RADIUS 服务器搭建配置

功能测试指导书

信锐网科技术有限公司

2015 年 05 月 25 日

第一章 功能概述

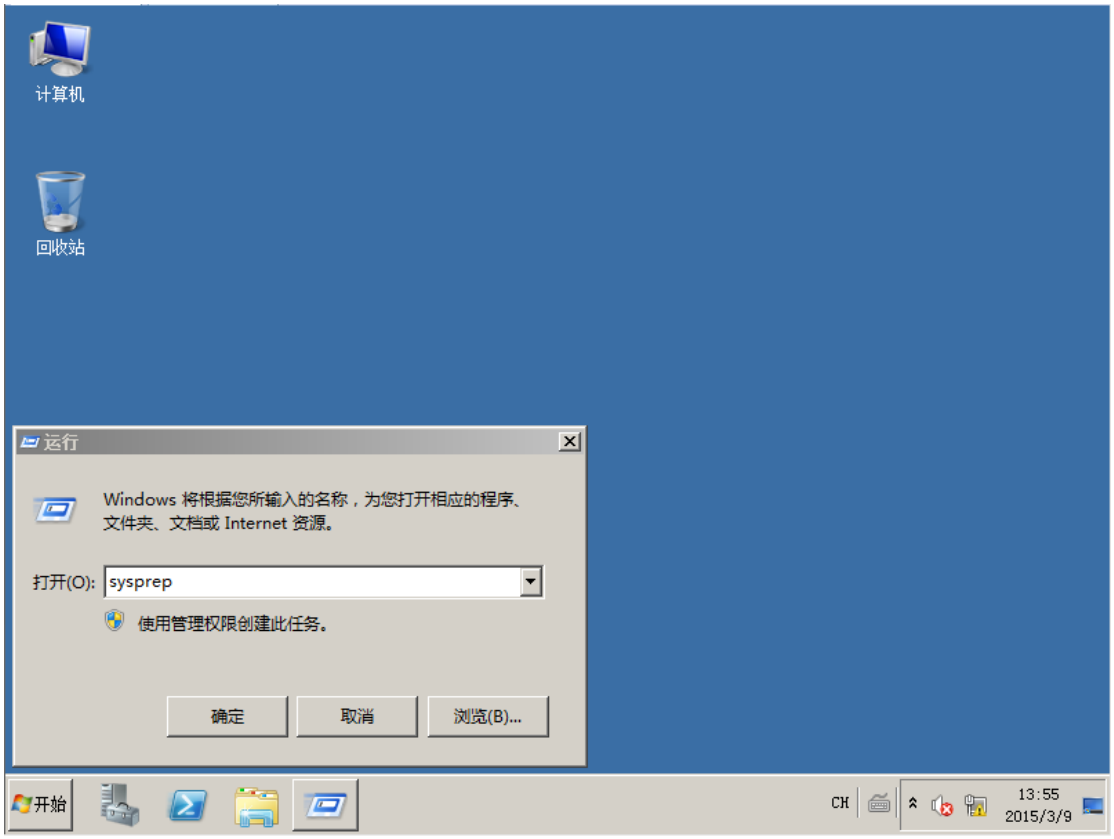
本文介绍 AD 域、CA 证书颁发机构以及 RADIUS 服务器搭建和服务器配置。

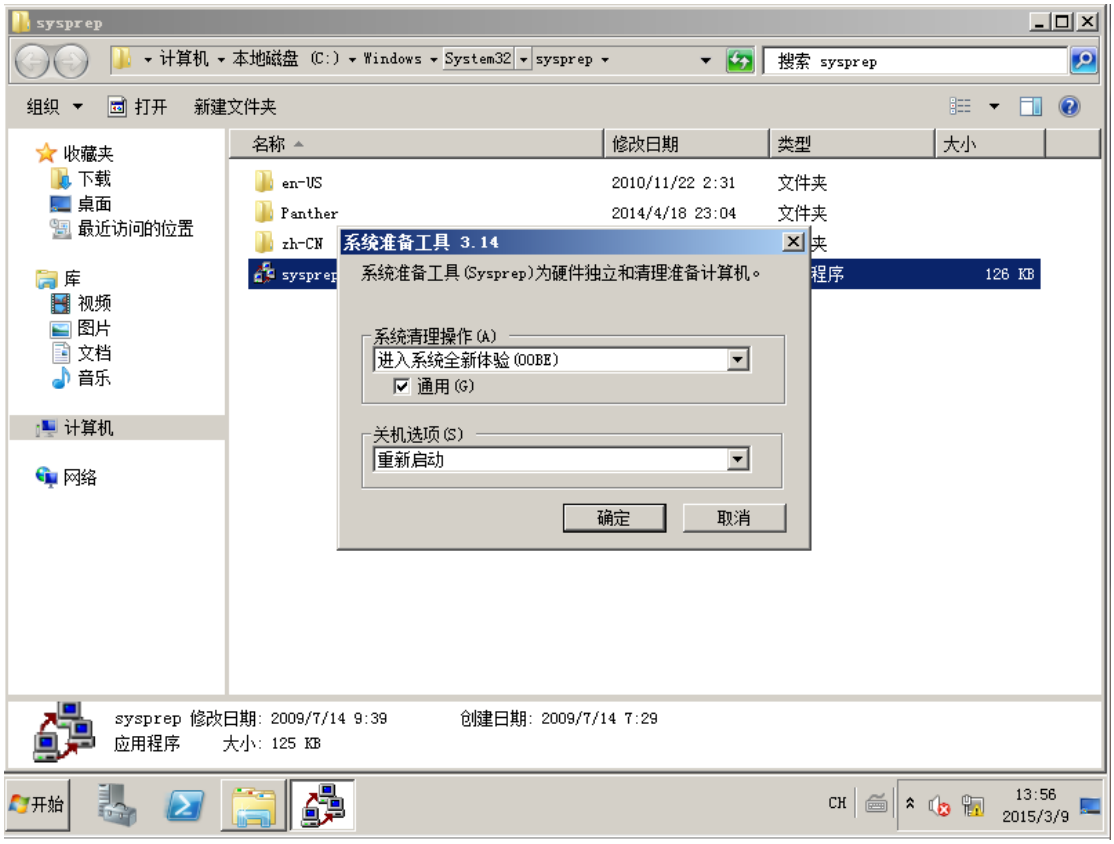
第二章 场景需求

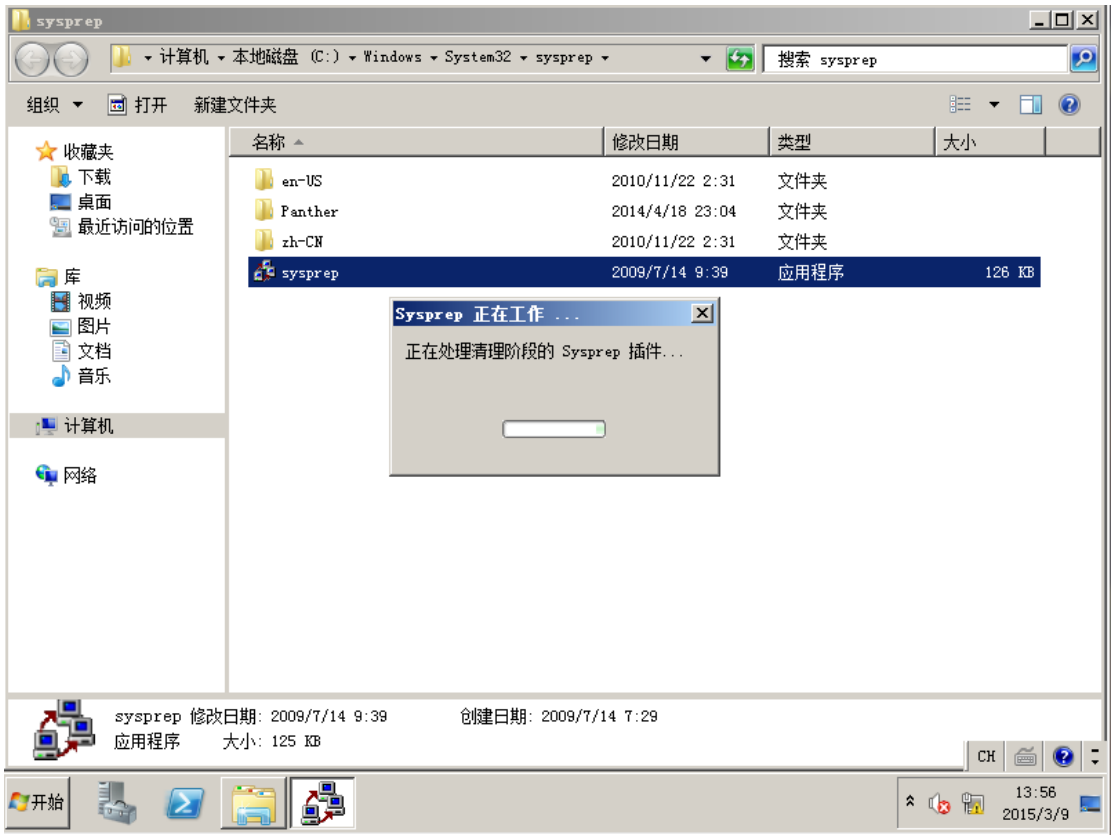
2.1 服务器搭建部分

2.1.1 系统重封装

因为这两台虚拟机都是克隆的，避免实验中出现不必要的问题，将两台 Windows server 2008 R2 系统重新封装。使用 sysprep 命令

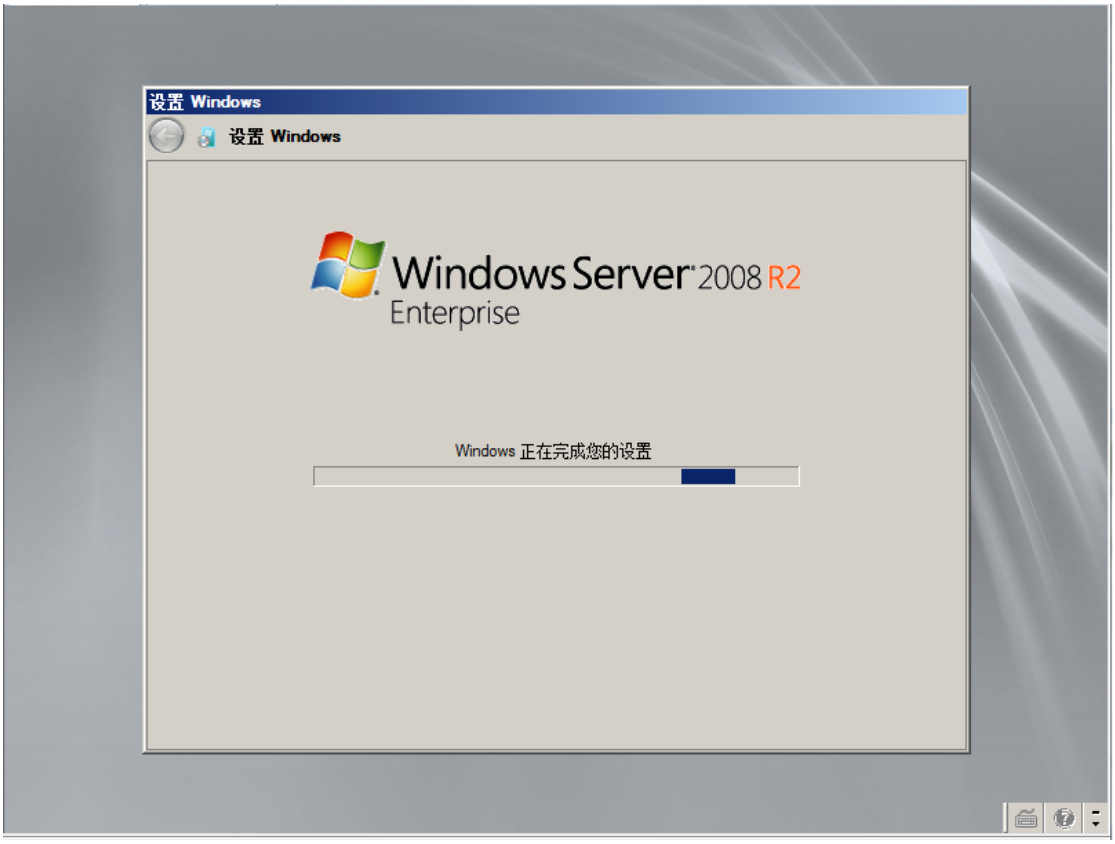



sysprep
计算机 ▸ 本地磁盘 (C:) ▸ Windows ▸ System32 ▸ sysprep ▸
搜索 sysprep
组织
打开
新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
网络
名称
修改日期
类型
大小
en-US 2010/11/22 2:31 文件夹
Panther 2014/4/18 23:04 文件夹
zh-CN 2010/11/22 2:31 文件夹
sysprep 2009/7/14 9:39 应用程序 126 KB
系统准备工具 3.14
系统准备工具(Sysprep)为硬件独立和清理准备计算机。
系统清理操作(A)
进入系统全新体验(OOBE)
通用(G)
关机选项(S)
重新启动
确定
取消
sysprep 修改日期: 2009/7/14 9:39 创建日期: 2009/7/14 7:29
应用程序 大小: 125 KB
开始
CH
13:56
2015/3/9


sysprep
计算机 ▸ 本地磁盘 (C:) ▸ Windows ▸ System32 ▸ sysprep ▸
搜索 sysprep
组织
打开
新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
网络
名称
修改日期
类型
大小
en-US 2010/11/22 2:31 文件夹
Panther 2014/4/18 23:04 文件夹
zh-CN 2010/11/22 2:31 文件夹
sysprep 2009/7/14 9:39 应用程序 126 KB
Sysprep 正在工作 ...
正在处理清理阶段的 Sysprep 插件...
sysprep 修改日期: 2009/7/14 9:39 创建日期: 2009/7/14 7:29
应用程序 大小: 125 KB
开始
CH
13:56
2015/3/9


设置 Windows
设置 Windows
Windows Server 2008 R2
Enterprise
国家或地区(C): 中国
时间和货币(T): 中文(简体，中国)
键盘布局(K): 中文(简体) - 美式键盘
版权所有 © 2009 Microsoft Corporation。保留所有权利。
下一步(N)
CH


设置 Windows
设置 Windows
请阅读许可条款
MICROSOFT 软件许可条款
MICROSOFT WINDOWS SERVER 2008 R2 ENTERPRISE SERVICE PACK 1
这些许可条款是您与以下各方之间达成的协议：
· 将软件随服务器一起分发的服务器制造商；或
· 将软件随服务器一起分发的软件安装商。
请阅读条款内容。这些条款适用于上述软件，包括您用来接收该软件的介质（如有）。印刷的书面许可条款（可能随软件一起提供）将取代任何屏幕上显示的许可条款。这些条款也适用于 Microsoft 为该软件提供的任何
· 更新
我接受许可条款(A)
开始(S)

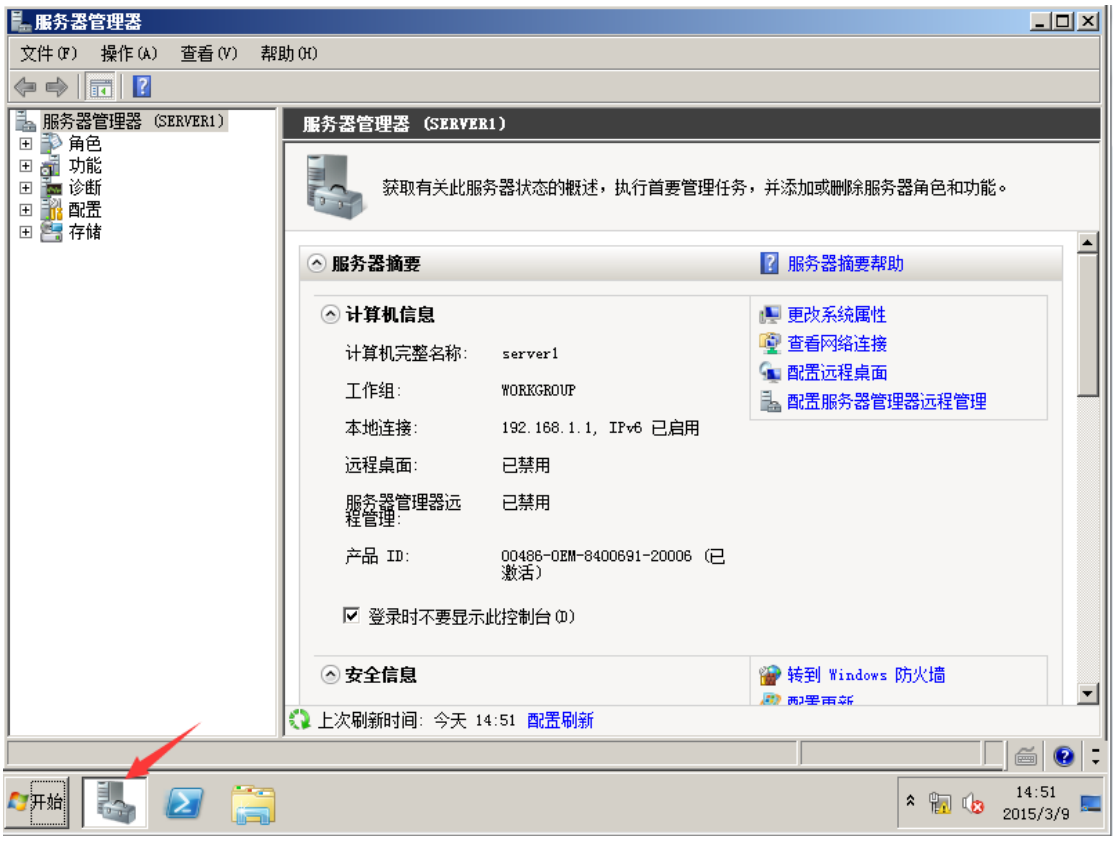

设置 Windows
设置 Windows
Windows Server 2008 R2
Enterprise
Windows 正在完成您的设置


用户首次登录之前必须更改密码。
确定
取消
Windows Server 2008 R2
Enterprise

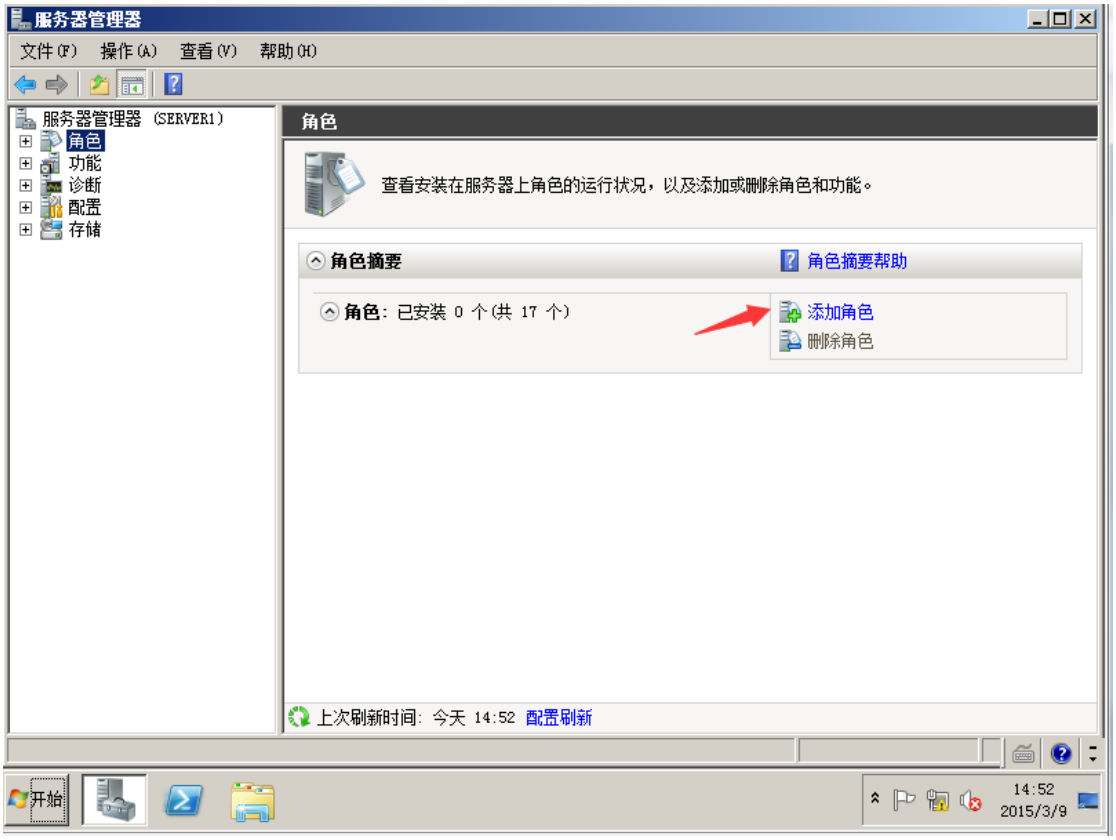
2.1.2 在 server1 上完成 AD 和 DNS 搭建

首先给服务器命名 server1、server2 并配置静态 IP 地址。

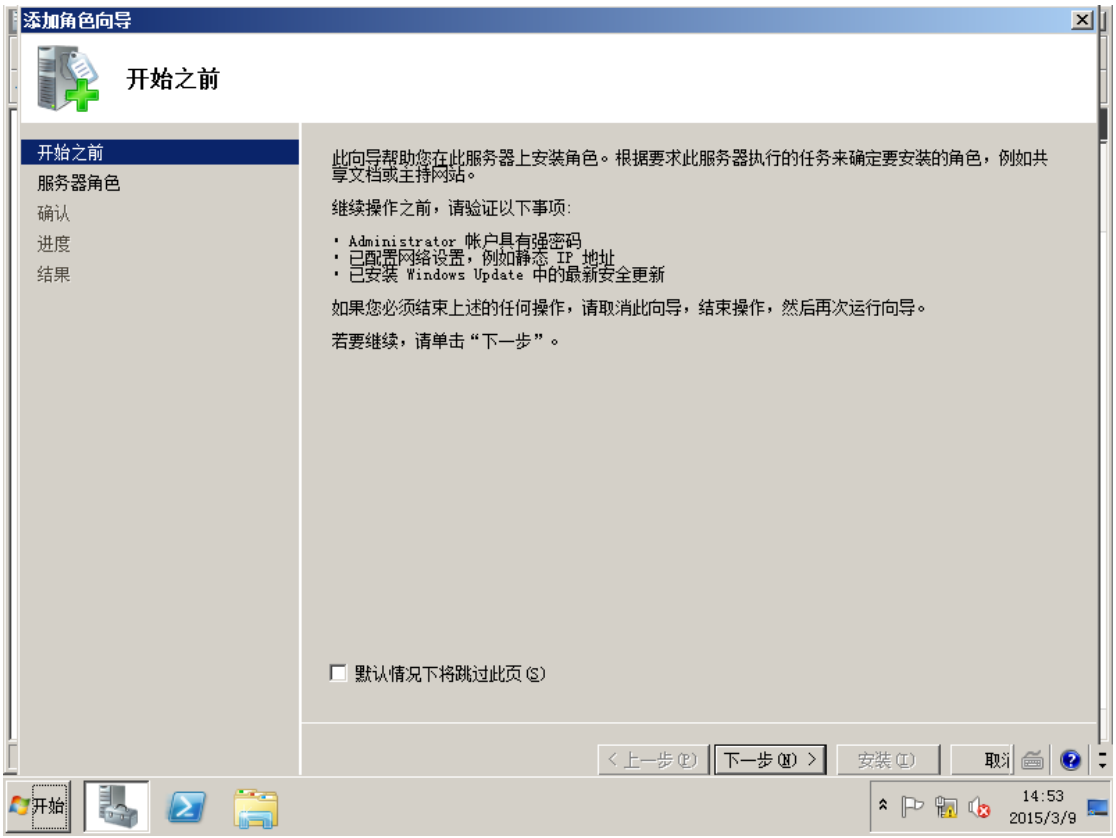
第一步打开服务管理器查看该服务器的基本信息。



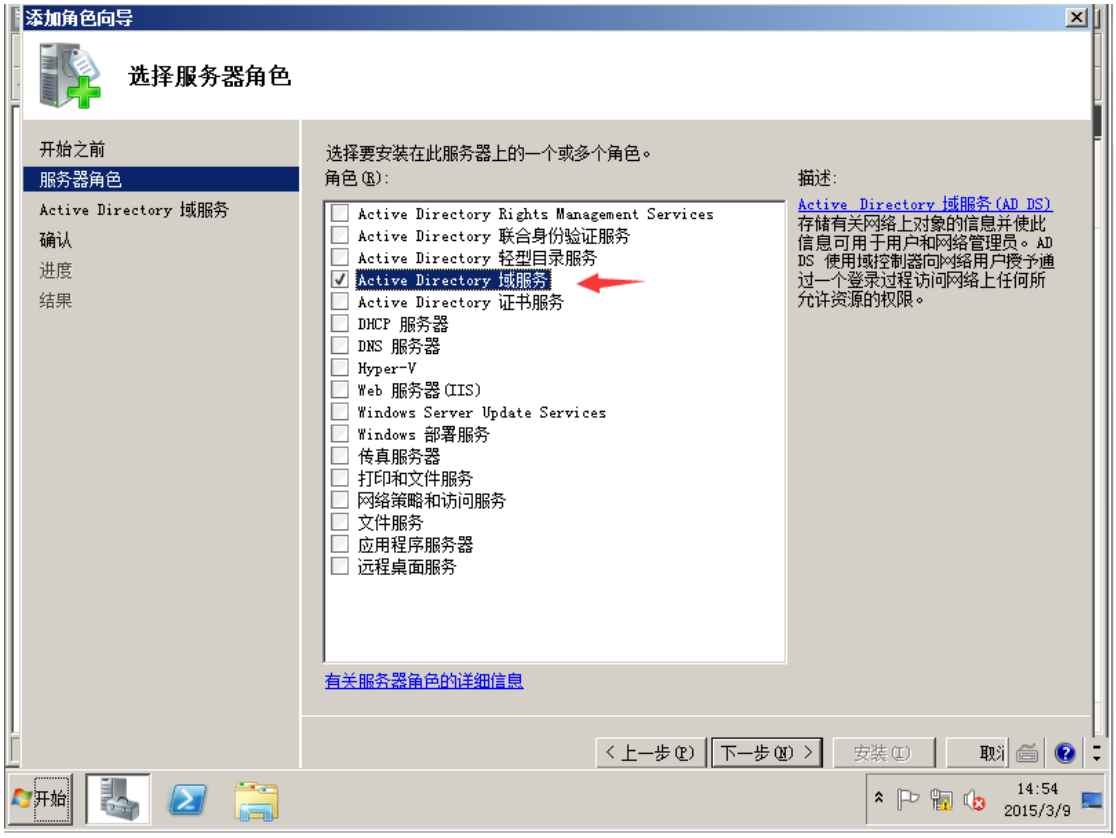
在服务器管理器界面选择角色，选择添加角色。


服务器管理器
文件(F) 操作(A) 查看(V) 帮助(H)
服务器管理器 (SERVER1)
角色
功能
诊断
配置
存储
角色
查看安装在服务器上角色的运行状况，以及添加或删除角色和功能。
角色摘要
角色摘要帮助
角色：已安装 0 个(共 17 个)
添加角色
删除角色
上次刷新时间：今天 14:52 配置刷新
开始
14:52
2015/3/9

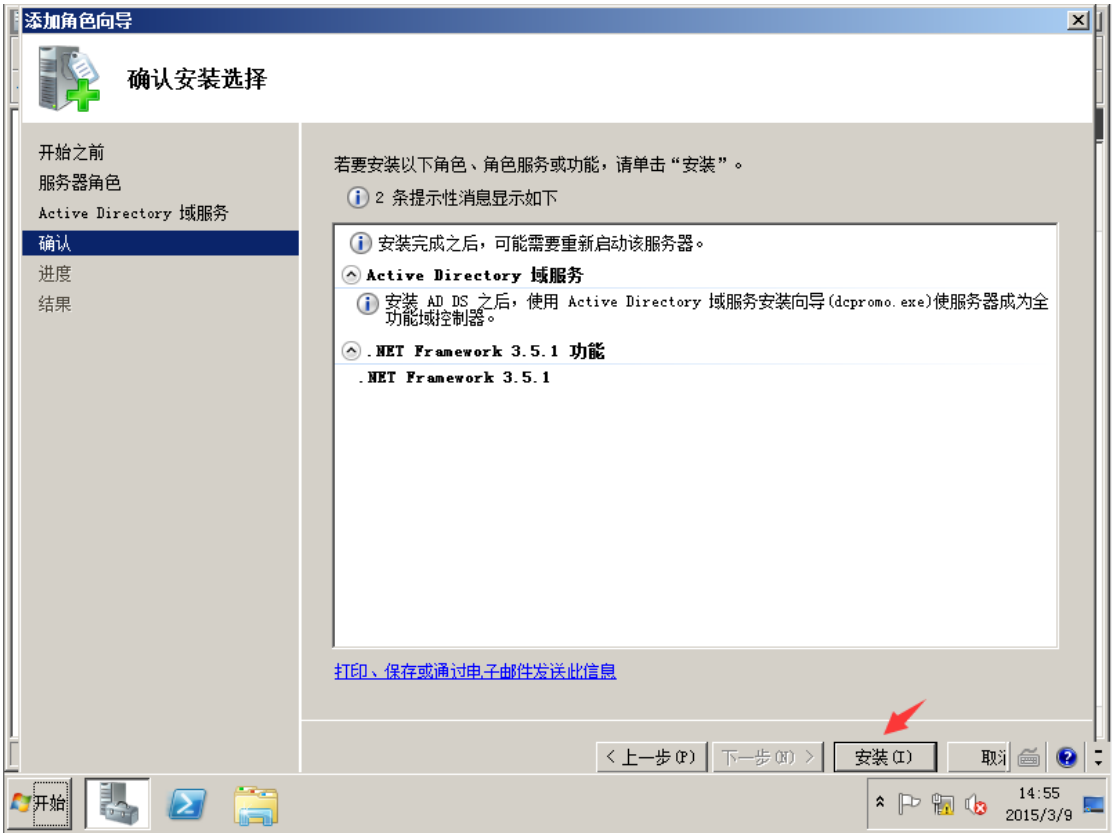
默认选择下一步


添加角色向导
开始之前
开始之前
服务器角色
确认
进度
结果
此向导帮助您在此服务器上安装角色。根据要求此服务器执行的任务来确定要安装的角色，例如共享文档或主持网站。
继续操作之前，请验证以下事项:
• Administrator 帐户具有强密码
• 已配置网络设置，例如静态 IP 地址
• 已安装 Windows Update 中的最新安全更新
如果您必须结束上述的任何操作，请取消此向导，结束操作，然后再次运行向导。
若要继续，请单击“下一步”。
默认情况下将跳过此页(S)
< 上一步(P)
下一步(N) >
安装(I)
取消
开始
14:53
2015/3/9

选择 Active Directory 域服务器这个服务器角色

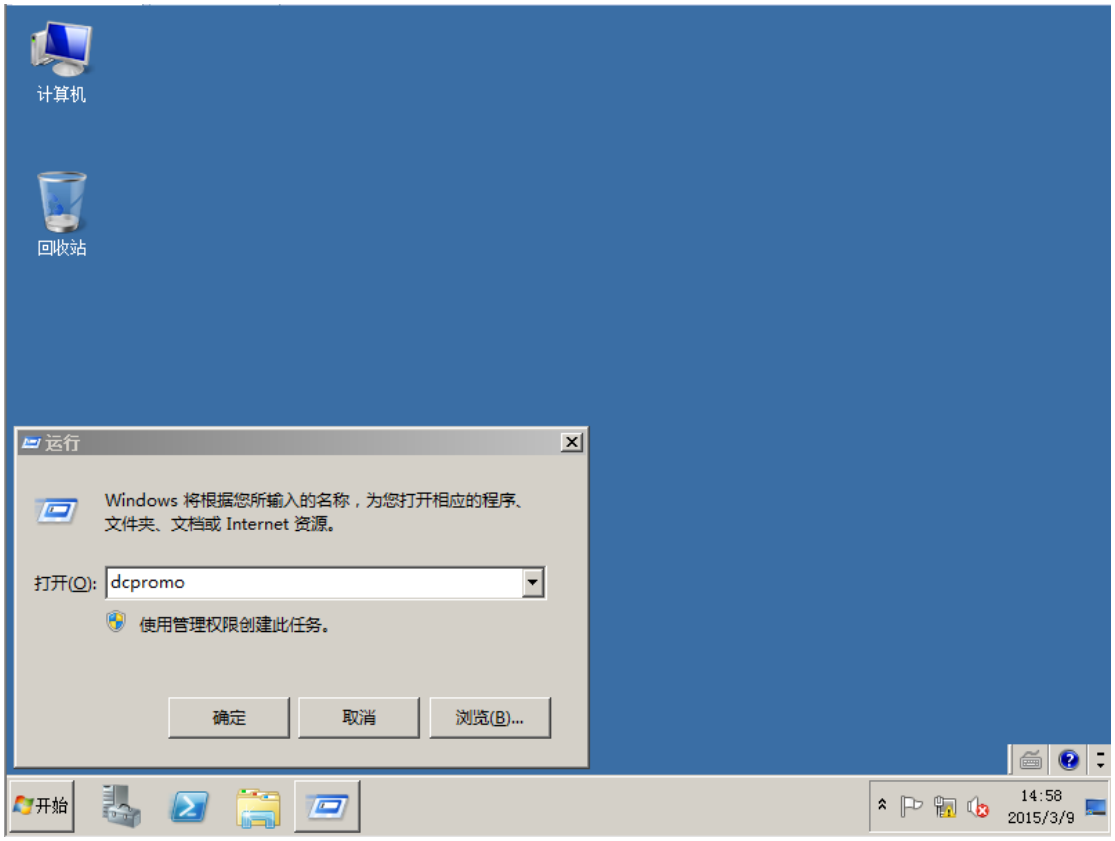


下一步，选择安装。

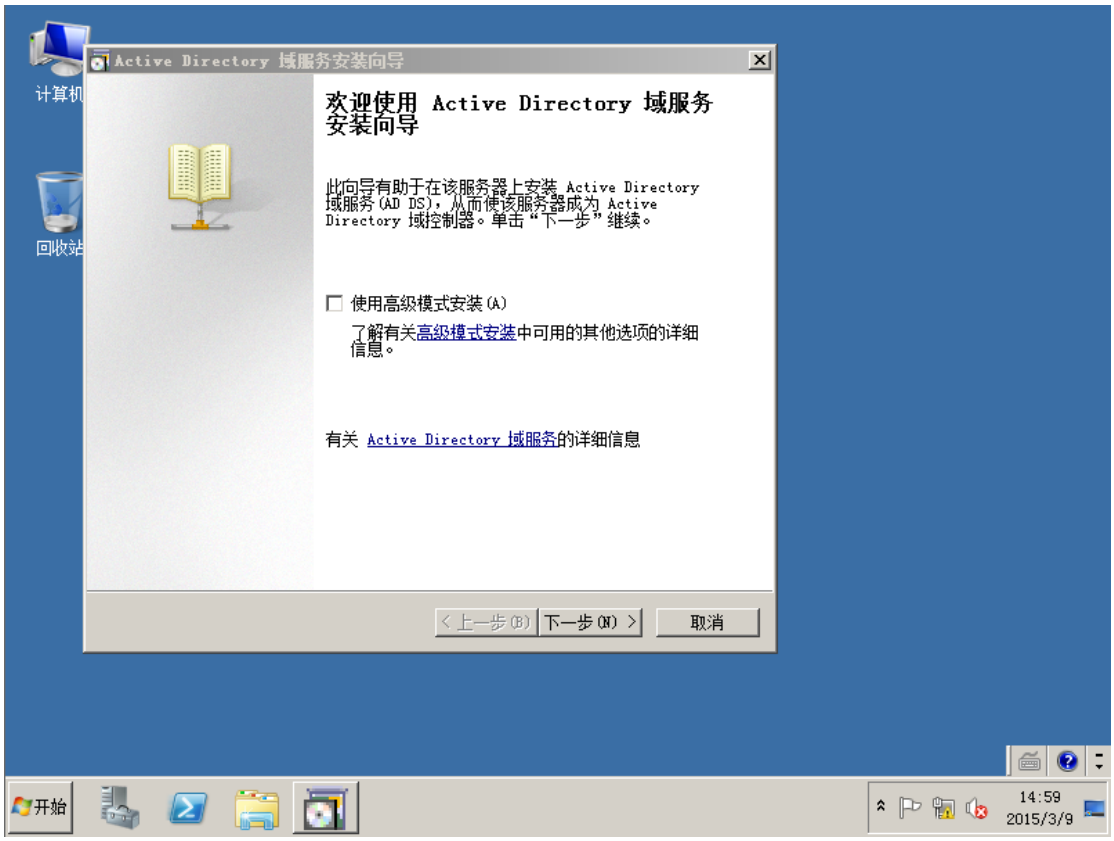


安装完成之后，关闭此对话框。

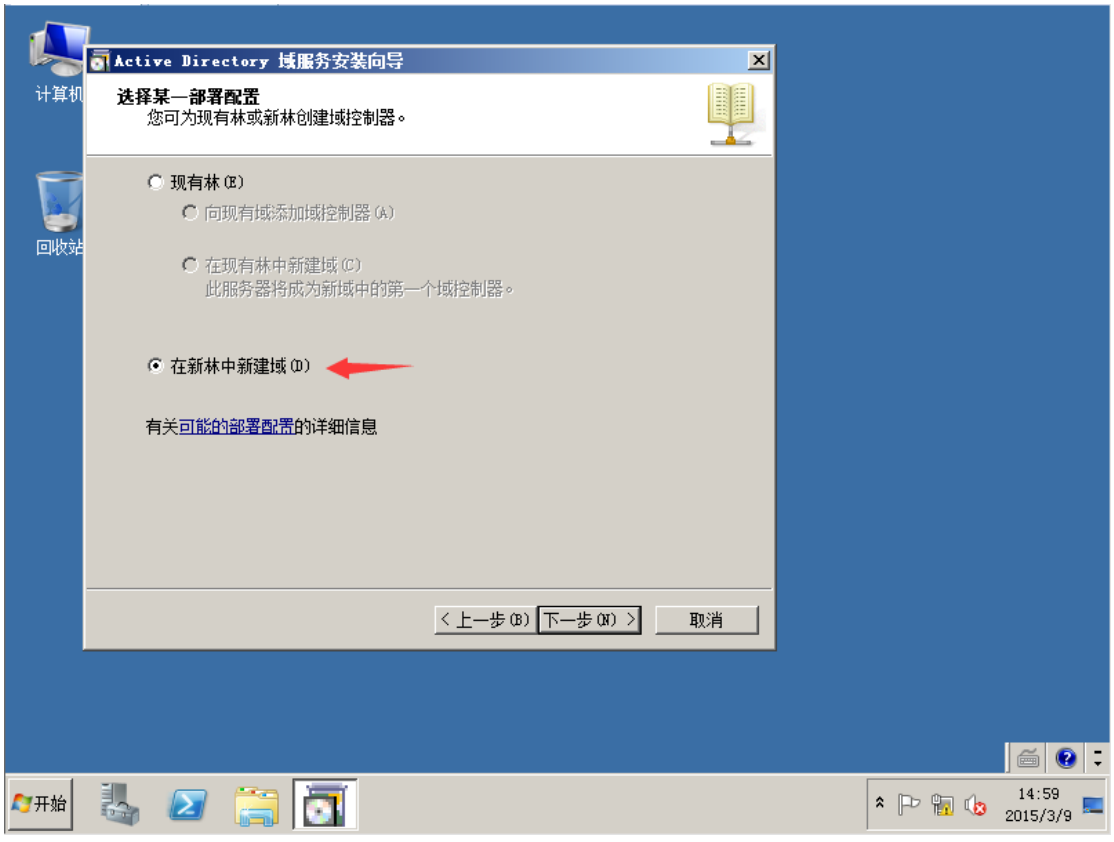
在运行里，输入 dcpromo 完成域控制器的安装。



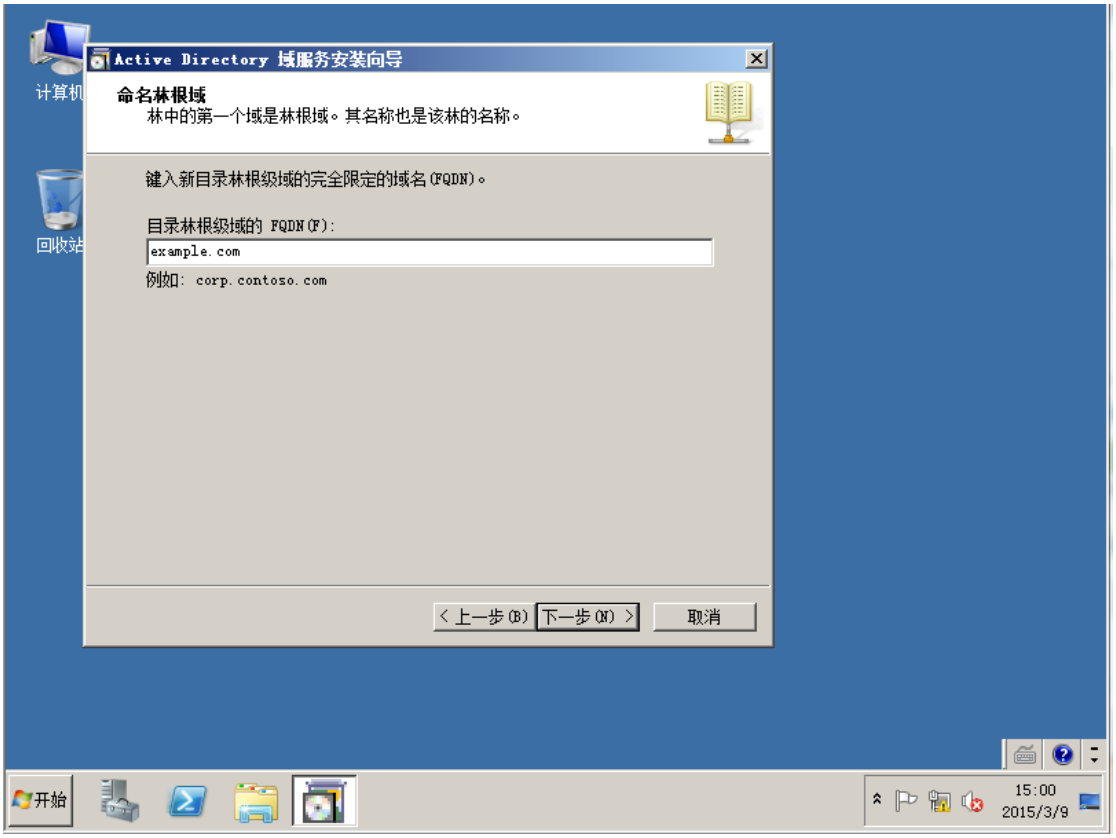
直接选择下一步



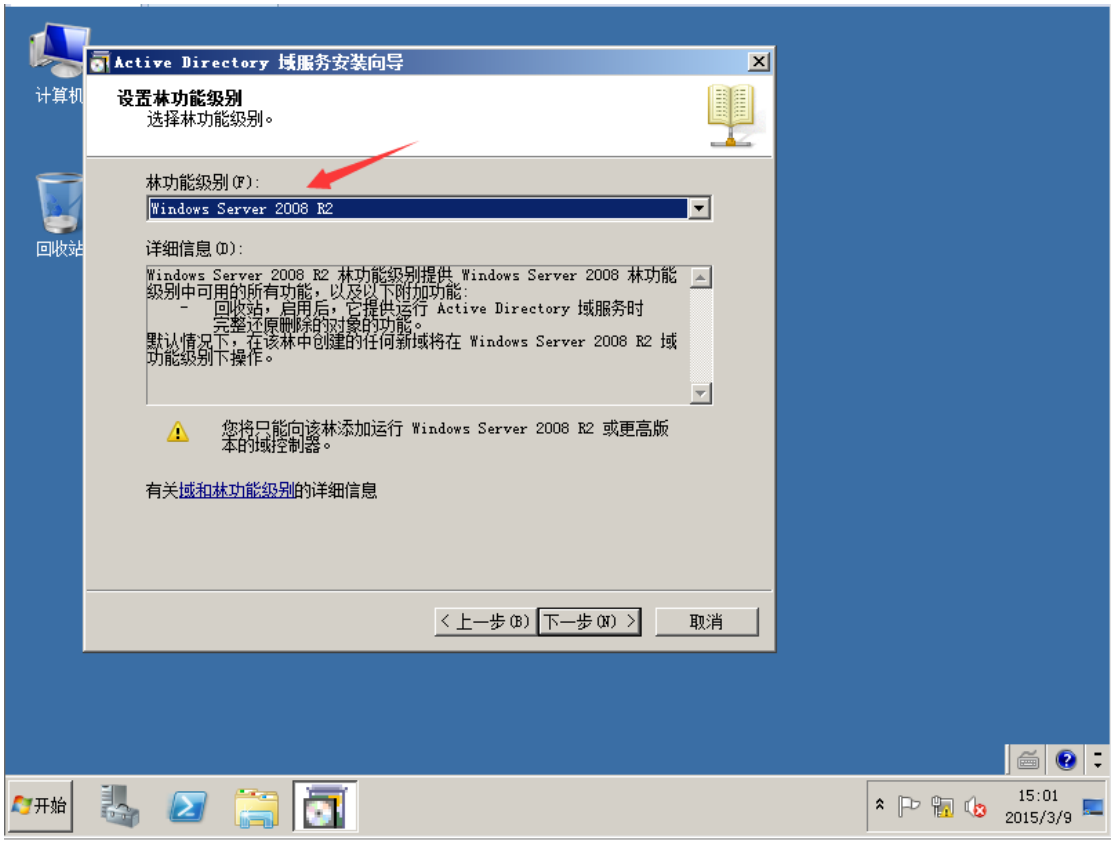
选择，在新林中新建域，选择下一步



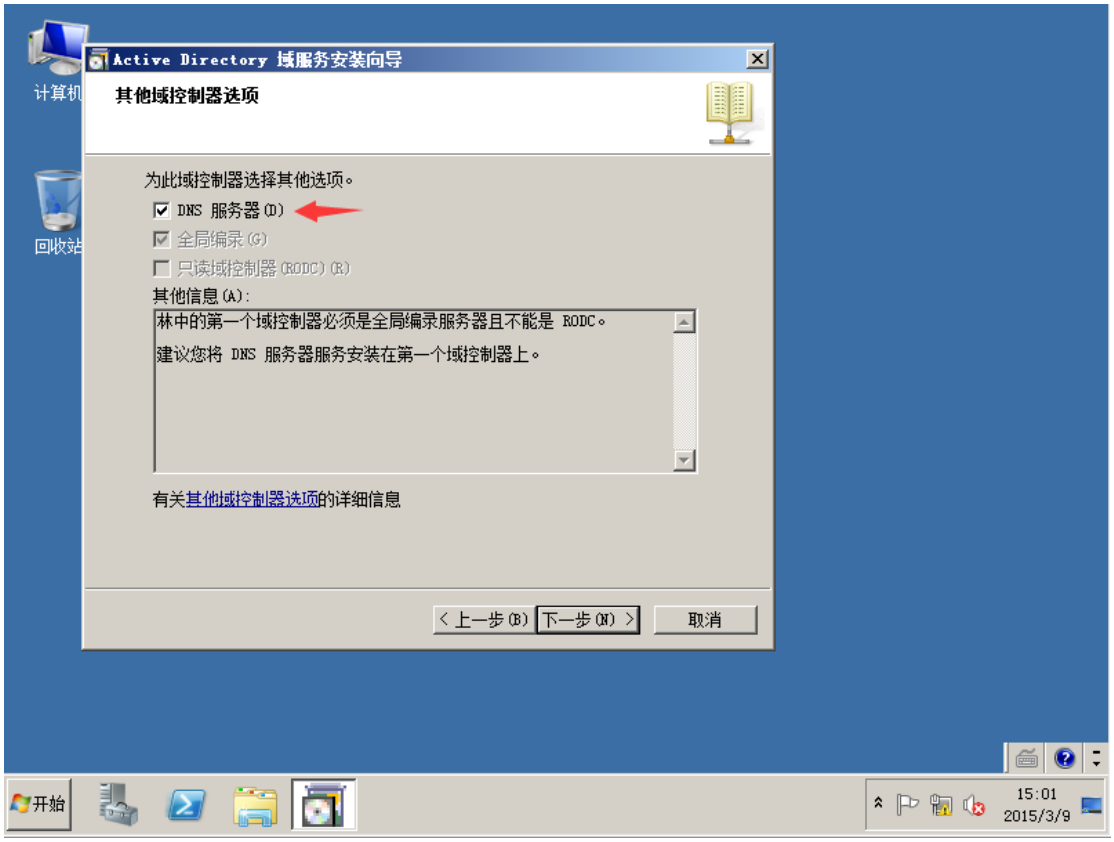
输入创建域的 FQDN ，例如：example.com



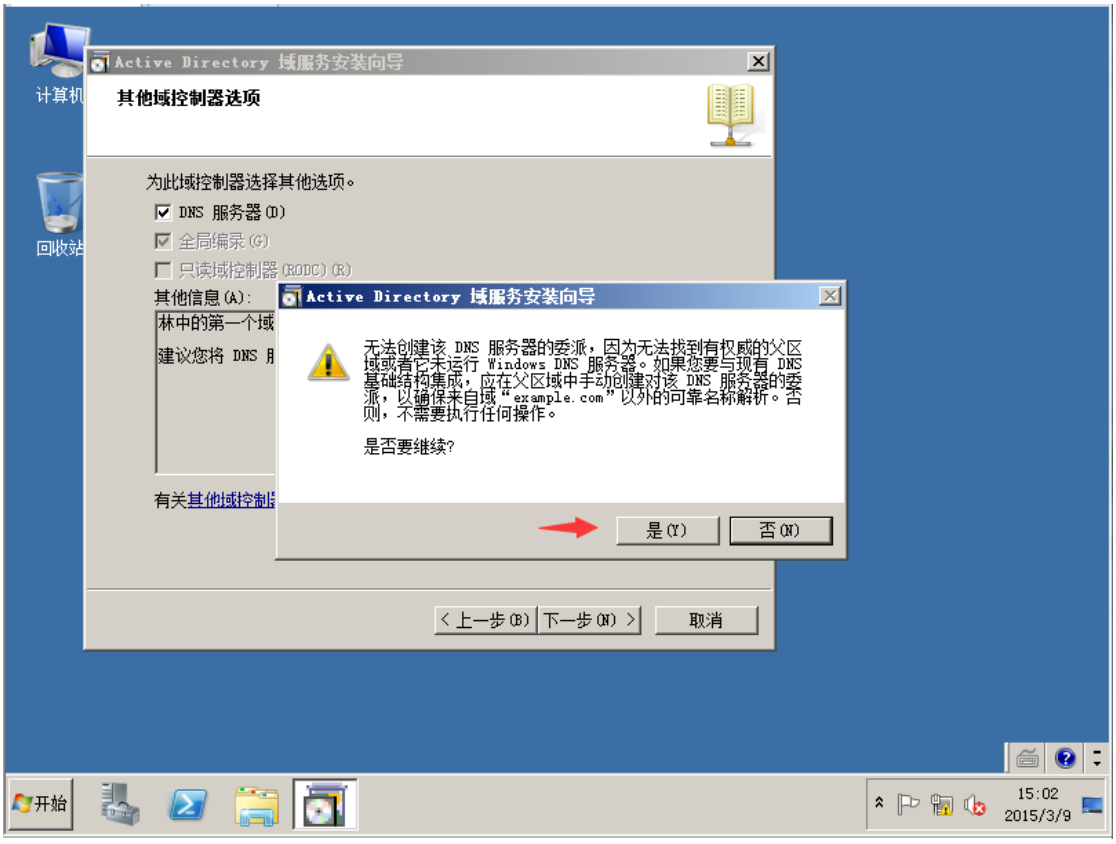
下一步在此界面现在林功能级别为 windows server 2008 R2，然后选择下一步



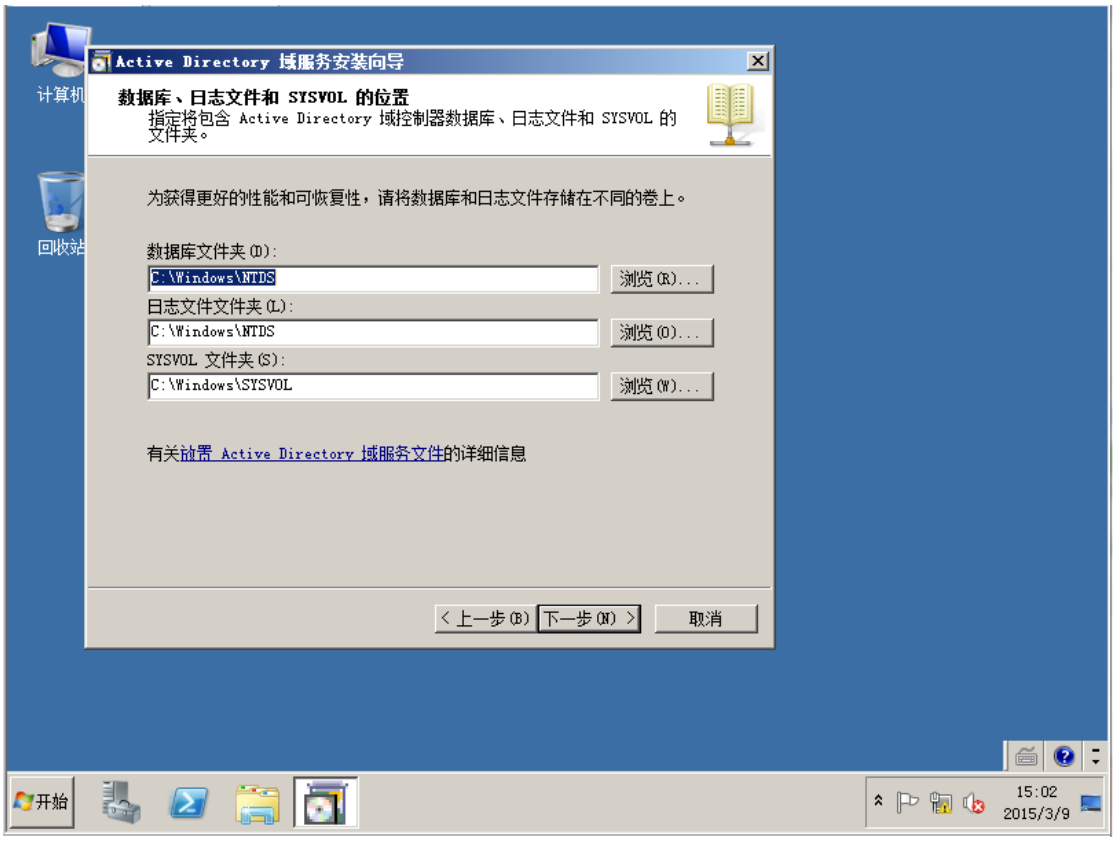
在此选择 DNS 服务器，一并安装。



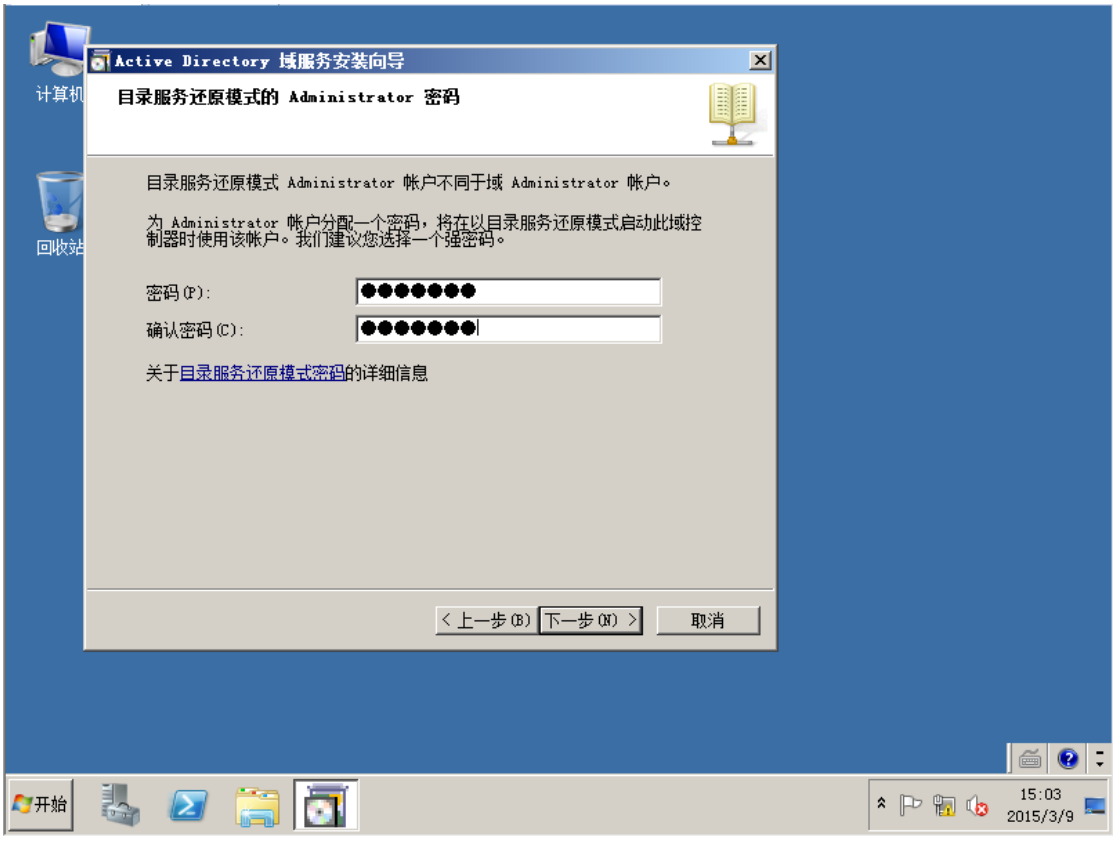
忽略此提示，选择‘是’



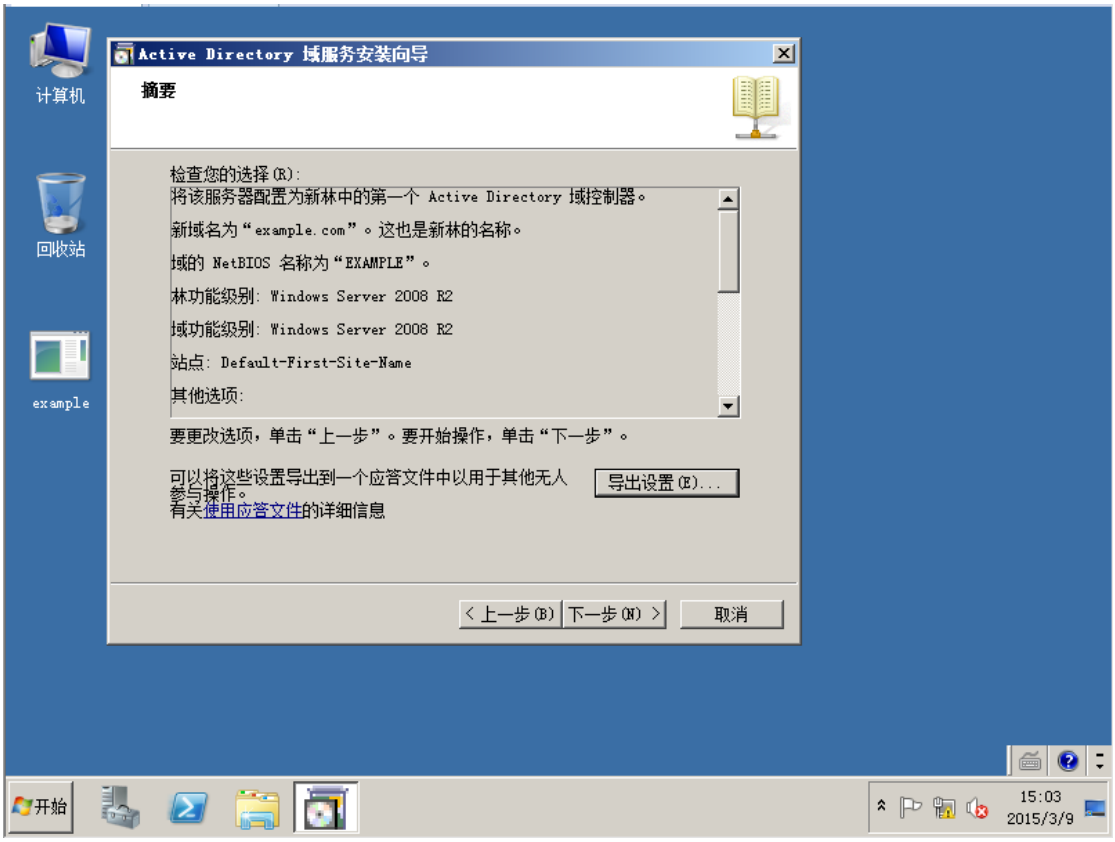
此次选择默认，下一步



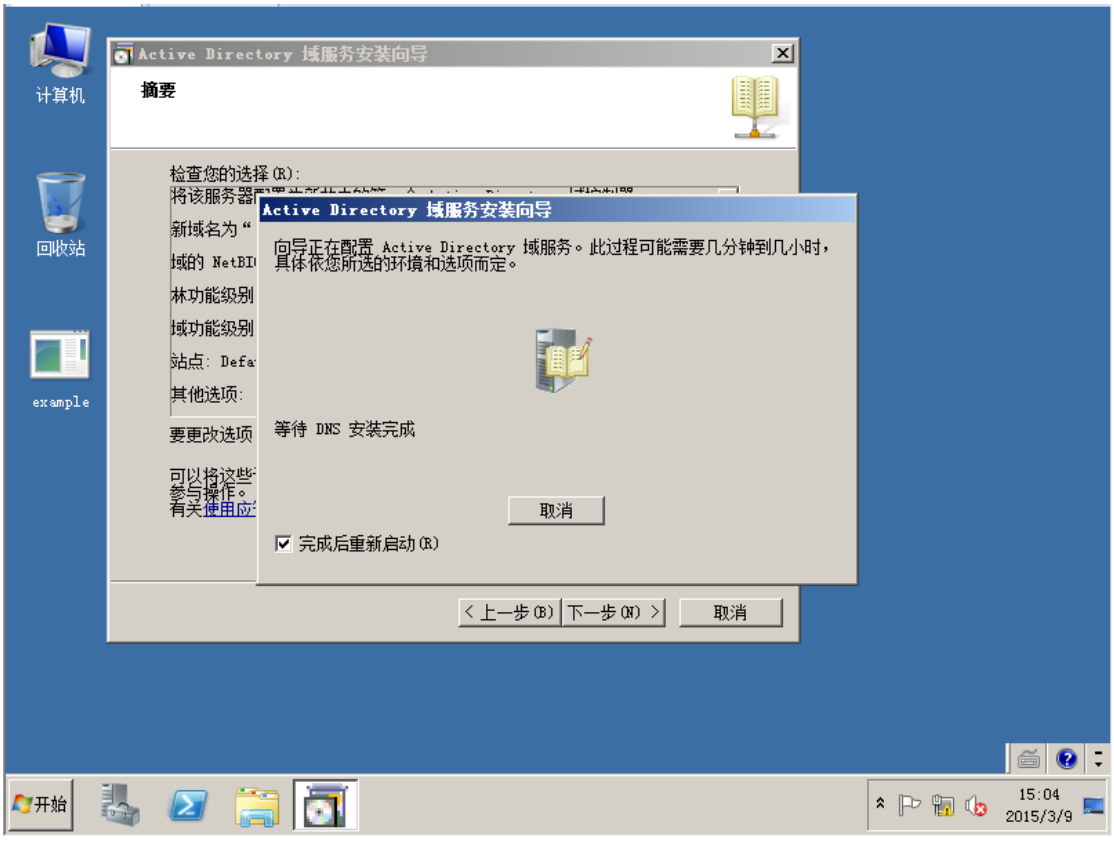
此处输入目录还原模式的独立密码。



此次选择下一步，保持默认。

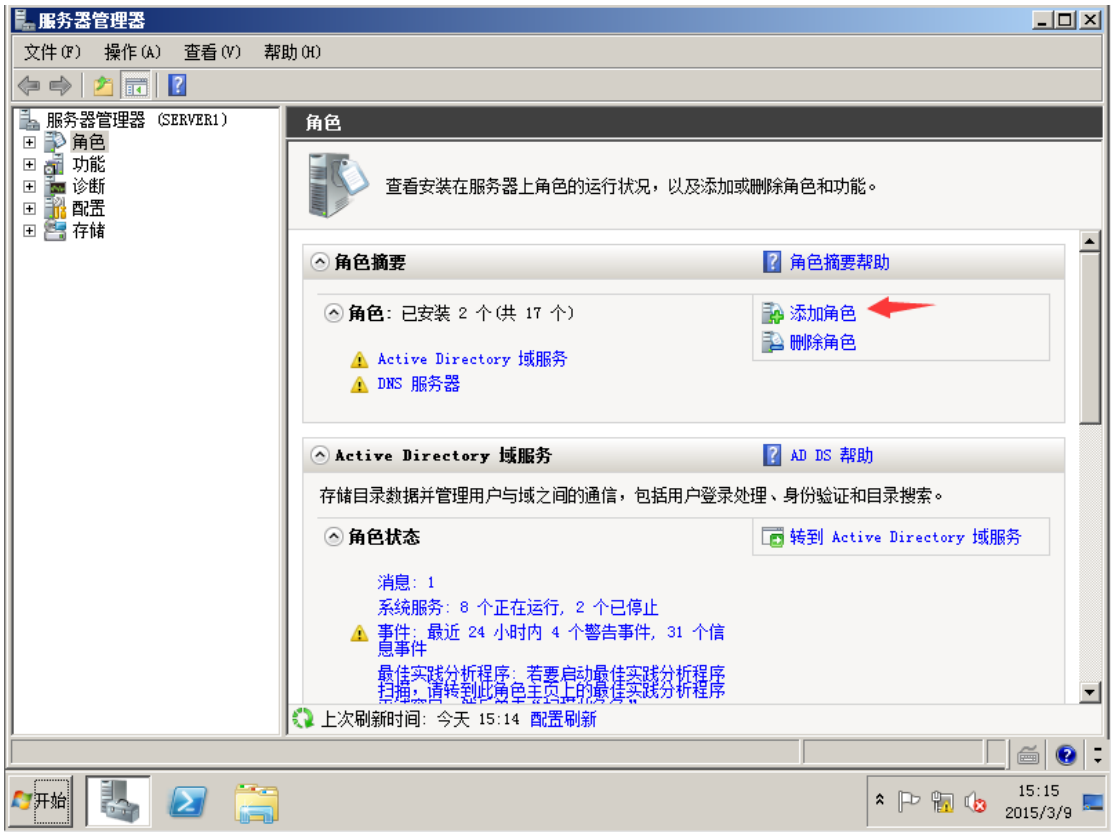


在此勾上完成后重新启动，重启之后，AD 域安装成功。

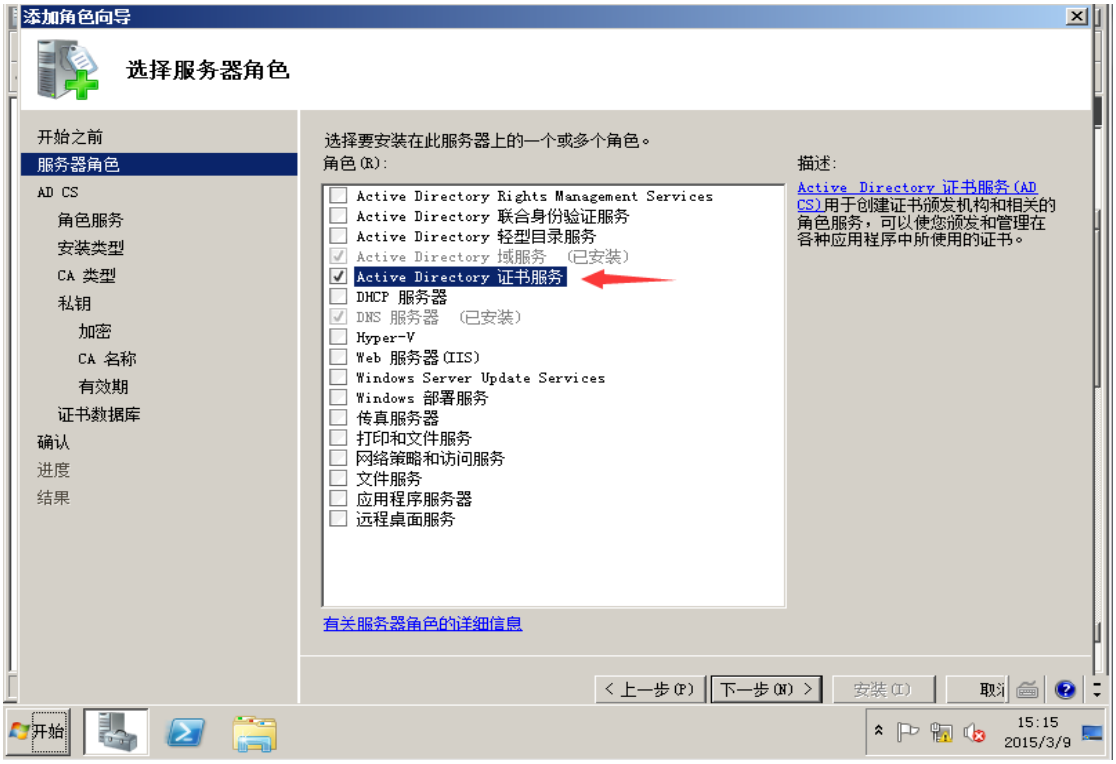


重启之后，原来 server1 的管理员帐号成为了域控制器的管理员帐号，权限最高。域管理员帐号域用户名登录方式 example\administrator 或者 administrator@exampel.com

2.1.3 在 server1 上搭建证书颁发机构 CA

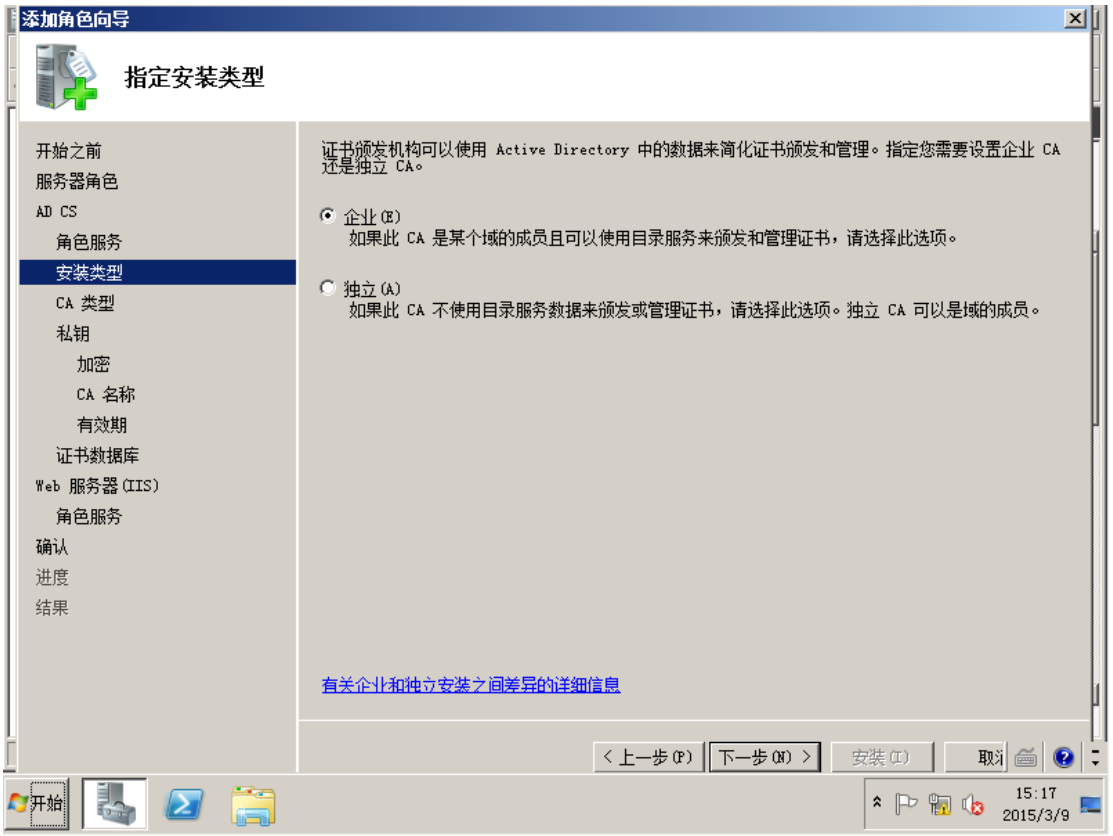


此处选择服务器角色 Active Directory 证书服务



选择证书颁发机构和 web 注册，支持用户通过网页方式申请 CA 证书。

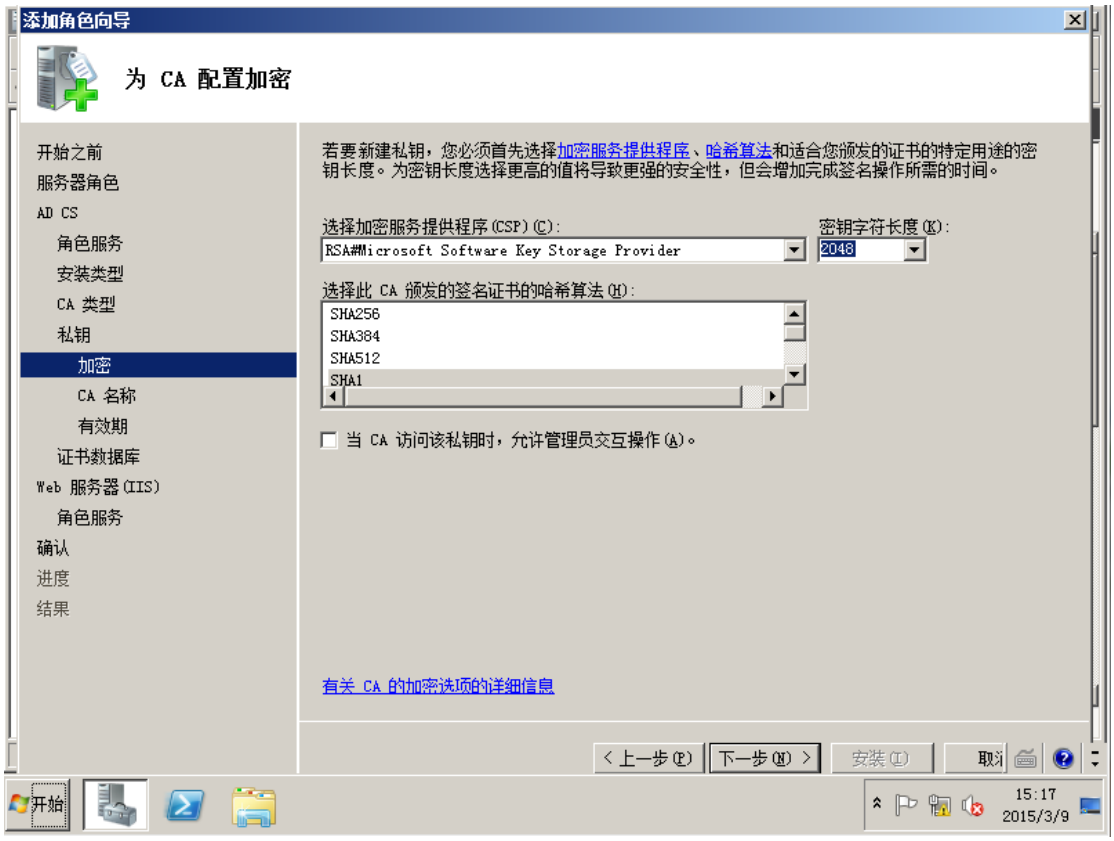
此处选择企业 CA



此处选择根 CA，然后下一步。

此处选择新建私钥，然后下一步

保持默认，然后下一步。

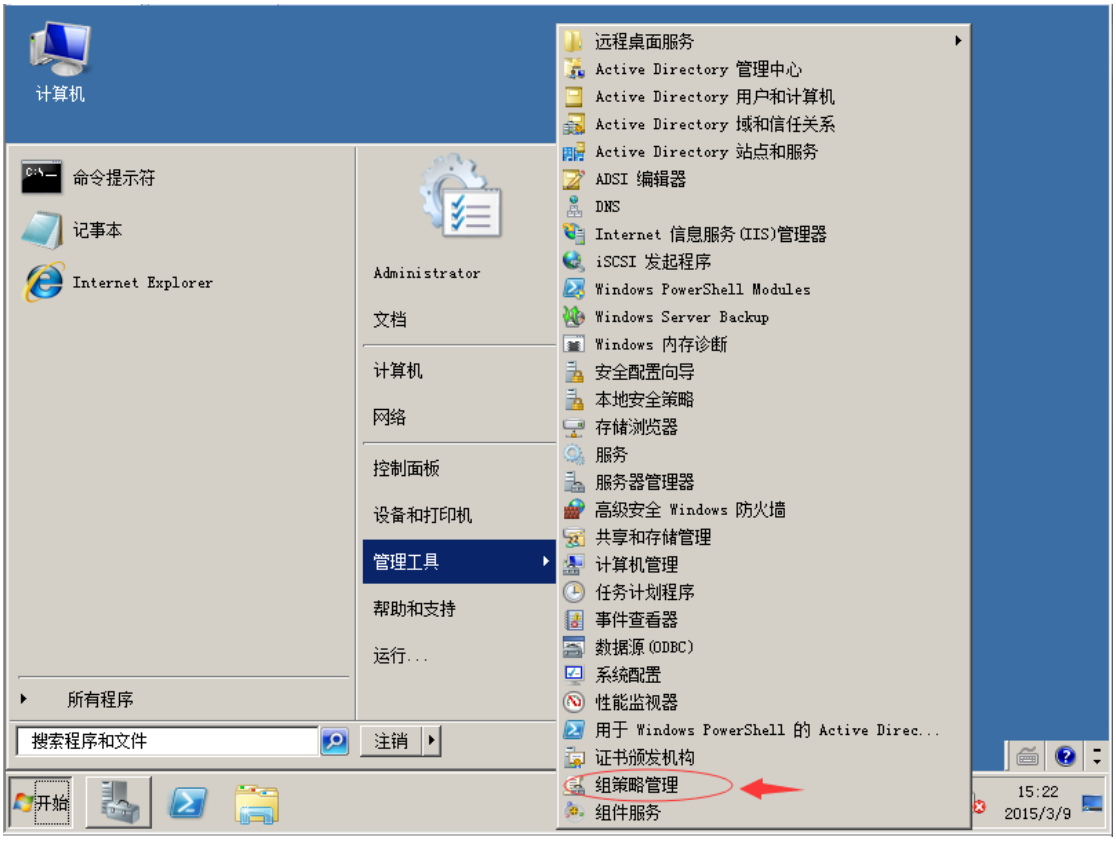

添加角色向导
为 CA 配置加密
开始之前
服务器角色
AD CS
角色服务
安装类型
CA 类型
私钥
加密
CA 名称
有效期
证书数据库
Web 服务器(IIS)
角色服务
确认
进度
结果
若要新建私钥，您必须首先选择加密服务提供程序、哈希算法和适合您颁发的证书的特定用途的密钥长度。为密钥长度选择更高的值将导致更强的安全性，但会增加完成签名操作所需的时间。
选择加密服务提供程序(CSP)(C):
RSA#Microsoft Software Key Storage Provider
密钥字符长度(K):
2048
选择此 CA 颁发的签名证书的哈希算法(H):
SHA256
SHA384
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
开始
15:17
2015/3/9


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):
example-SERVER1-CA
可分辨名称后缀(D):
DC=example,DC=com
可分辨名称的预览(V):
CN=example-SERVER1-CA,DC=example,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
开始
15:18
2015/3/9

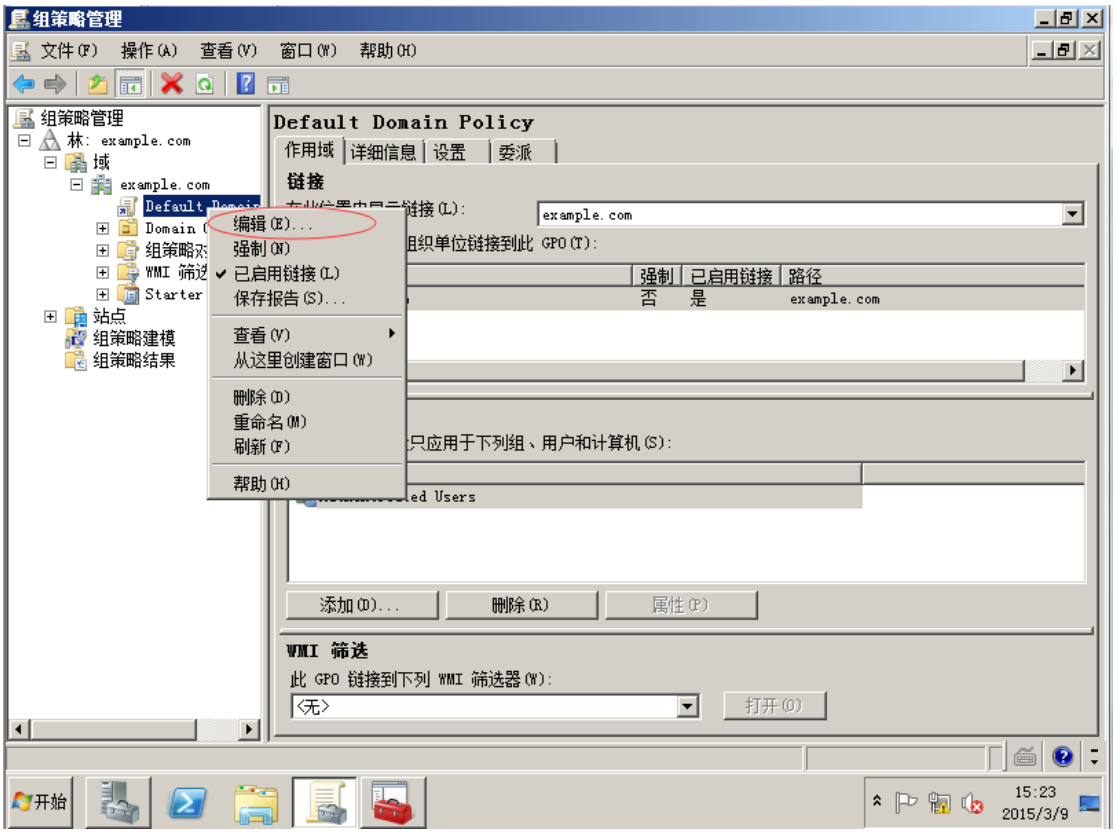
保持默认，然后下一步。

此次选择安装，安装完成之后，关闭此对话框，CA 安装完毕。

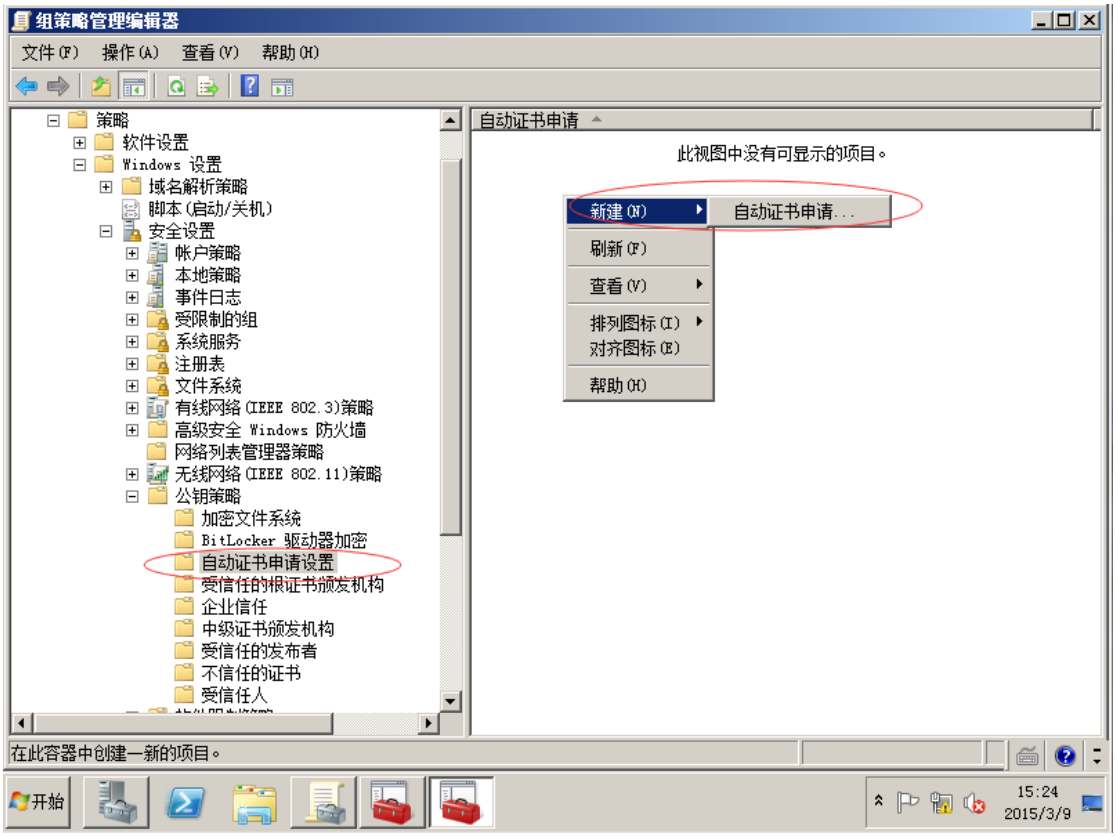
配置组策略，新加域的计算机，自动颁发计算机证书。在管理工具中选择组策略管理



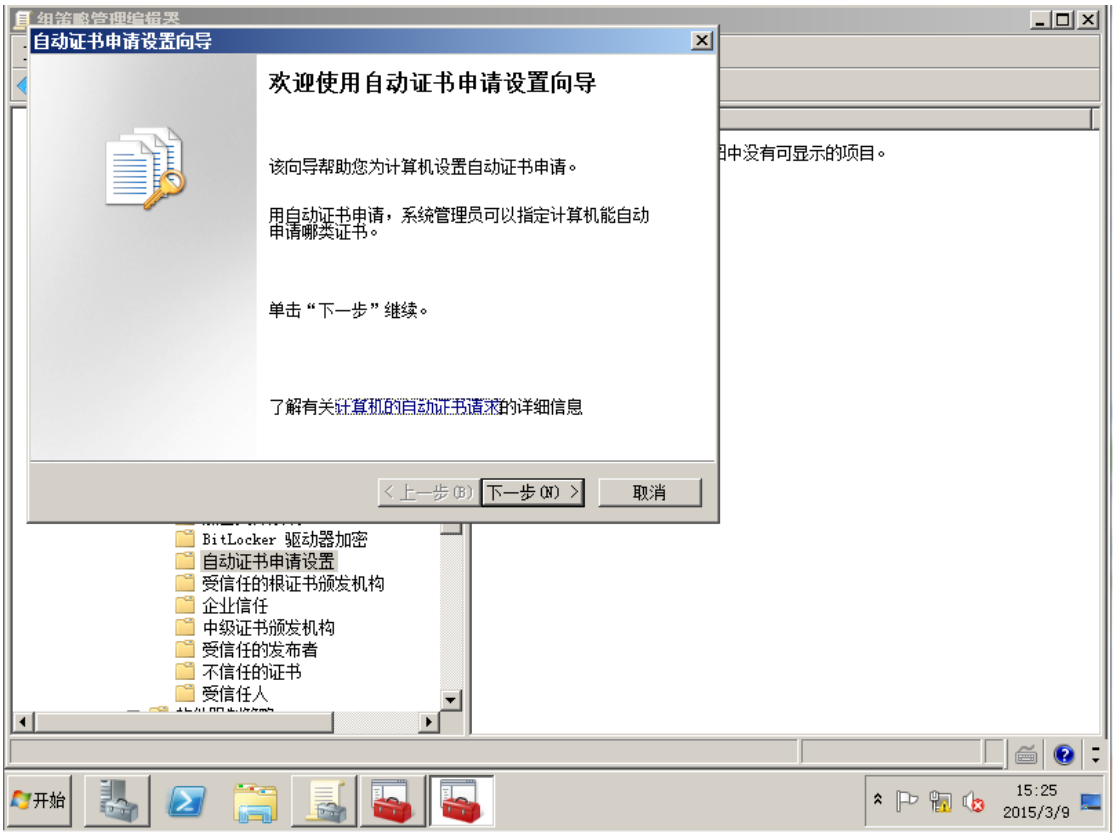
选择域默认 GPO 链接，选择编辑



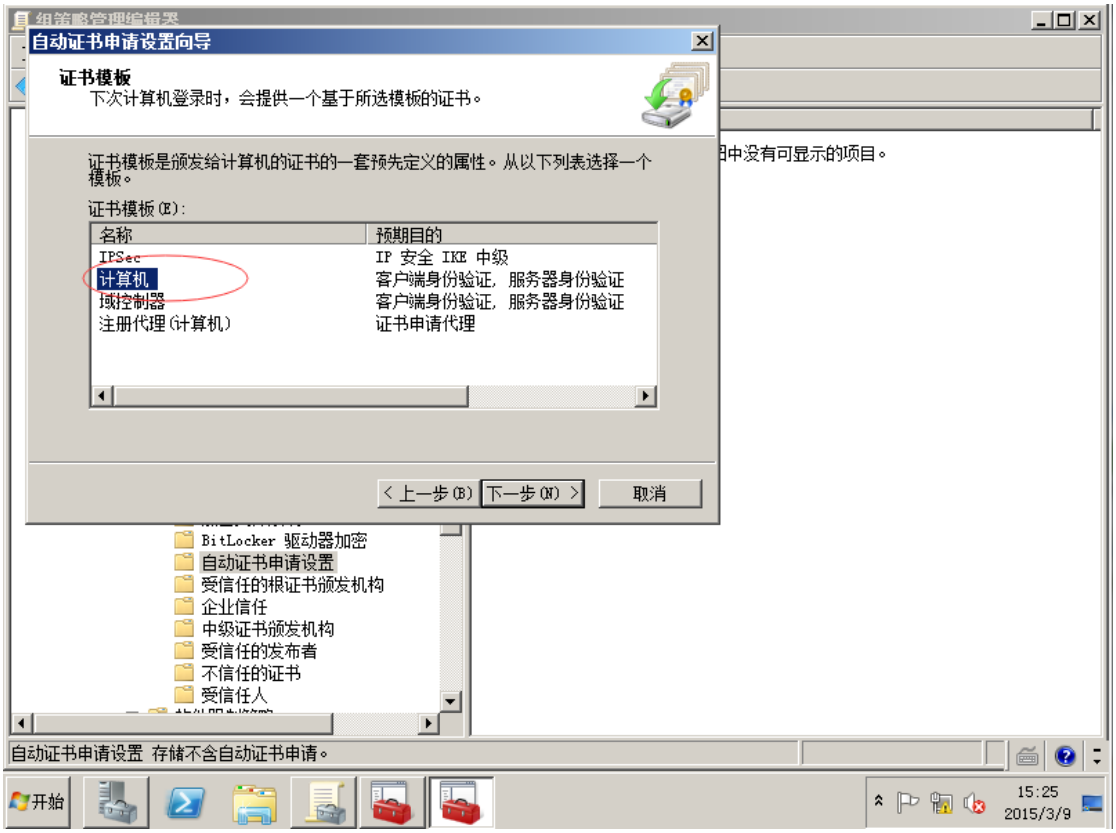
在计算机设置中找到自动证书申请设置，在右边的空白处，右键选择新建自动证书申请。



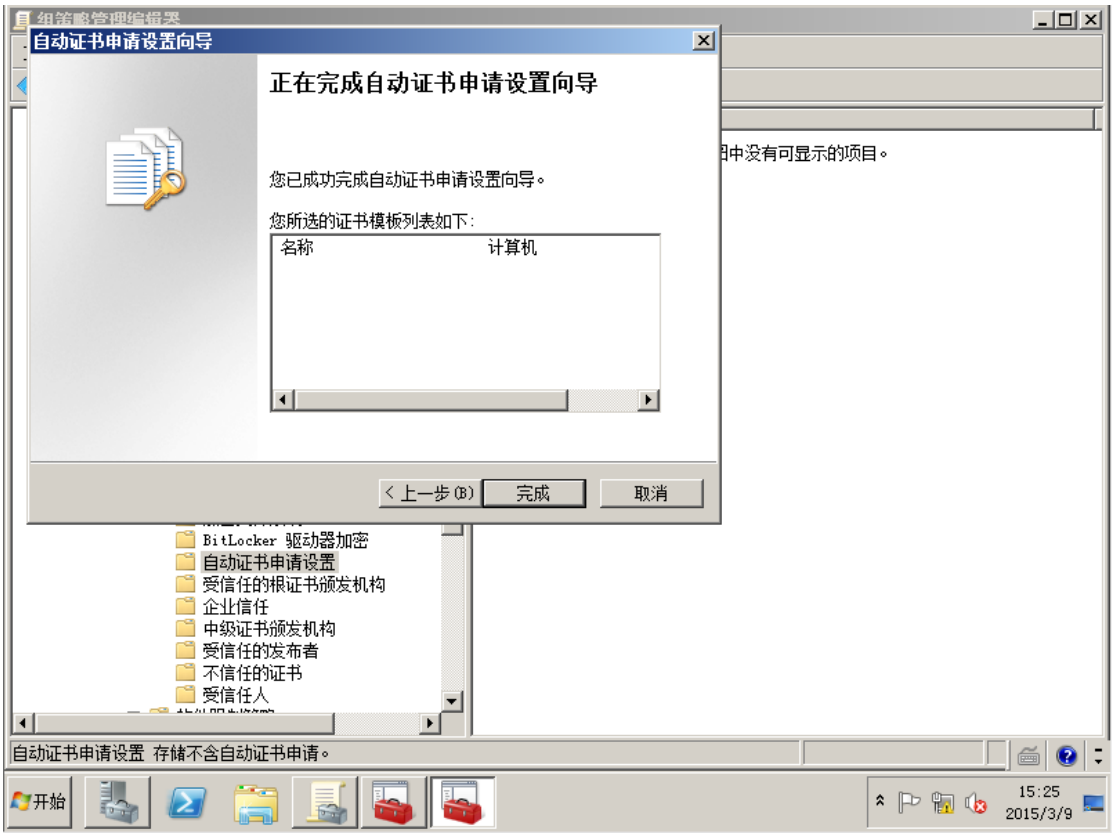
在此配置向导页面，选择下一步。



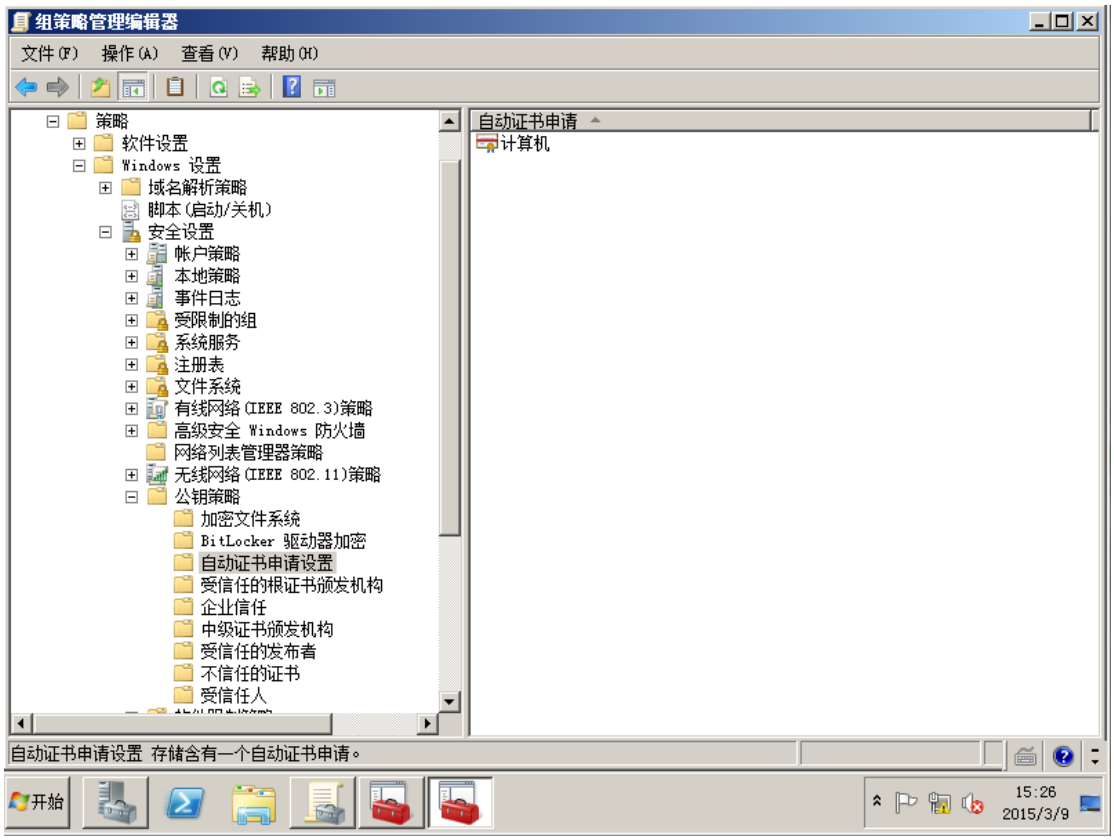
此处选择计算机，然后下一步。



此处选择完成即可。

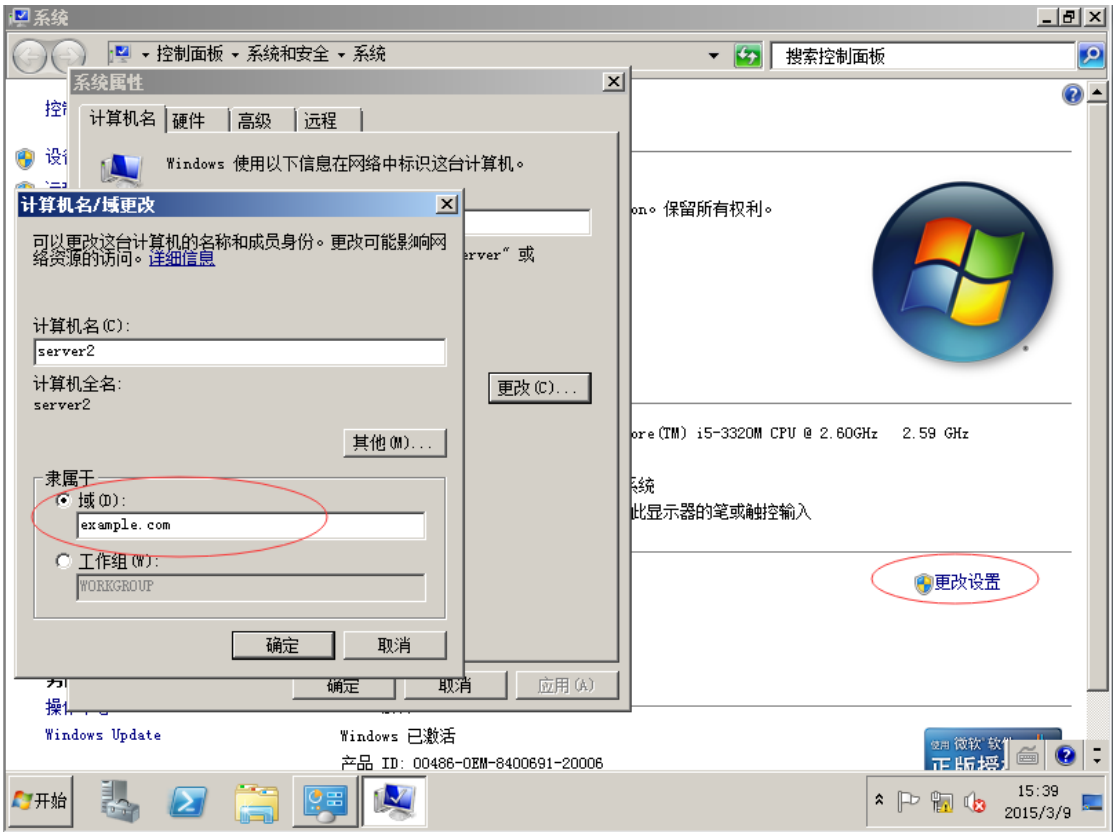


正常设置之后，此次会有一个自动颁发计算机证书的策略。

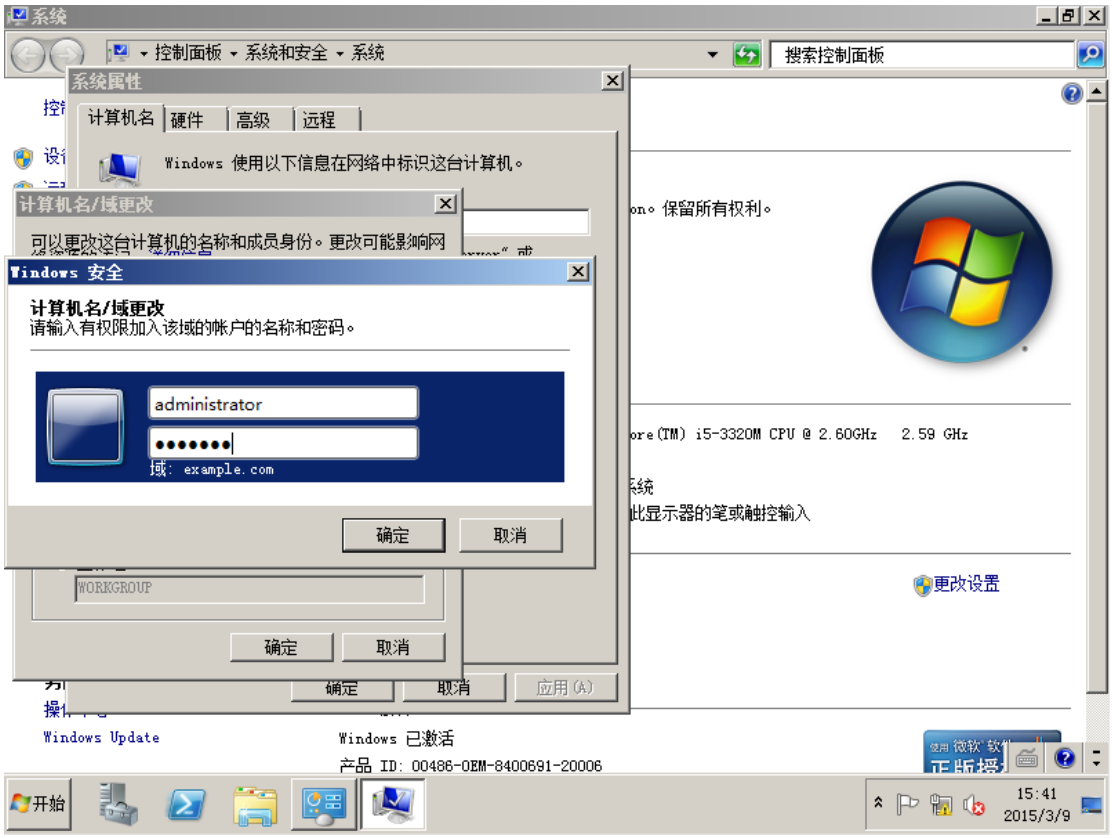


2.1.4 在 server2 上搭建 Radius 服务器

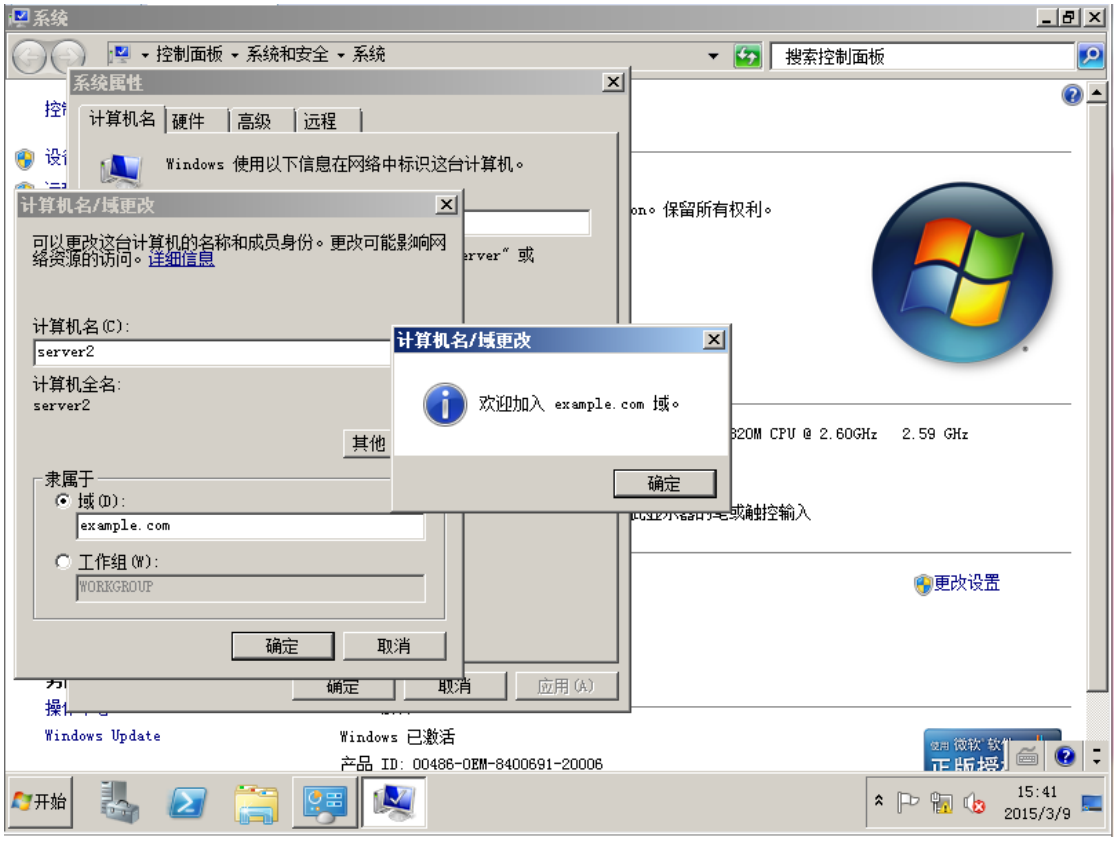
将 server2 加入到 example.com 域中，在系统属性中选择更改设置—更改计算机名称—域，写上域的名称。



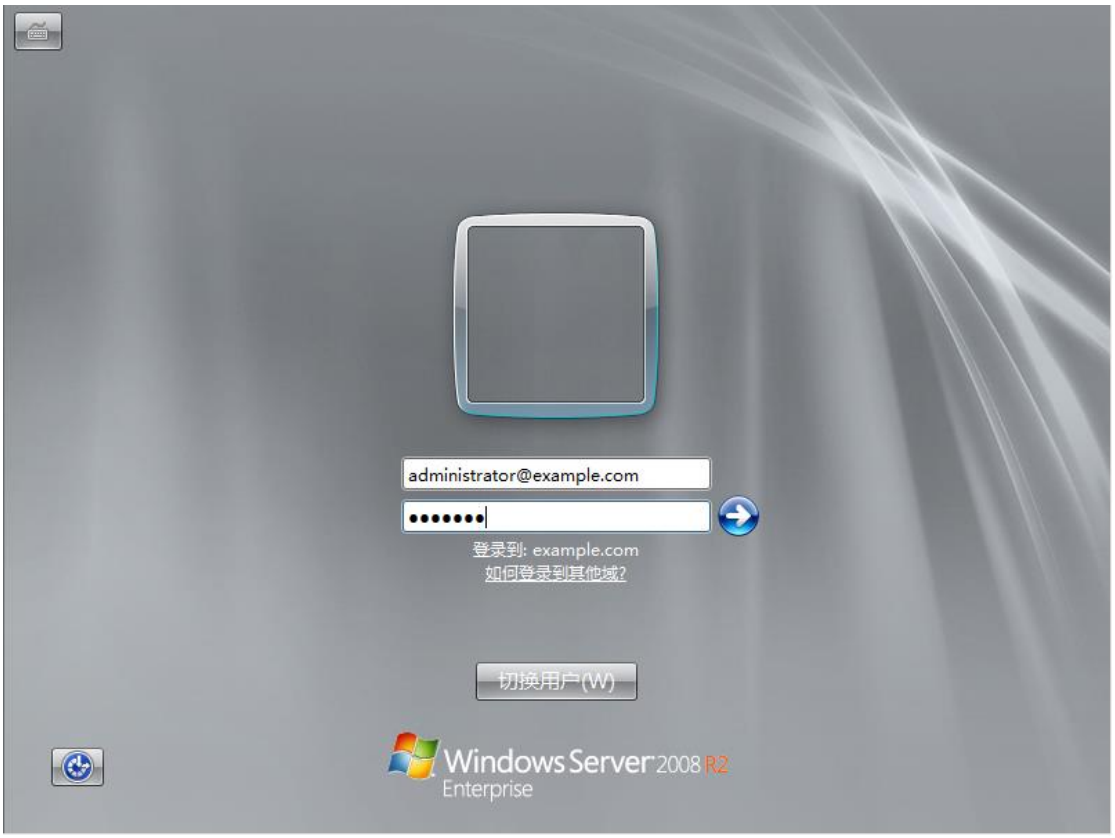
在此输入域控制器的管理员帐号密码，允许 server2 加入域。



此处提示 server2 已经成功加入到域中，完成之后需要重启计算机。

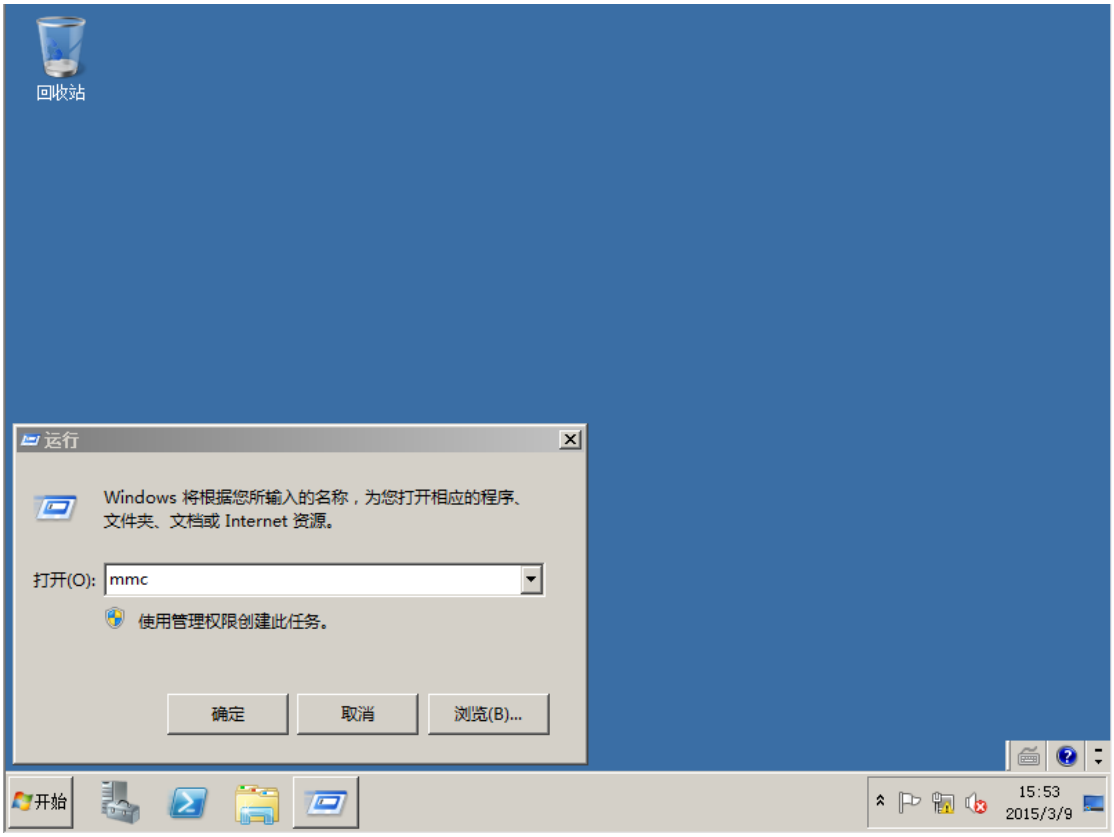


Server2 重启之后，已经加入到域中，在此我们使用域控制器的管理员帐号来登录 server2.

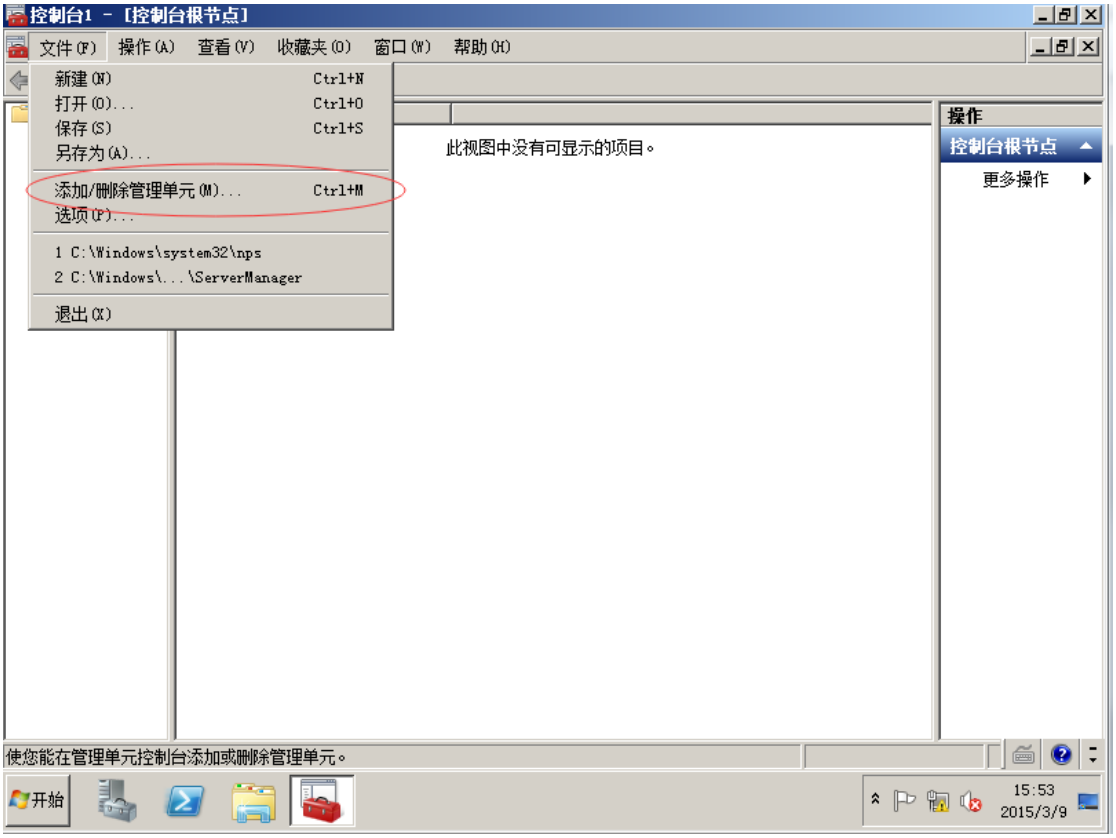


打开服务器管理器可以看到 server2 已经加入到 example.com 域中。

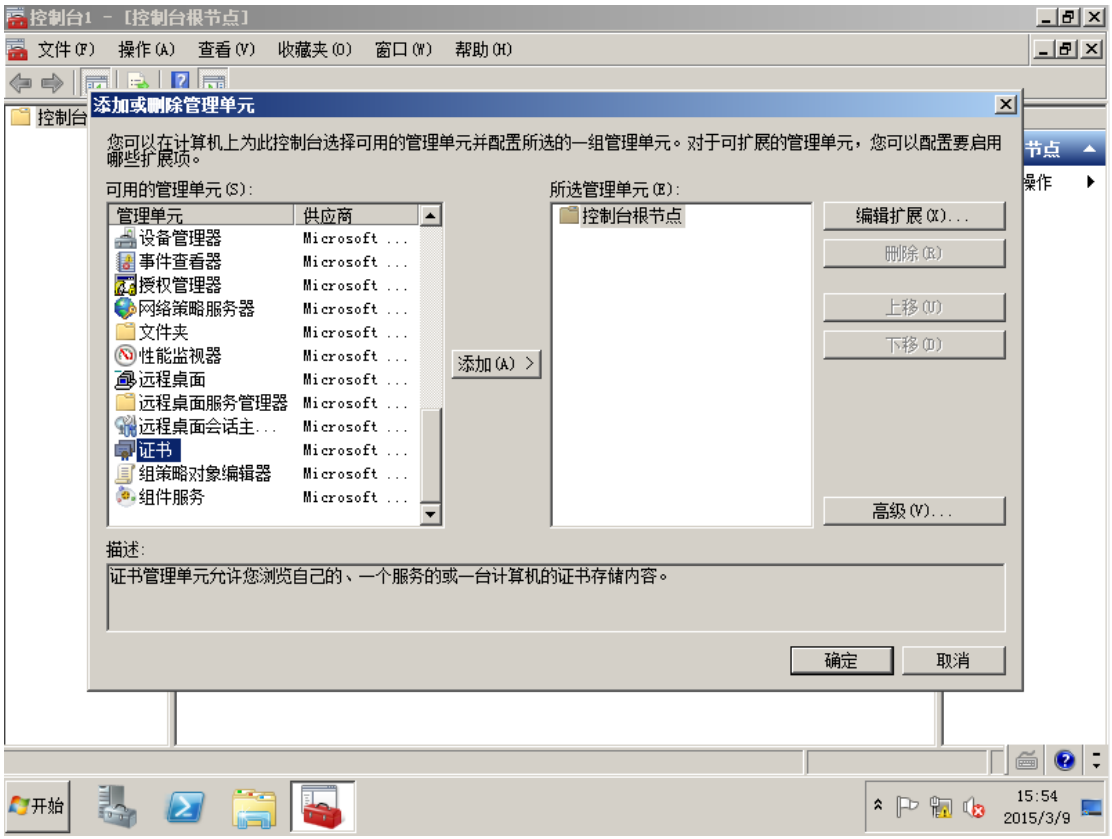
在运行中输入 mmc，打开控制台



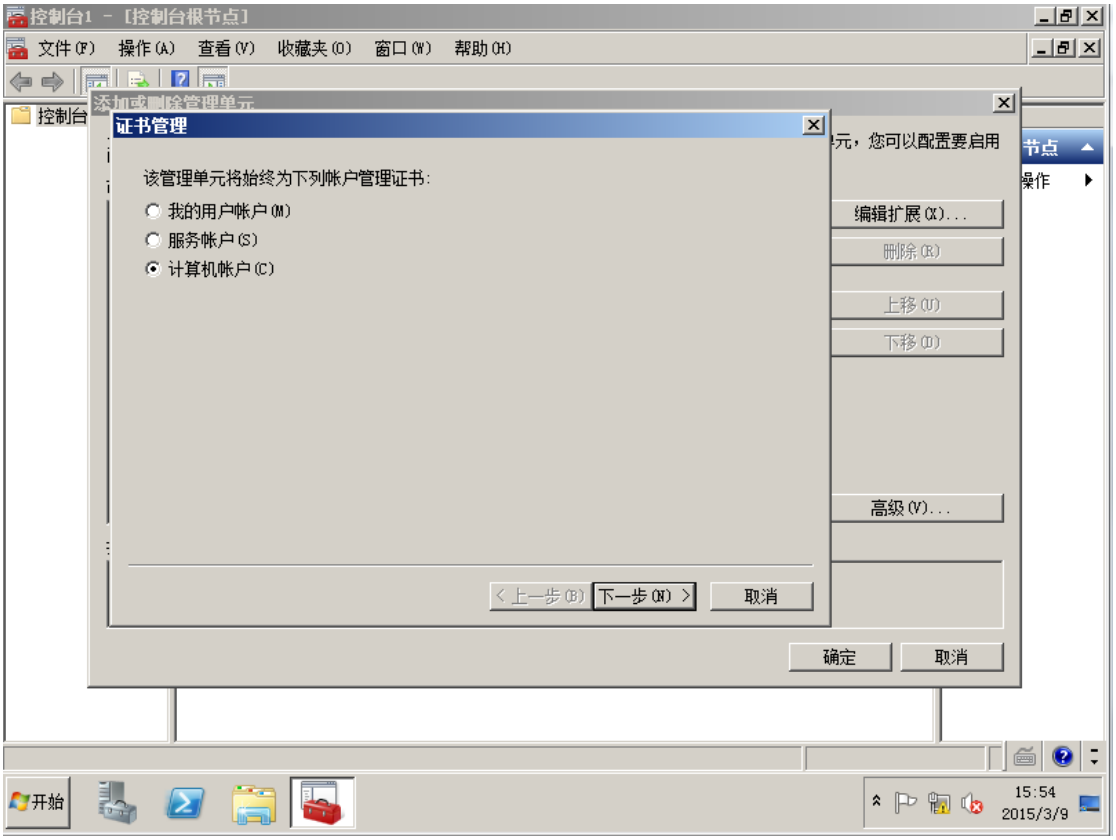
选择添加删除管理单元



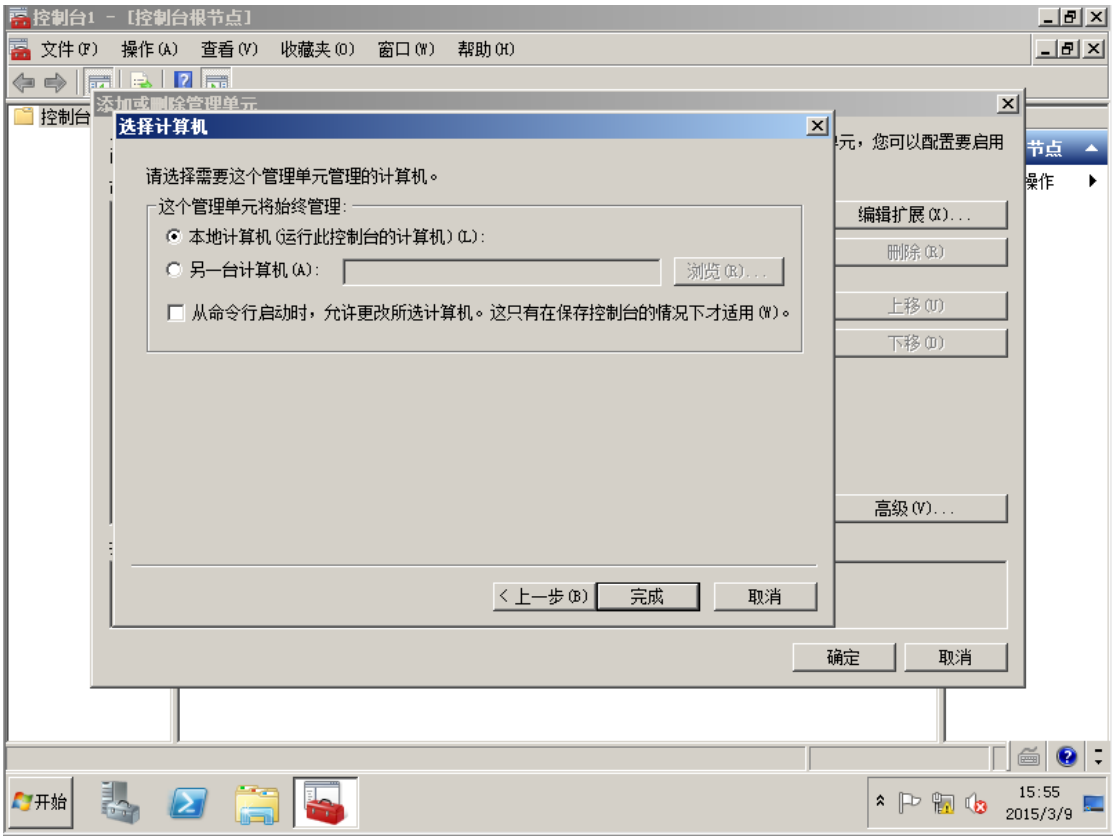
左边选择证书，然后选择添加。

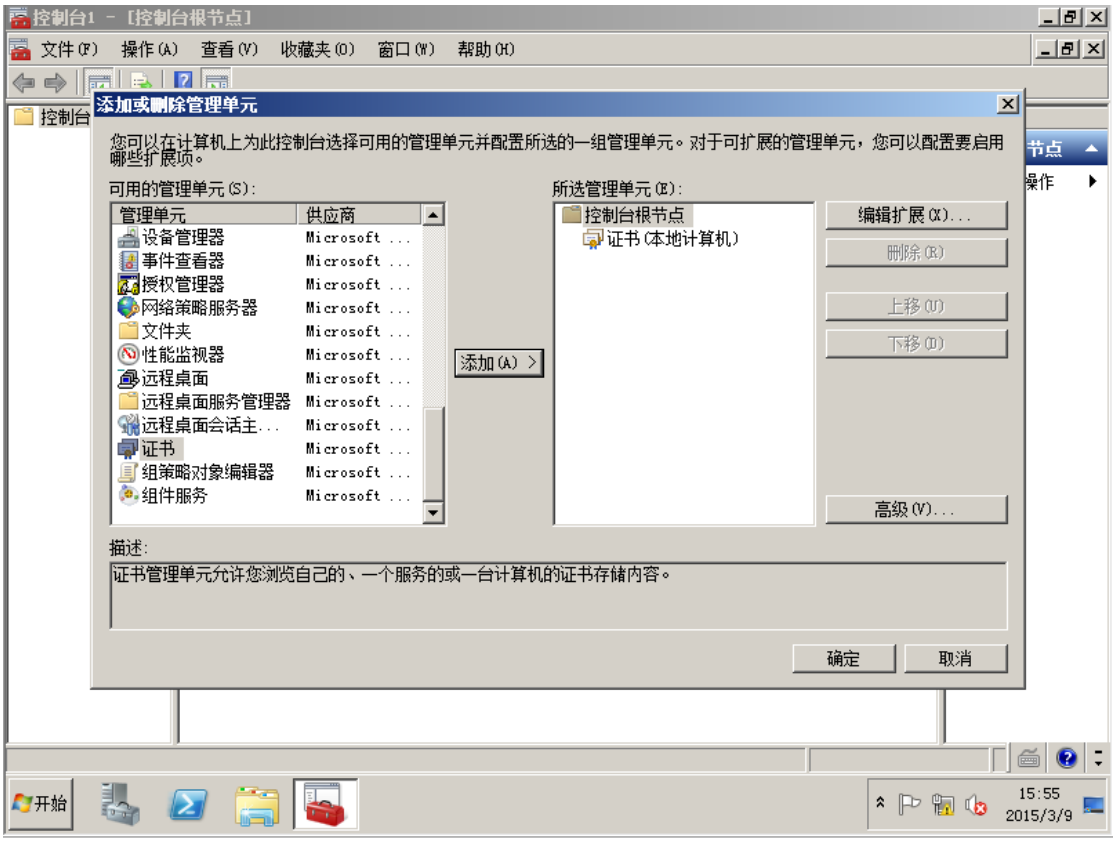


在此选择计算机证书，然后下一步。

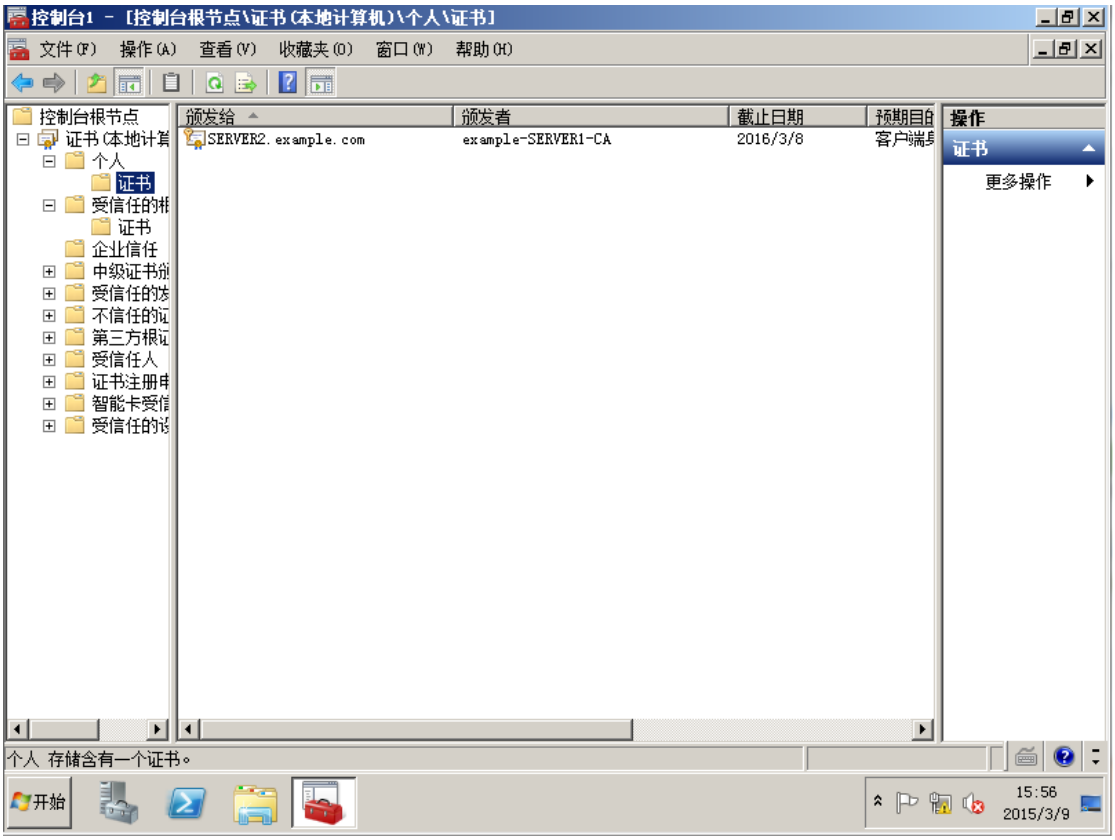


保持默认，选择下一步。

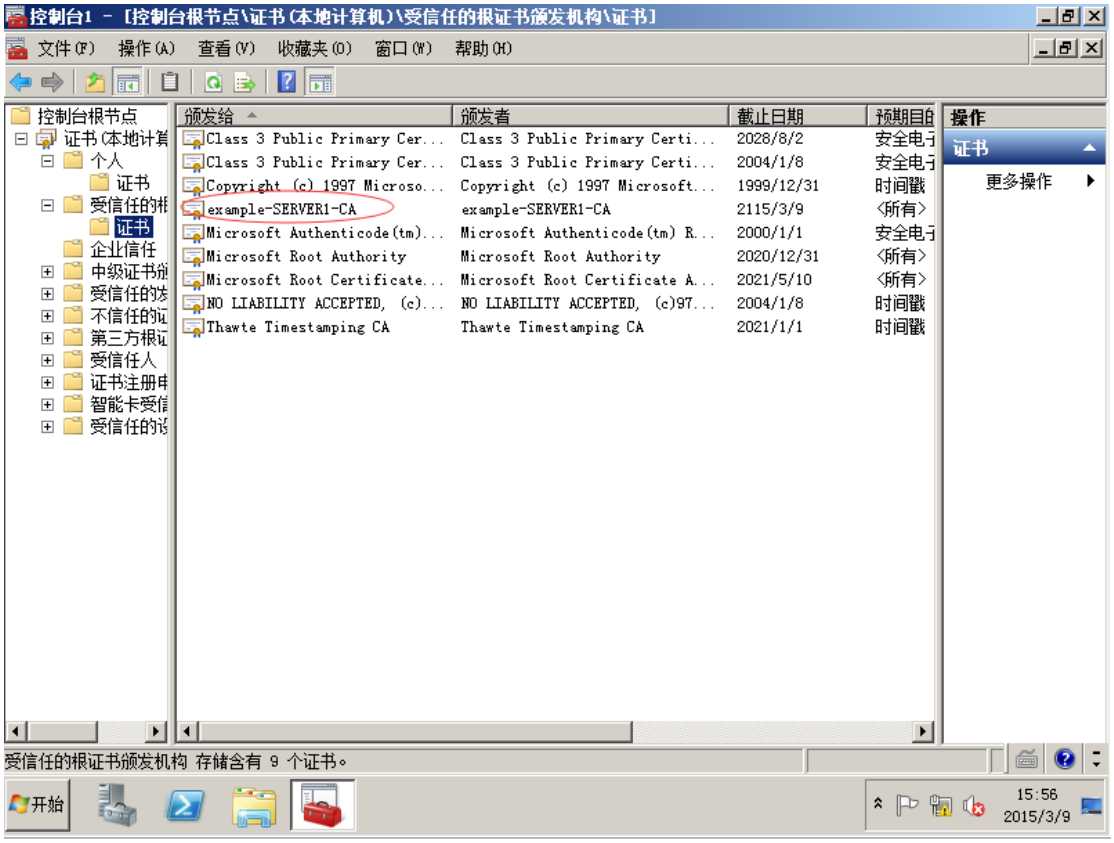




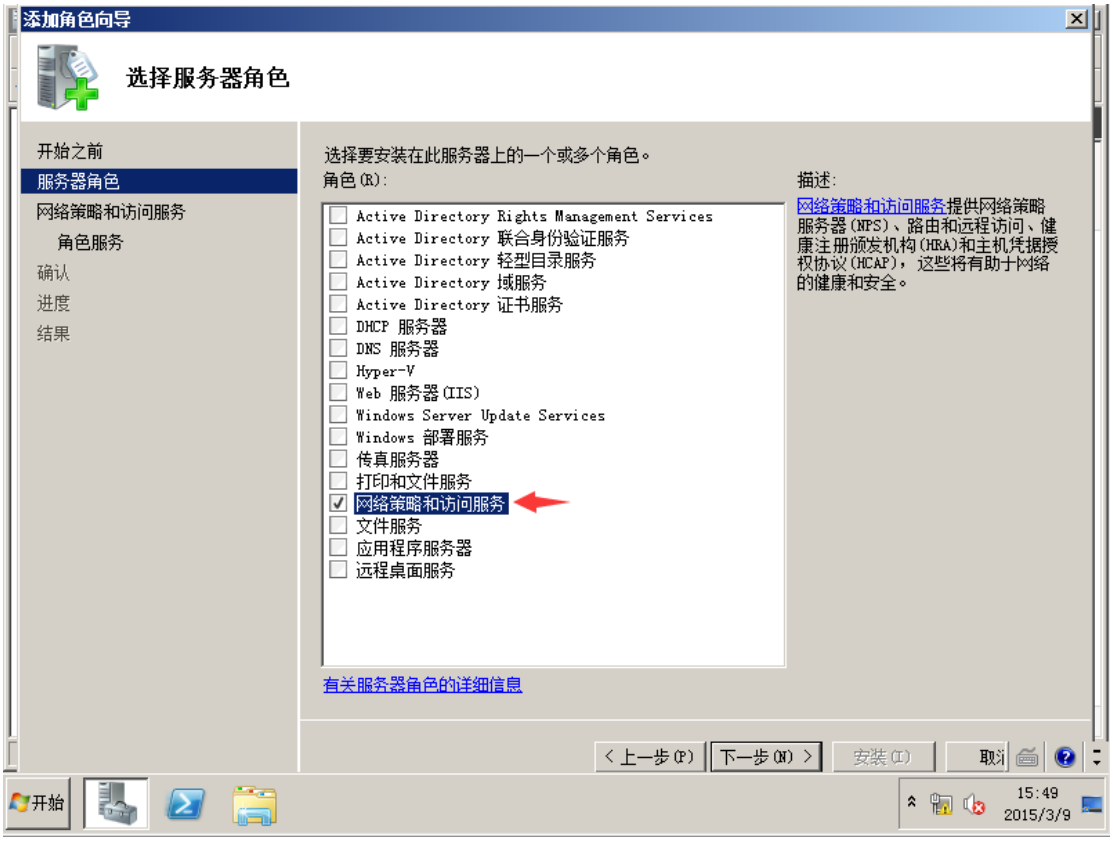
在个人证书中，可以看到一个计算机证书，之前的自动颁发证书策略生效。



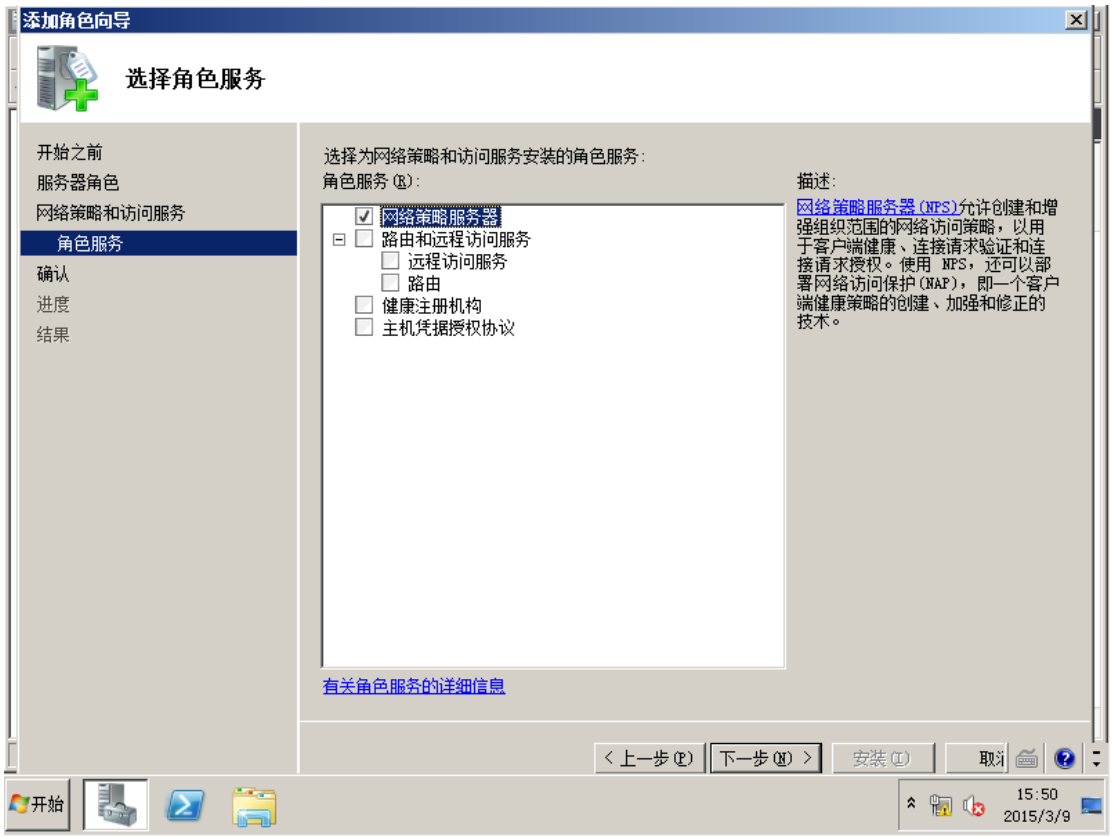
在受信任的根证书中可以看到 server1 颁发的根证书。



打开服务器管理器，选择添加角色，选择网络策略和访问服务

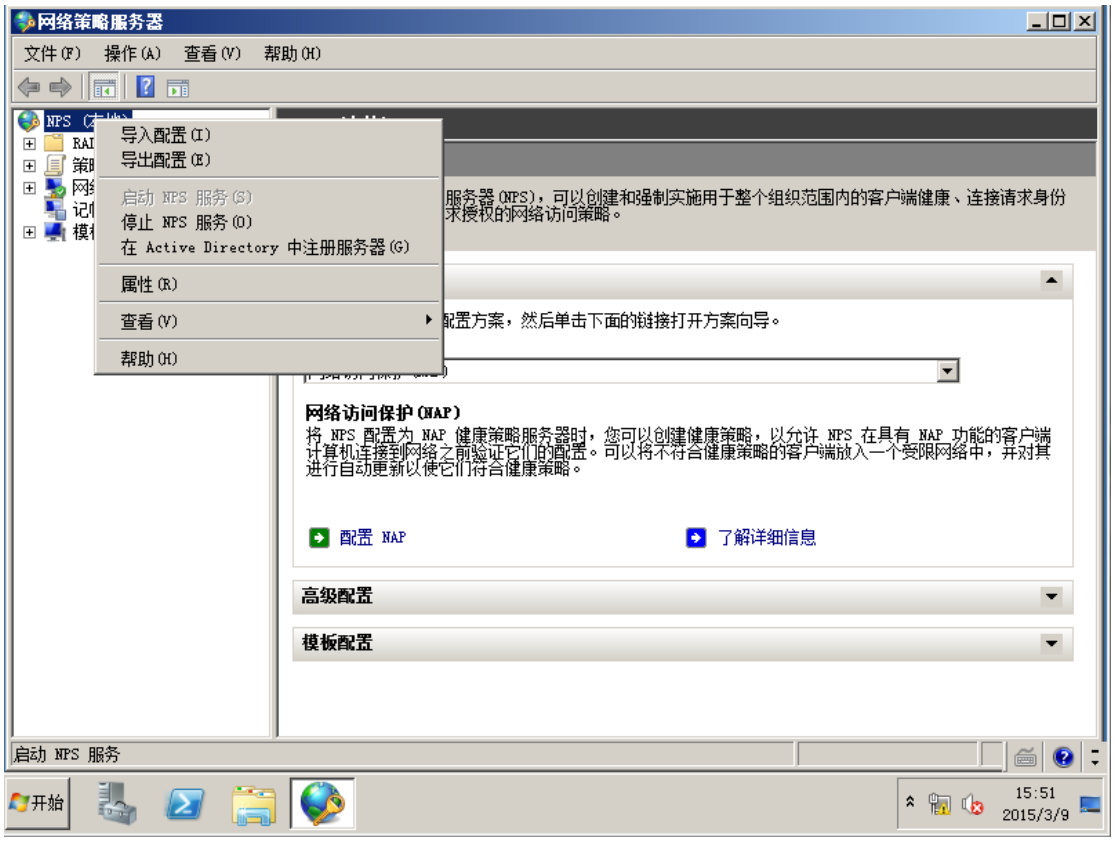


选择网络策略服务器

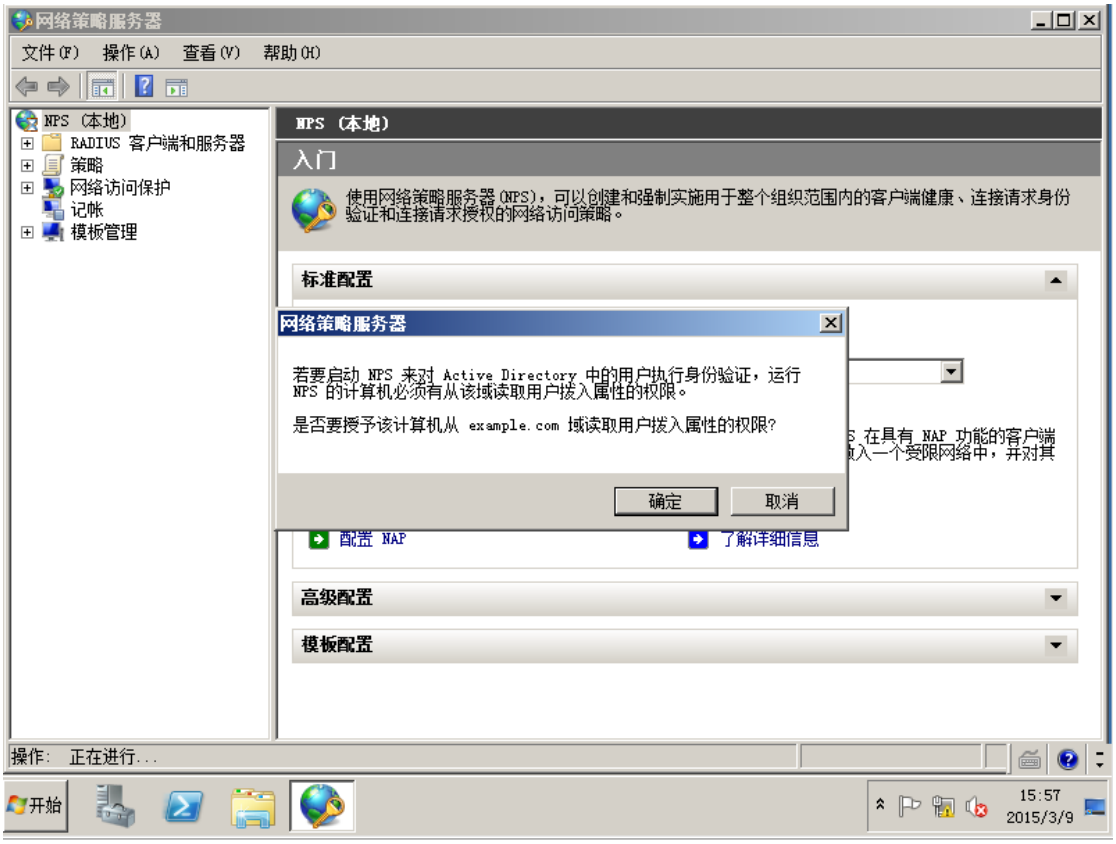


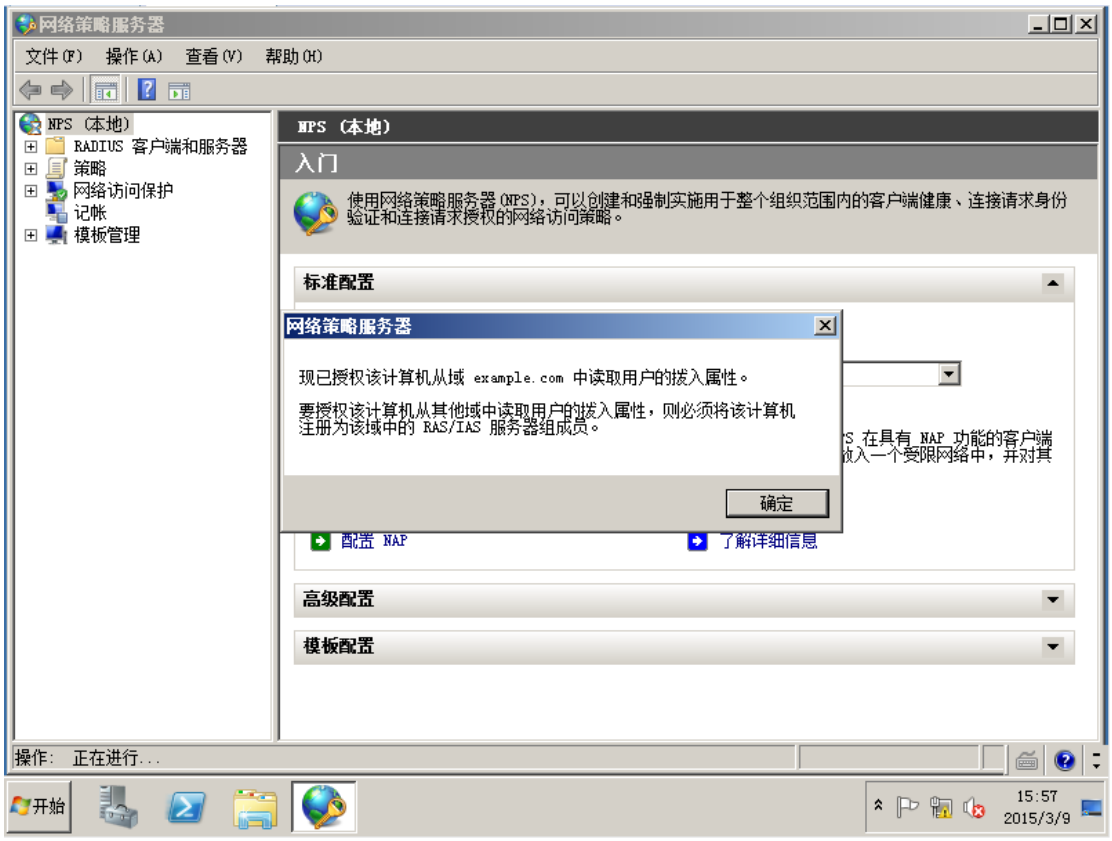
选择安装。

安装完成之后，打开 NPS，在此页面选择在 active directory 中注册服务器。

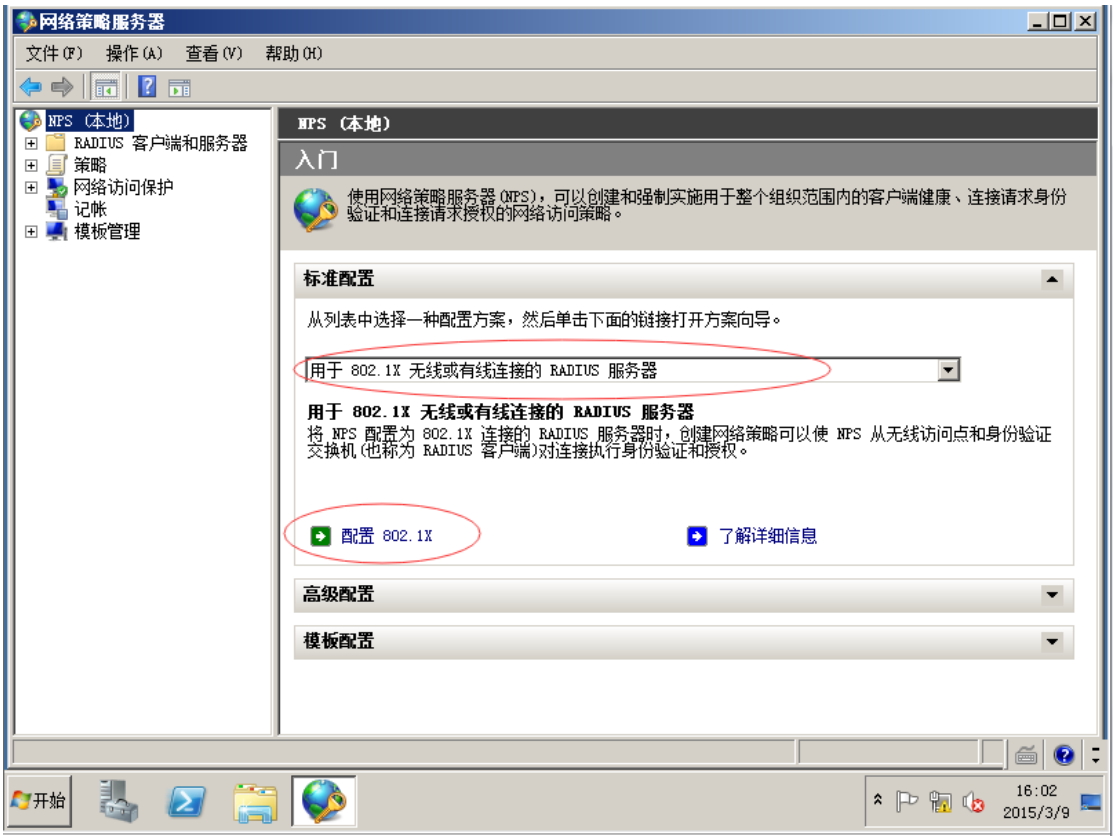


在此选择，确定。

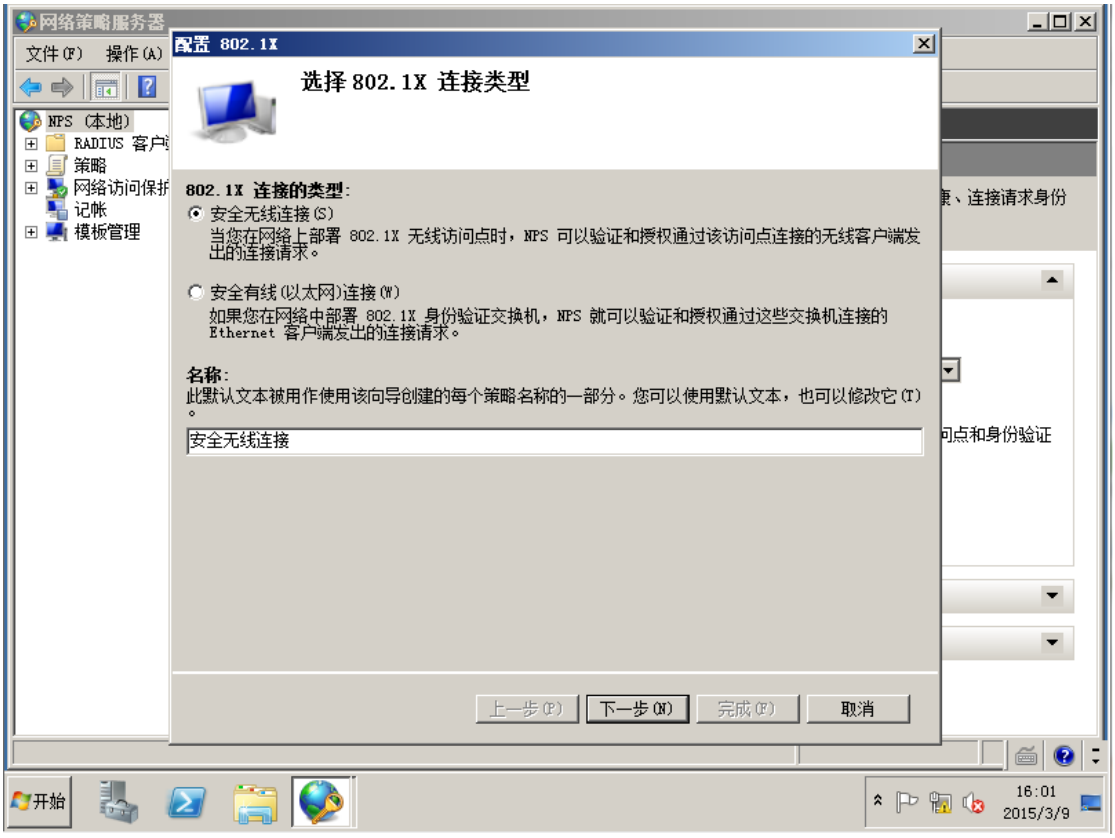




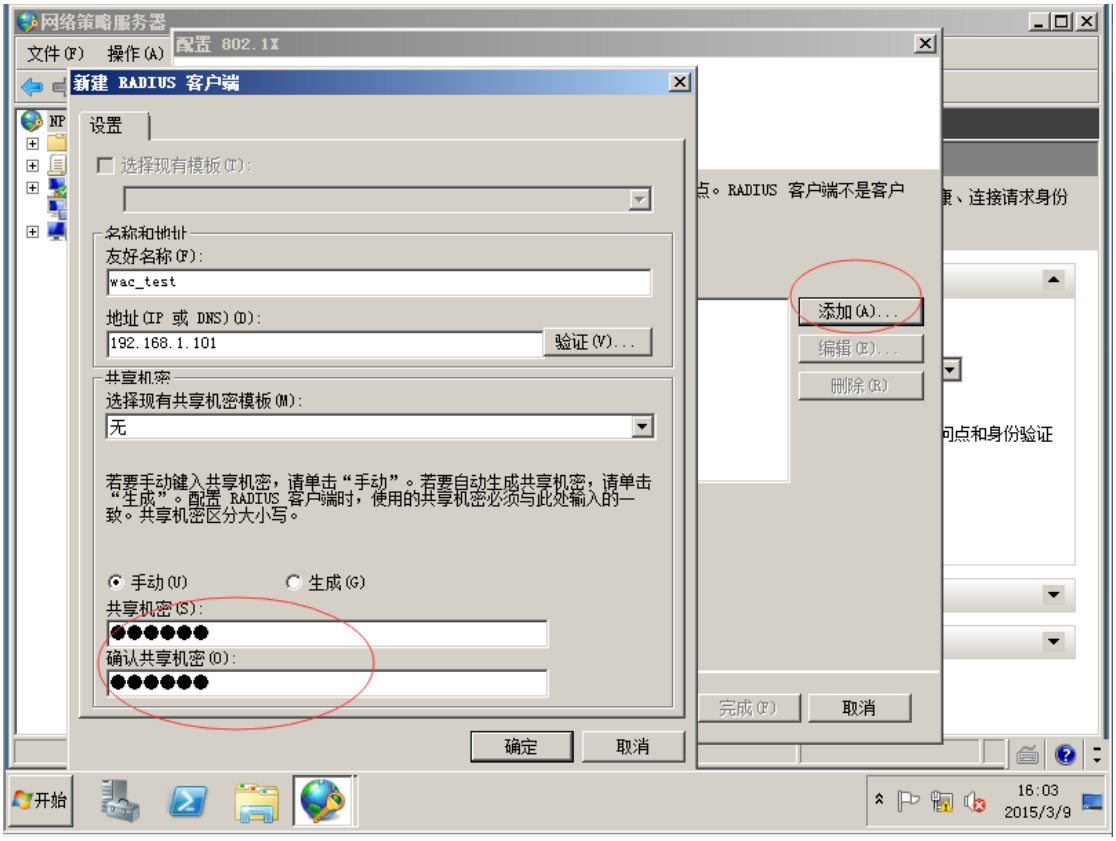
在此选择用于 802.11x 无线有线连接的 radius 服务器，然后选择配置 802.11x



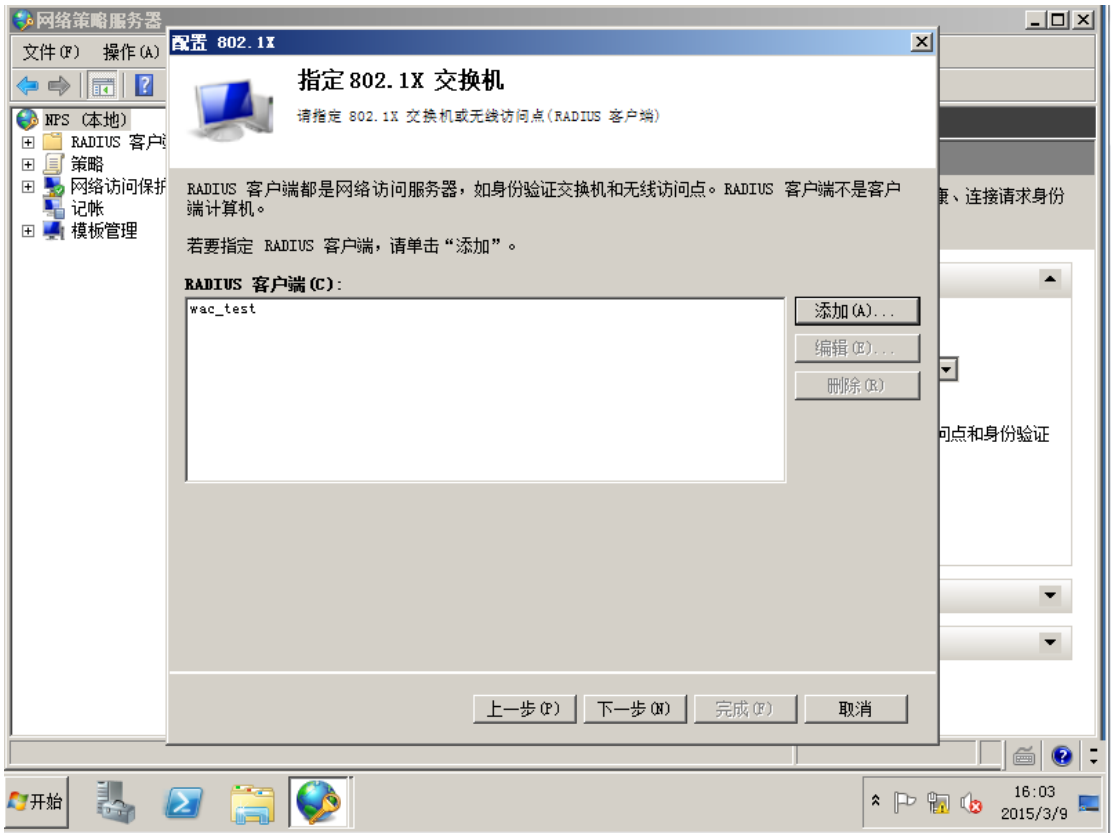
选择安全的无线连接，然后选择下一步。



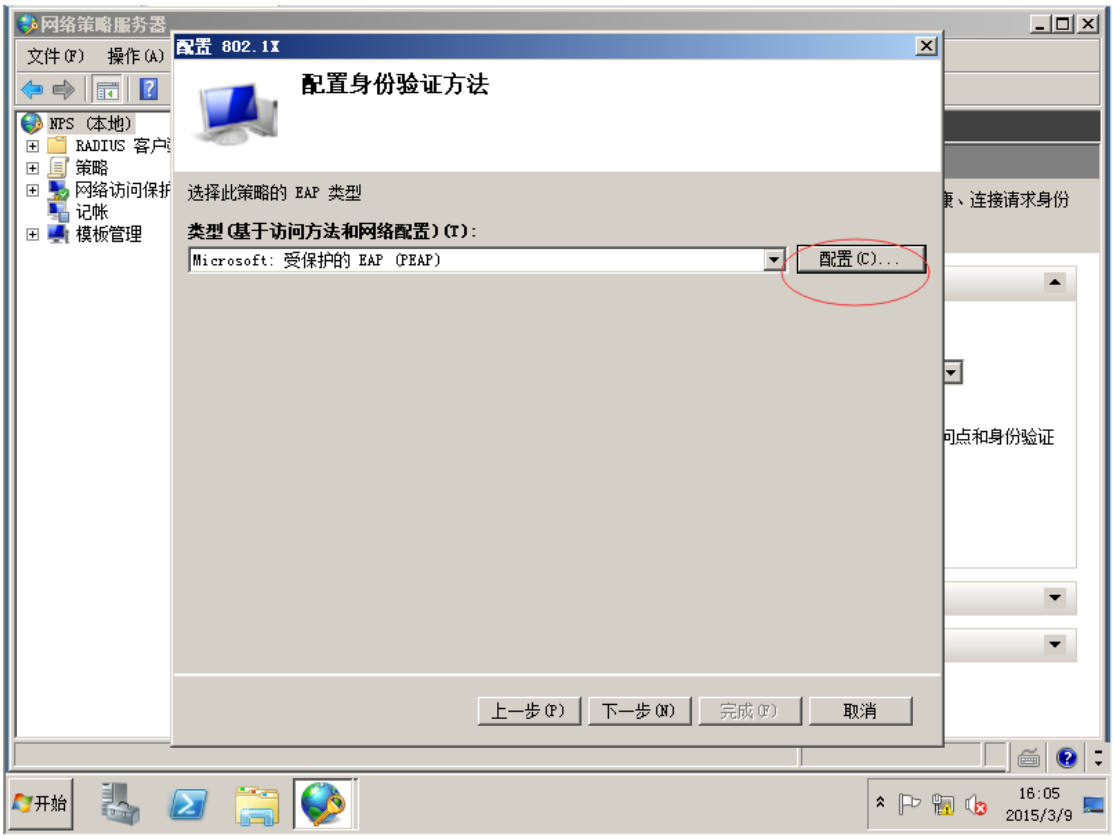
在 radius 客户端选择添加，此次写入 WAC 的 IP 地址和共享密码。



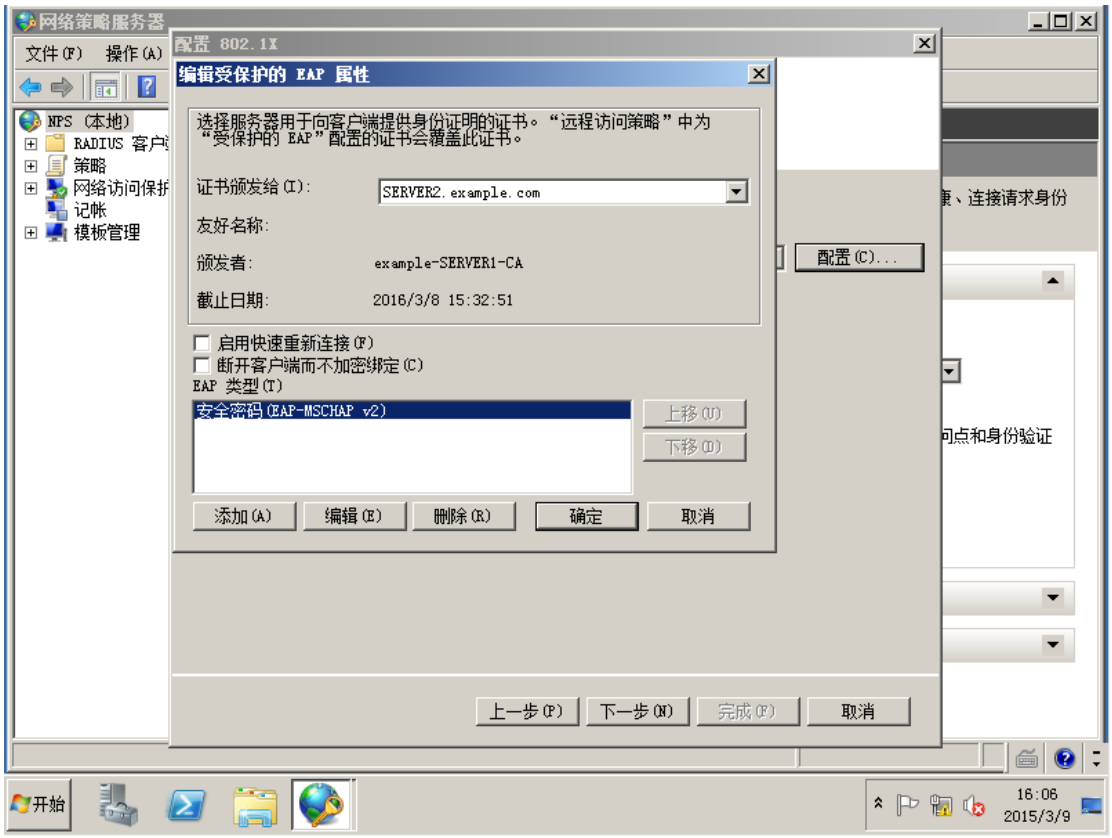
添加完成之后，选择下一步。



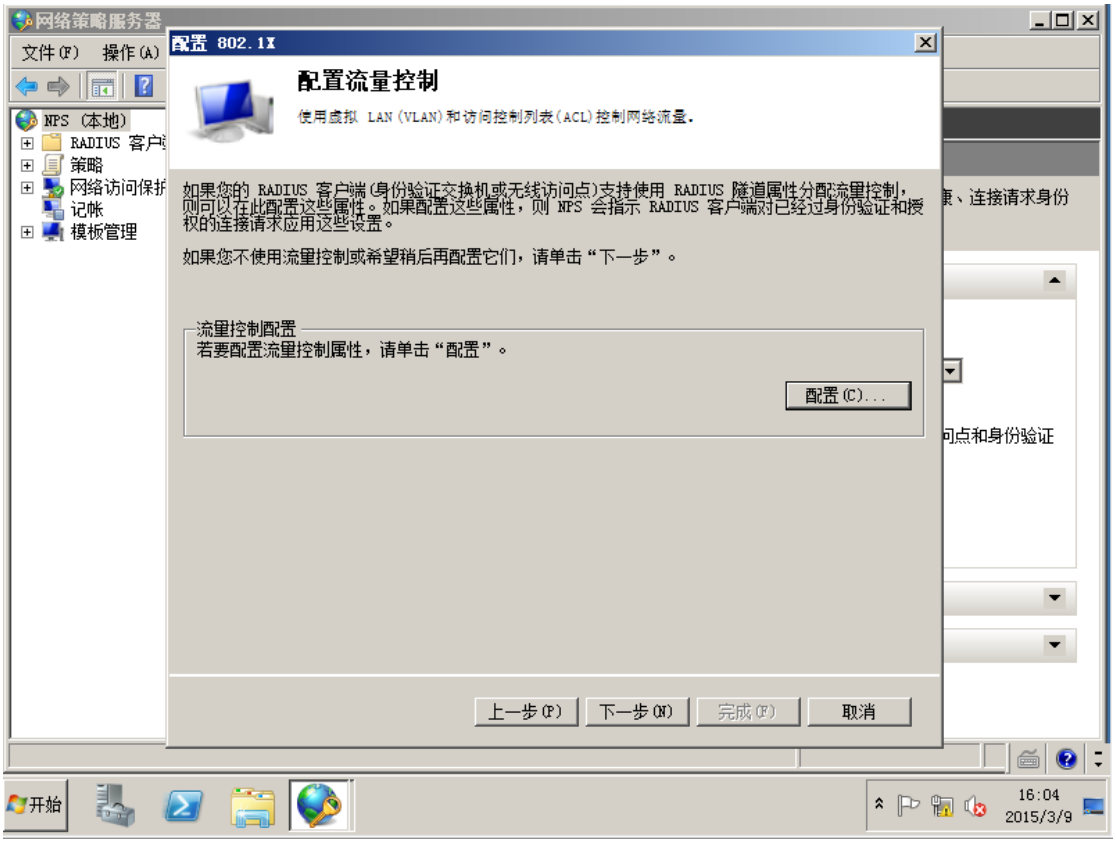
在此页面选择受保护的 EAP（PEAP），然后选择配置。



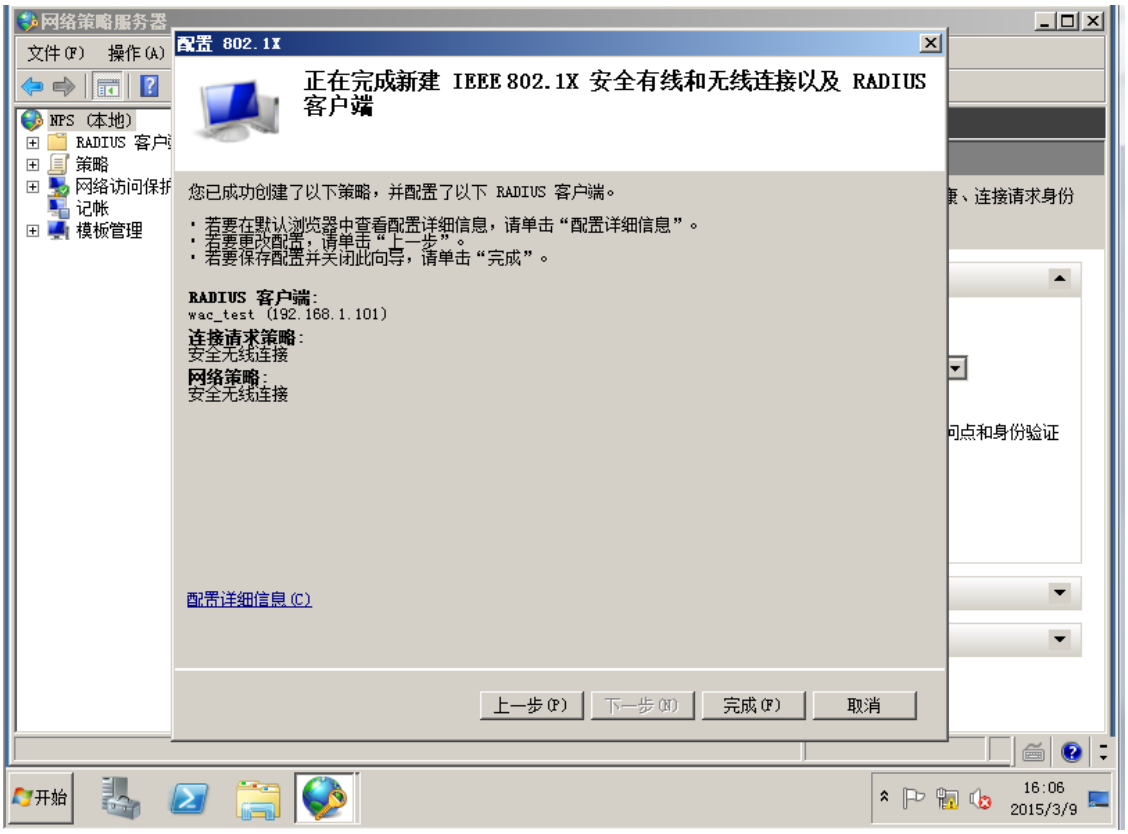
此处保持默认。



此处选择默认，然后选择下一步。

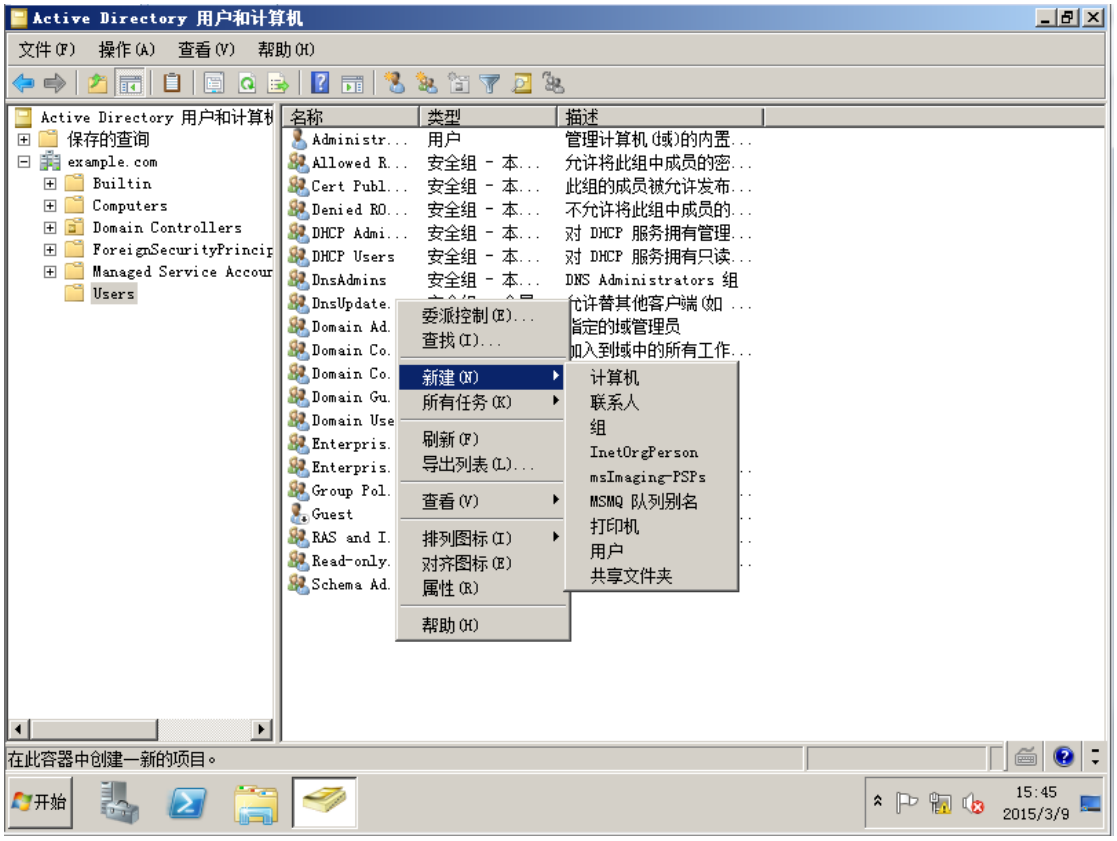


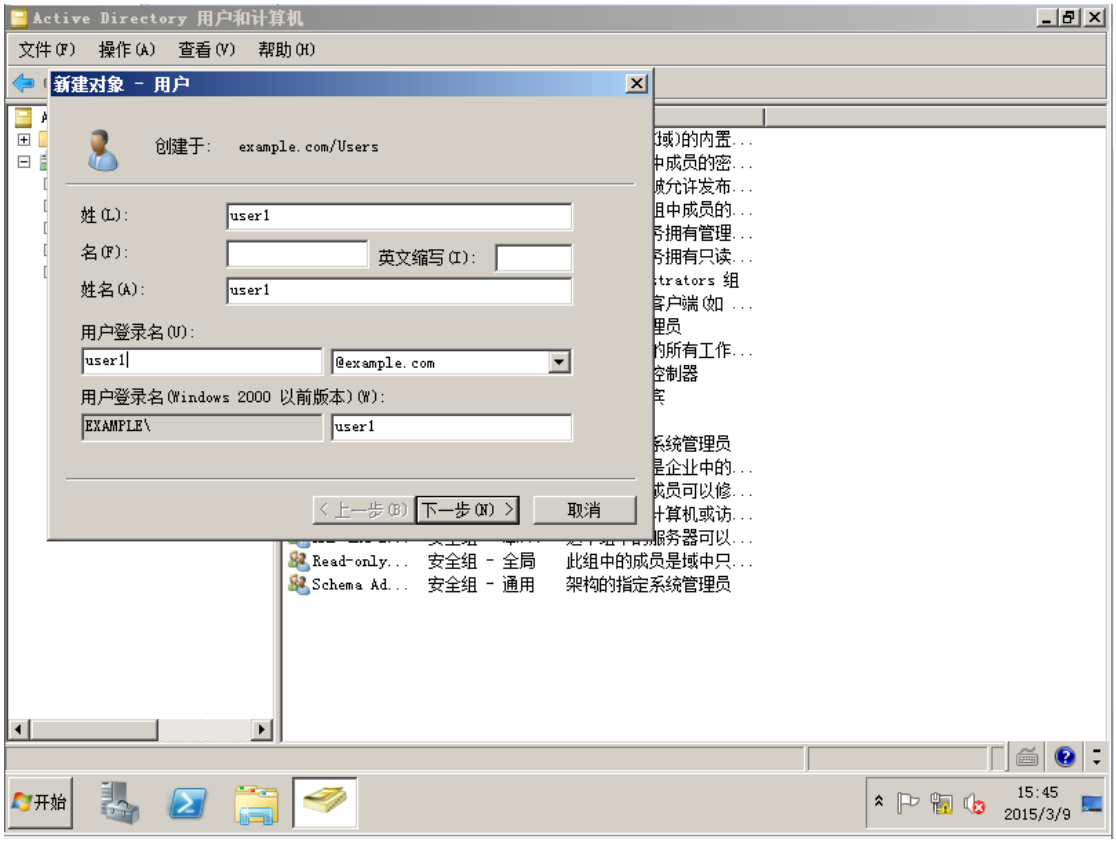
选择完成。

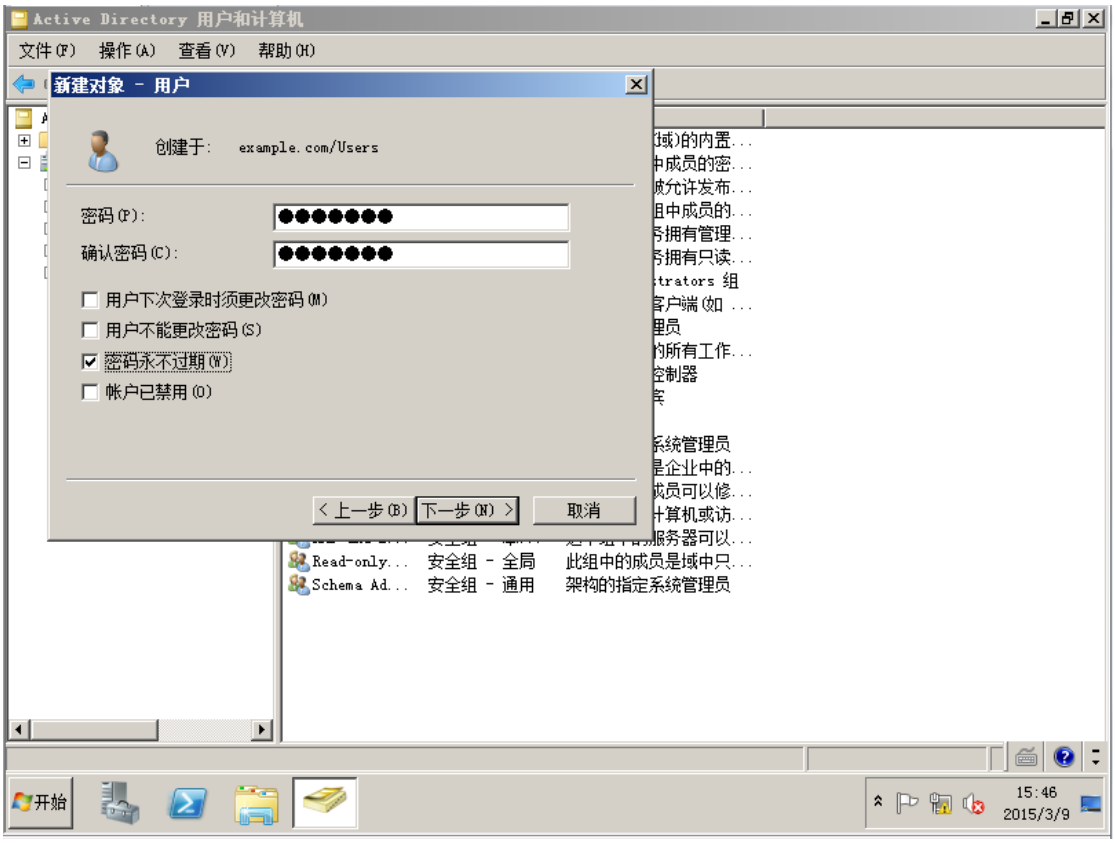

网络策略服务器
文件(F)
操作(A)
NPS (本地)
RADIUS 客户端
策略
网络访问保护
记帐
模板管理
配置 802.1X
正在完成新建 IEEE 802.1X 安全有线和无线连接以及 RADIUS 客户端
您已成功创建了以下策略，并配置了以下 RADIUS 客户端。
• 若要在默认浏览器中查看配置详细信息，请单击“配置详细信息”。
• 若要更改配置，请单击“上一步”。
• 若要保存配置并关闭此向导，请单击“完成”。
RADIUS 客户端:
wac_test (192.168.1.101)
连接请求策略:
安全无线连接
网络策略:
安全无线连接
配置详细信息(C)
上一步(P)
下一步(N)
完成(F)
取消
开始
16:06
2015/3/9

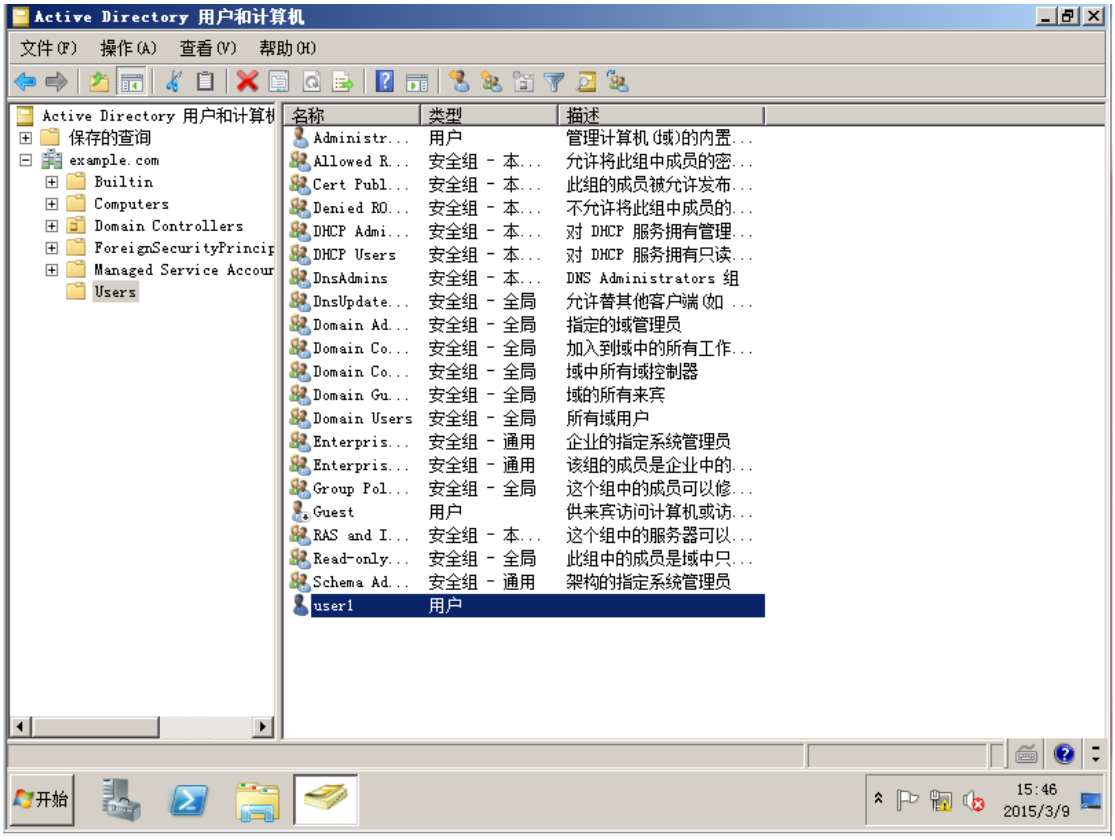
2.2 服务器设置

2.2.1 AD 域创建一个 user1 的用户，以便测试使用

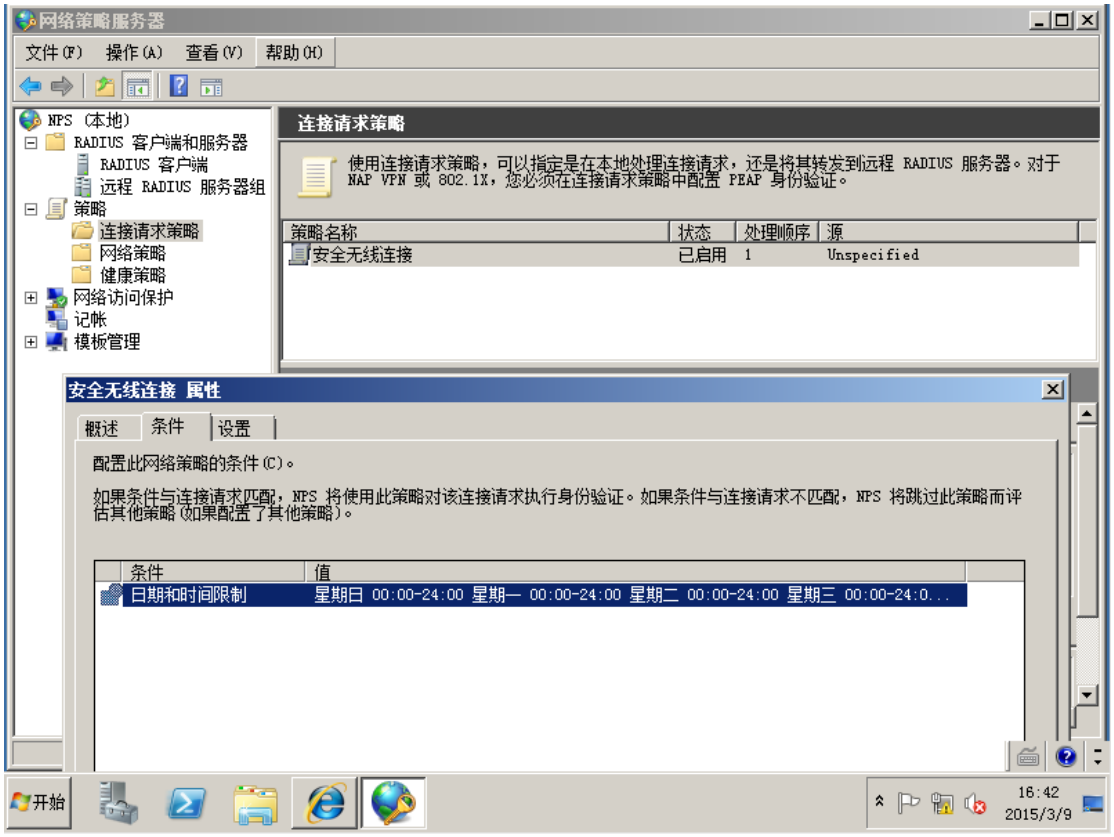

Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
example.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
名称 类型 描述
委派控制(E)...
查找(I)...
新建(N)
所有任务(K)
刷新(F)
导出列表(L)...
查看(V)
排列图标(I)
对齐图标(E)
属性(R)
帮助(H)
计算机
联系人
组
InetOrgPerson
msImaging-PSPs
MSMQ 队列别名
打印机
用户
共享文件夹
在此容器中创建一新的项目。
开始
15:45
2015/3/9


Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
新建对象 - 用户
创建于: example.com/Users
姓(L): user1
名(F):
英文缩写(I):
姓名(A): user1
用户登录名(U):
user1
@example.com
用户登录名(Windows 2000 以前版本)(W):
EXAMPLE\
user1
< 上一步(B)
下一步(N) >
取消
Read-only... 安全组 - 全局 此组中的成员是域中只...
Schema Ad... 安全组 - 通用 架构的指定系统管理员
开始
15:45
2015/3/9

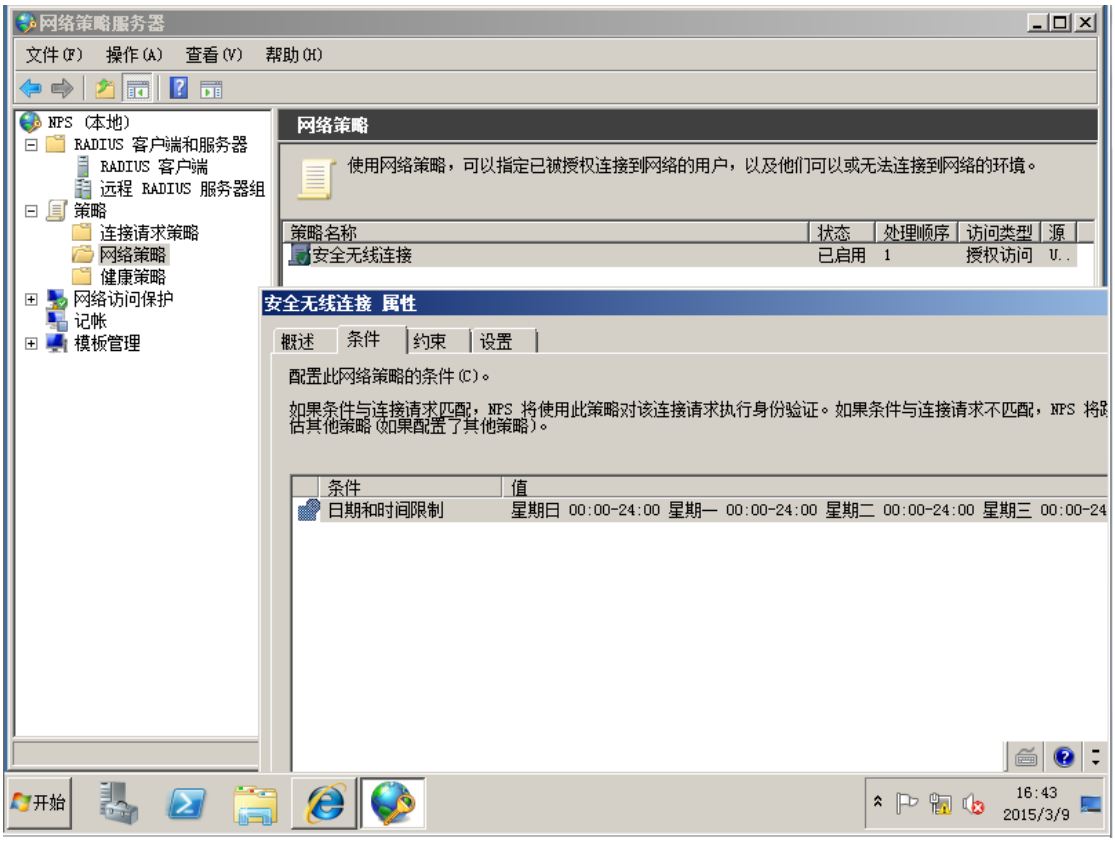

Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
新建对象 - 用户
创建于: example.com/Users
密码(P):
确认密码(C):
用户下次登录时须更改密码(M)
用户不能更改密码(S)
密码永不过期(W)
帐户已禁用(O)
< 上一步(B) 下一步(N) > 取消
Read-only... 安全组 - 全局 此组中的成员是域中只...
Schema Ad... 安全组 - 通用 架构的指定系统管理员
开始
15:46
2015/3/9

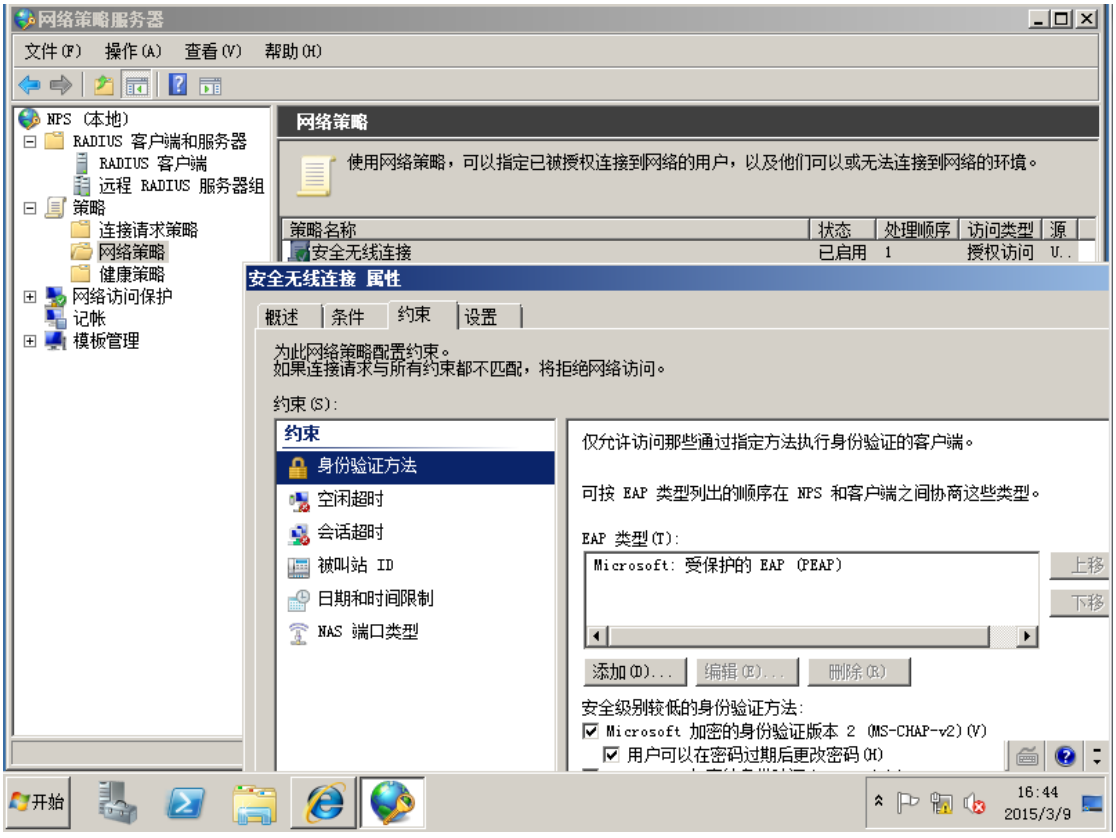

Active Directory 用户和计算机
文件(F) 操作(A) 查看(V) 帮助(H)
Active Directory 用户和计算机
保存的查询
example.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Accour
Users
名称 类型 描述
Administr... 用户 管理计算机(域)的内置...
Allowed R... 安全组 - 本... 允许将此组中成员的密...
Cert Publ... 安全组 - 本... 此组的成员被允许发布...
Denied RO... 安全组 - 本... 不允许将此组中成员的...
DHCP Admi... 安全组 - 本... 对 DHCP 服务拥有管理...
DHCP Users 安全组 - 本... 对 DHCP 服务拥有只读...
DnsAdmins 安全组 - 本... DNS Administrators 组
DnsUpdate... 安全组 - 全局 允许替其他客户端(如 ...
Domain Ad... 安全组 - 全局 指定的域管理员
Domain Co... 安全组 - 全局 加入到域中的所有工作...
Domain Co... 安全组 - 全局 域中所有域控制器
Domain Gu... 安全组 - 全局 域的所有来宾
Domain Users 安全组 - 全局 所有域用户
Enterpris... 安全组 - 通用 企业的指定系统管理员
Enterpris... 安全组 - 通用 该组的成员是企业中的...
Group Pol... 安全组 - 全局 这个组中的成员可以修...
Guest 用户 供来宾访问计算机或访...
RAS and I... 安全组 - 本... 这个组中的服务器可以...
Read-only... 安全组 - 全局 此组中的成员是域中只...
Schema Ad... 安全组 - 通用 架构的指定系统管理员
user1 用户
开始
15:46
2015/3/9

2.2.2 修改 radius 服务器连接请求条件允许任何时间登录



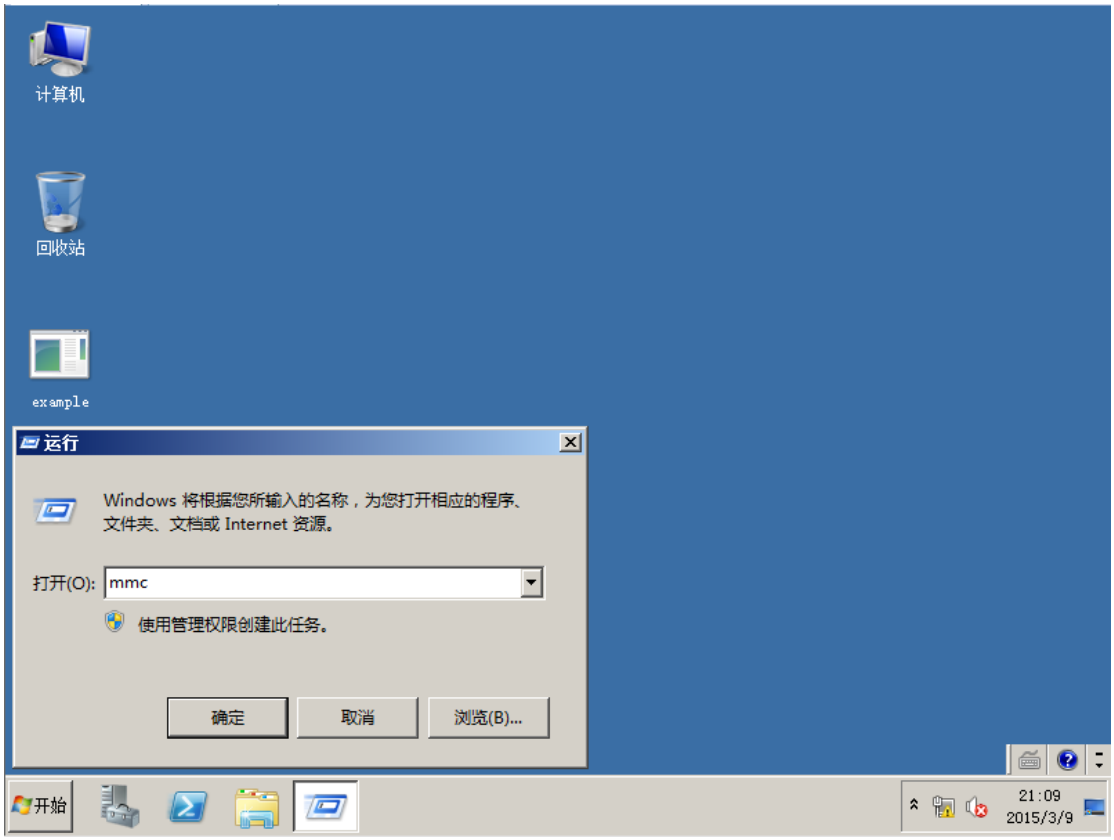
2.2.4 修改 radius 网络策略运行任何时间登录



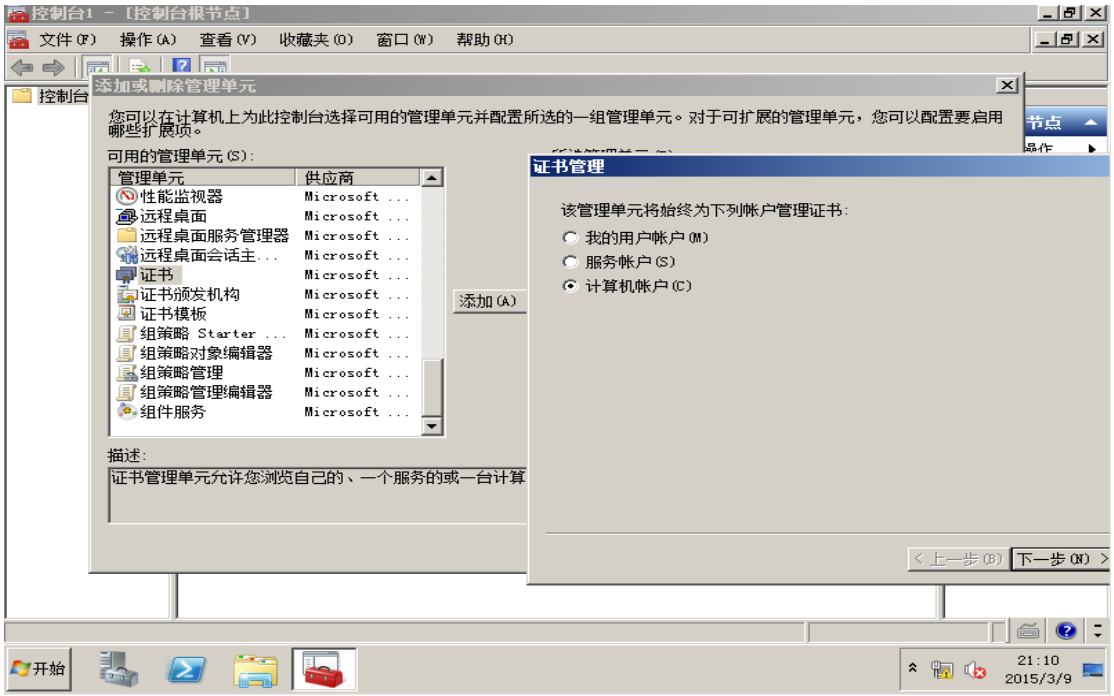


2.2.4 给 NAC 导入 CA 根证书

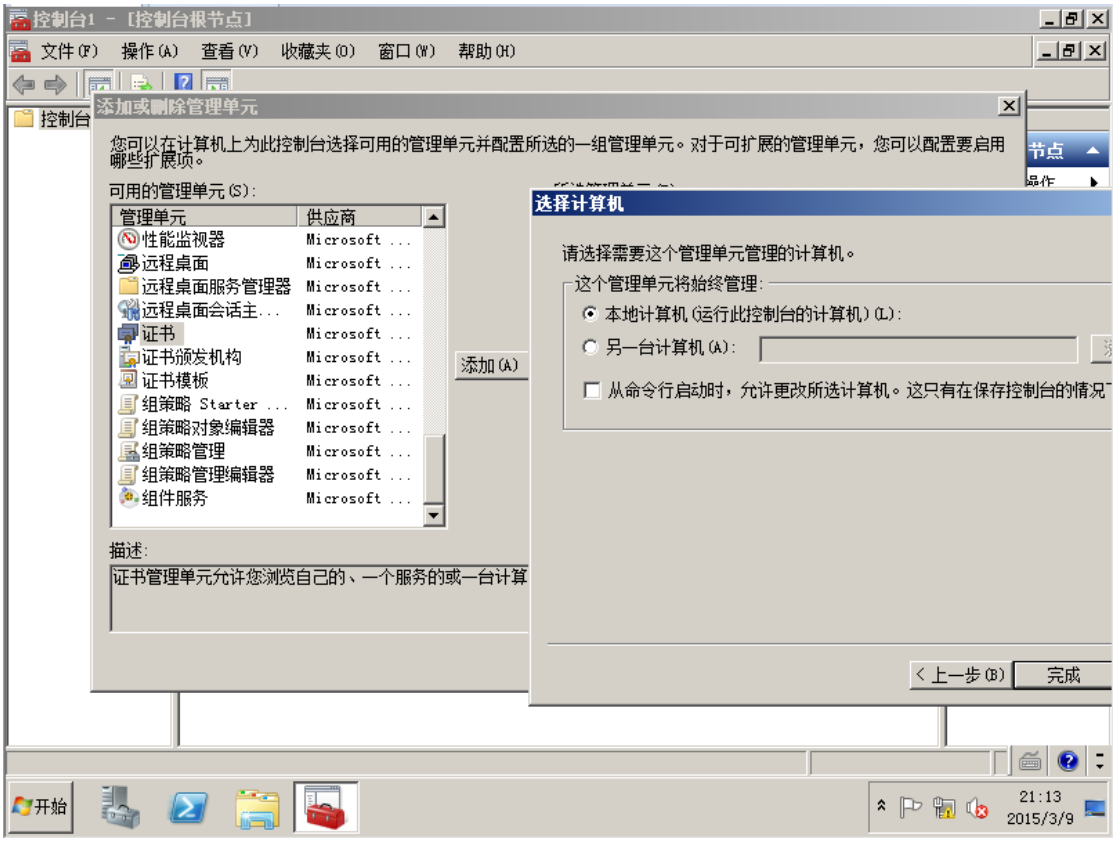
运行 mmc，打开控制台



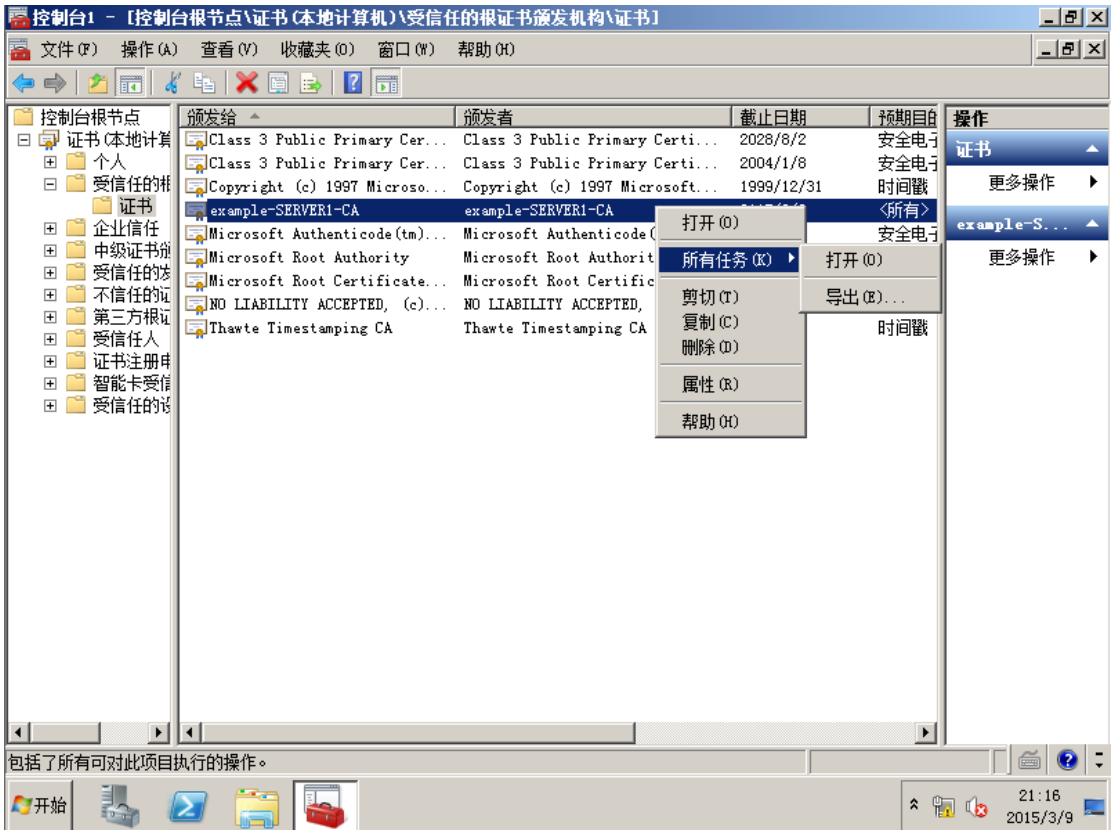
选择添加证书管理单元，选择计算机账户，然后选择下一步。



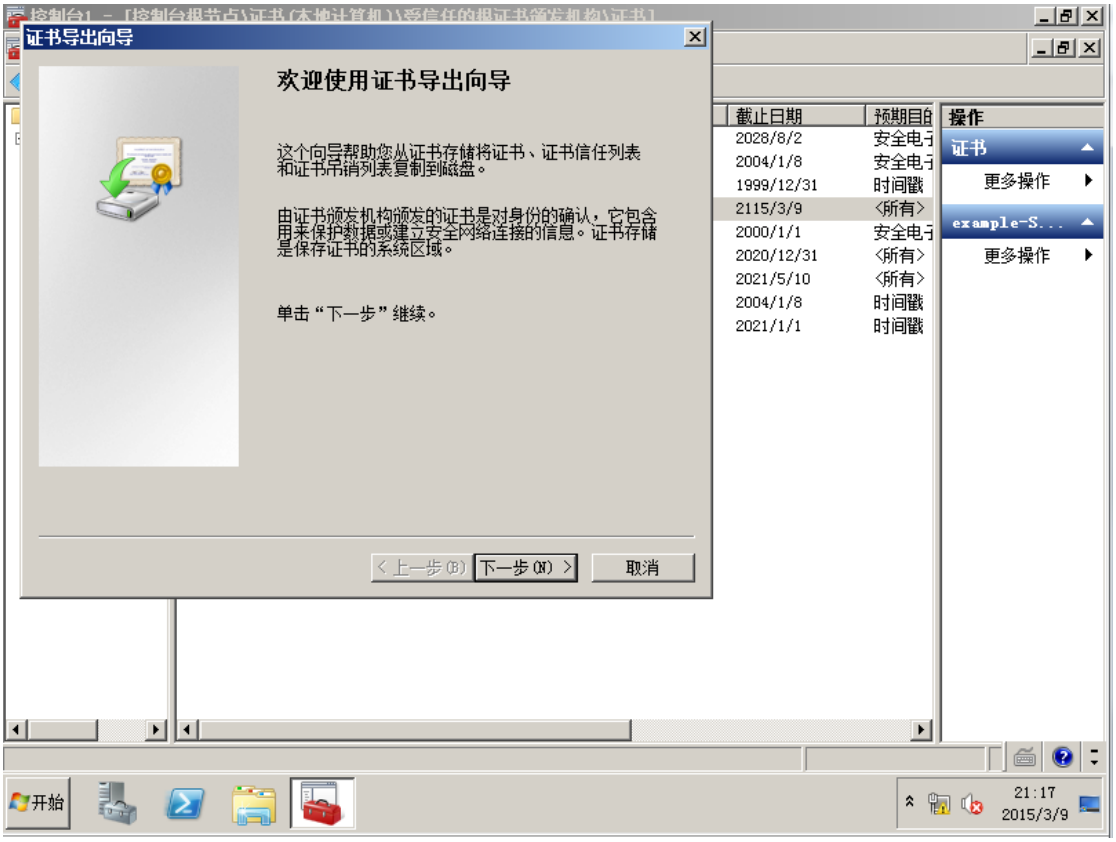
默认，然后选择完成。



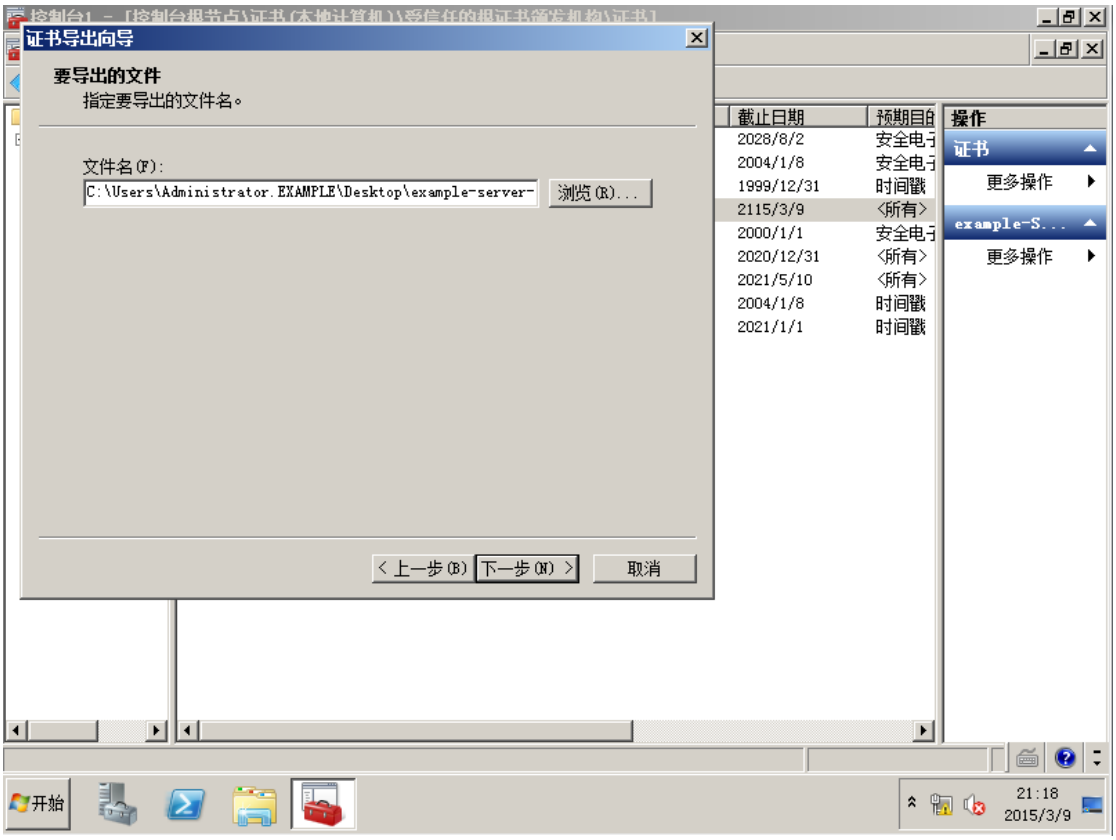
找到受信任的根证书，将此证书导出。



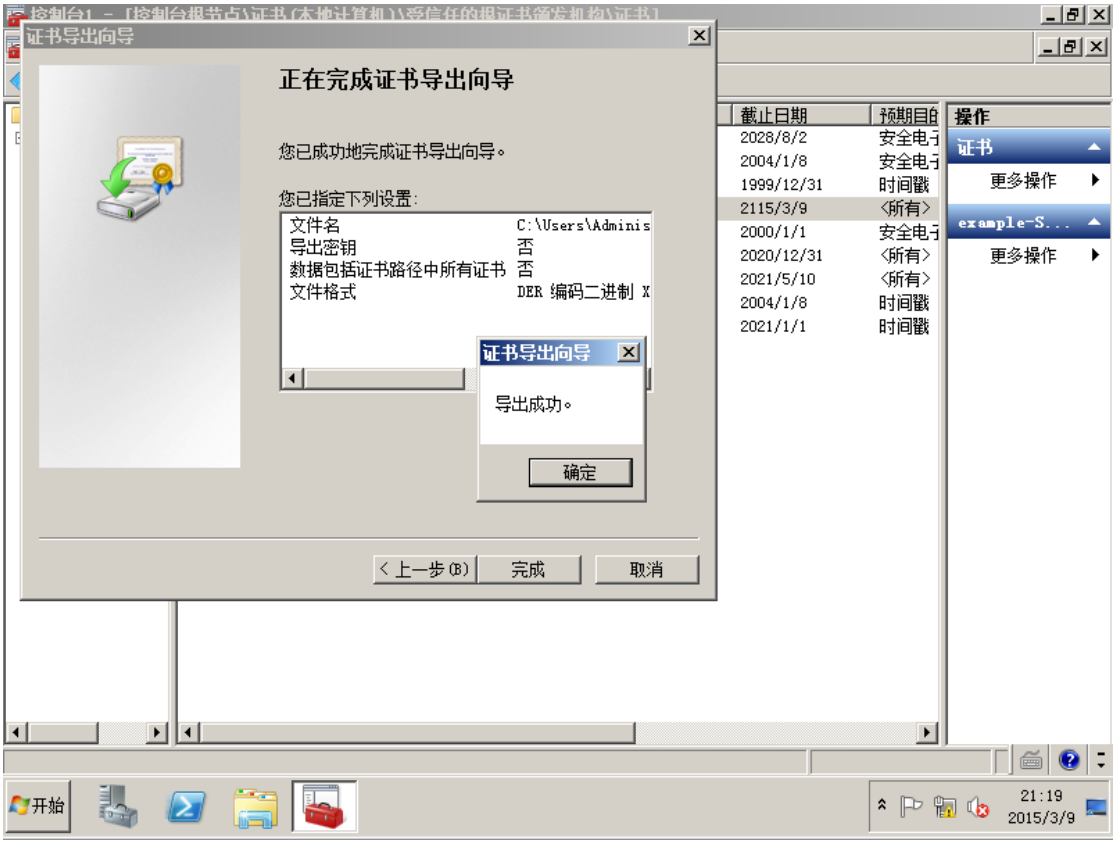
保持默认，然后选择下一步。



到此界面选择保存到桌面，名还是导出之前的名字，example-server1-ca.cer

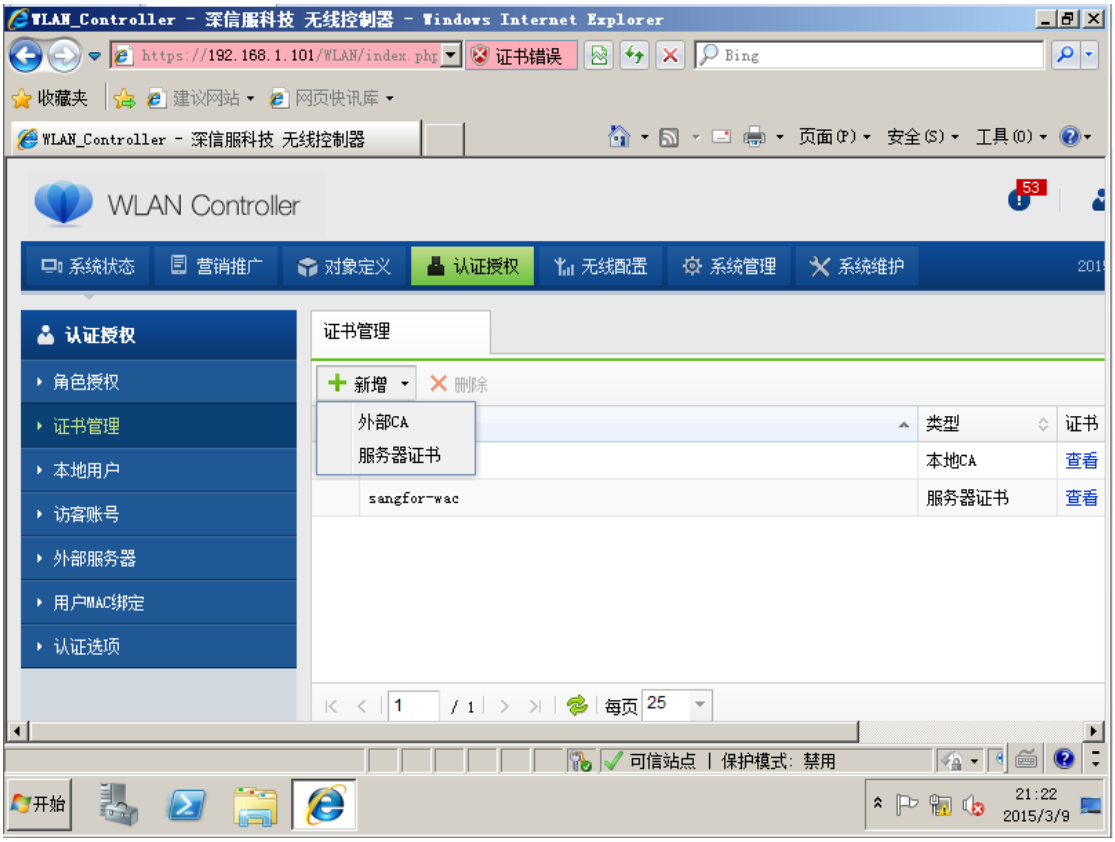


选择完成，导出成功。



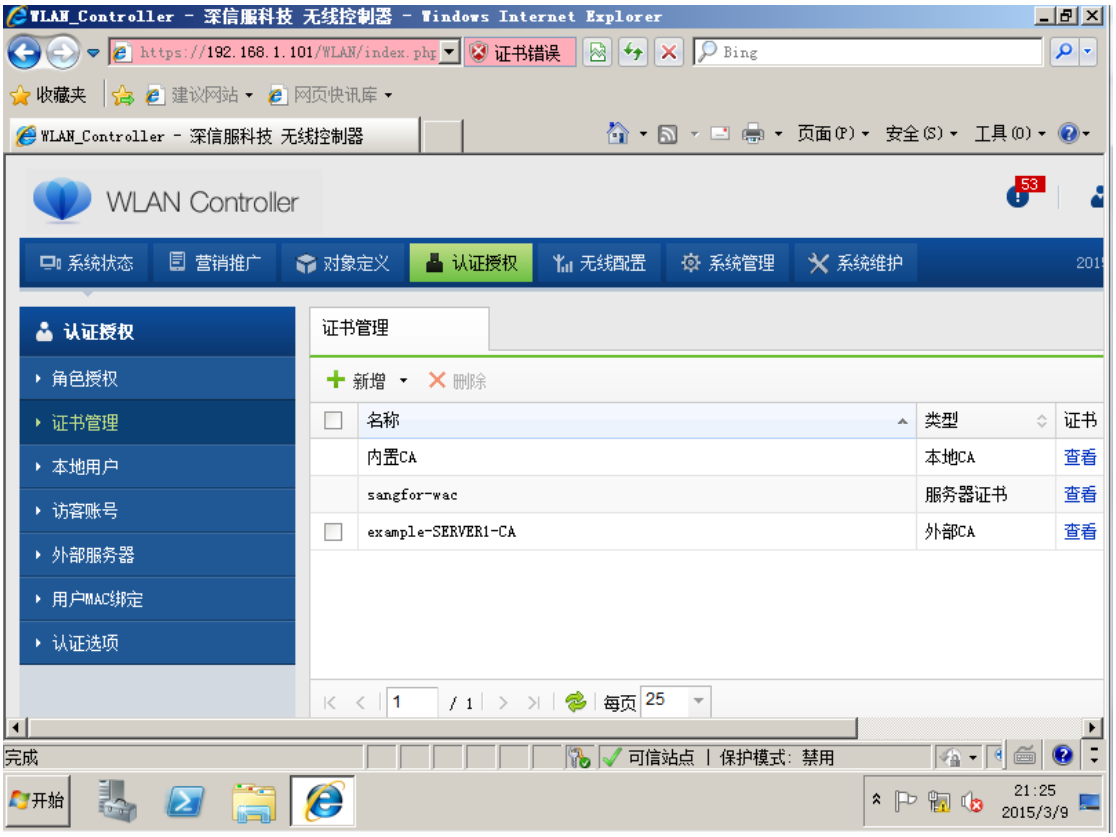
此时可以看到桌面上有一个证书。

进入设备后台，找到证书管理，选择新增外部 CA，将刚刚导出的 CA 证书，导入进去。



导入证书后，其他保持默认，选择提交

证书导入成功。（后续配置网络自动配置工具会用到）



第三章 注意事项

1、在测试的时候，建议我们测试搭建的 radius、ca 不要在客户的生产设备上直接搭建，建议开一个虚拟机，在虚拟机里面做测试。

2、在验证外部服务器有效性时，如果提示服务可用，但是帐号密码提示错误，可将 radius 隶属于 domain controller 这个组中。