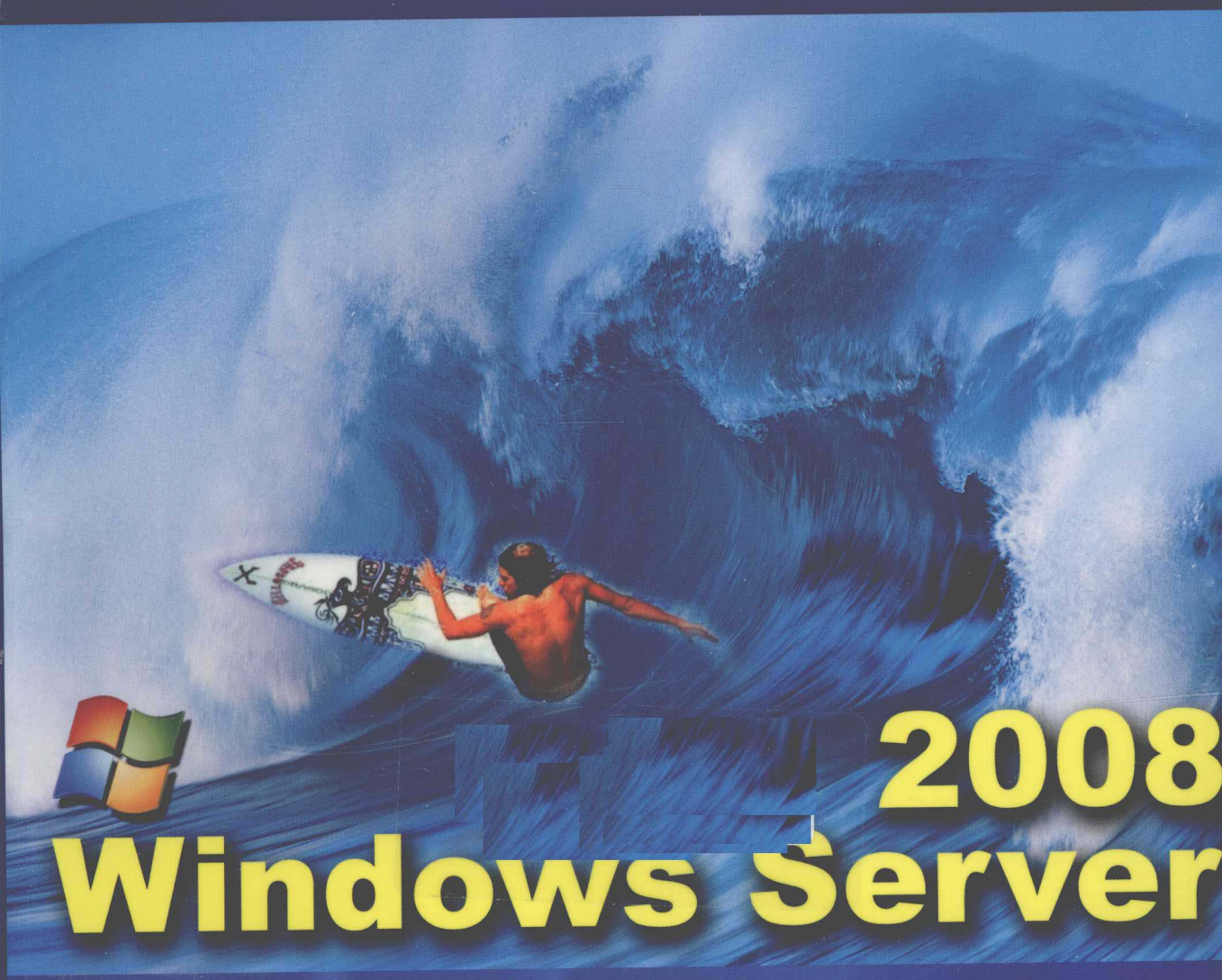
王淑江　刘晓辉　等编著



Windows Server 2008 R2活动目录内幕

- 网络专家编写，与广大读者分享研究成果与成功经验
- 技术全面深入，全面涵盖Windows Server 2008活动目录知识点
- 面向网络实战，亦步亦趋照葫芦画瓢即可管理Windows Server 2008活动目录
- 内容通俗易懂，没有枯燥乏味的理论罗列只有重要技术与关键操作
- 结构安排合理，本书介绍的知识与技术保证在实践中管用够用好用实用

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Windows Server 2008 R2 活动目录内幕

王淑江　刘晓辉　等编著

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书深入地介绍以 Windows Server 2008 R2 AD DS 域服务为基础的网络应用，内容包括：部署、迁移、升级域控制器、额外域控制器、子域以及域树，管理用户、计算机账户、电子邮件、数字证书、Internet 访问控制以及委派，以实际案例为例阐述组策略管理、首选项管理、高级组策略管理的方法，结合微软最新的虚拟化技术说明界面虚拟化（RemoteApp）、应用程序虚拟化（APPV）在网络中的部署方法，以及 Active Directory 的管理。

本书内容具有很强的实践性和指导性，读者需要具有一定的网络知识。本书可以作为企事业、各单位信息部门参考用书，可以作为高级网络培训班的参考教材，也可以作为计算机网络专业毕业生在即将走向工作岗位以前的实习参考书。

图书在版编目（CIP）数据

Windows Server 2008 R2 活动目录内幕 / 王淑江等编著. —北京：电子工业出版社，2010.9
ISBN 978-7-121-11705-3

Ⅰ. ①W… Ⅱ. ①王… Ⅲ. ①服务器—操作系统（软件），Windows Server 2008 Ⅳ. ①TP316.86

中国版本图书馆 CIP 数据核字（2010）第 168207 号

策划编辑：郭鹏飞
责任编辑：鄂卫华
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：35.5　字数：909 千字
印　　次：2010 年 9 月第 1 次印刷
定　　价：59.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

Windows Server 2008 R2 是微软最新的服务器操作系统，该操作系统秉承“按需定制”的原则，可以根据需要选择安装组件。网络中常用的基础服务以“角色”的方式体现，更多的管理任务以“功能”的方式体现。由于系统安装的服务少，因而能够减少网络攻击面，提升网络安全。其中的 AD DS 域服务是 Windows 网络的基础网络服务，是 Windows 系列应用型产品的核心平台，是用户管理、计算机管理的基础。

本书以实战部署为基础，详细介绍 Windows Server 2008 R2 的 Active Directory 管理、虚拟化应用以及部分高级管理功能。以用户（域用户和计算机账户）管理为基础，详细探讨用户在网络中的作用以及应用模式，结合实际应用在每个章节中体现用户是实际管理目标和使用的主体目标这一基本原则，实现用户在网络中如何访问互联网以及非安全的用户如何隔离处理这一基本目标，引导读者独立完成在不同的应用中管理用户的操作。

本书共分 22 章，详细描述从 Windows Server 2008 R2 安装开始到服务器部署，以及基于 Active Directory 的日常应用，内容概要介绍如下。

第 1 章，部署域控制器，介绍在全新的网络环境中部署基于 Windows Server 2008 R2 的域控制器和额外域控制器的方法，本书中的应用实例以本章中部署的 Active Directory 为基础。第 2 章，部署子域与域树，介绍在域中创建信任的方法以及如何部署子域和域树。第 3 章，部署只读域控制器，只读域控制器是 Windows Server 2008 的新域控制器类型，在分支机构管理中可以替代子域管理。第 4 章，用户管理，介绍用户管理中涉及的组织单位、组和用户，以及相应的管理任务。第 5 章，计算机管理，介绍在域环境中，计算机的管理方法，包括加域、降域实现的方法和 WSUS 服务的部署。第 6 章，用户数字证书，介绍数字证书在域环境中的部署方法，掌握计算机证书自动申请的方法，以及用户证书的管理。第 7 章，组策略管理，以实际应用案例为例介绍网络部署组策略的方法。第 8 章，部署首选项，介绍组策略管理的新功能，该功能和组策略不同点是用户应用首选项策略后，可以继续配置策略，客户端计算机用户对发布的策略具备可控权限。第 9 章，用户与远程桌面服务，介绍远程桌面服务的部署方法，该应用属于微软虚拟化应用中界面虚拟化的一部分。第 10 章，用户与应用程序虚拟化，介绍微软虚拟化应用中“应用程序虚拟化”的部署方法，该程序安装包集成在“MDOP R2”管理包中。第 11 章，用户互联网访问控制，介绍在域环境中，使用 ISA Server 2006 管理用户访问互联网的方法。第 12 章，AGPM 高级组策略管理，介绍集成在“MDOP R2”管理包中 AGPM 管理组策略的方法，该模式将在未来取代 GPMC 管理组策略。第 13 章，用户与 IIS 服务，介绍用户在域环境中使用 Web 服务、FTP 服务，以及增强 IIS 服务访问安全的方法。第 14 章，用户与文件共享，介绍共享文件在 Active Directory 中的部署，以及安全部署和访问共享文件夹的方法。第 15 章，升级域控制器，介绍 Windows Server 2003 的域控制器升级到 Windows Server 2008 R2 AD DS 域服务的方法以及需要注意的问题。第 16 章，域

对象迁移，介绍将 Windows Server 2003 的 Active Directory 域控制器中的域对象迁移到 Windows Server 2008 R2 AD DS 域服务中的方法，此方法也是升级域的方法之一。第 17 章，权限委派，介绍委派用户管理 Active Directory 的方法，注意客户端计算机用户需要到微软网站中下载管理包。第 18 章，用户隔离，介绍使用“网络策略和访问”角色部署增强用户安全验证的方法，此角色将和 DHCP 角色结合使用。第 19 章，备份恢复，介绍使用 Windows Server Backup 功能备份和恢复 AD DS 域服务的方法。第 20 章，事件日志，介绍 Windows Server 2008 R2 中日志和事件的处理方法，注意事件采集功能的实现方法。

本书由王淑江、刘晓辉等编著，赵卫东、刘淑梅、马倩、杨伏龙、李文俊、石长征、王同明、郭腾、白华、刘媛、莫展宏、由磊、李海宁、陈志成、田俊乐、王春海等也编写了本书的部分内容。在这个日新月异的信息化时代，网络新技术、新应用不断涌现。为此，我们将密切关注网络技术的发展和读者的需要，将更新、更实用的技术介绍给读者，将更好的产品和应用推荐给大家。由于编者水平有限，并且本书涉及的系统与知识点很多，虽然作者力求完善，但书中难免有不妥和错误之处，欢迎大家与我们联系和交流。

我们的联系方式：Guo Pengfei@phei.com.cn。

编著者

2010.7

目录

CONTENTS

第1章 部署域控制器

网络硬件（网络布线、网络交换机、服务器、客户端计算机）设备全部就绪后，管理员最重要的任务是部署域控制器。在部署 Windows Server 2008 操作系统的网络中，最基础、最重要、最核心的功能就是部署 AD DS 域服务，AD DS 域服务是管理 Windows 网络中用户、计算机、文件资源、打印资源、安全管理以及拓展应用的基础。本章将详细介绍部署基于 Windows Server 2008 的域控制器及额外域控制器的方法。

1.1 基础知识

在部署 AD DS 域服务前，管理员需要了解关于 AD DS 域服务的基础知识。如果是全新的网络，管理员可以直接部署 Windows Server 2008 AD DS 域服务。在部署的过程中，如果部署 Active Directory 集成区域 DNS 服务器，设置服务器参数时，需要将“首选 DNS 服务器”设置为本机的 IP 地址。域控制器必须使用静态 IP 地址。

1.1.1 服务器类型

在网络中，服务器是最基本的硬件平台，操作系统将运行在服务器之上。在部署 AD DS 域服务的网络中，有多种服务器类型，下面分别介绍相关的服务器概念。

1. 独立服务器

安装完成 Windows Server 2008 操作系统后，运行该操作系统的计算机就成为一台独立服务器。该服务器可以独立部署应用程序。最明显的特征是该服务器没有加入到“域”中。

2. 成员服务器

独立服务器添加到“域”中之后，就成为成员服务器。该服务器接受 AD DS 域服务的统一管理，接受并应用 Active Directory 发布的组策略，该计算机被添加到 Active Directory 的“Computers”组织单位中。

3. 域控制器

域控制器是网络中的第一台运行 AD DS 域服务的服务器，管理员可以使用“Dcpromo.exe”命令行工具或者添加“AD DS 域服务”角色向导直接将独立服务器提升为域控制器，在所有的域控制器（域控制器、额外域控制器、只读域控制器）中，只有域控制器可以将独立服务器直接提升为域控制器。该计算机被添加到“Domain Controllers”组织单位中。在部署的过程中，注意功能级别的设置。所有操作主机角色默认安装在第一台域控制器中。

4. 额外域控制器

成员服务器使用“Dcpromo.exe”命令行工具或者添加“AD DS 域服务”角色向导后，将被提升为额外域控制器，该计算机被添加到“Domain Controllers”组织单位中。该服务器上运行“AD DS 域服务”，提供管理任务，存储 Active Directory 数据库。操作主机角色默认没有安装在额外域控制器中。

1.1.2 Active Directory 集成区域 DNS

Active Directory 集成区域 DNS 服务器，是在域控制器上运行的 DNS 服务。Active Directory 集成区域 DNS 服务器仅当在域控制器上部署 DNS 服务器时有效，此时，区域数据存放在活动目录中并且随着活动目录数据的复制而复制。在默认情况下，每一个运行在域控制器上的 DNS 服务器都将成为主要 DNS 服务器，并且可以修改 DNS 区域中的数据（多点更新），这样避免了标准主要区域出现的单点故障。活动目录集成主要区域支持安全的动态更新。

在 Active Directory 集成区域中，没有主 DNS 服务器和辅助 DNS 服务器的区别，即所有的 DNS 服务器都是主 DNS 服务器。通过防止不希望的外界对象注册动态 DNS 记录实现了对动态 DNS 的安全保护，只有属于 Active Directory 域成员的机器能够动态地在 Active Directory 中注册记录。

以 Active Directory 能力为基础的多主机更新和增强的安全性。在标准区域存储模式中，以单主机更新模式为基础进行 DNS 更新。在该模式中，区域的单个授权 DNS 服务器被指派为该区域的主要来源。该服务器在本地文件中保留了区域的主控副本。通过该模式，区域的主服务器代表单个固定的故障点。如果该服务器不可用，则来自 DNS 客户端的更新请求不对该区域进行处理。Active Directory 集成区域只存在于主要区域，DNS 服务器不能在目录中存储辅助区域。当所有区域都存储在 Active Directory 中时，Active Directory 的多主机复制模型将不再需要辅助区域。

通过与目录集成的存储区，对 DNS 的动态更新在多主机更新模式的基础上进行。在该模式下，任何权威 DNS 服务器（例如，运行 DNS 服务器的域控制器）都被指定为区域的主要来源。因为区域的主控副本保留在完全复制到所有域控制器的 Active Directory 数据库中，所以该区域可由在该域的任何域控制器上运行的 DNS 服务器更新。通过 Active Directory 的多主机更新模式，只要域控制器在网络上可用而且可以访问，与目录集成的区域的任何主要服务器就可以处理来自 DNS 客户端的更新区域请求。同时，在使用目录集成的区域时，可以编辑访问控制列表（ACL）以保证目录树中 DnsZone 对象容器的安全性。该功能提供了至区域或区域中指定资源记录的分散访问。

1.1.3 功能级别

功能级别确定在域或林中启用的 AD DS 域服务的功能，该功能将限制哪些 Windows Server 操作系统可以在域或林中的域控制器上运行。功能级别不会影响连接到域或林中的工作站和成员服务器的运行。创建新域或新林时，管理员可以选择使用的功能级别，建议尽量设置为高级别的功能级别，以尽可能充分利用 AD DS 域服务功能。

1. 林功能级别

林功能启用了林中所有域功能。有以下三个功能级别：Windows 2000 本机模式、Windows

Server 2003 以及 Windows Server 2008。默认设置部署完成 Active Directory 域服务后，在 Windows 2000 林功能级别下工作。可以将 Windows 2000 林功能级别提升为 Windows Server 2003 以及 Windows Server 2008。

2. 域功能级别

域功能级别启用整个域和该域的功能。在 Windows Server 2008 的 Active Directory 域服务中，支持三种域功能级别：Windows 2000 本机模式、Windows Server 2003 以及 Windows Server 2008。默认情况下，部署完成 Active Directory 域服务后，在 Windows 2000 域功能级别下工作。可以将 Windows 2000 域功能级别提升为 Windows Server 2003 以及 Windows Server 2008。

3. 林和域功能提升

从较低功能级别到较高功能级别的改变称之为提升（Raise），这种提升过程是不可逆的，即只能从低版本向高版本提升，但无法降低到低版本。该过程适用于林功能级别和域功能级别。提升功能级别后，无法将不支持的 Windows 操作系统添加到当前功能级别的林中，例如如果当前的林功能级别为 Windows Server 2008，则不能将运行 Windows Server 2003 和 Windows 2000 Server 的域控制器添加到 Windows Server 2008 的林中。

4. 功能级别类型

Windows Server 2008 R2 的功能级别分为 Windows 2000、Windows Server 2003、Windows Server 2008 和 Windows Server 2008 R2。

- Windows 2000。该域功能级别的应用范围包括运行 Windows 2000、Windows Server 2003、Windows Server 2008 和 Windows Server 2008 R2 操作系统的域控制器，如果企业网络环境中包含上述三种域控制器，建议使用该功能级别。简单地说适用于多版本操作系统并存的网络环境。
- Windows Server 2003。该域功能级别的应用范围包括运行 Windows Server 2003、Windows Server 2008 和 Windows Server 2008 R2 操作系统的域控制器，该域功能级别支持许多新的功能，例如域重命名等。如果企业网络环境中包含上述两种域控制器，建议使用该功能级别。提升该功能级别后，将不支持 Windows 2000 域控制器。
- Windows Server 2008。该域功能级别的应用范围包括运行 Windows Server 2008 和 Windows Server 2008 R2 操作系统的域控制器，该域功能级别支持许多只有 Windows Server 2008 才具备的功能，例如精确的密码控制策略，可重新启动的 Active Directory 服务等。如果企业部署新的网络环境，建议使用该功能级别。提升该功能级别后，将不支持 Windows 2000、Windows Server 2003 域控制器。
- Windows Server 2008 R2。Windows Server 2008 R2 功能级别提供 Windows Server 2008 中可用的所有功能，包括回收站和完整还原删除的对象的功能。默认情况下，在该林中创建的任何新域将在 Windows Server 2008 R2 域功能级别下操作。

1.1.4 AD DS 域服务部署模式

在 Windows Server 2008 中部署 AD DS 域服务有两种模式，分别为命令行（Dcpromo.exe）模式和向导模式。

1. 命令行（Dcpromo. exe）模式

该模式是继承 Windows Server 2000/2003 传统，将独立服务器或者成员服务器提升为域控制器，在使用命令行（Dcpromo.exe）模式前，管理员无需安装“Active Directory 域服务”角色，如果“Dcpromo.exe”检测到计算机中没有安装“Active Directory 域服务”角色，将自动在后台安装需要的角色。

2. 向导模式

向导模式部署 AD DS 域服务，分为两部分：添加 AD DS 域服务角色和 Active Directory 域服务安装向导。添加 AD DS 域服务角色将完成角色的安装。Active Directory 域服务安装向导将服务器提升为域控制器。

1.2 部署 AD DS 域服务

Windows Server 2008 默认安装完成后，管理员如果要将服务器提升为域控制器，需要完成以下任务：重命名计算机、更改计算机的 IP 地址以及设置网络类型，然后才可以安装 AD DS 域服务。安装 AD DS 域服务分两个阶段：安装角色和提升域服务。

提 示

有关 Windows Server 2008 的安装与配置，请参见《Windows Server 2008 组网技术详解（服务器搭建与升级篇）》（张栋、刘晓辉，电子工业出版社，2010.2）一书。

1.2.1 设置参数

Windows Server 2008 安装完成后，网络参数需要管理员手动设置。默认安装的 Windows Server 2008 同时启用 IPv4 和 IPv6 两种协议，在安装 AD DS 域服务时，不建议同时启用两种协议，选择一种即可。如果安装过程中需要同时安装 Active Directory 集成区域 DNS 服务器，将“首选 DNS 服务器”IP 地址指向当前服务器 IP 地址。

1. 重命名计算机

Windows Server 2008 R2 安装完成后，默认为安装的计算机随机生成一个名称，例如“WIN-CT5F543TTOE”，在网络应用中，应该为安装 Windows Server 2008 的计算机定义简捷并且有实用价值的计算机名称，提高管理效率以及可用性。

第 1 步，Windows Server 2008 启动后，自动运行“初始配置任务”程序，如果管理员关闭了此程序，可以在命令行模式下，键入“oobe”启动“初始配置任务”程序，显示如图 1-1 所示的“初始配置任务”窗口。

第 2 步，单击“提供计算机名和域”超链接，打开“系统属性”对话框。单击“更改”按钮，显示如图 1-2 所示的“计算机名/域更改”对话框。

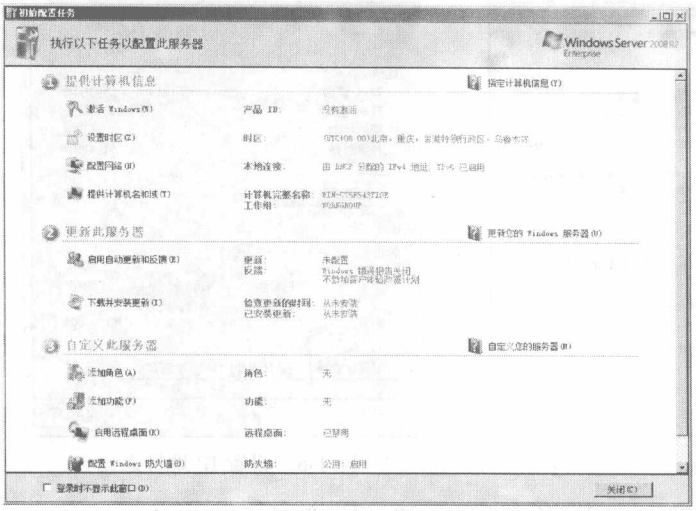


图 1-1　更改计算机名之一

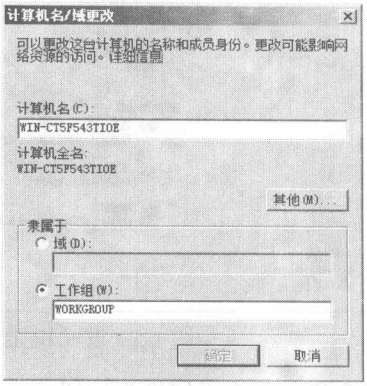


图 1-2　更改计算机名之二

第 3 步，在“计算机名”文本框中，键入该计算机的有效名称，如图 1-3 所示。

第 4 步，单击“确定”按钮，显示如图 1-4 所示“计算机名/域更改”对话框，提示需要重新启动计算机。连续单击“确定”按钮，重新启动服务器，完成计算机名称的更改。

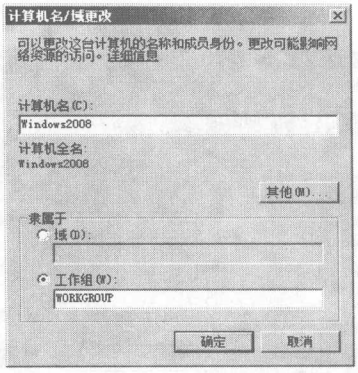


图 1-3　更改计算机名之三

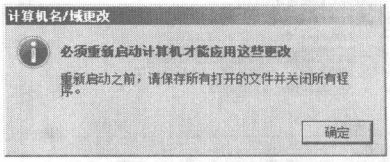


图 1-4　提示重新启动

2. 设置静态 IP 地址

Windows Server 2008 安装完成后，同时启用 IPv4 协议和 IPv6 协议，在本例中使用 IPv4 协议，关闭 IPv6 协议。作为运行 AD DS 域服务的域控制器，必须使用静态 IP 地址。本例中将部署 Active Directory 集成区域 DNS 服务器，需要将“首选 DNS 服务器”的 IP 地址指向本机的 IP 地址。如果在网络中存在其他 DNS 服务器，则将“首选 DNS 服务器”的 IP 地址指向其他 DNS 服务器。

第 1 步，选择“开始”→“控制面板”→“网络和共享中心”选项，显示如图 1-5 所示的“网络和共享中心”窗口。

第 2 步，选择“未识别的网络（公用网络）”区域的“连接”→“本地连接”→“查看状态”超链接，显示如图 1-6 所示的“本地连接 状态”对话框。

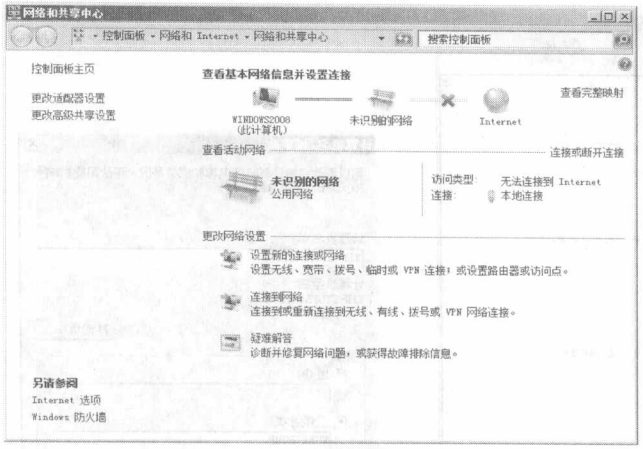


图 1-5　设置 IP 地址之一

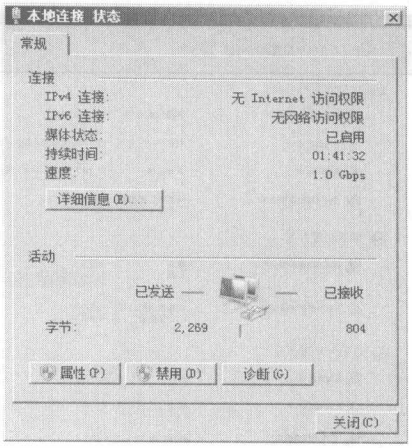


图 1-6　设置 IP 地址之二

第 3 步，单击“属性”按钮，显示如图 1-7 所示的“本地连接 属性”对话框。Windows Server 2008 操作系统支持 TCP/IPv6 和 TCP/IPv4 协议，在本例中只使用“TCP/IPv4”协议，取消“Internet 协议版本 6（TCP/IPv6）”选项。

第 4 步，选择“Internet 协议版本 4（TCP/IPv4）”选项，单击“属性”按钮，显示如图 1-8 所示的“Internet 协议版本 4（TCP/IPv4）属性”对话框，设置域控制器的 IP 地址、网关以及 DNS 地址参数。

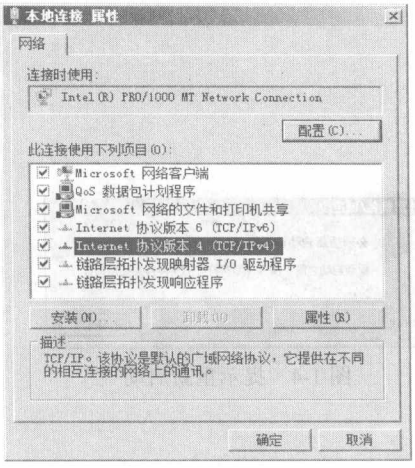


图 1-7　设置 IP 地址之三

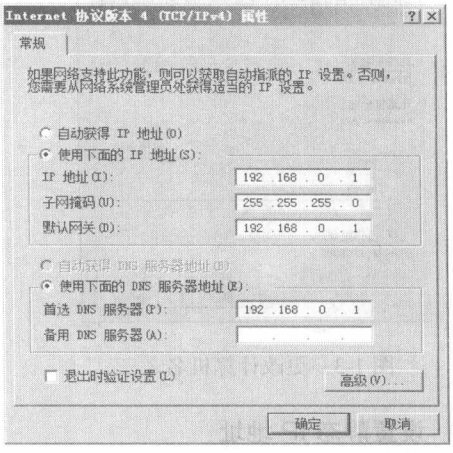


图 1-8　“Internet 协议版本 4（TCP/IPv4）属性”对话框

第 5 步，单击“确定”按钮，关闭“Internet 协议版本 4（TCP/IPv4）属性”对话框，返回到“本地连接属性”对话框。单击“关闭”按钮，完成 IP 地址的设置。

3. 设置网络类型

Windows Server 2008 操作系统安装完成后，默认网络类型为“公用网络”，在部署 Active Directory 的网络中建议使用“专用”网络。

第 1 步，选择“开始”→“控制面板”→“网络和共享中心”选项，显示如图 1-9 所示的“网络和共享中心”窗口。