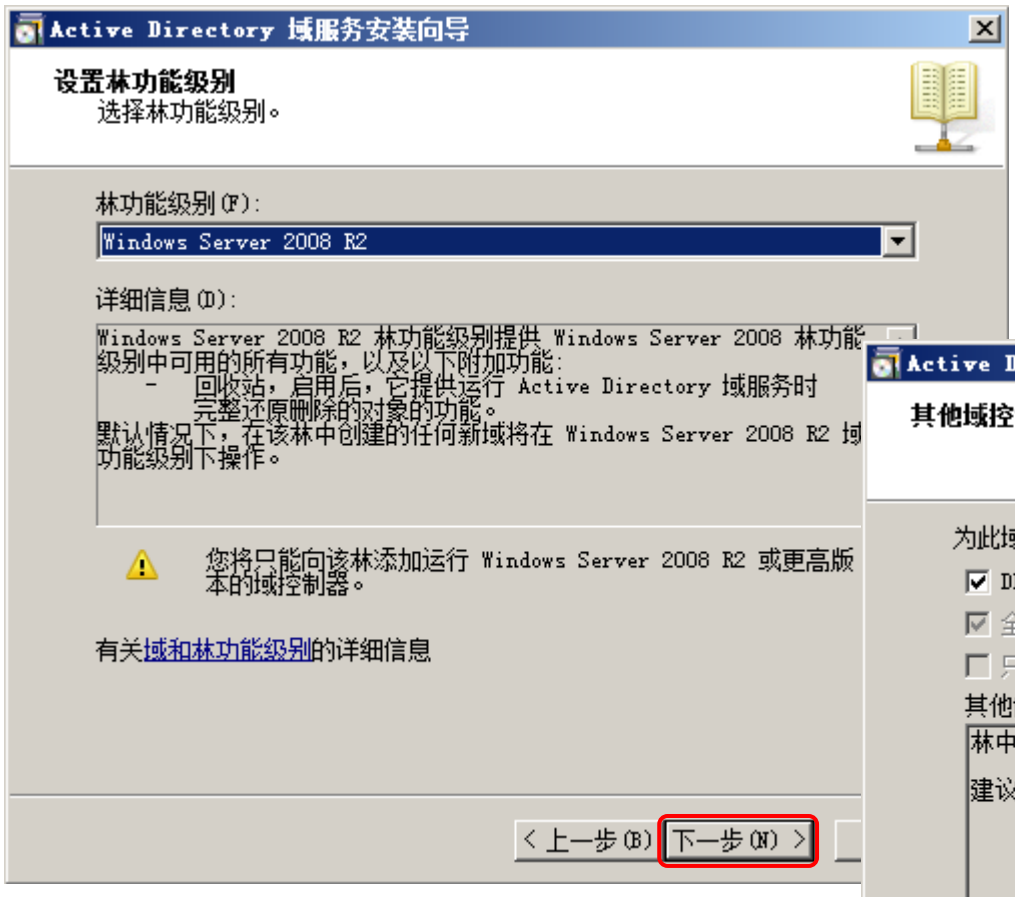
选择**在新林中新建域，**点击**下一步**



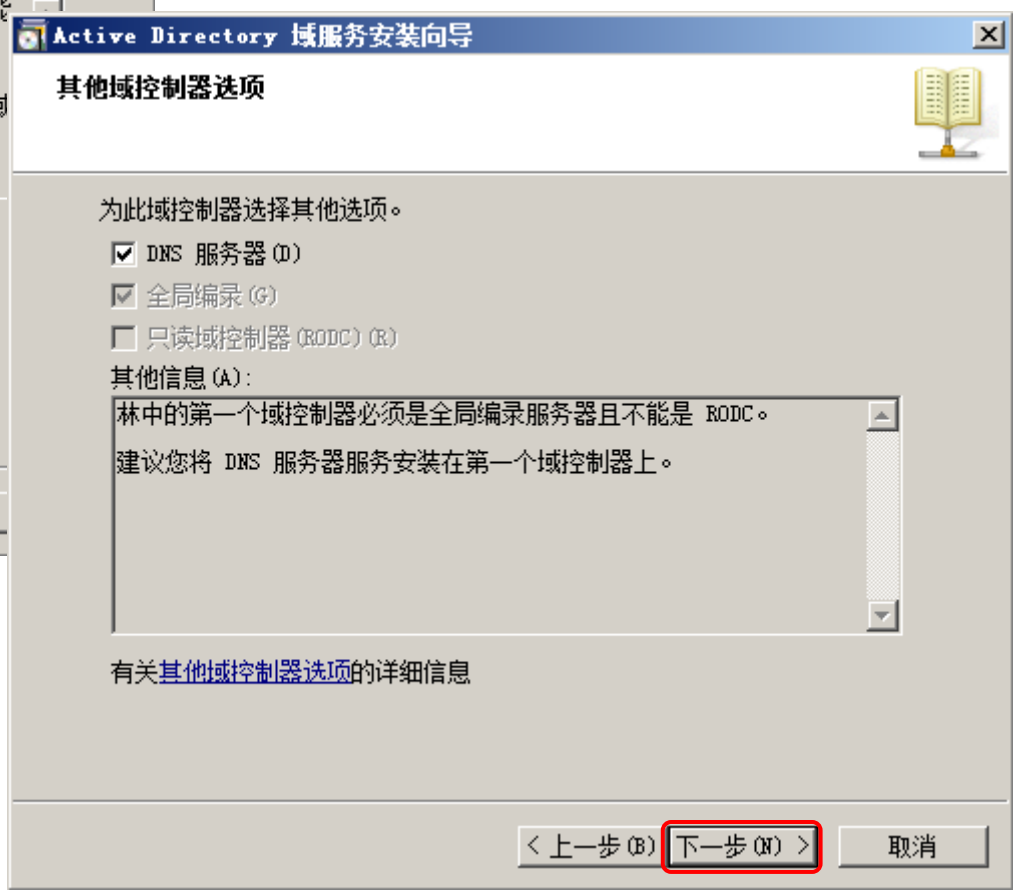
输入 FQDN：**stonex.com，**点击**下一步**



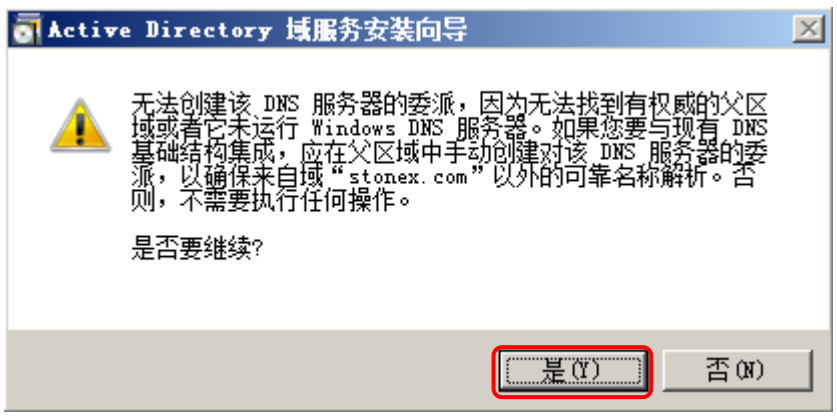
选择林功能级别，这里我选择 **Windows Server 2008 R2**，点击**下一步**



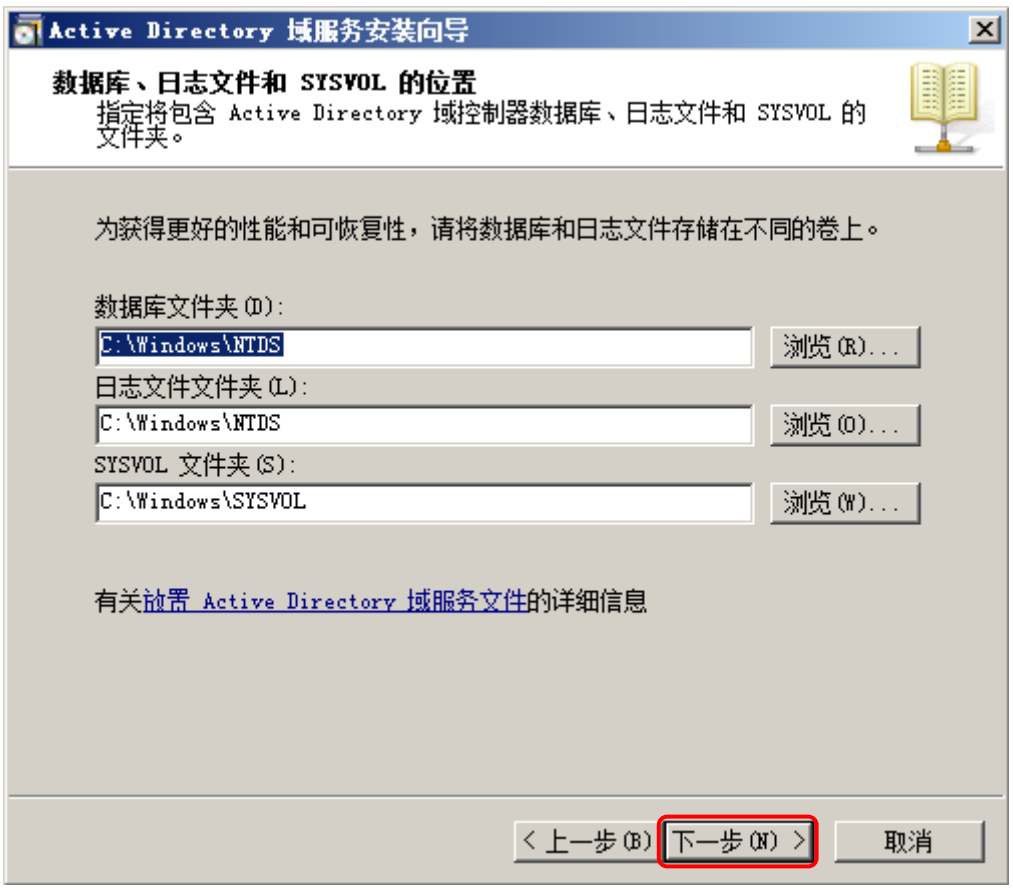
安装 DNS 服务器，点击**下一步**



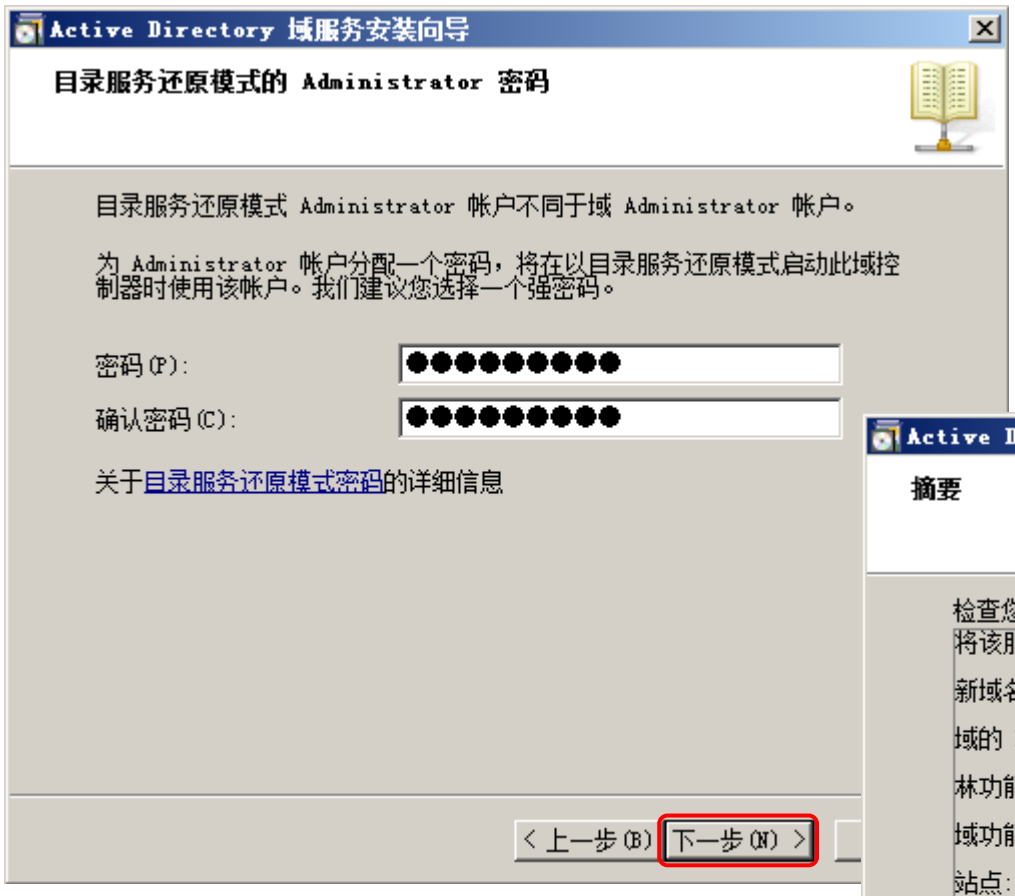
选择**是**



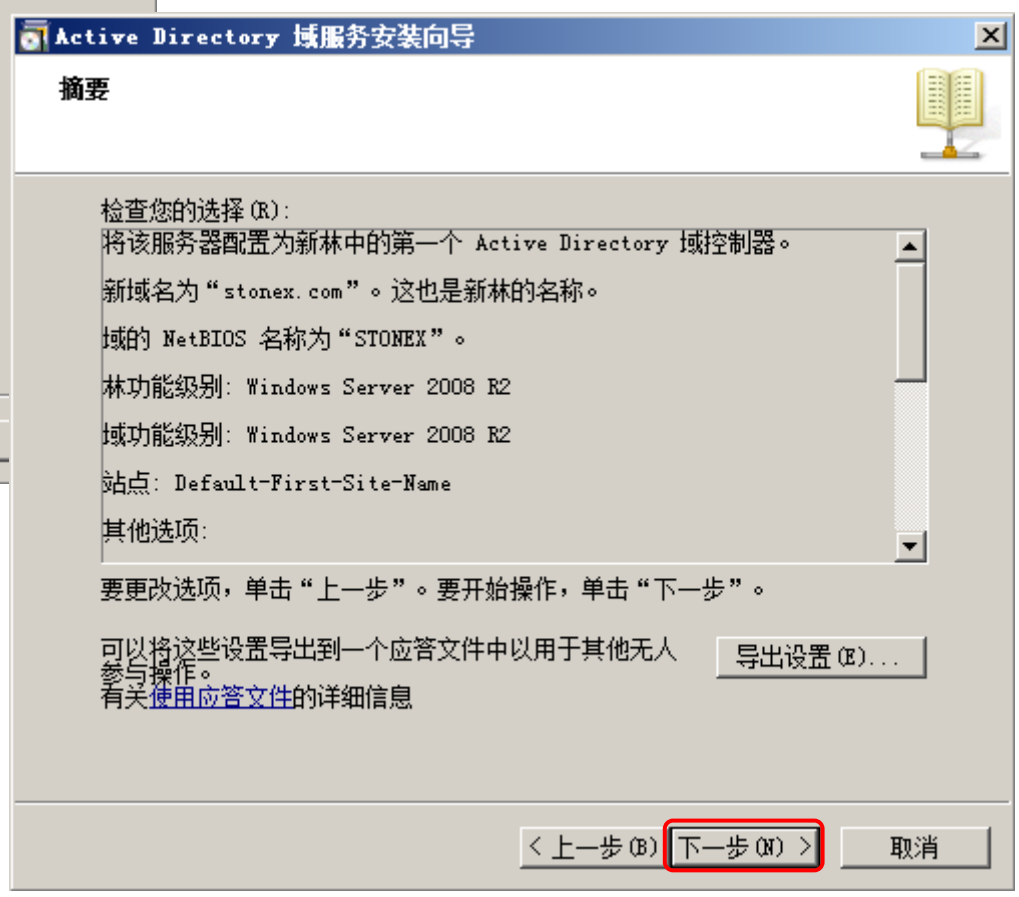
点击**下一步**



设置目录服务还原的**密码**，点击**下一步**

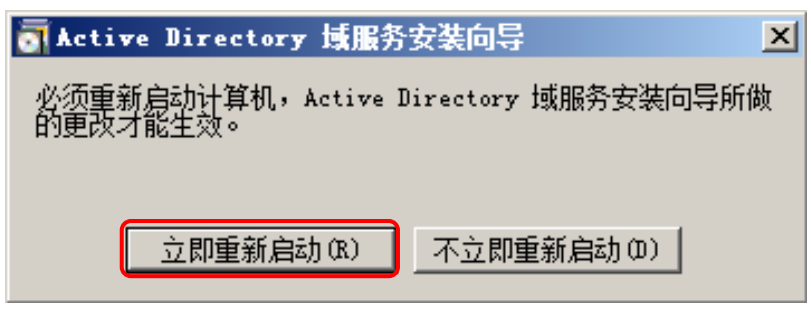


点击**下一步**



点击**完成**

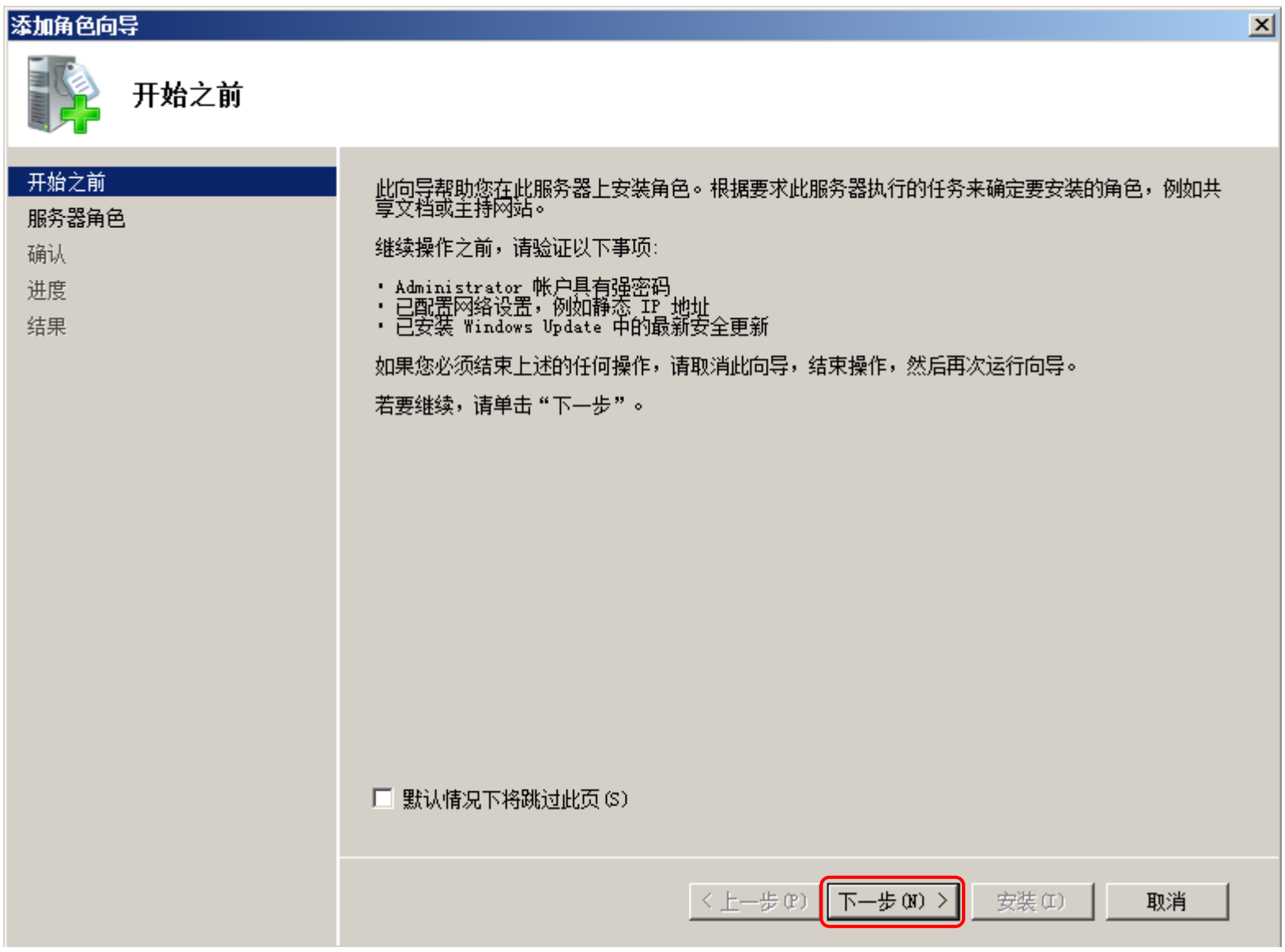
安装完成之后需**重启计算机**



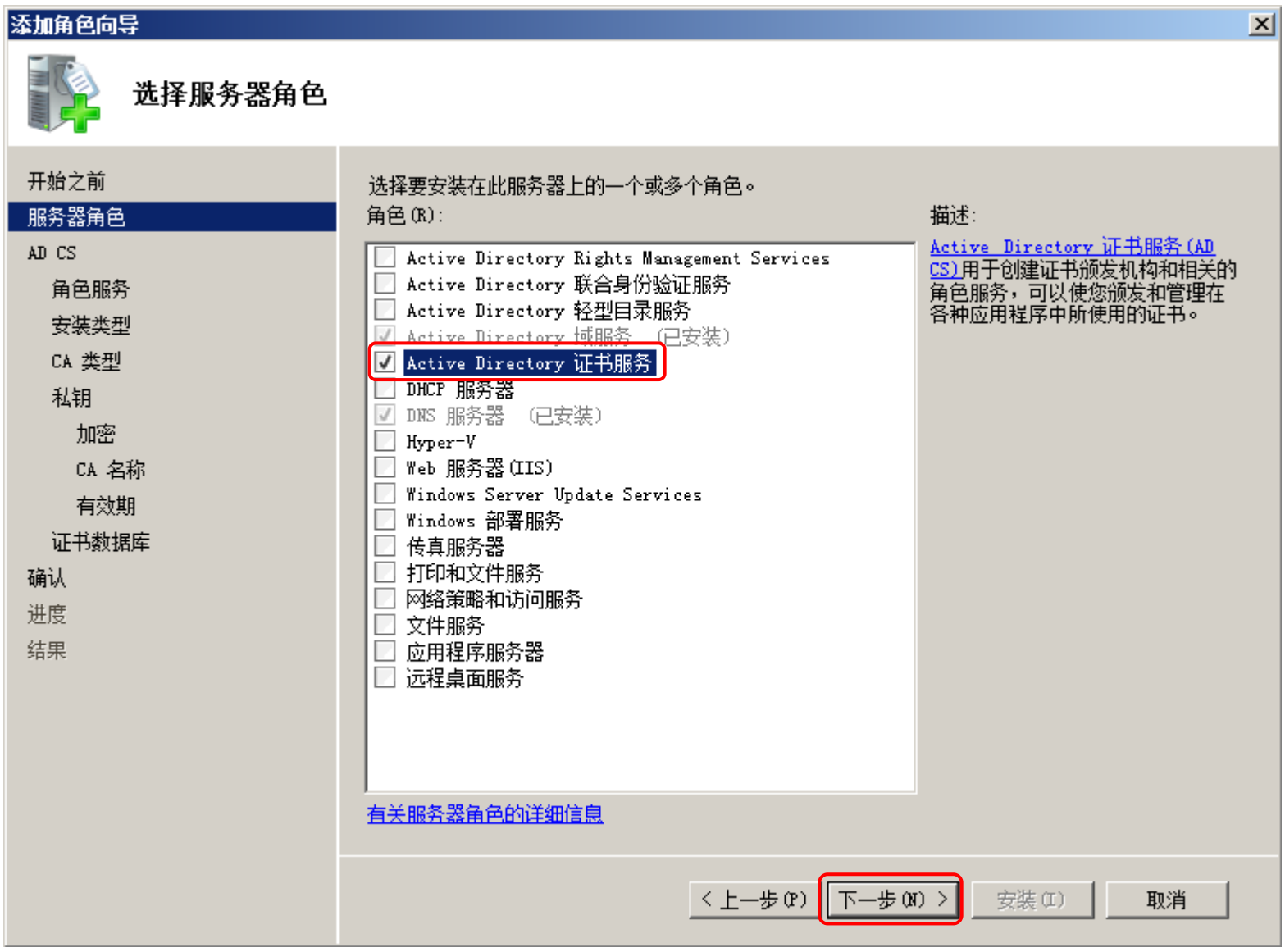
1.2 安装证书服务+IIS

点击**服务器管理器 > 角色 > 添加角色**

点击**下一步**

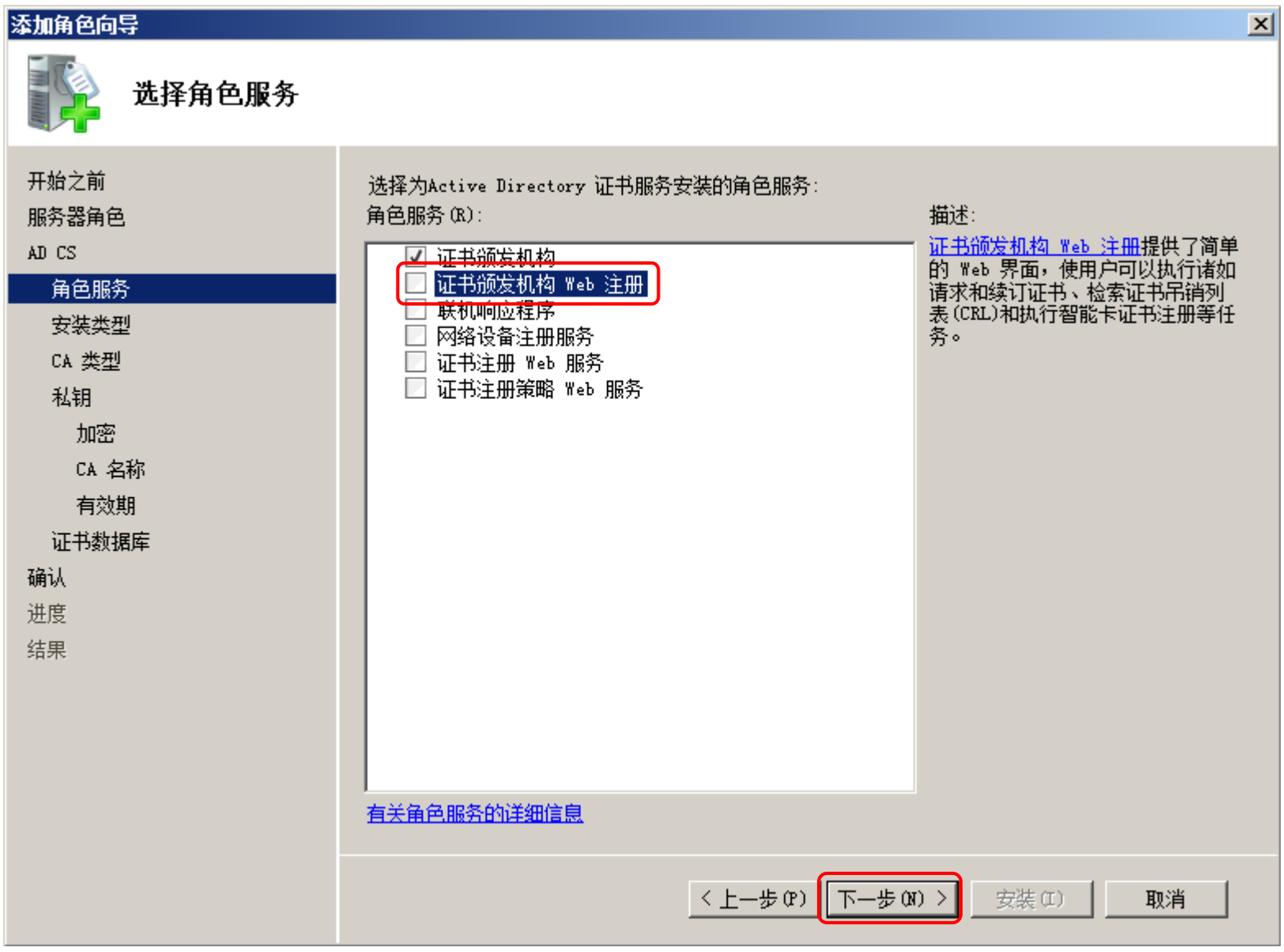


选中 **Active Directory 证书服务**，点击**下一步**



点击**下一步**

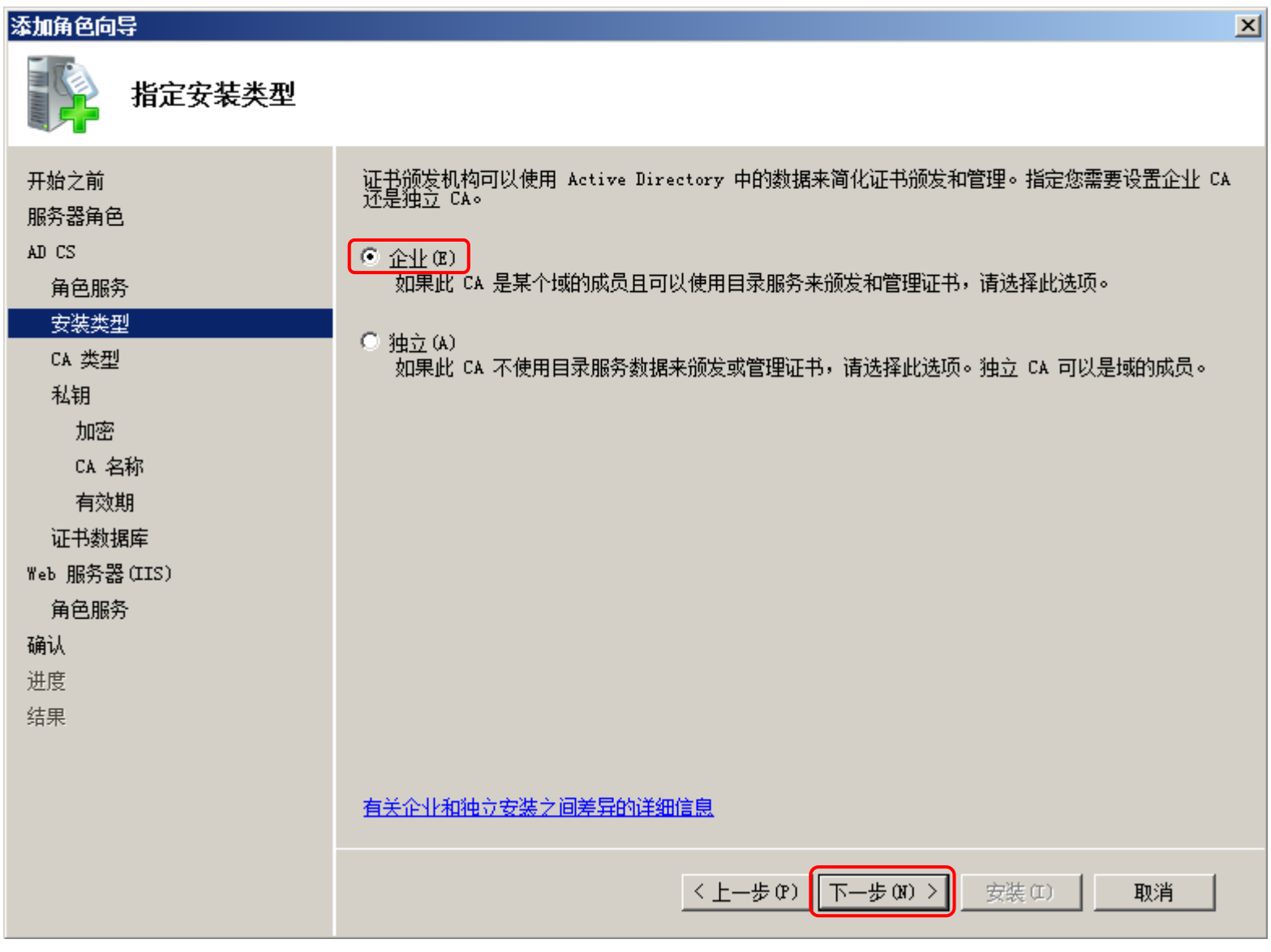
选中**证书颁发机构 Web 注册**，默认就会选中**证书颁发机构**



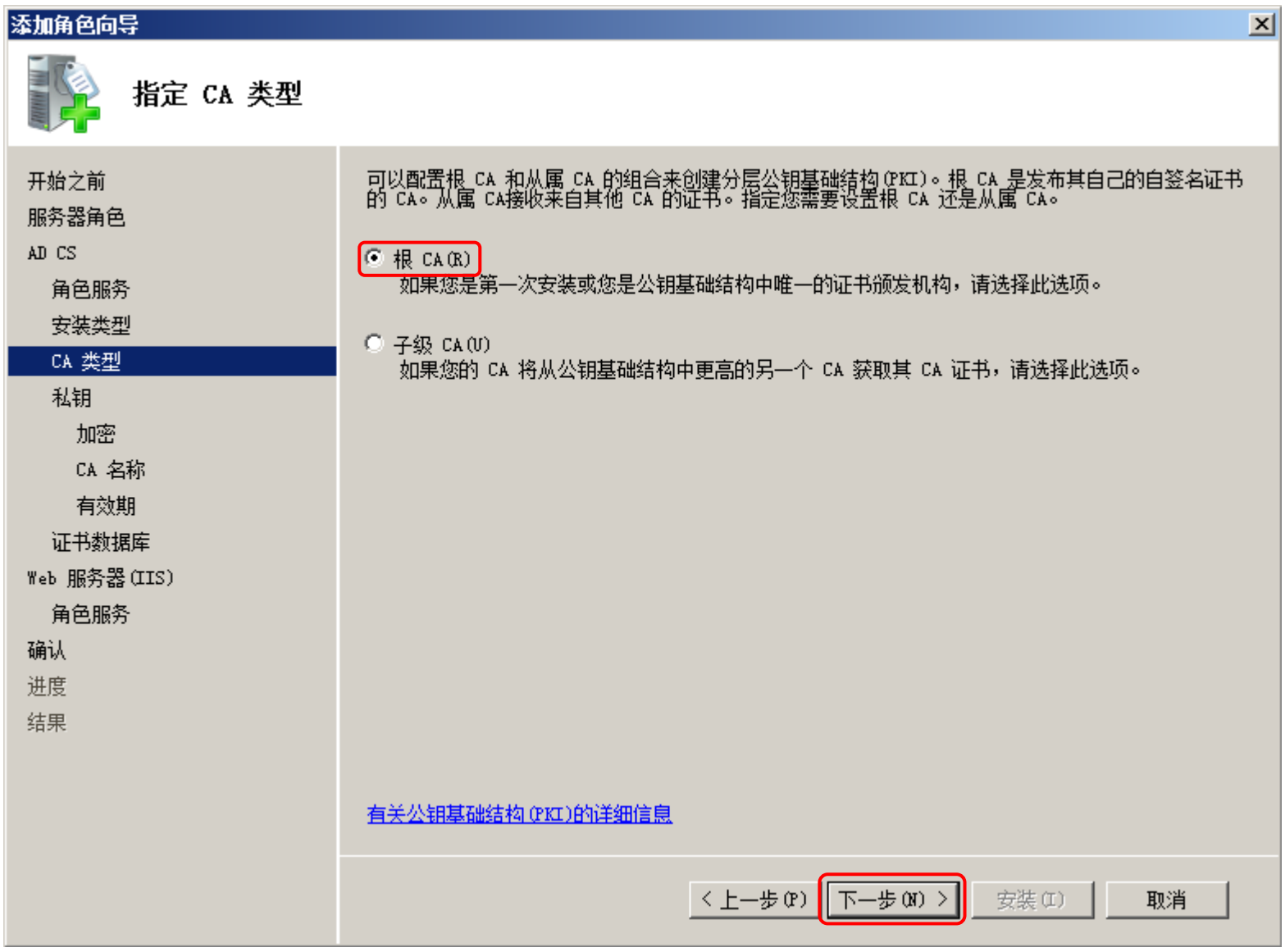
添加**证书颁发机构 Web 注册**，需安装 IIS 服务器

点击**下一步**

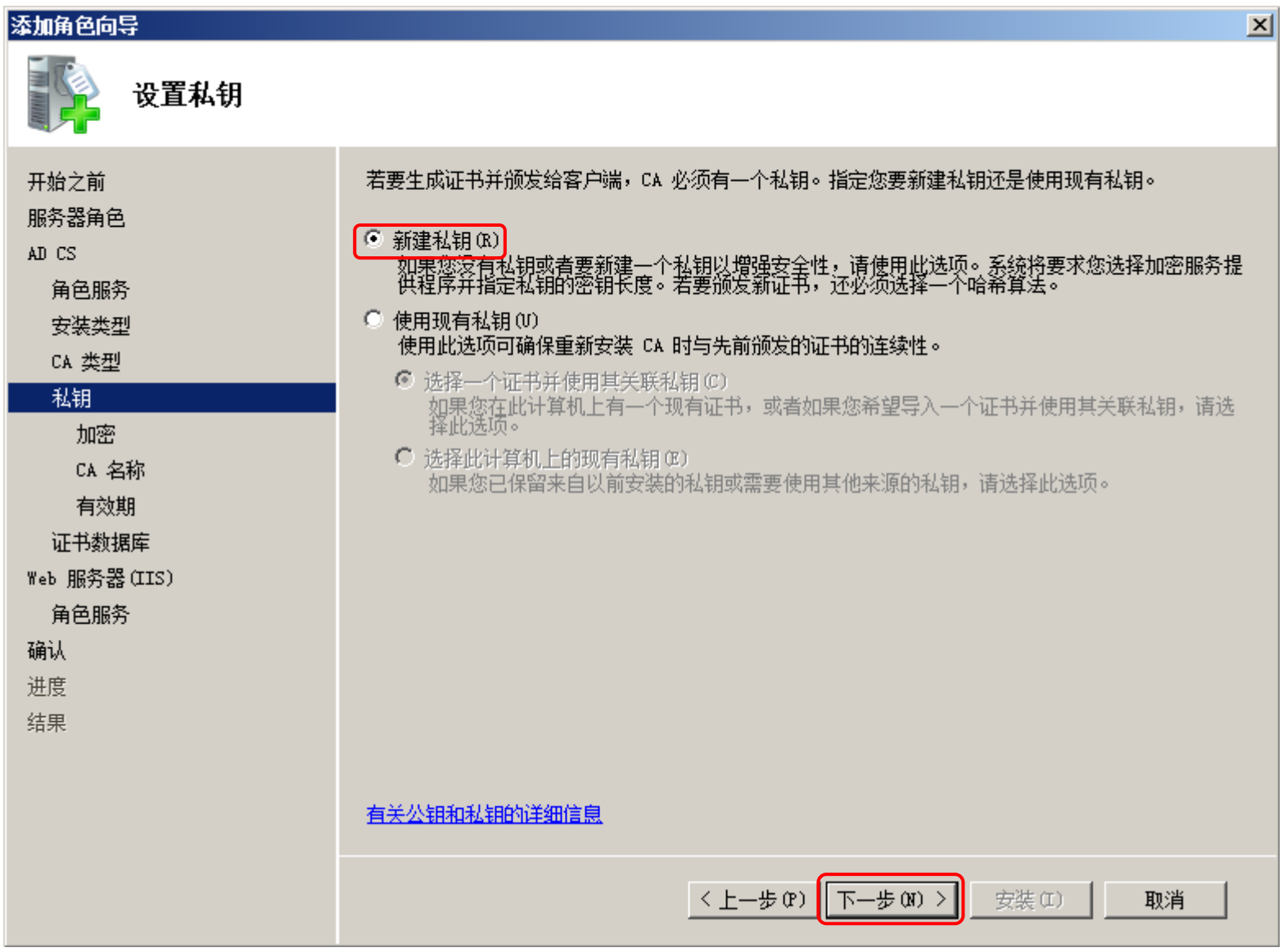
选中**企业**，点击**下一步**



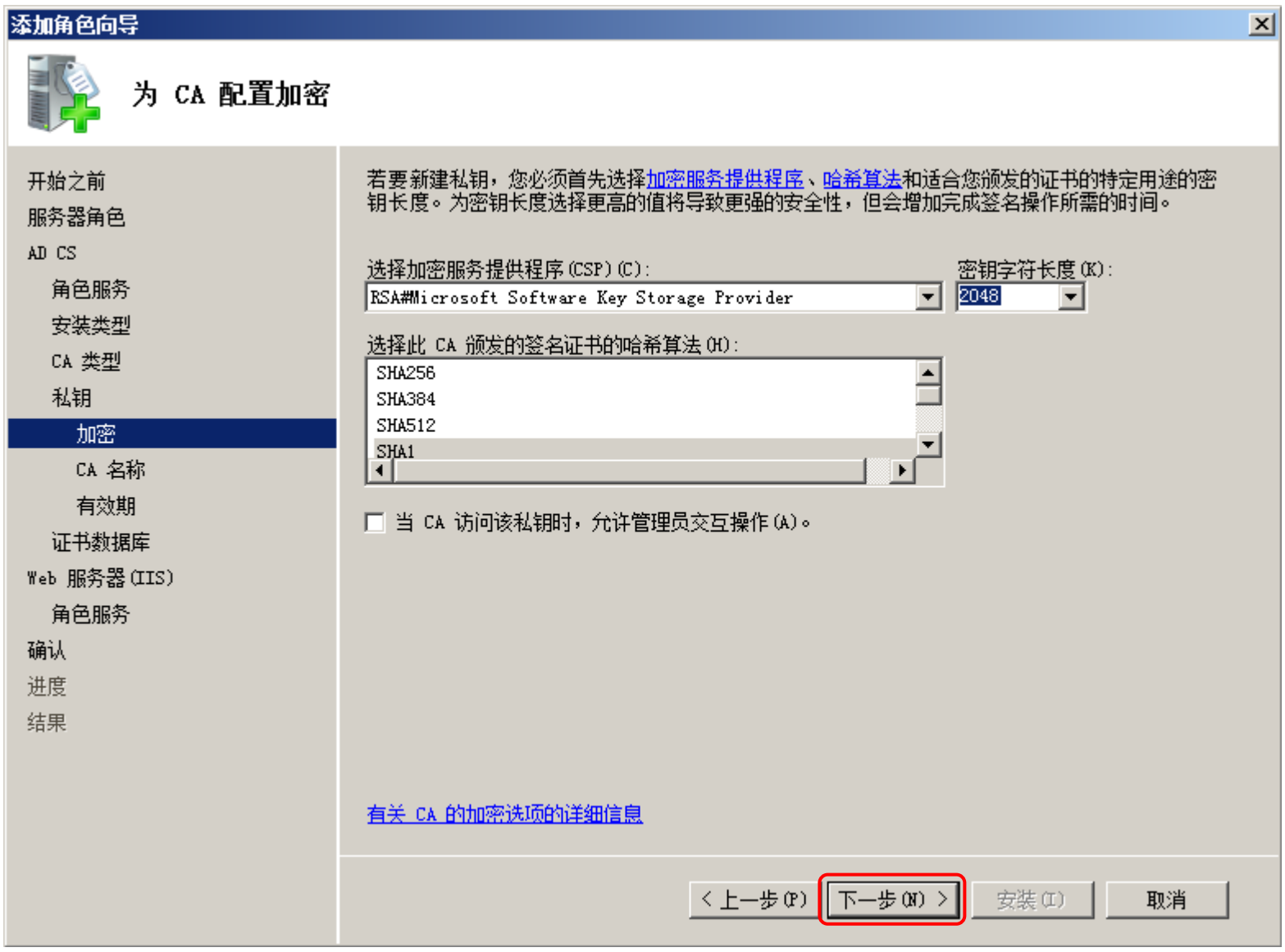
选中**根 CA**，点击**下一步**



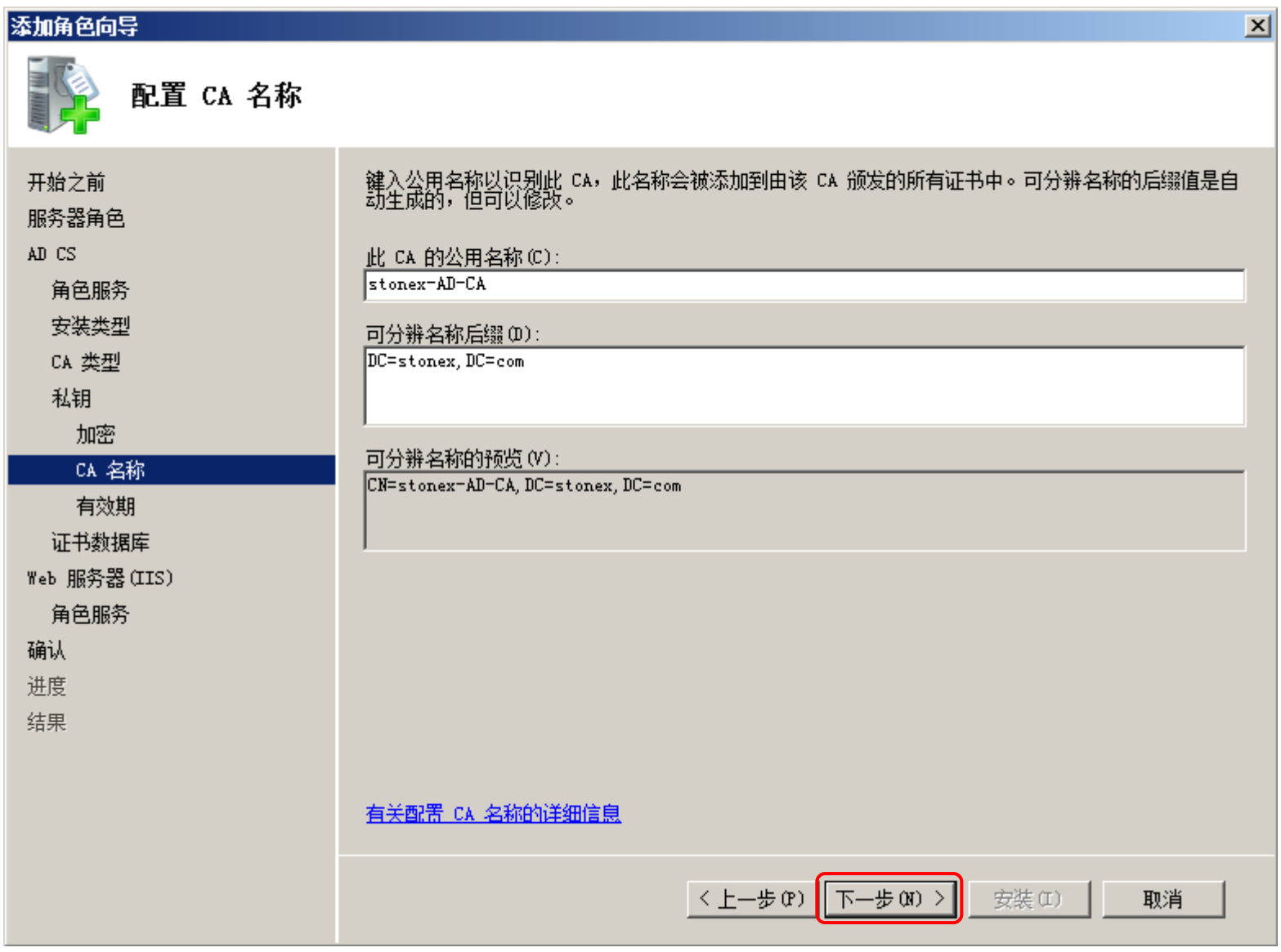
选中**新建秘钥**，点击**下一步**



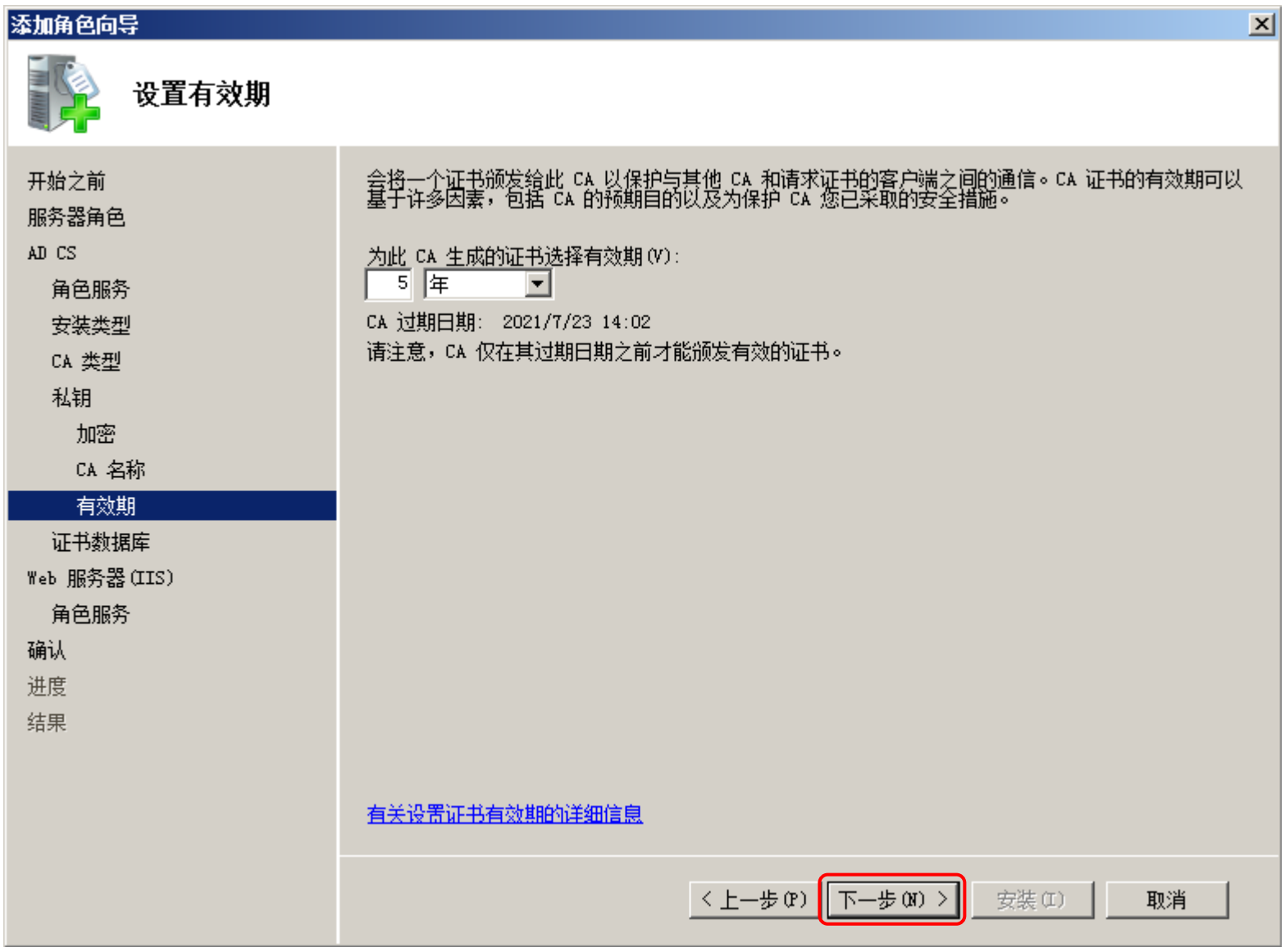
点击**下一步**


添加角色向导
为 CA 配置加密
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
若要新建私钥，您必须首先选择加密服务提供程序、哈希算法和适合您颁发的证书的特定用途的密钥长度。为密钥长度选择更高的值将导致更强的安全性，但会增加完成签名操作所需的时间。
选择加密服务提供程序(CSP)(C):
RSA#Microsoft Software Key Storage Provider
密钥字符长度(K):
2048
选择此 CA 颁发的签名证书的哈希算法(H):
SHA256
SHA384
SHA512
SHA1
当 CA 访问该私钥时，允许管理员交互操作(A)。
有关 CA 的加密选项的详细信息
< 上一步(P)
下一步(N) >
安装(I)
取消

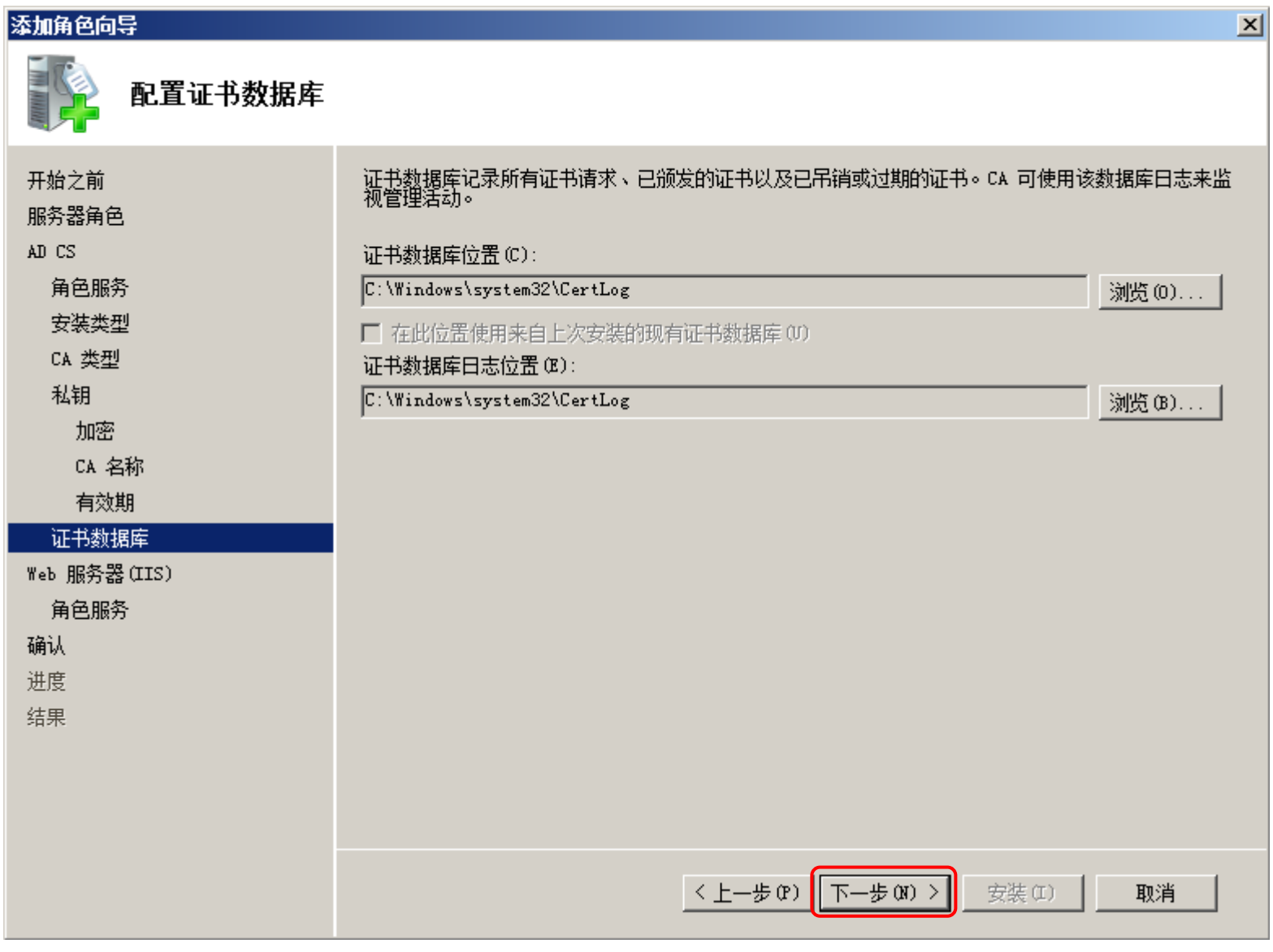
点击**下一步**


添加角色向导
配置 CA 名称
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
键入公用名称以识别此 CA，此名称会被添加到由该 CA 颁发的所有证书中。可分辨名称的后缀值是自动生成的，但可以修改。
此 CA 的公用名称(C):
stonex-AD-CA
可分辨名称后缀(D):
DC=stonex,DC=com
可分辨名称的预览(V):
CN=stonex-AD-CA,DC=stonex,DC=com
有关配置 CA 名称的详细信息
< 上一步(P)
下一步(N) >
安装(I)
取消

点击**下一步**

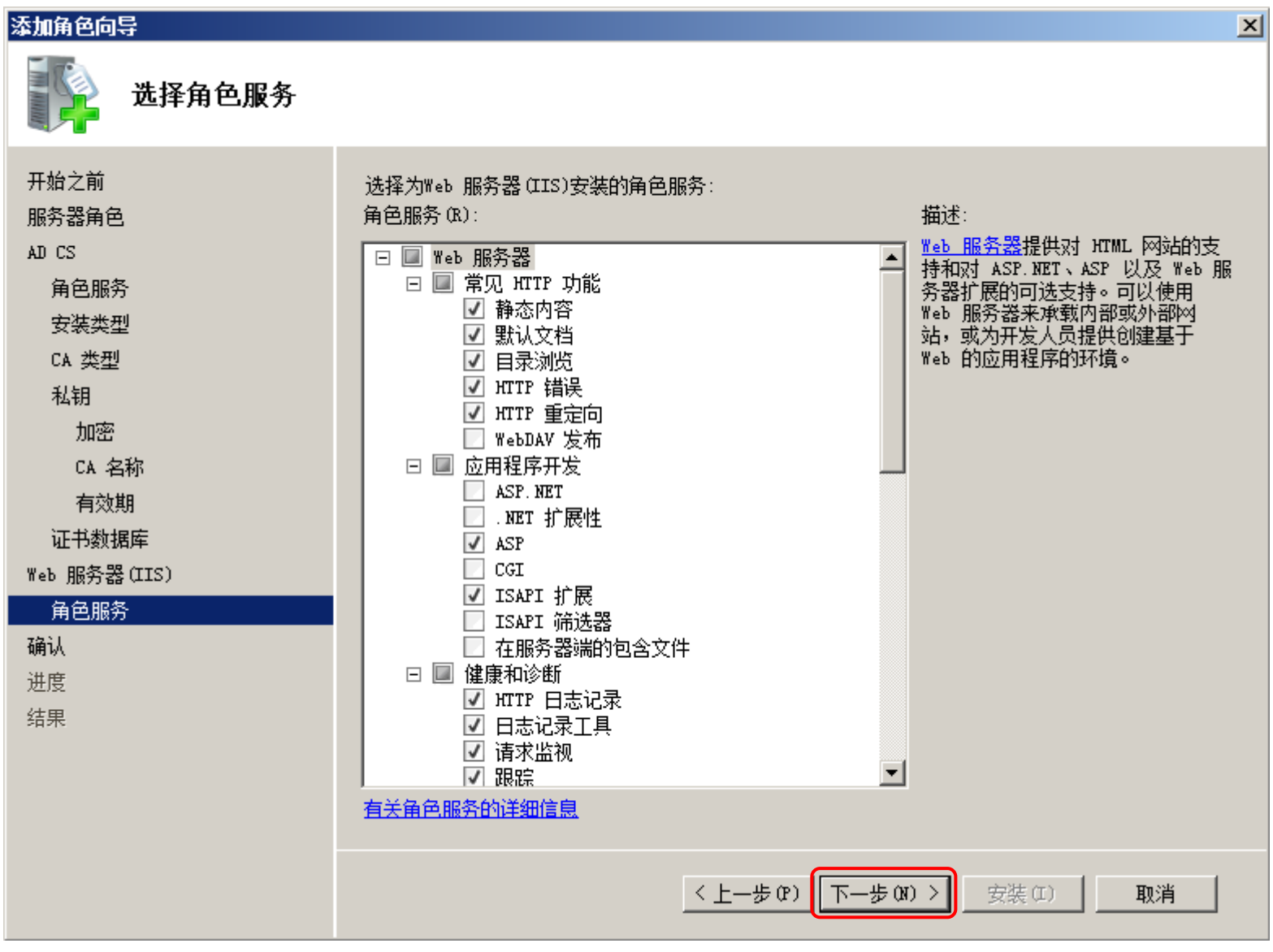

添加角色向导
设置有效期
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
会将一个证书颁发给此 CA 以保护与其他 CA 和请求证书的客户端之间的通信。CA 证书的有效期可以基于许多因素，包括 CA 的预期目的以及为保护 CA 您已采取的安全措施。
为此 CA 生成的证书选择有效期(V):
5
年
CA 过期日期: 2021/7/23 14:02
请注意，CA 仅在其过期日期之前才能颁发有效的证书。
有关设置证书有效期的详细信息
< 上一步(P)
下一步(N) >
安装(I)
取消

点击**下一步**


添加角色向导
配置证书数据库
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
证书数据库记录所有证书请求、已颁发的证书以及已吊销或过期的证书。CA 可使用该数据库日志来监视管理活动。
证书数据库位置(C):
C:\Windows\system32\CertLog
浏览(O)...
在此位置使用来自上次安装的现有证书数据库(U)
证书数据库日志位置(E):
C:\Windows\system32\CertLog
浏览(B)...
< 上一步(P)
下一步(N) >
安装(I)
取消

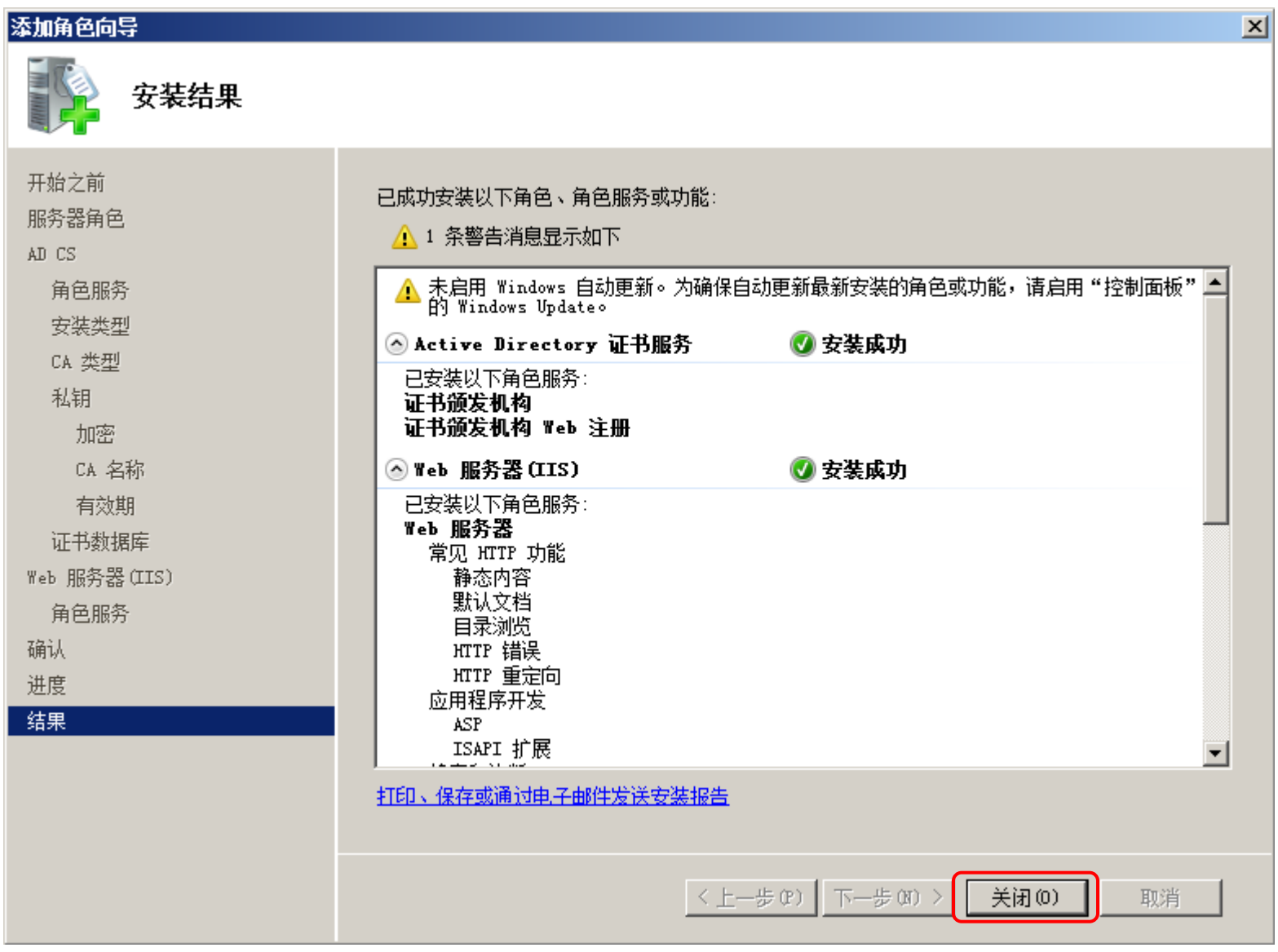
点击**下一步**，安装 IIS 服务器

点击**下一步**



点击**安装**

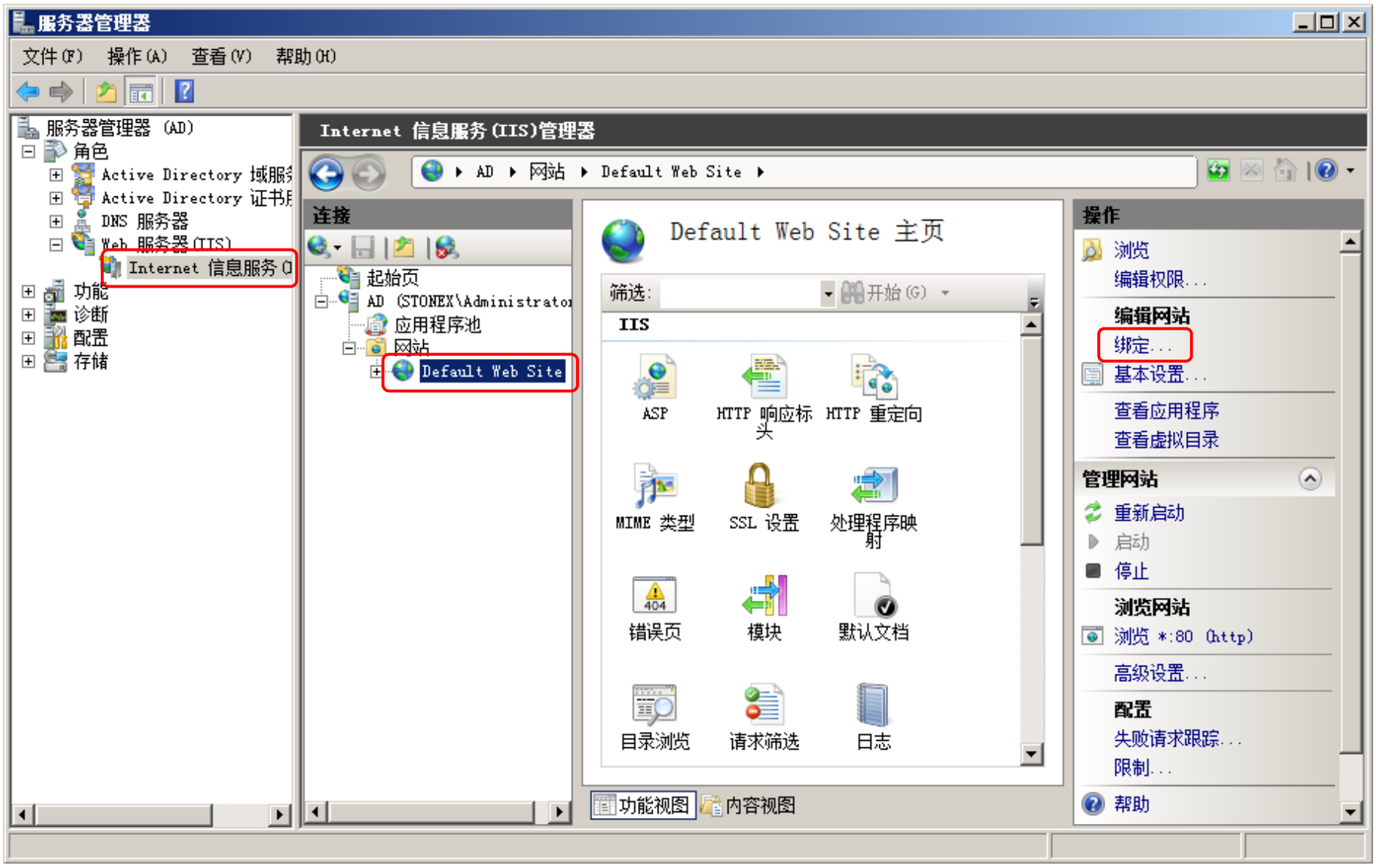
点击**关闭**，完成安装 Active Directory 证书服务和 IIS 服务器



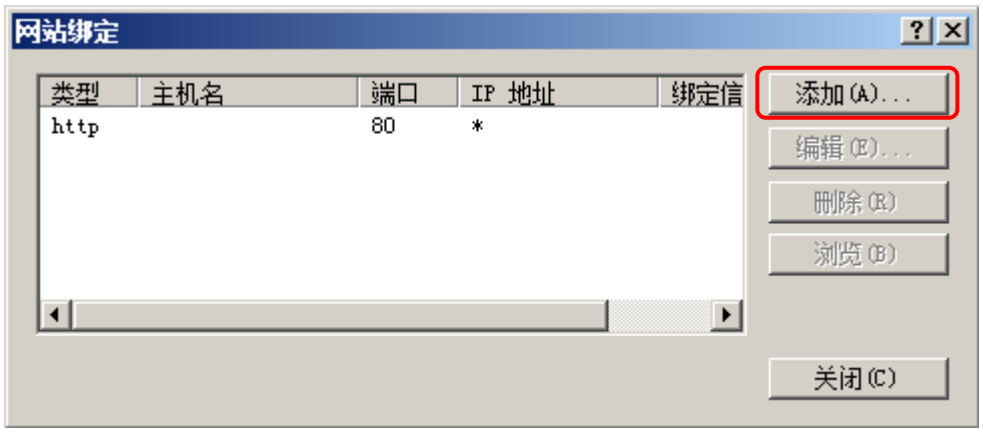
1.3 配置 IIS 开启 https

无线客户端需要通过 https 访问证书服务器才能申请用户证书，因此需要配置 IIS 支持 https 访问， IIS 默认不支持 https 访问。

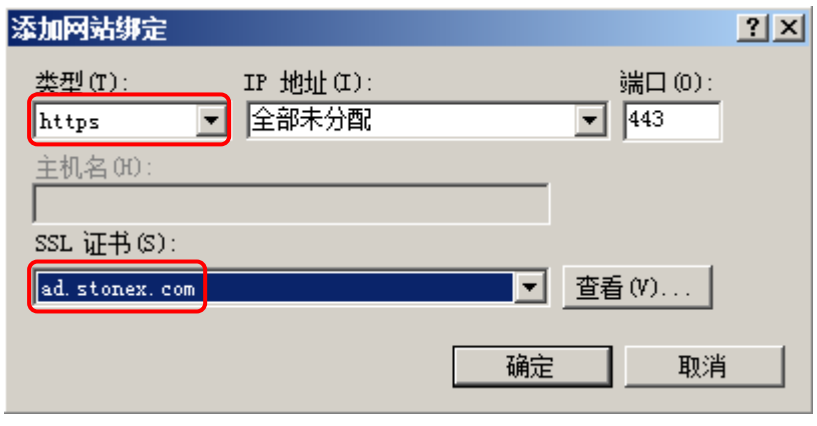
选中 **Internet 信息服务（IIS 管理器）**，选中 **Default Web Site**，点击**绑定**



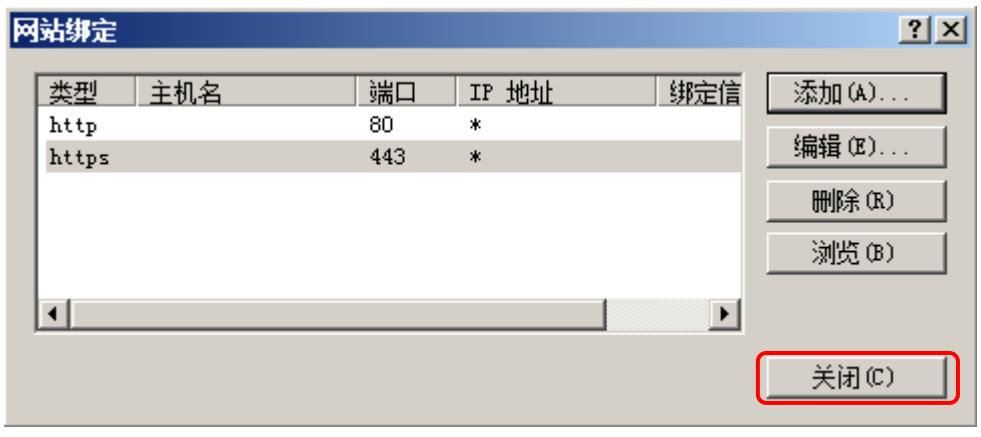
点击**添加**



类型选择 **https**，证书选择 **ad.stonex.com**，点击**确定**



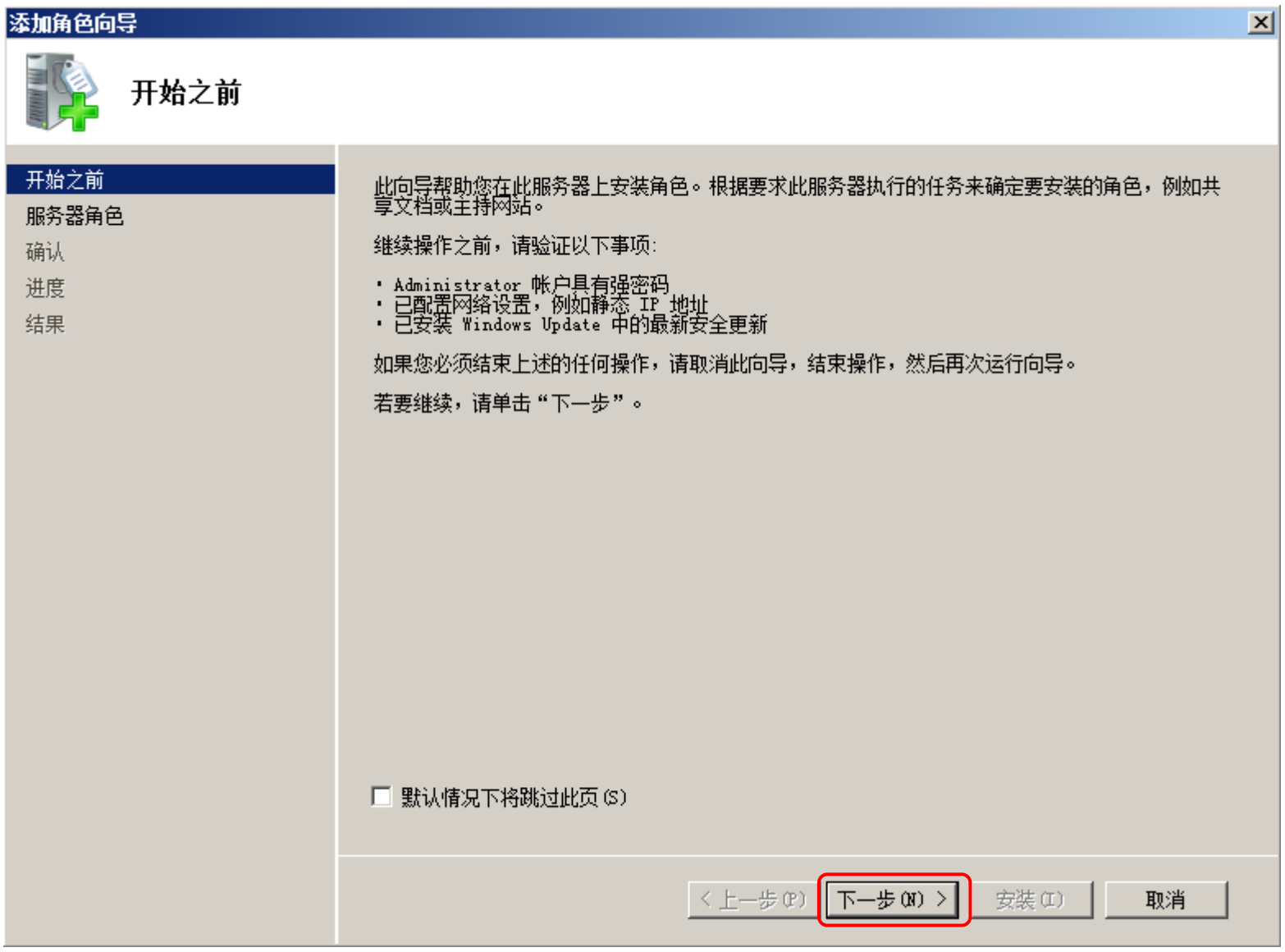
点击**关闭**，配置完成



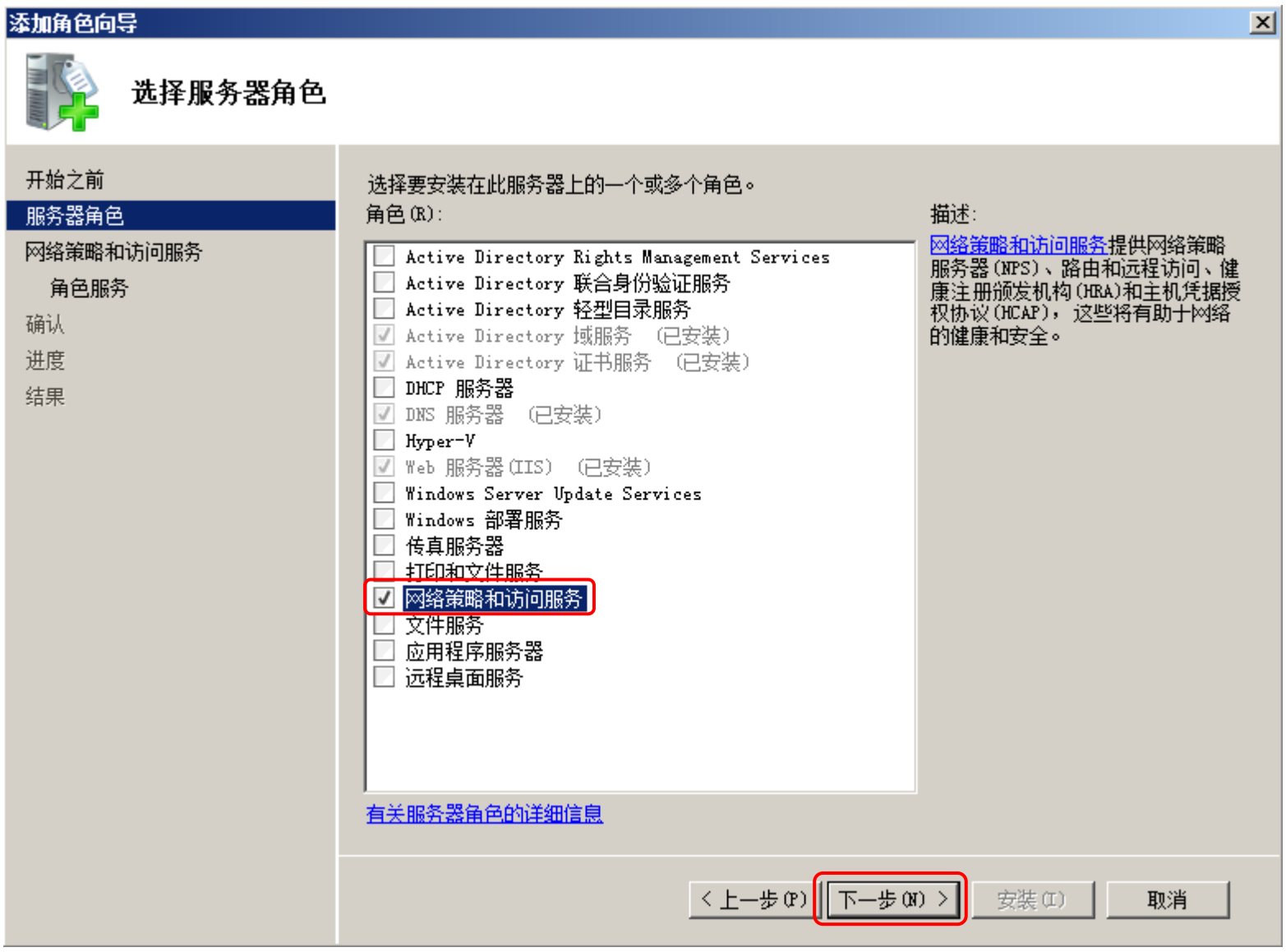
1.4 安装 NPS

点击**服务器管理器 > 角色 > 添加角色**

点击**下一步**

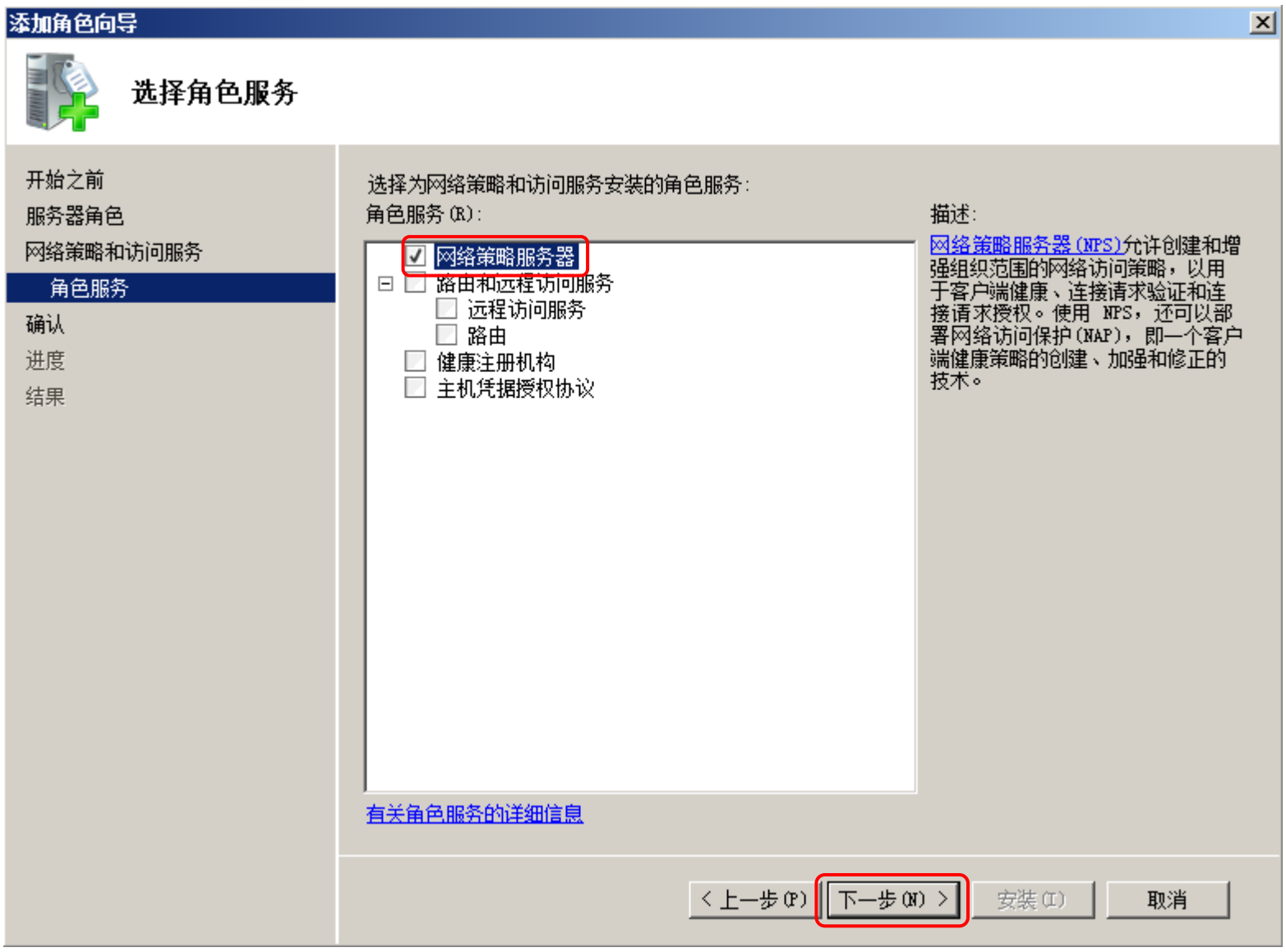


选中**网络策略和访问服务**，点击**下一步**



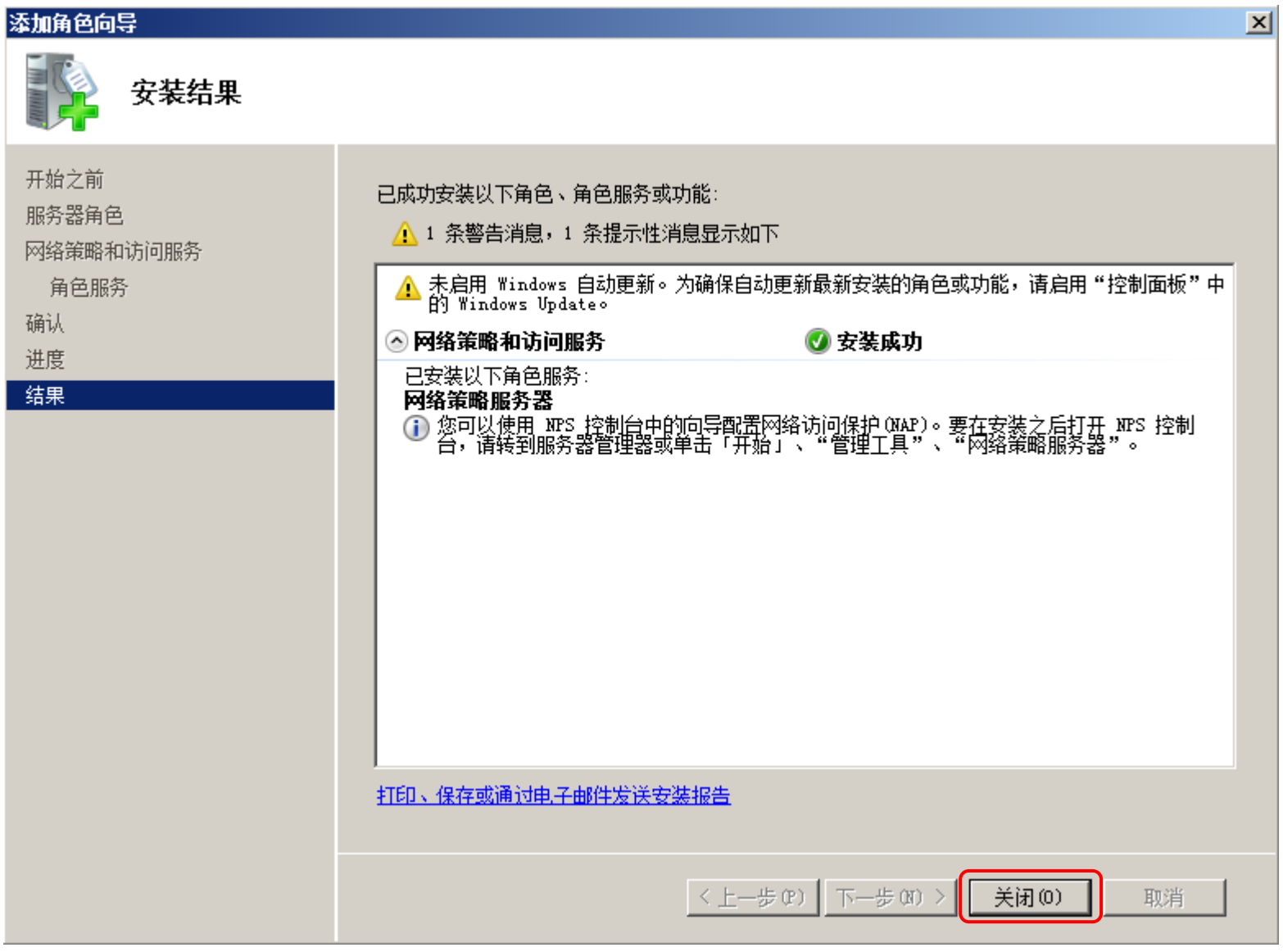
点击**下一步**

勾选**网络策略服务器**，点击**下一步**



点击**安装**

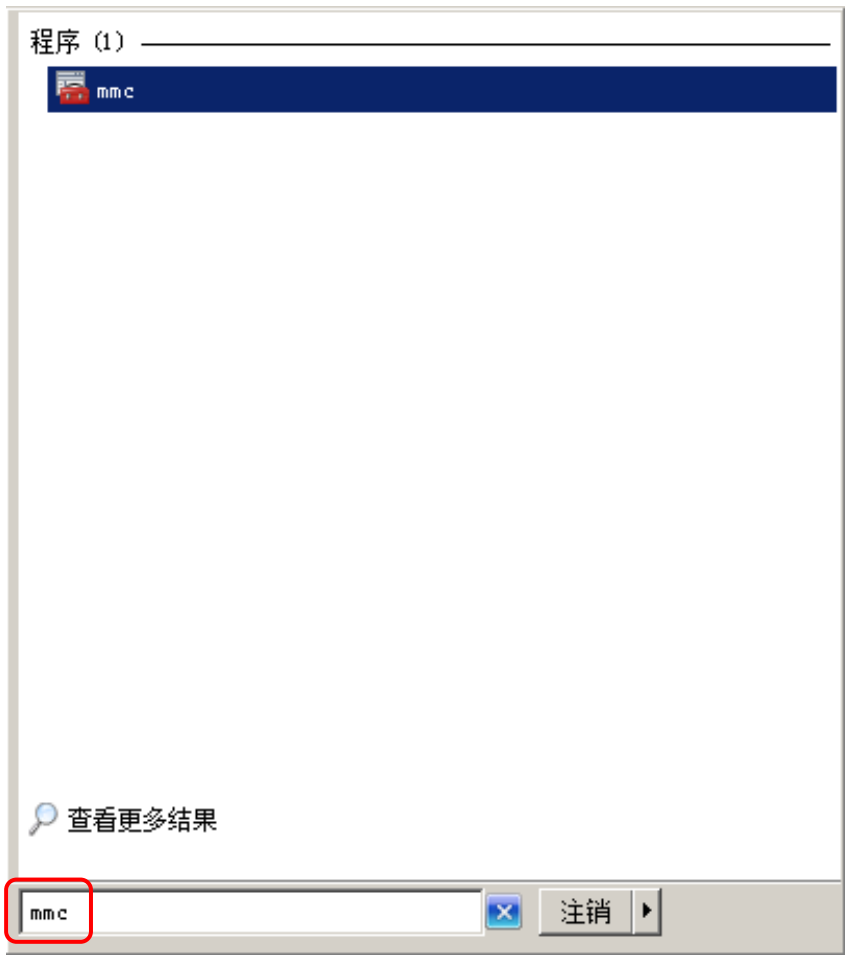
点击**关闭**，NPS 安装完成



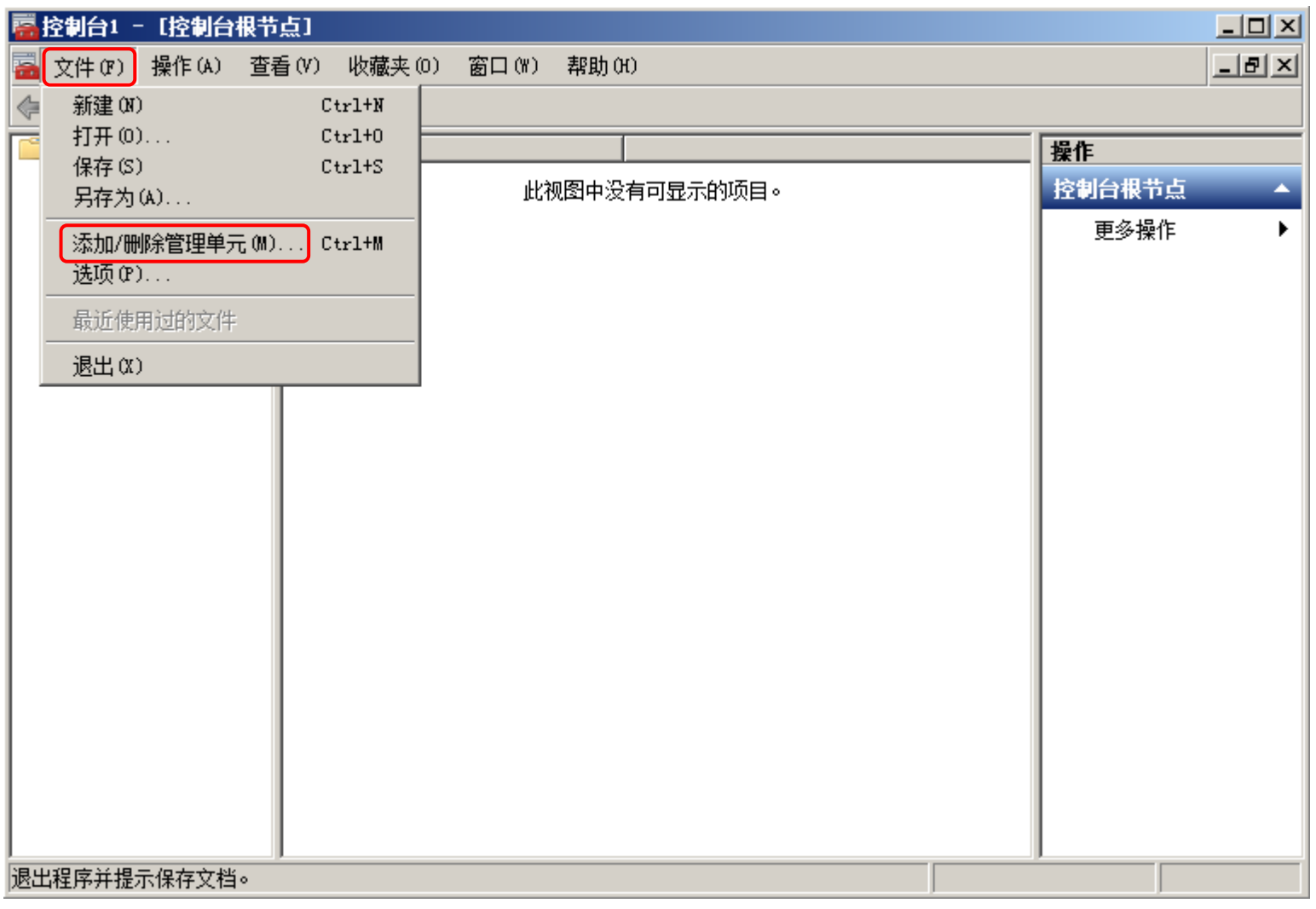
1.5 管理 NPS（RADIUS 服务器）计算机证书

执行 802.1X 认证，RADIUS 服务器需要向认证的无线客户端提供一张计算机证书，以便客户端确认正在与他们交互的是合法的 RADIUS 服务器，而不是伪装的。管理计算机证书使用管理控制台（MMC）.

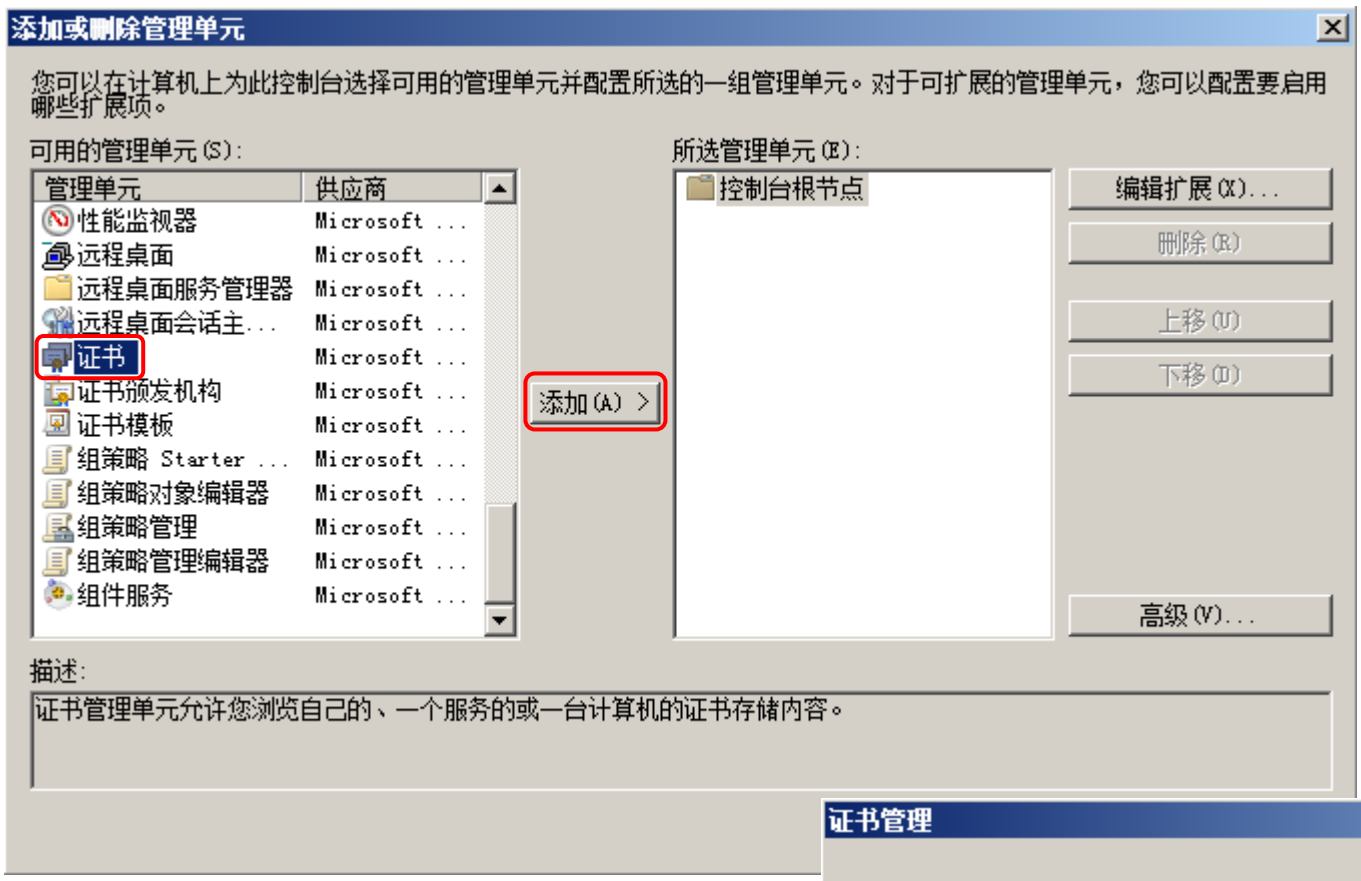
点击**开始** > 输入 **mmc**，打开**管理控制台**



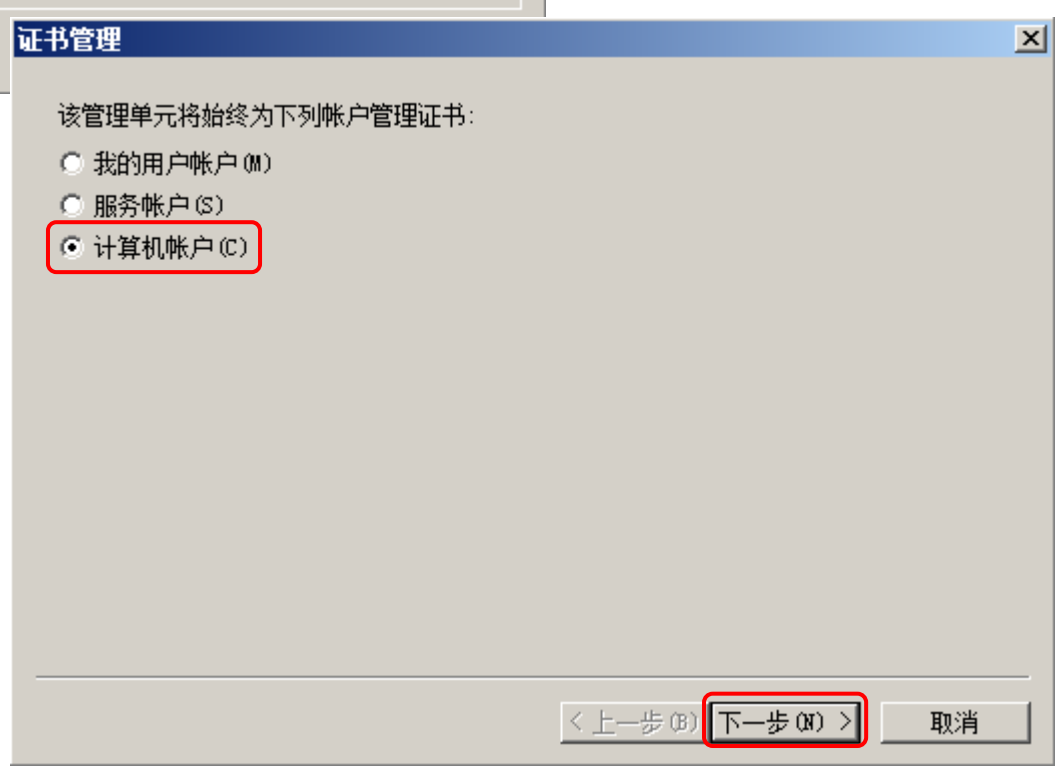
点击**文件** > **添加/删除管理单元**



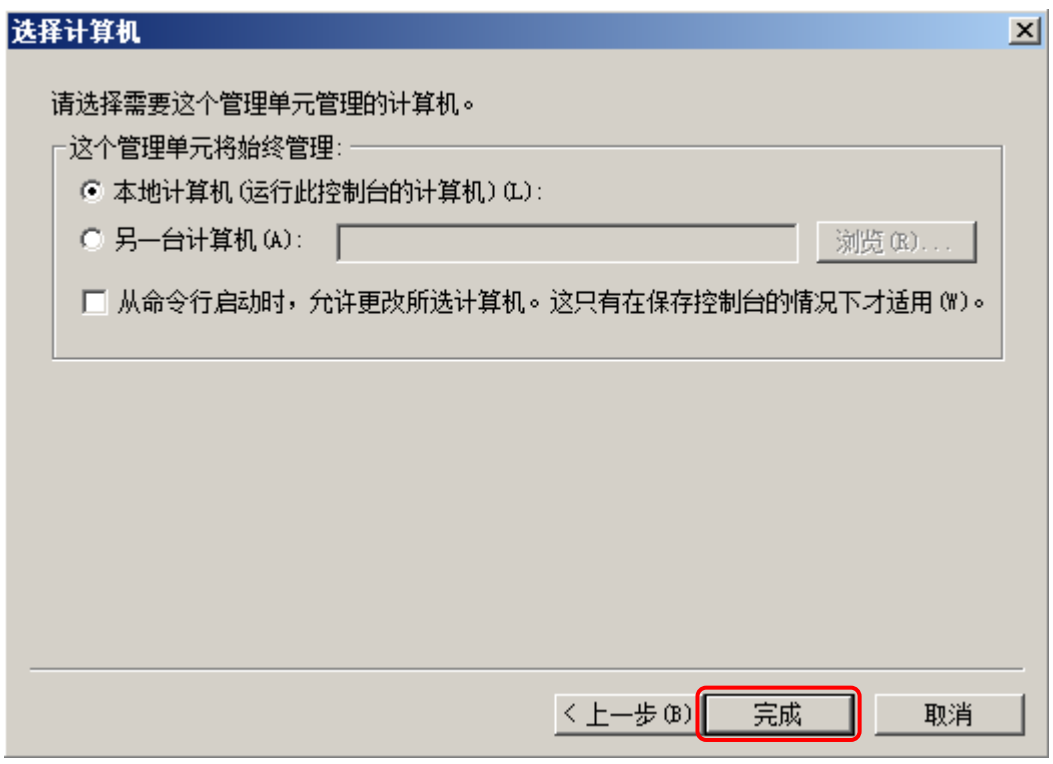
选择**证书** > 点击**添加**



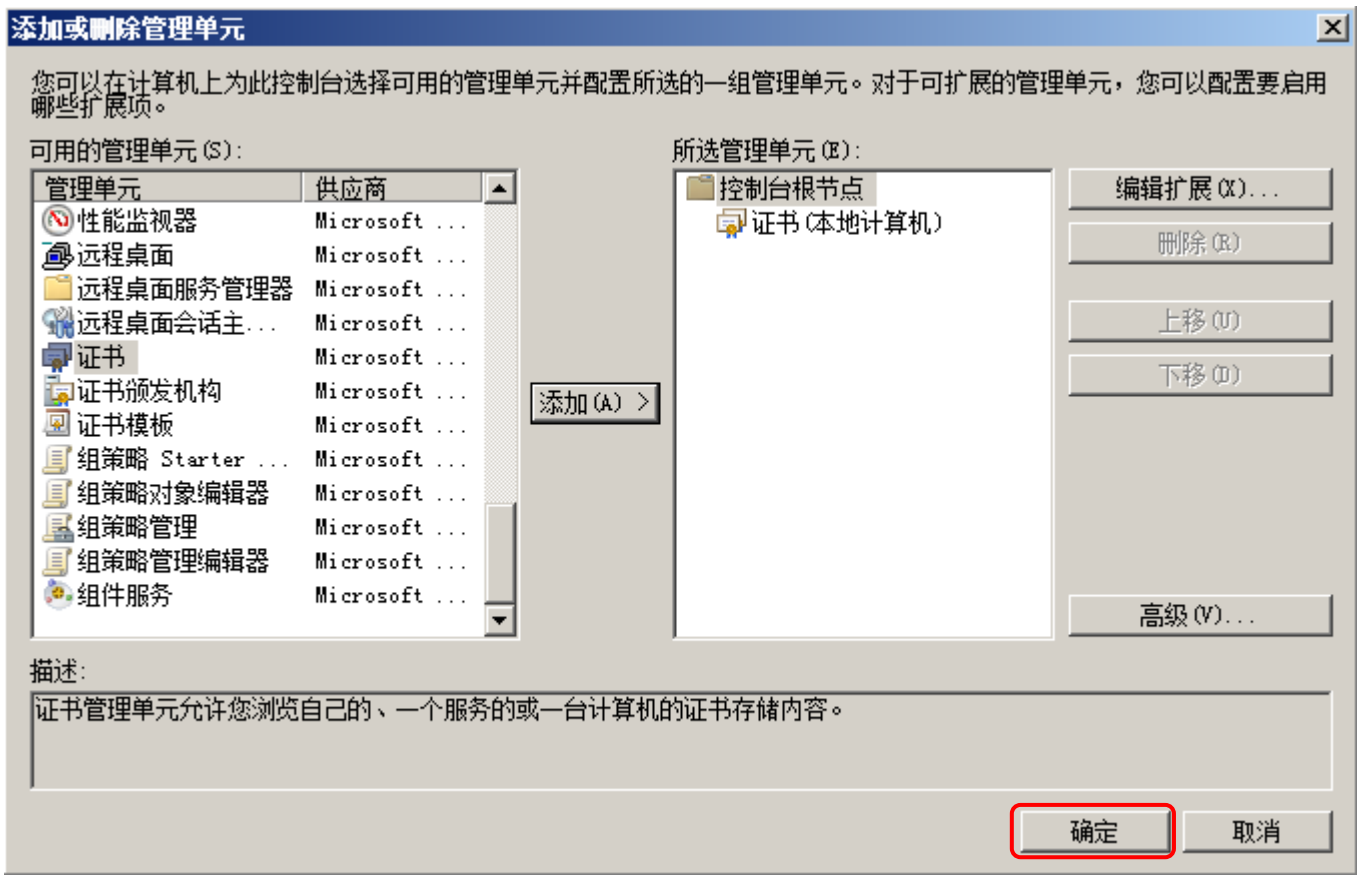
选择**计算机账号**，点击**下一步**



点击**完成**



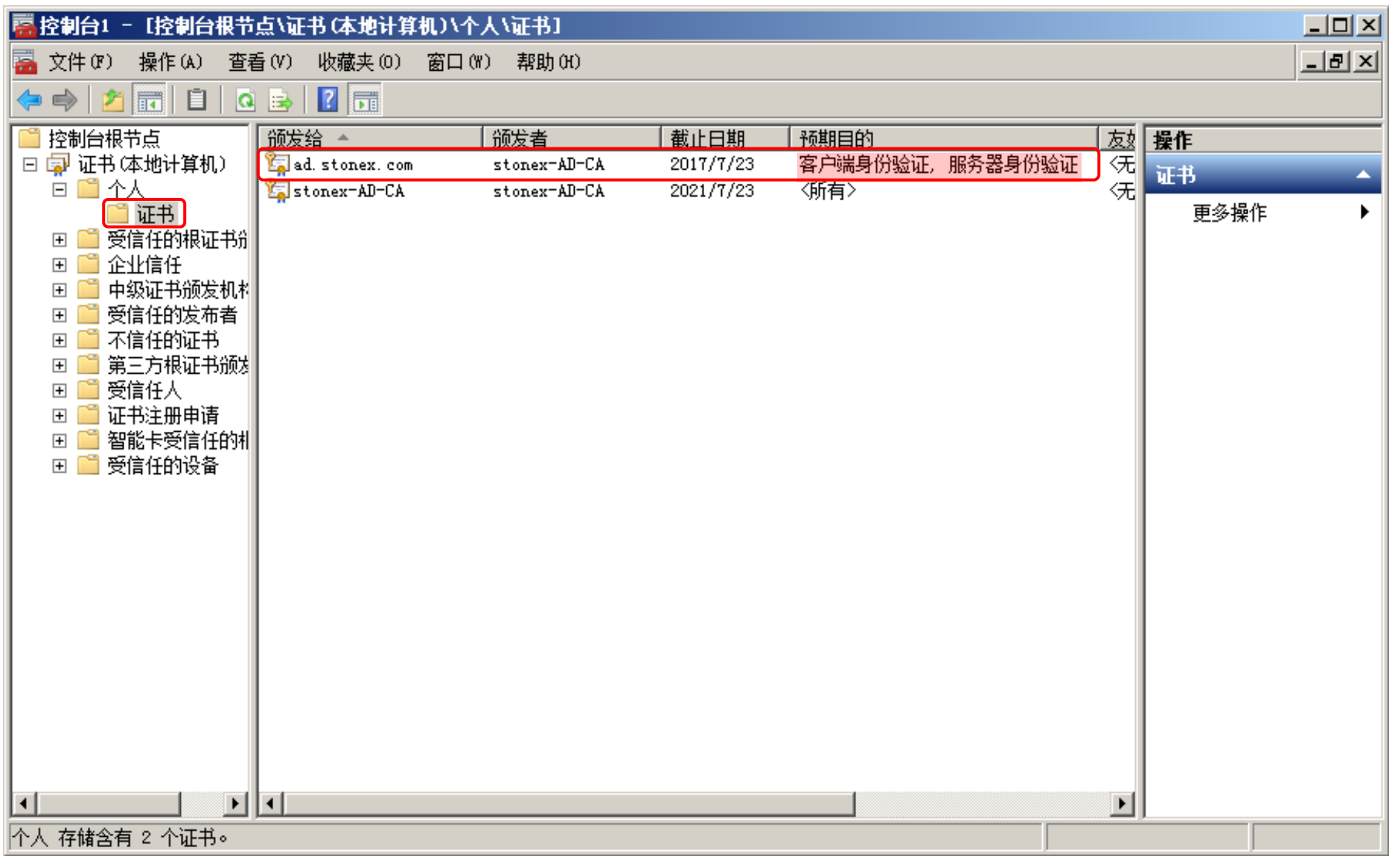
点击**确定**



点击**个人** > **证书**，可以查看所有计算机证书

ad.stonex.com 就是根 CA 颁发给 RADIUS 服务器的计算机证书

注意：如果 NPS 单独安装在一台 Windows Server 2008 服务器上，则默认没有这张证书，需要手动申请一张计算机证书.

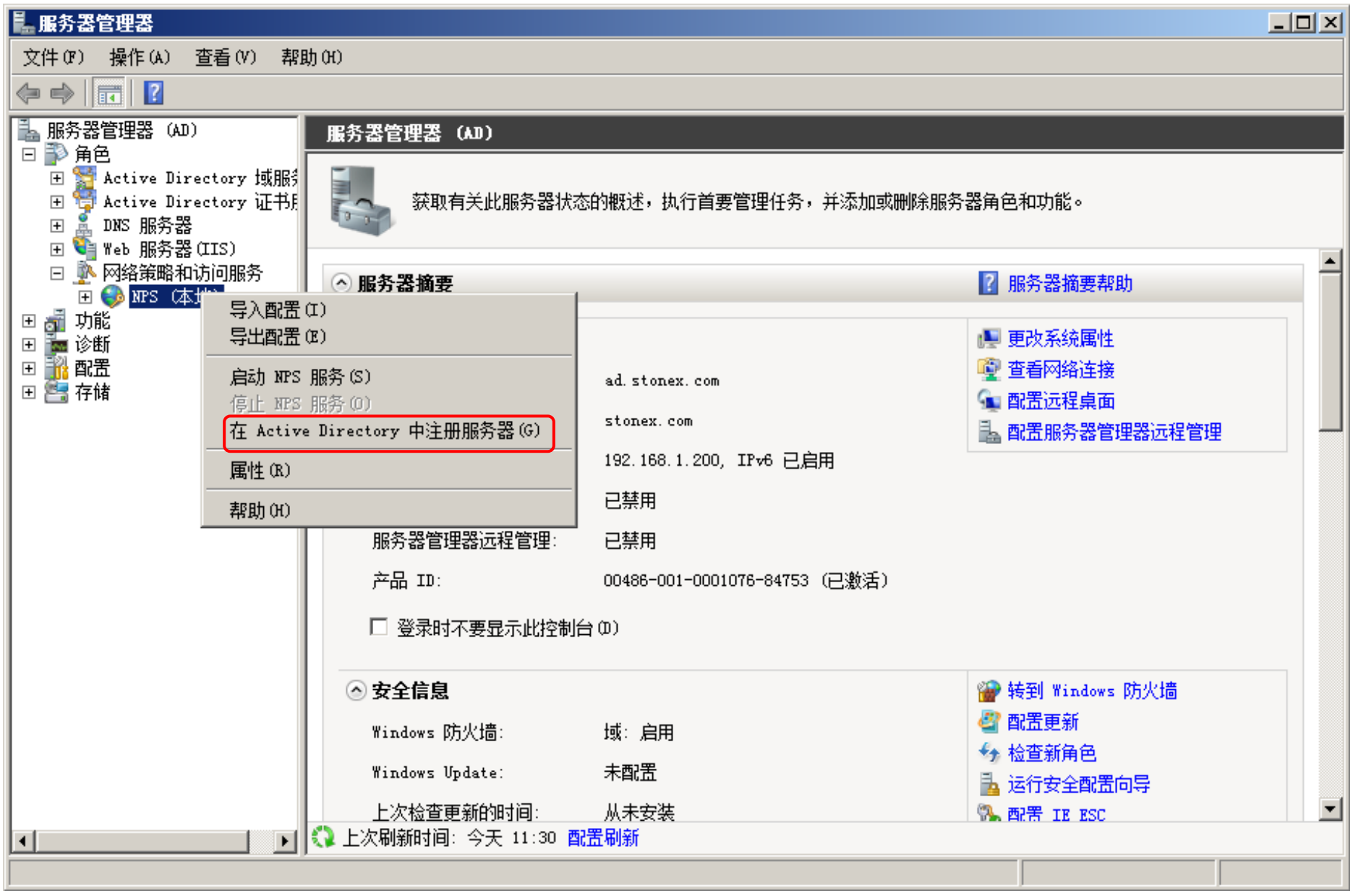


1.6 配置 NPS

配置 NPS 分为三个步骤：

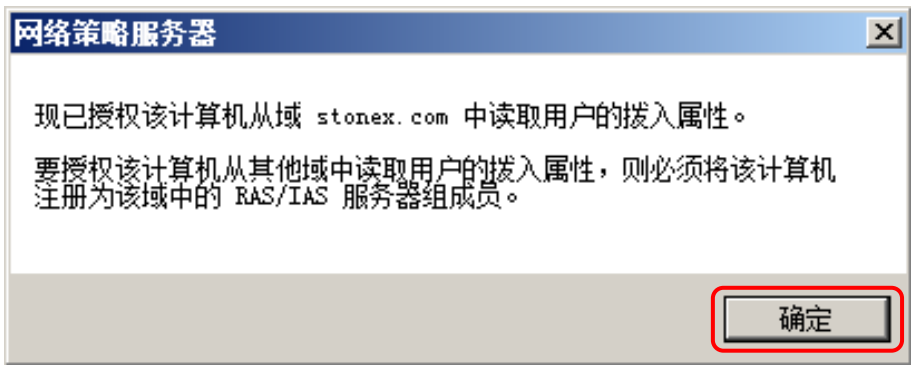
1. 在 Active Directory 中注册服务器，授权 NPS 从域中读取用户的拨入属性
2. 添加 RAIDUS 客户端
3. 创建网络策略

点击**服务器管理器** > **角色** > **网络策略和访问服务** > 右击 **NPS（本地）** > 选中**在 Active Directory 中注册服务器**

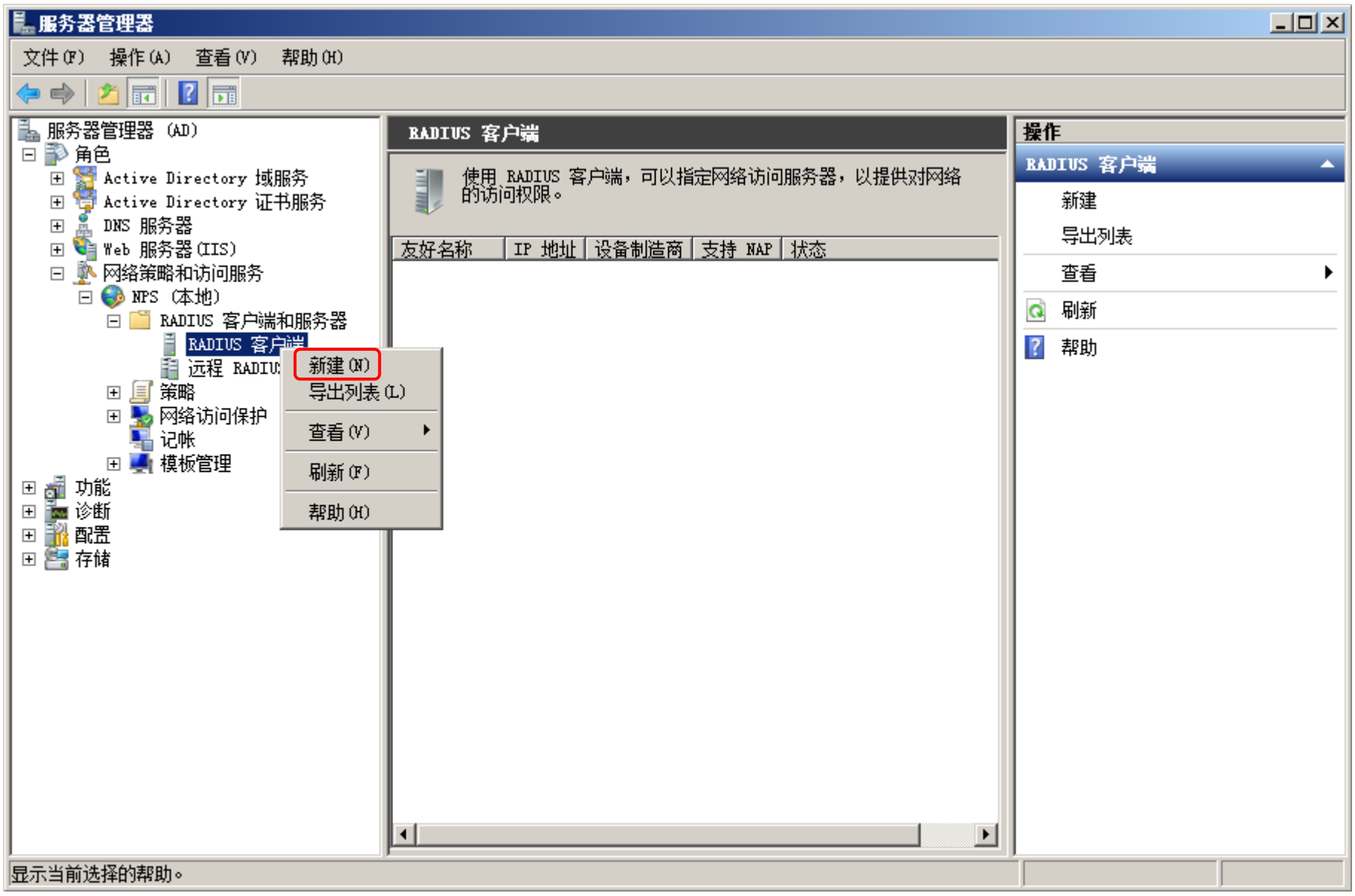


点击**确定**

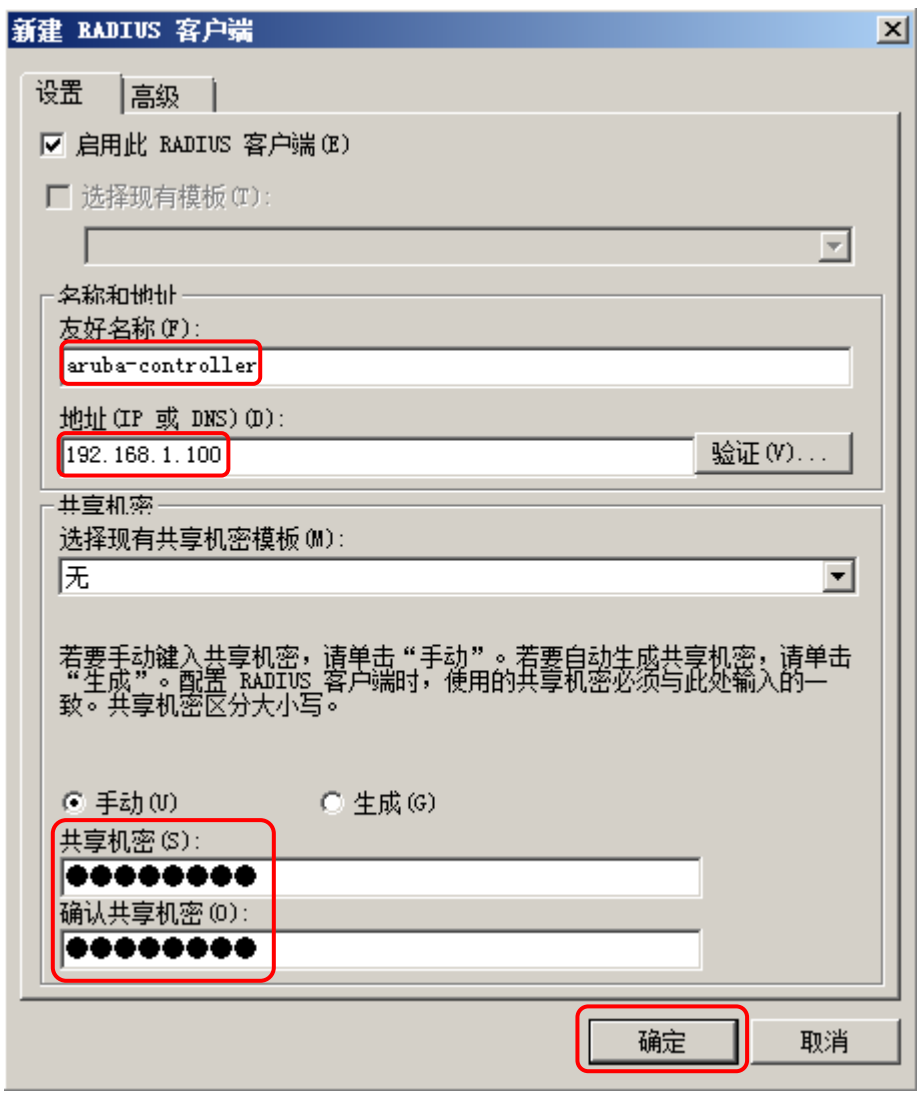
点击**确定**



点击 **NPS（本地）** > **RADIUS 客户端和服务器** > 右击 **RADIUS 客户端** > **新建**

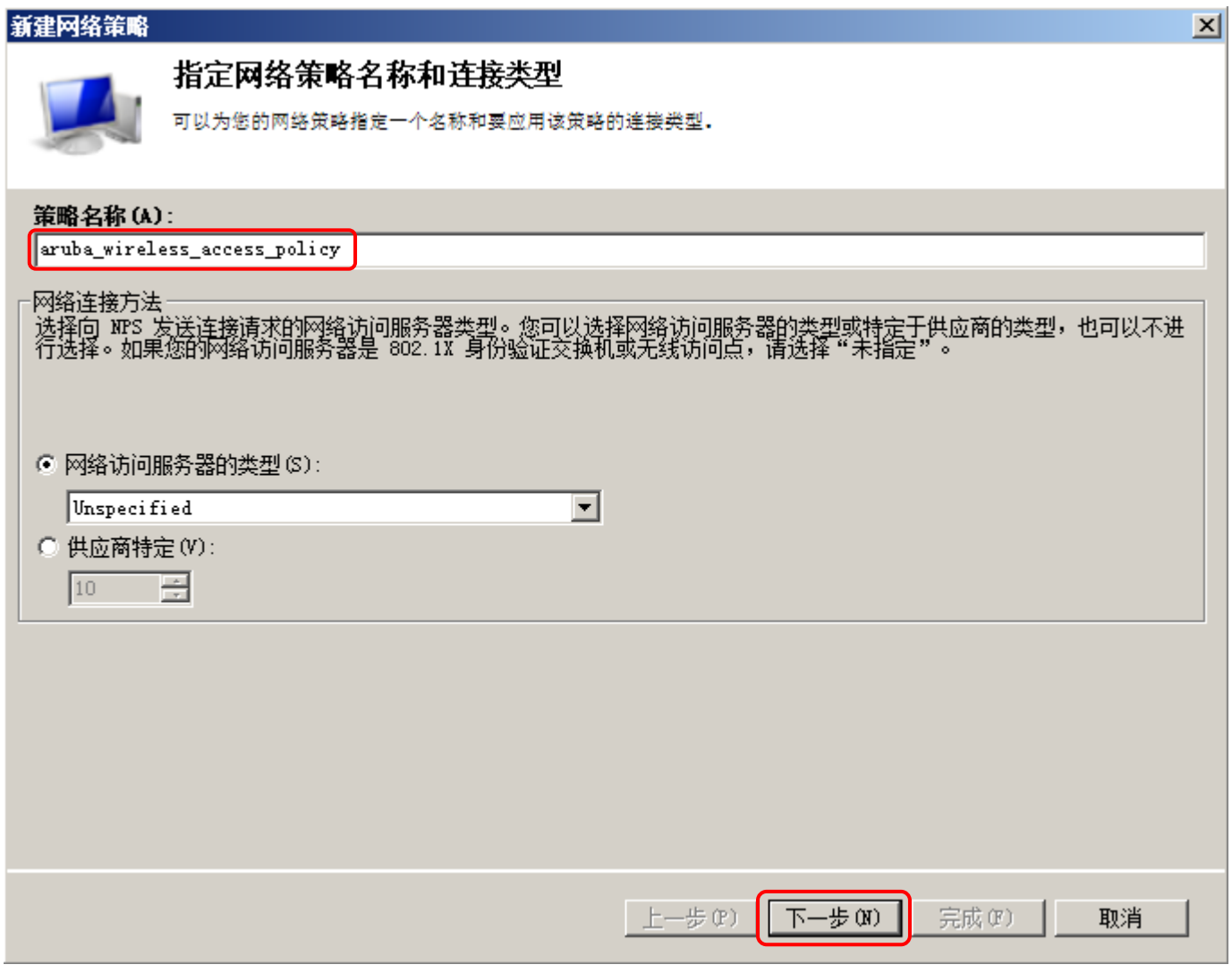


填写 RADIUS 基本信息：**友好名称、IP 地址、共享密钥，**点击**确定**



点击 **NPS（本地）** > **策略** > 右击**网络策略** > **新建**

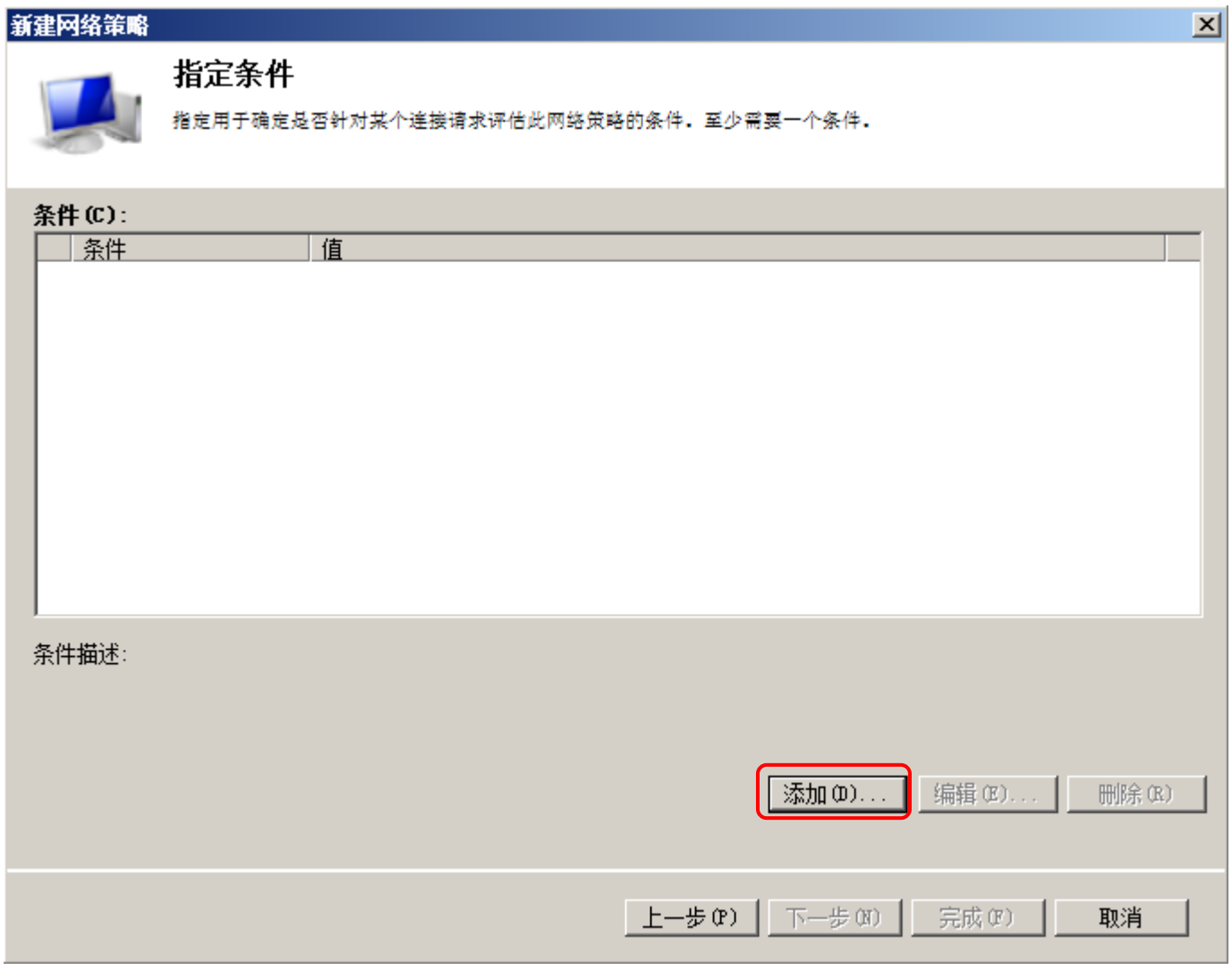
输入**策略名称**，点击**下一步**



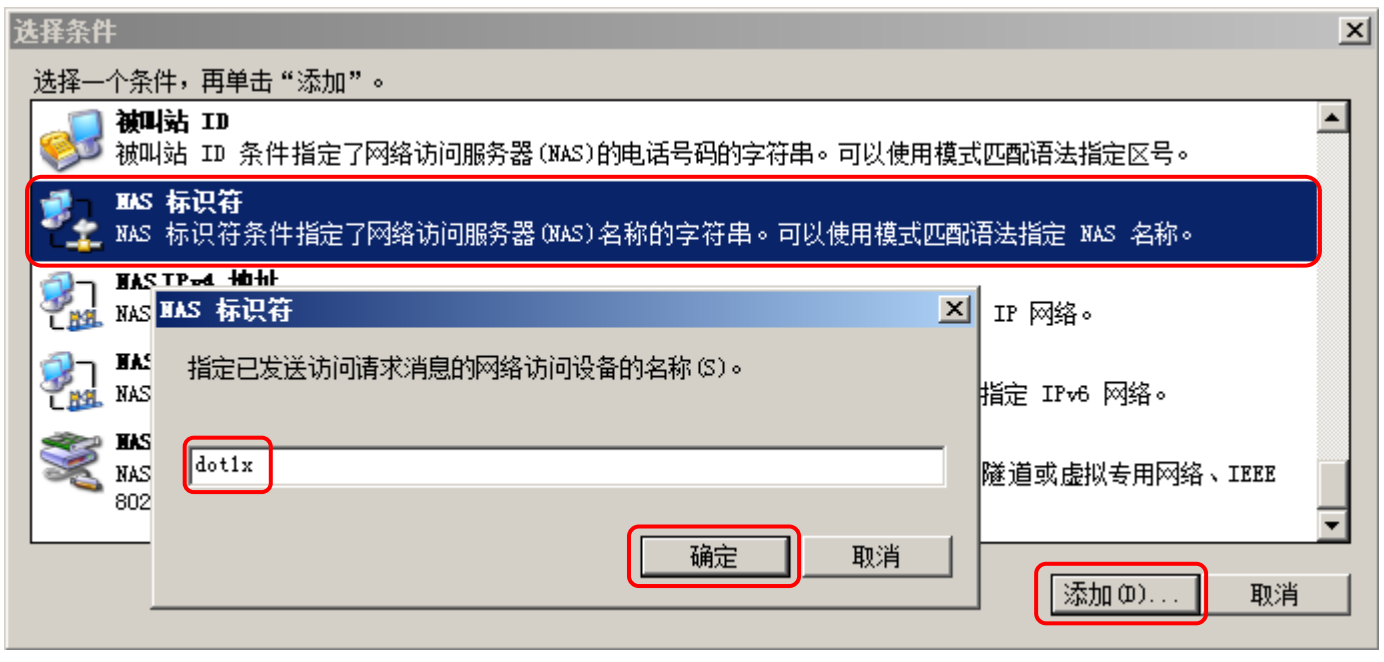
指定条件：如果某个连接请求匹配了制定条件，则击中该网络策略。

点击**添加**，添加指定条件，这里我们选择 NAS 标识符（**dot1x**）作为条件，一旦某个连接请求匹配了该 NAS 标识符，则击中该网络策略；

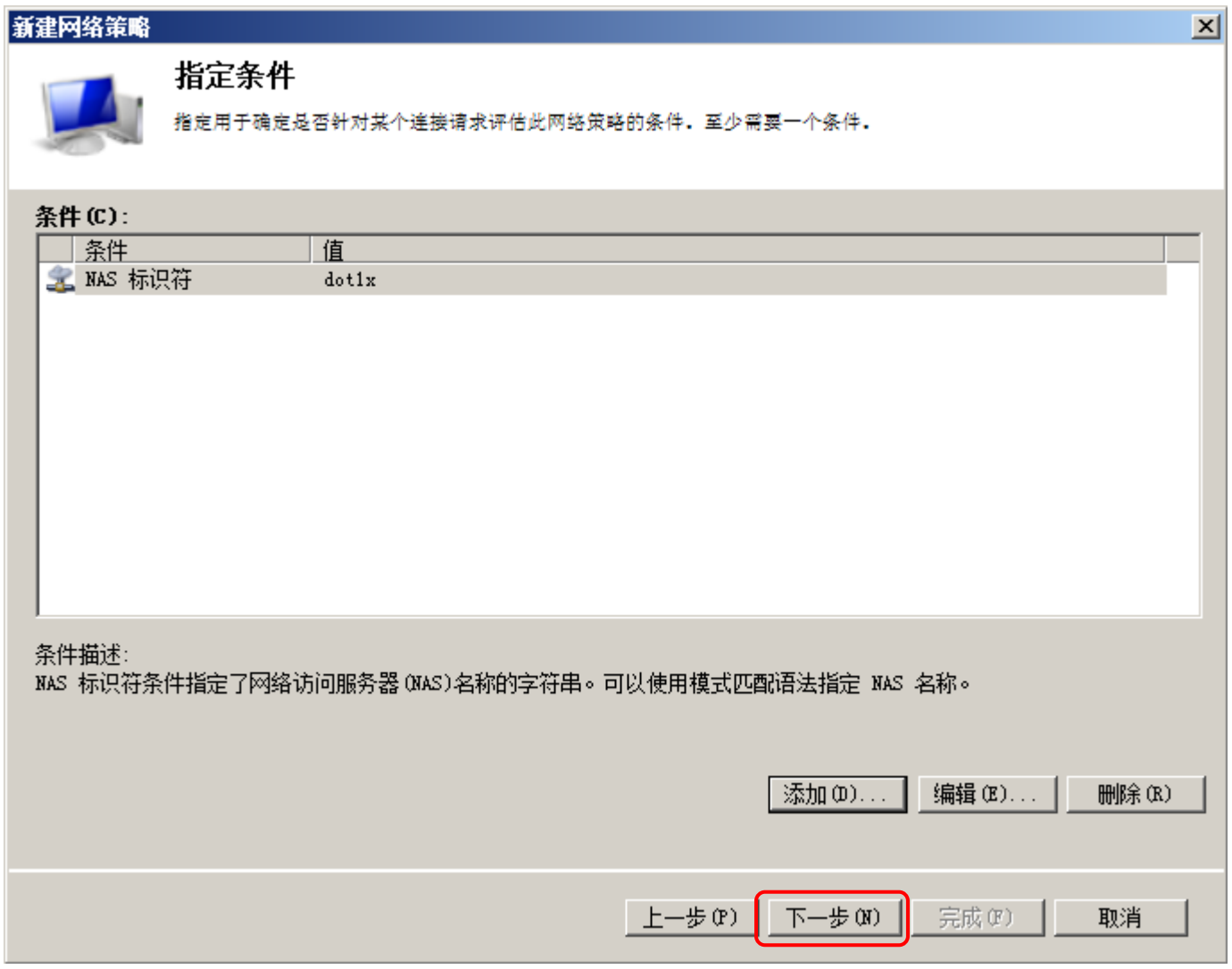
指定条件可以添加多个，至少需要一个指定条件



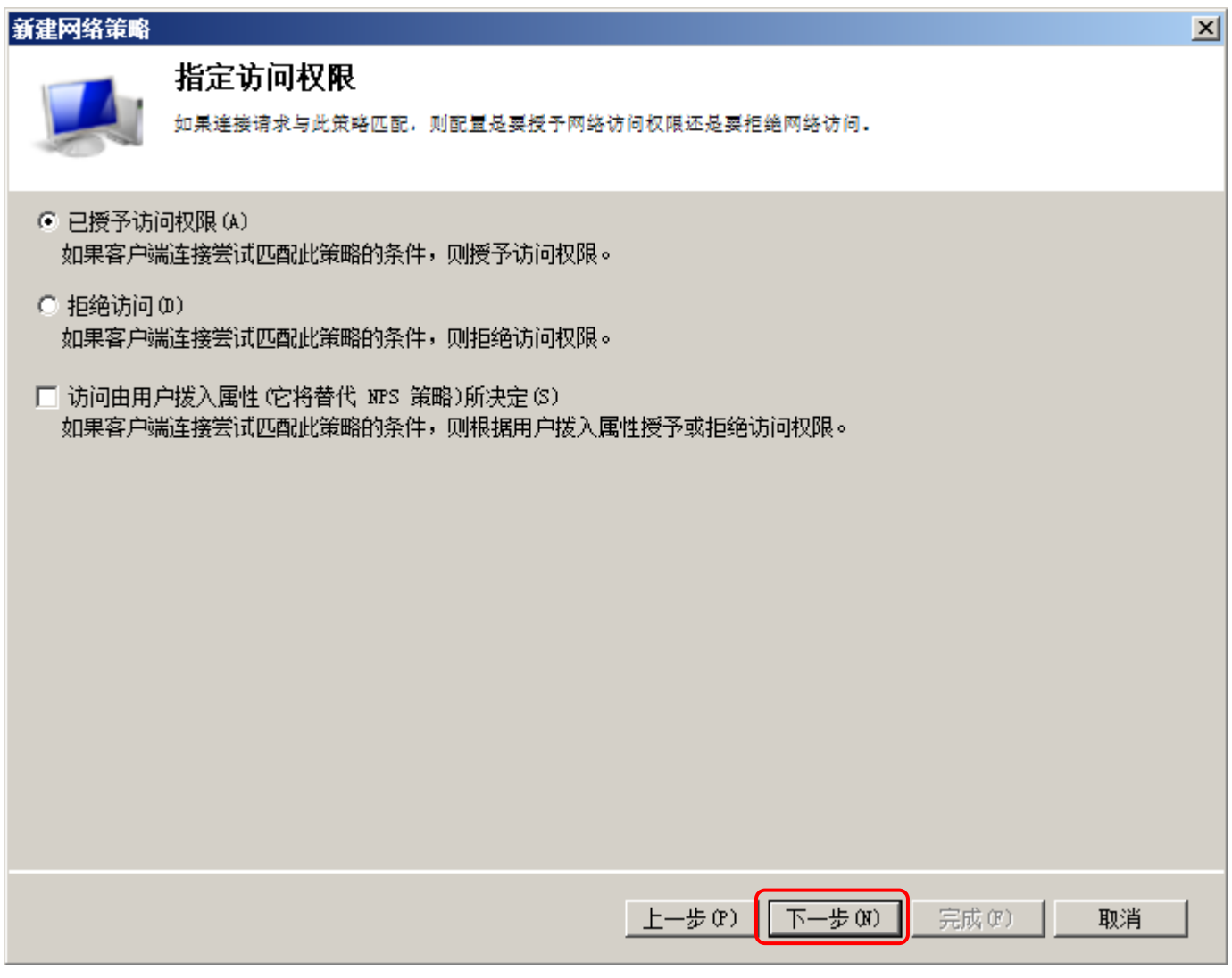
选中 **NAS 标识符**，点击**添加**，输入 NAS 标识符 **dot1x**，点击**确定**



点击**下一步**


新建网络策略
指定条件
指定用于确定是否针对某个连接请求评估此网络策略的条件。至少需要一个条件。
条件(C):
条件
值
NAS 标识符
dot1x
条件描述:
NAS 标识符条件指定了网络访问服务器(NAS)名称的字符串。可以使用模式匹配语法指定 NAS 名称。
添加(D)...
编辑(E)...
删除(R)
上一步(P)
下一步(N)
完成(F)
取消

点击**下一步**


新建网络策略
指定访问权限
如果连接请求与此策略匹配，则配置是要授予网络访问权限还是要拒绝网络访问。
已授予访问权限(A)
如果客户端连接尝试匹配此策略的条件，则授予访问权限。
拒绝访问(D)
如果客户端连接尝试匹配此策略的条件，则拒绝访问权限。
访问由用户拨入属性(它将替代 NPS 策略)所决定(S)
如果客户端连接尝试匹配此策略的条件，则根据用户拨入属性授予或拒绝访问权限。
上一步(P)
下一步(N)
完成(F)
取消

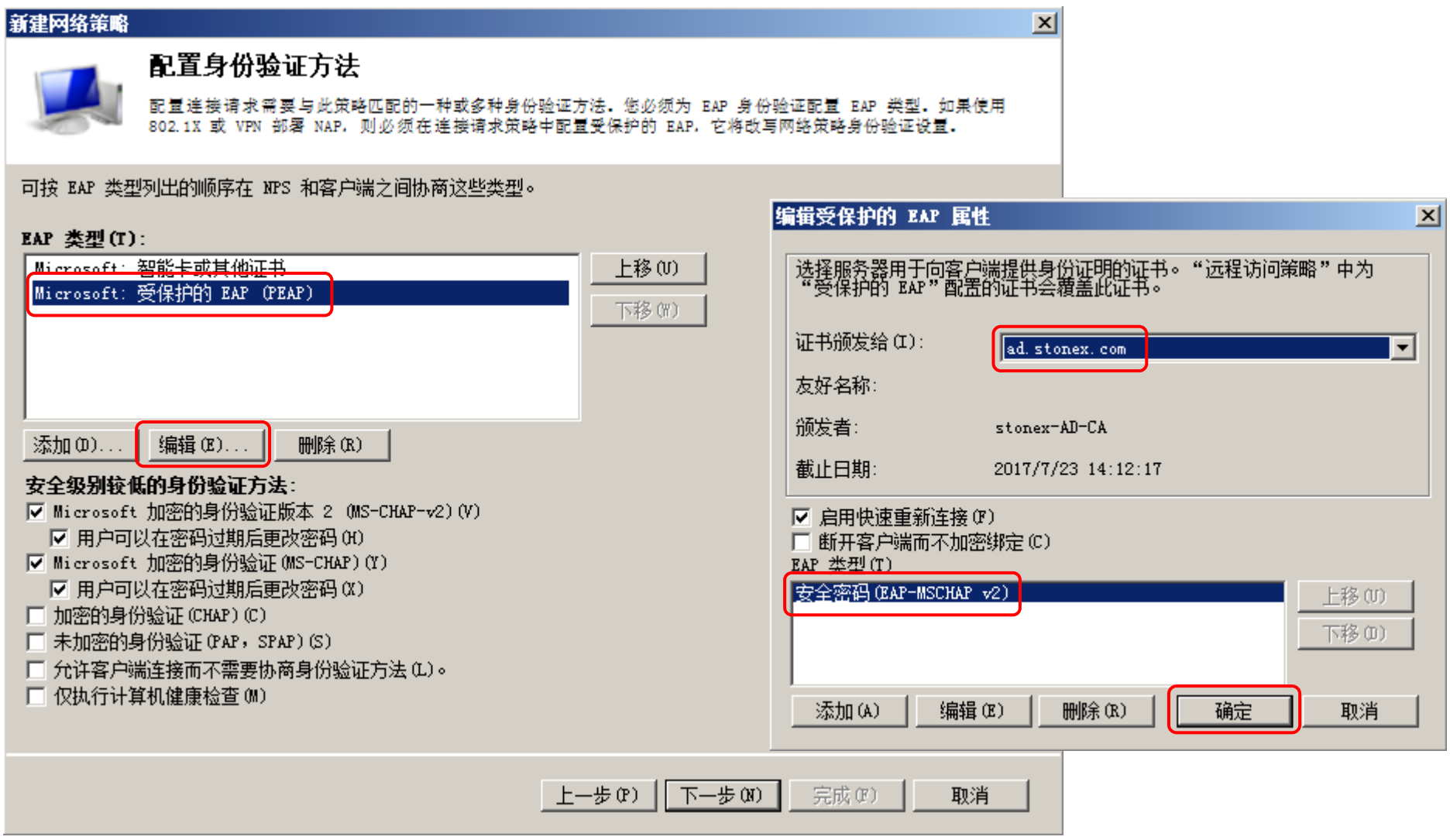
配置身份验证方法，这里我们添加 EAP-PEAPv0（PEAP-MSCHAPv2）和 EAP-TLS 两种 802.1X 认证

点击**添加**，选中**智能卡或其他证书**（即 EAP-TLS 认证），点击**确定**

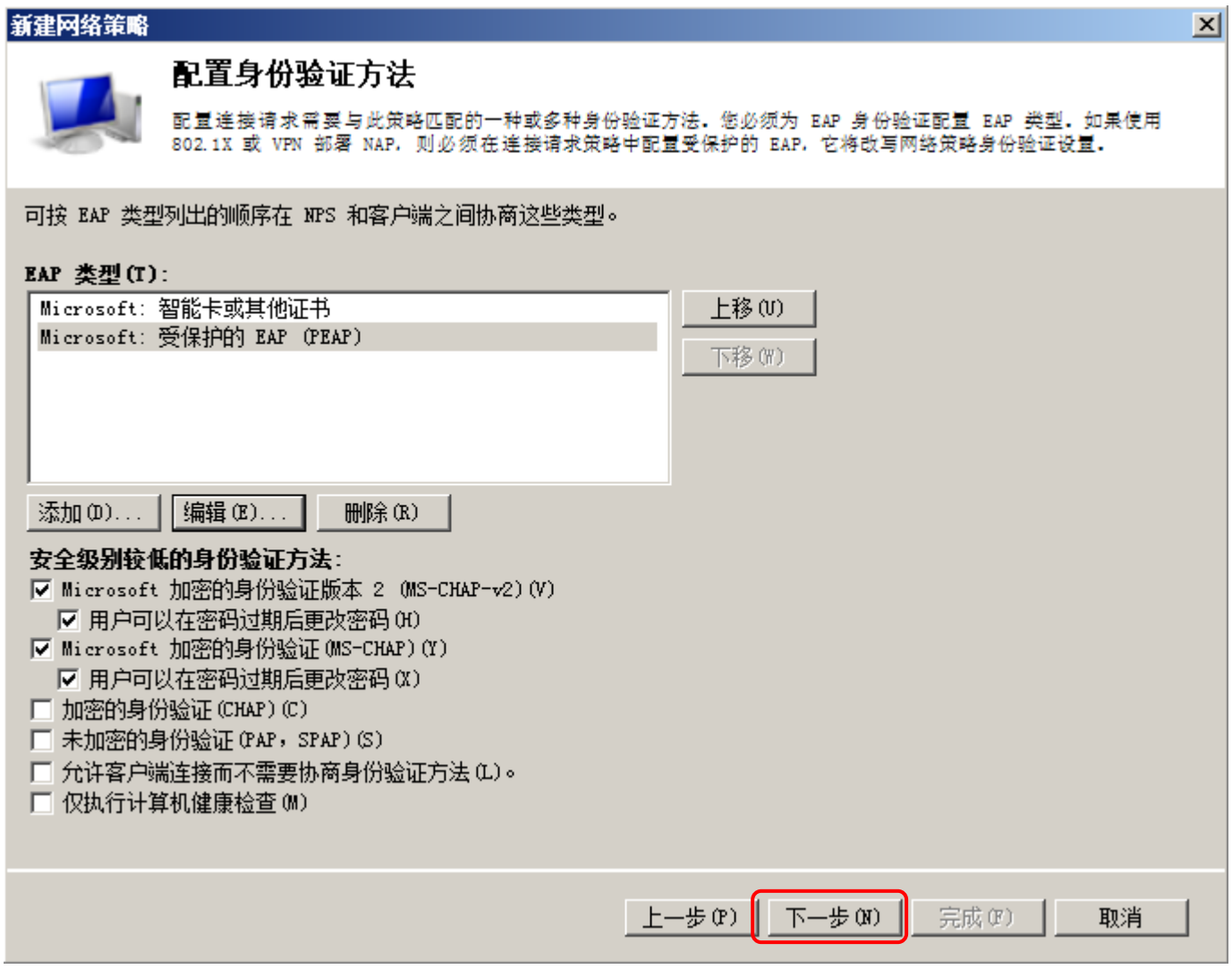
选中**智能卡或其他证书**，点击**编辑**，可以查看 EAP-TLS 认证方式向无线客户端表明其身份，提供的计算机证书是 ad.stonex.com

点击**添加**，选中 **Microsoft：受保护的 EAP（PEAP）**，点击**确定**

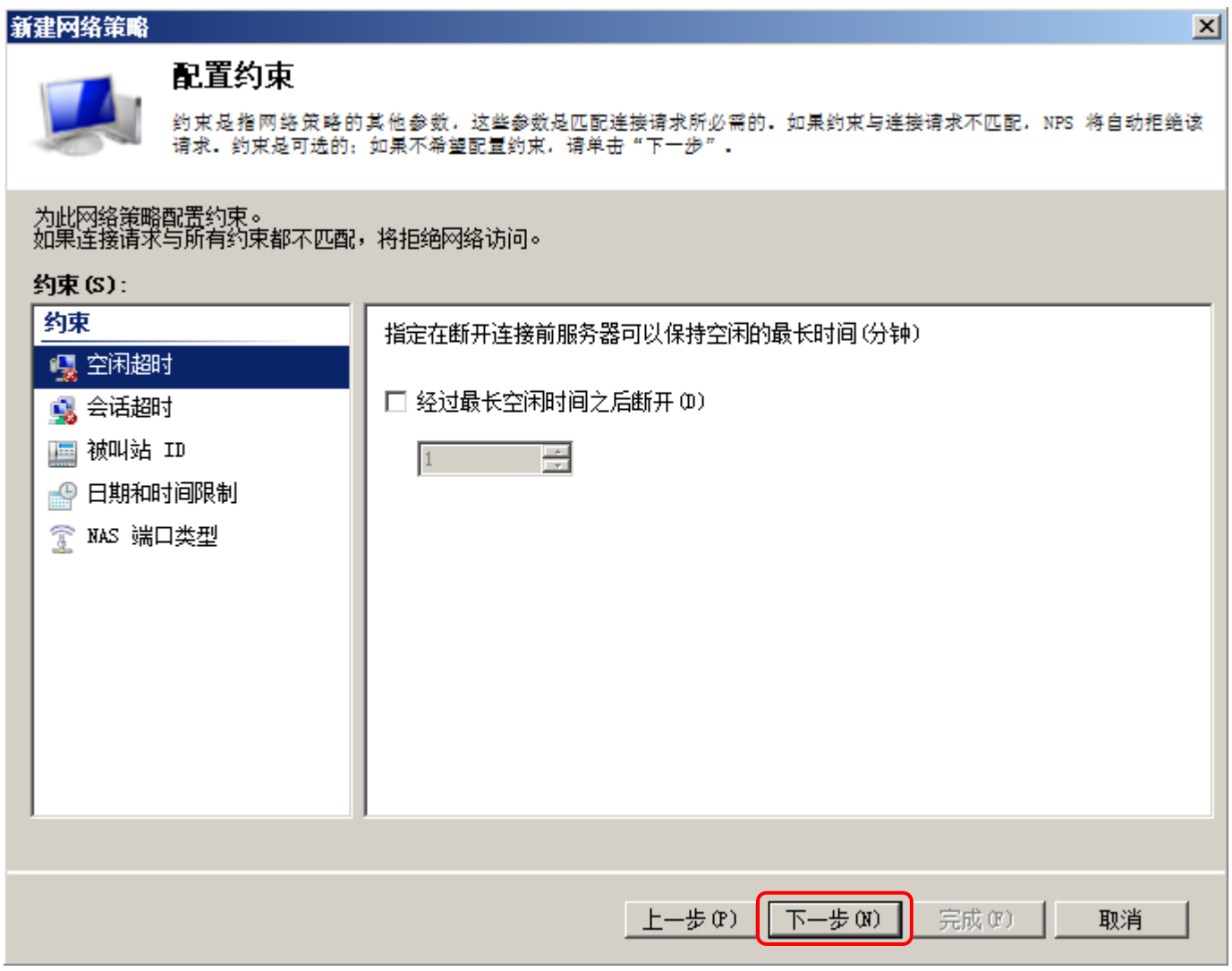
选中 **Microsoft：受保护的 EAP（PEAP）**，点击**编辑**，可以查看 Microsoft：受保护的 EAP（PEAP）认证方式向无线客户端表明其身份，提供的计算机证书是 ad.stonex.com，内层 EAP 是 EAP-MSCHVPv2。



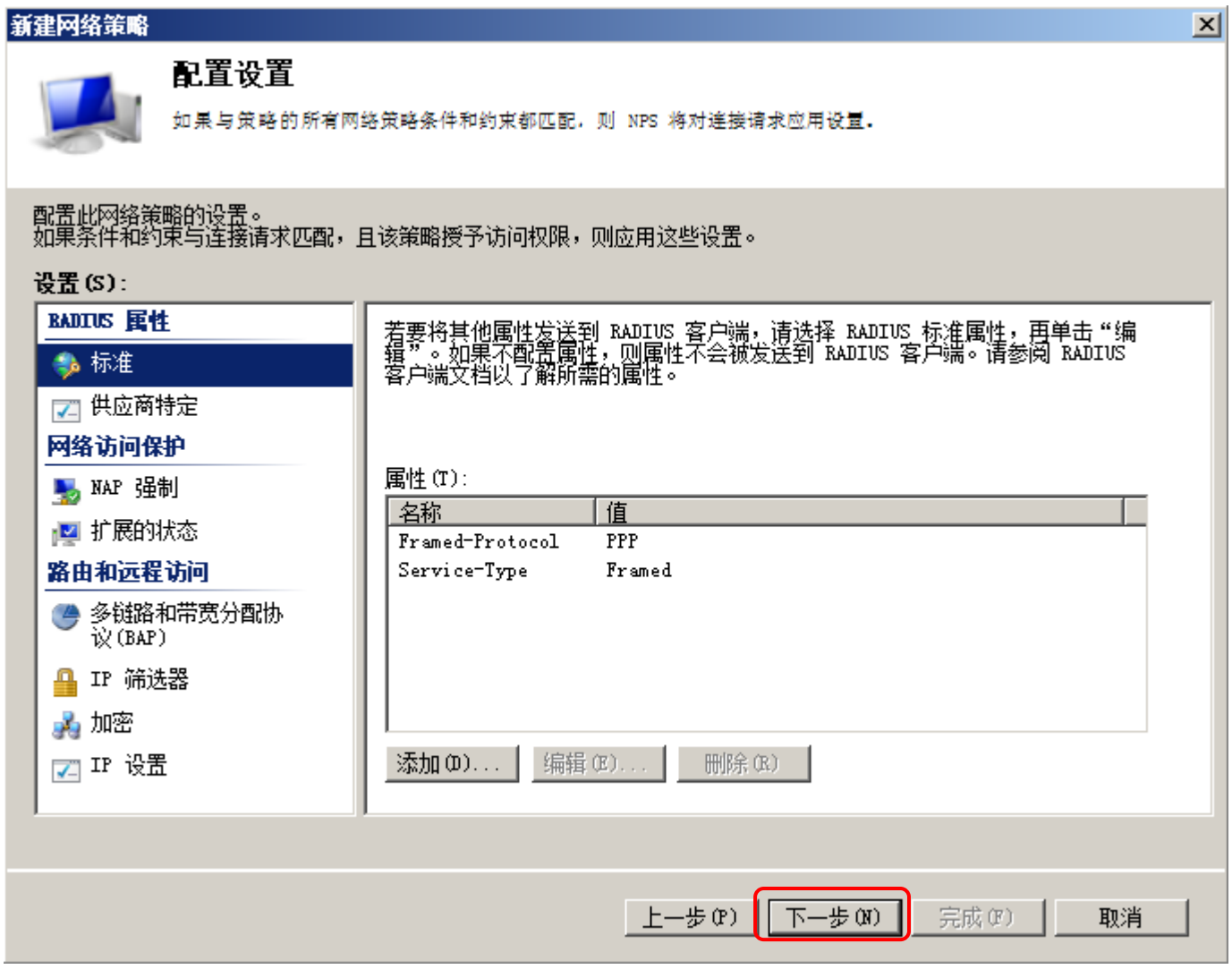
点击**下一步**


新建网络策略
配置身份验证方法
配置连接请求需要与此策略匹配的一种或多种身份验证方法。您必须为 EAP 身份验证配置 EAP 类型。如果使用 802.1X 或 VPN 部署 NAP，则必须在连接请求策略中配置受保护的 EAP，它将改写网络策略身份验证设置。
可按 EAP 类型列出的顺序在 NPS 和客户端之间协商这些类型。
EAP 类型(T):
Microsoft: 智能卡或其他证书
Microsoft: 受保护的 EAP (PEAP)
上移(U)
下移(W)
添加(D)...
编辑(E)...
删除(R)
安全级别较低的身份验证方法:
Microsoft 加密的身份验证版本 2 (MS-CHAP-v2)(V)
用户可以在密码过期后更改密码(H)
Microsoft 加密的身份验证(MS-CHAP)(Y)
用户可以在密码过期后更改密码(X)
加密的身份验证(CHAP)(C)
未加密的身份验证(PAP，SPAP)(S)
允许客户端连接而不需要协商身份验证方法(L)。
仅执行计算机健康检查(M)
上一步(P)
下一步(N)
完成(F)
取消

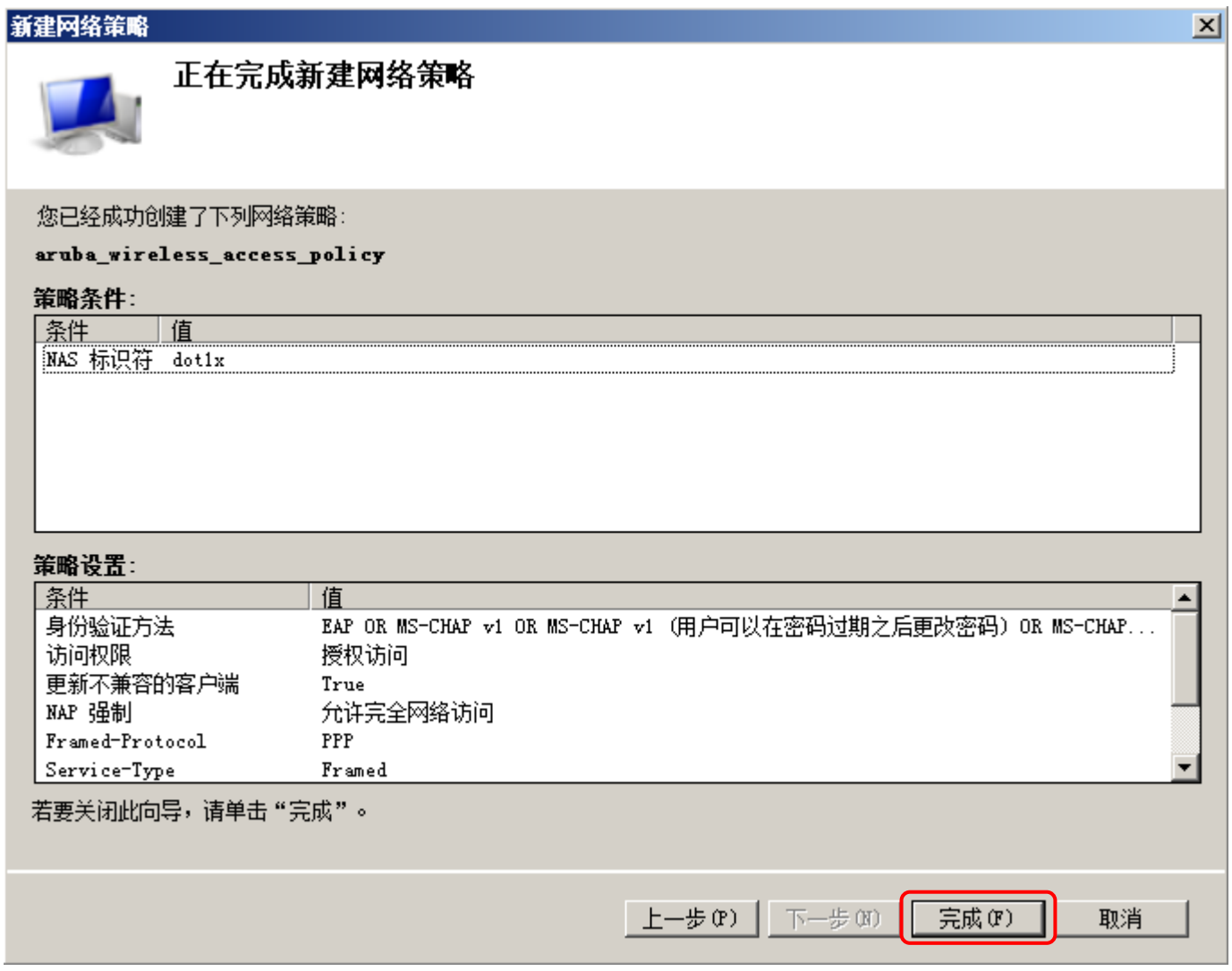
点击**下一步**

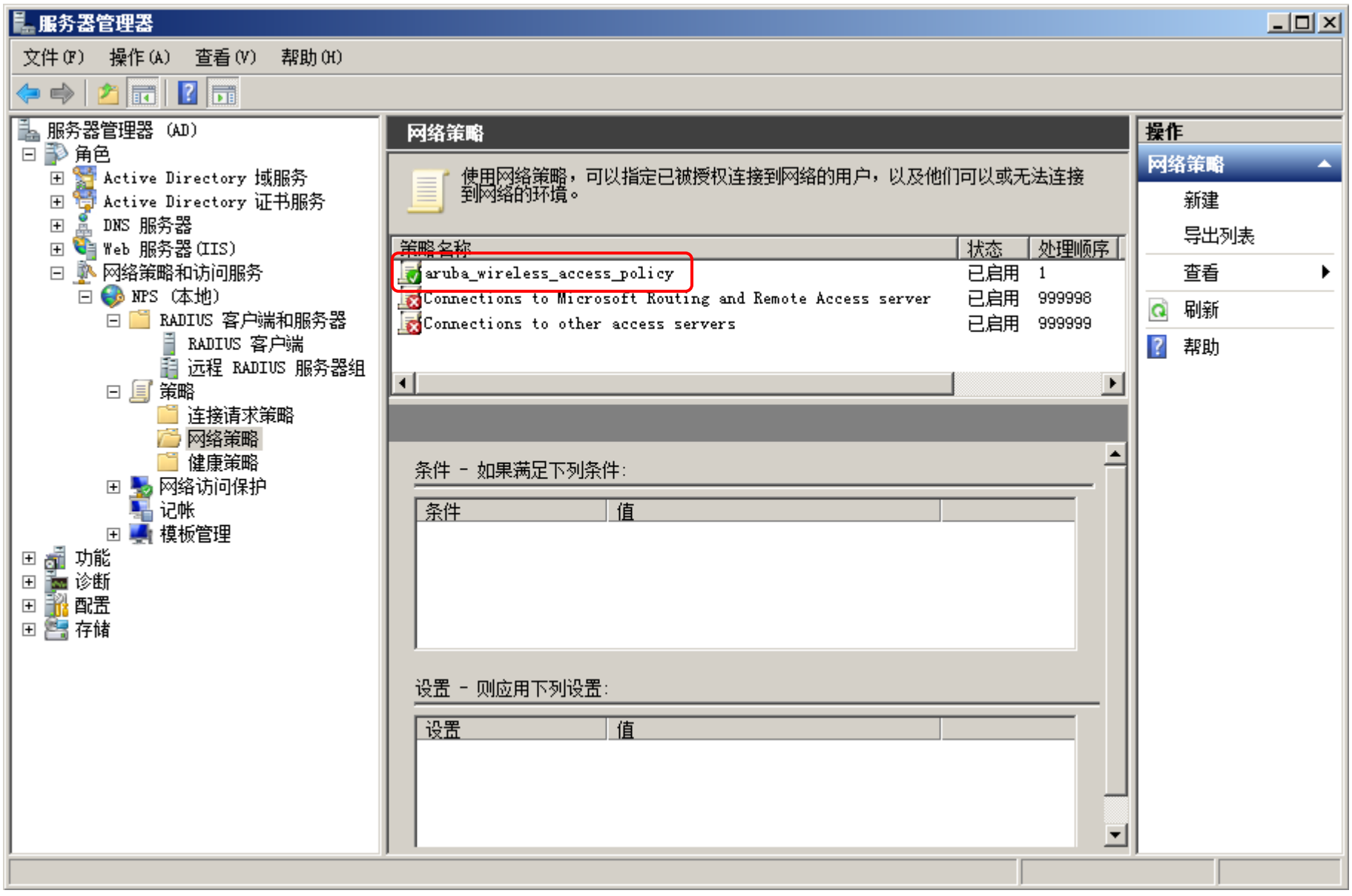

新建网络策略
配置约束
约束是指网络策略的其他参数，这些参数是匹配连接请求所必需的。如果约束与连接请求不匹配，NPS 将自动拒绝该请求。约束是可选的；如果不希望配置约束，请单击“下一步”。
为此网络策略配置约束。
如果连接请求与所有约束都不匹配，将拒绝网络访问。
约束(S):
约束
空闲超时
会话超时
被叫站 ID
日期和时间限制
NAS 端口类型
指定在断开连接前服务器可以保持空闲的最长时间(分钟)
经过最长空闲时间之后断开(D)
1
上一步(P)
下一步(N)
完成(F)
取消

点击**下一步**


新建网络策略
配置设置
如果与策略的所有网络策略条件和约束都匹配，则 NPS 将对连接请求应用设置。
配置此网络策略的设置。
如果条件和约束与连接请求匹配，且该策略授予访问权限，则应用这些设置。
设置(S):
RADIUS 属性
标准
供应商特定
网络访问保护
NAP 强制
扩展的状态
路由和远程访问
多链路和带宽分配协议(BAP)
IP 筛选器
加密
IP 设置
若要将其他属性发送到 RADIUS 客户端，请选择 RADIUS 标准属性，再单击“编辑”。如果不配置属性，则属性不会被发送到 RADIUS 客户端。请参阅 RADIUS 客户端文档以了解所需的属性。
属性(T):
名称
值
Framed-Protocol
PPP
Service-Type
Framed
添加(D)...
编辑(E)...
删除(R)
上一步(P)
下一步(N)
完成(F)
取消

点击**完成**


新建网络策略
正在完成新建网络策略
您已经成功创建了下列网络策略:
aruba_wireless_access_policy
策略条件:
条件
值
NAS 标识符
dot1x
策略设置:
条件
值
身份验证方法
EAP OR MS-CHAP v1 OR MS-CHAP v1 (用户可以在密码过期之后更改密码) OR MS-CHAP...
访问权限
授权访问
更新不兼容的客户端
True
NAP 强制
允许完全网络访问
Framed-Protocol
PPP
Service-Type
Framed
若要关闭此向导，请单击“完成”。
上一步(P)
下一步(N)
完成(F)
取消


服务器管理器
文件(F) 操作(A) 查看(V) 帮助(H)
服务器管理器 (AD)
角色
Active Directory 域服务
Active Directory 证书服务
DNS 服务器
Web 服务器(IIS)
网络策略和访问服务
NPS (本地)
RADIUS 客户端和服务器
RADIUS 客户端
远程 RADIUS 服务器组
策略
连接请求策略
网络策略
健康策略
网络访问保护
记帐
模板管理
功能
诊断
配置
存储
网络策略
使用网络策略，可以指定已被授权连接到网络的用户，以及他们可以或无法连接到网络的环境。
策略名称
状态
处理顺序
aruba_wireless_access_policy
已启用
1
Connections to Microsoft Routing and Remote Access server
已启用
999998
Connections to other access servers
已启用
999999
条件 - 如果满足下列条件:
条件
值
设置 - 则应用下列设置:
设置
值
操作
网络策略
新建
导出列表
查看
刷新
帮助

2.配置 Aruba 无线控制器

Aruba 控制器的 Controller ip 为 192.168.1.100

两个 VLAN 接口：Interface vlan 10 地址为 172.16.1.1/24，interface vlan 20 地址为 172.16.2.1/24

三个用户角色，Staff、Leader、IT

AP 所属的 AP Group 名称为 Demo-AP-Group

以上网络配置不体现在此文档

2.1 配置 EAP-PEAPv0（EAP-MSCHAPv2）认证

```
aaa authentication-server radius win-nps-server
    host 192.168.1.220
    key aruba123
    nas-identifier dot1x
```

#配置认证服务器，设置 NAS-ID 为 dot1x，以击中匹配设置的策略（aruba_wireless_access_policy）

```
aaa server-group nps-server-group
    auth-server win-nps-server
```

#配置认证服务器组

```
aaa profile peap-aaa-profile
    authentication-dot1x peap-auth-dot1x
    dot1x-default-role Staff
    dot1x-server-group nps-server-group
```

#配置 AAA Profile

#用户通过认证后拿到的默认用户角色为 Staff

```
wlan ssid-profile peap-ssid-profile
    essid PEAP
    opmode wpa2-aes
```

#配置 SSID Profile

```
wlan virtual-ap peap-vap-profile
    aaa-profile peap-aaa-profile
    ssid-profile peap-ssid-profile
    vlan 10
```

#配置 Virtual AP Profile

#用户通过认证后，默认拿到的 IP 地址属于 Vlan 10

```
ap-group Demo-AP-Group
    virtual-ap peap-vap-profile
```

#添加 virtual AP Profile 到 AP 组 Demo-AP-Group 下

2.2 配置 EAP-TLS 认证

```
aaa authentication-server radius win-nps-server
    host 192.168.1.220
    key aruba123
    nas-identifier dot1x
```

#配置认证服务器，设置 NAS-ID 为 dot1x，以击中匹配设置的策略（aruba_wireless_access_policy）

```
aaa server-group nps-server-group
    auth-server win-nps-server
```

#配置认证服务器组

```
aaa profile eap-tls-aaa-profile
    authentication-dot1x eap-tls-auth-dot1x
    dot1x-default-role Staff
    dot1x-server-group nps-server-group
```

#配置 AAA Profile

#用户通过认证后拿到的默认用户角色为 Staff

```
wlan ssid-profile eap-tls-ssid-profile
    essid PEAP
    opmode wpa2-aes
```

#配置 SSID Profile

```
wlan virtual-ap eap-tls-vap-profile
    aaa-profile eap-tls-aaa-profile
    ssid-profile eap-tls-ssid-profile
    vlan 10
```

#配置 Virtual AP Profile

#用户通过认证后，默认拿到的 IP 地址属于 Vlan 10

```
ap-group Demo-AP-Group
    virtual-ap eap-tls-vap-profile
```

#添加 virtual AP Profile 到 AP 组 Demo-AP-Group 下

以上步骤完成完成以后，AP 会是放出两个 SSID，PEAP 和 EAP-TLS

3.证书管理与配置客户端测试 802.1X 认证

根据 802.1X 认证类型的不同，无线客户端和 RADIUS 服务器所需要的证书也不同，EAP-PEAPv0（EAP-MSCHAPv2）和 EAP-TLS 认证所需的证书如下：

认证类型	安装在客户端上的证书	安装在 RAIDUS 服务器上的证书
EAP-PEAPv0（EAP-MSCHAPv2）	**根 CA 证书** 用于验证 RADIUS 服务器的合法性	**计算机证书** 向客户端证明其身份
EAP-TLS	**用户证书** 向 RADIUS 服务器证明其身份合法性 **根 CA 证书** 用于验证 RADIUS 服务器的合法性	**计算机证书** 向客户端证明其身份 **根 CA 证书** 用于验证用户证书的合法性

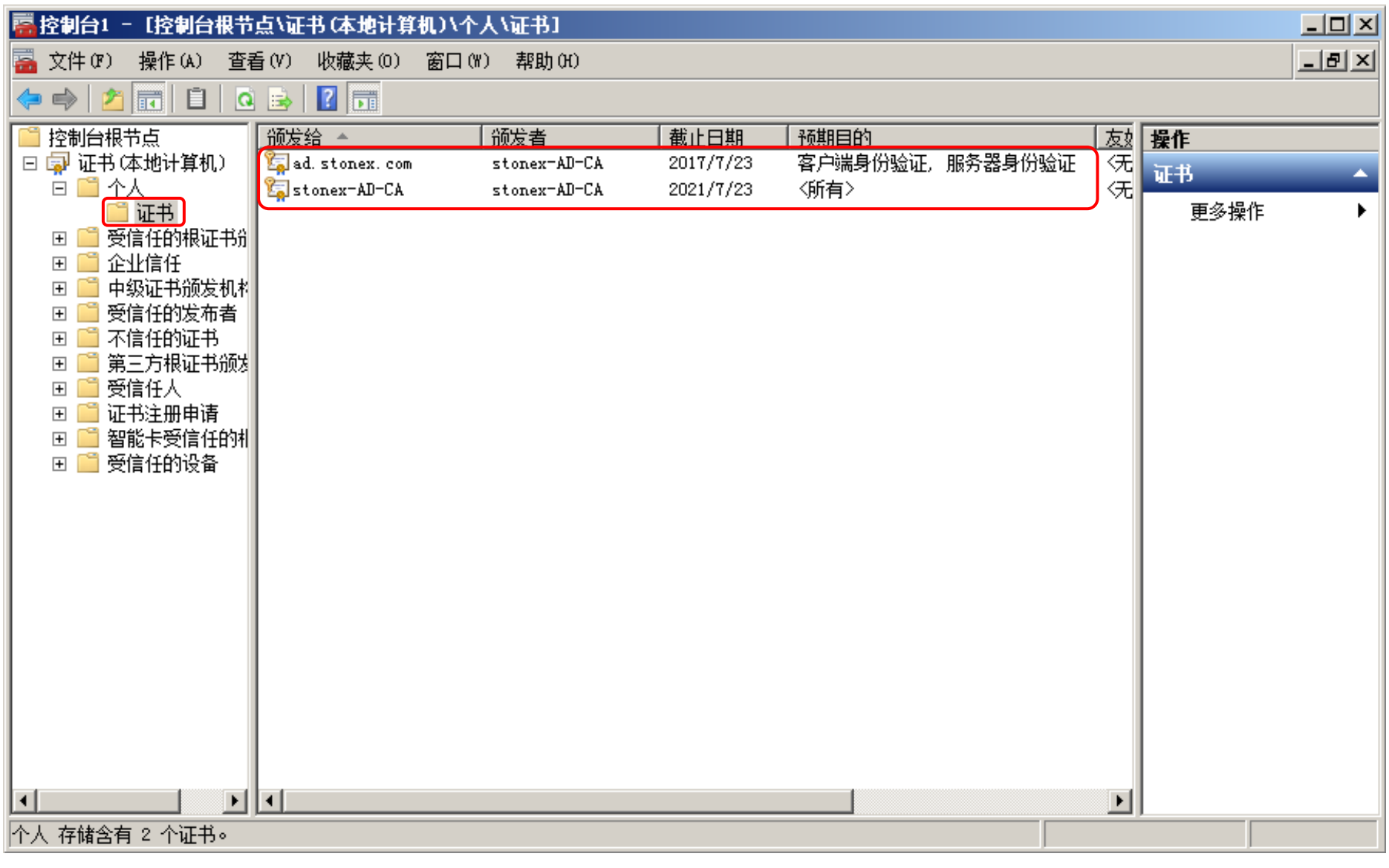
注意：以上为 EAP 终结在 RADIUS 服务器上的情况

根 CA 证书是 CA 认证中心给自己颁发的证书，是信任链的起始点。安装根 CA 证书意味着对这个 CA 认证中心的信任。

3.1 管理 NPS（RADIUS 服务器）的证书

管理 NPS（RADIUS 服务器）证书参考 1.5 章节

NPS 上的计算机证书和根 CA 证书如下图所示



3.2 管理无线客户端的证书

对于 Windows 客户端来说，可以分为加域的客户端和没有加入域的客户端（工作组模式）两种：

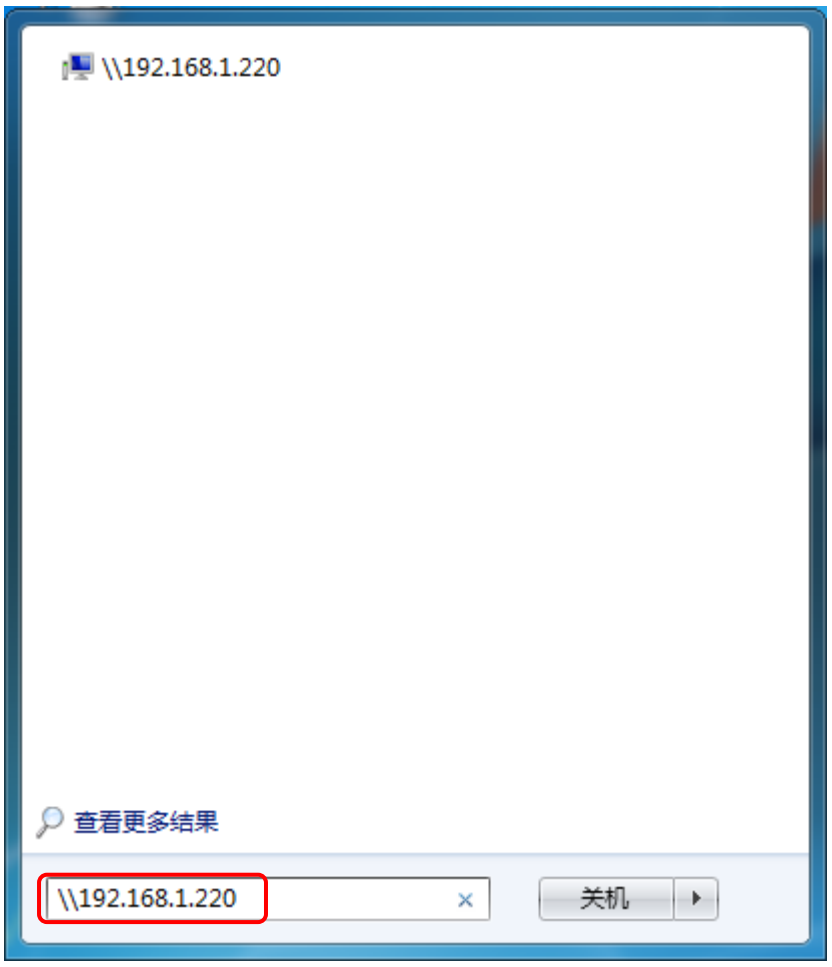
- 没有加入域的客户端，需要手动安装根 CA 证书和用户证书
- 加入域的客户端，会自动安装根 CA 证书，用户证书可以手动安装，也可以通过域策略自动下发安装。

3.2.1 没有加域的客户端安装根 CA 证书

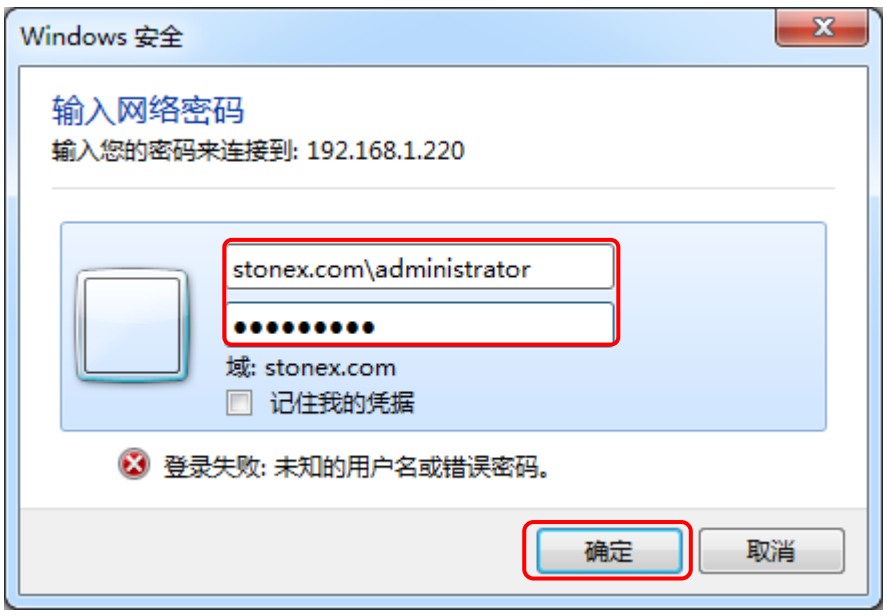
没有加入域的客户端（工作组模式）需要手动导入根 CA 证书到计算机，如果客户端加入了域则可以省略此步骤。有两种方法可以导入根证书：

- **方案一：**客户端需要接入网络，以访问证书服务器的共享文件夹方式来导入根 CA 证书

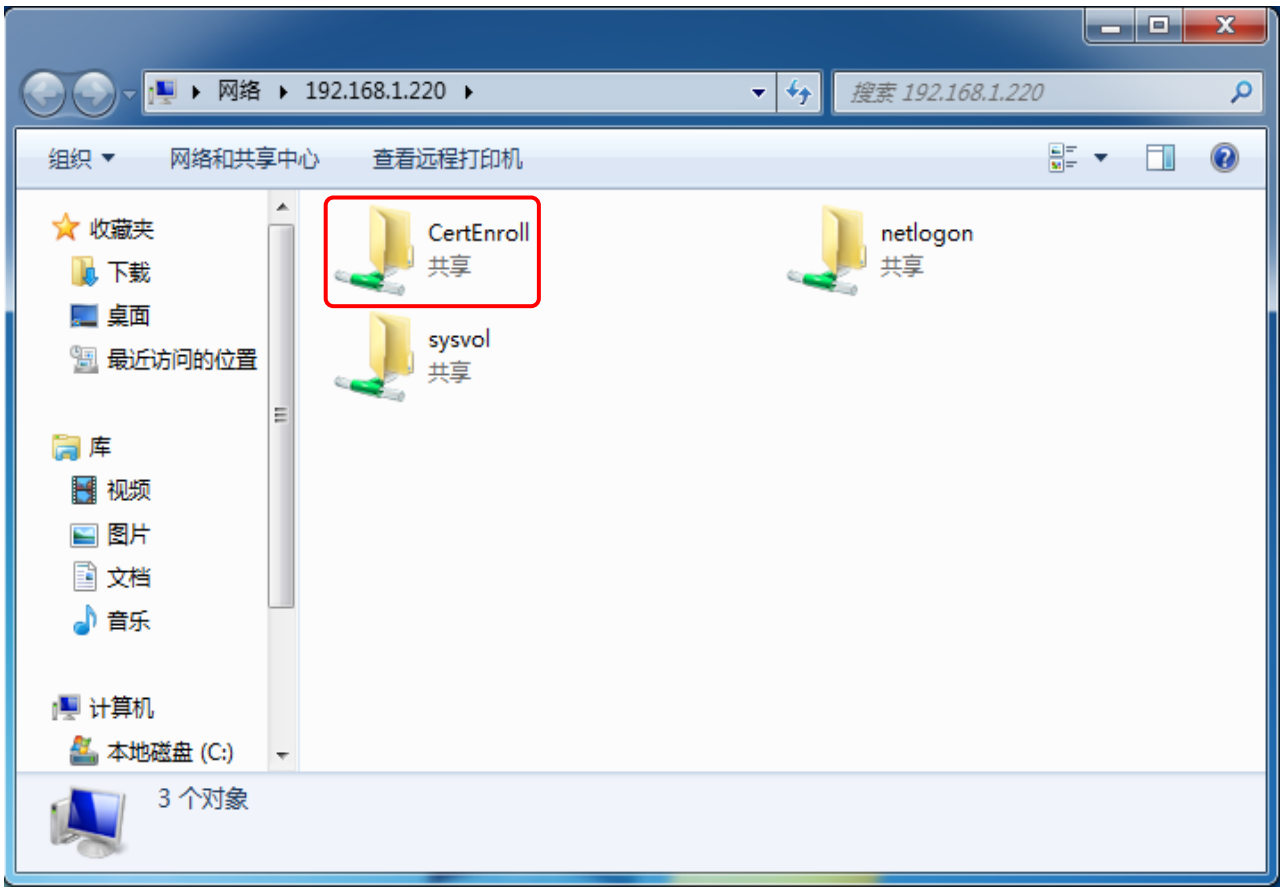
点击**开始** > 输入**\\192.168.1.220**



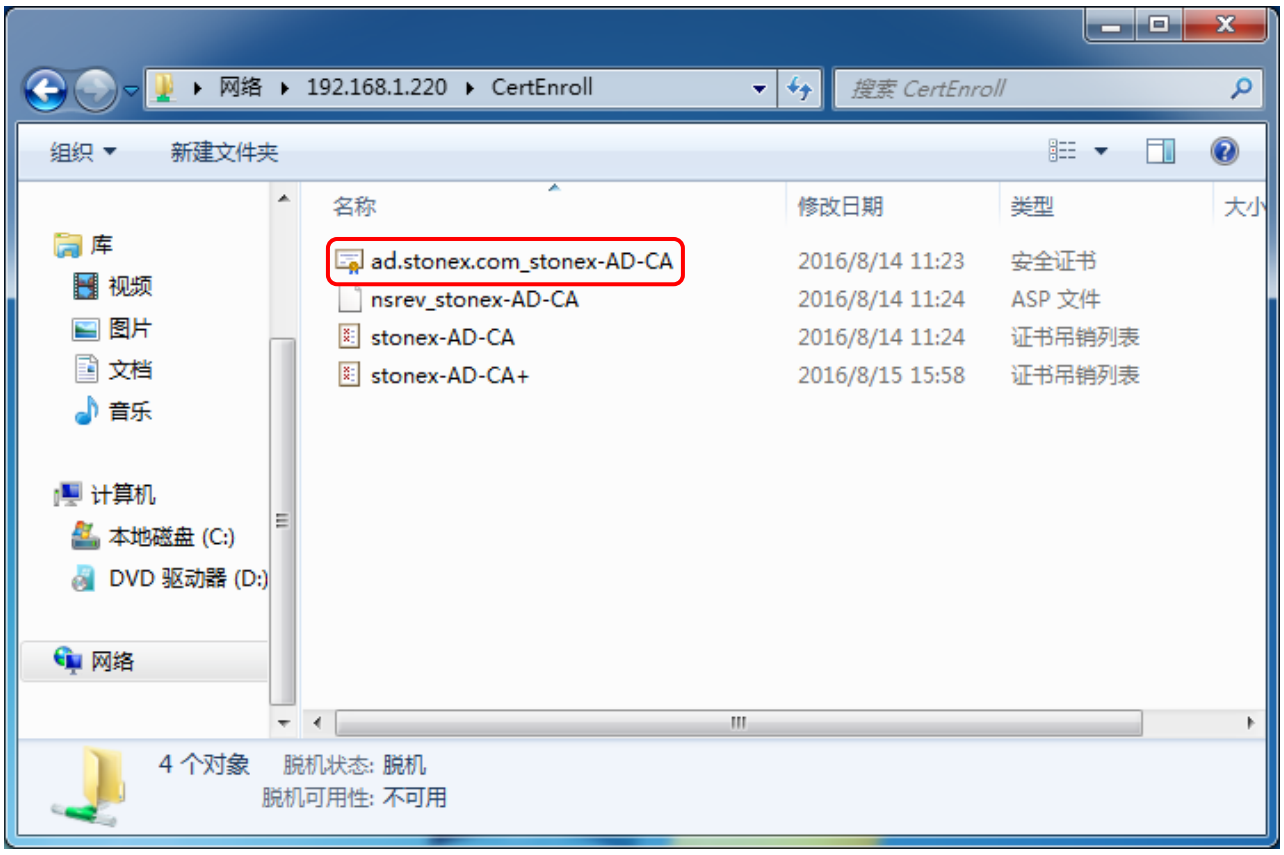
输入用户名和密码，点击**确定**



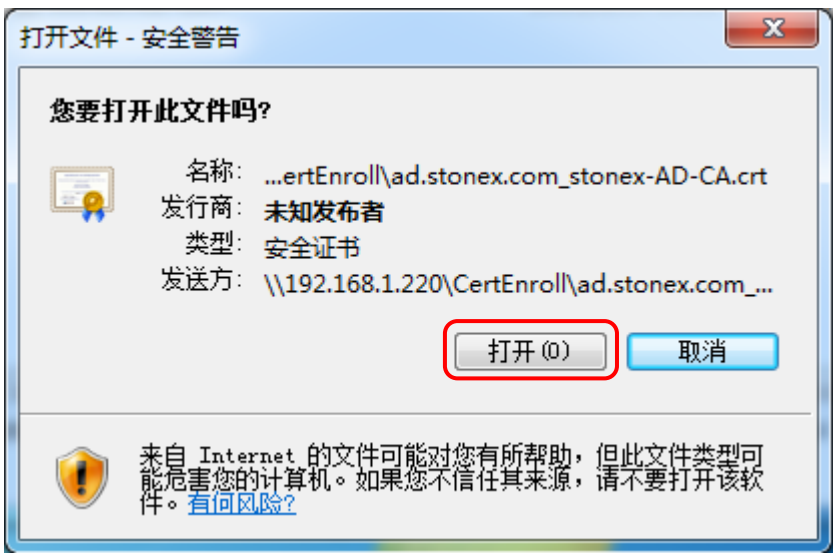
打开文件夹 **CertEnroll**



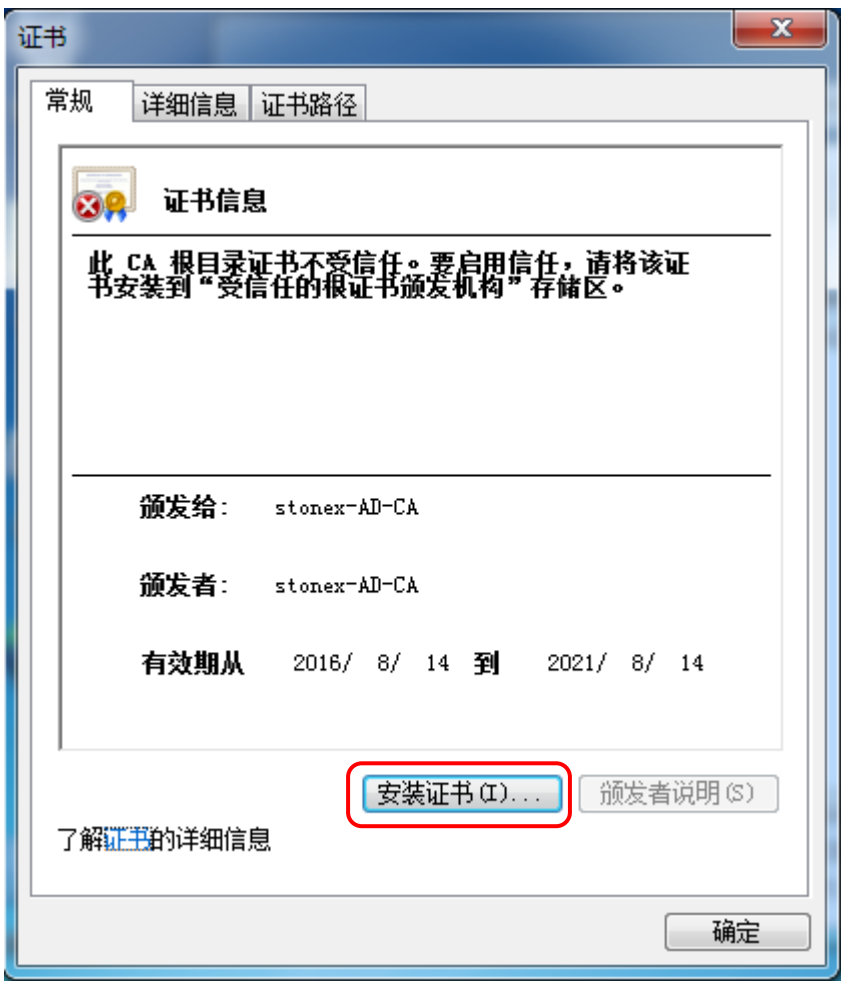
点击 **ad.stonex.com_stonex-AD-CA** 进行安装



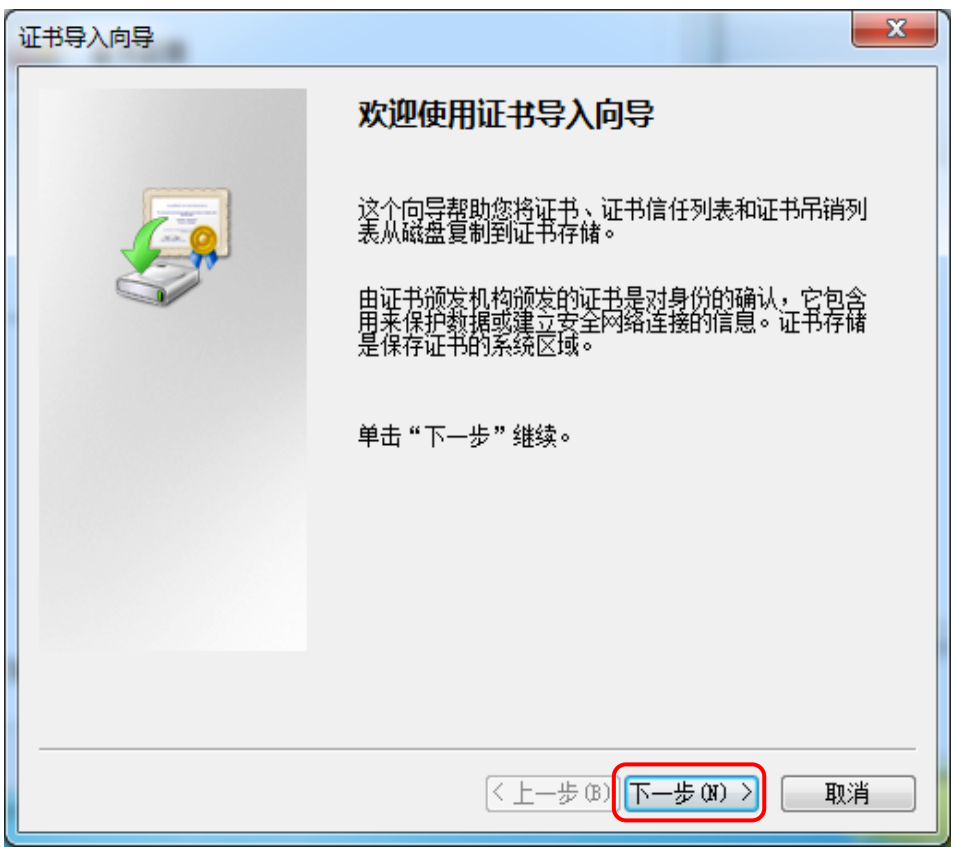
点击**打开**



点击**安装证书**

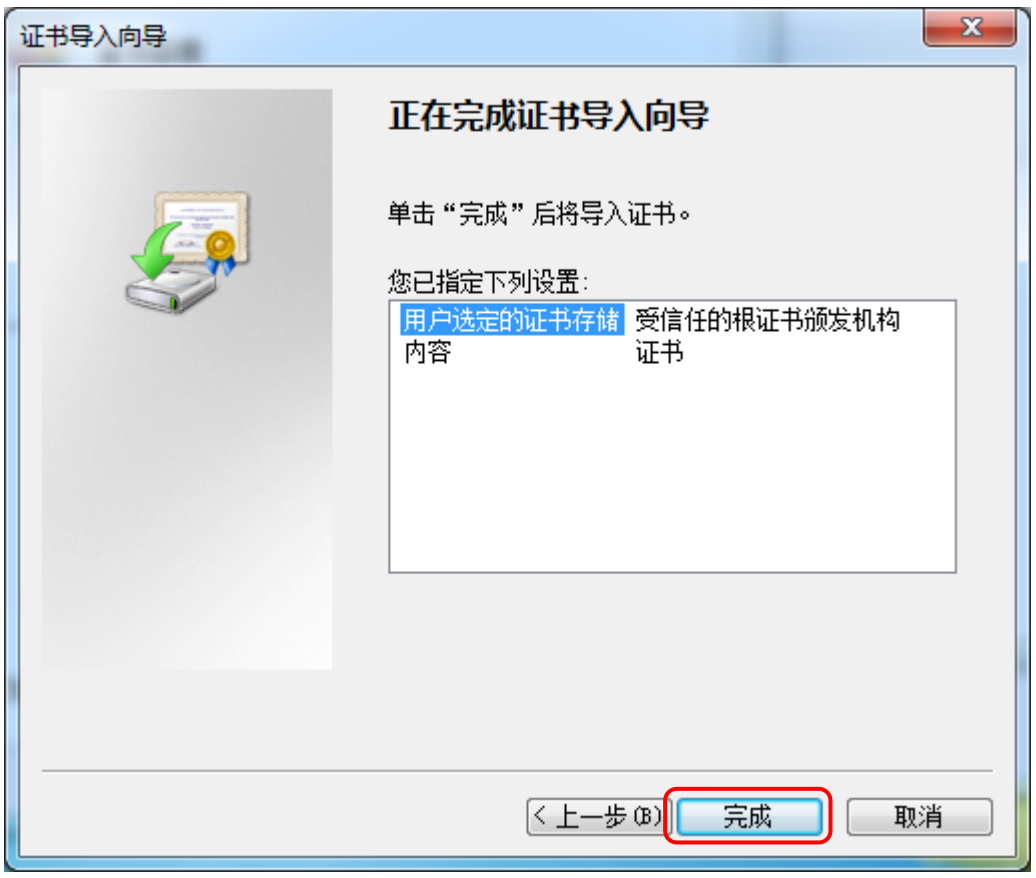


点击**下一步**

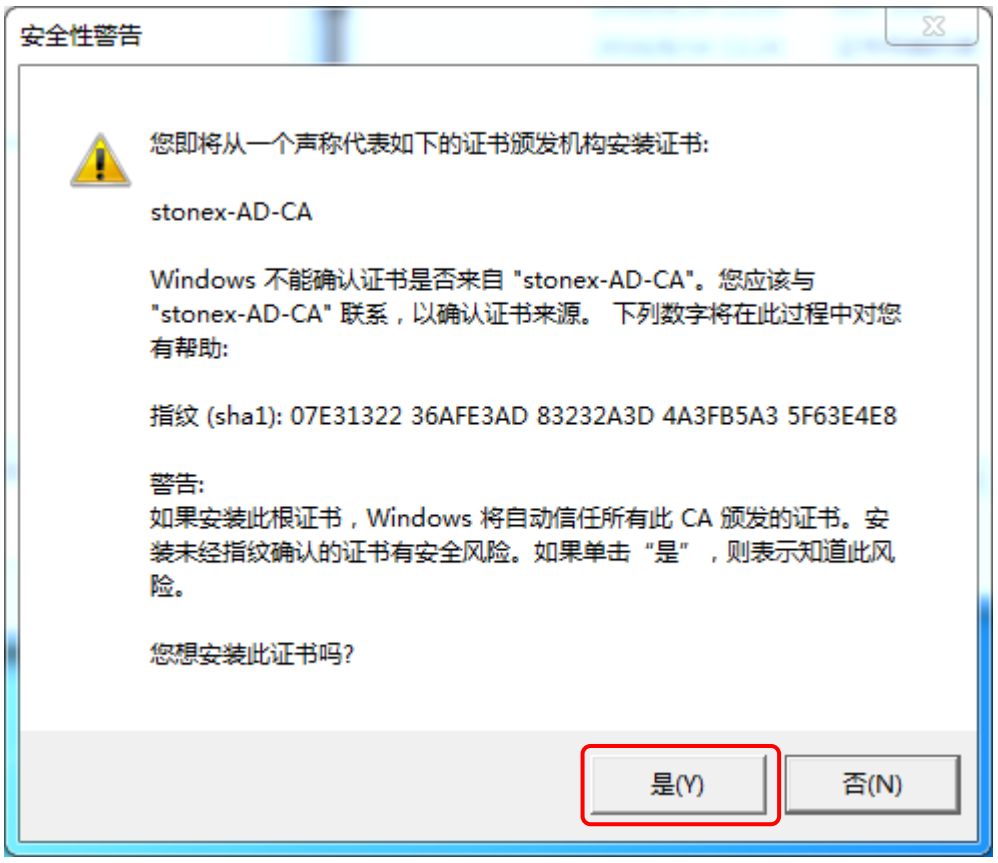


选择将证书存储在**受信任的根证书颁发机构**，点击**下一步**

点击**完成**



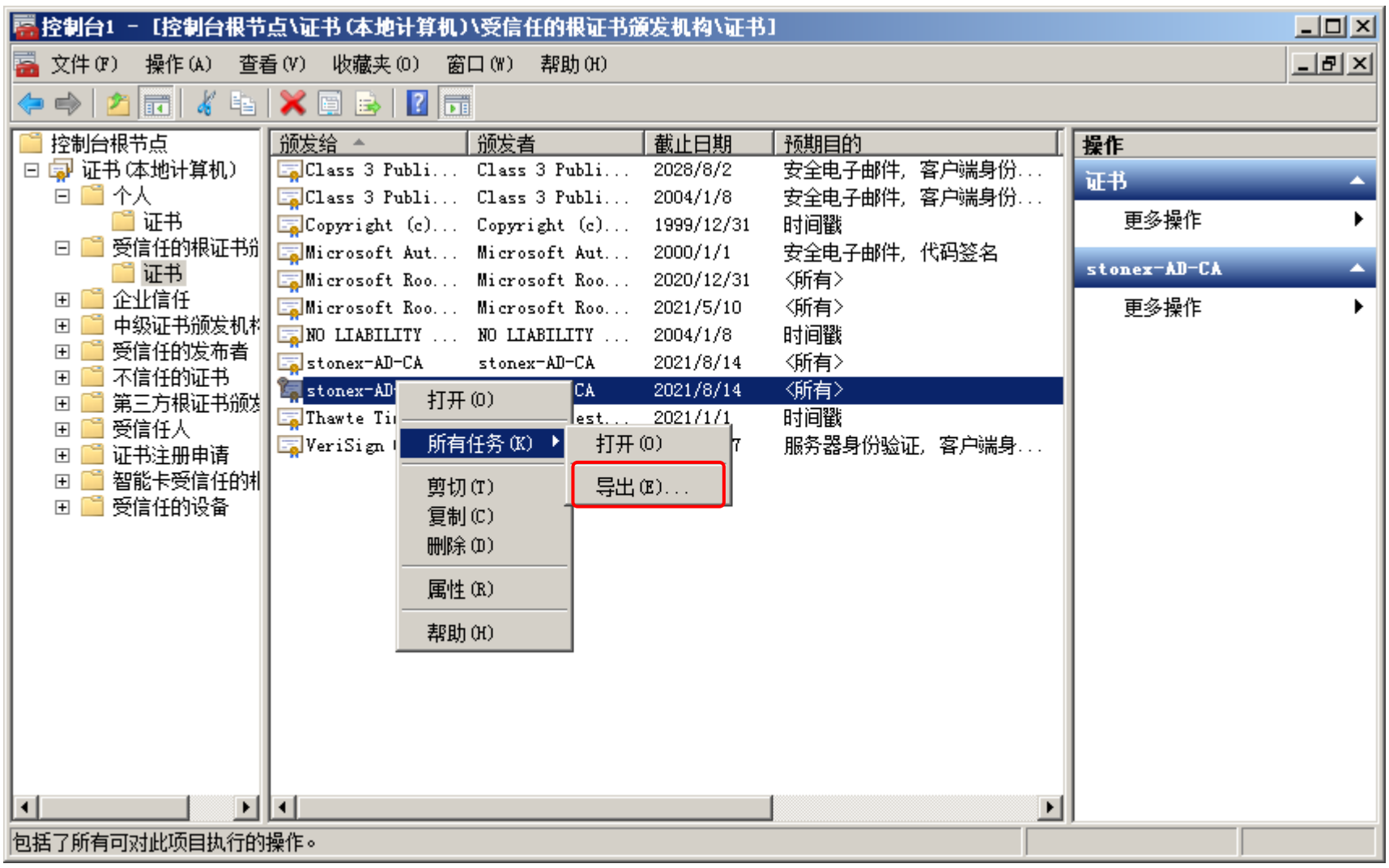
选择**是**



点击**确定**，根证书安装完成

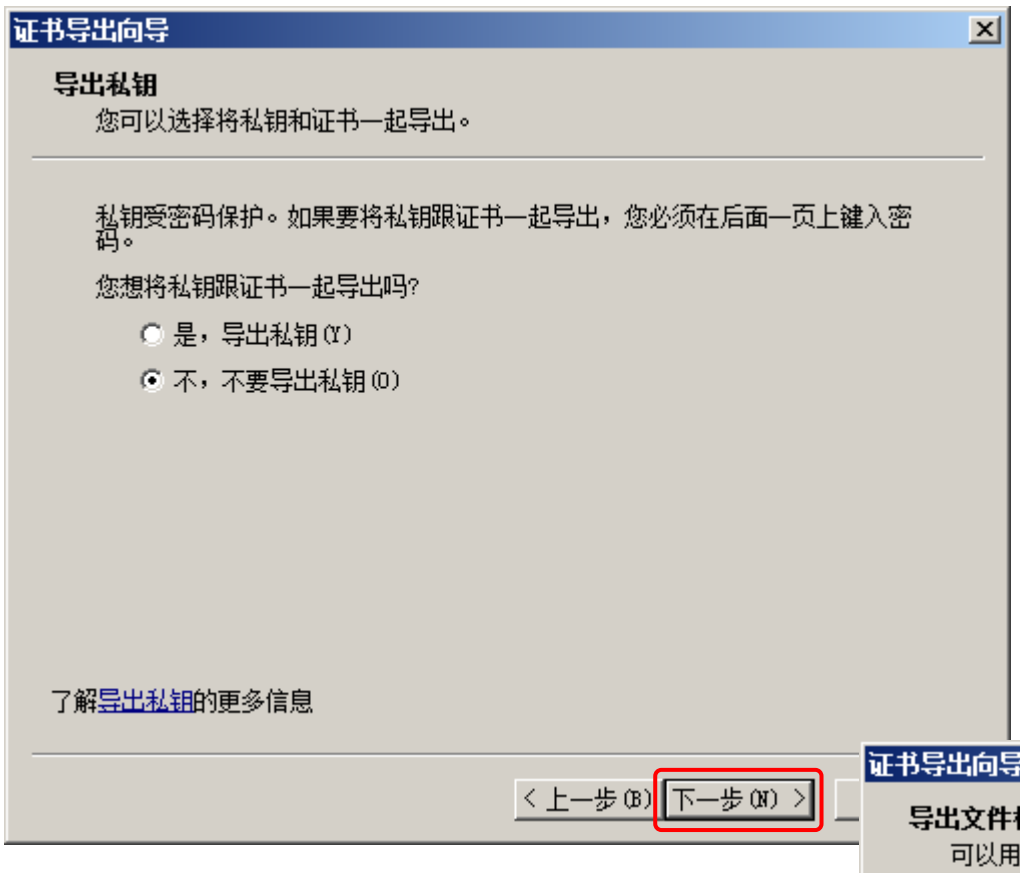
- **方案二：**从服务器导出根 CA 证书，再导入到客户端计算机上

右击**根证书（stonex-AD-CA） -> 所有任务 -> 导出**

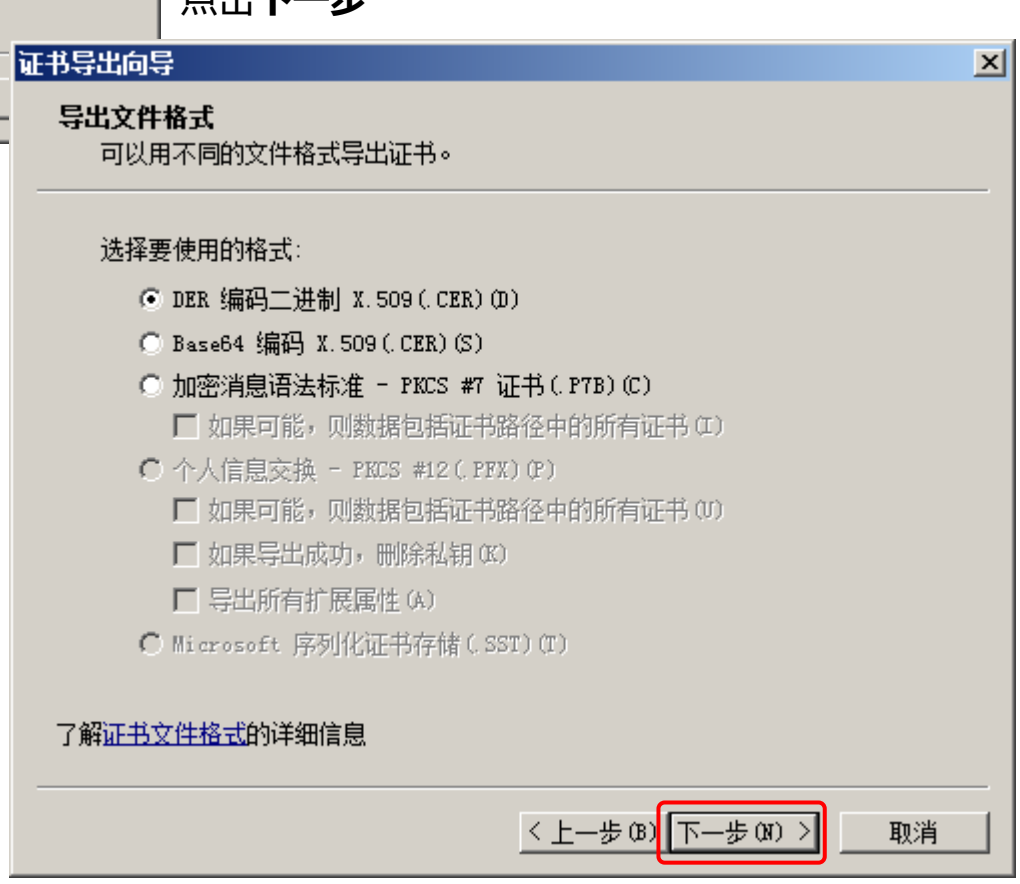


点击**下一步**

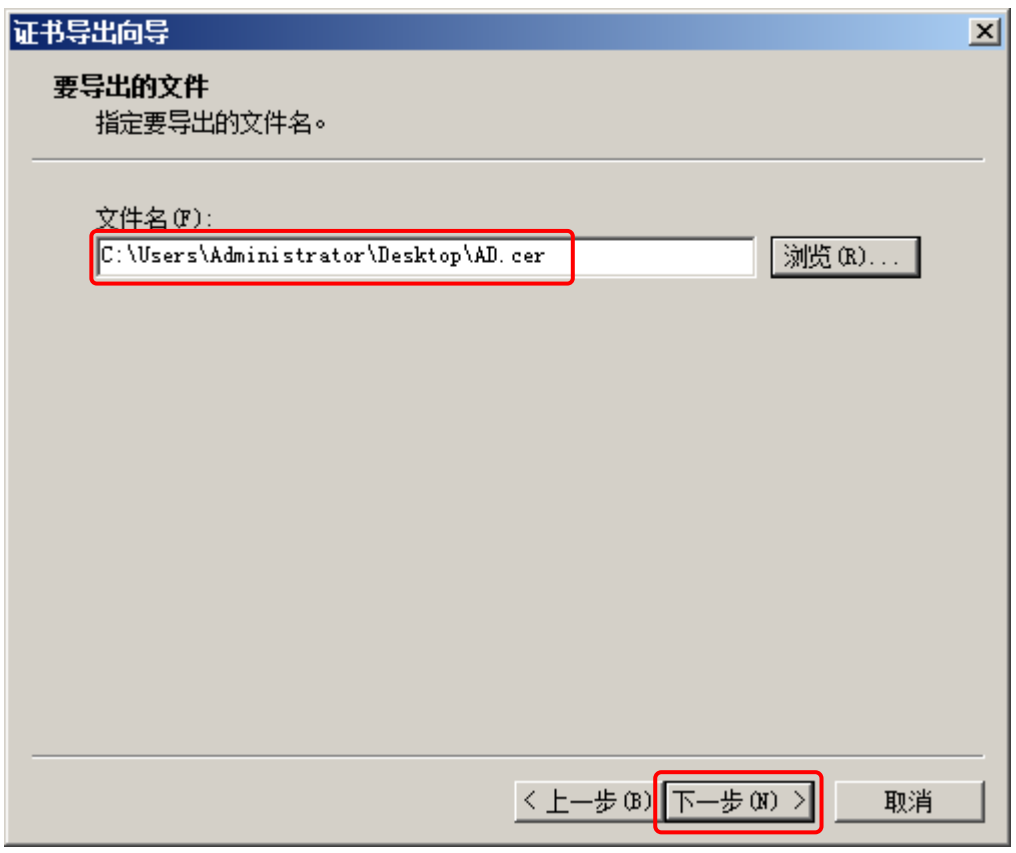
点击**下一步**



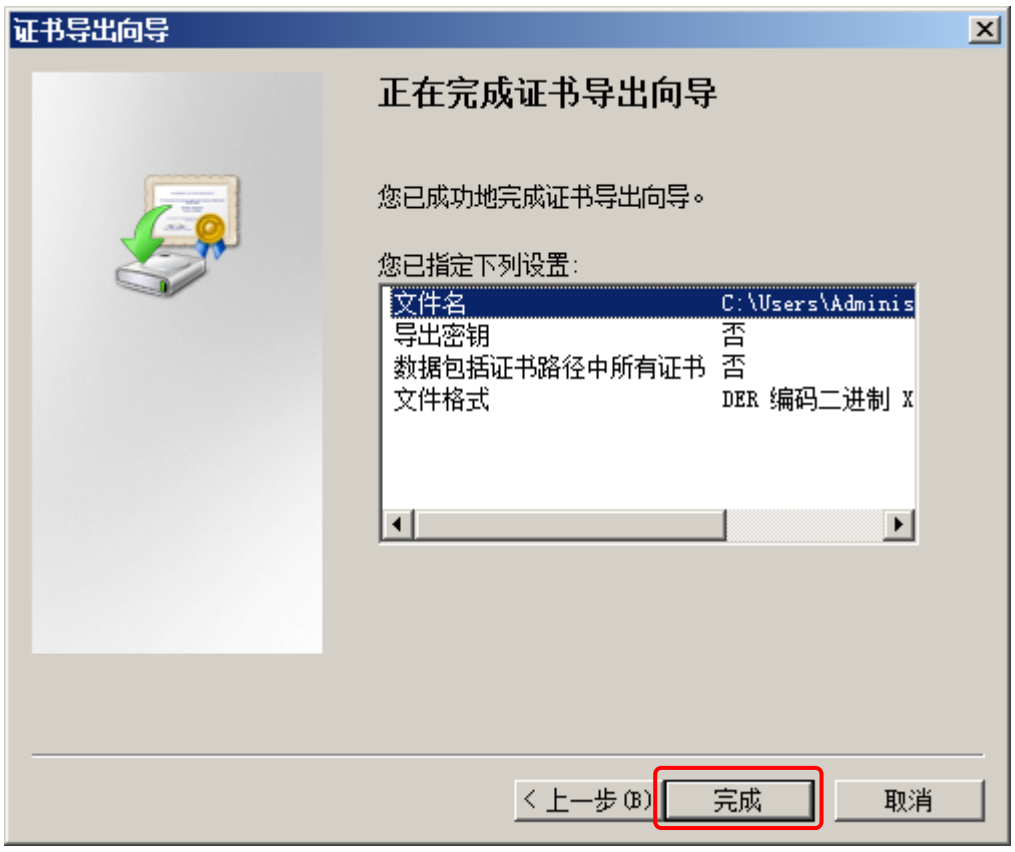
点击**下一步**



选择证书导出的路径，点击**下一步**

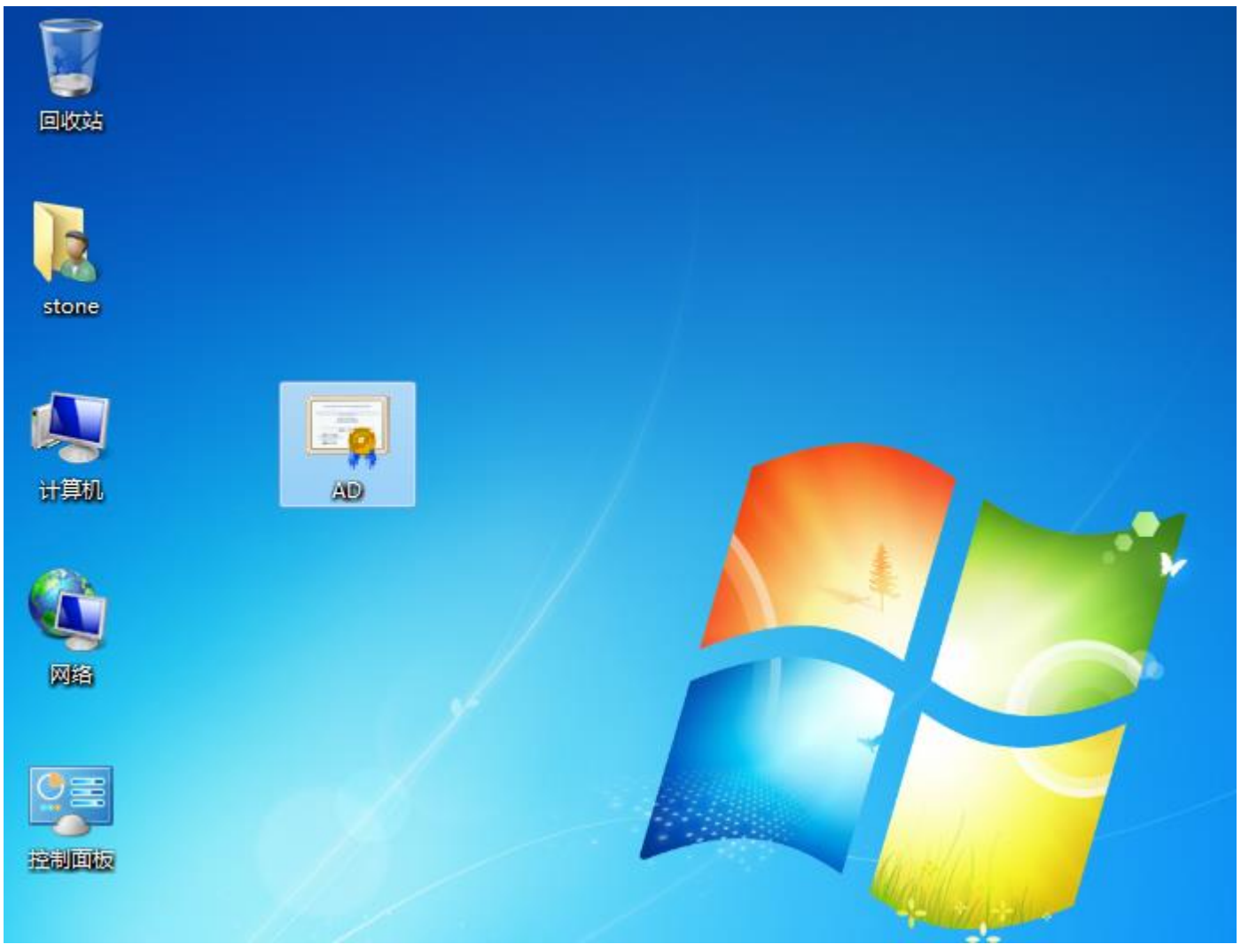


点击**完成**

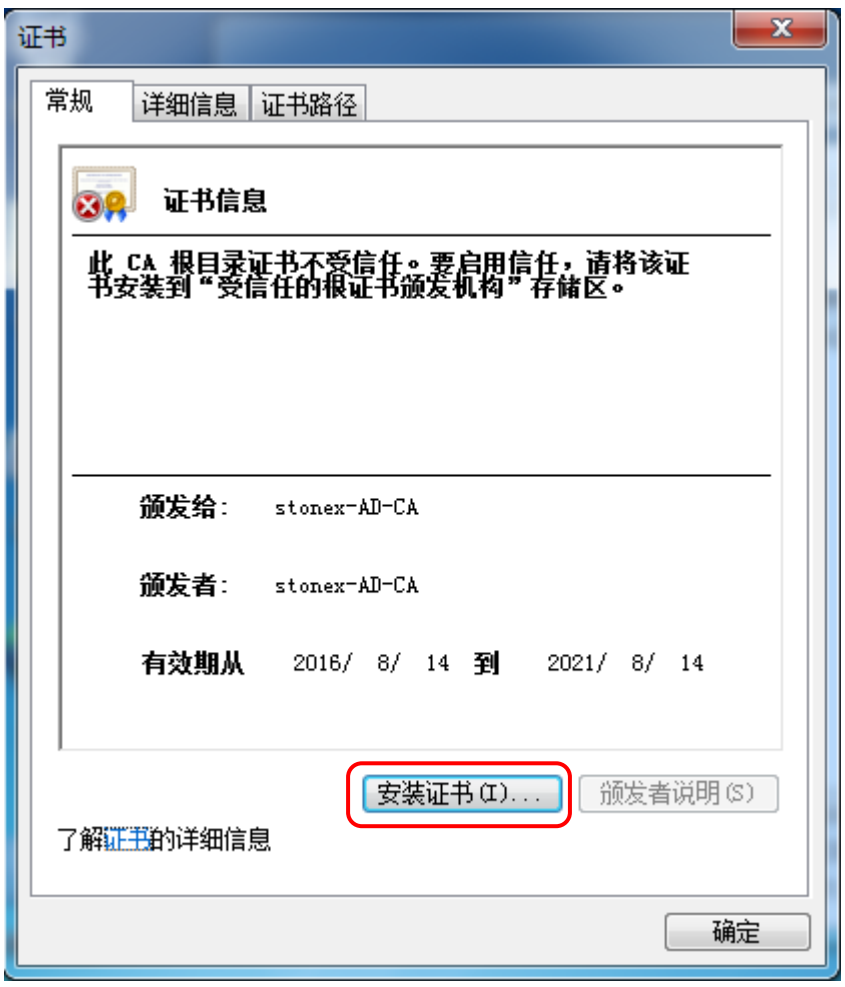


点击**完成**，证书导出成功

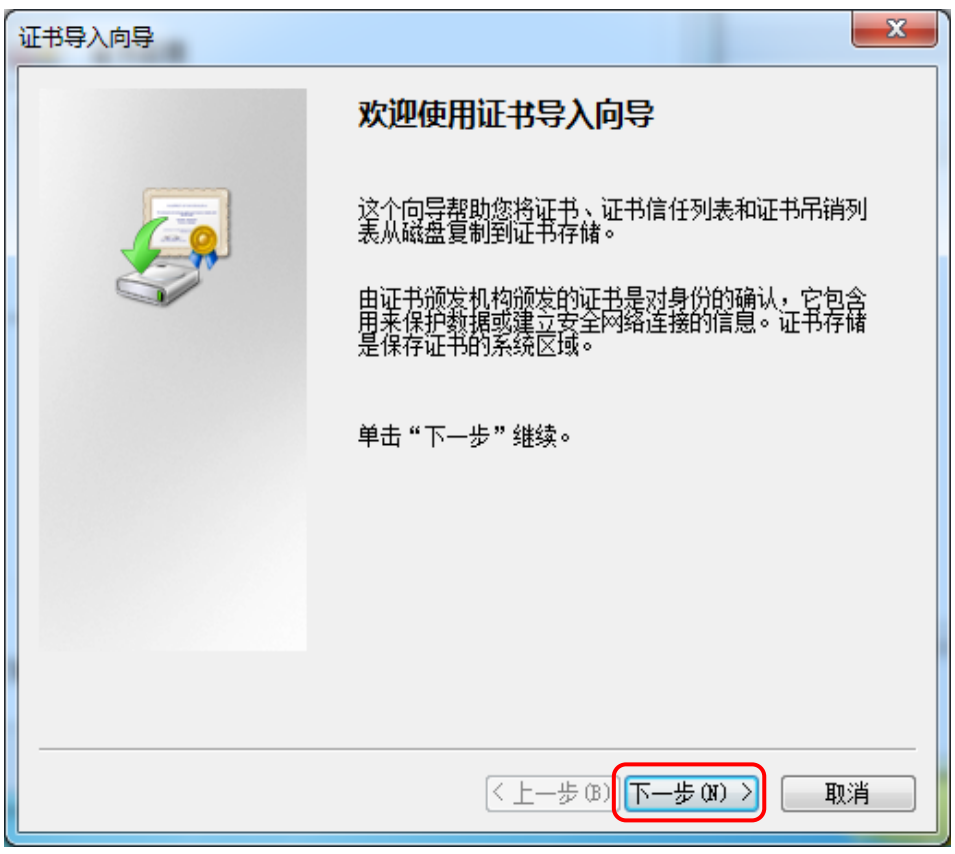
证书导出成功之后，可通过 USB 介质将根证书复制到客户端计算机上，如下所示，点击进行安装



点击**安装证书**

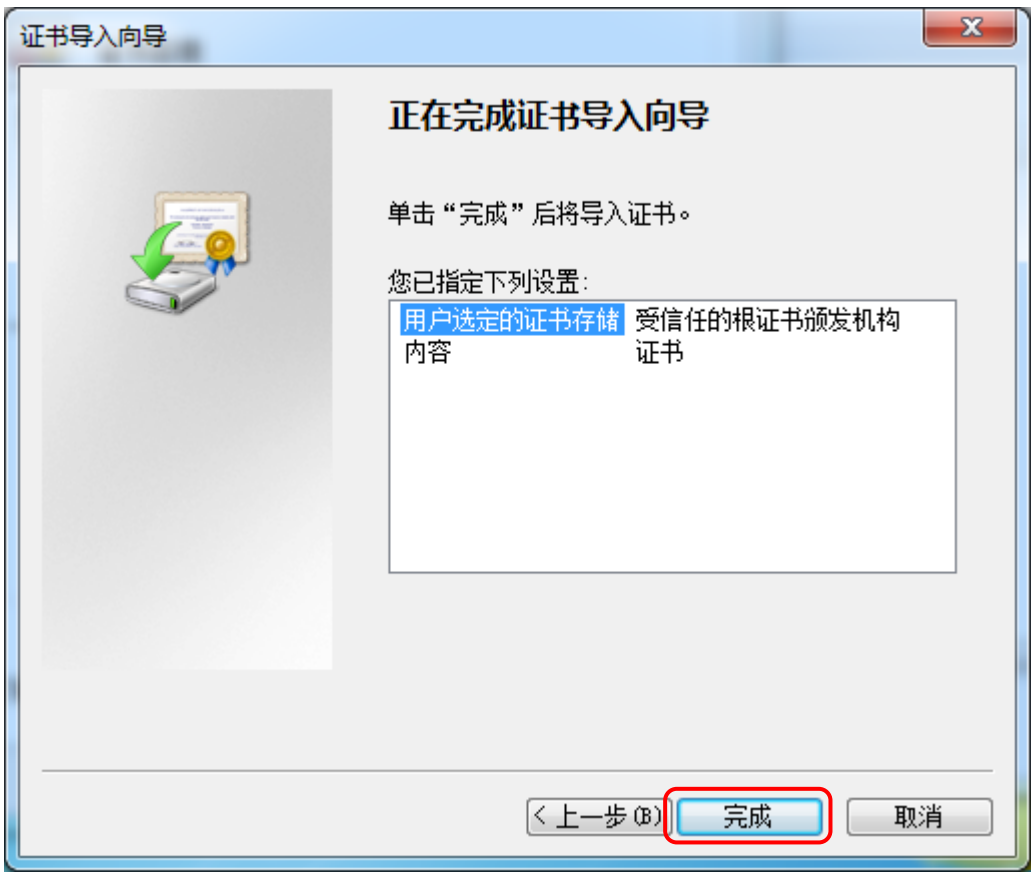


点击**下一步**

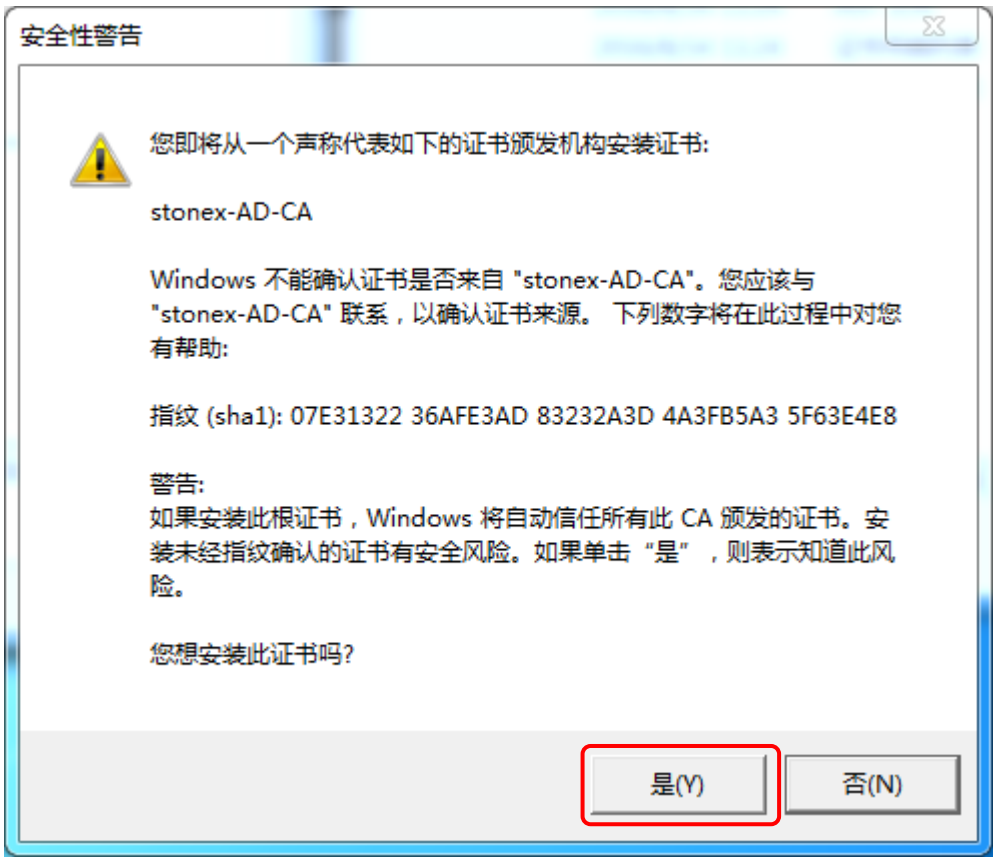


选择将证书存储在**受信任的根证书颁发机构**，点击**下一步**

点击**完成**



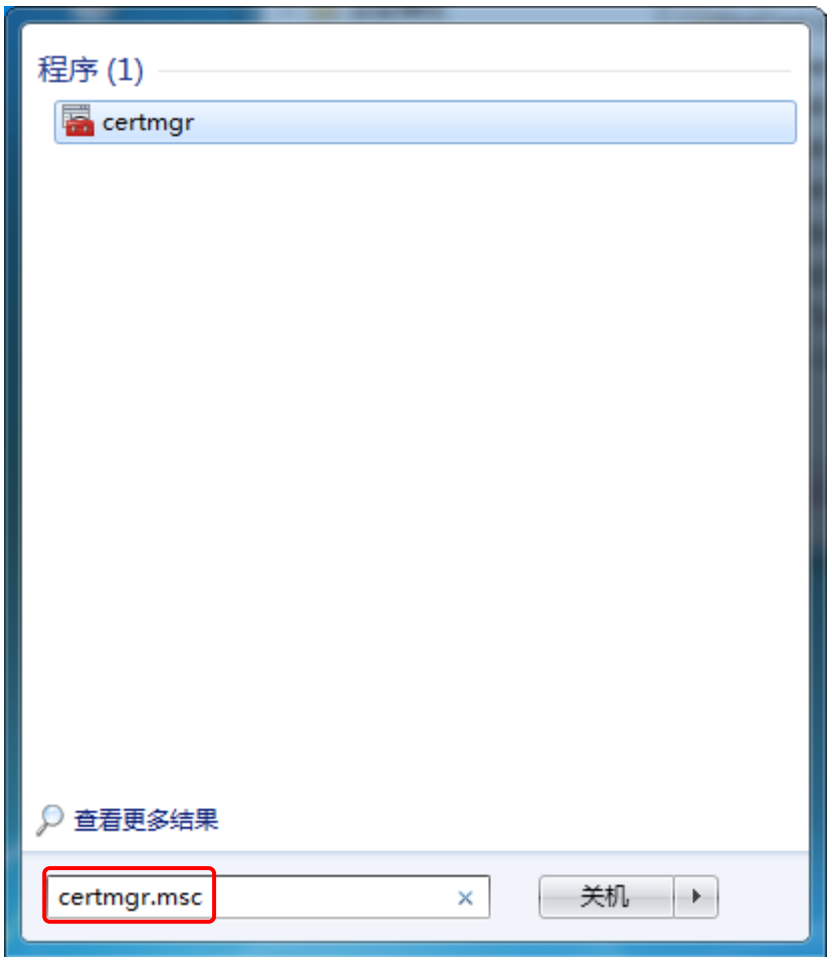
选择**是**

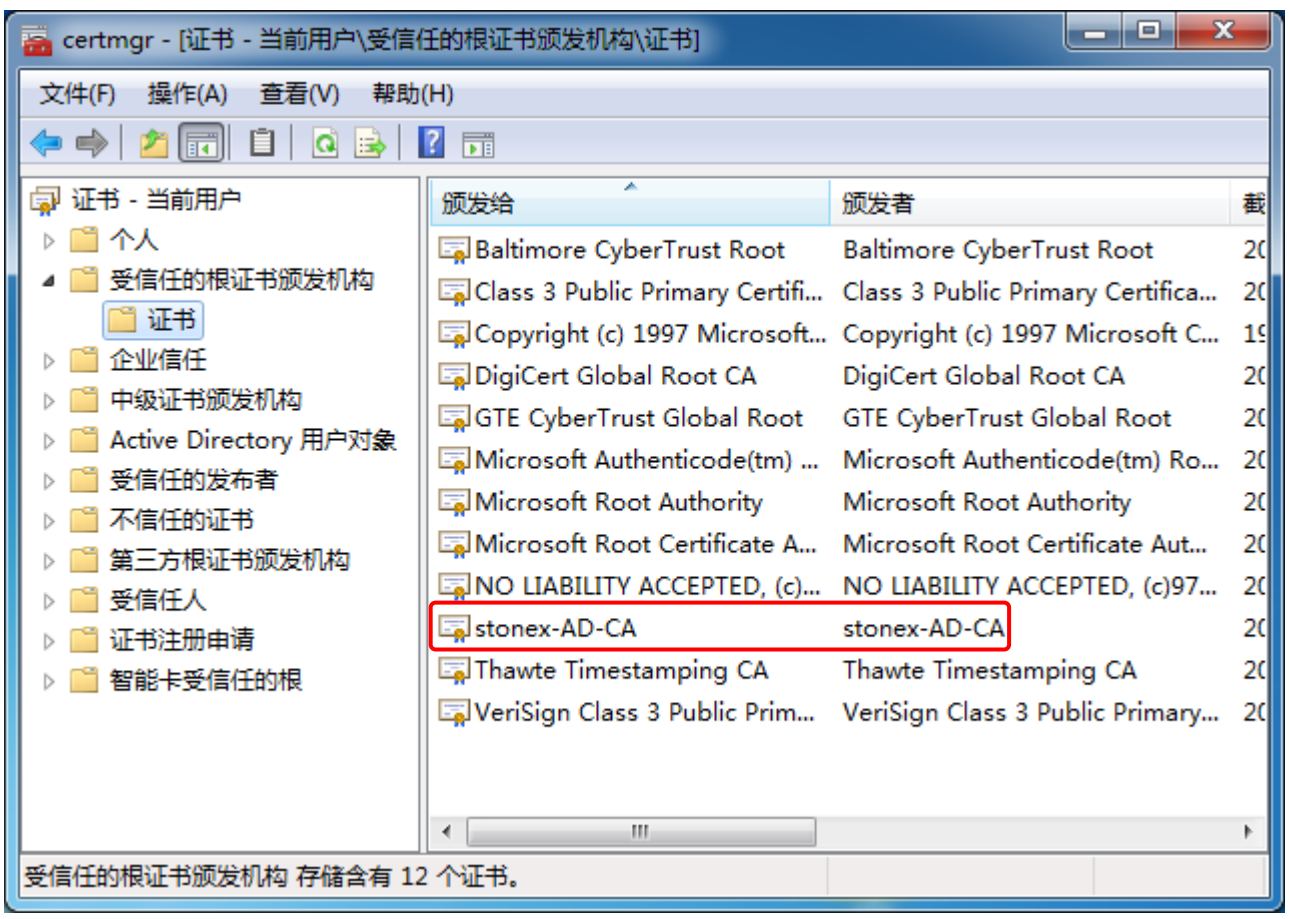


点击**确定**，根证书安装完成

根证书安装完成之后，可通过证书管理器工具控制台（certmgr.msc）进行查看验证

点击**开始** > 输入 **certmgr.msc**，打开**证书管理工具控制台**

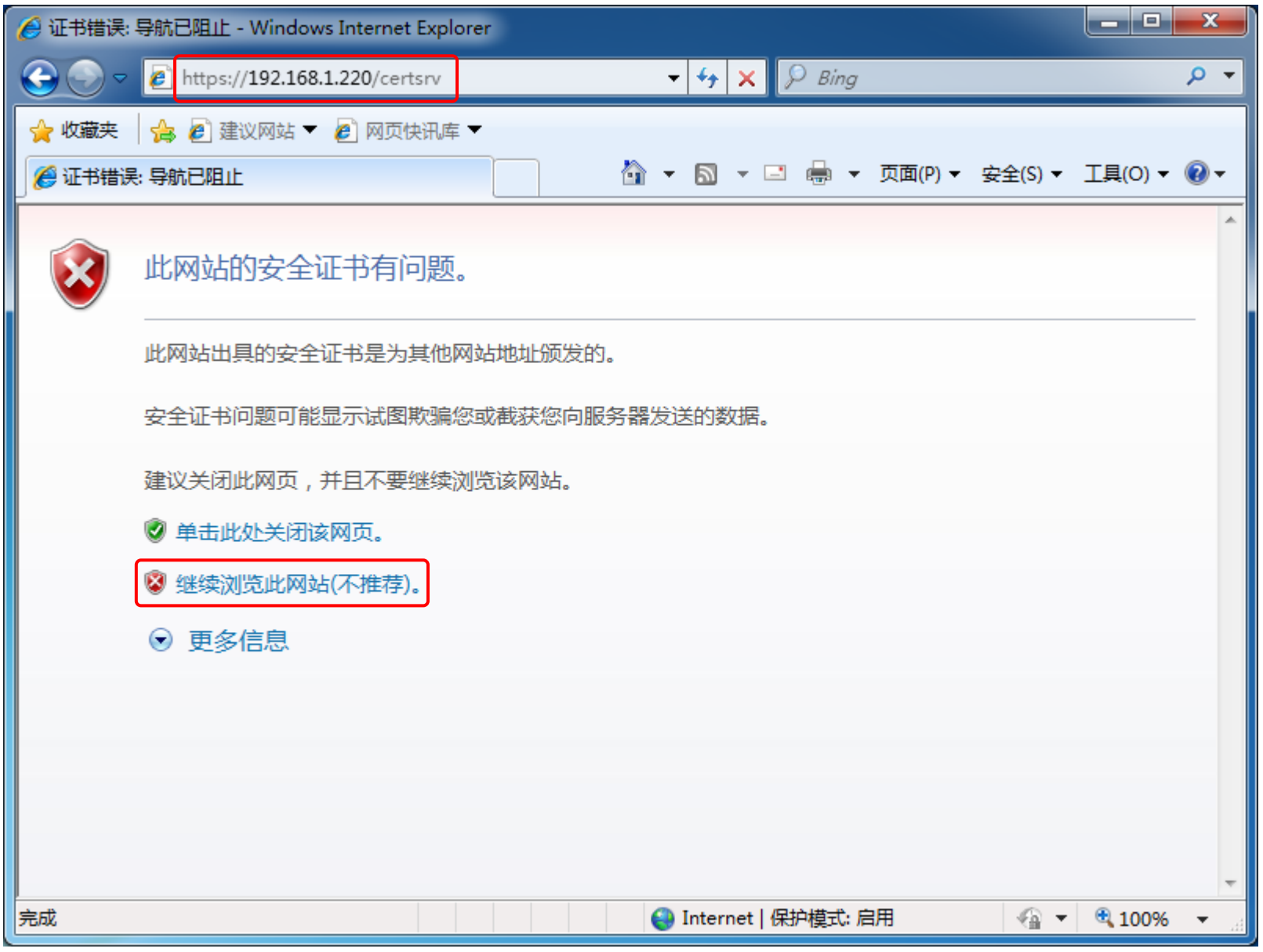




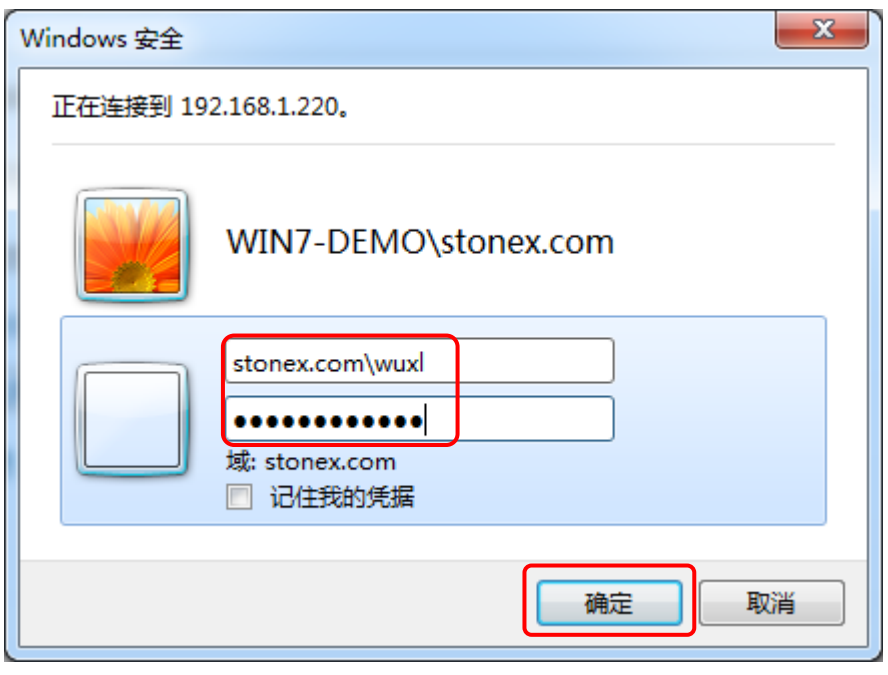
3.2.2 没有加域的客户端安装用户证书

打开浏览器，输入地址 https://192.168.1.220/certsrv

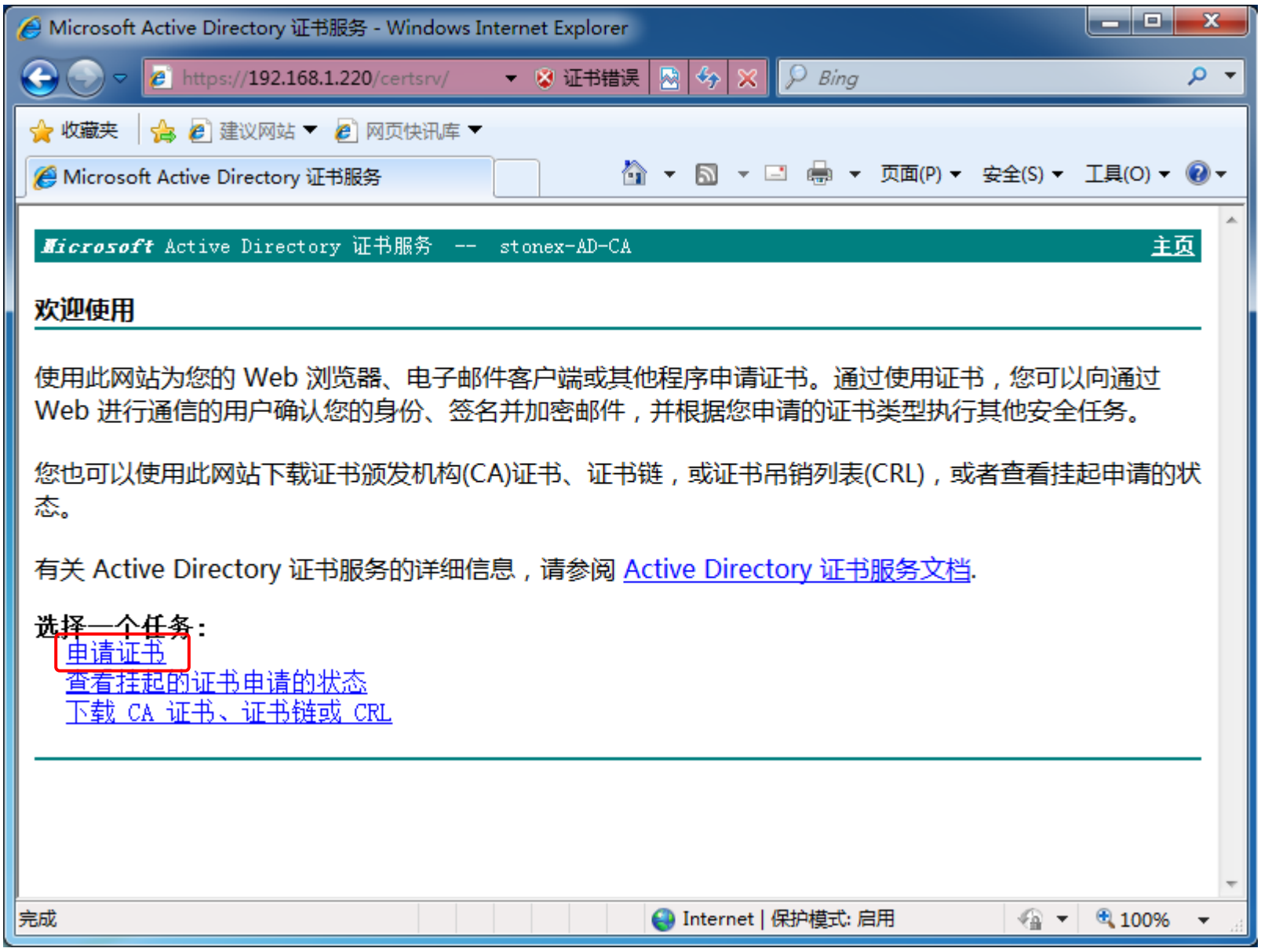
选择**继续浏览此网站（不推荐）**



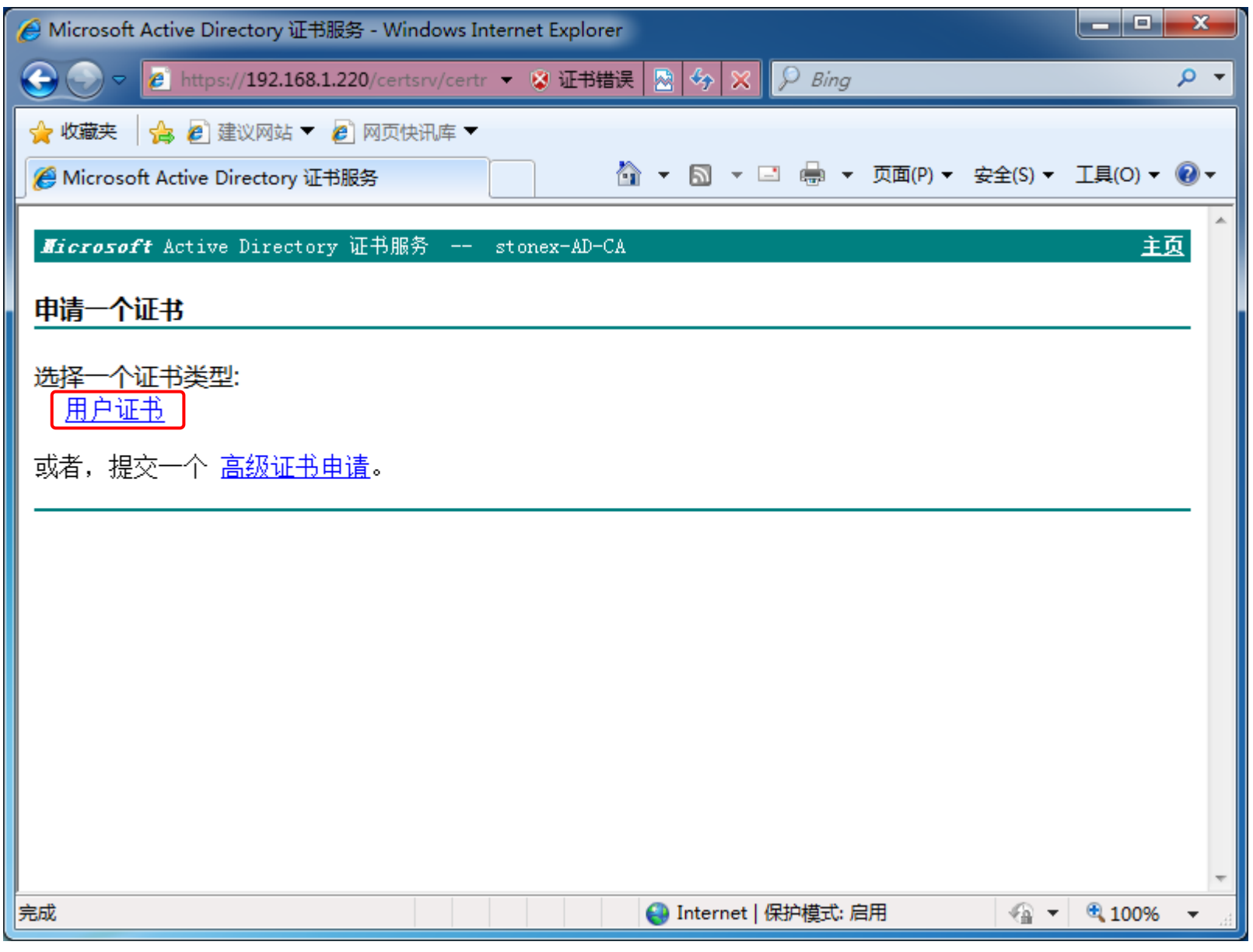
输入用户名和密码，点击**确定**



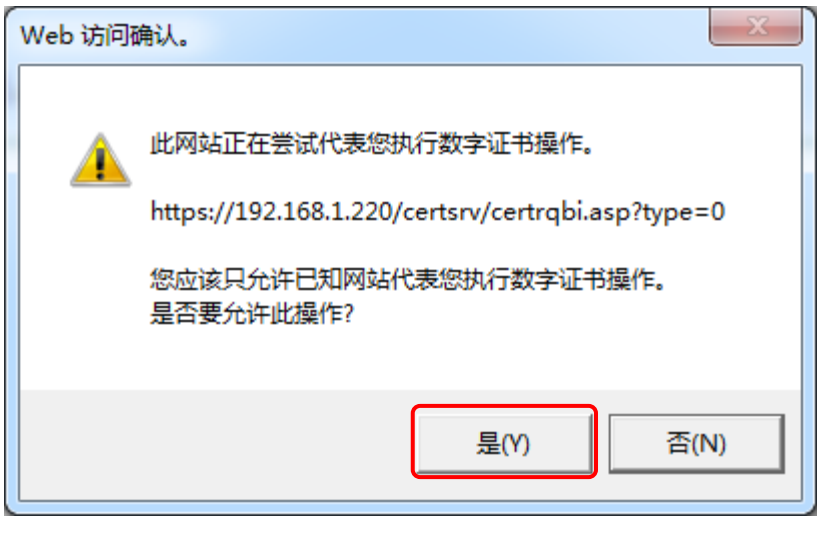
选择**申请证书**



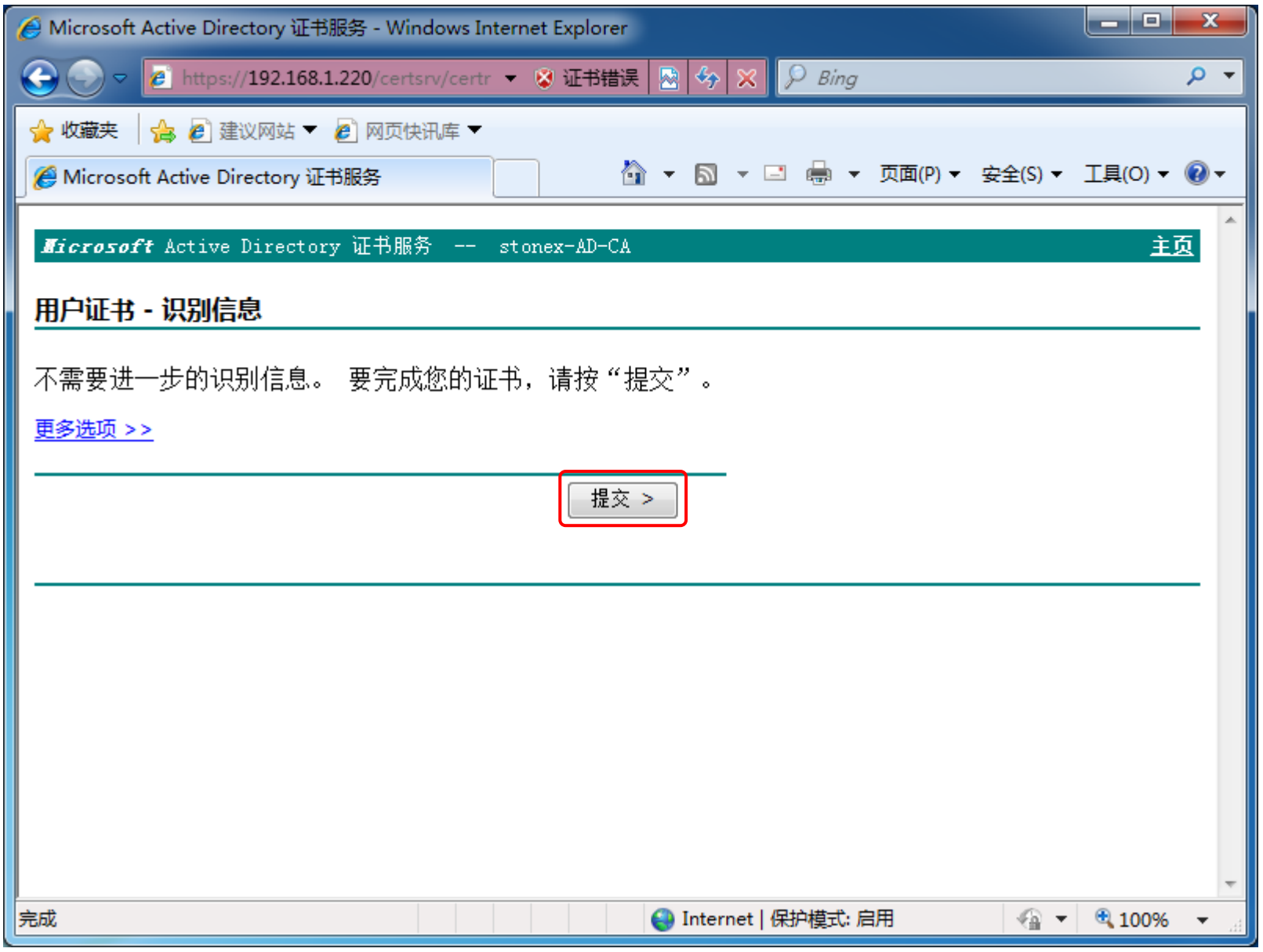
选择**用户证书**



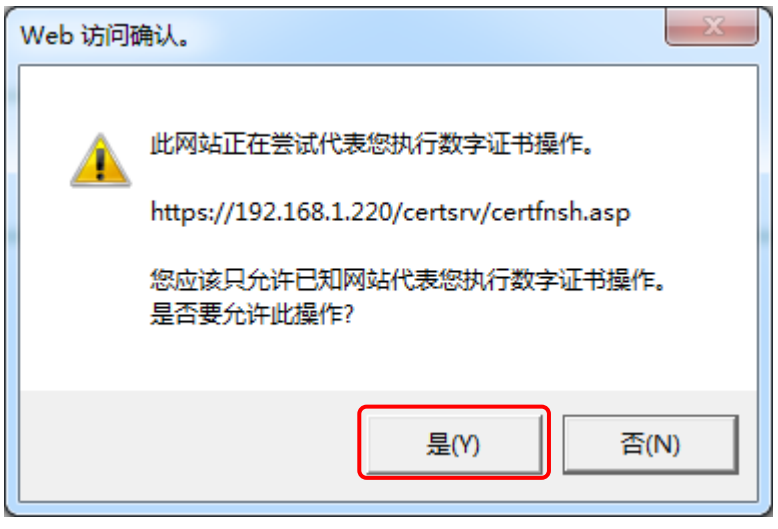
选择**是**


Web 访问确认。
此网站正在尝试代表您执行数字证书操作。
https://192.168.1.220/certsrv/certrqbi.asp?type=0
您应该只允许已知网站代表您执行数字证书操作。
是否要允许此操作?
是(Y)
否(N)

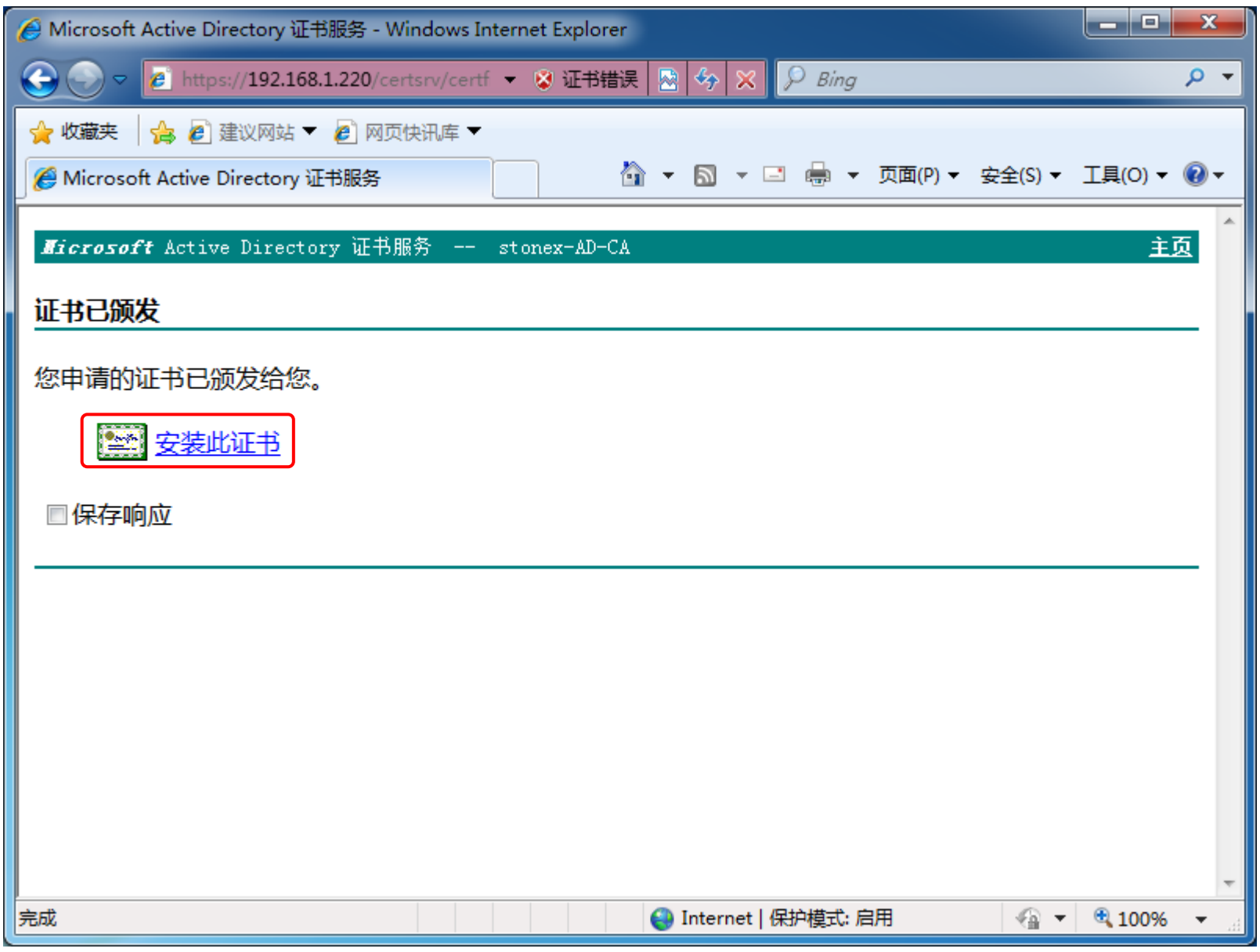
点击**提交**


Microsoft Active Directory 证书服务 - Windows Internet Explorer
https://192.168.1.220/certsrv/certr
证书错误
Bing
收藏夹
建议网站
网页快讯库
Microsoft Active Directory 证书服务
页面(P)
安全(S)
工具(O)
Microsoft Active Directory 证书服务 -- stonex-AD-CA
主页
用户证书 - 识别信息
不需要进一步的识别信息。 要完成您的证书，请按“提交”。
更多选项 >>
提交 >
完成
Internet | 保护模式: 启用
100%

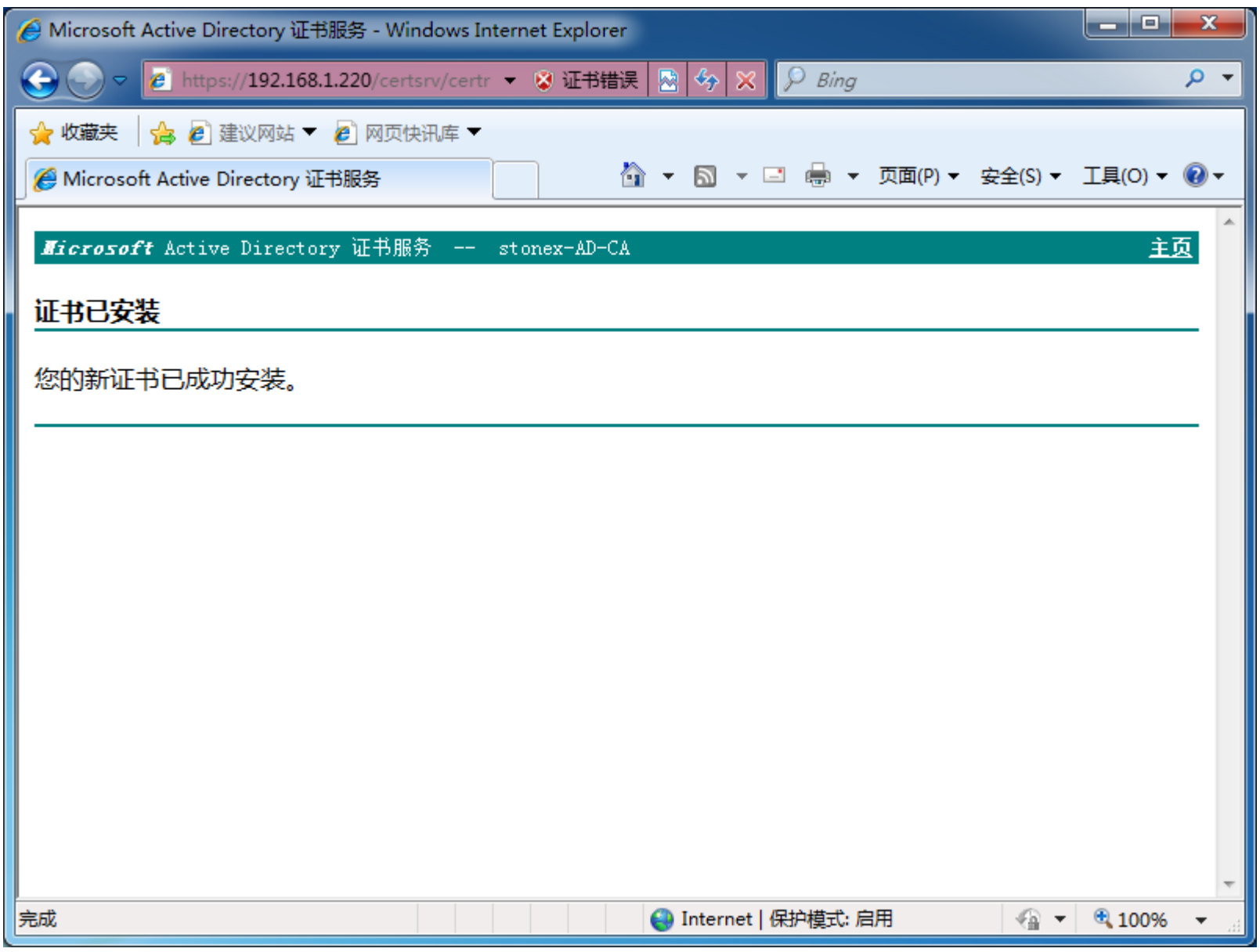
选择**是**


Web 访问确认。
此网站正在尝试代表您执行数字证书操作。
https://192.168.1.220/certsrv/certfnsh.asp
您应该只允许已知网站代表您执行数字证书操作。
是否要允许此操作?
是(Y)
否(N)

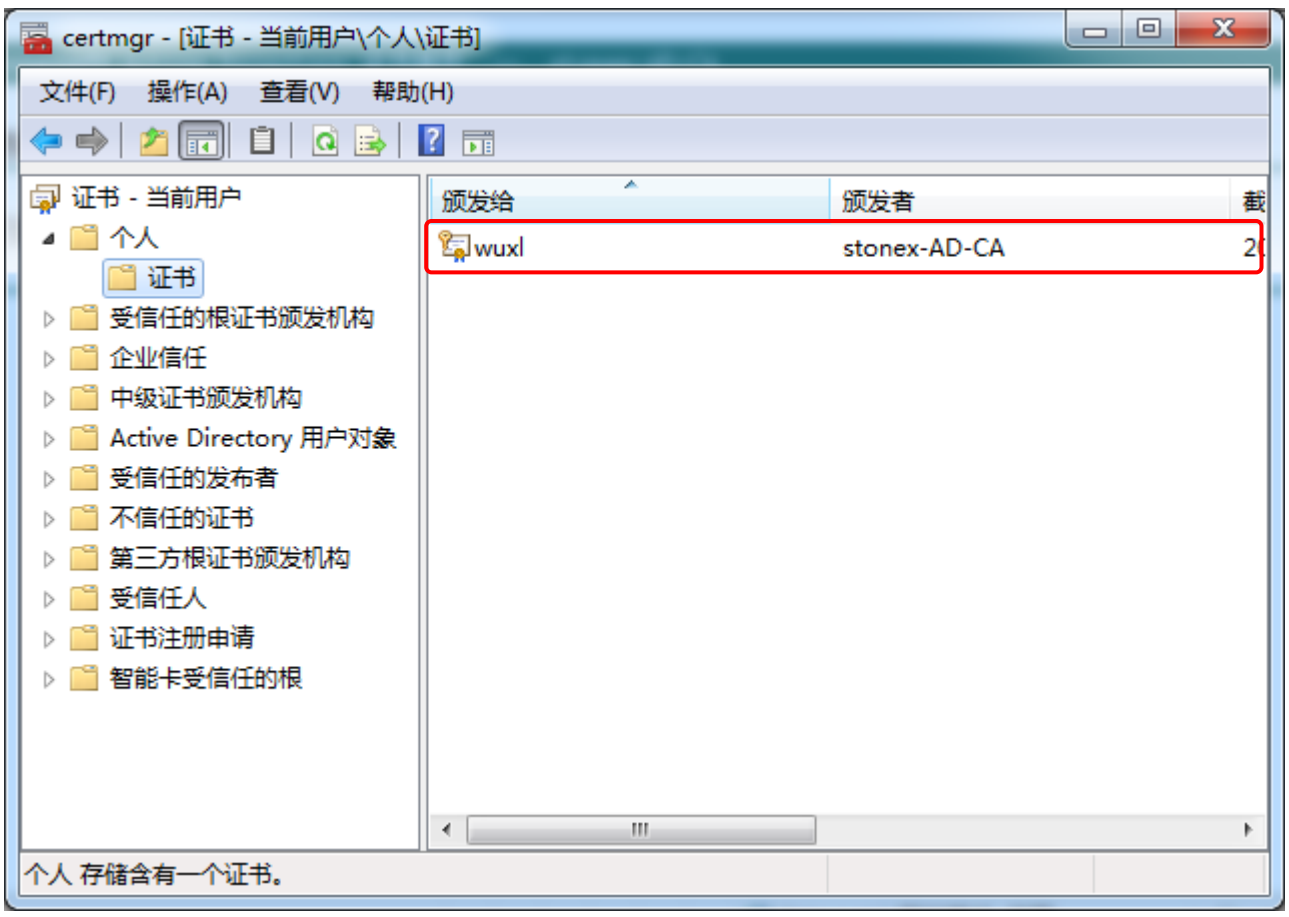
点击**安装此证书**



证书安装成功



可通过证书管理器工具控制台进行查看验证

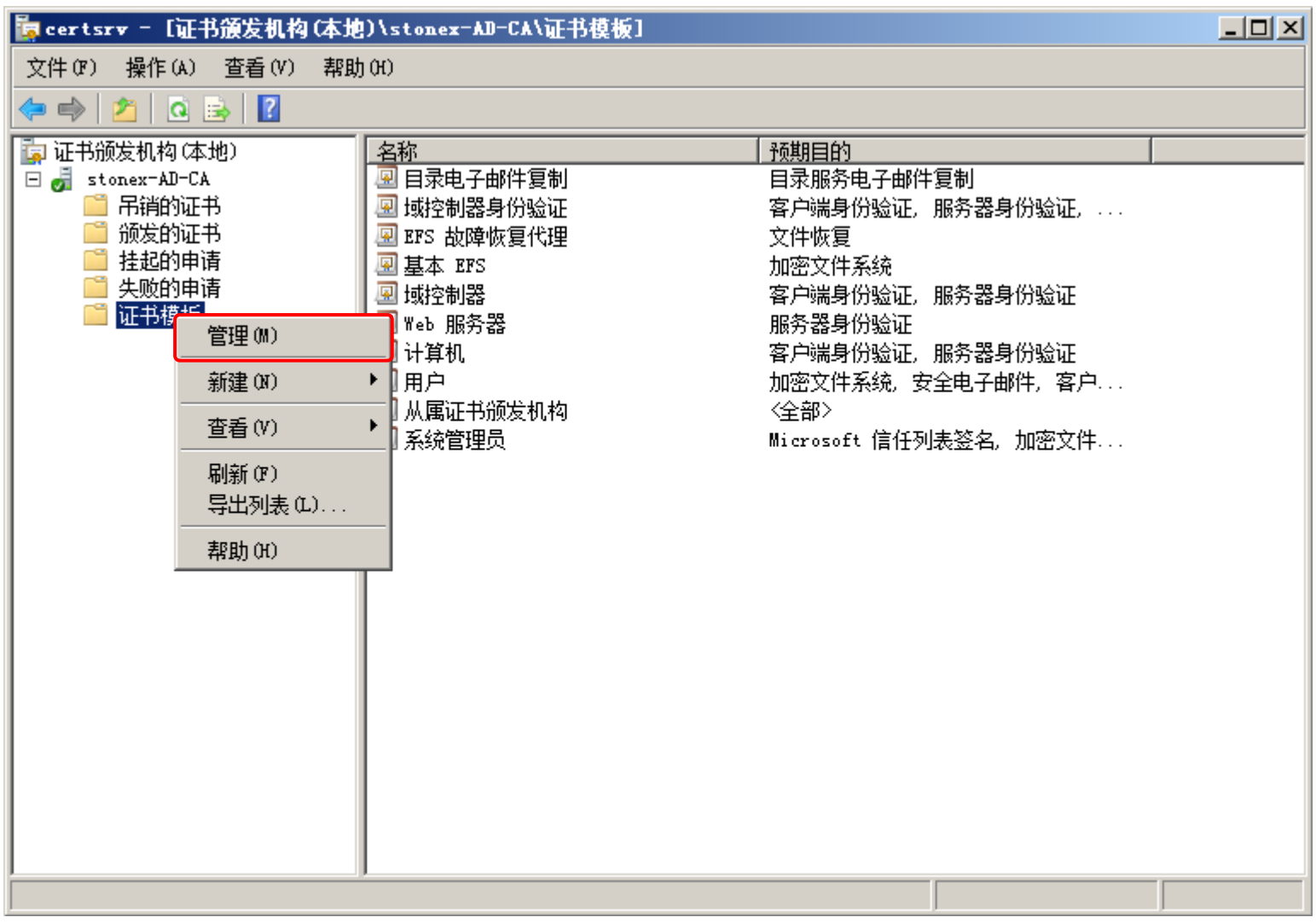


3.2.3 加域的客户端手动安装用户证书

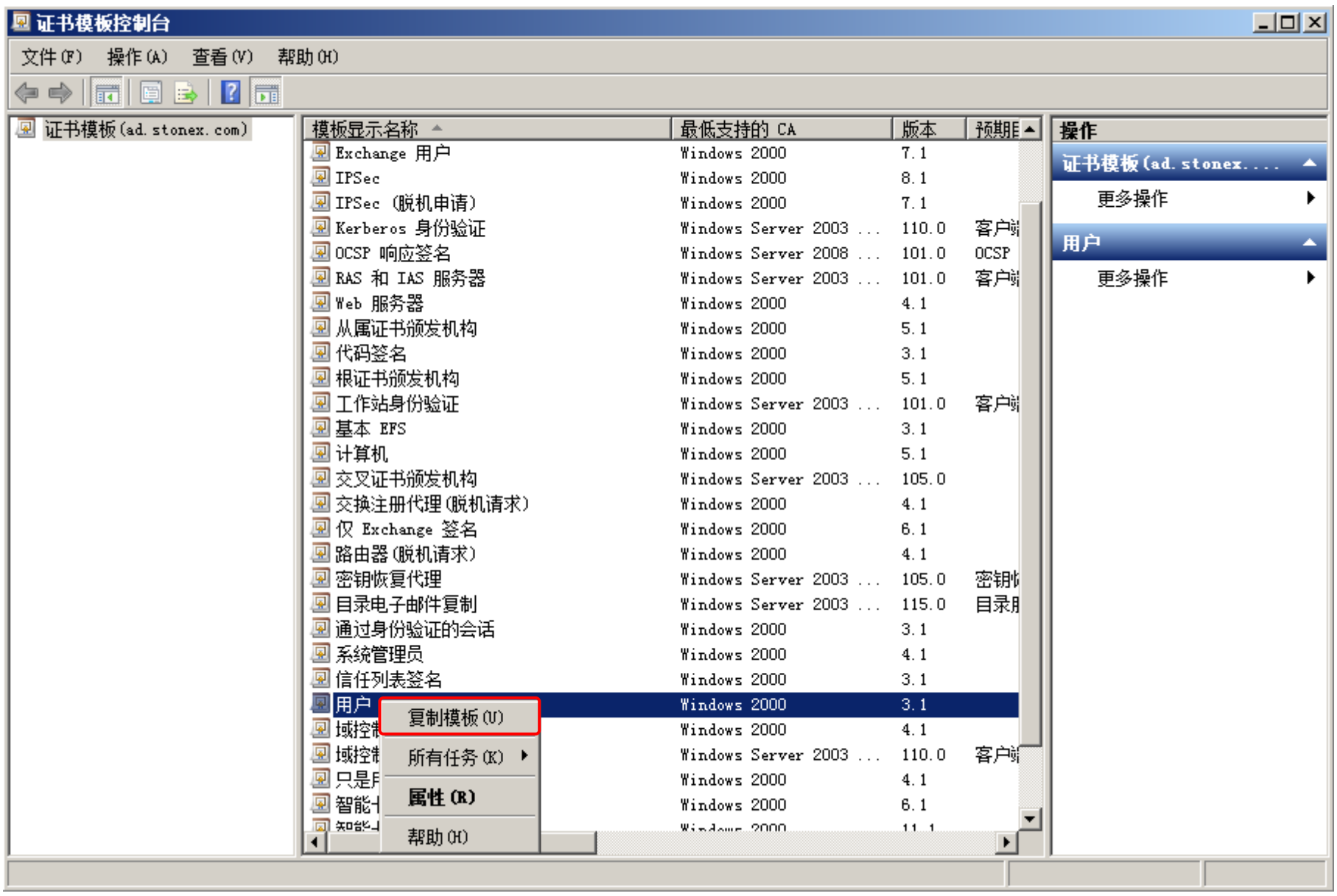
加域的客户端手动安装用户证书步骤与没有加域的客户端安装用户证书一样，参考 3.2.2 章节

3.2.4 加域的客户端通过组策略自动安装用户证书

点击**开始** -> **管理工具** -> **证书颁发机构**，右击**证书模板**，点击**管理**

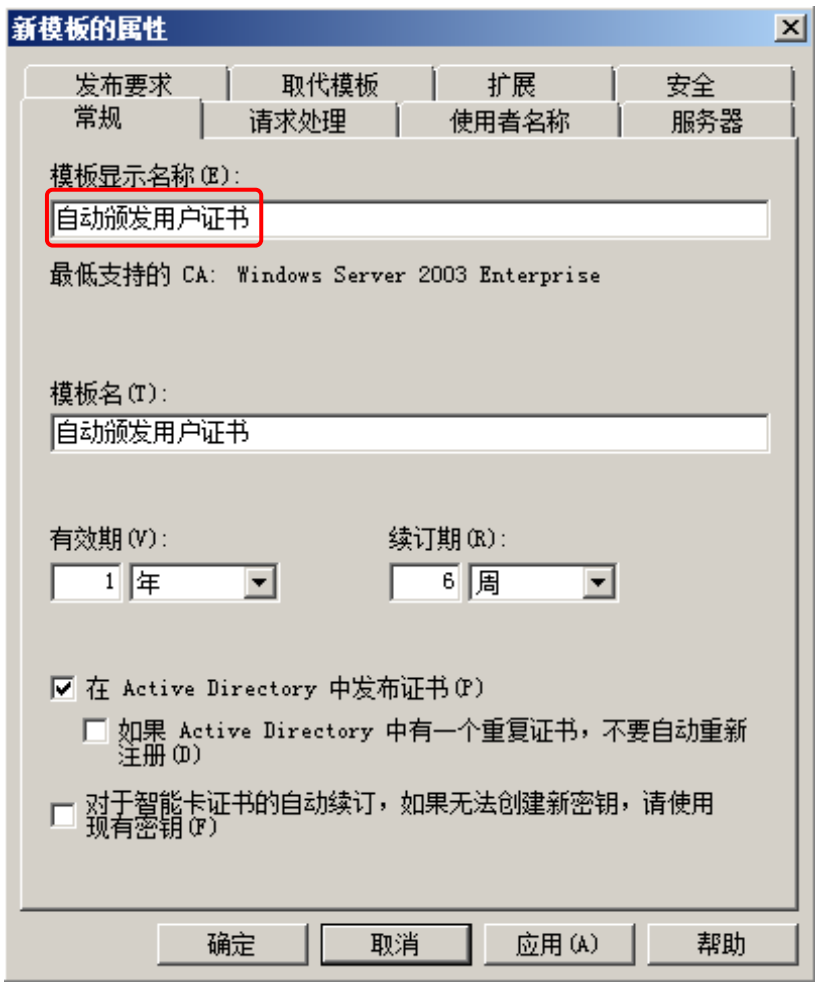


右击**用户**，点击**复制模板**

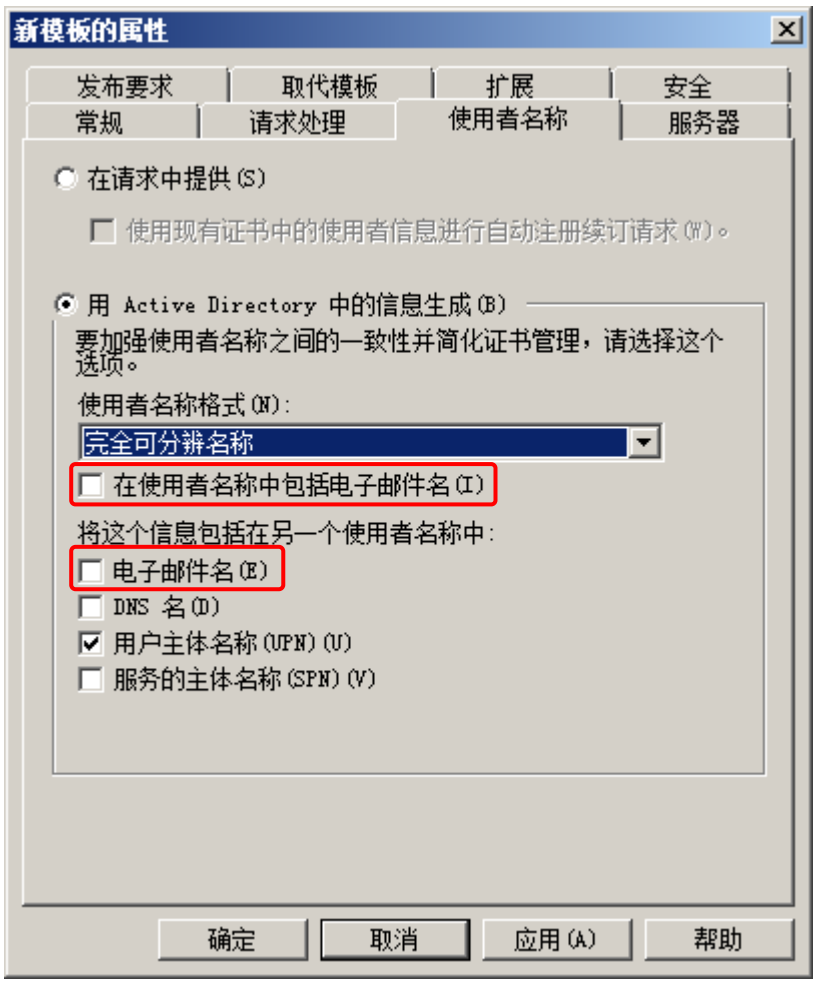


点击**确定**

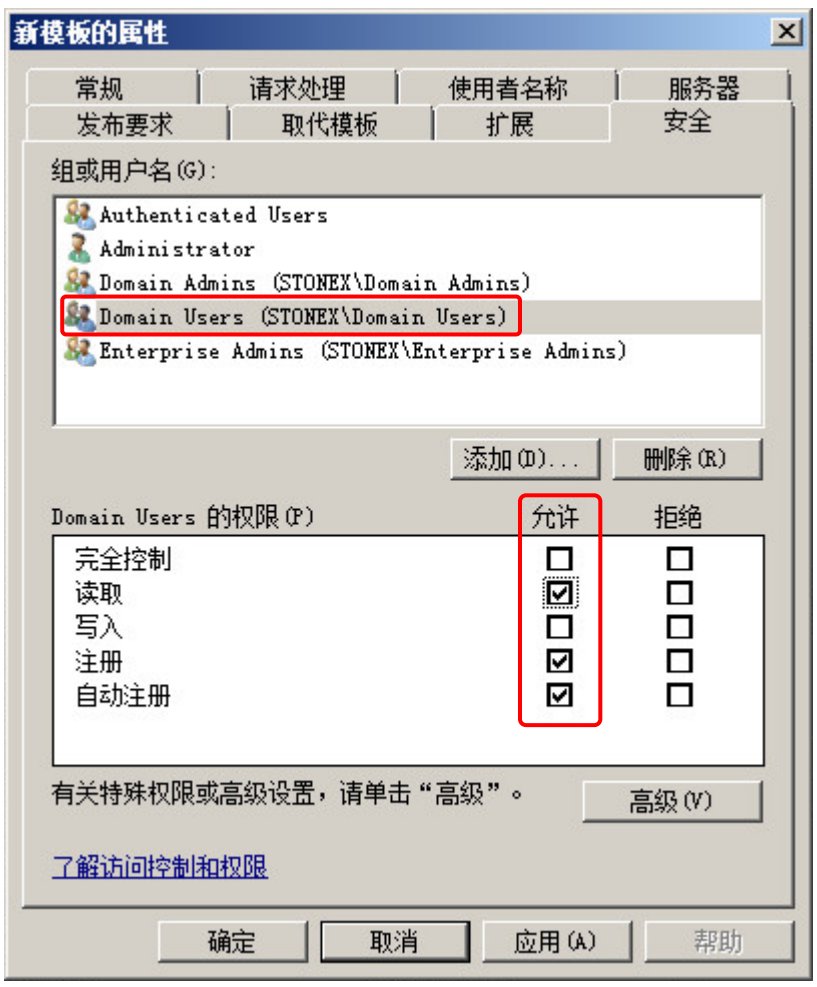
更改模板名称，这里更改名称为**自动颁发用户证书**



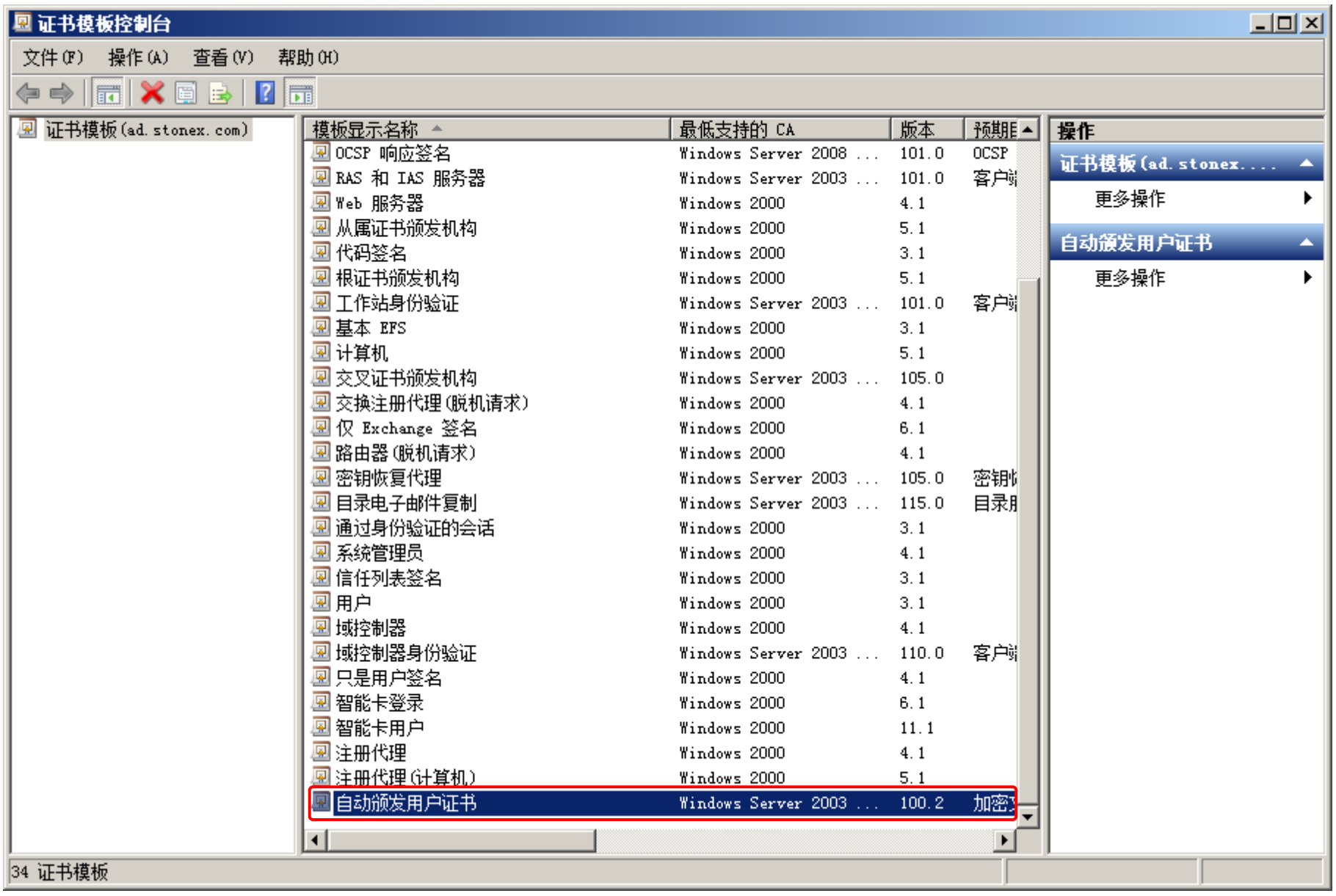
切换至**使用者名称，**确保证书信息中不包含电子邮件名，否则有些创建的用户没有设置电子邮件名，自动颁发证书时会报错。



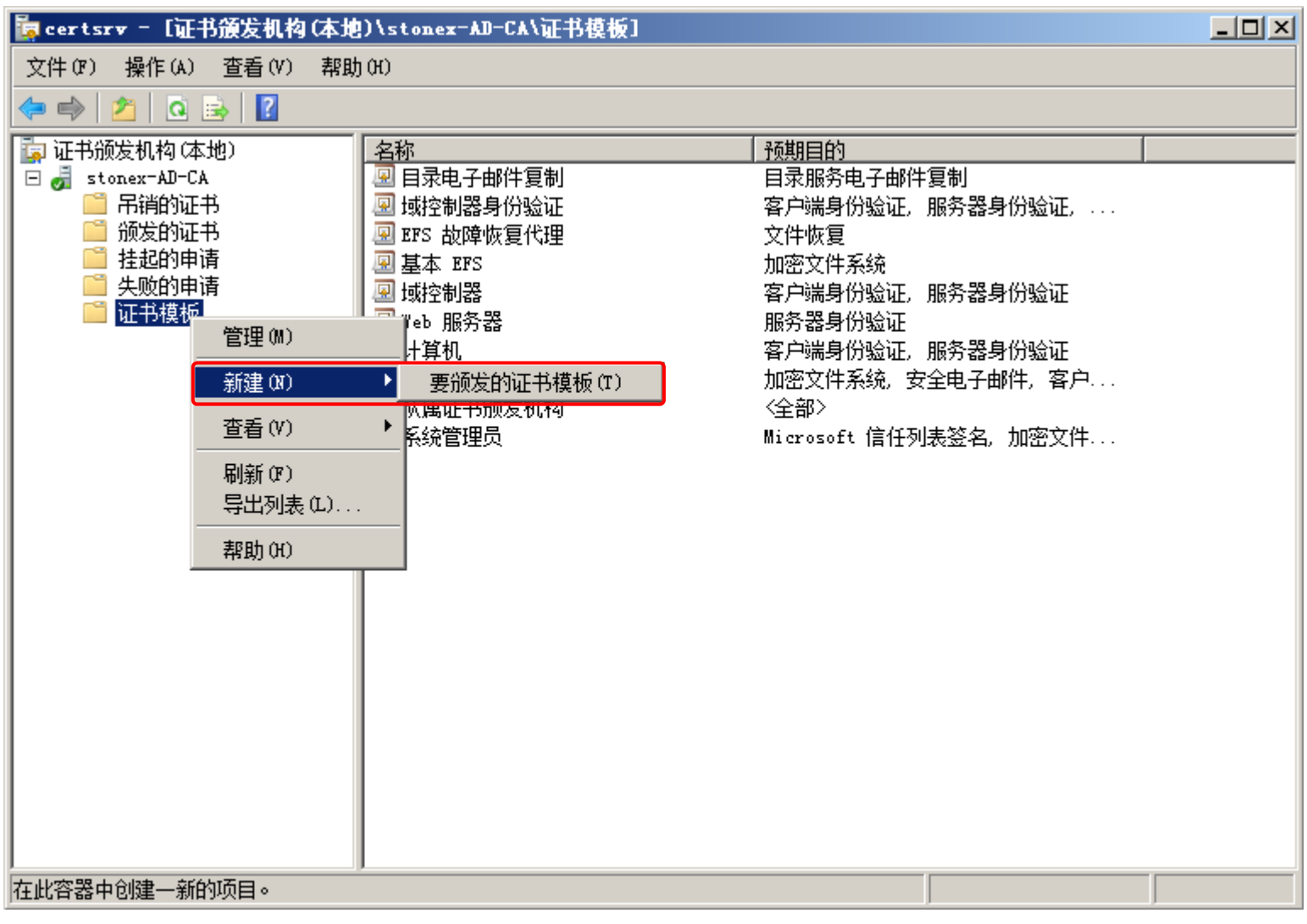
切换至**使用者名称，**选中 Domain Users，勾选允许**读取、注册和自动注册的权限**



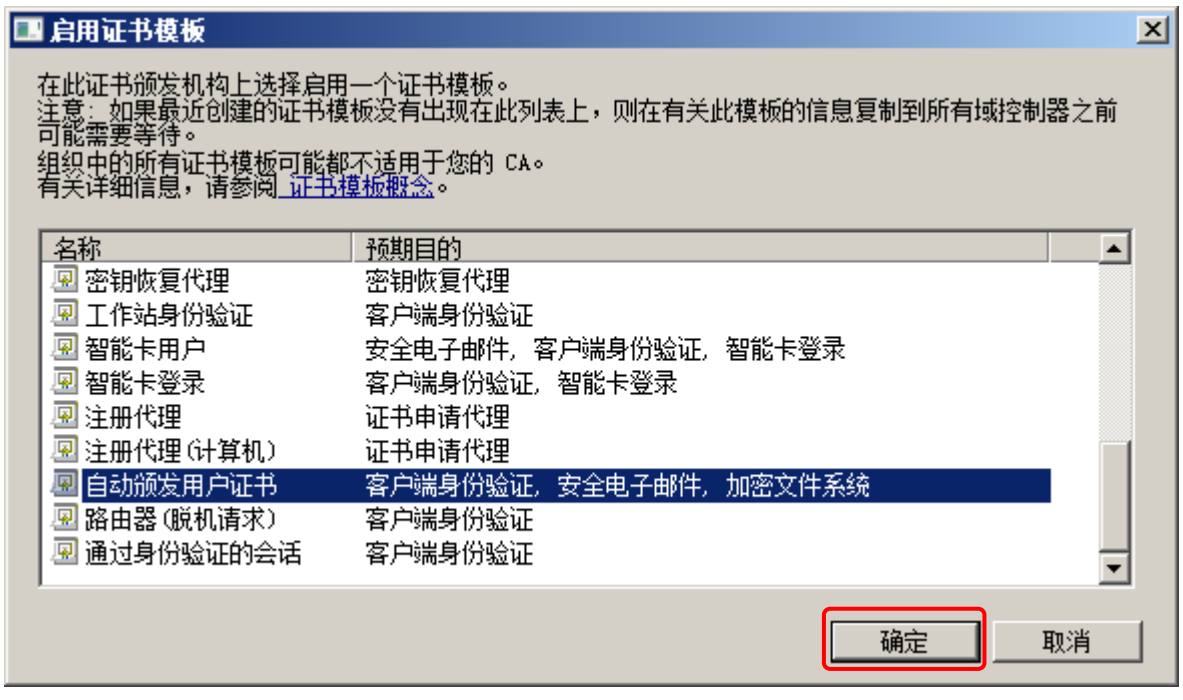
新建证书模板：自动颁发用户证书，步骤完成

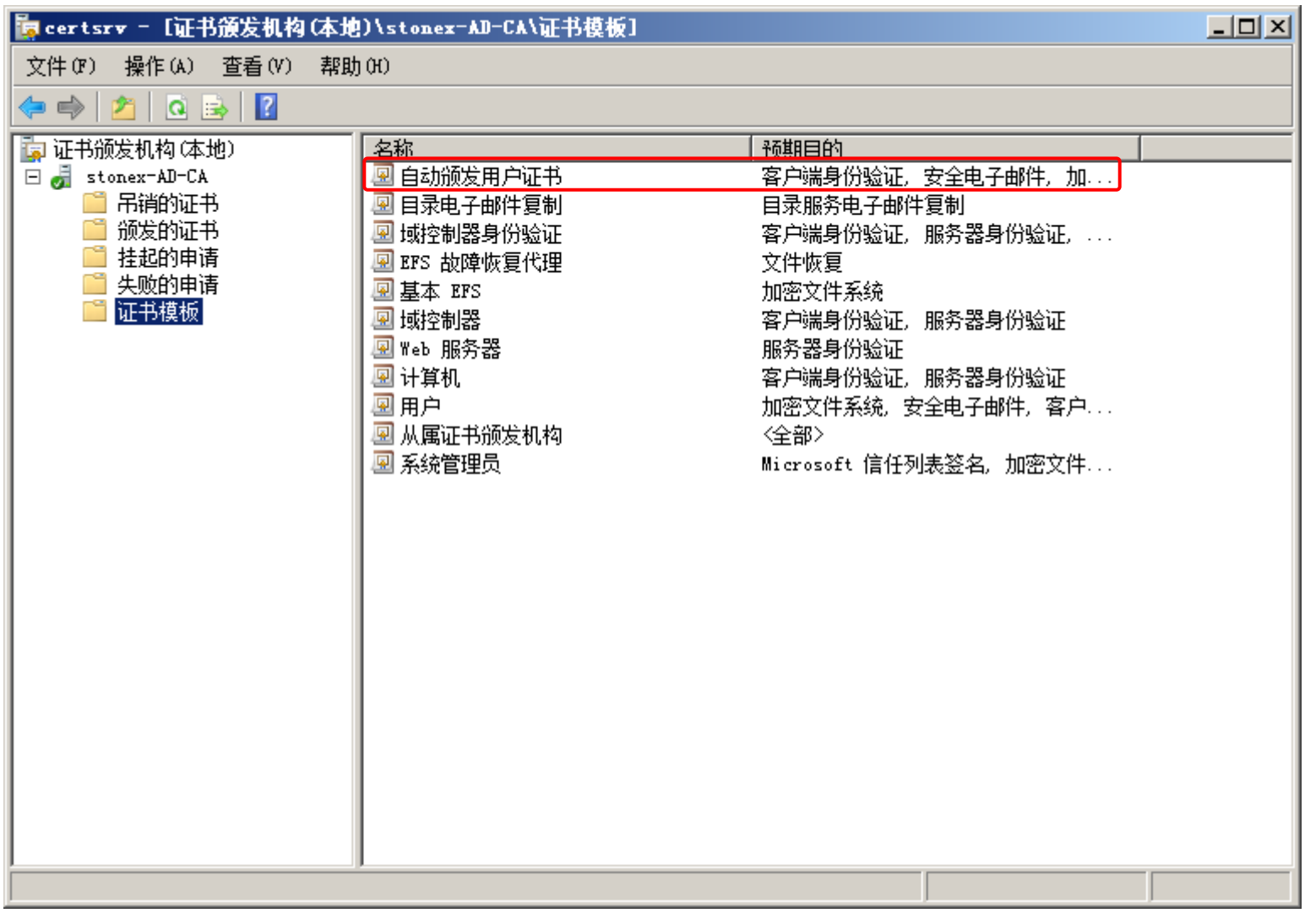


打开证书颁发机构，右击**证书模板 -> 新建 -> 要颁发的证书模板**



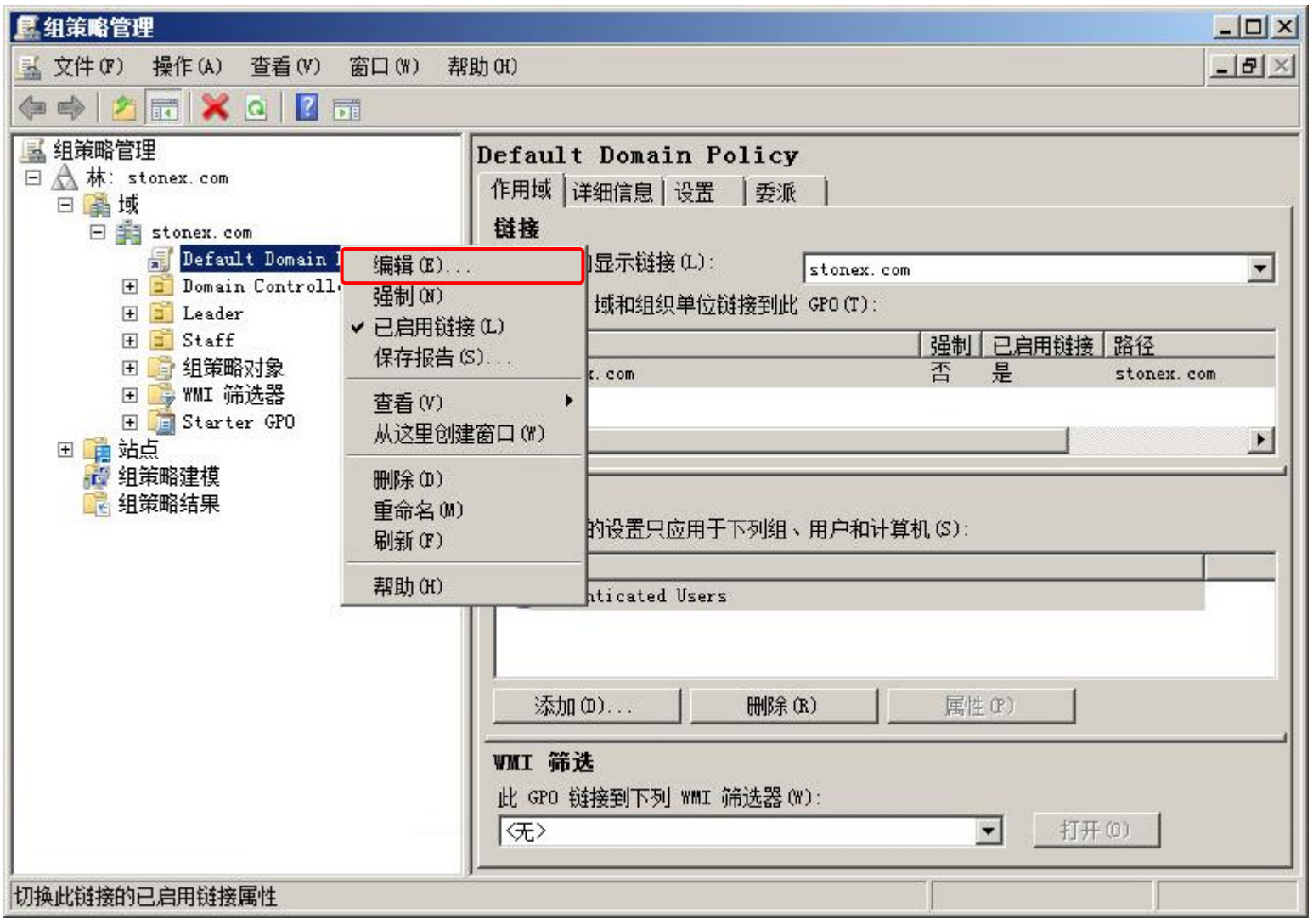
选中自动颁发用户证书，点击**确定**





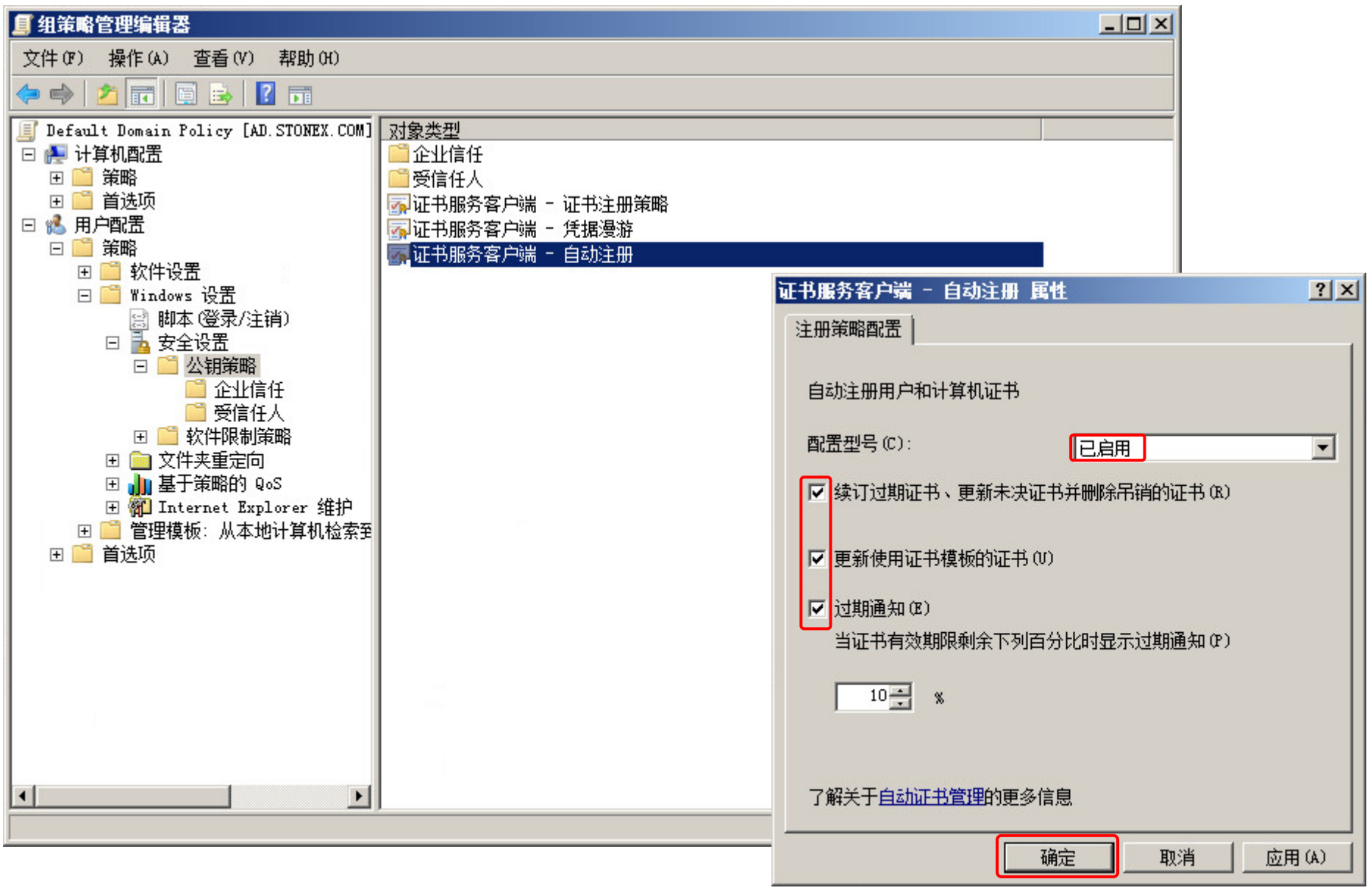
点击**开始 -> 管理工具 -> 组策略管理，**

点击**林 -> 域 -> stonex.com**，右击 **Default Domain Policy -> 编辑**



点击**用户配置 -> 策略 -> 安全设置 -> 公钥策略**

选中**证书服务客户端 – 自动注册**，选择**已启用**，勾选以下三项，点击确定

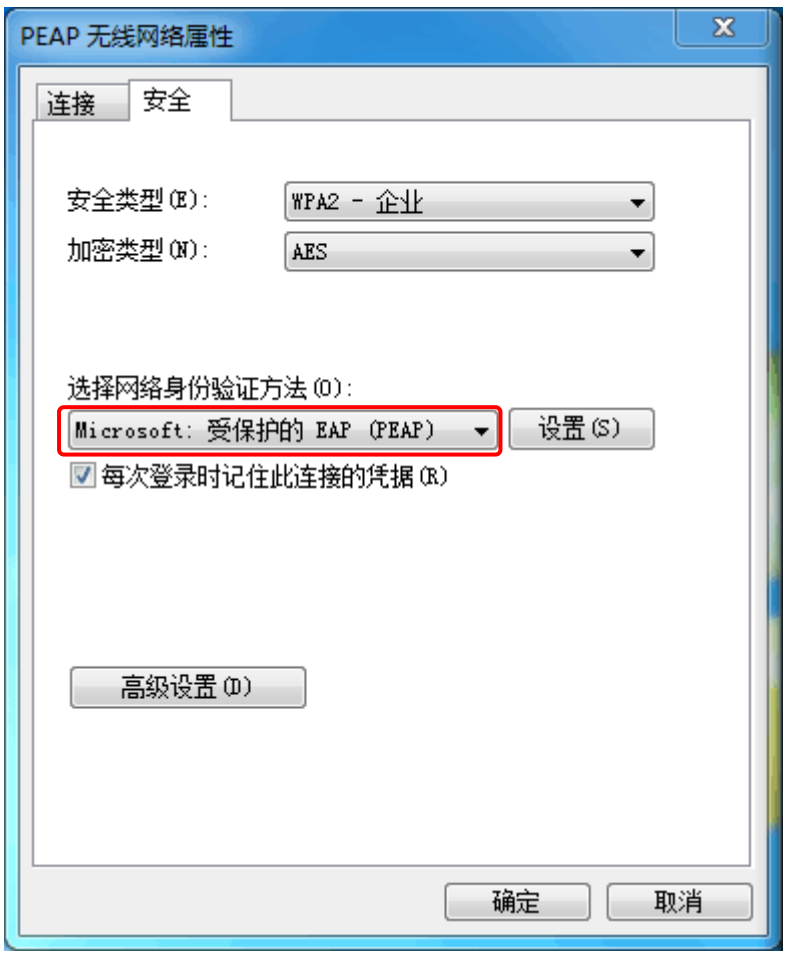


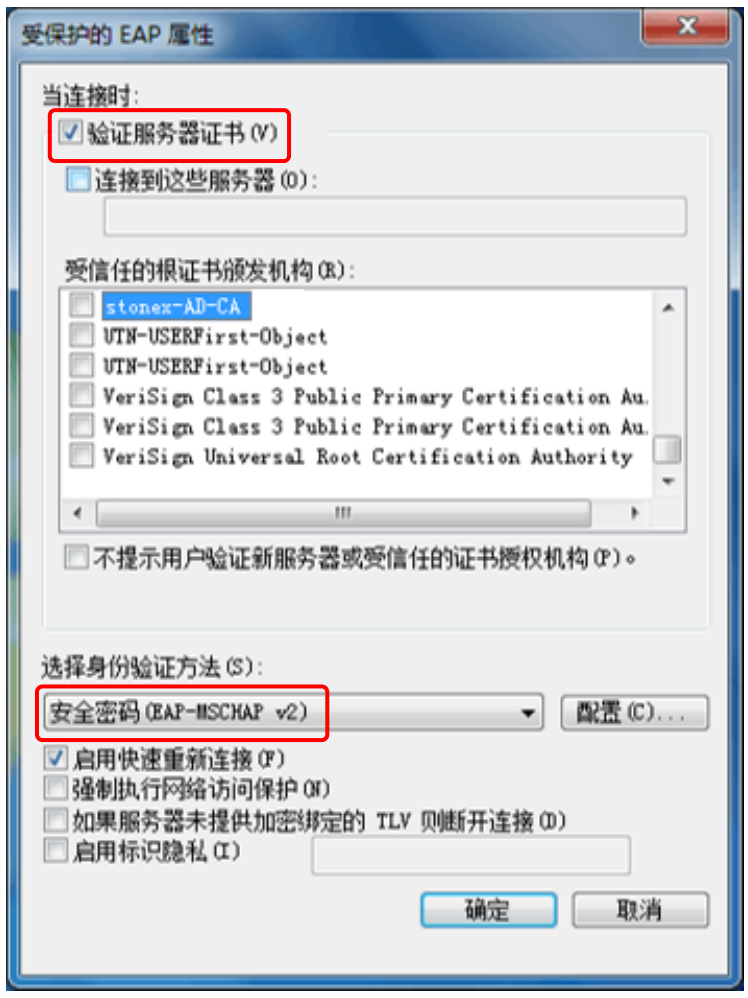
通过域策略自动下发用户证书配置完成，配置完成后可通过命令 **gpupdate /force** 强制更新组策略

加域的客户端使用域账号登录成功后，会自动安装相应的用户证书。

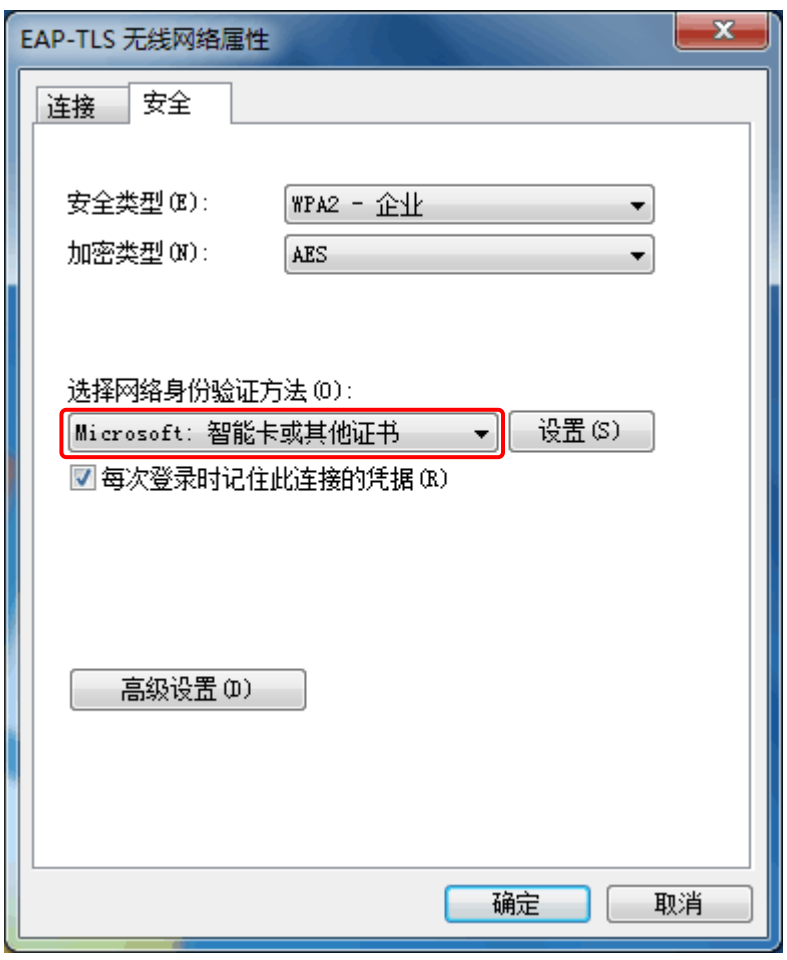
3.3 配置客户端测试连接 802.1X 认证

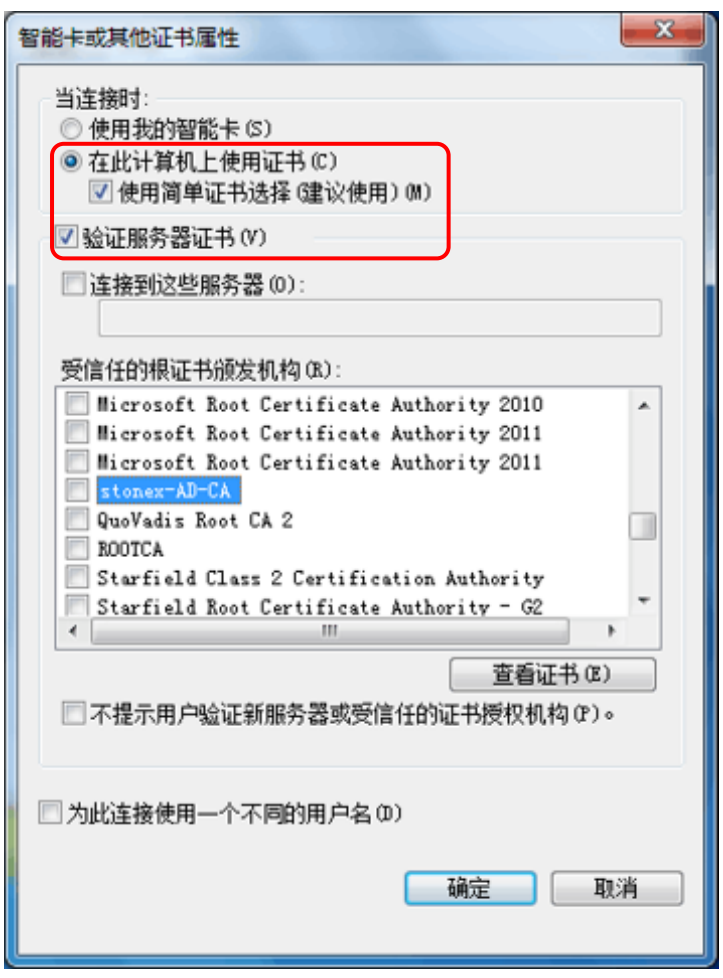
EAP-PEAPv0（PEAP-MSCHAPv2）的 Windows 客户端配置如下：





EAP-TLS 的 Windows 客户端配置如下：



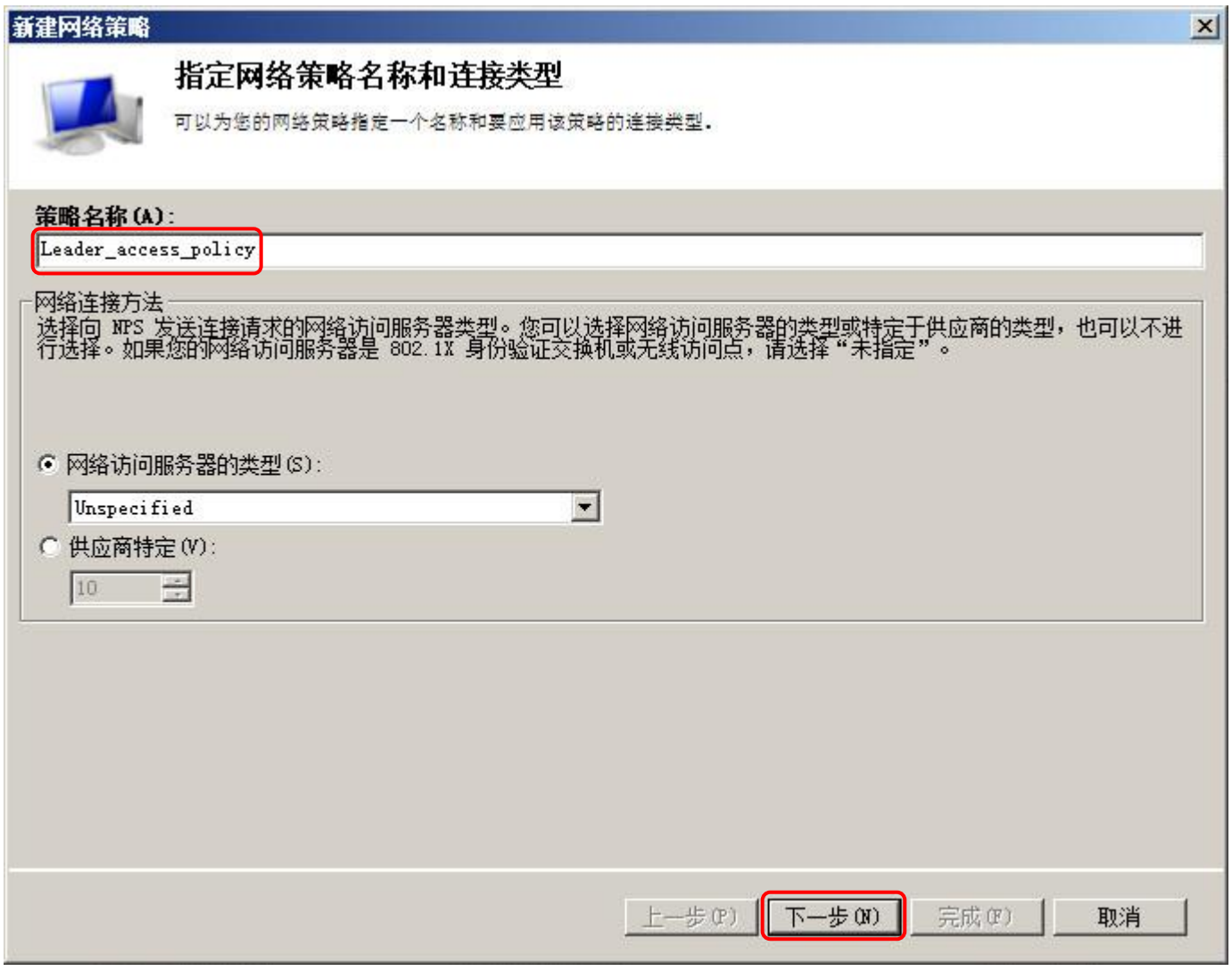


配置完成之后，可以成功通过 802.1X 认证，连接无线网络。

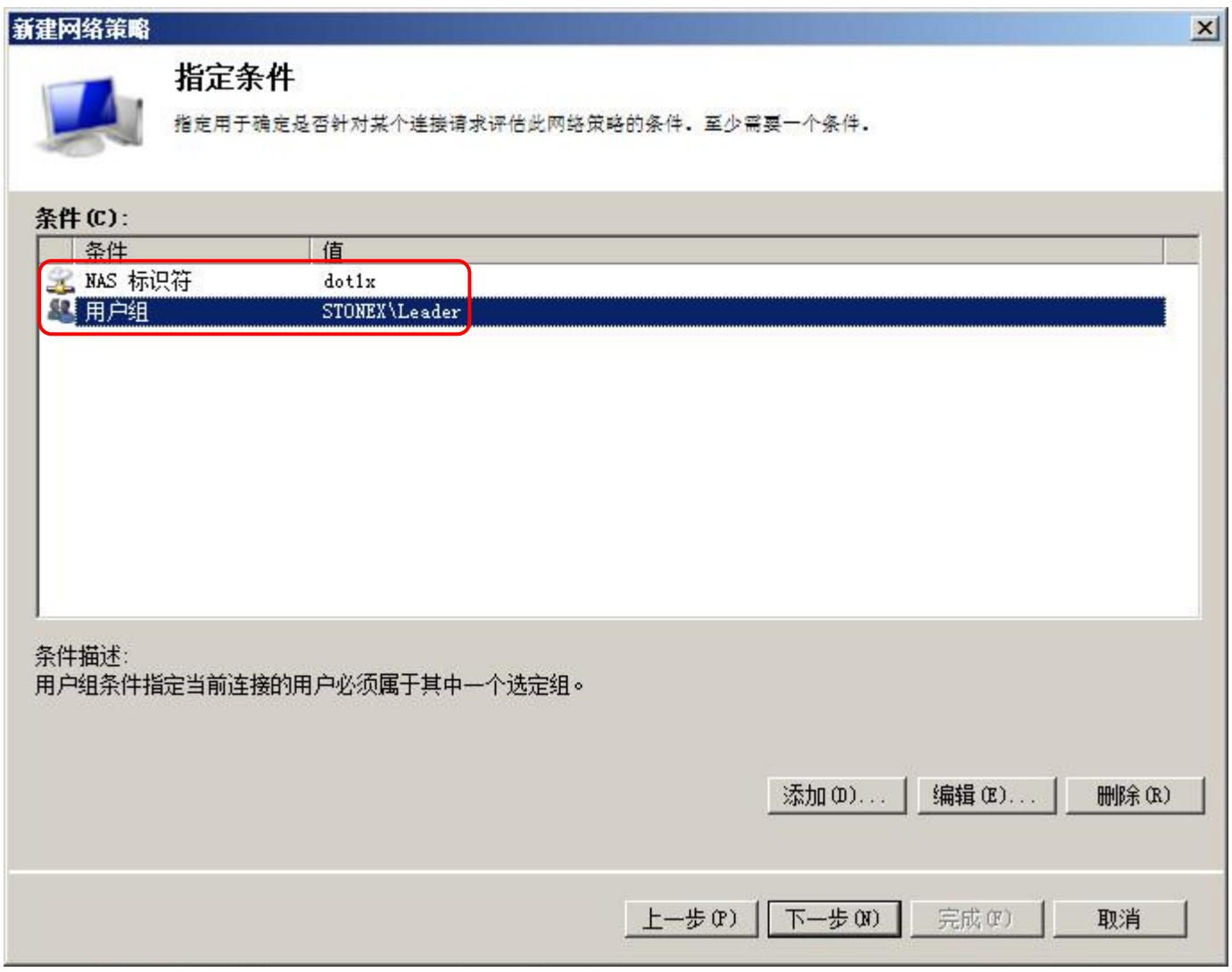
4.实现用户角色控制

通过配置网络策略还可以实现用户角色的控制，此处示例是实现不同组的用户获取不同的 User-Role。

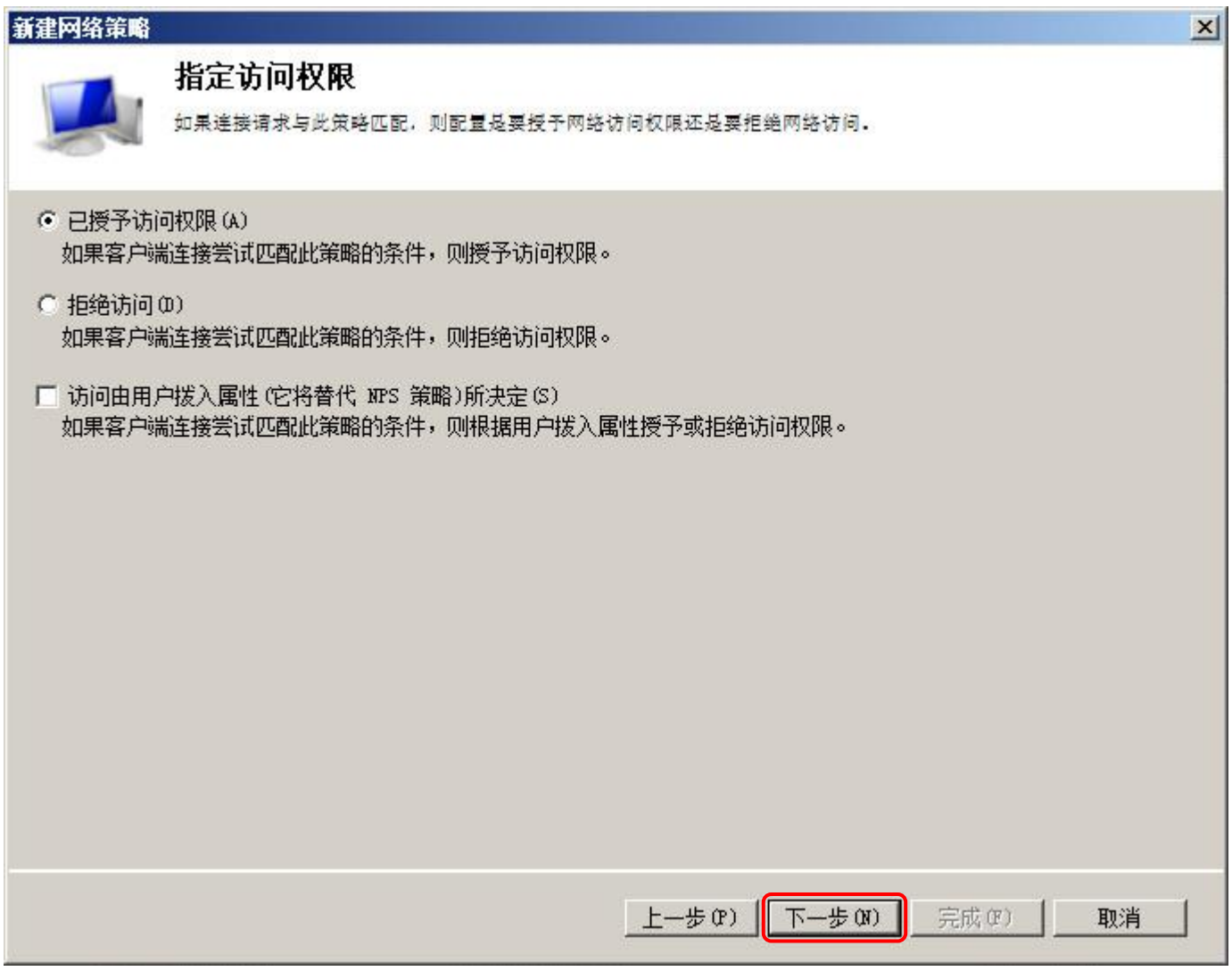
新建一个网络策略，点击下一步



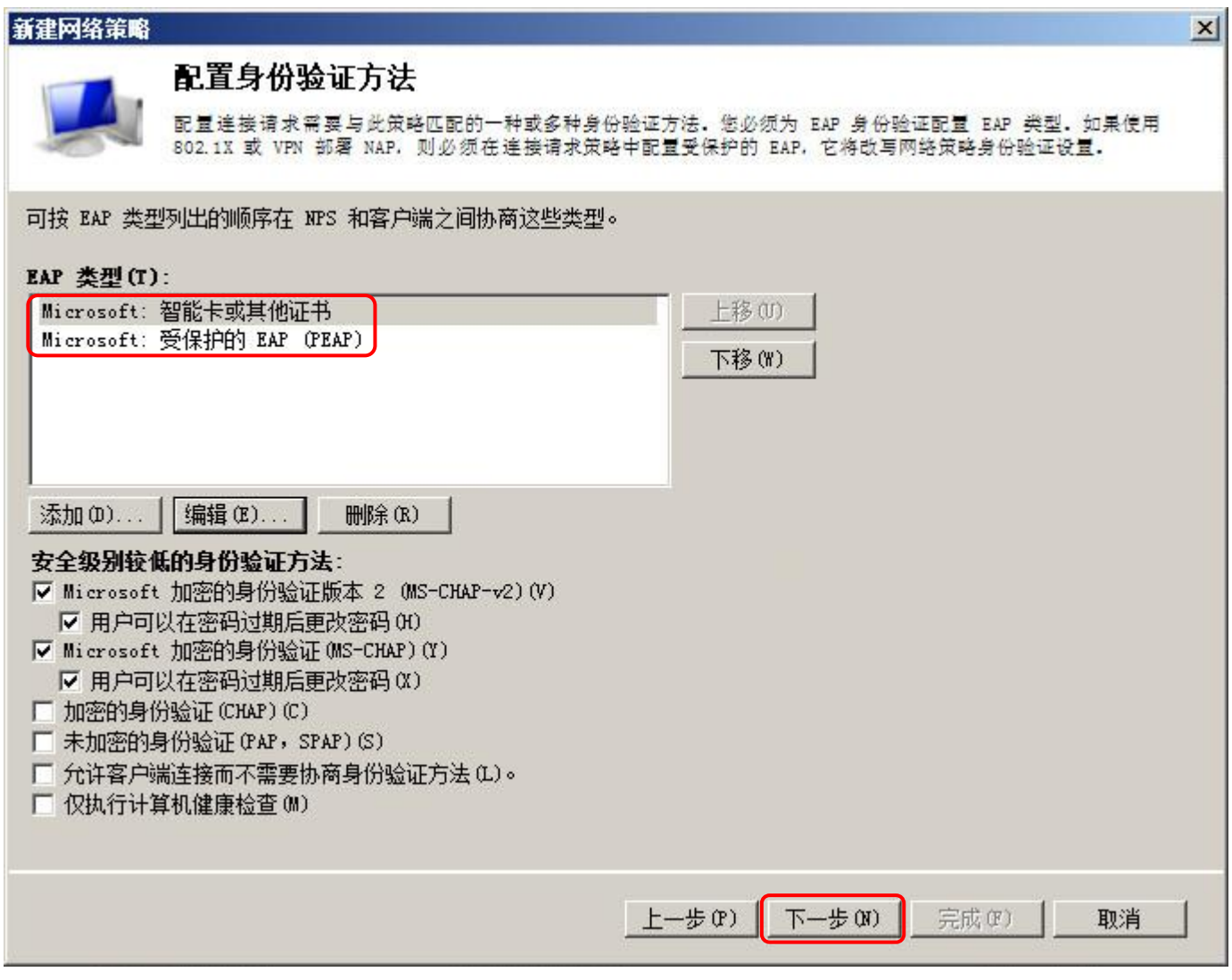
此处添加条件，NAS 标识符 dot1x 和用户组 Leader，点击下一步



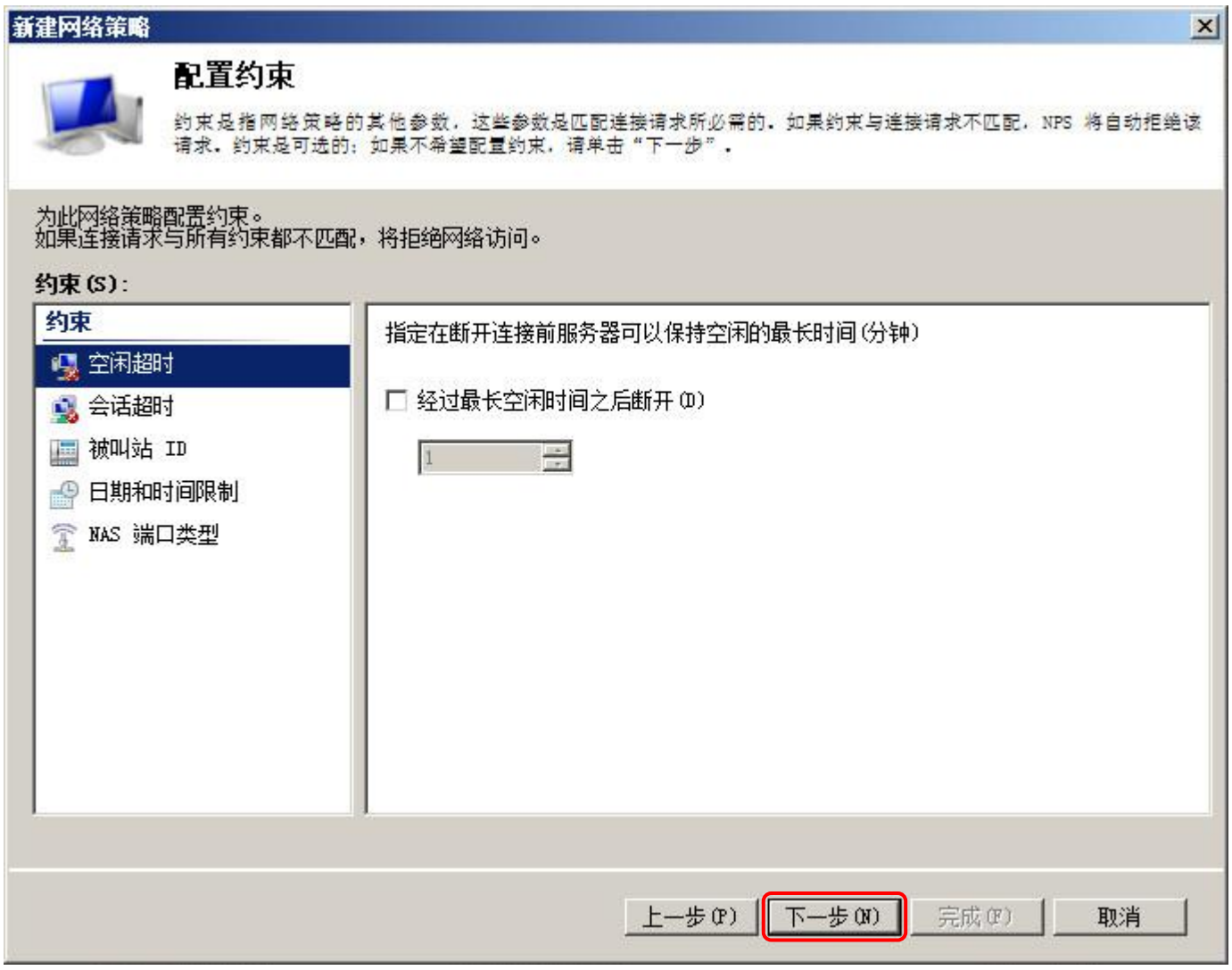
点击下一步


新建网络策略
指定访问权限
如果连接请求与此策略匹配，则配置是要授予网络访问权限还是要拒绝网络访问。
已授予访问权限(A)
如果客户端连接尝试匹配此策略的条件，则授予访问权限。
拒绝访问(D)
如果客户端连接尝试匹配此策略的条件，则拒绝访问权限。
访问由用户拨入属性(它将替代 NPS 策略)所决定(S)
如果客户端连接尝试匹配此策略的条件，则根据用户拨入属性授予或拒绝访问权限。
上一步(P)
下一步(N)
完成(F)
取消

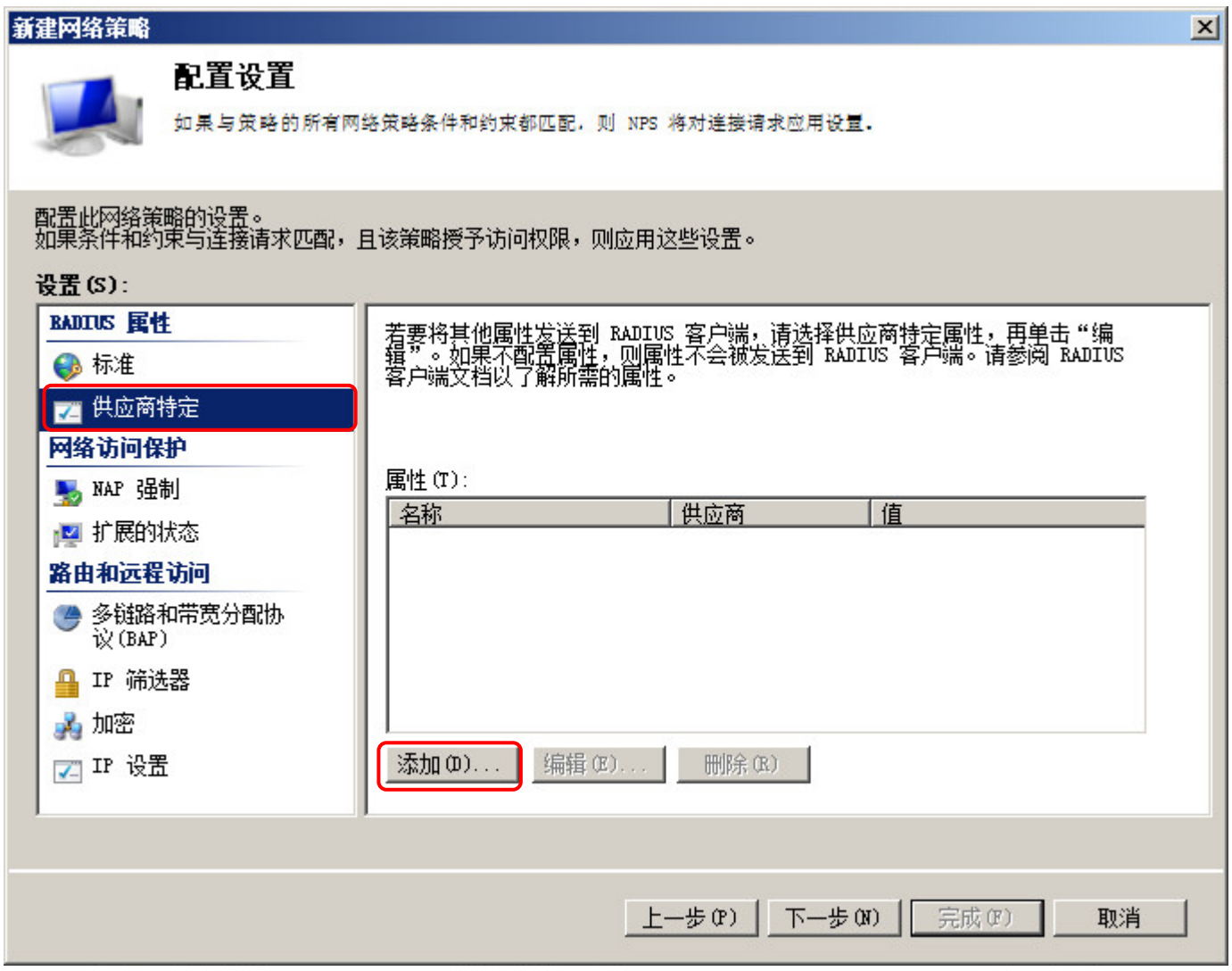
点击下一步


新建网络策略
配置身份验证方法
配置连接请求需要与此策略匹配的一种或多种身份验证方法。您必须为 EAP 身份验证配置 EAP 类型。如果使用 802.1X 或 VPN 部署 NAP，则必须在连接请求策略中配置受保护的 EAP，它将改写网络策略身份验证设置。
可按 EAP 类型列出的顺序在 NPS 和客户端之间协商这些类型。
EAP 类型(T):
Microsoft: 智能卡或其他证书
Microsoft: 受保护的 EAP (PEAP)
上移(U)
下移(W)
添加(D)...
编辑(E)...
删除(R)
安全级别较低的身份验证方法:
Microsoft 加密的身份验证版本 2 (MS-CHAP-v2)(V)
用户可以在密码过期后更改密码(H)
Microsoft 加密的身份验证(MS-CHAP)(Y)
用户可以在密码过期后更改密码(X)
加密的身份验证(CHAP)(C)
未加密的身份验证(PAP，SPAP)(S)
允许客户端连接而不需要协商身份验证方法(L)。
仅执行计算机健康检查(M)
上一步(P)
下一步(N)
完成(F)
取消

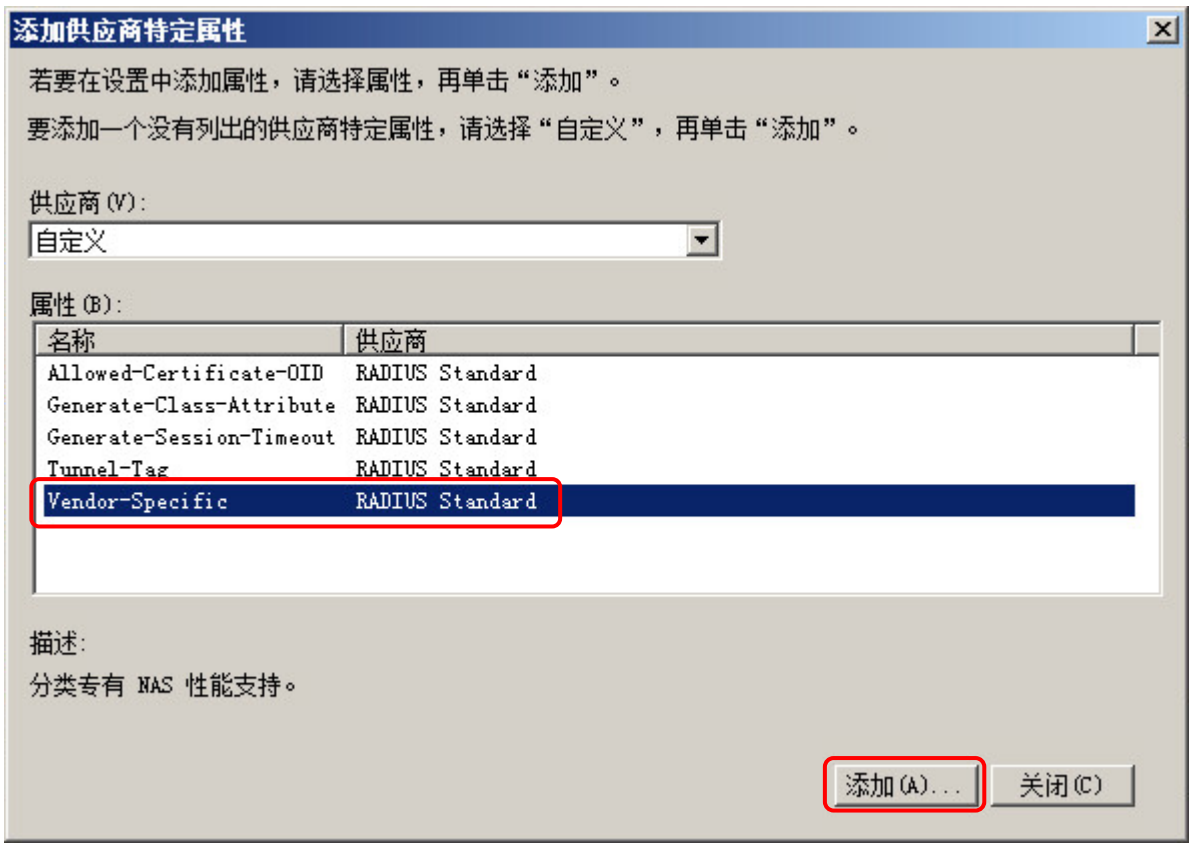
点击下一步



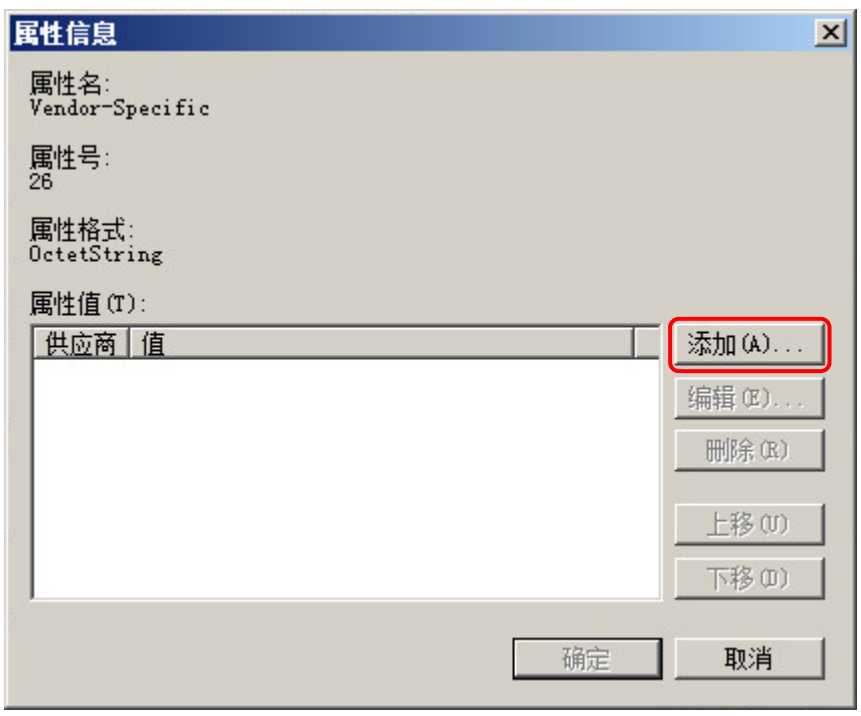
添加 VSA 属性，点击添加



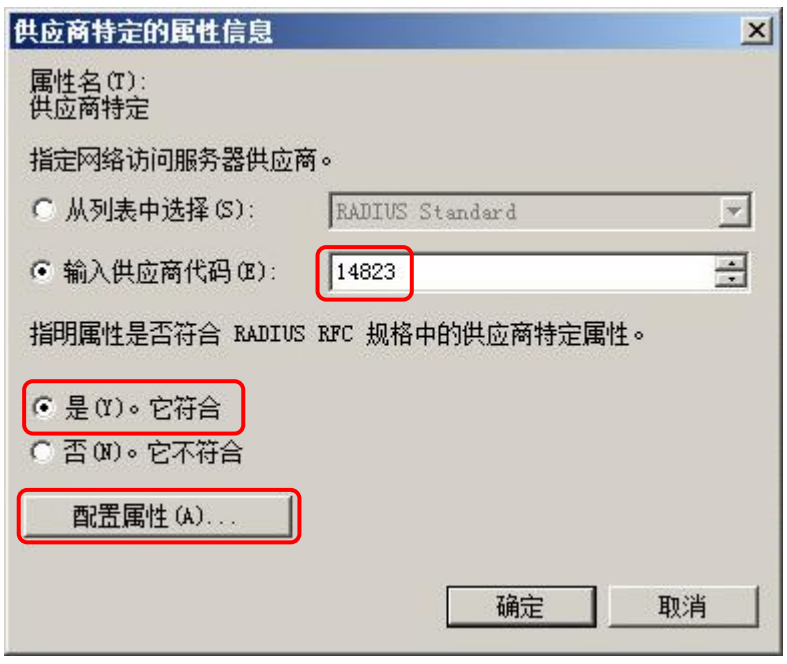
选择 Vendor-Specific，点击添加



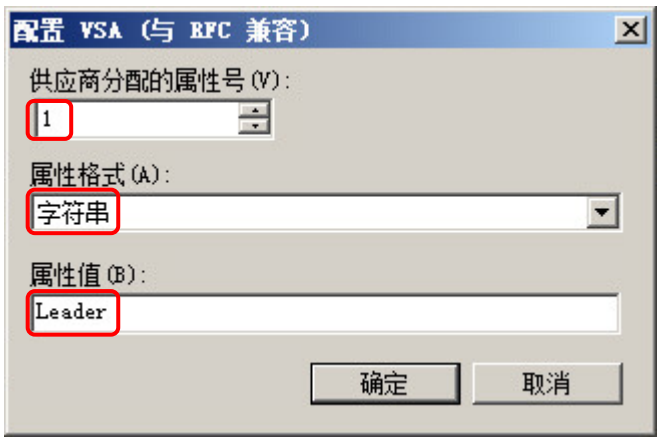
点击添加



输入供应商代码：Aruba 的为 14823

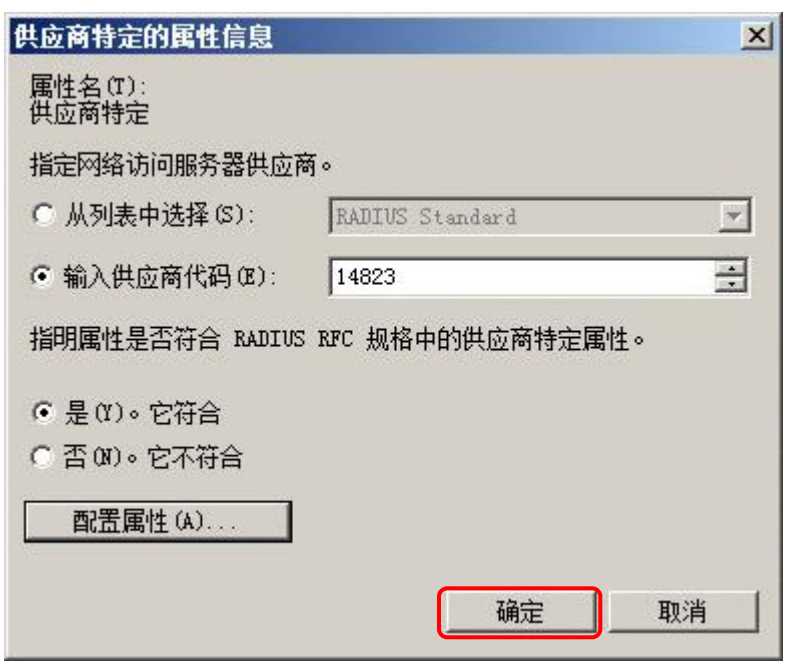


配置属性如下：

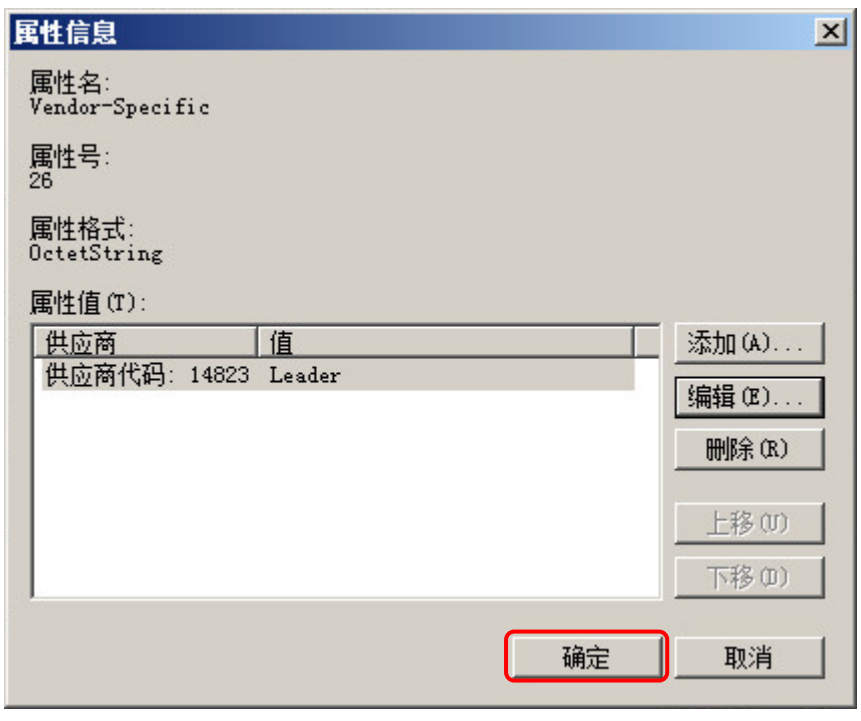


此处的属性值 Leader 就是要定义的 User-role

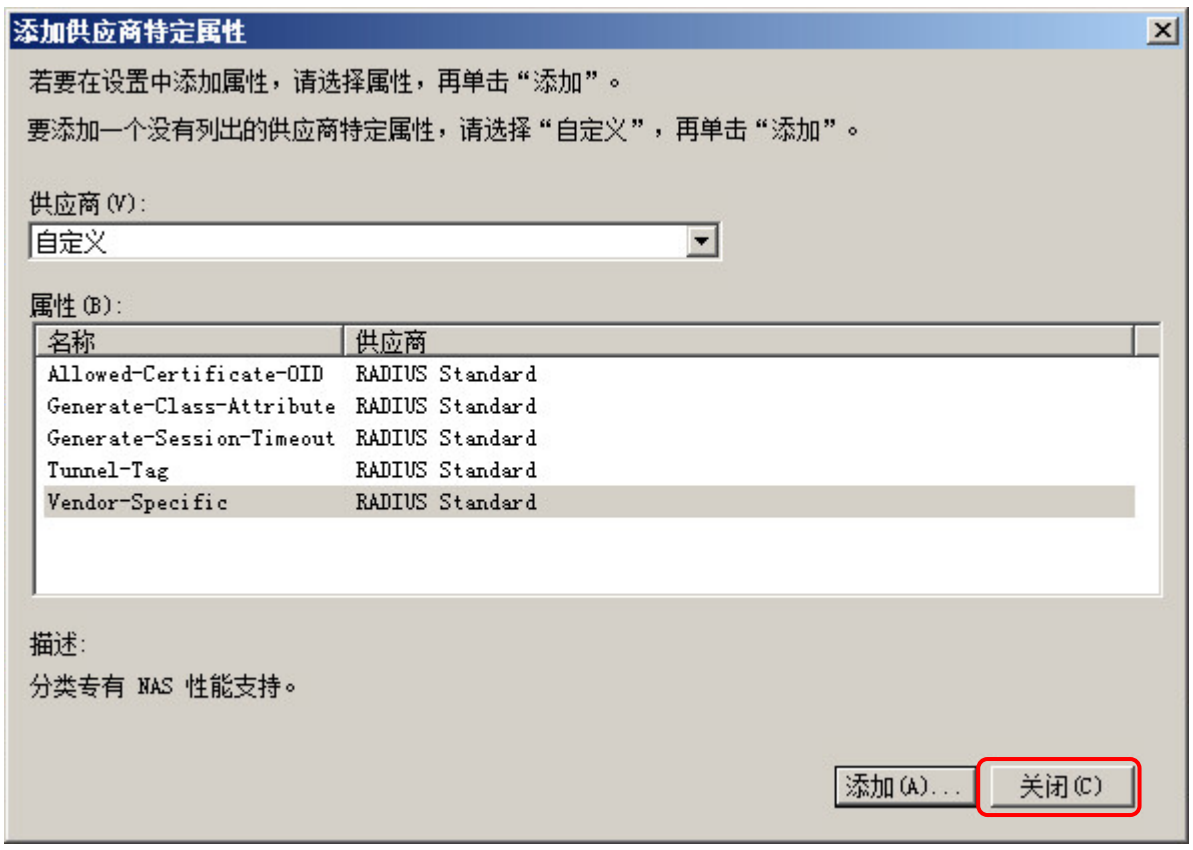
点击确定



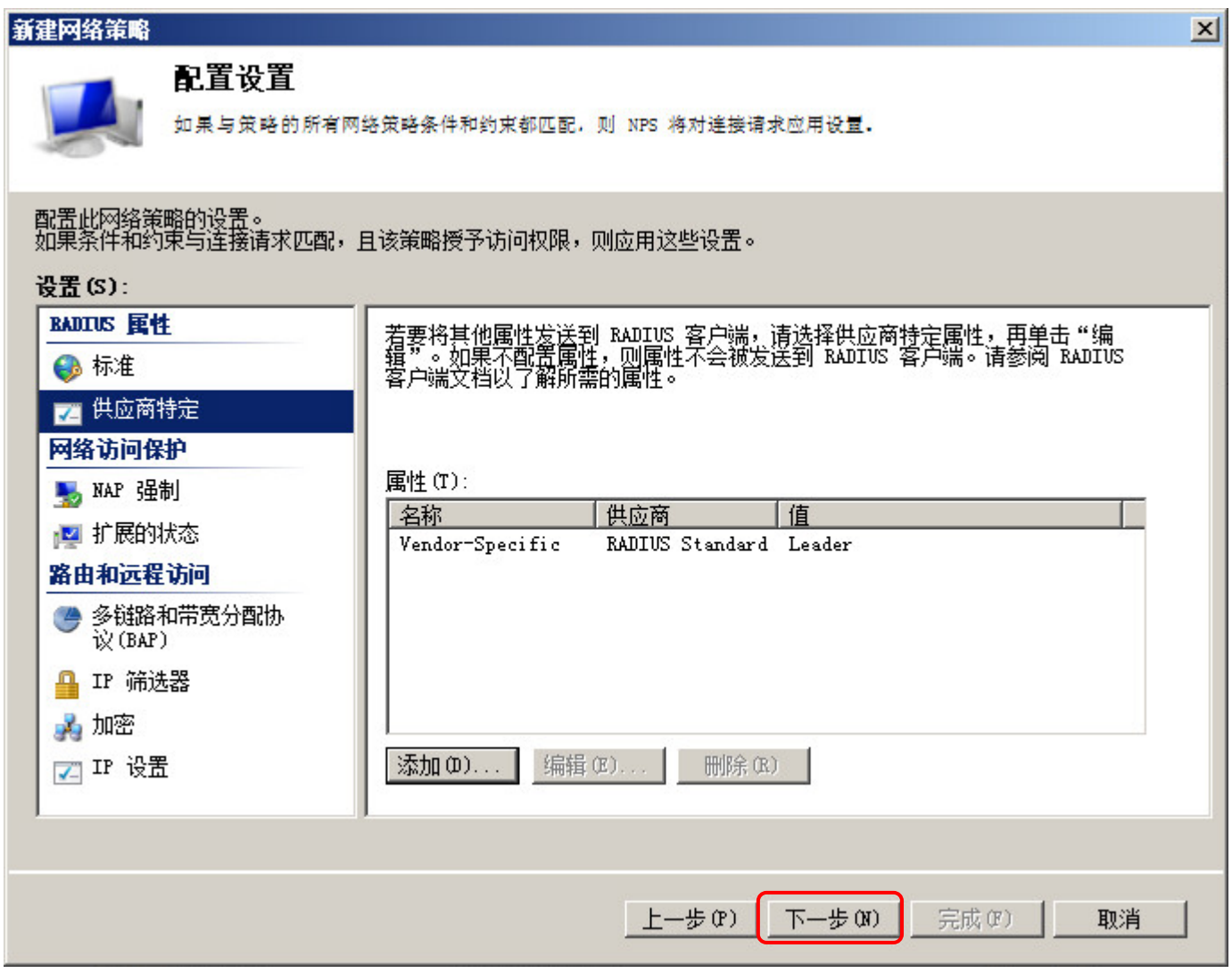
点击确定



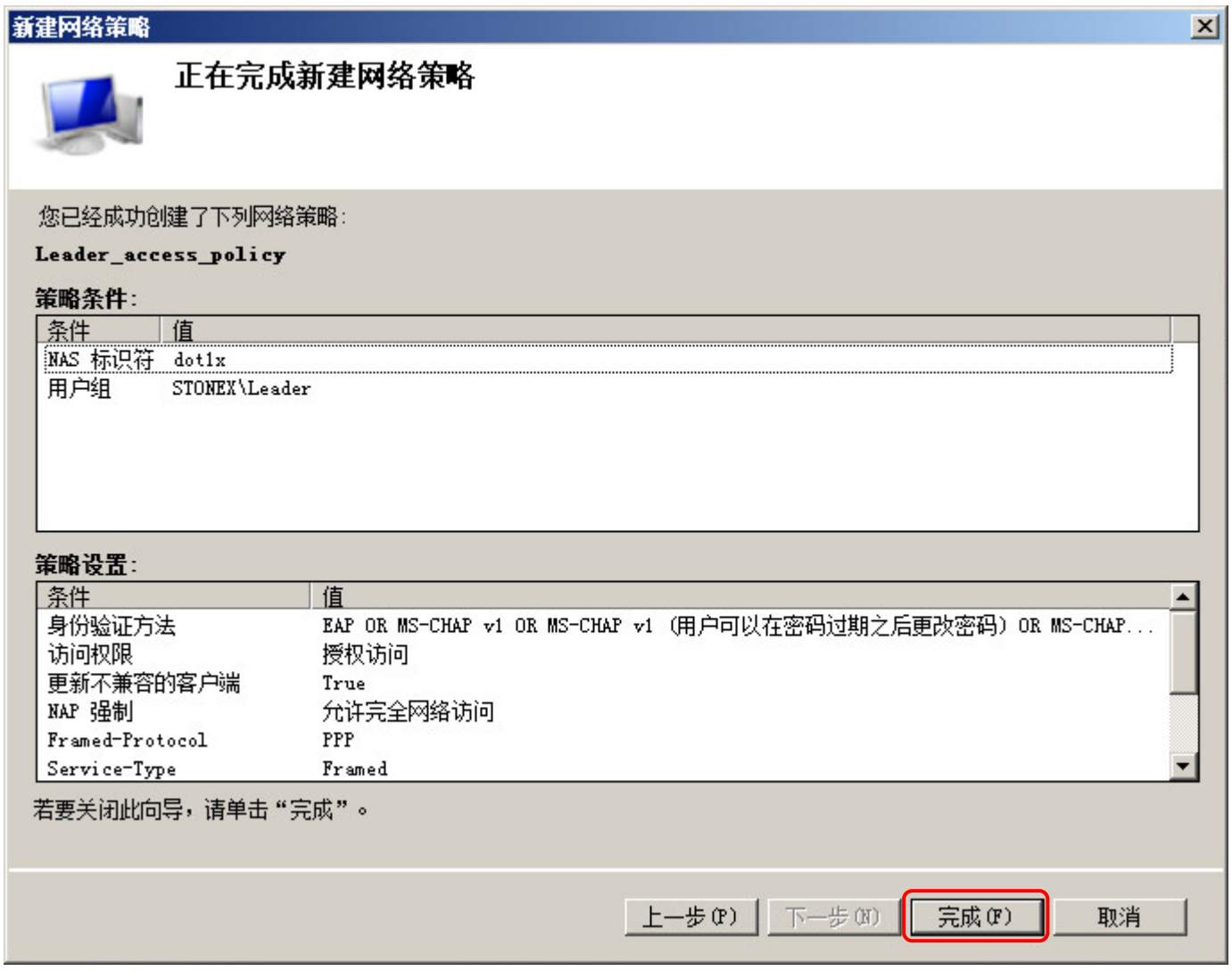
点击关闭


添加供应商特定属性
若要在设置中添加属性，请选择属性，再单击“添加”。
要添加一个没有列出的供应商特定属性，请选择“自定义”，再单击“添加”。
供应商(V):
自定义
属性(B):
名称
供应商
Allowed-Certificate-OID
RADIUS Standard
Generate-Class-Attribute
RADIUS Standard
Generate-Session-Timeout
RADIUS Standard
Tunnel-Tag
RADIUS Standard
Vendor-Specific
RADIUS Standard
描述:
分类专有 NAS 性能支持。
添加(A)...
关闭(C)

点击下一步


新建网络策略
配置设置
如果与策略的所有网络策略条件和约束都匹配，则 NPS 将对连接请求应用设置。
配置此网络策略的设置。
如果条件和约束与连接请求匹配，且该策略授予访问权限，则应用这些设置。
设置(S):
RADIUS 属性
标准
供应商特定
网络访问保护
NAP 强制
扩展的状态
路由和远程访问
多链路和带宽分配协议(BAP)
IP 筛选器
加密
IP 设置
若要将其他属性发送到 RADIUS 客户端，请选择供应商特定属性，再单击“编辑”。如果不配置属性，则属性不会被发送到 RADIUS 客户端。请参阅 RADIUS 客户端文档以了解所需的属性。
属性(T):
名称
供应商
值
Vendor-Specific
RADIUS Standard
Leader
添加(D)...
编辑(E)...
删除(R)
上一步(P)
下一步(N)
完成(F)
取消

点击完成



配置完成之后，属于 Leader 组的用户认证会获取到 User-role：Leader

还可以使用其他的 VSA 属性实现灵活的用户角色/策略控制

查看查看还有哪些 ARUBA VSA 属性：

```
(Aruba650) #show aaa radius-attributes | include 14823
Aruba-Mdps-Device-Version          21     String       Aruba      14823
Aruba-Mdps-Max-Devices             18     Integer      Aruba      14823
Aruba-Location-Id                  6      String       Aruba      14823
Aruba-Template-User                8      String       Aruba      14823
Aruba-No-DHCP-Fingerprint          14     Integer      Aruba      14823
Aruba-AirGroup-Device-Type         27     Integer      Aruba      14823
Aruba-Mdps-Device-Profile          33     String       Aruba      14823
Aruba-Mdps-Device-Udid             15     String       Aruba      14823
Aruba-AirGroup-Shared-User         25     String       Aruba      14823
Aruba-Mdps-Device-Serial           22     String       Aruba      14823
Aruba-AP-IP-Address                34     IP Addr      Aruba      14823
Aruba-Auth-Survivability           28     String       Aruba      14823
Aruba-User-Role                    1      String       Aruba      14823
Aruba-Port-Id                      7      String       Aruba      14823
Aruba-Priv-Admin-User              3      Integer      Aruba      14823
Aruba-Mdps-Device-Product          20     String       Aruba      14823
Aruba-WorkSpace-App-Name           31     String       Aruba      14823
Aruba-AS-Credential-Hash           30     String       Aruba      14823
Aruba-User-Vlan                    2      Integer      Aruba      14823
Aruba-AirGroup-Shared-Role         26     String       Aruba      14823
Aruba-Device-Type                  12     String       Aruba      14823
Aruba-Mdps-Device-Imei             16     String       Aruba      14823
Aruba-Essid-Name                   5      String       Aruba      14823
Aruba-AP-Group                     10     String       Aruba      14823
Aruba-AS-User-Name                 29     String       Aruba      14823
Aruba-CPPM-Role                    23     String       Aruba      14823
Aruba-Mdps-Device-Name             19     String       Aruba      14823
Aruba-Mdps-Provisioning-Settings   32     String       Aruba      14823
Aruba-AirGroup-User-Name           24     String       Aruba      14823
Aruba-Mdps-Device-Iccid            17     String       Aruba      14823
Aruba-Framed-IPv6-Address          11     String       Aruba      14823
Aruba-Named-User-Vlan              9      String       Aruba      14823
```