配置 NPS、无线局域网控制器和无线网络

目录

简介

先决条件

- 要求
- 使用的组件
- 规则

背景信息

PEAP 概述

- PEAP 第一阶段：TLS加密通道
- PEAP 第二阶段：采用 EAP 身份验证的通信

配置

- 网络图
- 配置
  - 配置 Microsoft Windows 2008 Server
  - 将 Microsoft Windows 2008 Server 配置为域控制器
  - 在 Microsoft Windows 2008 Server 上安装和配置 DHCP 服务
  - 安装并配置Microsoft Windows 2008 Server作为CA服务器
  - 将客户端连接到域
  - 在Microsoft Windows 2008 Server上安装网络策略服务器
  - 安装证书
  - 为PEAP-MS-CHAP v2身份验证配置网络策略服务器服务
  - 将用户添加到 Active Directory
  - 配置无线局域网控制器和LAP
  - 为RADIUS身份验证配置WLC
  - 为客户端配置 WLAN
  - 为PEAP-MS-CHAP v2身份验证配置无线客户端

验证

故障排除

相关信息

简介

本文档介绍如何使用 Microsoft NPS 作为 RADIUS 服务器来配置 PEAP 和 MS-CHAP 身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- Windows 2008基础安装知识

- 思科控制器安装知识

在尝试此配置之前，请确保已满足以下要求：

- 在测试实验室的每台服务器上安装Microsoft Windows Server 2008。
- 更新所有Service Pack。
- 安装控制器和轻量接入点(LAP)。
- 配置最新的软件更新。

有关Cisco 5508系列无线控制器的初始安装和配置信息，请参阅Cisco 5500系列无线控制器安装指南。



注意：本文档旨在为读者提供有关Microsoft服务器上进行PEAP-MS-CHAP身份验证所需的配置的示例。本文档中介绍的Microsoft Windows服务器配置已在实验室中经过测试，发现可以按预期工作。如果配置有问题，请与Microsoft联系以获得帮助。思科技术支持中心(TAC)不支持Microsoft Windows服务器配置。

Microsoft Windows 2008安装和配置指南可在Microsoft Tech Net上找到。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件版本7.4的Cisco 5508无线控制器
- 采用轻量接入点协议(LWAPP)的Cisco Aironet 3602接入点(AP)
- 安装了NPS、证书颁发机构(CA)、动态主机控制协议(DHCP)和域名系统(DNS)服务的Windows 2008企业服务器
- Microsoft Windows 7客户端电脑
- Cisco Catalyst 3560 系列交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

本文档提供了在思科统一无线网络中以Microsoft网络策略服务器(NPS)作为RADIUS服务器的受保护的可扩展身份验证协议(PEAP)和Microsoft质询握手身份验证协议(MS-CHAP)版本2身份验证的配置示例。

PEAP 概述

PEAP使用传输级安全(TLS)在经过身份验证的PEAP客户端（例如无线笔记本电脑）和PEAP身份验证器（例如Microsoft NPS或任何RADIUS服务器）之间创建加密通道。PEAP不指定身份验证方法，但为其他可扩展身份验证协议(EAP)（例如EAP-MS-CHAP v2）提供额外的安全性，这些协议可以通过PEAP提供的TLS加密通道运行。PEAP身份验证过程包括两个主要阶段。

PEAP 第一阶段：TLS加密通道

无线客户端将与 AP 相关联。基于IEEE 802.11的关联在客户端和接入点之间创建安全关联之前，提供开放系统或共享密钥身份验证。在客户端与接入点之间成功建立基于 IEEE 802.11 的关联之后，TLS 会话就会与 AP 进行协商。在无线客户端和NPS之间成功完成身份验证后，客户端和NPS之间将协商TLS会话。在此协商中派生的密钥将用来加密随后的所有通信。

PEAP 第二阶段：采用 EAP 身份验证的通信

EAP 通信（包括 EAP 协商）发生在由 PEAP 在 PEAP 认证过程的第一阶段中创建的 TLS 通道内。NPS使用EAP-MS-CHAP v2对无线客户端进行身份验证。LAP和控制器仅在无线客户端和RADIUS服务器之间转发消息。无线LAN控制器(WLC)和LAP无法解密这些消息，因为它不是TLS终端。

成功进行身份验证尝试（其中用户已提供了带PEAP-MS-CHAP v2的有效基于密码的凭证）的RADIUS消息序列为：

1. NPS向客户端发送身份请求消息：EAP 请求/身份。
2. 客户端回复一个身份响应消息：EAP 响应/身份。
3. NPS发送MS-CHAP v2质询消息：EAP 请求/EAP 类型=EAP MS-CHAP-V2（质询）。
4. 客户端回复一个 MS-CHAP v2 质询和响应：EAP 响应/EAP 类型=EAP-MS-CHAP-V2（响应）。
5. 当服务器成功对客户端进行身份验证时，NPS会发回MS-CHAP v2成功数据包：EAP 请求/EAP 类型=EAP-MS-CHAP-V2（成功）。
6. 当客户端对服务器的身份验证成功时，该客户端回复一个 MS-CHAP v2 成功数据包：EAP 响应/EAP 类型=EAP-MS-CHAP-V2（成功）。
7. NPS发送指示身份验证成功的EAP类型长度值(TLV)。
8. 客户端回复一个 EAP-TLV 状态成功消息。
9. 服务器完成身份验证并以明文发送EAP-Success消息。如果部署了 VLAN 用于客户端隔离，则此消息中还包含 VLAN 属性。

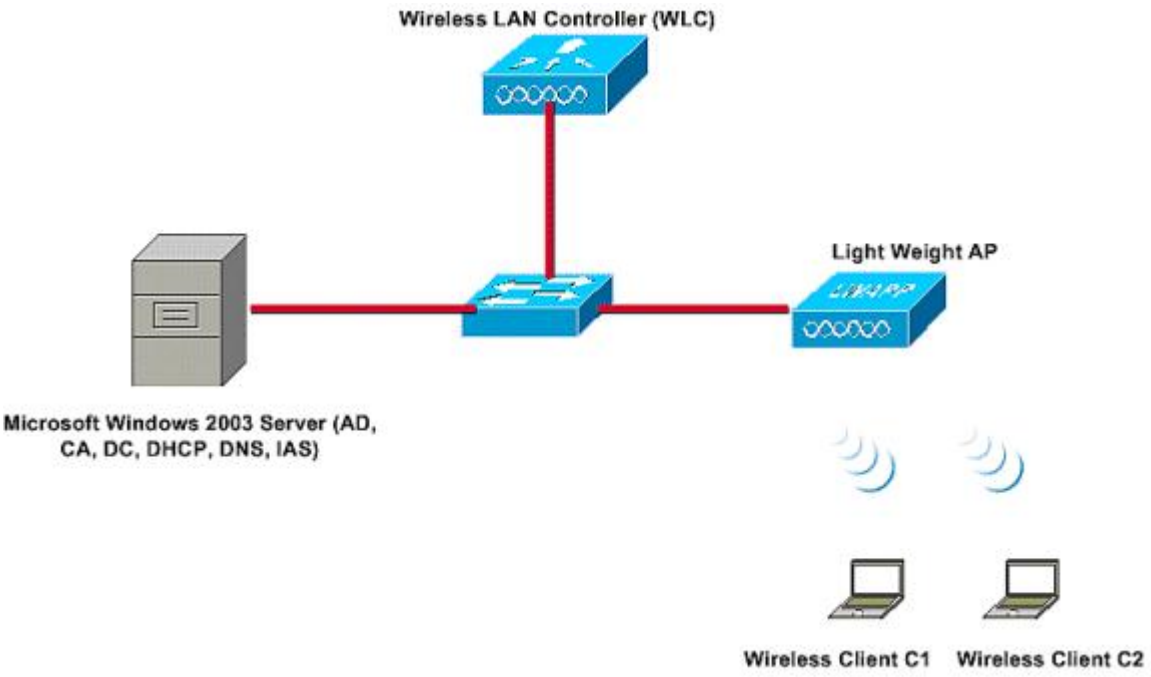
配置

在本节中，您将看到配置PEAP-MS-CHAP v2的信息。

注意：使用命令查找工具可获取本节所用命令的详细信息。只有注册的思科用户才能访问内部思科工具和信息。

网络图

此配置使用以下网络设置：



网络图

在此设置中，Microsoft Windows 2008 Server 担当以下角色：

- 域的域控制器
- DHCP/DNS 服务器
- CA 服务器
- NPS — 用于对无线用户进行身份验证
- Active Directory - 用于维护用户数据库

服务器通过第2层交换机连接到有线网络，如下所示。WLC和注册的LAP也通过第2层交换机连接到网络。

无线客户端使用Wi-Fi保护访问2(WPA2)- PEAP-MS-CHAP v2身份验证连接到无线网络。

配置

本示例的目的是配置Microsoft 2008服务器、无线LAN控制器和轻量AP，以使用PEAP-MS-CHAP v2身份验证对无线客户端进行身份验证。此过程有三个主要步骤：

1. 配置 Microsoft Windows 2008 Server.
2. 配置WLC和轻量AP。
3. 配置无线客户端.

配置 Microsoft Windows 2008 Server

在本示例中，Microsoft Windows 2008服务器的完整配置包括以下步骤：

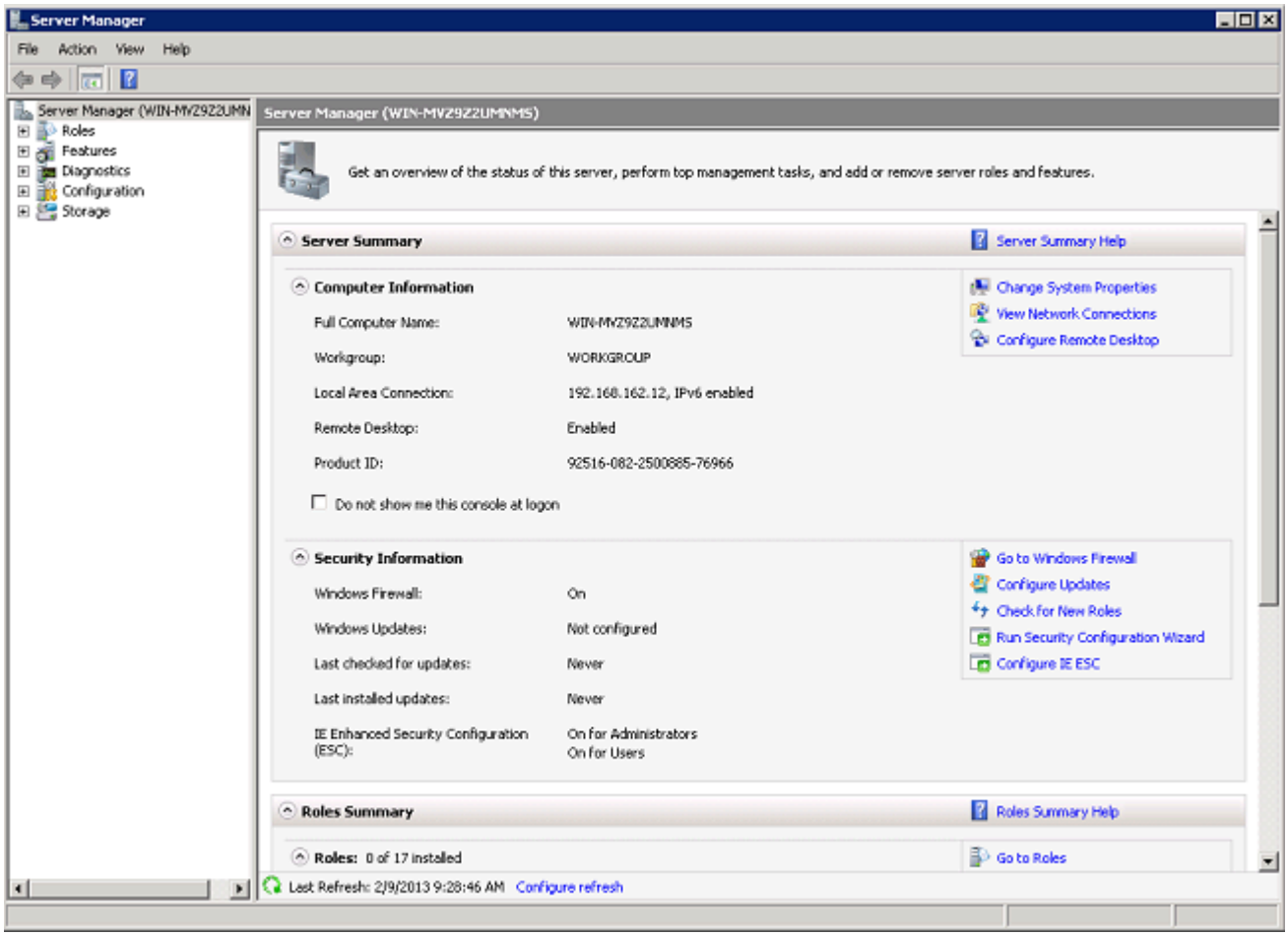
1. 将服务器配置为域控制器。

2. 安装和配置DHCP服务。
3. 安装服务器并将其配置为CA服务器。
4. 将客户端连接到域.
5. 安装NPS
6. 安装证书。
7. 为PEAP身份验证配置NPS。
8. 将用户添加到 Active Directory.

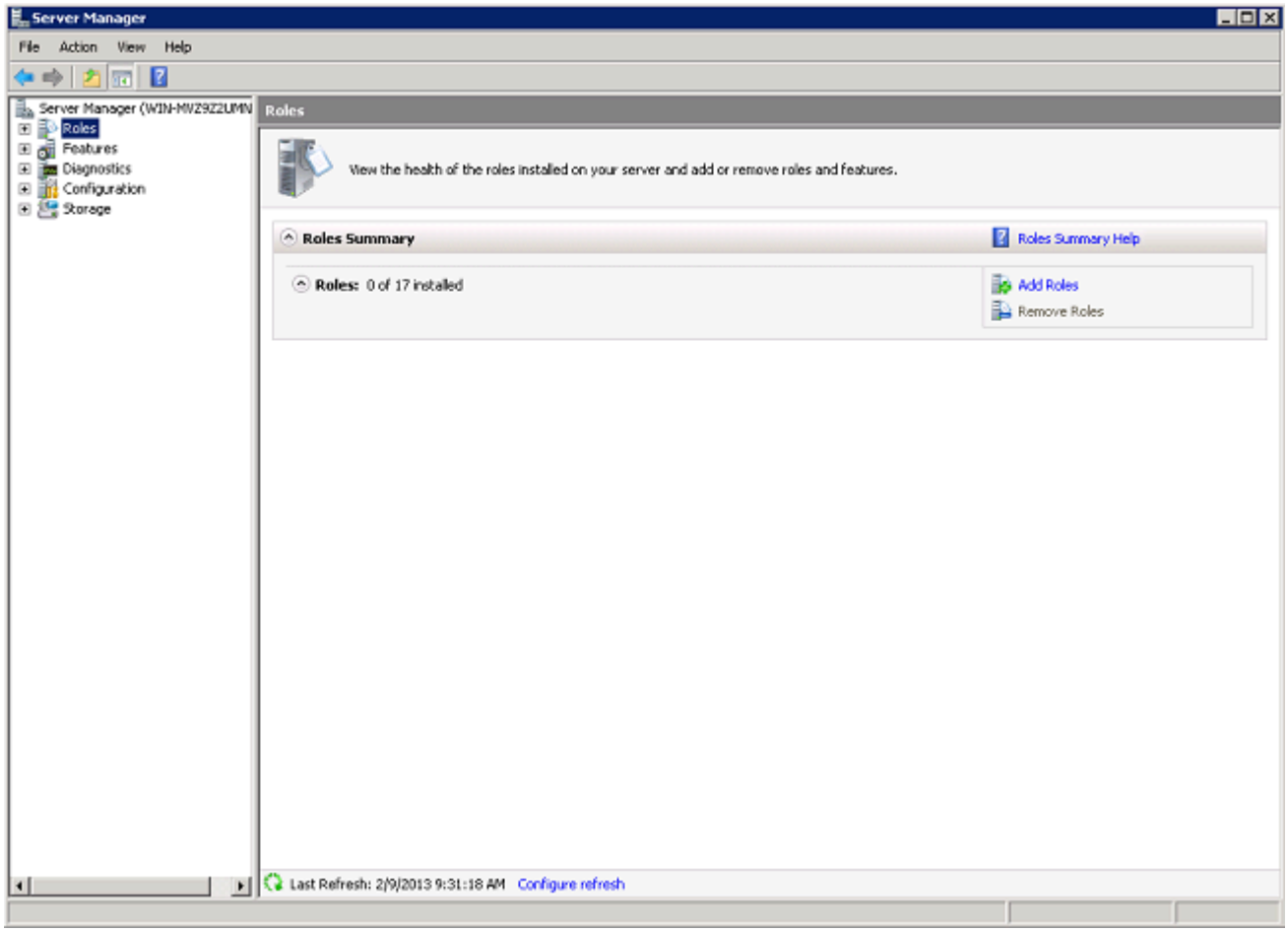
将 Microsoft Windows 2008 Server 配置为域控制器

要将Microsoft Windows 2008服务器配置为域控制器，请完成以下步骤：

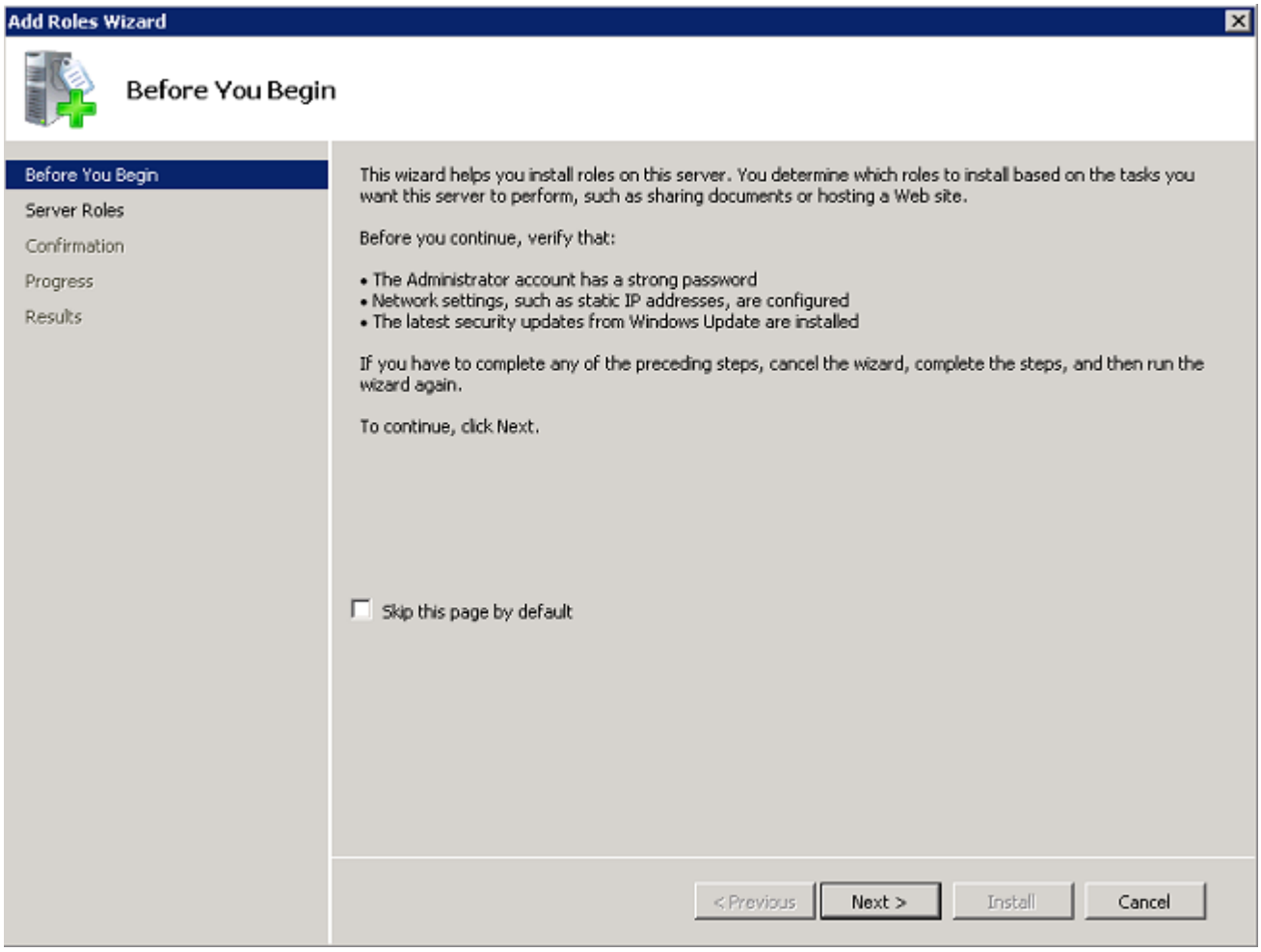
1. 单击开始> 服务器管理器。



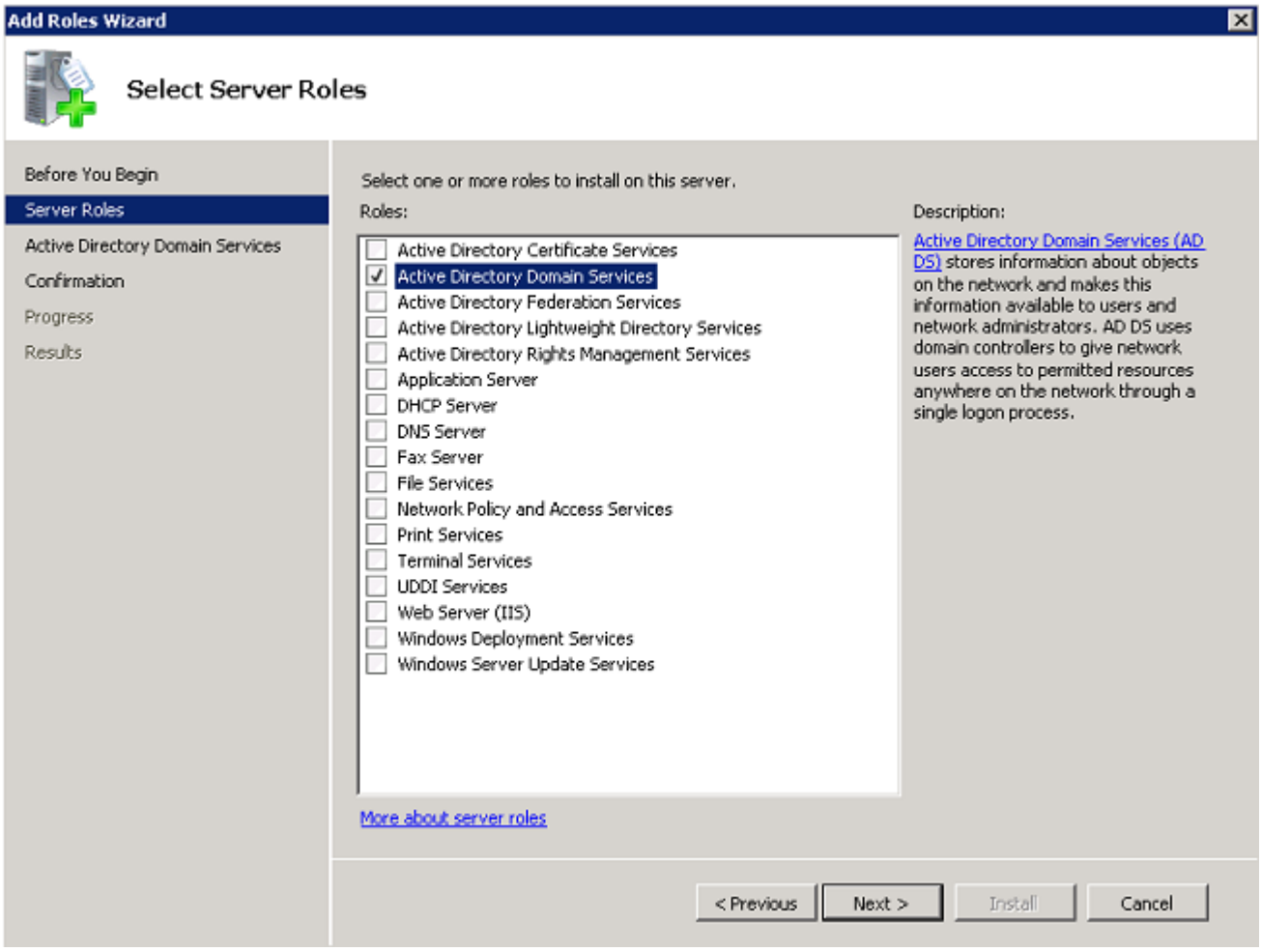
2. 单击Roles> Add Roles。


Server Manager
File Action View Help
Server Manager (WIN-MVZ9ZZUMN
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 0 of 17 installed
Add Roles
Remove Roles
Last Refresh: 2/9/2013 9:31:18 AM
Configure refresh

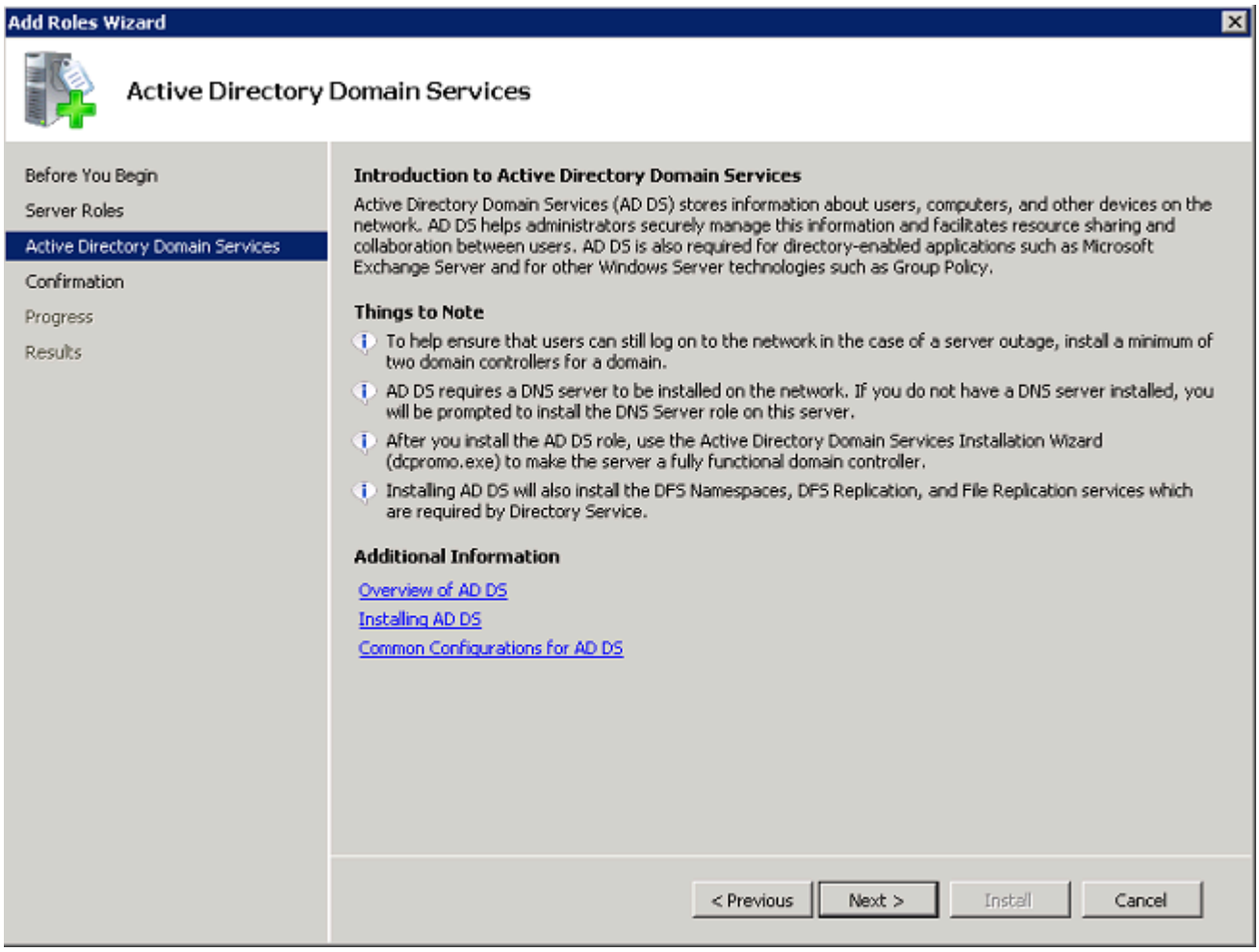
3. 单击 Next。



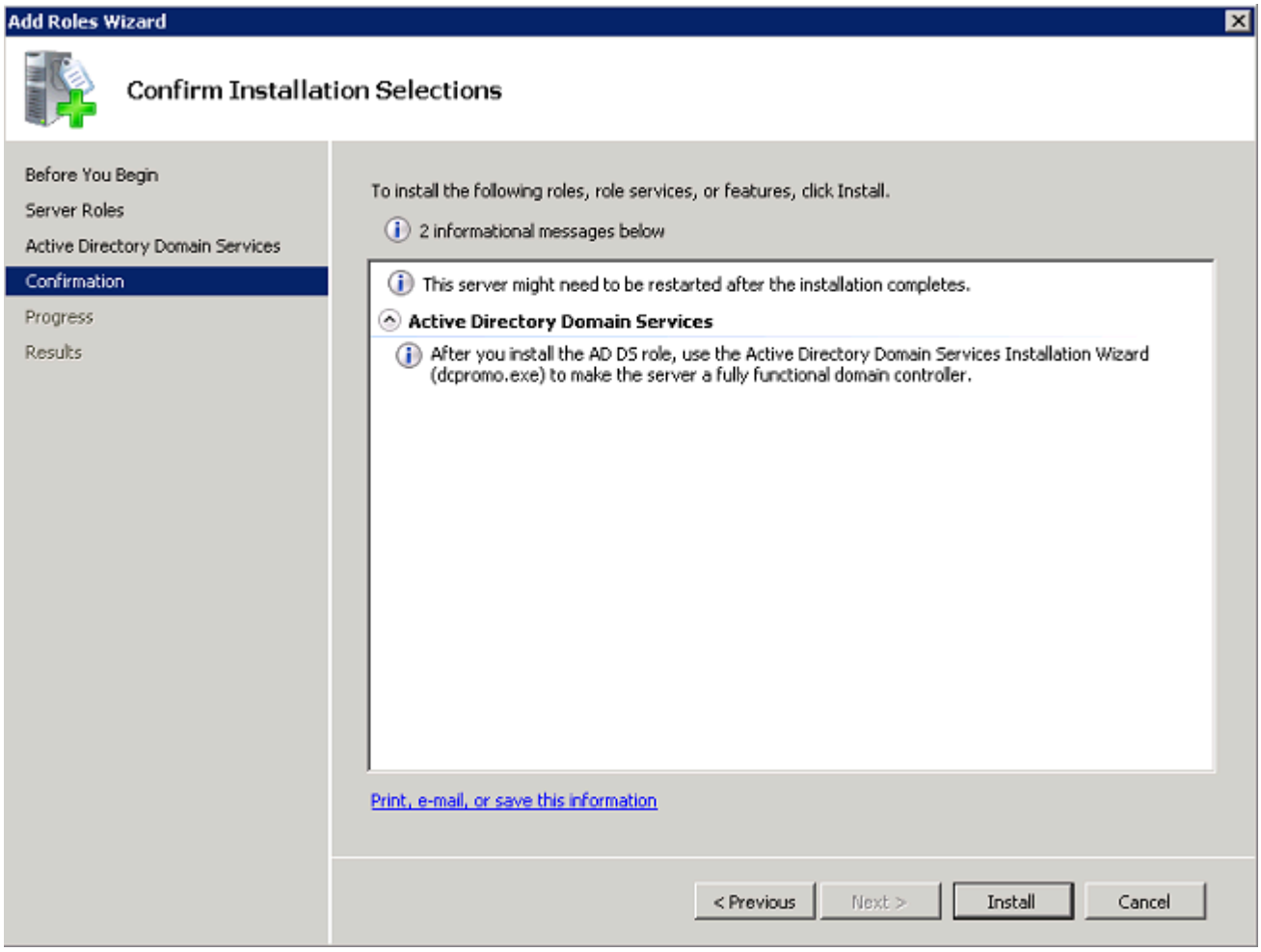
4. 选择服务Active Directory域服务，然后单击下一步。



5. 查看Active Directory域服务简介，然后点击下一步。

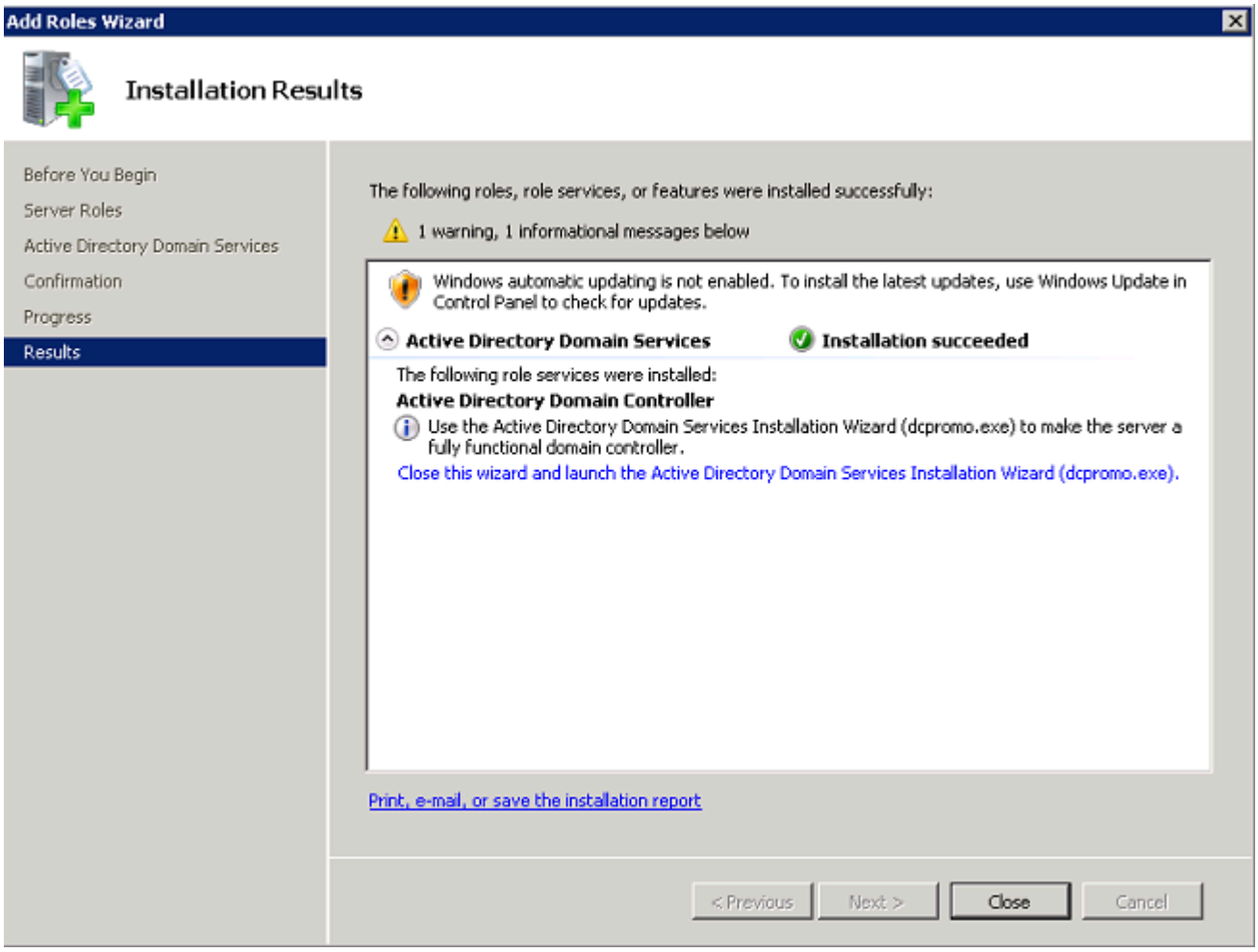


6. 单击安装开始安装过程。

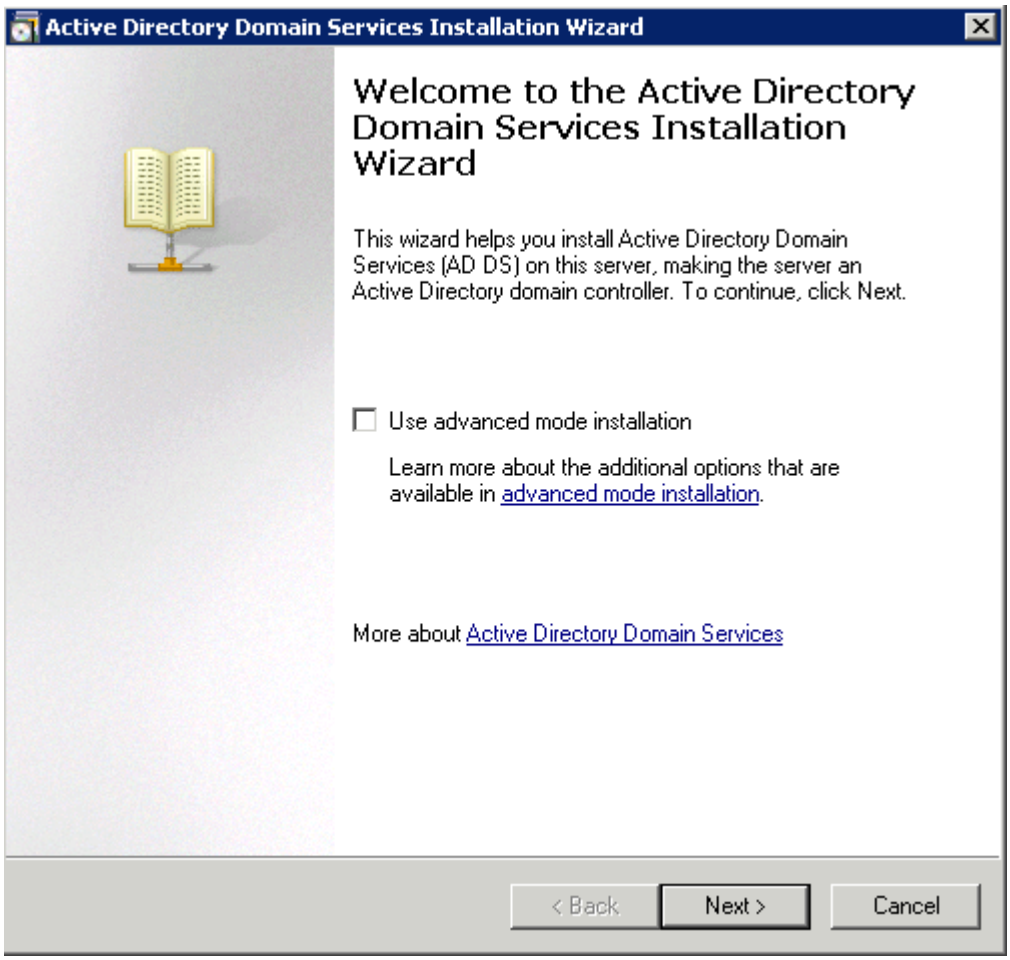


安装继续并完成。

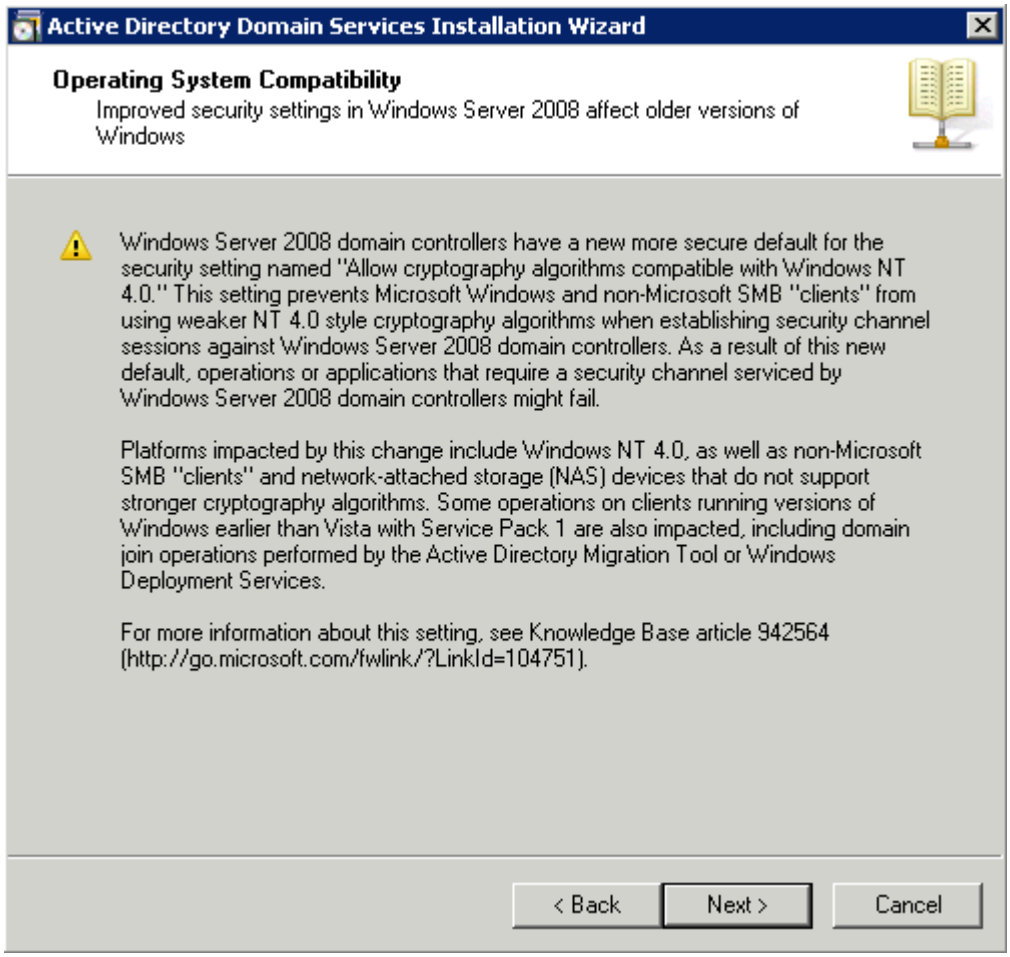
7. 单击Close this wizard（关闭此向导），然后启动Active Directory域服务安装向导(dcpromo.exe)以继续安装和配置Active Directory。



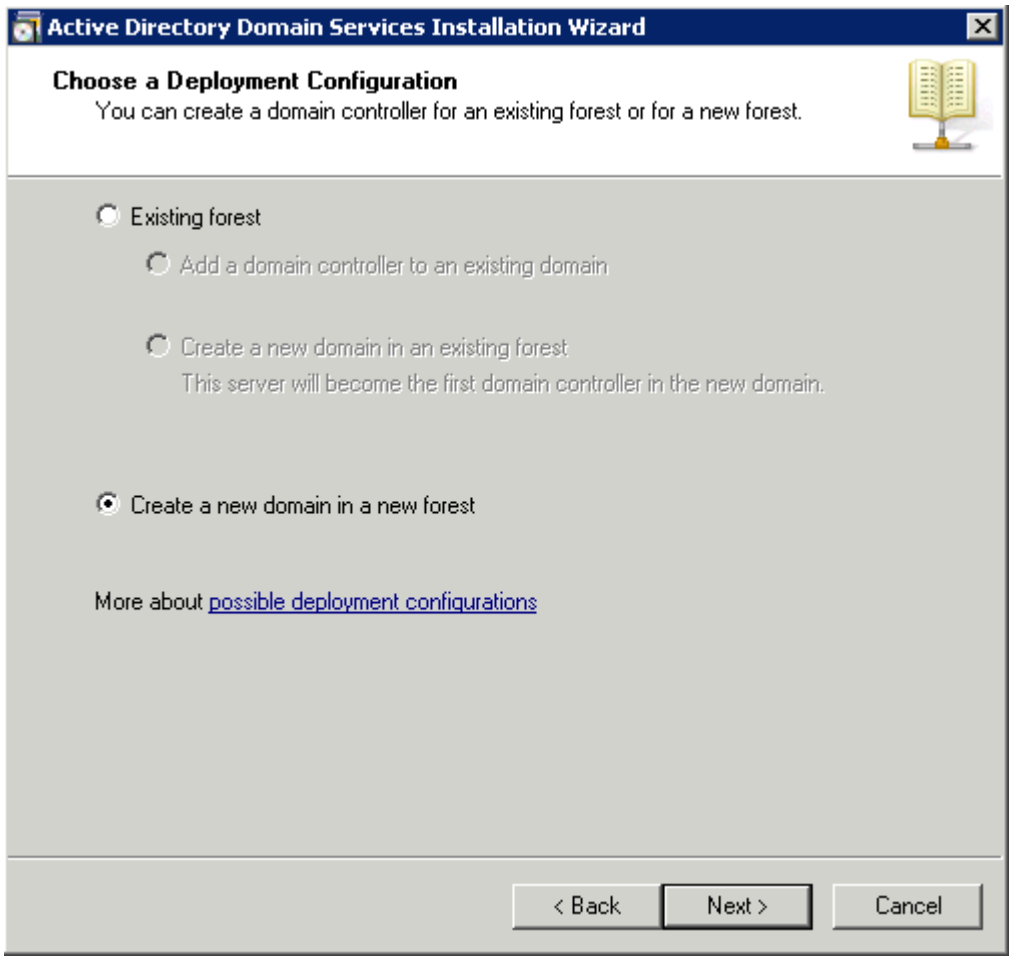
8. 单击下一步运行Active Directory域服务安装向导。



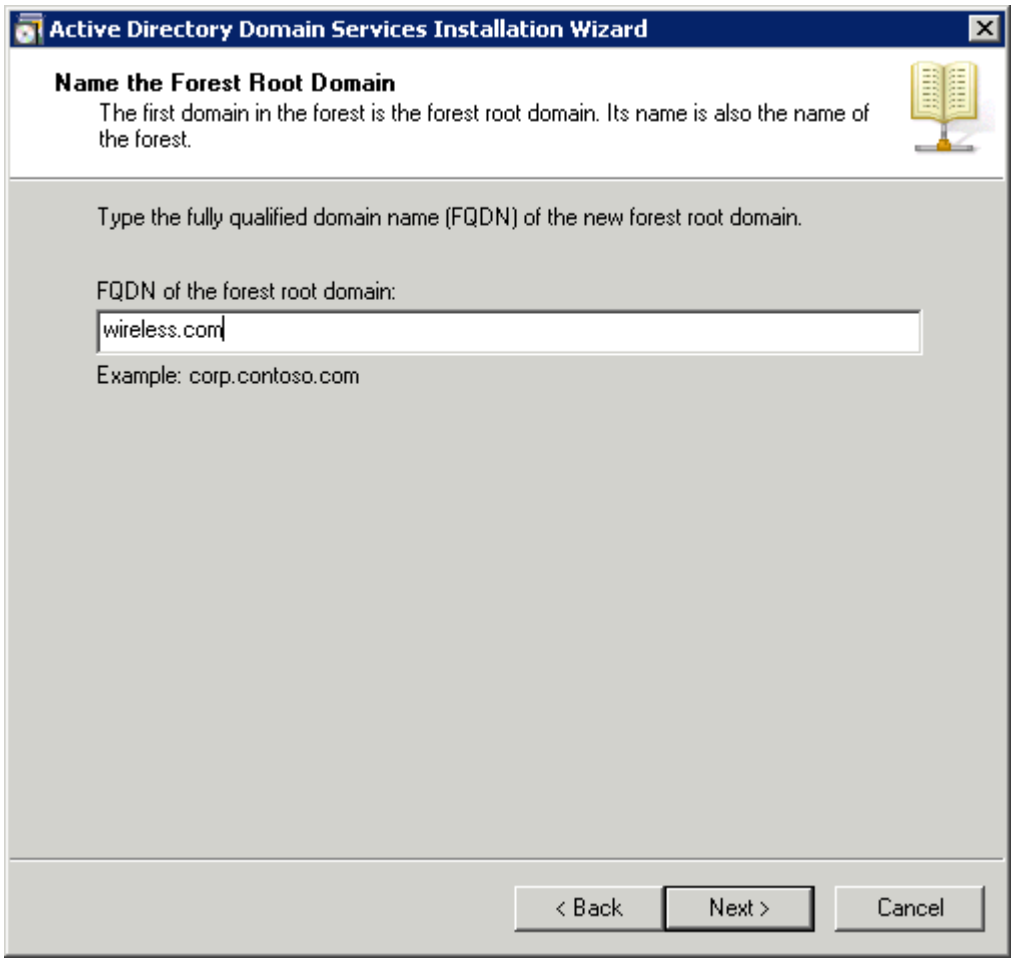
9. 查看有关操作系统兼容性的信息，然后单击下一步。



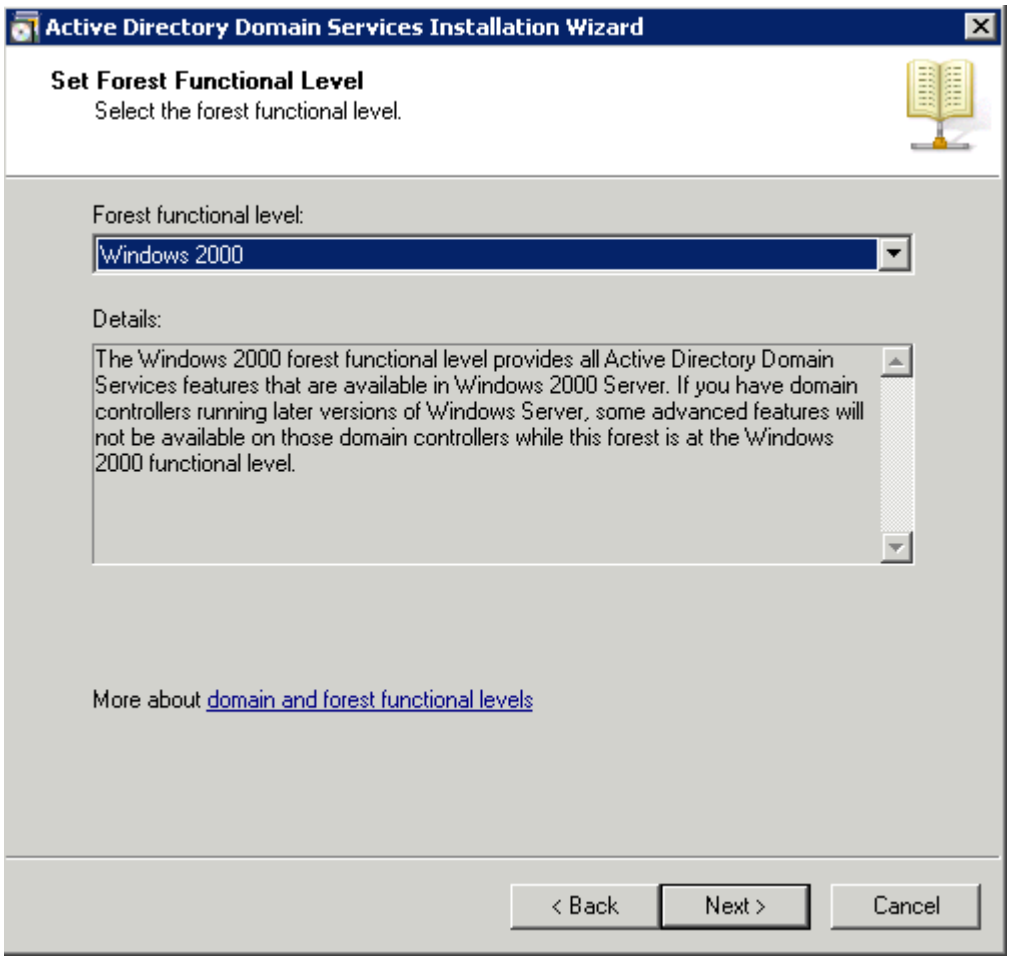
10. 单击在新林中创建新域>下一步以创建新域。



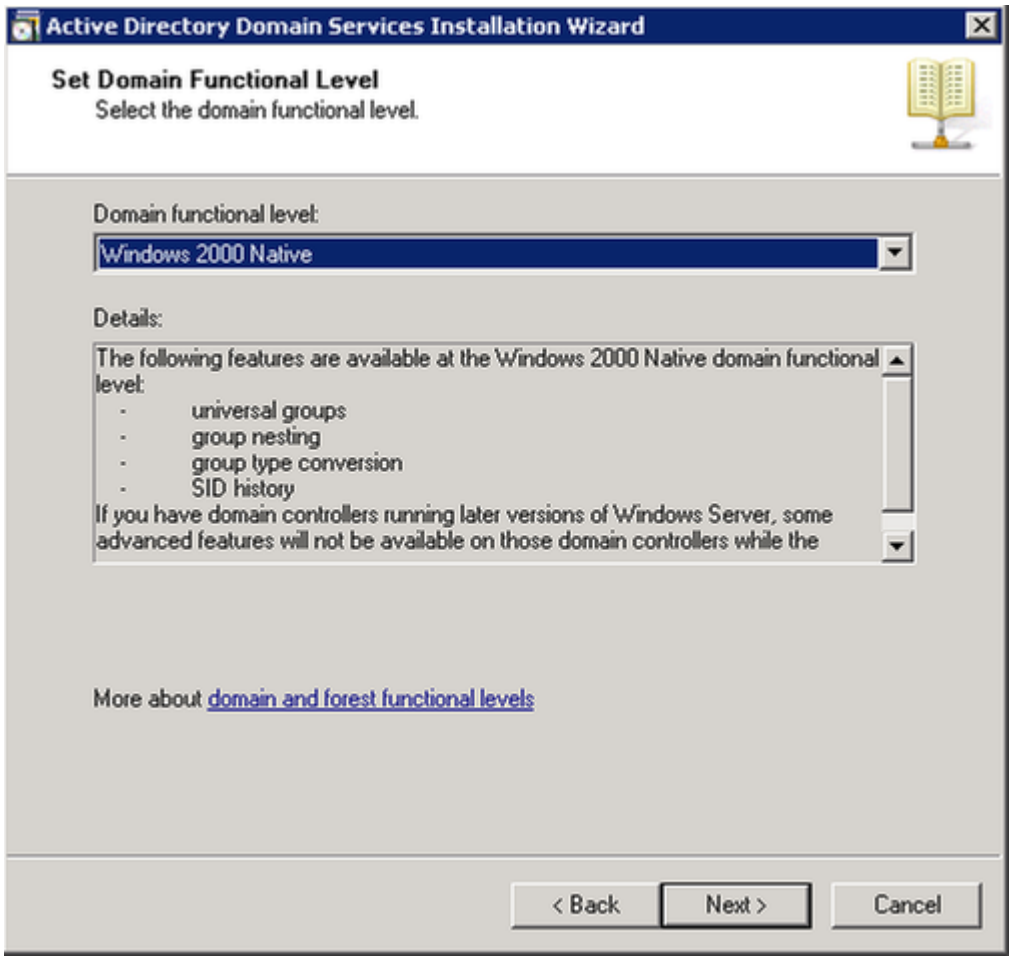
11. 输入新域的完整DNS名称，然后单击Next。



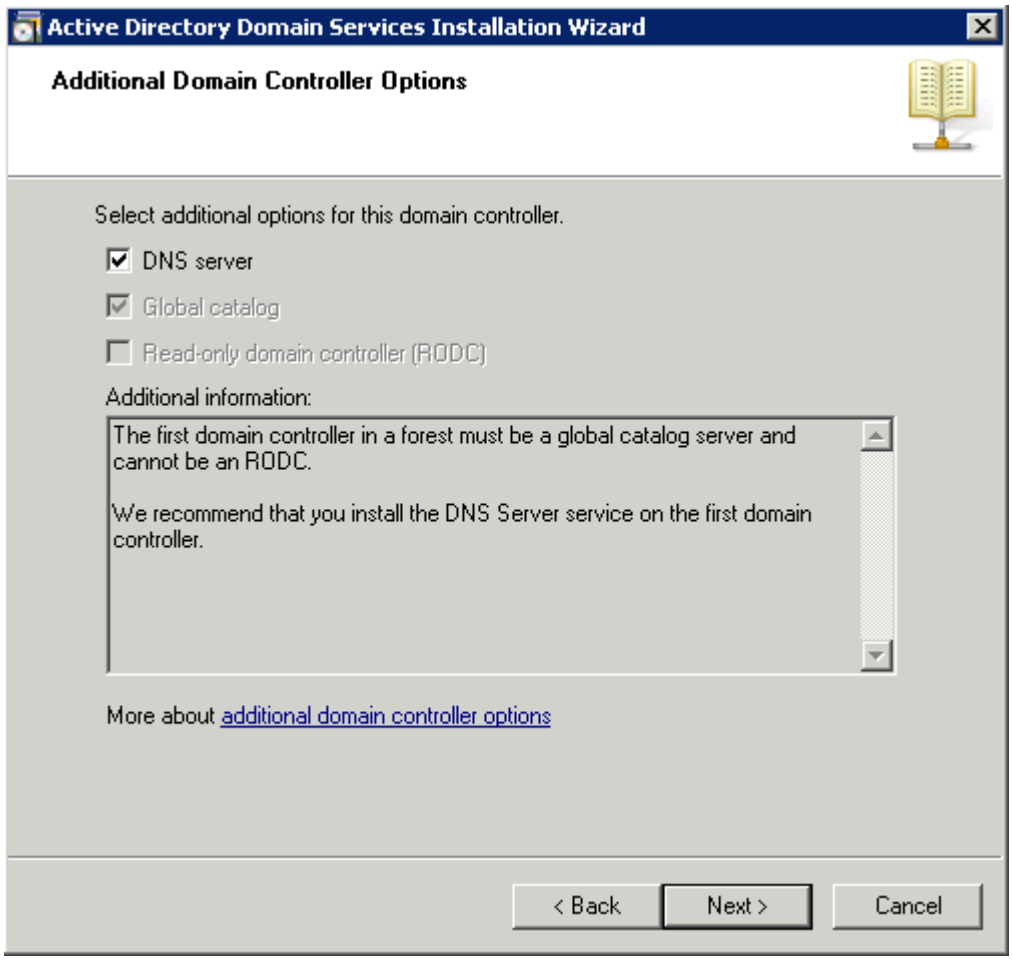
12. 选择域的林功能级别，然后单击下一步。



13. 选择域的域功能级别，然后单击Next。



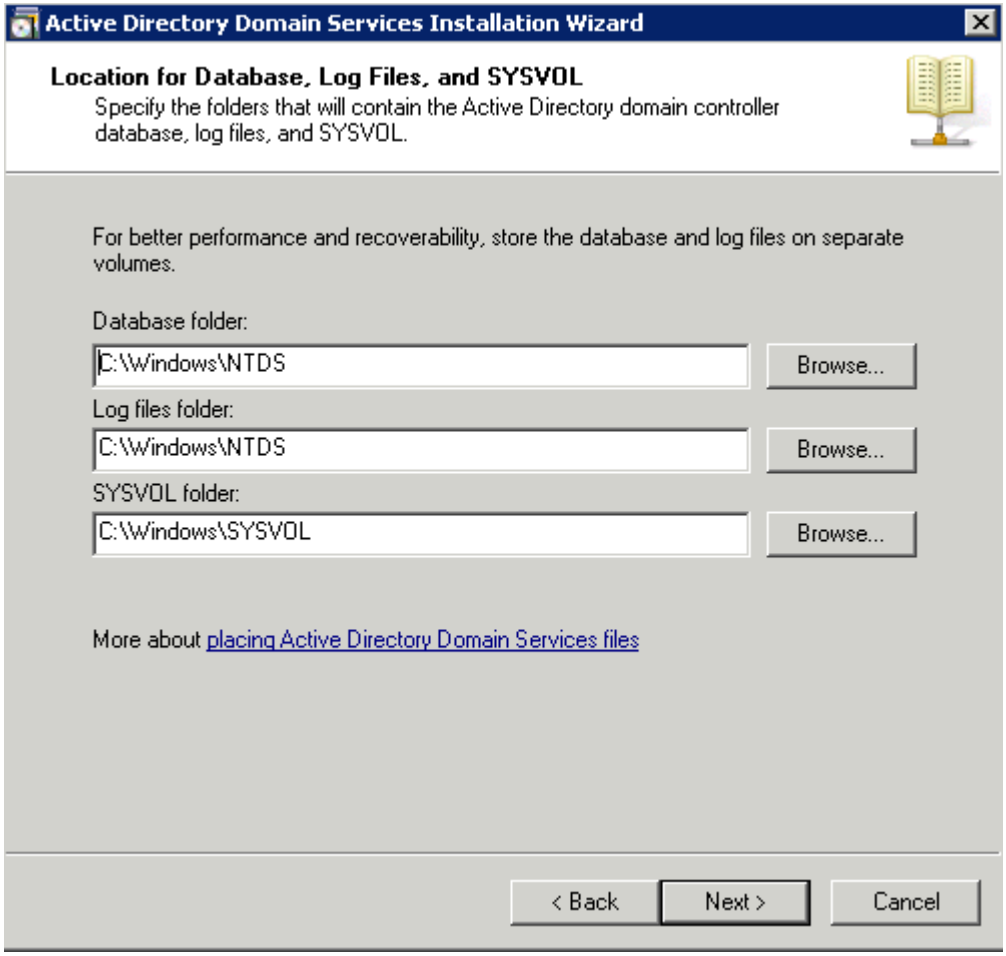
14. 确保已选择DNS服务器，然后单击Next。



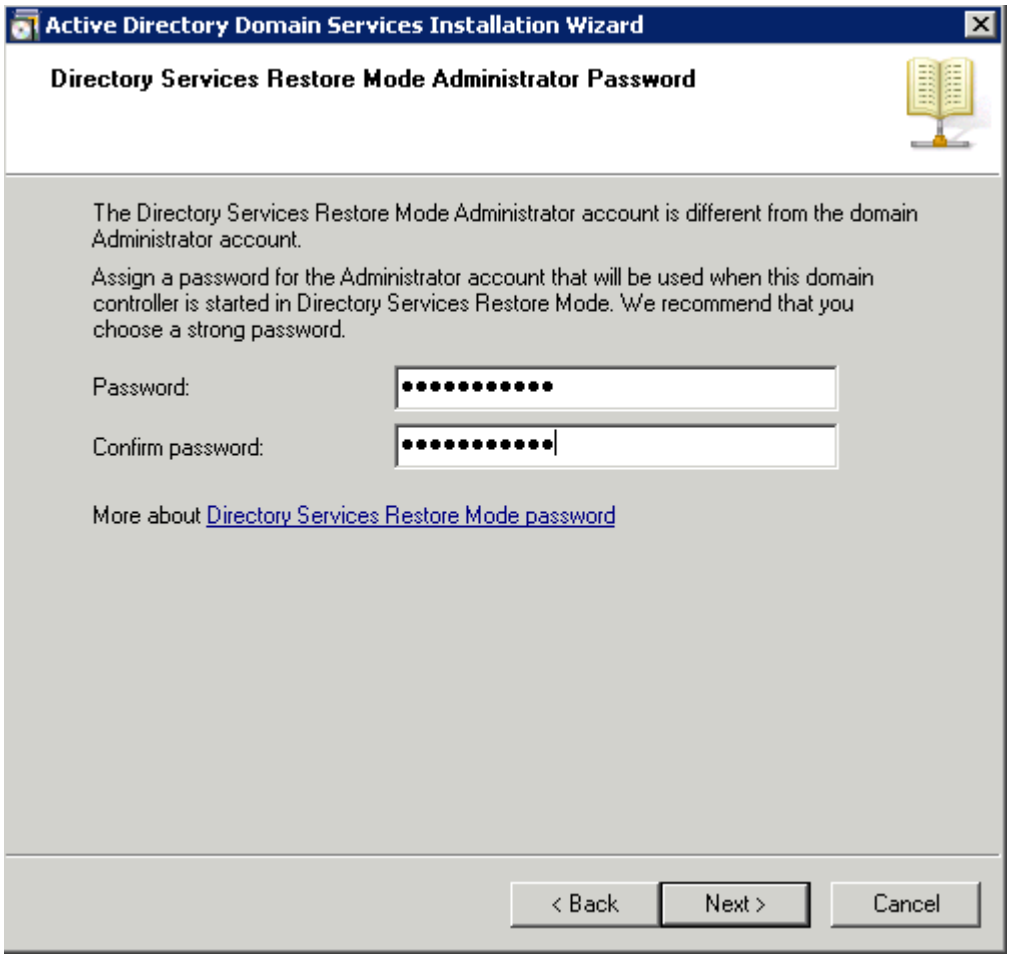
15. 单击Yes，安装向导将在DNS中为域创建新区域。



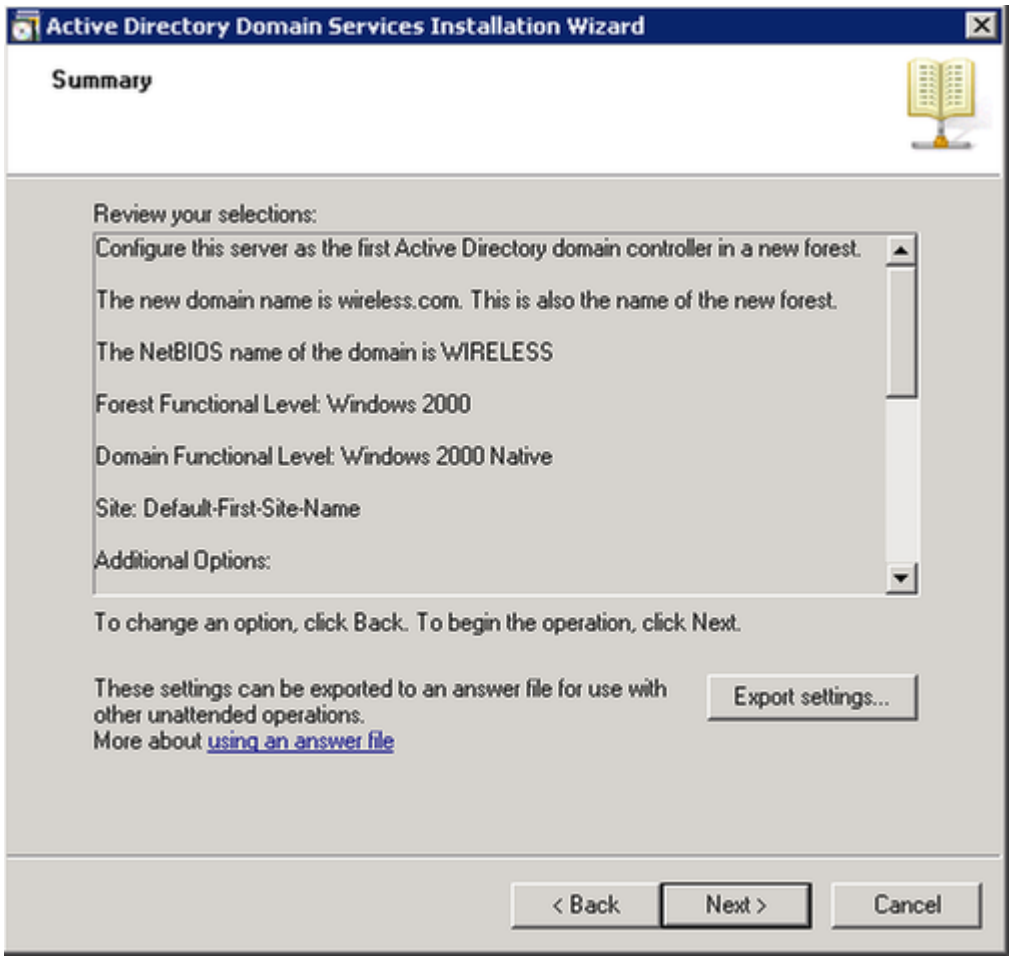
16. 选择Active Directory必须用于其文件的文件夹，然后单击下一步。



17. 输入管理员密码，然后单击下一步。

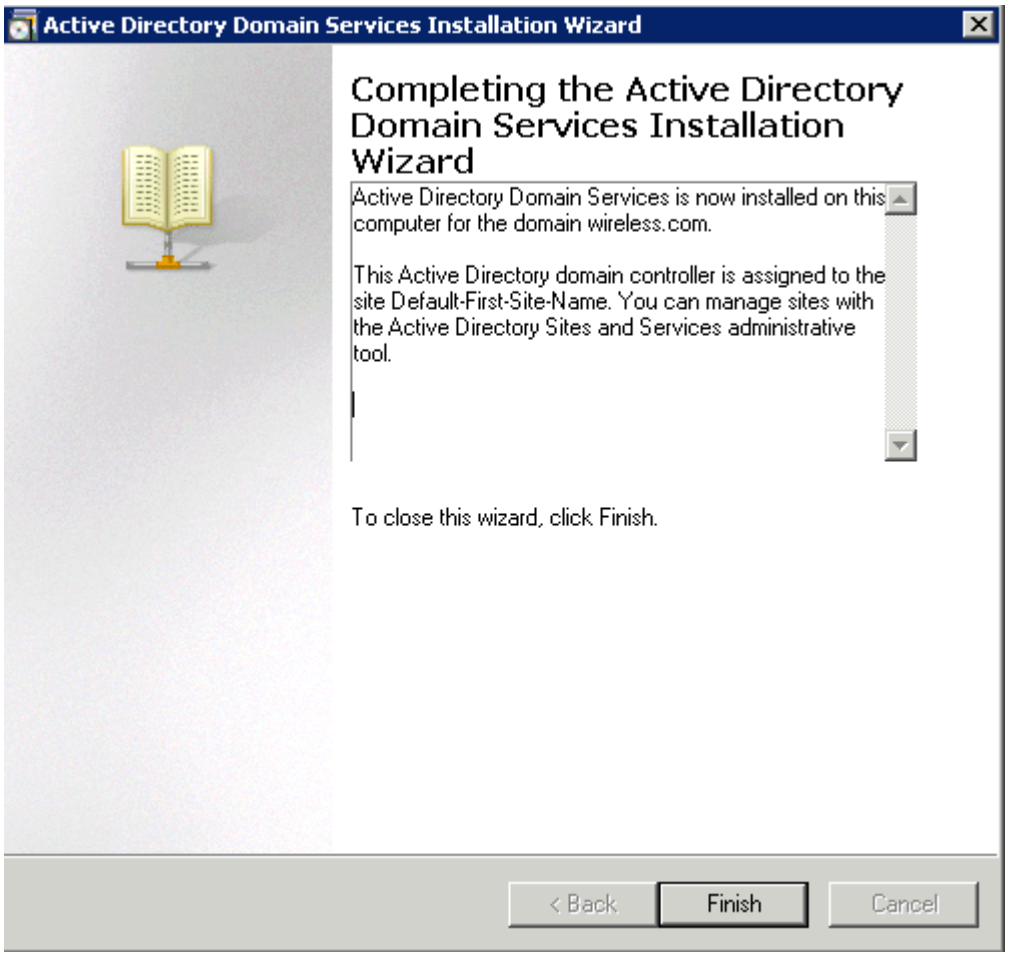


18. 检查您的选择，然后单击下一步。

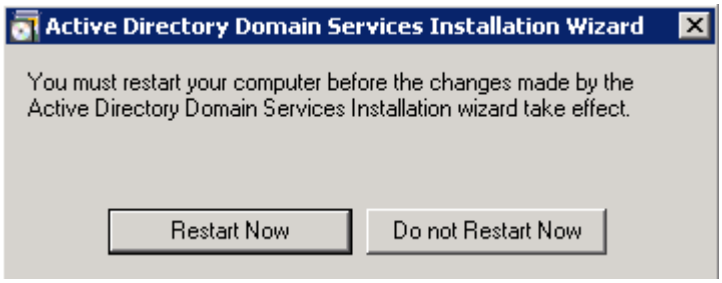


安装继续进行。

19. 单击完成关闭向导。



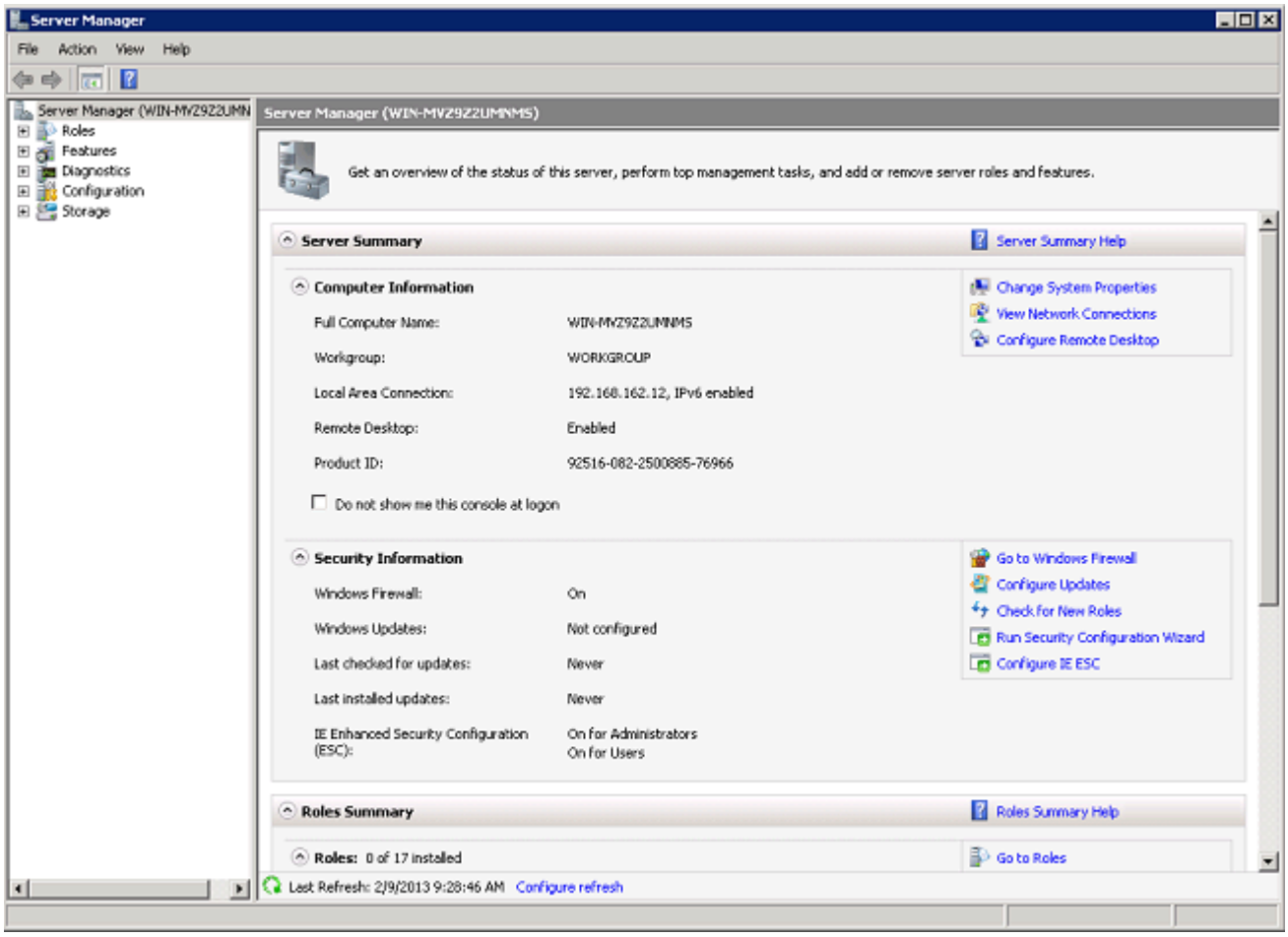
20. 重新启动服务器，使更改生效。



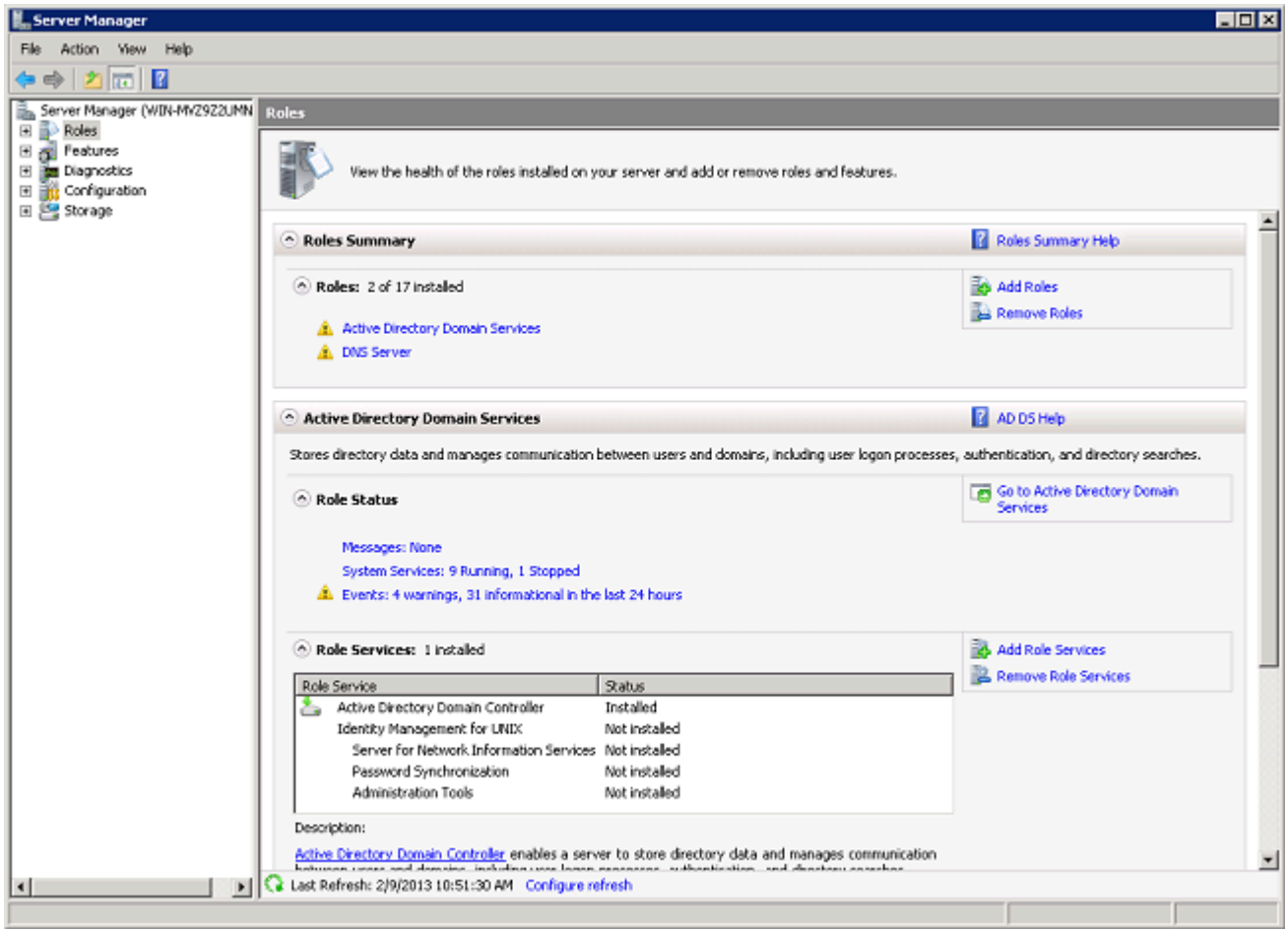
在 Microsoft Windows 2008 Server 上安装和配置 DHCP 服务

Microsoft 2008 Server 上的 DHCP 服务用于向无线客户端提供 IP 地址。要安装和配置DHCP服务，请完成以下步骤：

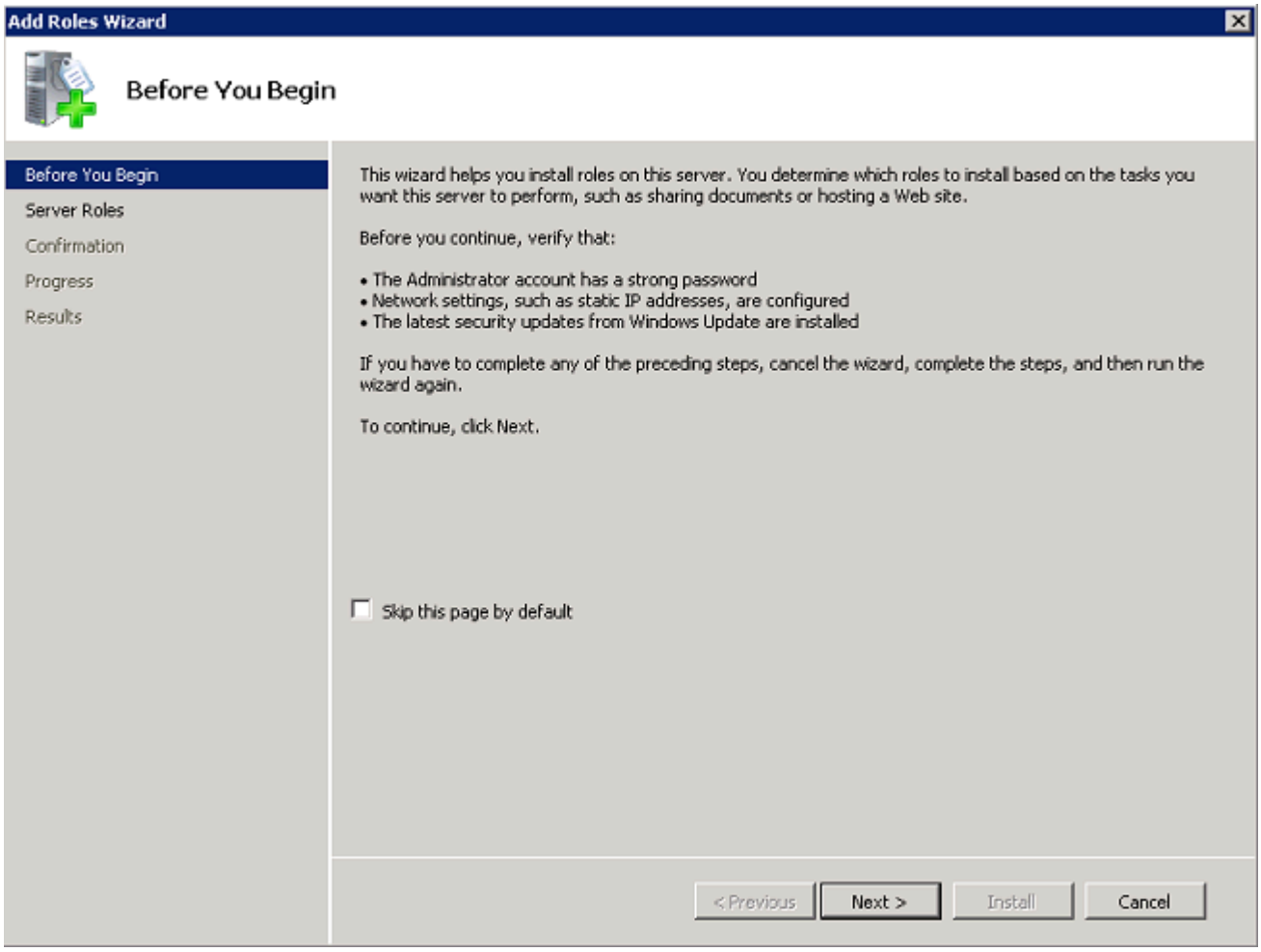
1. 单击开始>服务器管理器。



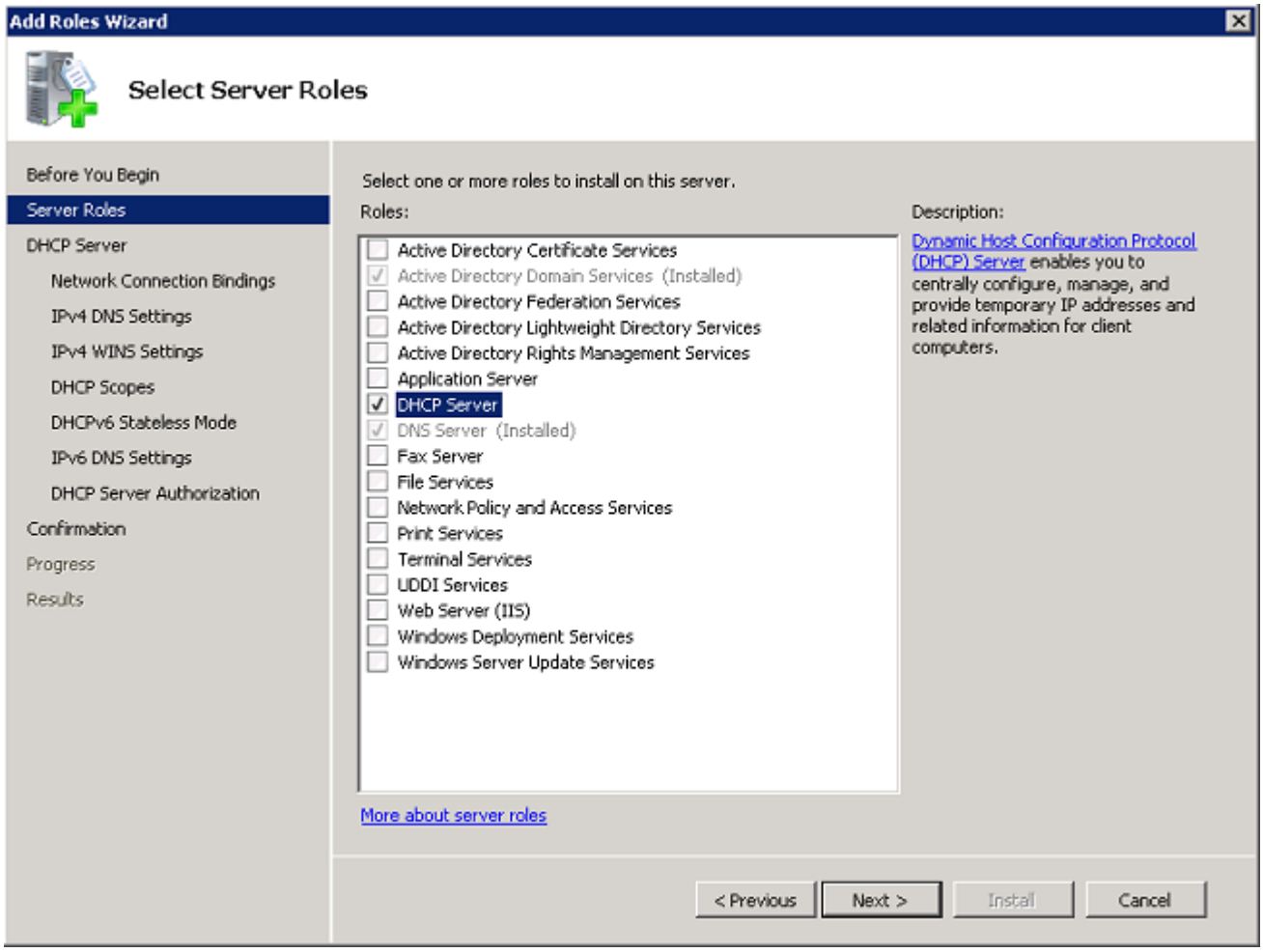
2. 单击Roles> Add Roles。


Server Manager
File Action View Help
Server Manager (WIN-MVZ9Z2UMN
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 2 of 17 installed
Add Roles
Remove Roles
Active Directory Domain Services
DNS Server
Active Directory Domain Services
AD DS Help
Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.
Role Status
Go to Active Directory Domain Services
Messages: None
System Services: 9 Running, 1 Stopped
Events: 4 warnings, 31 informational in the last 24 hours
Role Services: 1 installed
Add Role Services
Remove Role Services
Role Service
Status
Active Directory Domain Controller
Installed
Identity Management for UNIX
Not installed
Server for Network Information Services
Not installed
Password Synchronization
Not installed
Administration Tools
Not installed
Description:
Active Directory Domain Controller enables a server to store directory data and manages communication
Last Refresh: 2/9/2013 10:51:30 AM
Configure refresh

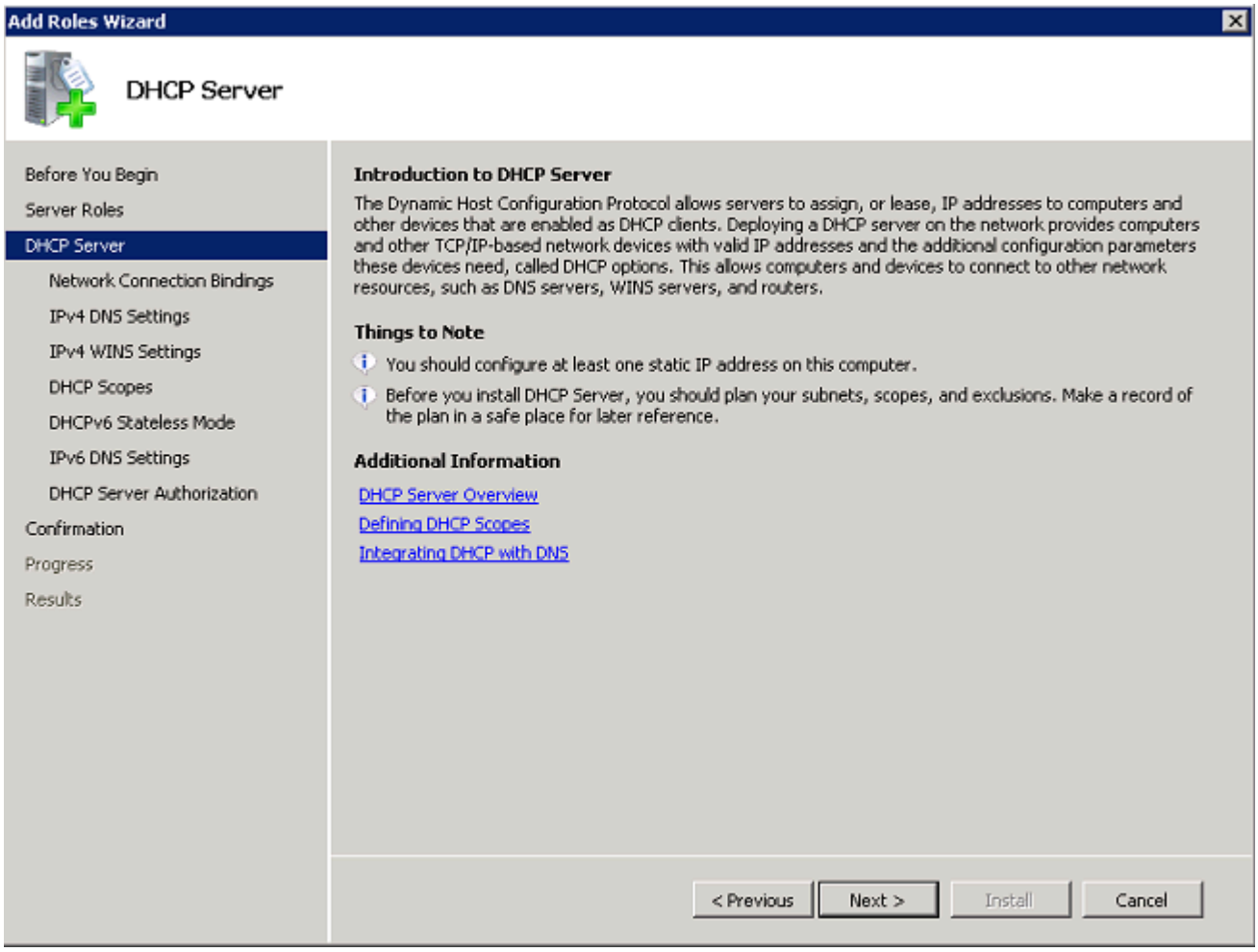
3. 单击 Next。



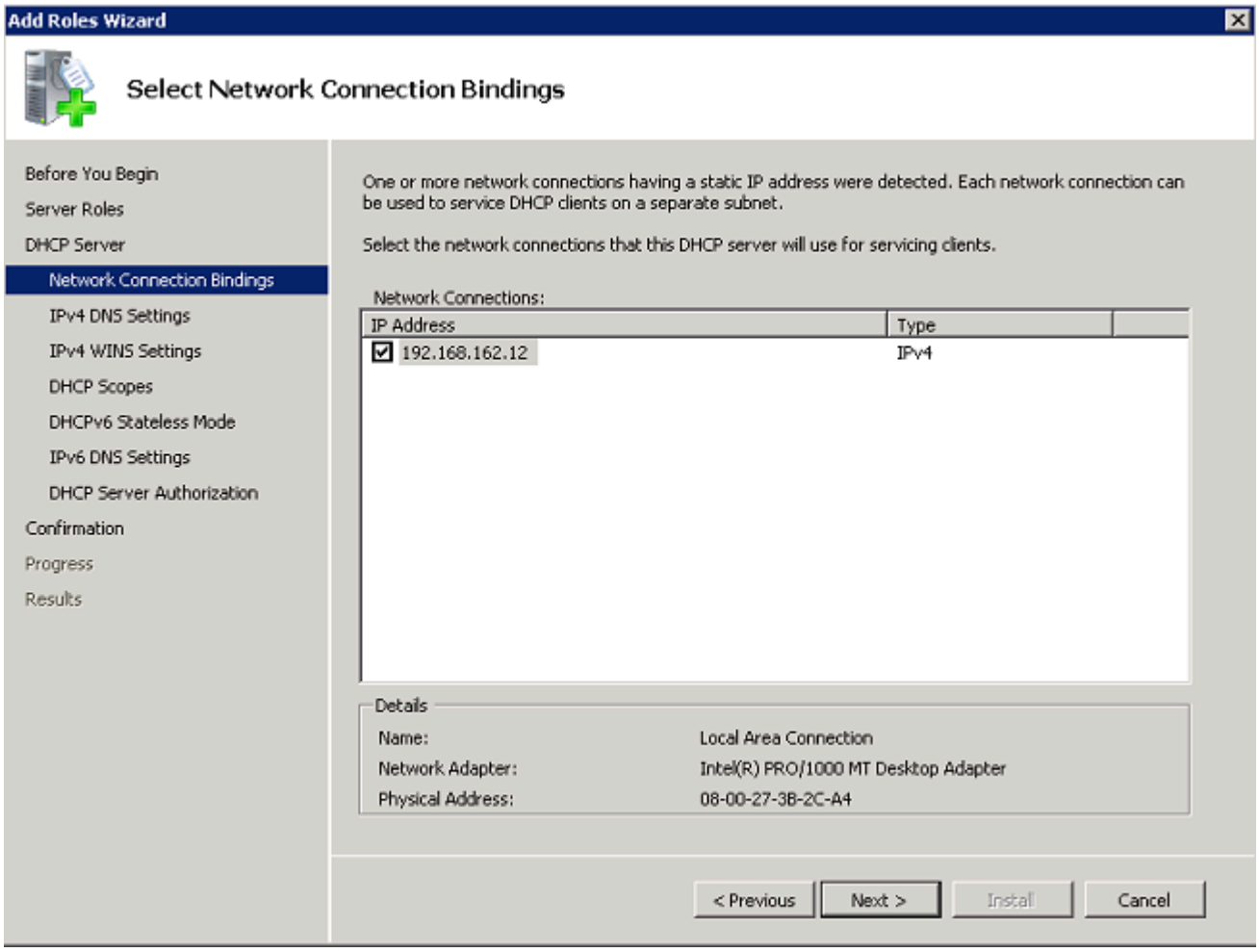
4. 选择服务DHCP Server，然后单击Next。



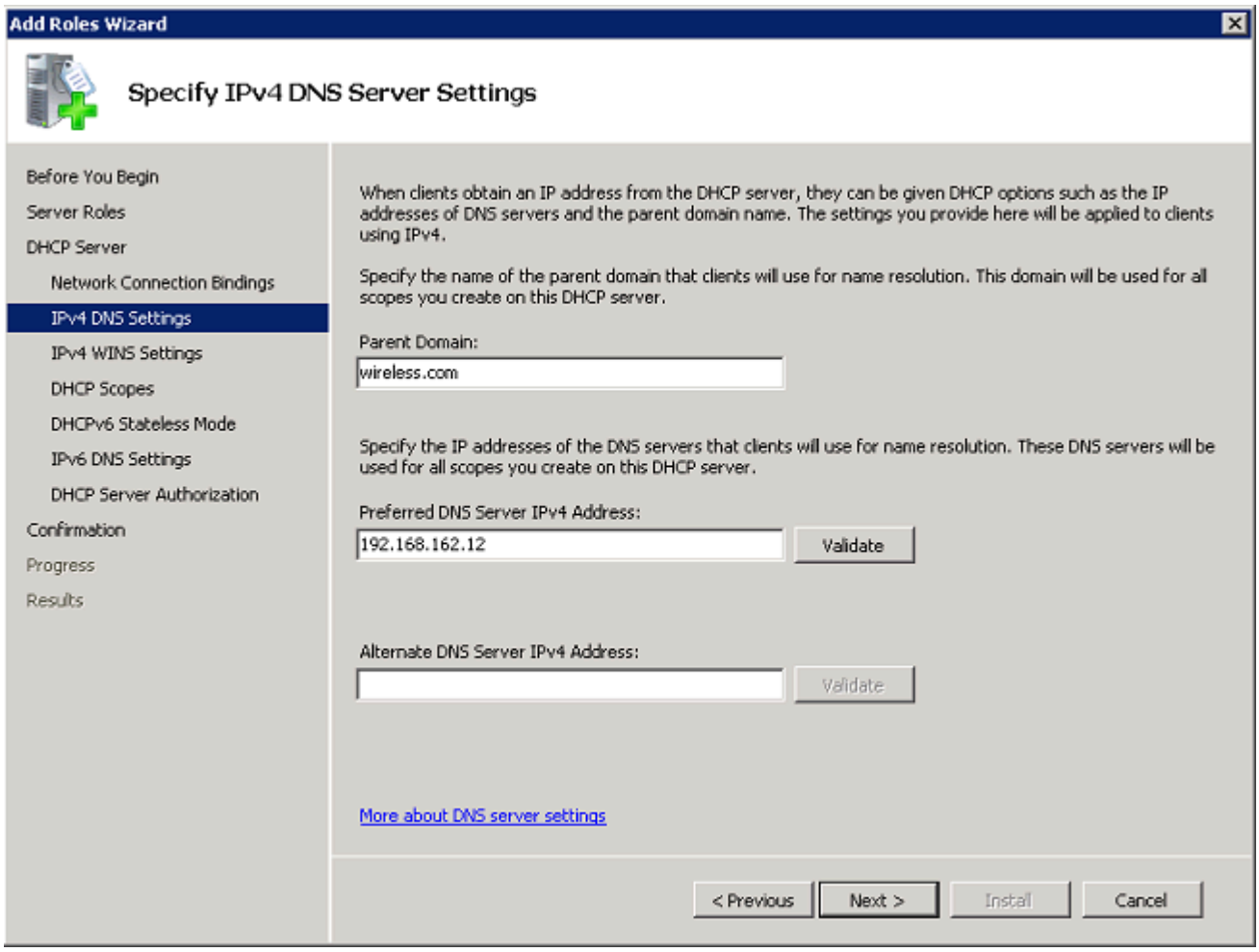
5. 查看DHCP服务器简介，然后单击下一步。



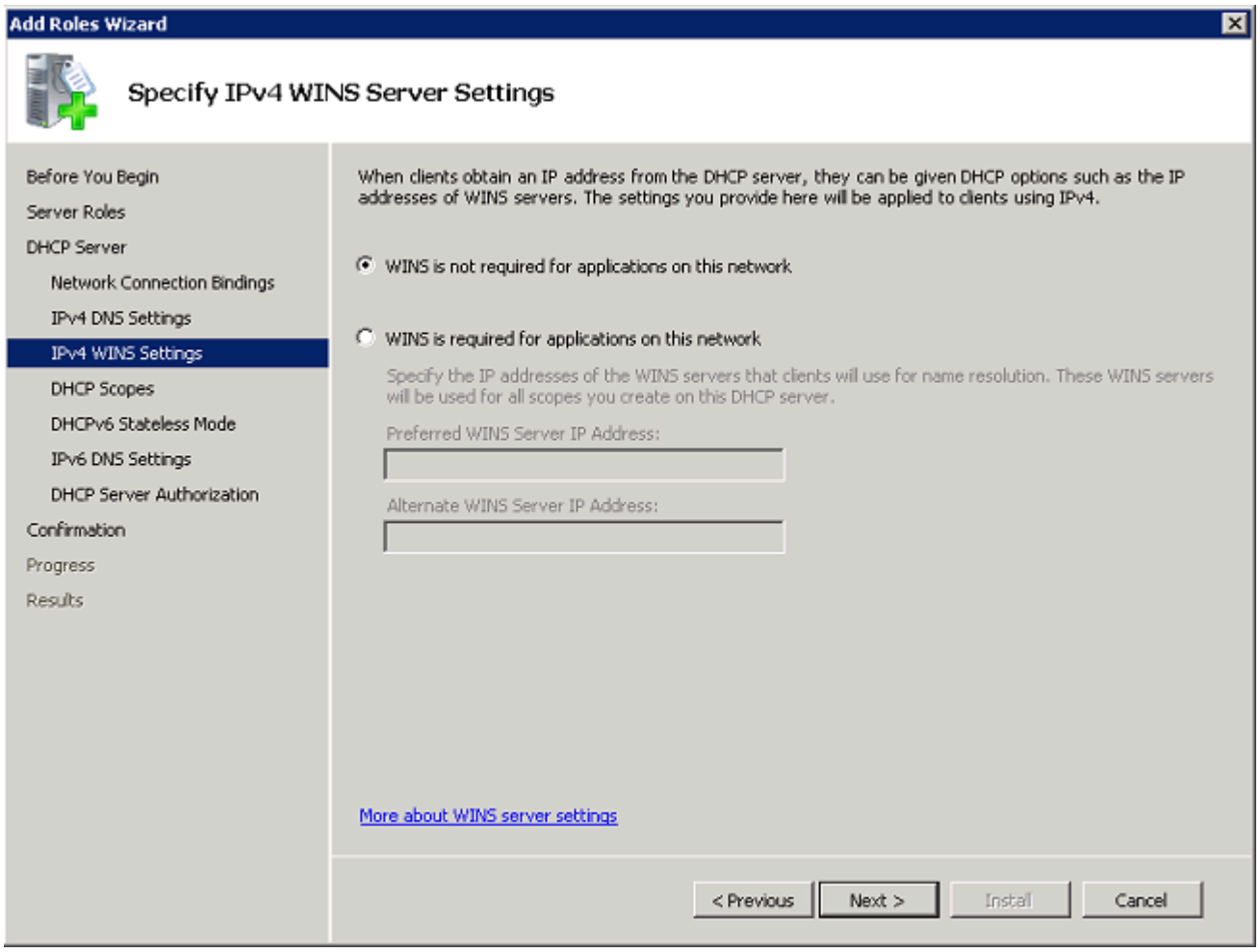
6. 选择DHCP服务器必须为请求监控的接口，然后单击Next。



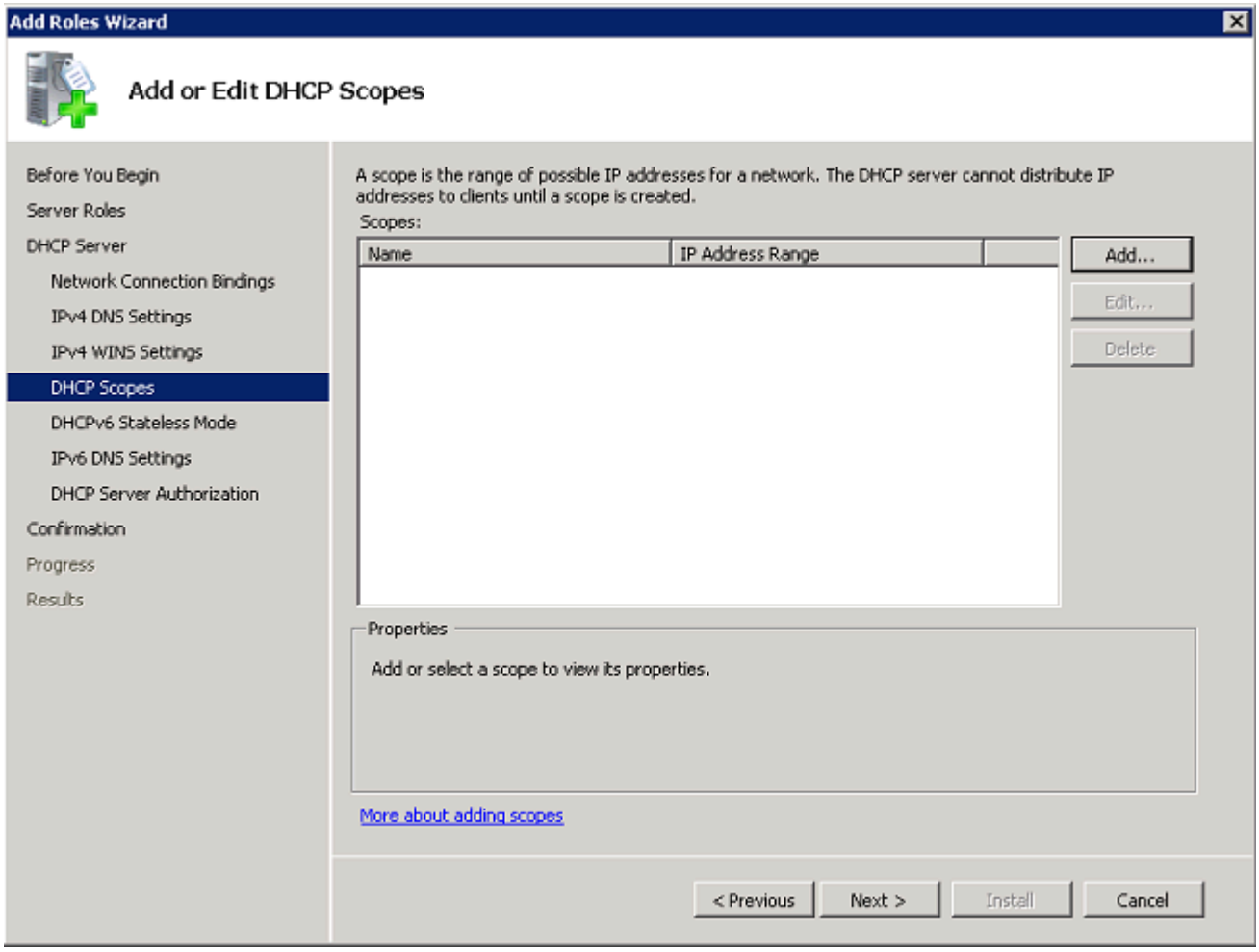
7. 配置DHCP服务器必须提供给客户端的默认DNS设置，然后单击Next。



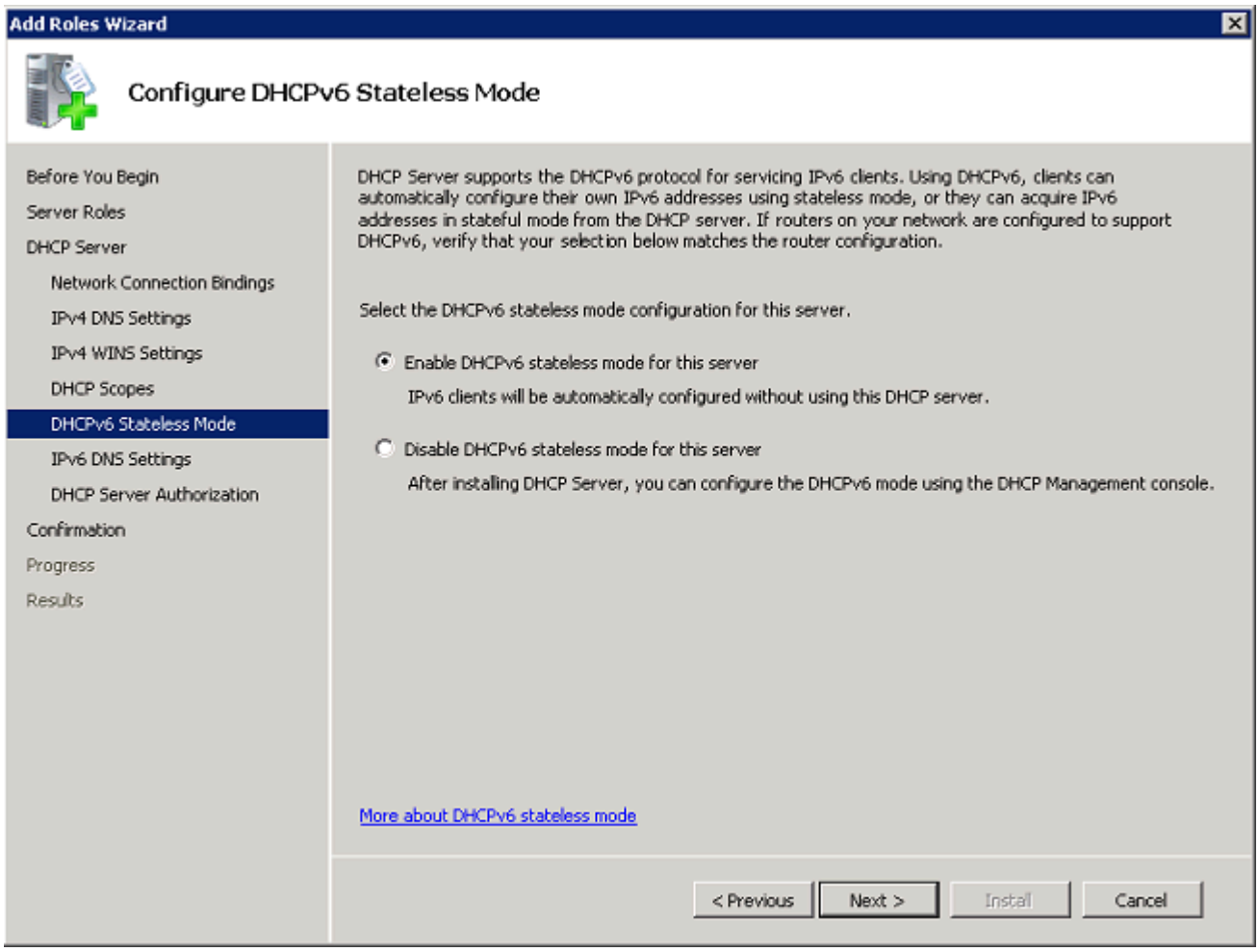
8. 如果网络支持WINS，则配置WINS。



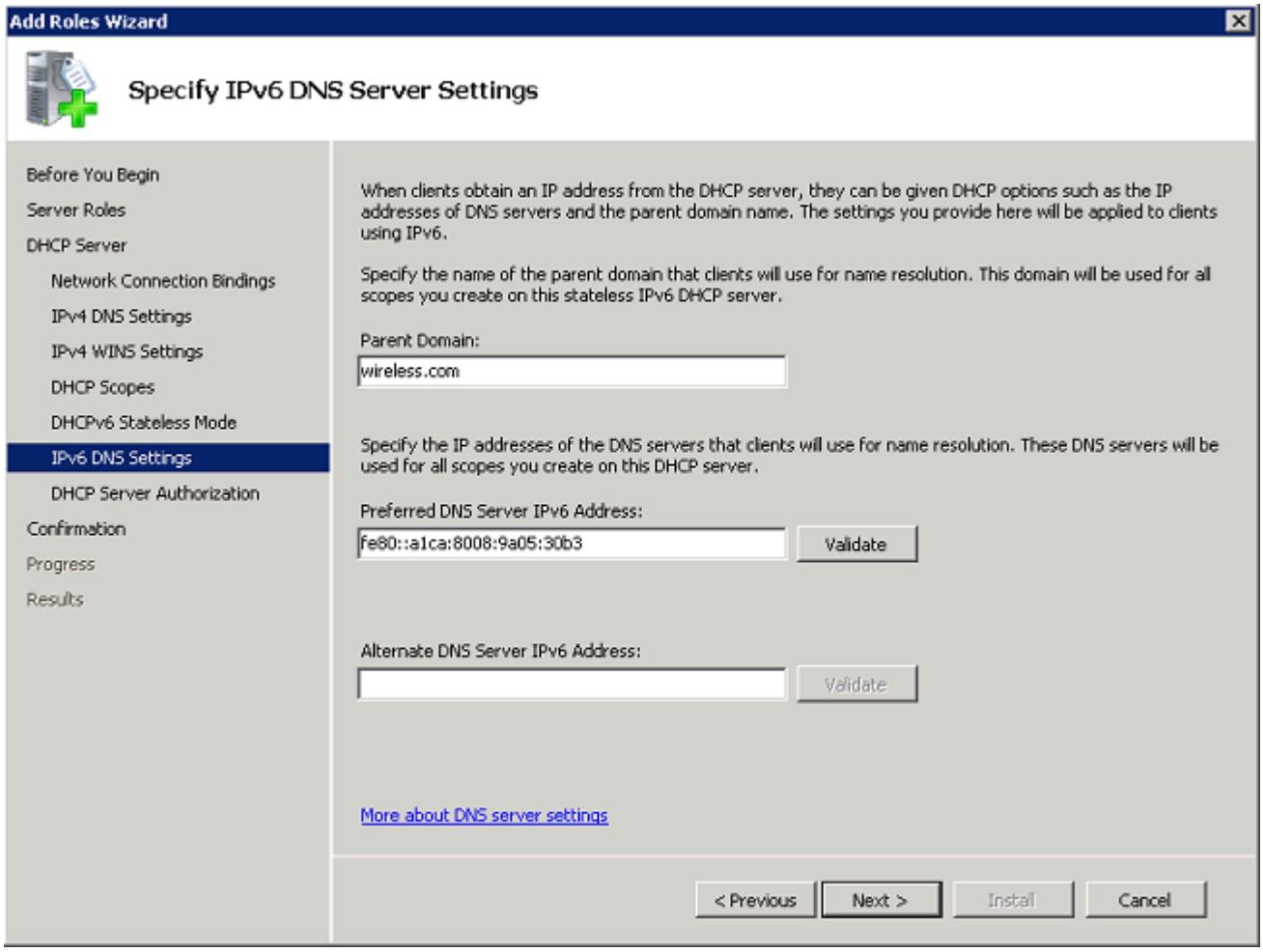
9. 单击Add以使用向导创建DHCP作用域，或单击Next稍后创建DHCP作用域。点击下一步继续。



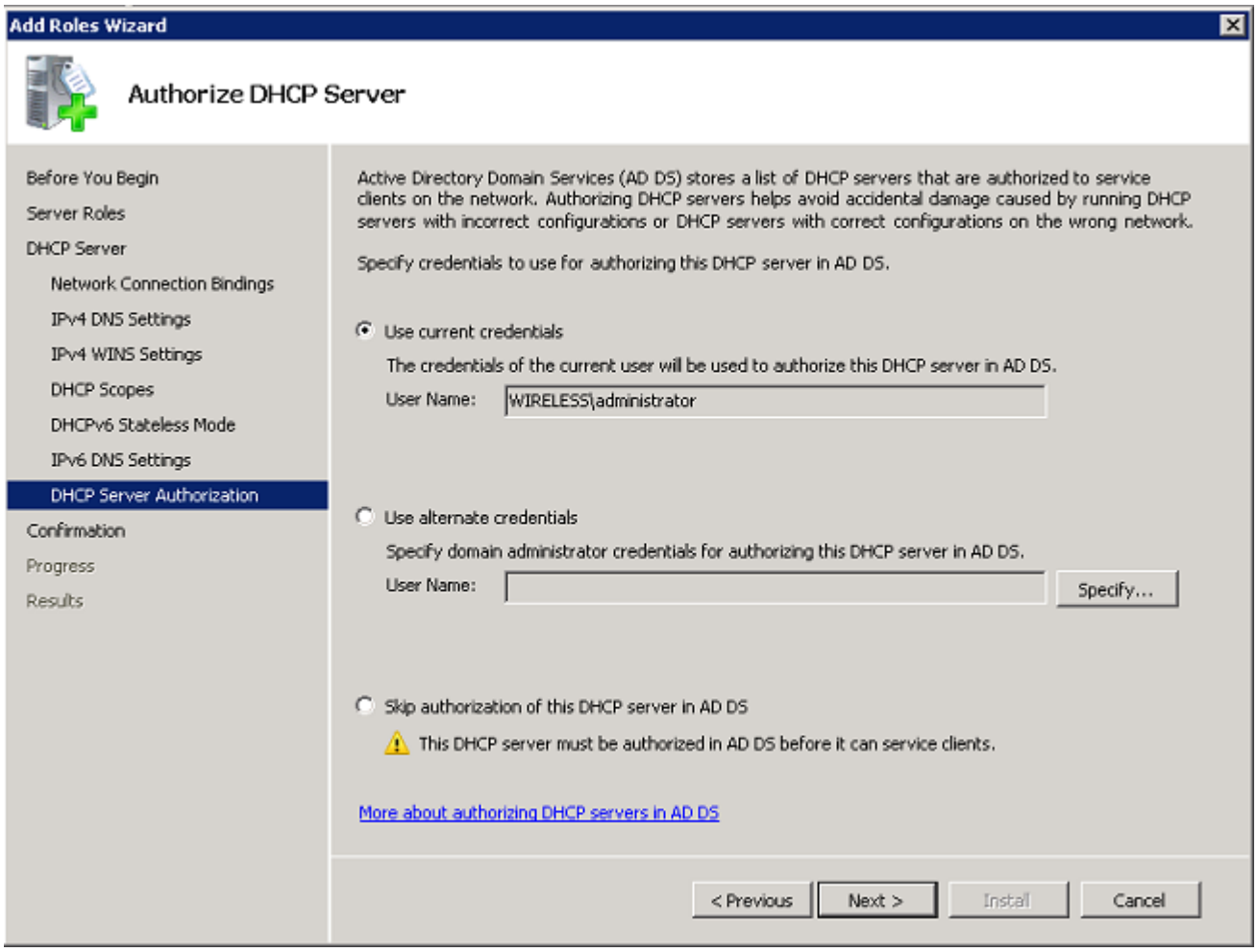
10. 在服务器上启用或禁用DHCPv6支持，然后单击Next。



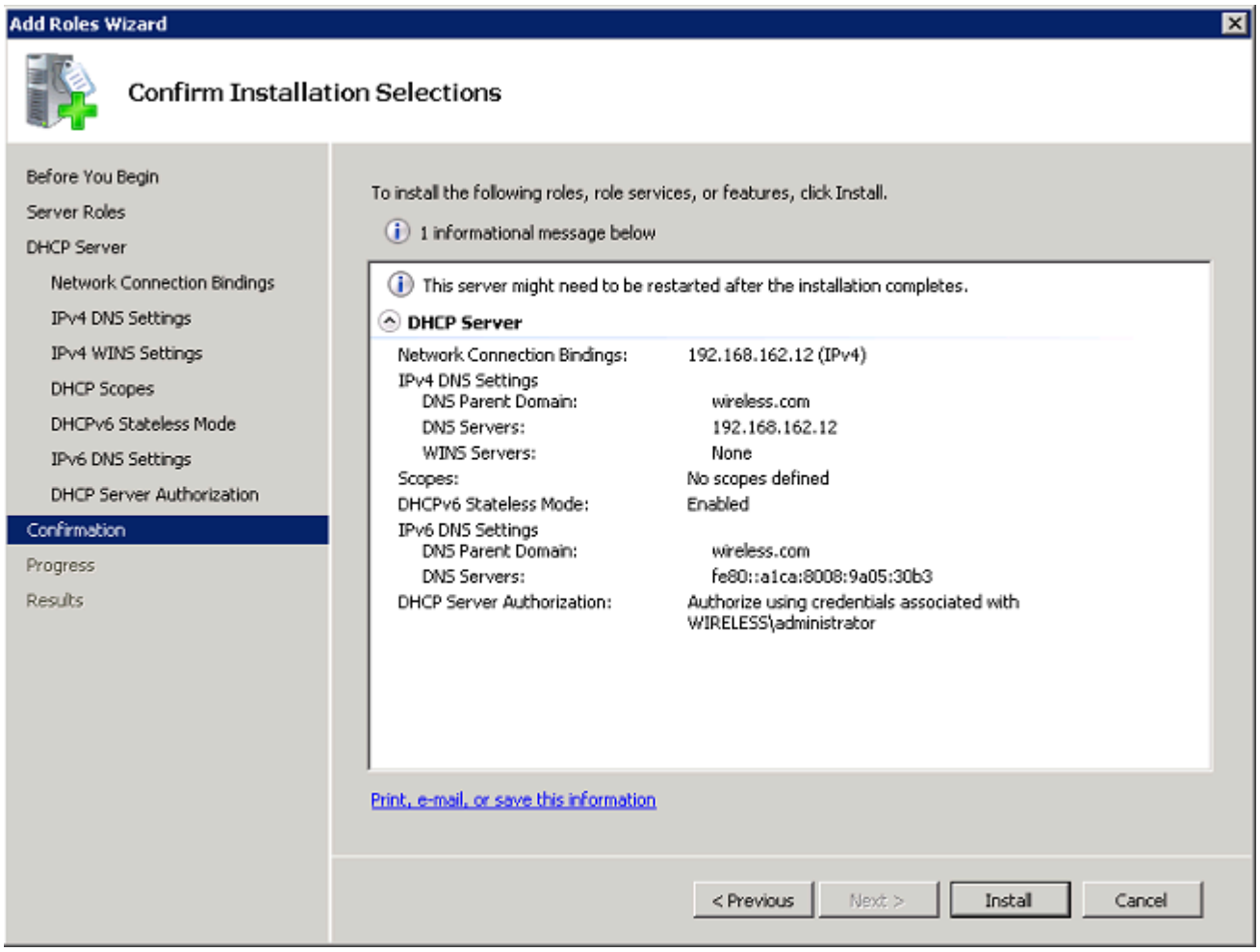
11. 如果上一步中启用了DHCPv6，请配置IPv6 DNS设置。点击下一步继续。



12. 提供域管理员凭据以授权Active Directory中的DHCP服务器，然后单击Next。

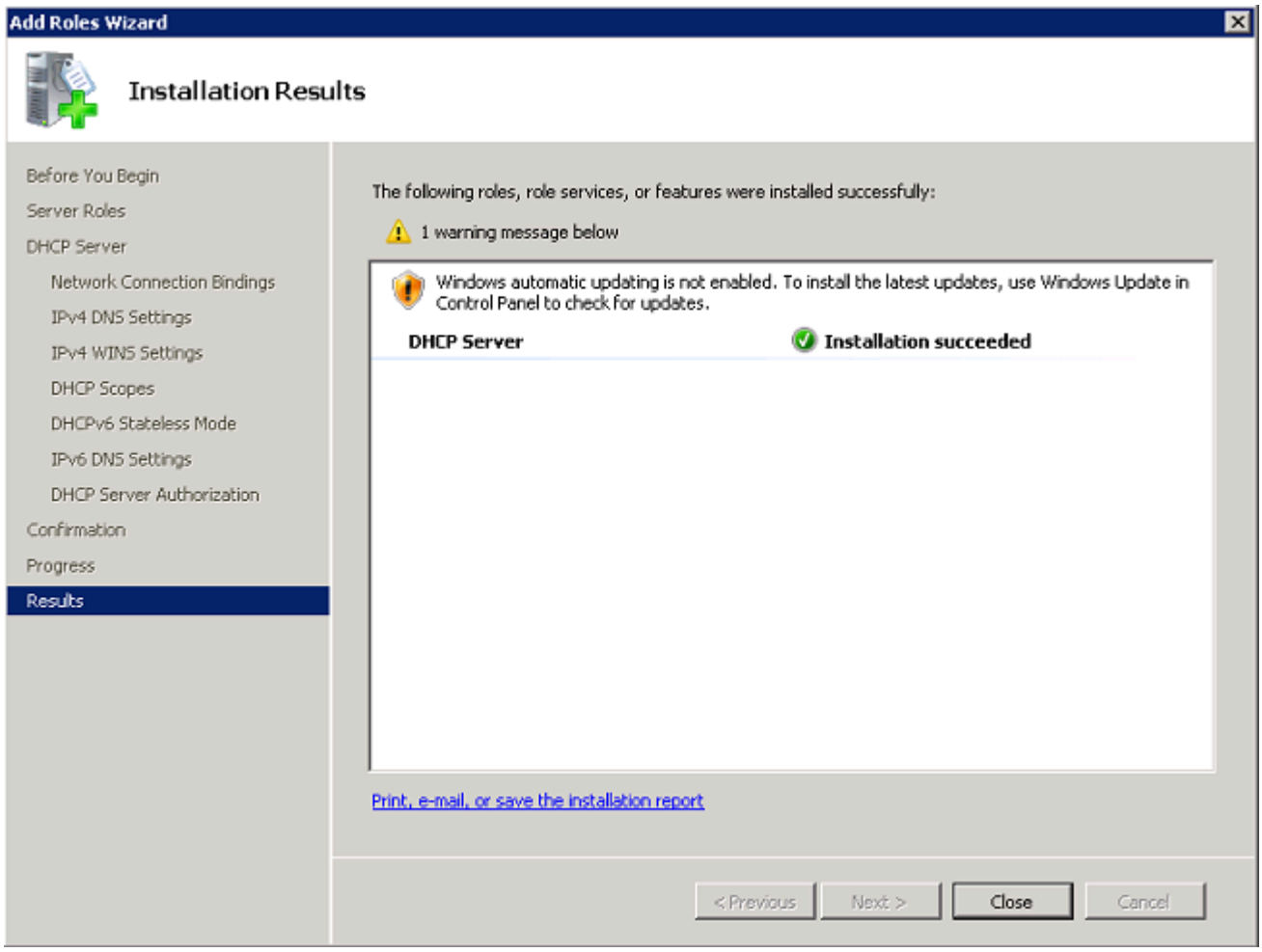


13. 查看确认页面上的配置，然后单击安装完成安装。



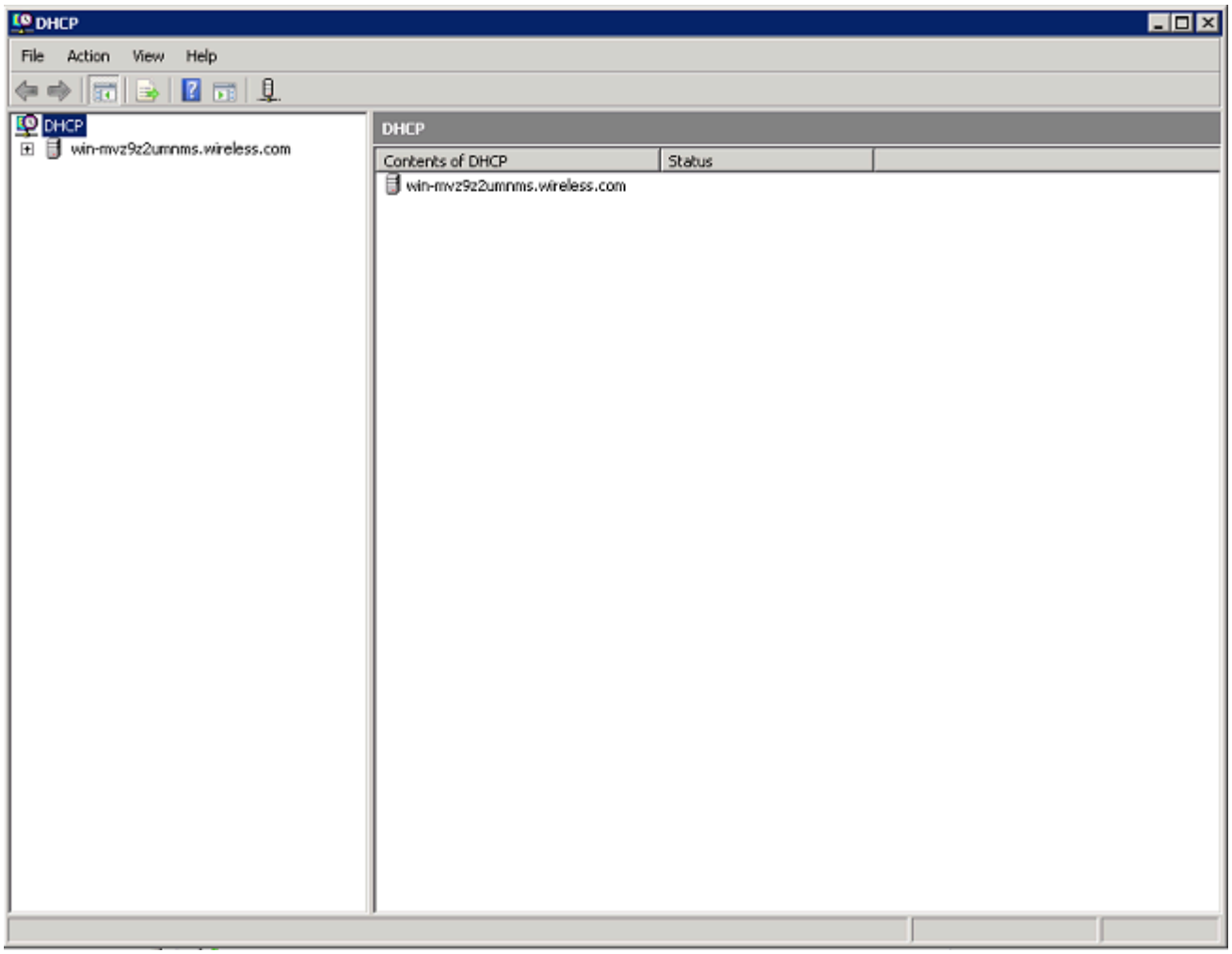
安装继续进行。

14. 单击Close关闭向导。

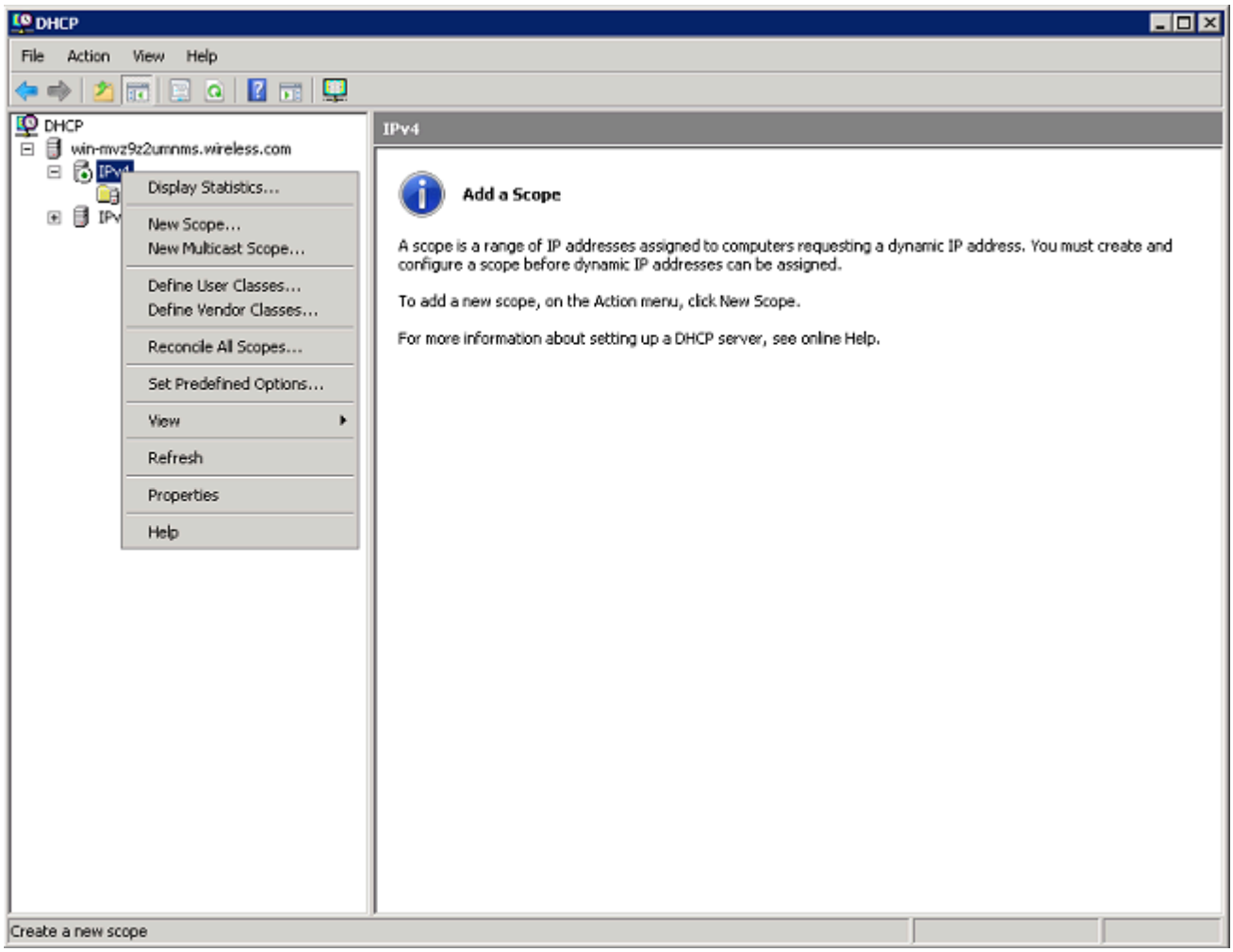


DHCP服务器现已安装。

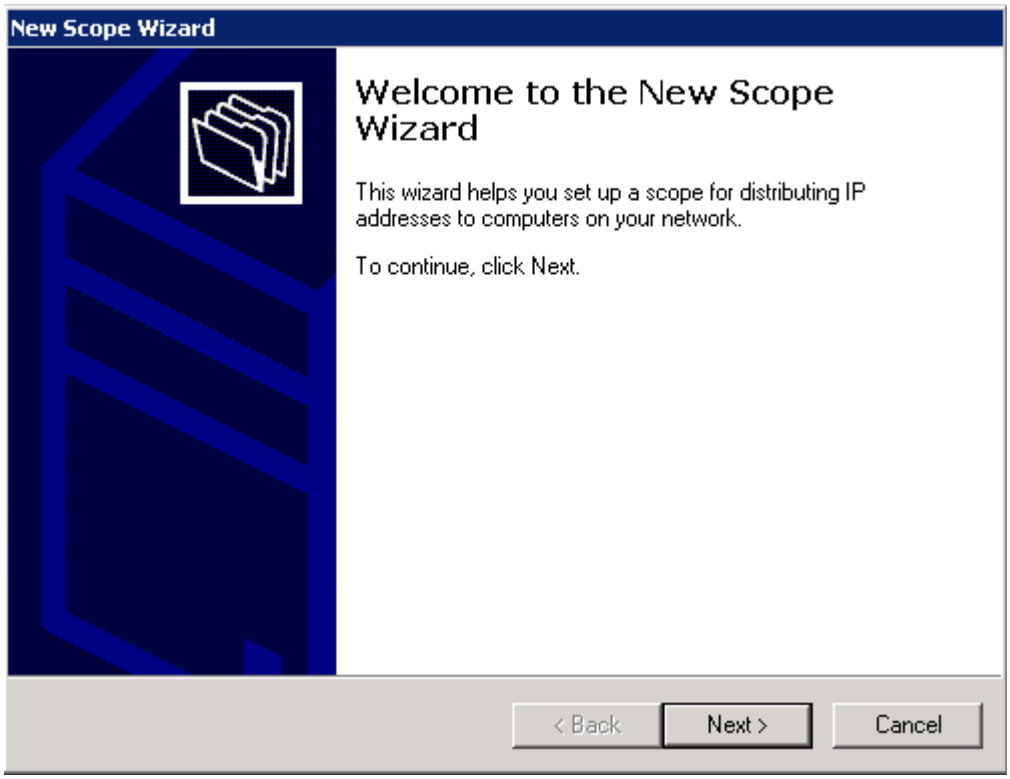
15. 单击开始>管理工具 > DHCP以配置DHCP服务。



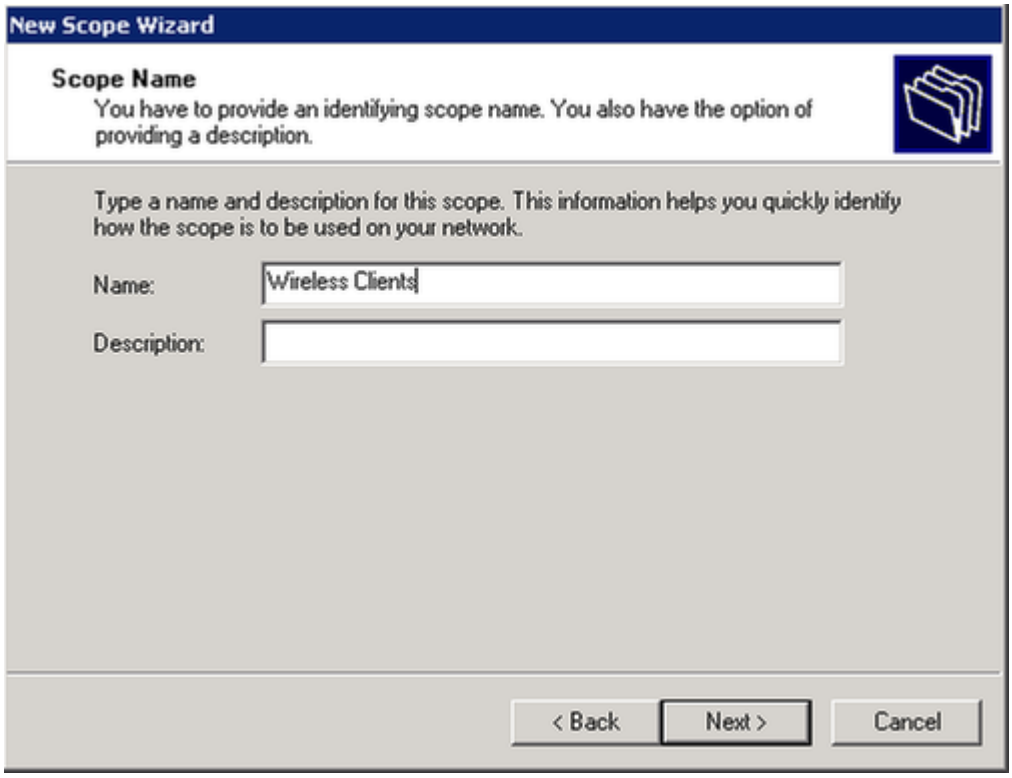
16. 展开DHCP服务器（如本示例的前一映像所示），右键单击IPv4，然后选择New Scope以创建DHCP范围。



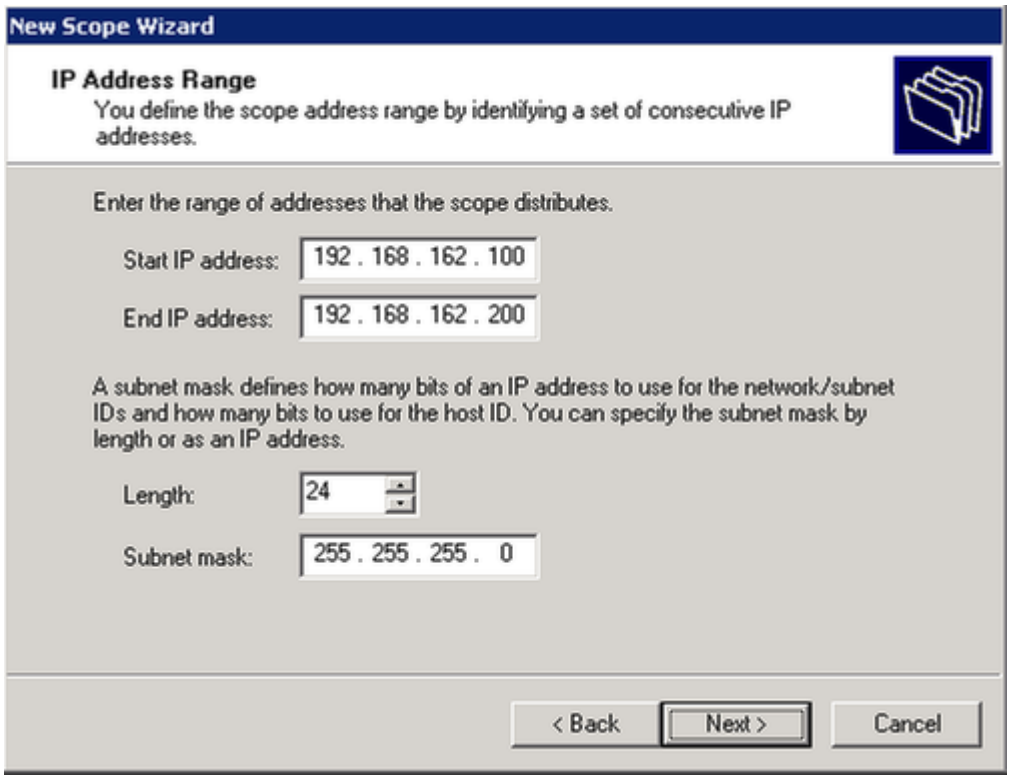
17. 单击下一步，通过“新建作用域向导”配置新作用域。



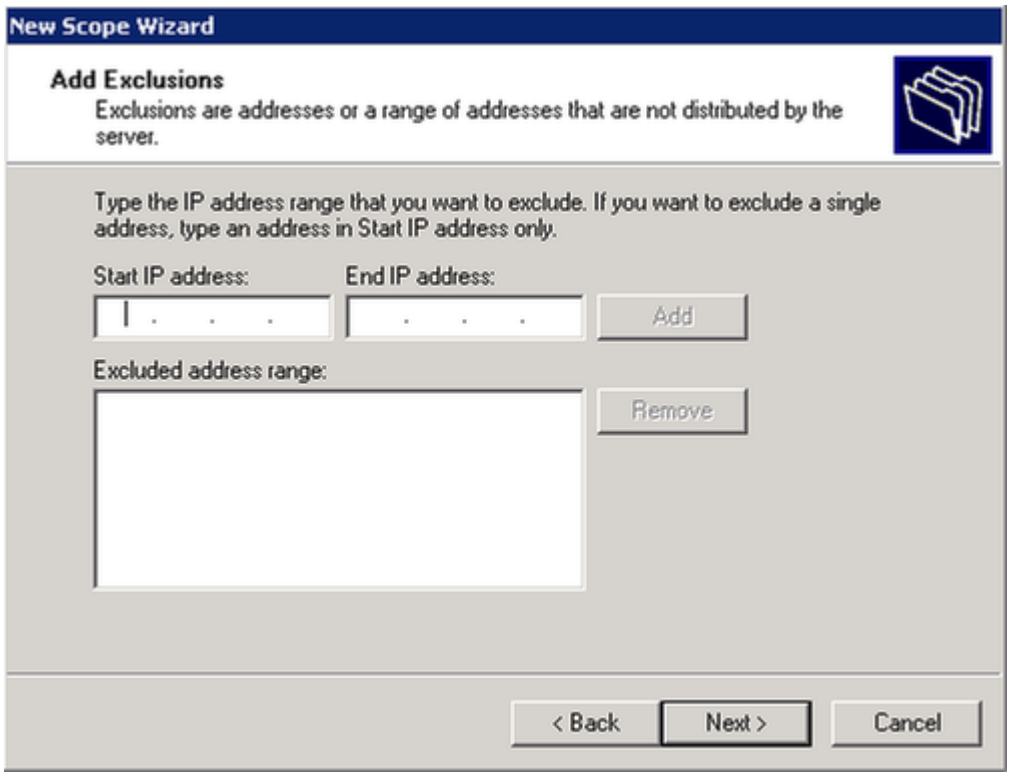
18. 为新作用域提供名称（本示例中为Wireless Clients），然后单击Next。



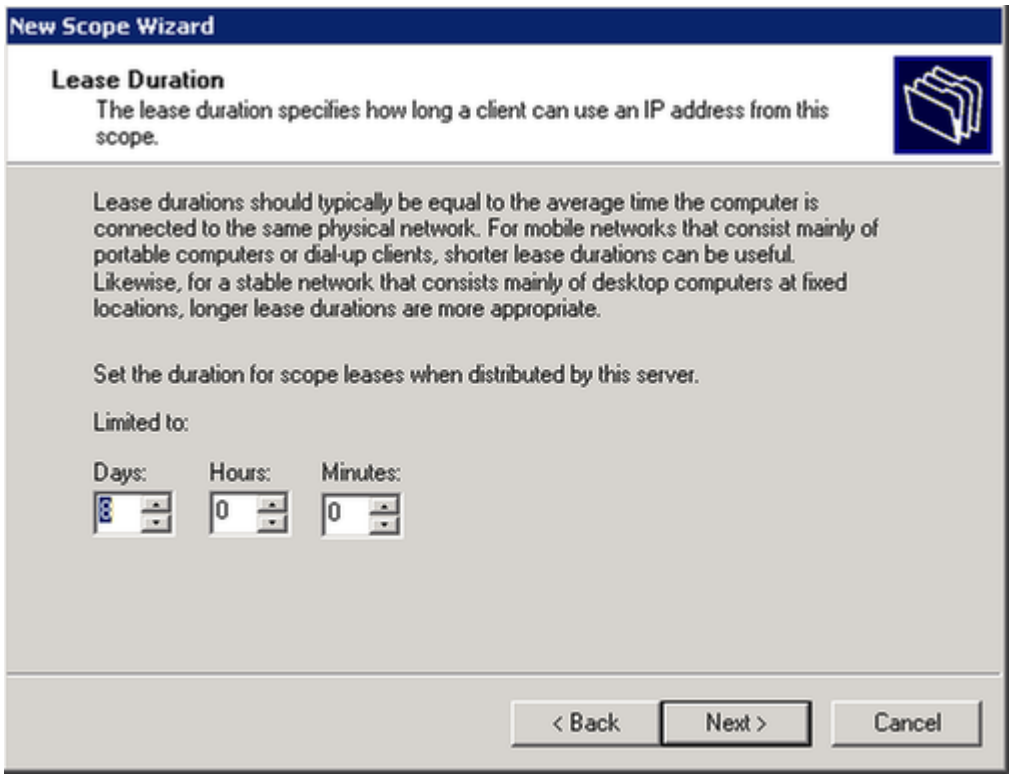
19. 输入可用于DHCP租用的IP地址范围。点击下一步继续。



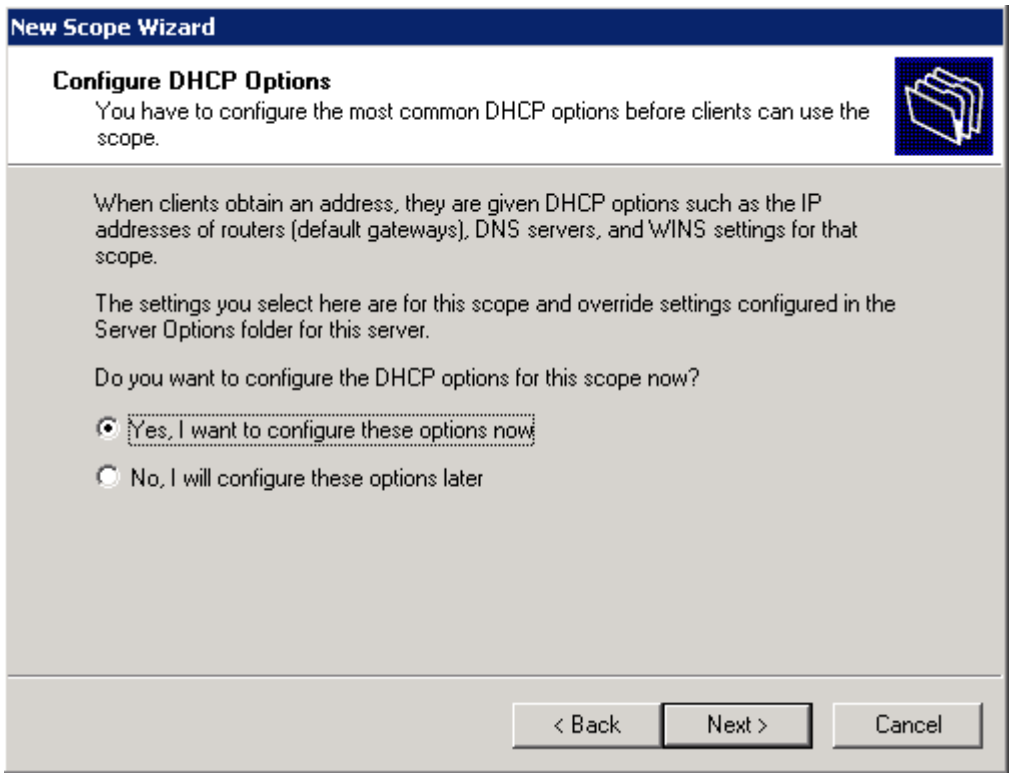
20. 创建排除地址的可选列表。点击下一步继续。



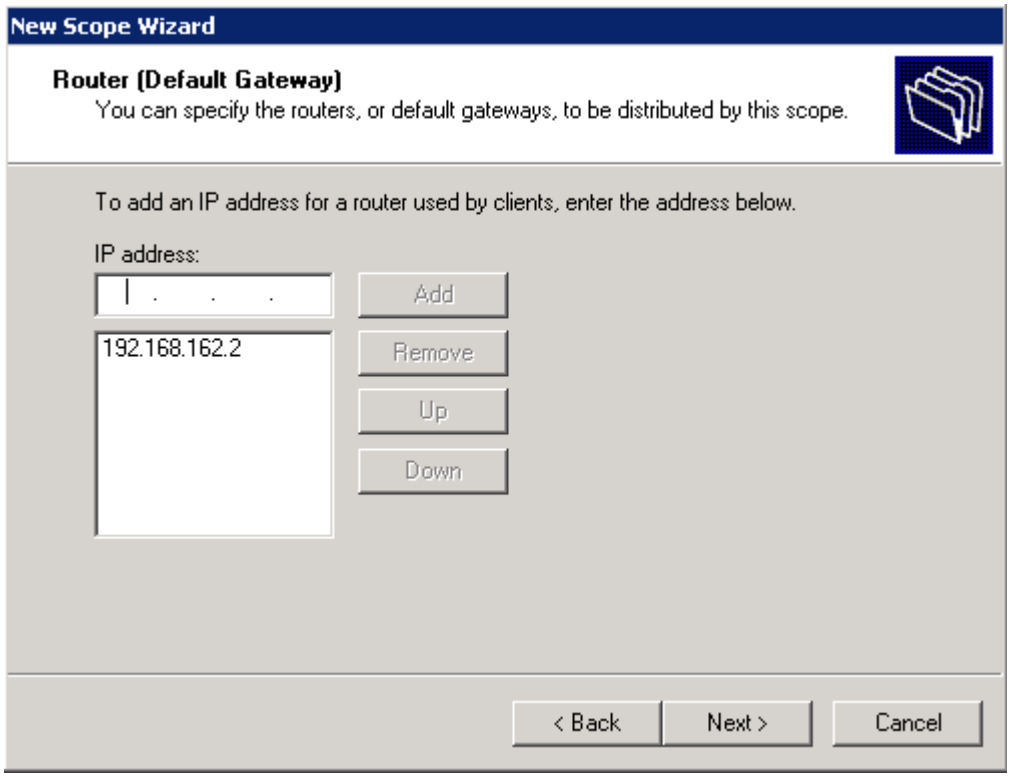
21. 配置租用时间，然后单击Next。



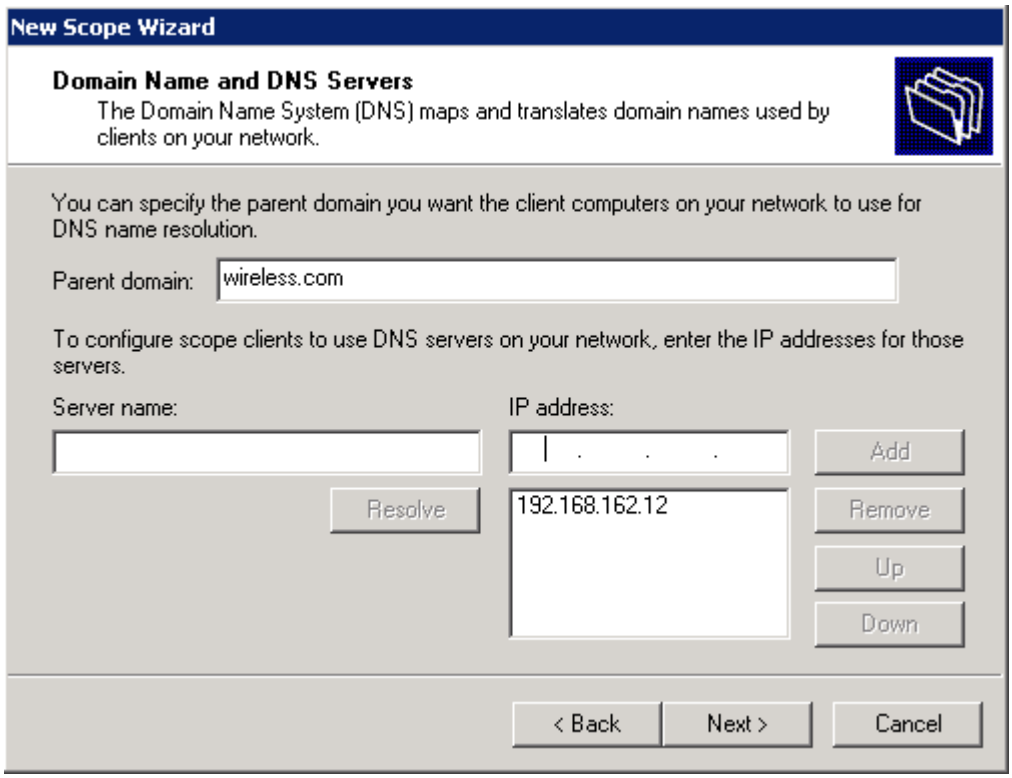
22. 单击Yes， I want to configure these options now，然后单击Next。



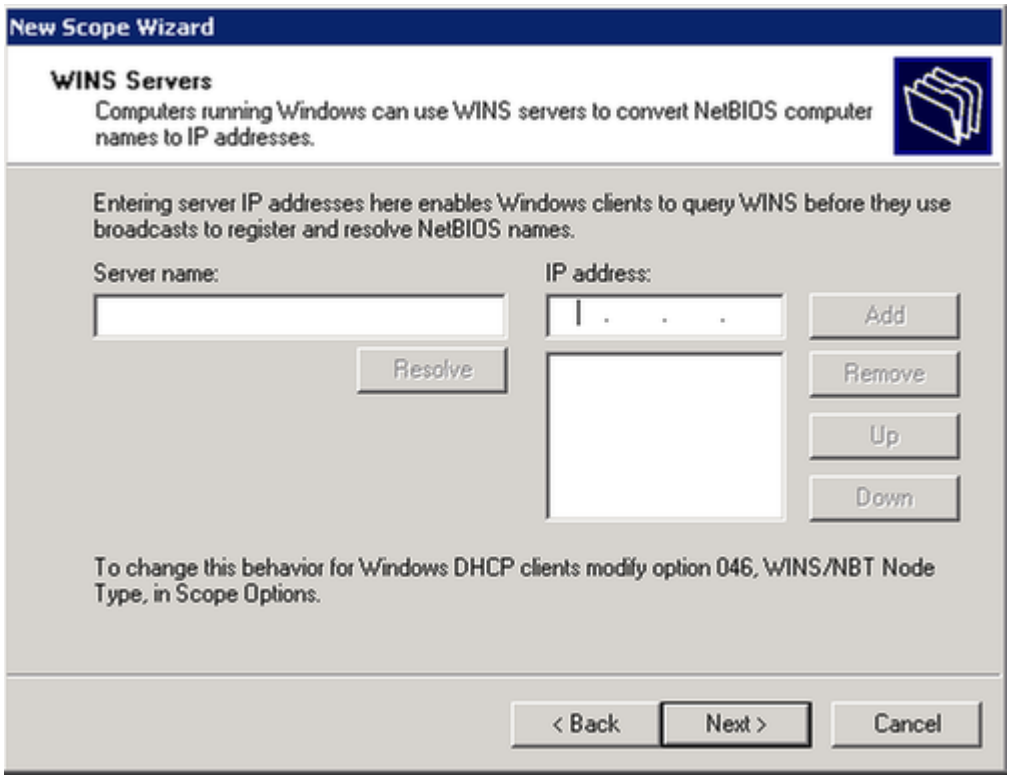
23. 输入此作用域的默认网关IP地址，单击Add > Next。



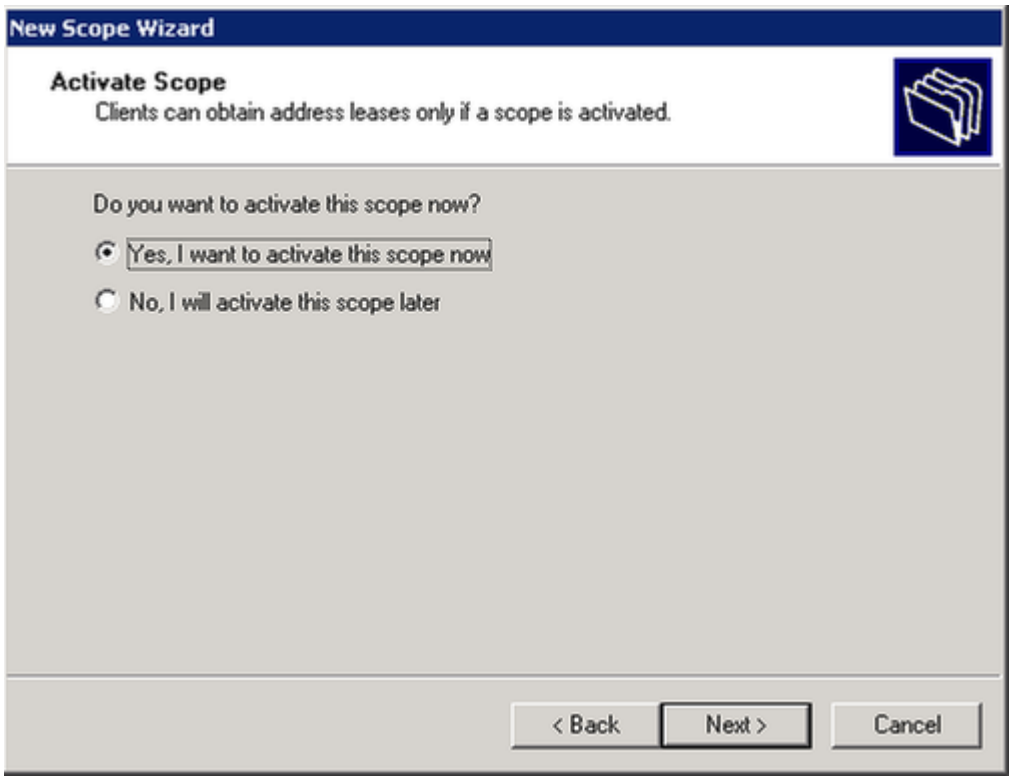
24. 配置客户端要使用的DNS域名和DNS服务器。点击下一步继续。



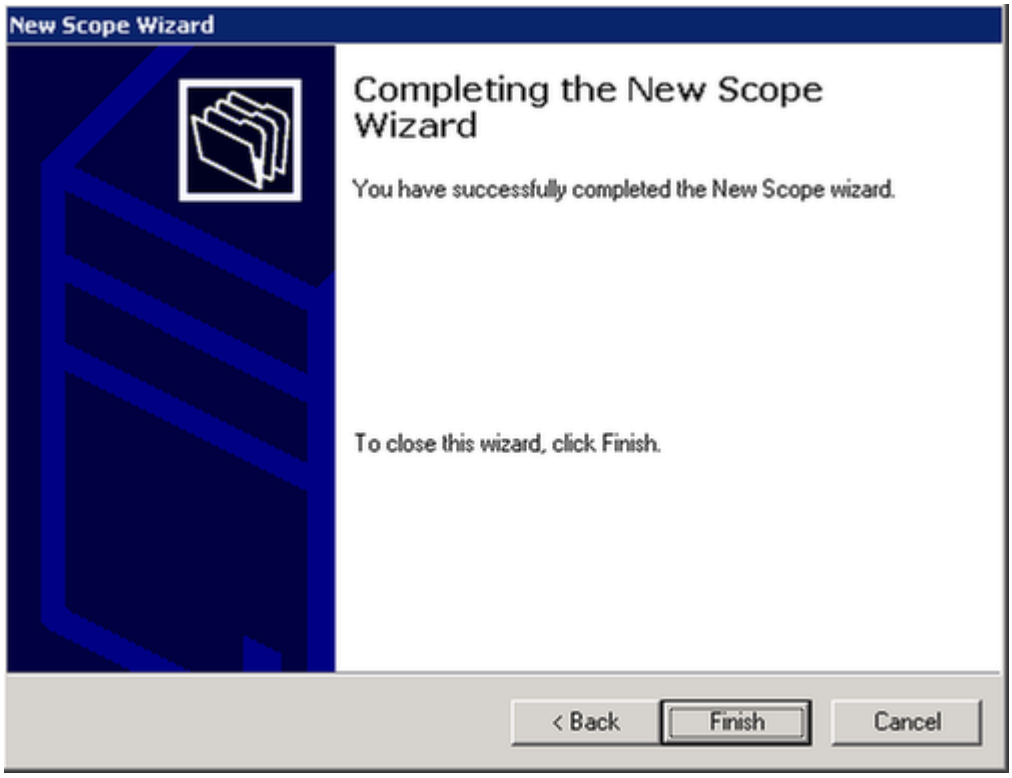
25. 如果网络支持WINS，请输入此作用域的WINS信息。点击下一步继续。



26. 要激活此作用域，请点击是，我要立即激活此作用域>下一步。



27. 单击Finish完成并关闭向导。



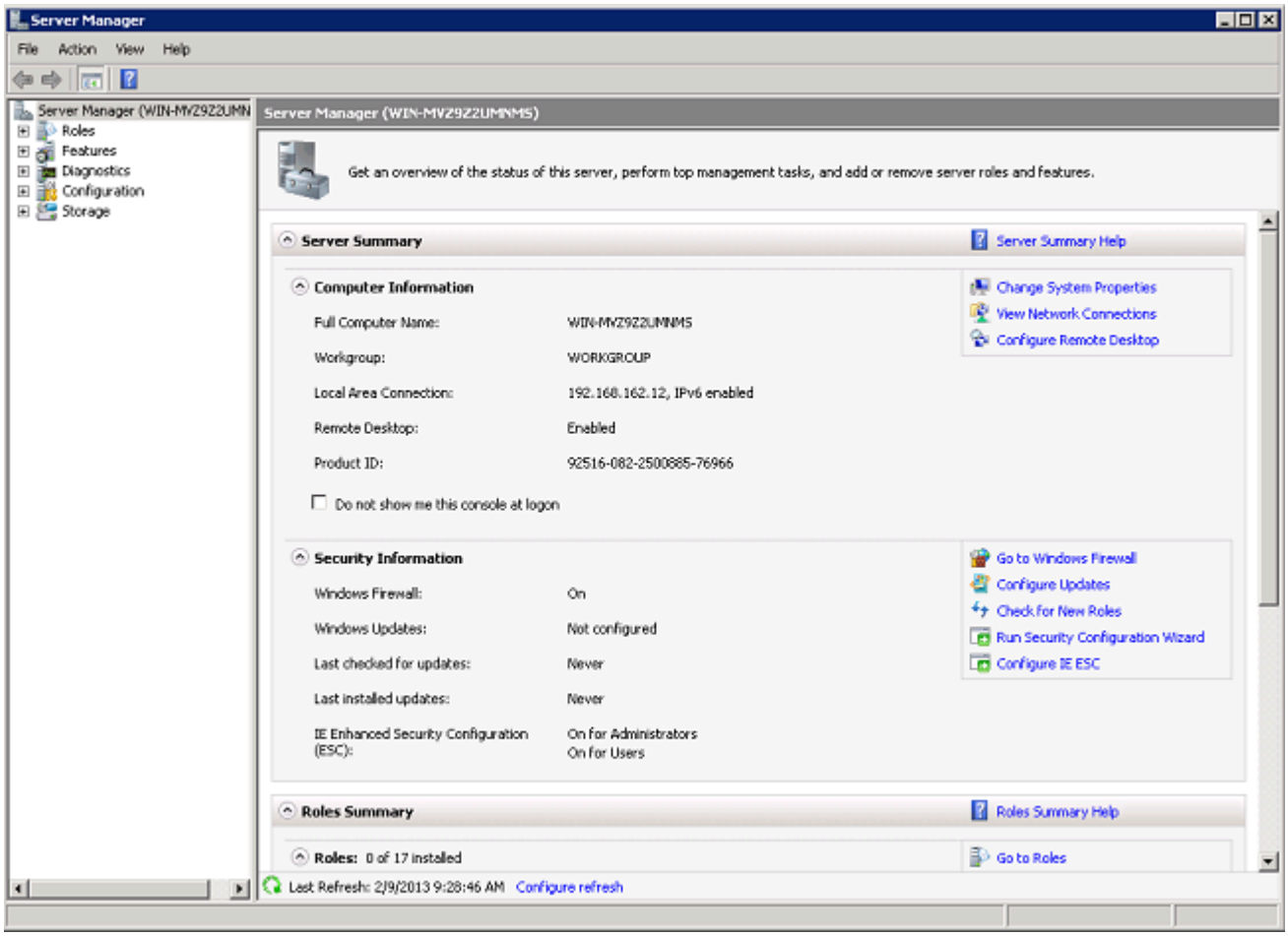
安装并配置Microsoft Windows 2008 Server作为CA服务器

使用EAP-MS-CHAP v2的PEAP根据服务器上存在的证书验证RADIUS服务器。此外，服务器证书必须由受客户端计算机信任的公共CA颁发（即，公共CA证书已存在于客户端计算机证书存储库的

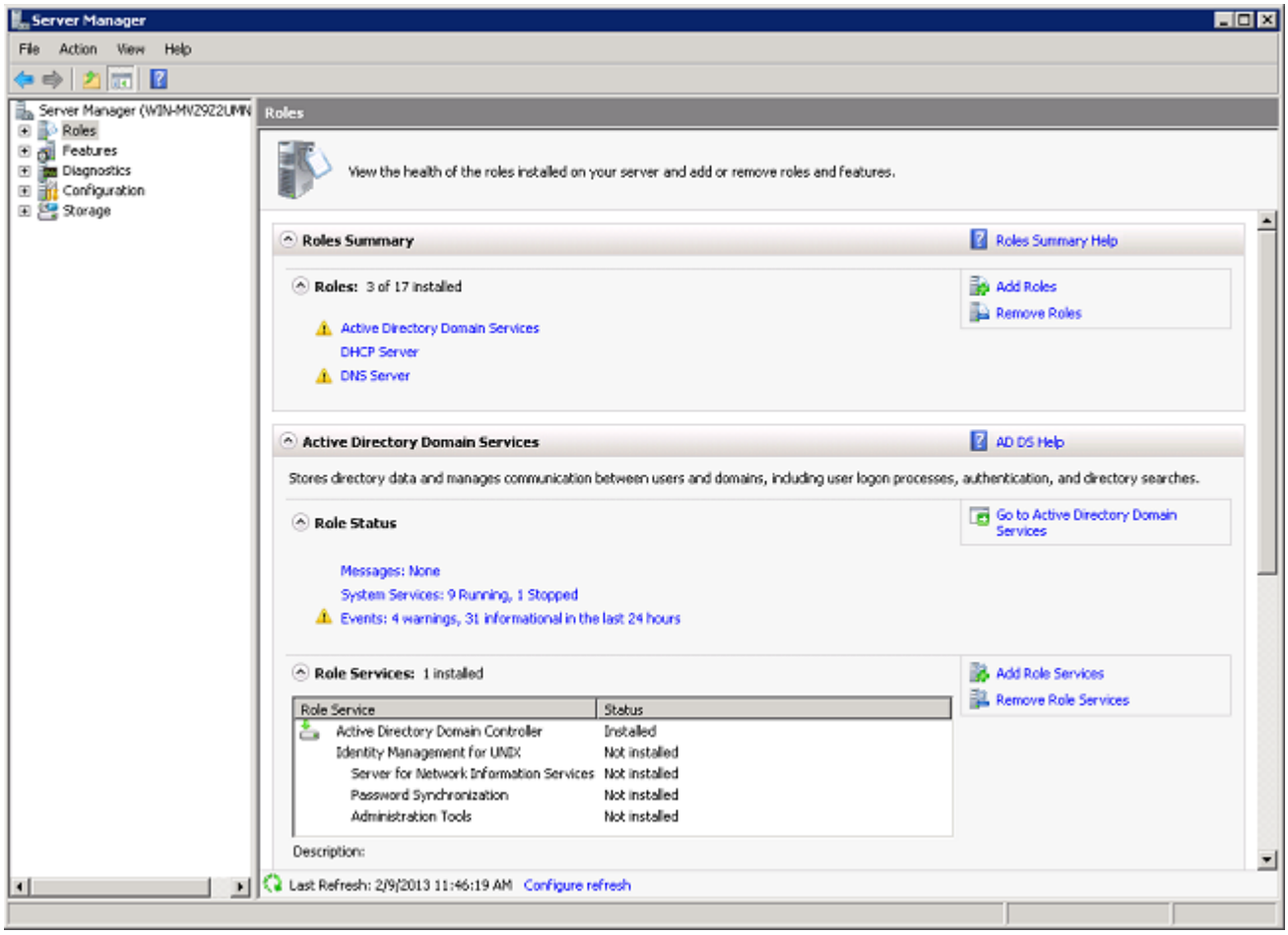
受信任的根证书颁发机构文件夹中）。

要将Microsoft Windows 2008服务器配置为向NPS颁发证书的CA服务器，请完成以下步骤：

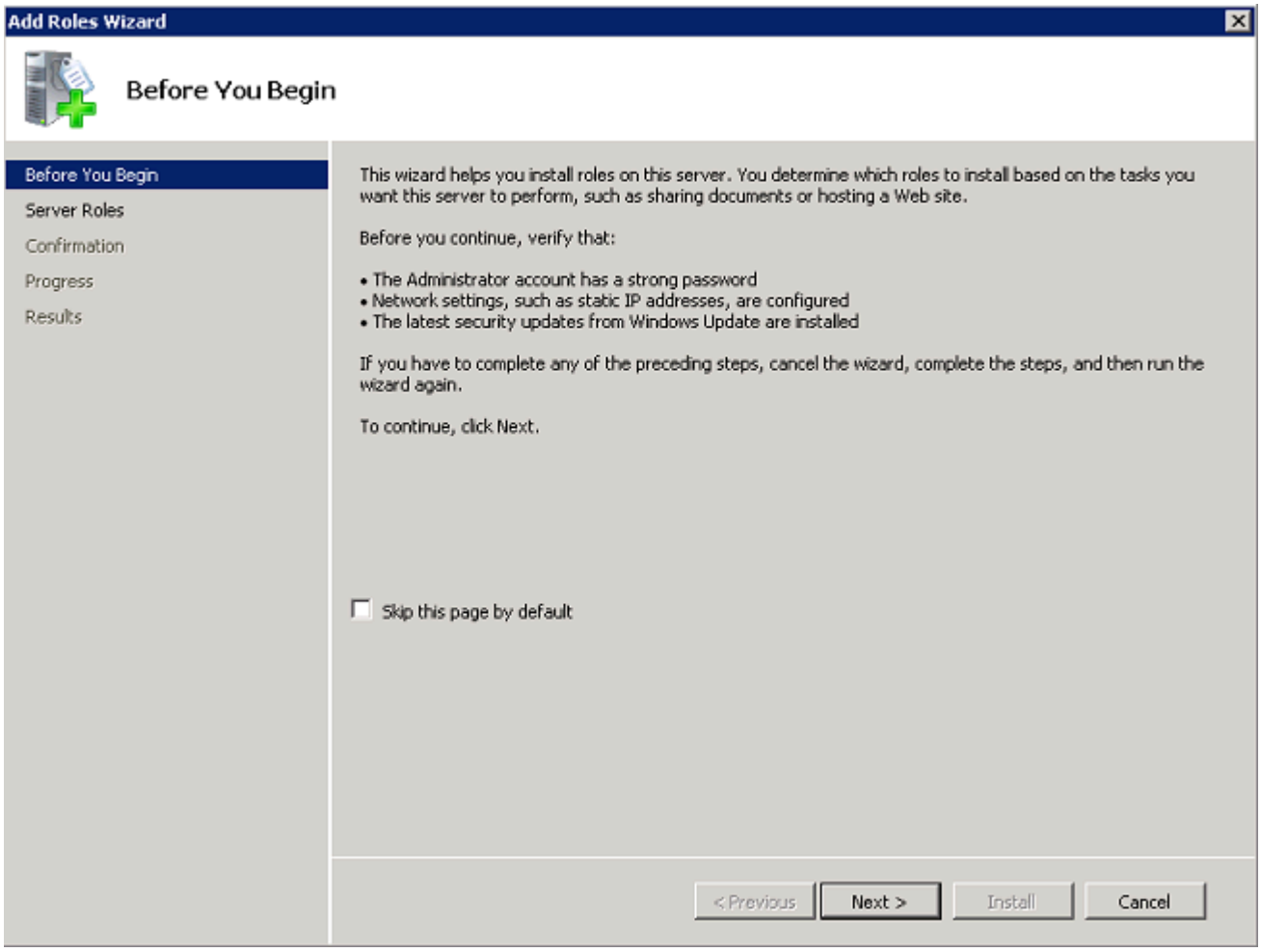
1. 单击开始> 服务器管理器。



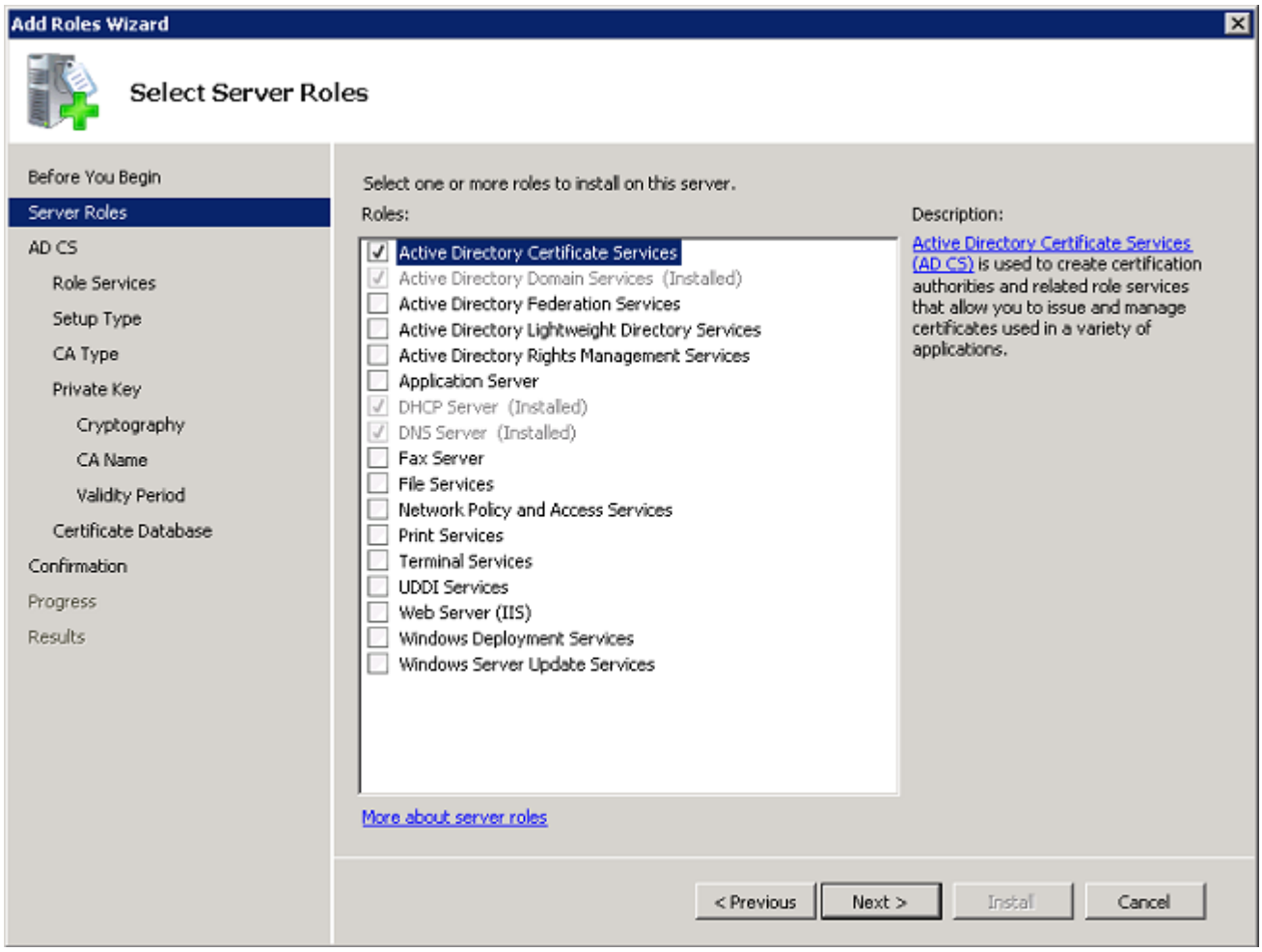
2. 单击Roles> Add Roles。


Server Manager
File Action View Help
Server Manager (WIN-MV29Z2UMN
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 3 of 17 installed
Add Roles
Remove Roles
Active Directory Domain Services
DHCP Server
DNS Server
Active Directory Domain Services
AD DS Help
Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.
Role Status
Go to Active Directory Domain Services
Messages: None
System Services: 9 Running, 1 Stopped
Events: 4 warnings, 31 informational in the last 24 hours
Role Services: 1 installed
Add Role Services
Remove Role Services
Role Service
Status
Active Directory Domain Controller
Installed
Identity Management for UNIX
Not installed
Server for Network Information Services
Not installed
Password Synchronization
Not installed
Administration Tools
Not installed
Description:
Last Refresh: 2/9/2013 11:46:19 AM
Configure refresh

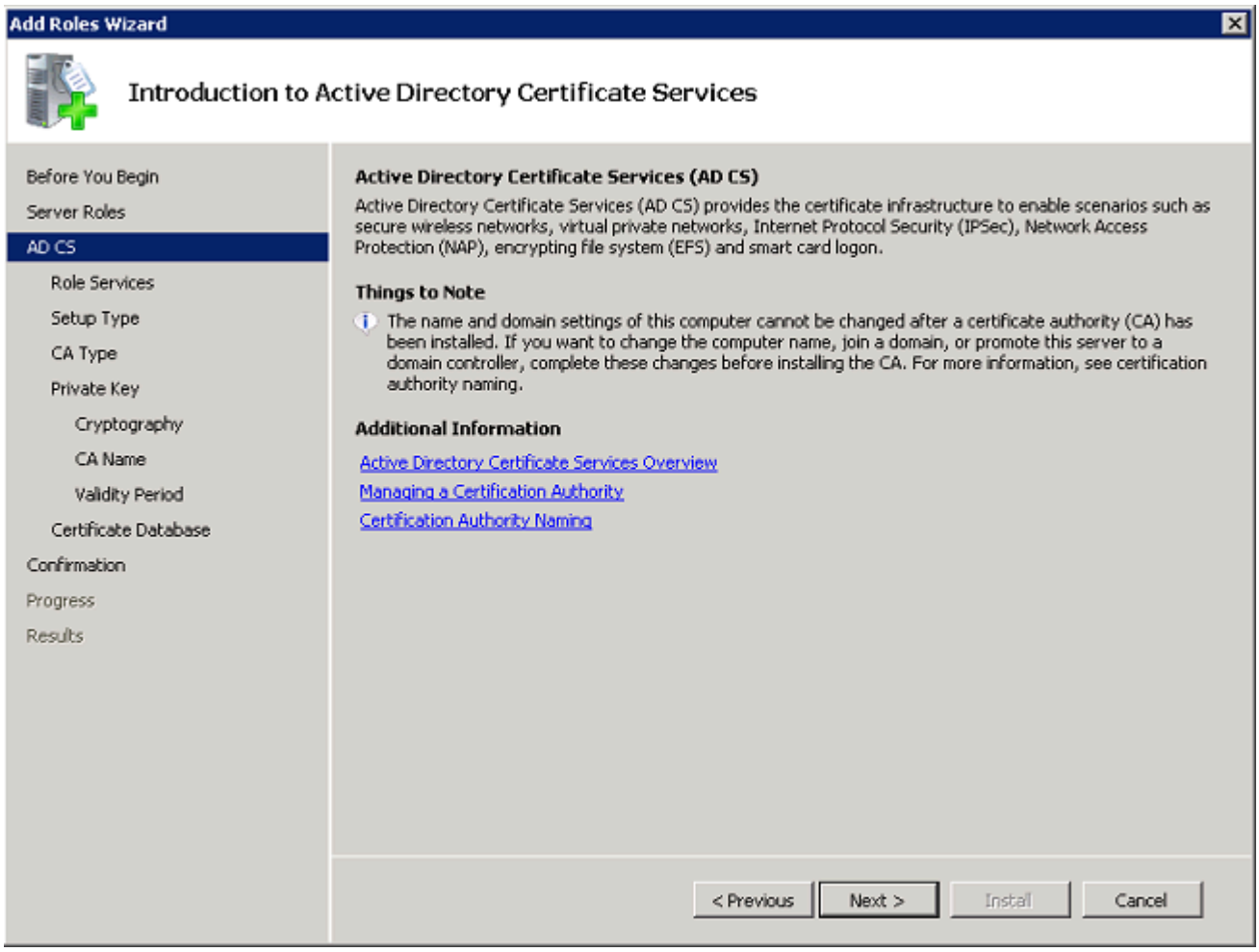
3. 单击 Next。



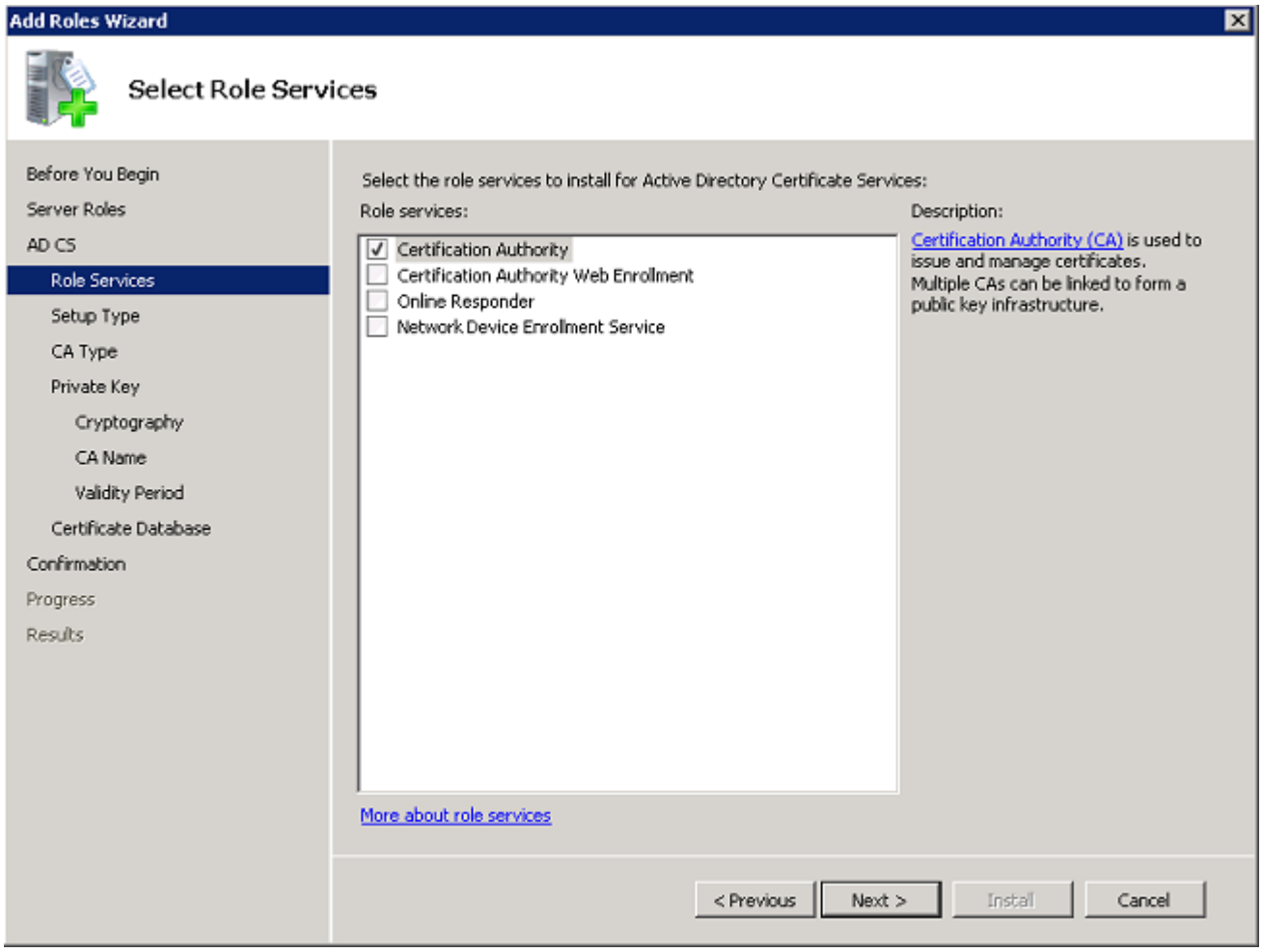
4. 选择服务Active Directory证书服务，然后单击下一步。



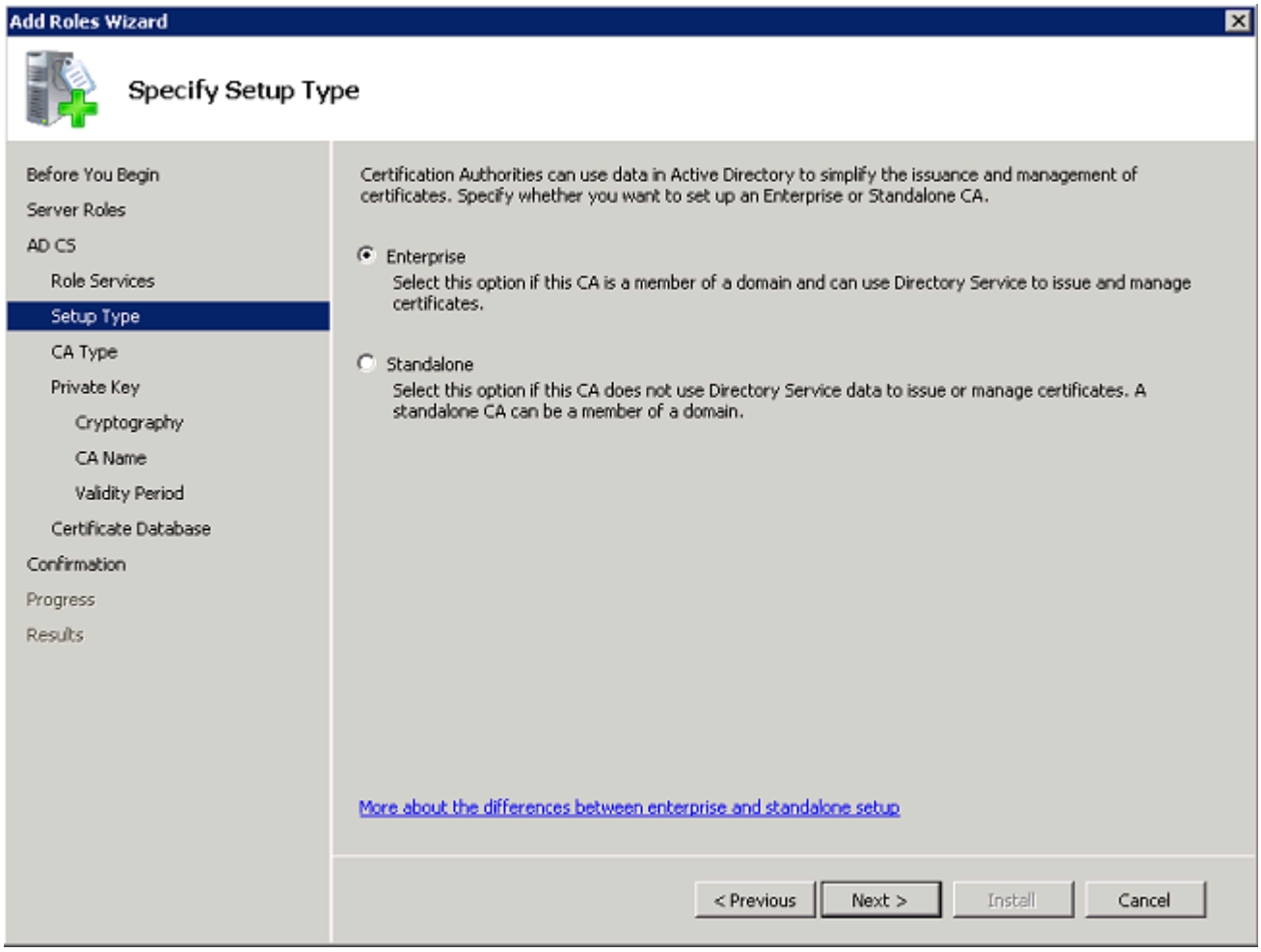
5. 查看Active Directory证书服务简介，然后点击下一步。



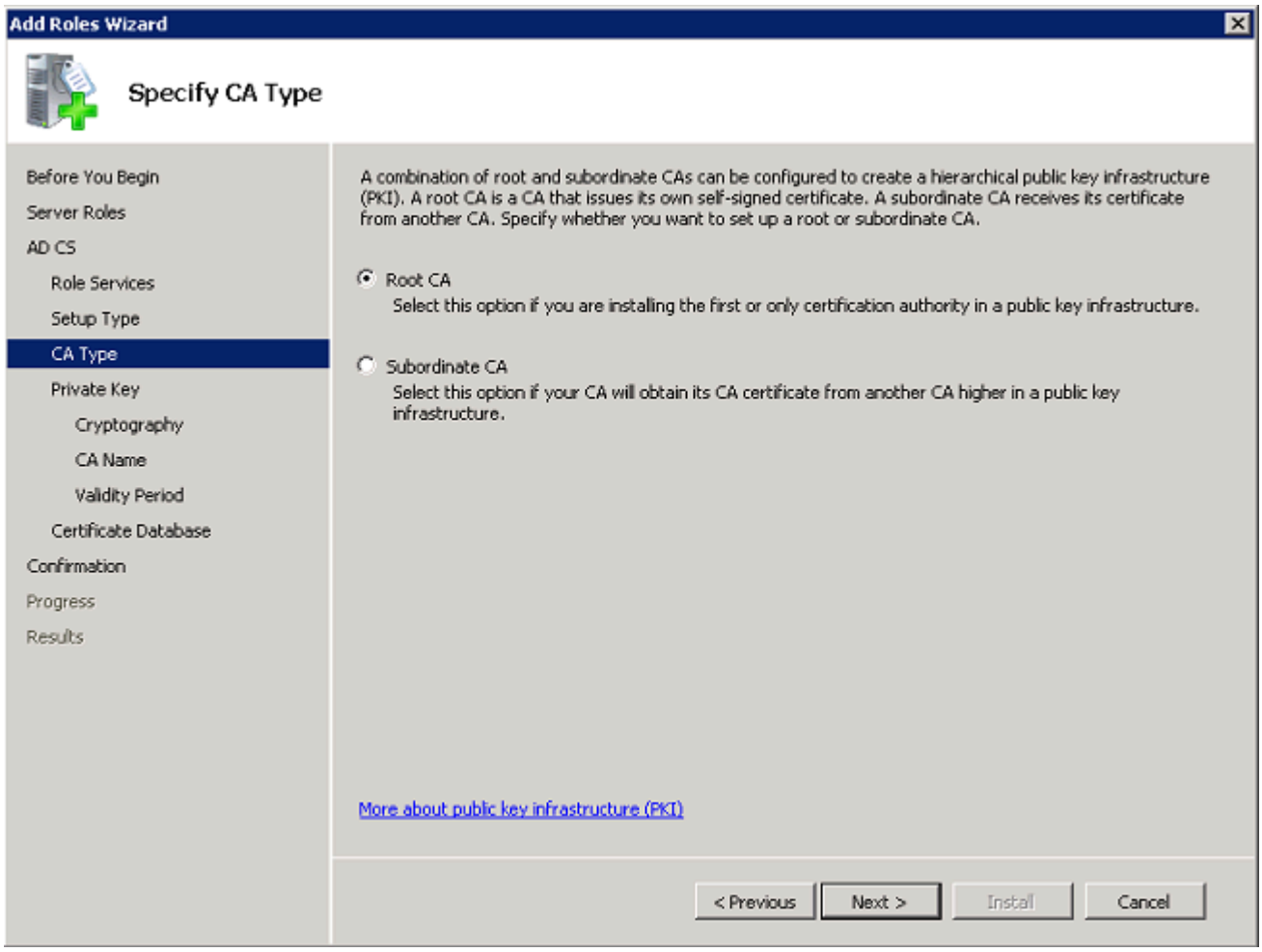
6. 选择证书颁发机构，然后单击下一步。



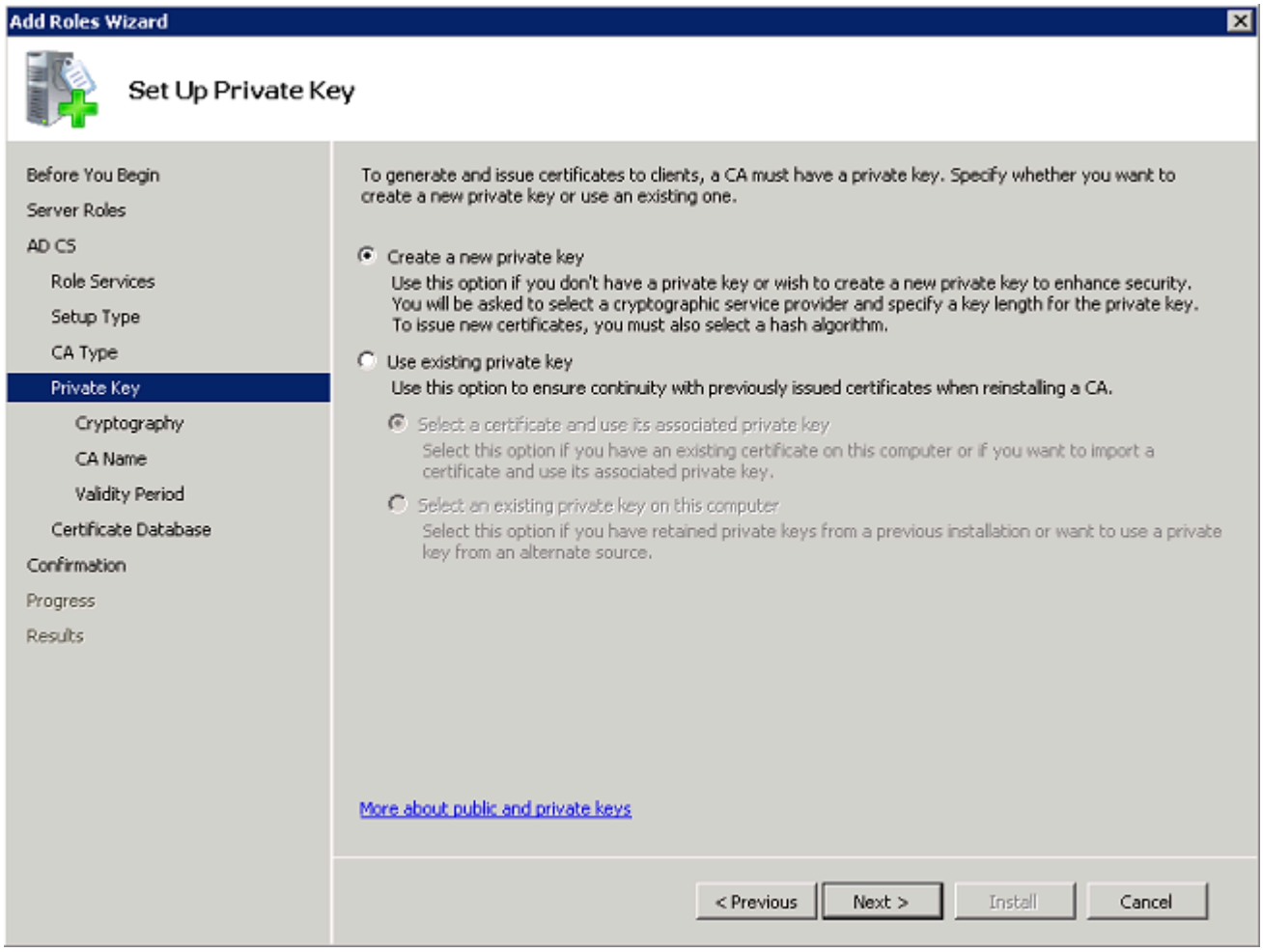
7. 选择Enterprise，然后单击Next。



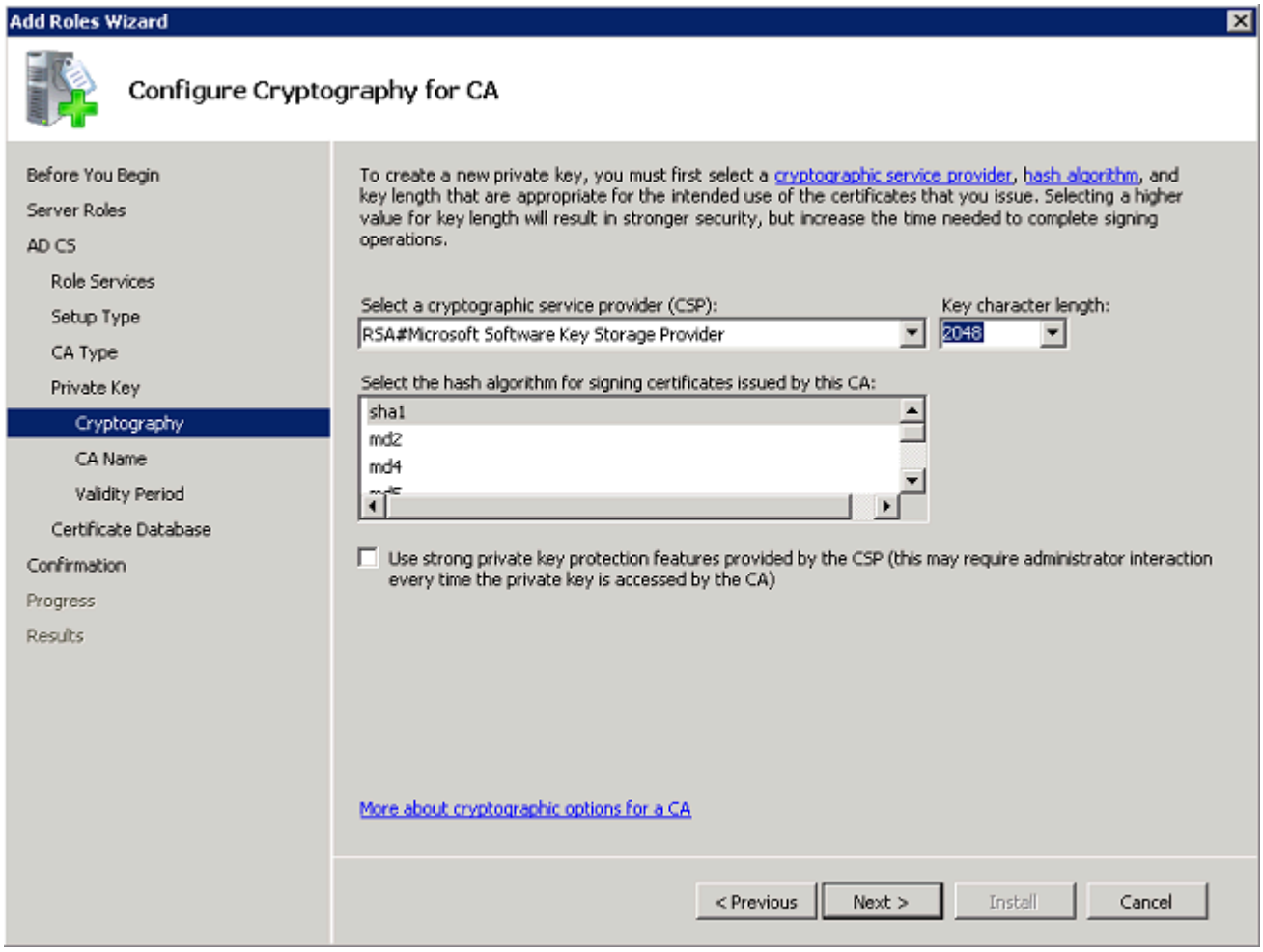
8. 选择根CA，然后单击下一步。



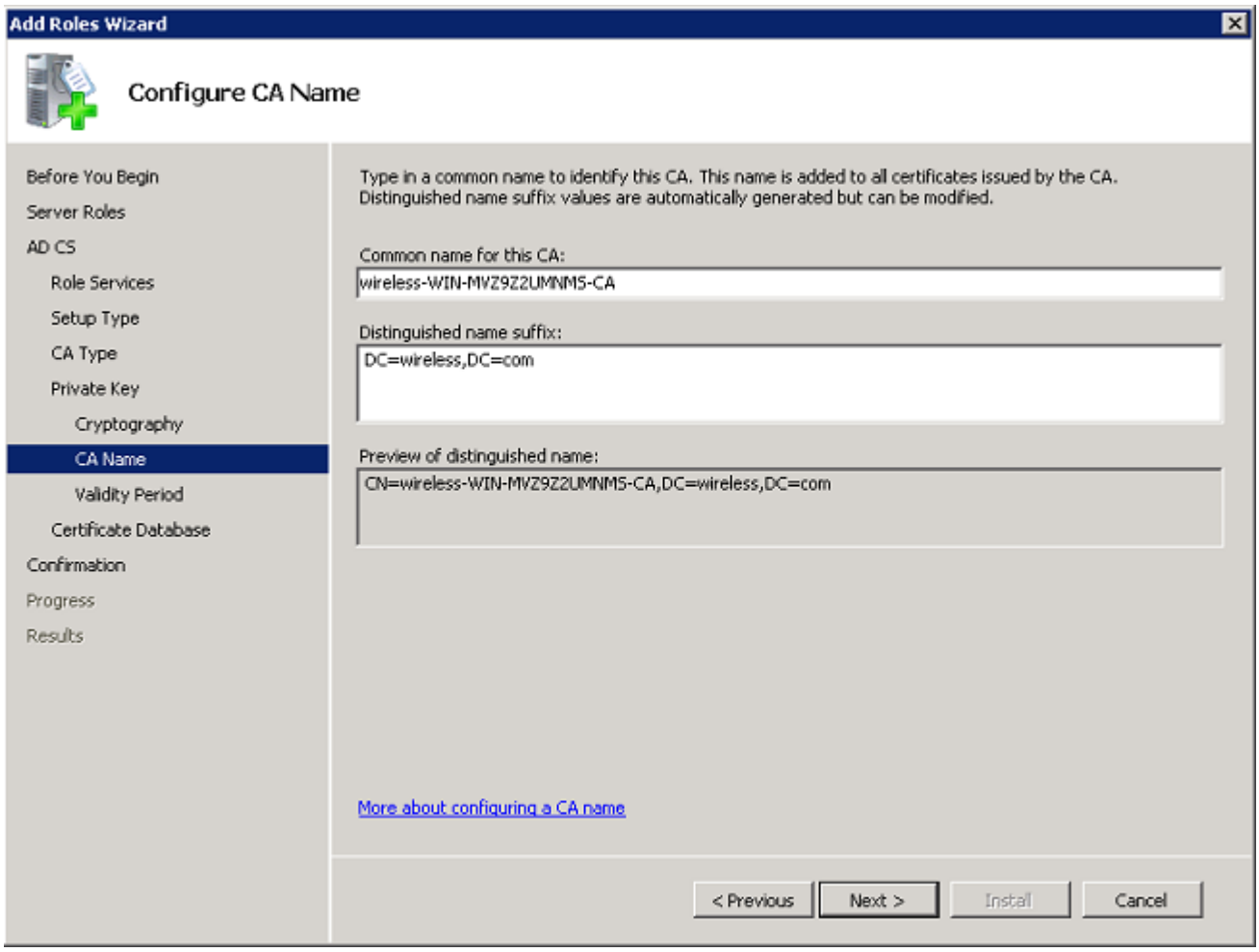
9. 选择Create a new private key，然后单击Next。



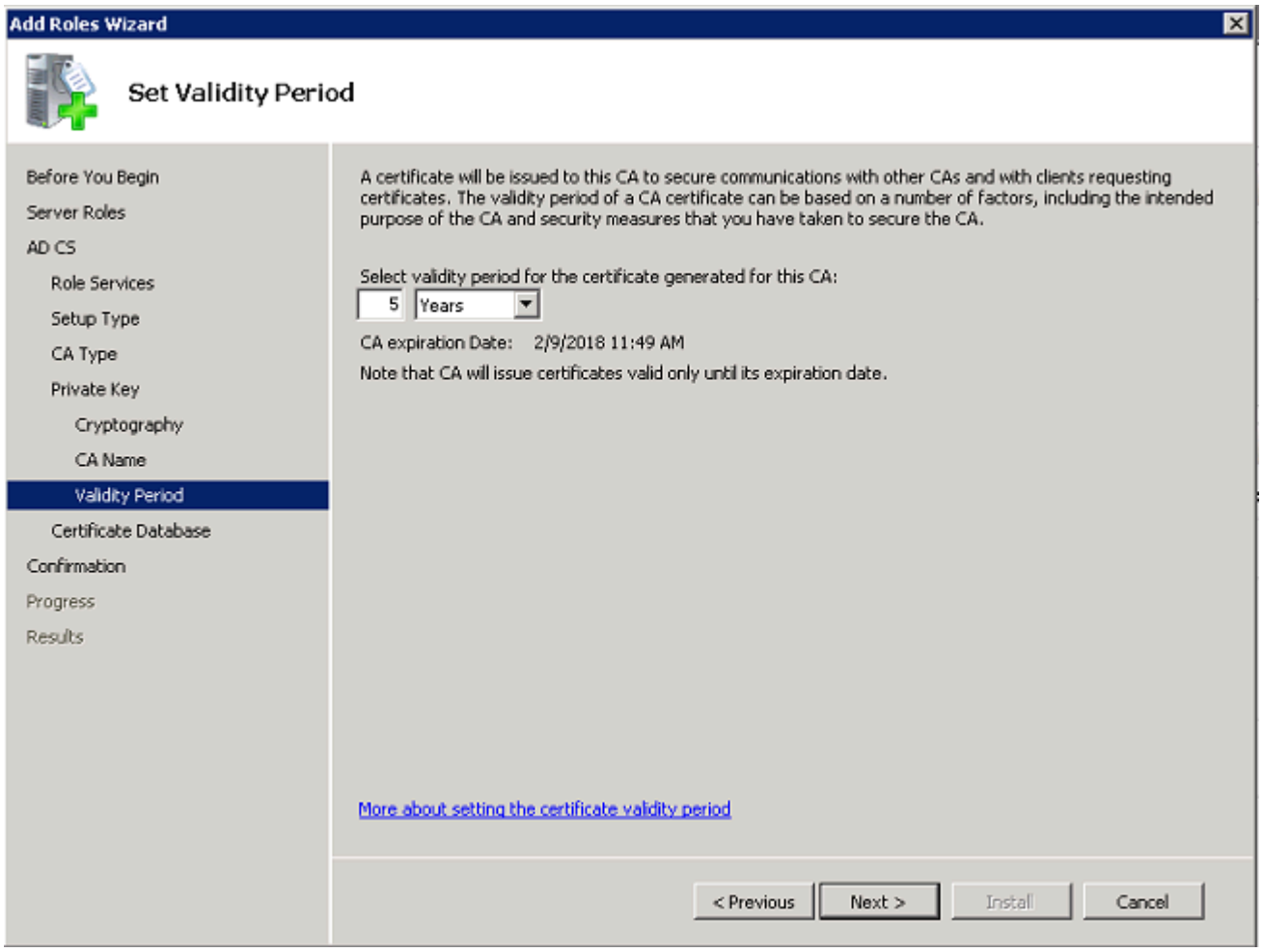
10. 在Configure Cryptography for CA上单击Next。



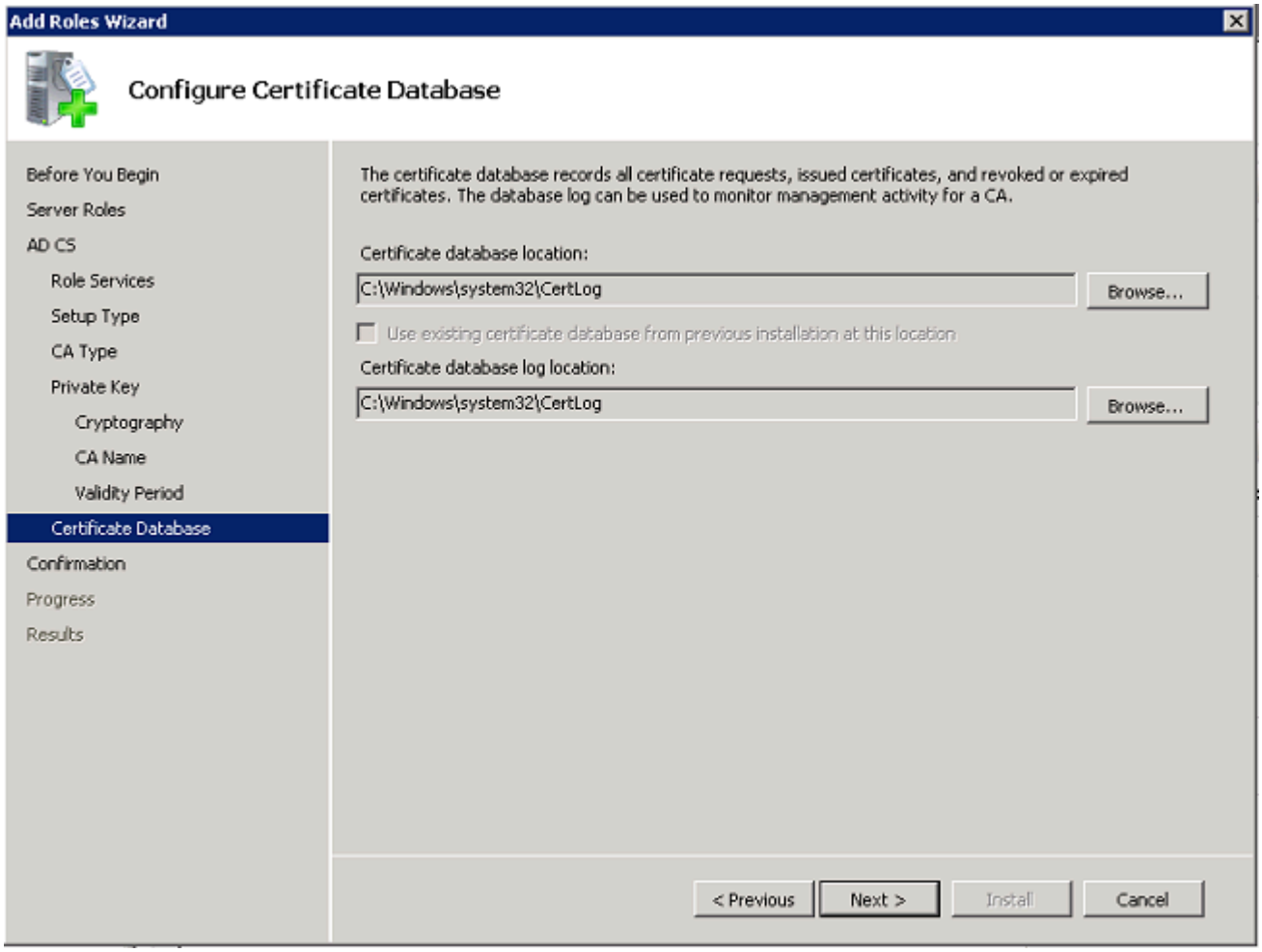
11. 单击下一步接受此CA的默认公用名。



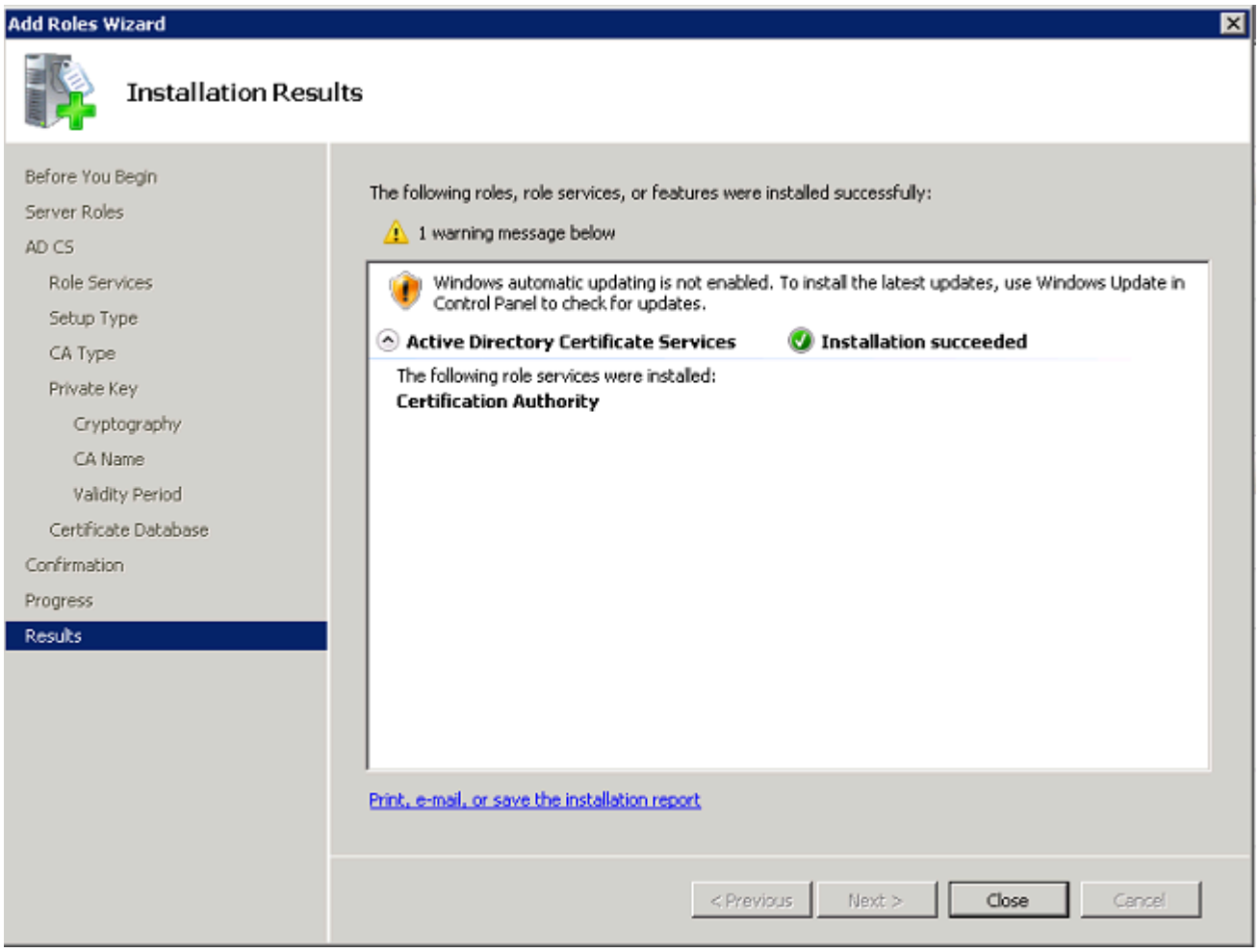
12. 选择此CA证书的有效时间长度，然后单击Next。



13. 单击下一步接受默认证书数据库位置。



14. 检查配置，然后单击安装启动Active Directory证书服务。

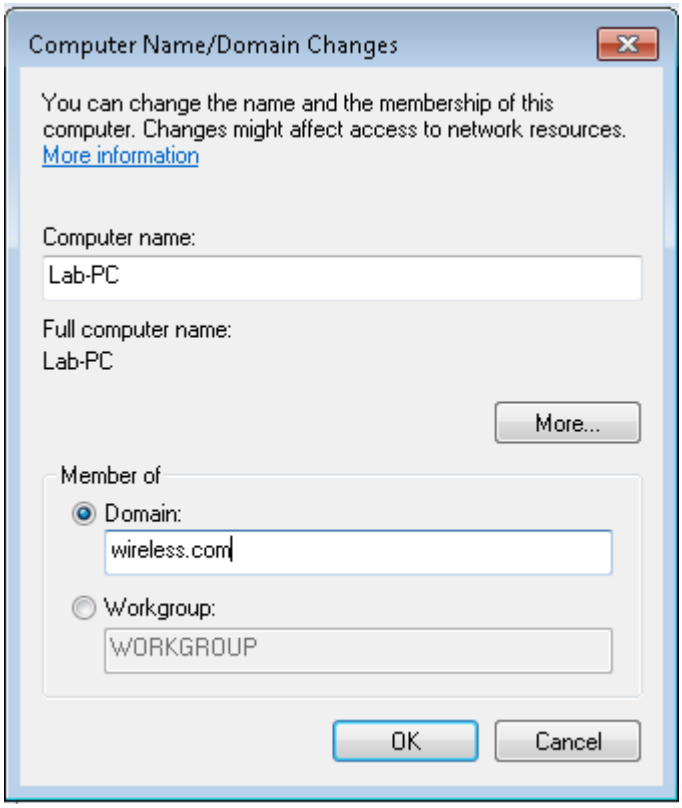


15. 安装完成后，单击Close。

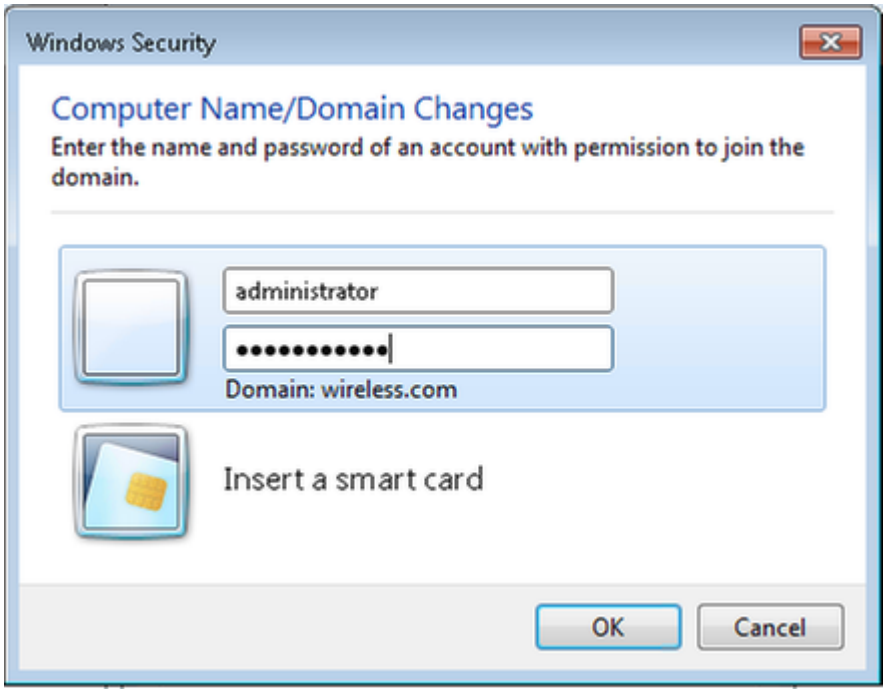
将客户端连接到域

完成以下步骤，将客户端连接到有线网络，并从新域下载域特定信息：

1. 使用直通以太网电缆将客户端连接到有线网络。
2. 启动客户端，并使用客户端用户名和密码登录。
3. 单击开始>运行，输入cmd，然后单击确定。
4. 在命令提示符下，输入ipconfig，然后单击Enter以验证DHCP是否正常工作，以及客户端是否从DHCP服务器收到IP地址。
5. 要将客户端加入域，请单击开始，右键单击计算机，选择属性，然后选择更改设置（位于右下角）。
6. 单击 Change。
7. 单击Domain，输入域名wireless（在本例中），然后单击OK。



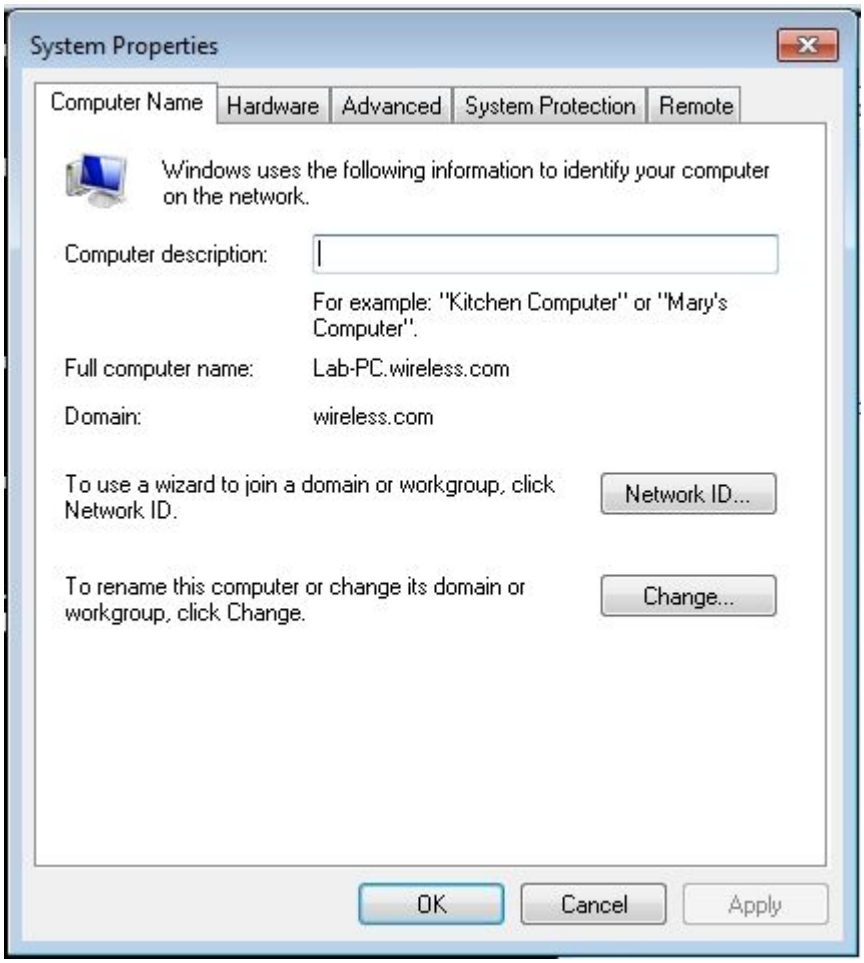
8. 输入用户名administrator和客户端加入的域特定的密码。这是服务器上Active Directory中的管理员帐户。



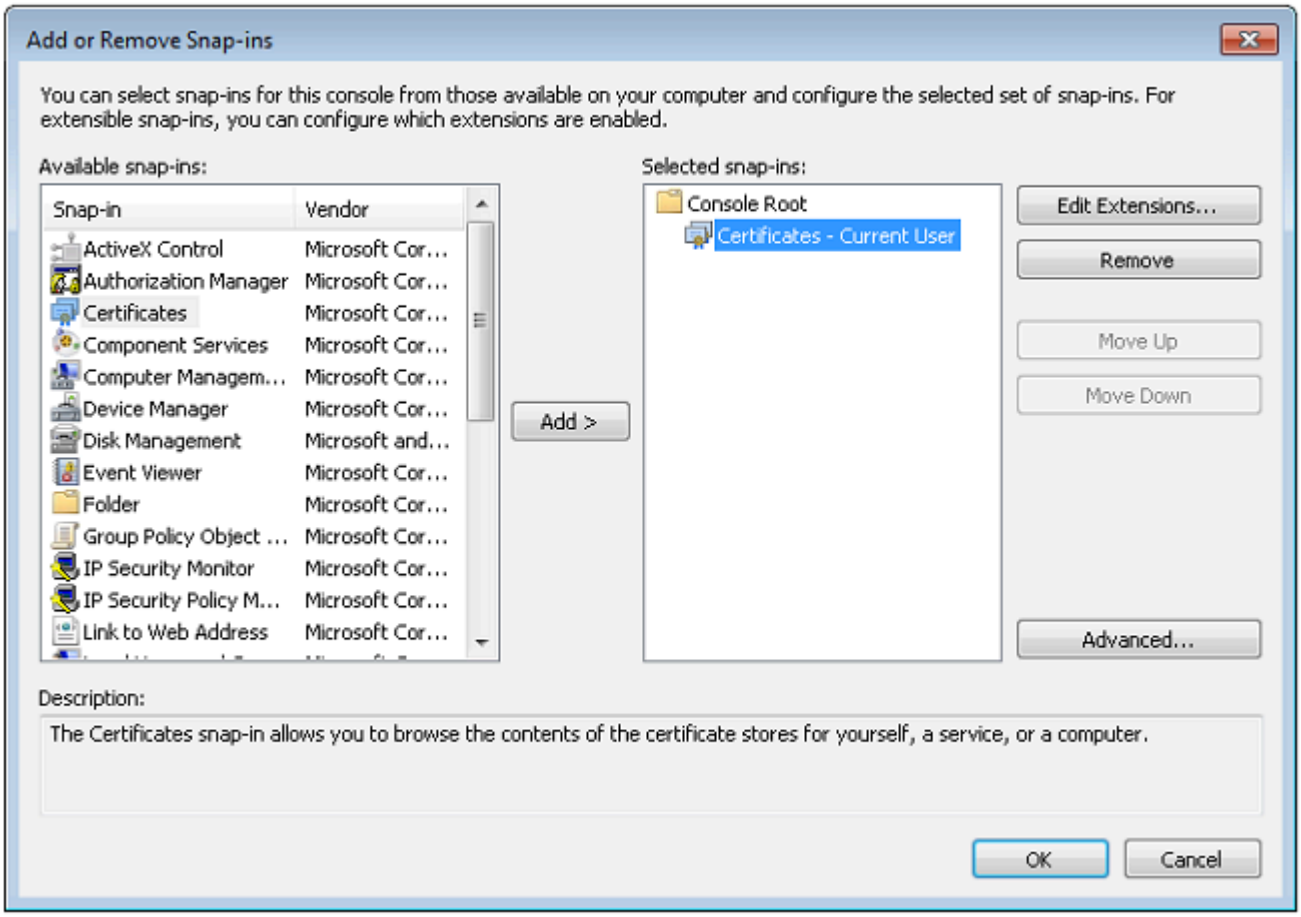
9. 单击确定，然后再次单击确定。



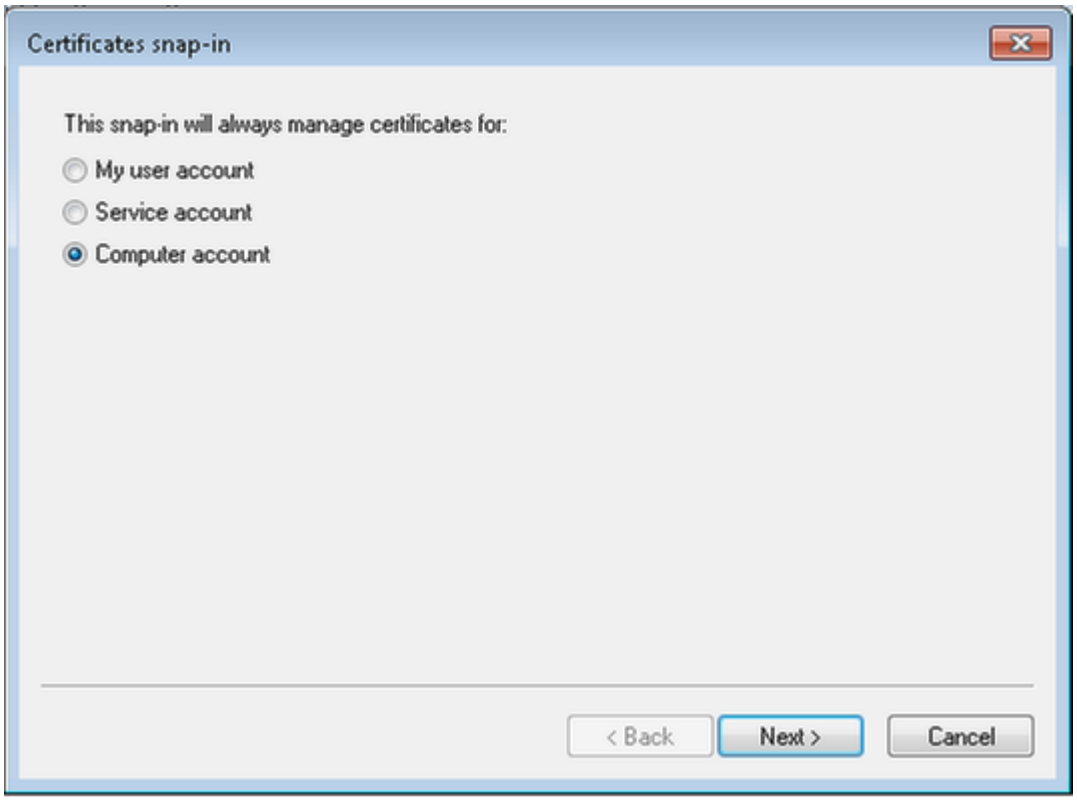
10. 单击Close> Restart Now重新启动计算机。
11. 计算机重新启动后，请使用以下内容登录：用户名 = Administrator；密码 = <域密码>；域 = Wireless。
12. 单击Start，右键单击Computer，选择Properties，然后选择右下角的Change Settings以验证您是否在无线域中。
13. 下一步是验证客户端从服务器收到了 CA 证书（信任）。



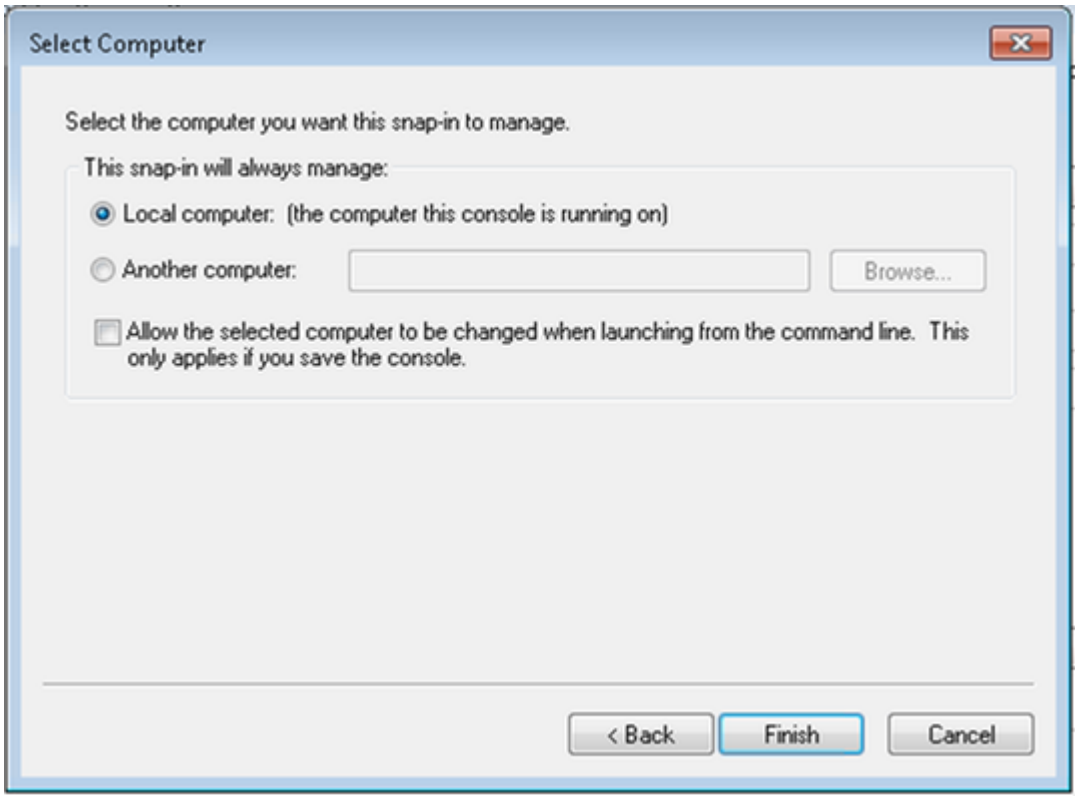
14. 单击Start，输入mmc，然后按Enter。
15. 单击文件，然后单击“添加/删除”管理单元。
16. 选择“证书”，并单击“添加”。



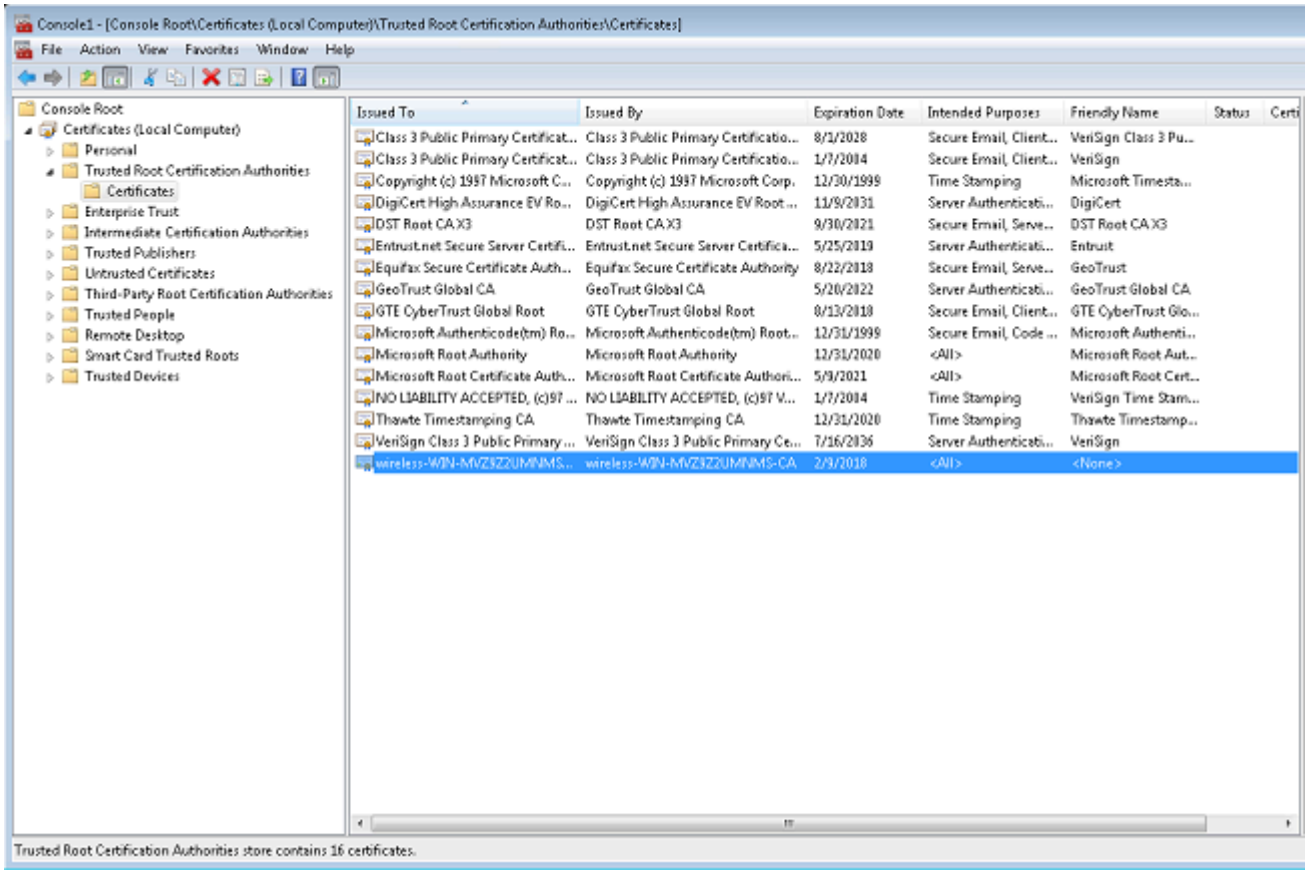
17. 单击Computer account，然后单击Next。



18. 单击Local computer，然后单击Next。



19. Click OK.
20. 展开Certificates(Local Computer)和Trusted Root Certification Authorities文件夹，然后单击Certificates。在列表中查找无线域CA证书。在本示例中，CA证书称为wireless-WIN-MVZ9Z2UMNMS-CA。

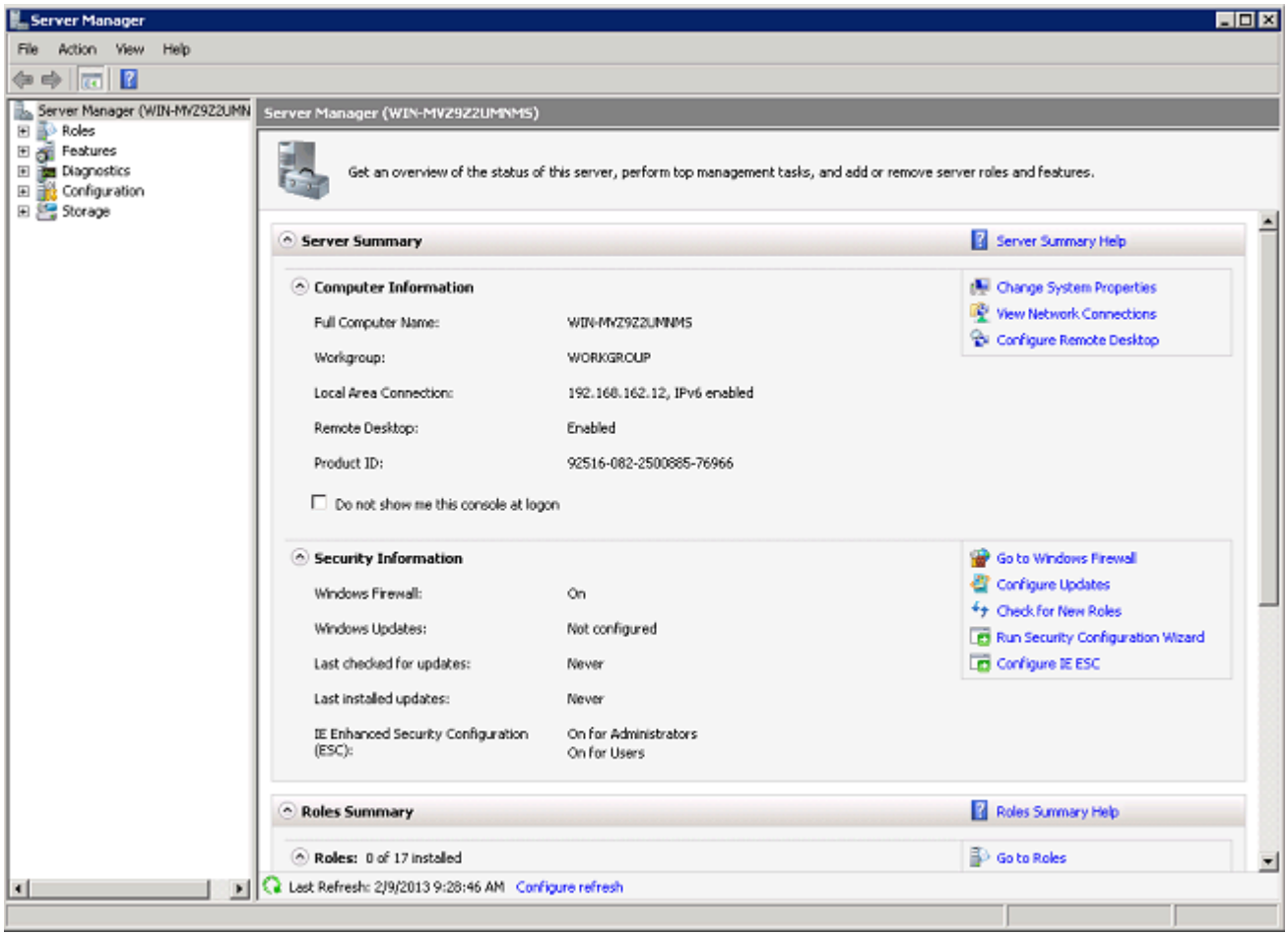


21. 重复此过程，以便将更多客户端添加到域中。

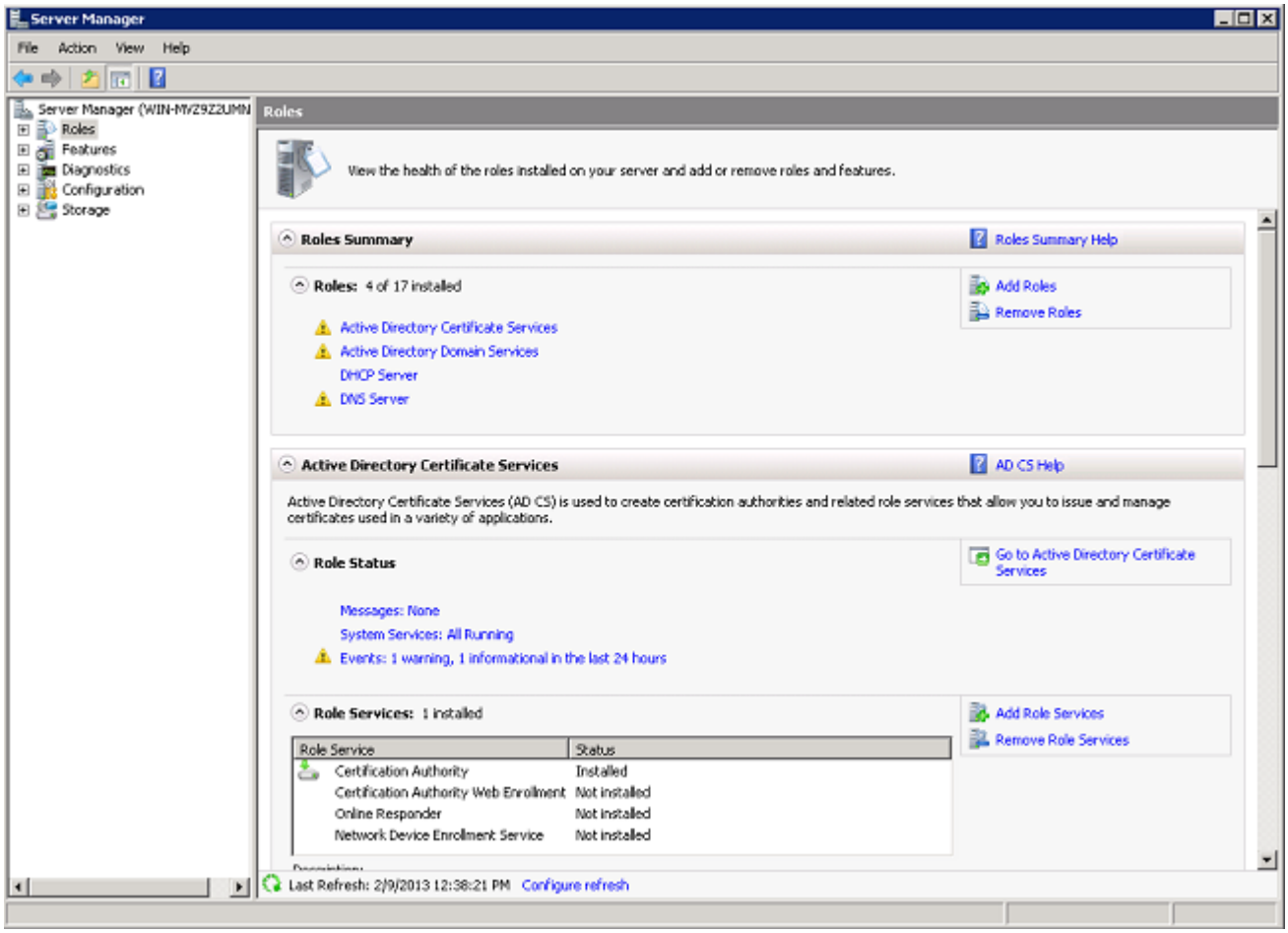
在Microsoft Windows 2008 Server上安装网络策略服务器

在此设置中，NPS用作RADIUS服务器，通过PEAP身份验证对无线客户端进行身份验证。完成以下步骤以便在Microsoft WINDOWS 2008服务器上安装和配置NPS:

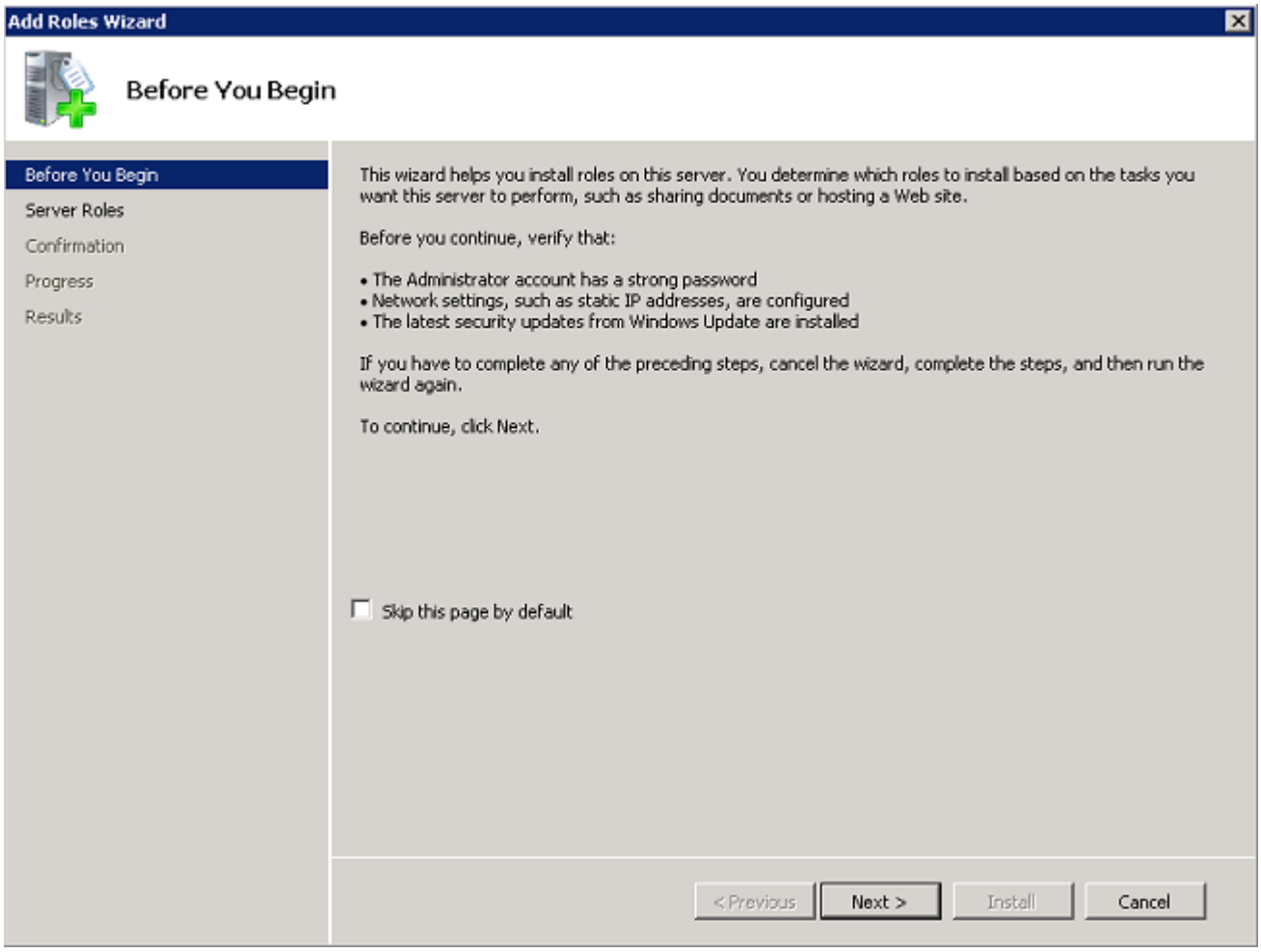
1. 单击开始> 服务器管理器。



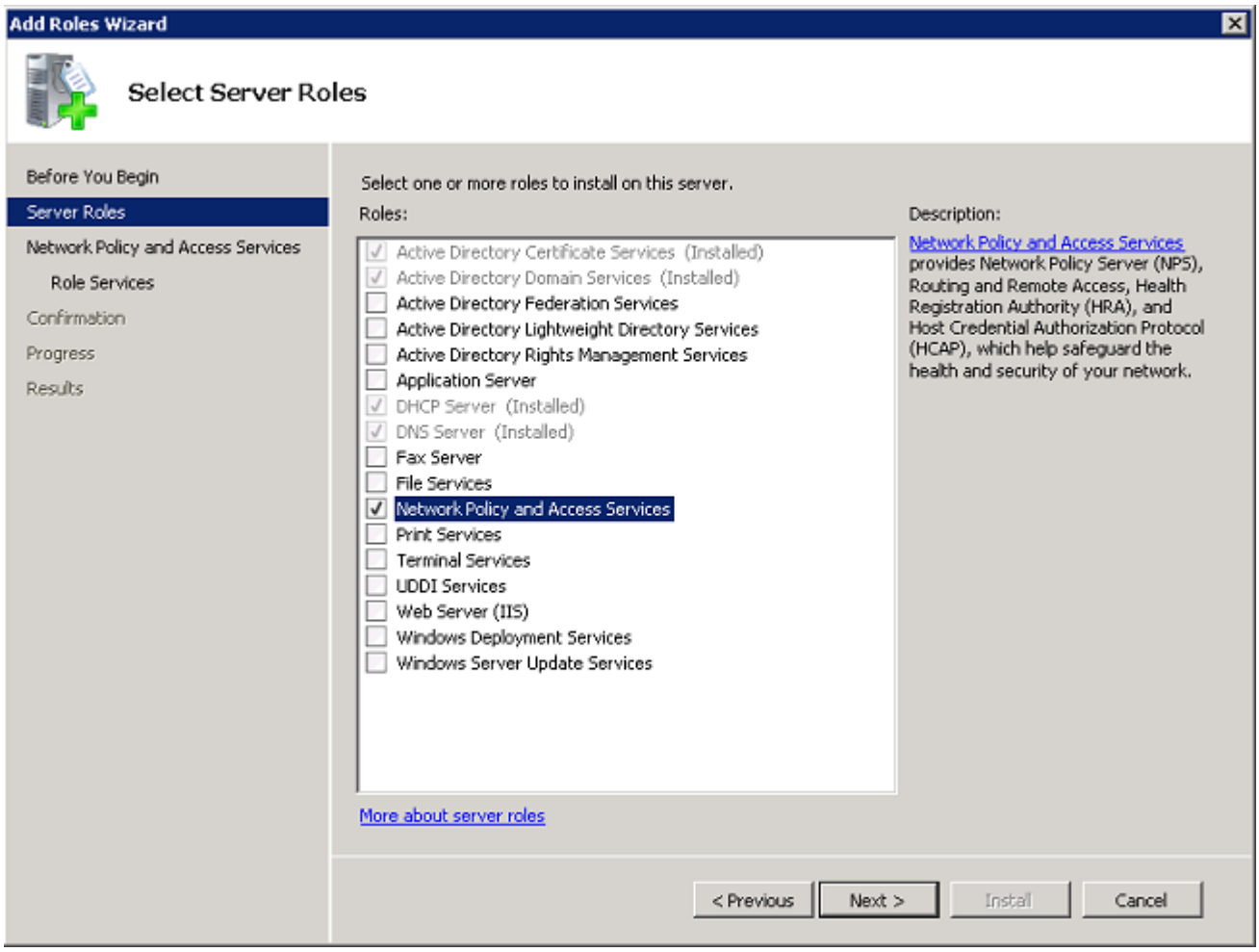
2. 单击Roles> Add Roles。


Server Manager
File Action View Help
Server Manager (WIN-NYZ9ZZUMN
Roles
Features
Diagnostics
Configuration
Storage
Roles
View the health of the roles installed on your server and add or remove roles and features.
Roles Summary
Roles Summary Help
Roles: 4 of 17 installed
Add Roles
Remove Roles
Active Directory Certificate Services
Active Directory Domain Services
DHCP Server
DNS Server
Active Directory Certificate Services
AD CS Help
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
Role Status
Go to Active Directory Certificate Services
Messages: None
System Services: All Running
Events: 1 warning, 1 informational in the last 24 hours
Role Services: 1 installed
Add Role Services
Remove Role Services
Role Service
Status
Certification Authority
Installed
Certification Authority Web Enrollment
Not installed
Online Responder
Not installed
Network Device Enrollment Service
Not installed
Last Refresh: 2/9/2013 12:38:21 PM
Configure refresh

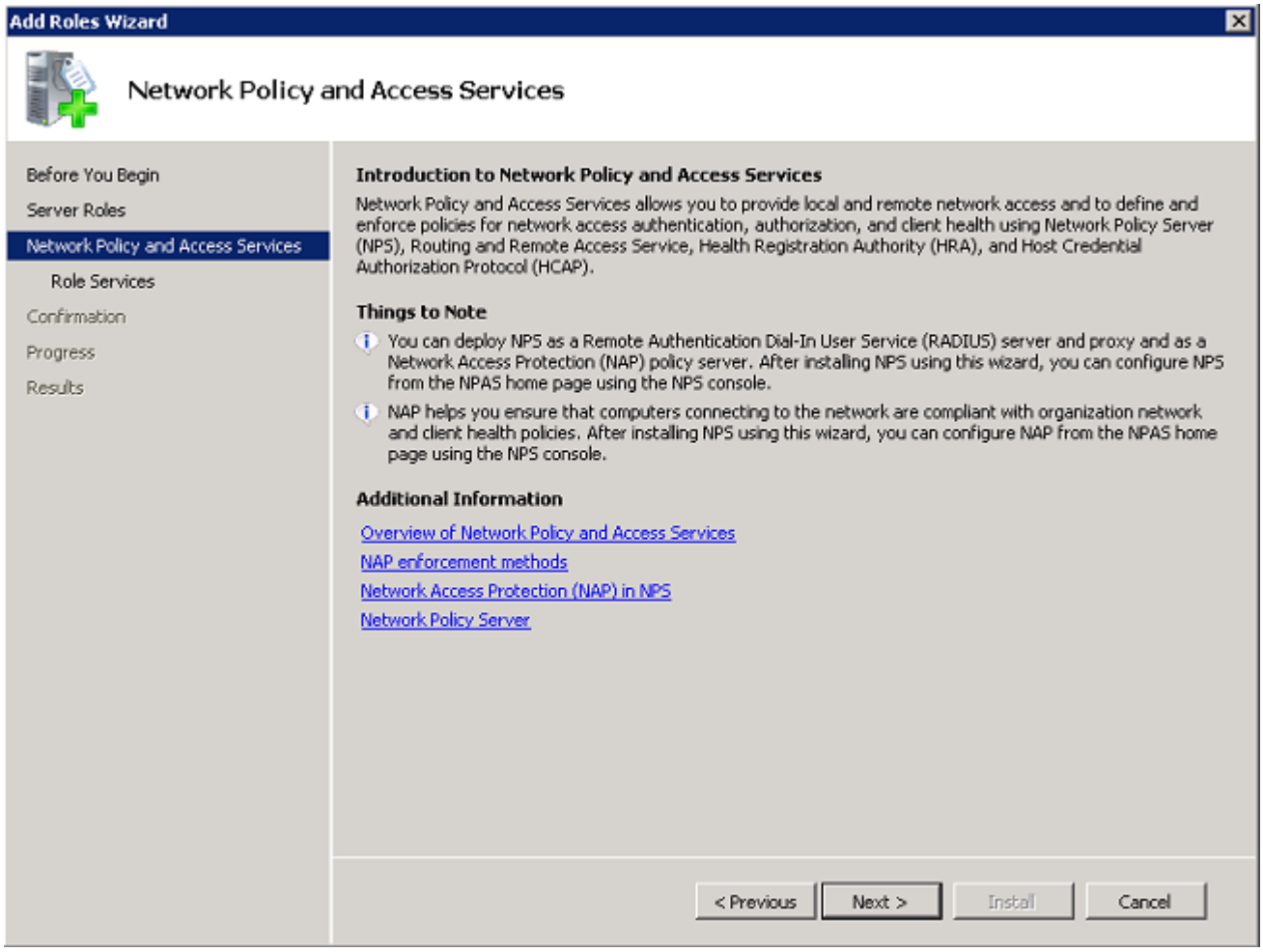
3. 单击 Next。



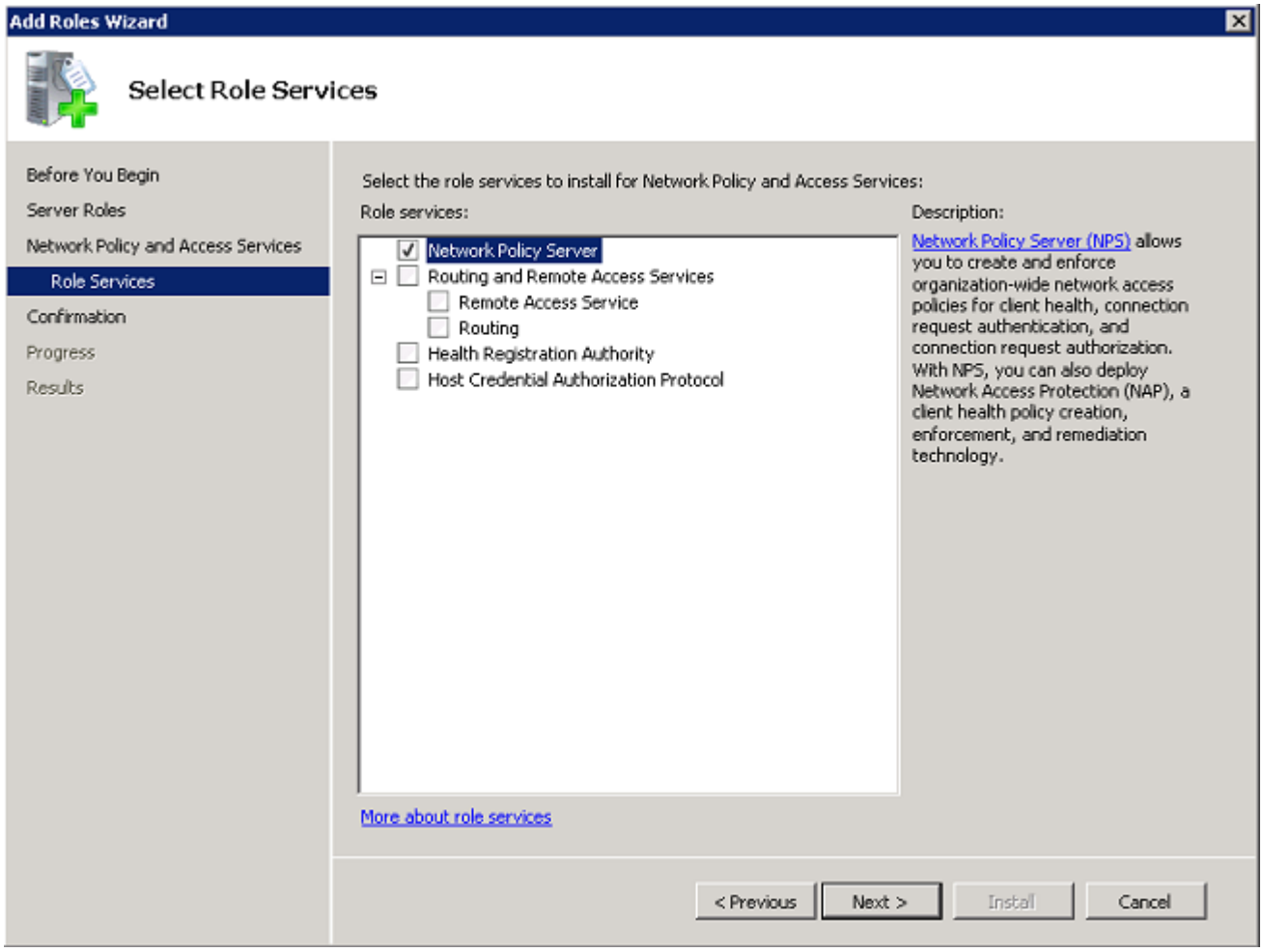
4. 选择服务Network Policy and Access Services，然后单击Next。



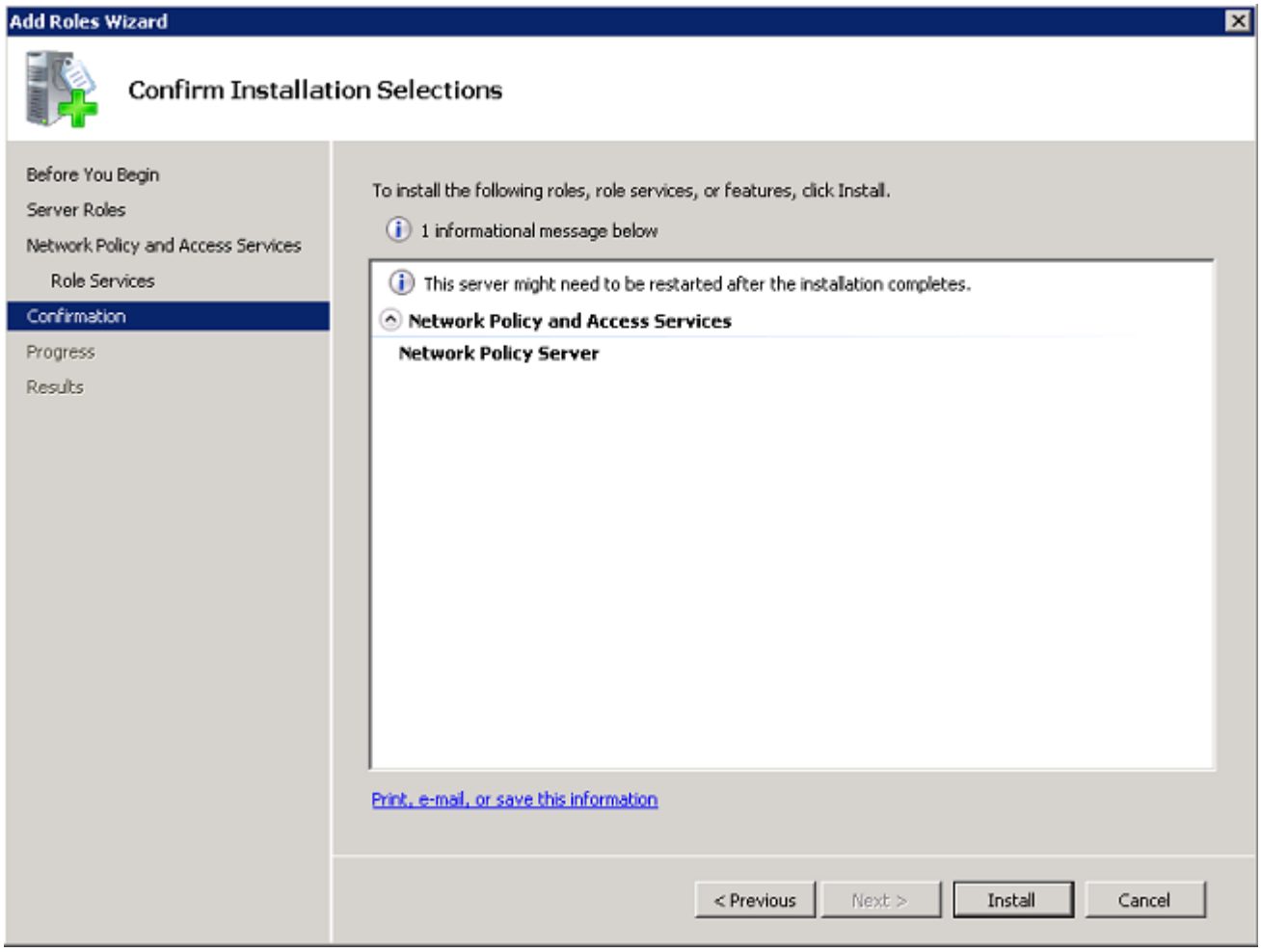
5. 查看Introduction to Network Policy and Access Services，然后单击Next。



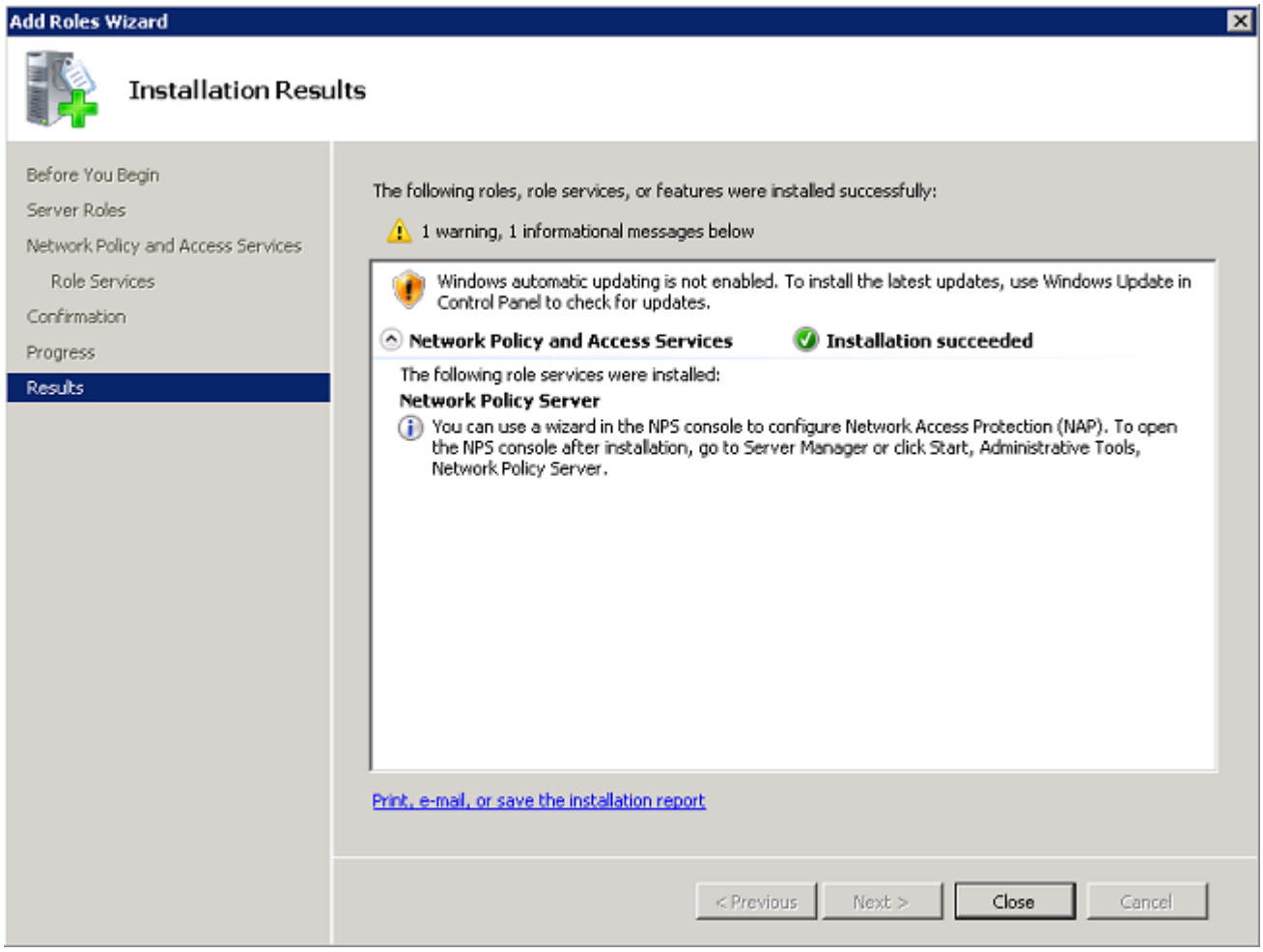
6. 选择Network Policy Server，然后单击Next。



7. 查看确认，然后单击Install。



安装完成后，将显示一个类似于此的屏幕。

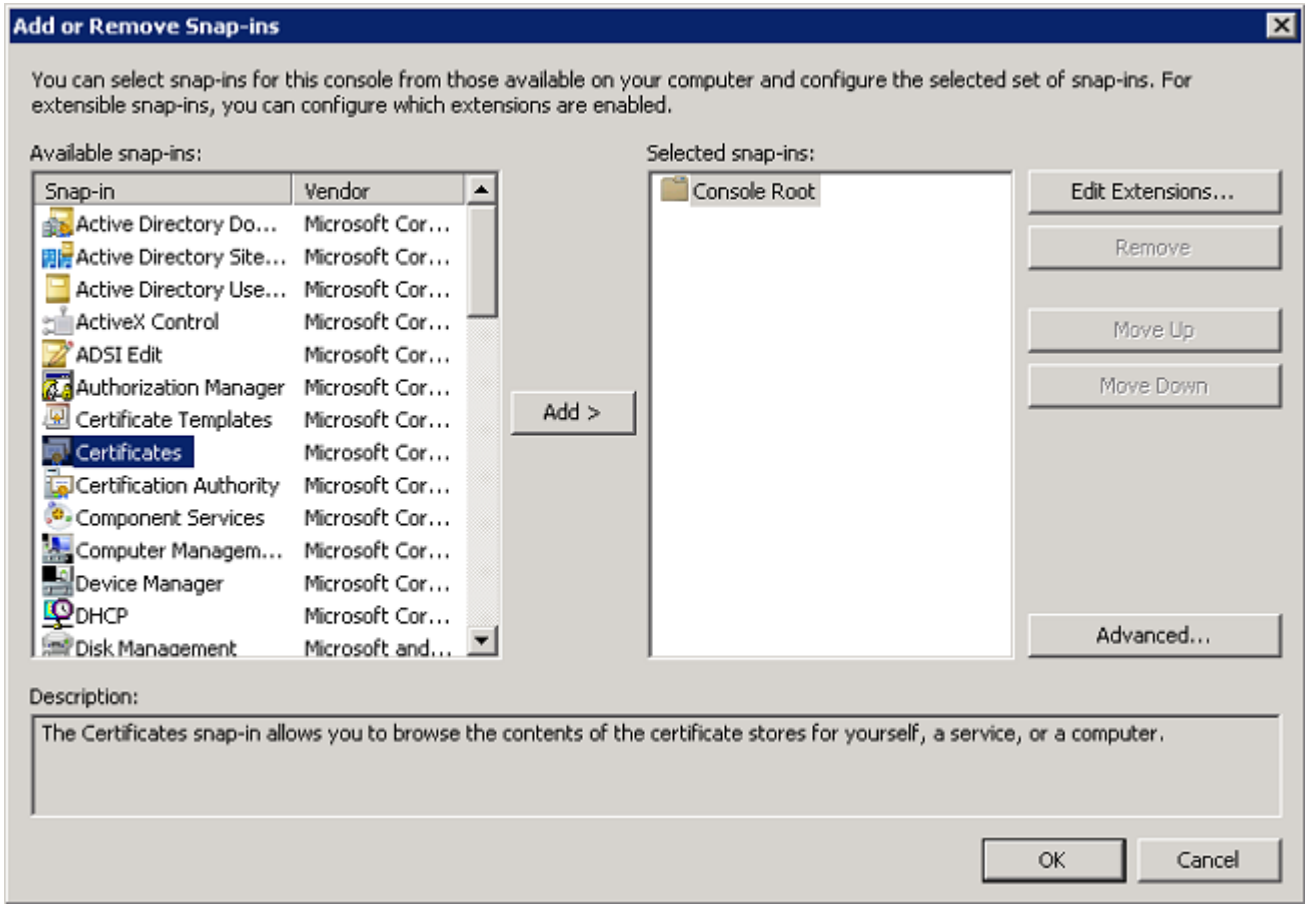


8. 单击 Close。

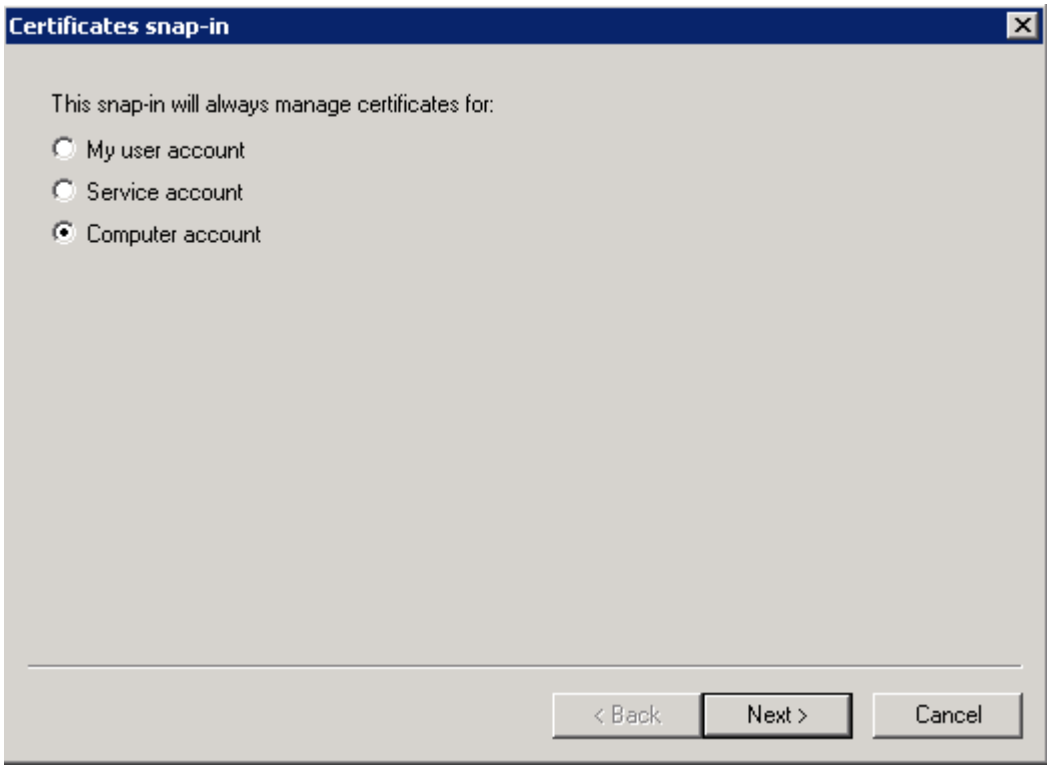
安装证书

要安装NPS的计算机证书，请完成以下步骤：

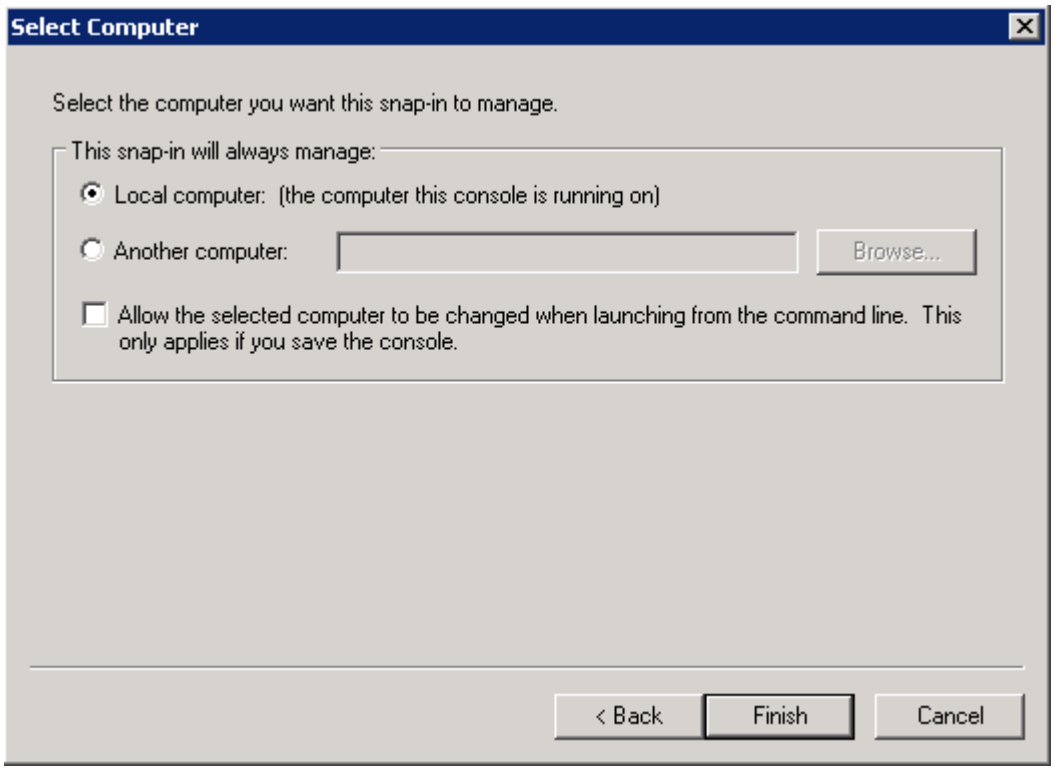
1. 单击Start，输入mmc，然后按Enter。
2. 单击File > Add/Remove Snap-in。
3. 选择“证书”，并单击“添加”。



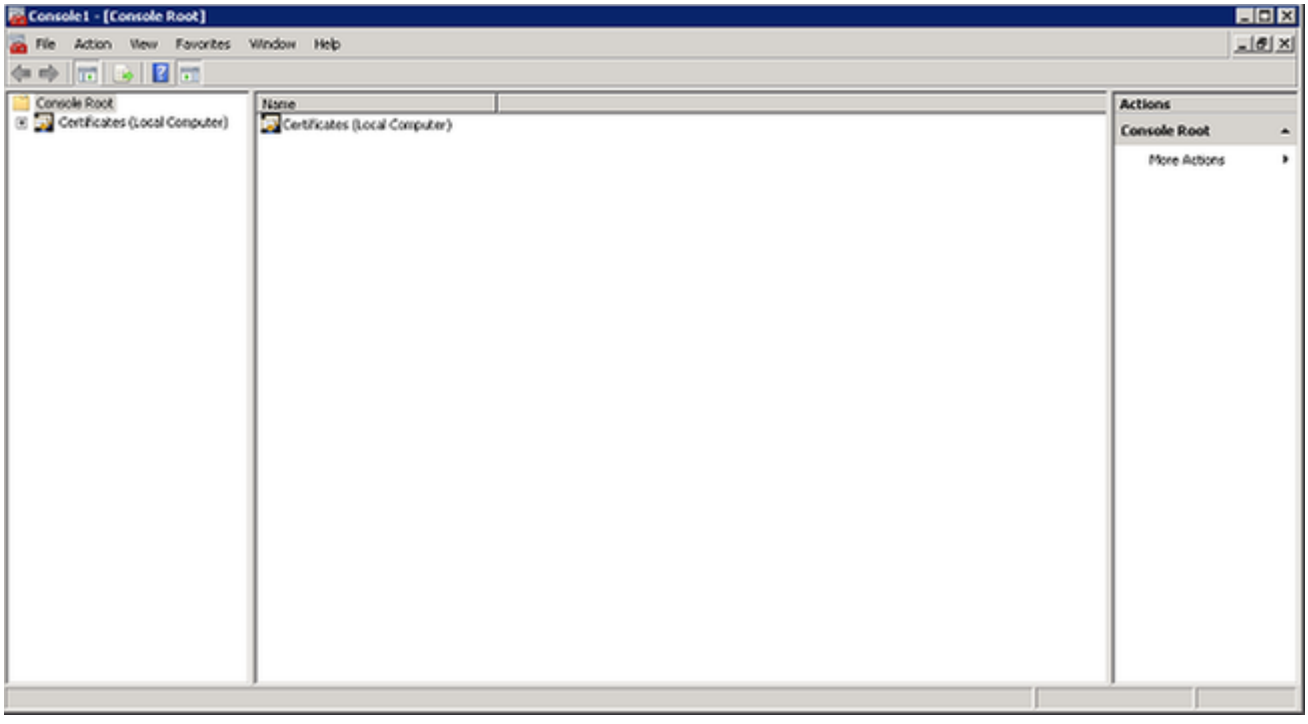
4. 选择计算机帐户，然后单击“下一步”。



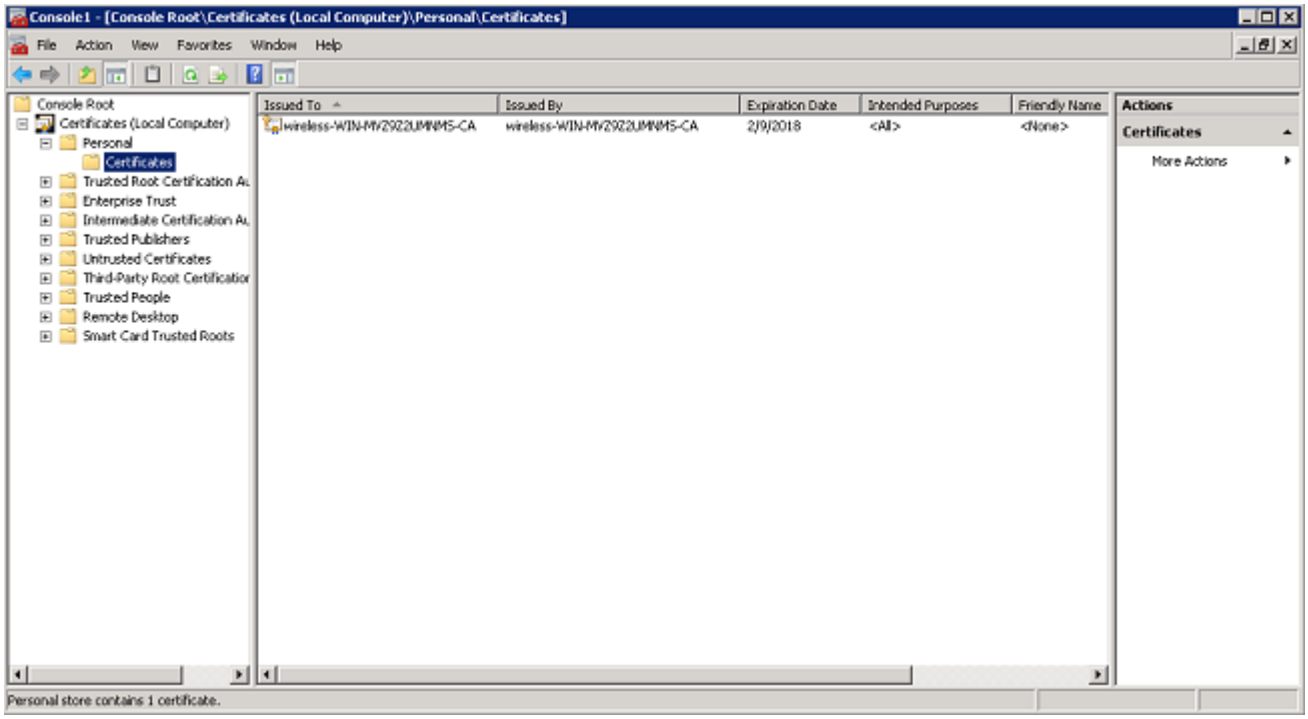
5. 选择Local Computer，然后单击Finish。



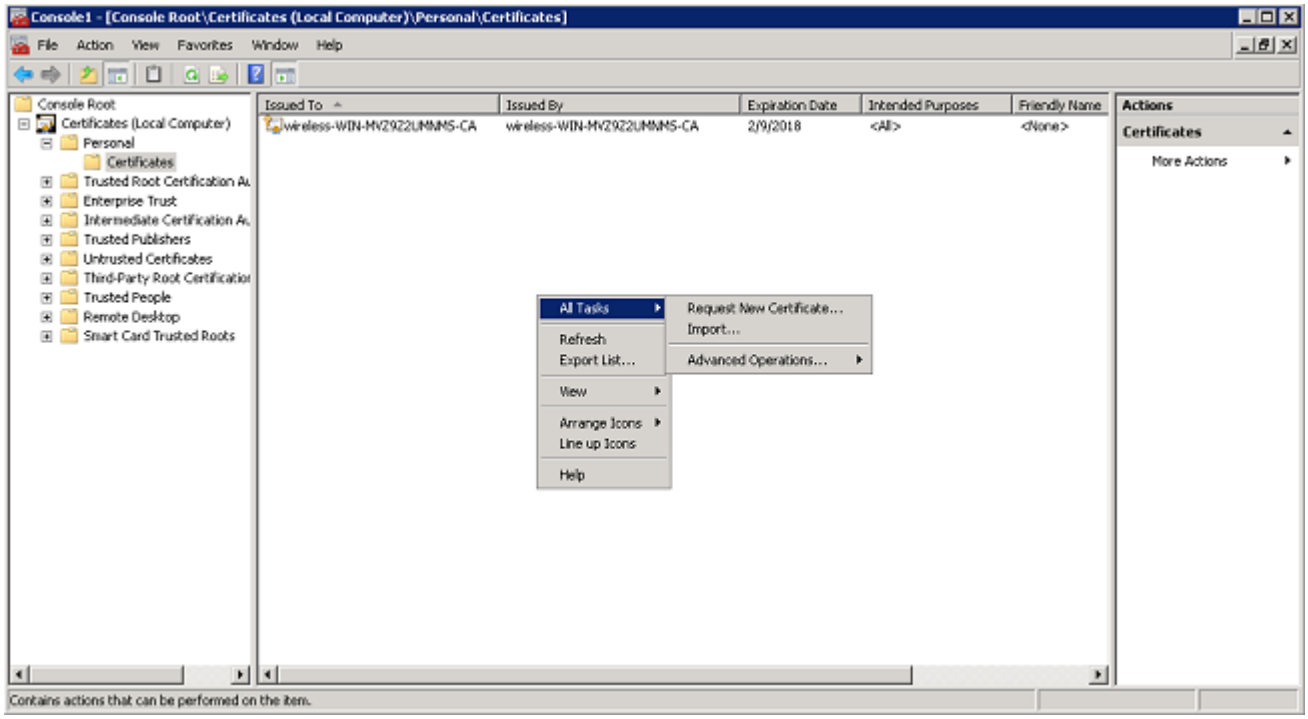
6. 单击OK返回到Microsoft管理控制台(MMC)。



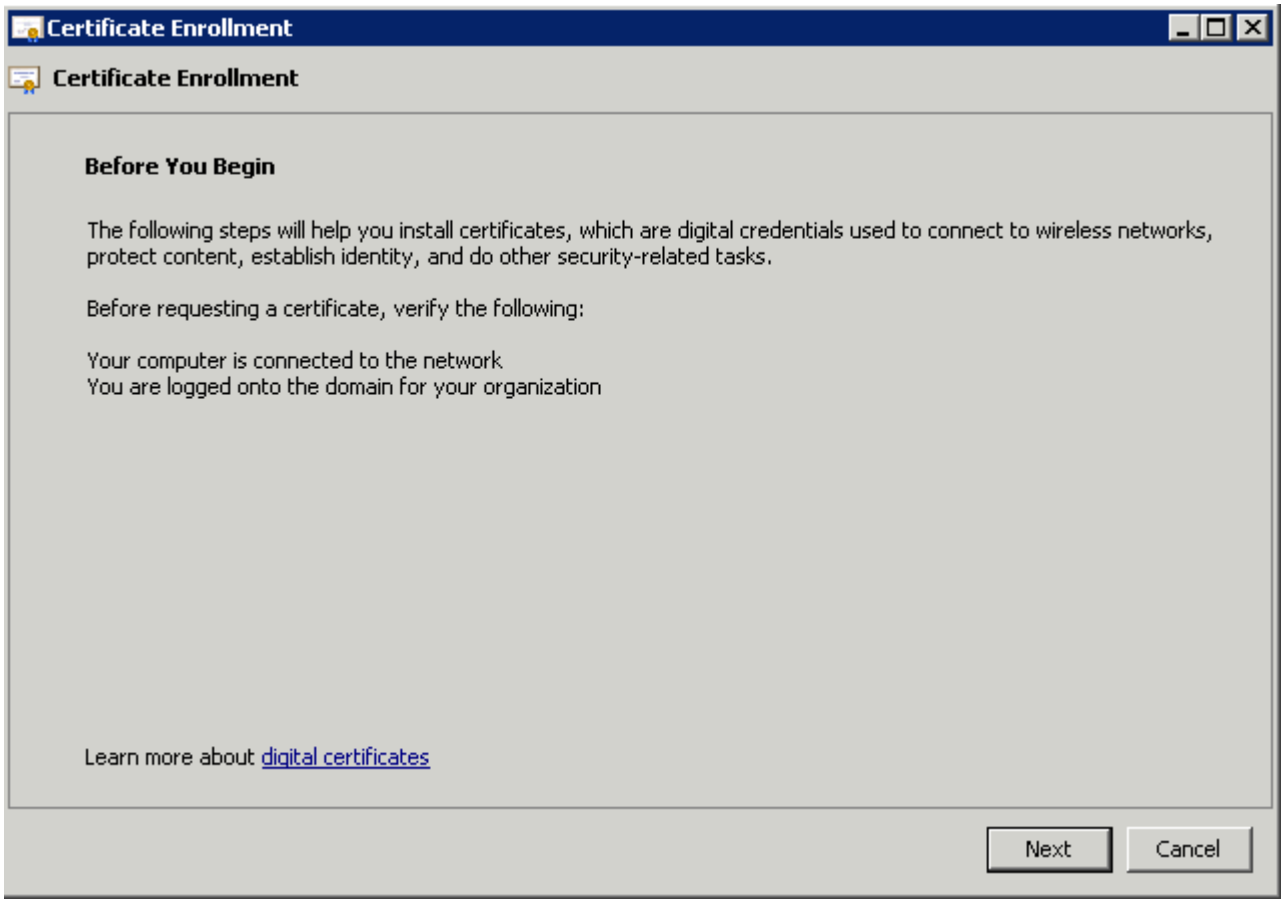
7. 展开Certificates(Local Computer)和Personal文件夹，然后单击Certificates。



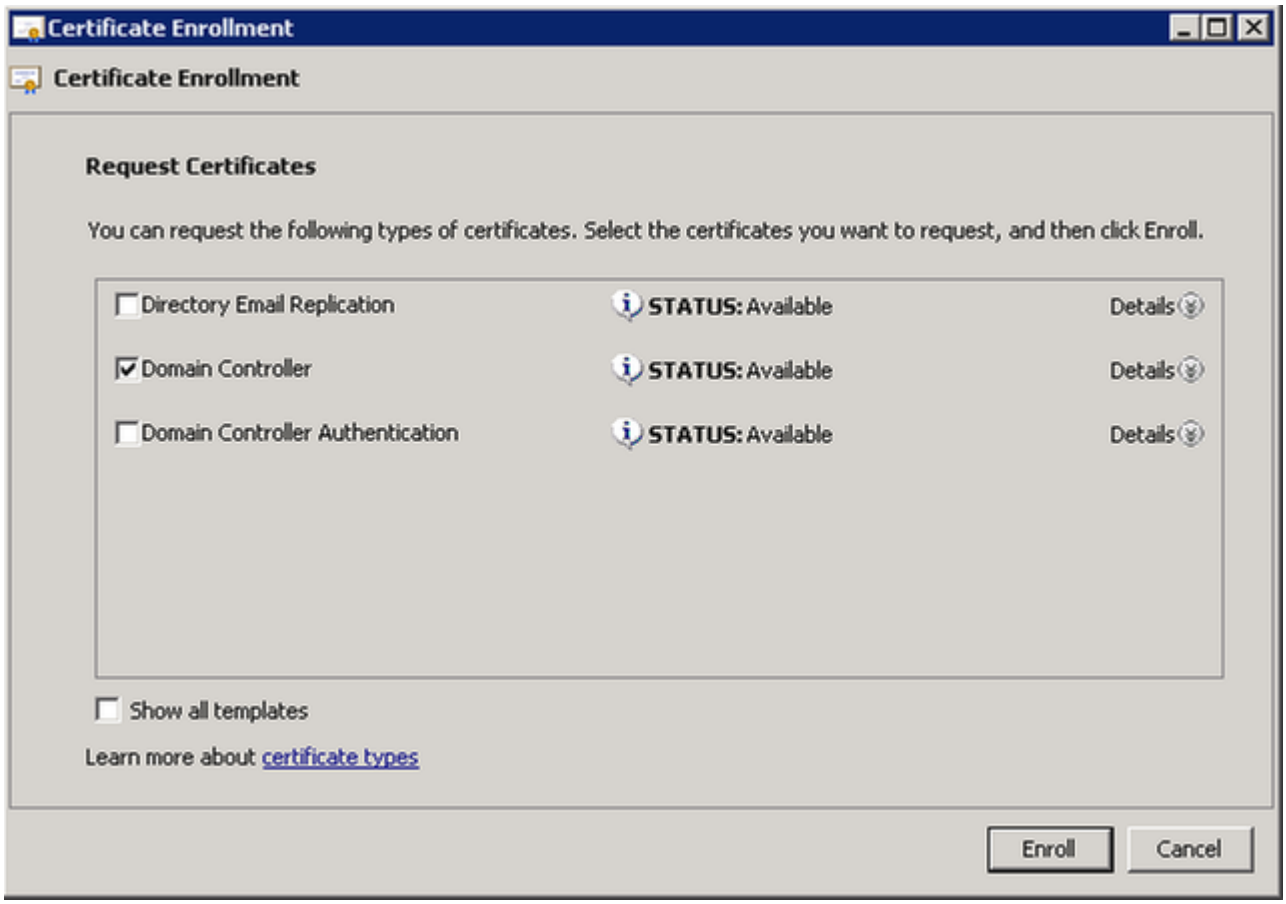
8. 在CA证书下方的空白处右键单击，然后选择所有任务>请求新证书。



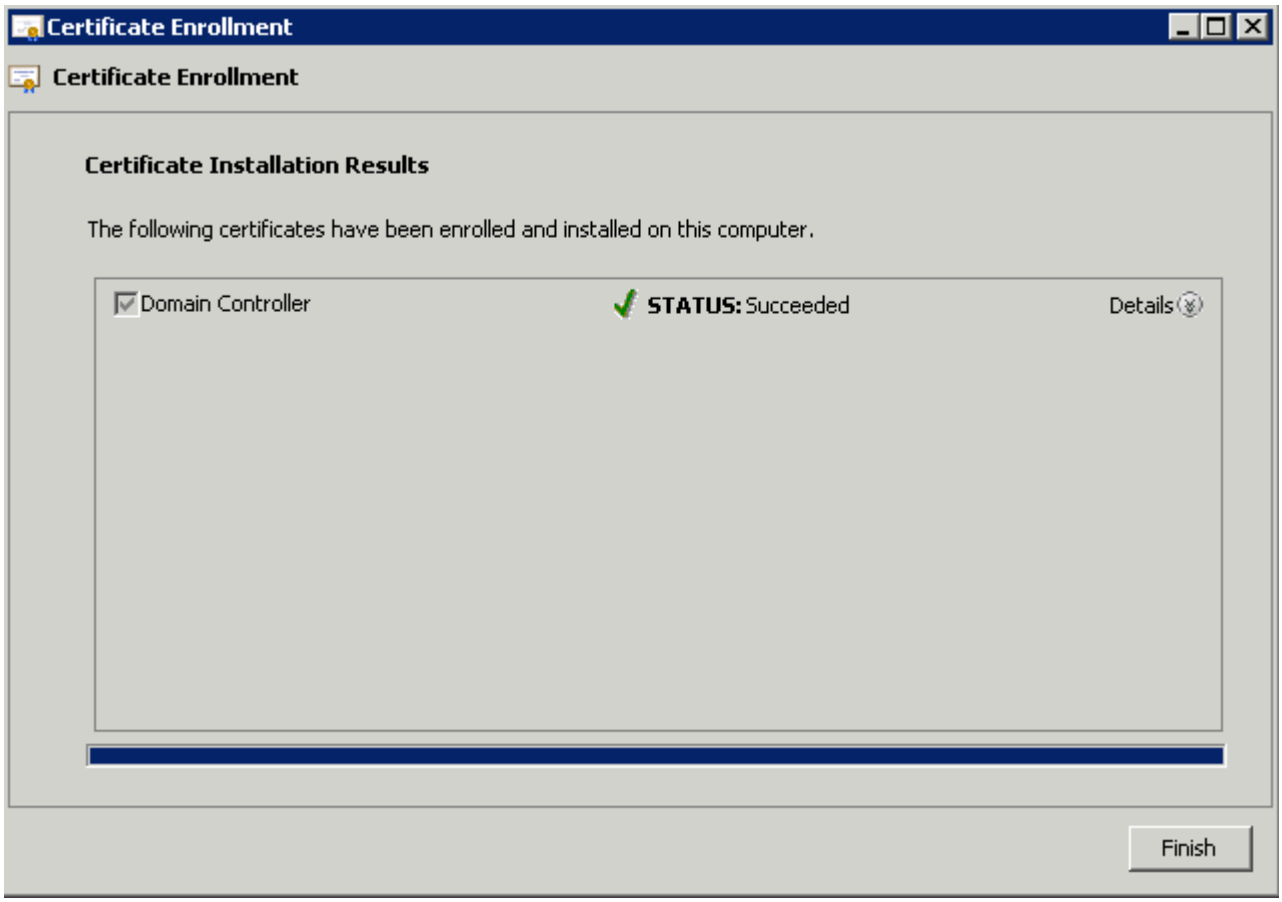
9. 单击 Next。



10. 选择Domain Controller，然后单击Enroll。

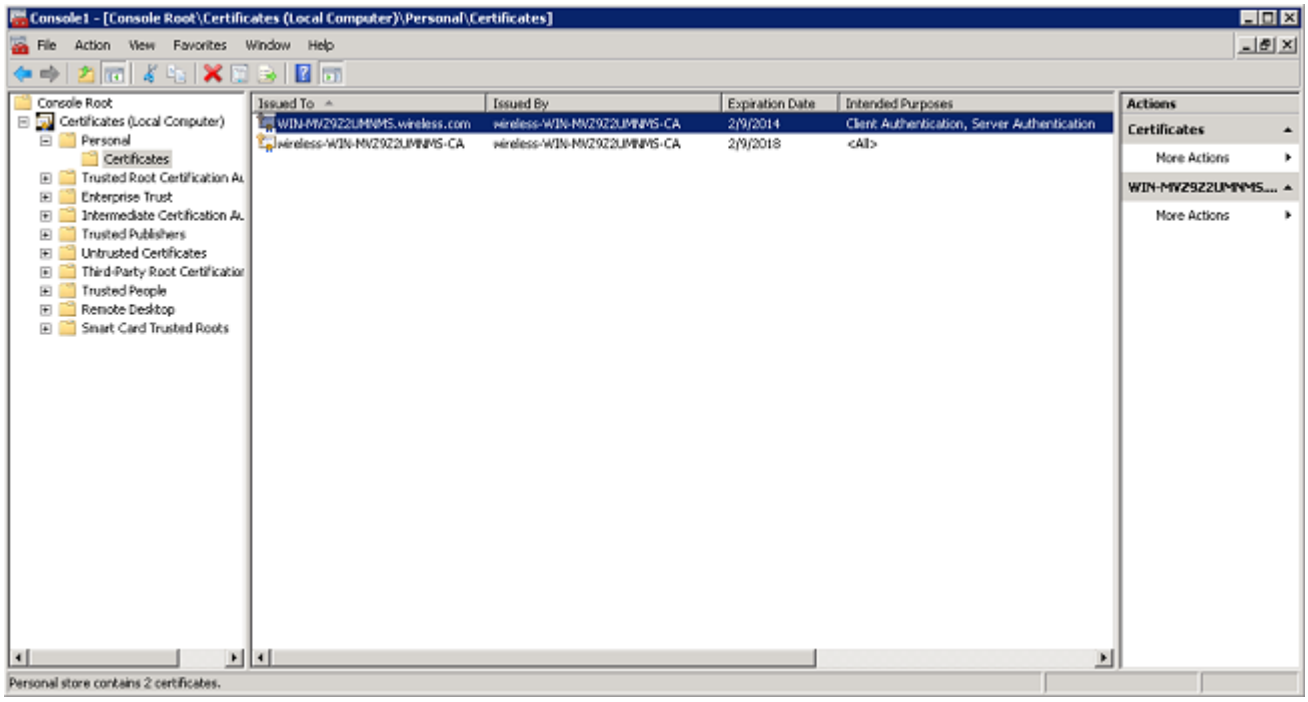


11. 安装证书后，单击Finish。



NPS证书现已安装。

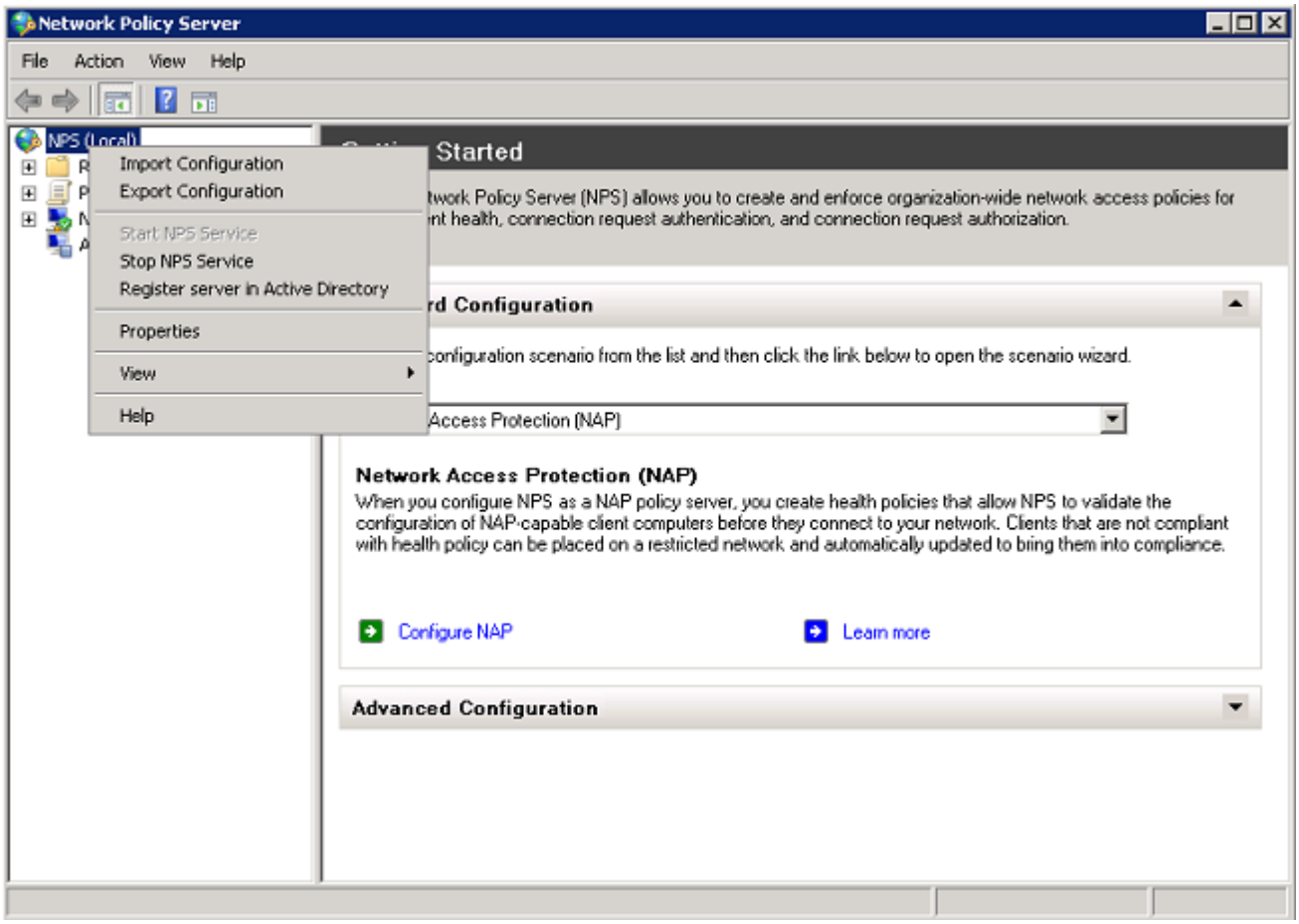
12. 确保证书的Intended Purpose显示为Client Authentication， Server Authentication。



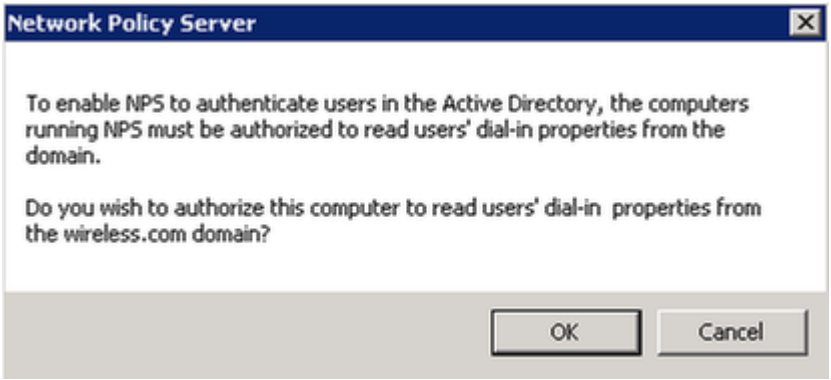
为PEAP-MS-CHAP v2身份验证配置网络策略服务器服务

要配置NPS进行身份验证，请完成以下步骤：

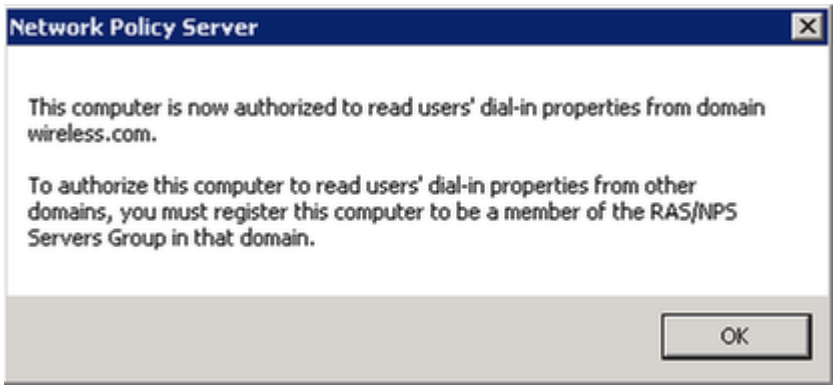
1. 单击开始> Administrative Tools> Network Policy Server。
2. 右键单击NPS（本地），然后选择在Active Directory中注册服务器。



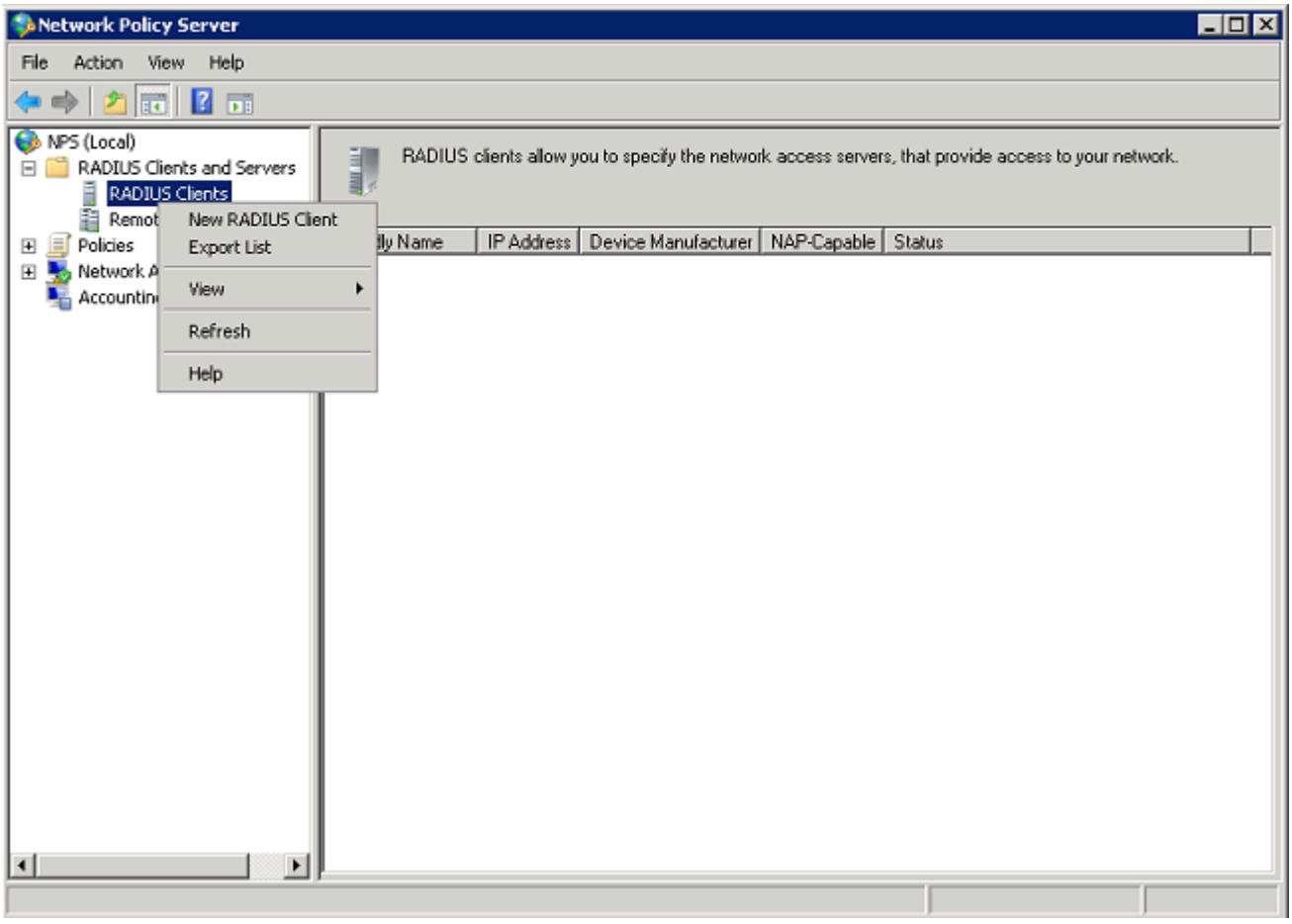
3. Click OK.



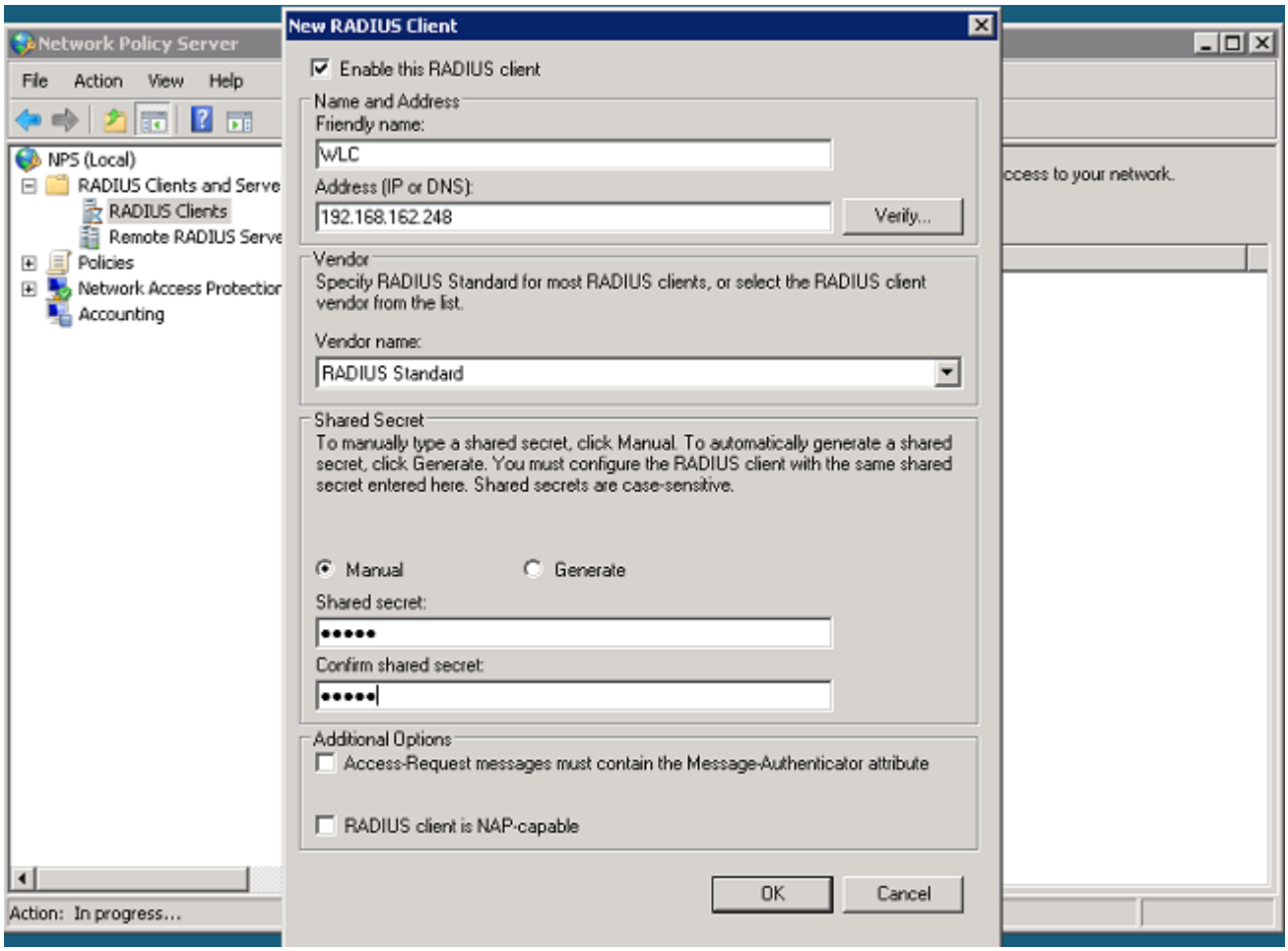
4. Click OK.



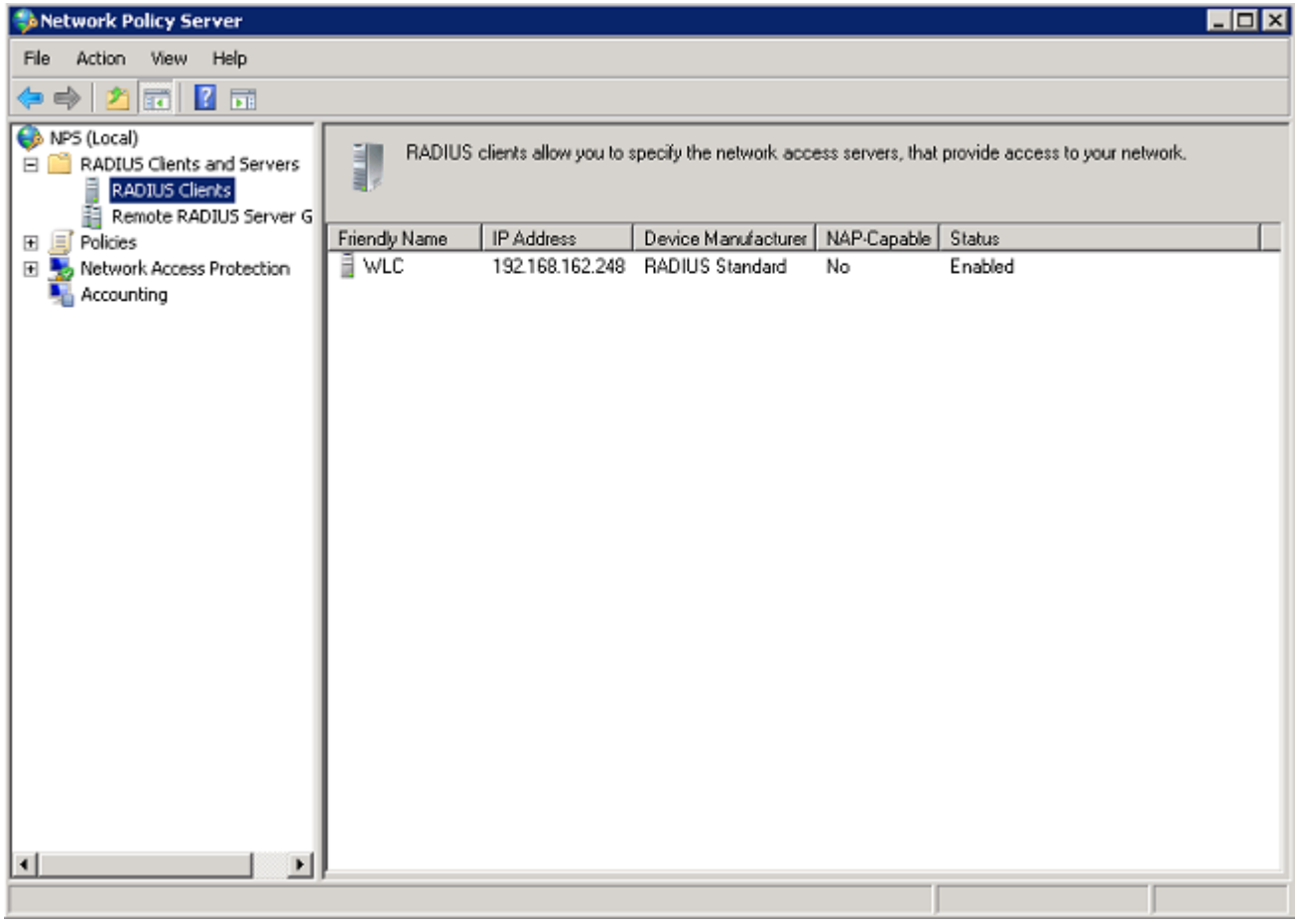
5. 将无线局域网控制器添加为NPS上的身份验证、授权和记帐(AAA)客户端。
6. 展开RADIUS客户端和服务器。右键单击 RADIUS 客户端，然后选择“新建 RADIUS 客户端”。



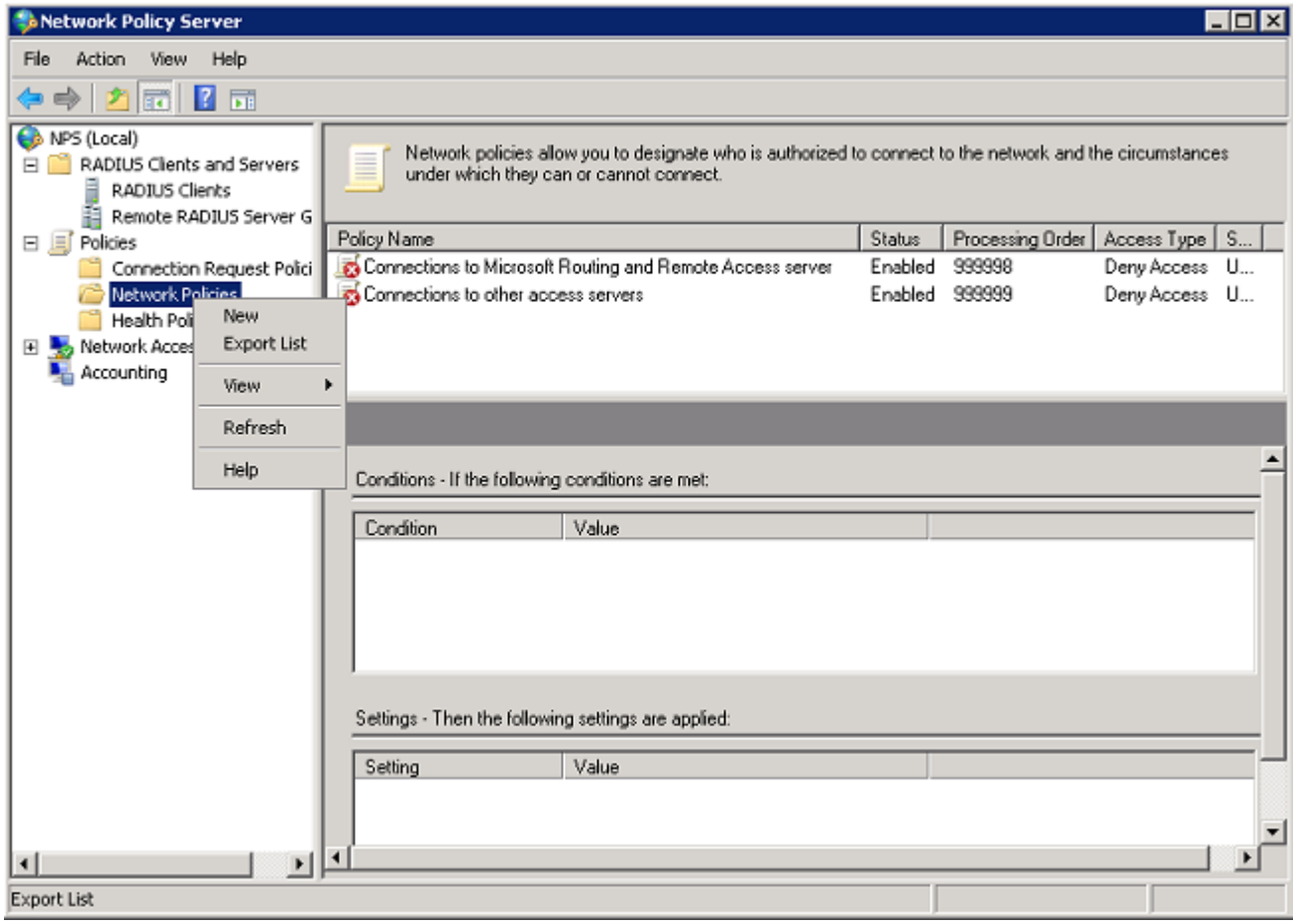
7. 输入Friendly name（本示例中为WLC）、WLC的管理IP地址（本示例中为192.168.162.248）和共享密钥。相同的共享密钥用于配置WLC。



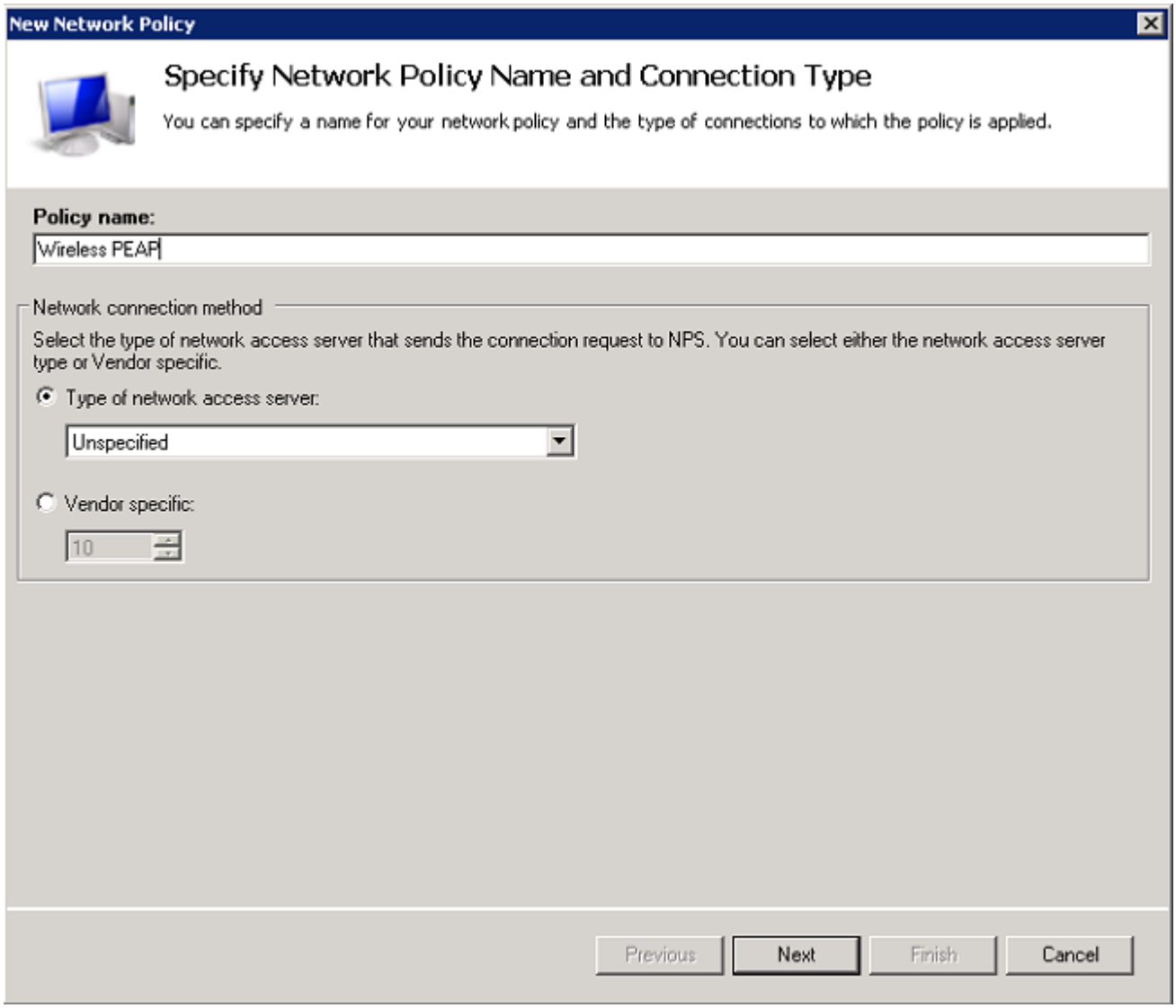
8. 单击OK返回上一屏幕。



9. 为无线用户创建新的网络策略。展开Policies，右键单击Network Policies，然后选择New。

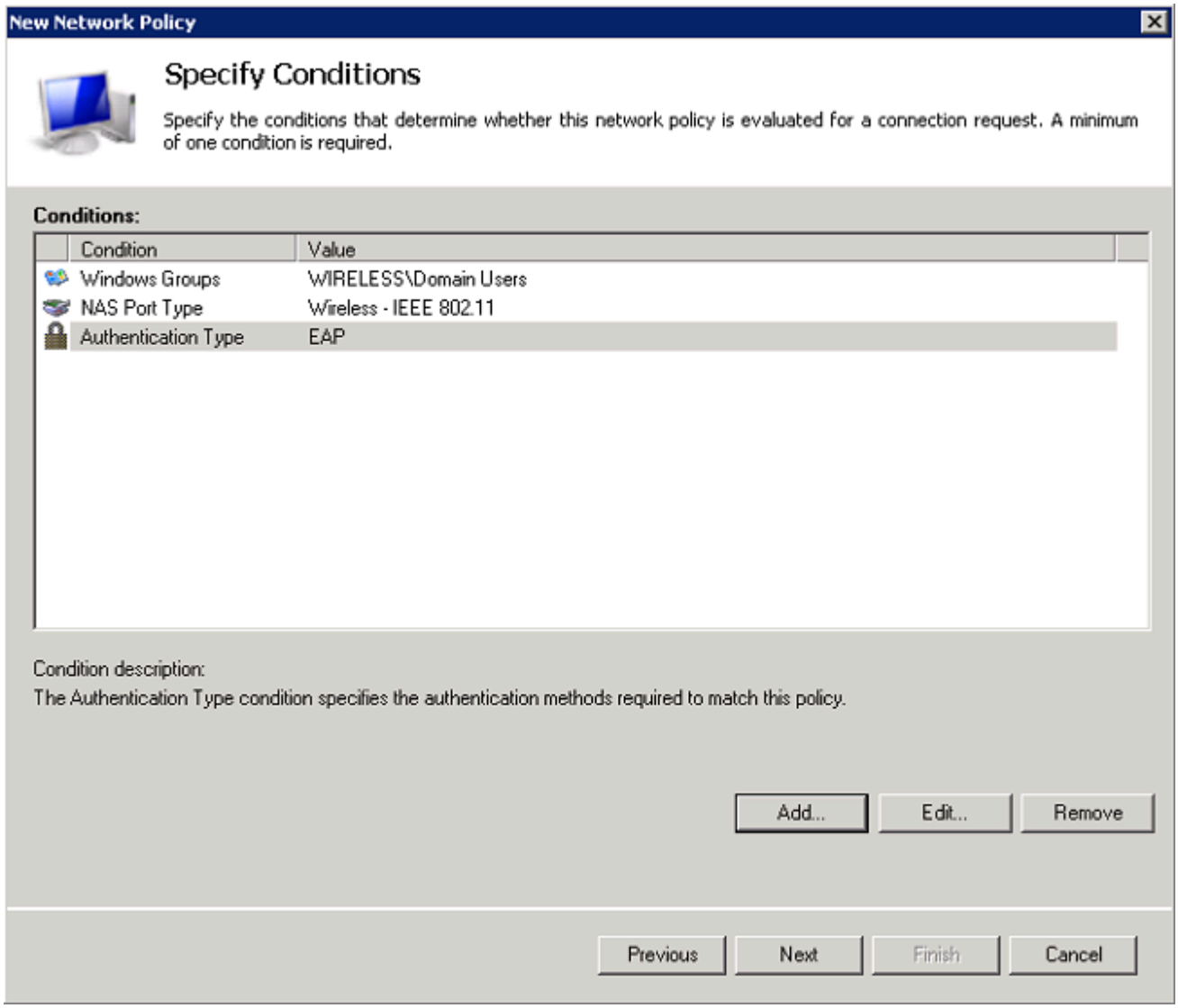


10. 输入此规则的策略名称（本示例中为Wireless PEAP），然后点击Next。

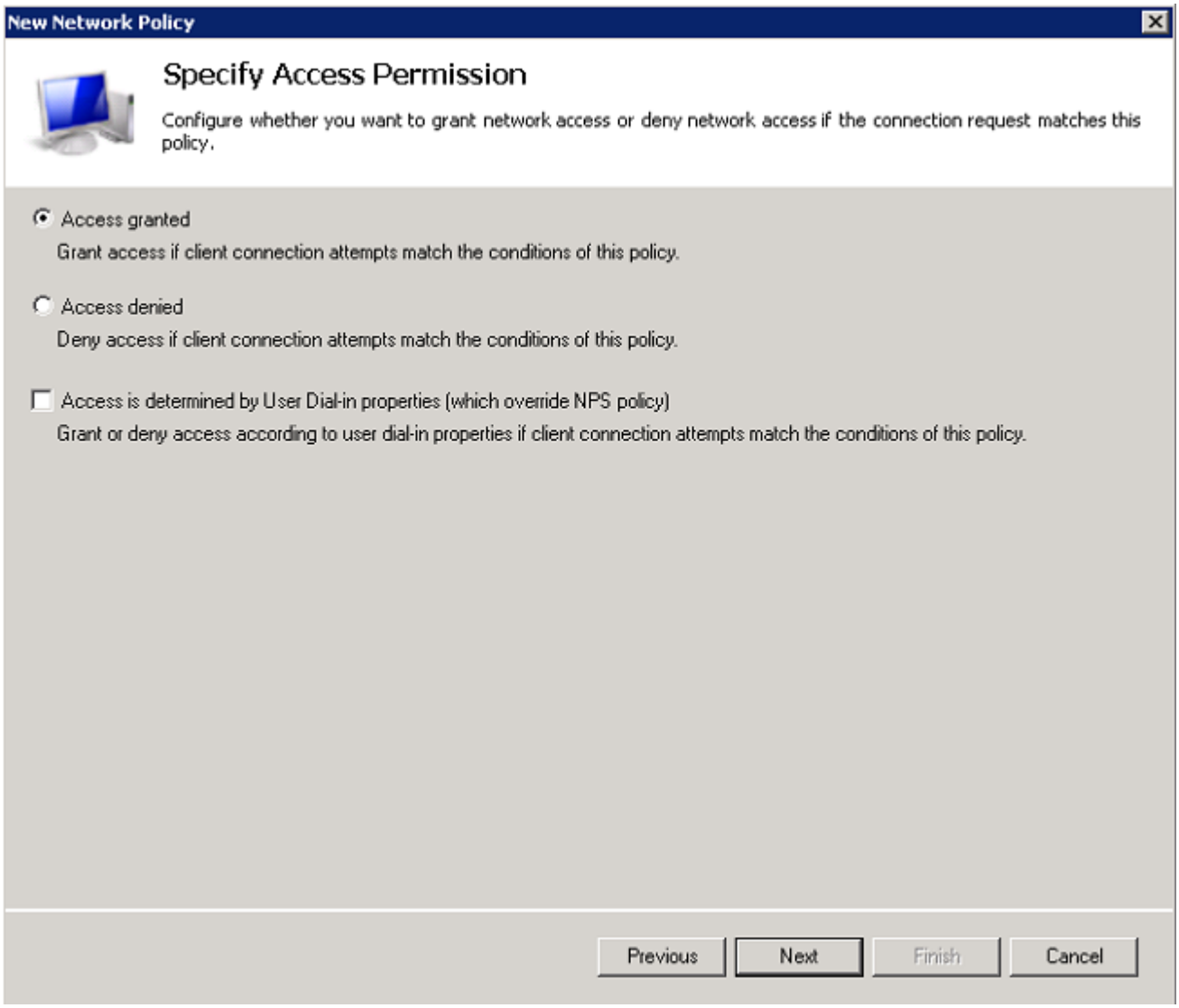


11. 要使此策略仅允许无线域用户，请添加以下三个条件，然后单击下一步:

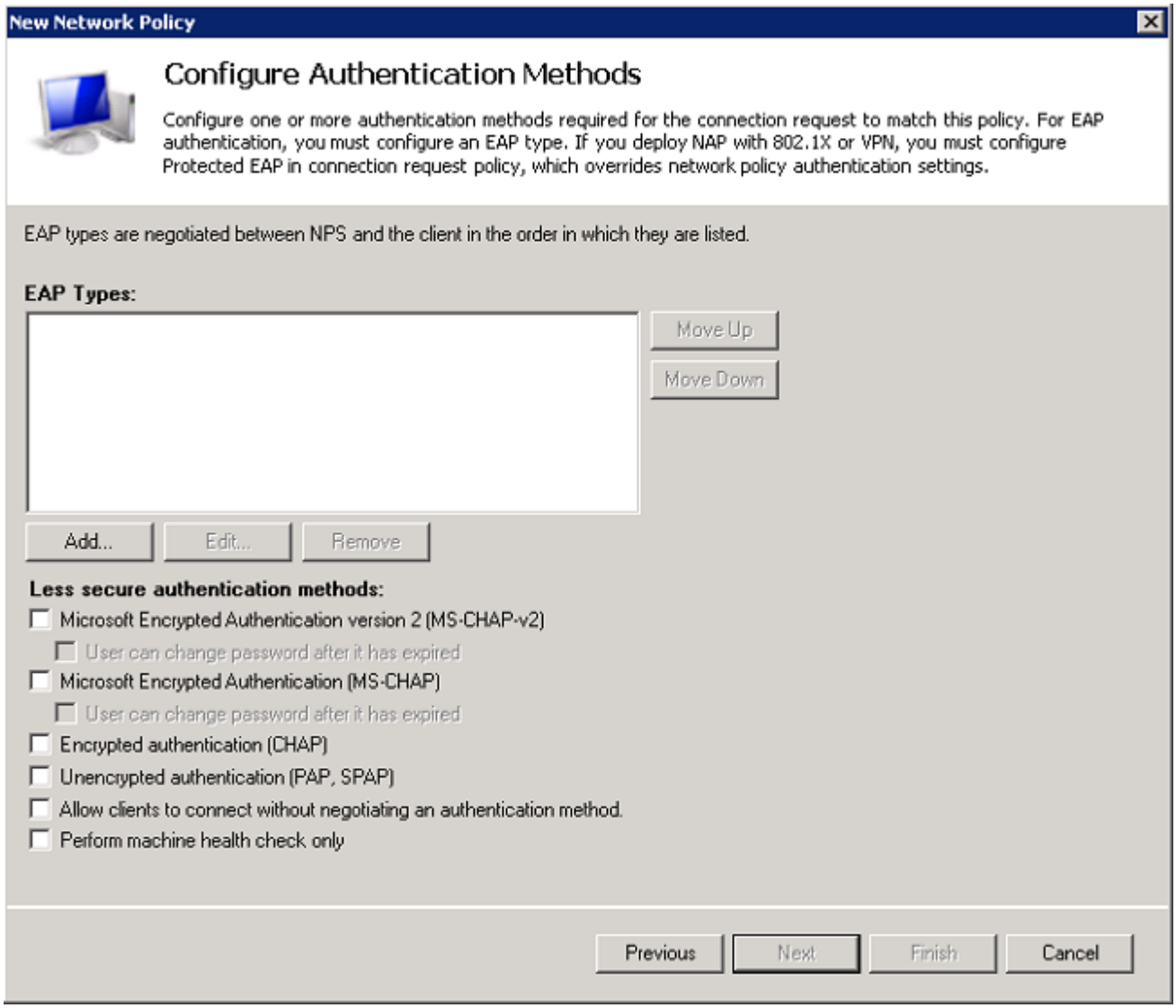
- Windows组 — 域用户
- NAS端口类型 — 无线 — IEEE 802.11
- 身份验证类型 — EAP



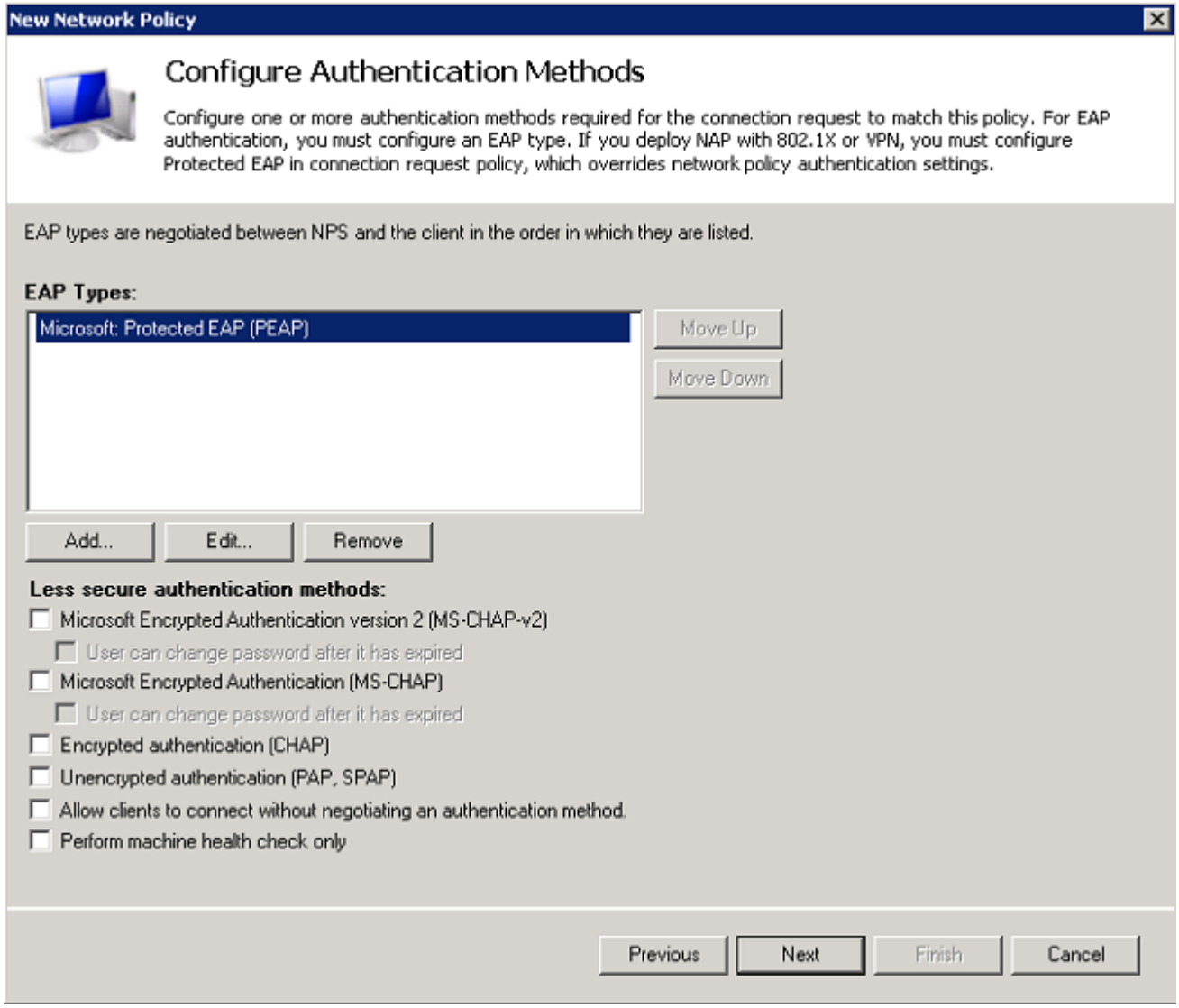
12. 单击Access granted以授予与此策略匹配的连接尝试，然后单击Next。



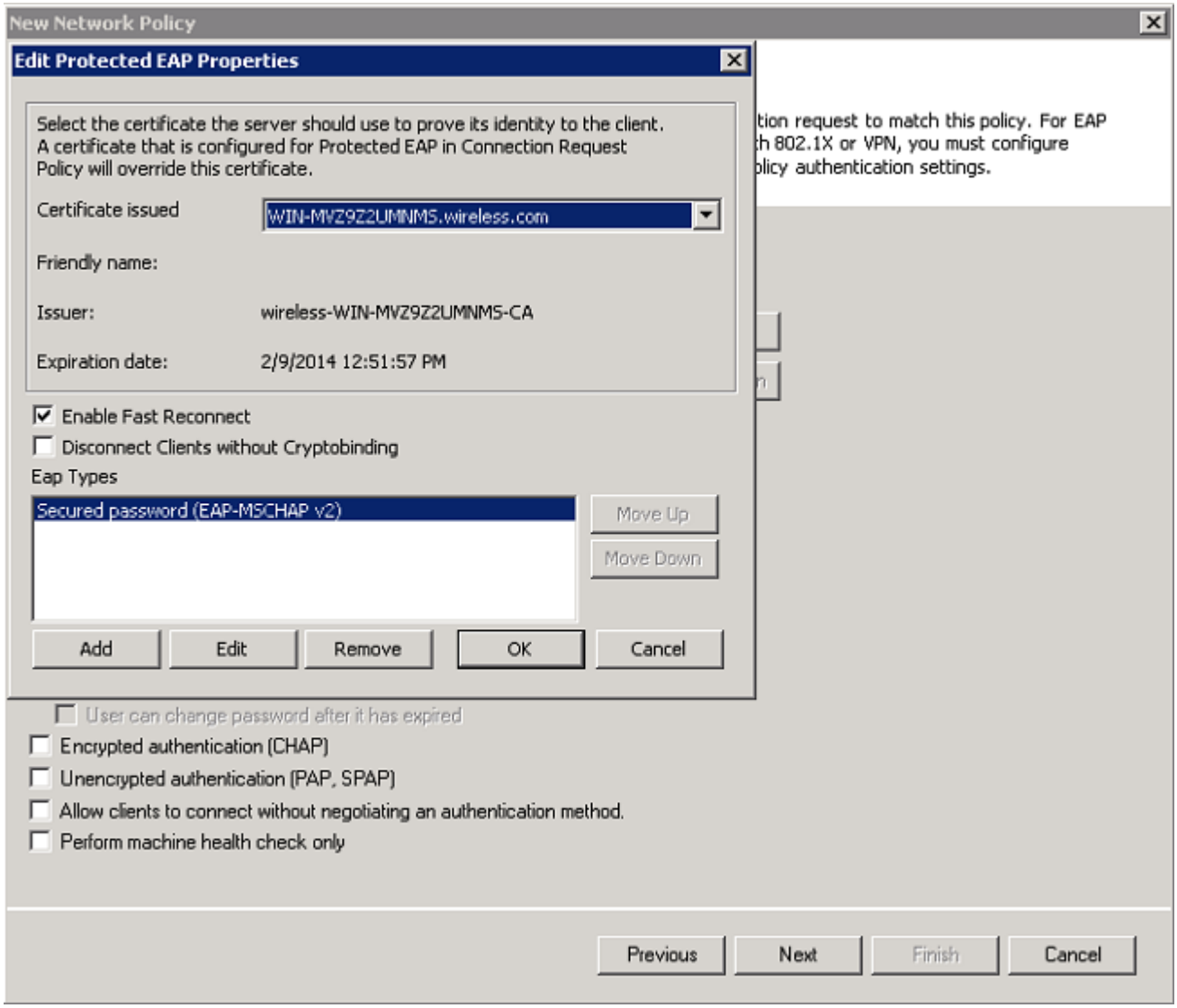
13. 在Less secure authentication methods下禁用所有身份验证方法。



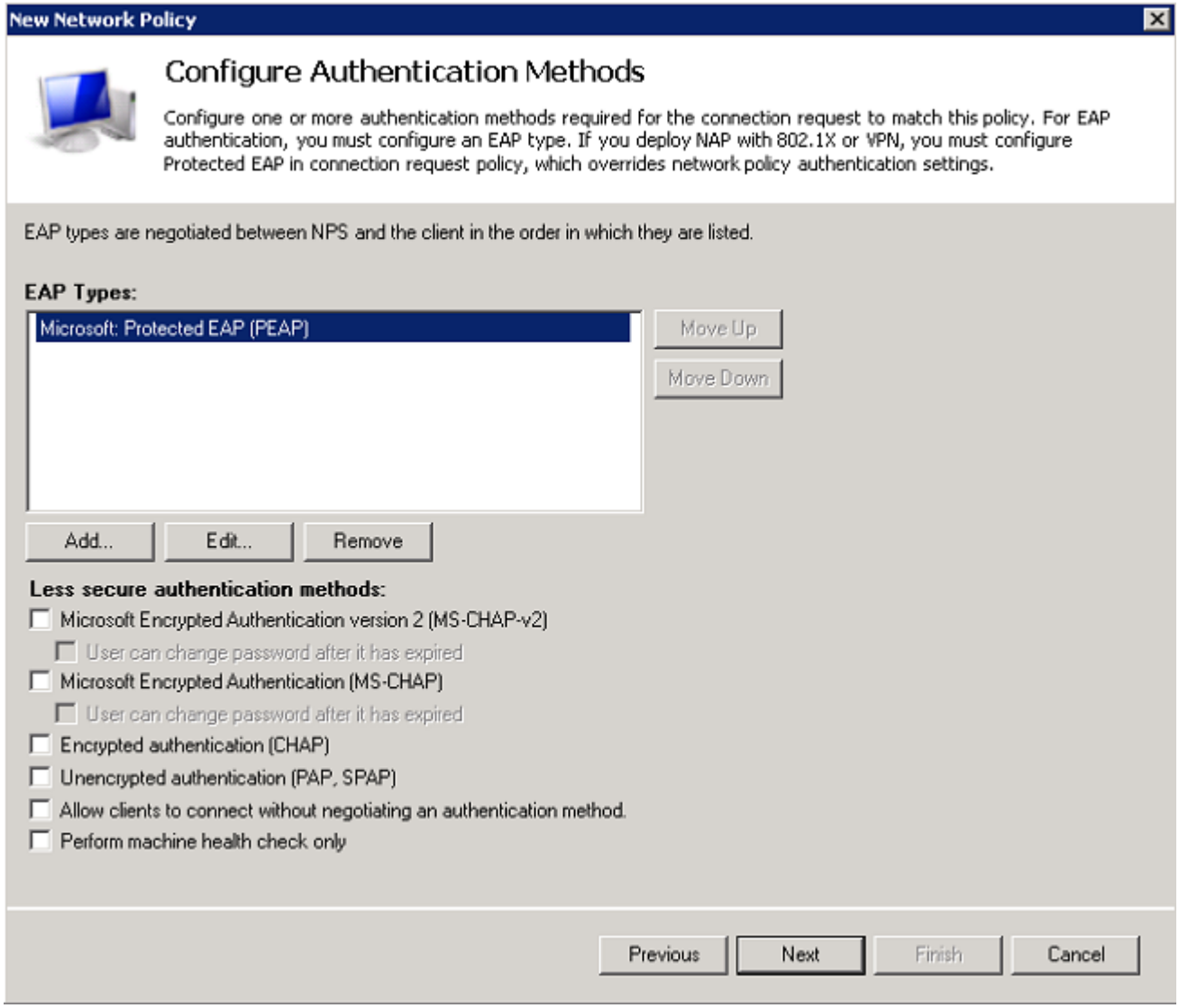
14. 单击Add，选择PEAP，然后单击OK以启用PEAP。



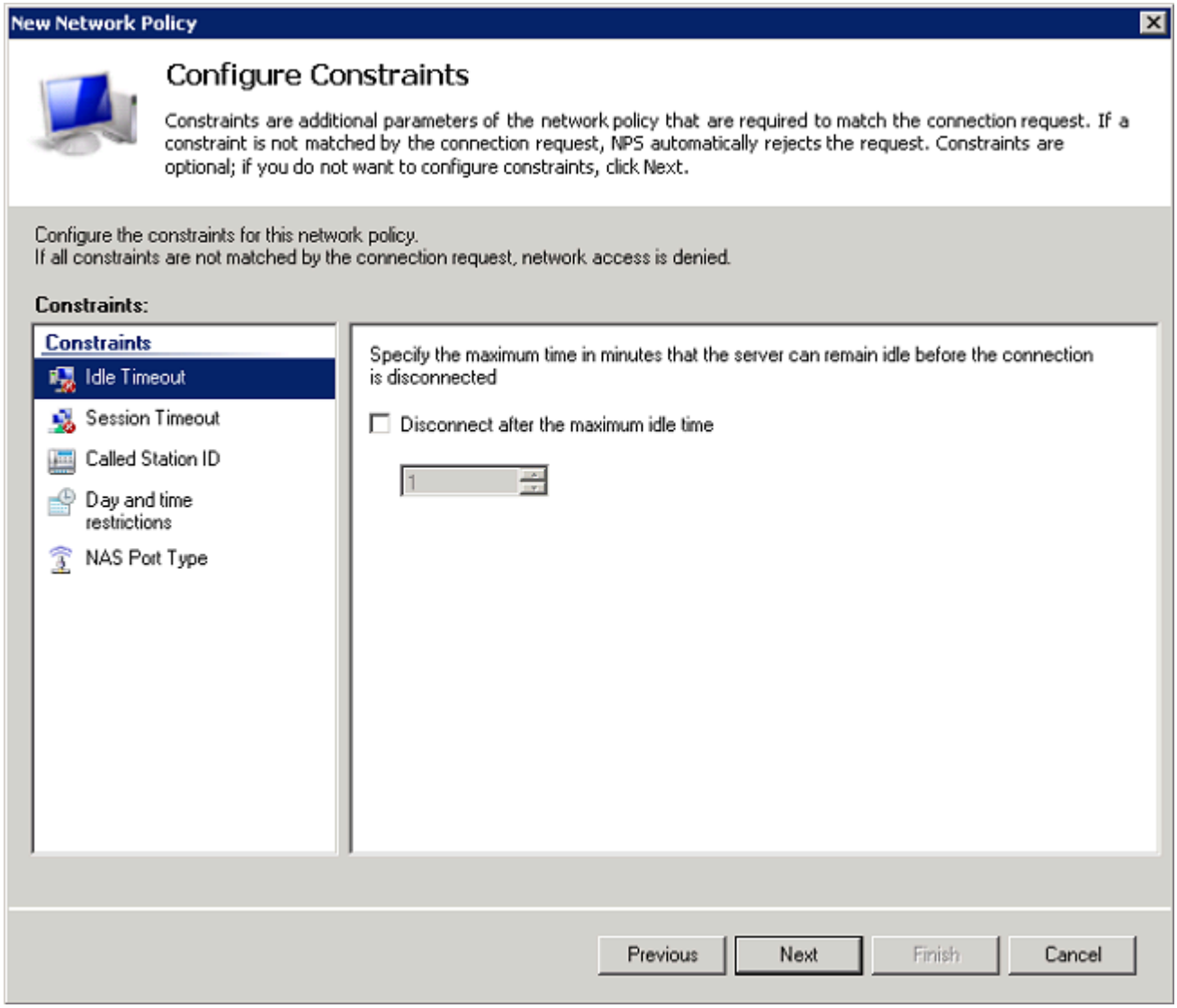
15. 选择Microsoft:受保护的EAP(PEAP)，然后点击Edit。确保在Certificate issued下拉列表中选择之前创建的域控制器证书，然后单击OK。


New Network Policy
Edit Protected EAP Properties
Select the certificate the server should use to prove its identity to the client.
A certificate that is configured for Protected EAP in Connection Request
Policy will override this certificate.
Certificate issued
WIN-MVZ9Z2UMNMS.wireless.com
Friendly name:
Issuer:
wireless-WIN-MVZ9Z2UMNMS-CA
Expiration date:
2/9/2014 12:51:57 PM
Enable Fast Reconnect
Disconnect Clients without Cryptobinding
Eap Types
Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add
Edit
Remove
OK
Cancel
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.
Perform machine health check only
Previous
Next
Finish
Cancel

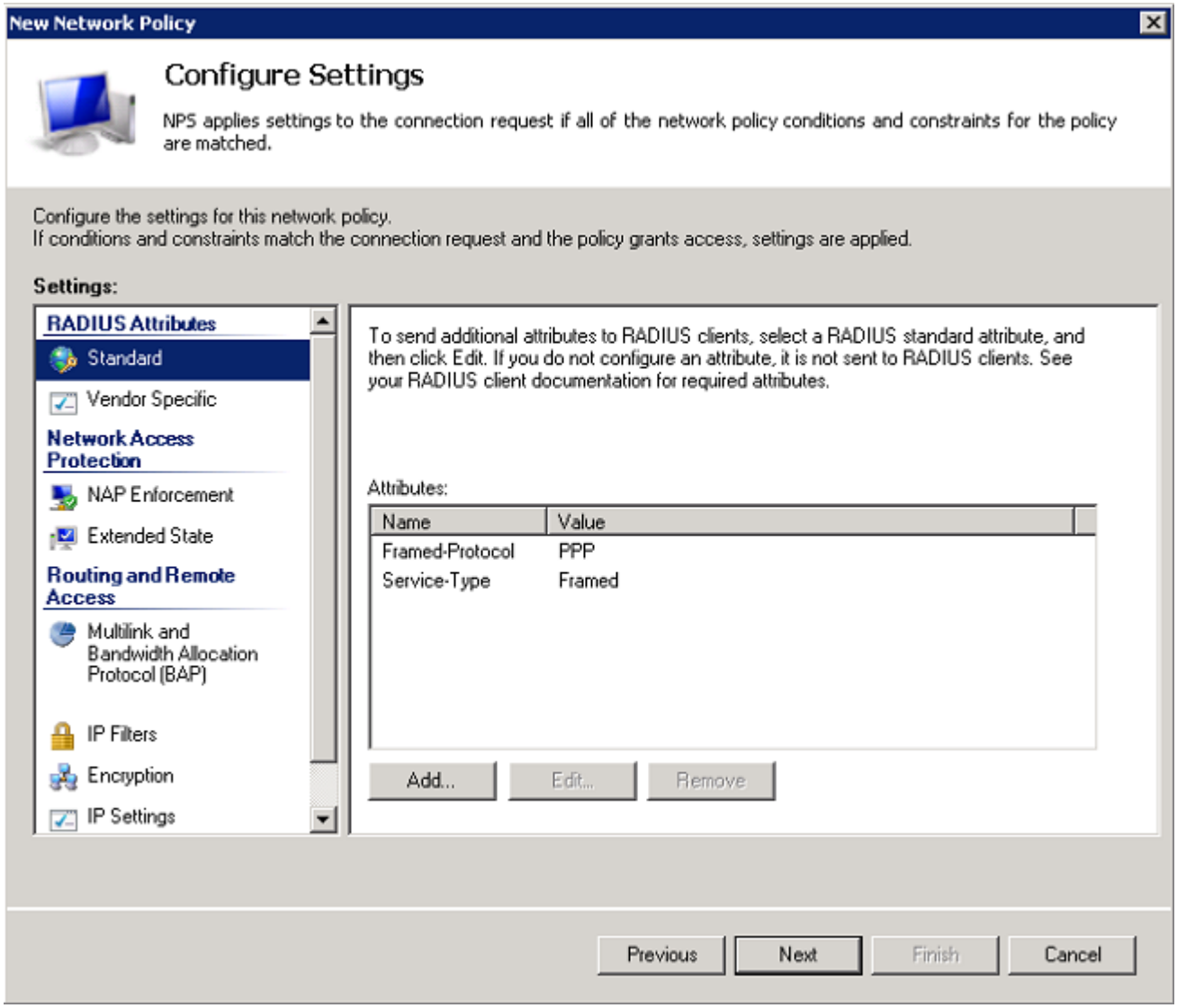
16. 单击 Next。


New Network Policy
Configure Authentication Methods
Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Protected EAP (PEAP)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method.
Perform machine health check only
Previous
Next
Finish
Cancel

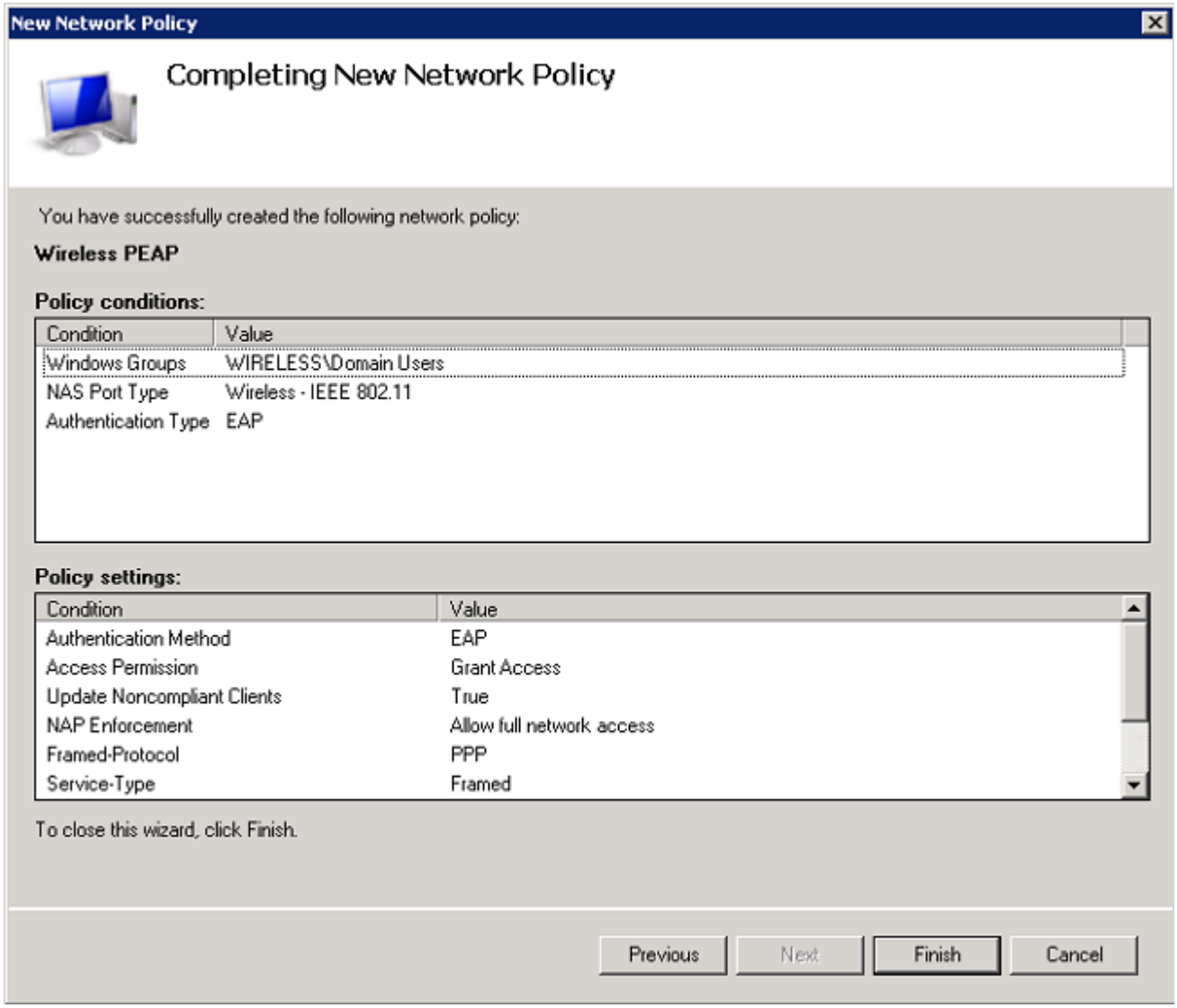
17. 单击 Next。


New Network Policy
Configure Constraints
Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected
Disconnect after the maximum idle time
1
Previous
Next
Finish
Cancel

18. 单击 Next。


New Network Policy
Configure Settings
NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Network Access Protection
NAP Enforcement
Extended State
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Framed-Protocol
PPP
Service-Type
Framed
Add...
Edit...
Remove
Previous
Next
Finish
Cancel

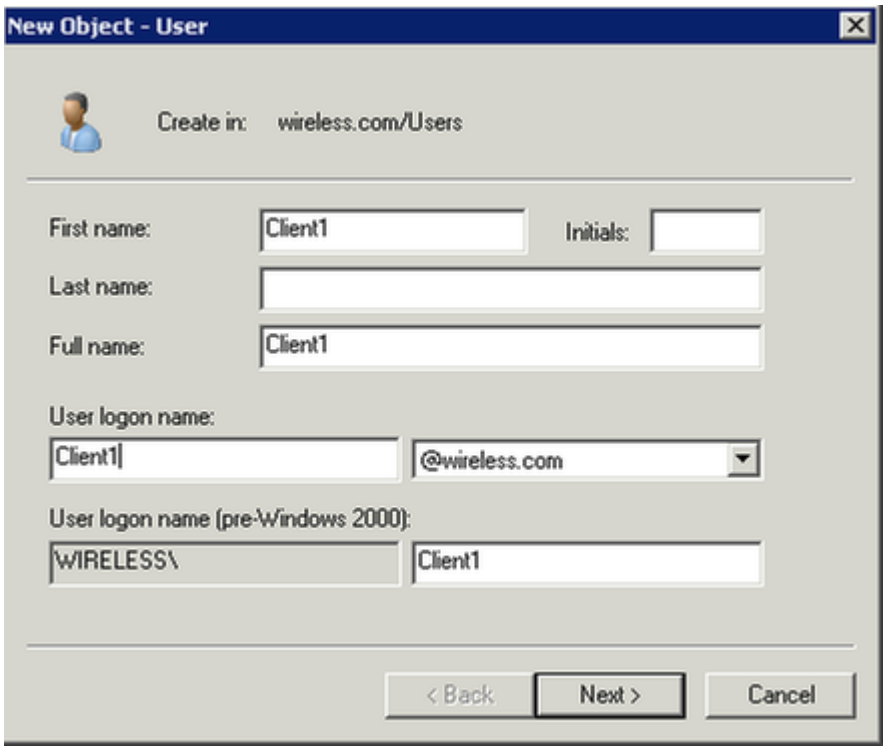
19. 单击 完成。



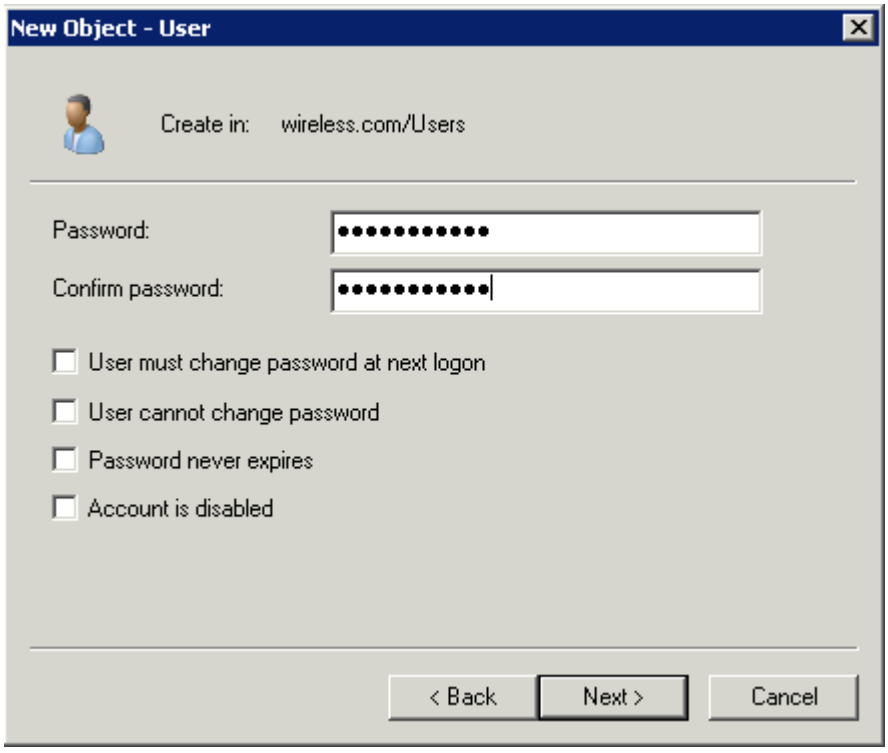
将用户添加到 Active Directory

在本示例中，用户数据库在Active Directory上维护。完成以下步骤以将用户添加到Active Directory数据库：

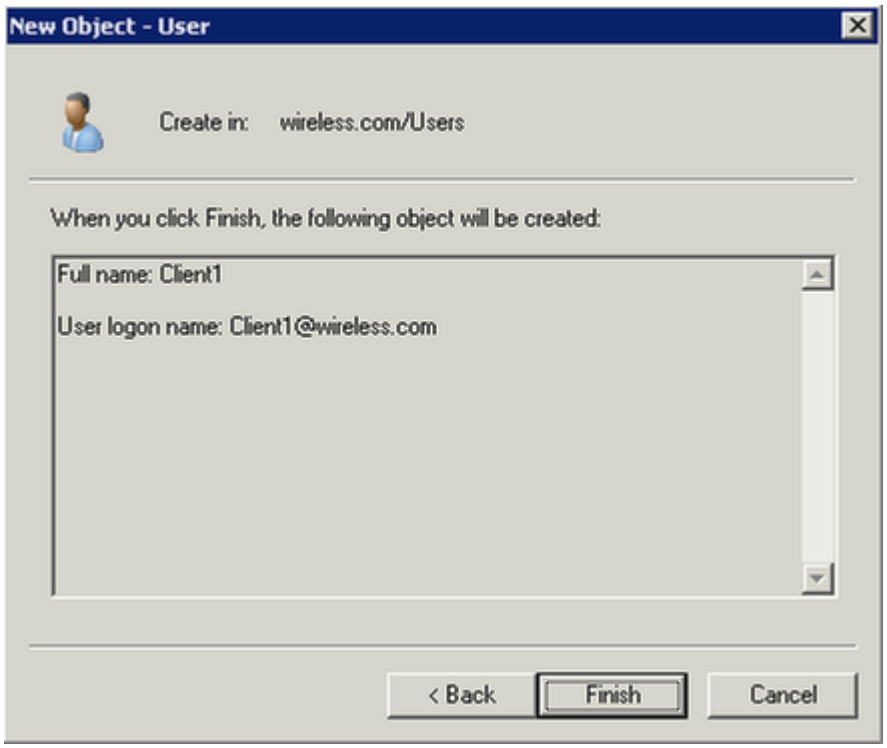
1. 打开 Active Directory 用户和计算机。单击开始> 管理工具> Active Directory用户和计算机。
2. 在Active Directory用户和计算机控制台树中，展开域，右键单击Users> New，然后选择User。
3. 在“新建对象 — 用户”对话框中，输入无线用户的名称。此示例在First name字段中使用名称Client1，在User logon name字段中使用名称Client1。单击 Next。



4. 在New Object - User对话框中，在Password和Confirm password字段中输入您选择的密码。确保未选中User must change password at next logon复选框，然后单击Next。



5. 在“新建对象 – 用户”对话框中，单击完成。



6. 重复步骤 2 到步骤 4，以便创建更多用户帐户。

配置无线局域网控制器和LAP

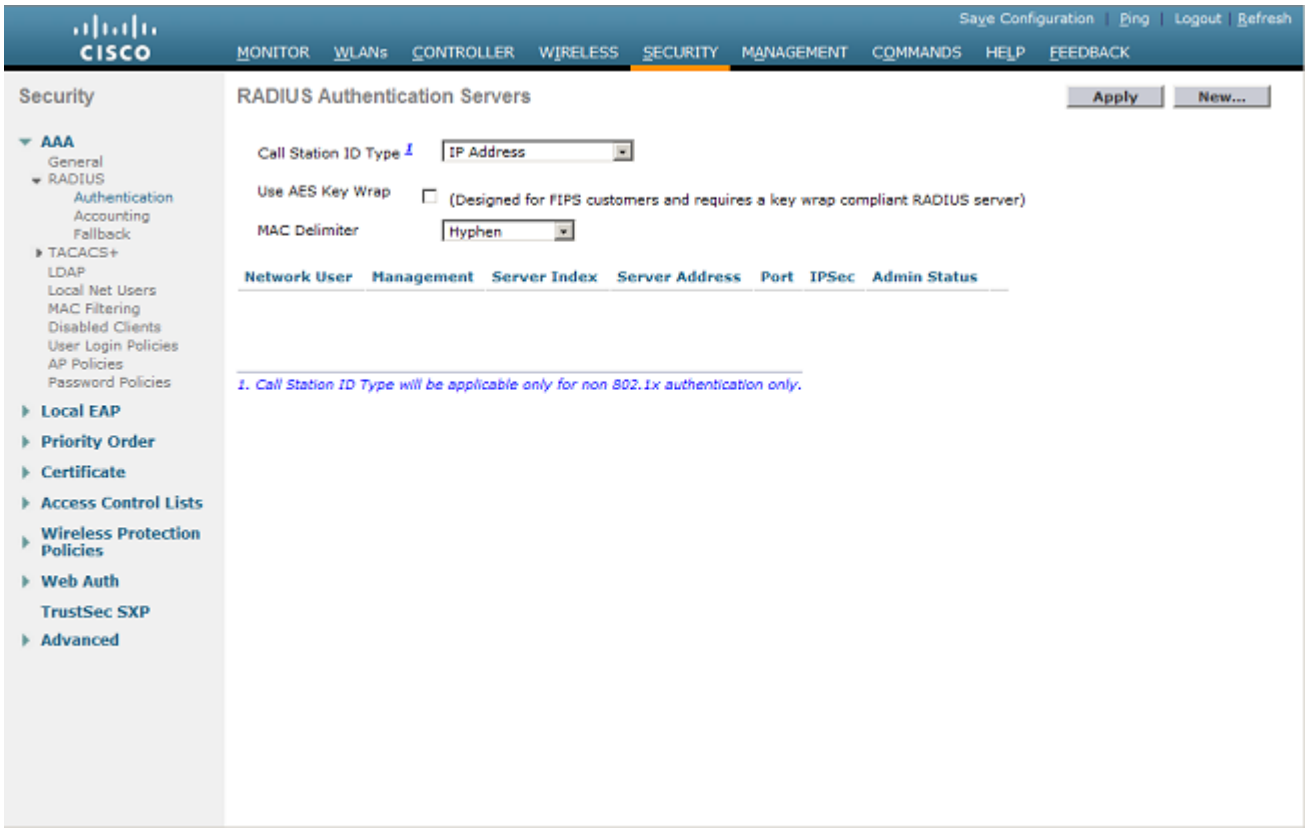
为此设置配置无线设备（无线局域网控制器和LAP）。

为RADIUS身份验证配置WLC

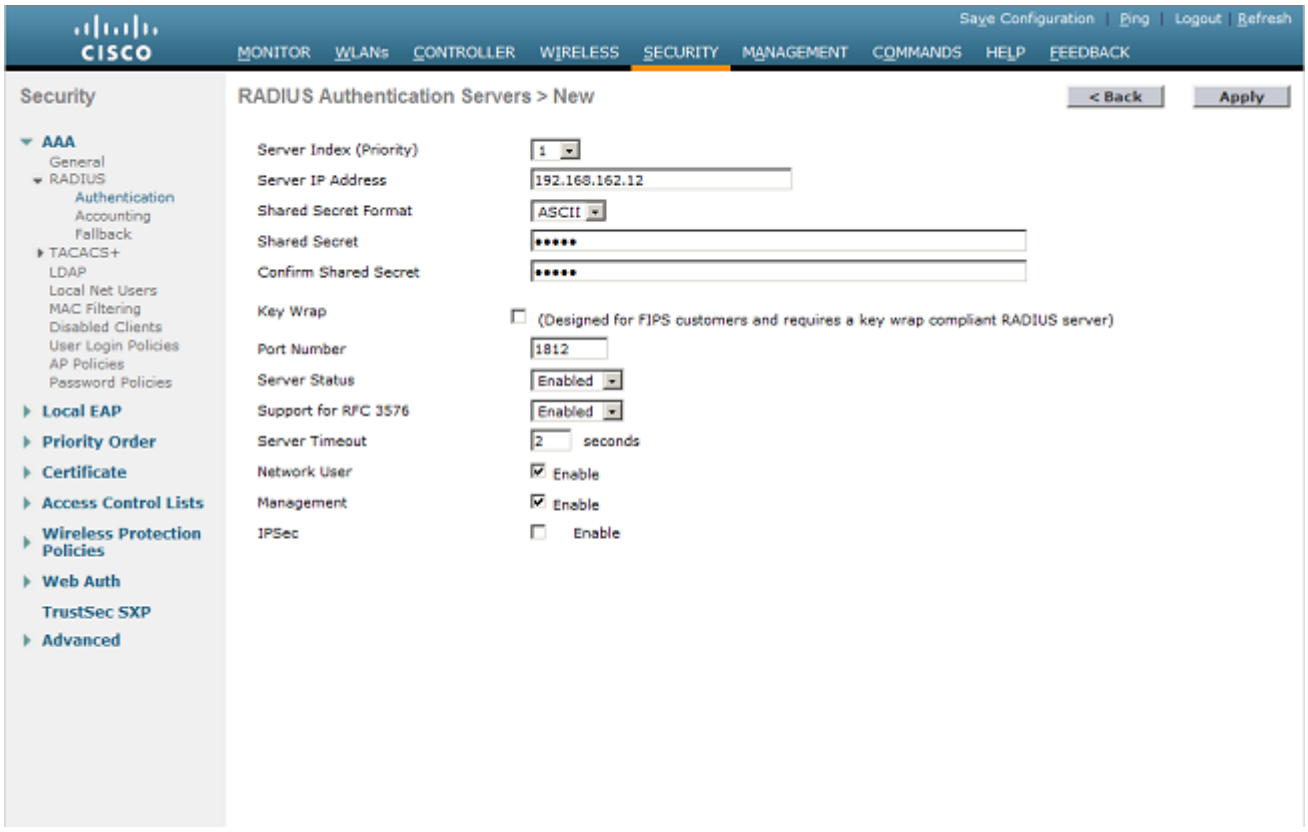
将WLC配置为使用NPS作为身份验证服务器。必须配置WLC以将用户凭证转发到外部RADIUS服务器。然后，外部 RADIUS 服务器验证用户凭证，并向无线客户端提供访问权限。

要在Security > RADIUS Authentication页中将NPS添加为RADIUS服务器，请完成以下步骤：

1. 从控制器接口选择Security> RADIUS > Authentication，以显示RADIUS Authentication Servers页面。单击New以定义RADIUS服务器。



2. 定义RADIUS服务器参数。这些参数包括 RADIUS 服务器的 IP 地址、共享密钥、端口号和服务器状态。Network User和Management复选框确定基于RADIUS的身份验证是否适用于管理和网络（无线）用户。本示例使用NPS作为IP地址为192.168.162.12的RADIUS服务器。单击Apply。



为客户端配置 WLAN

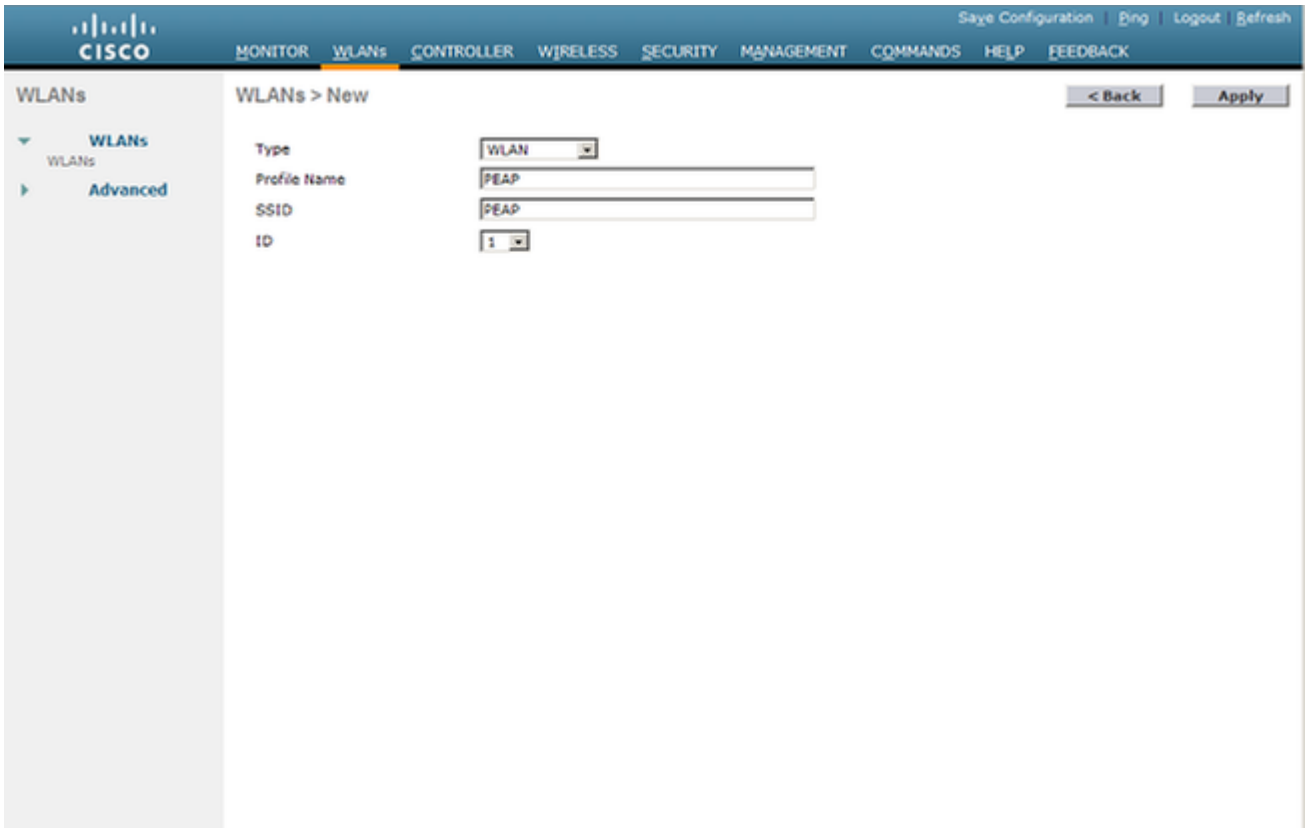
配置无线客户端连接的服务集标识符(SSID)(WLAN)。本示例中将创建 SSID，并将其命名为 PEAP。

将第2层身份验证定义为WPA2，以便客户端执行基于EAP的身份验证（本示例中为PEAP-MS-CHAP v2），并使用高级加密标准(AES)作为加密机制。将其他所有值均保留默认值。

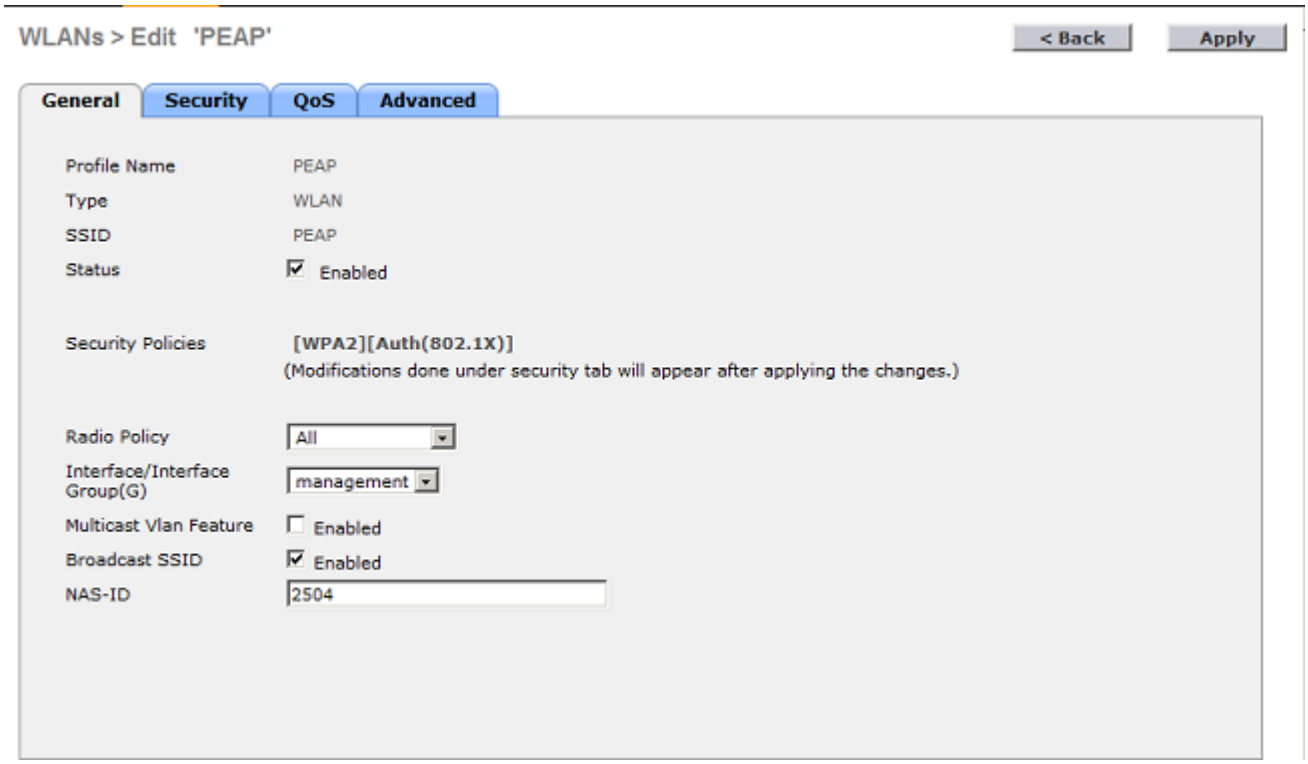
注意：本文档将 WLAN 与管理接口绑定。当您的网络中有多个 VLAN 时，可以创建一个单独的 VLAN 并将其绑定到 SSID。有关如何在 WLC 上配置 VLAN 的信息，请参阅无线局域网控制器上的 VLAN 配置示例。

要在WLC上配置WLAN，请完成以下步骤：

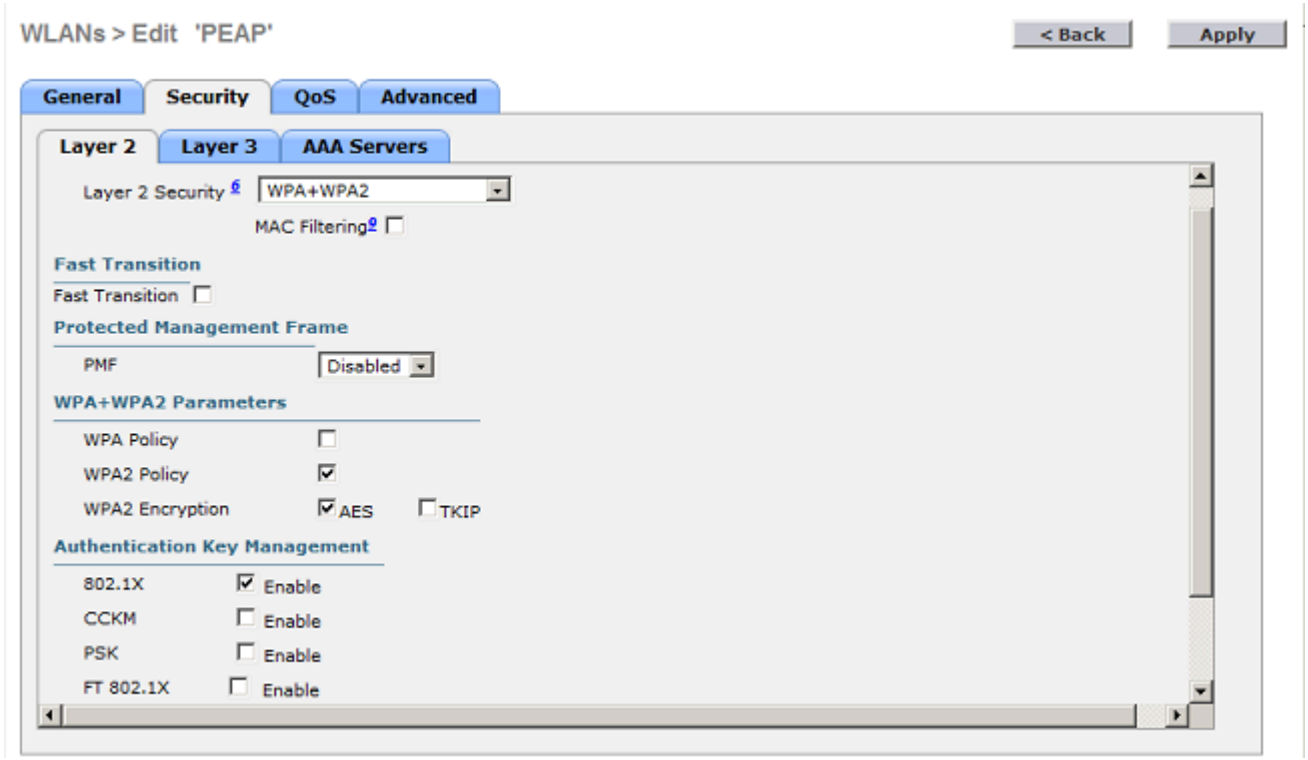
1. 从控制器接口单击WLANs以显示WLANs页面。此页列出了控制器上现有的 WLAN。
2. 选择新建创建新的 WLAN。输入 WLAN 的 WLAN ID 和 WLAN SSID，然后单击应用。



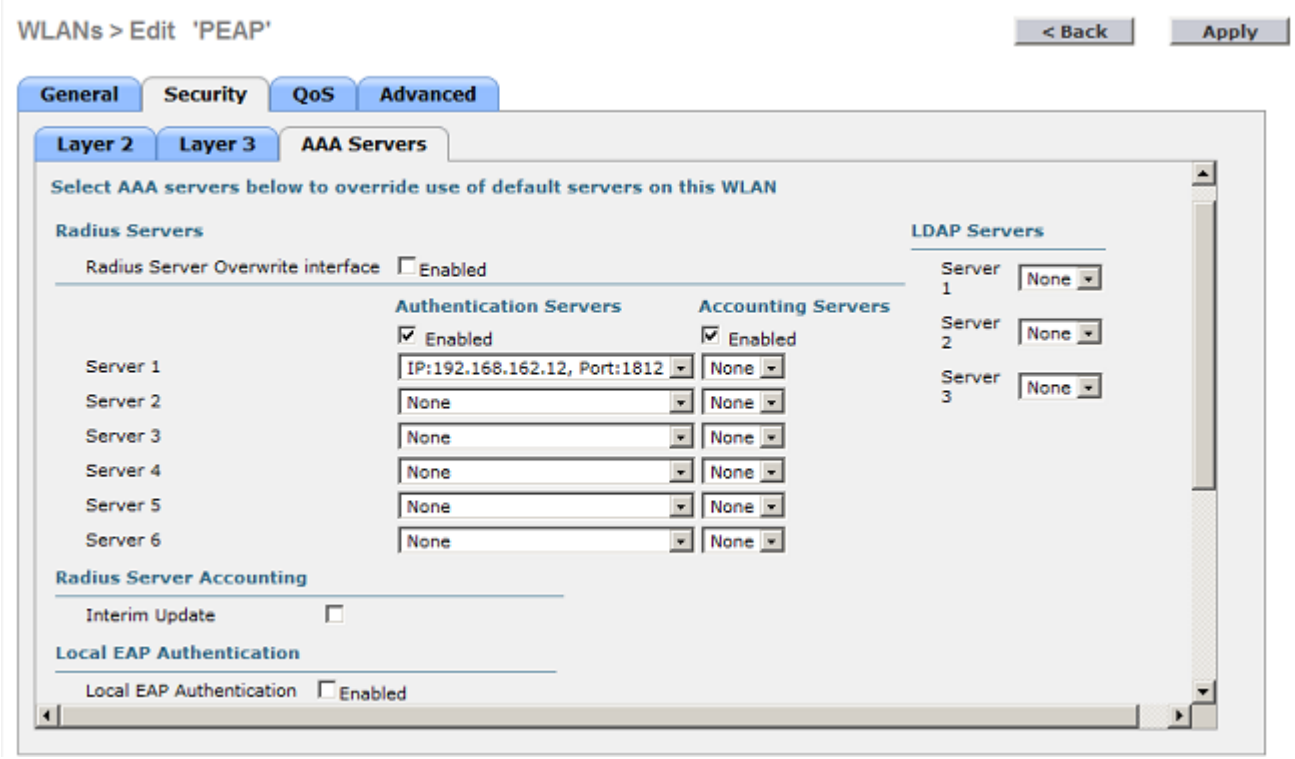
3. 要配置802.1x的SSID，请完成以下步骤：
    1. 单击General选项卡并启用WLAN。



2. 单击Security > Layer 2选项卡，将Layer 2 security设置为WPA + WPA2，根据需要选中WPA+WPA2 Parameters（例如，WPA2 AES）复选框，然后单击802.1x作为身份验证密钥管理。



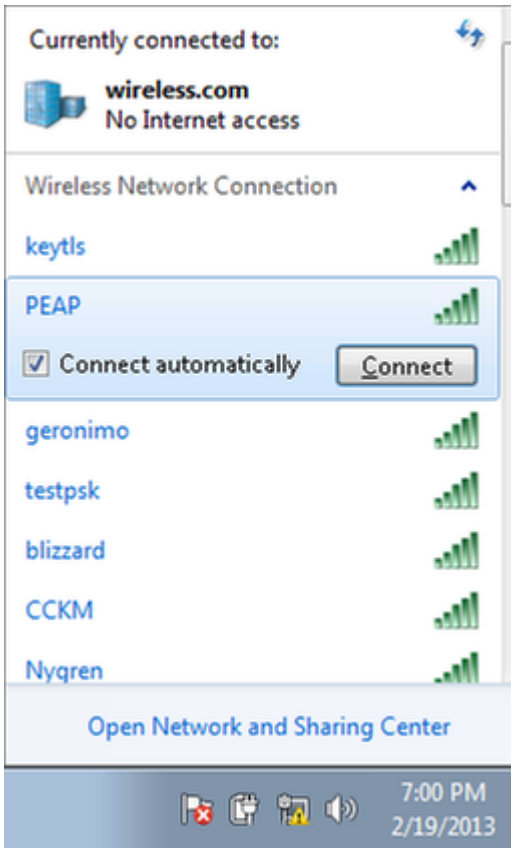
3. 单击Security > AAA Servers选项卡，从Server 1下拉列表中选择NPS的IP地址，然后单击Apply。



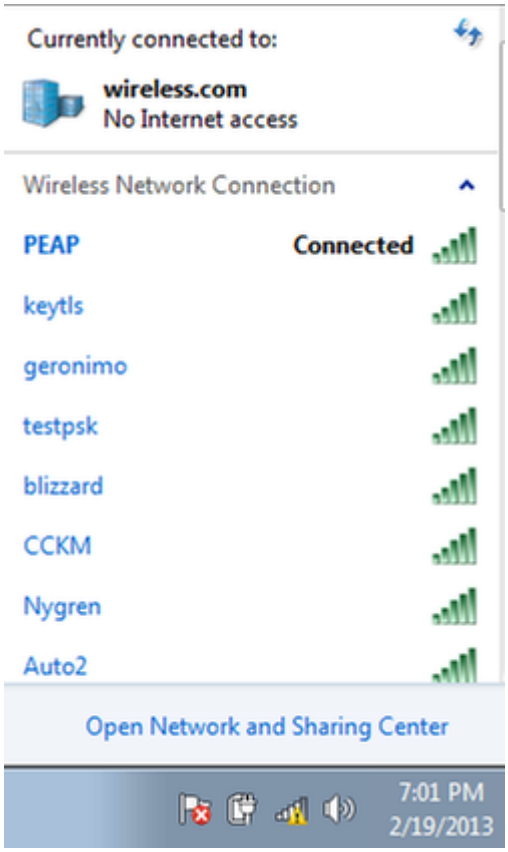
为PEAP-MS-CHAP v2身份验证配置无线客户端

完成以下步骤，使用Windows零配置工具配置无线客户端以连接到PEAP WLAN。

1. 单击任务栏中的Network图标。单击PEAP，然后单击Connect。



2. 客户端现在必须连接到网络。



3. 如果连接失败，请尝试重新连接到WLAN。如果问题仍然存在，请参阅故障排除部分。

验证

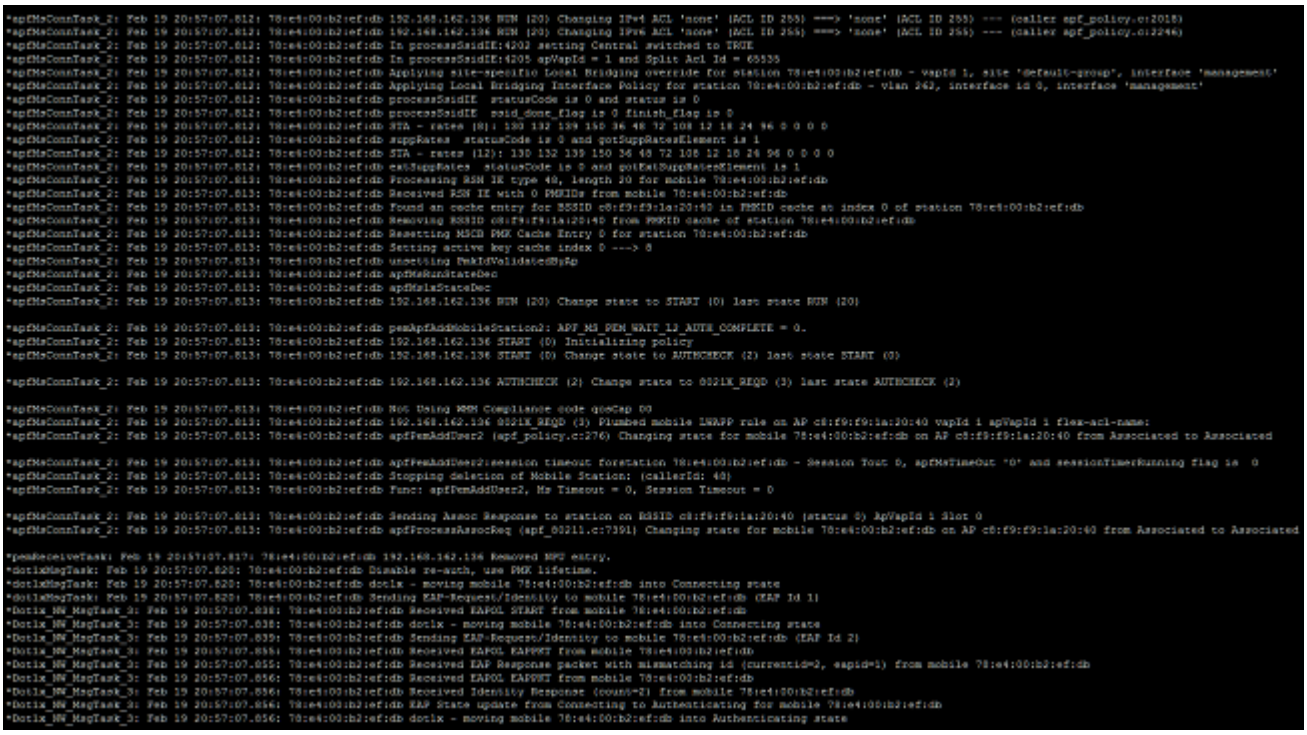
当前没有可用于此配置的验证过程。

故障排除

如果您的客户端未连接到WLAN，则本节提供可用于对配置进行故障排除的信息。

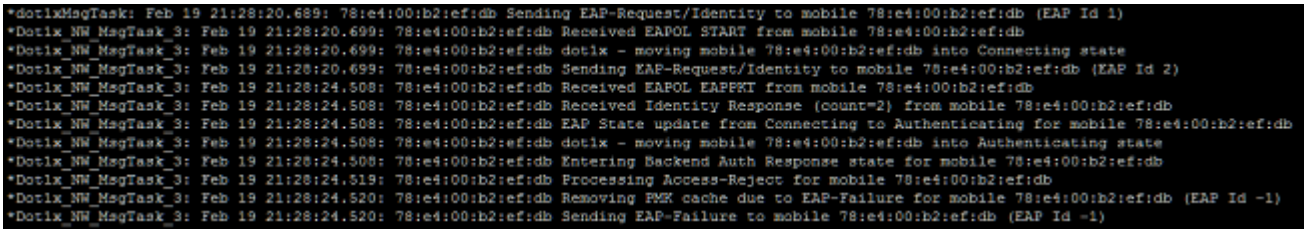
有两个工具可用于诊断802.1x身份验证故障：debug client命令和Event Viewer（在Windows中）。

如果从WLC执行客户端调试，它不会占用大量资源，也不会影响服务。要启动调试会话，请打开WLC的命令行界面(CLI)，然后输入debug client mac address，其中mac address是无法连接的无线客户端的无线mac地址。当此调试运行时，尝试连接客户端；wlc的CLI上必须存在类似于以下示例的输出：



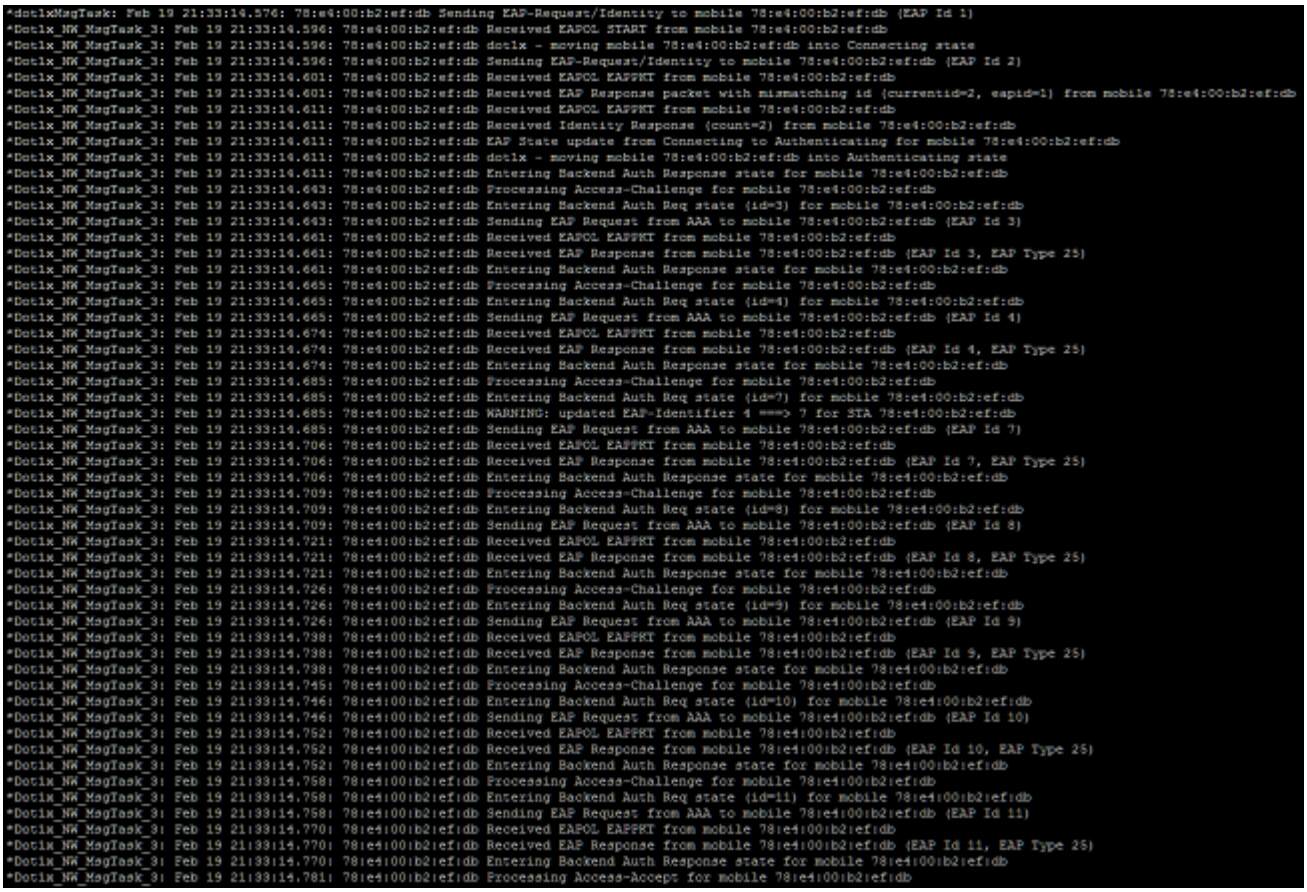
这是配置错误时可能出现的问题的示例。此处，WLC调试显示WLC已进入身份验证状态，这意味着WLC等待来自NPS的响应。这通常是由于WLC或NPS上的共享密钥不正确造成的。您可以通过Windows Server事件查看器进行确认。如果您找不到日志，请求从未发送到NPS。

从WLC调试找到的另一个示例是access-reject。access-reject显示NPS接收并拒绝客户端凭证。以下是接收访问拒绝的客户端示例：



当您看到access-reject时，请检查Windows Server事件日志中的日志，以确定NPS使用access-reject响应客户端的原因。

成功的身份验证在客户端调试中具有access-accept，如下例所示：

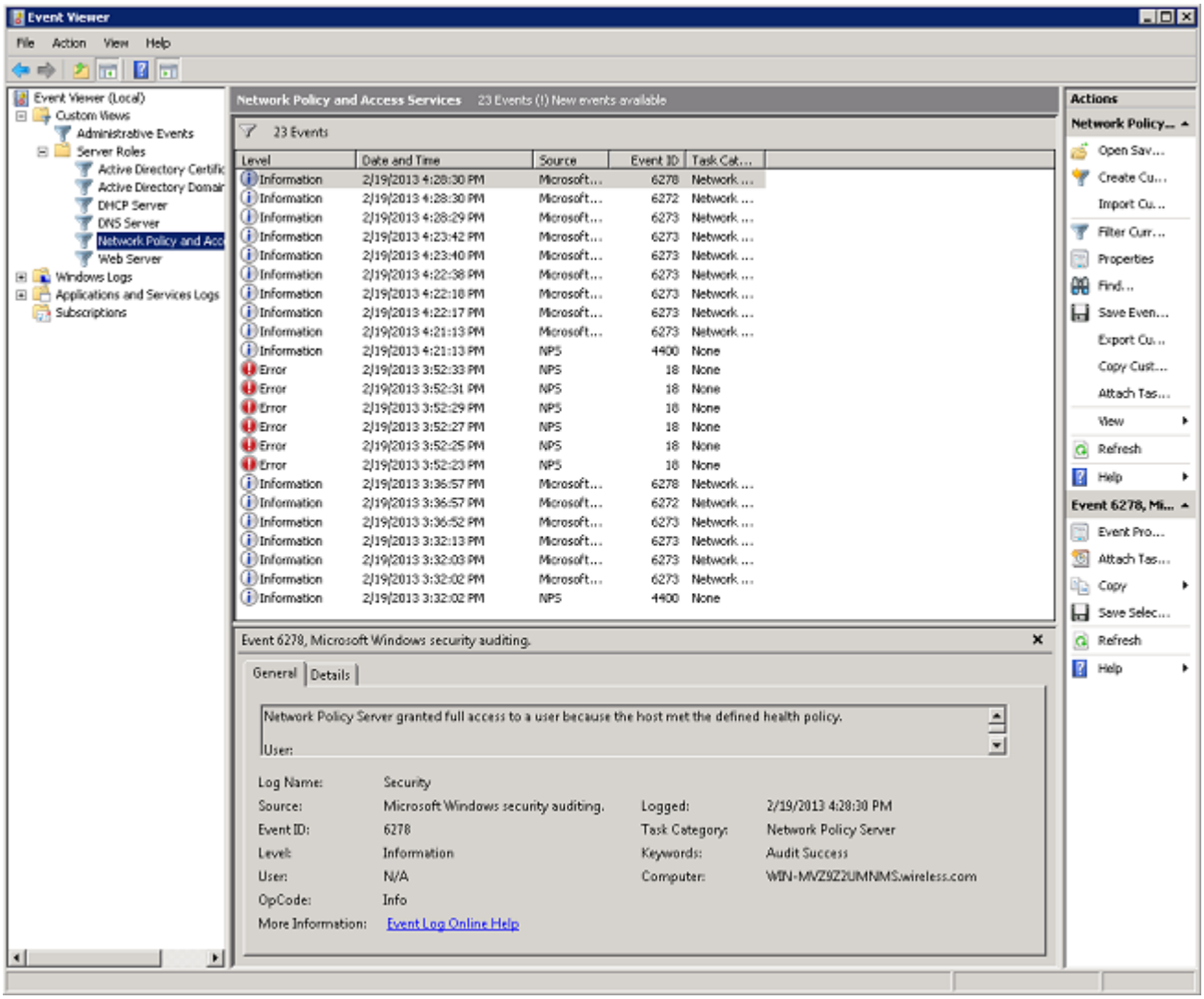


如果要对访问拒绝和响应超时进行故障排除，则需要访问RADIUS服务器。WLC充当在客户端和RADIUS服务器之间传递EAP消息的身份验证器。RADIUS服务的制造商必须检查并诊断以访问拒绝或响应超时响应的RADIUS服务器。

注意：TAC不为第三方RADIUS服务器提供技术支持；但是，RADIUS服务器上的日志通常解释客户端请求被拒绝或忽略的原因。

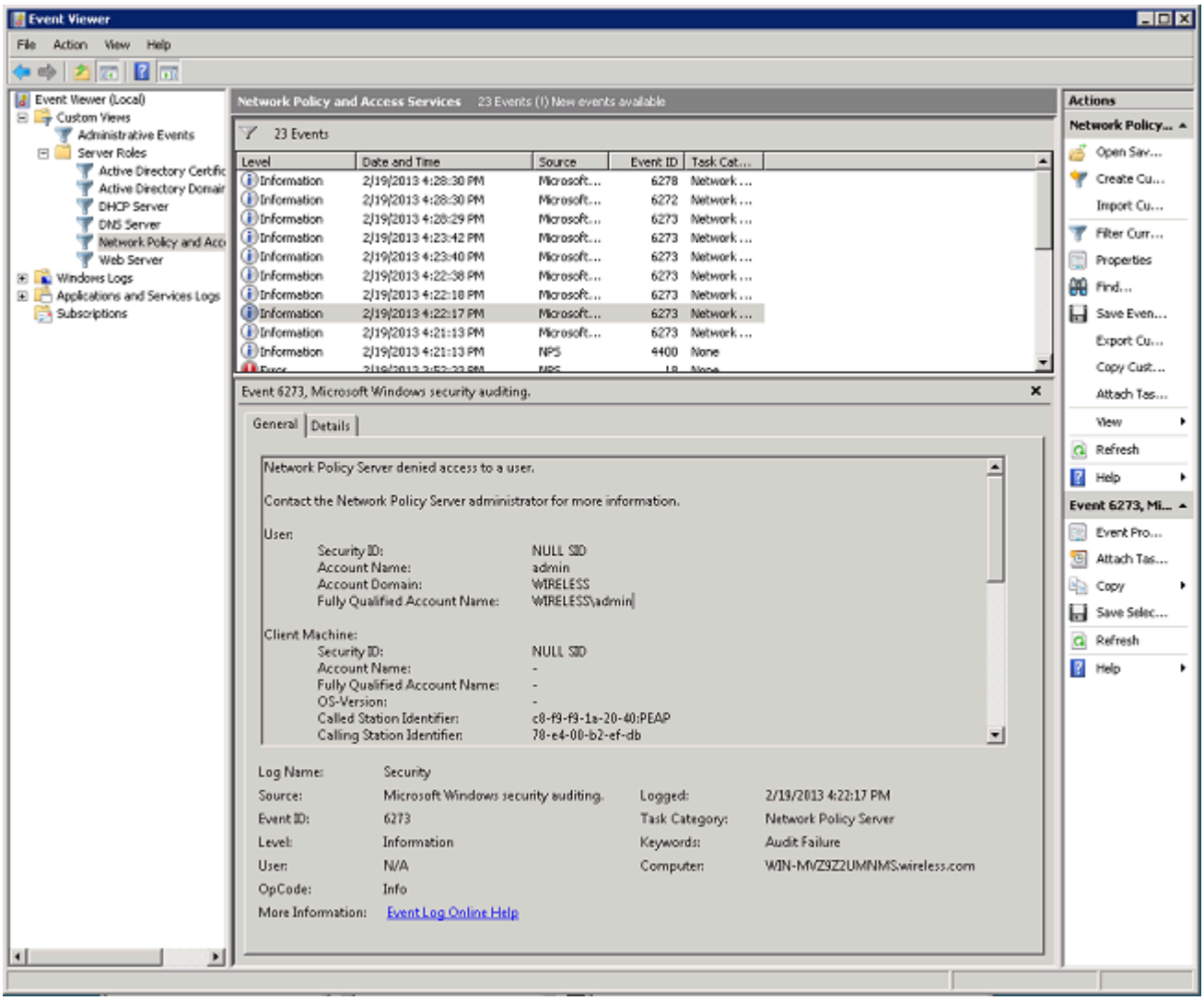
要对NPS的访问拒绝和响应超时进行故障排除，请在服务器上的Windows事件查看器中检查NPS日志。

1. 单击开始>管理员工具>事件查看器以启动事件查看器并查看NPS日志。
2. 展开Custom Views > Server Roles > Network Policy and Access。

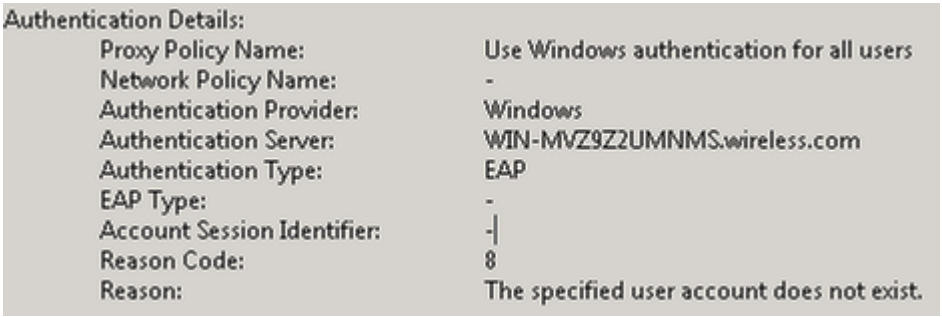


在“事件视图”的此部分，有已通过和失败的身份验证的日志。检查这些日志，对客户端未通过身份验证的原因进行故障排除。通过和失败的身份验证均显示为信息。滚动浏览日志，查找身份验证失败并收到基于WLC调试的访问拒绝的用户名。

以下是NPS拒绝用户访问时的示例：

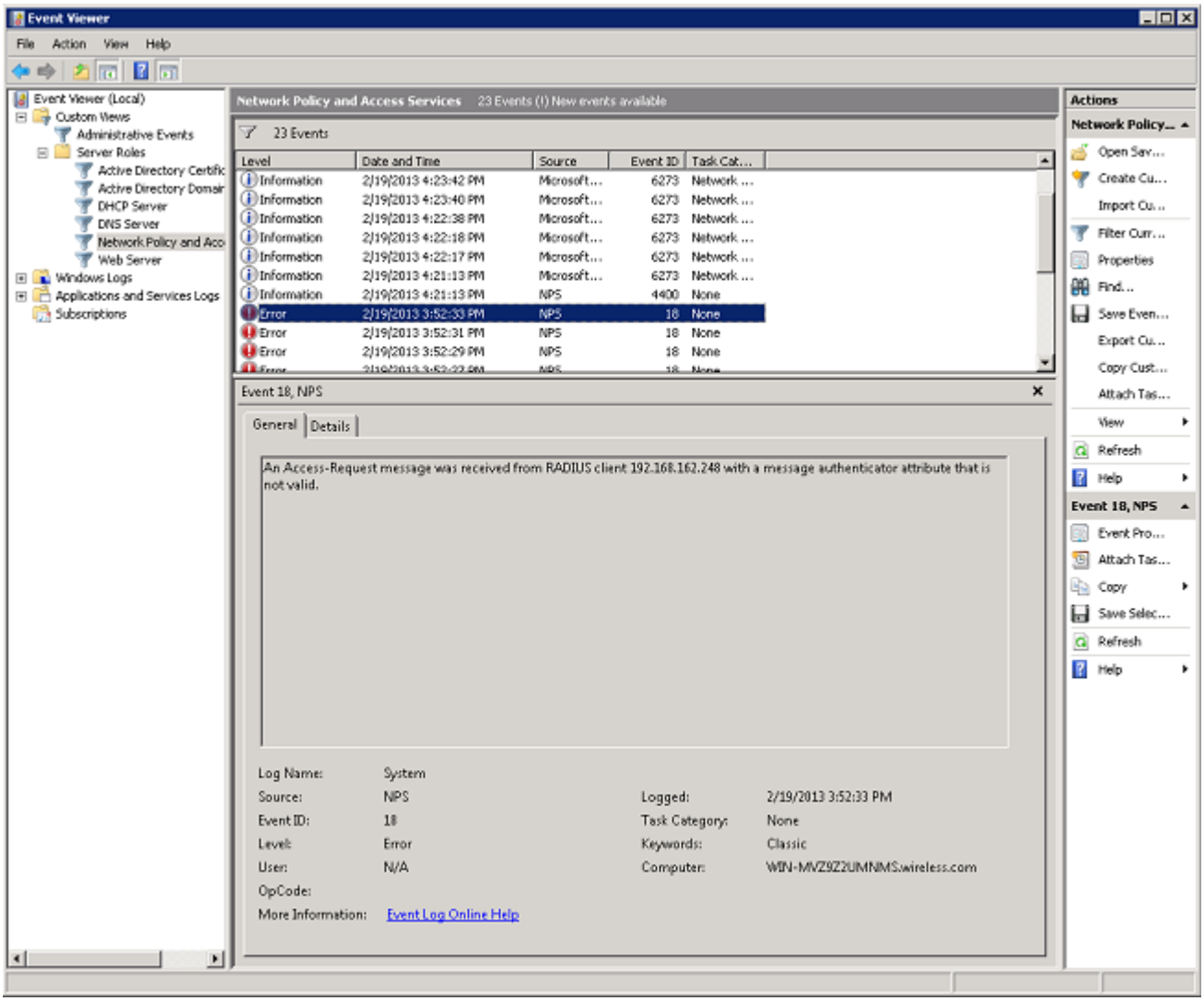


当您在事件查看器中查看deny语句时，请检查Authentication Details部分。在本示例中，您可以看到，由于用户名不正确，NPS拒绝用户访问：



如果WLC没有收到来自NPS的响应，则NPS上的事件视图在您需要排除故障时也会为您提供帮助。 这通常是由于NPS和WLC之间的共享密钥不正确造成的。

在本示例中，由于共享密钥不正确，NPS放弃来自WLC的请求：



相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。