Microsoft 微软资深顾问

戴有炜 最新力作

12年磨一剑，历经5次改版
持续畅销， 惠及百万读者

Windows Server 2008 R2

Active Directory 配置指南

专业品质
实力保障

- 微软MCSA、MCSE 、MCITP认证考试最佳实用参考书籍
- 独家以Active Directory域服务（AD DS）创建与配置为主题
- 通过虚拟技术，只要一台电脑就可以建立完整的网络学习环境
- 充分掌握Active Directory整体相关知识
- 秉承作者一贯的兼具理论与实践的写作风格，广获读者支持

戴有炜 编著

碁峰 www.gotop.com.tw

清华大学出版社

Windows Server 2008 R2

Active Directory 配置指南

- 循序渐进地介绍Active Directory域服务（AD DS）的基本概念。
- 独家以Active Directory 域服务（AD DS）的创建与配置为主题。
- 按部就班地介绍如何进行全新的Server Core安装，让您可以很容易地建立一个更安全、管理负担更低的运行环境。
- 深入探讨使用组策略管理用户工作环境，包括：组策略概述、组策略的处理规则、WMI筛选器、组策略建模、组策略结果、Starter GPO的设置和使用等。
- 完整涵盖最经典的实用技术，包括：限制使用者执行软件、限制访问可移动存储设备、一次同时新增多个用户账户等。
- 身为IT人员必备的知识与技能，包括：操作主机的管理、AD DS的备份与恢复、Active Directory回收站、Active Directory数据库的维护与优化、将资源发布到AD DS、Active Directory数据库的转移与重组、站点的配置与管理、AD DS与防火墙等。
- 详细说明域环境的配置，包含子域、域控制器、RODC的安装、自动安装域控制器、加入域、离线加入域与脱离域等。
- 软件部署的完整介绍，包含软件发布、软件分配、软件升级、自动修复软件、Microsoft Office的部署、重新部署等，使系统管理员可以更容易地管理用户所需的软件。
- 介绍如何建立信任关系，包含快捷方式信任、林信任、外部信任等，让网络之间的沟通更容易且有效率。
- 采用Windws Server 2008 R2 Hyper-V的虚拟环境，因此只要一台电脑就可以建立完整的学习环境。
- 涵盖最新的只读域控制器、可重新启动的AD DS 、组的使用原则、限制访问可移动存储设备等。
- 结合作者多年的实践经验，详细列举操作时的心得和技巧，引导您部署稳定的、全年无休的基本工作环境。

上架指导：计算机/Windows操作系统
封面设计：王　翔

ISBN 978-7-302-24230-7
9 787302 242307 >
定价：59.00元

Download at http://www.pin5i.com/

Windows Server 2008 R2 Active Directory 配置指南

戴有炜 编著

清华大学出版社
北 京

Download at http://www.pin5i.com/

内 容 简 介

《Windows Server 2008 R2 Active Directory配置指南》是台湾微软资深顾问、微软认证讲师、微软认证系统工程师戴先生的最新力作，他所编写的相关专题图书畅销两岸，实用是本书的最大特点。

作者完全站在读者的角度，通过不断测试与验证书中所述内容，并融合多年的教学经验，全面介绍了Windows Server 2008 R2的强大功能和使用方法。全书共13章，包括Active Directory域服务（AD DS）、建立AD DS域、域用户与组账户的管理、使用组策略管理用户工作环境、使用组策略部署软件、限制软件的运行、创建域树和林、管理域和林信任、Active Directory数据库的复制、操作主机的管理、AD DS的维护、将资源发布到AD DS、自动信任根CA。

本书面向广大初、中级网络技术人员、网络管理和维护人员、网络系统集成人员，也可作为高等院校相关专业和技术培训班的教学用书，同时还可作为MCSA/MCSE/MCITP认证考试的参考用书。

图书在版编目（CIP）数据

Windows Server 2008 R2 Active Directory 配置指南/戴有炜编著.—北京：清华大学出版社，2011.1
ISBN 978-7-302-24230-7
I. ①W… II. ①戴… III. ①服务器—操作系统（软件），Windows Server 2008 R2—指南 IV.①TP316.86-62
中国版本图书馆 CIP 数据核字（2010）第 231065 号

责任编辑：夏非彼　张　楠
责任校对：闫秀华
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座

印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：190×260　**印　张**：30.5　**字　数**：781 千字
版　　次：2011 年 1 月第 1 版　　**印　　次**：2011 年 1 月第1 次印刷
印　　数：1～4000
定　　价：59.00 元

产品编号：040286-01

Download at http://www.pin5i.com/

序

首先要感谢读者长久以来的支持与厚爱！本书仍然采用我一贯的编写风格，也就是完全站在读者的角度考虑问题。我花费相当多的时间不断测试与验证书中所讲述的内容，并融合多年的教学经验，然后以最容易让读者理解的方式将其写到书中。

本书的宗旨是希望通过完整与清晰的操作步骤，让读者能够轻松地使用与管理Windows Server 2008 R2的网络环境，因此书中不但理论解说清楚，而且范例充足。对需要参加微软认证考试的读者来说，本书更是不可或缺的参考书籍。

本套书分为《Windows Server 2008 R2安装与管理》、《Windows Server 2008 R2网络管理与架站》、《Windows Server 2008 R2 Active Directory配置指南》三本，内容丰富扎实，相信这几本书仍然不会辜负读者朋友的期望，给予您在学习Windows Server 2008 R2上的最大帮助。

感谢所有让这本书能够顺利出版的朋友们，无论是给予宝贵意见、帮助技术校稿、出借测试设备或提供软件资源的朋友们，尤其是“总合生活股份有限公司”，这家专门承接微软技术支持项目的公司，一直都给予我全方位的支持，包含各种最新、最快的资源与各种测试设备。

同时还要感谢参与改编工作的杨帆、刘景轩、蒋伟、卢亮、夏毓彦、高萍、王翔、赵聃、李铃、朱阔成、王金柱、王国春、施妍然、冯秀娟、孟宗斌、卞雨桂、张皓、张君慧、魏忠波等同志的共同努力。

戴有炜

2010.12

Download at http://www.pin5i.com/

目　录

第 1 章　Active Directory 域服务（AD DS）.....1

1-1　Active Directory 域服务概述.....2

1-1-1　Active Directory 域服务的适用范围（Scope）.....2

1-1-2　名称空间（Namespace）.....2

1-1-3　对象（Object）与属性（Attribute）.....3

1-1-4　容器（Container）与组织单位（Organization Units, OU）.....3

1-1-5　域树（Domain Tree）.....4

1-1-6　信任（Trust）.....5

1-1-7　林（Forest）.....6

1-1-8　架构（Schema）.....7

1-1-9　域控制器（Domain Controller）.....7

1-1-10　Active Directory 的复制模式.....8

1-1-11　域中的其他成员计算机.....8

1-1-12　DNS 服务器.....9

1-1-13　Lightweight Directory Access Protocol（LDAP）.....10

1-1-14　全局编录（Global Catalog）.....11

1-1-15　站点（Site）.....11

1-1-16　目录分区（Directory Partition）.....12

1-2　Windows Server 2008 R2 域控制器的新功能.....13

1-2-1　只读域控制器（RODC）.....13

1-2-2　可重新启动的 AD DS（Restartable AD DS）.....14

1-2-3　Active Directory 回收站.....15

1-3　域功能级别与林功能级别.....15

1-3-1　域功能级别（Domain Functionality Level）.....15

1-3-2　林功能级别（Forest Functionality Level）.....16

1-4　Active Directory 轻型目录服务（AD LDS）.....17

Download at http://www.pin5i.com/

第2章 建立AD DS域 19

2-1 创建AD DS域前的准备工作 20

2-1-1 选择适当的DNS域名 20

2-1-2 准备好一台用来支持AD DS的DNS服务器 20

2-1-3 选择Active Directory数据库的存储位置 22

2-2 创建AD DS域 23

2-2-1 使用Windows窗口来安装第一台域控制器 24

2-2-2 使用应答文件来安装第一台域控制器 32

2-2-3 使用命令行来安装第一台域控制器 33

2-3 确认AD DS域是否正常 34

2-3-1 检查DNS服务器内的日志是否完整 34

2-3-2 排除注册失败的问题 37

2-3-3 检查Active Directory数据库文件与SYSVOL文件夹 38

2-3-4 新添加的管理工具 40

2-3-5 查看事件日志文件 40

2-4 提升域与林功能级别 41

2-4-1 提升域功能级别 42

2-4-2 提升林功能级别 42

2-5 添加额外域控制器与RODC 42

2-5-1 使用Windows窗口界面来安装额外域控制器 43

2-5-2 使用应答文件来安装额外域控制器 51

2-5-3 使用命令行来安装额外域控制器 52

2-5-4 使用安装媒体来安装额外域控制器 53

2-5-5 更改RODC的委派与密码复制策略设置 56

2-6 RODC阶段式安装 57

2-6-1 使用Windows窗口创建RODC账户 58

2-6-2 将服务器附加到RODC账户 62

2-7 将Windows计算机加入或脱离域 67

2-7-1 将Windows计算机加入域 67

2-7-2 使用已加入域的计算机登录 70

2-7-3 脱机加入域 71

2-7-4 脱离域 73

2-8 在域成员计算机内安装AD DS管理工具 74

Download at http://www.pin5i.com/

2-8-1 在 Windows Server 2008 R2 计算机上安装 AD DS 管理工具 74
2-8-2 在 Windows Server 2008 计算机上安装 AD DS 管理工具 75
2-8-3 在 Windows 7 计算机上安装 AD DS 管理工具 75
2-8-4 在 Windows Vista 计算机上安装 AD DS 管理工具 76
2-9 删除域控制器和域 77
2-9-1 使用 Windows 窗口来删除域控制器或域 78
2-9-2 使用应答文件来删除域控制器或域 81
2-9-3 使用命令行来删除域控制器或域 82
2-10 域升级与在现有域环境中安装域控制器 83
2-10-1 将现有 Windows 2000 或 Windows Server 2003 林升级 83
2-10-2 在现有 Windows 2000 或 Windows Server 2003 林中添加 Windows Server 2008 或 Windows Server 2008 R2 域 86
2-10-3 在现有 Windows 2000 或 Windows Server 2003 域中添加 Windows Server 2008 或 Windows Server 2008 R2 域控制器 86
第 3 章 域用户与组账户的管理 87
3-1 管理域用户账户 88
3-1-1 创建组织单位与域用户账户 89
3-1-2 用户登录账户 90
3-1-3 创建 UPN 的后缀 92
3-1-4 账户的一般管理工作 93
3-1-5 域用户账户的属性设置 95
3-1-6 搜索用户账户 97
3-1-7 域控制器之间数据的复制 102
3-2 一次同时添加多个用户账户 103
3-2-1 使用 csvde.exe 来添加用户账户 104
3-2-2 使用 ldifde.exe 来添加、修改与删除用户账户 105
3-2-3 使用 dsadd.exe 等程序来添加、修改与删除用户账户 106
3-3 域组账户 108
3-3-1 域内的组类型 108
3-3-2 组的使用范围 109
3-3-3 域组的创建与管理 110
3-3-4 AD DS 内置的组 111
3-3-5 特殊组账户 113

Download at http://www.pin5i.com/

3-4 组的使用准则 113
3-4-1 A、G、DL、P策略 114
3-4-2 A、G、G、DL、P策略 114
3-4-3 A、G、U、DL、P策略 115
3-4-4 A、G、G、U、DL、P策略 115
第4章 使用组策略管理用户工作环境 116
4-1 组策略概述 117
4-1-1 组策略的功能 117
4-1-2 组策略对象 118
4-1-3 策略设置与首选设置 121
4-1-4 组策略的应用时限 122
4-2 策略设置实例演练 123
4-2-1 策略设置实例演练一：计算机配置 123
4-2-2 策略设置实例演练二：用户配置 125
4-3 首选设置实例演练 128
4-3-1 首选设置实例演练一 129
4-3-2 首选设置实例演练二 134
4-4 组策略的处理规则 138
4-4-1 一般的继承与处理规则 138
4-4-2 例外的继承设置 140
4-4-3 特殊的处理设置 143
4-4-4 更改管理GPO的域控制器 147
4-4-5 更改组策略的应用间隔时间 149
4-5 使用组策略来管理计算机与用户环境 151
4-5-1 计算机配置的管理模板策略 151
4-5-2 用户配置的管理模板策略 152
4-5-3 账户策略 153
4-5-4 用户权限分配策略 158
4-5-5 安全选项策略 160
4-5-6 登录/注销、启动/关机脚本 161
4-5-7 文件夹重定向 165
4-6 使用组策略来限制访问可移动存储设备 172
4-7 WMI筛选器 176

Download at http://www.pin5i.com/

4-8 组策略建模与组策略结果 179
4-9 组策略的委派管理 186
4-9-1 站点、域或组织单位的 GPO 链接委派 186
4-9-2 编辑 GPO 的委派 187
4-9-3 添加 GPO 的委派 187
4-9-4 WMI 筛选器的委派 188
4-10 Starter GPO 的设置和使用 189
第 5 章 使用组策略部署软件 191
5-1 软件部署概述 192
5-1-1 将软件分配给用户 192
5-1-2 将软件分配给计算机 192
5-1-3 将软件发布给用户 192
5-1-4 自动修复软件 193
5-1-5 删除软件 193
5-2 将软件发布给用户 194
5-2-1 发布软件 194
5-2-2 客户端安装被发布的软件 197
5-2-3 测试自动修复软件的功能 198
5-2-4 取消已发布的软件 199
5-3 将软件分配给用户或计算机 200
5-3-1 分配给用户 200
5-3-2 分配给计算机 201
5-4 软件升级和重新部署 201
5-4-1 软件升级 201
5-4-2 重新部署 205
5-5 部署 Microsoft Office 206
5-5-1 部署 Microsoft Office 2003 206
5-5-2 部署 Microsoft Office 2007 212
5-6 发布 ZAP 应用程序 217
5-7 软件部署的其他设置 220
5-7-1 更改部署默认值 220
5-7-2 更改高级部署设置 221
5-7-3 扩展名和软件关联的优先级 222

Download at http://www.pin5i.com/

5-7-4 软件分类 222
5-8 将软件重新封装成 MSI 应用程序 224
第 6 章 限制软件的运行 227
6-1 软件限制策略概述 228
6-1-1 哈希规则 228
6-1-2 证书规则 228
6-1-3 路径规则 229
6-1-4 网络区域规则 229
6-1-5 规则的优先级 230
6-2 启用软件限制策略 230
6-2-1 新建哈希规则 231
6-2-2 新建路径规则 233
6-2-3 新建证书规则 235
6-2-4 新建网络区域规则 238
6-2-5 不要将软件限制策略应用到本地系统管理员 239
第 7 章 创建域树和林 241
7-1 创建第一个域 242
7-2 创建子域 242
7-2-1 使用 Windows 窗口来创建子域 243
7-2-2 使用应答文件来创建子域 250
7-2-3 使用命令行来创建子域 252
7-3 创建林中的第 2 个域树 252
7-3-1 选择适当的 DNS 架构 253
7-3-2 使用 Windows 窗口来创建第 2 个域树 255
7-3-3 使用应答文件来创建第 2 个域树 262
7-3-4 使用命令行来创建第 2 个域树 263
7-4 删除子域和域树 264
7-4-1 使用 Windows 窗口来删除子域或域树 264
7-4-2 使用应答文件来删除子域或域树 267
7-4-3 使用命令行来删除子域或域树 269
7-5 更改域控制器的计算机名称 270

Download at http://www.pin5i.com/

第 8 章 管理域和林信任 272

8-1 域和林信任概述 273

8-1-1 信任域和受信任域 273

8-1-2 跨域访问资源的流程 273

8-1-3 信任的种类 276

8-1-4 创建信任前的注意事项 280

8-2 创建**快捷方式信任** 281

8-3 创建**林信任** 287

8-3-1 创建林信任前的注意事项 288

8-3-2 开始创建**林信任** 289

8-3-3 设置**选择性身份验证** 297

8-4 创建**外部信任** 299

8-5 管理和删除信任 302

8-5-1 信任的管理 302

8-5-2 信任的删除 305

第 9 章 Active Directory 数据库的复制 307

9-1 站点与 Active Directory 数据库的复制 308

9-1-1 同一个站点之间的复制 309

9-1-2 不同站点之间的复制 310

9-1-3 目录分区与复制拓扑 311

9-1-4 复制协议 311

9-2 默认站点的管理 312

9-2-1 默认的站点 312

9-2-2 Servers 文件夹与复制设置 313

9-3 利用站点来管理 Active Directory 复制 316

9-3-1 创建站点与子网 317

9-3-2 创建站点链接 319

9-3-3 将域控制器转移到所属的站点 321

9-3-4 指定首选的 bridgehead 服务器 322

9-3-5 站点链接与 Active Directory 数据库的复制设置 324

9-3-6 站点链接桥 326

9-3-7 站点链接桥的两个示例讨论 328

Download at http://www.pin5i.com/

9-4 管理全局编录服务器 330
9-4-1 添加属性到全局编录内 330
9-4-2 全局编录的功能 331
9-4-3 通用组成员身份缓存 333
9-5 解决 Active Directory 复制冲突的问题 334
9-5-1 属性戳记 335
9-5-2 冲突的种类 335
第 10 章 操作主机的管理 339
10-1 操作主机概述 340
10-1-1 架构操作主机 340
10-1-2 域命名操作主机 340
10-1-3 RID 操作主机 341
10-1-4 PDC 模拟器操作主机 341
10-1-5 基础结构操作主机 344
10-2 操作主机的放置优化 344
10-2-1 基础结构操作主机的放置 345
10-2-2 PDC 模拟器操作主机的放置 345
10-2-3 林级别操作主机的放置 346
10-2-4 域级别操作主机的放置 346
10-3 找出扮演操作主机角色的域控制器 347
10-3-1 找出架构操作主机 347
10-3-2 找出域命名操作主机 348
10-3-3 找出 RID、PDC 与基础结构操作主机 349
10-4 转移操作主机角色 349
10-5 夺取操作主机角色 353
10-5-1 操作主机关机所造成的影响 353
10-5-2 夺取操作主机角色实例演练一 355
10-5-3 夺取操作主机角色实例演练二 357
第 11 章 AD DS 的维护 361
11-1 系统状态概述 362
11-1-1 Active Directory 数据库 362
11-1-2 SYSVOL 文件夹 363

Download at http://www.pin5i.com/

11-2 备份 AD DS 363
11-2-1 安装 Windows Server Backup 功能 363
11-2-2 备份系统状态 364
11-3 还原 AD DS 367
11-3-1 进入目录服务还原模式的方法 367
11-3-2 执行 AD DS 的非授权还原 369
11-3-3 针对被删除的 AD DS 对象执行授权还原 374
11-4 Active Directory 数据库的转移与重组 377
11-4-1 可重新启动的 AD DS（Restartable AD DS） 377
11-4-2 转移 Active Directory 数据库文件 378
11-4-3 重组 Active Directory 数据库 382
11-5 重设**目录服务还原模式**的系统管理员密码 386
11-6 更改**可重新启动的 AD DS** 的登录设置 387
11-7 Active Directory 回收站 387
11-7-1 **Active Directory 回收站**的系统需求 388
11-7-2 启用 **Active Directory 回收站** 389
11-7-3 还原被删除的对象 389

第 12 章 将资源发布到 AD DS 396

12-1 将共享文件夹发布到 AD DS 397
12-1-1 利用 **Active Directory 用户和计算机**控制台 397
12-1-2 利用**计算机管理**控制台 399
12-2 搜索 AD DS 内的资源 400
12-2-1 通过网络 400
12-2-2 通过 **Active Directory 用户和计算机**控制台 402
12-3 将共享打印机发布到 AD DS 404
12-3-1 发布打印机 404
12-3-2 通过 AD DS 搜索共享打印机 407
12-3-3 利用**打印机位置**来搜索打印机 407

第 13 章 自动信任根 CA 412

13-1 自动信任 CA 的设置准则 413
13-2 自动信任内部的独立 CA 413
13-2-1 下载独立根 CA 的证书并保存 414

Download at http://www.pin5i.com/

13-2-2 将独立根 CA 的证书导入到**受信任的根证书颁发机构**策略 416
13-3 自动信任外部的 CA 419
13-3-1 下载独立根 CA 的证书并保存 419
13-3-2 申请可以为**证书信任列表**签名的证书 420
13-3-3 创建**证书信任列表（CTL）** 423
附录 A AD DS 与防火墙 428
A-1 AD DS 相关的端口 429
A-1-1 用户登录时会用到的端口 429
A-1-2 计算机登录时会用到的端口 430
A-1-3 创建域信任时会用到的端口 430
A-1-4 验证域信任时会用到的端口 430
A-1-5 访问文件资源时会用到的端口 431
A-1-6 运行 DNS 查询时会用到的端口 431
A-1-7 运行 Active Directory 数据库复制时会用到的端口 431
A-1-8 文件复制服务（FRS）会用到的端口 431
A-1-9 分布式文件系统（DFS）会用到的端口 432
A-1-10 其他可能需要开放的端口 432
A-2 限制动态 RPC 端口的使用范围 432
A-2-1 限制所有服务的动态 RPC 端口范围 433
A-2-2 限制 Active Directory 数据库复制时指定的静态端口 434
A-2-3 限制 FRS 使用指定的静态端口 435
A-2-4 限制 DFS 使用指定的静态端口 435
A-3 IPSec 与 VPN 端口 437
A-3-1 IPSec 所使用的协议与端口 437
A-3-2 PPTP VPN 所使用的协议与端口 437
A-3-3 L2TP/IPSec 所使用的协议与端口 437
附录 B 服务器核心安装的管理 438
B-1 **服务器核心安装**概述 439
B-2 **服务器核心安装**的基本设置 440
B-2-1 更改计算机名 440
B-2-2 更改 IP 地址 441
B-2-3 启用**服务器核心安装** 443

Download at http://www.pin5i.com/

B-2-4 加入域 443
B-2-5 将域用户加入本地 Administrators 组 444
B-2-6 更改日期与时间、地区及语言选项 445
B-3 在**服务器核心安装**内安装服务器角色 445
B-3-1 查看现有的角色与功能 445
B-3-2 DNS 服务器角色 446
B-3-3 DHCP 服务器角色 446
B-3-4 文件服务角色 447
B-3-5 Hyper-V 角色 447
B-3-6 打印服务角色 448
B-3-7 Active Directory 证书服务（AD CS）角色 448
B-3-8 Active Directory 轻型目录服务（AD LDS）角色 448
B-3-9 Active Directory 域服务（AD DS）角色 448
B-3-10 Stream Media Services 角色 448
B-3-11 Web 服务器（IIS）角色 449
B-4 在**服务器核心安装**内安装功能 450
B-5 **服务器核心安装**的远程管理 451
B-5-1 通过远程桌面来管理**服务器核心安装** 452
B-5-2 通过 RemoteApp 来管理**服务器核心安装** 453
B-5-3 通过 MMC 管理控制台来管理**服务器核心安装** 458
B-5-4 通过服务器管理器来管理**服务器核心安装** 460
B-5-5 通过 Windows Remote Shell 来管理**服务器核心安装** 467
B-5-6 安装硬件设备 467
B-5-7 其他注意事项 468
B-6 常用命令列表 468
B-6-1 设置与安装命令 469
B-6-2 网络与防火墙命令 470
B-6-3 更新、错误报告与回应 470
B-6-4 服务、程序与性能 471
B-6-5 事件日志 471
B-6-6 磁盘与文件系统 472
B-6-7 硬件设备驱动器 472

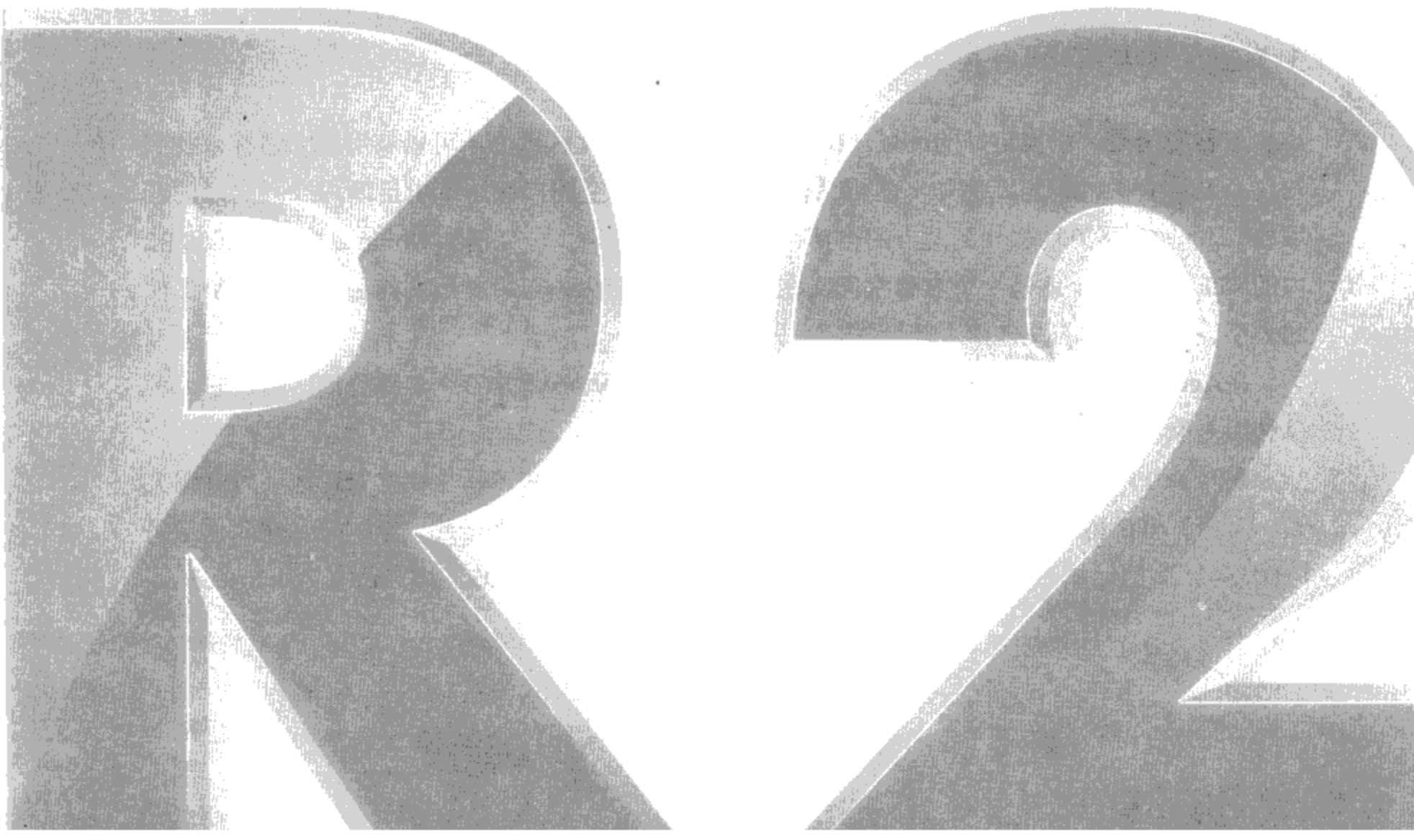
Download at http://www.pin5i.com/

第1章

Active Directory 域服务（AD DS）

在Windows Server 2008 R2的网络环境中，Active Directory域服务（Active Directory Domain Services，AD DS）为您提供用于组织、管理与控制网络资源的各种强大功能。

- Active Directory域服务概述
- Windows Server 2008 R2域控制器的新功能
- 域功能级别与林功能级别
- Active Directory轻型目录服务（AD LDS）



Download at http://www.pin5i.com/

1-1 Active Directory域服务概述

何谓**Directory**呢？我们日常生活中使用的电话簿内记录着亲朋好友的姓名、电话与地址等数据，它就是**Telephone Directory**（电话目录）；计算机中的文件系统（File System）内记录着文件的文件名、大小与日期等数据，它就是**File Directory**（文件目录）。

如果这些Directory内的文件能够系统地加以整理的话，用户就能够很容易且迅速地查找到所需文件，而Directory Service（目录服务）所提供的服务，就是要让用户很容易且迅速地在Directory内查找所需文件。在现实生活中，查号台也是一种目录服务；在因特网上，Baidu网站所提供的搜索功能也是一种目录服务。

Active Directory域内的Directory则是用来存储用户账户、计算机账户、打印机与共享文件夹等对象，我们把这些对象的存储位置称为**目录数据库**（Directory Database）。Active Directory域内负责提供目录服务的组件就是**Active Directory域服务**（Active Directory Domain Services，AD DS），它负责目录数据库的存储、添加、删除、修改与查询等工作。

1-1-1 Active Directory域服务的适用范围（Scope）

Active Directory域服务的适用范围非常广泛，它可以用在一台计算机、一个小型局域网（LAN）或数个广域网（WAN）的结合中。它包含此范围内所有的对象，例如文件、打印机、应用程序、服务器、域控制器与用户账户等。

1-1-2 名称空间（Namespace）

名称空间是一块界定好的区域（Bounded Area），在此区域内，可以利用某个名称来找到与这个名称有关的信息，例如一本电话簿就是一个**名称空间**，在这本电话簿内（界定好的区域内），可以利用姓名来找到此人的电话、地址与生日等数据。又例如Windows Server 2008 R2内的NTFS文件系统就是一个**名称空间**，在这个文件系统内，可以利用文件名来找到这个文件的大小、修改日期与文件内容等数据。

在**Active Directory域服务**（AD DS）内，Active Directory就是一个**名称空间**，通过它，可以利用对象名称来找到与这个对象有关的所有信息。

在TCP/IP网络环境中是利用Domain Name System（DNS）来解析主机名与IP地址的对应关系，而因为**Active Directory域服务**（AD DS）与DNS紧密地集成在一起，它的域名**空间**也是采用DNS架构，因此域名是采用DNS格式来命名的，例如可以将AD DS的域名命名为sayms.com。

Download at http://www.pin5i.com/

1-1-3 对象（Object）与属性（Attribute）

AD DS域内的资源是以对象的形式存在的，例如用户、计算机与打印机都是对象，而对象是通过**属性**来描述其特征，也就是对象本身是一些**属性**的集合，例如若要为用户**王乔治**创建一个账户的话，则必须添加一个对象类型（Object Class）为**用户**的对象（也就是用户账户），然后在这个用户账户内输入**王乔治**的姓、名、登录账户、电话号码与电子邮件等数据，这其中的用户账户就是对象，而姓、名、登录账户、电话号码与电子邮件等数据就是该对象的属性（如表1-1所示）。

表 1-1

对象（object）	属性（attributes）
用户（user）	姓
	名
	登录账户
	电话号码
	电子邮件
	网页
	职称
	部门
	…

如图1-1所示中的**王乔治**就是对象类型为**用户**的对象。

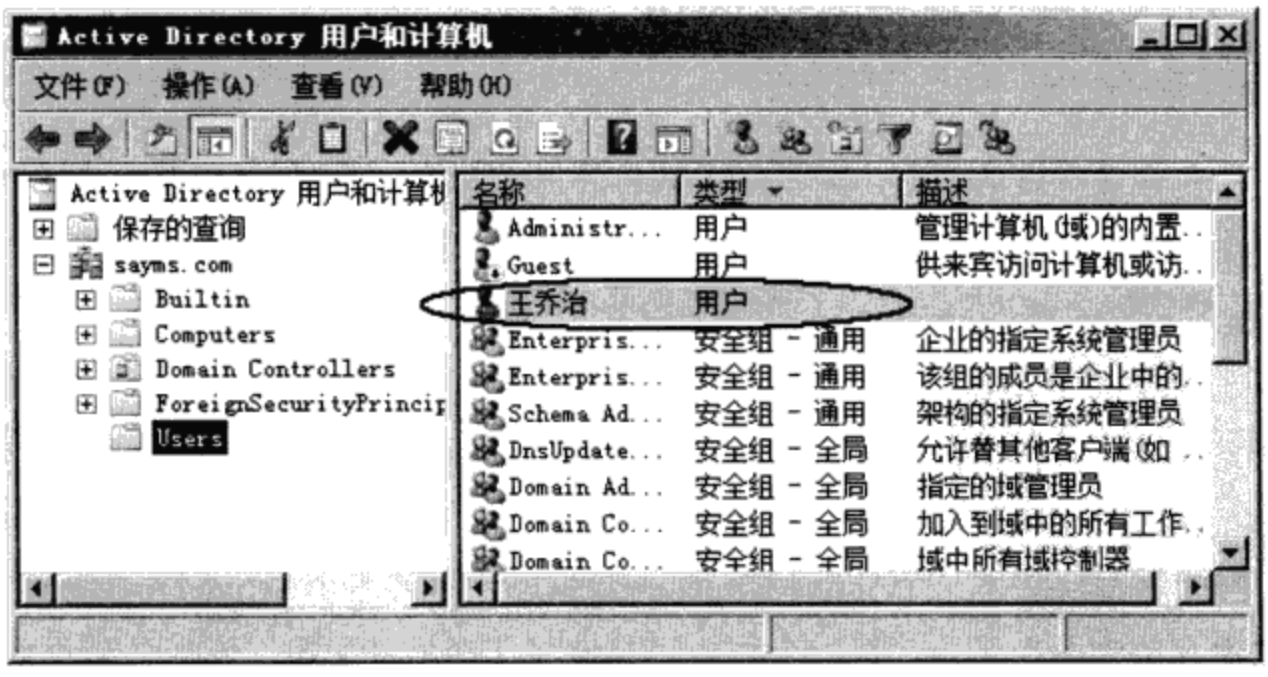


图 1-1

1-1-4 容器（Container）与组织单位（Organization Units, OU）

容器与对象相似，它也有自己的名称，也是一些属性的集合，不过容器内可以包含其他对

Download at http://www.pin5i.com/

象（例如**用户**、**计算机**等对象），也可以包含其他容器，而组织单位则是一个比较特殊的容器，其内除了可以包含其他对象与组织单位之外，还有**组策略**（Group Policy）的功能。

如图 1-2所示就是一个名称为**业务部**的组织单位，其内包含着数个对象，其中两个为**用户**对象、两个为**计算机**对象、两个为组织单位的对象。

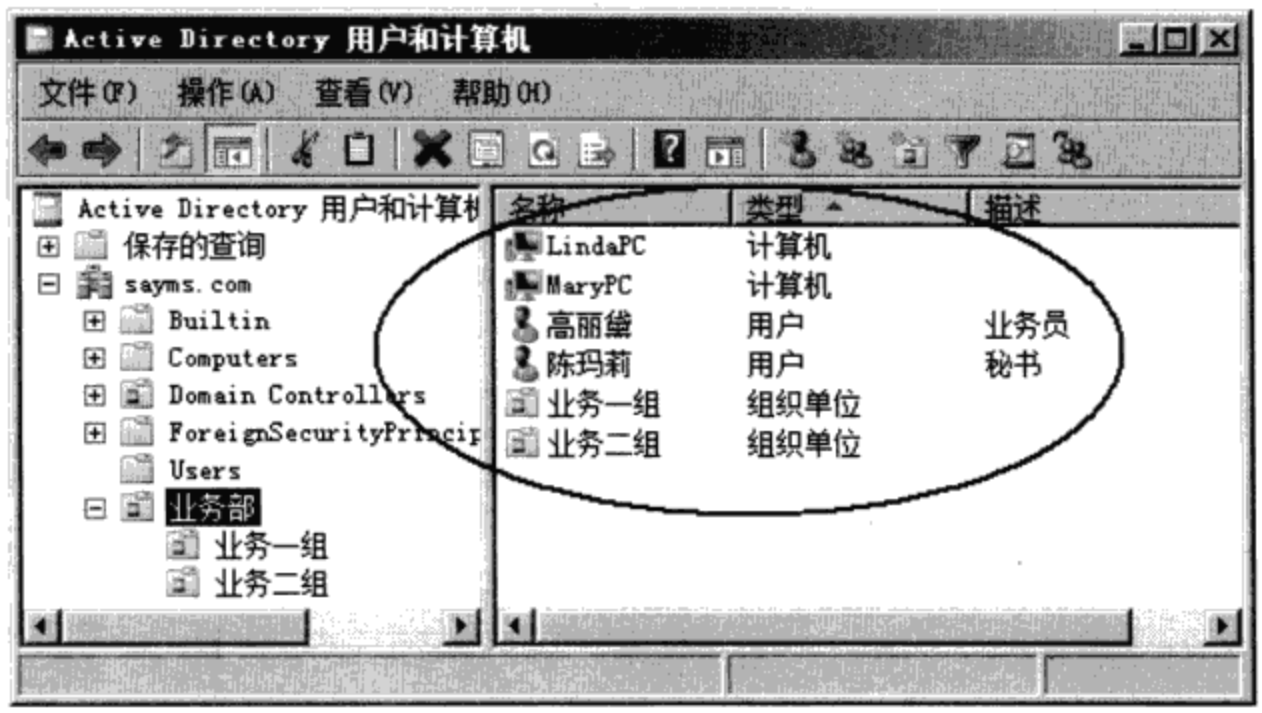


图 1-2

AD DS是以层次架构（Hierarchical）将对象、容器与组织单位等组合在一起，并将其存储到Active Directory数据库内。

1-1-5 域树（Domain Tree）

可以架构包含数个域的网络，而且是以域树的形式存在，如图 1-3所示就是一个域树，其中最上层的域名为sayms.com，它是此域树的根域（Root Domain）；根域之下还有2个子域（sales.sayms.com与mkt.sayms.com），之下还有3个子域。

图中域树符合DNS域名空间的命名原则，其名称空间是有连续性的（Contiguous），也就是子域的域名内包含着其父域的域名，例如域sales.sayms.com的后缀包含着其前一层（父域）的域名sayms.com；而nor.sales.sayms.com的后缀包含着其前一层的域名sales.sayms.com。

在域树内的所有域共享一个Active Directory数据库，不过这个Active Directory数据库内的数据是分散地存储在各个域内，每一个域内只存储属于该域的数据，例如该域内的用户账户（这些数据是存储在域控制器内）。

Download at http://www.pin5i.com/

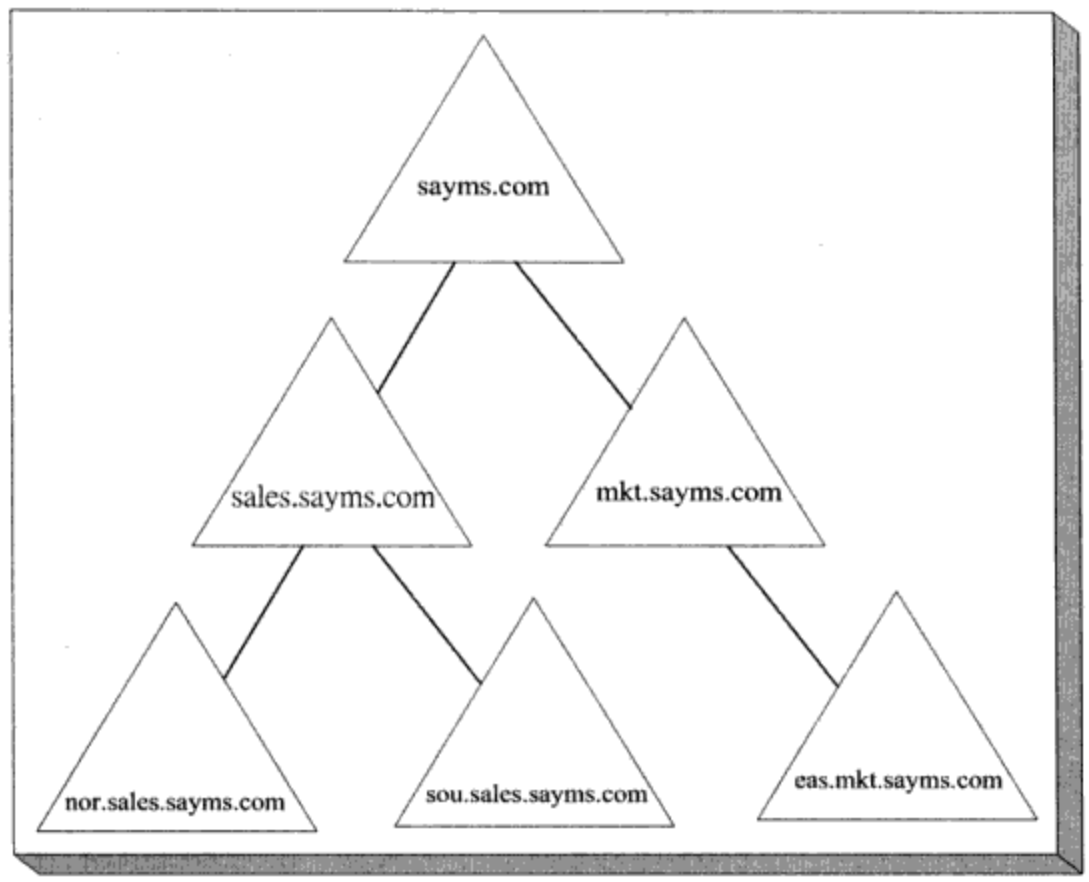


图 1-3

1-1-6 信任（Trust）

两个域之间必须创建信任关系（Trust Relationship），才可以访问对方域内的资源。而任何一个新AD DS域被加入到域树后，这个域会自动信任其前一层的父域，同时父域也会自动信任这个新子域，而且这些信任关系具备双向传递性（Two-Way Transitive）。由于这个信任工作是通过Kerberos Security Protocol来完成，因此也被称为Kerberos Trust。

Q 域A的用户登录到其所隶属的域后，这个用户可否访问B域内的资源呢?

A 只要域B信任域A就没有问题。

Q 甲用户隶属于域A，乙计算机隶属于域B，请问甲用户是否可利用乙计算机登录到域A呢?

A 只要域B信任域A就没有问题。

下面通过图 1-4来解释双向传递性，图中域 A信任域B（箭头由A指向B）、域 B又信任域C，因此域 A自动信任域 C；另外域 C信任域 B（箭头由C指向B）、域 B又信任域 A，因此域 C自动信任域 A。结果是域 A 和域 C 之间也就自动创建起双向的信任关系，这个因为传递性而得到的信任关系，可称之为隐性的信任关系（Implicit Trust）。

Download at http://www.pin5i.com/

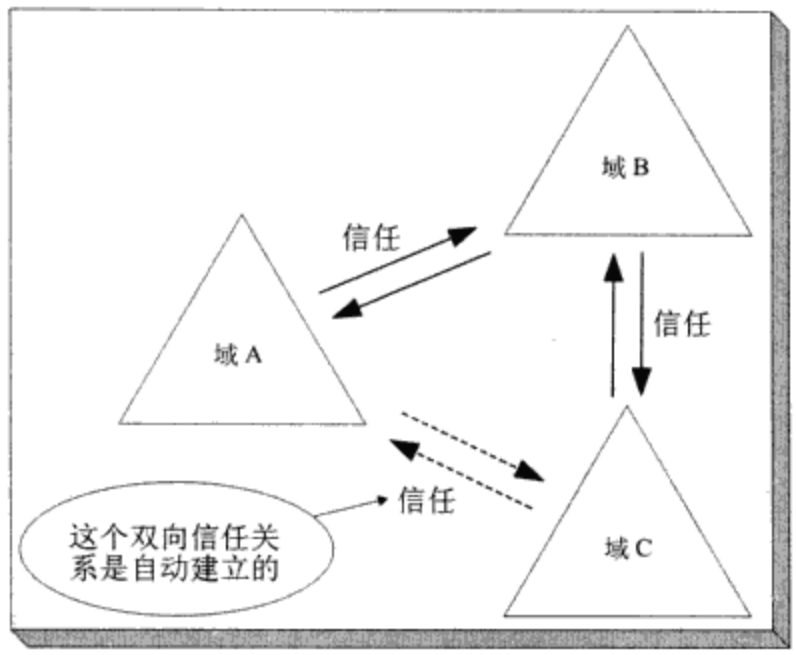


图 1-4

所以当任何一个AD DS域加入到域树后，它会自动双向信任这个域树内的所有域，因此只要拥有适当权限，这个新域的用户便可访问其他域内的资源，同理其他域的用户也可以访问这个新域内的资源。

1-1-7 林（Forest）

林是由一或数个域树所组成，每一个域树都有自己唯一的名称空间，例如图 1-5中，一个域树内的每一个域名都是以sayms.com结束，而另一个则都是以sayisa.com结束。

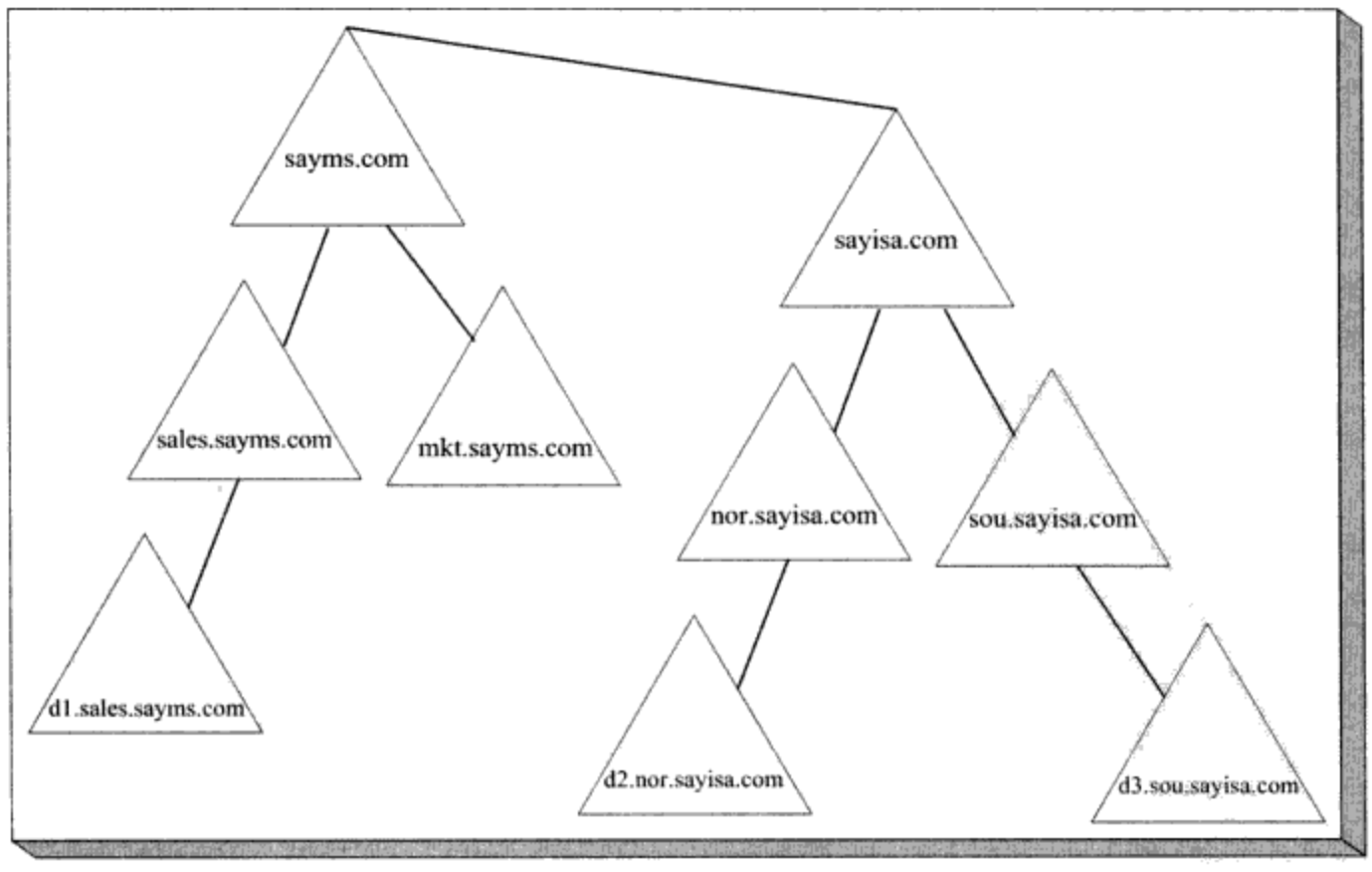


图 1-5

Download at http://www.pin5i.com/

所创建的第1个域树的根域，就是整个林的根域（Forest root Domain），同时其域名就是林的林名称。例如图 1-5中的sayms.com是第1个域树的根域，它也是整个林的根域，而林的名称就是sayms.com。

当在创建林时，每一个域树的根域与林根域之间双向的、转移性的信任关系都会自动被创建起来，因此每一个域树中的每一个域内的用户，只要拥有权限，都可以访问其他任何一个域树内的资源，也可以到其他任何一个域树内的计算机登录。

1-1-8 架构（Schema）

AD DS内的对象类型与属性数据定义在**架构**（Schema）内，例如定义了**用户**对象类型内包含了哪一些属性（姓、名、电话号码等）、每一个属性的数据类型等信息。

应用程序可以在**架构**内添加其所需的对象类型或属性，Schema Admins组内的用户（默认仅包含Administrator）也可以修改**架构**内的数据。在一个林内的所有域树共享相同的**架构**。

1-1-9 域控制器（Domain Controller）

Active Directory域服务（AD DS）的目录数据存储在域控制器内。一个域内可以有多台域控制器，每一台域控制器的地位（几乎）是平等的，它们各自存储着一份（几乎）完全相同的Active Directory数据库。当在任何一台域控制器内添加一个用户账户后，这个账户默认是被创建在此域控制器的Active Directory数据库内，之后这个账户会自动被复制到其他域控制器的Active Directory数据库，如图1-6所示，以便让所有域控制器内的AD DS数据都能够同步（Synchronize）。

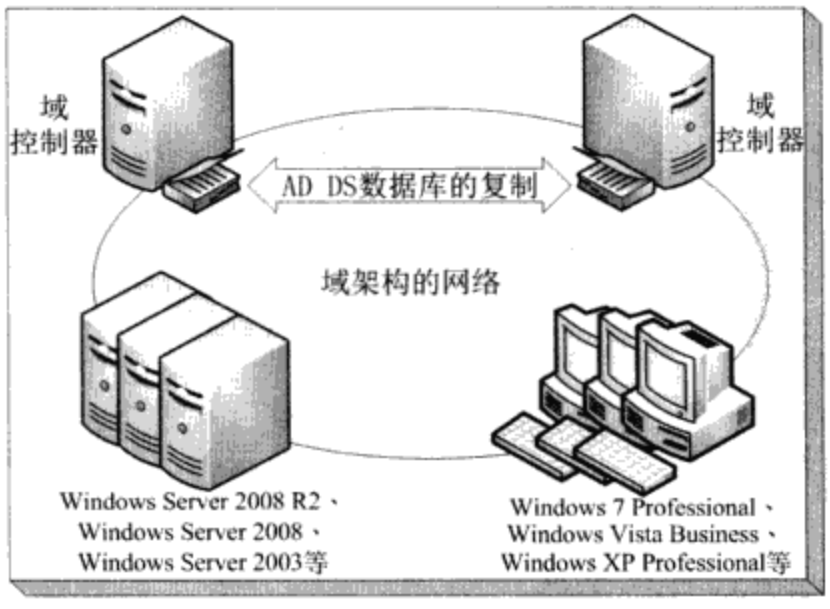


图 1-6

当用户在域内的某台计算机登录时，会由其中一台域控制器根据其Active Directory数据库

Download at http://www.pin5i.com/

内的账户数据来审核用户所输入的账户与密码是否正确。若是正确的，用户就可以登录成功；反之，将被拒绝登录。

多台域控制器可以提供容错功能，也就是即使有一台域控制器故障了，仍然能够由其他域控制器来提供服务。另外它也可以改善用户登录效率，因为多台域控制器可以分担审核用户登录身份（账户名称与密码）的负担。

域控制器是由服务器级别的计算机所扮演，在Windows Server 2008 R2家族中除了Windows Web Server 2008 R2与Windows Server 2008 R2 for Itanium-Based Systems之外，其他都可以扮演域控制器的角色。

1-1-10 Active Directory的复制模式

域控制器之间在复制Active Directory数据库时，分为以下两种复制模式。

- **多主机复制模式**（Multi-master Replication Model）：Active Directory数据库内大部分的数据是利用这种模式进行复制。在这种模式之中，可以直接更新任何一台域控制器内的Active Directory对象，之后这个更新的对象会被自动复制到其他域控制器。例如当在任何一台域控制器的Active Directory数据库内添加一个用户账户后，这个账户会自动被复制到域内的其他域控制器。
- **单主机复制模式**（Single-master Replication Model）：在Active Directory数据库内的少部分数据是采用**单主机复制模式**来复制。在这种模式之中，当提出更改对象数据的要求时，会由其中一台域控制器（被称为**操作主机**）负责接收与处理此要求，也就是说该对象是先被更新在**操作主机**，再由这台**操作主机**将它复制到其他的域控制器。例如当添加或删除一个域时，这个变动的数据会被写到扮演**域命名操作主机**（Domain Naming Operations Master）角色的域控制器内，再由这台域控制器将它复制到其他的域控制器。

1-1-11 域中的其他成员计算机

除了域控制器之外，如果要充分管理其他计算机的话，请将这些计算机加入域。另外用户如果要在这些计算机上利用Active Directory数据库内的域用户账户来登录的话，这些计算机也必须加入域（在未加入域的计算机上只能够使用本地用户账户登录）。域中的成员计算机包括成员服务器以及其他常用的Windows计算机。

1. 成员服务器（Member Server）

服务器级别的计算机加入域后被称为**成员服务器**，成员服务器内没有Active Directory数据库，它们也不负责审核AD DS域的用户名与密码，而是将其传输给域控制器来审核。成员服务

Download at http://www.pin5i.com/

器可以是：

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows 2000 Server

若上述服务器没有被加入域的话，则它们被称为**独立服务器**（Stand-alone Server）或**工作组服务器**（Workgroup Server）。但无论是独立服务器或成员服务器，它们都有**本地安全账户数据库**（SAM），系统可以用它来审核本地用户（非AD DS域用户）的身份。

> **提示**
>
> Windows Server 2008与Windows Server 2008 R2域控制器并不支持Windows NT 4.0成员服务器，因此需要Windows 2000 Server或Windows Server 2003域控制器来支持Windows NT 4.0成员服务器。

2. 其他常用的 Windows 计算机

例如：

- Windows 7 Ultimate、Windows 7 Enterprise、Windows 7 Professional
- Windows Vista Ultimate、Windows Vista Enterprise、Windows Vista Business
- Windows XP Professional

当上述计算机加入域后，用户就可以在这些计算机上利用AD DS域用户账户来登录，否则只能够利用本地账户来登录。

> **注意**
>
> Windows 7 Home Premium、Windows 7 Home Basic、Windows 7 Starter、Windows Vista Home Premium、Windows Vista Home Basic、Windows Vista Starter、Windows XP Home Edition等计算机无法加入域，故只能够利用本地用户账户来登录。

在Windows网络环境下，可以将Windows Server 2008 R2、Windows Server 2008、Windows Server 2003 R2、Windows Server 2003、Windows 2000 Server独立服务器或成员服务器升级为域控制器，也可以将域控制器降级为独立服务器或成员服务器。

1-1-12 DNS服务器

域控制器需要将自己注册到DNS服务器内，以便让其他计算机通过DNS服务器来找到这台域控制器，因此搭建域环境需要有可支持AD DS的DNS服务器。此DNS服务器最好支持**动态**

Download at http://www.pin5i.com/

更新（Dynamic Update）功能，以便当域控制器的角色有变动或域成员计算机的IP地址等数据更改时，可以自动更新DNS服务器内的记录。

1-1-13 Lightweight Directory Access Protocol（LDAP）

LDAP（Lightweight Directory Access Protocol）是一种用来访问Active Directory数据库的目录服务协议。AD DS是通过**LDAP名称路径**（LDAP Naming Path）来表示对象在Active Directory数据库内的位置，以便利用它来访问Active Directory数据库内的对象。**LDAP名称路径**包括DN、RDN等。

1. Distinguished Name（DN）

它是对象在Active Directory数据库内的完整路径，如图1-7所示中的用户账户名称为**林小洋**，其DN为：CN=林小洋，OU=业务一组，OU=业务部，DC=sayms，DC=com。其中的DC（Domain Component）表示DNS域名中的组件，例如sayms.com中的sayms与com；OU为组织单位；CN为Common Name的缩写。除了DC与OU之外，其他都是利用CN来表示，例如用户与计算机对象都属于CN。上述DN表示法中的**sayms.com**为域名，**业务部**、**业务一组**都是组织单位。此DN表示**林小洋**这个账户是存储在**sayms.com\业务部\业务一组**路径内。

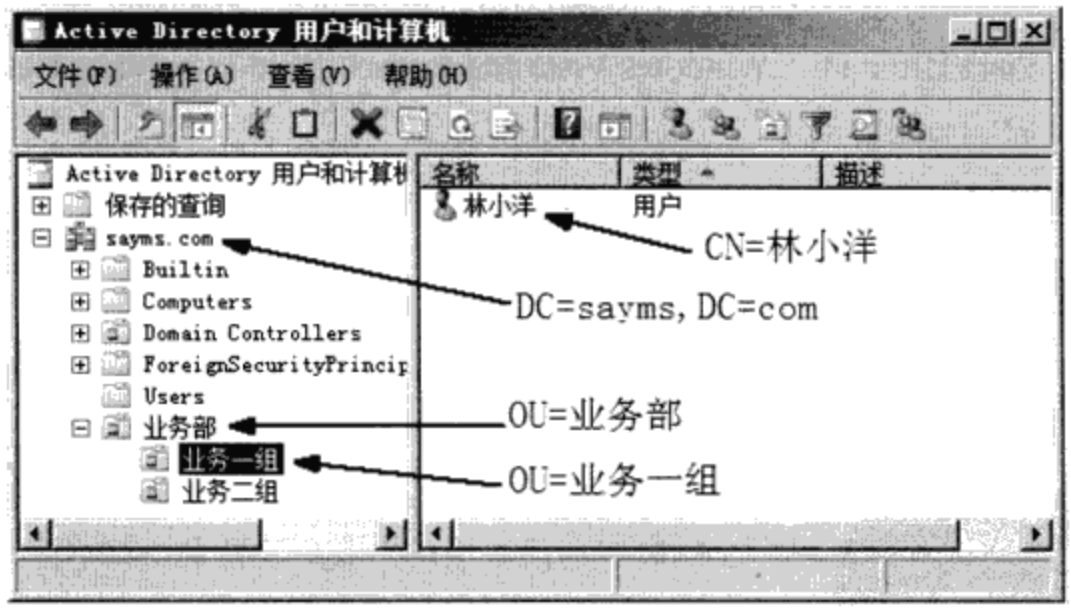


图1-7

2. Relative Distinguished Name（RDN）

它是在DN的完整路径中，用来代表某个对象的部分路径，例如上述路径中，**林小洋**的RDN为**CN=林小洋**。

除了DN与RDN这两个对象名称外，还有以下名称。

- **Global Unique Identifier（GUID）**：GUID是一个128bit的数值，所创建的任何一个对

Download at http://www.pin5i.com/

象，系统都会自动指定一个唯一的GUID给这个对象。虽然可以改变对象的名称，但是其GUID永远不会改变。

- **User Principal Name（UPN）**：每一个用户还可以有一个比DN更短、更容易记忆的UPN，如图1-7所示中的林小洋是隶属于域sayms.com，则其UPN可为bob@sayms.com。用户在登录时所输入的用户名称最好是UPN，因为无论这个用户的账户被转移到哪一个域，都不会改变他的UPN，因此用户可以一直使用同一个UPN来登录。
- **Service Principal Name（SPN）**：SPN是一个包含多重值的名称，它是根据DNS主机名来创建的。SPN用来代表某台计算机所支持的服务，它让其他计算机可以通过SPN来与这台计算机的服务通信。

1-1-14 全局编录（Global Catalog）

虽然在域树内的所有域共享一个Active Directory数据库，但其内的数据却是分散在各个域内，而每一个域只存储该域本身的数据。为了让用户、应用程序能够快速找到位于其他域内的资源，因此在AD DS内设计了**全局编录**（Global Catalog）。

全局编录的数据是存储在域控制器内，这台域控制器被称为**全局编录服务器**，它存储着林内所有域的Active Directory数据库内的每一个对象，不过只存储对象的部分属性，而不是全部属性，这些属性都是常被用来搜索的属性，例如登录账户名称、UPN、电话号码等。**全局编录**让用户即使不知道对象是位于哪一个域内，仍然可以很迅速地找到所需对象。

用户登录时，**全局编录服务器**还负责提供该用户所隶属的**通用组**数据；或是当用户利用UPN登录时，它会负责提供该用户是隶属于哪一个域的信息。

一个林内的所有域树共享相同的**全局编录**，而林内的第一台域控制器，默认就是**全局编录服务器**。必要的时候，也可以另外指派其他域控制器来扮演**全局编录服务器**。

1-1-15 站点（Site）

站点是由一个或数个IP子网（Subnet）所组成，这些子网之间通过“高速且可靠的链接”串接起来，也就是这些子网之间的链接速度要够快且稳定，否则就应该将它们分别划分为不同的站点。

一般来说，一个LAN（局域网）之内各个子网之间的链接都符合速度快且高可靠性的要求，因此可以将一个LAN规划为一个站点；而WAN（广域网）内各个LAN之间的链接速度一般都不快，因此WAN之中的各个LAN应分别划分为不同的站点，如图 1-8所示。

域是逻辑的（Logical）分组，而站点则是实体的（Physical）分组。在AD DS内，每一个站点可能会包含多个域；而一个域内的计算机也可能分别属于不同的站点。

Download at http://www.pin5i.com/

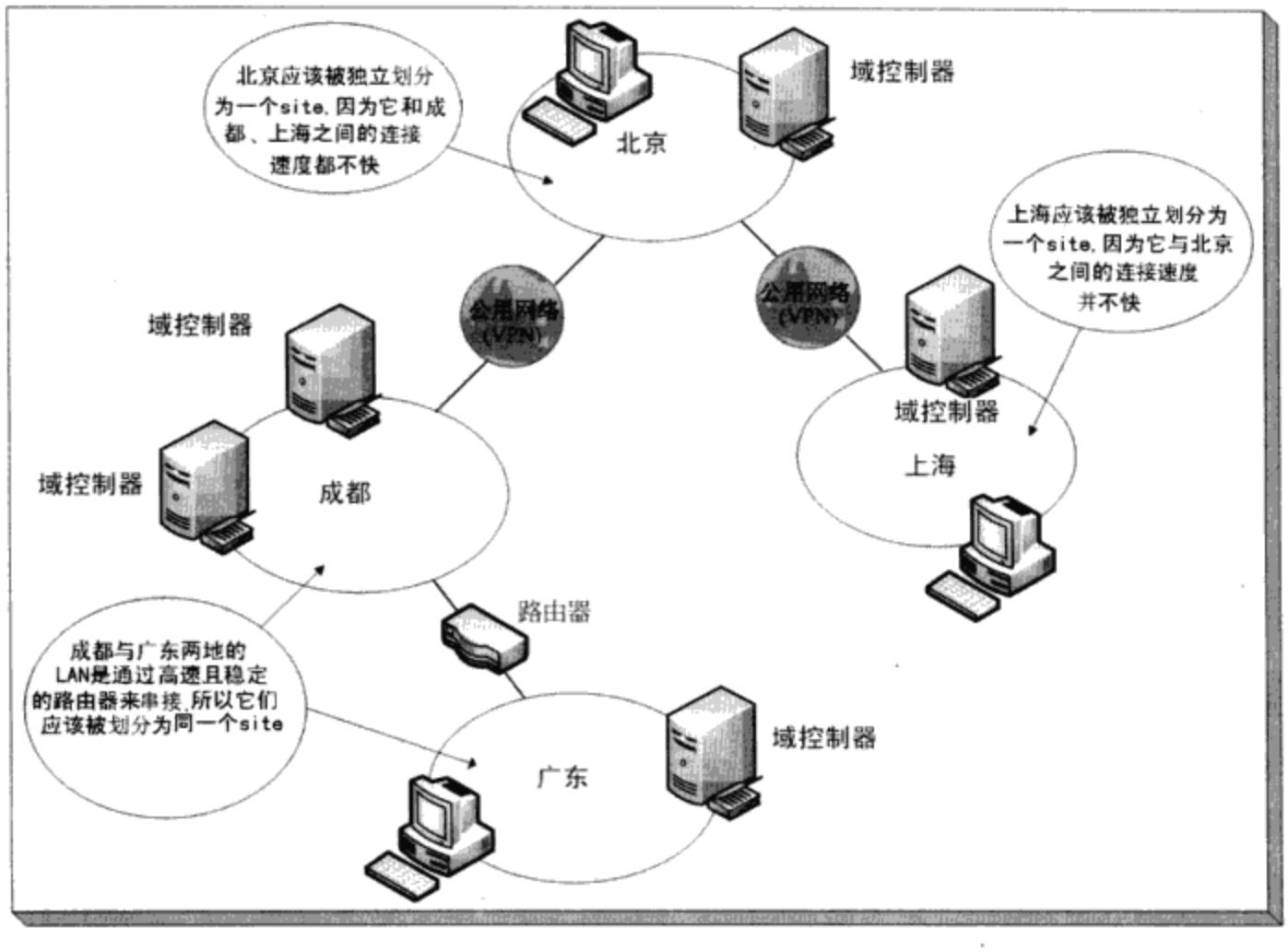


图 1-8

如果一个域的域控制器是分布在不同的站点内，而这些站点之间是低速链接（Slow WAN Link）的话，由于两个站点的域控制器之间会互相复制Active Directory数据库，因此必须谨慎划分执行复制的时段，例如尽量在网络空闲时期执行复制操作，同时复制频率也不要太高，以避免复制时占用两个站点之间的链接带宽，影响两个站点之间其他数据的传输效率。

而同一个站点之内的域控制器，由于它们之间是通过快速的链接串接在一起，因此在复制Active Directory数据库时，可以有效的、快速的复制。AD DS会设置让同一个站点内、隶属于同一个域的域控制器之间自动执行复制的工作，且其默认的复制频率也比不同站点之间要高。

不同站点之间在复制时所传送的数据会被压缩，以减少站点之间链接带宽的负担；不过同一个站点内的域控制器之间在复制时不会压缩数据。

1-1-16 目录分区（Directory Partition）

Active Directory数据库被逻辑地划分为以下几个目录分区。

- **架构目录分区**（Schema Directory Partition）：它存储着整个林中所有对象与属性的定义数据，也存储如何创建新对象与属性的规则。整个林内所有域共享一份相同的**架构目录分区**，它会被复制到林中所有域内的所有域控制器。
- **配置目录分区**（Configuration Directory Partition）：其内存储着整个AD DS的结构，例如有哪些域、有哪些站点、有哪些域控制器等数据。整个林共享一份相同的**配置目录**

Download at http://www.pin5i.com/

分区，它会被复制到整个林中的所有域控制器。

- **域目录分区**（Domain Directory Partition）：每一个域各自拥有一个唯一的**域目录分区**，其内存储着与该域有关的对象，例如用户、计算机与打印机等对象，此**域目录分区**只会被复制到该域的所有域控制器，并不会被复制到其他域的域控制器。
- **应用程序目录分区**（Application Directory Partition）：一般来说，**应用程序目录分区**是由应用程序所创建，其内存储着与该应用程序有关的数据，例如Windows Server 2008 R2作为DNS服务器时，若所创建的DNS区域为**Active Directory集成区域**的话，则它便会在Active Directory数据库内创建**应用程序目录分区**，以便存储该区域的数据。**应用程序目录分区**会被复制到林中的特定域控制器，而不是所有的域控制器。

1-2 Windows Server 2008 R2域控制器的新功能

Windows Server 2008 R2针对域控制器做了些功能上的加强，例如添加**只读域控制器**、**可重新启动的AD DS**与**Active Directory回收站**。

1-2-1 只读域控制器（RODC）

在Windows Server 2008 R2（与Windows Server 2008）内添加一个新类型的域控制器，称为**只读域控制器**（Read-Only Domain Controller，RODC）。顾名思义，它的Active Directory数据库只可以读取、不可以被修改，也就是说用户或应用程序无法直接修改RODC的Active Directory数据库。RODC的Active Directory数据库内容只能够从其他**可写域控制器**复制过来。RODC主要是设计给远程分公司的网络来使用，因为一般来说远程分公司的网络规模比较小、用户人数比较少，此网络的安全措施并不像总公司一样完备，同时也可能比较缺乏IT技术人员，因此采用RODC可避免因为其Active Directory数据库被破坏而影响到整个AD DS环境的运行。

1. RODC 的 Active Directory 数据库内容

除了账户的密码之外，RODC的Active Directory数据库内会存储AD DS域内的所有对象与属性。远程分公司内的应用程序要读取Active Directory数据库内的对象时，可以通过RODC来迅速地取得。

不过因为RODC并不存储用户账户的密码，因此它在验证用户名与密码时，仍需将它们送到总公司的可写域控制器来验证。

由于RODC的Active Directory数据库是只读的，因此远地分公司的应用程序要更改Active Directory数据库的对象或用户要更改密码的话，这些更改要求都会被转发到总公司的可写域控制器来处理，总公司的可写域控制器再通过Active Directory数据库的复制程序将这些变动复制

Download at http://www.pin5i.com/

到RODC。

2. 单向复制（Unidirectional Replication）

总公司的可写域控制器的Active Directory数据库有变动时，这些变动数据会被复制到RODC。然而因为用户或应用程序无法直接修改RODC的Active Directory数据库，因此总公司的可写域控制器不会向RODC索取变动数据，因而可以降低网络的负担。

除此之外，可写域控制器通过DFS分布式文件系统将SYSVOL文件夹（用来存储与组策略有关等设置）复制给RODC时，也是采用单向复制。

3. 认证缓存（Credential Caching）

RODC在验证用户账户的密码时，仍然需将它们发到总公司的可写域控制器来验证，如果希望加快验证速度的话，可以将用户的密码存储到RODC的认证缓存区。

需要通过**密码复制策略**（Password Replication Policy）来设置可以被RODC缓存的账户。建议不要缓存太多的账户，因为分公司的安全措施比较差，若RODC被入侵的话，则存储在缓存区内的认证信息可能会外泄。

4. 系统管理员角色隔离（Administrator Role Separation）

可以通过**系统管理员角色隔离**功能来将任何一位域用户指派为RODC的本地系统管理员，此用户可以在RODC这台域控制器登录，然后执行管理工作，例如更新驱动程序等，但是他却无法登录其他域控制器，也无法执行其他的域管理工作。**系统管理员角色隔离**功能可以将RODC的管理工作分配给用户，但却不会危害到域安全。

5. 只读域名系统（Read-Only Domain Name System）

可以在RODC上架设DNS服务器，RODC会复制DNS服务器的所有应用程序目录分区，包含ForestDNSZones与 DomainDNSZones。客户端可以向此台扮演RODC角色的DNS服务器提出DNS查询请求。

不过RODC上的DNS服务器并不支持客户端直接动态更新，因此当客户端要更新记录时，此DNS服务器会将其转发到其他DNS服务器，让客户端转向此DNS服务器更新，而RODC上的DNS服务器也会自动从这台DNS服务器来复制这条更新的数据。

1-2-2 可重新启动的AD DS（Restartable AD DS）

在旧版的Windows Server 2003域控制器内，若要进行Active Directory数据库维护工作的话

Download at http://www.pin5i.com/

（例如数据库脱机重整），就必须重新启动计算机，然后进入**目录服务还原模式**（Directory Service Restore Mode）来执行维护工作。

如果这台域控制器也同时提供其他网络服务的话，例如它同时也是DHCP服务器，则重新启动计算机将造成这些服务的暂时中断。

除了进入**目录服务还原模式**之外，Windows Server 2008 R2（与Windows Server 2008）域控制器还提供新的**可重新启动的AD DS**功能，也就是说若要执行Active Directory数据库维护工作的话，只需要将AD DS服务停止即可，不需要重新启动计算机来进入**目录服务还原模式**，如此不但可以让Active Directory数据库的维护工作更容易、更快地完成，而且其他服务也不会被中断。完成维护工作后再重新启动AD DS服务即可。

在AD DS服务停止的情况下，只要还有其他域控制器在线的话，仍然可以在这台AD DS服务停止的域控制器上利用域用户账户来登录。若没有其他域控制器在线的话，则在这台AD DS服务已停止的域控制器上，默认只能够利用**目录服务还原模式**的系统管理员账户来进入**目录服务还原模式**。

1-2-3 Active Directory回收站

在旧版Windows系统中，系统管理员若不小心将Active Directory对象删除的话，将造成不少困扰，例如误删组织单位的话，则其内所有对象都会不显示，此时虽然系统管理员可以进入**目录还原模式**来救回被误删的对象，不过比较耗费时间，而且在进入**目录还原模式**这段时间内，域控制器会暂时停止对客户端提供服务，因而在Windows Server 2008 R2中新增加**Active Directory回收站**（Active Directory Recycle Bin），它让系统管理员不需要进入**目录还原模式**，就可以快速找回被删除的对象。

1-3 域功能级别与林功能级别

Active Directory域服务将域与林划分为不同的功能级别，每个级别各有不同的特色与限制。

1-3-1 域功能级别（Domain Functionality Level）

Active Directory域服务（AD DS）的**域功能级别**设置只会影响到该域本身，不会影响到其他域。**域功能级别**分为以下4种模式。

- **Windows 2000本机模式**：域内的域控制器可以是Windows 2000 Server、Windows Server

Download at http://www.pin5i.com/

2003、Windows Server 2003 R2、Windows Server 2008与Windows Server 2008 R2。

- **Windows Server 2003**：域内的域控制器可以是Windows Server 2003、Windows Server 2003 R2、Windows Server 2008与Windows Server 2008 R2。
- **Windows Server 2008**：域内的域控制器可以是Windows Server 2008与Windows Server 2008 R2。
- **Windows Server 2008 R2**：域内的域控制器只能够是Windows Server 2008 R2。

不同的**域功能级别**各有不同的特色，如表1-2所示（仅列出部分），其中的**Windows Server 2008 R2**拥有AD DS的所有功能。可以提升域功能级别，例如将**Windows Server 2003**提升到**Windows Server 2008**，不过一旦提升后就不可以再降级（但也有例外情况，详细内容请参考第2-4节）。

表 1-2

域功能特色	Windows 2000本机模式	Windows Server 2003	Windows Server 2008	Windows Server 2008 R2
验证机制保证	不支持	不支持	不支持	支持（见提示1）
前次交互式登录信息	不支持	不支持	支持（见提示2）	支持
高级加密服务	不支持	不支持	支持（见提示3）	支持
更改域控制器的计算机名称	不支持	支持	支持	支持
通用组	安全组：支持 发布组：支持	支持：同左	支持：同左	支持：同左
Group Nesting	支持	支持	支持	支持
SID历史数据	支持：使用户账户在不同域之间转移时，仍然拥有其原来的权限与权利	支持：同左	支持：同左	支持：同左

提示

1. 让应用程序可以根据令牌（Token）内的用户登录类型（智能卡或用户名称/密码）来验证用户。
2. 会显示用户上次成功/失败登录的时间、登录失败的次数等信息。
3. 高级加密服务（Advanced Encryption Services，AES 128与AES 256）适用于Kerberos验证协议。

1-3-2 林功能级别（Forest Functionality Level）

Active Directory域服务（AD DS）的**林功能级别**设置，会影响到该林内的所有域。**林功能级别**分为以下4种模式。

Download at http://www.pin5i.com/

- **Windows 2000**：林内的域控制器可以是Windows 2000 Server、Windows Server 2003、Windows Server 2003 R2、Windows Server 2008与Windows Server 2008 R2。
- **Windows Server 2003**：林内的域控制器可以是Windows Server 2003、Windows Server 2003 R2、Windows Server 2008与Windows Server 2008 R2。
- **Windows Server 2008**：林内的域控制器可以是Windows Server 2008与Windows Server 2008 R2。
- **Windows Server 2008 R2**：林内的所有域控制器都必须是Windows Server 2008 R2。

不同的林功能级别具有不同的特色，如表1-3所示（仅列出部分）。可以提升林功能级别，例如将**Windows Server 2003**提升到**Windows Server 2008**，不过一旦提升后就不可以再降级（但也有例外情况，详细内容请参考第2-4节）。



提示

Windows Server 2008林功能级别并未拥有比Windows Server 2003林功能级别更多的功能，不过在Windows Server 2008林功能级别之内所添加的域，其域功能级别会被设置为Windows Server 2008。

表1-3

林功能特色	Windows 2000	Windows Server 2003与 Windows Server 2008	Windows Server 2008 R2
Active Directory回收站	不支持	不支持	支持
全局编录的复制优化	不支持	支持	支持
不同林间的信任关系	不支持	支持	支持
域名更改	不支持	支持	支持
只读域控制器（RODC）	不支持	支持	支持
Linked-value Replication	不支持	支持：可大幅提升复制的效率	支持：同左

1-4 Active Directory轻型目录服务（AD LDS）

从前面的介绍中已经知道Active Directory数据库是一个符合LDAP规范的目录服务数据库，它除了可以用来存储AD DS域内的对象（例如用户账户、计算机账户等）之外，也提供**应用程序目录分区**，以便让支持目录访问的应用程序（Directory-Enabled Application）可以将该程序的相关数据存储到Active Directory数据库内。

然而前面所介绍的环境中，必须创建AD DS域与域控制器，才能够使用AD DS目录服务与数据库。为了让没有域的环境也能够拥有跟AD DS一样的目录服务，以便让支持目录访问的应用程序可以由一个目录数据库来存储数据，因此Windows Server 2008 R2（与Windows Server

Download at http://www.pin5i.com/

2008）提供了一个称为**Active Directory轻型目录服务**（Active Directory Lightweight Directory Services，**AD LDS**）的功能。



提示

此服务在Windows Server 2003内被称为Active Directory Application Mode（ADAM）。

AD LDS可以在计算机内创建多个目录服务的环境，每一个环境被称为是一个**AD LDS实例**（Instance），每一个**AD LDS实例**分别拥有独立的目录设置与架构（Schema），也分别拥有专属的目录数据库，以供支持目录访问的应用程序来使用。



提示

若要在Windows Server 2008 R2内安装AD LDS角色的话，请【单击左下角的**服务器管理器**图标➲单击**角色**选项➲单击**添加角色**选项➲…➲选择 **Active Directory轻型目录服务**】。然后就可以通过以下途径来创建**AD LDS实例**：【开始➲管理工具➲Active Directory轻型目录服务安装向导】，也可以通过【开始➲管理工具➲ADSI编辑器】来管理**AD LDS实例**内的目录设置、架构、对象等。

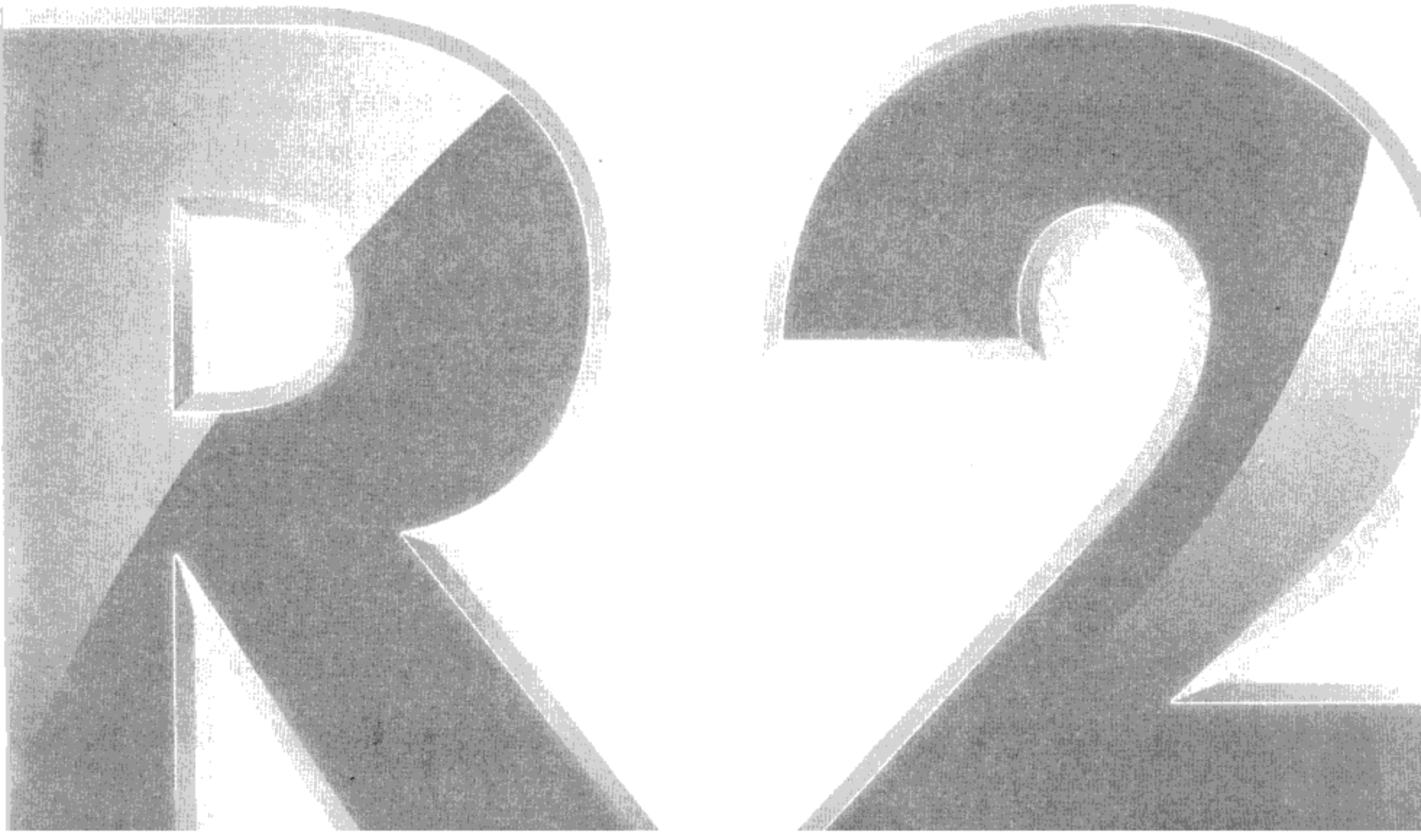
Download at http://www.pin5i.com/

第2章

建立 AD DS 域

创建AD DS（Active Directory Domain Services）域后，就可以通过AD DS的强大功能来更容易、更有效率地管理网络。

- 创建AD DS域前的准备工作
- 创建AD DS域
- 确认AD DS域是否正常
- 提高域与林功能级别
- 添加额外域控制器与RODC
- RODC阶段式安装
- 将Windows计算机加入或脱离域
- 在域成员计算机内安装AD DS管理工具
- 删除域控制器和域
- 域升级与在现有域环境中安装域控制器



Download at http://www.pin5i.com/

2-1 创建AD DS域前的准备工作

创建AD DS域的方法是先安装一台服务器，然后再将其升级（Promote）为域控制器。在创建AD DS域前，请先确定以下的准备工作是否已经完成：

- 选择适当的DNS域名。
- 准备好一台用来支持AD DS的DNS服务器。
- 选择Active Directory数据库的存储位置。

2-1-1 选择适当的DNS域名

由于AD DS域名是采用DNS的架构与命名方式，因此必须先为AD DS域取一个符合DNS格式的域名，例如sayms.com。虽然域名可以在域创建完成后更改，不过步骤繁琐，因此请事先谨慎命名。

2-1-2 准备好一台用来支持AD DS的DNS服务器

由于在AD DS域中，域控制器会将自己所扮演的角色注册到DNS服务器内，以便让其他计算机通过DNS服务器来找到这台域控制器，因此必须要有一台DNS服务器，而且它必须支持Service Location Resource Record（SRV RR），同时最好支持**动态更新**（Dynamic Update）、Incremental Zone Transfer与Fast Zone Transfer等功能。

- **Service Location Resource Record（SRV RR）**：域控制器需要将其所扮演的角色注册到DNS服务器的SRV日志内，因此DNS服务器必须支持SRV日志。Windows 2000 Server（含）以后的Windows服务器与BIND Version 8.1.2（或新版本）DNS服务器都支持此功能。
- **动态更新**：虽然并不一定需要具备动态更新功能，但是强烈建议安装此功能，否则域控制器无法自动将自己注册到DNS服务器的SRV日志内，必须由系统管理员手动将数据输入到DNS服务器，如此势必增加管理负担。Windows 2000 Server（含）以后的Windows服务器与BIND Version 8.1.2（或新版本）DNS服务器都支持此功能。
- **Incremental Zone Transfer（IXFR）**：它让此DNS服务器与其他DNS服务器之间在执行**区域转发**（Zone Transfer）时，只会复制最新修改过的日志，而不是复制区域内的所有日志。它可提高复制效率、减少网络负担。Windows 2000 Server（含）以后的Windows服务器与BIND Version 8.2.1（或新版本）DNS服务器都支持此功能。
- **Fast Zone Transfer**：它让DNS服务器可以使用**快速传送格式**（Fast Transfer Format）将区域内的日志复制给其他DNS服务器。**快速传送格式**具备数据压缩与每一次传送信

Download at http://www.pin5i.com/

息内可包含多条日志的功能。Windows 2000 Server(含)以后的Windows服务器与BIND Version 4.9.7（或新版本）DNS服务器都支持此功能。

Windows DNS服务器默认已启用**快速传送**功能，但有些厂商的DNS服务器（例如旧版的BIND）并不支持此功能，故若要通过**区域转发**将日志复制给此DNS服务器的话，必须禁用此功能。Windows Server 2008 R2 DNS服务器禁用**快速传送**的方法为：【开始➲管理工具➲DNS➲对着DNS服务器右击➲属性➲如图 2-1所示选择**高级**标签下的**BIND辅助区域**复选框】。

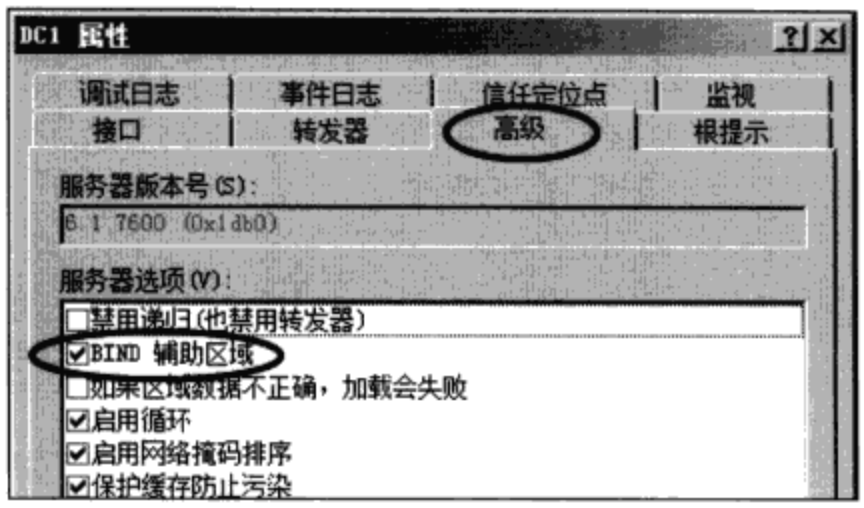


图 2-1

可以采用以下两种方式之一来架设DNS服务器：

- 在将服务器升级为域控制器时，让系统自动在这台服务器上安装 DNS服务器角色。系统还会自动在此DNS服务器内创建一个支持AD DS域的区域，例如AD DS域名为sayms.com，则其所自动创建的区域名为sayms.com，并自动启用**安全**动态更新。请先在这台即将变成域控制器与DNS服务器的计算机上，清除其**首选DNS服务器**的IP地址或输入自己的IP地址（如图 2-2所示），无论选择哪一种配置方式，升级时系统都可以自动安装DNS服务器角色。

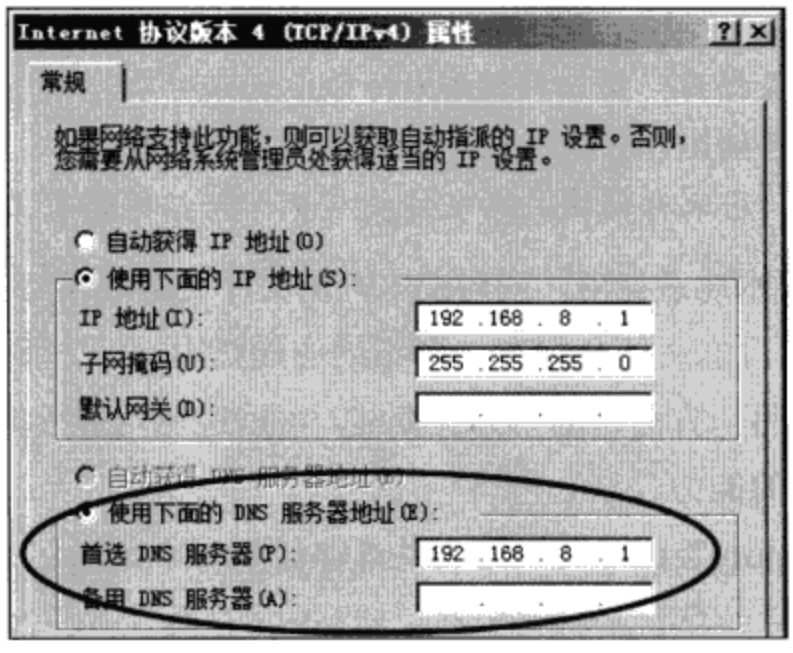


图 2-2

Download at http://www.pin5i.com/

- 使用现有的DNS服务器或另外安装一台DNS服务器，然后在这台DNS服务器内创建一个用来支持AD DS域的区域，例如AD DS域名为sayms.com，则请创建一个名称为sayms.com的区域，并启用**动态更新**功能，如图 2-3所示为在一台Windows Server 2008 R2 DNS服务器所看到的界面，可以选择**安全**或**非安全**动态更新。注意先在即将变成域控制器的计算机上，将其**首选 DNS服务器**的IP地址，指定到这台DNS服务器。

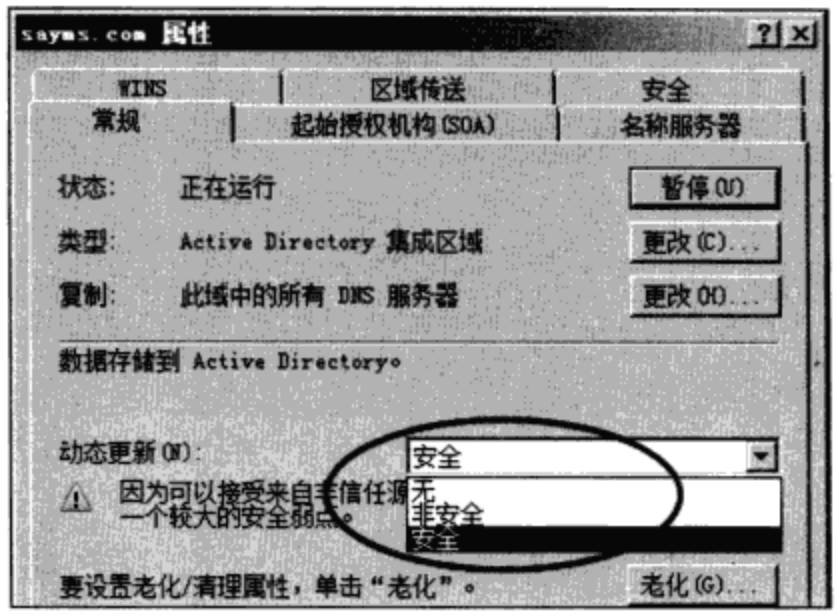


图2-3

提示

请通过【单击左下角的**服务器管理器**图标➲单击**角色**对话框右边的**添加角色**➲…➲选择**DNS服务器**➲…】的方法来安装DNS服务器，然后通过【开始➲管理工具➲DNS➲对着**正向查找区域**右击➲新建区域】的方法来新建区域。

2-1-3 选择Active Directory数据库的存储位置

域控制器需要使用磁盘空间来存储以下三个与Active Directory有关的数据。

- **Active Directory数据库**：用来存储Active Directory对象。
- **日志文件**：用来存储Active Directory数据库的变动日志。
- **SYSVOL文件夹**：用来存储域共享文件夹（例如与组策略有关的文件）。

它们都必须被存储到本地磁盘内，同时SYSVOL文件夹必须存储在NTFS磁盘内。建议将Active Directory数据库与日志文件分别存储到不同的硬盘内，一方面是因为两块硬盘独立运行，可以提高运行效率，另一方面是因为分开存储，可以避免两份数据同时出问题，以提高恢复Active Directory数据库的能力。

也应该将Active Directory数据库与日志文件都存储到NTFS磁盘，以便通过NTFS权限来增加这些文件的安全性，而系统默认是将它们都存储到Windows Server 2008 R2的安装磁盘内（它是NTFS磁盘）。

如果要将Active Directory数据库、日志文件或SYSVOL文件夹存储到另外一个NTFS磁盘

Download at http://www.pin5i.com/

内，但是计算机内目前并没有其他NTFS磁盘的话，此时可以采用以下方法来创建NTFS磁盘：

- 若磁盘内还有未划分的可用空间，此时可以使用【开始➲管理工具➲计算机管理➲存储➲磁盘管理➲对着未分配的可用空间右击】的方法来创建一个新的NTFS磁盘。
- 使用**CONVERT**命令来将现有的FAT或FAT32磁盘转换为NTFS磁盘，例如要将D磁盘转换成NTFS磁盘的话：【开始➲命令提示符】或单击左下方任务栏的**Windows PowerShell**图标，然后执行以下命令：

```
CONVERT D:  /FS:NTFS
```

- 如果该磁盘当前有任何一个文件正在使用中的话，则系统无法立即执行转换的工作，此时可以选择让系统在下次重新启动时再自动转换。

注意

Active Directory数据库与日志文件的存储位置可以事后使用**ntdsutil**命令来更改（见第11章）。但若要更改SYSVOL的存储地点的话，建议采用以下方法：删除域控制器的AD DS，然后在重新安装AD DS时指定新的存储位置。

2-2 创建AD DS域

以下使用图 2-4来说明如何创建第1个林中的第1个域（根域）：先安装一台Windows Server 2008 R2服务器，然后将其升级为域控制器并创建域。架设此域的第2台域控制器（Windows Server 2008 R2）、一台成员服务器（Windows Server 2008 R2）与一台加入AD DS域的Windows 7计算机。

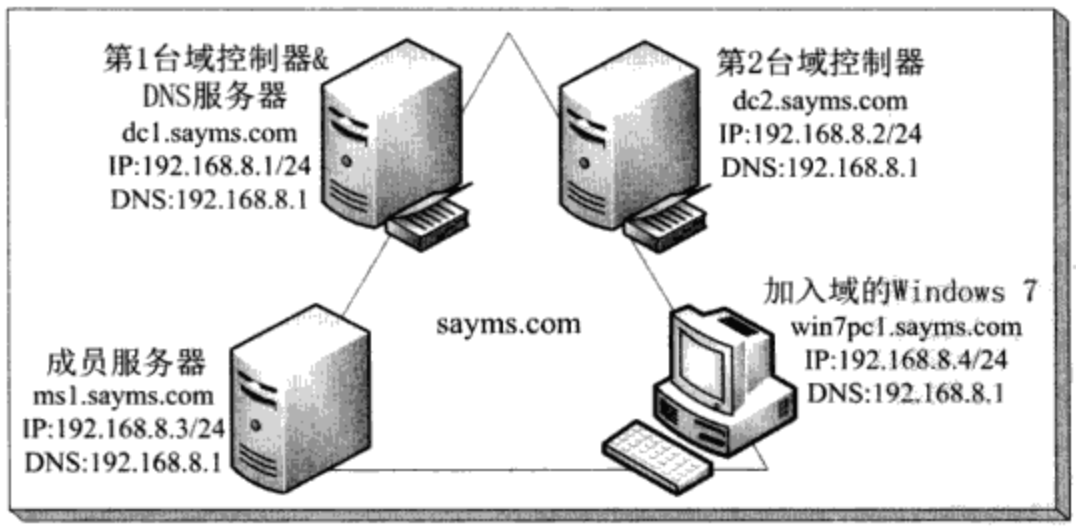


图2-4

提示

建议使用Windows Server 2008 R2 Hyper-V所提供的虚拟机来搭建图中的网络环境。

Download at http://www.pin5i.com/

要将图 2-4左上角的服务器升级为域控制器，也就是在其内安装**Active Directory域服务**（AD DS），而当您在执行这个升级工作时，因为它是第一台域控制器，因此这个升级动作会同时完成以下操作：

- 创建第一个新林。
- 创建此新林中的第一个域树。
- 创建此新域树中的第一个域。
- 创建此新域中的第一台域控制器。

换句话说，在您创建图 2-4中第一台域控制器dc1.sayms.com时，它就会同时创建此域控制器所隶属的域sayms.com，同时也会创建域sayms.com所隶属的域树，而域sayms.com也是此域树的根域。由于这是第一个域树，因此它同时会创建一个新林，林名称就是第一个域树的根域的域名，也就是sayms.com。域sayms.com就是整个林的**林根域**（Forest Root Domain）。

我们将分别使用以下三种方法来安装域控制器：

- 使用Windows窗口来安装第一台域控制器。
- 使用应答文件来安装第一台域控制器。
- 使用命令行来安装第一台域控制器。

2-2-1 使用Windows窗口来安装第一台域控制器

我们将通过添加服务器角色的方式来将图 2-4中左上角的服务器dc1.sayms.com升级为网络中的第一台域控制器，操作步骤如下。

STEP 1 请先在图 2-4中左上角的服务器dc1.sayms.com上安装Windows Server 2008 R2，将其计算机名称设置为dc1，IPv4地址等依照图中所示来配置（图中采用TCP/IPv4）。注意将计算机名称设置为dc1即可，等升级为域控制器后，它会自动被改为dc1.sayms.com。

STEP 2 选用以下两种方式之一来安装Active Directory域服务。

- 单击左下角的**服务器管理器**图标：此时请转至**STEP 3**。
- 通过【开始➲运行➲输入**dcpromo**后单击**确定**按钮】的方法：此时它会自动执行**STEP 3** ~ **STEP 9**安装AD DS的步骤，故请直接跳到**STEP 10**。

STEP 3 单击左边的**角色**➲单击右边的**添加角色**。

STEP 4 出现**开始之前**界面时直接单击**下一步**按钮。

STEP 5 在图 2-5中选中**Active Directory域服务**复选框，在弹出的界面中单击**添加必需的功能**选项，单击**下一步**按钮。

Download at http://www.pin5i.com/



图 2-5

STEP 6 在**Active Directory域服务**界面中单击下一步按钮。

STEP 7 在**确认**界面中单击安装按钮。

STEP 8 图 2-6为完成安装后的界面，请直接单击关闭按钮。从图中可知还必须运行**Active Directory域服务安装向导（dcpromo.exe）**后，这台服务器才会成为功能完整的域控制器。

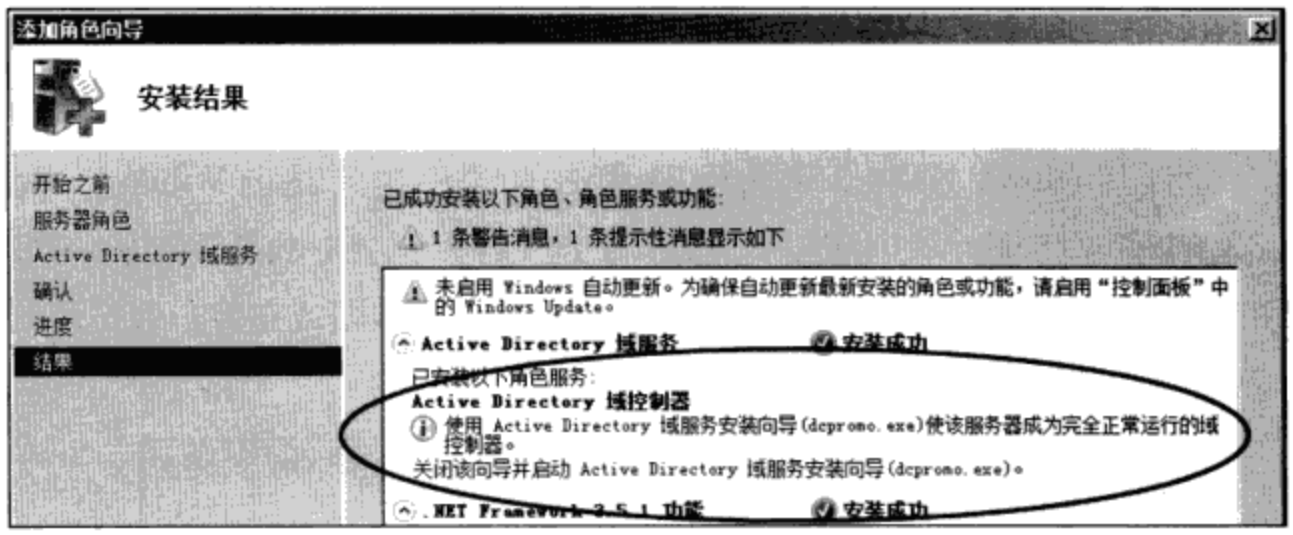


图 2-6

STEP 9 在图 2-7中**【单击角色下的Active Directory域服务➲单击运行Active Directory域服务安装向导（dcpromo.exe）】**。

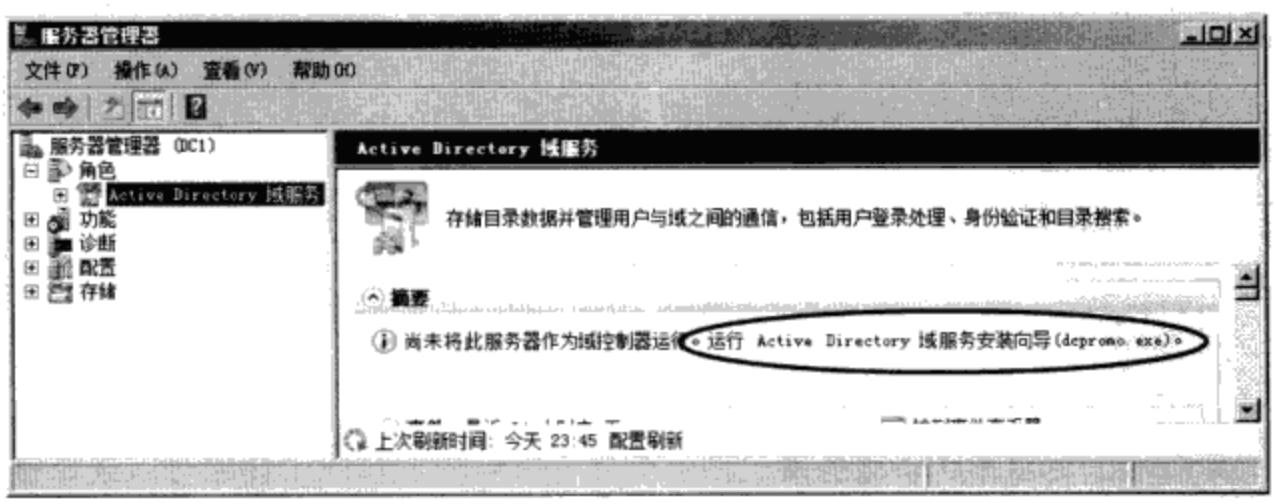


图 2-7

Download at http://www.pin5i.com/

STEP 10 如图 2-8所示，选择**使用高级模式安装**复选框后单击下一步按钮。

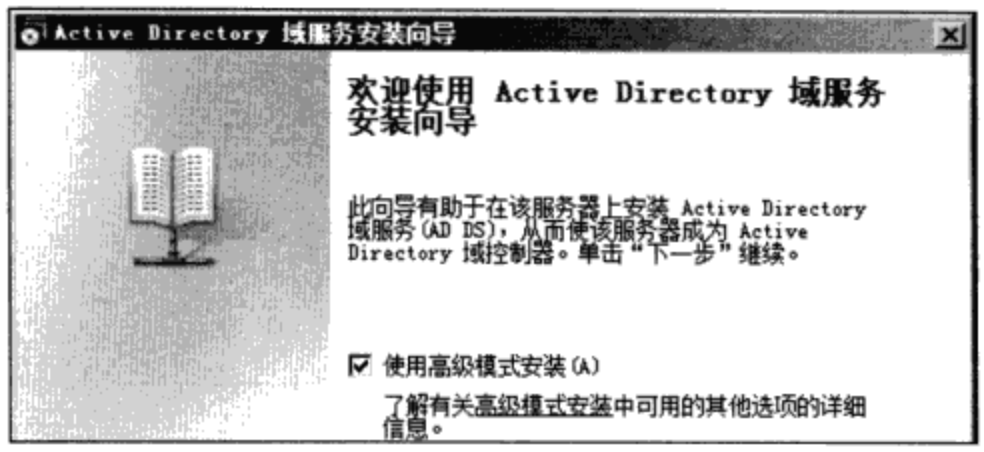


图 2-8

提示

也可以不选择**使用高级模式安装**复选框，此时有一些设置会自动采用默认值，因此安装过程中与这些设置有关的界面不会出现。

STEP 11 出现如图2-9所示的**操作系统兼容性**界面时单击下一步按钮。由于AD DS域的**允许与Windows NT 4.0兼容的加密算法**原则默认并不允许客户端采用安全性较差的旧式密码算法来与Windows Server 2008 R2/Windows Server 2008域控制器通信，因此它会让Windows NT 4.0等采用旧算法的客户端无法与Windows Server 2008 R2/Windows Server 2008域控制器连接。这个原则也会影响到SAMBA等非Microsoft的SMB客户端与NAS存储设备。您可以通过启用此策略或在客户端安装更新程序的方式来解决此问题。



图 2-9

提示

若此服务器未指定**首选DNS服务器**的话，则接下来会先显示一个让您可以选择安装DNS服务器的界面。

Download at http://www.pin5i.com/

STEP 12 如图 2-10所示，选择**在新林中新建域**单选按钮后单击 下一步 按钮。

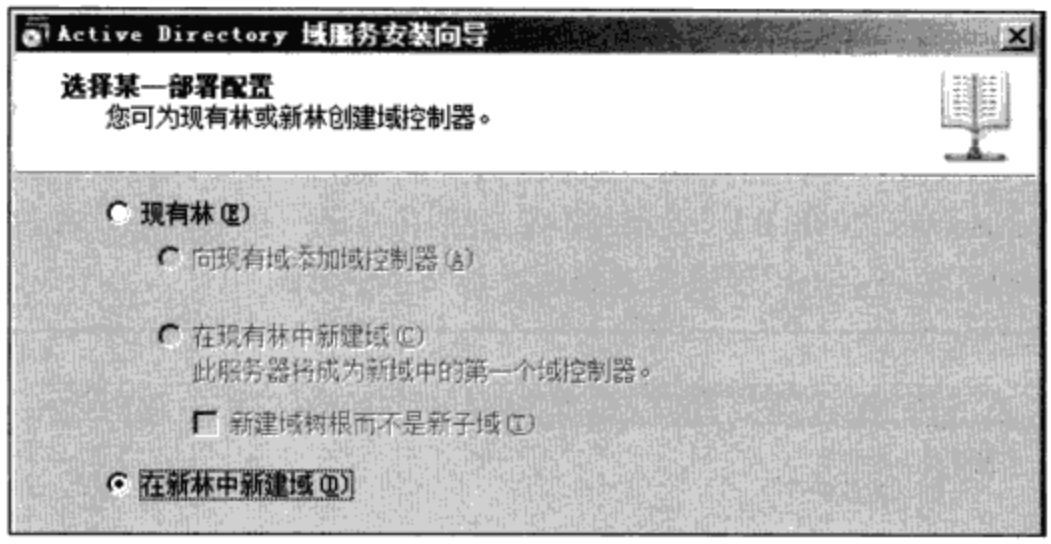


图2-10

STEP 13 在图 2-11中输入域名sayms.com后单击 下一步 按钮。安装向导会检查此域名是否已在网络中被占用，若是的话，安装程序会要求您重新设置一个新的域名。

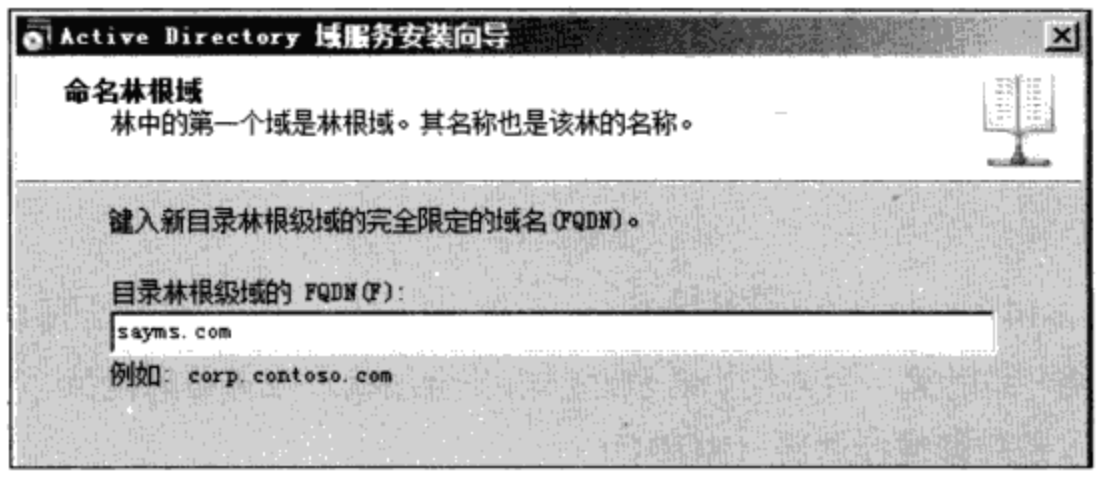


图2-11

STEP 14 在图 2-12中安装向导会自动设置一个NetBIOS格式的域名（不分大小写），它让Windows 98、Windows NT等不支持DNS域名的旧系统可以使用NetBIOS域名来访问此域内的资源。默认的NetBIOS域名为DNS域名中第1个句点左边的文字，例如sayms.com中的SAYMS，若此域名在网络中已被占用，则安装向导会自动更换名称。

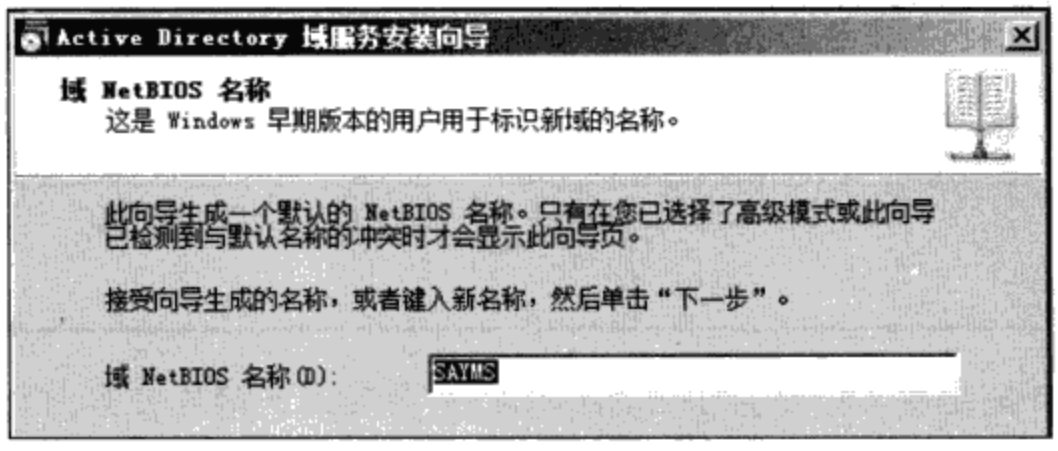


图2-12

Download at http://www.pin5i.com/

STEP 15 在图 2-13中我们选择**Windows Server 2008 R2**林功能级别。

注意

若您将林功能级别设置为**Windows 2000**、**Windows Server 2003**或**Windows Server 2008**的话，则接下来安装向导会另外要求您选择域功能级别，由于此处我们选择的林功能级别为**Windows Server 2008 R2**，此时域功能级别将自动（也只能够）被设置为**Windows Server 2008 R2**，故不会出现要求您选择域功能级别的界面。

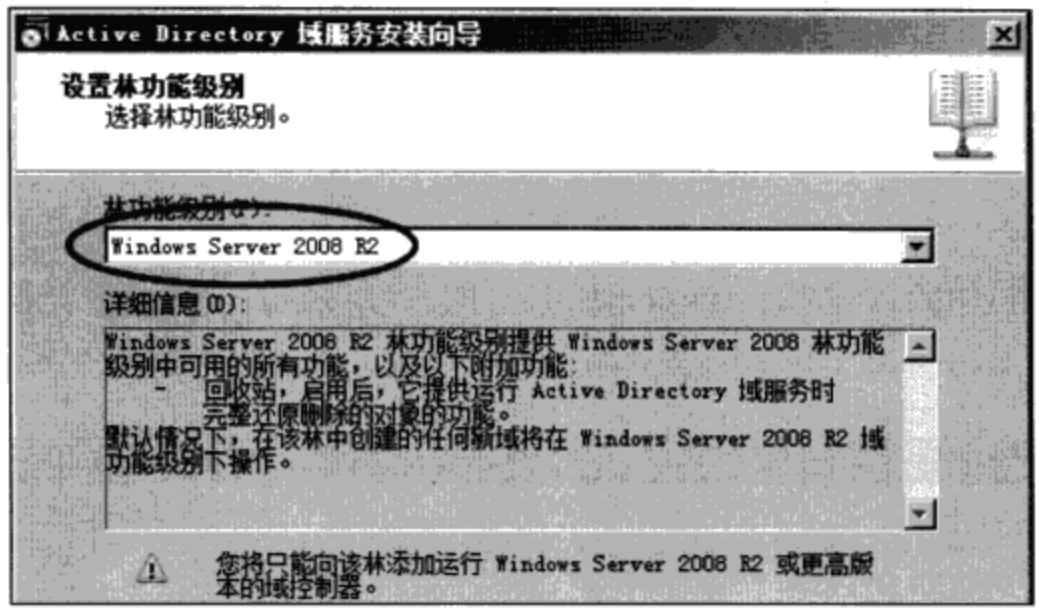


图2-13

STEP 16 在图 2-14中直接单击下一步按钮。由图中可知它将直接在这台服务器上安装DNS服务器，同时第一台域控制器也必须扮演**全局编录服务器**的角色，第一台域控制器不可以是**只读域控制器（RODC）**。

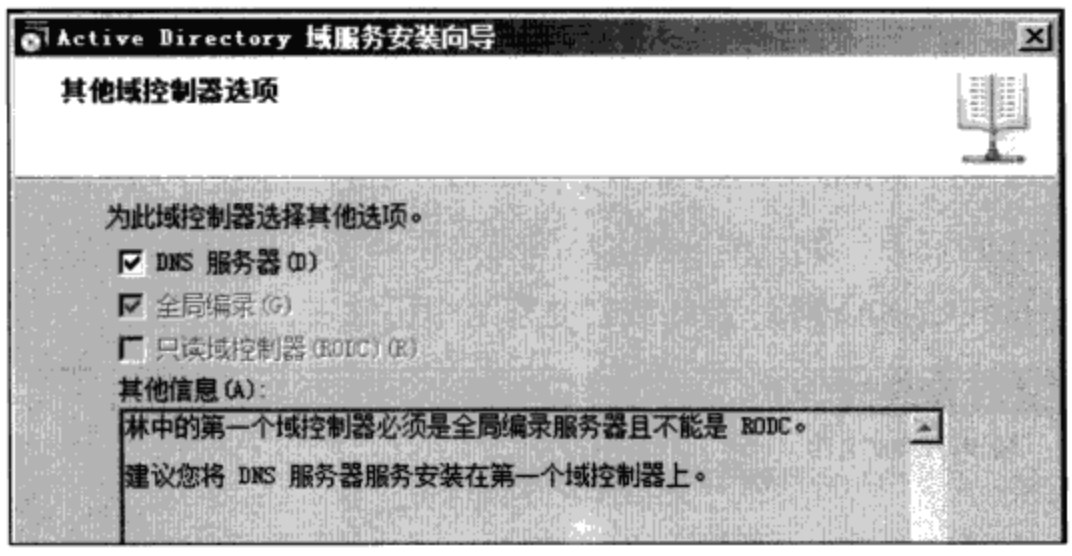


图2-14

提示

若您要使用安装在其他计算机上的DNS服务器的话，请先在其内创建支持此域（sayms.com）的区域，并启用**动态更新**功能。

Download at http://www.pin5i.com/

STEP 17 若出现图 2-15的话，表示安装向导找不到父域，因而无法通过父域来委派，不过由于此sayms.com域为根域，并不需要通过父域来委派，故请直接单击**是（Y）**按钮即可。

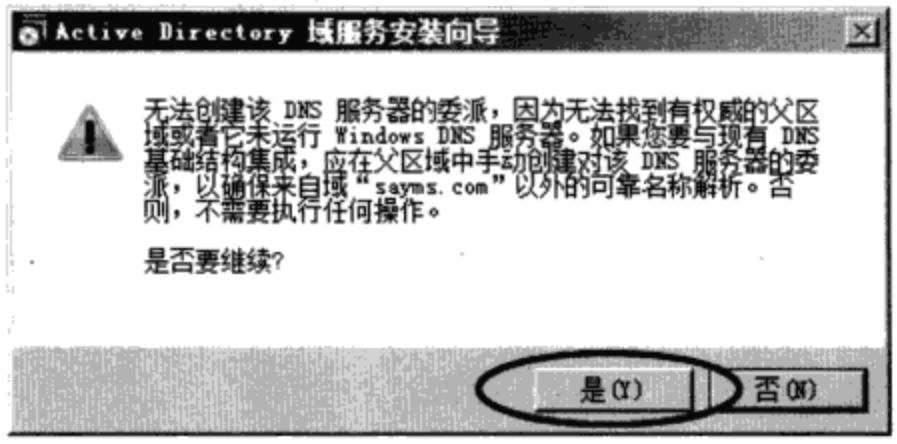


图 2-15

STEP 18 在图 2-16中直接单击**下一步**按钮，其中：

- 数据库文件夹用来存储Active Directory数据库。
- 日志文件文件夹用来存储Active Directory数据库的改动记录，此日志文件可用来恢复Active Directory数据库。
- SYSVOL文件夹用来存储域共享文件（例如与组策略有关的文件），注意它必须位于NTFS 磁盘内。

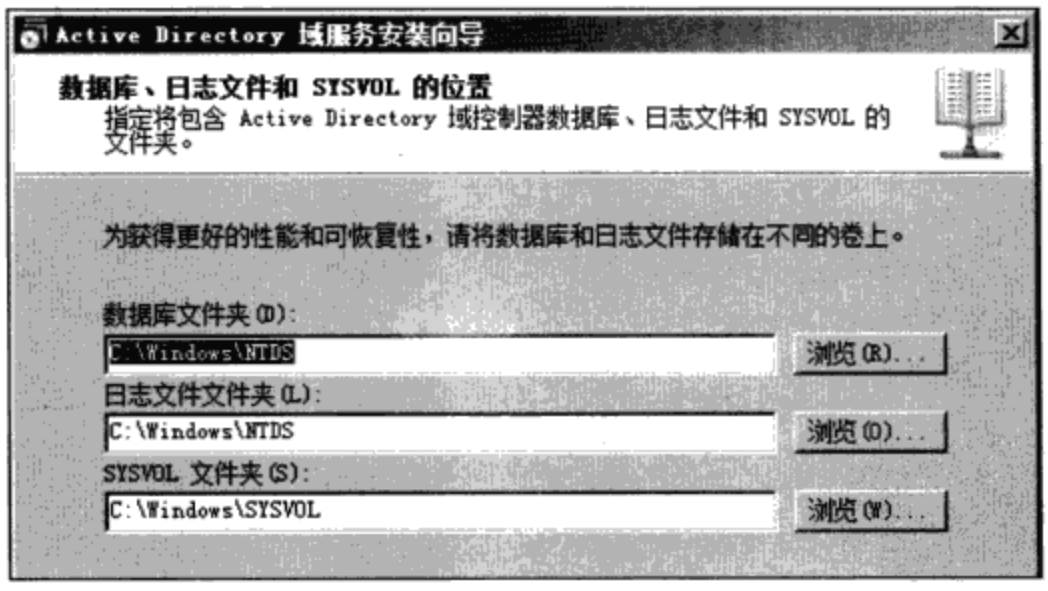


图 2-16

STEP 19 在图 2-17中设置目录服务还原模式的系统管理员密码，完成后单击**下一步**按钮。目录服务还原模式是一个安全模式（Safe Mode），进入此模式可以修复Active Directory数据库。您可以在系统启动时单击**F8**键来选择此模式，不过必须输入此处所设置的密码。

Download at http://www.pin5i.com/

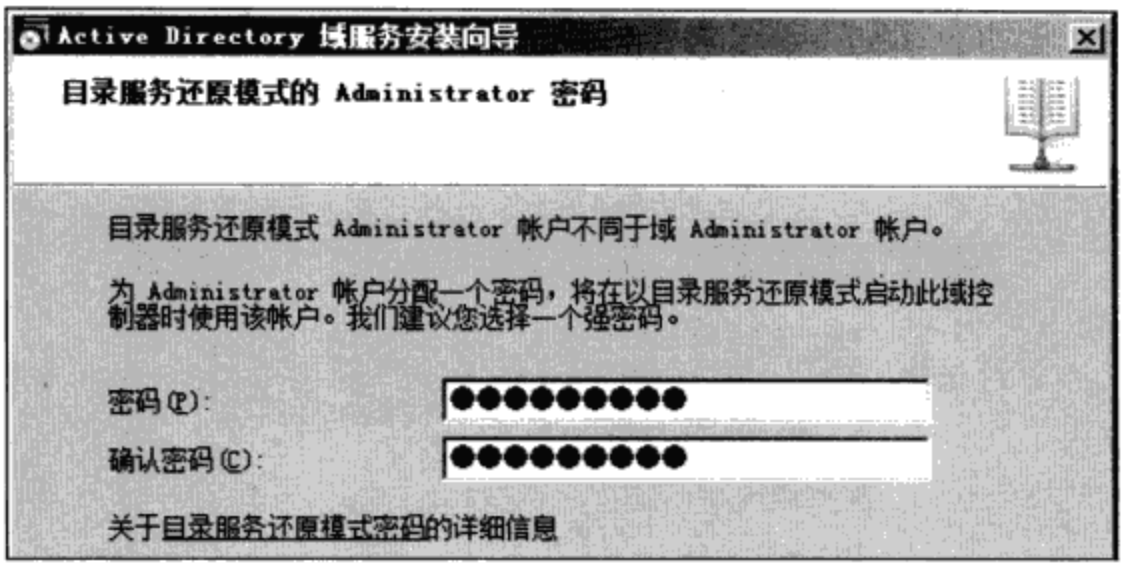


图2-17

注意

用户的密码默认至少需要7个字符，且不可包含用户名称中超过两个以上的连续字符，还有至少要包含A～Z、a～z、0～9、非字母数字（例如!、$、#、%）等4组字符中的3组，例如123saymsSAYMS是有效的密码，而1234567是无效的密码。

STEP 20 在图 2-18的**摘要**界面中直接单击 下一步 按钮。

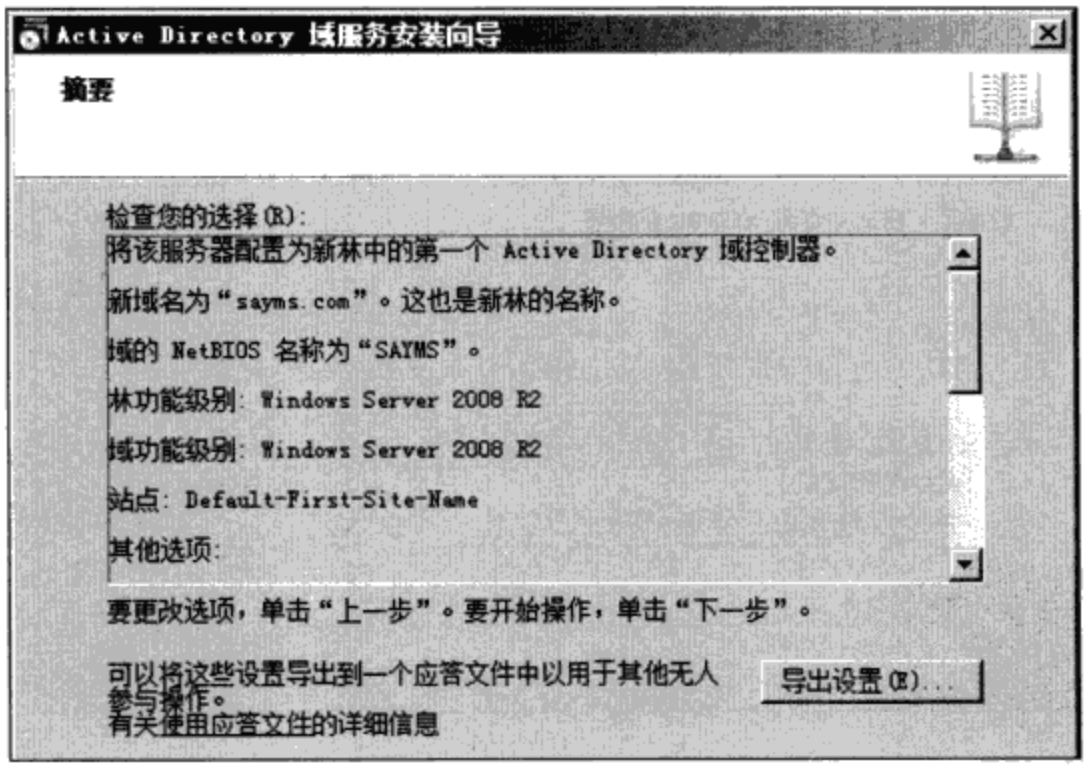


图2-18

提示

您可以单击 导出设置 按钮来将设置存储为**应答文件**（Answer File），它可供dcpromo.exe来安装域控制器时使用，不过安装向导并不会将目录服务还原模式的系统管理员密码存储到此文件。

Download at http://www.pin5i.com/

STEP 21 可在图 2-19中选择**完成后重新启动**复选框或完成后手动重新启动。

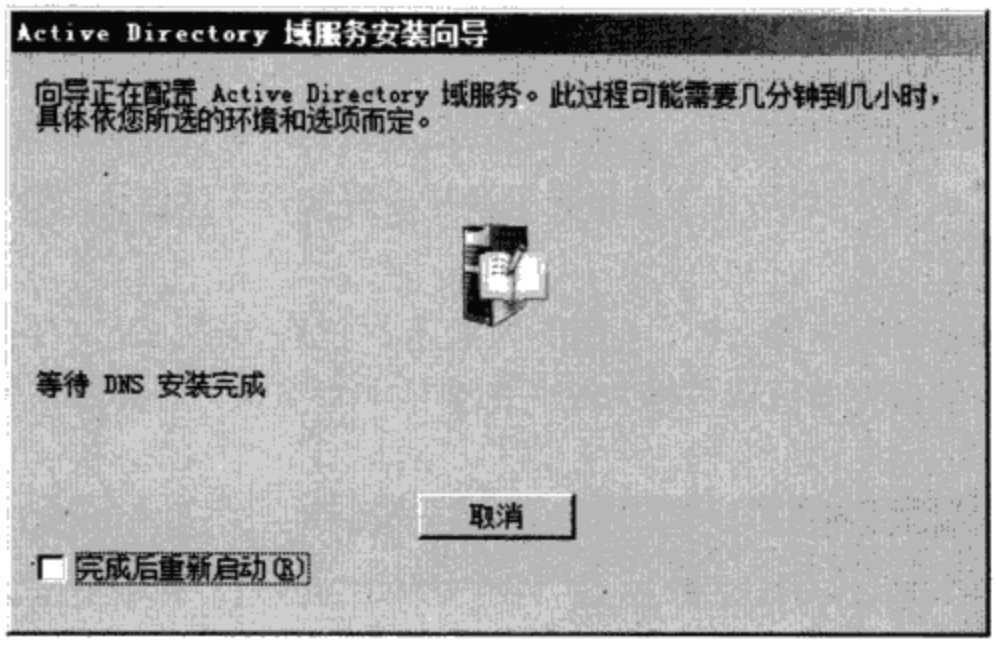


图 2-19

STEP 22 重新启动系统后，请重新登录。

完成域控制器的安装后，原本这台计算机的本机用户账户会被转移到Active Directory数据库。另外由于它本身也是DNS服务器，因此会如图 2-20所示将**首选 DNS服务器**的IP地址改为代表自己的127.0.0.1。

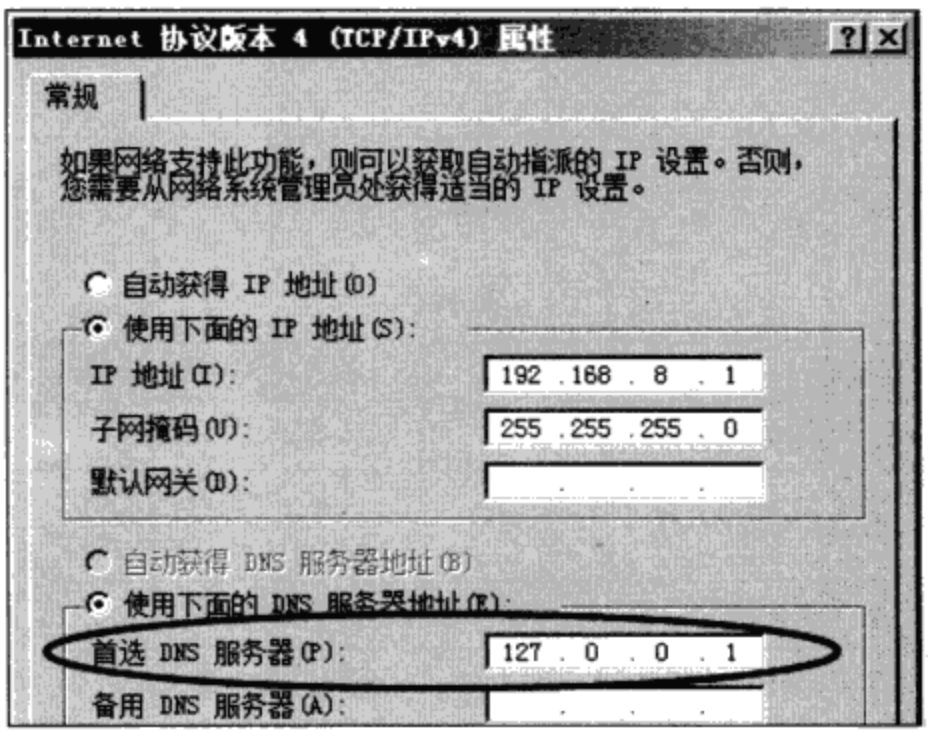


图 2-20

提示

此计算机升级为域控制器后，它会自动在**Windows防火墙**中开放与AD DS相关的端口，以便其他计算机可以与此域控制器通信。

Download at http://www.pin5i.com/

2-2-2 使用应答文件来安装第一台域控制器

您可以将安装第1台域控制器时所必须提供给安装向导的数据，例如域名、林功能级别、Active Directory数据库的存储路径、目录服务还原模式的系统管理员密码等，事先输入到**应答文件**（Answer File）内，然后让安装向导直接从**应答文件**来读取这些数据，不需要再手动输入。

请使用**记事本**来编辑应答文件，如图2-21所示，我们必须在此文件内创建一个名称为**DCInstall**的字段，然后在此区段内输入相关的参数与参数值，各参数的说明如表2-1所示。



图2-21

表 2-1

参数值	说明	参数值可为
InstallDNS	是否要安装DNS服务器	Yes或No
NewDomain	指定新域的种类	Forest（新林的根域）、Tree（新域树的根域）、Child（现有林中的子域）
NewDomainDNSName	设置DNS域名	例如sayms.com
DomainNetBiosName	设置NetBIOS域名	例如SAYMS
ReplicaOrNewDomain	创建新域中的第1台域控制器、现有域中只读域控制器（RODC）或现有域中的其他域控制器	Domain、ReadOnlyReplica或Replica
ForestLevel	林功能级别	0（Windows 2000）、2（Windows Server 2003）、3（Windows Server 2008）、4（Windows Server 2008 R2）

Download at http://www.pin5i.com/

（续表）

参数值	说明	参数值可为
DomainLevel	域功能级别	0（Windows 2000）、2（Windows Server 2003）、3（Windows Server 2008）、4（Windows Server 2008 R2）
CreateDNSDelegation	是否要在上层创建委派域	Yes或No
DatabasePath	设置AD DS数据库的存储路径	例如C:\Windows\NTDS，可以使用环境变量，例如：%systemroot%\NTDS
LogPath	设置AD DS记录文件的存储路径	
SYSVOLPath	设置SYSVOL文件夹的路径	
SafeModeAdminPassword	设置安全模式（目录还原模式）的系统管理员密码	不可以为空白密码
RebootOnCompletion	安装完成后是否重新启动计算机	Yes或No

应答文件创建完成后，请通过以下命令（参考图 2-22）来安装第1台域控制器，假设应答文件的文件名为answer.txt，且此文件位于C:\Test文件夹内：

```
dcpromo /unattend:"C:\Test\answer.txt"
```


提示

dcpromo.exe读取应答文件中SafeModeAdminPassword的密码后，会自动将此密码清除后再保存到应答文件内。



图 2-22

2-2-3 使用命令行来安装第一台域控制器

您可以通过【开始➲命令提示符】或单击左下方的**Windows PowerShell**图标，然后运行如下所示的**dcpromo.exe**命令来安装网络中的第一台域控制器（参考图 2-23）：

```
dcpromo/unattend /InstallDns:yes /newDomain:forest
/replicaOrNewDomain:domain /newDomainDnsName:sayms.com
/DomainNetbiosName:SAYMS /forestLevel:4 /domainLevel:4
```


Download at http://www.pin5i.com/

```
/createDNSDelegation:no /databasePath:"%SystemRoot%\NTDS"
/logPath:"%SystemRoot%\NTDS"/sysvolpath:"%SystemRoot%\SYSVOL"
/safeModeAdminPassword:111aaAA /rebootOnCompletion:yes
```

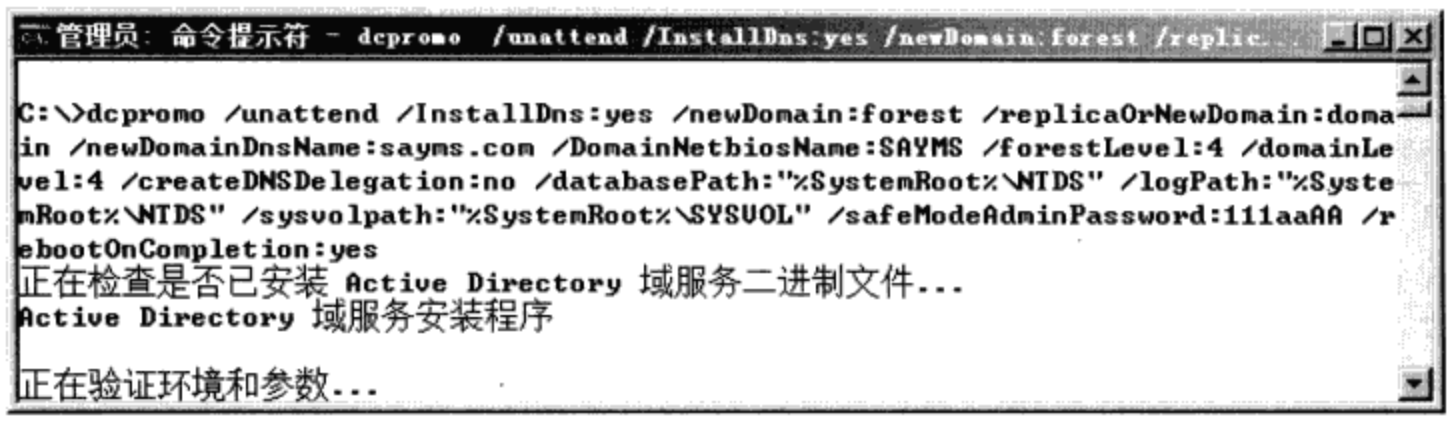


图2-23

提示

您可以使用 **dcpromo /?:Promotion** 命令来查看其详细语法。

2-3 确认AD DS域是否正常

AD DS域创建完成后，下面来检查DNS服务器内的SRV日志、主机日志，还有域控制器内的SYSVOL文件夹、Active Directory数据库文件等是否都已经创建完成。

2-3-1 检查DNS服务器内的日志是否完整

由于域控制器会将它的主机名、IP地址与所扮演的角色等数据注册到DNS服务器内，以便让其他计算机可以通过DNS服务器来找到这台域控制器，因此我们首先来检查DNS服务器内是否已经有域控制器的相关文件。

1. 检查主机日志

首先检查域控制器是否已将其主机名与IP地址注册到DNS服务器内。请到扮演DNS服务器角色的计算机（dc1.sayms.com）上选择【开始➲管理工具➲DNS】，如图2-24所示应该会有一个名为sayms.com的区域，图中的**主机（A）**日志表示域控制器dc1.sayms.com已经正确地将其主机名与IP地址注册到DNS服务器内。

Download at http://www.pin5i.com/

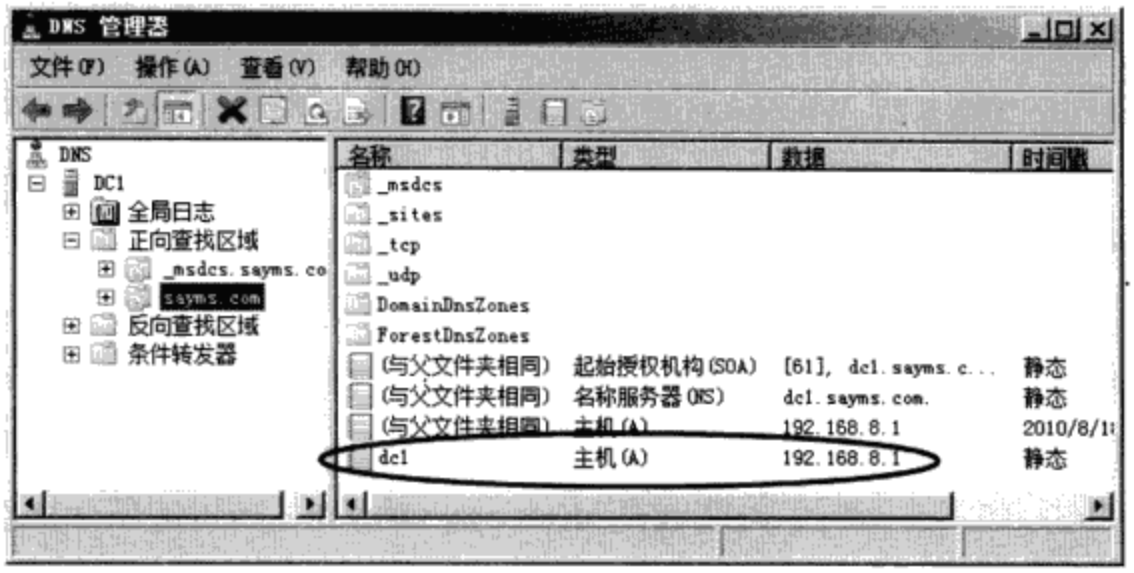


图 2-24

2. 检查 SRV 日志——使用 DNS 控制台

如果域控制器已经正确地将其所扮演的角色注册到DNS服务器的话，则应该还会有如图2-25所示的 _tcp、_udp 等文件夹（域控制器创建完成并重新开机后，可能需要等一会儿才会有这些文件夹出现）。

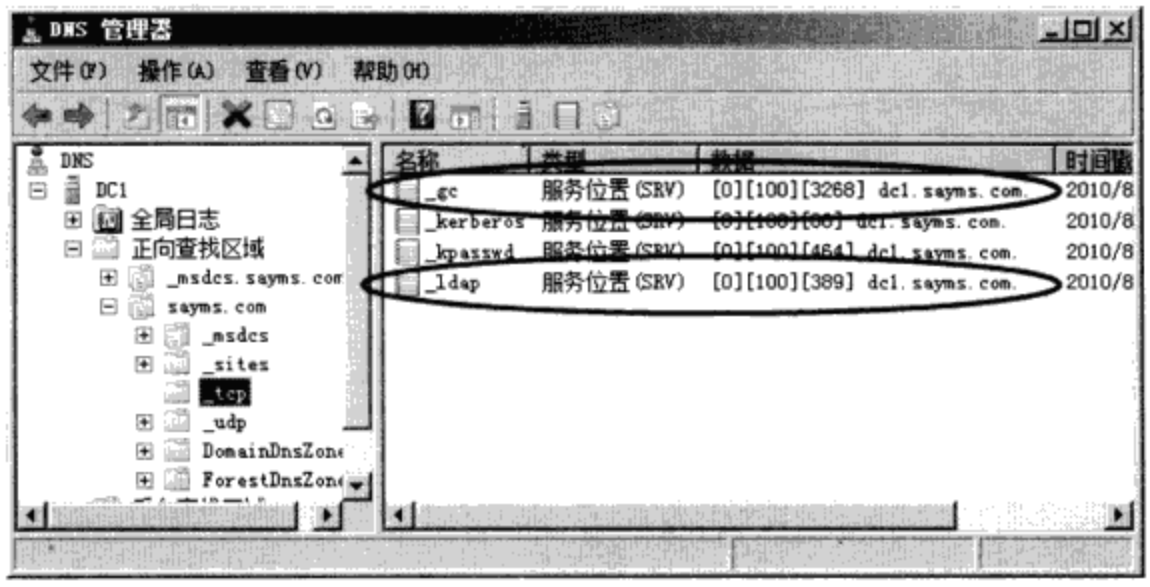


图 2-25

图 2-25中_tcp文件夹右方数据类型为**服务位置（SRV）**的_ldap日志，表示dc1.sayms.com已经成功的注册为域控制器。由图中的_gc日志还可以看出**全局编录服务器**的角色也是由dc1.sayms.com所扮演。

提示

LDAP服务器是用来提供Active Directory数据库访问的服务器，而域控制器就是扮演着LDAP服务器的角色。

DNS区域内有这些数据后，其他要加入域的计算机，就可以通过此区域来得知域控制器为dc1.sayms.com。这些加入域的成员（域控制器、成员服务器、Windows 7、Windows Vista、

Download at http://www.pin5i.com/

Windows XP Professional等）默认也会将其主机与IP地址数据注册到此区域内。

Windows Server 2008 R2、Windows Server 2008、Windows Server 2003 R2、Windows Server 2003、Windows 2000 Server等Windows Server 域控制器不但会将自己所扮演的角色注册到_tcp、_sites等相关的文件夹内，还会另外注册到_msdcs文件夹。

如果DNS服务器是在安装AD DS时顺便安装的，则它除了会自动创建一个用来支持AD DS的区域（sayms.com）外，还会创建一个名称为_msdcs.sayms.com的区域，它是专供Windows Server域控制器来注册的，此时这些域控制器会将其文件注册到_msdcs.sayms.com区域内，而不是_msdcs文件夹。如图 2-26所示为注册在_msdcs.sayms.com区域内的部分日志。

在您创建完成第1个域之后，系统就会自动创建一个名称为Default-First-Site-Name的站点（site），而我们所创建的域控制器默认也是位于此站点内，因此在DNS服务器内也会有这些日志，例如图 2-27中位于此站点内扮演**全局编录服务器**（gc）、**Kerberos服务器**、**LDAP服务器**等三个角色的域控制器都是dc1.sayms.com。

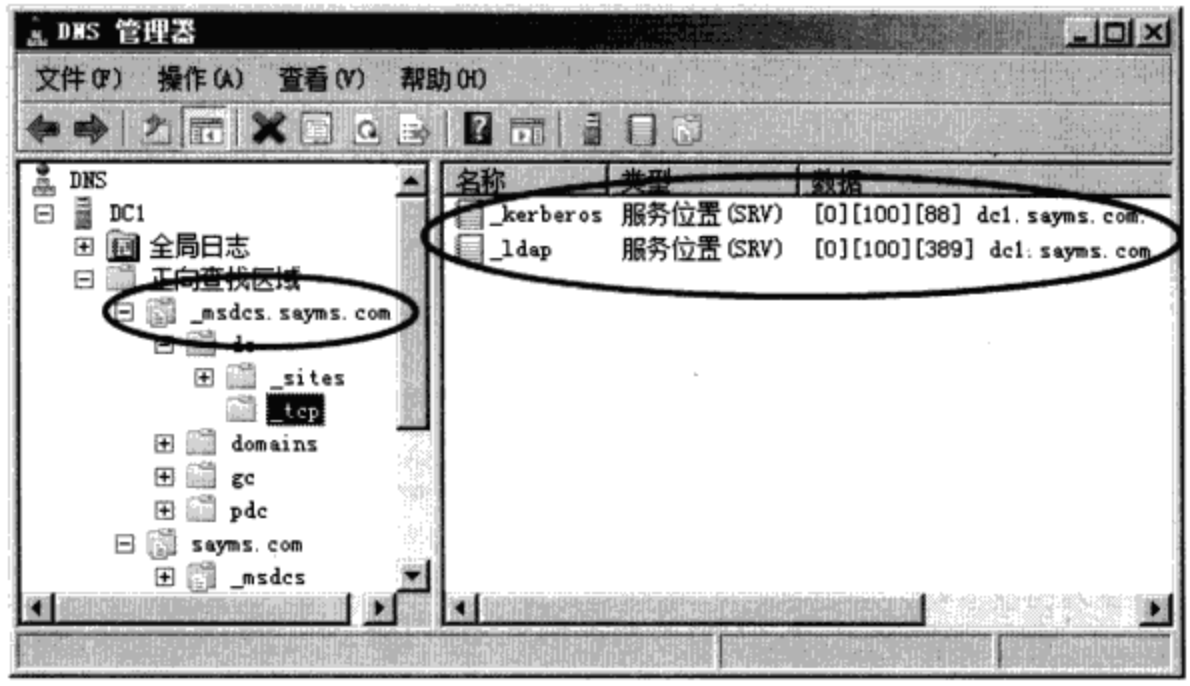


图 2-26

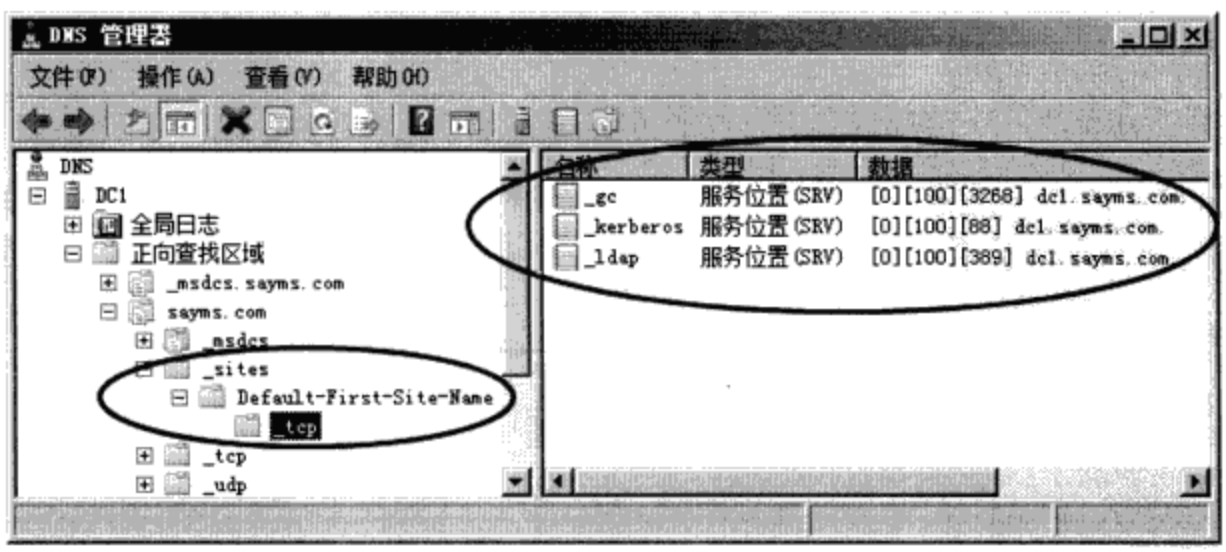


图 2-27

Download at http://www.pin5i.com/

3. 检查 SRV 日志——使用 NSLOOKUP 命令

您也可以使用**NSLOOKUP**命令来检查DNS服务器内的SRV日志，操作步骤如下。

STEP 1 请选择【开始➲命令提示符】（或单击左下角的**Windows PowerShell**图标）。

STEP 2 运行**nslookup**命令。

> **提示**
>
> 若出现错误信息：DNS request timed out的话，表示在DNS服务器内没有此DNS服务器自己的PTR日志（需创建在反向查找区域内），您可以不理会此错误信息。

STEP 3 输入**set type=srv**后单击Enter键，表示要显示SRV日志。

STEP 4 如图 2-28所示，输入 **_ldap._tcp.dc._msdcs.sayms.com**后单击Enter键，由图中可看出域控制器dc1.sayms.com已经成功地将其扮演LDAP服务器角色的信息注册到DNS服务器内。

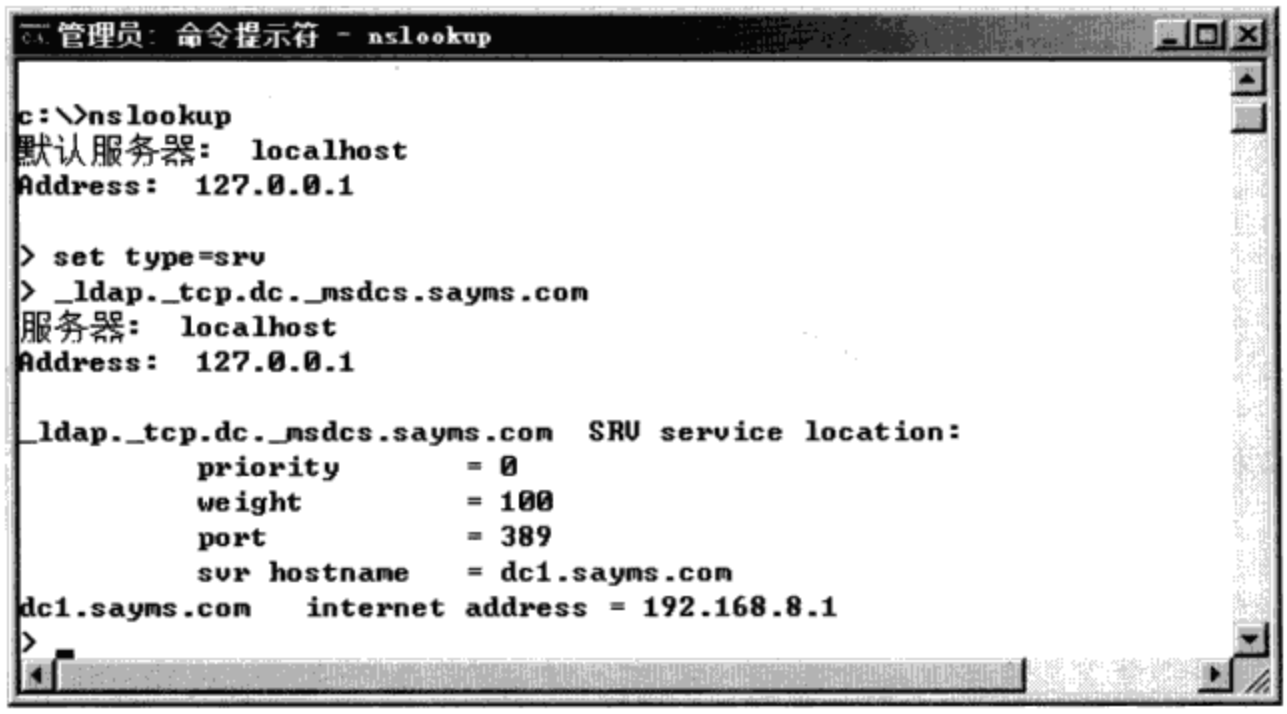


图 2-28

STEP 5 有需要的话，还可以使用其他类似的命令来查看其他SRV日志，例如使用**_gc._tcp.sayms.com**命令来查看扮演**全局编录服务器**的域控制器。您也可以使用**ls –t SRV sayms.com**命令来查看所有的SRV日志，不过需先在DNS服务器上将sayms.com区域的**允许区域转发**权限开放给您的计算机，否则无法在您的计算机上查询，而且会显示**Query Refused**的警告信息。

2-3-2 排除注册失败的问题

如果因为域控制器（或域成员计算机）本身的设置有误或者是网络问题，造成它们无法将

Download at http://www.pin5i.com/

数据注册到DNS服务器的话，那么您可以在问题解决后，通过重新启动这些计算机的方式来重新注册，或是使用以下的方法来手动注册：

- 若域控制器（或域成员）的主机名与IP地址未正确注册到DNS服务器的话，请到这台计算机上使用**ipconfig /registerdns**命令来手动注册，然后到DNS服务器的区域内检查是否已经有正确的日志，例如域控制器的主机名为dc1.sayms.com，IP地址为192.168.8.1，则请检查DNS区域sayms.com内是否有dc1的主机（A）日志，其IP地址是否为192.168.8.1。
- 若您发现域控制器并没有将其所扮演的角色注册到DNS服务器内的话，也就是并没有类似前面图 2-25中的_tcp等文件夹与相关SRV日志时，则请到此域控制器上使用【开始➲管理工具➲服务➲如图 2-29所示对着**Netlogon**服务右击➲重新启动】的方式来注册。



图 2-29

提示

域控制器默认每隔24小时会自动向DNS服务器注册1次。

2-3-3 检查Active Directory数据库文件与SYSVOL文件夹

Active Directory数据库文件与日志文件默认是存储在**%systemroot%\ntds**文件夹内，故您可以通过【开始➲运行➲输入**%systemroot%\ntds**➲单击确定按钮】的方式来检查文件夹与文件是否已经被正确地创建完成，如图 2-30所示中的ntds.dit就是Active Directory数据库文件，而edb.log、edb00001.log等扩展名为.log的文件是日志文件（扩展名默认会被隐藏）。

Download at http://www.pin5i.com/

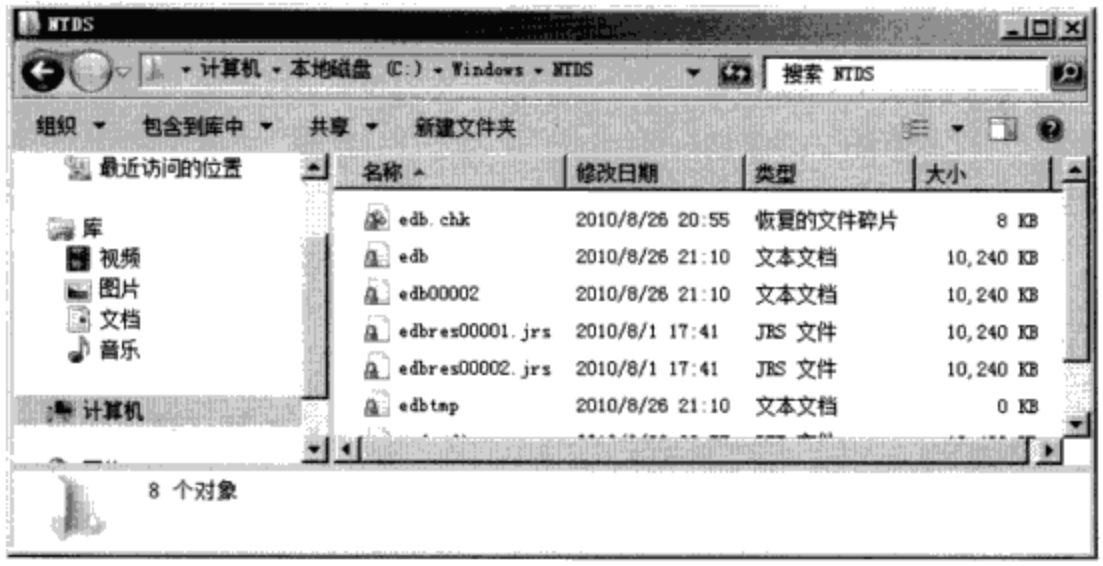


图2-30

另外SYSVOL默认是被创建在**%systemroot%\SYSVOL**文件夹内，因此您可以通过【开始➲运行➲输入**%systemroot%\SYSVOL**➲单击确定按钮】的方式来检查，如图 2-31所示。

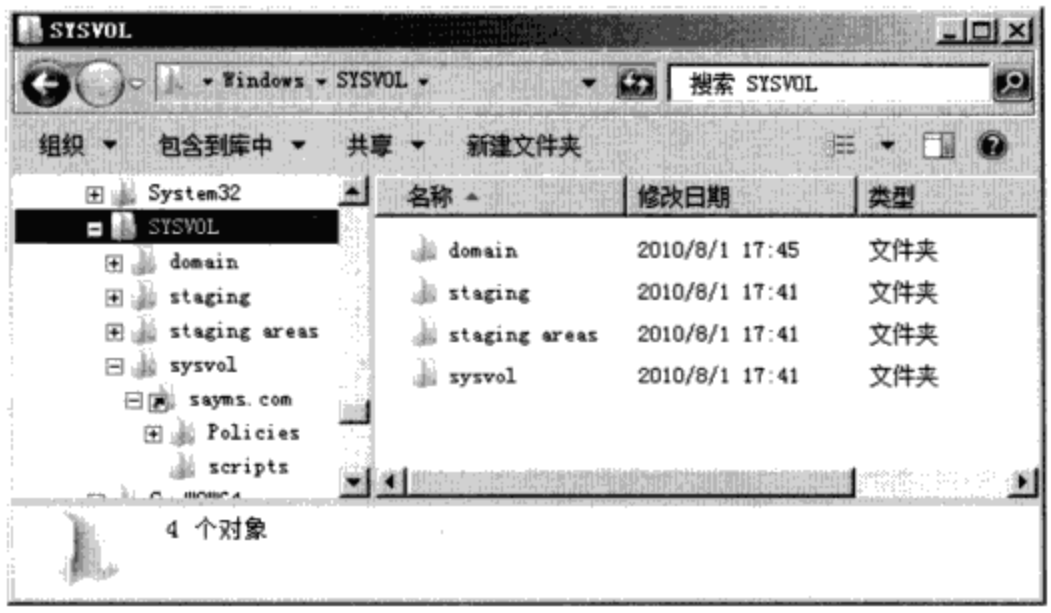


图2-31

图中SYSVOL文件夹之下有4个子文件夹，其中的sysvol与其内的scripts都应该会被设为共享文件夹。您可以按如图 2-32所示的方式（使用**计算机管理**窗口）或按如图 2-33所示的方式（使用**net share**命令）来检查它们是否已被设置为共享文件夹。

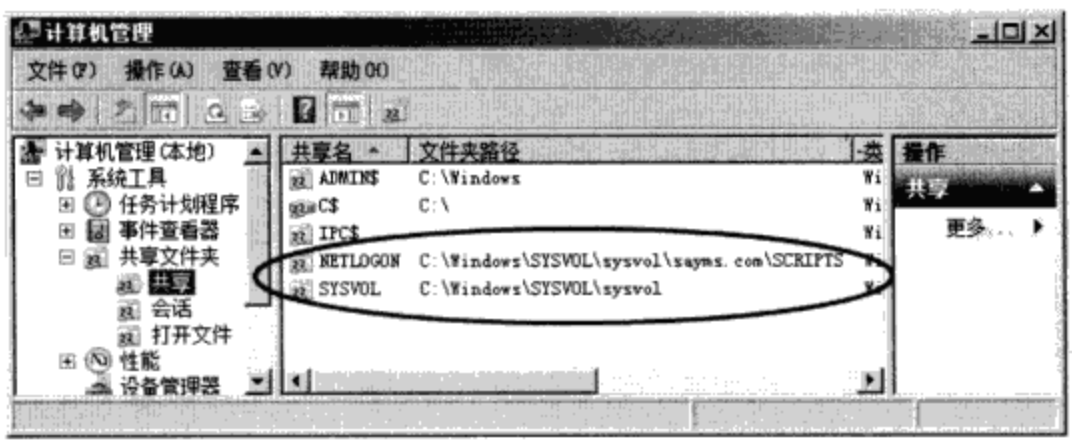


图2-32

Download at http://www.pin5i.com/

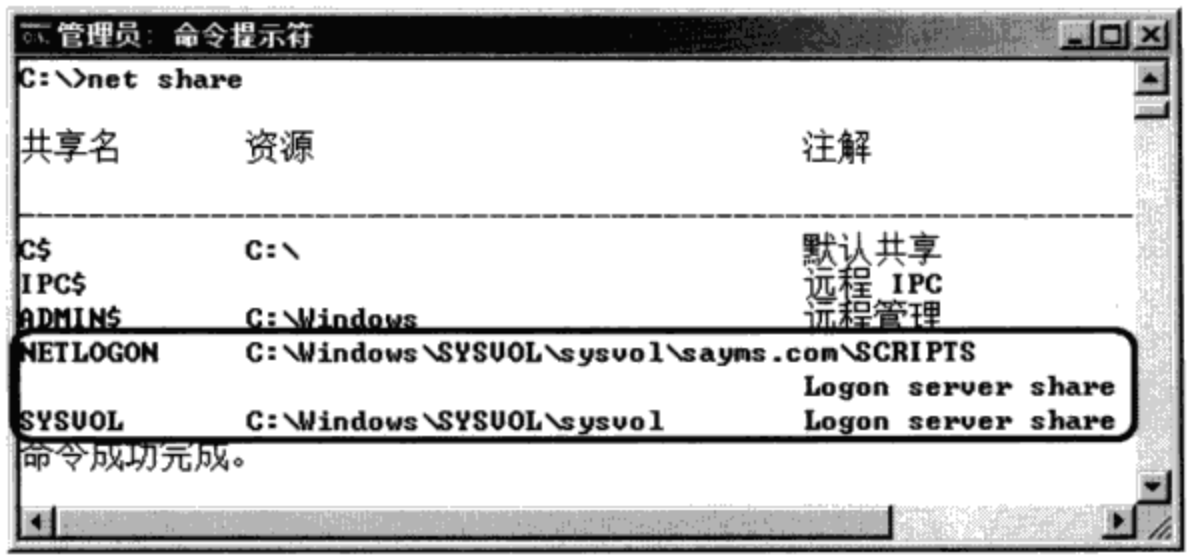


图2-33

2-3-4 新添加的管理工具

AD DS安装完成后，在【开始➲管理工具】内添加一些AD DS的管理工具，例如**Active Directory用户和计算机**、**Active Directory管理中心**、**Active Directory站点和服务**等（如图2-34所示）。

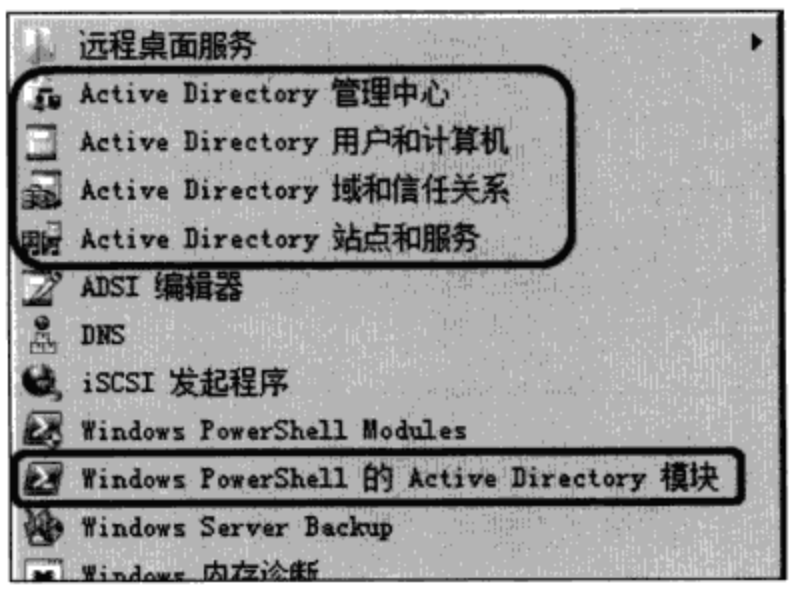


图2-34

2-3-5 查看事件日志文件

您可以通过【开始➲管理工具➲事件查看器】的方式来查看事件日志文件，以便检查任何与AD DS有关的问题，如图2-35所示，可以使用**系统**、**DFS Replication**、**DNS服务器**、**目录服务**等日志文件来检查。

Download at http://www.pin5i.com/

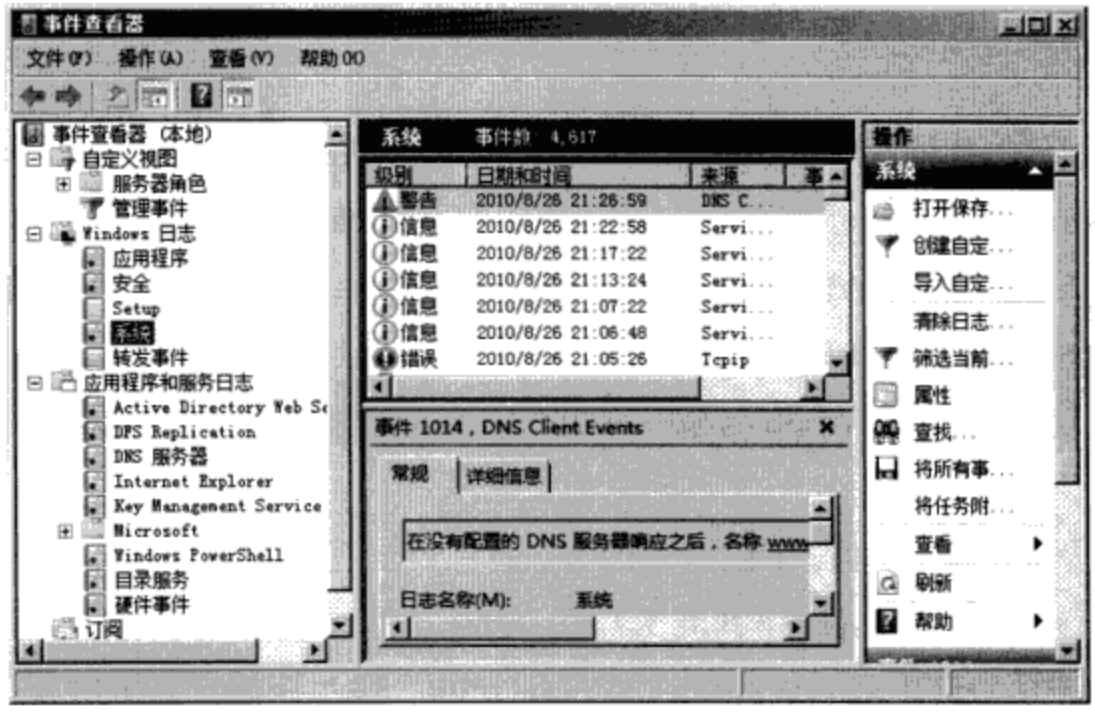


图 2-35

2-4 提升域与林功能级别

我们在第1-3节内已经详细说明了域与林功能各级别的差异，此处将介绍如何将现有的级别提升。您可以通过【开始➲管理工具➲ Active Directory管理中心➲单击域名**sayms（本地）**➲单击图 2-36右方的**提升林功能级别**或**提升域功能级别…】**的方法来提高级别。

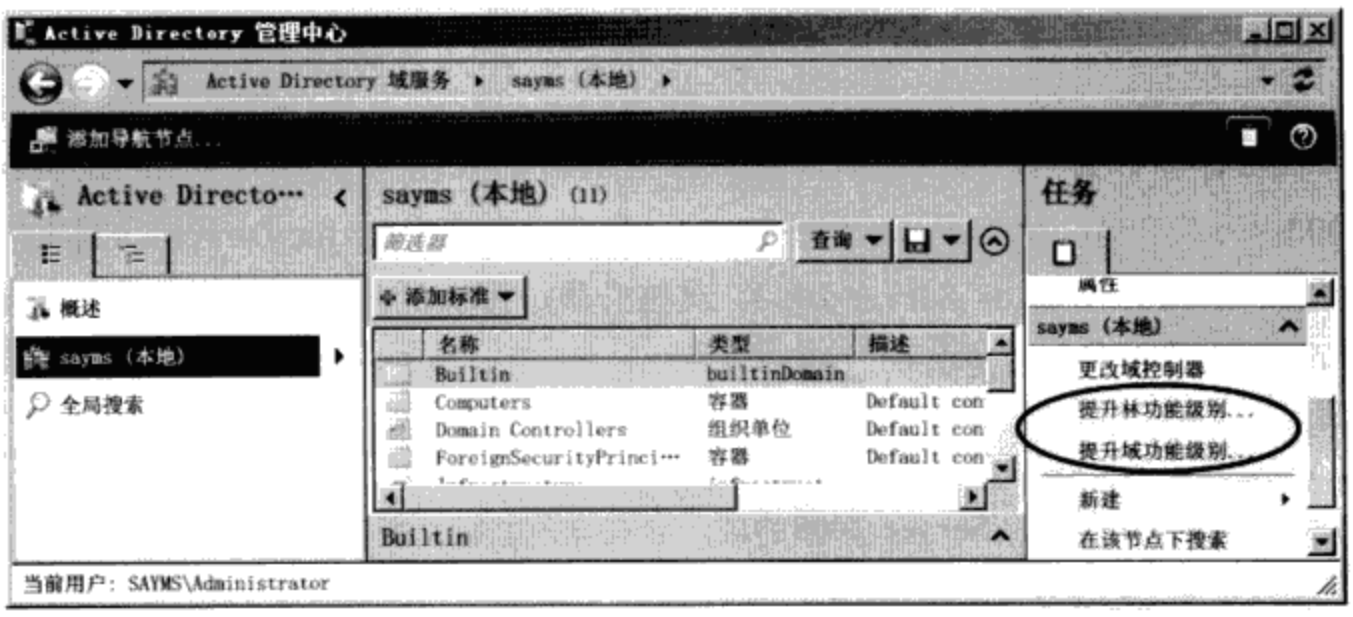


图 2-36

您也可以通过【开始➲管理工具➲Active Directory用户和计算机➲对着域名sayms.com右击➲提升域功能级别…】或【开始➲管理工具➲Active Directory域和信任关系➲对着**Active Directory域和信任关系**右击➲提高林功能级别…】的方法来提高级别。

Download at http://www.pin5i.com/

2-4-1 提升域功能级别

若目前的域功能级别为 **Windows 2000**本机模式，则您可以选择将其提升为 **Windows Server 2003**、**Windows Server 2008**或 **Windows Server 2008 R2**。

若目前的域功能级别为 **Windows Server 2003**，则您可以选择将其提升为**Windows Server 2008**或**Windows Server 2008 R2**。

若目前的域功能级别为 **Windows Server 2008**，则您只能将其提升为**Windows Server 2008 R2**。

一旦提升级别后，就无法再改回原来的级别，但有一个例外，就是将域功能级别从**Windows Server 2008**提升为**Windows Server 2008 R2** 后，若林功能级别为**Windows Server 2008**或较低的话，就可以将域功能级别降回**Windows Server 2008**。这些升级、降级信息会被自动复制到所有域控制器，不过可能需要花费15s或更久的时间。

2-4-2 提升林功能级别

若当前的林功能级别为 **Windows 2000**，则您可以选择将其提升为 **Windows Server 2003**、**Windows Server 2008**或 **Windows Server 2008 R2**。

若目前的林功能级别为 **Windows Server 2003**，则您可以选择将其提升为**Windows Server 2008**或**Windows Server 2008 R2**。

若目前的林功能级别为 **Windows Server 2008**，则您只能将其提升为**Windows Server 2008 R2**。

一旦提升级别后，就无法再改回原来的级别，但有一个例外，就是将林功能级别从**Windows Server 2008**提升为**Windows Server 2008 R2** 后，只要没有启用**Active Directory回收站**，就可以将林功能级别降回**Windows Server 2008**。这些升级、降级信息会被自动复制到所有域控制器，不过可能需要花费15s或更久的时间。

> **注意**
>
> 域功能级别为**Windows Server 2008**的域，会在林功能级别提升为**Windows Server 2008 R2**后，其域功能级别也将自动被提升为**Windows Server 2008 R2**。

2-5 添加额外域控制器与RODC

域内若有多台域控制器的话，就可以拥有以下的优势。

- 改善用户登录的效率：因为多台域控制器可以同时分担审核用户名与密码的工作负

Download at http://www.pin5i.com/

担，因此可以加快用户登录的速度。

- 提供容错功能：即使其中一台域控制器故障了，仍然可以由其他域控制器来提供服务，让用户可以正常的登录。

在安装额外域控制器（Additional Domain Controller）时，需要将Active Directory数据库由现有的域控制器复制到这台新的域控制器，然而如果数据库非常庞大的话，这个复制操作势必会增加网络负担，尤其是这台新域控制器位于远程网络内。Windows Server 2008 R2提供了两种复制Active Directory数据库的方式。

- 通过网络直接复制：如果Active Directory数据库庞大的话，这种方法会影响网络效率。
- 通过安装媒体：您需要事先到一台域控制器内制作**安装媒体**（Installation Media），其内包含着Active Directory数据库，接着将**安装媒体**复制到U盘、CD、DVD等媒体或共享文件夹内。然后在安装额外域控制器时，要求安装向导到这个媒体内读取**安装媒体**内的Active Directory数据库，这种方式可以大幅降低对网络所造成的冲击。若在**安装媒体**制作完成之后，现有域控制器的Active Directory数据库内有新数据的话，这些少量数据会在完成额外域控制器的安装后，再通过网络自动复制过来。

本节的说明同时适用于一般的**可写域控制器**（Writable Domain Controller）与**只读域控制器**（Read-Only Domain Controller，RODC）。

2-5-1 使用Windows窗口界面来安装额外域控制器

我们将通过添加服务器角色的方式来将图 2-37中右上角的服务器dc2.sayms.com升级为额外域控制器。

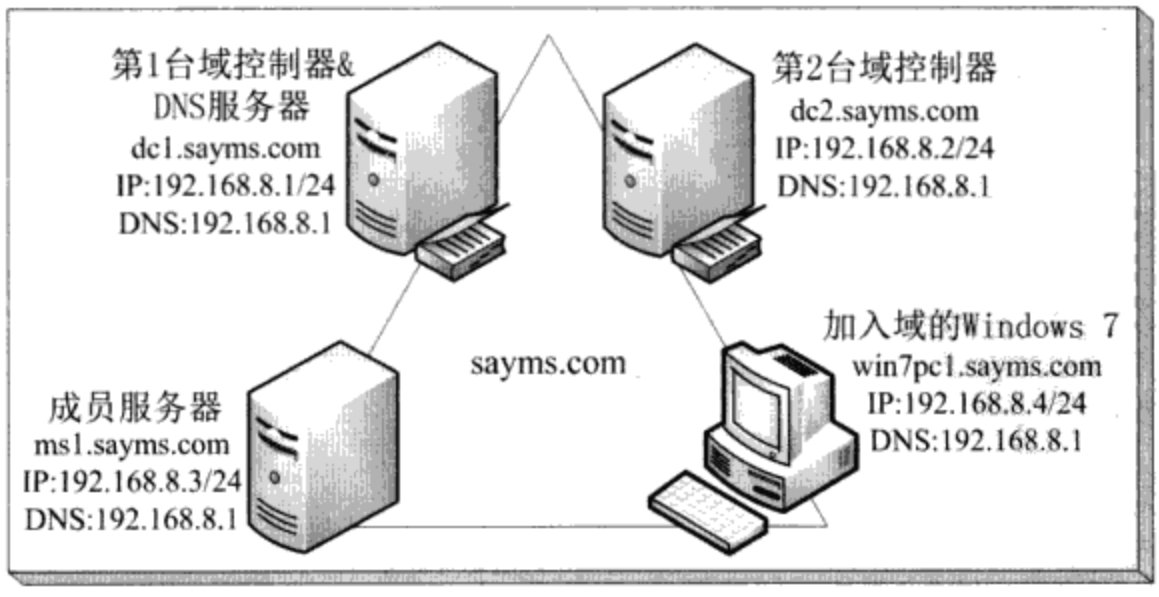


图2-37

STEP 1 请先在图 2-37中右上角的服务器dc2.sayms.com上安装Windows Server 2008 R2，将计算机名称设置为dc2，IPv4地址等依照图中所示来设置（图中采用TCP/IPv4）。注意将计算机名设置为dc2即可，等升级为域控制器后，它会自动被改为

Download at http://www.pin5i.com/

dc2.sayms.com。

STEP 2 选用以下两种方式之一来安装**Active Directory域服务**（AD DS）：

- 单击左下角的**服务器管理器**图标：转至**STEP 3**。
- 通过【开始➲运行➲输入dcpromo后单击确定按钮】的方法：此时系统会自动运行**STEP 3**～**STEP 9**的安装步骤，故请直接跳到**STEP 10**。

STEP 3 单击**角色**界面右边的**添加角色**。

STEP 4 在出现**开始之前**界面时单击下一步按钮。

STEP 5 在图 2-38中选择**Active Directory域服务**复选框，在弹出的界面中单击**添加必需的功能**选项，单击下一步按钮。



图2-38

STEP 6 在**Active Directory域服务**界面中单击下一步按钮。

STEP 7 在**确认**界面中单击安装按钮。

STEP 8 在**结果**界面中单击关闭按钮。

STEP 9 在图 2-39中【单击**Active Directory域服务**➲单击**运行Active Directory域服务安装向导（dcpromo.exe）**】。

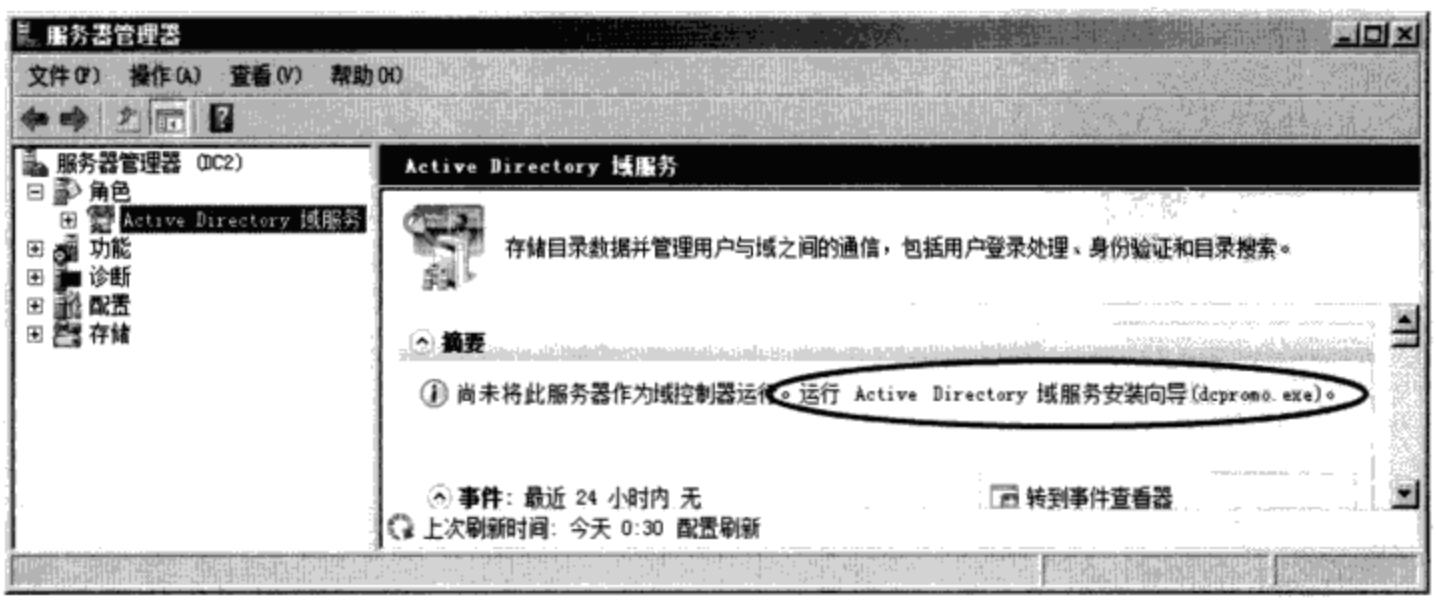


图2-39

Download at http://www.pin5i.com/

STEP 10 如图 2-40所示选择**使用高级模式安装**复选框后单击下一步按钮。

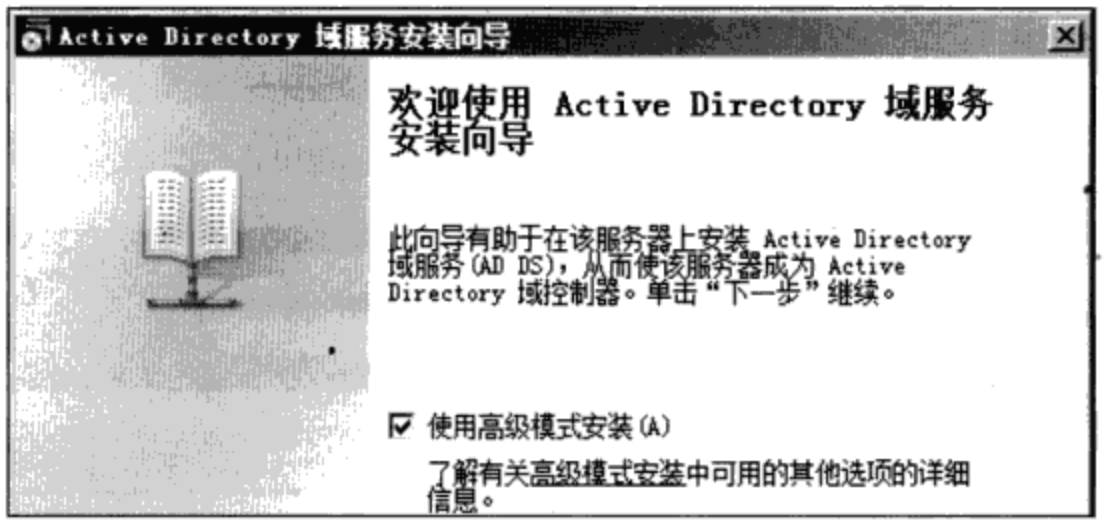


图2-40

提示

若您没有通过安装媒体或没有通过指定源域控制器来复制Active Directory数据库的话，可以不选择**使用高级模式安装**复选框。

STEP 11 在出现**操作系统兼容性**界面时单击下一步按钮。

STEP 12 如图 2-41所示，选择**现有林**下的**向现有域添加域控制器**单选按钮后单击下一步按钮。

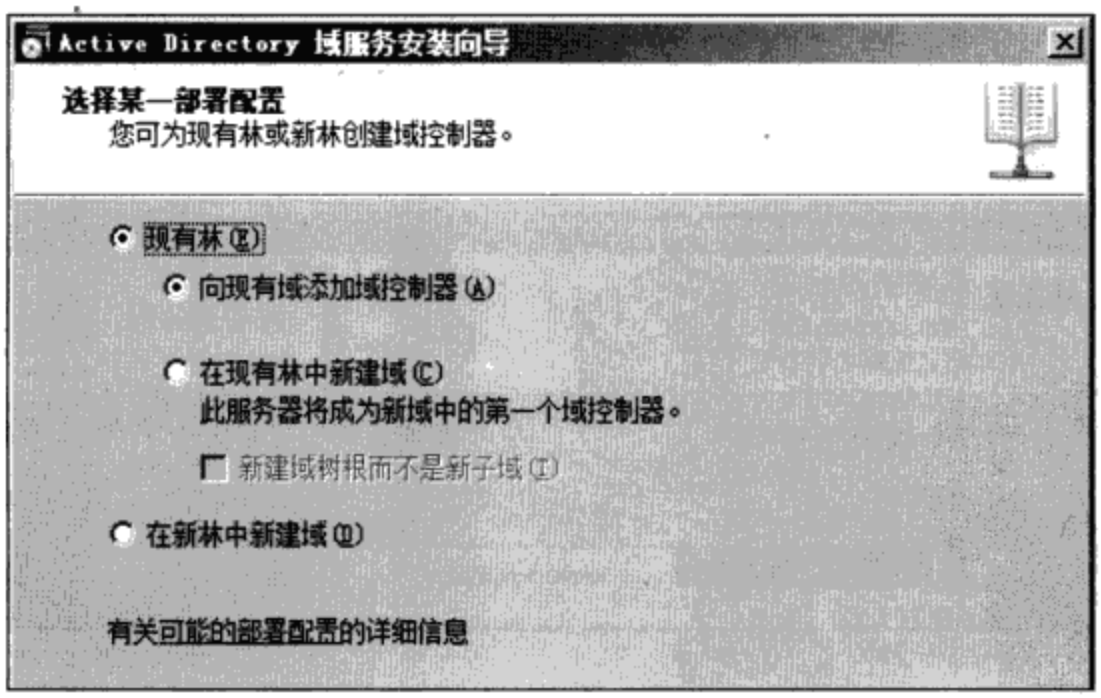


图2-41

STEP 13 在图 2-42中【输入域名sayms.com➲单击设置按钮➲输入Administrator与其密码后单击确定按钮➲单击下一步按钮】。

Download at http://www.pin5i.com/

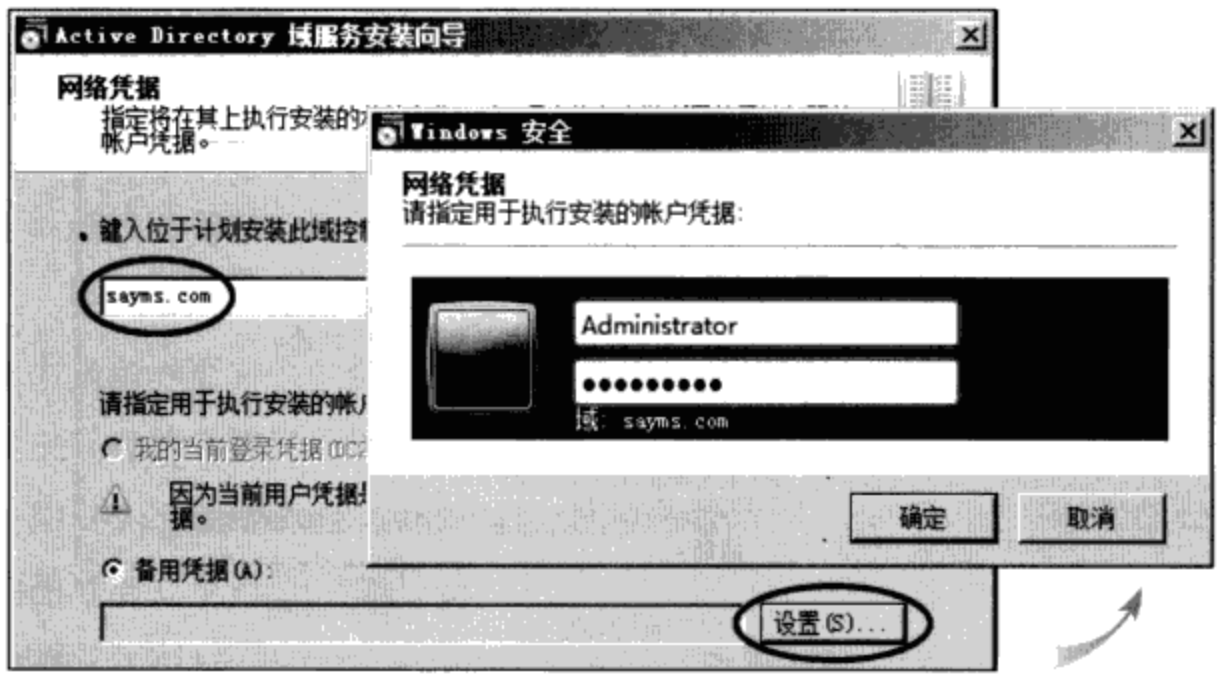


图2-42

注意

在图2-42中请输入林中任何一个域名都可以，安装向导只是使用它来取得这个林中有哪些域存在的信息，以便下一个界面能够列出这些域名，您就可以从这些域中选择要添加额外域控制器的域。只有Enterprise Admins或Domain Admins内的用户有权限创建额外域控制器。如果您现在登录的账户没有权限在此域中创建额外域控制器的话（例如我们现在所登录的账户为本地Administrator），就需要如图所示在**备用凭据**处另外指定有权限的用户账户。

STEP 14 在图 2-43中选择要添加域控制器的域后单击下一步按钮。

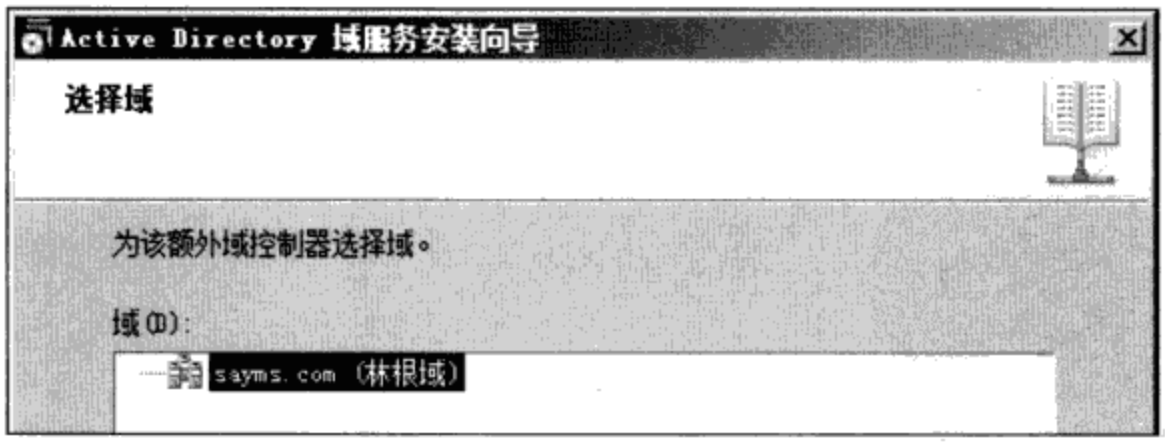


图2-43

STEP 15 在图2-44中选择新域控制器所在的AD DS站点，目前只有一个默认的站点Default-First-Site-Name，请直接单击下一步按钮。

Download at http://www.pin5i.com/

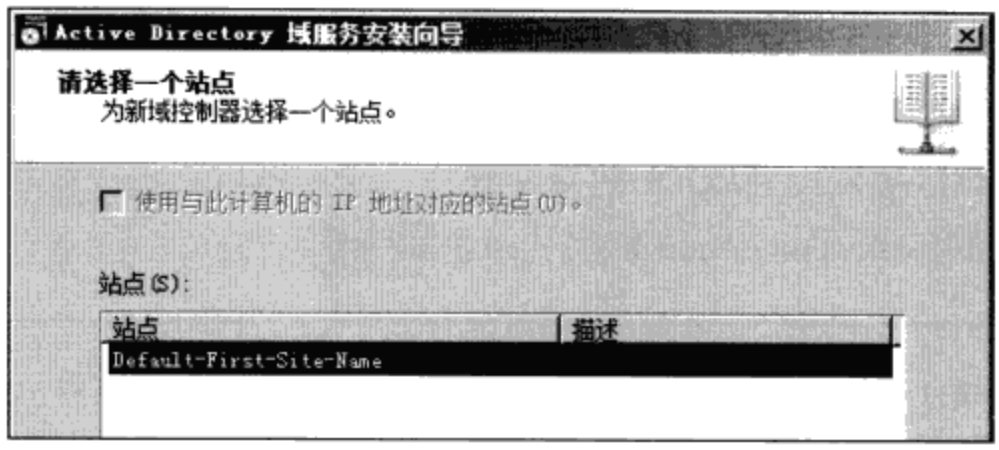


图2-44

STEP 16 在图 2-45中直接单击 下一步 按钮。由图中可知它会在这台服务器上安装DNS服务器，同时会将其设置为**全局编录服务器**。若要安装RODC的话，请选择**只读域控制器（RODC）**复选框。

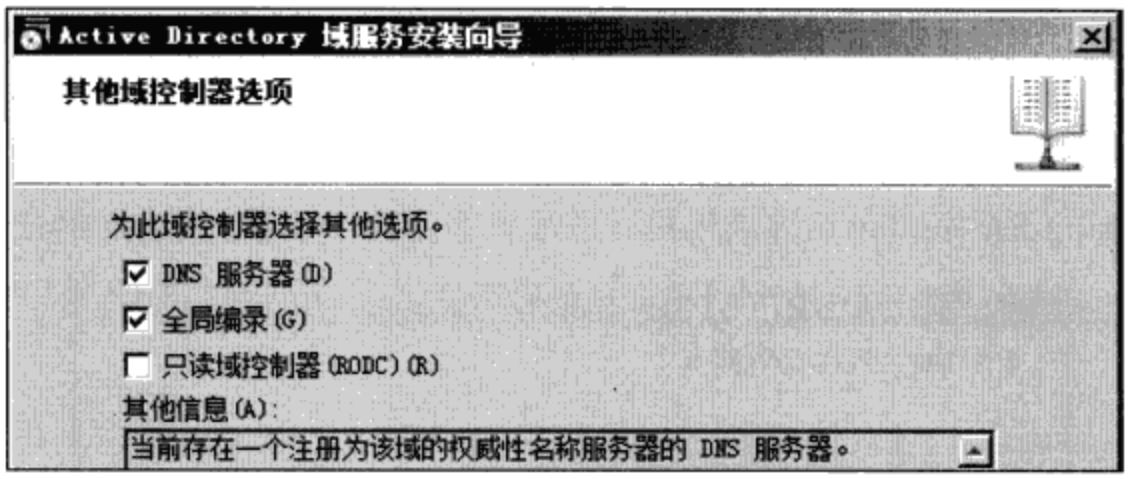


图2-45

STEP 17 若在图2-45中未选择**只读域控制器（RODC）**复选框的话，请直接跳到**STEP 19**。若是安装RODC的话，则会出现如图2-46所示界面，用于设置**密码复制策略**，图中默认是没有任何用户的密码被允许复制到RODC，而且一些重要账户（例如Administrators、Server Operators等组内的用户）的密码已明确的被拒绝复制到RODC。

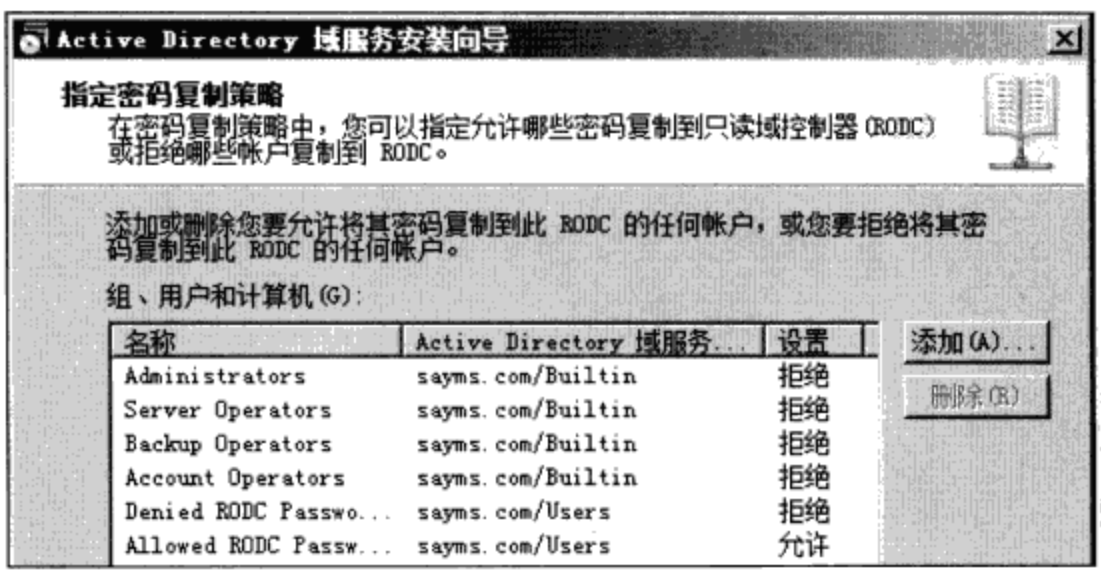


图2-46

Download at http://www.pin5i.com/

STEP 18 虽然图中已经允许Allowed RODC Password Replication Group组内的用户密码可以被复制到RODC，不过此组内默认并没有任何成员。您可以通过单击添加按钮来添加密码可以被复制到RODC的用户账户（或是将用户账户加入到Allowed RODC Password Replication Group组内），单击下一步按钮。

提示

在安装域中的第1台RODC时，系统会自动创建与RODC有关的组账户，这些账户会通过AD DS的复制机制自动复制给其他域控制器，不过可能需要花费一点时间，尤其是复制给位于不同站点的域控制器。之后您在其他站点安装RODC时，若安装向导无法从这些域控制器得到这些组信息的话，它会显示警告信息，此时请等这些组信息完成复制后，再继续安装这台RODC。

STEP 19 可以在图 2-47中将此RODC的管理工作委派给指定的用户或组。被委派的用户或组在这台RODC将拥有本地系统管理员的权限，而且如果是采用阶段式安装RODC的话（后述），则他们也可以将此RODC服务器**附加到**（attach to）Active Directory数据库内的计算机账户。若您没有在界面中委派用户或组的话，则只有Domain Admins或Enterprise Admins组内的用户有权限管理此RODC与执行附加的工作。

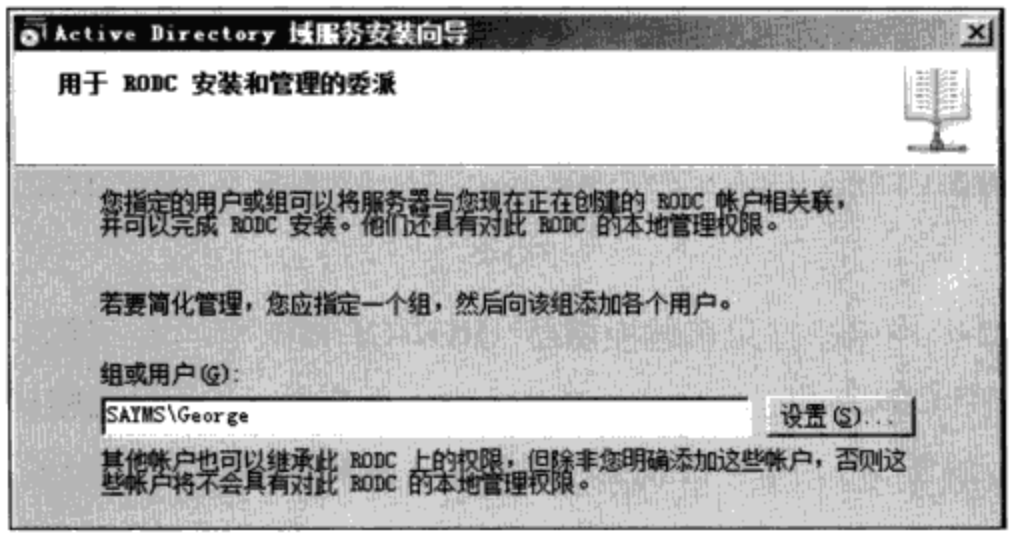


图 2-47

STEP 20 若出现如图 2-48所示界面的话，请直接单击是（Y）按钮。

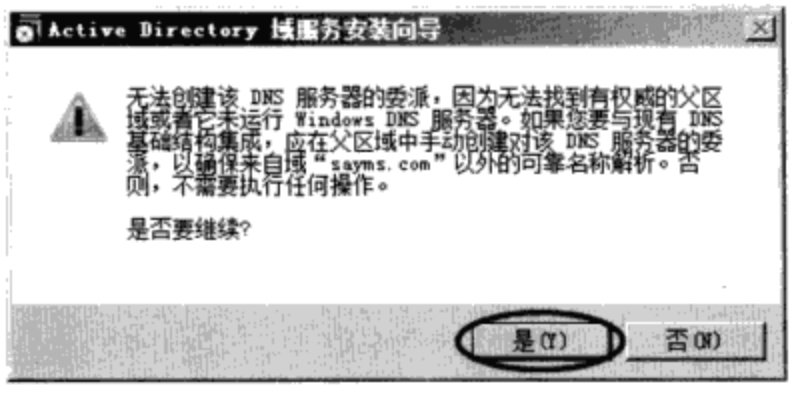


图 2-48

Download at http://www.pin5i.com/

STEP 21 如图2-49所示，选择**通过网络**从现有域控制器复制数据单选按钮后单击下一步按钮。

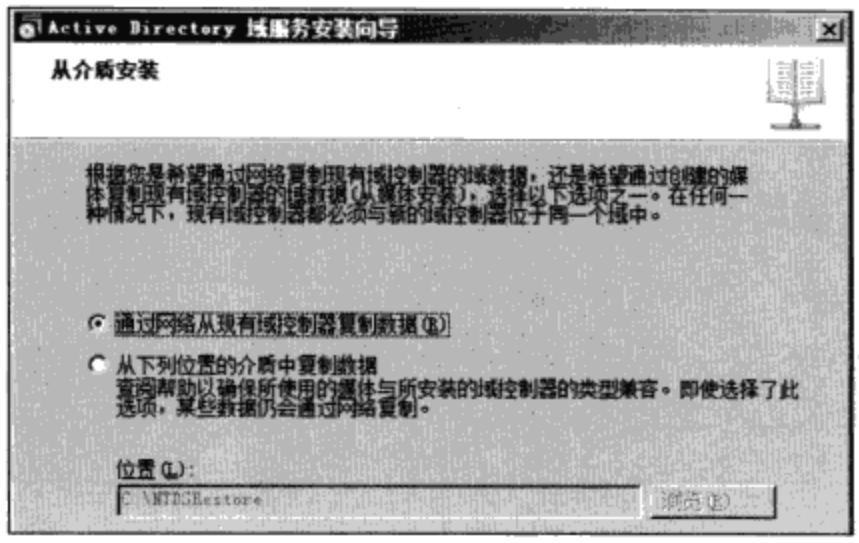


图2-49

STEP 22 在图 2-50中单击下一步按钮使安装向导自动选择Active Directory数据库的源域控制器（或手动选择特定的域控制器）。若是安装可写域控制器的话，则其源域控制器不可以是RODC。

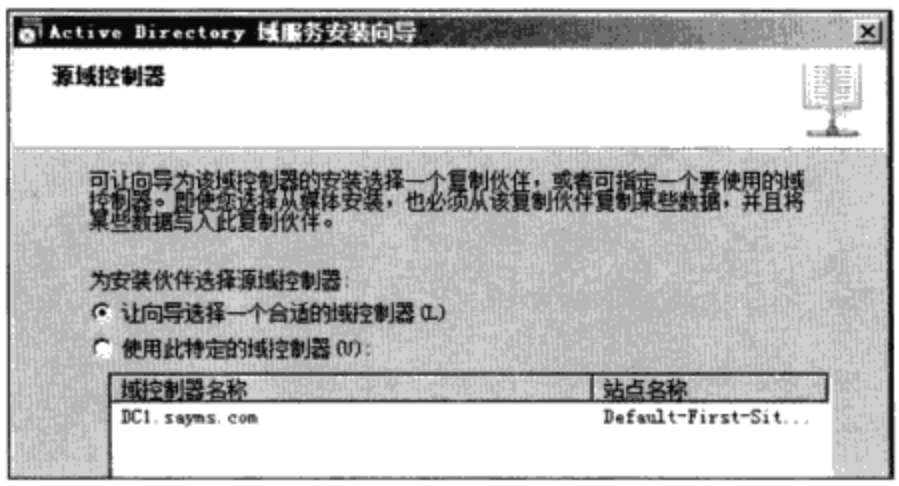


图2-50

STEP 23 在图 2-51中直接单击下一步按钮。

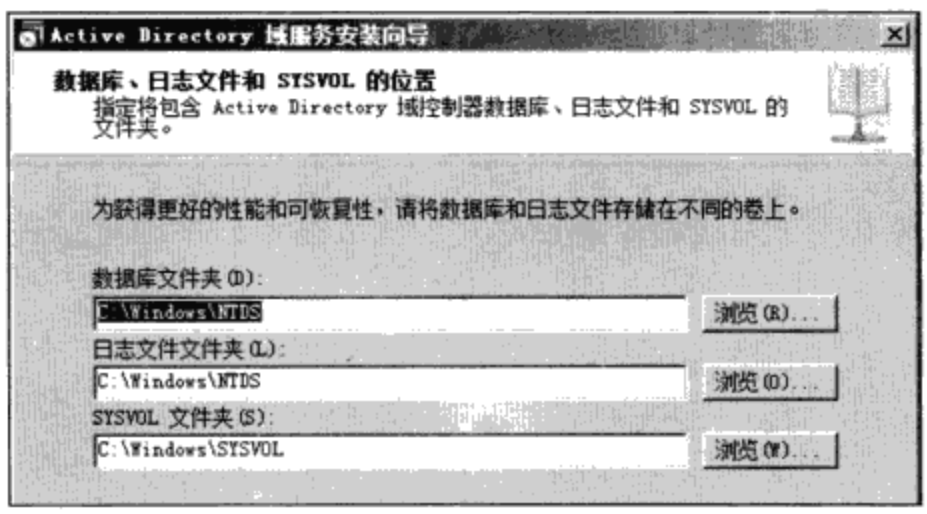


图2-51

Download at http://www.pin5i.com/

STEP 24 在图 2-52中设置目录服务还原模式的系统管理员密码，完成后单击**下一步**按钮。

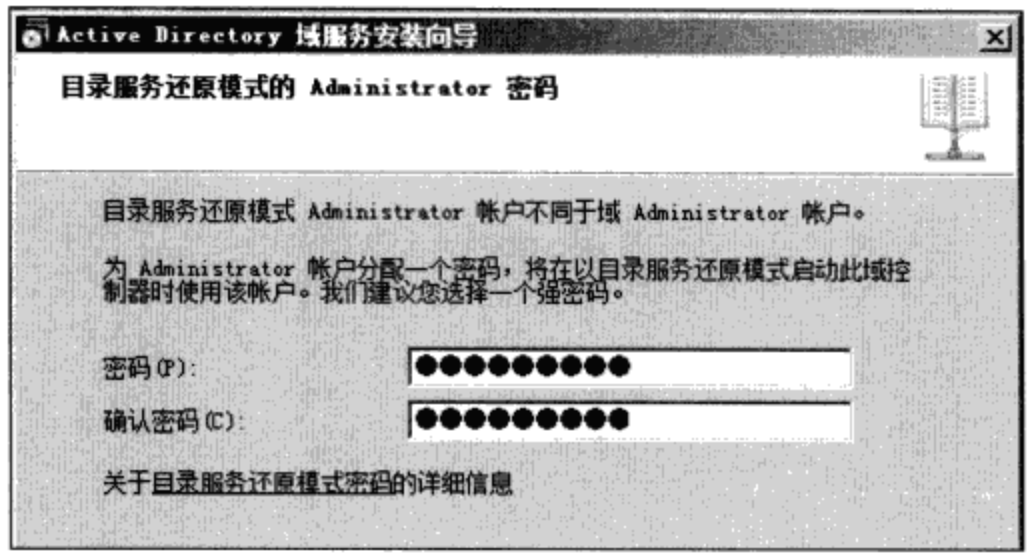


图 2-52

STEP 25 在图 2-53中直接单击**下一步**按钮。

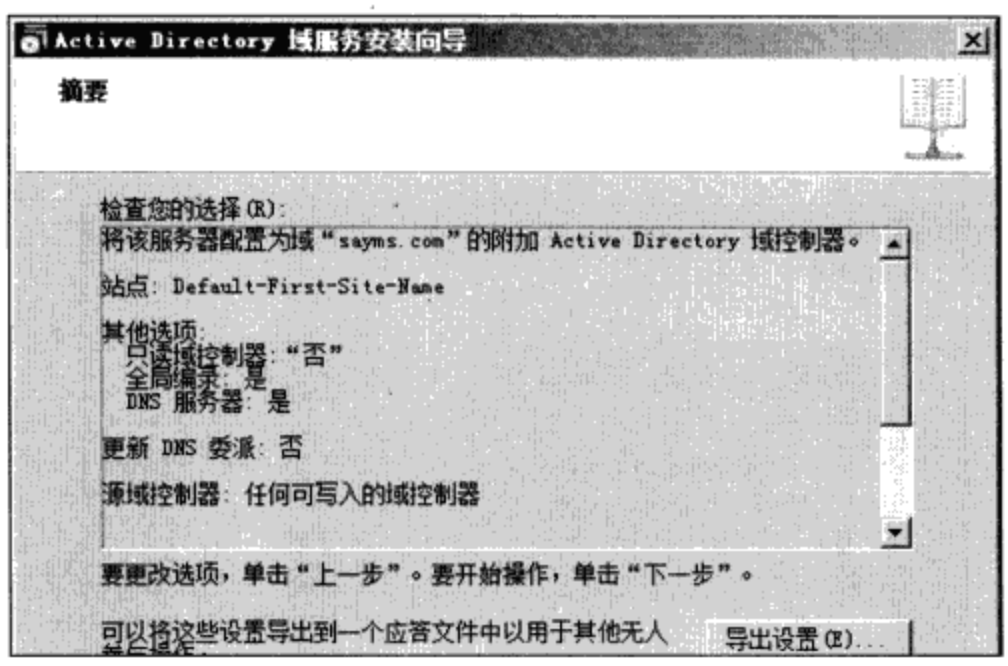


图 2-53

提示

您可以单击**导出设置**按钮来将设置存储为**应答文件**(Answer File)，它可供利用dcpromo.exe来安装域控制器时使用。安装向导并不会将目录服务还原模式的系统管理员密码存储到此文件。

STEP 26 可在图 2-54中选择**完成后重新启动**复选框或完成后手动重新启动。

Download at http://www.pin5i.com/

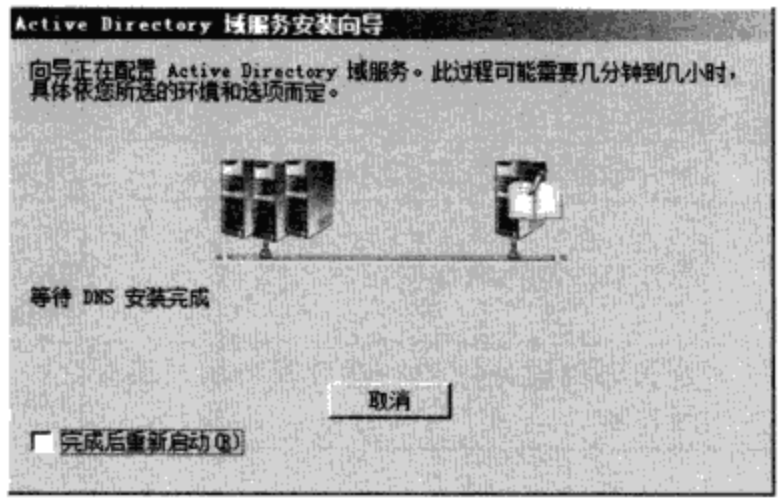


图2-54

STEP 27 检查DNS服务器内是否存在这台域控制器dc2.sayms.com的相关日志（可参考前面的内容检查DNS服务器内的日志是否具备完整的说明）。

提示

这台域控制器的Active Directory数据库内容是从其他域控制器复制过来的，而原本这台计算机内的本地用户账户会被删除。

2-5-2 使用应答文件来安装额外域控制器

您可以将安装额外域控制器时所必须提供给安装向导的数据，例如域名、是否要安装DNS服务器、是否要将其设置为**全局编录服务器**、Active Directory数据库的存储路径、目录服务还原模式的系统管理员密码等，事先输入到**应答文件**（Answer File）内，然后让安装向导直接从**应答文件**来读取这些数据，不需要再手动输入。

请使用**记事本**来编辑应答文件，如图 2-55所示，图中我们必须在此文件内创建一个名称为**DCInstall**的区段，然后在此区段内输入相关的参数与参数值，图中参数除了列于表 2-1中的之外，其余请参见表2-2。

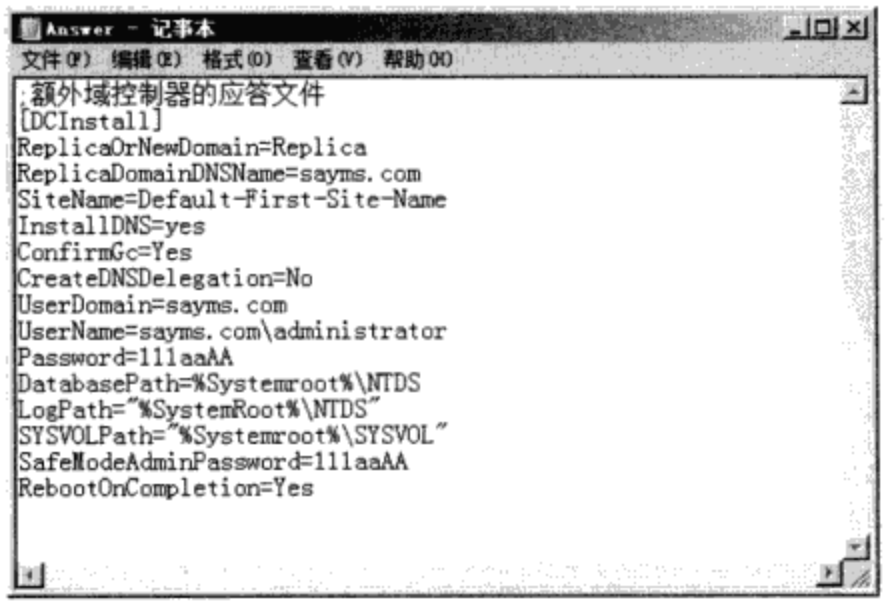


图2-55

Download at http://www.pin5i.com/

表 2-2

参数值	说明	参数值可为
ReplicaDomainDNSName	额外域控制器所在的DNS域名	例如sayms.com
SiteName	额外域控制器所在的站点名称	若尚未另外创建站点的话，则目前只有内置的第1个站点，其名为Default-First-Site-Name
ConfirmGc	是否要将额外域控制器设置为全局编录服务器	Yes或No
UserDomain	执行安装工作的用户的域名、账户名与密码	必须是Enterprise Admins或此域Domain Admins组内的用户
UserName		
Password		

完成应答文件的创建后，请通过以下命令（参考图 2-56）来安装额外域控制器，假设应答文件的文件名为Answer.txt，且其位于C:\Test文件夹内：

```
dcpromo /unattend:"C:\Test\answer.txt"
```



图2-56

提示

dcpromo.exe读取到应答文件中的SafeModeAdminPassword与Password的密码后，会自动将此密码清除后再保存到应答文件内。

2-5-3 使用命令行来安装额外域控制器

您可以通过【开始➲命令提示符】或单击左下方任务栏的**Windows PowerShell**图标，然后运行如下所示的**dcpromo.exe**命令来自动安装额外域控制器（参考图 2-57）：

```
dcpromo /unattend /replicaOrNewDomain:replica
/replicaDomainDNSName:sayms.com/siteName:Default-First-Site-Name
/InstallDns:yes/confirmGC:yes
/createDNSDelegation:no /userDomain:sayms.com
/userName:sayms.com\administrator  /password:111aaAA
/databasePath:"%SystemRoot%\NTDS"
/logPath:"%SystemRoot%\NTDS"
```


Download at http://www.pin5i.com/

```
/sysvolpath:"%SystemRoot%\SYSVOL"
/safeModeAdminPassword:111aaAA /rebootOnCompletion:yes
```



图 2-57

提示

您可以使用**dcpromo /?:Promotion**命令来查看其详细语法。

2-5-4 使用安装媒体来安装额外域控制器

我们先在一台域控制器上制作**安装媒体**（Installation Media），也就是将Active Directory数据库存储到**安装媒体**内，并将**安装媒体**复制到U盘、CD、DVD等媒体或共享文件夹内。然后在安装额外域控制器时，要求安装向导从**安装媒体**来读取Active Directory数据库，这种方式可以大幅降低对网络所造成的冲击。

1. 制作安装媒体

请到现有的一台域控制器上运行**ntdsutil**命令来制作**安装媒体**：

- 若此安装媒体是要给**可写域控制器**来使用的话，则您必须在现有的一台**可写域控制器**上运行**ntdsutil**命令。
- 若此安装媒体是要给**RODC**（只读域控制器）来使用的话，则您可以在现有的一台**可写域控制器**或**RODC**上运行**ntdsutil**命令。

操作步骤如下：

STEP 1 请到域控制器上使用域系统管理员的身份登录。

STEP 2 选择【开始➲命令提示符】（或单击左下方任务栏的**Windows PowerShell**图标）。

STEP 3 输入以下命令后单击Enter键（完整的操作界面可参考图 2-58）：

```
ntdsutil
```

STEP 4 在**ntdsutil**提示符下，输入以下命令后单击Enter键，它会将域控制器的Active

Download at http://www.pin5i.com/

Directory数据库设置为活动。

```
activate instance ntds
```

STEP 5 在**ntdsutil**提示符下，输入以下命令后单击Enter键：

```
ifm
```

STEP 6 在**ifm**提示符下，输入以下命令后单击Enter键，此命令假设是要将**安装媒体**的内容放置到C:\InstallationMedia文件夹内。

```
create full c:\InstallationMedia
```

> **提示**
>
> 其中的**full**表示要制作供可写域控制器使用的**安装媒体**，如果要制作供RODC使用的安装媒体的话，请将**full**改为**rodc**。

STEP 7 连续输入两次**quit**命令，单击Enter键来结束**ntdsutil**命令。图 2-58为完整的操作界面。

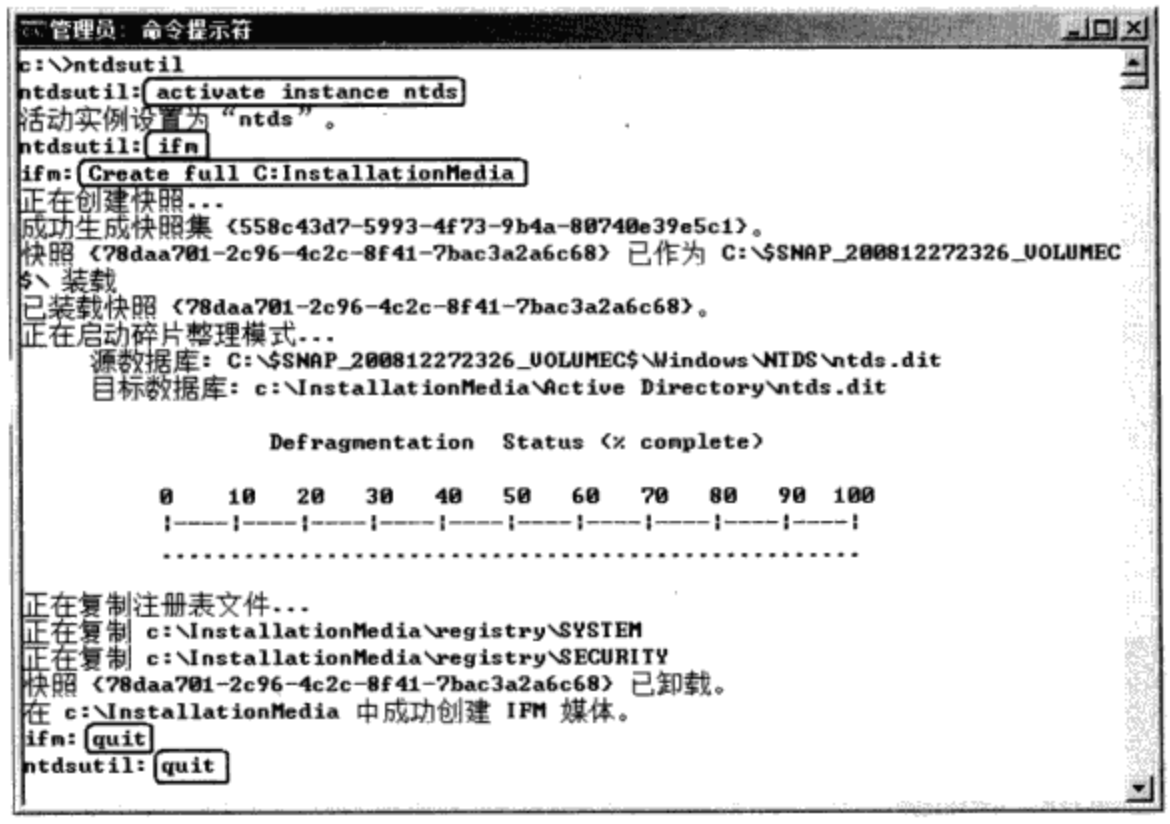


图2-58

STEP 8 将整个C:\InstallationMedia文件夹内的所有数据复制到U盘、CD、DVD等媒体或共享文件夹内。

2. 安装额外域控制器

将内含**安装媒体**的U盘、CD或DVD拿到即将扮演额外域控制器角色的计算机上，或是将

Download at http://www.pin5i.com/

其放到可以访问得到的共享文件夹内。

由于使用**安装媒体**来安装额外域控制器的方法与前一节大致相同，因此以下仅列出不同之处。以下假设**安装媒体**被复制到额外域控制器的C:\InstallationMedia文件夹内：

- 使用Windows窗口界面来安装：在图 2-59中改为选择**从下列位置的介质中复制数据**单选按钮，并在**位置**处输入存储**安装媒体**的文件夹C:\InstallationMedia。

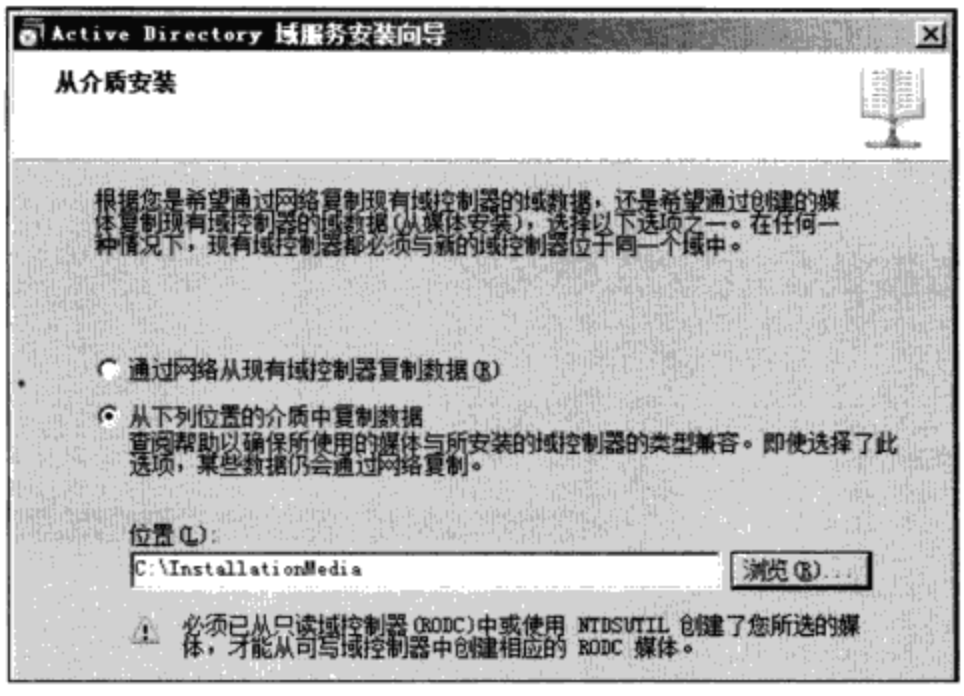


图 2-59

- 使用应答文件来安装：请在应答文件中添加如图 2-60所示的ReplicationSourcePath选项，并将其指定到**安装媒体**所在的文件夹C:\InstallationMedia。

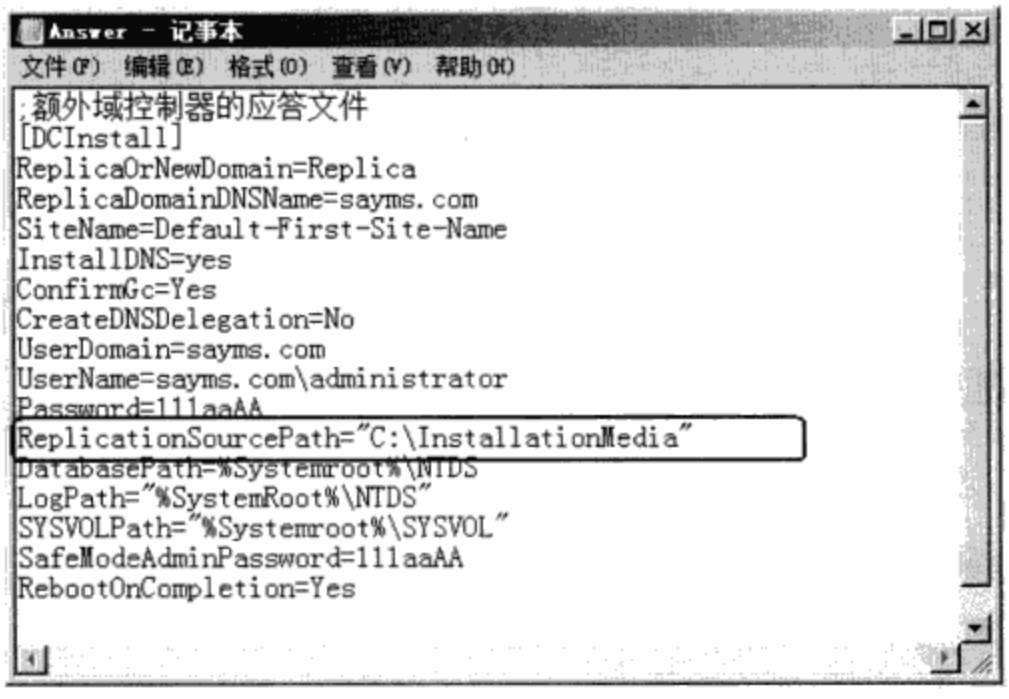


图 2-60

- 使用命令行来安装：使用**dcpromo.exe**命令来安装的选项与前一节相同，不过需添加**/ReplicationSourcePath: "C:\InstallationMedia"**选项。

安装过程中，会从**安装媒体**所在的文件夹C:\InstallationMedia中复制Active Directory数据

Download at http://www.pin5i.com/

库。若在**安装媒体**制作完成之后，现有域控制器的Active Directory数据库内有新变动数据的话，这些少量数据会在完成额外域控制器的安装后，再通过网络自动复制过来。

2-5-5 更改RODC的委派与密码复制策略设置

如果您要更改密码复制策略设置或RODC系统管理工作的委派设置的话，请在打开**Active Directory用户和计算机**窗口后，通过【如图 2-61所示，单击容器**Domain Controllers**右方扮演RODC角色的域控制器➲单击上方的**属性**图标➲打开图 2-62中的**密码复制策略**和**管理者**标签】的方式来设置。

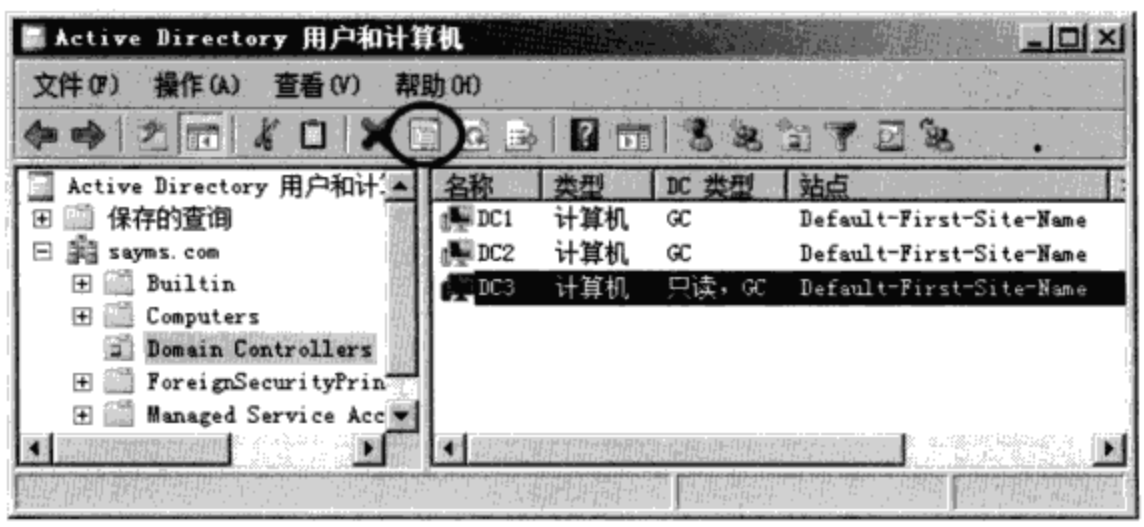


图2-61

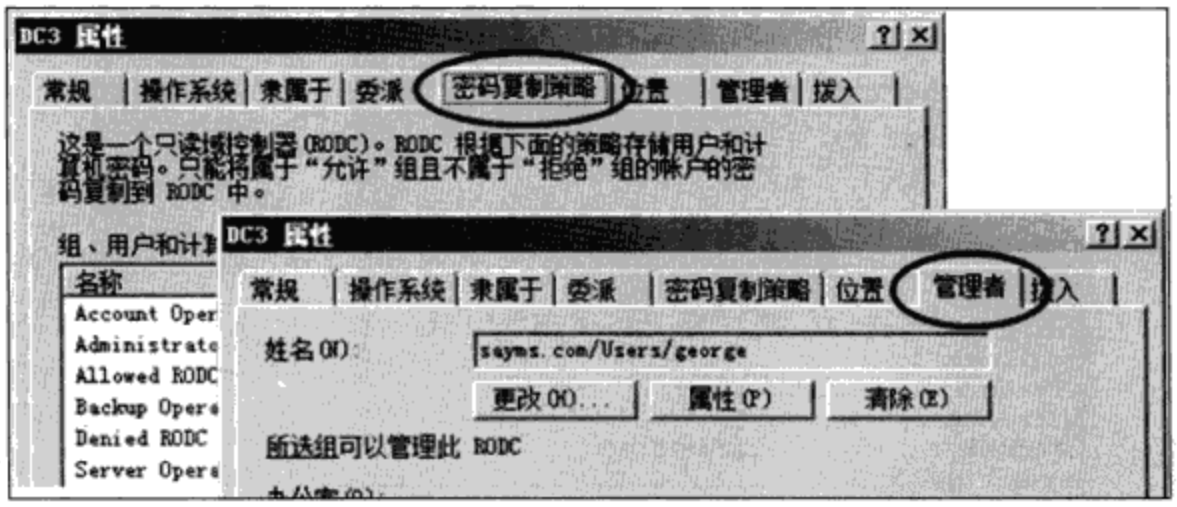


图2-62

您也可以通过**Active Directory管理中心**来更改上述设置：请在打开**Active Directory管理中心**后，通过【如图 2-63所示，选择容器**Domain Controllers**界面中扮演RODC角色的域控制器➲双击右方的**属性**选项➲打开图 2-64中的**管理者**区域和**扩展**区域中的**密码复制策略**标签】的方式来设置。

Download at http://www.pin5i.com/



图 2-63

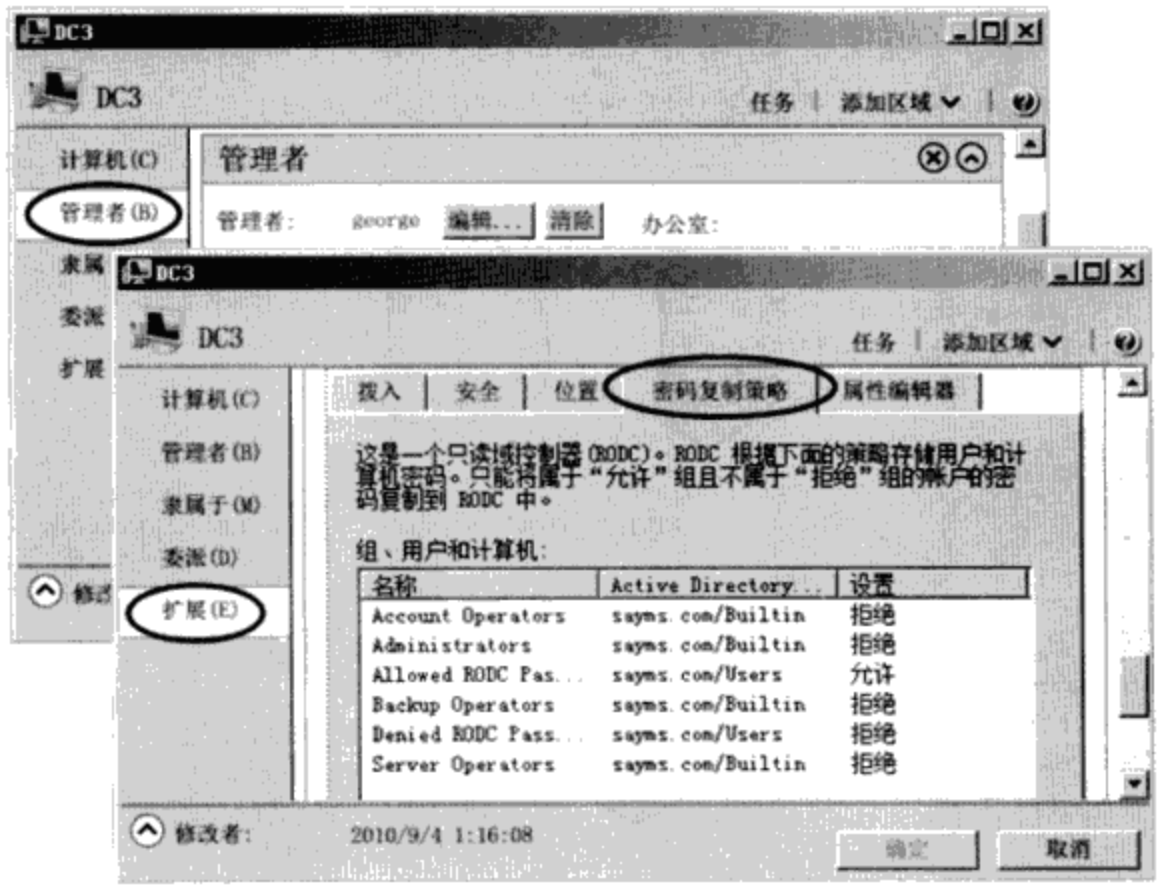


图 2-64

2-6 RODC阶段式安装

您可以采用两个阶段的安装方式来安装RODC（只读域控制器），这两个阶段分别由不同的用户来完成，这种安装方式通常是用来安装远程分公司所需的RODC。

- 第1阶段：新建RODC账户。此阶段通常是在总公司内执行，且需由Domain Admins组内的用户来完成，也就是只有域系统管理员才有权限来执行这一阶段的工作。

Download at http://www.pin5i.com/

在这个阶段内，系统管理员需在Active Directory数据库内为RODC新建计算机账户、设置选项、将第2阶段的安装工作委派给指定的用户或组。

- 第2阶段：将服务器附加到RODC账户。此阶段通常是在分公司内执行，被委派的用户或组有权限在这个阶段来完成安装RODC的工作。被委派的用户或组并不需要具备域系统管理员的权限。如果在总公司的域系统管理员并没有委派其他用户或组的话，则只有Domain Admins或Enterprise Admins组内的用户有权限执行这个阶段的安装工作。在这个阶段内，被委派的用户需要在远程分公司内将即将成为RODC的服务器**附加**（Attach）到第1个阶段中所新建的计算机账户，以便完成RODC的安装工作。

2-6-1 使用Windows窗口创建RODC账户

一般来说，阶段式安装主要是用来在远程分公司安装RODC，也就是在另外一个AD DS站点内安装RODC，不过为了方便起见，本节假设它是被安装到同一个站点内，也就是默认的站点Default-First-Site-Name（后面章节会介绍如何创建更多的站点）。

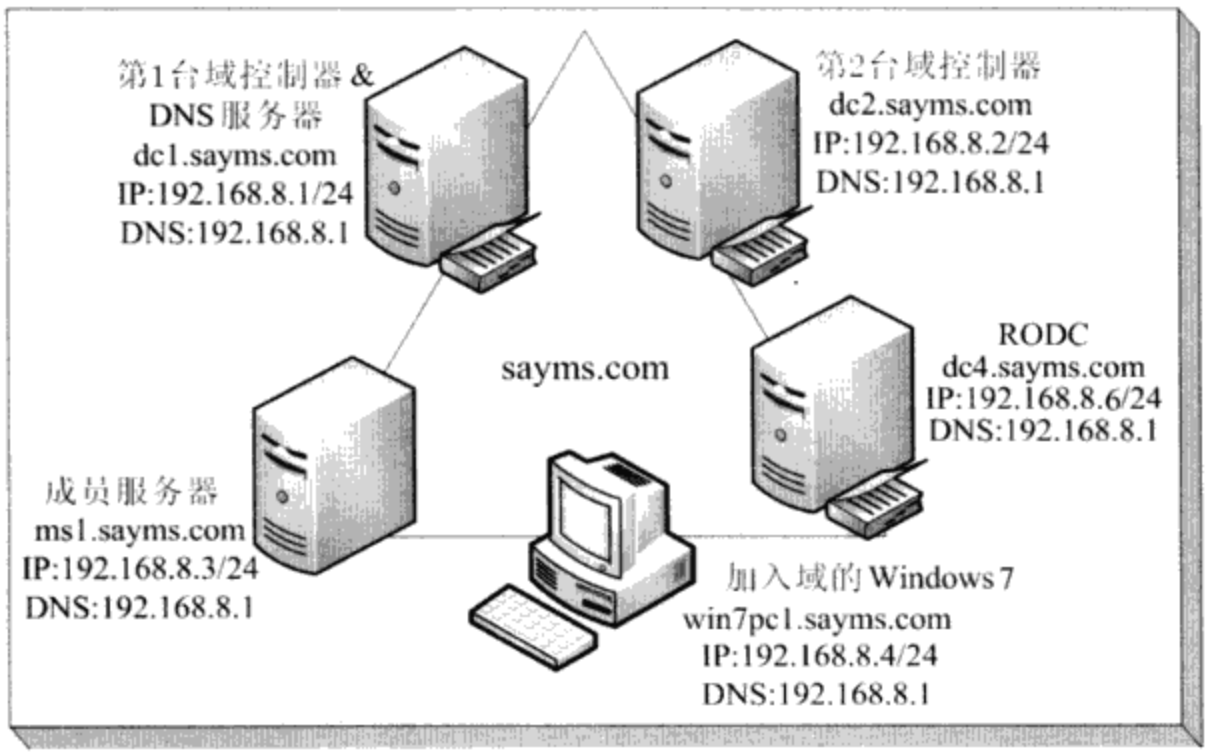


图2-65

STEP 1 请先在图 2-65中右边的服务器dc4.sayms.com上安装Windows Server 2008 R2，将其计算机名设置为dc4，IPv4地址等依照图中所示来设置（此处采用TCP/IPv4）。注意这台计算机目前不可以加入域。请将其计算机名设置为dc4即可，等升级为域控制器后，它会自动被改为dc4.sayms.com。

STEP 2 请到现有的一台域控制器上使用域系统管理员身份登录。

STEP 3 通过【开始➲管理工具➲Active Directory用户和计算机（或**Active Directory管理中心**）➲如图 2-66所示对着容器Domain Controllers右击➲预创建只读域控制器账户】的方式设置。

Download at http://www.pin5i.com/

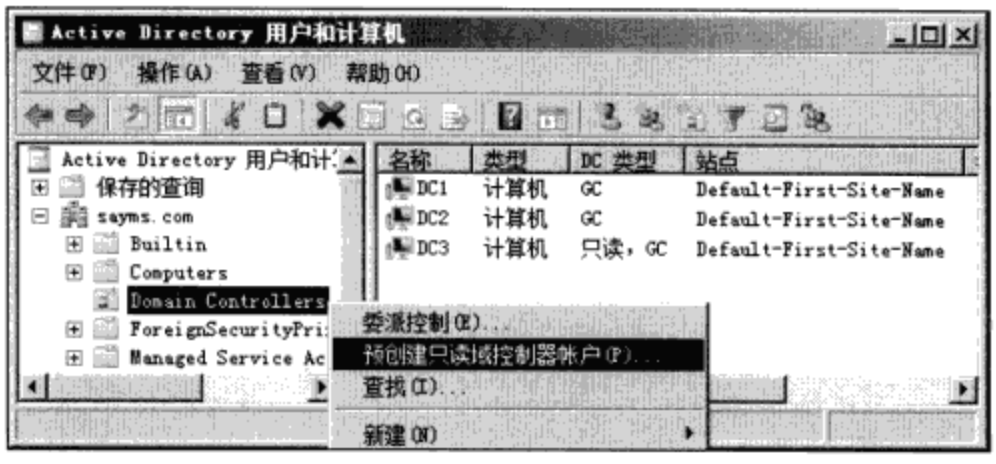


图 2-66

STEP 4 如图 2-67所示选择**使用高级模式安装**复选框后单击 下一步 按钮。

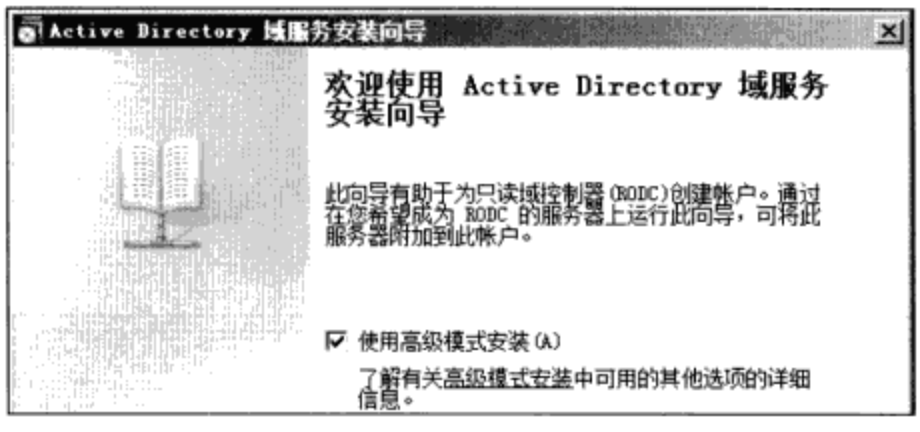


图 2-67

STEP 5 当出现**操作系统兼容性**界面时单击 下一步 按钮。

STEP 6 目前登录的用户为域Administrator，它有权限安装域控制器，故请在图 2-68中选择**我的当前登录凭据**单选按钮后单击 下一步 按钮。

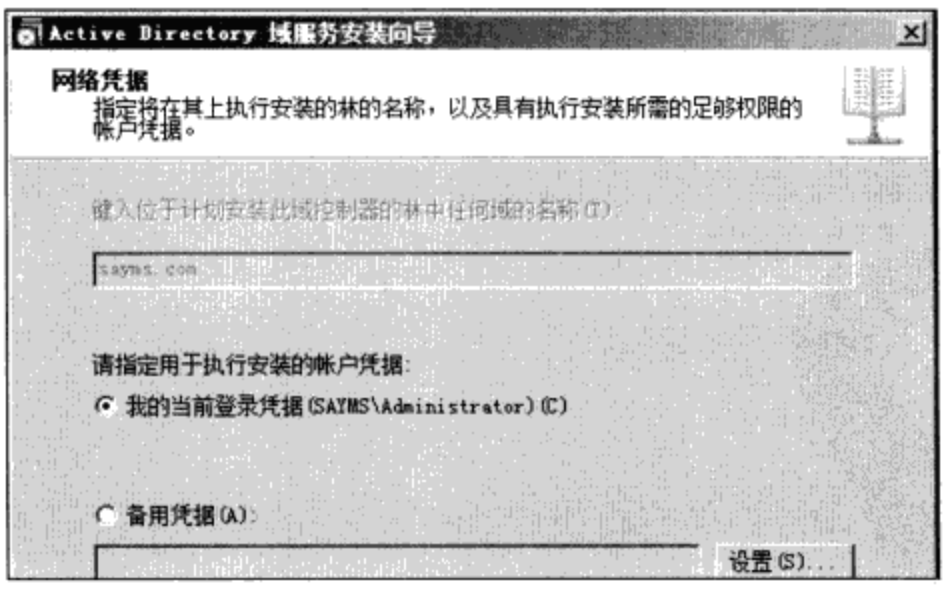


图 2-68

注意

若目前所登录的用户没有权限安装域控制器的话，请选择图中的**备用凭据**单选按钮，然后通过单击 设置 按钮来输入有权限的用户名与密码。

Download at http://www.pin5i.com/

STEP 7 在图 2-69中输入即将扮演RODC角色的服务器的计算机名，例如dc4，完成后单击下一步按钮。

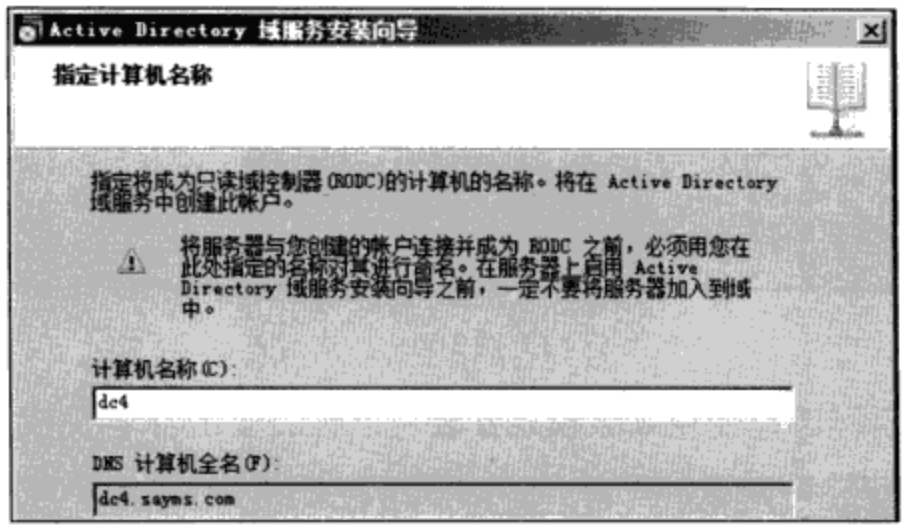


图2-69

STEP 8 在图 2-70中选择新域控制器所在的AD DS站点，目前只有一个默认的站点Default-First-Site-Name，请直接单击下一步按钮。

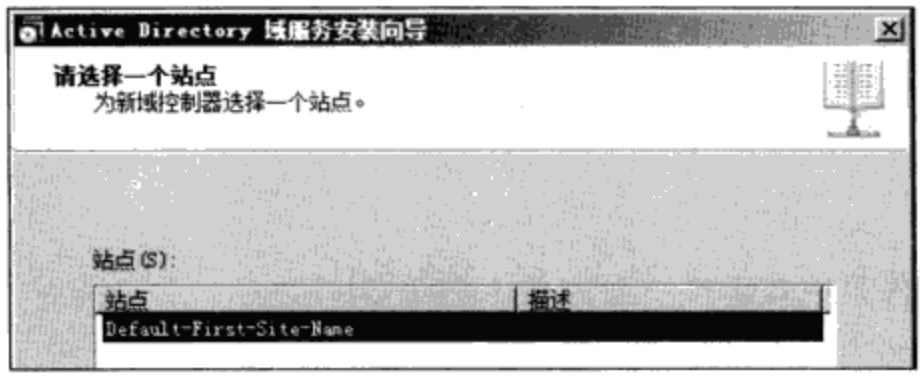


图2-70

STEP 9 在图 2-71中直接单击下一步按钮。由图中可知它会在这台服务器上安装DNS服务器，同时会将其设置为**全局编录**，并自动选择**只读域控制器 (RODC)**。

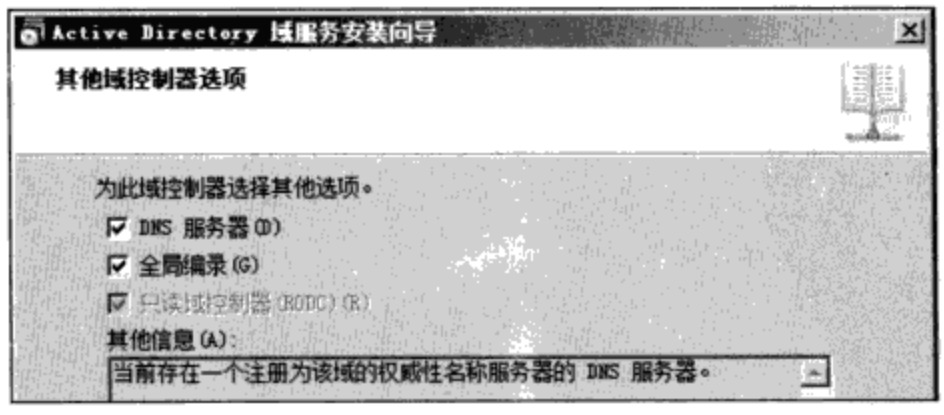


图2-71

STEP 10 通过图2-72来设置**密码复制策略**，图中默认值是没有任何用户的密码被允许复制到RODC，而且一些重要账户（例如Administrators、Server Operators等组内的用户）的密码已明确的被拒绝复制到RODC。虽然图中已经允许Allowed RODC Password

Download at http://www.pin5i.com/

Replication Group组内的用户密码可以被复制到RODC，不过此组内默认并没有任何成员。您可以通过单击添加按钮来添加密码可以被复制到RODC的用户账户（或是将用户账户加入到Allowed RODC Password Replication Group组内），单击下一步按钮。

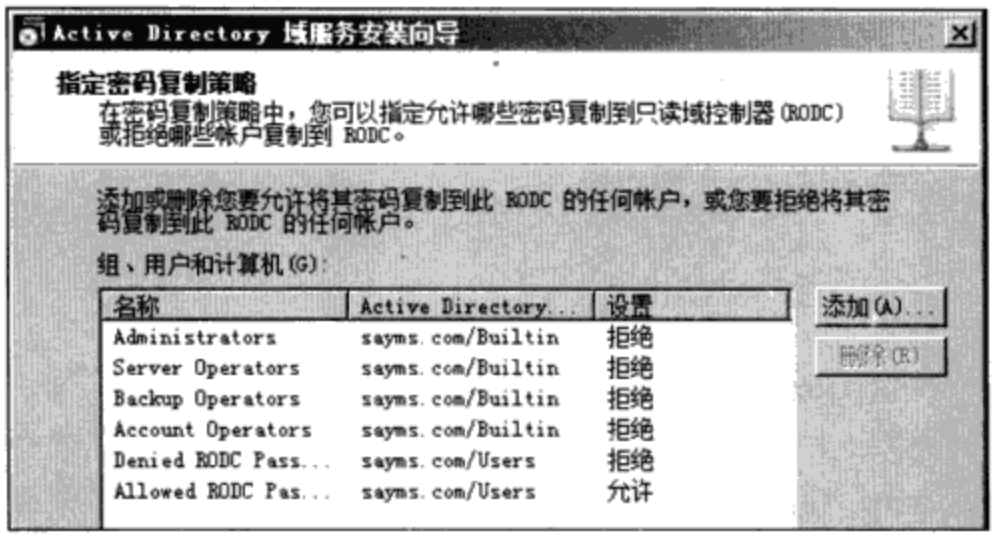


图2-72

提示

在安装域中的第1台RODC时，系统会自动创建与RODC有关的组账户，这些账户会通过AD DS的复制机制自动复制给其他域控制器，不过可能需要花费一点时间，尤其是复制给位于不同站点的域控制器。之后您在其他站点安装RODC时，若安装向导无法从这些域控制器得到这些组信息的话，它会显示警告信息，此时请等这些组信息完成复制后，再继续安装这台RODC。

STEP 11 在图 2-73中将安装RODC的工作委派给指定的用户或组，例如图中将其委派给域（SAYMS）用户George。RODC安装完成后，该用户在此台RODC内会自动被赋予本地系统管理员的权限。若您没有在界面中委派用户或组的话，则只有Domain Admins或Enterprise Admins组内的用户有权限执行安装（附加）此RODC的工作。

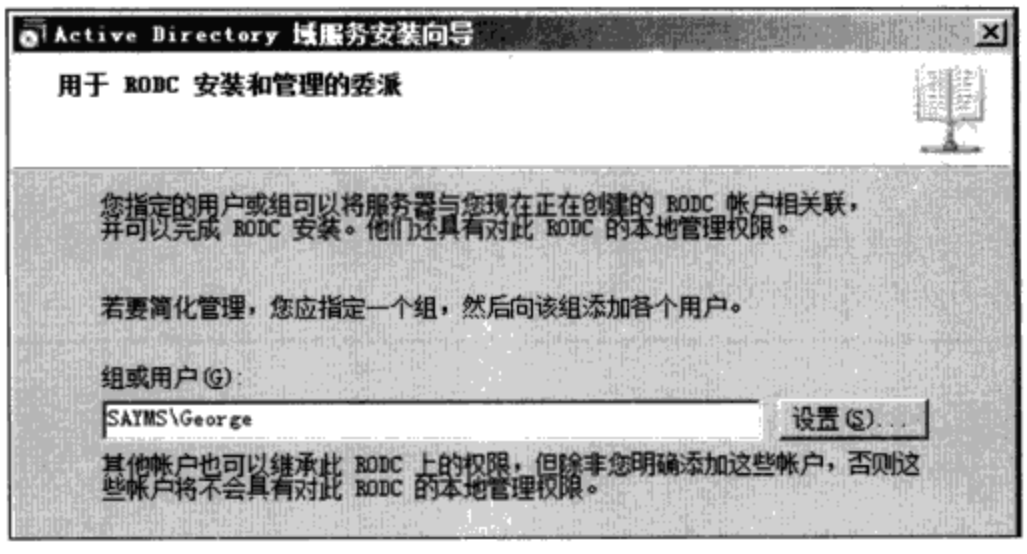


图2-73

Download at http://www.pin5i.com/

STEP 12 在图 2-74中直接单击下一步按钮。您可以单击导出设置按钮来将设置存储为**应答文件**（Answer File），以后如果有需要的话，可以使用此文件来创建RODC账户。

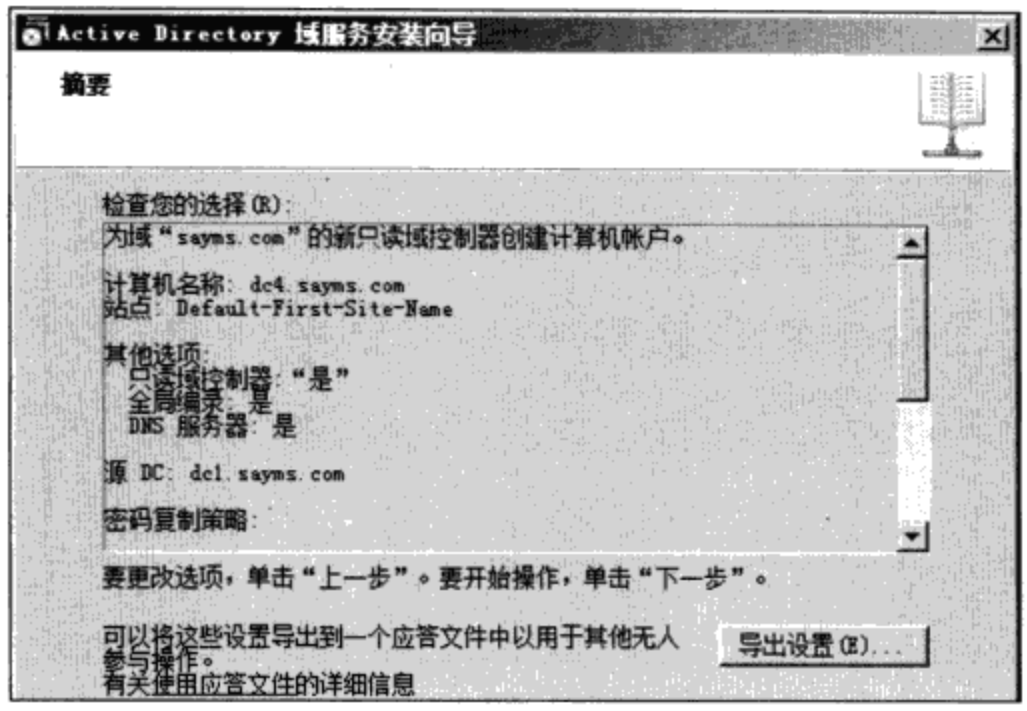


图2-74

STEP 13 在**完成Active Directory域服务安装向导**界面中单击下一步按钮。

STEP 14 图 2-75为完成后的界面。

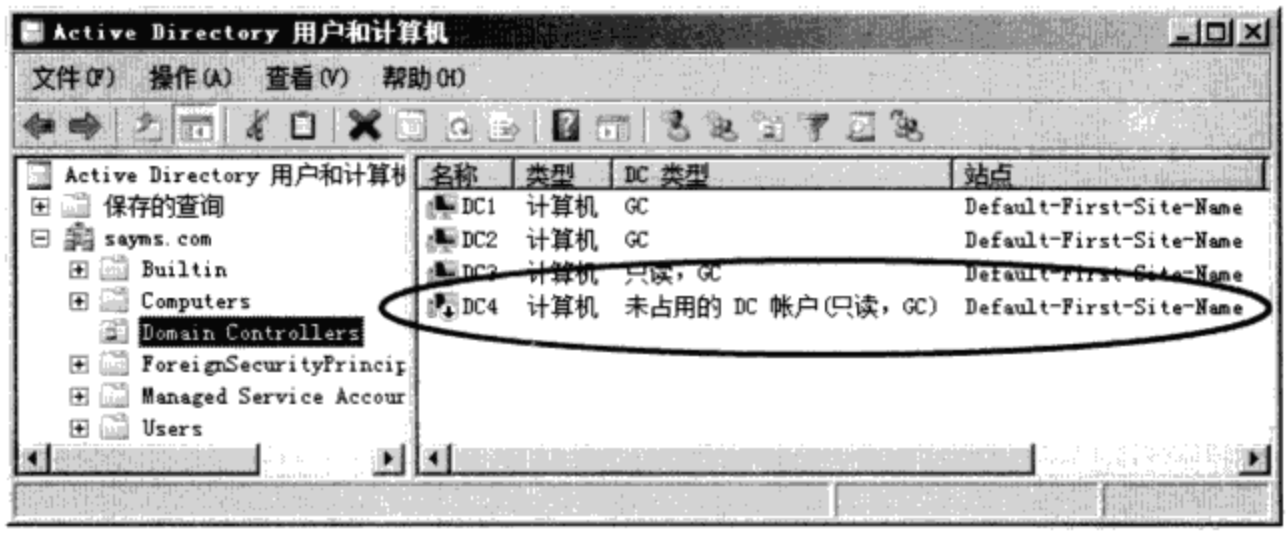


图2-75

提示

本节不再介绍如何使用应答文件与命令行来创建RODC账户，可参考图2-74中通过导出设置按钮所创建的应答文件。

2-6-2 将服务器附加到RODC账户

STEP 1 到即将成为RODC的服务器上使用系统管理员的身份登录，然后打开**命令提示符**窗口（或单击左下角的**Windows PowerShell**图标）。

Download at http://www.pin5i.com/

STEP 2 如图 2-76所示运行**dcpromo /UseExistingAccount:Attach**。



图2-76

STEP 3 如图 2-77所示选择**使用高级模式安装**复选框后单击下一步按钮。

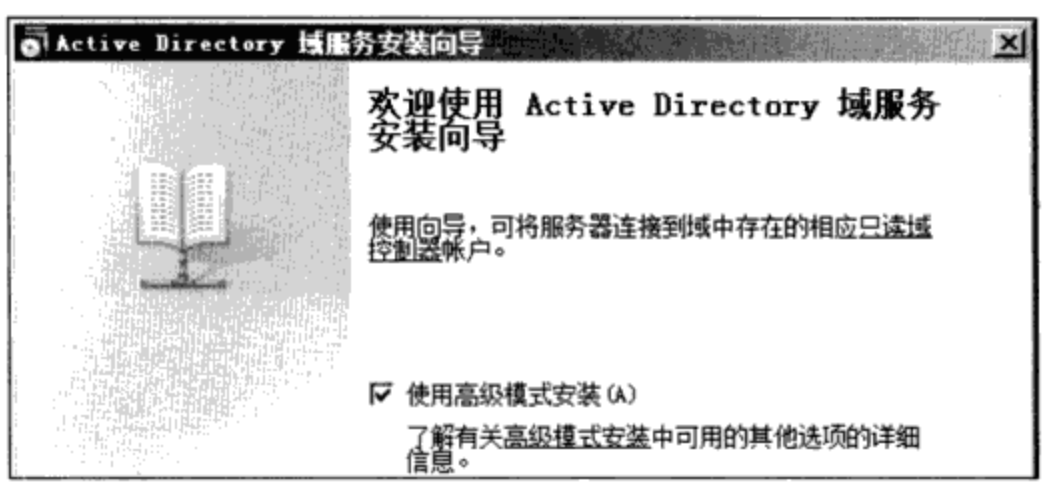


图2-77

提示

若您没有通过安装媒体或指定源域控制器来复制Active Directory数据库的话，可以不选择**使用高级模式安装**复选框。

STEP 4 在图 2-78中【输入域名sayms.com➲单击设置按钮➲输入被委派的用户名（george）和密码后单击确定按钮➲单击下一步按钮】。



图2-78

Download at http://www.pin5i.com/

注意

可输入被委派的用户账户、Enterprise Admins或Domain Admins组内的用户账户。

STEP 5 在图 2-79中选择Active Directory数据库中与这台服务器相对应的RODC计算机账户后单击下一步按钮。

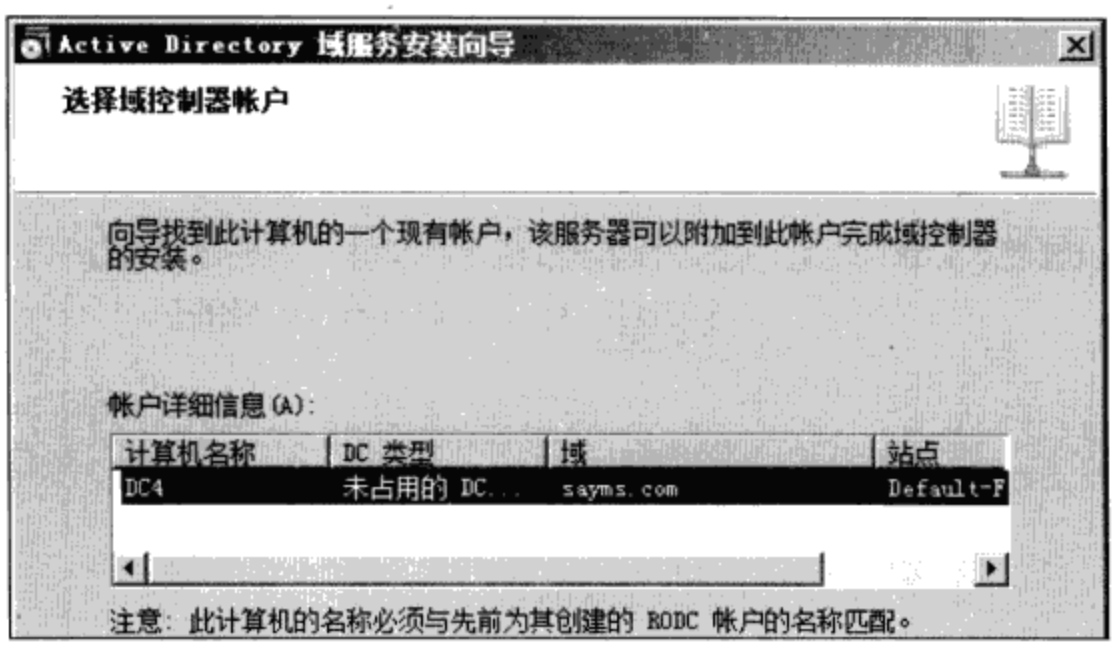


图2-79

STEP 6 在图 2-80中选择**通过网络从现有域控制器复制数据库**单选按钮。您也可以通过**介质**来安装，不过需要先制作**安装媒体**，其方法请参考**制作安装媒体**的相关内容。

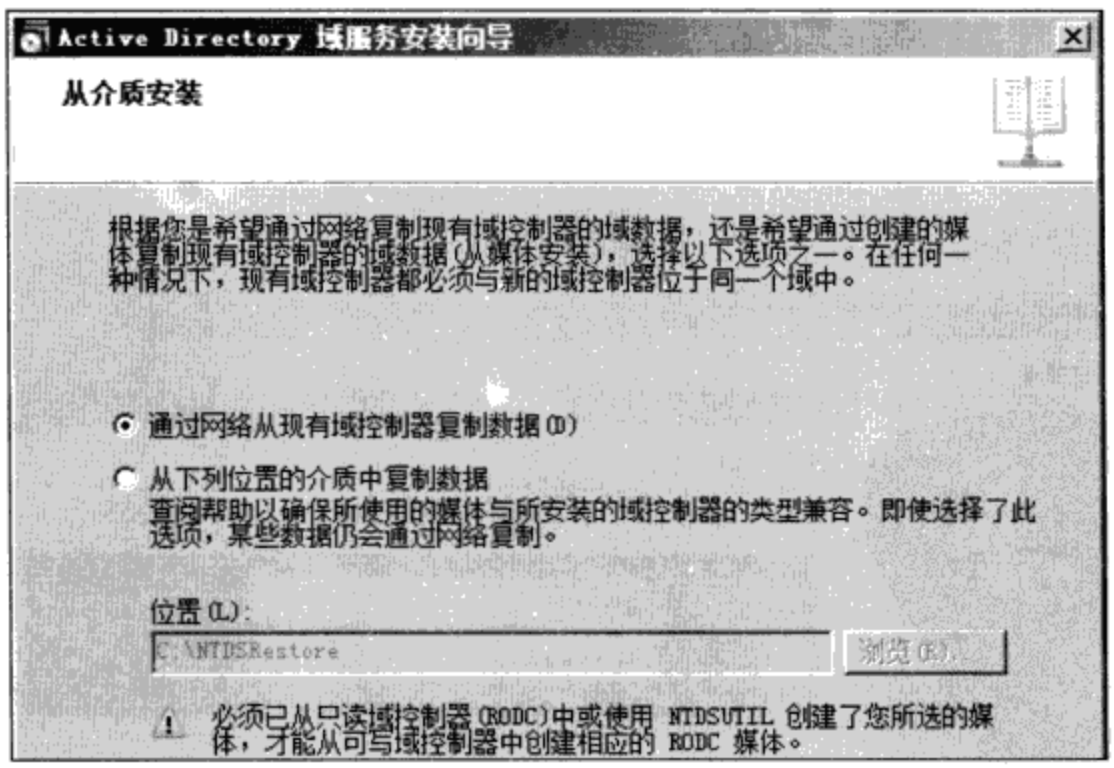


图2-80

STEP 7 在图 2-81中单击下一步按钮让向导自动选择Active Directory数据库的源域控制器（或手动选择特定的域控制器）。

Download at http://www.pin5i.com/

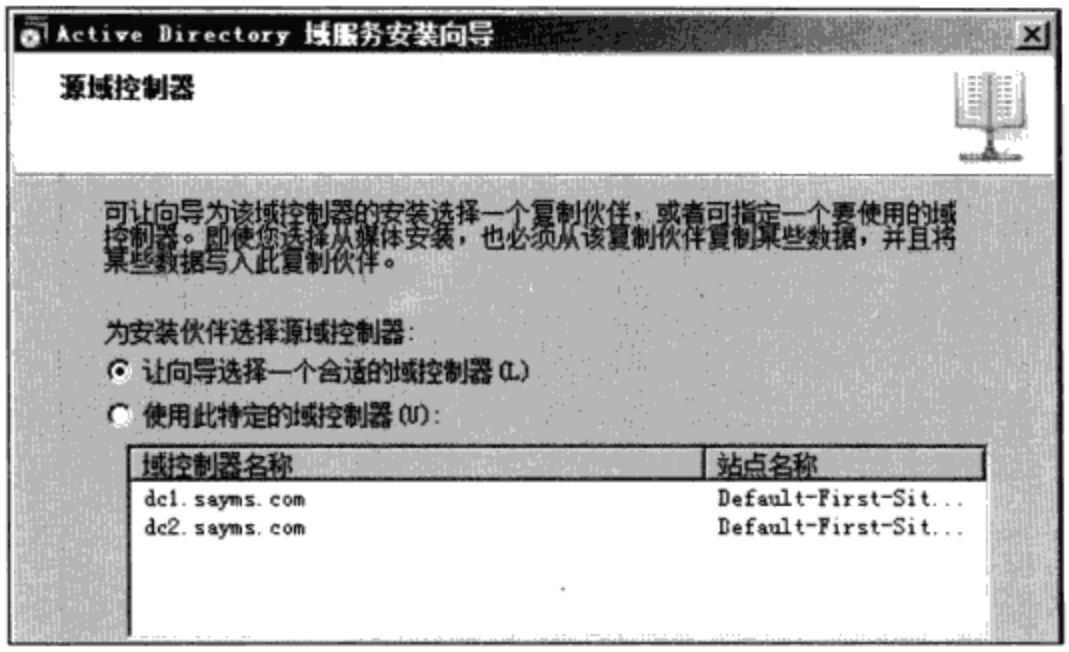


图 2-81

STEP 8 在图 2-82中直接单击下一步按钮。

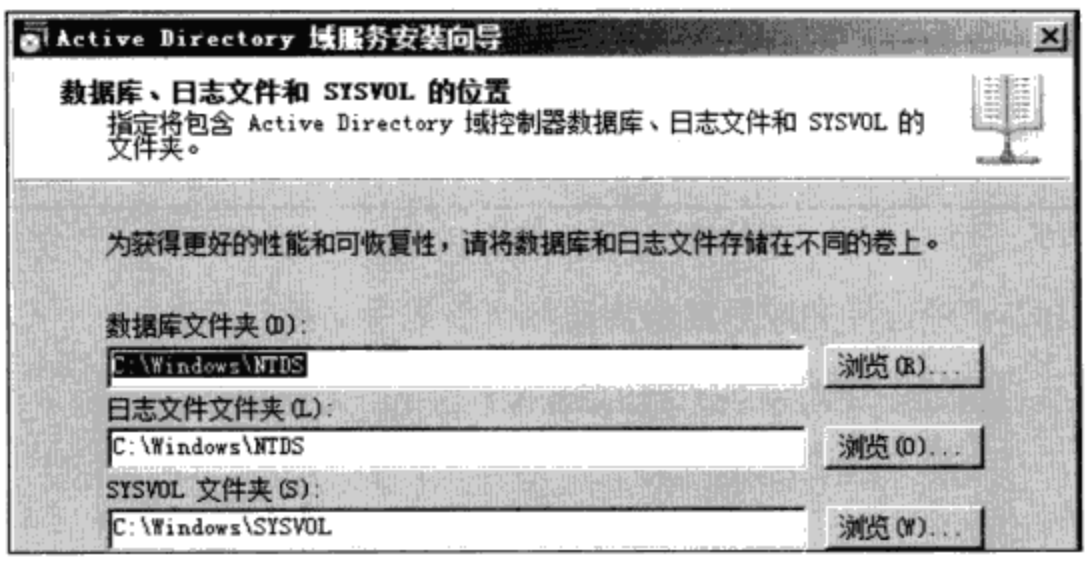


图 2-82

STEP 9 在图 2-83中设置目录服务还原模式的系统管理员密码，完成后单击下一步按钮。

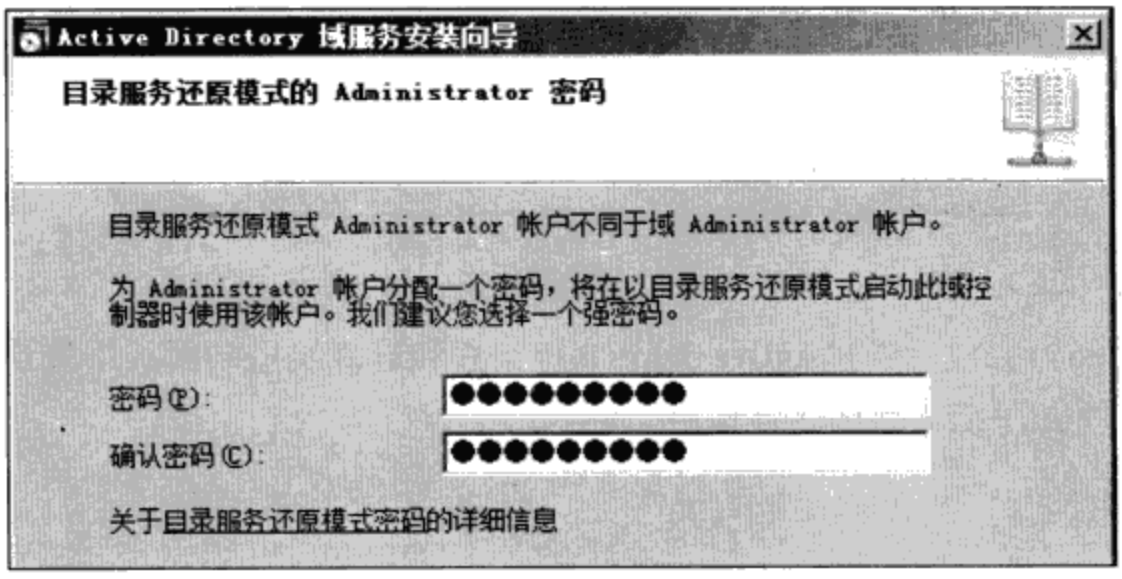


图 2-83

Download at http://www.pin5i.com/

STEP 10 在图 2-84中直接单击下一步按钮。

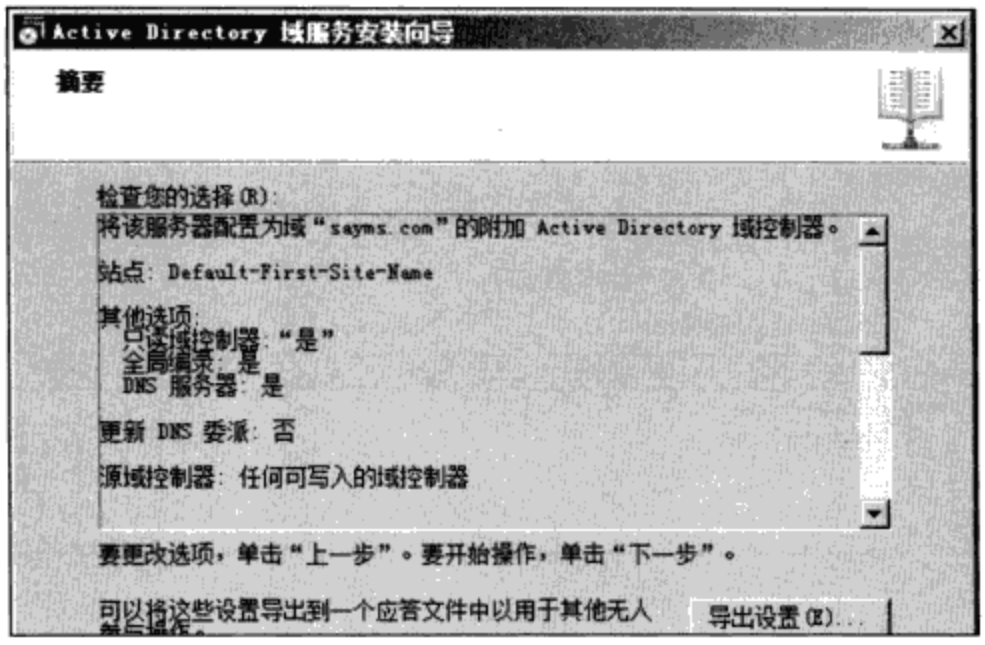


图 2-84

提示

您可以单击导出设置按钮来将设置存储为**应答文件**（Answer File），它可供利用dcpromo.exe来安装只读域控制器时使用。

STEP 11 可在图 2-85中选择**完成后重新启动**复选框或手动重新启动。

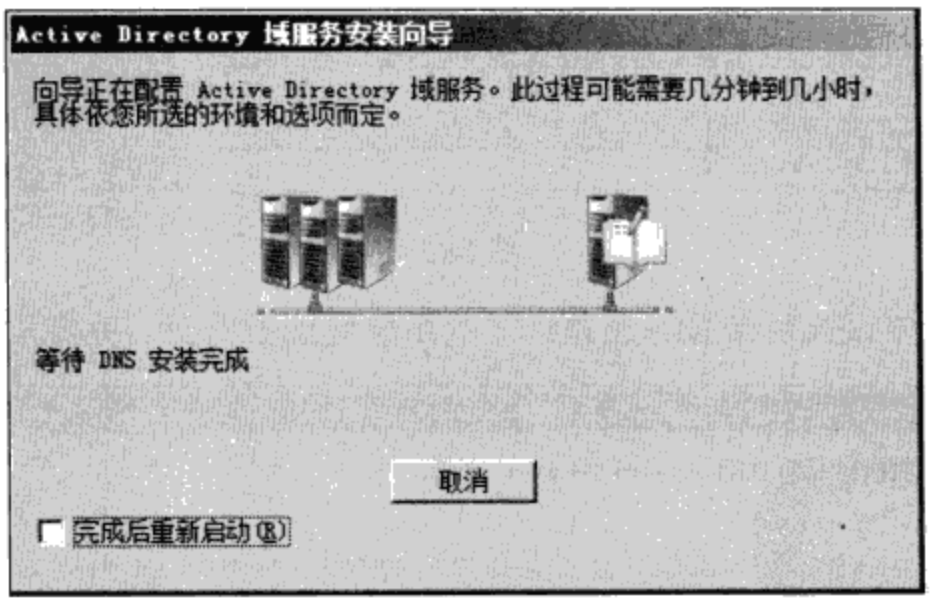


图 2-85

STEP 12 图2-86为完成后通过**Active Directory用户和计算机**控制面板所看到的界面，其中DC4图形上原本的向下箭头已消失。

Download at http://www.pin5i.com/

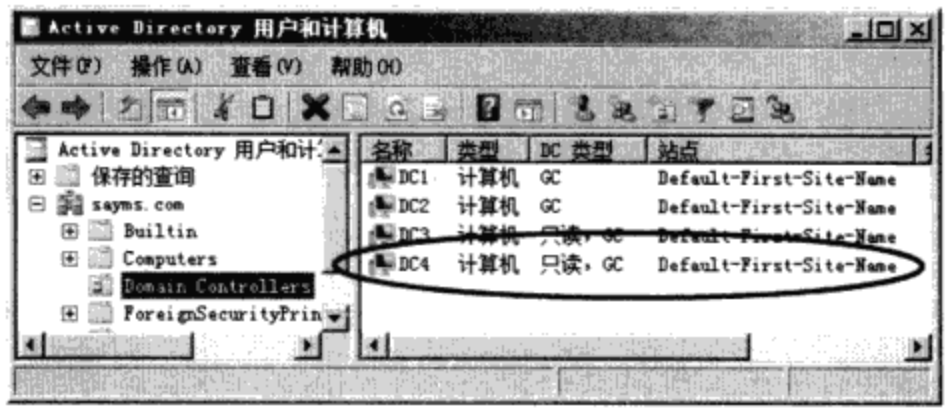


图 2-86

2-7 将Windows计算机加入或脱离域

Windows系统的计算机加入域后，便可以访问Active Directory数据库和其他域资源，例如用户可以在这些计算机上使用域用户账户来登录域和访问域内其他计算机内的共享文件夹。以下Windows 计算机都可以被加入域：

- Windows Server 2008 R2、Windows Server 2008。
- Windows Server 2003 R2、Windows Server 2003。
- Windows 7 Ultimate、Windows 7 Enterprise、Windows 7 Professional。
- Windows Vista Ultimate、Windows Vista Enterprise、Windows Vista Business。
- Windows XP Professional。
- Windows 2000 Server、Windows 2000 Professional。

2-7-1 将Windows计算机加入域

下面要将图 2-87左下角的服务器ms1加入域，假设它是Windows Server 2008 R2；同时也要将右下角的Windows 7计算机加入域，假设它是Windows 7 Professional。以下使用服务器ms1（Windows Server 2008 R2）为例进行说明。

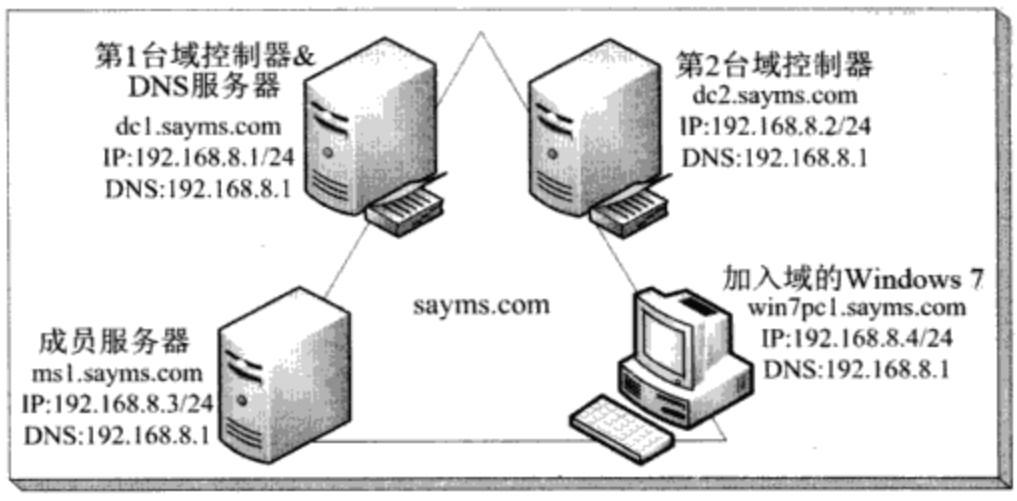


图 2-87

Download at http://www.pin5i.com/

提示

加入域的客户端计算机，其计算机账户默认会自动被创建在容器Computers内，如果您希望将此计算机账户放置到其他容器或组织单位的话，可以事先在该容器或组织单位内创建此计算机账户，可通过【对着该容器或组织单位右击➲添加➲计算机➲输入计算机名】的方式设置。

STEP 1 请先将该台计算机的计算机名设置为ms1，IPv4地址等设置如图 2-87所示（此处选择TCP/IPv4）。等加入域后，计算机名自动会被改为ms1.sayms.com。

STEP 2 通过【开始➲对着**计算机**右击➲属性➲如图 2-88所示单击**更改设置**选项】的方式进行设置。

注意

必须是Administrator才有权限更改设置。因为Windows Server 2008 R2或Windows 7计算机默认已经启用**用户账户控制**，故若您不是Administrator的话，它会先要求您输入Administrator的密码。

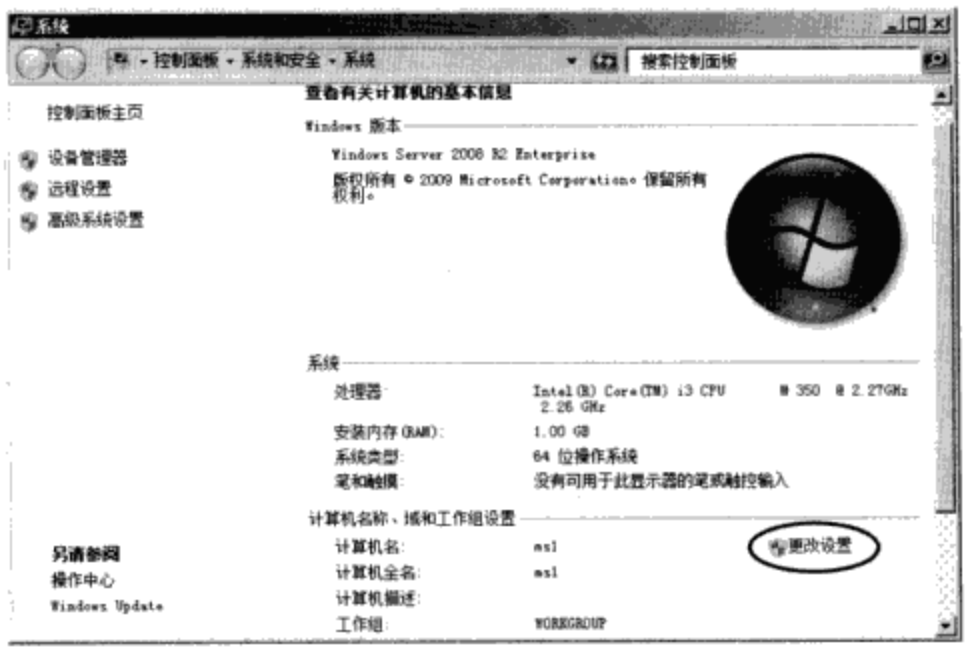


图 2-88

STEP 3 单击图 2-89中的更改按钮。

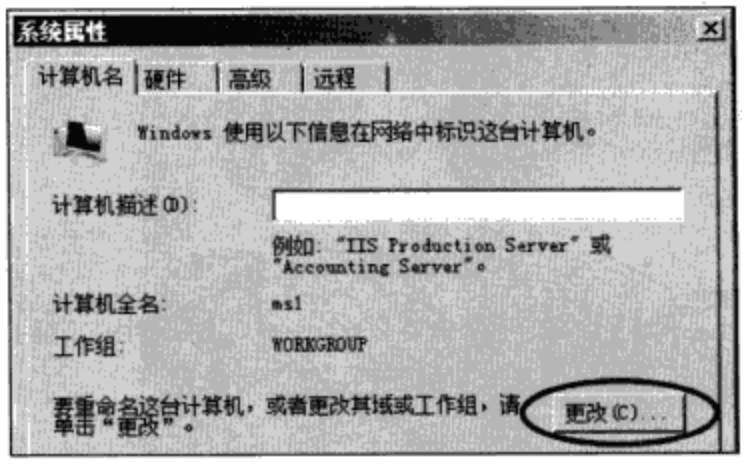


图 2-89

Download at http://www.pin5i.com/

STEP 4 通过【选择图2-90中的**域**➲输入域名sayms.com➲单击确定按钮➲输入Administrator与其密码➲单击确定按钮】的方式进行设置。



图2-90

注意

1. 若出现错误警告界面的话，请检查**首选DNS服务器**是否设置了正确的IP地址。
2. 可输入任何一个域用户名与密码，不过这些账户都只有10次将计算机加入域的机会，但是系统管理员没有次数限制。

STEP 5 若出现类似图 2-91的对话框，表示加入域成功，请单击确定按钮。



图2-91

注意

若出现错误界面的话，请检查所输入的用户名与密码是否正确。

STEP 6 在出现提醒您需要重新启动计算机的界面时单击确定按钮。

STEP 7 返回到图 2-92中可看出，加入域后，其完整计算机名的后缀就会附上域名，如图中的ms1.sayms.com，单击关闭按钮。

Download at http://www.pin5i.com/

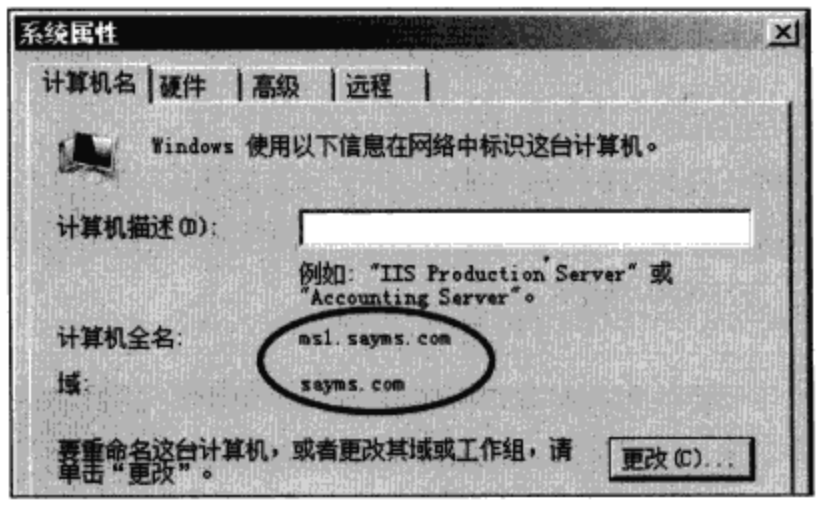


图2-92

STEP 8 依照界面提示重新启动计算机。

STEP 9 请重复以上步骤将图 2-87中的Windows 7计算机加入域。

2-7-2 使用已加入域的计算机登录

您可以在已经加入域的计算机上，使用本地或域用户账户来登录。

1. 使用本地用户账户登录

在登录界面中单击Ctrl + Alt + Del 键后，将出现如图 2-93所示的界面，图中默认是让您使用本地系统管理员Administrator的身份登录，因此您只要输入本地Administrator的密码就可以登录。

此时系统会使用本地安全性数据库来检查用户名与密码是否正确，若正确，您就可以登录成功，也可以访问此计算机内的资源（若有权限的话），不过无法访问域上其他计算机的资源，除非在连接其他计算机时另外再输入有权限的用户名与密码。

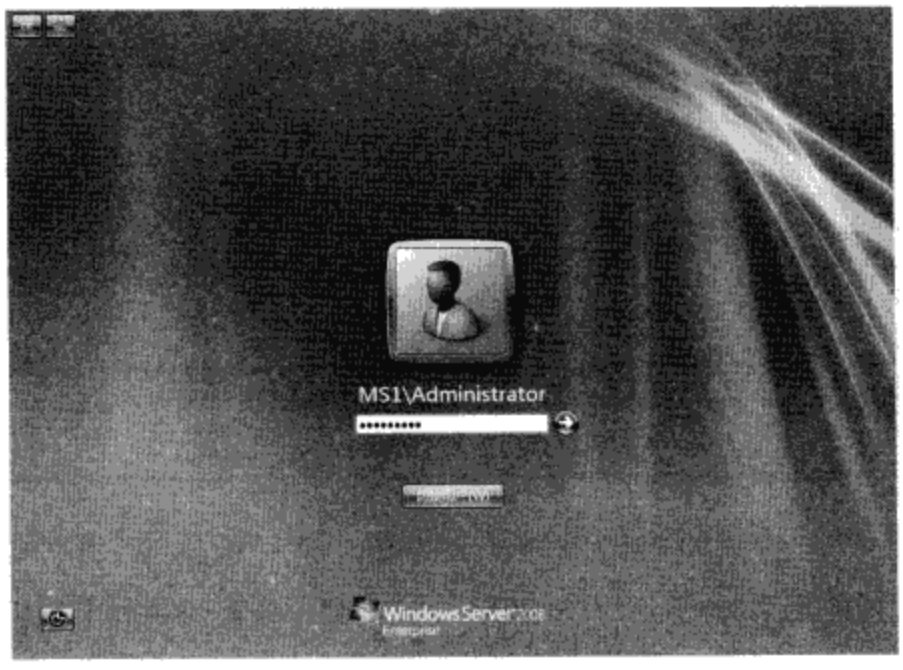


图2-93

Download at http://www.pin5i.com/

2. 使用域用户账户登录

如果要改用域系统管理员Administrator的身份登录的话，可通过【单击图2-93中的**切换用户**按钮➲单击**其他用户**➲如图 2-94所示输入域系统管理员的账户（sayms\administrator）与密码】的方式来登录。

注意账户名称前要加上域名**sayms.com**或**sayms**，例如sayms.com\Administrator或sayms\Administrator，此时账户与密码将会被传送给域控制器，并使用Active Directory数据库来检查用户名与密码是否正确，若正确，您就可以登录成功，并且可以直接连接域内的任何一台计算机与访问其内的资源（若有权限的话），不需要再另外手动输入用户名与密码。

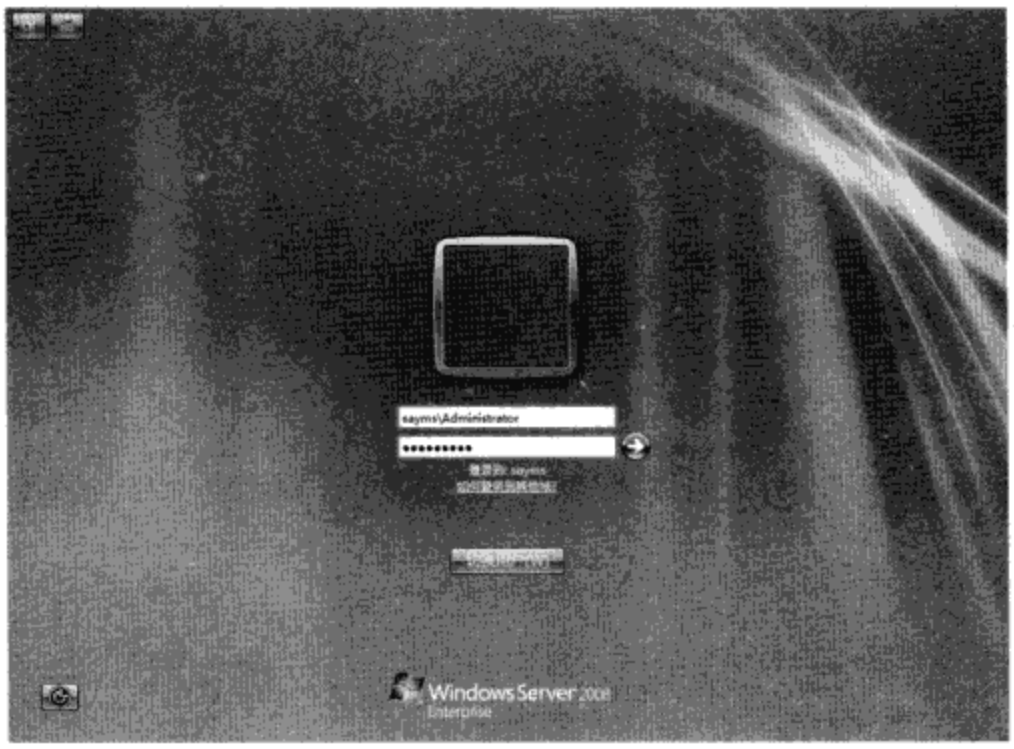


图2-94

2-7-3 脱机加入域

以前旧版的Windows客户端计算机若要加入域的话，该计算机需连上网络，而且必须能够直接与域控制器通信，现在的Windows Server 2008 R2与Windows 7计算机具备脱机加入域的功能（Offline Domain Join），也就是让它们在并未与域控制器连接的情况下，就可以被加入域。我们需要通过运行**djoin.exe**程序来运行脱机加入域的程序。

我们需要到一台已经加入域的Windows Server 2008 R2或Windows 7计算机上，使用djoin.exe来创建一个文本文件，此文件内包含即将加入域的计算机所需的所有信息。接着到即将加入域的脱机计算机上（Windows Server 2008 R2或Windows 7），使用djoin.exe来将上述文件内的信息导入到此计算机内。

以下假设域名为sayms.com，一台已经加入域的成员服务器为ms1，即将脱机加入域的计算机为win7pc2。为了实际演练脱机加入域功能，因此请确认win7pc2是处于脱机状态。脱机将

Download at http://www.pin5i.com/

win7pc2加入域的步骤如下所示：

STEP 1 到成员服务器ms1上运行以下的djoin.exe程序（参考图 2-95），它会创建一个文本文件，此文件内包含脱机计算机win7pc2所需的所有信息，其中sayms.com为域名、win2pc2为脱机计算机的计算机名、win7pc2.txt为所创建的文本文件。此命令默认会将计算机账户win7pc2创建到**Computers**容器内（如图 2-96所示）。

djoin /provision /domain sayms.com /machine win7pc2 /savefile win7pc2.txt

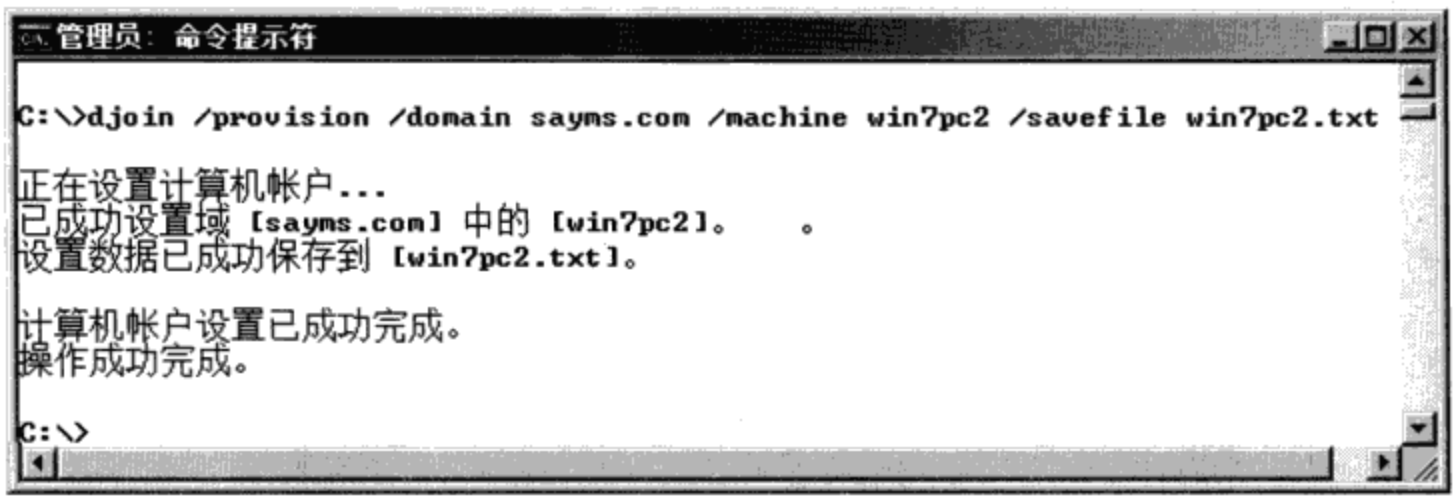


图 2-95

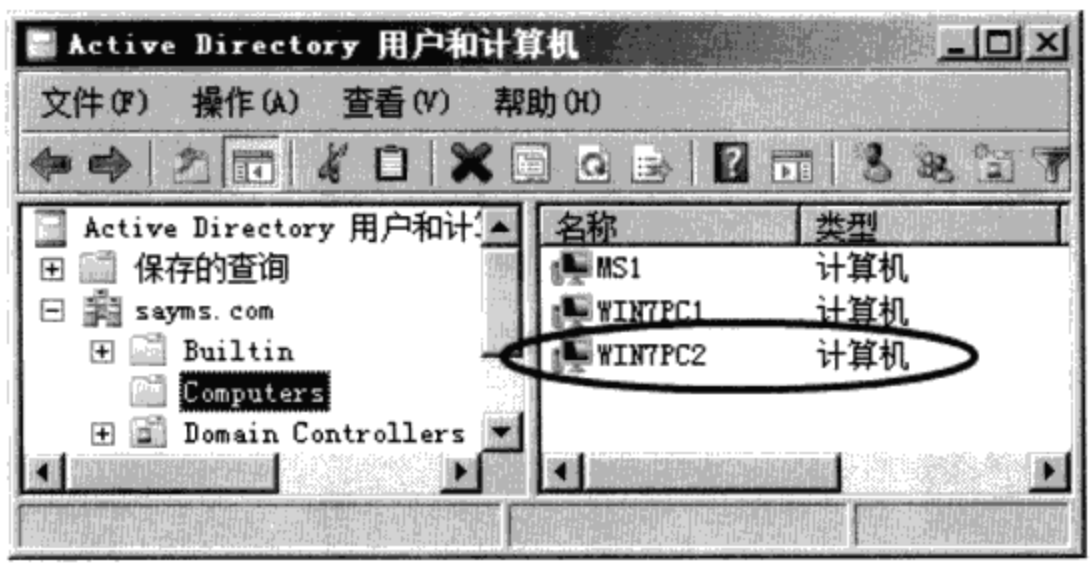


图 2-96

STEP 2 到即将加入域的脱机计算机win7pc2上使用djoin.exe来将上述文件内的信息导入到win7pc2。Windows 7计算机必须以系统管理员的身份来运行此程序，因此请选择【开始➲所有程序➲附件➲对着**命令提示符**右击➲以管理员身份运行】，然后运行以下命令（参见图 2-97）：

djoin /requestODJ /loadfile win7pc2.txt /windowspath %SystemRoot% /localos

Download at http://www.pin5i.com/

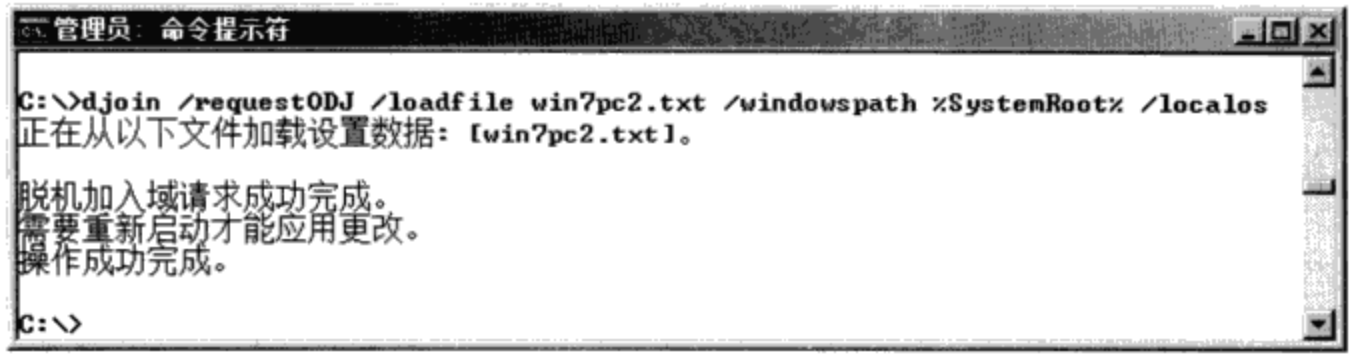


图 2-97

STEP 3 当win7pc2连上网络、可以与域控制器通信时，请重新启动win7pc2，它便完成了加入域的程序。

2-7-4 脱离域

脱离域的方法与加入域的方法大同小异，不过您必须是Enterprise Admins、Domain Admins的成员或本地系统管理员才有权限将此计算机脱离域。还有因为Windows Server 2008 R2或Windows 7计算机默认已经启用**用户账户控制**，因此若您没有权限更改此设置的话，系统会先要求您输入账户与密码。

脱离域的方法为：【开始➲对着**计算机**右击➲属性➲**更改设置**➲单击更改按钮➲选择图2-98中的**工作组**单选按钮➲输入适当的工作组名称（例如WORKGROUP）➲出现**欢迎加入工作组**界面时单击确定按钮➲重新启动计算机】。

提示

图中的工作组名称可以自行设置或输入网络上现有的工作组名称。将计算机设置为同一个工作组的好处之一是它让您在浏览网络上的计算机时，可以比较快速地找到同一个工作组内的计算机。

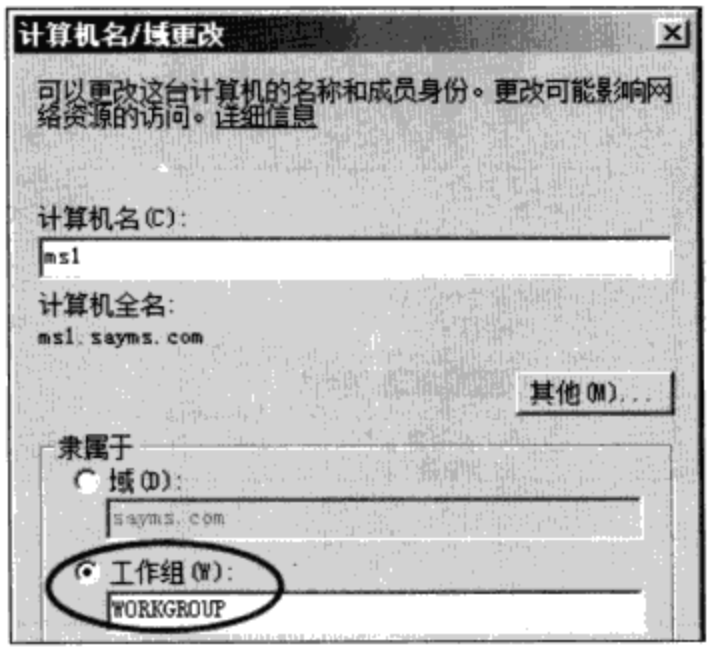


图 2-98

Download at http://www.pin5i.com/

接下来会出现如图 2-99所示的提示界面：一旦脱离域后，在这台计算机上只能够使用本地用户账户来登录，无法再使用域用户账户，因此请确认您知道本地系统管理员的密码后再单击**确定**按钮，否则请单击**取消**按钮。

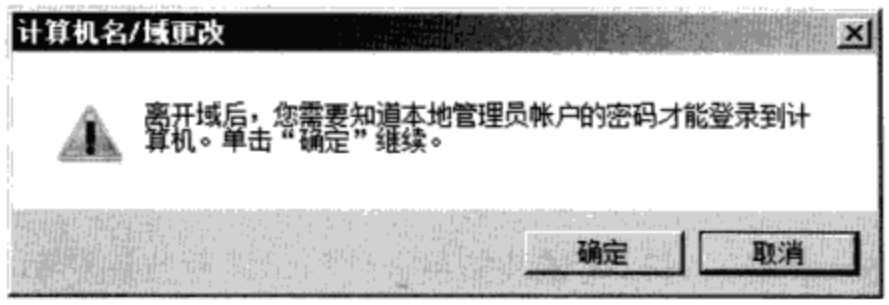


图 2-99

2-8 在域成员计算机内安装AD DS管理工具

非域控制器的Windows Server 2008 R2、Windows Server 2008、Windows 7 与Windows Vista等成员计算机内默认并没有管理AD DS的工具，因此需要另外安装这些工具。

2-8-1 在Windows Server 2008 R2计算机上安装AD DS管理工具

在Windows Server 2008 R2成员服务器内安装AD DS管理工具的方法为：【单击左下角的**服务器管理器**图标➲单击**功能**右方的**添加功能**➲展开图 2-100中的**远程服务器管理工具**➲角色管理工具➲选择**AD DS和AD LDS工具**➲…】，之后便可以在【开始➲管理工具】内选择**Active Directory用户和计算机**、**Active Directory管理中心**等工具。

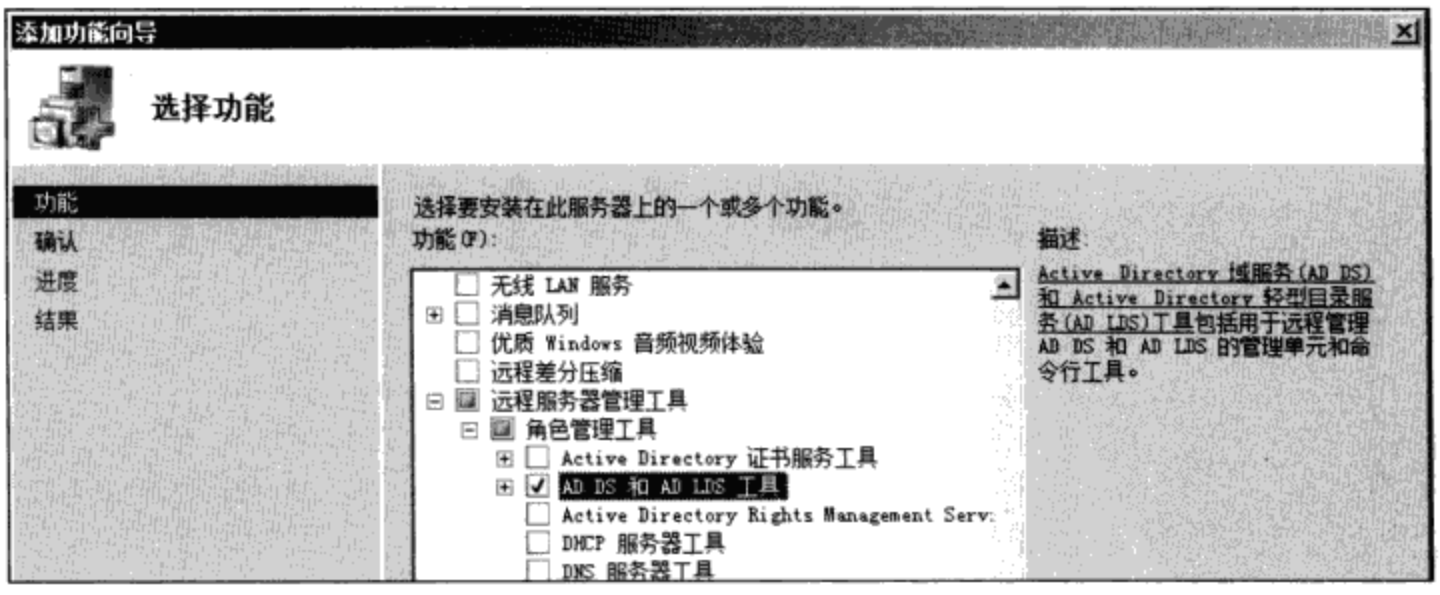


图 2-100

提示

只有域系统管理员才有权限管理AD DS，本地系统管理员无此权限。

Download at http://www.pin5i.com/

2-8-2 在Windows Server 2008 计算机上安装AD DS管理工具

在Windows Server 2008成员服务器内安装AD DS管理工具的方法为：【单击左下角的**服务器管理器**图标➲单击**功能**选项➲添加功能➲展开**远程服务器管理工具**➲展开**角色管理工具**➲如图 2-101所示选择**Active Directory 域服务工具**➲…】，完成后就可以在【开始➲管理工具】中选择**Active Directory用户和计算机控制台**等工具。

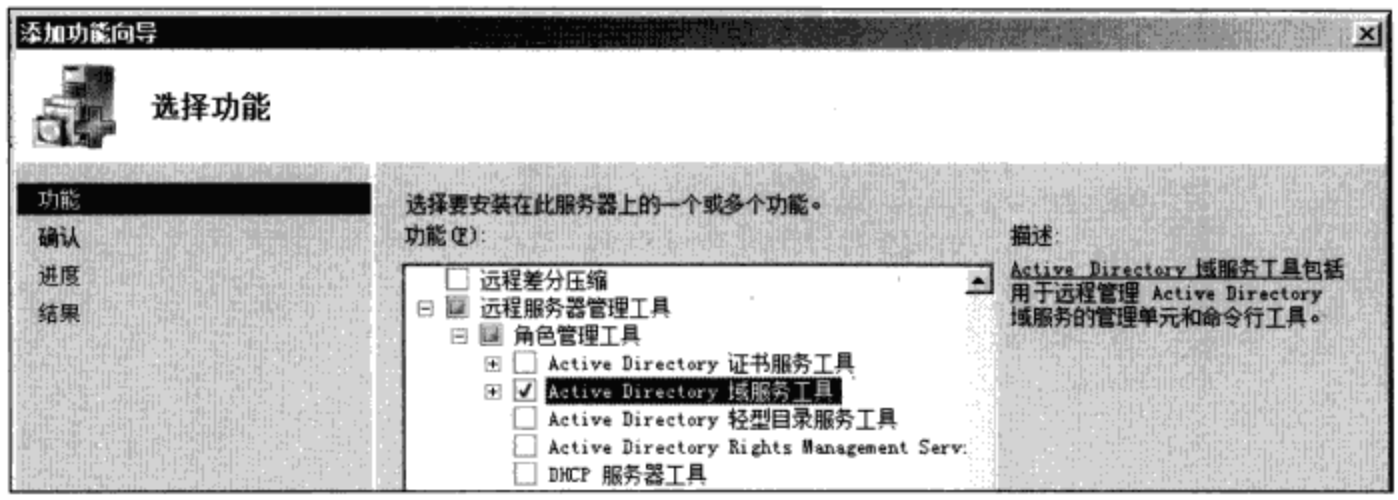


图 2-101

2-8-3 在Windows 7计算机上安装AD DS管理工具

请到微软网站下载与安装Remote Server Administration Tools for Windows 7，安装完成后选择【开始➲控制面板➲单击最下方的**程序**➲单击最上方的**打开或关闭Windows功能**➲在图2-102中选择所需的AD DS管理工具➲…】，之后便可在【开始➲管理工具】内来选择**Active Directory用户和计算机**、**Active Directory管理中心**等工具。

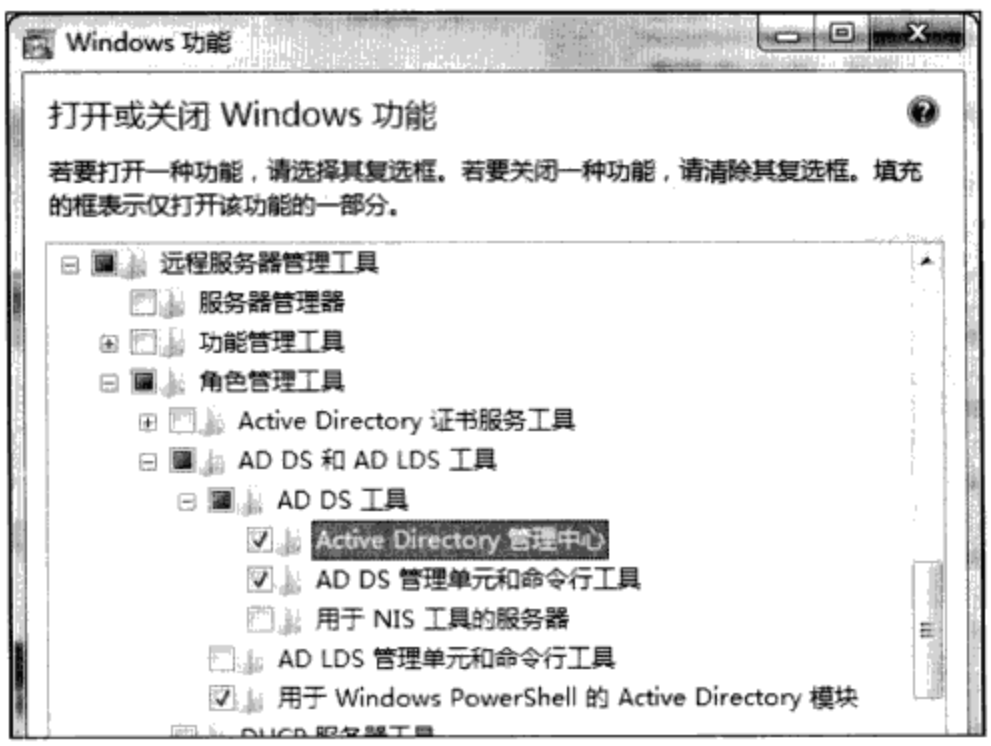


图 2-102

Download at http://www.pin5i.com/

若**管理工具**未显示在**开始**菜单中的话：【请对着屏幕左下角的**开始**按钮右击➲属性➲如图 2-103所示单击**「开始」菜单**右边的自定义按钮➲选择**系统管理工具**下的**在“所有程序”菜单和「开始」菜单上显示**】单选按钮，完成后就可以在【开始➲管理工具】或【开始➲所有程序➲管理工具】中来选择**Active Directory用户和计算机**、**Active Directory管理中心**等工具。

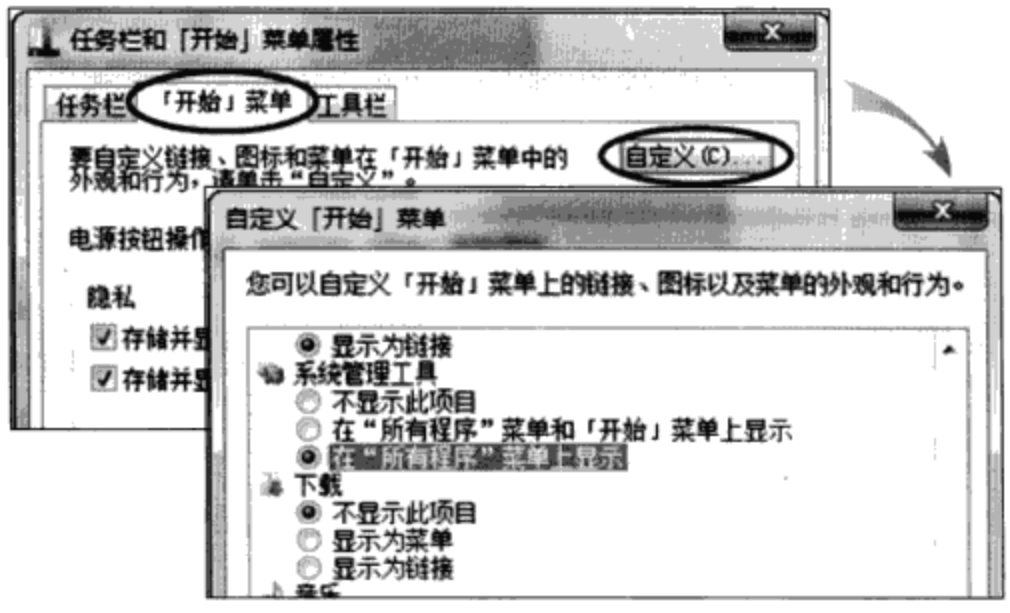


图 2-103

2-8-4 在Windows Vista计算机上安装AD DS管理工具

安装的前提是：需Windows Vista Service Pack 1（含）以上，且需到微软网站下载与安装Microsoft Remote Server Administration Tools for Windows Vista。安装完成后，请通过【开始➲控制面板➲单击最下方的**程序**➲单击最上方的**打开或关闭Windows功能**➲在图 2-104中展开**远程服务器管理工具**➲角色管理工具➲选择**Active Directory 域服务工具**➲单击确定按钮】的方法来安装。

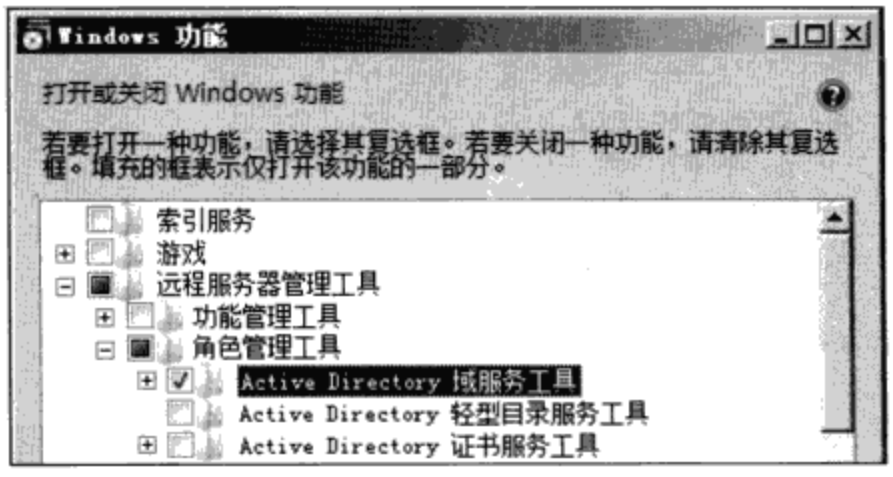


图 2-104

接着需要将**管理工具**的快捷方式显示在**开始**菜单中，可通过【对着屏幕左下角的**开始**按钮右击➲属性➲如图 2-105所示单击**「开始」菜单**右边的自定义按钮➲选择**系统管理工具**下

Download at http://www.pin5i.com/

的**在“所有程序”菜单和「开始」菜单上显示**单选按钮➲开始➲管理工具】的方式来选择**Active Directory用户和计算机**等工具。

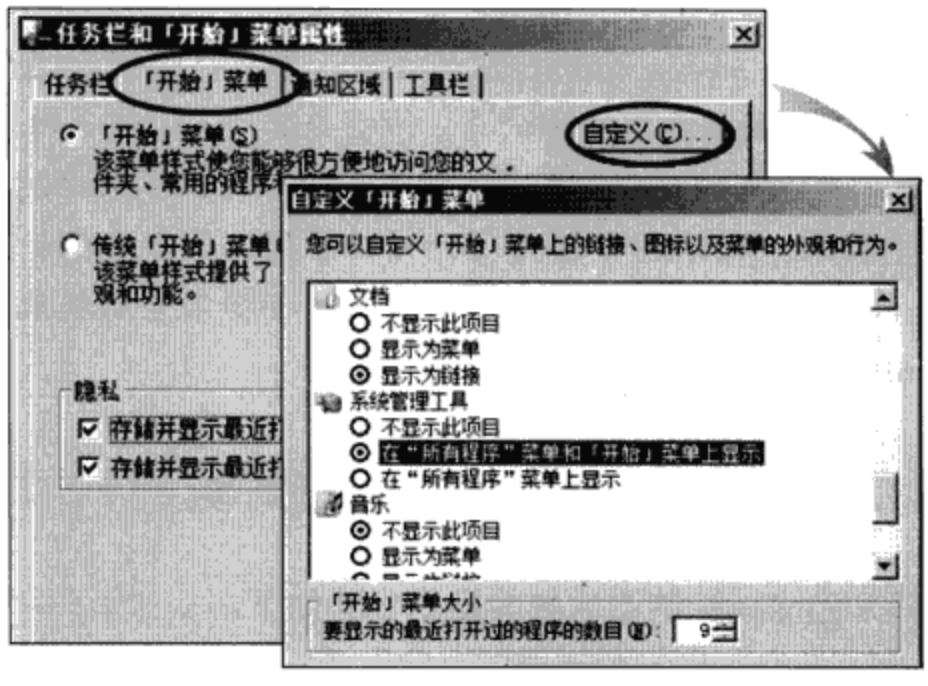


图 2-105

2-9 删除域控制器和域

您可以通过降级的方式来删除域控制器，也就是将AD DS 从域控制器内删除。在降级前请先注意以下事项：

- 若域内还有其他域控制器存在的话，则降级后会变为该域的成员服务器，例如将图2-106中的dc2.sayms.com降级的话，由于还有另外一台域控制器dc1.sayms.com存在，故dc2.sayms.com会被降级为域sayms.com的成员服务器，且其计算机账户会被从组织单位Domain Controllers转移到容器Computers内。您必须是Domain Admins或Enterprise Admins组的成员才有权限删除域控制器。
- 若这台域控制器是域内的最后一台域控制器，例如假设图 2-106中的 dc2.sayms.com已被降级，此时再将dc1.sayms.com降级的话，因为此域内已经没有其他域控制器存在了，故域会被删除，而dc1.sayms.com也会被降级为独立服务器。您必须是Enterprise Admins

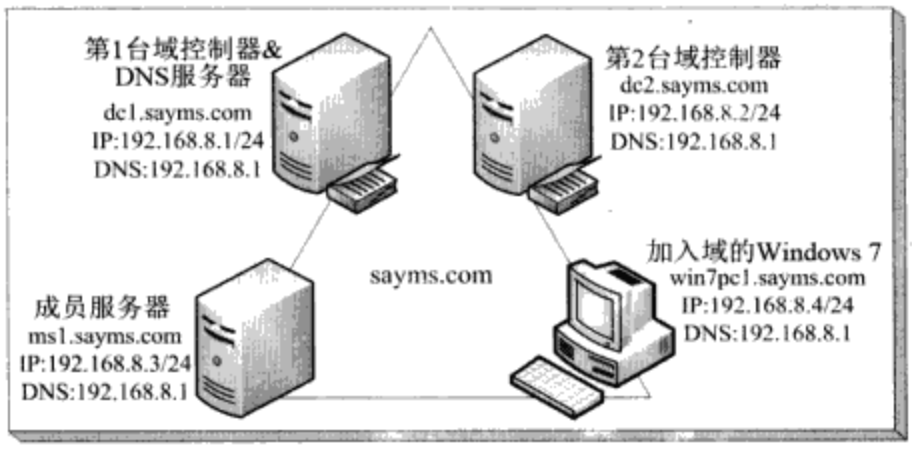


图 2-106

Download at http://www.pin5i.com/

组的成员才有权限删除最后一台域控制器，也就是删除域。若此域之下还有子域的话，请先删除子域。

- 若您所删除的域控制器是林内（林根域内）的最后一台域控制器，则删除后，林就不存在了。您必须是Enterprise Admins组的成员，才有权限删除这台域控制器和林。
- 若这台域控制器是**全局编录服务器**的话，请检查其所属站点（site）内是否还有其他**全局编录服务器**，若没有的话，请先另外指派一台域控制器来扮演**全局编录服务器**，否则将影响用户登录，指派的方法为【开始➲管理工具➲Active Directory站点和服务➲Sites➲ Default-First-Site-Name➲Servers➲选择要扮演**全局编录服务器**的服务器➲对着 **NTDS Settings**右击➲属性➲选择**全局编录**】。

2-9-1 使用Windows窗口来删除域控制器或域

使用Windows窗口来删除域控制器或域的操作步骤如下。

STEP 1 请到即将删除AD DS的域控制器上选择【开始➲运行➲输入**dcpromo**后单击确定按钮】。

提示

在**AD DS服务**停止时，或无法与其他域控制器通信的情况之下，若要删除域控制器的话，请使用**dcpromo /forceremoval**命令来强迫删除域控制器（将AD DS从域控制器内删除）。

STEP 2 在欢迎使用Active Directory域服务安装向导界面中单击下一步按钮。

STEP 3 若出现如图 2-107所示的界面，表示这台域控制器目前是**全局编录服务器**，降级后它将不再扮演**全局编录服务器**的角色，因此请确认站点内还有其他**全局编录服务器**后单击确定按钮。

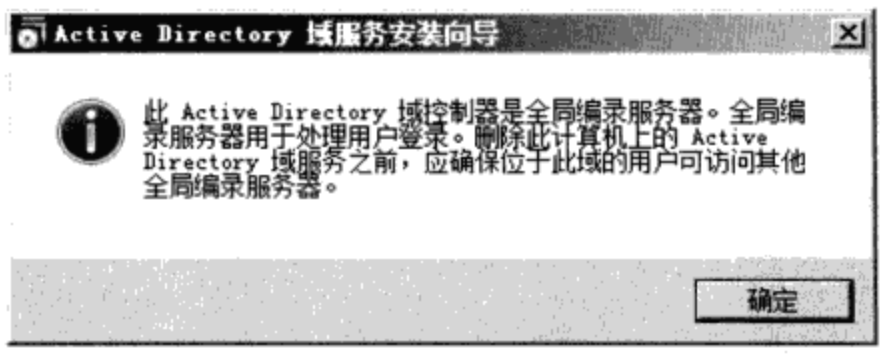


图2-107

STEP 4 在图 2-108中依照下面的说明来选择后单击下一步按钮。

- 若此服务器是域内的最后一台域控制器：请选择**删除该域，因为此服务器是该域中的最后一个域控制器**复选框，降级后这台服务器将变成独立服务器。
- 注意域删除后，所有域用户账户都会被删除，也无法再使用这些账户登录，域用户的密码编译密钥也会被删除，因此请先导出密钥，并先解密所有被加密的

Download at http://www.pin5i.com/

文件（例如通过EFS加密的文件或通过公钥加密的电子邮件），否则域删除后将永远无法访问这些数据。

- 若此服务器不是域内的最后一台域控制器：请不要选择此选项，降级后这台服务器将变成这个域的成员服务器。

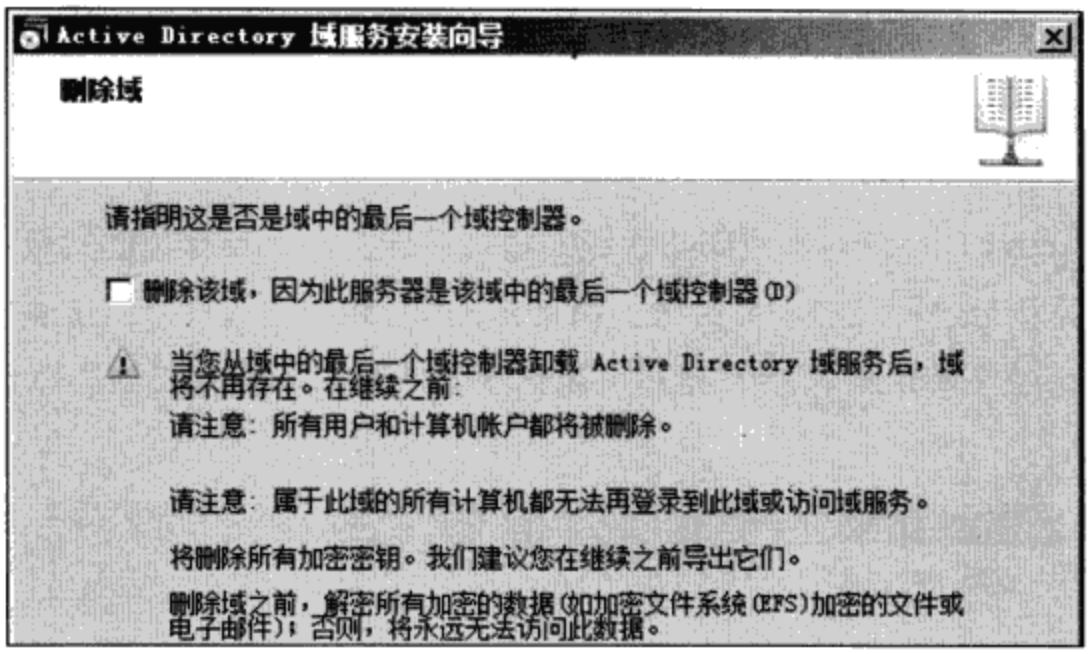


图2-108

STEP 5 若没有出现如图2-109所示的界面的话，请直接跳到**STEP 8**。图 2-109表示这台域控制器包含可写的Active Directory集成DNS区域（不包含RODC的只读DNS区域），安装向导会将此区域的**应用程序目录分区**删除。若此界面出现其他应用程序所创建的**应用程序目录分区**的话，请尽量先使用该应用程序所提供的工具程序（若有的话）来删除此**应用程序目录分区**，单击下一步按钮。

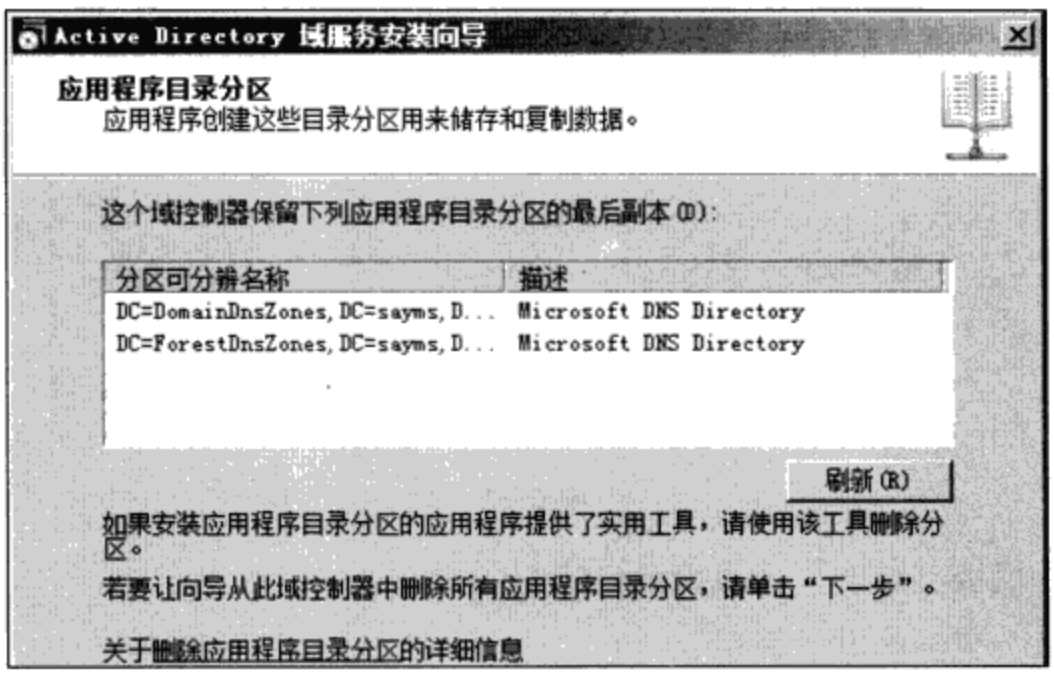


图2-109

STEP 6 选择如图 2-110所示的**确认删除**界面中的选项后单击下一步按钮。它会将此域控制器中所有的**应用程序目录分区**删除。

Download at http://www.pin5i.com/

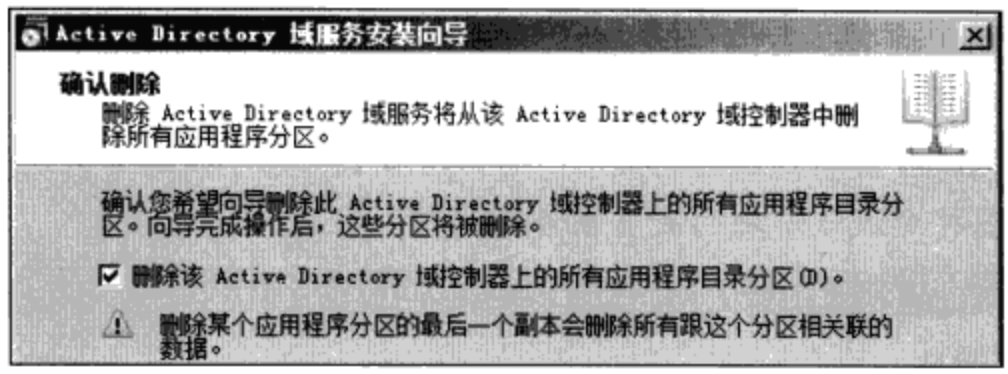


图2-110

STEP 7 由于Active Directory集成DNS区域即将被删除，因此若有其他父域将此区域的查询工作委派给这台域控制器的话，请选择图 2-111中的选项，以便删除父域的委派设置，此时在单击 下一步 按钮后可能需要输入有权限删除父域委派设置的账号与密码。

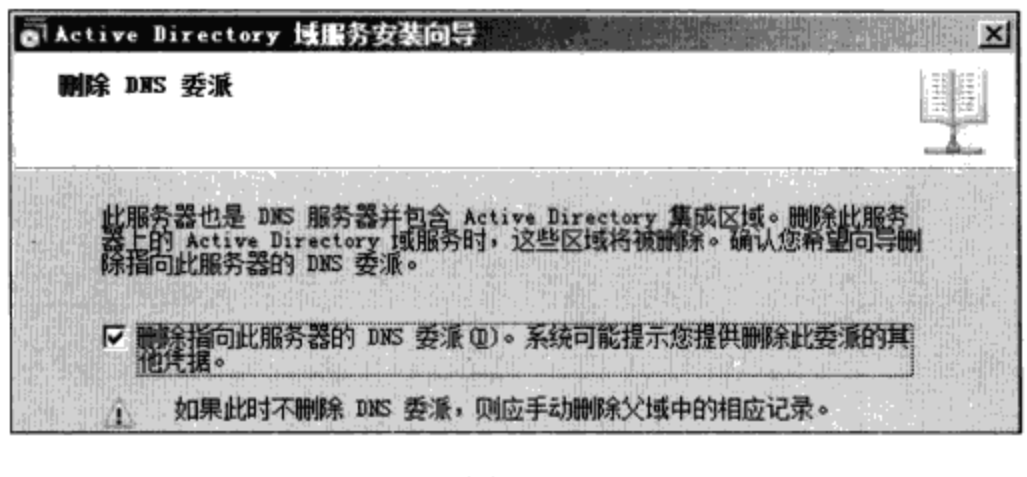


图2-111

STEP 8 在图 2-112中为这台即将被降级为独立服务器或成员服务器的计算机，设置其本地Administrator的新密码，单击 下一步 按钮。

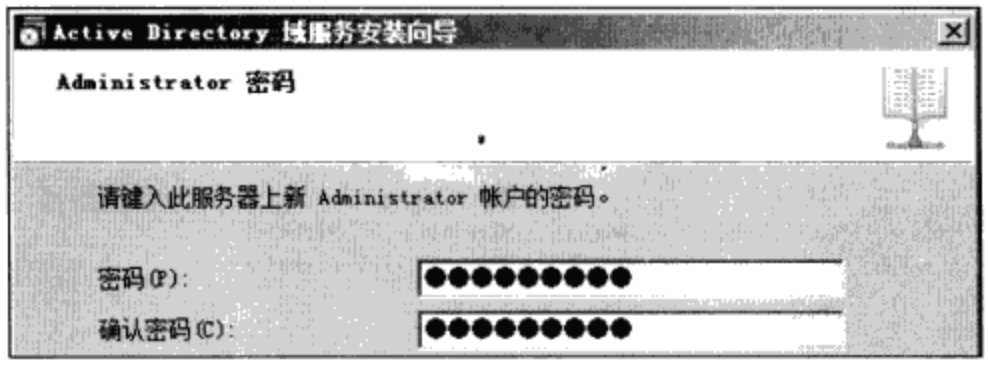


图2-112

STEP 9 当出现**摘要**界面时，请直接单击 下一步 按钮。

STEP 10 完成后，重新启动计算机。

虽然这台服务器已经不再是域控制器了，不过其**Active Directory域服务**组件仍然存在，并没有被删除，因此以后若要再升级为域控制器的话，只需要运行**dcpromo.exe**即可，不需要再通过添加角色的方式来安装**Active Directory域服务**。

Download at http://www.pin5i.com/

还有虽然Active Directory集成DNS区域的**应用程序目录分区**已删除，但是DNS服务器组件仍然存在。

若想要删除**Active Directory域服务**或**DNS服务器**的话，可通过【单击左下角的**服务器管理器**图标➲单击**角色**➲选择**Active Directory域服务**或**DNS服务器**➲单击右边的**删除角色**➲…】的方式进行设置。

2-9-2 使用应答文件来删除域控制器或域

您可以将删除域控制器时所必须提供给安装向导的数据事先输入到**应答文件**内，然后让安装向导直接从应答文件中读取这些数据。请使用**记事本**来编辑应答文件，如图 2-113所示为删除额外域控制器的应答文件，而图 2-114为删除整个域与林的应答文件，图中我们必须在此文件内创建一个名称为**DCInstall**的字段，然后在此区域内输入相关的参数与参数值，各参数的说明如表 2-3所示。

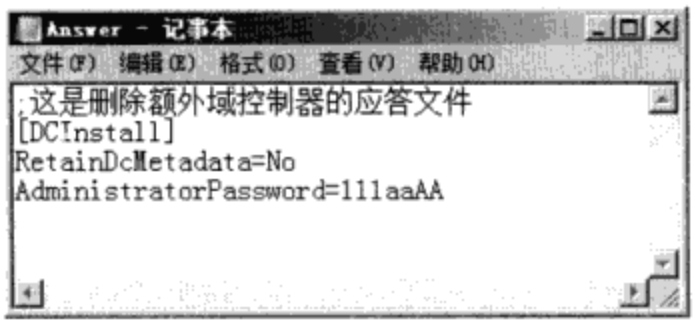


图2-113

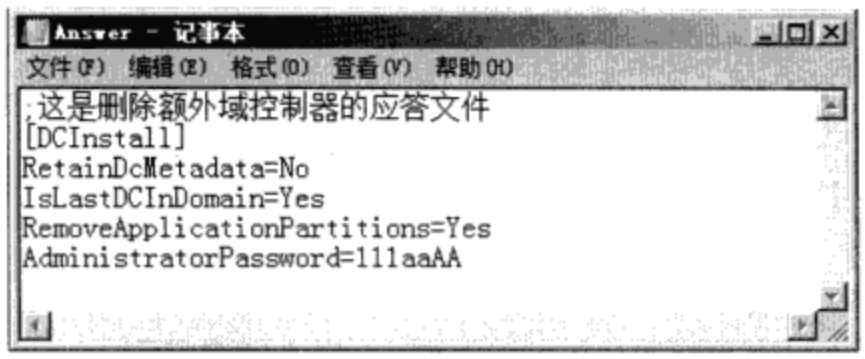


图2-114

表 2-3

参数值	说明	参数值可为
RetainDCMetadata	是否在域中保留域控制器的metadata，以供RODC删除AD DS时使用	Yes或No（默认为No）
IsLastDCInDomain	是否为此域内的最后一台域控制器	Yes或No（默认为No）
RemoveApplicationPartitions	是否删除应用程序目录分区	Yes或No（默认为No）
AdministratorPassword	设置本地Administrator的密码	

提示

以上两个应答文件都假设您是使用系统管理员的身份登录，否则您还必须指定有权删除域控制器或域的用户账户与密码，其他更多的参数可参考第7章或微软网站的文件说明。

创建完成应答文件后，请通过以下命令（参考图 2-115）来删除域控制器或域，假设应答文件的文件名为Answer.txt，且此文件位于C:\Test文件夹内：

```
dcpromo /unattend:"c:\test\Answer.txt"
```


Download at http://www.pin5i.com/



图2-115

提示

dcpromo.exe读取到应答文件中AdministratorPassword的密码后，会自动将此密码清除后再保存到应答文件内。

2-9-3 使用命令行来删除域控制器或域

您可以通过【开始➲命令提示符】(或单击左下方的**Windows PowerShell**图标)，然后运行**dcpromo.exe**命令来删除域控制器或域。例如以下命令可用来删除额外域控制器（参考图2-116)：

```
dcpromo /unattend /RetainDCMetadata:no /AdministratorPassword:111aaAA
```



图2-116

而以下命令可用来自动删除域：

```
dcpromo /unattend /RetainDCMetadata:no /IsLastDCInDomain:yes
/RemoveApplicationPartitions:yes /AdministratorPassword: 111aaAA
```

提示

您可以使用 **dcpromo /?:Promotion** 来查看此命令的详细语法。

Download at http://www.pin5i.com/

2-10 域升级与在现有域环境中安装域控制器

若现有网络环境为Windows 2000或Windows Server 2003林，而您要将Windows Server 2008或Windows Server 2008 R2域控制器加入到此环境中的话，以下是几个可能的情况：

- 将现有Windows 2000或Windows Server 2003林升级。
- 在现有Windows 2000或Windows Server 2003林中添加Windows Server 2008或Windows Server 2008 R2域。
- 在现有Windows 2000或Windows Server 2003林中添加Windows Server 2008或Windows Server 2008 R2域控制器。

2-10-1 将现有Windows 2000或Windows Server 2003林升级

必须事先在Windows 2000或Windows Server 2003域内执行准备工作，否则在升级时会出现如图 2-117所示的界面，而且无法继续执行升级的操作。升级的操作步骤如下。

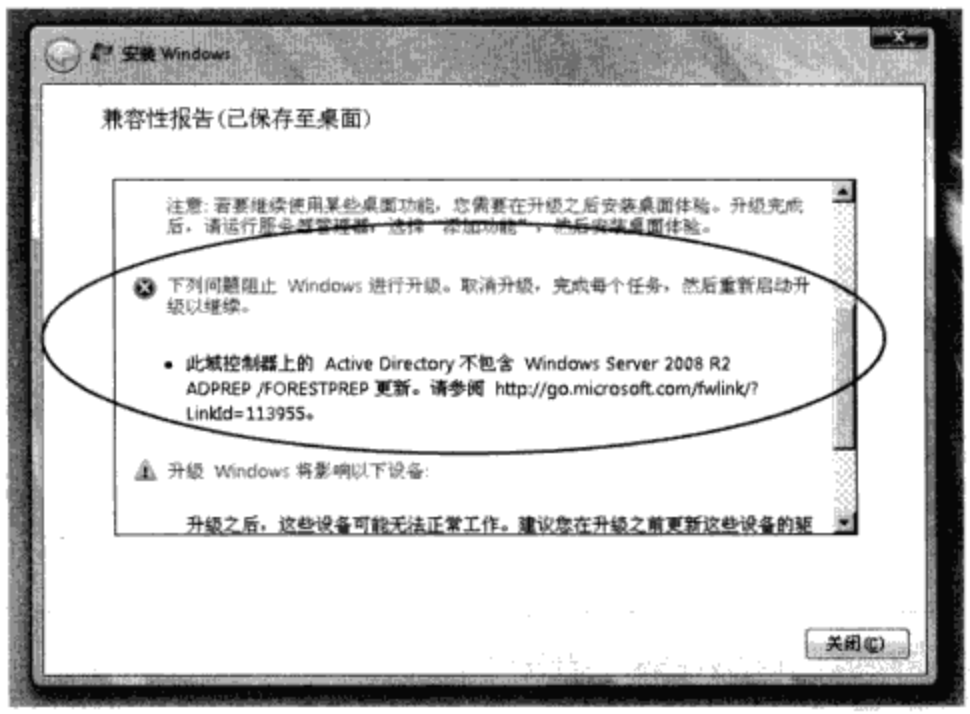


图2-117

STEP 1 找出林内的**架构主机**（Schema Master）与每一个域内的**结构主机**（Infrastructure Master）。林内的第1台域控制器默认就是该林的**架构主机**，而域内第1台域控制器默认就是该域的**结构主机**（详见第10章）。您也可以使用以下方法来找出这两台主机（以Windows Server 2003为例）。

- 架构主机：通过【开始➲运行➲输入**regsvr32 schmmgmt.dll** 命令后单击**确定**按钮➲开始➲运行➲输入MMC命令后单击**确定**按钮➲选择**文件**菜单➲添加/删

Download at http://www.pin5i.com/

除管理单元➲单击添加按钮➲从列表中选择 **Active Directory架构**➲...】的方法来创建**Active Directory架构**控制台。接着如图 2-118所示，对着**Active Directory架构**右击，在弹出的快捷菜单中选择**操作主机**命令，从图中可知目前扮演**架构主机**的域控制器是2003dc.sayms.com。

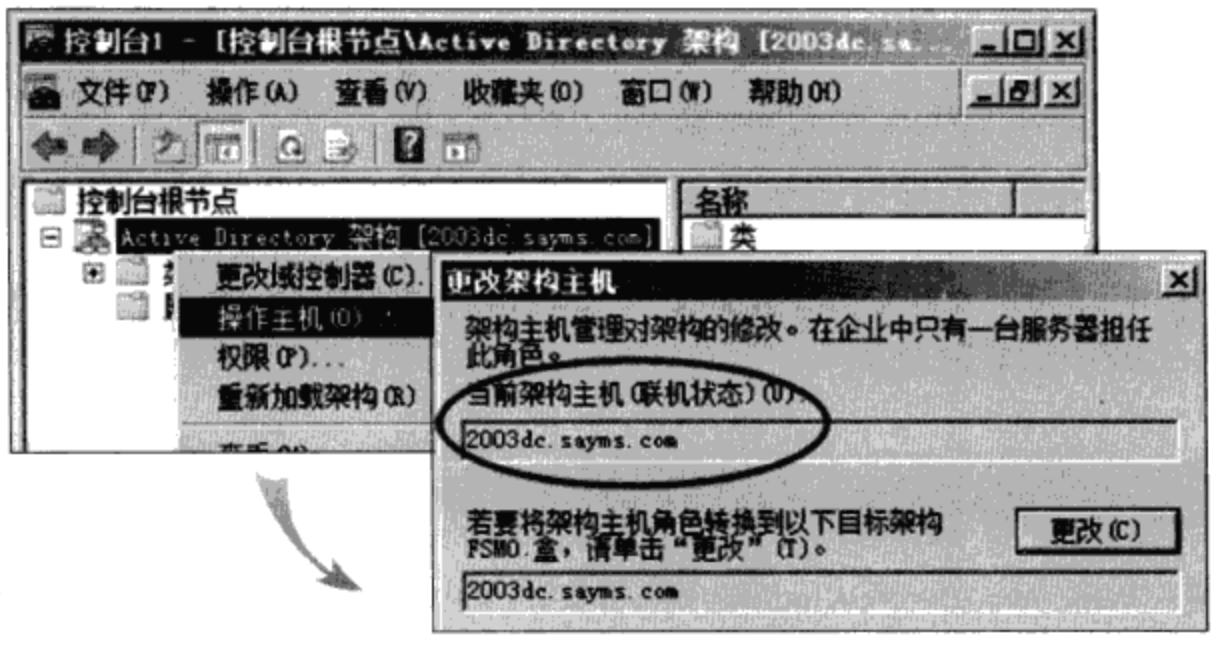


图2-118

↘ 结构主机：选择【开始➲管理工具➲Active Directory用户和计算机➲如图 2-119所示对着域名右击➲操作主机➲单击**基础结构**标签】，从图中可知**结构主机**为2003dc.sayms.com。

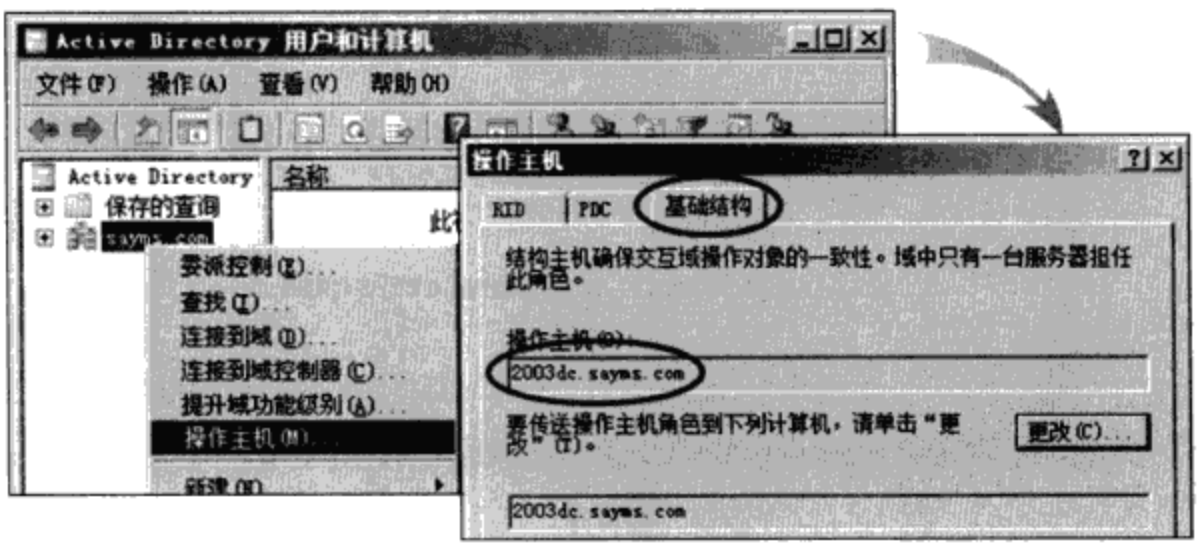


图2-119

STEP 2 建议先通过【开始➲所有程序➲附件➲系统工具➲Windows Server Backup】的方法来备份**架构主机**与**结构主机**的硬盘数据，包含系统的状态数据。

STEP 3 到**架构主机**上使用Enterprise Admins或Schema Admins组的成员登录。

STEP 4 将Windows Server 2008 DVD或Windows Server 2008 R2 DVD放到光驱内。

STEP 5 通过【开始➲命令提示符】的方式，切换到光驱（例如**D:**）。

Download at http://www.pin5i.com/

- Windows Server 2008 DVD：使用**cd \sources\adprep**命令切换到adprep文件夹。
- Windows Server 2008 R2 DVD：使用**cd \support\adprep**命令切换到adprep文件夹。

注意

在执行下一个步骤之前，所有的Windows 2000 Server域控制器必须先升级到Service Pack 4或以上的版本。

STEP 6 运行**adprep /forestprep**命令，确认已完成界面上的要求后单击C键和Enter键。

STEP 7 请等待更新信息被复制到其他域控制器后，再继续以下步骤。以升级Windows Server 2003域为例，如果是同一个站点的域控制器的话，其等待复制的时间可能需要15s或更久。

STEP 8 到**结构主机**上使用Domain Admins组的成员登录。

STEP 9 将Windows Server 2008 DVD或Windows Server 2008 R2 DVD放到光驱内。

STEP 10 通过【开始➲命令提示符】的方式，切换到光驱（例如**D:**）。

- Windows Server 2008 DVD：使用**cd \sources\adprep**命令来切换到adprep文件夹。
- Windows Server 2008 R2 DVD：使用**cd \support\adprep**命令来切换到adprep文件夹。

注意

在执行下一个步骤之前，Windows 2000 Server或Windows Server 2003的域功能级别必须是**Windows 2000纯模式**（也就是**本机模式**）或**Windows Server 2003**。

STEP 11 运行**adprep /domainprep /gpprep**命令。

注意

由于**adprep /domainprep /gpprep**会将SYSVOL文件夹内的GPO权限设置，复制到所有其他域控制器，因此如果网络内有许多域控制器或GPO较多的话，这个复制操作会占用较多的网络带宽，从而影响网络的性能，此时建议您先执行不会复制GPO权限设置的命令：

```
adprep  /domainprep
```

等以后适当时机再来运行以下命令：

```
adprep  /domainprep /gpprep
```

此时这个命令只会复制GPO的权限设置，其他操作不会再重复运行。

STEP 12 请等待更新信息被复制到其他域控制器后，再继续以下步骤。以升级Windows Server 2003域为例，如果是同一个站点的域控制器的话，其等待复制的时间可能需要15s或更久。

Download at http://www.pin5i.com/

STEP 13 接下来可以开始将域控制器升级到Windows Server 2008或Windows Server 2008 R2：将Windows Server 2008 DVD或Windows Server 2008 R2 DVD放到光驱内，稍等一下系统会自动启动DVD内的安装程序，单击立即安装按钮。

2-10-2 在现有Windows 2000或Windows Server 2003林中添加Windows Server 2008或Windows Server 2008 R2域

在创建新的Windows Server 2008或Windows Server 2008 R2域前，请注意以下事项：

- 请先到**架构主机**上使用**adprep /forestprep**命令来扩展现有的Windows 2000或Windows Server 2003林的架构（若尚未扩展的话），方法请参考前一小节中与**架构主机**有关的说明。
- 这个新域内是否需要Windows 2000 Server或Windows Server 2003域控制器，请根据您的需求事先决定好域功能级别。

完成以上的操作后，您就可以开始在现有的Windows 2000或Windows Server 2003林中添加Windows Server 2008或Windows Server 2008 R2域。

2-10-3 在现有Windows 2000或Windows Server 2003域中添加Windows Server 2008或Windows Server 2008 R2域控制器

在现有域内创建新的Windows Server 2008或Windows Server 2008 R2域控制器之前，请注意以下事项：

- 请先到**架构主机**上使用**adprep /forestprep**命令来扩展现有Windows 2000或Windows Server 2003林的架构（若尚未扩展的话），方法请参考前面与**架构主机**有关的说明。
- 请先到**结构主机**上运行**adprep /domainprep /gpprep**命令，方法请参考前面与**结构主机**有关的说明。
- 若要安装**只读域控制器（RODC）**的话，请先在一台域控制器上登录，然后运行**adprep /rodcprep**命令，不过现有林功能级别必须为Windows Server 2003，且所要安装的第一台Windows Server 2008或Windows Server 2008 R2域控制器不可为RODC。

完成以上操作后，您就可以开始在现有Windows 2000或Windows Server 2003域中安装Windows Server 2008或Windows Server 2008 R2域控制器。

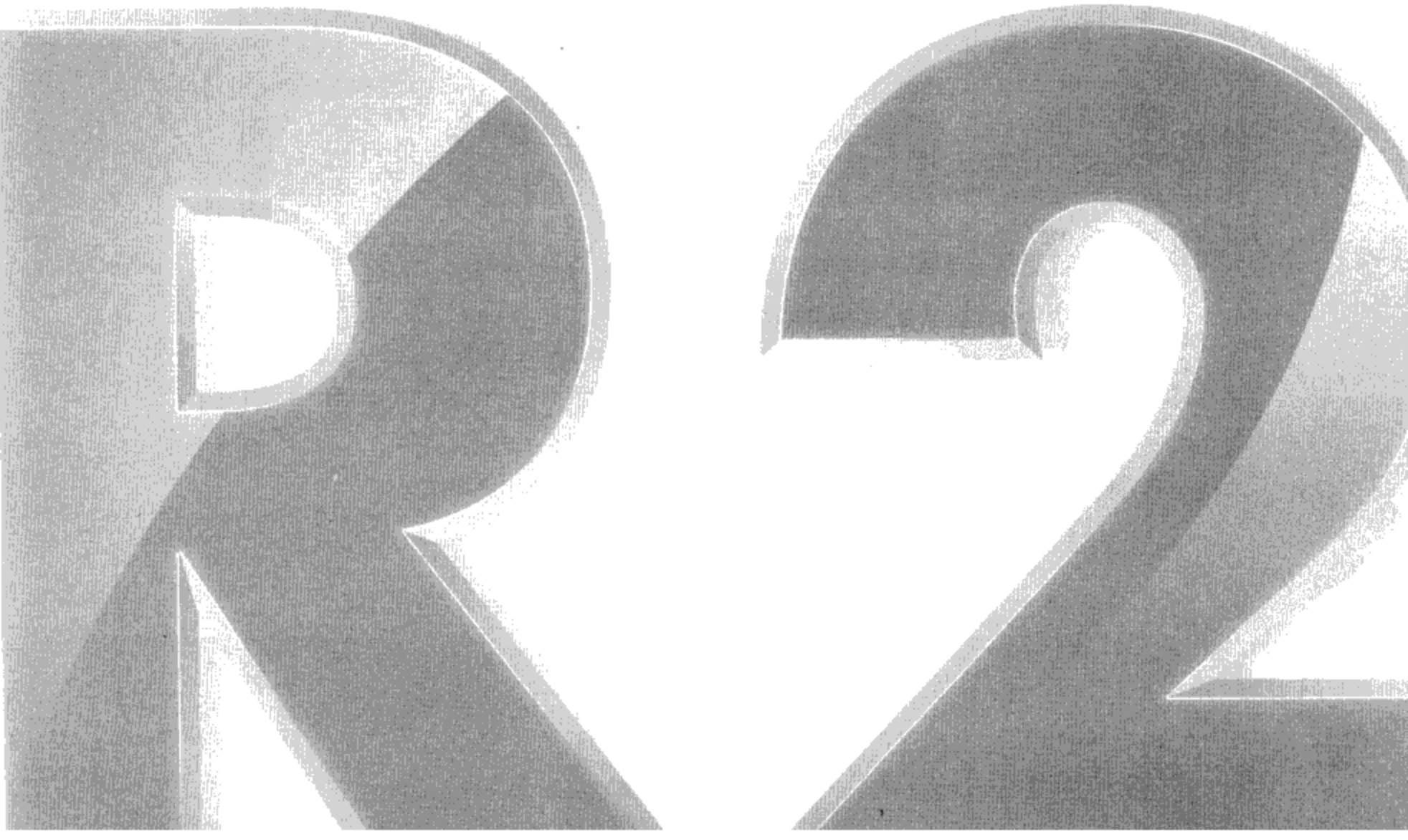
Download at http://www.pin5i.com/

第3章

域用户与组账户的管理

域系统管理员需要为每一个域用户分别创建一个用户账户，让他们可以使用这个账户来登录域、访问网络上的资源。域系统管理员同时也需要了解如何使用组，以便有效率地管理资源的访问。

- 管理域用户账户
- 一次同时添加多个用户账户
- 域组账户
- 组的使用准则



Download at http://www.pin5i.com/

3-1 管理域用户账户

域系统管理员可以使用**Active Directory管理中心**或**Active Directory用户和计算机**来创建与管理域用户账户。当用户使用域用户账户登录域后，便可以直接连接域内的所有计算机、访问有权访问的资源。换句话说，域用户在域内的一台计算机上登录成功后，当他要连接域内的其他计算机时，并不需要再手动登录其他计算机。这个只须登录一次的功能，被称为**单点登录**（Single Sign-on）。

> **提示**
>
> 本地用户账户并不具备**单点登录**的功能，也就是说使用本地用户账户登录后，当要连接其他计算机时，需要再手动登录。

在服务器还没有升级成为域控制器之前，原来位于其本地安全数据库内的本地账户，会在升级成域控制器后被转移到Active Directory数据库内，而且是被放置到容器Users内，您可以通过**Active Directory管理中心**来查看，如图 3-1中所示（请先单击上方的**树视图**图标），同时这台服务器的计算机账户会被放置到图中的组织单位Domain Controllers内。其他加入域的计算机账户默认会被放置到图中的容器Computers内。

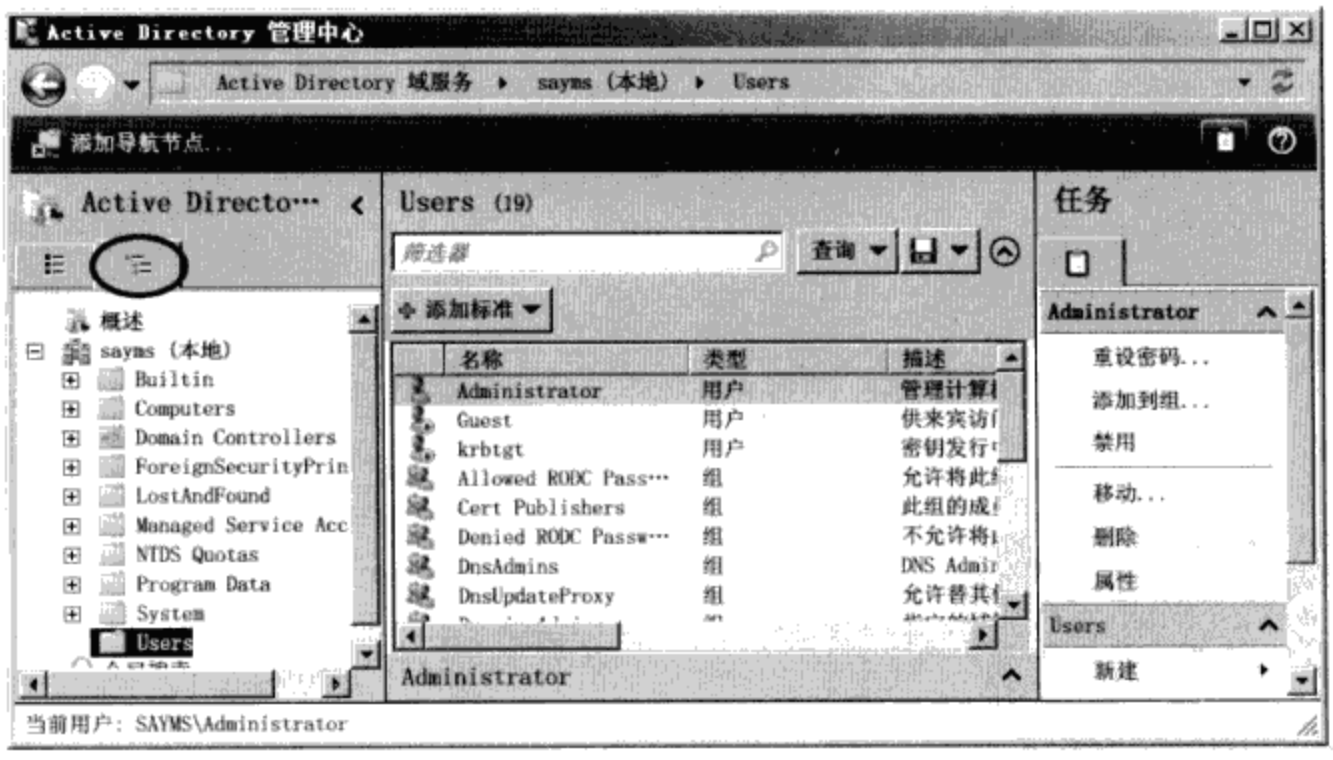


图3-1

您也可以通过**Active Directory用户和计算机**来查看，如图 3-2所示。

Download at http://www.pin5i.com/

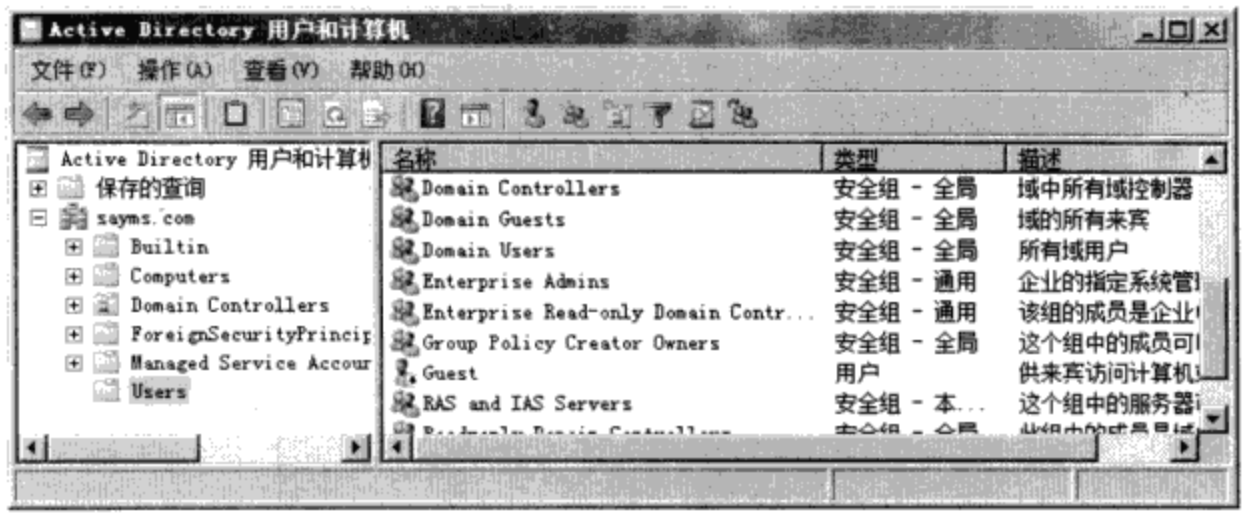


图 3-2

只有在创建域内的第1台域控制器时，该服务器原来的本地账户才会被转移到Active Directory数据库，其他域控制器原有的本地账户并不会被转移到Active Directory数据库，而是被删除。

3-1-1 创建组织单位与域用户账户

您可以将用户账户创建到任何一个容器或组织单位内。以下假设要先创建名称为**业务部**的组织单位，然后在其内创建域用户账户mary。

创建组织单位**业务部**的方法为：【开始➲管理工具➲选择**Active Directory管理中心**（或**Active Directory用户和计算机**）➲对着域名右击➲新建➲组织单位➲如图 3-3所示输入组织单位名称**业务部**➲单击确定按钮】。

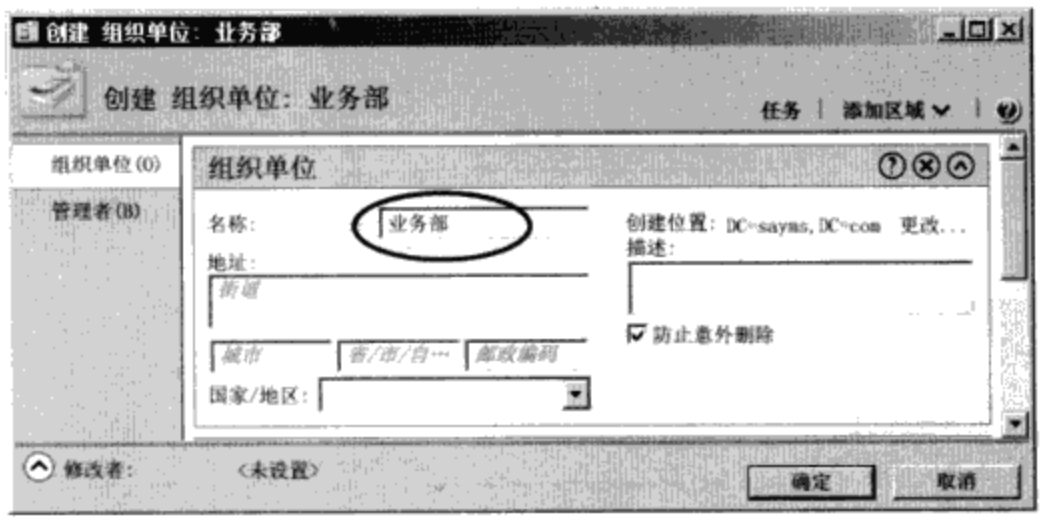


图 3-3

注意

图中默认已选择**防止意外删除**复选框，因此您无法将此组织单位删除，除非取消选择此选项。若是使用**Active Directory用户和计算机**，请先【选择**查看**菜单➲高级功能➲对着此组织单位右击➲属性➲如图 3-4所示取消选择**对象**标签之下的**防止对象被意外删除**复选框】。

Download at http://www.pin5i.com/

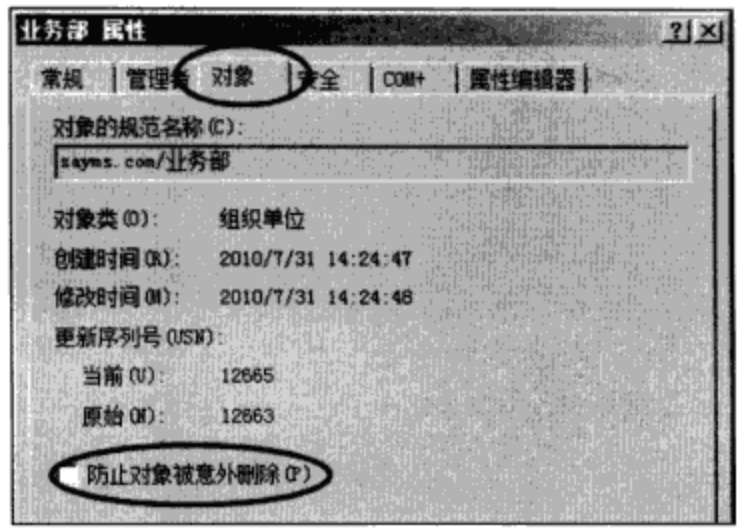


图3-4

在组织单位**业务部**内创建用户账户mary的方法为：【对着组织单位**业务部**右击➲新建➲用户】。

3-1-2 用户登录账户

域用户可到域成员计算机上（非域控制器）使用两种账户来登录域，它们分别是图3-5中的**用户UPN登录**与**用户SamAccountName登录**。

> **注意**
>
> 一般的域用户默认是无法在域控制器上登录的，若要开放的话，请参考第4章的说明。

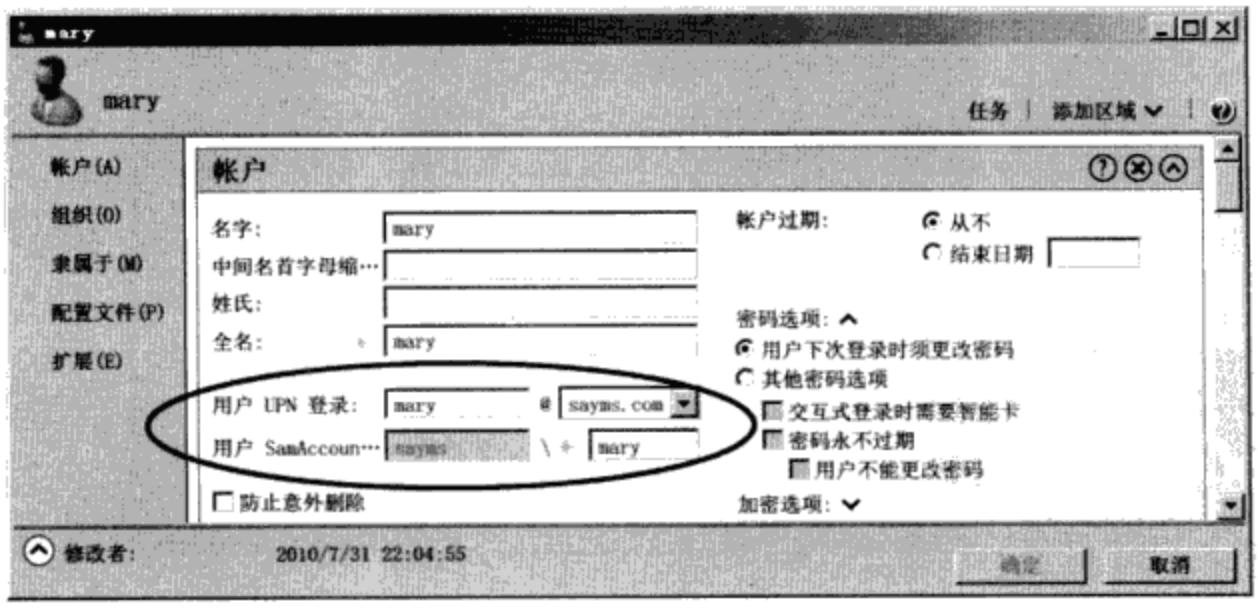


图3-5

1. 用户 UPN 登录

此名称又称为UPN（User Principal Name），它的格式与电子邮件账户相同，如图3-5中的mary@sayms.com，这个名称只能在隶属于域的计算机上登录域时使用（如图3-6所示）。整个

Download at http://www.pin5i.com/

林内，这个名称必须是唯一的。

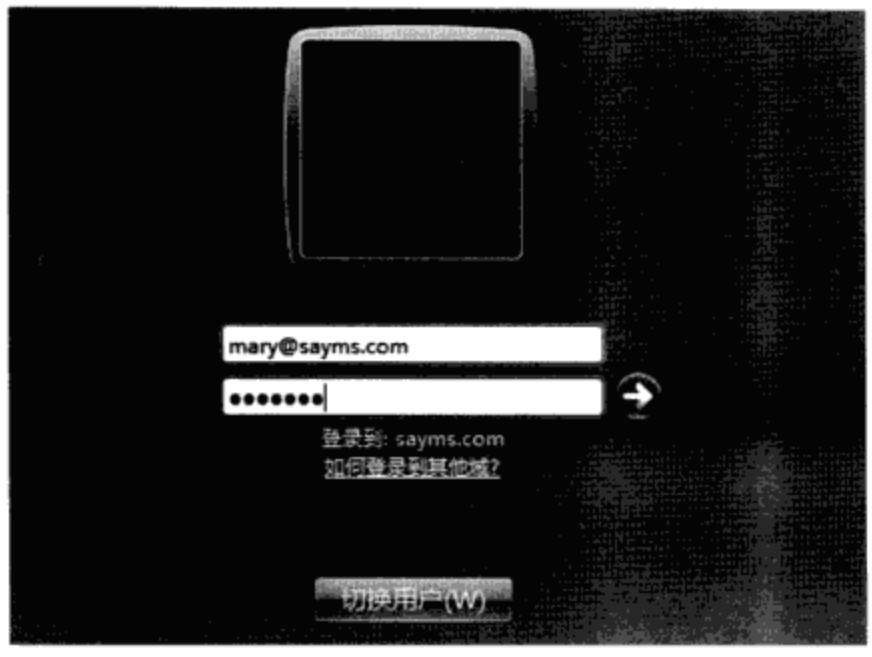


图3-6

UPN并不会随着账户被转移到其他域而改变，举例来说，用户mary的用户账户是位于域sayms.com内，其默认的UPN为mary@sayms.com，之后即使这个用户账户被转移到林中的另一个域内，例如域sayiis.com，其UPN仍然是mary@sayms.com，并没有被改变，因此mary仍然可以继续使用原来的UPN登录。

2. 用户 SamAccountName 登录

如图 3-5所示中的SAYMS\mary，这是旧格式的登录账户。Windows 2000之前版本的旧客户端需使用这种格式的名称来登录域。在隶属于域的Windows 2000（含）之后的计算机上也可以采用这种名称来登录，如图 3-7所示。同一个域内，这个名称必须是唯一的。

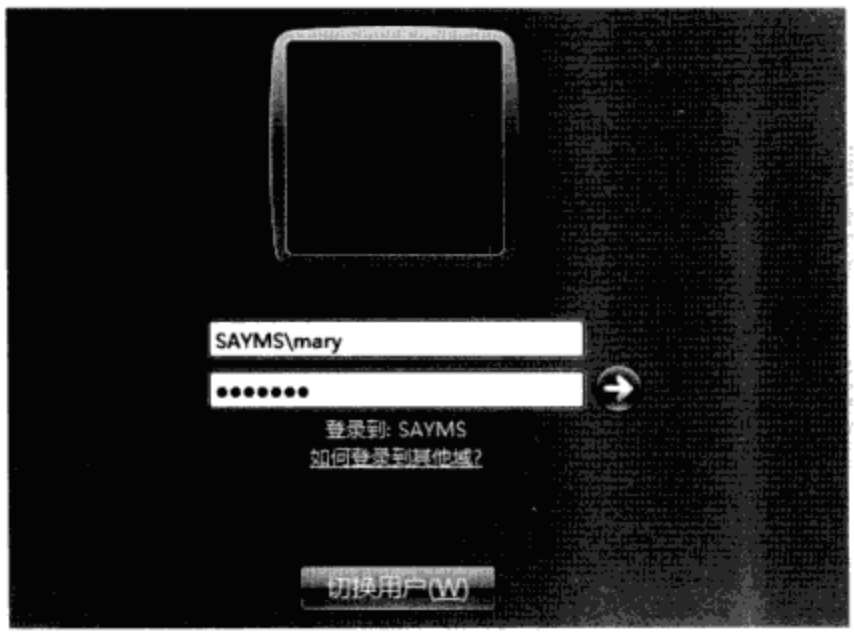


图3-7

Download at http://www.pin5i.com/

提示

若是使用Active Directory用户和计算机的话，则上述**用户UPN登录**与**用户SamAccountName登录**分别被称为**用户UPN登录名称**与**用户SamAccountName登录名称**（Windows 2000之前的版本）。

3-1-3 创建UPN的后缀

用户账户的UPN后缀默认是账户所在域的域名，例如用户账户是被创建在域sayms.com内，则其UPN后缀为sayms.com。在某些情况之下，用户可能希望能够改用其他后缀，例如：

- 由于UPN的格式与电子邮件账户相同，因此用户可能希望UPN可以与电子邮件账户相同，以便让用户不论是登录域或收发电子邮件，都可以使用一致的名称。
- 如果域树内有较多层的子域，则域名会太长，例如sales.tw.sayms.com，故用户的UPN后缀也会太长，如此将造成用户在登录时的不便。

而我们可以通过添加UPN后缀来让用户拥有其他后缀：

STEP 1 选择【开始➲管理工具➲Active Directory域和信任关系➲如图 3-8所示，单击**Active Directory域和信任关系**后单击上方的**属性**图标】。

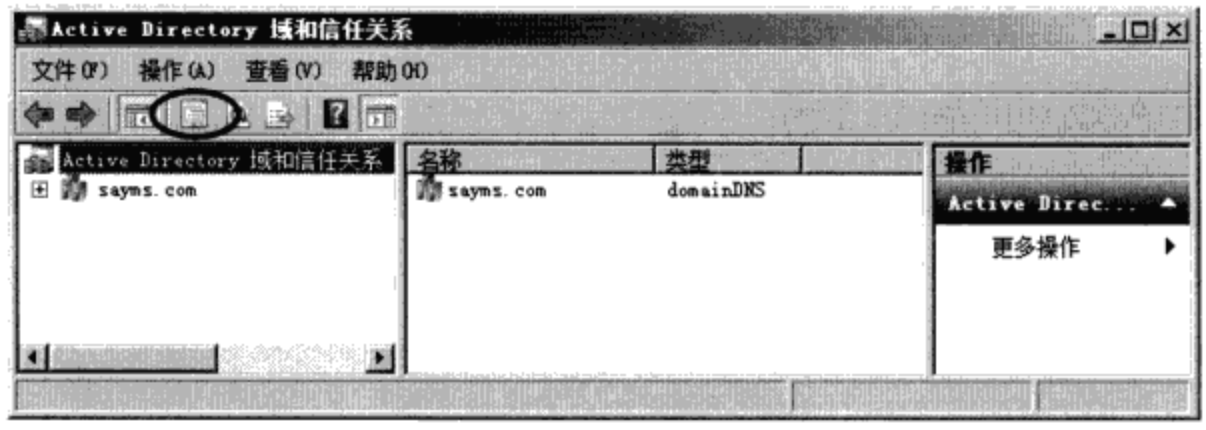


图3-8

STEP 2 在图 3-9中输入其他的UPN后缀后单击**添加**和**确定**按钮。后缀不一定要符合DNS格式，例如可以是sayiis.com，也可以是sayiis。

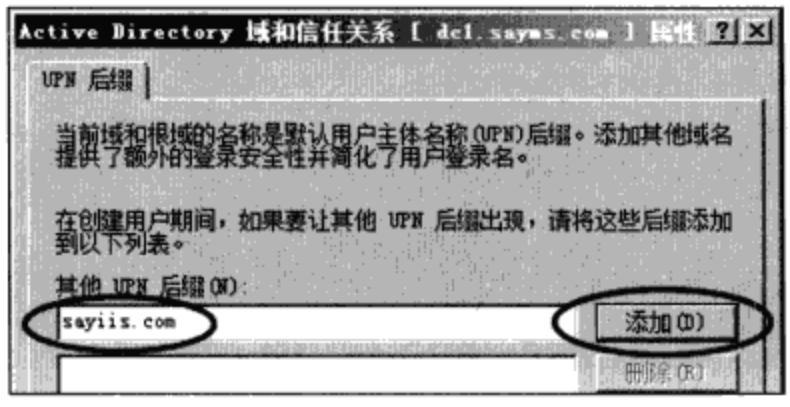


图3-9

Download at http://www.pin5i.com/

STEP 3 完成后，您就可以通过**Active Directory管理中心**（或**Active Directory用户和计算机**）来更改用户的UPN后缀，如图 3-10所示。

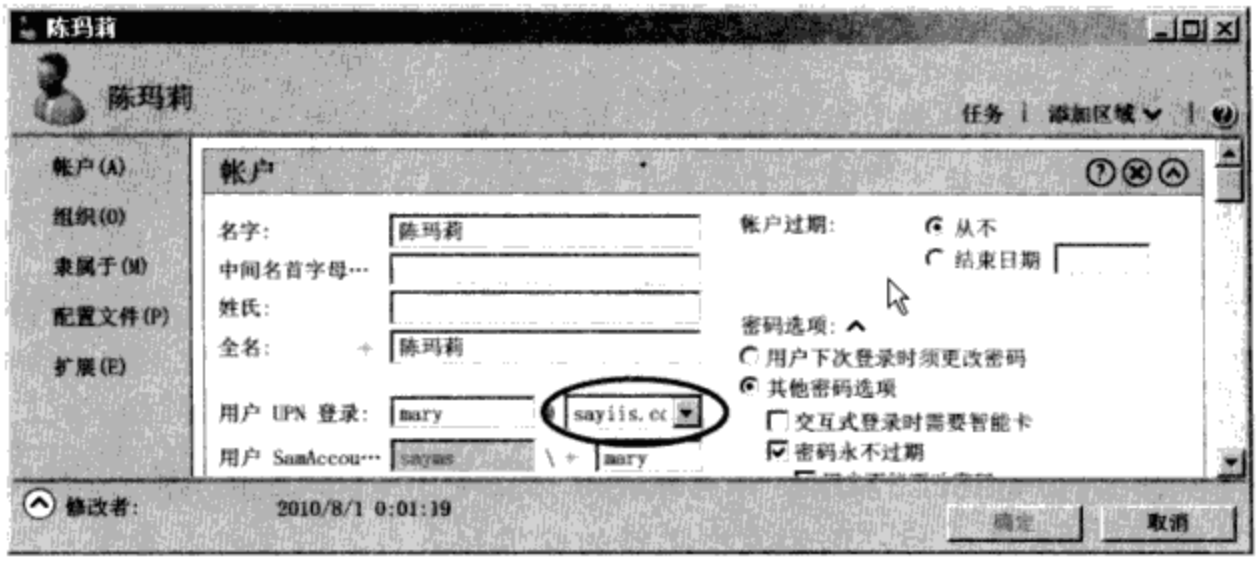


图 3-10

3-1-4 账户的一般管理工作

本节将介绍用户账户的一般管理工作，例如重设密码、禁用（启用）账户、移动账户、删除账户、更改登录名称与解除锁定等。您可以如图 3-11所示单击要修改的用户账户（例如图中的**陈玛莉**），然后通过右方选项来设置。

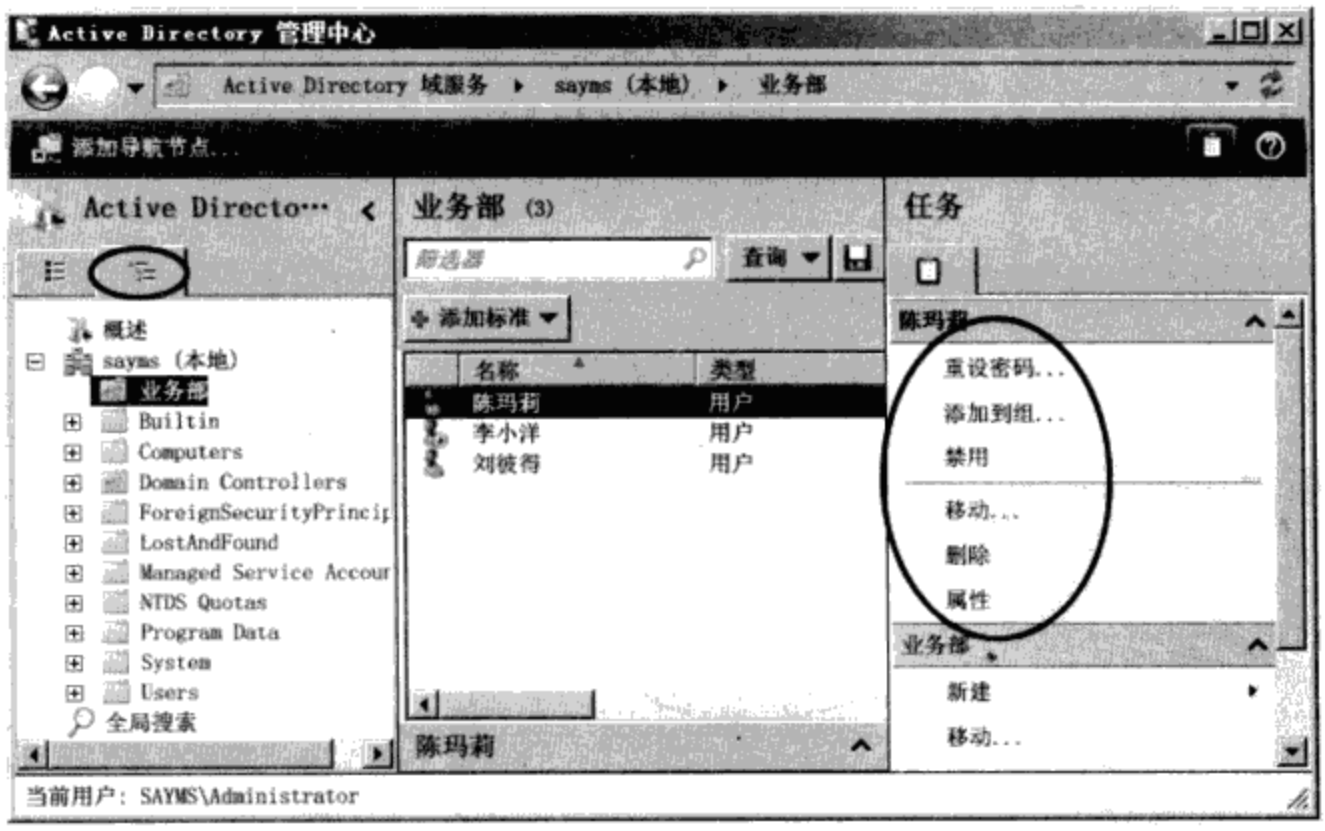


图 3-11

- **重设密码**：当用户忘记密码或密码使用期限到期时，系统管理员可以在此处为用户设置一个新的密码。

Download at http://www.pin5i.com/

- **禁用（或启用）账户**：如果某个员工因故在一段时间内无法来上班的话，此时您可以先将该用户的账户禁用，待该员工回来上班后，再将其重新启用即可。若用户账户已被禁用，则该用户账户图形上会有一个向下的箭头符号（例如图3-11中的用户**李小洋**）。
- **移动账户**：您可以将账户转移到同一个域内的其他组织单位或容器。
- **重命名**：重命名以后（请通过【对着用户账户右击➲属性】的方法），该用户原来所拥有的权限、权利与组关系都不会受到影响。例如当某员工离职时，您可以暂时先将其用户账户禁用，等到新员工进来接替他的工作时，再将此账户名称改为新员工的名称、重新设置密码、更改登录账户名称、修改其他相关个人数据，然后再重新启用此账户即可。在每一个用户账户添加完成之后，系统都会为其创建一个唯一的安全标识符（Security Identifier，SID），而系统是使用这个SID来代表该用户，同时权限设置等都是通过SID来记录的，例如某个文件的权限列表内，它会记录着哪一些SID具备着哪一些权限，而不是哪一些用户名拥有哪一些权限。由于用户账户名称或登录名称更改后，其安全标识符（SID）并没有被改变，因此用户的权限、权利与组关系都不变。您可以通过双击用户账户或右方的**属性**来更改用户账户名称与登录名称等相关设置。
- **删除账户**：如果这个账户以后再也用不到的话，就可以将此账户删除。当您将账户删除后，即使再添加一个相同名称的用户账户，此新账户并不会继承原账户的权限、权利与组关系，因为系统会给予这个新账户一个新的安全标识符（SID），而系统是使用SID来记录用户的权限、权利与组关系的，因此对系统来说，这是两个不同的账户，当然就不会继承原账户的权限、权利与组关系。
- **解除被锁定的账户**：我们可以通过**账户策略**来设置用户输入密码失败多次后，就将此账户锁定，而系统管理员可以使用以下方法来解除锁定：【双击该用户账户➲单击图3-12中的**解锁账户**（账户被锁定后才会有此选项）】。

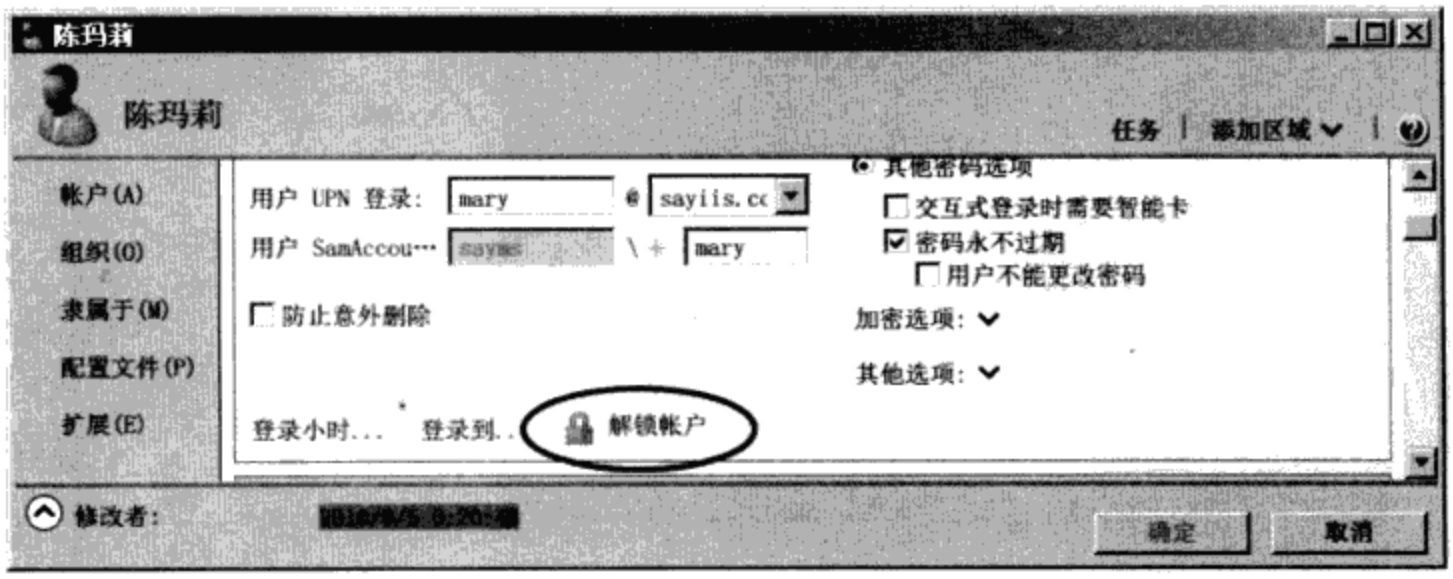


图3-12

Download at http://www.pin5i.com/

3-1-5 域用户账户的属性设置

每一个域用户账户内都有一些相关的属性数据，例如地址、电话与电子邮件信箱等，域用户可以通过这些属性来查找Active Directory数据库内的用户，例如通过电话号码来查找用户，因此为了更容易找到所需的用户账户，这些属性数据应该越完整越好。我们将通过 **Active Directory管理中心**来介绍用户账户的部分属性，请先双击要设置的用户账户。

1. 组织数据的设置

组织数据就是指显示的名称、职务、部门、地址、电话、电子邮件、网页等，如图 3-13 所示，这部分的属性都很简单，请自行浏览这些字段。

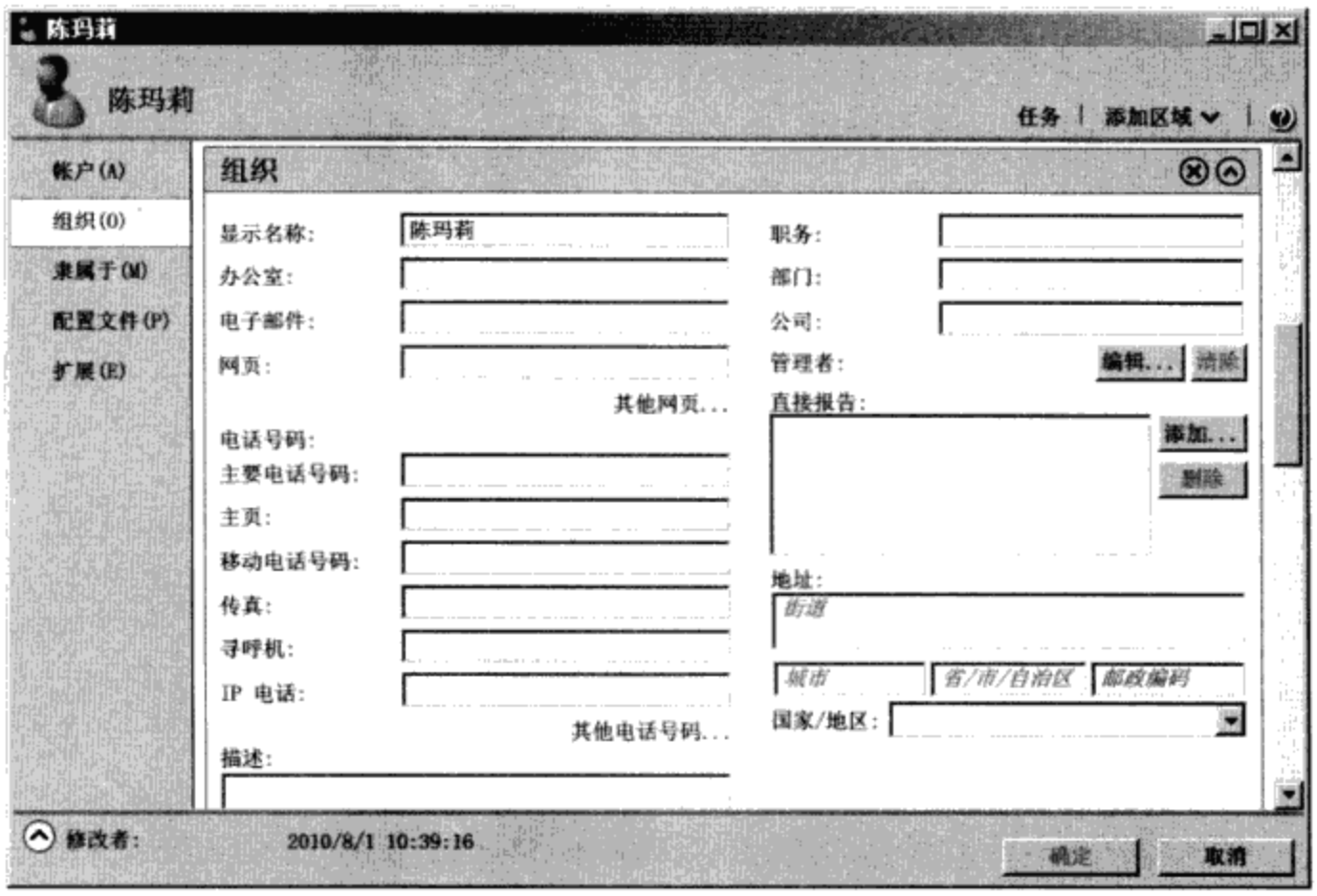


图3-13

2. 账户过期的设置

我们可以通过如图 3-14所示的**账户过期**选项来设置账户的有效期限，默认选中**从不**单选按钮，若要设置过期的话，请选中**结束日期**单选按钮，然后输入格式为yyyy/m/d的过期日期。

Download at http://www.pin5i.com/

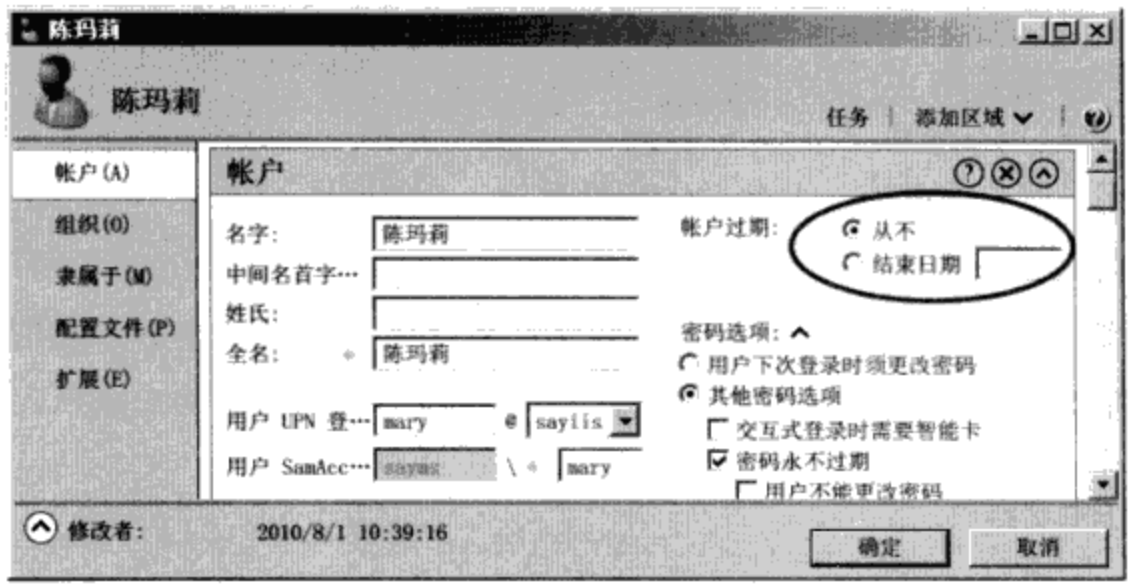


图3-14

3. 登录小时的设置

登录小时用来指定用户可以登录到域的时段，默认是任何时段都可登录域，若要更改设置的话，请单击图 3-15中的**登录小时…**，然后通过弹出的**登录小时数**对话框来设置。图中横轴每一方块代表一个小时，纵轴每一方块代表一天，填满方块与空白方块分别代表允许与不允许登录的时段，默认是开放所有的时段。选好时段后选择**允许登录**或**拒绝登录**单选按钮来允许或拒绝用户在上述时段登录。

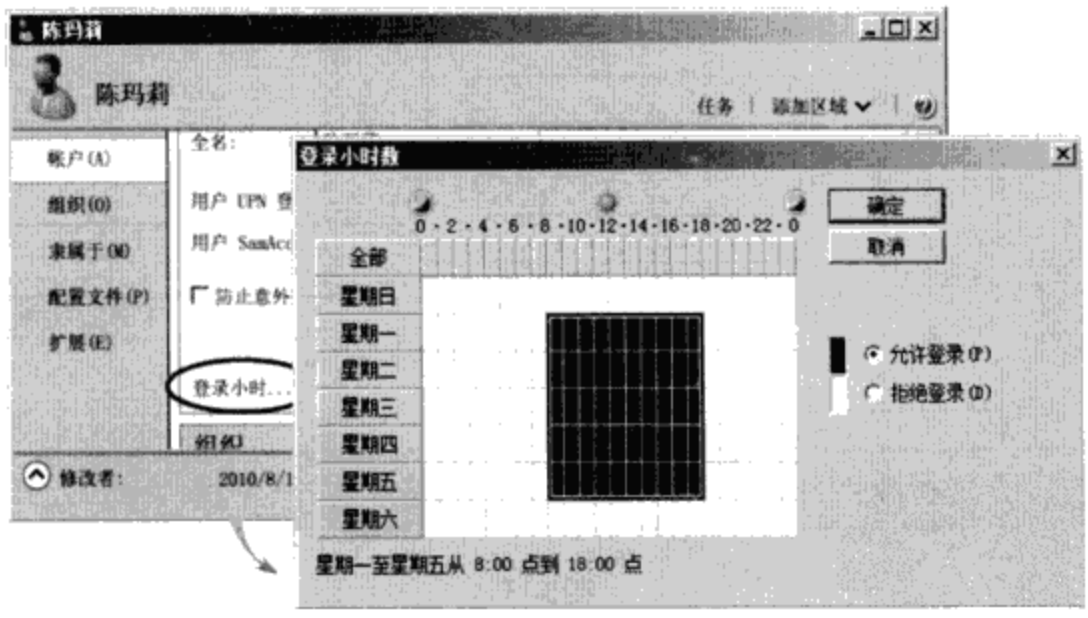


图3-15

4. 限制用户只能通过某些计算机登录

一般域用户默认可以使用域内的任何一台计算机（域控制器除外）来登录域，不过我们也可以通过以下方法来限制用户只使用某些特定计算机来登录域：【单击图 3-16中的**登录到…**➲在弹出的**登录到**对话框中选择**下列计算机**➲输入计算机名后单击添加按钮】，计算机名可为

Download at http://www.pin5i.com/

NetBIOS名称（例如win7pc1）或DNS名称（例如win7pc1.sayms.com）。

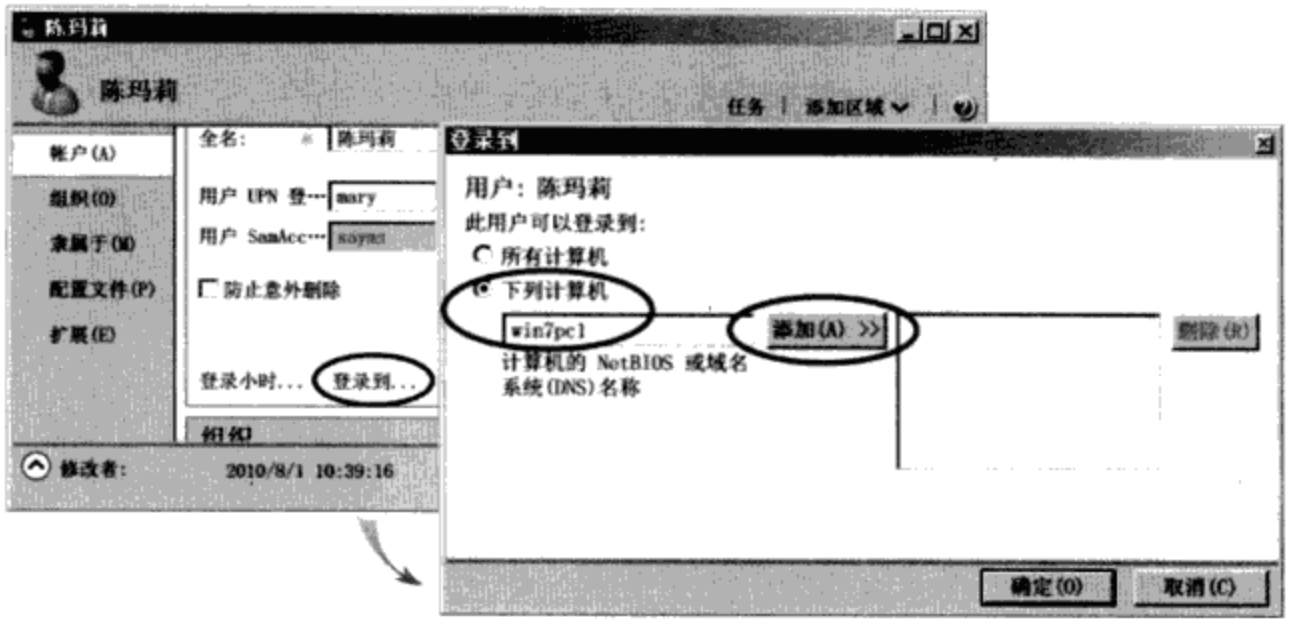


图3-16

3-1-6 搜索用户账户

AD DS将用户账户、组账户、计算机账户、打印机、共享文件夹等对象存储在Active Directory数据库内，域系统管理员可以轻易地在Active Directory数据库中搜索与管理所需的用户账户。

若您要在某个组织单位（或容器）内来搜索用户账户的话，只要如图 3-17所示【单击组织单位➲在中间窗口上方输入要搜索的用户账户名称即可】，搜索到的用户账户会被显示在中间窗口的下方。

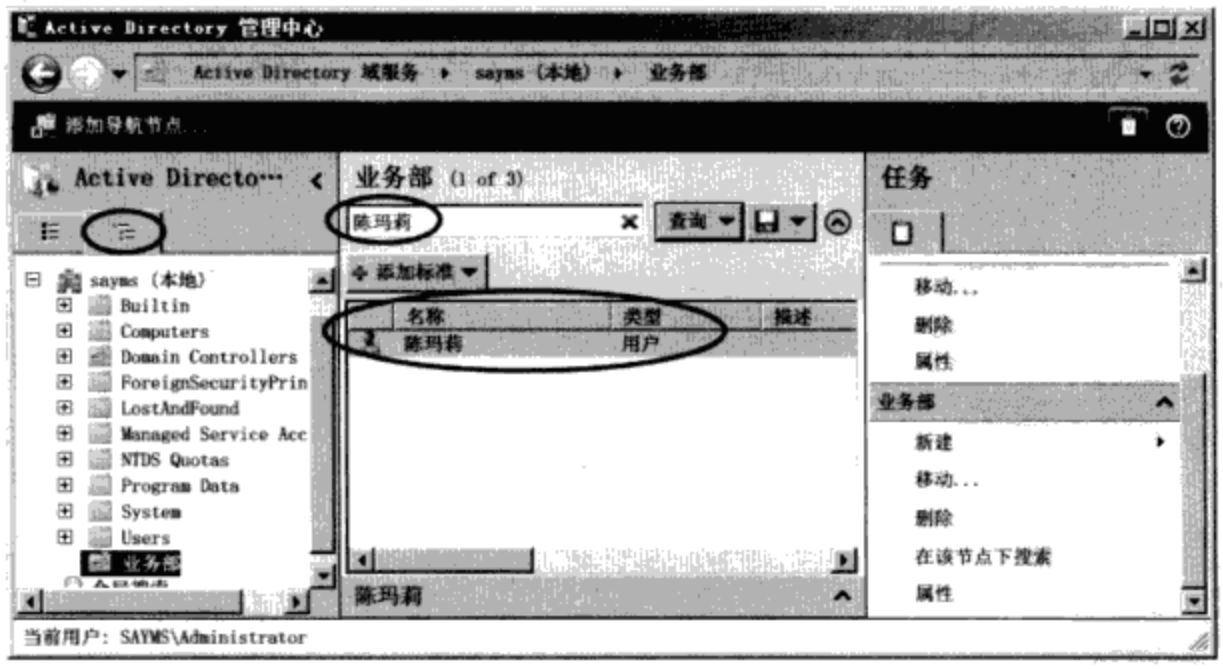


图3-17

若要搜索整个域的话，请通过【单击上方域名（例如sayms）➲在中间窗口上方输入要搜索的用户账户名称➲单击右方**任务**窗格中的**在该节点下搜索**选项】的方法，或是如图 3-18所

Download at http://www.pin5i.com/

示，通过【选择左边的**全局搜索**➲在中间窗口上方输入要搜索的用户账户名称➲单击搜索按钮】的方法进行操作。

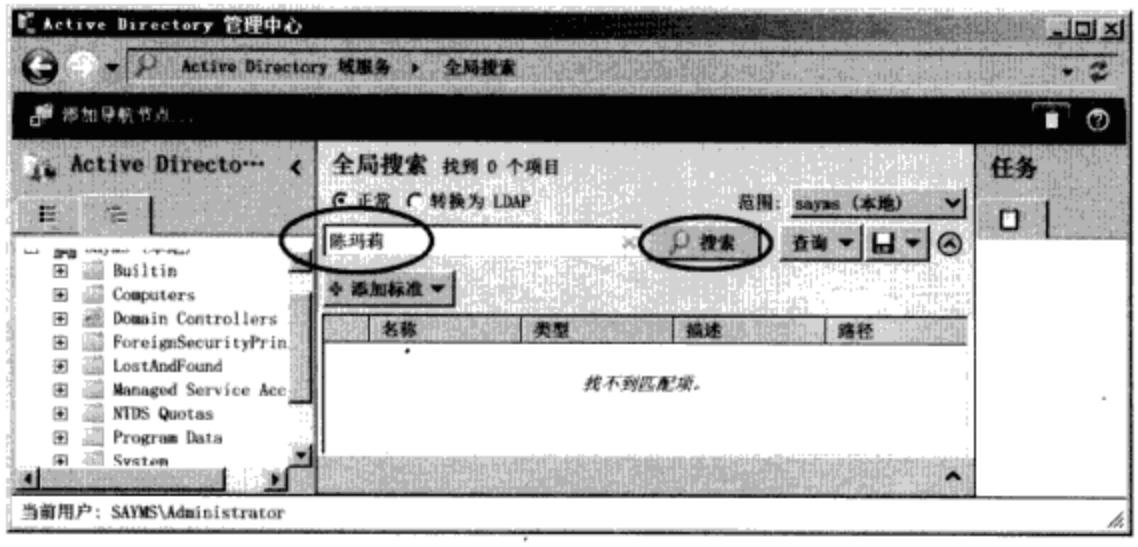


图3-18

您也可以通过**全局编录搜索**来搜索位于其他域内的对象，不过需先将搜索领域更改为**全局编录搜索**，如图 3-19所示。

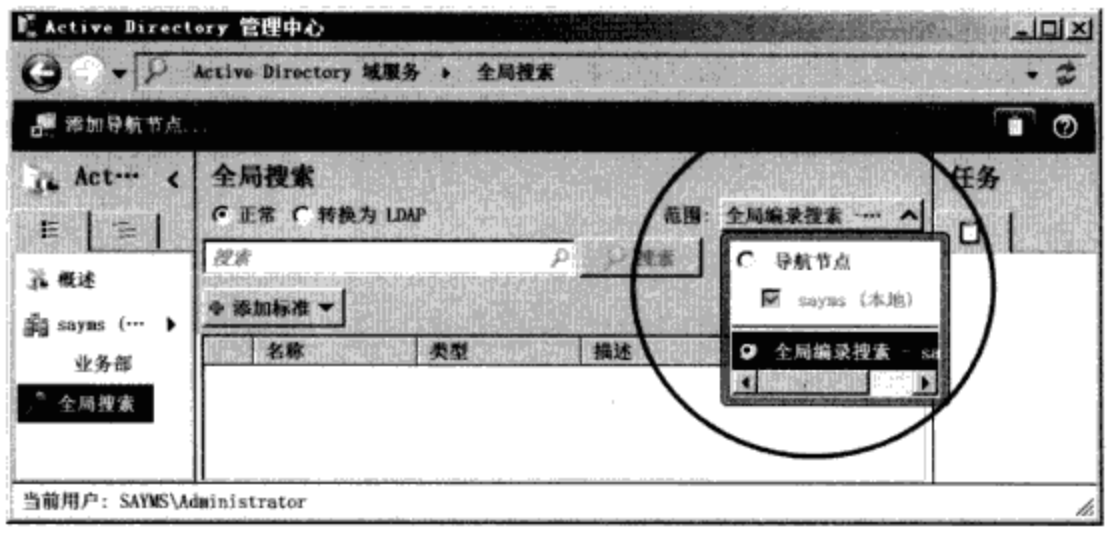


图3-19

您也可以通过图 3-20中的**概述**界面来运行全局搜索操作。

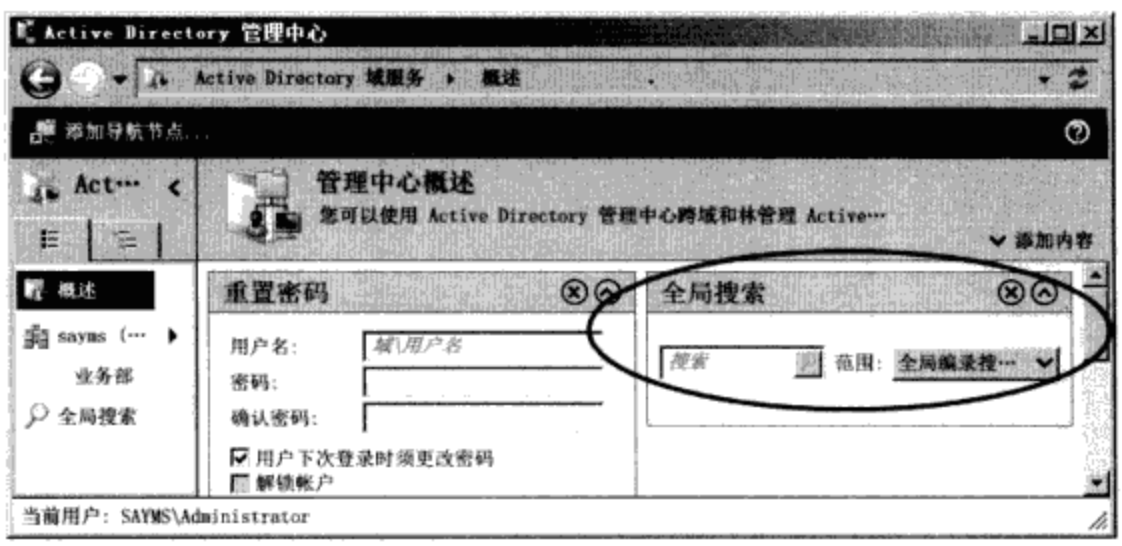


图3-20

Download at http://www.pin5i.com/

您可以进一步通过指定的条件来搜索用户账户，例如若要搜索**业务部**内电话号码是空白的所有用户账户的话，则请按如图 3-21所示进行操作：【单击组织单位**业务部**中的添加标准按钮➲选择**类型**复选框➲单击添加按钮➲如图 3-22所示在**类型**处选择**等于**，然后输入**用户**】。

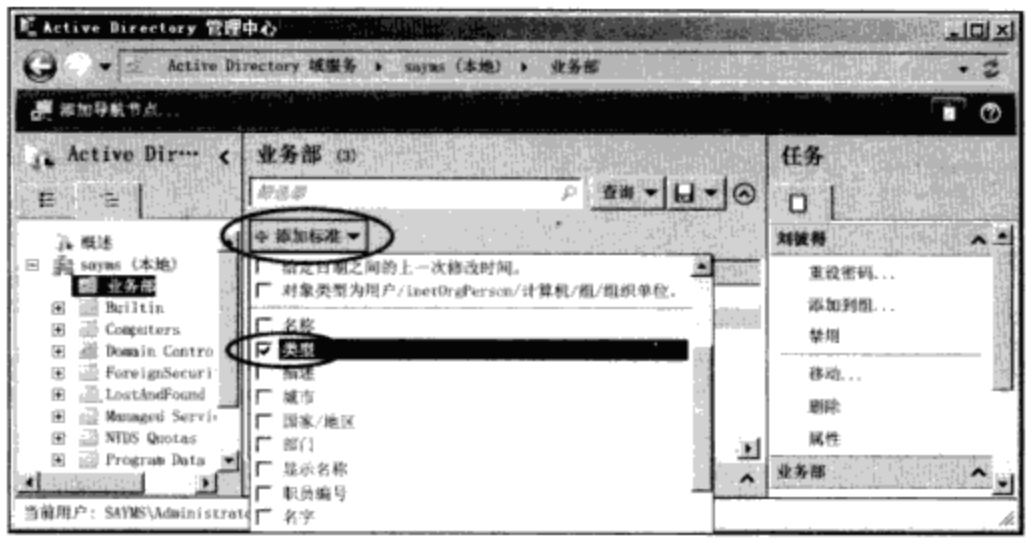


图 3-21

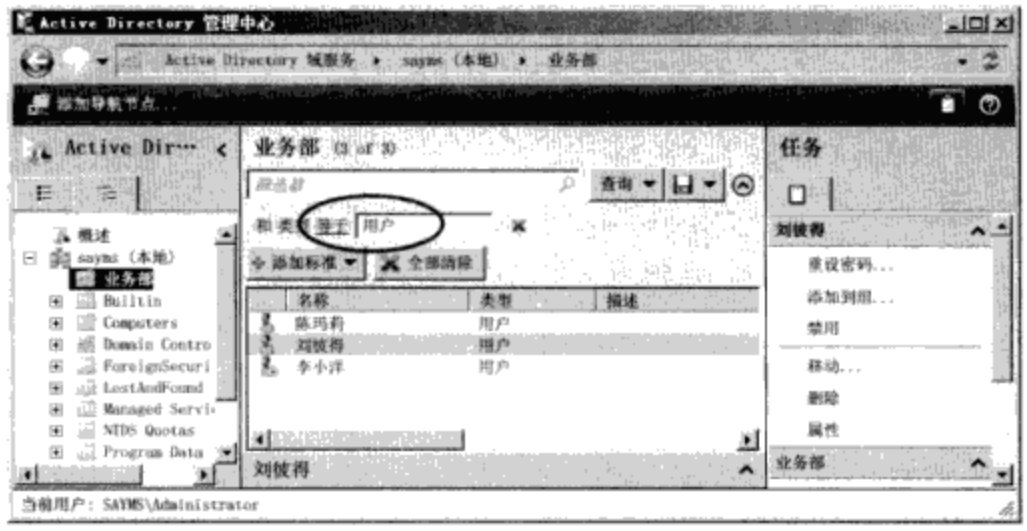


图 3-22

接着如图3-23所示，通过【单击添加标准按钮➲选择**电话号码**复选框➲单击添加按钮➲在图3-24中单击**起始为**➲选择**为空**】的方式进行操作，系统便会显示**业务部**内所有电话号码属性值是空白的用户账户。

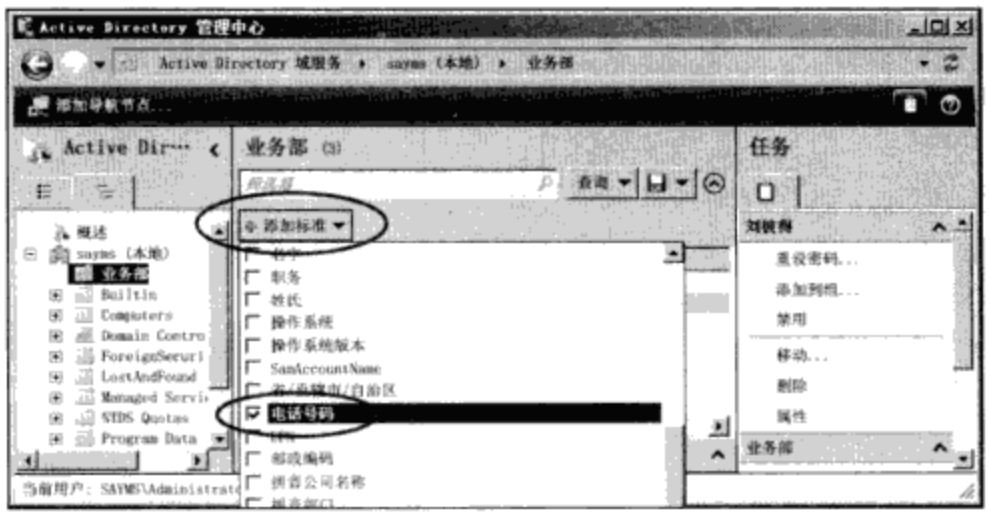


图 3-23

Download at http://www.pin5i.com/



图3-24

您可以将所定义的查询（搜索）条件保存起来，也就是单击图 3-25中的保存图标，之后可以通过此查询内所定义的条件来搜索，如图 3-26所示。

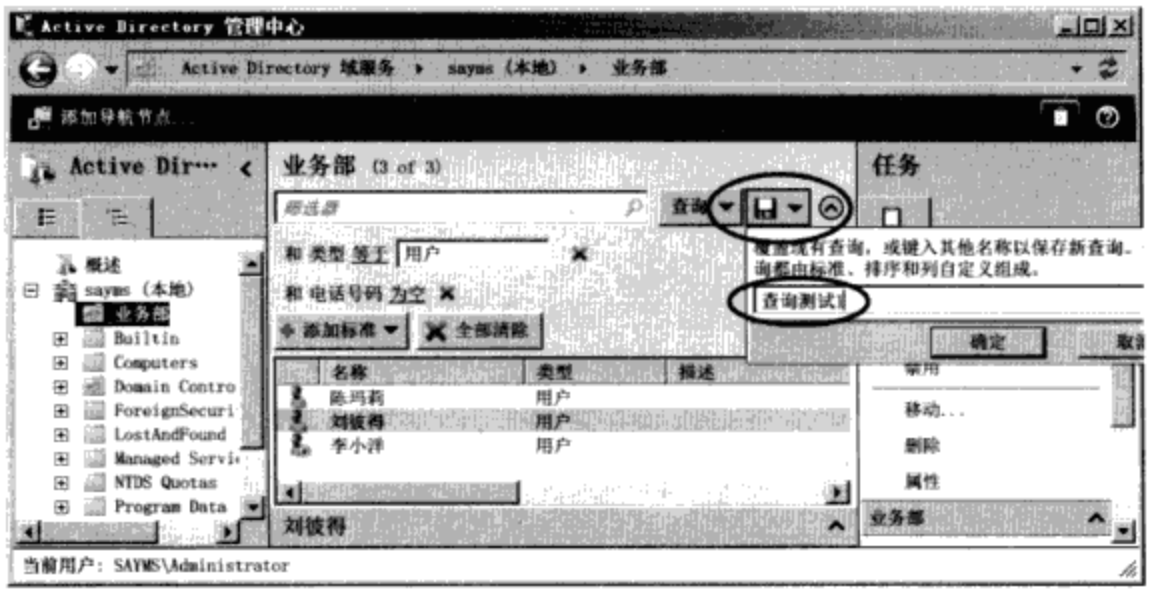


图3-25

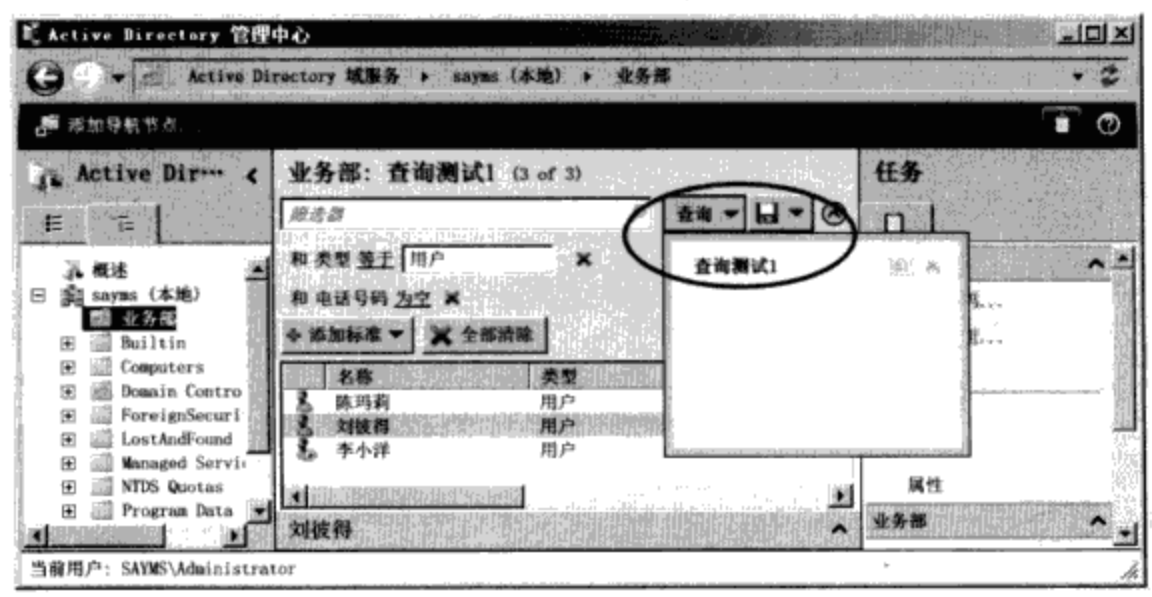


图3-26

若要在没有安装**Active Directory管理中心**的成员服务器或其他成员计算机上来搜索

Download at http://www.pin5i.com/

Active Directory对象的话，以Windows 7计算机为例，可以通过【开始➲计算机➲网络➲如图 3-27所示单击上方的**搜索Active Directory**】的方法来搜索。

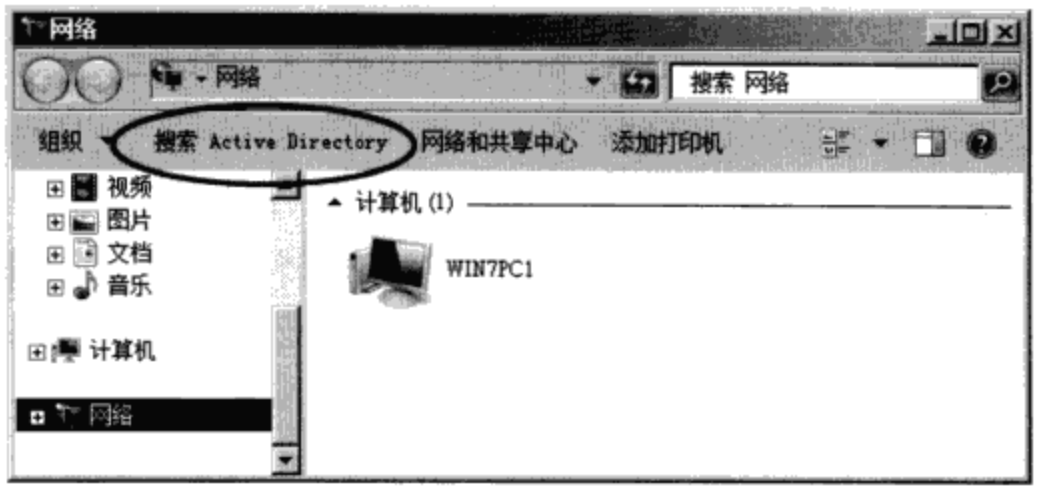


图 3-27

接着如图 3-28所示，在**查找**处选择**用户、联系人及组**，在**范围**处选择**整个目录**（也就是**全局编录**）或域名，在**名称**处输入要搜索的名称后单击开始查找按钮，然后就可以从最下面的**搜索结果**中查看和管理所找到的账户。

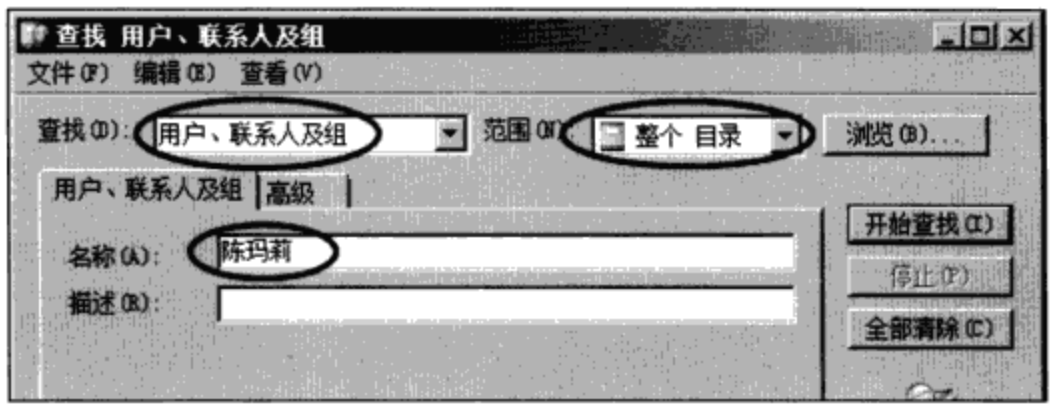


图 3-28

若要进一步通过指定条件来搜索用户账户的话，例如若要搜索**业务部**内电话号码是空白的所有用户账户的话，则请按如图 3-29所示进行操作：【单击**高级**标签➲通过**字段**来选择**用户**对象与**电话号码**属性➲**条件**选择**不存在**➲单击添加按钮➲单击开始查找按钮】，您可以同时设置多个搜索条件。

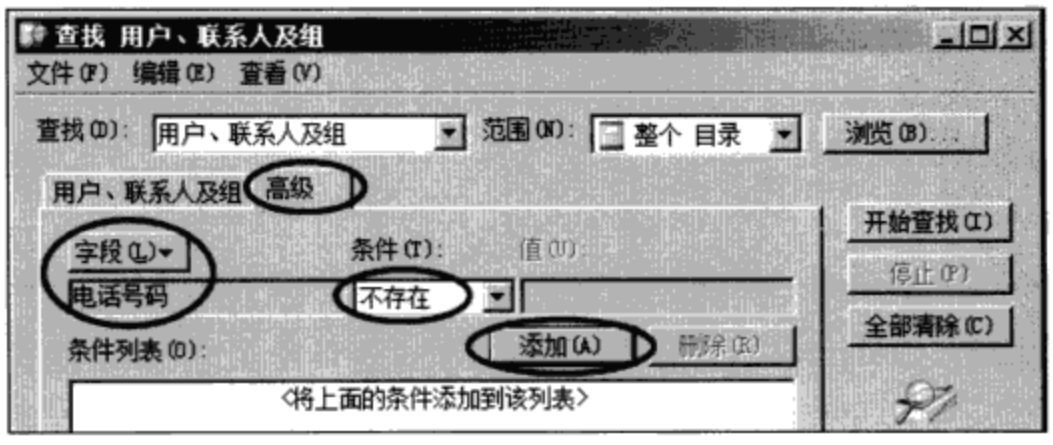


图 3-29

Download at http://www.pin5i.com/

3-1-7 域控制器之间数据的复制

若域内有多台域控制器的话，则当您更改Active Directory数据库内的数据时，例如使用**Active Directory管理中心**（或**Active Directory用户和计算机**）来添加、删除、修改用户账户或其他对象，则这些变动数据会先被存储到您所连接的域控制器，之后再自动被复制到其他域控制器。

您可以如图3-30所示通过【对着域名单击右键➲更改域控制器➲当前域控制器】的方法来得知当前所连接的域控制器，例如图中的dc1.sayms.com，而这台域控制器何时才会将其最新的变动数据复制给其他域控制器呢？可分为以下两种情况。



图3-30

- 自动复制：如果是同一个站点内的域控制器，则默认是15s后自动复制，因此其他域控制器可能会等15s或更久的时间才会收到这些最新的数据；如果是位于不同站点的域控制器，则需视情况来决定（详见第9章）。
- 手动复制：有时候可能需要使用手动方式来复制，例如因为网络故障造成前一次复制失败，而您不希望等到下一次的自动复制，而是能够立刻再执行复制工作。以下假设要从域控制器DC1复制到DC2。请到任何一台域控制器上通过【开始➲管理工具➲Active Directory站点和服务➲Sites➲Default-First-Site-Name➲Servers➲展开目的地域控制器（DC2）➲如图3-31所示单击**NTDS Settings**➲对着来源域控制器单击右键➲立即复制】的方式进行操作。

提示

如果是与**组策略**（Group Policy）有关的设置，则这些设置会先被存储到扮演**PDC模拟器操作主机**（PDC Emulator Operations Master）角色的域控制器内，然后再由**PDC模拟器操作主机**复制给其他的域控制器。**PDC模拟器操作主机**的说明请见第10章。

Download at http://www.pin5i.com/

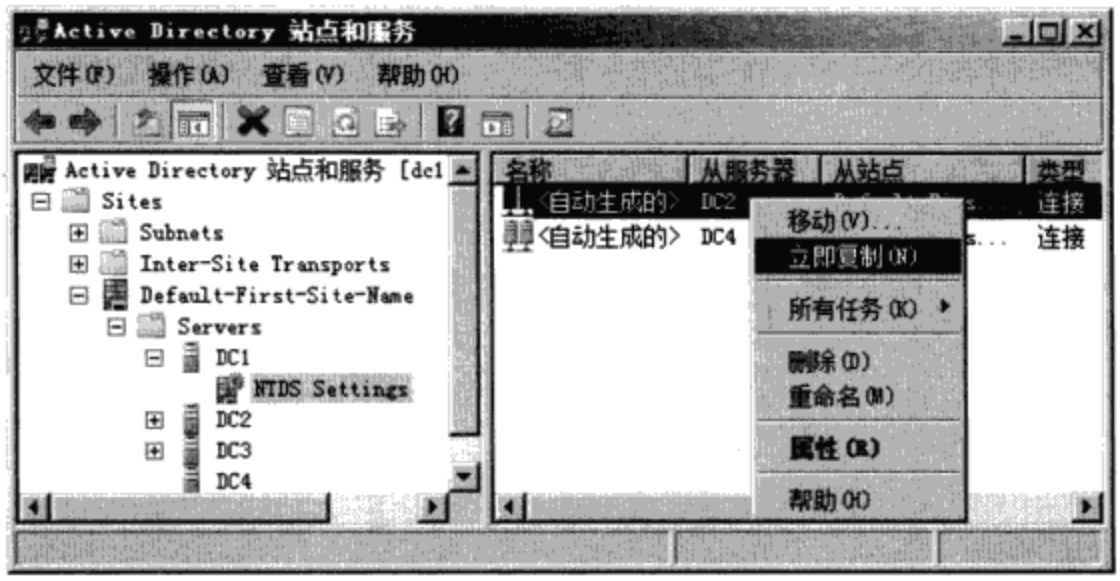


图 3-31

3-2 一次同时添加多个用户账户

如果您使用**Active Directory管理中心**（或**Active Directory用户和计算机**）的图形界面来创建大量用户账户的话，将浪费很多时间在重复操作相同的步骤，此时您可以使用系统内置的工具程序**csvde.exe**、**ldifde.exe**或**dsadd.exe**等来节省您创建用户账户的时间。

- csvde.exe：您可以使用它来添加用户账户（或其他类型的对象），但是不能够使用它来修改或删除用户账户。您需要事先将用户账户数据创建到纯文本文件（Text File）内，然后使用csvde.exe将文件内的这些用户账户一次同时导入到Active Directory数据库。
- ldifde.exe：您可以使用它来添加、删除、修改用户账户（或其他类型的对象）。您需要事先将用户账户数据创建到纯文本文件内，然后使用ldifde.exe将文件内的这些用户账户一次同时导入到Active Directory数据库。
- dsadd.exe、dsmod.exe与dsrm.exe：dsadd.exe用来添加用户账户（或其他类型的对象）、dsmod.exe用来修改用户账户、dsrm.exe用来删除用户账户。您需要先创建批处理文件，然后使用这3个程序将要添加、修改或删除的用户账户创建到此批处理文件中。

以csvde.exe与ldifde.exe这两个程序为例，您需要先使用可以编辑纯文本文件的程序（例如**记事本**）来将用户账户数据创建到文件内：

- 必须指明要将用户账户创建到何处，也就是需指定存储路径（Distinguished Name，DN）。
- 必须包含对象的类型，例如user。
- 必须包含**用户SamAccountName登录**。
- 应该要包含**用户UPN登录**。
- 可以包含用户的其他信息，例如电话号码、地址等。
- 无法设置用户的密码。
- 由于所创建的用户账户都没有密码，因此最好指定将用户账户禁用。

Download at http://www.pin5i.com/

3-2-1 使用csvde.exe来添加用户账户

我们将使用**记事本**（Notepad）来说明如何创建以供csvde.exe使用的文件，此文件的内容如图 3-32所示。

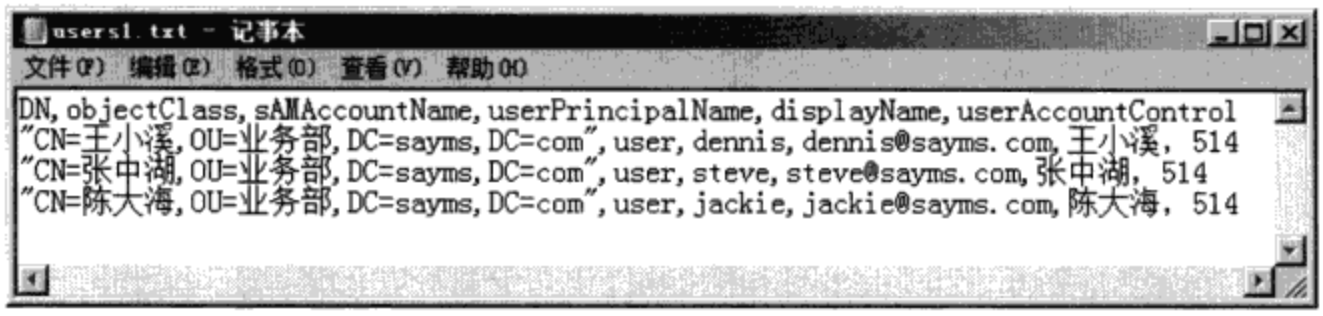


图 3-32

图中第2行（含）以后都是要创建的每一个用户账户的属性数据，各属性数据之间使用逗号（，）隔开。第1行是用来定义第2行（含）以后相对应的每一个属性。例如第1行的第1个字段为DN（Distinguished Name），表示第2行开始每一行的第1个字段代表新对象的存储路径；又例如第1行的第二个字段为objectClass，表示第2行开始每一行的第2个字段代表新对象的对象类型。我们使用图中的数据进行说明，如表3-1所示。

表3-1 属性说明

属性	值与说明
DN（Distinguished Name）	CN=王小溪，OU=业务部，DC=sayms，DC=com：对象的存储路径
objectClass	user：对象类型
sAMAccountName	dennis：**用户SamAccountName登录**
userPrincipalName	dennis@sayms.com：**用户UPN登录**
displayName	王小溪：显示名称
userAccountControl	514：表示禁用此账户（512表示启用）

文件创建好后，请打开**命令提示符**窗口（或单击**Windows PowerShell**图标），然后运行以下命令（参考图 3-33），假设文件名为users1.txt，且文件是位于C:\Test文件夹内：

```
csvde  -i  -f  c:\test\users1.txt
```

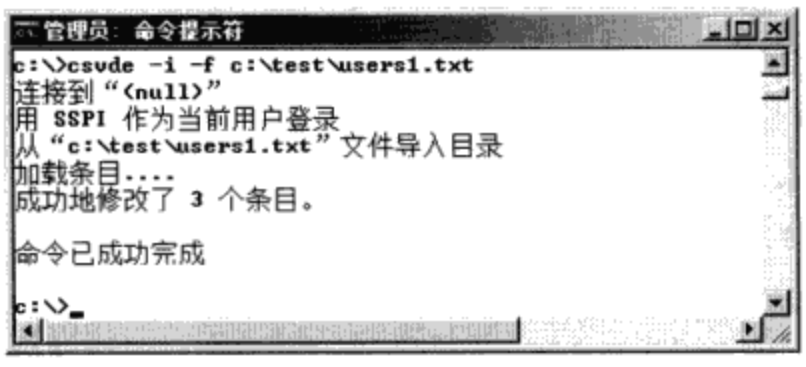


图 3-33

Download at http://www.pin5i.com/

图 3-34为执行后所创建的账户，图中向下箭头符号表示账户被禁用。

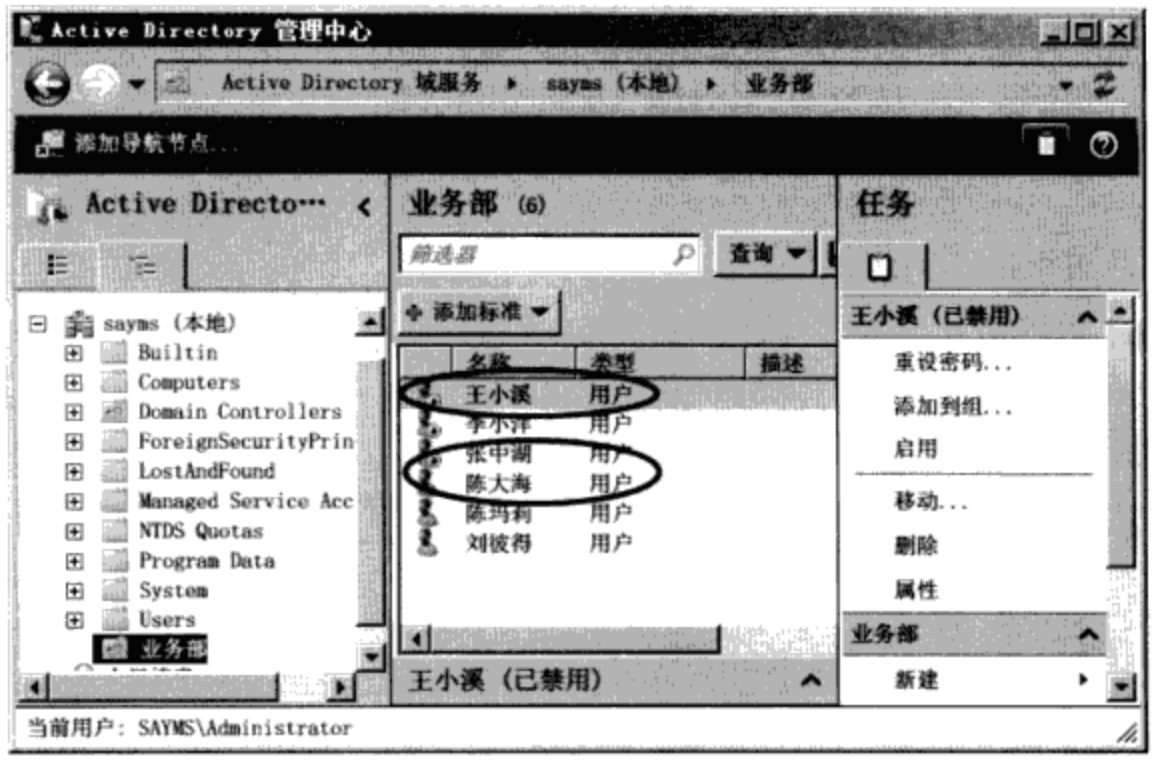


图 3-34

3-2-2 使用ldifde.exe来添加、修改与删除用户账户

以下我们使用**记事本**来说明如何创建以供ldifde.exe使用的文件。此文件的内容类似于图3-35。



图 3-35

请参考图 3-36来创建文件，若此文件最后还要添加其他账户的话，请在减号之后至少空一行后再输入数据。注意保存时需按如图 3-36所示在**编码**下拉列表中选择**Unicode**，否则文件内的中文字在导入到Active Directory数据库时会有问题。

Download at http://www.pin5i.com/

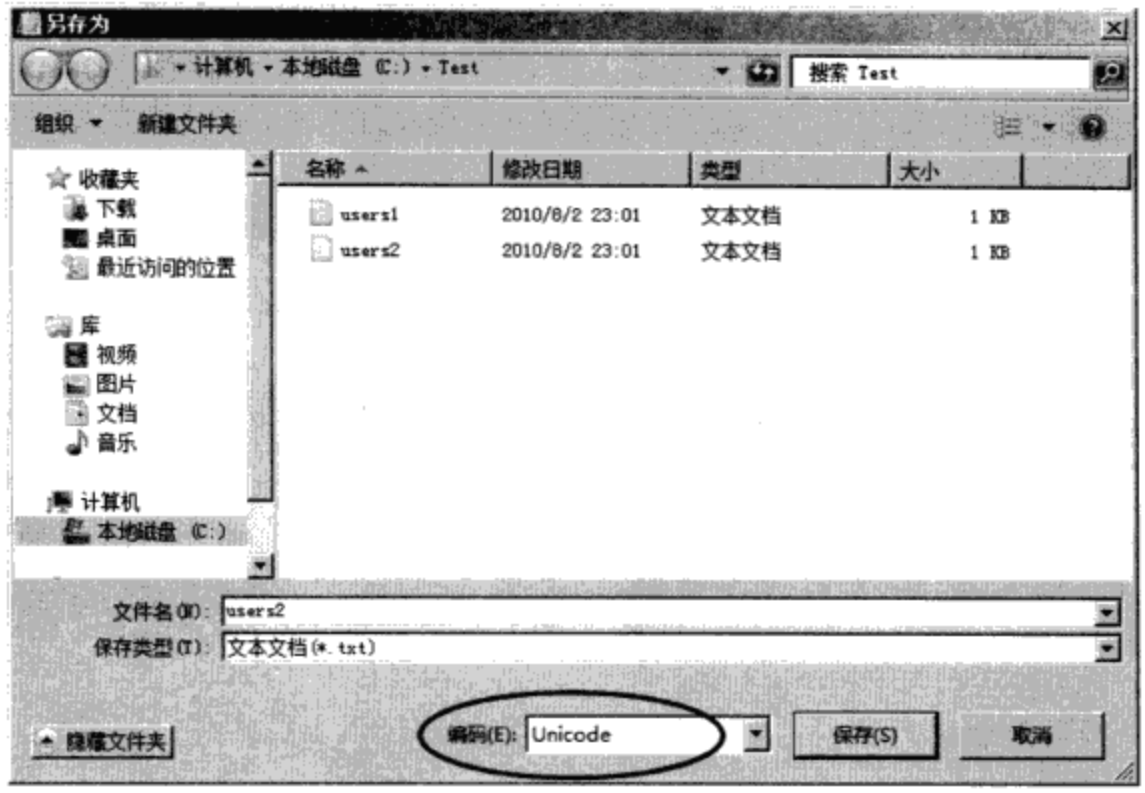


图 3-36

完成后请打开**命令提示符**窗口（或单击**Windows PowerShell**图标），然后运行以下命令（参考图 3-37），假设文件名为users2.txt，且文件是位于C:\Test文件夹内：

```
ldifde  -i  -f  c:\test\users2.txt
```

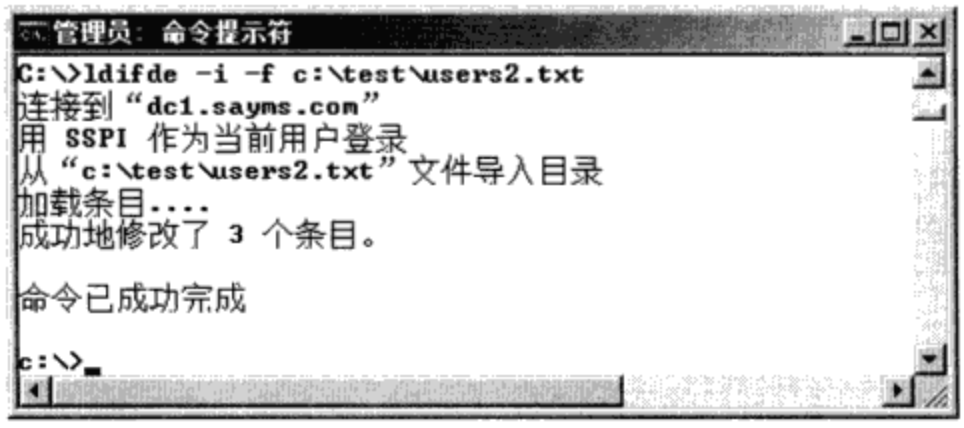


图 3-37

若要将数据导入到指定的域控制器的话，请加入**-s** 参数，例如：

```
ldifde -s  dc1.sayms.com  -i  -f  c:\test\users2.txt
```

> **提示**
>
> csvde与ldifde命令的详细语法可使用**csvde /?**与**ldifde /?**来查看。

3-2-3 使用dsadd.exe等程序来添加、修改与删除用户账户

以下使用**记事本**来说明如何创建一个批处理文件（Batch File），然后将dsadd、dsmod与dsrm命令输入到此文件内，并使用它们来添加、修改与删除用户账户。此文件的内容类似于图

Download at http://www.pin5i.com/

3-38，图中针对这3个命令各列举一个范例。

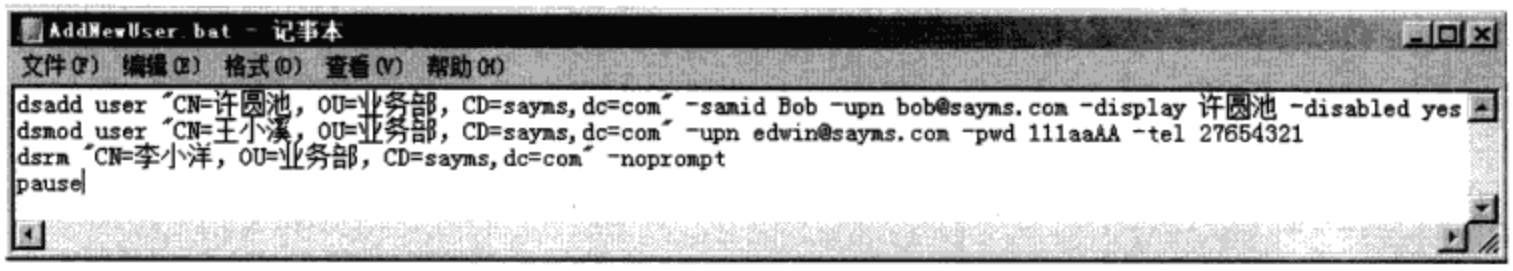


图 3-38

- 第1行dsadd命令：它用来添加一个位于**CN=许圆池,OU=业务部,CD=sayms,dc=com** 的用户账户，其中的**-samid Bob**用来将其用户SamAccountName登录设置为Bob 、 **-upn bob@sayms.com**用来将其用户UPN登录设置为bob@sayms.com、**-display许圆池**用来将其显示名称设置为许圆池、**-disabled yes**表示禁用此账户。
- 第2行dsmod命令：用来修改位于**CN=王小溪,OU=业务部,CD=sayms,dc=com**的用户账户，其中**-upn edwin@sayms.com**用来将其用户UPN登录更改为edwin@sayms.com、**-pwd 111aaAA**用来将其密码更改为111aaAA、**-tel 27654321**用来将其电话号码更改为27654321。
- 第3行dsrm命令：用来删除位于**CN=李小洋,OU=业务部,CD=sayms,dc=com**的用户账户，其中的 **–noprompt**表示不显示删除确认的界面。
- 最后一行的pause命令是为了让界面暂停，以便检查执行的结果。

请参考图3-38来创建文件，注意保存时因为**记事本**默认会自动附加.txt的扩展名（系统默认会隐藏扩展名），然而我们必须将其存储成扩展名是.bat或.cmd的文件，因此保存时请按如图3-39所示在文件名前后附加双引号，例如“AddNewUser.bat”，否则其扩展名将是.txt。

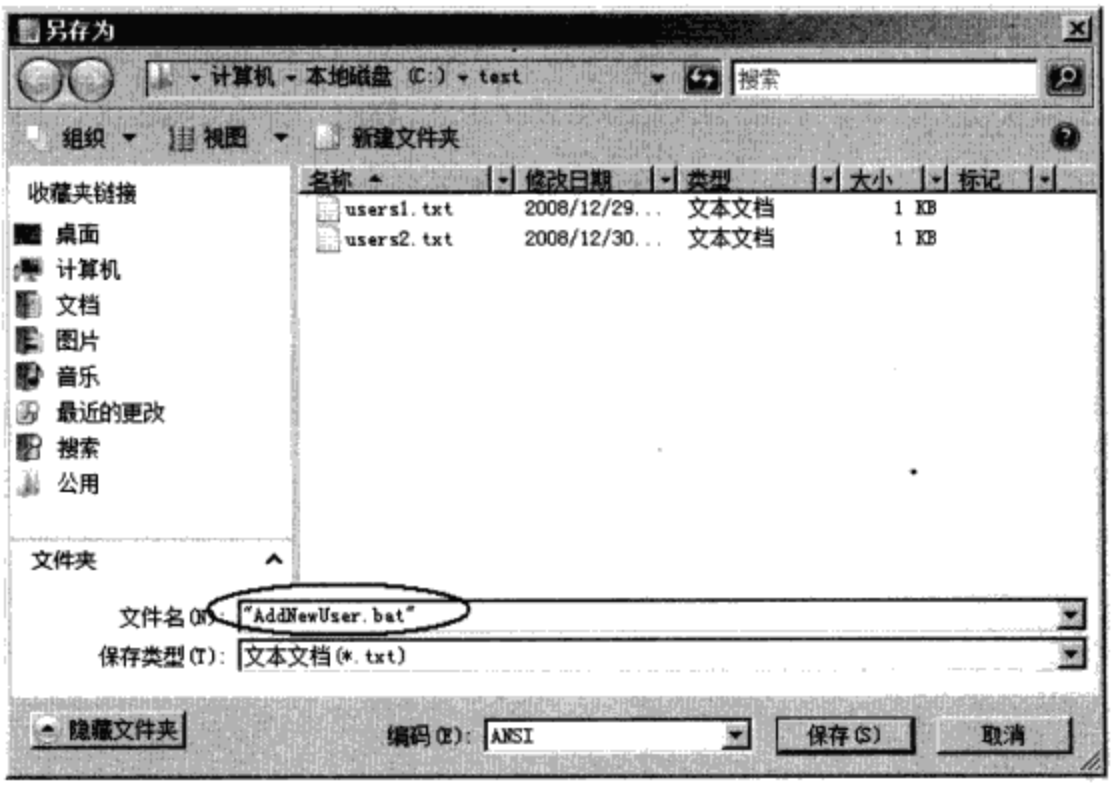


图 3-39

Download at http://www.pin5i.com/

完成后请通过直接在**Windows资源管理器**内双击此批处理文件的方式来执行它，此时系统会依序运行此文件内的命令，如图 3-40所示。

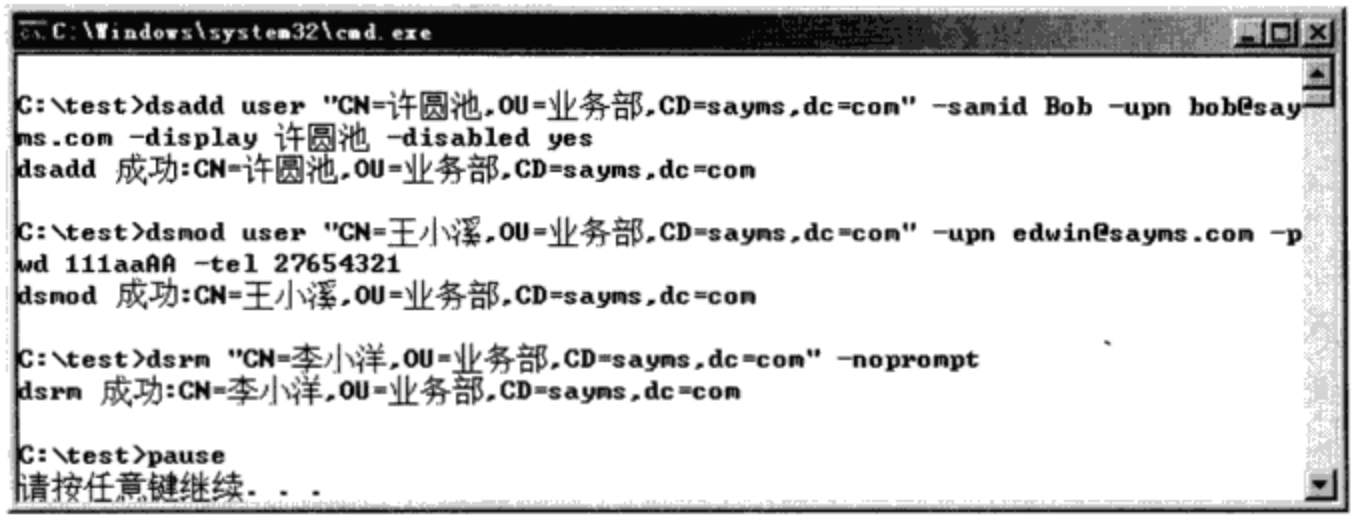


图3-40

提示

dsadd.exe、dsmod.exe与dsrm.exe等3个程序还有许多参数可以使用，其详细语法请使用**dsadd /?**、**dsmod /?**与**dsrm /?**来查看。

3-3 域组账户

如果能够善用组（Group）来管理用户账户，则必定能够减轻许多网络管理的负担。例如当您针对**业务部**组设置权限后，**业务部**组内的所有用户都会自动拥有此权限，因此就不需要个别针对每一个用户来设置。

提示

域组账户也都有唯一的安全标识符（Security Identifier，SID）。

3-3-1 域内的组类型

AD DS的域组可分为以下两种类型，且它们之间可以相互转换。

- 安全组（Security Group）：它可以被用来指定权限与权利，例如您可以指定安全组对文件具备**读取**的权限。它也可以用在与安全无关的工作上，例如可以发送电子邮件给安全组。
- 发布组（Distribution Group）：它是被用在与安全（权限与权利的设置等）无关的工作上，例如您可以发送电子邮件给发布组，但是无法给予发布组权限与权利。

Download at http://www.pin5i.com/

3-3-2 组的使用范围

以组的使用领域（Scope）来看，域组可分为**本地域组**（Domain Local Group）、**全局组**（Global Group）与**通用组**（Universal Group）三种（如表 3-1所示）。

表 3-1

特性 \ 组	通用组	全局组	本地域组
可包含的成员	所有域内的用户、全局组、通用组	相同域内的用户与全局组	所有域内的用户、全局组、通用组；相同域内的本地域组
可以在哪一个域内被设置权限	所有域	所有域	同一个域
组转换	可以被转换成本地域组；可以被转换成全局组（只要原组内的成员不含通用组即可）	可以被转换成通用组（只要原组不隶属于任何一个全局组即可）	可以被转换成通用组（只要原组内的成员不含本地域组即可）

1. 本地域组

本地域组主要是被用来指派访问权限，不过只能够将同一个域内的资源的权限指派给本地域组，以便可以访问此域内的资源：

- 本地域组内的成员，可以包含林中任何一个域内的用户、全局组、通用组；它也可以包含相同域内的本地域组，但是无法包含其他域内的本地域组。
- 本地域组只能够访问所属域内的资源，无法访问其他不同域内的资源；换句话说当您在设置权限时，您只可以设置相同域内的本地域组的权限，但是无法设置其他不同域内的本地域组的权限。

2. 全局组

全局组主要是用来组织用户，也就是您可以将多个即将被赋予相同权限的用户账户，加入到同一个全局组内：

- 全局组内的成员，只能够包含相同域内的用户与全局组。
- 全局组可以访问林中任何一个域内的资源，也就是说您可以在任何一个域内设置全局组的权限（此全局组可以位于任何一个域内），以便让此全局组具备权限来访问此域内的资源。

3. 通用组

通用组可以在所有域内被设置访问权限，以便访问所有域内的资源：

Download at http://www.pin5i.com/

- 通用组具备**通用领域**的特性，其成员能够包含林中任何一个域内的用户、全局组、通用组，但是无法包含任何一个域内的本地域组。
- 通用组可以访问林中任何一个域内的资源，也就是说您可以在任何一个域内来设置通用组的权限（此通用组可以位于任何一个域内），以便让此通用组具备权限来访问此域内的资源。

3-3-3 域组的创建与管理

1. 组的添加、删除与重命名

要添加域组时，可通过【开始➲管理工具➲Active Directory管理中心➲选择域名➲对着任何一个容器或组织单位单击右键➲添加➲组】的方法进行操作，然后在图3-41中输入组名、输入供旧版操作系统（例如Windows NT）来访问的组名、选择组类型与组范围等。若要删除组的话，可通过【对着组账户右击➲删除】的方法进行操作。

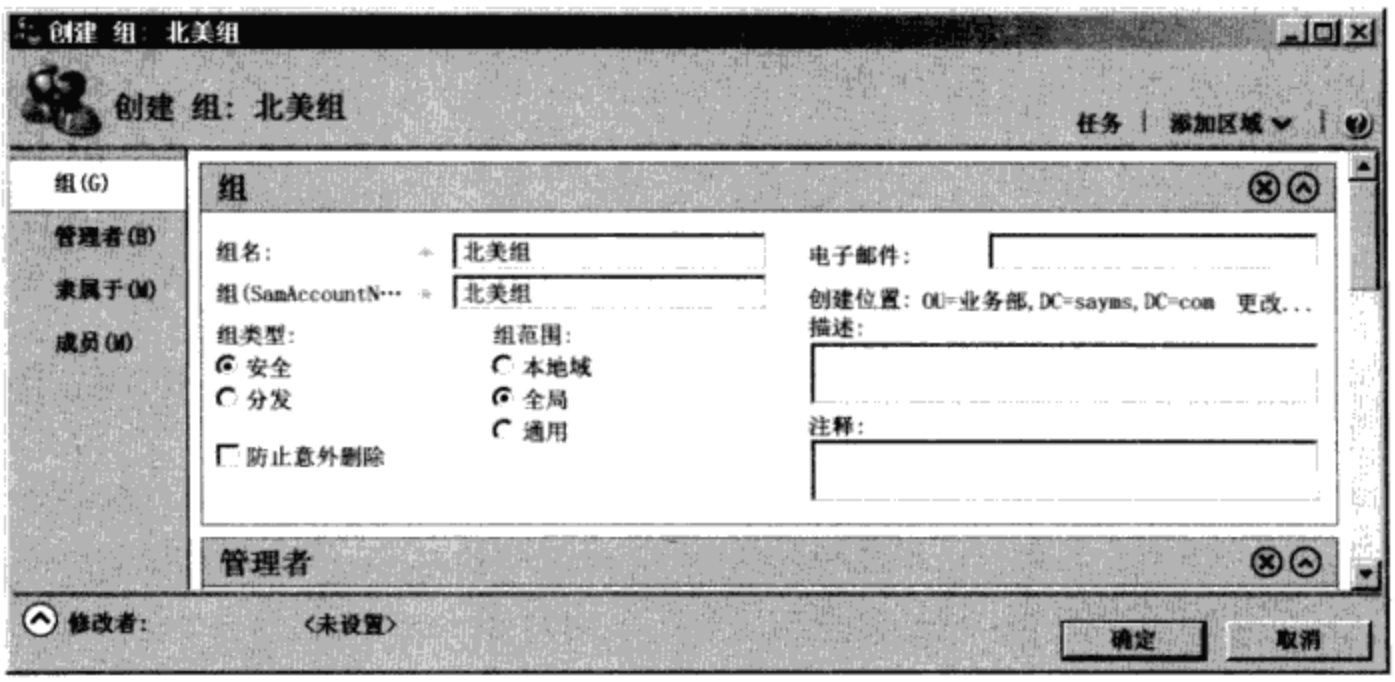


图3-41

2. 新增组的成员

若要将用户、组等加入到组内的话，可通过【如图3-42所示，单击**成员**选项组右方的添加按钮➲单击高级按钮➲单击立即查找按钮➲在图3-43中选择要被加入的成员（单击Shift或Ctrl键可同时选择多个账户）➲单击确定按钮➲…】的方法进行操作。

Download at http://www.pin5i.com/

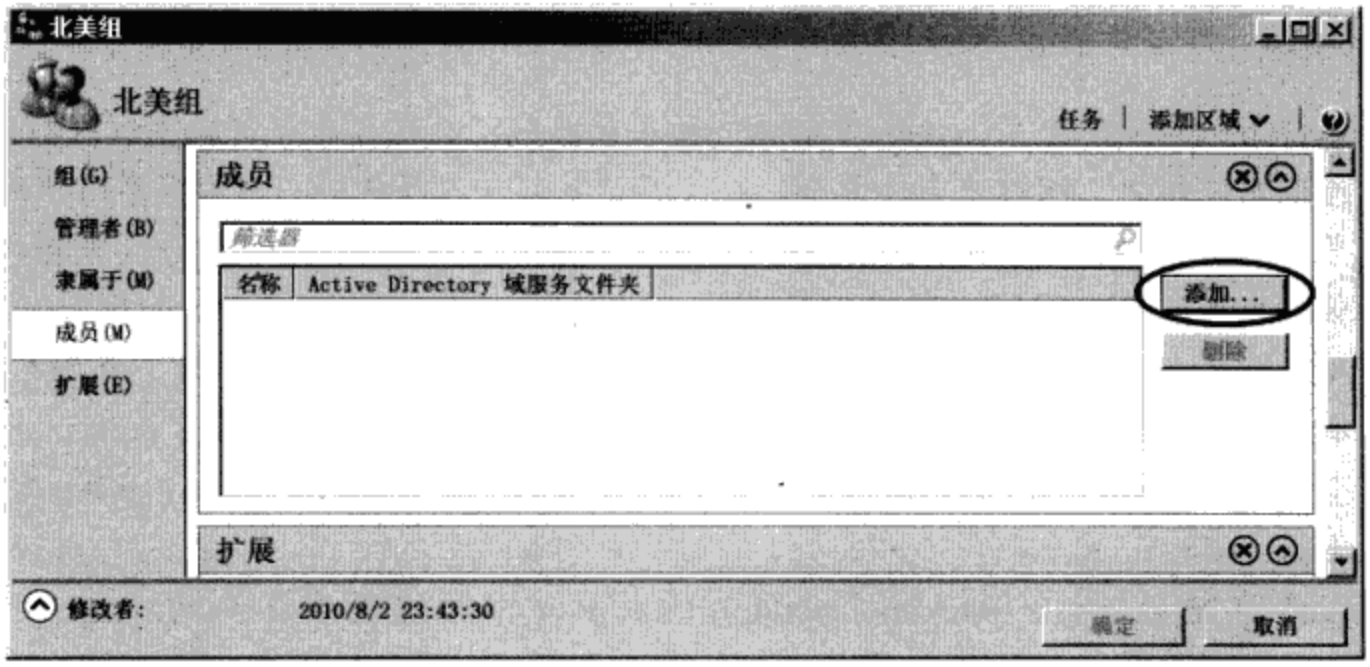


图 3-42

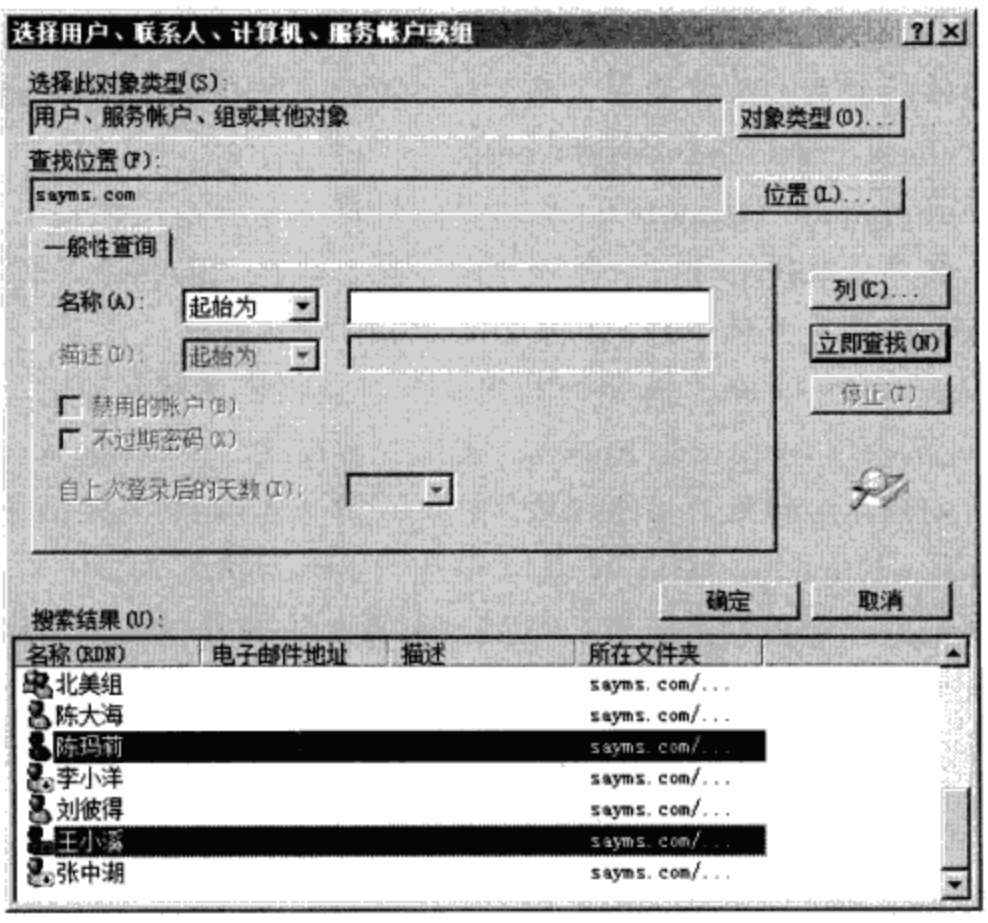


图 3-43

3-3-4 AD DS内置的组

AD DS内有许多内置组，它们分别隶属于本地域组、全局组、通用组。

1. 内置的本地域组

这些本地域组本身已被赋予一些权利与权限，以便让其具备管理AD DS的能力。只要您将用户或组账户加入到这些内置的本地域组内，这些账户也会自动具备相同的权利与权限。以下

Download at http://www.pin5i.com/

列出一些较常用的本地域组，它们位于容器Builtin内。

- Account Operators: Account Operators的成员默认可以在容器与组织单位内添加/删除/修改用户账户、组账户与计算机账户，不过有部分容器例外，例如容器Builtin与组织单位Domain Controllers，同时也不允许在部分容器内添加计算机账户，例如Users。他们也无法修改或删除某些组的成员，例如Administrators、Backup Operators等。
- Administrators: Administrators的成员具备系统管理员权限，他们对所有域控制器拥有最大控制权，可以执行AD DS管理工作。此组默认的成员包含了Administrator、全局组Domain Admins、通用组Enterprise Admins，您无法将Administrator从此组内删除。
- Backup Operators: Backup Operators的成员可以通过图形界面的Windows Server Backup功能或wbadmin.exe程序来备份与还原域控制器内的文件，不论它们是否有权限访问这些文件。Backup Operators的成员也可以将域控制器关机。
- Guests: 此组内的用户无法永久改变其桌面的工作环境，当他们登录时，系统会为他们创建一个临时的用户配置文件，而注销时此配置文件就会被删除。此组默认的成员为用户账户Guest与全局组Domain Guests。
- Network Configuration Operators: 此组内的用户，可以在域控制器上运行常规的网络设置操作，例如更改IP地址，但是不可以安装、删除驱动程序与服务，也不可以运行与网络服务器设置有关的工作，例如DNS与DHCP服务器的设置。
- Performance Monitor Users: 此组内的用户可以监视域控制器的运行效率。
- Pre-Windows 2000 Compatible Access: 此组主要是为了与Windows NT 4.0兼容，其成员可以访问AD DS内的用户与组账户。默认成员为特殊组Authenticated Users。只有在用户的计算机是Windows NT 4.0时，才将用户加入到此组内。
- Print Operators: 此组内的成员可以在域控制器上管理打印机、将域控制器关机。
- Remote Desktop Users: 此组内的用户可以从远程计算机通过远程桌面服务登录。
- Server Operators: 此组内的成员可以备份与还原域控制器内的文件；锁定与解开域控制器；将域控制器上的硬盘格式化；更改域控制器的系统日期与时间；将域控制器关机等。
- Users: 此组的成员只拥有一些基本权限，例如运行应用程序，但是他们不能修改操作系统的设置、不能更改其他用户的数据、不能将服务器关机。此组默认的成员为全局组Domain Users。

2. 内置的全局组

AD DS内置的全局组本身并没有任何的权利与权限，但是可以将其加入到具备权利或权限的本地域组，或另外直接指派权利或权限给此全局组。这些内置全局组位于容器Users内。以下列出较常用的全局组。

- Domain Admins: 域成员计算机会自动将此组加入到本地组Administrators内，因此

Download at http://www.pin5i.com/

Domain Admins组内的每一个成员，在域内的每一台计算机上都具备系统管理员权限。此组默认的成员为域用户Administrator。

- Domain Computers: 所有加入域的计算机都会被自动加入到此组内。
- Domain Controllers: 域内所有域控制器都会被自动加入到此组内。
- Domain Users: 域成员计算机会自动将此组加入到本地组Users内，因此Domain Users内的用户享有本地组Users所拥有的权利与权限，例如拥有**允许本地登录**的权利。此组默认的成员为域用户Administrator，而以后所有添加的域用户账户都自动会隶属于此Domain Users组。
- Domain Guests: 域成员计算机会自动将此组加入到本地组Guests内。此组默认的成员为域用户账户Guest。

3. 内置的通用组

以下列出常用的内置通用组。

- Enterprise Admins: 此组只存在于林根域，其成员有权管理林内的所有域。此组默认的成员为林根域内的用户Administrator。
- Schema Admins: 此组只存在于林根域，其成员具备管理**架构**（Schema）的权利。此组默认的成员为林根域内的用户Administrator。

3-3-5 特殊组账户

除了前面所介绍的组之外，还有一些特殊组，而您无法更改这些特殊组的成员。以下列出几个较常使用的特殊组。

- Everyone: 任何一位用户都属于这个组。若Guest账户被启用的话，则您在指派权限给Everyone时需小心，因为若一位在您计算机内没有账户的用户通过网络来连接您的计算机时，他会被自动允许使用Guest账户来连接，此时因为Guest也是隶属于Everyone组，所以他将具备Everyone所拥有的权限。
- Authenticated Users: 任何使用有效用户账户来登录的用户，都属于这个组。
- Interactive: 任何在本地登录（单击Ctrl + Alt + Del登录）的用户，都属于这个组。
- Network: 任何通过网络来登录的用户，都属于这个组。
- Anonymous Logon: 任何未使用有效的一般用户账户来登录的用户，都隶属于此组，不过Anonymous Logon默认并不隶属于Everyone组。
- Dialup: 任何使用拨号连接方式来连接的用户，都隶属于此组。

3-4 组的使用准则

为了让网络管理更为容易，同时也为了减少以后维护的负担，因此在您使用组来管理网络

Download at http://www.pin5i.com/

资源时，建议您尽量采用以下的准则，尤其是大型网络：

- A、G、DL、P策略。
- A、G、G、DL、P策略。
- A、G、U、DL、P策略。
- A、G、G、U、DL、P策略。

A代表用户账户（user Account）、G代表全局组（Global group）、DL代表本地域组（Domain Local group）、U代表通用组（Universal group）、P代表权限（Permission）。

3-4-1 A、G、DL、P策略

A、G、DL、P策略就是先将用户账户（A）加入到全局组（G）、再将全局组加入到本地域组（DL）内，然后设置本地域组的权限（P），如图 3-44所示。以此图为例来说，只要针对图中的本地域组来设置权限，则隶属于该本地域组的全局组内的所有用户，都自动会具备该权限。

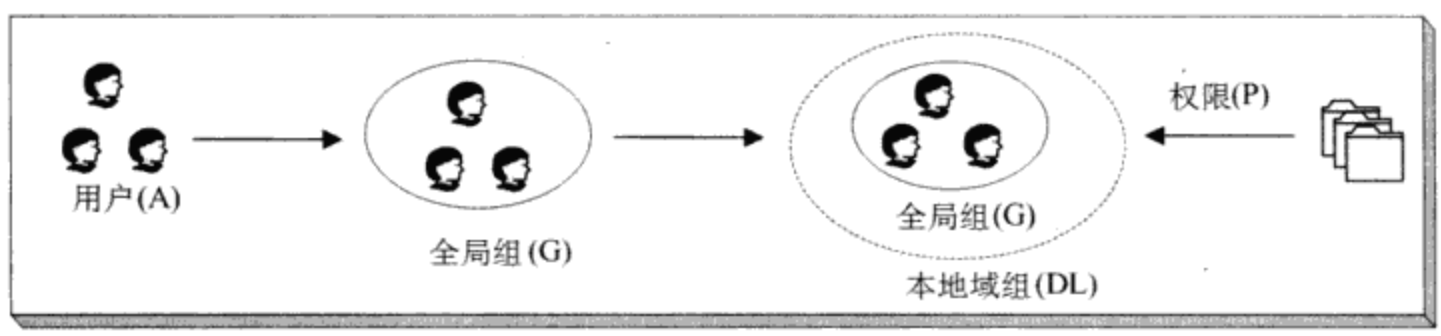


图3-44

举例来说，若甲域内的用户需要访问乙域内资源的话，则由甲域的系统管理员负责在甲域创建全局组、将甲域用户账户加入到此组内；而乙域的系统管理员则负责在乙域创建本地域组、设置此组的权限，然后将甲域的全局组加入到此组内。之后由甲域的系统管理员负责维护全局组内的成员，而乙域的系统管理员则负责维护权限的设置，如此便可以将管理的负担分散。

3-4-2 A、G、G、DL、P策略

A、G、G、DL、P策略就是先将用户账户（A）加入到全局组（G）、将此全局组加入到另一个全局组（G）内，再将此全局组加入到本地域组（DL）内，然后设置本地域组的权限（P），如图 3-45所示。图中的全局组（G3）内包含了两个全局组（G1与G2），它们必须是同一个域内的全局组，因为全局组内只能够包含位于同一个域内的用户账户与全局组。

Download at http://www.pin5i.com/

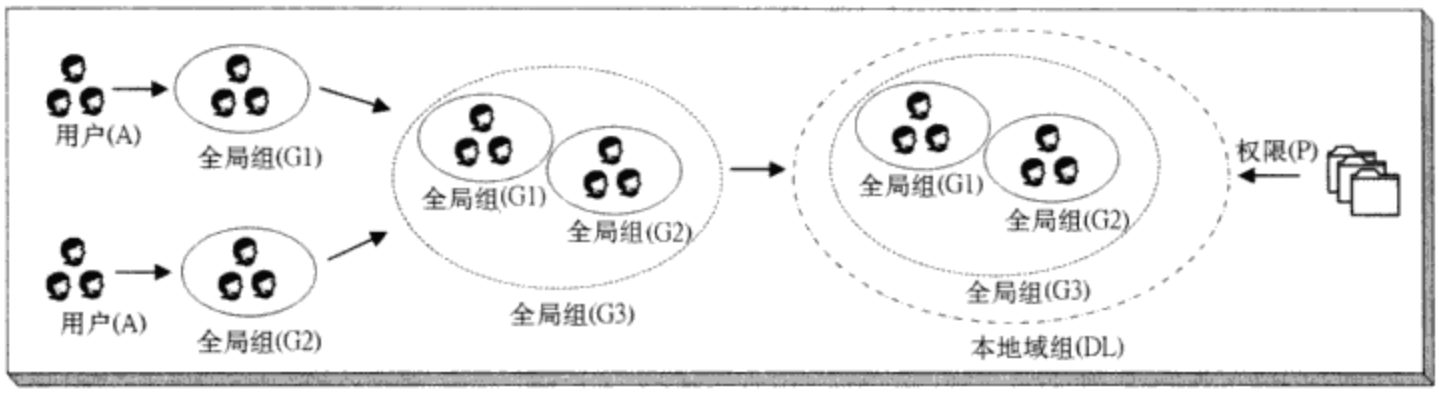


图 3-45

3-4-3 A、G、U、DL、P策略

图 3-45中的全局组G1与G2若不是与G3在同一个域内，则无法采用A、G、G、DL、P策略，因为全局组（G3）内无法包含位于另外一个域内的全局组，此时就必须将全局组G3改为通用组，也就是必须改用A、G、U、DL、P策略（如图3-46所示），此策略是先将用户账户（A）加入到全局组（G）、将此全局组加入到通用组（U）内，再将此通用组加入到本地域组（DL）内，然后设置本地域组的权限（P）。

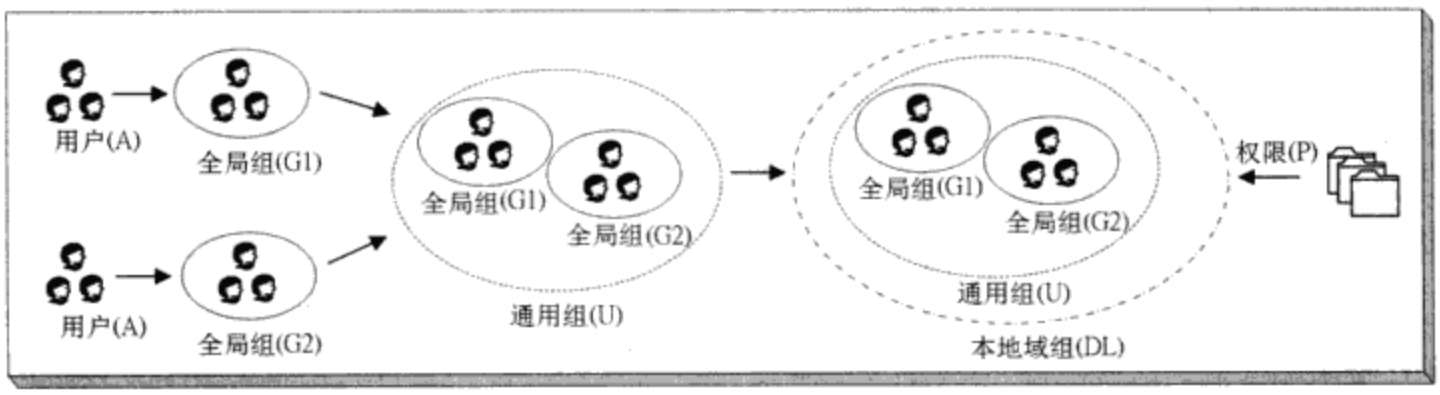


图 3-46

3-4-4 A、G、G、U、DL、P策略

A、G、G、U、DL、P策略与前面2种类似，在此不再重复说明。也可以不遵循以上的策略来使用组，不过会有一些缺点存在，例如可以：

- 直接将用户账户加入到本地域组内，然后设置此组的权限。它的缺点是并无法在其他域内设置此本地域组的权限，因为本地域组只能够访问所属域内的资源。
- 直接将用户账户加入到全局组内，然后设置此组的权限。它的缺点是如果网络内包含多个域，而每个域内都有一些全局组需要对此资源具备相同的权限的话，则需要分别为每一个全局组设置权限，这种方法比较浪费时间，会增加网络管理的负担。

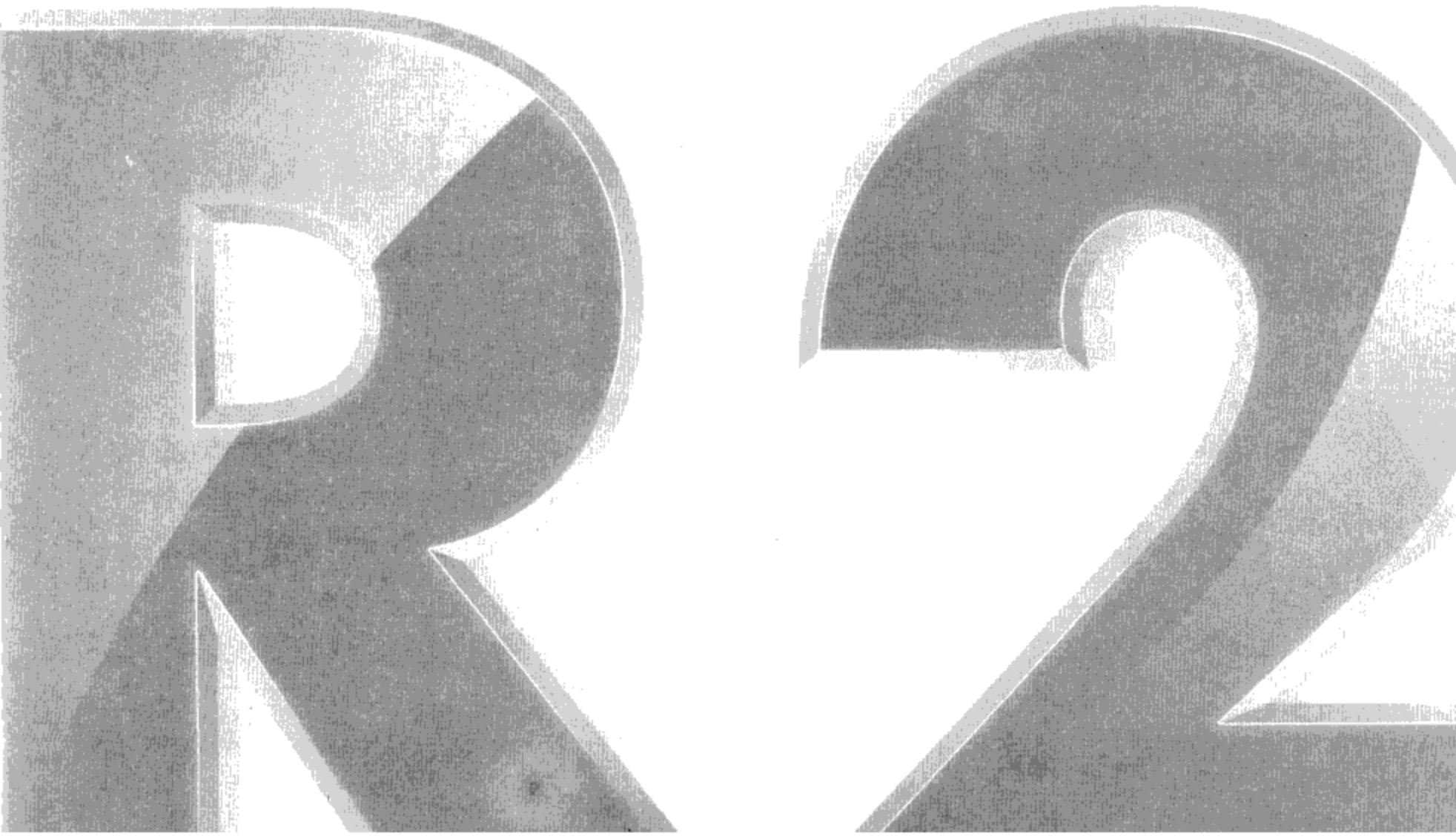
Download at http://www.pin5i.com/

第4章

使用组策略管理用户工作环境

通过AD DS的**组策略**（Group Policy）功能，可更容易地管理用户的工作环境与计算机环境、减轻网络管理负担、降低网络管理成本。

- 组策略概述
- 策略设置实例演练
- 首选设置实例演练
- 组策略的处理规则
- 利用组策略来管理计算机与用户环境
- 利用组策略来限制访问可移动存储设备
- WMI筛选器
- 组策略建模与组策略结果
- 组策略的委派管理
- Starter GPO的设置与使用



Download at http://www.pin5i.com/

4-1 组策略概述

组策略是一个能够让系统管理员充分管理用户工作环境的技术，通过它来确保用户拥有与权限相符的工作环境，也通过它来限制用户，如此不但可以让用户拥有适当的环境，也可以减轻系统管理员的管理负担。

4-1-1 组策略的功能

以下列举组策略所提供的主要功能。

- 账户策略的设置：例如设置用户的密码长度、密码使用期限、账户锁定策略等。
- 本地策略的设置：例如审核策略的设置、用户权限的分配、安全性的设置等。
- 脚本（Scripts）的设置：例如登录与注销、启动与关机脚本的设置。
- 用户工作环境的设置：例如隐藏用户桌面上所有的图标、删除**开始**菜单中的**运行**/**搜索**/**关机**等功能、在**开始**菜单中添加**注销**选项、删除浏览器内部分选项、强制通过指定的代理服务器上网等。
- 软件的安装与删除：用户登录或计算机启动时，自动为用户安装应用软件、自动修复应用软件或自动删除应用软件。
- 限制软件的运行：通过各种不同的软件限制规则来限制域用户只能运行指定的软件。
- 文件夹的重定向：例如改变**文件**、**开始**菜单等文件夹的存储位置。
- 限制访问可移动存储设备：例如限制将文件写入U盘，以免企业内的机密文件轻易地被带离公司。
- 其他众多的系统设置：例如让所有的计算机都自动信任指定的CA（Certificate Authority）、限制安装设备驱动程序（Device Driver）等。

您可以在AD DS中针对站点（Site）、域（Domain）与组织单位（OU）来设置组策略（如图 4-1所示）。

组策略内包含着**计算机配置**与**用户配置**两部分。

- 计算机配置：当计算机开机时，系统会根据**计算机配置**的属性来设置计算机的环境。举例来说，如果您针对域sayms.com设置了组策略，则此组策略内的**计算机配置**就会被应用到（Apply）这个域内的所有计算机。
- 用户配置：当用户登录时，系统会根据**用户配置**的属性来配置用户的工作环境。举例来说，若您针对组织单位**业务部**配置了组策略，则此组策略内的**用户配置**就会被应用到这个组织单位内的所有用户。

Download at http://www.pin5i.com/

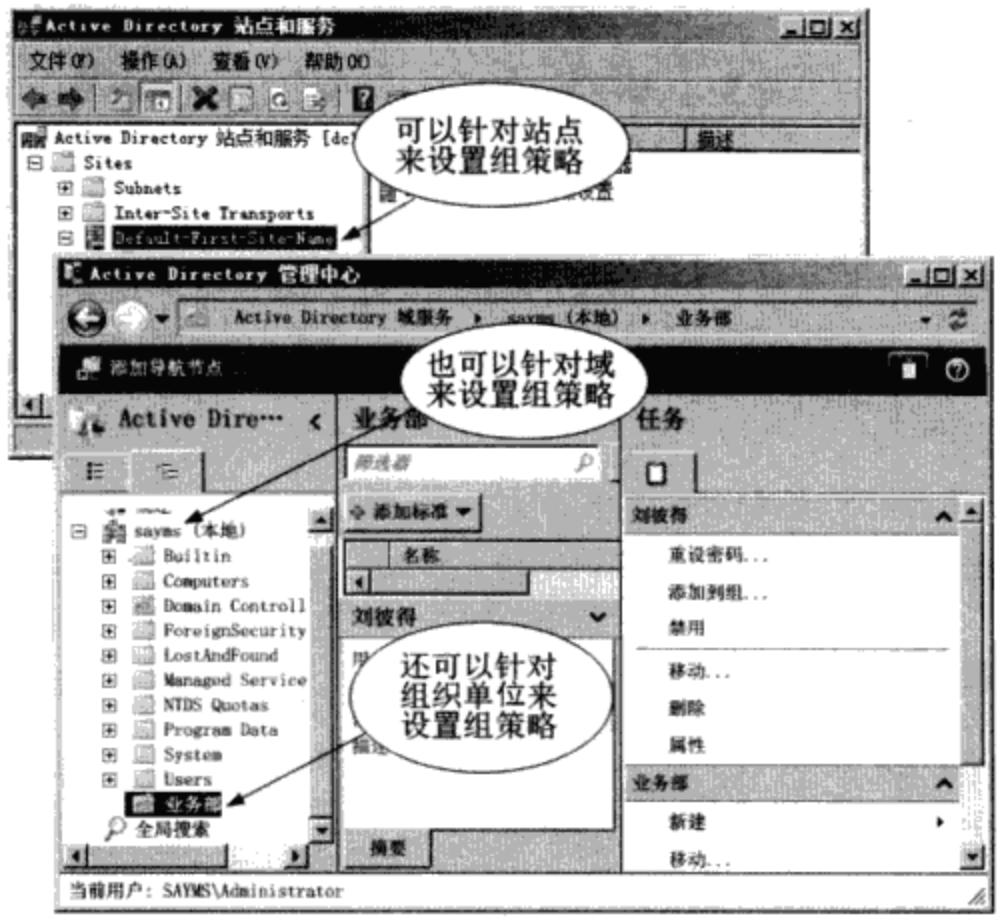


图4-1

除了可以针对站点、域与组织单位来配置组策略之外，您还可以在每一台计算机上配置**本地计算机策略**（Local Computer Policy），这个计算机策略只会应用到本地计算机与在此台计算机上登录的所有用户。

4-1-2 组策略对象

组策略是通过**组策略对象**（Group Policy Object，GPO）来设置的，而您只要将GPO链接（Link）到指定的站点、域或组织单位，此GPO内的设置值就会影响到该站点、域或组织单位内的所有用户与计算机。

1. 内置的 GPO

AD DS域已经有两个内置的GPO，其说明如下。

- Default Domain Policy: 此GPO默认已经被链接到域，因此其设置值会被应用到整个域内的所有用户与计算机。
- Default Domain Controller Policy: 此GPO默认已经被链接到组织单位Domain Controllers，因此其设置值会被应用到组织单位Domain Controllers内的所有用户与计算机。在组织单位Domain Controllers内，默认只有域控制器的计算机账户。

您可以通过【开始➲管理工具➲组策略管理➲如图 4-2所示】的方法来验证Default Domain Policy与Default Domain Controller Policy分别已经被链接到域sayms.com与组织单位Domain

Download at http://www.pin5i.com/

Controllers。

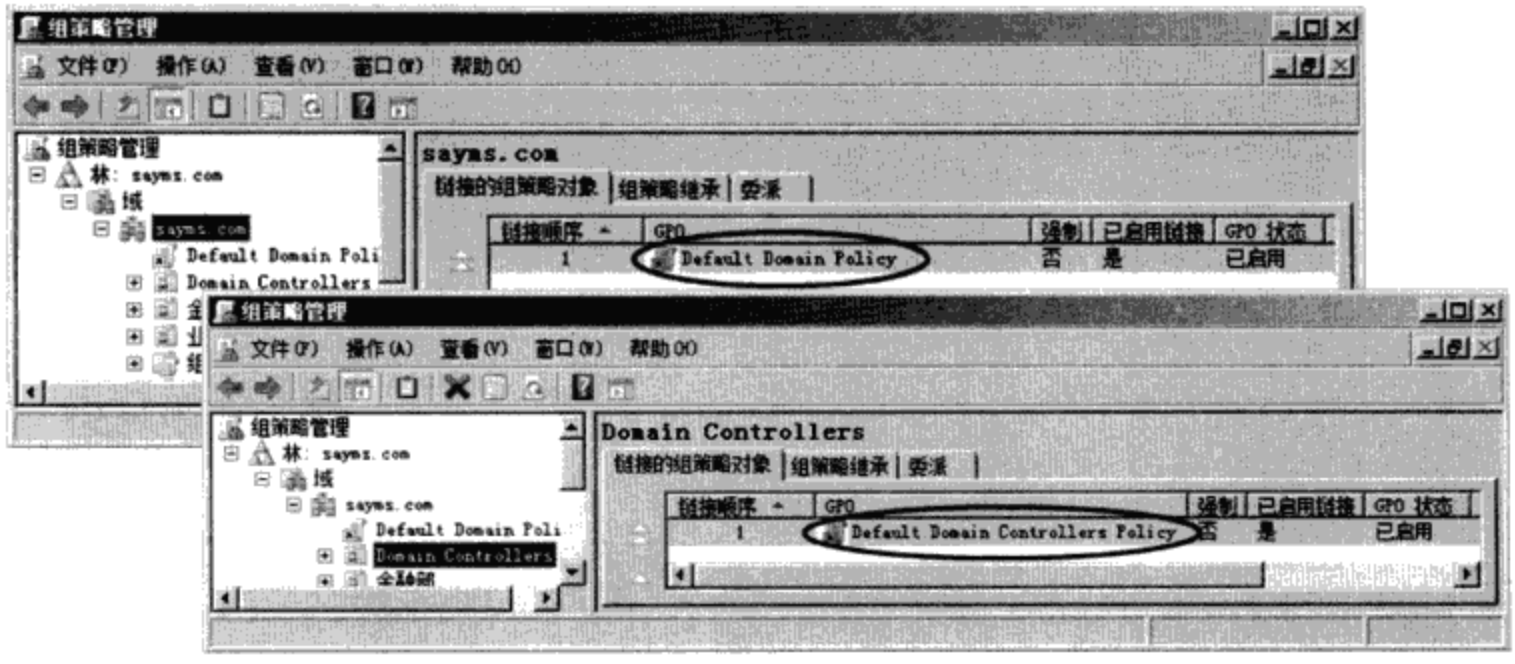


图4-2

注意

在尚未彻底了解组策略以前，请暂时不要随意更改Default Domain Policy或Default Domain Controller Policy这两个GPO的设置值，以免影响系统的正常运行。

2. GPO 的内容

GPO的内容被分为GPC与GPT两部分，它们分别被存储到不同的位置。

（1）GPC（Group Policy Container）

GPC是存储在Active Directory数据库内，它记录着此GPO的属性与版本等数据。域成员计算机可通过属性来获取GPT的存储地点，而域控制器可使用版本来判断其所拥有的GPO是否为最新版本，以便作为是否需要从其他域控制器复制最新GPO的依据。您可以通过以下方法来查看GPC：【开始➲管理工具➲Active Directory管理中心➲选择**树视图**图示➲单击域（例如sayms）➲展开容器**System** ➲如图 4-3所示单击**Policies**】图中间圈起来的部分为Default Domain Policy与Default Domain Controller Policy这两个 GPO的GPC，图中的数字分别是这两个 GPO的GUID （Global Unique Identifier）。

Download at http://www.pin5i.com/

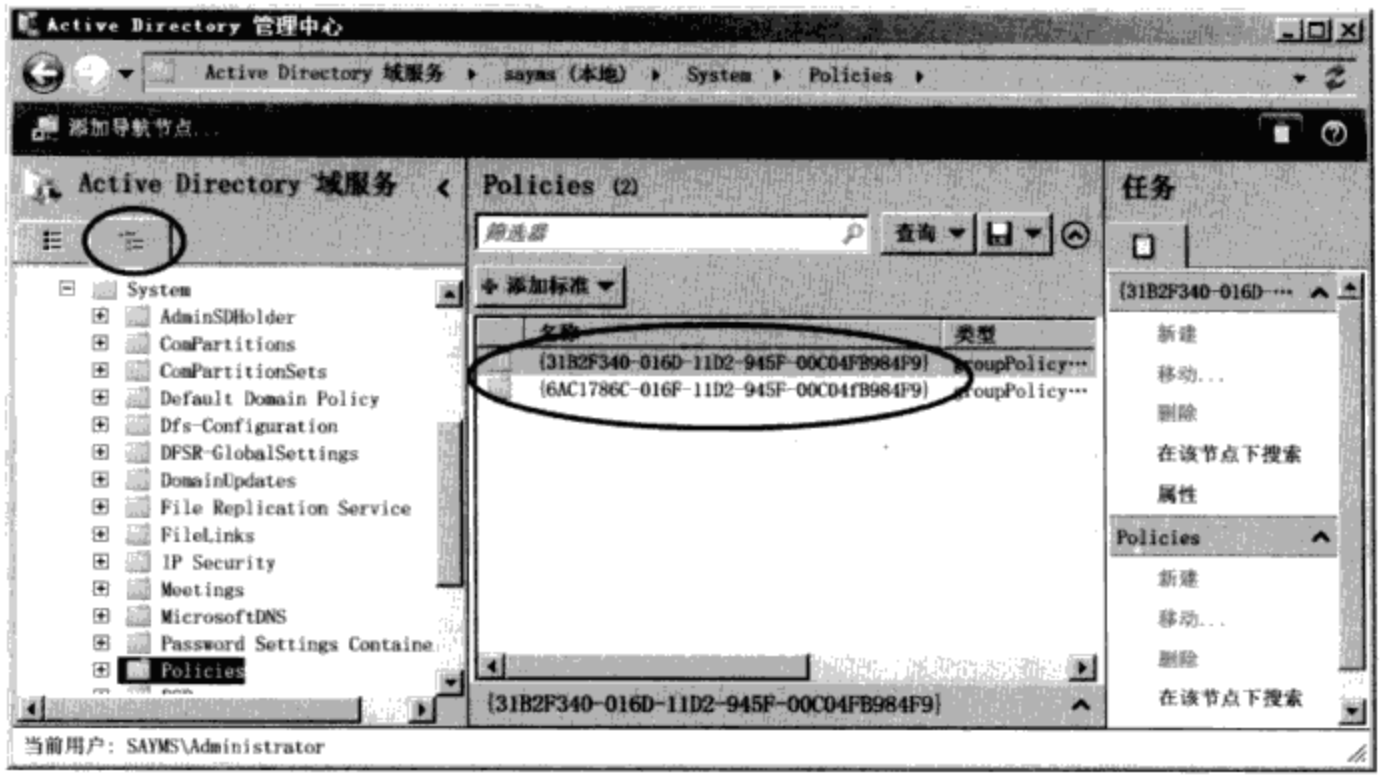


图4-3

如果您要查询GPO的GUID的话，例如要查询Default Domain Policy GPO的GUID，可通过如图 4-4所示【在**组策略管理**窗口中单击Default Domain Policy➲单击**详细信息**标签➲唯一 ID】的方法进行操作。

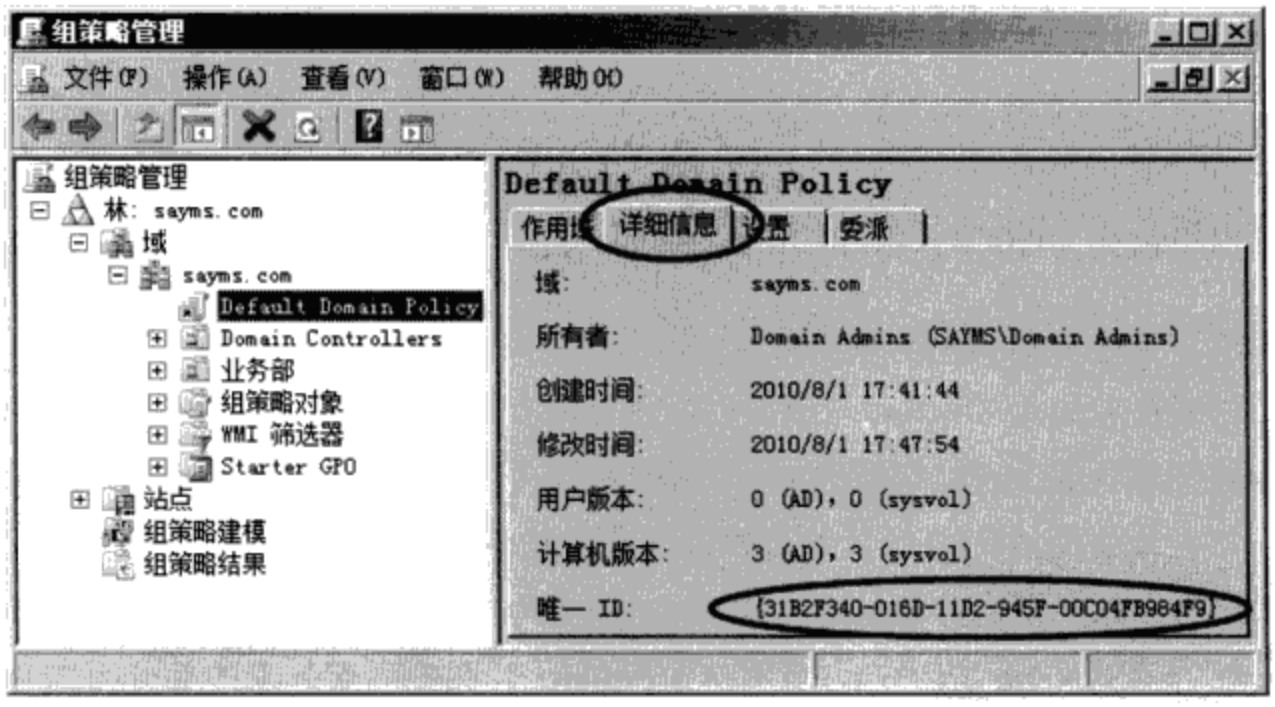


图4-4

（2）GPT（Group Policy Template）

GPT是用来存储GPO设置值与相关文件的，它是一个文件夹，而且是被创建在域控制器的**%systemroot%\SYSVOL\sysvol\域名\Policies**文件夹内。系统是使用GPO的GUID来作为GPT的文件夹名称，例如图 4-5中两个GPT文件夹分别是Default Domain Policy与Default Domain Controller Policy GPO的GPT。

Download at http://www.pin5i.com/

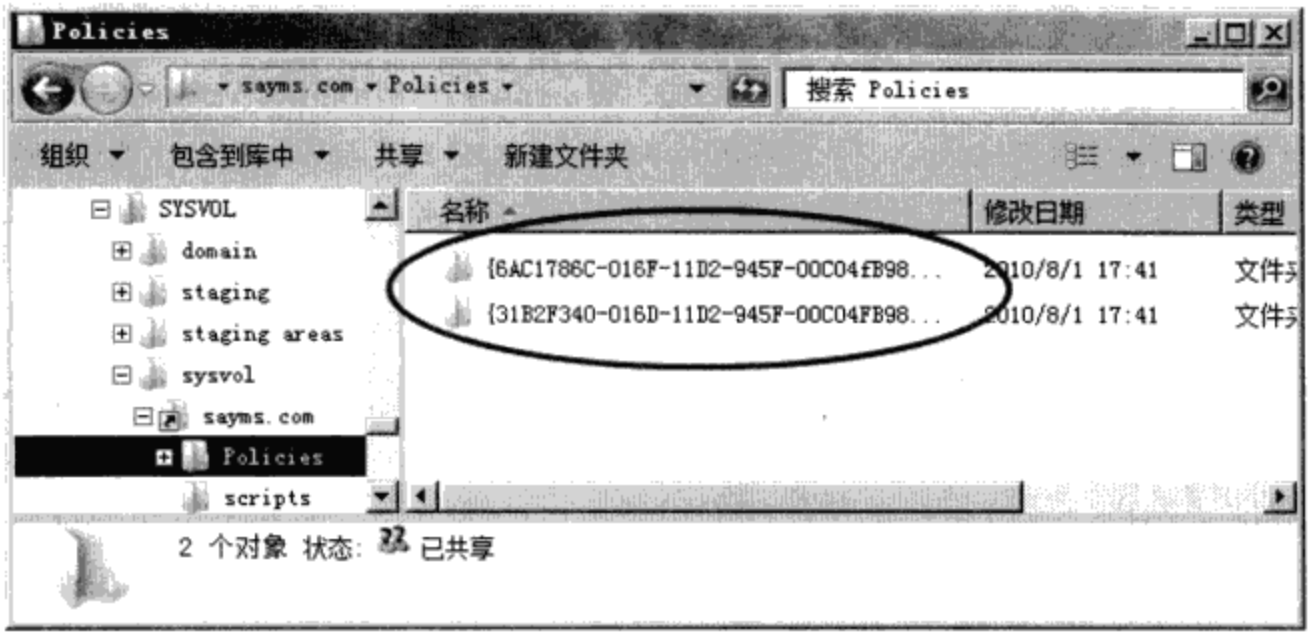


图4-5

提示

每一台计算机也都有**本地计算机策略**，可以通过【单击Windows + R 键➲输入**MMC**后单击确定按钮➲选择**文件**菜单➲添加/删除管理单元➲选择**组策略管理编辑器**➲依序单击添加、完成、确定按钮】的方法来创建管理**本地计算机策略**的工具。本地计算机策略的设置数据是被存储在本地计算机的**%systemroot%\System32\GroupPolicy**文件夹内，它是一个隐藏文件夹。

4-1-3 策略设置与首选设置

组策略内的设置可再区分为**策略设置**与**首选设置**两种。

- 只有域的组策略才有**首选设置**功能，本地计算机策略并无此功能。
- **策略设置**是强制性设置，客户端应用这些设置后就无法更改（有些设置虽然客户端可以自行更改设置值，不过下次应用策略时，仍然会被改为策略内的设置值）；然而**首选设置**非强制性，客户端可自行更改设置值，因此**首选设置**适合于用来当作默认值。
- 若要过滤**策略设置**的话，必须针对整个GPO来过滤，例如某个GPO已经被应用到**业务部**，但是我们可以通过过滤设置来让其不要应用到**业务部**经理Peter，也就是整个GPO内的所有设置项目都不会被应用到Peter；然而**首选设置**可以针对单一设置项目来过滤。
- 如果在**策略设置**与**首选设置**内有相同的设置项目，而且都已做了设置，但是其设置值却不相同时，则以**策略设置**优先，也就是最后的有效设置是**策略设置**内的设置值。
- 要应用**首选设置**的客户端必须安装支持**首选设置**的client-side extension（CSE）。Windows Server 2008 R2、Windows Server 2008、Windows 7计算机已包含此CSE，但是其他Windows系统需到微软网站下载此CSE，微软网站上提供Windows Vista（或新版）、Windows Server 2003 SP1（或新版）、Windows XP SP2（或新版）等系统所需的CSE，其更新程序编号为KB943729。若是Windows Vista SP1的话，则此CSE也已内含在Microsoft Remote Server Administration Tools for Windows Vista（RSAT）内。

Download at http://www.pin5i.com/

- 要应用**首选设置**的客户端还需要安装XMLLite。Windows Server 2008 R2、Windows Server 2008、Windows Server 2003 SP2、Windows 7、Windows Vista与Windows XP SP3计算机已内含XMLLite，不过Windows Server 2003 SP1与Windows XP SP2需要另外到微软网站下载与安装XMLLite，除非它们已经安装Internet Explorer 7（或以上的版本，XMLLite已包含在内）。

4-1-4 组策略的应用时限

当您修改了站点、域或组织单位的GPO设置值后，这些设置值并不是立刻就对站点、域或组织单位内的用户与计算机有效，而是必须等GPO设置值被应用到用户或计算机后才有效。GPO设置值内的计算机设置与用户设置的应用时限并不相同。

1. 计算机配置的应用时限

域内的成员计算机会在以下的场合应用GPO的计算机配置值：

- 计算机开机时会自动应用。
- 若计算机已经开机的话，则系统会每隔一段时间自动应用。
  - 域控制器：默认是每隔5分钟自动应用一次。
  - 非域控制器：默认是每隔90~120分钟自动应用一次。
  - 不论策略设置值是否有变动，系统仍然会每隔16个小时自动应用一次安全性配置策略。
- 手动应用：到域成员计算机上打开**命令提示符**窗口或单击**Windows PowerShell**图标、运行**gpupdate /target:computer /force**命令。

2. 用户配置的应用时限

域内的用户会在以下的场合应用GPO的用户配置值。

- 用户登录时会自动应用。
- 若用户已经登录的话，则系统默认会每隔90~120分钟之间自动应用一次，而且不论策略设置值是否有变动，系统仍然会每隔16小时自动应用一次安全性配置策略。
- 手动应用：到域成员计算机上打开**命令提示符**窗口或单击**Windows PowerShell**图标、运行**gpupdate /target:user /force**命令。

提示

运行**gpupdate /force**命令时会同时应用计算机与用户配置。部分的策略设置必须在计算机重新启动或用户登录时才有作用，例如**软件安装策略**与**文件夹重定向策略**。

Download at http://www.pin5i.com/

4-2 策略设置实例演练

在继续解释更高级的组策略功能之前，为了让您有比较清楚的概念，我们先分别使用两个实例来演练GPO的**计算机配置**与**用户配置**中的**策略设置**。

4-2-1 策略设置实例演练一：计算机配置

由于系统默认是只有某些组（例如administrators）内的用户，才有权利在扮演域控制器角色的计算机上登录，因此一般用户在域控制器上登录时，屏幕上会出现如图 4-6所示的警告信息，且无法登录，除非他们被赋予**允许本地登录**（Allow Logon Locally）的权限。

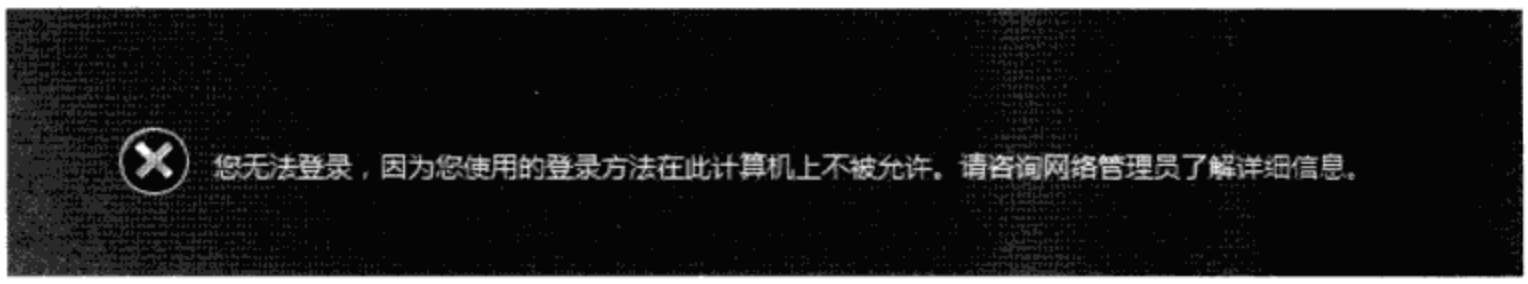


图4-6

假设要开放让域SAYMS内Domain Users组中的用户可以在域控制器上登录，我们将通过默认的Default Domain Controllers Policy GPO来设置，也就是要让这些用户在域控制器上拥有**允许本地登录**的权限。

注意

1. 此处是为了便于解释起见，才开放让Domain Users拥有**允许本地登录**的权限。在正常情况之下，域控制器等重要的服务器不应该允许一般用户来登录。
2. 若要在成员服务器、Windows 7、Windows Vista或Windows XP等非域控制器的计算机上练习的话，则以下步骤可免，因为Domain Users默认已经在这些计算机上拥有**允许本地登录**的权限。

STEP 1 请到域控制器上使用系统管理员身份登录。

STEP 2 选择【开始➲管理工具➲组策略管理】。

STEP 3 如图 4-7所示，通过【展开Domain Controllers ➲对着右边的Default Domain Controllers Policy单击右键➲编辑】的方法进行操作。

STEP 4 如图4-8所示，通过【展开**计算机配置**➲策略➲Windows设置➲安全设置➲本地策略➲用户权限分配➲双击**允许本地登录**】的方法进行操作。

Download at http://www.pin5i.com/

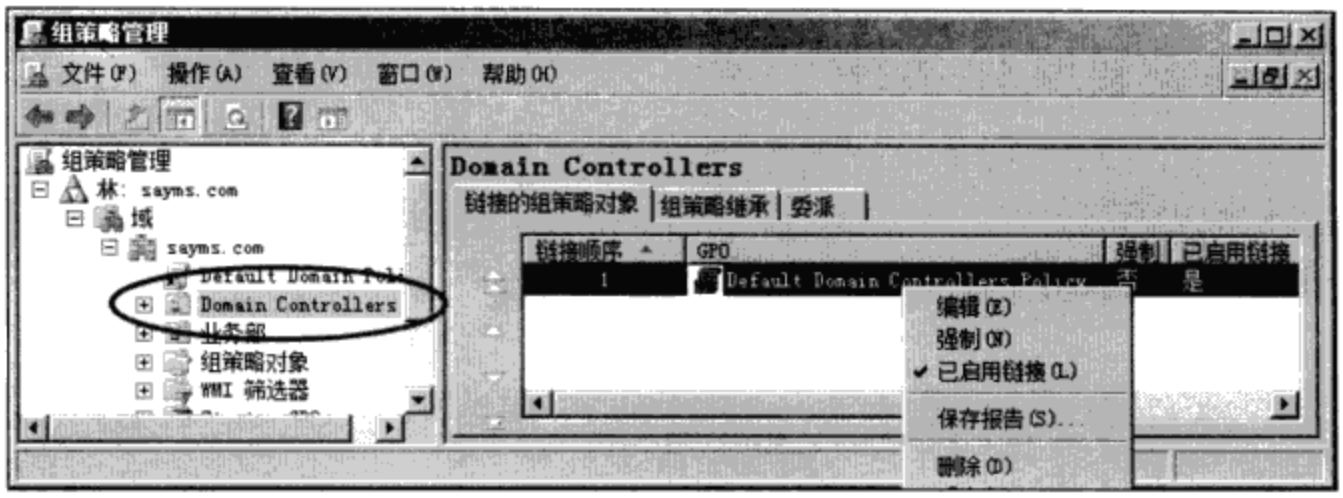


图4-7

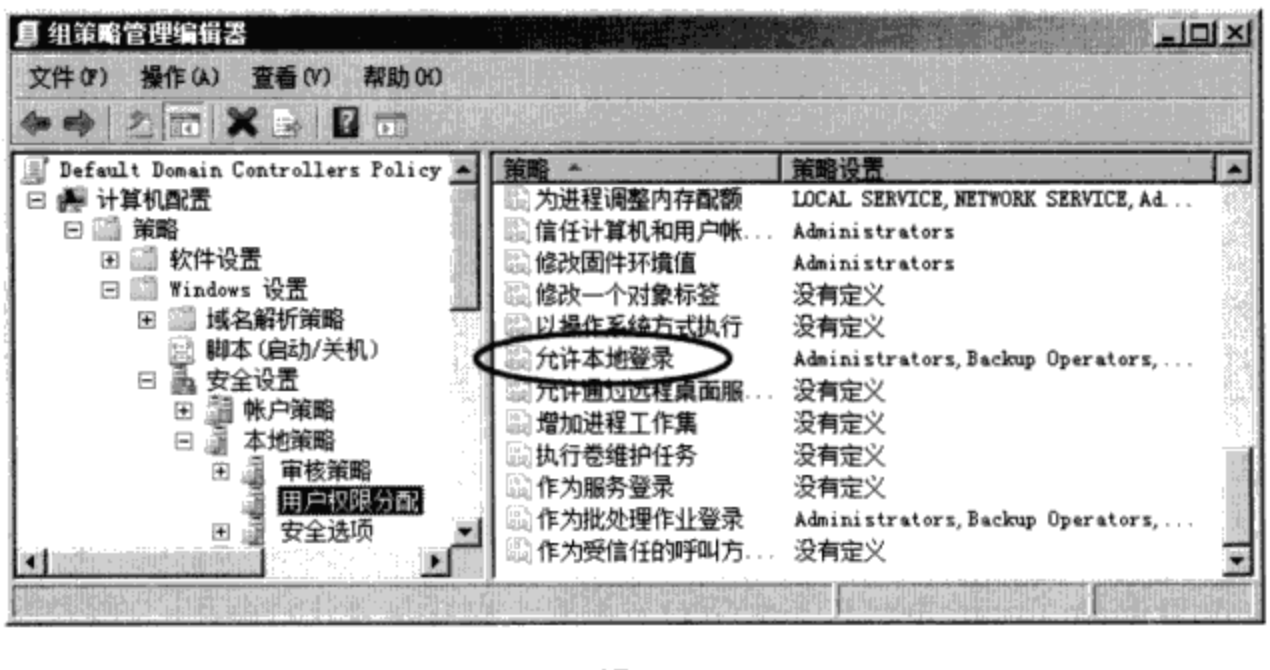


图4-8

STEP 5 如图 4-9所示，通过【单击添加用户或组按钮➲输入或选择域SAYMS内的Domain Users组➲单击2次确定按钮】的方式进行操作。由此图中可看出默认只有Account Operators、Administrators等组内的用户才拥有**允许本地登录**的权限。

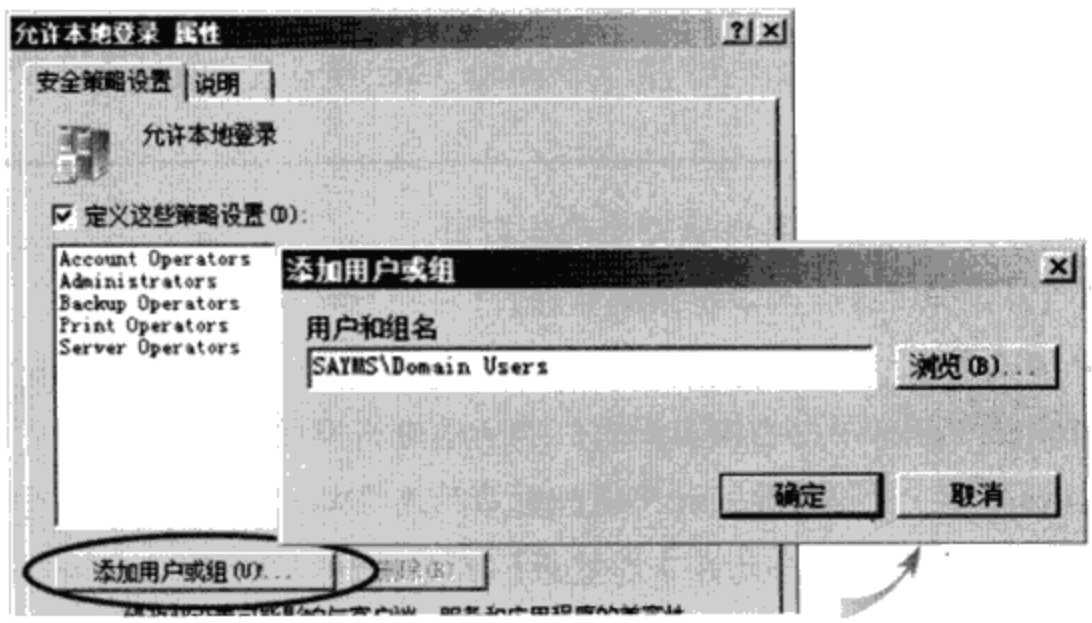


图4-9

Download at http://www.pin5i.com/

完成后，必须等这个策略应用到组织单位Domain Controllers内的域控制器后才有效（见前一小节的说明）。应用完成后，您就可以使用任何一个域用户账户到域控制器上登录来测试**允许本地登录**功能是否正常。

另外若域内有多台域控制器的话，由于策略设置默认会先被存储到扮演**PDC模拟器操作主机**角色的域控制器内（默认是由域中的第1台域控制器所扮演），因此必须等**PDC模拟器操作主机**内的策略设置被复制到其他域控制器，然后再等这些策略设置值应用到这些域控制器。

> **提示**
>
> 您可以通过【开始➲管理工具➲Active Directory用户和计算机➲对着域名右击➲操作主机➲**PDC**标签】的方法，来得知扮演**PDC模拟器操作主机**的域控制器。

系统可以使用以下两种方式来将**PDC模拟器操作主机**内的组策略设置复制到其他域控制器。

- 自动复制：**PDC模拟器操作主机**默认在15s后会自动将其复制出去，因此其他的域控制器可能需要等15s或更久时间才会接收到此设置值。
- 手动立即复制：假设**PDC模拟器操作主机**是DC1，而我们要将组策略设置手动复制到域控制器DC2。请在域控制器上通过【开始➲管理工具➲Active Directory站点和服务➲Sites➲Default-First-Site-Name➲ Servers➲展开目的地域控制器（DC2）➲NTDS Settings➲对着**PDC模拟器操作主机**（DC1）单击右键➲立即复制】的方法进行操作。

4-2-2 策略设置实例演练二：用户配置

假设域sayms.com内有一个组织单位**业务部**，而我们要针对其内的所有用户来设置，而且限定他们必须通过企业内部的代理服务器（Proxy Server）上网，假设代理服务器的网址为proxy.sayms.com、端口号为8080，同时我们要将其浏览器Internet Explorer的**连接**标签内更改代理服务器设置的功能禁用，以免用户私自通过此处更改这些设置值。

由于当前并没有任何GPO被链接到组织单位**业务部**，因此我们将先创建一个链接到**业务部**的GPO，然后通过修改此GPO设置值的方式来进行操作。

STEP 1 请到域控制器上使用系统管理员身份登录。

STEP 2 选择【开始➲管理工具➲组策略管理】。

STEP 3 如图 4-10所示，通过【展开**业务部**➲对着**业务部**单击右键➲在这个域中创建GPO并在此处链接】的方式进行操作。

Download at http://www.pin5i.com/

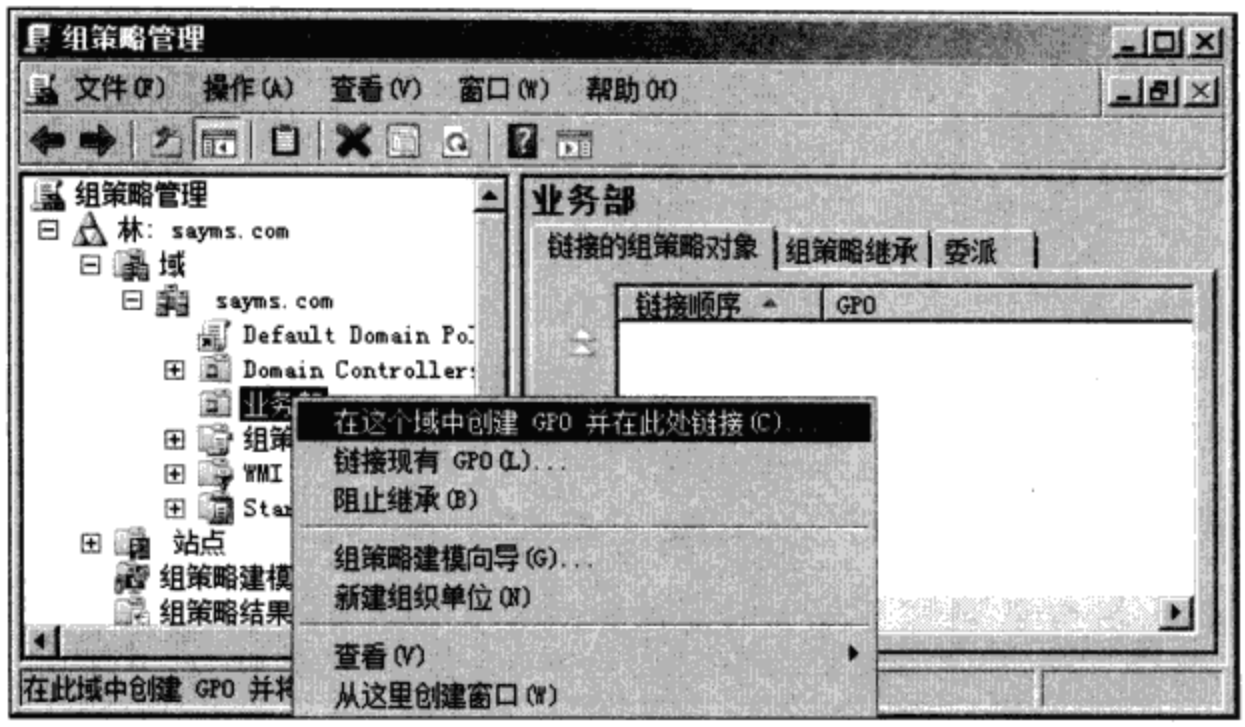


图4-10

提示

1. 您也可以先通过【对着组策略对象右击➲新建】的方法来创建GPO，然后再通过【对着组织单位**业务部**右击➲链接到现有的GPO】的方法来将其链接到组织单位**业务部**。
2. 若要备份或还原GPO的话，请通过【对着组策略对象单击右键➲**备份**或**从备份还原**】的方法进行操作。

STEP 4 在图4-11中为此GPO命名（例如**测试用的GPO**）后单击确定按钮。

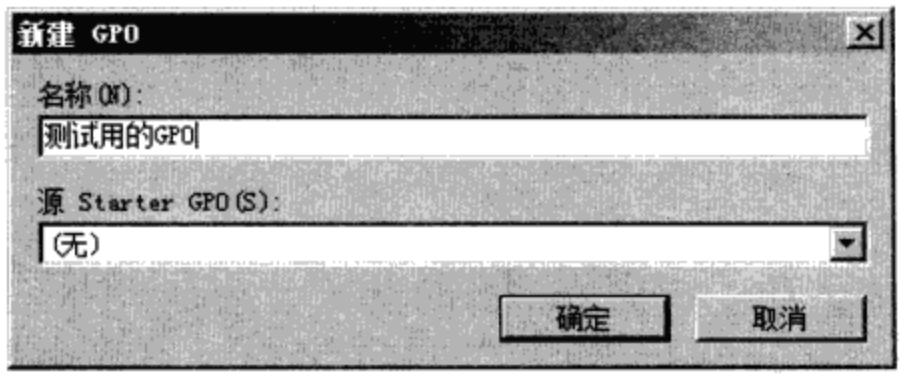


图4-11

STEP 5 如图4-12所示，通过【对着这个添加的GPO单击右键➲编辑】的方式进行操作。

STEP 6 如图4-13所示，通过【展开**用户配置**➲策略➲Windows设置➲Internet Explorer维护➲连接➲双击右边的**代理设置**➲在弹出的对话框中选择**启用代理服务器设置**复选框➲输入代理服务器的网址proxy.sayms.com、端口号为8080➲单击确定按钮】的方式进行操作。

Download at http://www.pin5i.com/

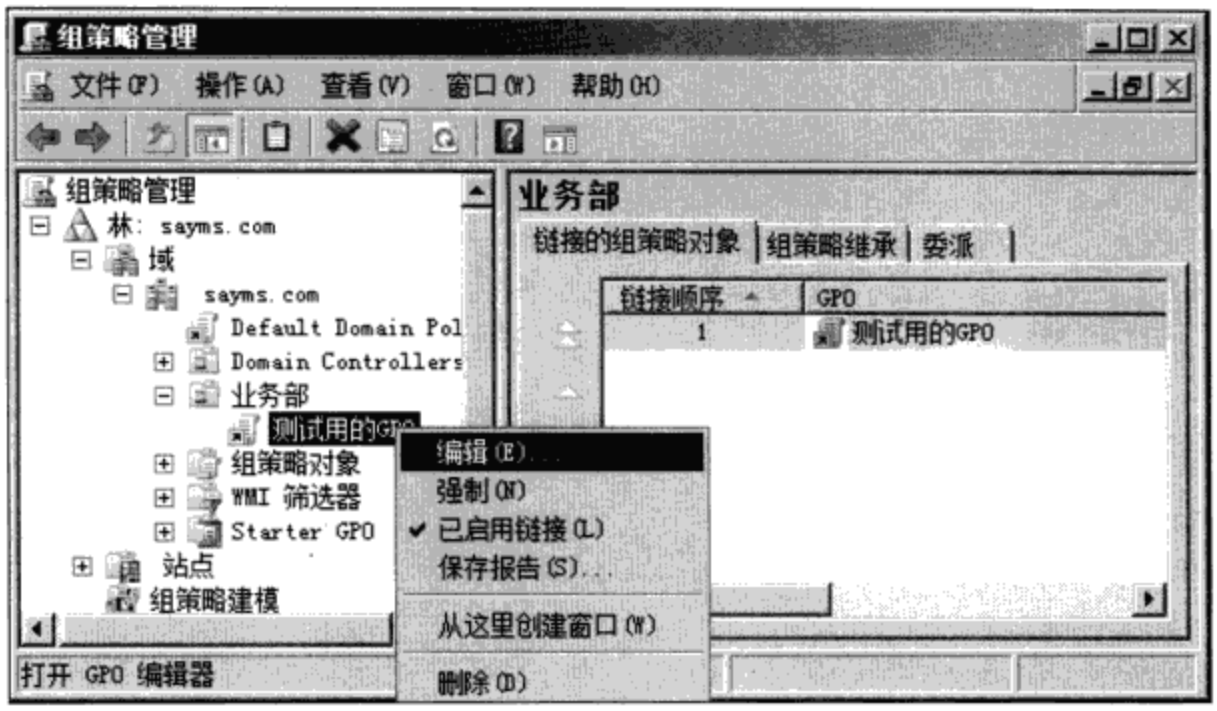


图4-12

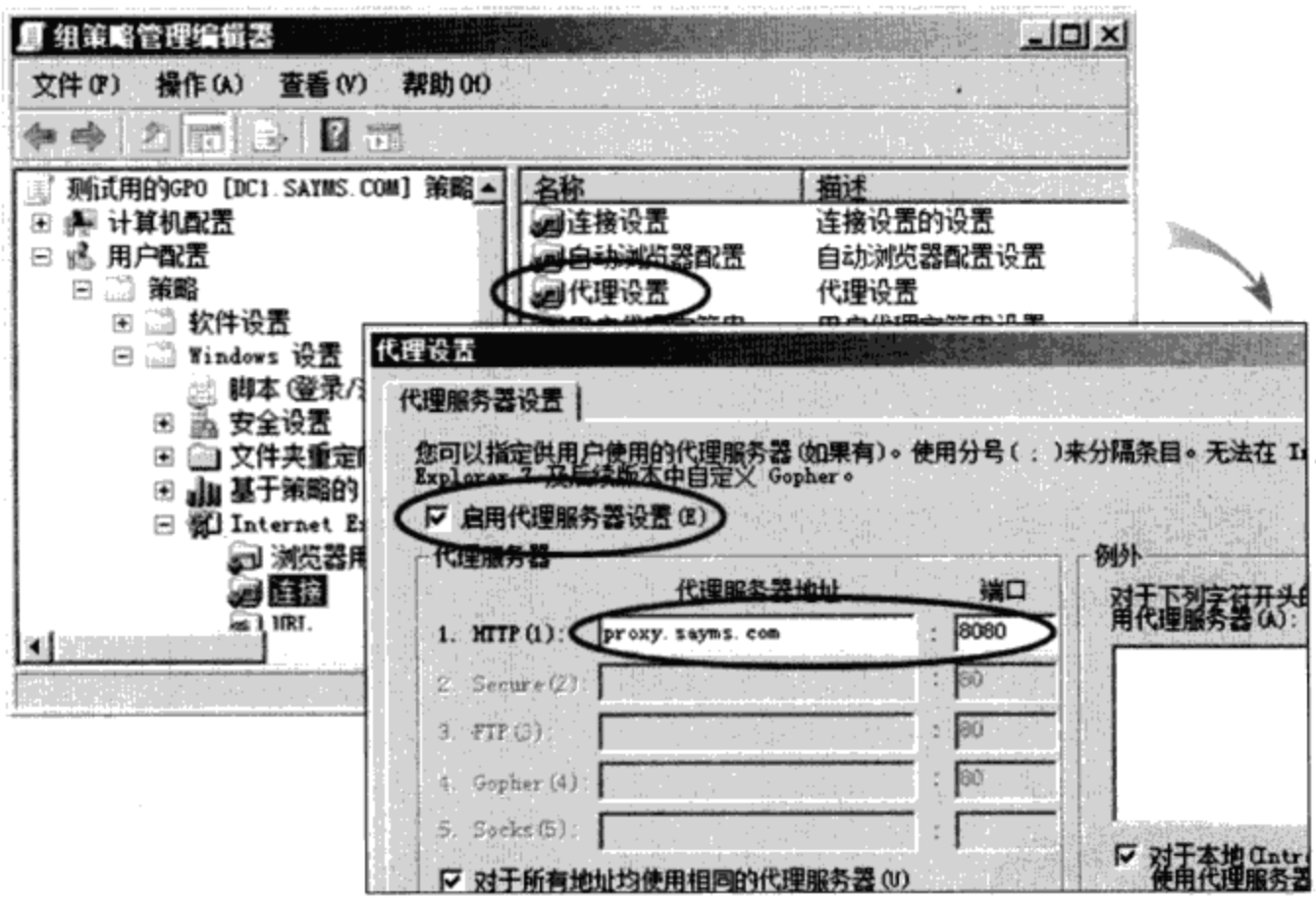


图4-13

STEP 7 如图 4-14所示，通过【展开**用户配置**➲策略➲管理模板➲Windows组件➲Internet Explorer➲将右方**禁用更改代理服务器设置**的状态改为**已启用**】的方式进行操作。

Download at http://www.pin5i.com/

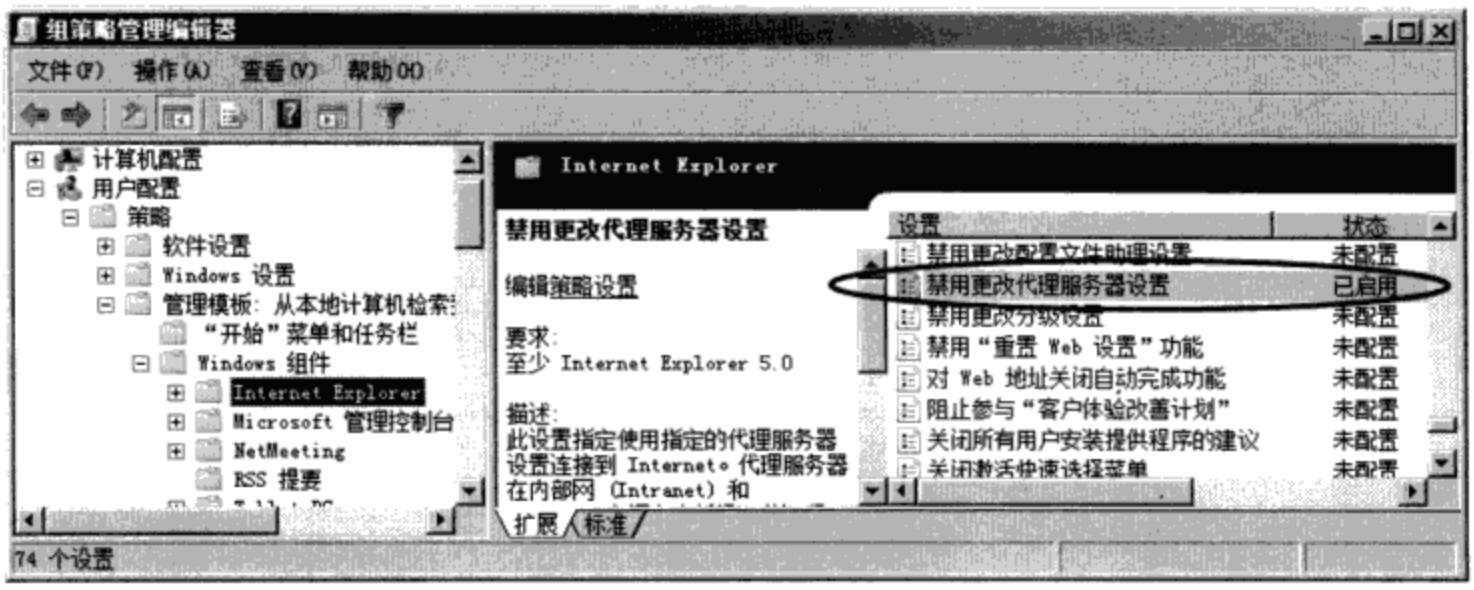


图4-14

STEP 8 请使用**业务部**内任何一位用户到域内任何一台计算机上登录。

STEP 9 运行浏览器Internet Explorer，选择**工具**菜单➲Internet选项，如图4-15所示单击**连接**标签下的局域网设置按钮，从弹出的对话框可知其代理服务器被指定到我们所设置的proxy.sayms.com、端口为8080，而且无法更改这些设置。

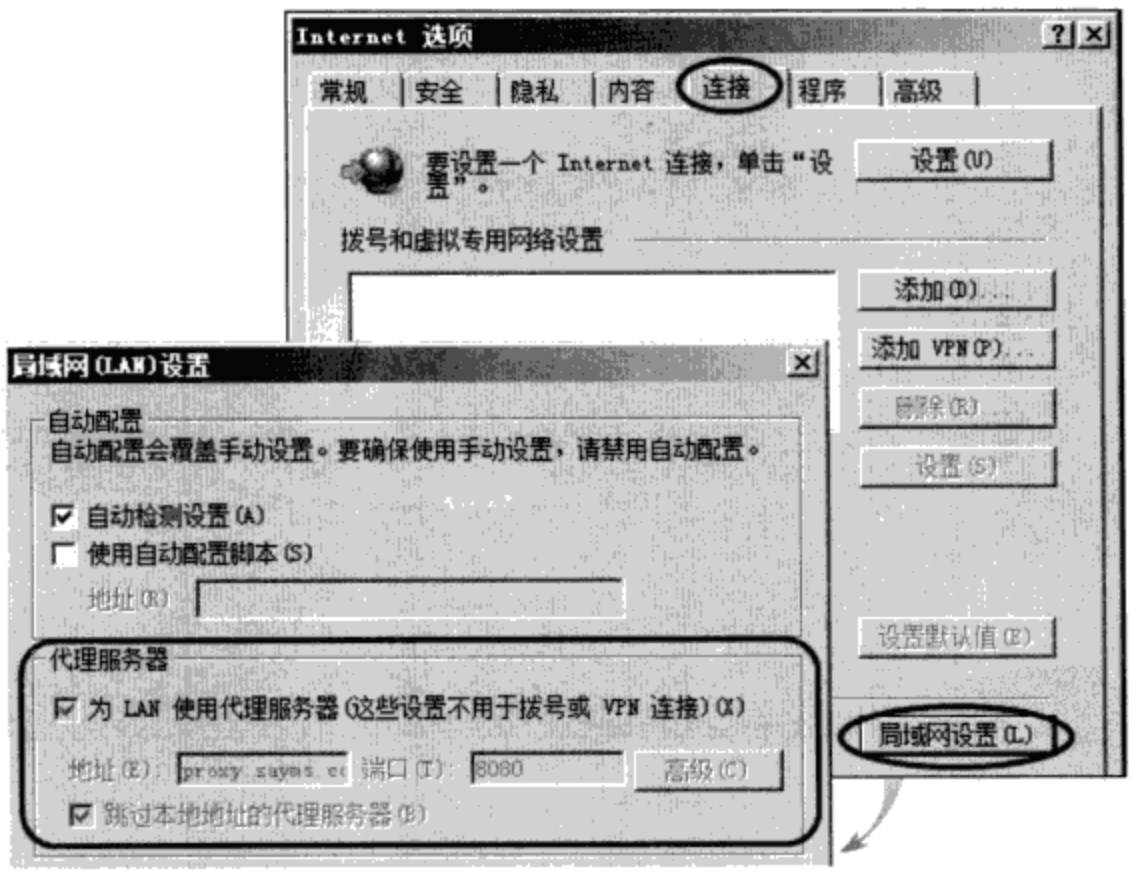


图4-15

4-3 首选设置实例演练

首选设置并非强制性，客户端可自行更改设置值，因此它适合用来当作默认值。

Download at http://www.pin5i.com/

4-3-1 首选设置实例演练一

我们要让位于组织单位**业务部**内的所有用户登录时，其驱动器号**Z:**都会自动链接到**\\dc1\tools**共享文件夹；另外还要使用过滤功能让组织单位**业务部**内的用户peter登录时，其磁盘驱动器**Y:**会自动链接到**\\dc1\database**共享文件夹，但是同样是位于**业务部**内的其他用户登录时不会有**Y:**磁盘。我们要使用前面所创建的**测试用的GPO**来练习。

STEP 1 请先到服务器dc1上创建文件夹tools与database，将它们设置为共享文件夹，假设允许**读取**权限给Everyone。

STEP 2 请到域控制器上使用系统管理员身份登录。

STEP 3 选择【开始➲管理工具➲组策略管理】。

STEP 4 如图4-16所示，通过【展开**业务部**➲对着**测试用的GPO**右击➲编辑】的方式进行操作。

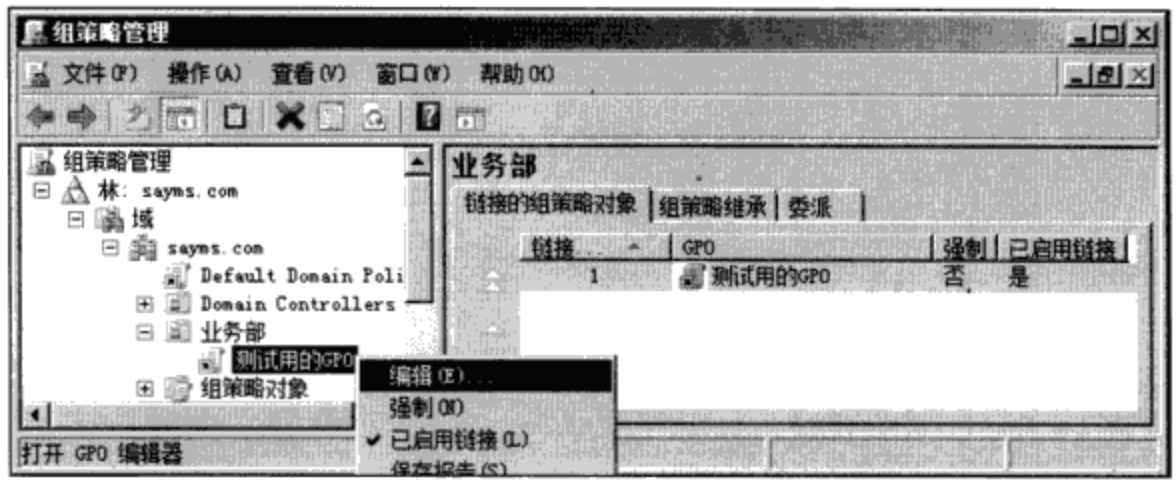


图4-16

STEP 5 如图 4-17所示，通过【展开**用户设置**➲首选项➲Windows设置➲对着**驱动器映射**单击右键➲新建➲映射驱动器】的方式进行操作。

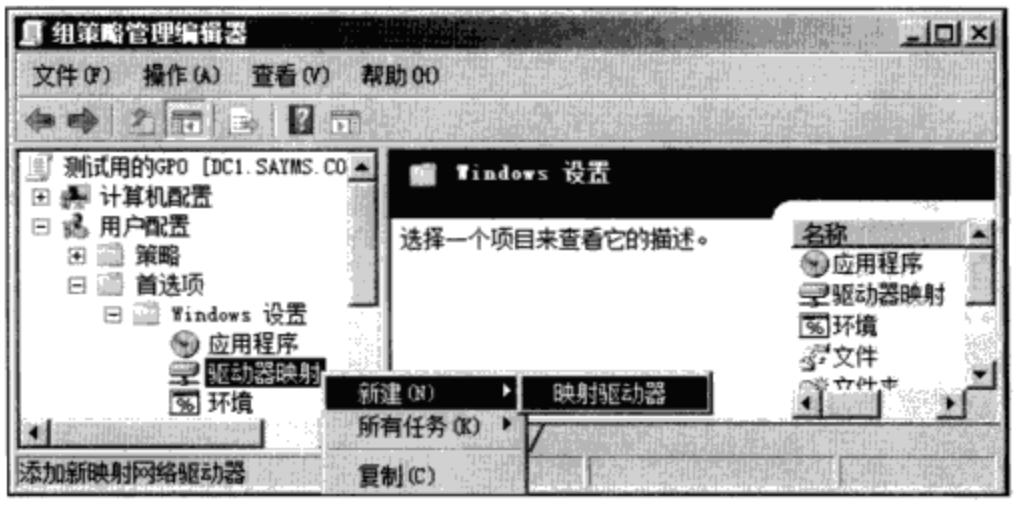


图4-17

提示

在Windows设置之下的应用程序、驱动器映射、环境、文件、文件夹等被称为扩展（Extension）。

Download at http://www.pin5i.com/

STEP 6 在图 4-18中的**操作**下拉列表中选择**更新**，**位置**文本框中输入共享文件夹路径**\\dc1\tools**，使用**Z:**磁盘来连接此共享文件夹，选择**重新连接**以便每次登录时都会自动使用**Z:**磁盘来连接。其中**操作**可有以下选择。

- 创建：会在客户端计算机创建用来连接此共享文件夹的Z:磁盘。
- 替换：客户端若已存在网络驱动器Z:的话，则将其删除后改为使用此处的设置来替换。若不存在Z:磁盘的话，则添加。
- 更新：修改客户端的Z:磁盘设置，例如修改客户端连接共享文件夹时所使用的用户账户与密码。若客户端不存在Z:磁盘的话，则添加。此处我们选择默认的更新。
- 删除：删除客户端的Z:磁盘。

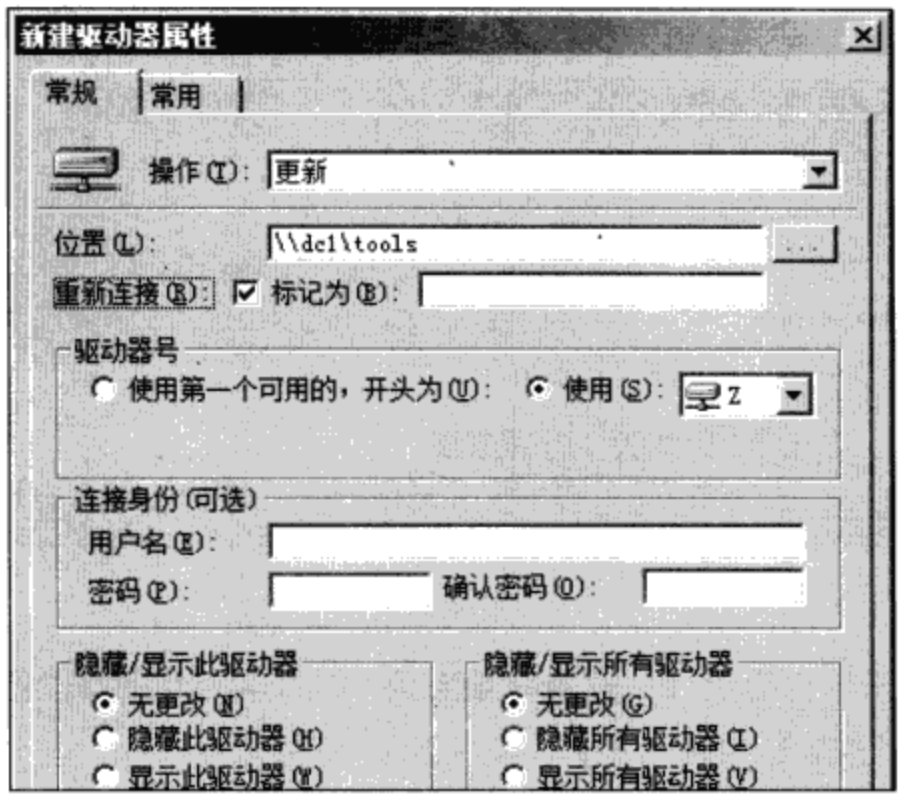


图4-18

STEP 7 单击图 4-19中**常用**标签，如图所示进行设置后单击确定按钮。

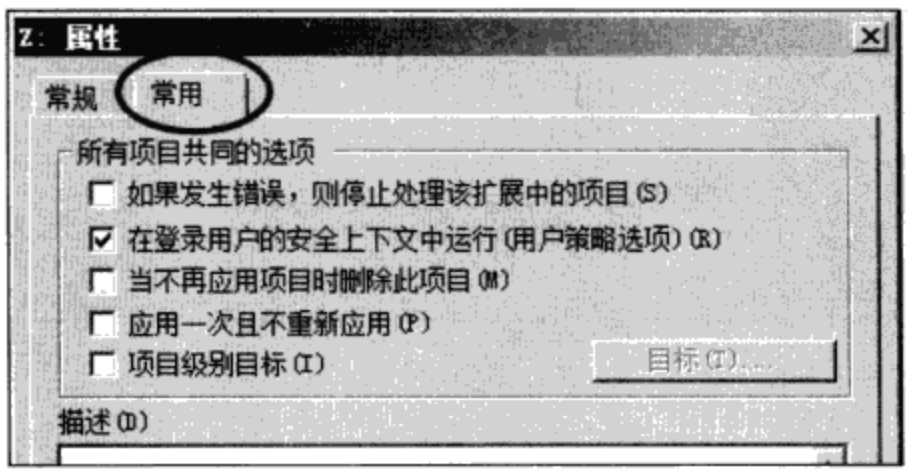


图4-19

Download at http://www.pin5i.com/

- 如果发生错误，则停止处理该扩展中的项目。若在这个**驱动器映射**扩展内有多个设置项目，则系统在处理本项目时发生错误的话，默认仍然会继续处理下一个项目，但若您选择此选项的话，它就会停止，不再继续处理下一个项目。
- 在登录用户的安全上下文中运行（用户策略选项）。客户端的CSE（Client-Side Extension）默认是使用本地系统账户（Local SYSTEM Account）的身份来处理**首选设置**的项目，这将使得CSE只能访问可供本地计算机访问的环境变量与系统资源，而此选项可以让CSE改用用户登录身份来处理**首选设置**的项目，CSE可以访问本地系统账户无权访问的资源或用户环境变量，例如本练习中使用网络驱动器**Z:**来连接网络共享文件夹\\dc1\tools，就需要选择此选项。
- 当不再应用项目时删除此项目。当GPO被删除后，客户端计算机内与该GPO**策略设置**相关的设置都会被删除，然而与**首选设置**有关的设置仍然会保留，例如本练习中的网络驱动器**Z:**仍然会被保留，但若您选择此选项的话，则与这个**首选设置**有关的设置就会被删除。
- 应用一次且不重新应用。客户端计算机会定期应用GPO的**首选设置**，因此若用户自行更改设置的话，则下一次重新应用后又会恢复为**首选设置**内的设置值，如果您希望用户能够自行更改设置值的话，请选择此选项，此时它只会应用**首选设置**一次。
- 项目级别目标（Item-Level Targeting）。它让您针对每个**首选设置**项目来决定此项目的应用目标，例如您可以选择将其只应用到特定的用户或Windows系统。

STEP 8 图4-20中右方为刚才创建且是使用**Z:**磁盘来连接\\dc1\tools共享文件夹的设置，这样的一个设置被称为一个项目（Item）。我们将继续创建下一个项目：【对着**驱动器映射**单击右键➲新建➲映射驱动器】。



图4-20

STEP 9 在图 4-21中的操作处选择**更新**，**位置**处输入共享文件夹路径**\\dc1\database**，选择**重新连接**，使用Y磁盘来连接此共享文件夹。

Download at http://www.pin5i.com/

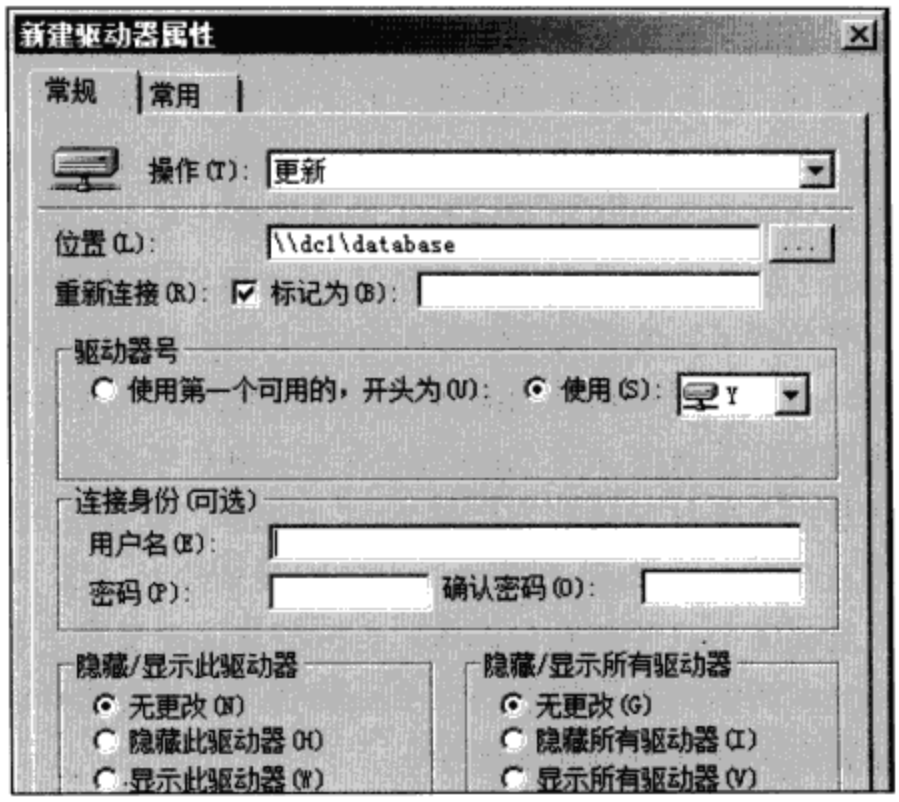


图4-21

STEP 10 单击图4-22中的**常用**标签，然后选择**在登录用户的安全上下文中运行（用户策略选项）**复选框，同时单击目标按钮，以便将此项目的应用对象指定到用户Peter。

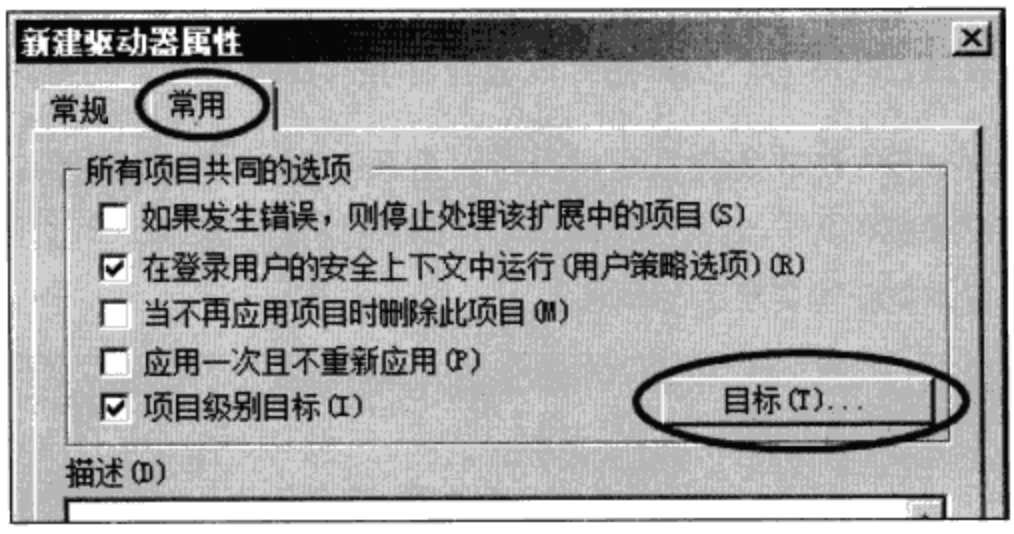


图4-22

STEP 11 在图4-23中通过【单击左上角的**新建项目**➲选择**用户**】的方式进行操作。

Download at http://www.pin5i.com/

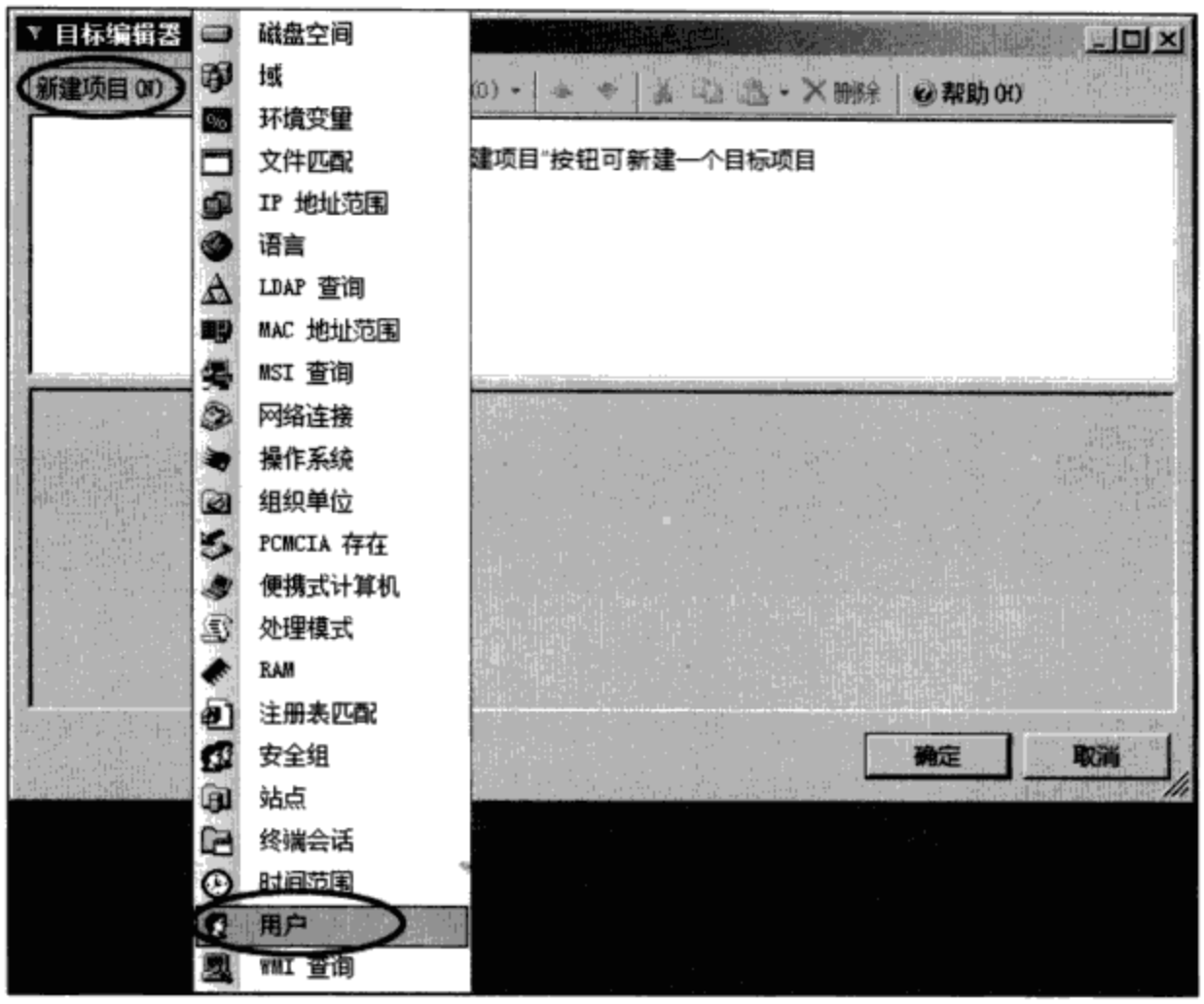


图4-23

STEP 12 在图4-24的**用户**文本框中通过单击右边的**浏览**按钮来选择仅将此项目应用到域SAYMS的用户Peter后单击确定按钮。

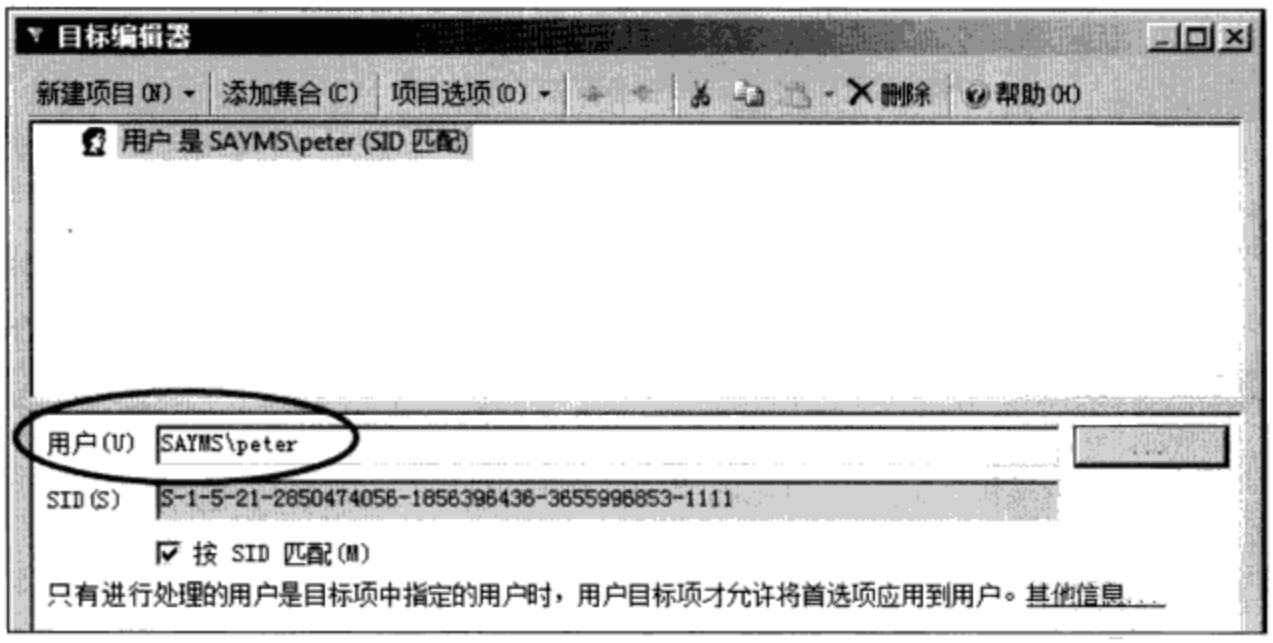


图4-24

STEP 13 返回到**新建驱动器属性**对话框时单击确定按钮。

STEP 14 完成设置后的两个项目如图4-25所示。

Download at http://www.pin5i.com/

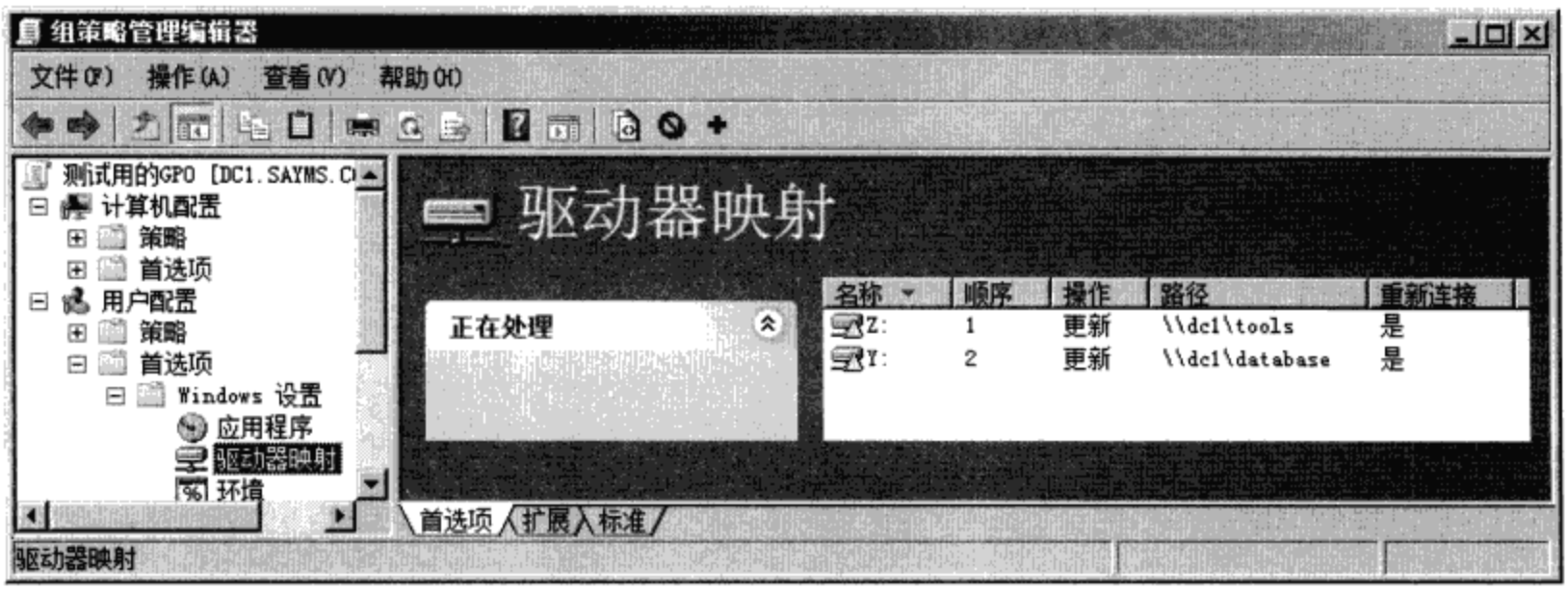


图4-25

STEP 15 请到域内的任何一台成员计算机上（请先确认已经安装了前面所介绍的**首选设置**CSE与XMLLite），使用**业务部**内的用户账户Peter的身份登录，然后选择【开始➲计算机】，之后您将如图 4-26所示看到其**Y:**与**Z:**磁盘分别会自动连接到我们指定的共享文件夹。但是如果您使用组织单位**业务部**内的其他用户账户登录的话，您只会看到**Z:**，不会看到**Y:**，因为我们只设置让Peter拥有**Y:**磁盘的登录权限。

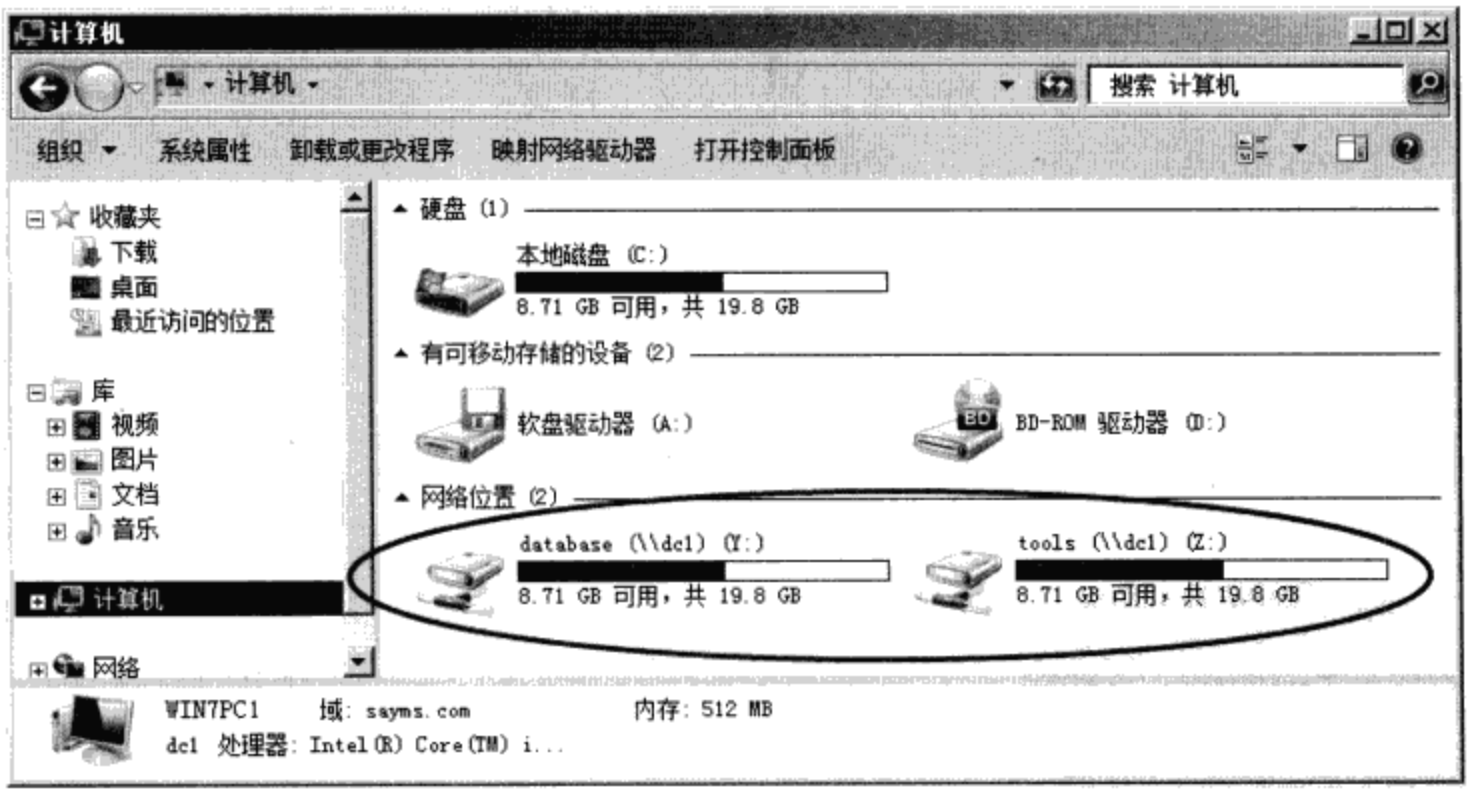


图4-26

4-3-2 首选设置实例演练二

以下将通过**首选设置**来为组织单位**业务部**内的计算机Win7PC1自动创建一个本地用户账户Henry，我们要使用前面所创建的**测试用的GPO**来练习。

Download at http://www.pin5i.com/

STEP 1 请到域控制器上使用系统管理员身份登录。

STEP 2 由于计算机账户Win7PC1并不是在组织单位**业务部**内，而是在容器Computers内，因此请先将此计算机账户移动到组织单位**业务部**内：【如图 4-27所示对着容器Computers内的Win7PC1单击右键➲移动➲选择**业务部**后单击确定按钮】。

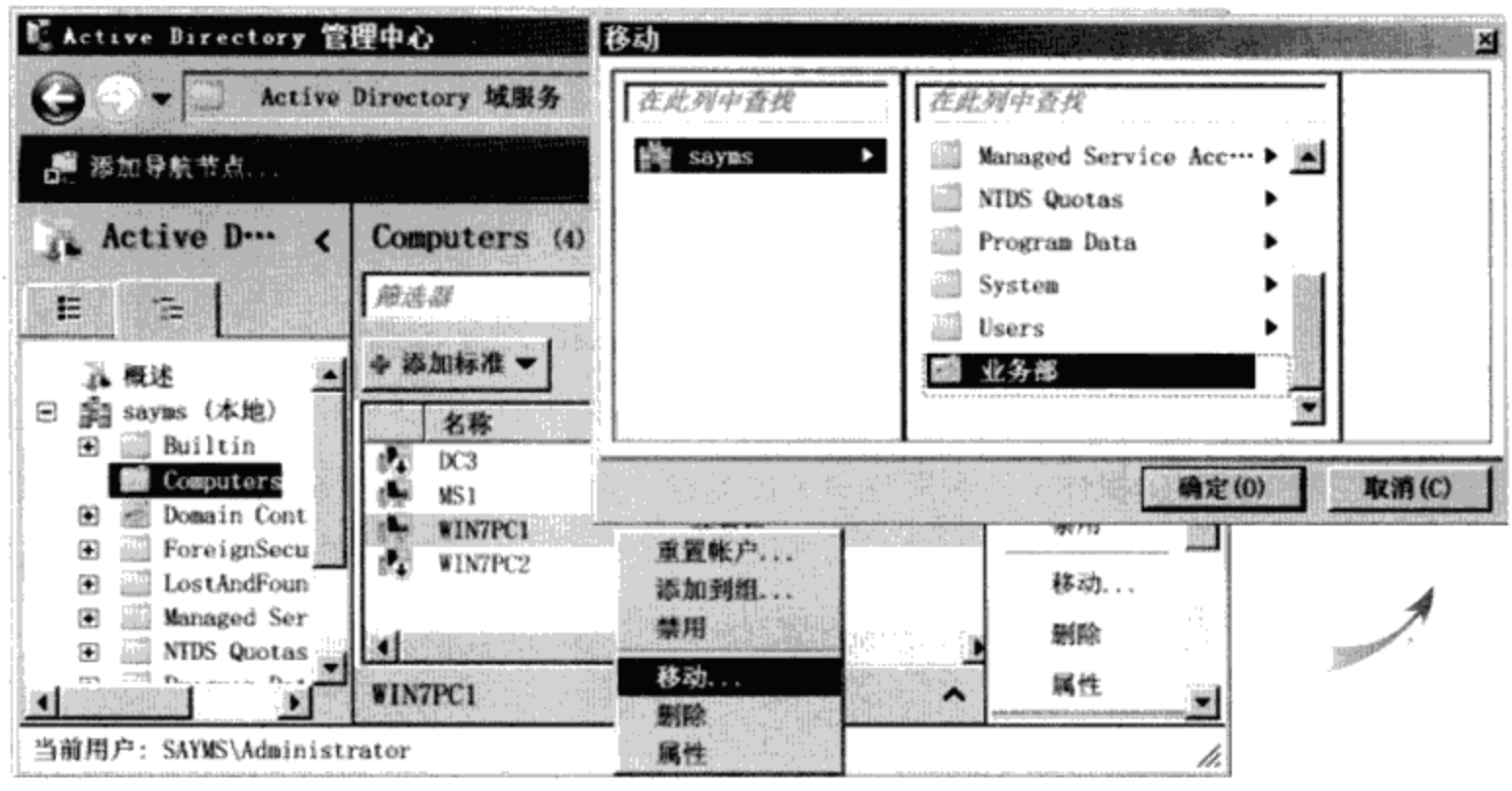


图 4-27

STEP 3 选择【开始➲管理工具➲组策略管理】。

STEP 4 如图 4-28所示，通过【展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑】的方式进行操作。

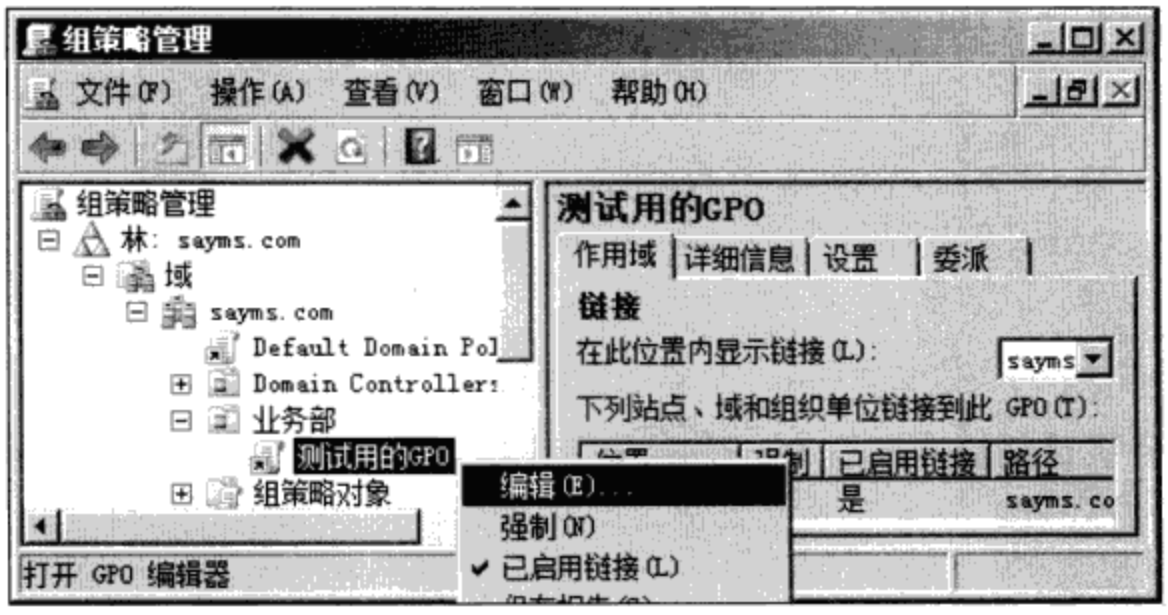


图 4-28

STEP 5 如图 4-29所示，通过【展开**计算机配置**➲首选项➲控制面板设置➲对着**本地用户和组**单击右键➲新建➲本地用户】的方式进行操作。

Download at http://www.pin5i.com/



图 4-29

STEP 6 在图 4-30中的**操作**下拉列表框中选择**创建**，输入用户的相关数据后单击 应用 按钮。其中**操作**下拉列表框中的其他选择请参考前一个实例演练的说明。

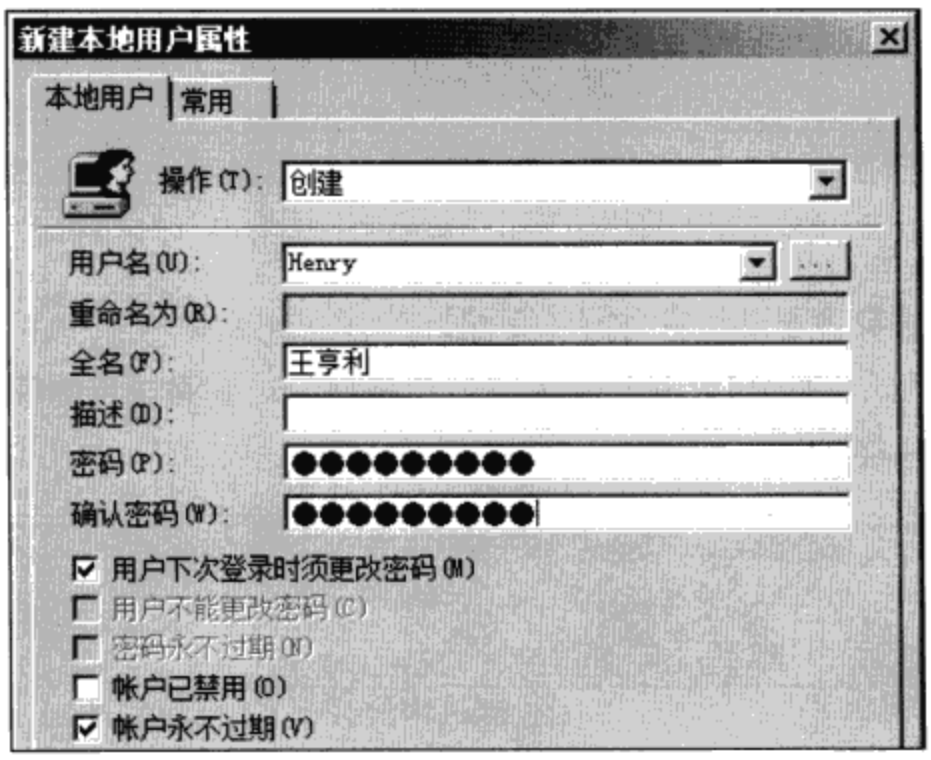


图 4-30

STEP 7 单击图 4-31中的**常用**标签，然后选择**应用一次且不再重新应用**复选框，同时也选择**项目级目标**复选框后单击 目标 按钮，以便将此项目的应用对象指定到计算机 Win7PC1。

Download at http://www.pin5i.com/

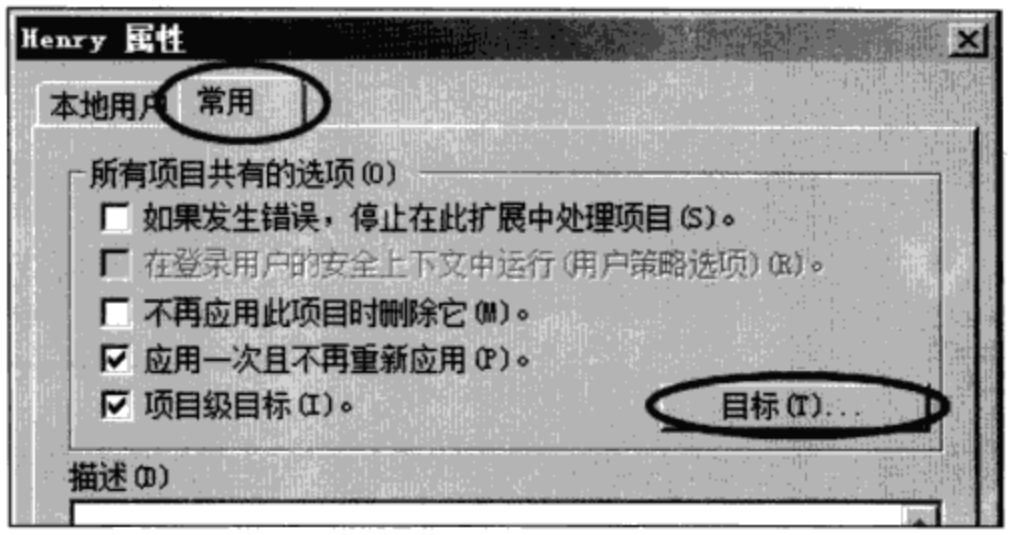


图 4-31

STEP 8 在图 4-32中【单击左上角的**新建项目**➲选择**计算机名称**】。

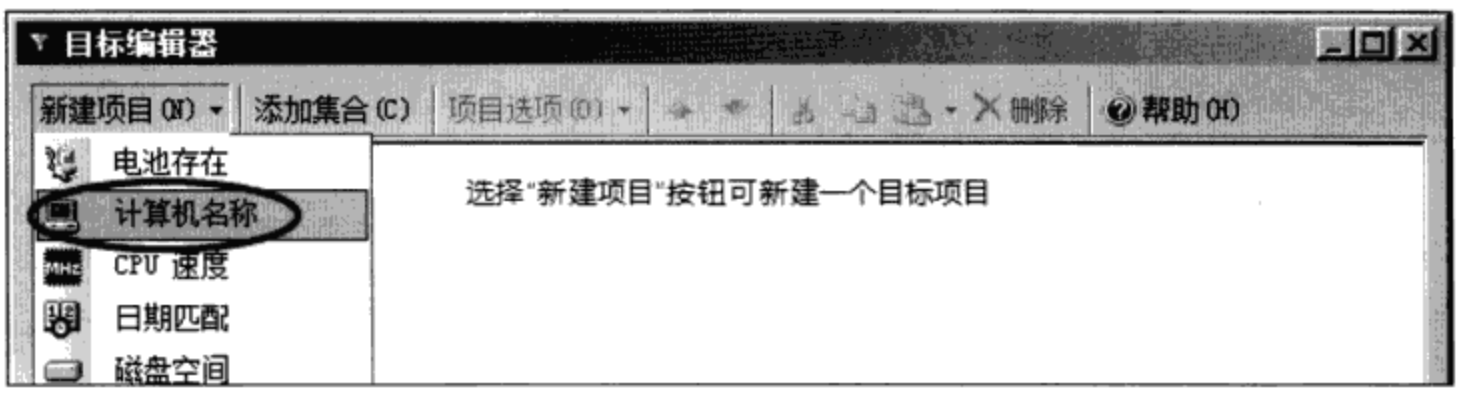


图 4-32

STEP 9 在图 4-33的**计算机名称**文本框中通过单击**浏览**按钮来选择仅将此项目应用到计算机Win7PC1后单击确定按钮。

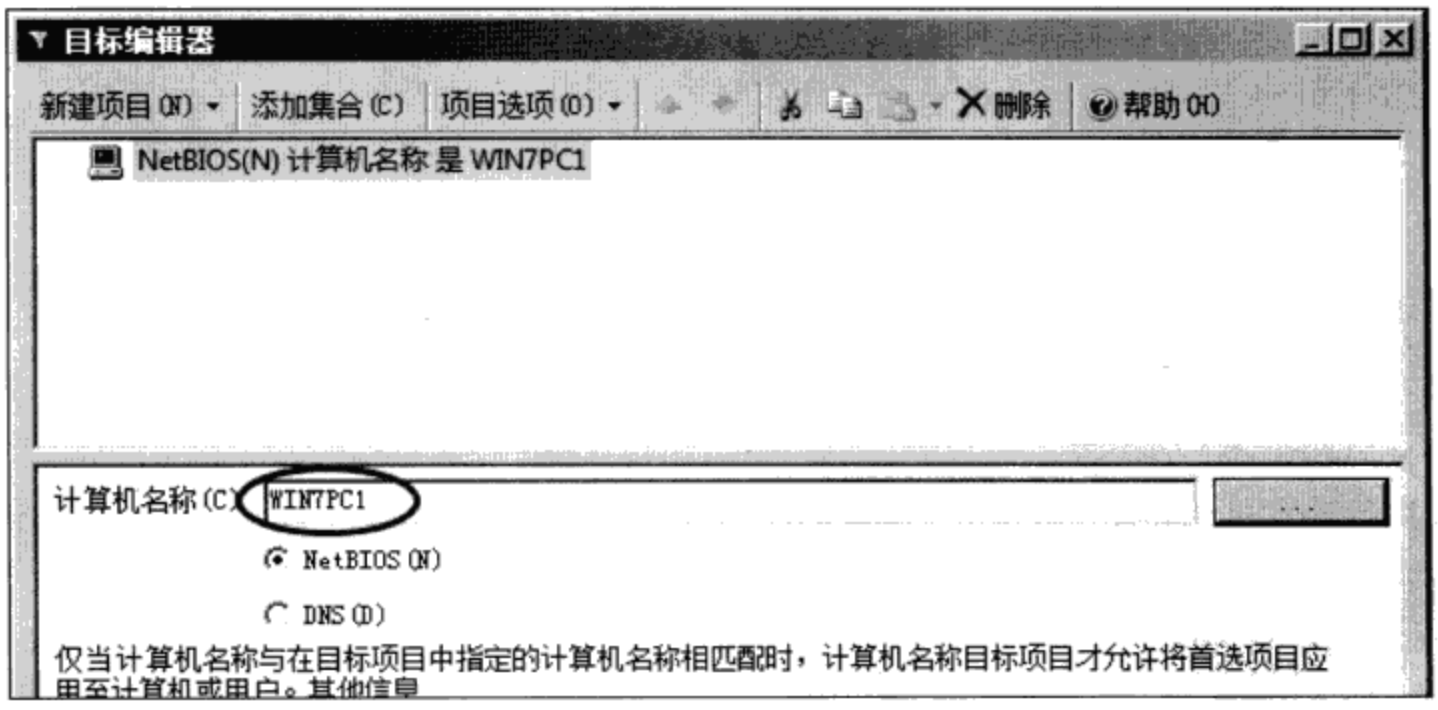


图 4-33

STEP 10 返回到前一个对话框后单击确定按钮。

STEP 11 图 4-34为完成后的对话框，图中右方为我们所设置的项目。

Download at http://www.pin5i.com/



图4-34

STEP 12 等上述组策略设置应用到域成员计算机Win7PC1后（重新启动此计算机或运行gpupdate程序），使用系统管理员身份登录，然后选择【开始➲管理工具➲计算机管理】，如图4-35所示为自动创建的用户账户Henry。

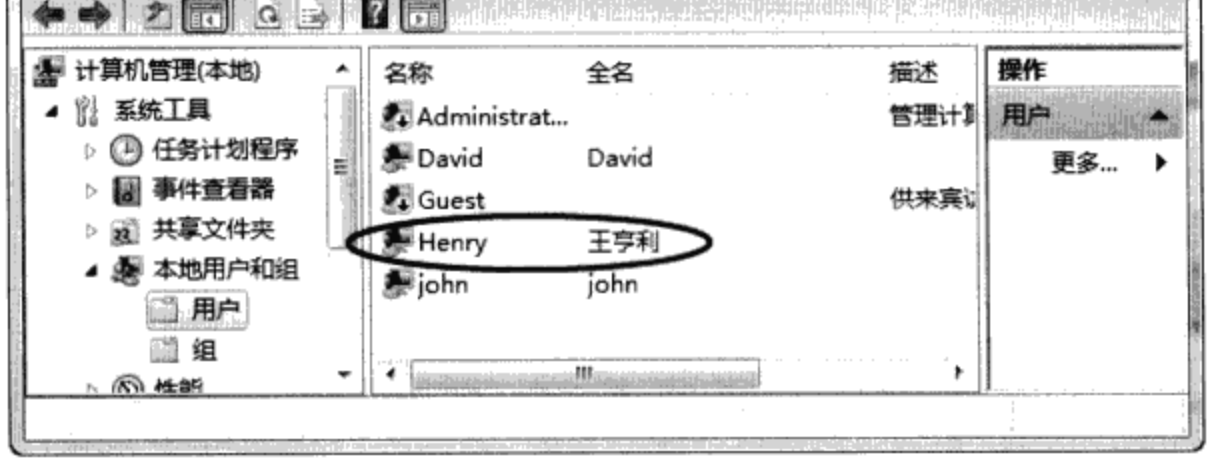


图4-35

4-4 组策略的处理规则

域成员计算机在处理（应用）组策略时具有一定的程序与规则，您必须了解它们，才能够通过组策略来充分管理用户与计算机的环境。

4-4-1 一般的继承与处理规则

组策略的设置是有继承性的，也有一定的处理规则：

Download at http://www.pin5i.com/

- 若高层父容器的某个策略被设置，但是其下层子容器并未设置此策略的话，则下层子容器会继承上层父容器的这个策略设置值。以图 4-36来说，如果位于高层的域sayms.com的GPO内，其**删除并组织访问“关机”命令**策略被设置为**已启用**，但是位于下层的组织单位**业务部**的这个策略被设置为**未配置**的话，则组织单位**业务部**会继承域sayms.com的这个设置值。若组织单位**业务部**之下还有其他子容器，且它们的这些策略也被设置为**尚未设置**的话，则它们也会继承这个设置值。

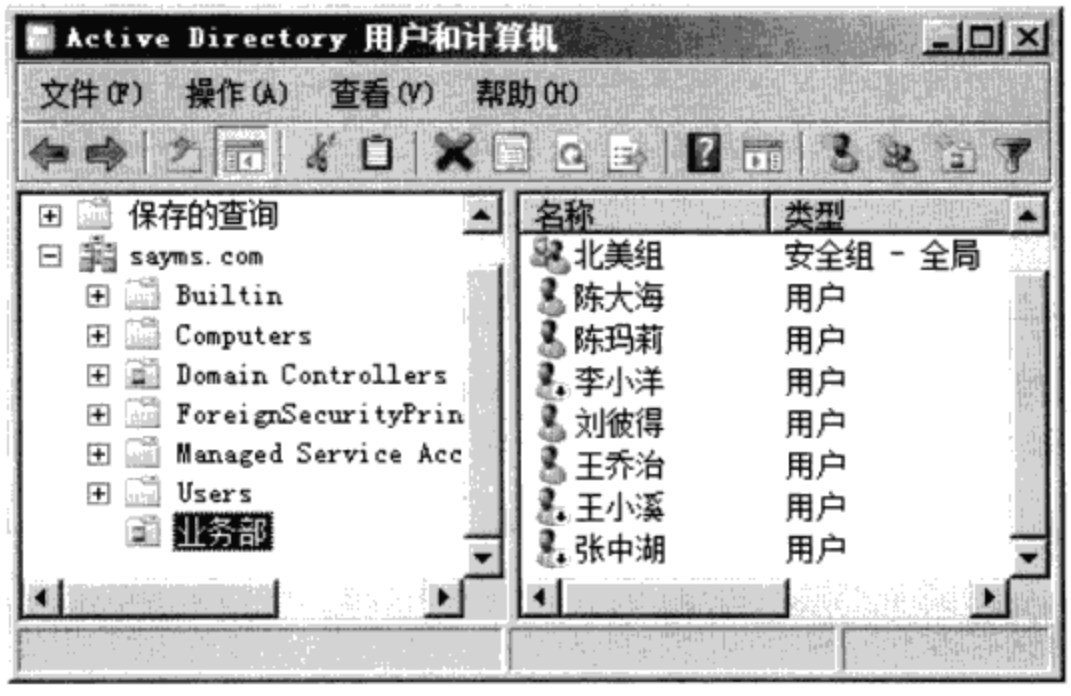


图4-36

- 若下层子容器内的某个策略被设置的话，则此设置值默认会覆盖由其上层父容器所继承下来的设置值。以图4-36为例，如果位于上层的域sayms.com的GPO内，其**删除并阻止访问“关机”命令**策略被设置为**已启用**，但是位于下层的组织单位**业务部**的这个策略被设置为**已禁用**，则组织单位**业务部**会覆盖域sayms.com的设置值，也就是对组织单位**业务部**来说，其**删除并阻止访问“关机”命令**策略是**已禁用**。
- 组策略设置是有累加性的，例如若您在组织单位**业务部**内创建了GPO，同时在站点、域内也都有GPO，则站点、域与组织单位内的所有GPO设置值都会被累加起来作为组织单位**业务部**的最后有效设置值。但是若站点、域与组织单位**业务部**之间的GPO设置有冲突时，则以处理顺序在后的GPO为优先，而系统处理GPO的顺序是：**站点的GPO最先处理、域的GPO次之、组织单位的GPO最后处理**，因此会以组织单位**业务部**的GPO设置优先。
- 系统是先处理**计算机配置**，再处理**用户配置**。若组策略内的**计算机配置**与**用户配置**有冲突时，虽然是后处理**用户配置**，但是在大部分的情况下却是以**计算机配置**优先。若您将多个GPO链接到同一处，则所有这些GPO的设置会被累加起来作为最后的有效设置值，但是若这些GPO的设置相互冲突时，则是以**链接顺序**在前面的GPO设置为优先，例如图 4-37中的**测试用的GPO**的设置优先于**防病毒软件策略**。

Download at http://www.pin5i.com/

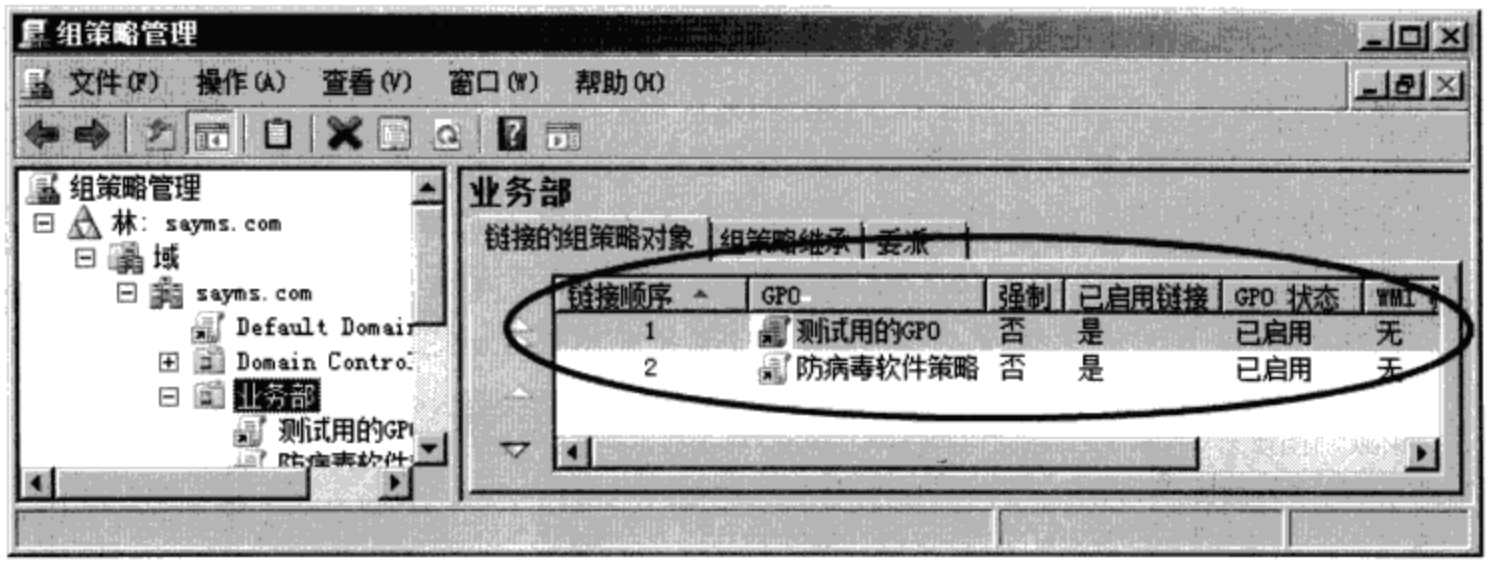


图4-37

提示

本地计算机策略的优先权最低，也就是说若**本地计算机策略**内的设置值与站点、域或组织单位的设置相冲突时，则以站点、域或组织单位的设置优先，**本地计算机策略**的设置无效。

4-4-2 例外的继承设置

除了一般的继承与处理规则外，您还可以设置以下的例外规则。

1. 阻止继承策略

您可以设置不让子容器继承父容器的设置，例如若不要让组织单位**业务部**继承域sayms.com的策略设置的话：【如图 4-38所示对着**业务部**单击右键➲阻止继承】，此时组织单位**业务部**将直接以自己的GPO设置为其设置值，若其GPO内的设置为**未配置**的话，则采用默认值。

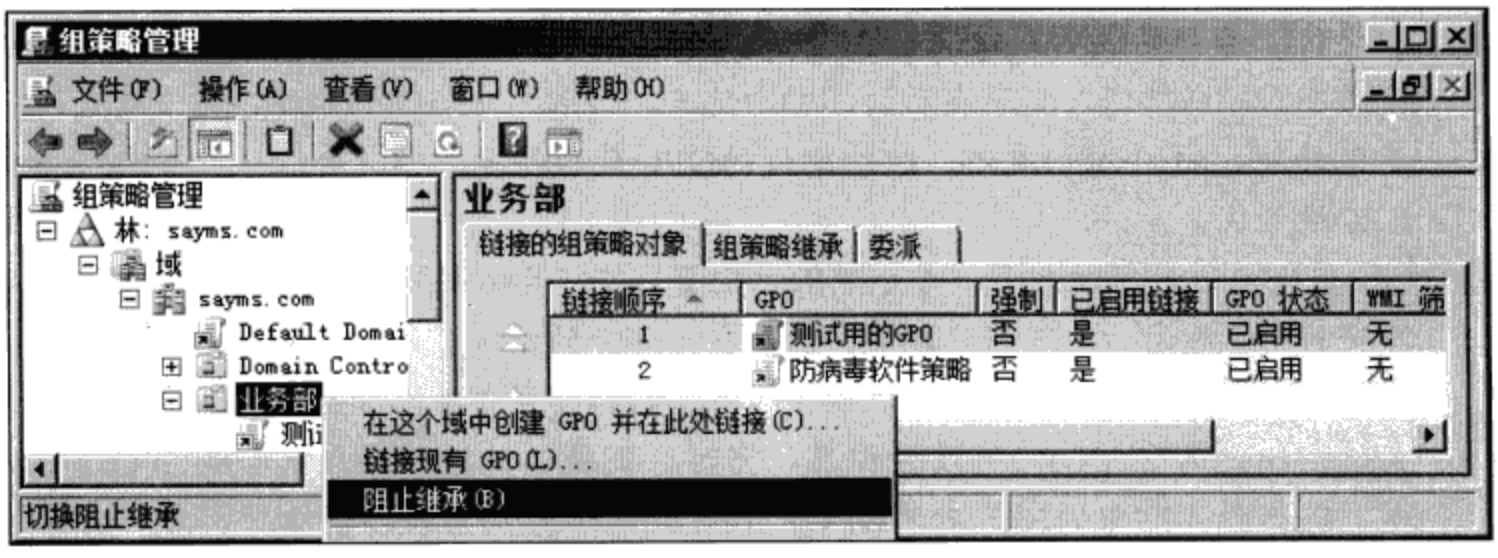


图4-38

Download at http://www.pin5i.com/

2. 强制继承策略（Enforcing Inheritance）

您可以在父容器内通过GPO的**强制**选项，来强制其下子容器必须继承此GPO的设置，无论子容器是否选择了**阻止继承**。例如假设我们在图 4-39中域sayms.com下创建了一个GPO：**企业安全防护策略**，并通过它来设置域内所有计算机的安全措施，然后通过【对着此策略右击➲强制】来强制其下的所有组织单位都必须继承此策略。

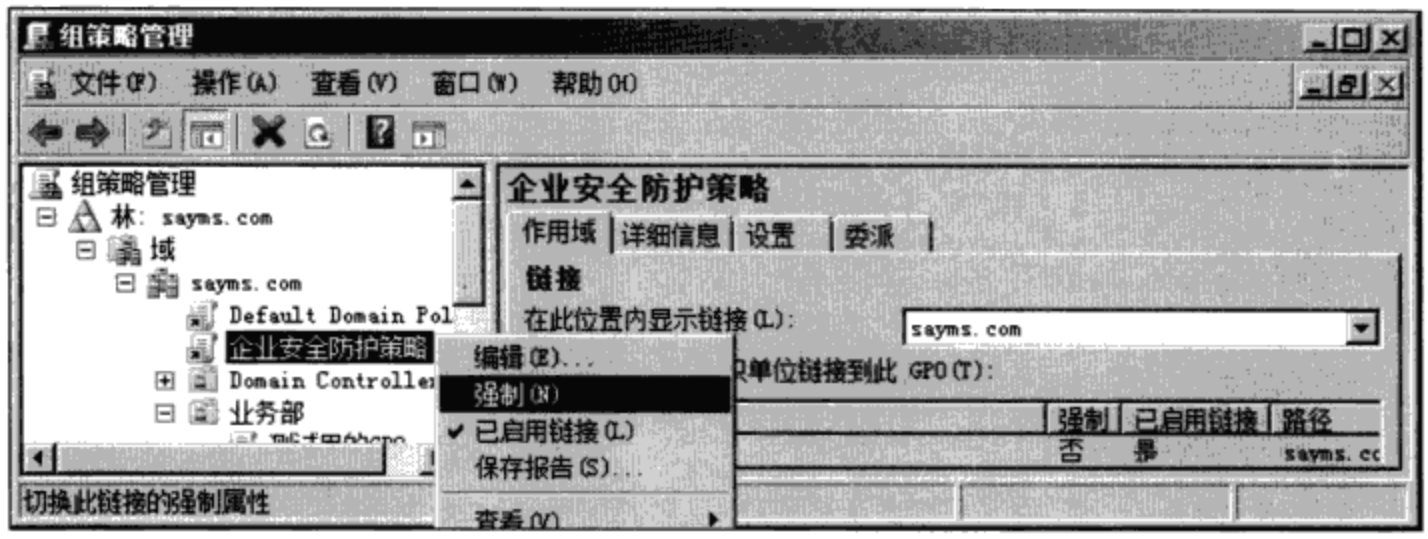


图 4-39

3. 过滤组策略设置

以组织单位**业务部**为例，当您针对此组织单位创建GPO后，此GPO的设置会被应用到这个组织单位内的所有用户与计算机，如图 4-40所示默认是被应用到Authenticated Users组（身份经过确认的用户）。

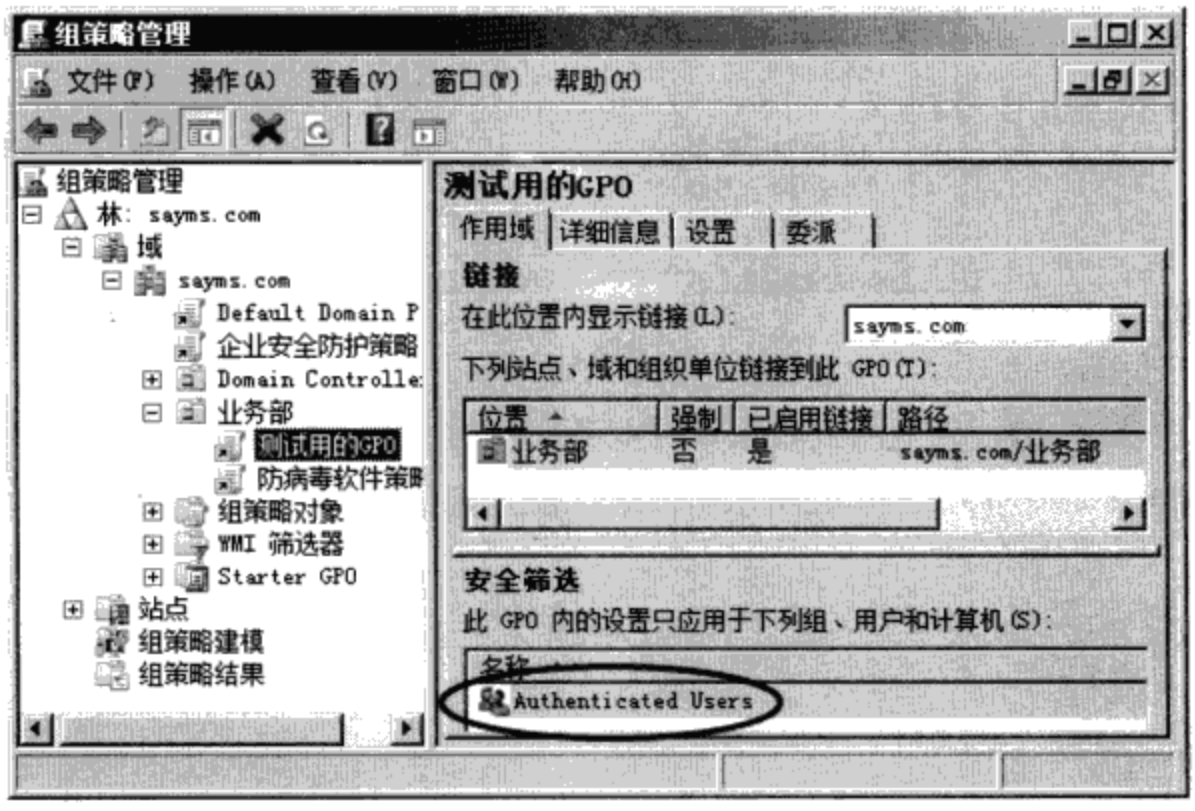


图 4-40

Download at http://www.pin5i.com/

不过您也可以让此GPO不要应用到特定的用户或计算机，例如此GPO对所有业务部的工作环境做了某些限制，但是您却不想将此限制附加给业务部经理。位于组织单位内的用户与计算机，默认对该组织单位的GPO都具备**读取**与**应用组策略**权限，您可以如图 4-41所示，通过单击GPO（例如**测试用的GPO**）➲单击**委派**标签➲单击高级按钮➲选择Authenticated Users】的方式进行查看。

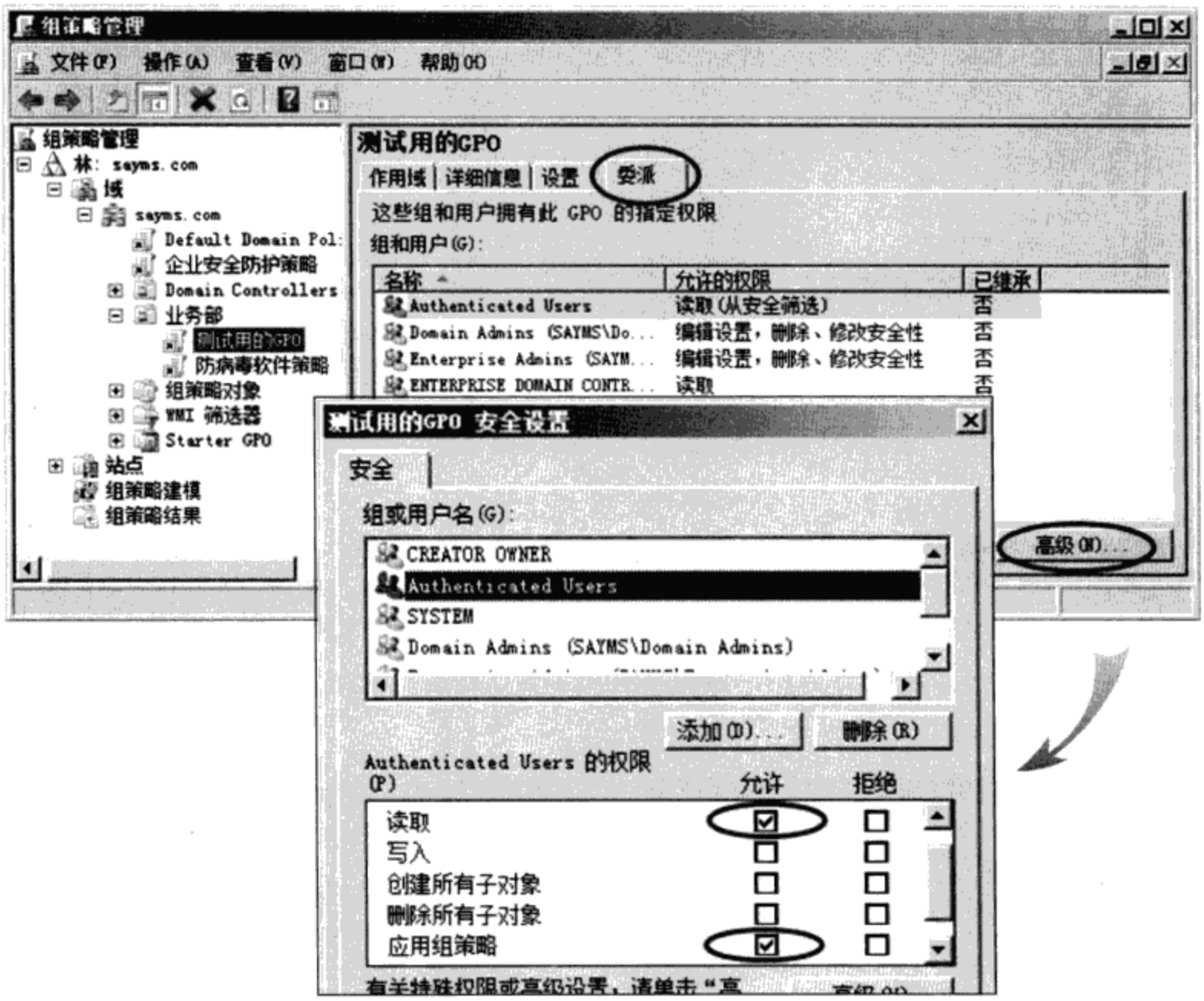


图4-41

若不想将此GPO的设置应用到组织单位**业务部**内的用户Peter的话:【请单击图 4-41中的添加按钮➲选择用户Peter➲如图 4-42所示将Peter的**应用组策略**权限设置为**拒绝**即可】。

Download at http://www.pin5i.com/

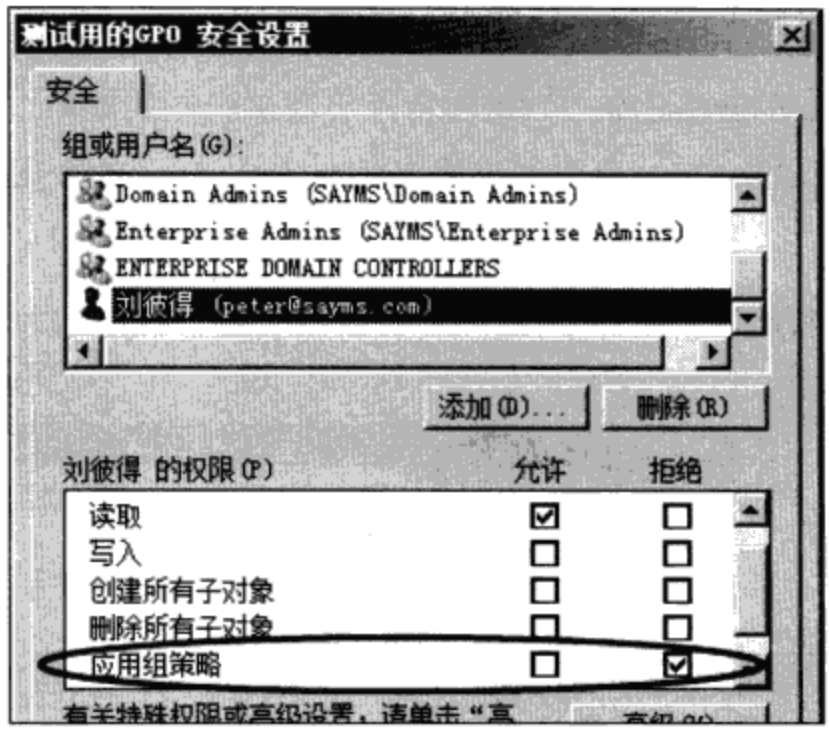


图 4-42

4-4-3 特殊的处理设置

这些特殊处理设置包含强制处理GPO、慢速链接的GPO处理、环回处理模式与禁用GPO。

1. 强制处理 GPO

客户端计算机在处理组策略的设置时，会将不同类型的策略交给不同的DLL（Dynamic-Link Libraries）来负责处理与应用，这些DLL被称为Client-Side Extension（CSE）。不过CSE在处理其所负责的策略时，只会处理上次处理过后的最新变动策略，这种做法虽然可以提高处理策略的效率，但有时候却无法达到您所期望的目标，例如您在GPO内对用户做了某项限制，在用户因这个策略而受到限制之后，若用户自行将此限制删除，则当下一次用户计算机在应用策略时，客户端的CSE会因为GPO内的策略设置值并没有变动而不处理此策略，因而无法自动将用户自行更改的设置改回来。

解决此问题的方法是强制要求客户端CSE一定要处理指定的策略，无论该策略设置值是否有变动。您可以针对不同策略来单独设置。举例来说，假设您强制组织单位**业务部**内所有计算机必须处理（应用）**软件安装策略**的话，则其设置方法是：如图 4-43所示在**测试用的GPO**的设置界面中通过【计算机设置➲策略➲管理模板➲系统➲组策略➲双击右方的**软件安装策略处理**➲选择**已启用**单选按钮➲选择**即使尚未更改组策略对象也进行处理**复选框➲单击确定按钮】的方式进行操作。从图 4-43中可知还可以针对其他策略进行设置。


提示

只要策略名称最后两个字是**处理**（Processing）的策略设置都可以做类似的更改。

Download at http://www.pin5i.com/

如果要自行手动让您的计算机来强制处理（应用）所有计算机策略设置的话，可以使用**gpupdate/target:computer/force**命令；如果要自行手动来强制处理所有用户策略设置的话，可以使用**gpupdate /target:user /force**命令；或使用**gpupdate /force**命令来同时强制处理计算机与用户设置。

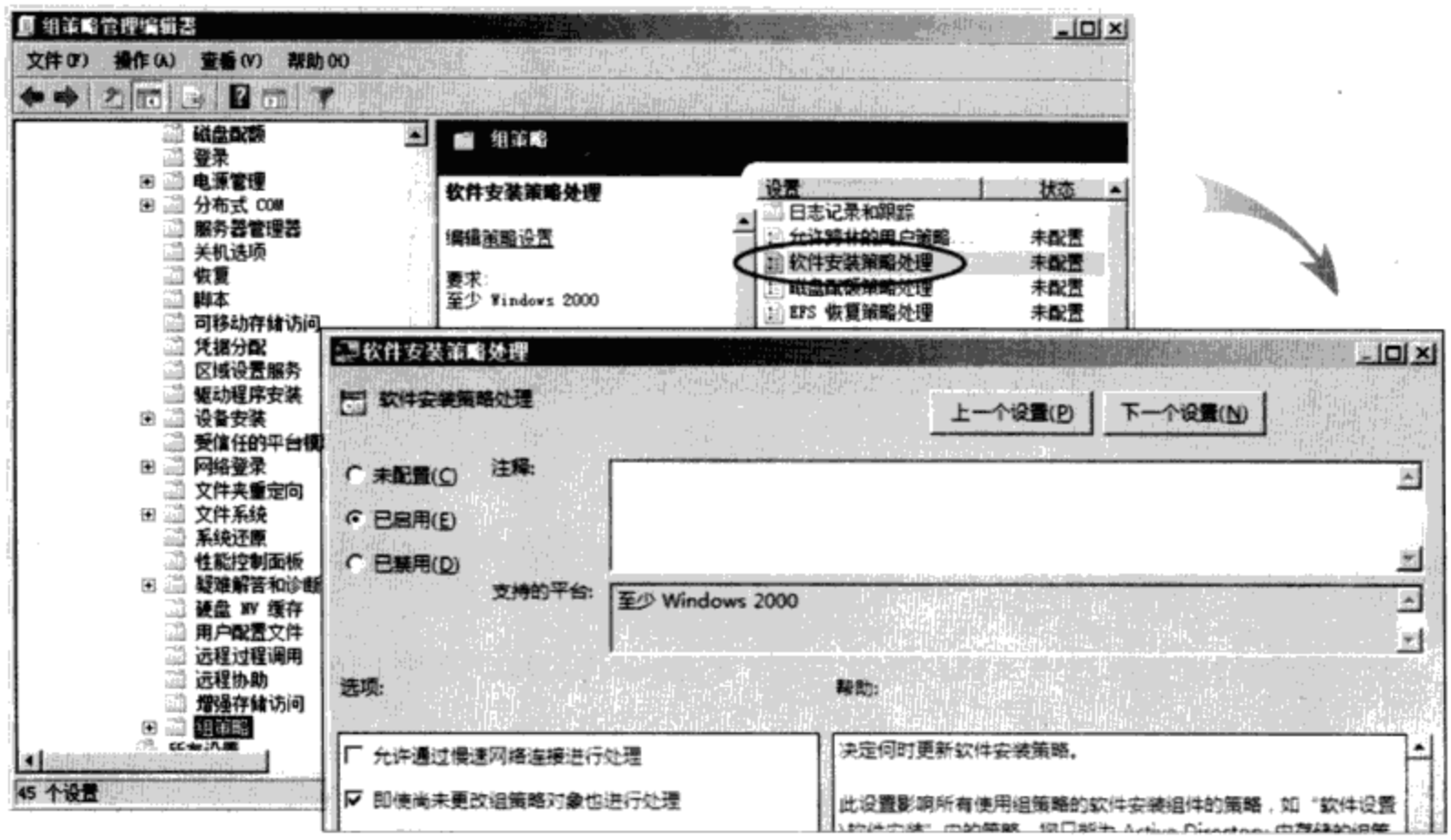


图4-43

2. 慢速链接的 GPO 处理

您可以让域成员计算机来自动检测其与域控制器之间的链接速度是否太慢，若是的话，就不要应用位于域控制器内指定的组策略设置。除了图 4-44中**注册表策略处理**与**安全性策略处理**这两个策略之外（无论是否慢速链接都会应用），其他策略都可以设置为慢速链接不应用。



图4-44

Download at http://www.pin5i.com/

假设您要求组织单位**业务部**内的每一台计算机都要自动检测是否为慢速链接：请在**测试用的GPO**的**计算机设置**界面中，如图 4-45所示，通过【双击**组策略**右方的**组策略慢速链接检测**➲选择**已启用**单选按钮➲在**连接速度**文本框中输入慢速链接的定义值➲单击确定按钮】的方式进行操作，图中我们设置只要连接速度低于500 Kbps，就视为慢速。如果您已禁用或未配置此策略的话，则默认也是将低于500 Kbps视为慢速链接。

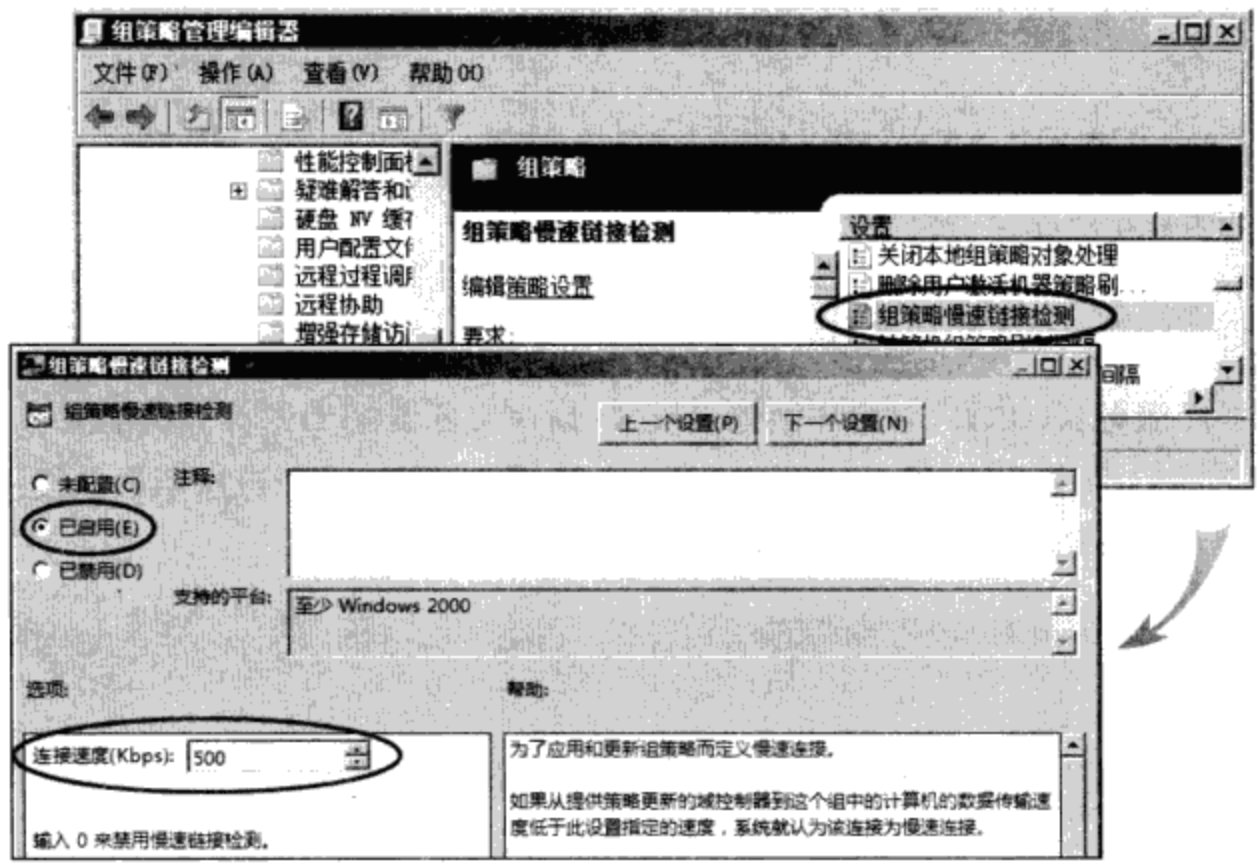


图4-45

接下来假设组织单位**业务部**内的每一台计算机即使与域控制器之间是慢速链接，也需要应用**软件安装策略处理**策略，其设置方法与图4-43相同，不过此时需在前图中选择**允许通过慢速网络连接进行处理**复选框。

3. 环回处理模式

一般来说，系统会根据用户或计算机账户在AD DS内的位置，来决定如何将GPO设置值应用到用户或计算机。例如服务器DC1的计算机账户位于组织单位**服务器**内，此组织单位有一个名称为**服务器GPO**的GPO，而用户Jackie的用户账户位于组织单位**业务部**内，此组织单位有一个名称为**测试用的GPO**的GPO，则当用户Jackie在DC1上登录域时，在正常的情况下，他的用户环境是由**测试用的GPO**的**用户配置**来决定，不过他的计算机环境却是由**服务器GPO**的**计算机配置**来决定。

然而若您在**测试用的GPO**的**用户配置**内，设置让组织单位**业务部**内的用户登录时，就自动为用户安装某应用程序的话，则这些用户到任何一台计算机上（包含DC1） 登录时，系统

Download at http://www.pin5i.com/

将为用户在这台计算机内安装此应用程序，但是您却不想为用户在这台重要的服务器DC1内安装应用程序，此时您要如何来解决这个问题呢？请启用**环回处理模式**（Loopback Processing Mode）。

若在**服务器GPO**启用了**环回处理模式**，则无论用户账户是位于何处，只要用户是使用组织单位**服务器**内的计算机（包含服务器DC1）登录，则用户的工作环境可改由**服务器GPO**的**用户配置**来决定，如此Jackie到服务器DC1登录时，系统就不会为他安装应用程序。**环回处理模式**分为以下两种。

- 替换模式：直接改由服务器GPO的用户配置来决定用户的环境，而忽略测试用的GPO的用户配置。
- 合并模式：先处理测试用的GPO的用户配置，再处理服务器GPO的用户配置，若两者有冲突，则以服务器GPO的用户配置优先。

假设我们要在**服务器GPO**内启用**环回处理模式**：请在**服务器GPO**的**计算机配置**界面中（如图 4-46所示），通过双击**组策略**右方的**用户组策略环回处理模式**➲选择**已启用**单选按钮➲在**模式**处选择**替换**或**合并**】的方式进行操作。

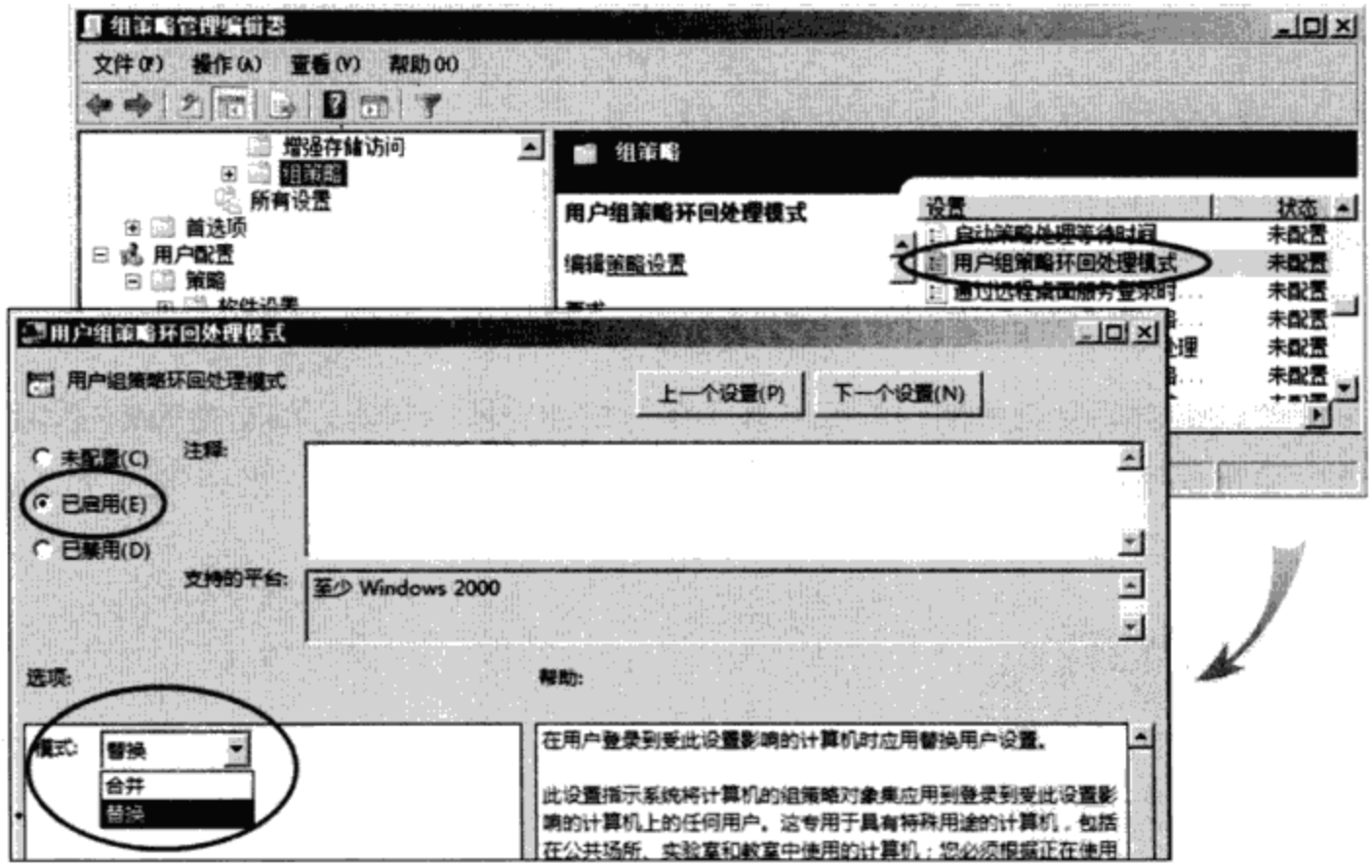


图 4-46

4. 禁用 GPO

若有需要的话，可以将整个GPO禁用，或单独将GPO的**计算机配置**或**用户配置**禁用。以**测试用的GPO**为例：

Download at http://www.pin5i.com/

- 若要将整个GPO禁用的话，请如图 4-47所示对着**测试用的GPO**右击，然后通过**已启用链接**选项来将此GPO禁用。

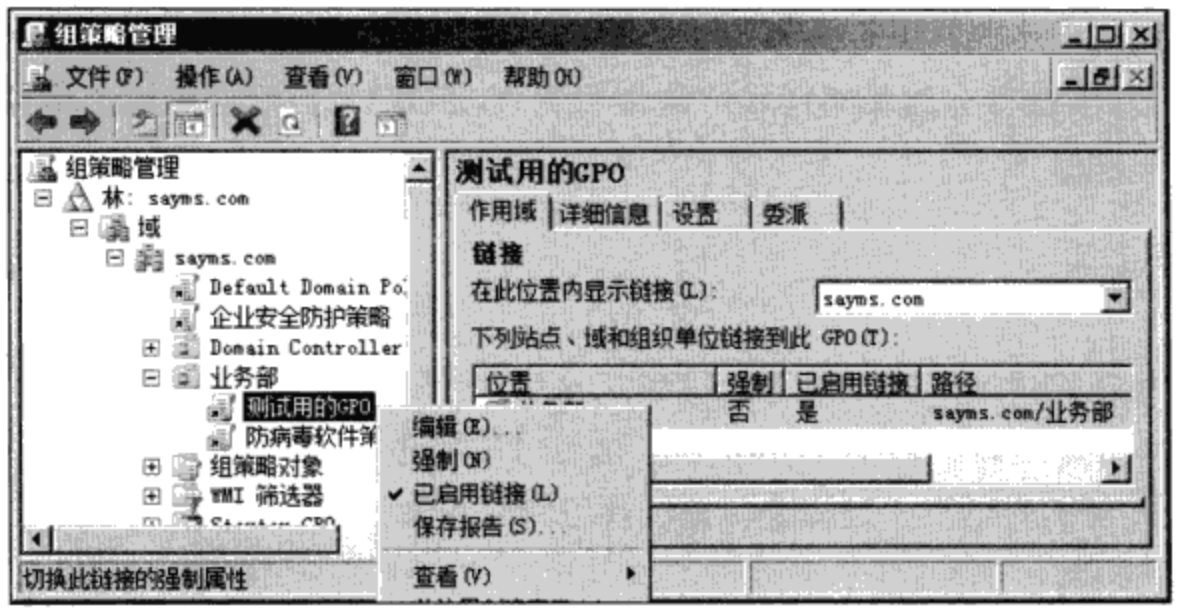


图 4-47

- 若要将GPO的**计算机配置**或**用户配置**单独禁用的话，通过【先进入**测试用的GPO**的编辑界面➲如图 4-48所示单击**测试用的GPO**➲单击**属性**图标➲选择**禁用计算机配置设置**或**禁用用户配置设置**复选框】的方式进行操作。

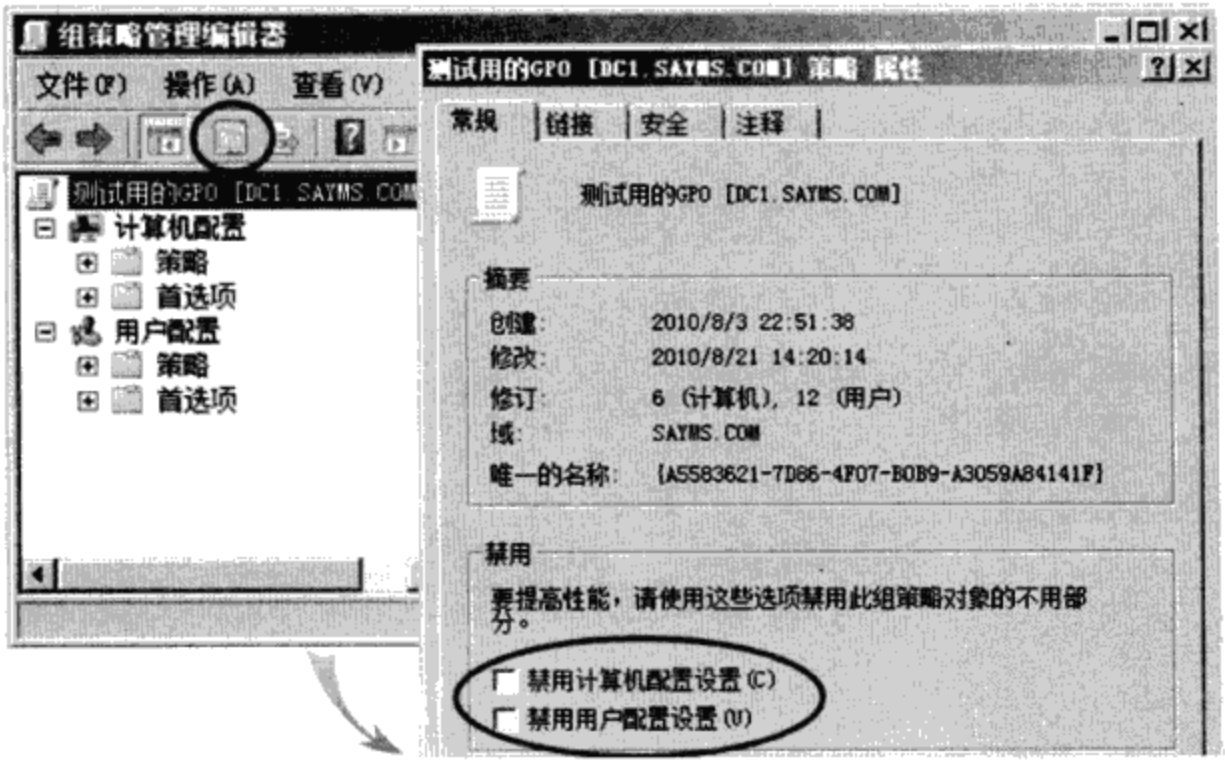


图 4-48

4-4-4 更改管理GPO的域控制器

当您添加、修改或删除组策略设置时，这些变动默认是先被存储到扮演**PDC模拟器操作主机**角色的域控制器，然后再由它将其复制到其他域控制器，域成员计算机再通过域控制器来应用这些策略。

Download at http://www.pin5i.com/

但若系统管理员人在上海，可是**PDC模拟器操作主机**却在远端的北京，此时上海的系统管理员希望其针对上海员工所设置的组策略，直接存储到位于上海的域控制器，以便上海的用户与计算机能够通过这台域控制器来迅速地应用这些策略。

您可以通过**DC选项**与**组策略**两种方式来将管理GPO的域控制器从**PDC模拟器操作主机**更改为其他域控制器。

1. 使用 DC 选项

假设供上海分公司使用的GPO为上海分公司专用GPO，则请进入编辑此GPO的界面（组策略管理编辑器界面），然后如图 4-49所示，通过【单击上海分公司专用GPO➲选择**查看**菜单➲DC选项➲在弹出的对话框中选择要用来管理组策略的域控制器】的方式进行操作。图中选择域控制器的选项有以下三种：

- 具有 PDC 模拟器操作主机令牌的域控制器：也就是使用**PDC模拟器操作主机**，这是默认值，也是建议值。
- 由 Active Directory管理单元使用的域控制器：当系统管理员运行**组策略管理编辑器**时，此**组策略管理编辑器**所连接的域控制器就是我们要选择的域控制器。
- 使用任何可用的域控制器：此选项让**组策略管理编辑器**可以任意挑选一台域控制器。不建议采用此种方式。

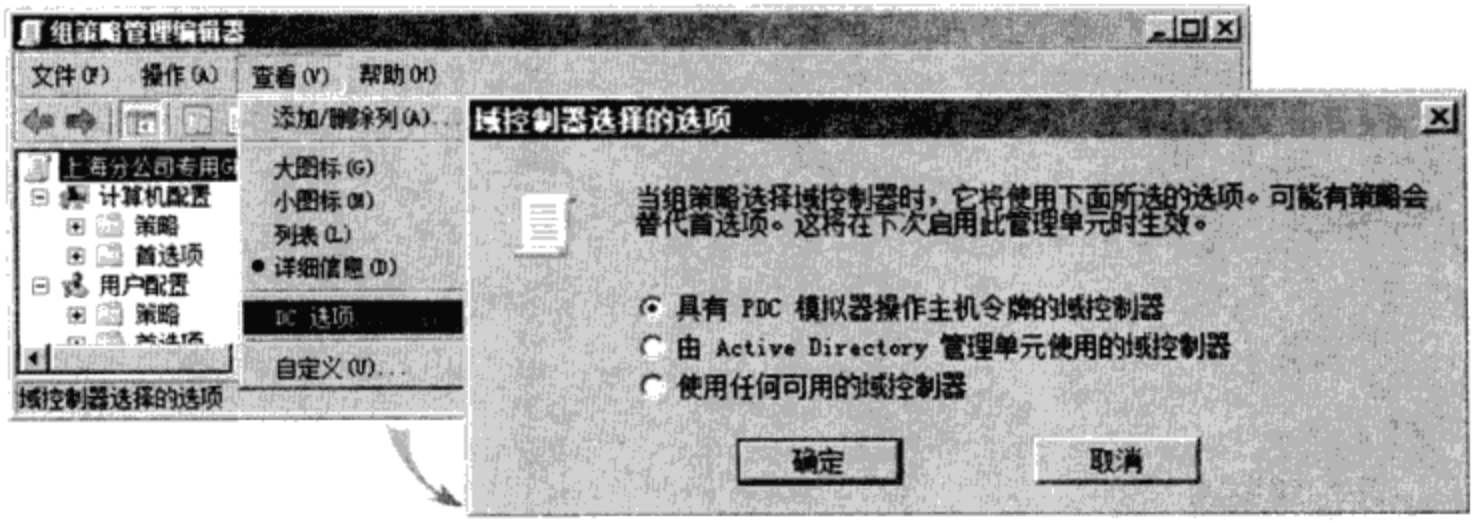


图 4-49

2. 使用策略设置

假设要针对上海系统管理员来设置，而我们需要针对其用户账户所在的组织单位来设置：【如图4-50所示进入编辑此组织单位的GPO界面（**组策略管理编辑器**界面）后，双击右方的**组策略域控制器选择**，然后按如图所示来选择域控制器，图中的选项说明同上，其中**主域控制器**就是**PDC模拟器操作主机**】。

Download at http://www.pin5i.com/

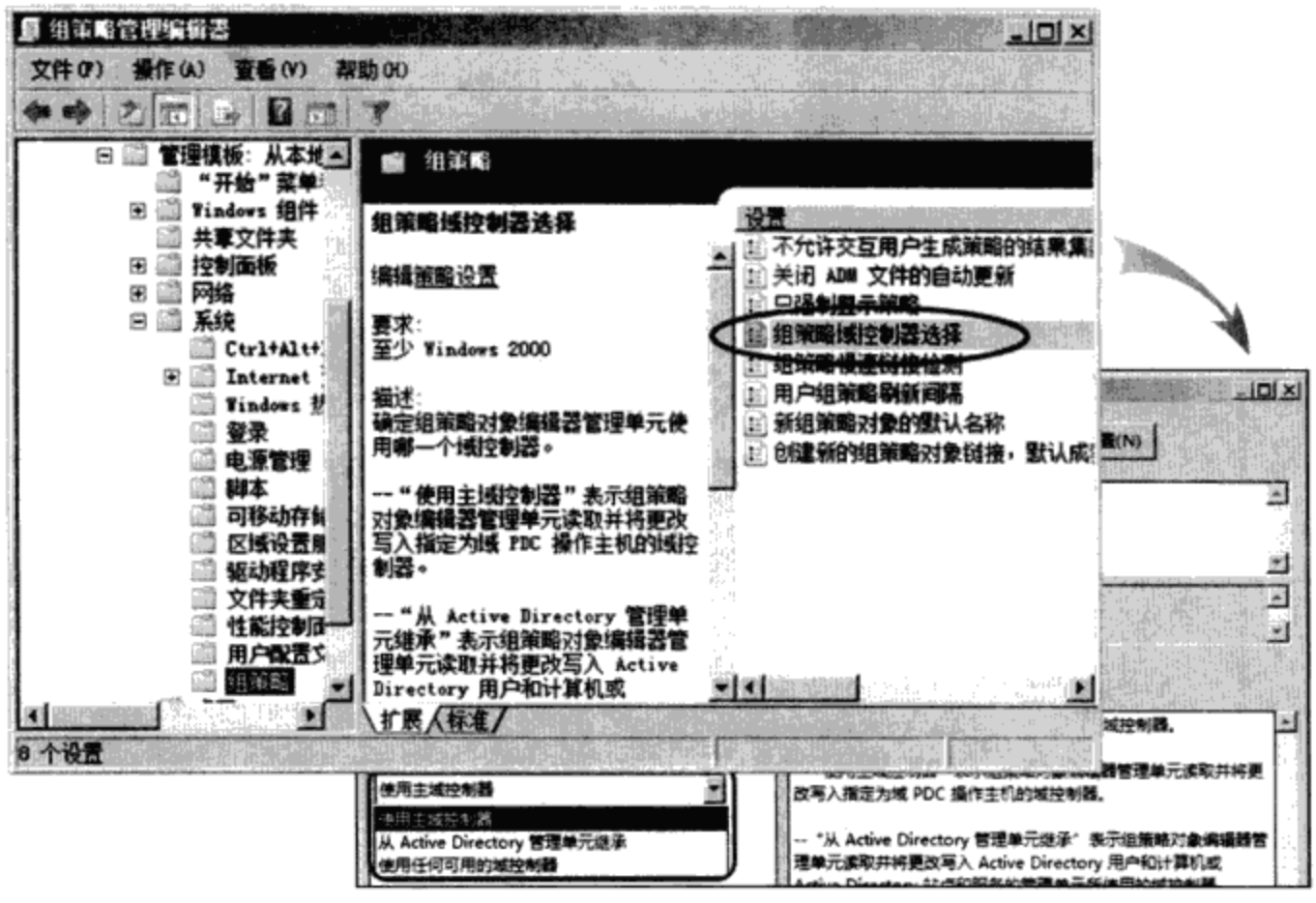


图 4-50

4-4-5 更改组策略的应用间隔时间

我们在前面已经介绍过域成员与域控制器何时会应用组策略的设置。您可以更改这些设置值，不过建议不要将刷新组策略的间隔时间设得太短，否则会增加网络负担。

1. 更改计算机配置的应用间隔时间

例如要更改组织单位**业务部**内所有计算机来应用**计算机配置**的间隔时间的话：请在**测试用的GPO**的**计算机配置**界面中，如图 4-51所示，通过【双击**组策略**右方的**计算机组策略刷新间隔**➲选择**已启用**单选按钮➲通过前图来设置➲单击确定按钮】的方式进行操作，图中设置为每隔90分钟加上0~30分钟的随机值，也就是每隔90~120分钟应用一次。若已禁用或未配置此策略的话，则默认每隔90～120分钟应用一次。若应用间隔设置为0分钟的话，则会每隔7秒钟应用一次。

若要更改域控制器应用**计算机配置**的间隔时间的话，请针对组织单位Domain Controllers内的GPO来设置（例如Default Domain Controllers，GPO），其策略名称是**域控制器的组策略刷新间隔**，在双击此策略后，如图 4-52所示可知其默认是每隔5分钟应用组策略一次。若已禁用或未配置此策略的话，则默认就是每隔5分钟应用一次。若将应用间隔时间设置为0分钟的话，则会每隔7秒钟应用一次。

Download at http://www.pin5i.com/

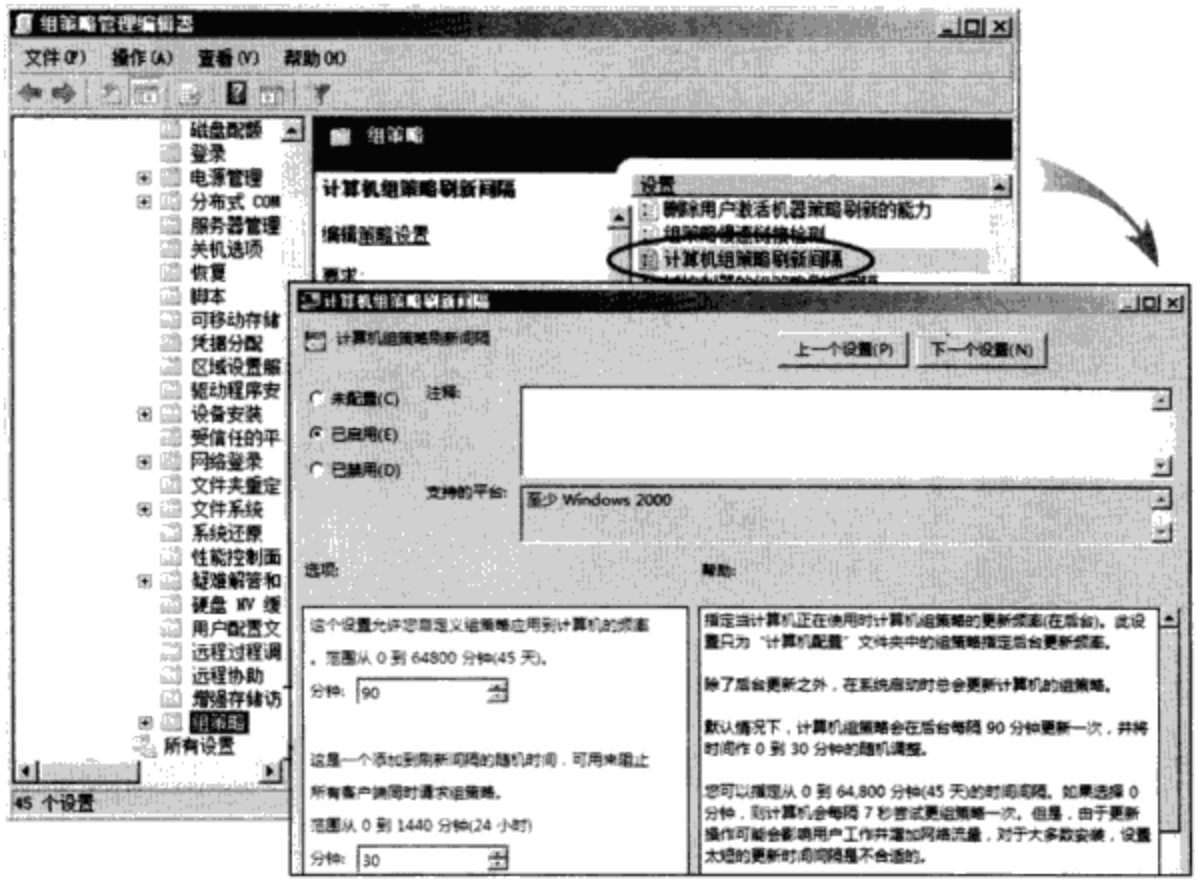


图 4-51

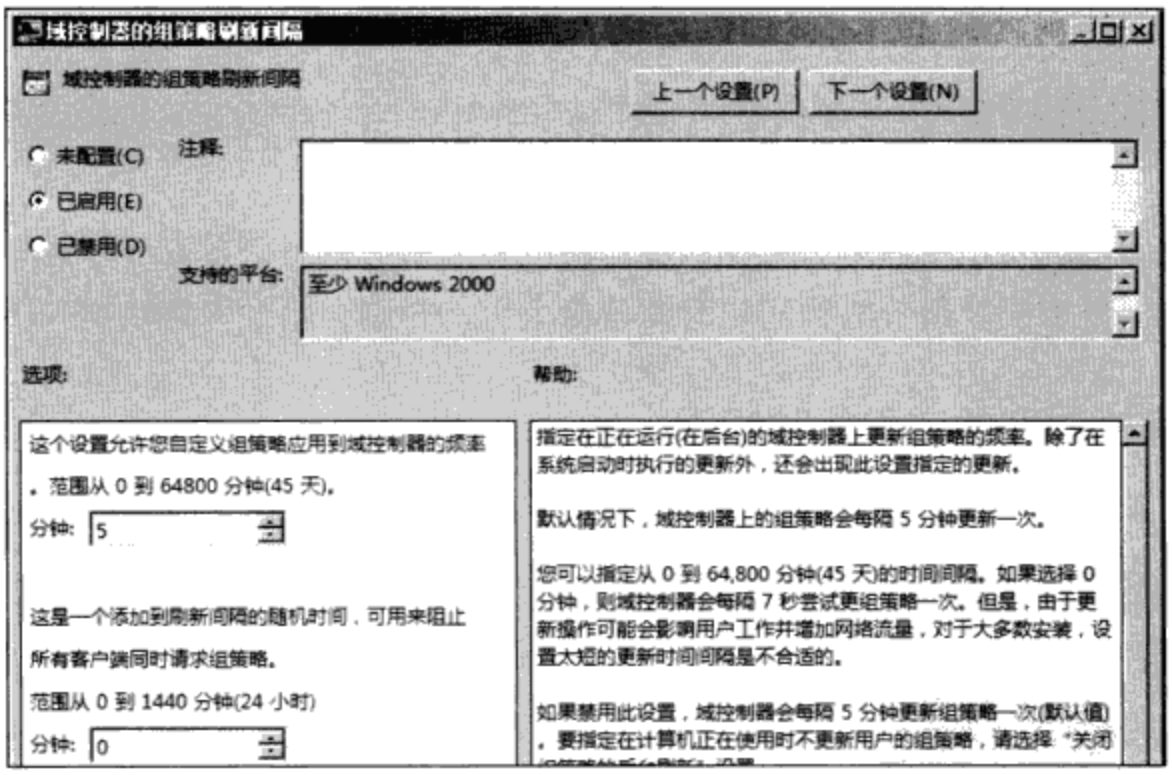


图 4-52

2. 更改用户配置的应用间隔时间

例如若要更改组织单位**业务部**内所有用户应用**用户配置**的间隔时间的话，请在**测试用的GPO**的**用户配置**界面中，通过图 4-53中**组策略**右方的**用户组策略刷新间隔**来设置，其默认也是每隔90分钟加上0~30分钟的随机值，也就是每隔90~120分钟应用一次。若已禁用或未配置此策略的话，则默认就是每隔90~120分钟应用一次。若将间隔时间设置为0分钟的话，则会每

Download at http://www.pin5i.com/

隔7秒钟应用一次。

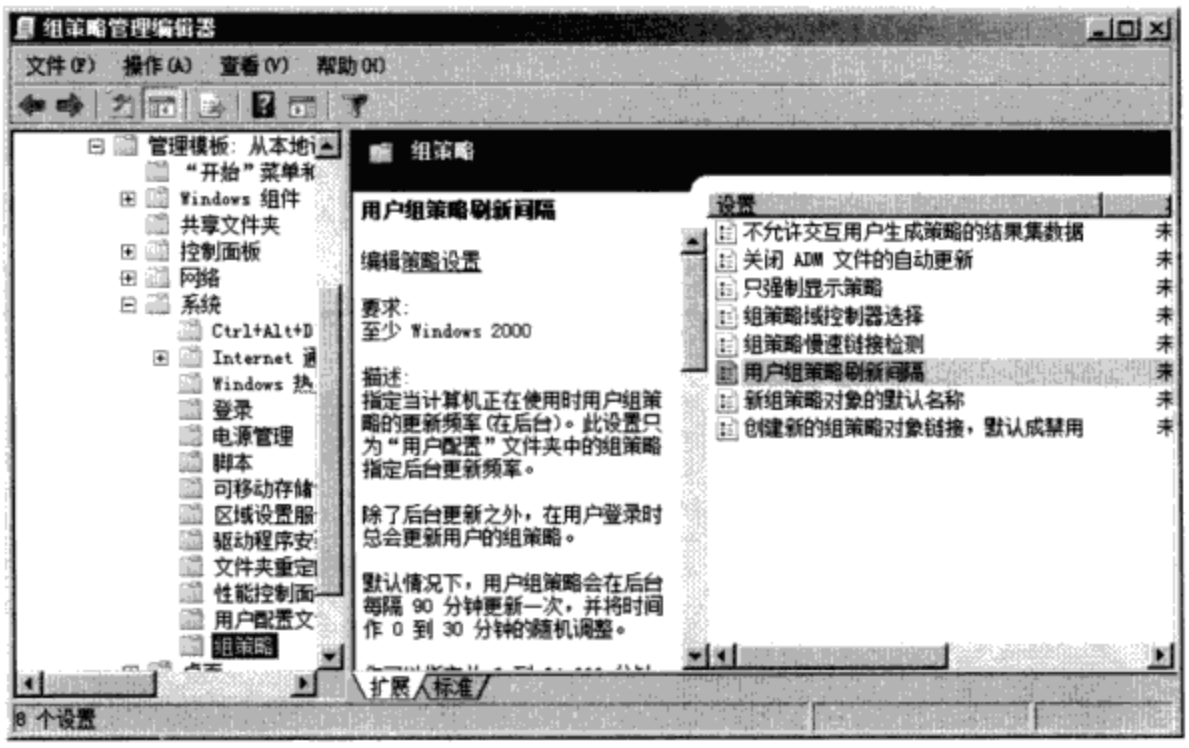


图4-53

4-5 使用组策略来管理计算机与用户环境

我们将通过GPO的以下几个设置来说明如何管理计算机与用户的工作环境：计算机配置的管理模板策略、用户配置的管理模板策略、账户策略、用户权限分配策略、安全选项策略、登录/注销、启动/关机脚本与文件夹重定向。

4-5-1 计算机配置的管理模板策略

在**策略设置实例演练一：计算机配置**中已练习过**管理模板策略**，此处仅说明两个常用设置。

- 显示"关闭事件追踪程序"：若禁用此策略的话，则用户将计算机关机时，系统就不会再要求用户提供关机的理由。其设置方法为：【系统➲双击右边的**显示"关闭事件追踪程序"**】。默认会将**关闭事件追踪程序**显示在服务器计算机上（例如Windows Server 2008 R2），而工作站计算机（例如Windows 7）不会显示。您可以针对服务器、工作站或两者来启用、禁用此策略。
- 显示用户以前交互式登录的信息：用户登录时屏幕上会显示用户上次成功登录与失败登录的日期与时间、自从上次登录成功后，登录失败的次数等信息（如图 4-54所示）。其设置方法为：【Windows组件➲Windows登录选项➲双击右边的**在用户登录期间显示有关以前登录的信息**】。客户端计算机必须是Windows Vista以上。

Download at http://www.pin5i.com/

注意

1. 请确认域功能级别是Windows Server 2008（含）以上后再启用此功能，否则用户登录时将无法获取登录信息，也无法登录。
2. 除了会应用到客户端计算机的GPO需启用此功能之外，您还必须在会应用到域控制器的GPO（例如Default Domain Controller Policy或Default Domain Policy）上启用此功能，否则用户登录时将无法获取登录信息，也无法登录。

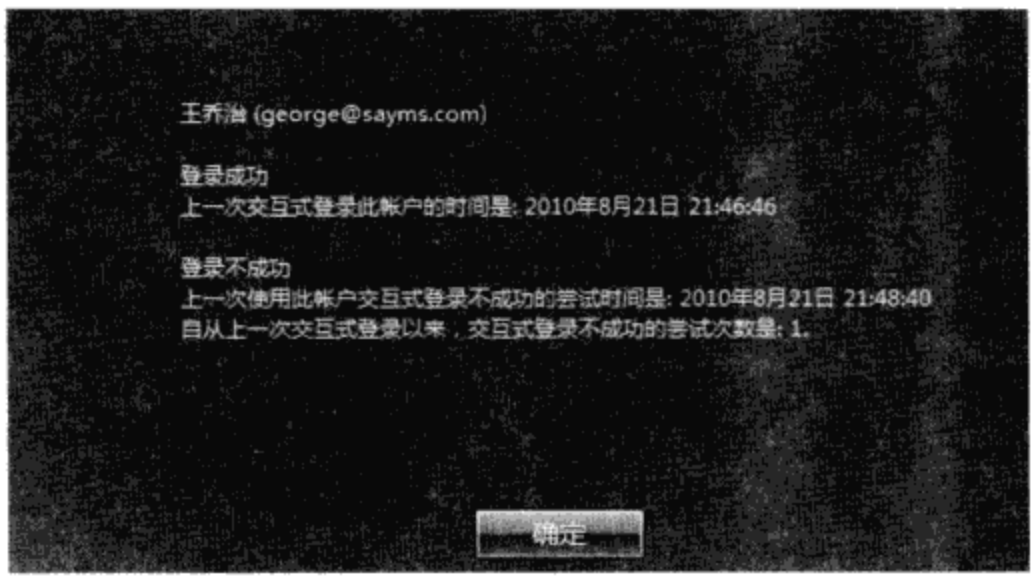


图4-54

您可以通过【打开Active Directory管理中心➲双击用户账户➲单击扩展区域➲单击属性编辑器】的方法来查看该用户的这些属性值（例如**msDS-LastSuccessfulInteractiveLogonTime**、**msDS-LastFailedInteractiveLogonTime**、**msDS-FailedInteractiveLogonCountAtLastSuccessfulLogon**等）。

您也可选择【打开**Active Directory用户和计算机**➲选择**查看**菜单➲高级功能➲对着用户账户单击右键➲属性➲单击**属性编辑器**标签➲从**属性**列表中来查看这些属性值】。

注意

如果您在客户端计算机上通过**本地计算机策略**来启用此策略，但是此计算机并未加入域功能级别为Windows Server 2008（含）以上的域的话，则用户在这台计算机登录时将无法获取登录信息，也无法登录。

4-5-2 用户配置的管理模板策略

在**策略设置实例演练二：用户配置**中已经练习过**管理模板策略**，此处仅说明几个常用设置。

- 限制用户只可以或不可以运行指定的Windows应用程序。其设置方法为：【系统➲双击

Download at http://www.pin5i.com/

右边的**只运行指定的Windows应用程序**或**不要运行已指定的Windows应用程序**】。在添加程序时，请输入该应用程序的可执行文件名称，例如eMule.exe。

Q 如果用户使用**资源管理器**更改此程序的文件名的话，是否这个策略就无法发挥作用?

A 是的，不过您可以使用第6章的**软件限制策略**来达到限制用户执行此程序的目的，即使其文件名被更改。

- 隐藏或只显示在控制面板内指定的项目。用户在控制面板内将看不到被隐藏起来的项目或只看得到被指定要显示的项目，其设置方法为【控制面板➲双击右边的**隐藏指定的“控制面板”项**或**只显示指定的“控制面板”项**】。在添加项目时，请输入项目名称，例如**鼠标**、**用户账户**等。
- 禁用单击Ctrl + Alt + Del键后所出现界面中的选项。用户单击Ctrl + Alt + Del键后，将无法选择界面中被您禁用的按钮，例如更改密码、启动任务管理器（或任务管理器）、注销等。其设置方法为【系统➲Ctrl + Alt + Del选项】。
- 隐藏和禁用桌面上所有的项目。其设置方法为【桌面➲隐藏和禁用桌面上的所有项目】。用户登录后，其桌面上所有的项目都会被隐藏，而且对着桌面无法单击鼠标右键。
- 删除Internet Explorer的**Internet选项**中的部分标签。用户将无法选择【**工具**菜单➲Internet选项】中被删除的标签，例如**安全**、**连接**、**高级**等标签。其设置方法为【Windows组件➲Internet Explorer➲双击右边的**Internet控制面板**】。
- 删除**开始**功能中的**关机**、**重新启动**、**睡眠和休眠**命令。其设置方法为【打开**开始**菜单和任务栏➲双击右边的**删除并阻止访问“关机”、“重新启动”、“睡眠”和“休眠”命令**】。在用户的**开始**菜单中，这些功能的图标都会被删除，同时单击Ctrl + Alt + Del键后也无法选择它们。

4-5-3 账户策略

我们可以通过账户策略来设置密码的使用准则与账户锁定方式。在设置账户策略时请特别注意以下说明：

- 针对域用户所设置的账户策略必须通过**域级别的GPO**来设置才有效，例如通过域sayms.com的Default Domain Policy GPO来设置，这个策略会被应用到域内的所有用户账户。通过站点或组织单位的GPO所设置的账户策略，对域用户没有作用。账户策略不但会被应用到所有的域用户账户，也会被应用到所有域成员计算机内的本地用户账户。
- 如果您针对某个组织单位（如图 4-55所示中的**金融部**）来设置账户策略，则这个账户

Download at http://www.pin5i.com/

策略只会被应用到位于此组织单位的计算机（例如图中的Win7PC101、Win7PC102、Win7PC103）的本地用户账户而已，但是对位于此组织单位内的域用户账户（例如图中的**王大杰**等）却没有影响。

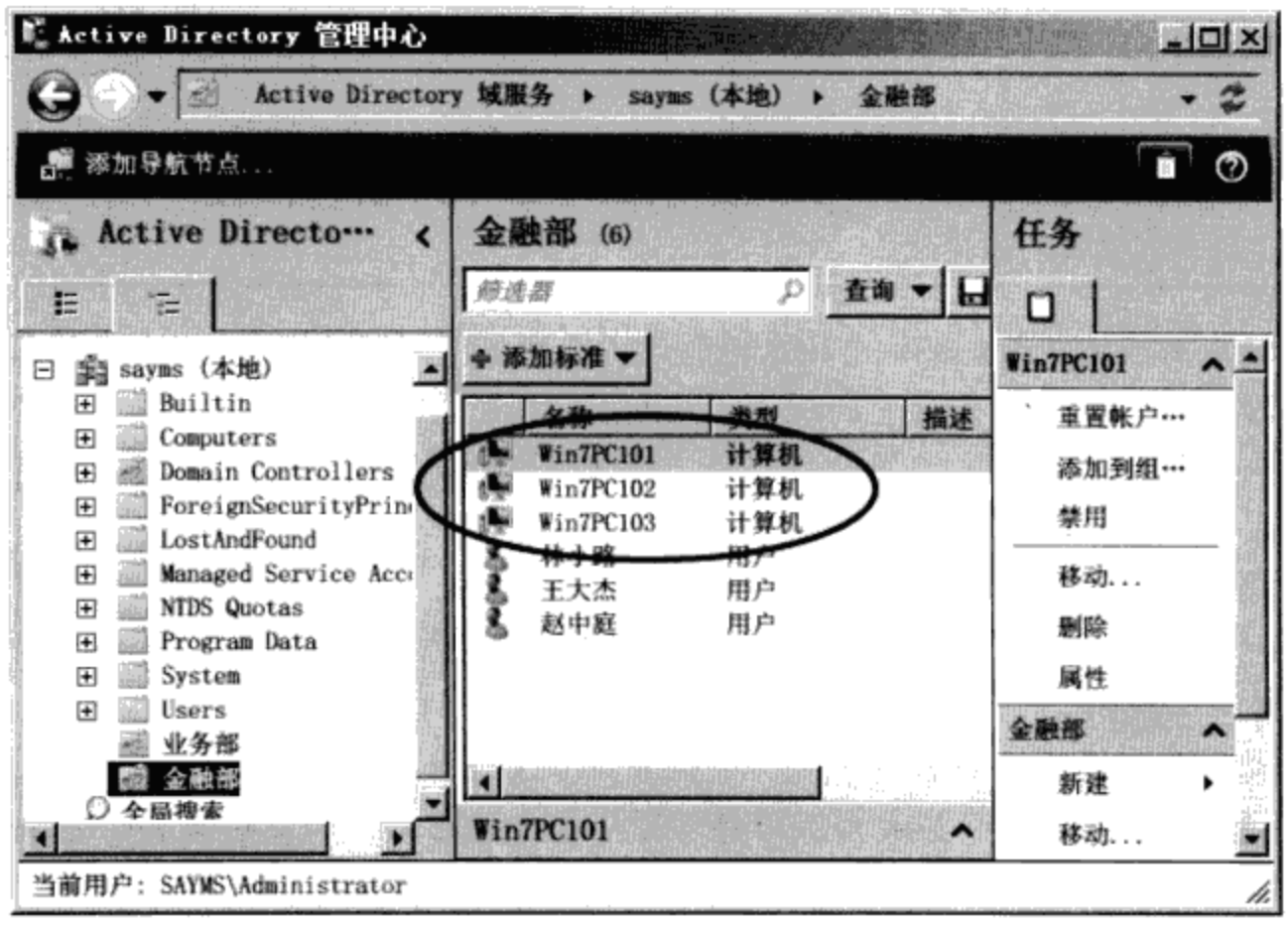


图4-55

提示

1. 若域与组织单位都设置账户策略，且设置有冲突时，则此组织单位内的成员计算机的本地用户账户会采用域的设置。
2. 域成员计算机也有自己的本地账户策略，不过若其设置与域/组织单位的设置有冲突的话，则采用域/组织单位的设置。

要设置域账户策略的话，如图4-56所示请通过【对着Default Domain Policy GPO（或其他域级别的GPO）单击右键➲编辑➲展开**计算机配置**➲策略➲Windows设置➲安全设置➲账户策略】的方法进行操作。

Download at http://www.pin5i.com/



图4-56

1. 密码策略

如图 4-57所示单击**密码策略**后就可以设置以下策略。

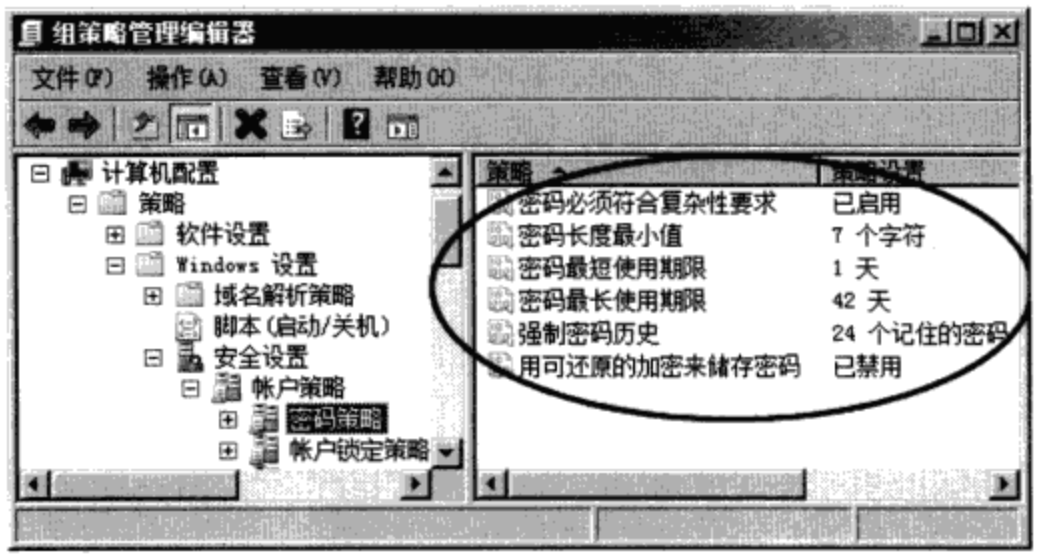


图4-57

（1）用可还原的加密来储存密码

若有应用程序需要读取用户的密码，以便验证用户身份的话，您就可以启用此功能，不过它相当于用户密码没有加密，因此不安全，默认为禁用。

（2）密码必须符合复杂性要求

若启用此功能的话，则用户的密码必须满足以下要求：

- 不可以包含用户账户名称中超过两个以上的连续字符。
- 长度至少要6个字符。
- 至少要包含A~Z、a~z、0~9、非字母数字（例如!、$、#、%）等4类字符中的3类。

因此若密码设置为123ABCdef是有效的，然而87654321是无效的，因为它只使用数字这一

Download at http://www.pin5i.com/

类字符。又例如若用户账户名称为peter，则123ABCpeter是无效的密码，因为包含用户账户名称两个以上的字符。AD DS域默认是启用此策略，独立服务器默认是禁用。

（3）密码最长使用期限

用来设置密码最长的使用期限（可为0~999天）。用户在登录时，若密码使用期限已到的话，系统会要求用户更改密码。若此处为0表示密码没有使用期限。AD DS域与独立服务器的默认值都是42天。

（4）密码最短使用期限

用来设置用户密码的最短使用期限（可为0~998天），在期限未到前，用户不得更改密码。若此处为0表示用户可以随时更改密码。AD DS域的默认值为1，独立服务器的默认值为0。

（5）强制密码历史

用来设置是否要记录用户曾经使用过的旧密码，以便决定用户在更改密码时，是否可以重复使用旧密码。此处可被设置为1~24或0。

- 1~24：表示要保存密码历史记录。例如若设为5，则用户的新密码不可与前5次所使用过的旧密码相同。
- 0：表示不保存密码历史记录，因此密码可以重复使用，也就是用户更改密码时，可以将其设置为以前曾经使用过的任何一个旧密码。

AD DS域的默认值为24，独立服务器的默认值为0。

（6）密码长度最小值

用来设置用户账户的密码最少需几个字符。此处可为0~14，若为0，表示用户账户可以没有密码。AD DS域的默认值为7，独立服务器的默认值为0。

2. 账户锁定策略（Account Lockout Policy）

您可以通过图 4-58中的**账户锁定策略**来设置锁定用户账户的方式。

（1）账户锁定阈值（Account Lockout Threshold）

我们可以让用户登录多次失败后（密码输入错误），就将该用户账户锁定，在未被解除锁定之前，用户无法再使用此账户来登录。此处用来设置登录失败的次数，其值可为0~999，若为0，表示账户永远不会被锁定。默认值为0。

Download at http://www.pin5i.com/

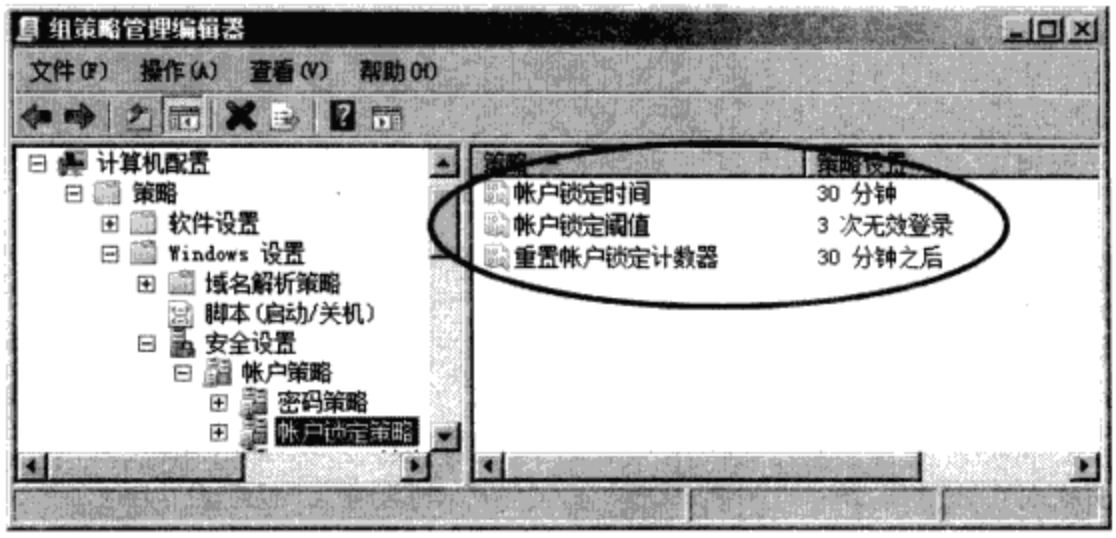


图4-58

（2）账户锁定时间（Account Lockout Duration）

用来设置锁定账户的期限，期限过后自动解除锁定。此处可为0~99999分钟，若为0分钟表示永久锁定，不会自动解除锁定，此时需要由系统管理员手动来解除锁定，也就是如图4-59所示单击**解锁账户**按钮即可（账户被锁定后才会有此选项）。

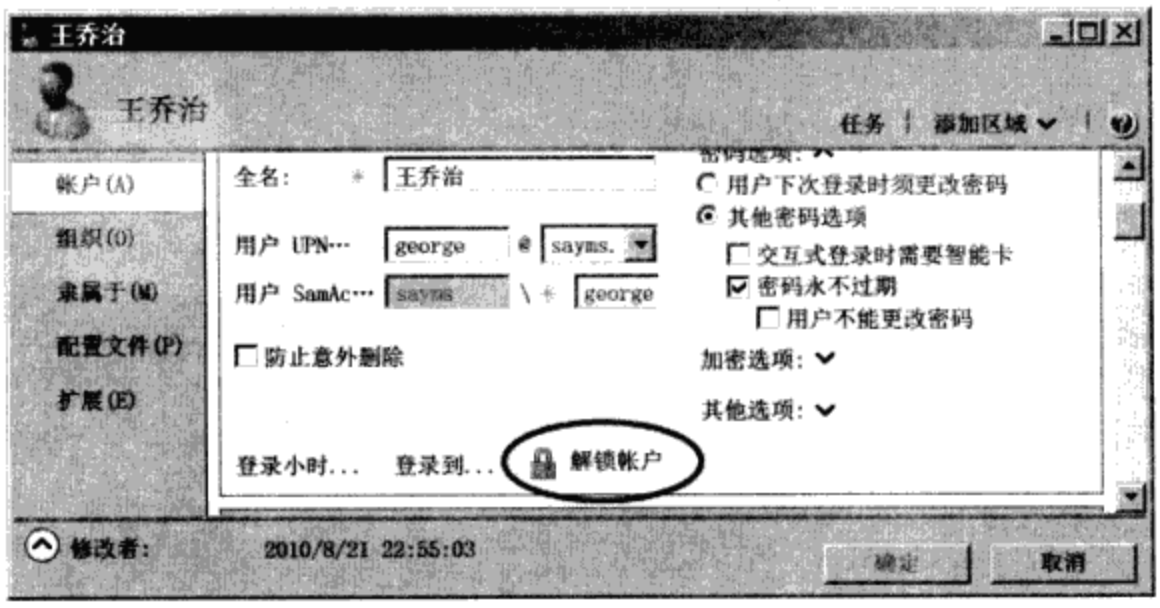


图4-59

（3）重置账户锁定计数器（Reset Account Lockout Counter After）

锁定计数器是用来记录用户登录失败的次数，其起始值为0，用户若登录失败，则锁定计数的值就会加1，若登录成功，则锁定计数器的值就会归零。若锁定计数器的值等于**账户锁定阈值**，该账户就会被锁定。

若用户连续两次登录失败之间的间隔时间超过此处设置值的话，锁定计数器值便会自动归零。以图 4-60为例，若用户连续3次登录失败的话，其账户就会被锁定。但在尚未连续3次登录失败之前，若前一次登录失败后到这一次失败之间的间隔时间已超过30分钟，则锁定计数器值就会从0开始计算，因此这次登录失败，仍然算是第1次。

Download at http://www.pin5i.com/

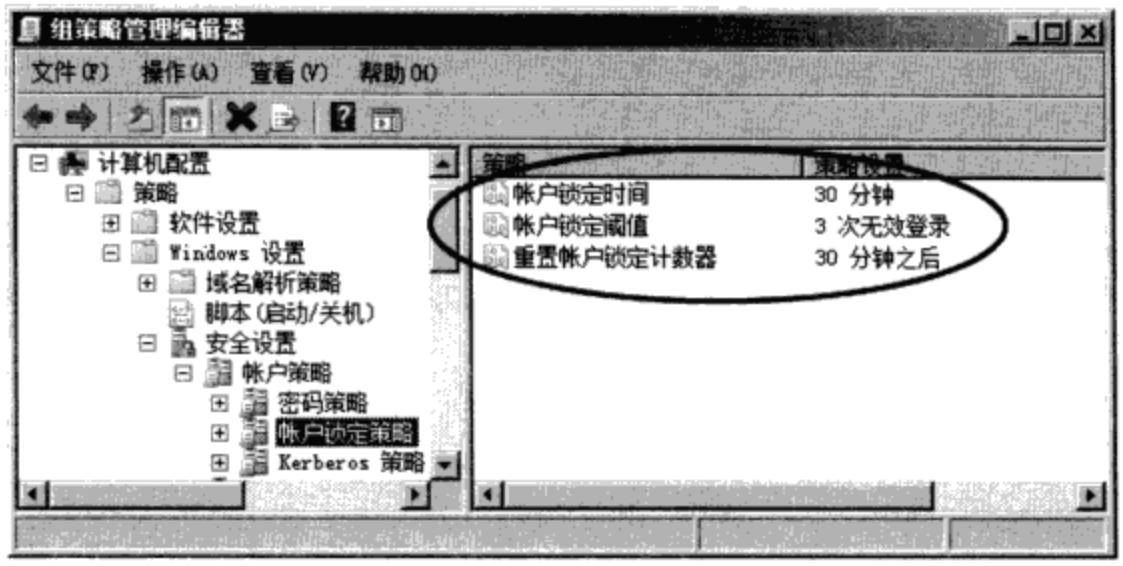


图4-60

4-5-4 用户权限分配策略

您可以通过图 4-61中的**用户权限分配**来将执行特殊操作的权限分配给用户或组（此图是以Default Domain Controllers Policy GPO为例）。

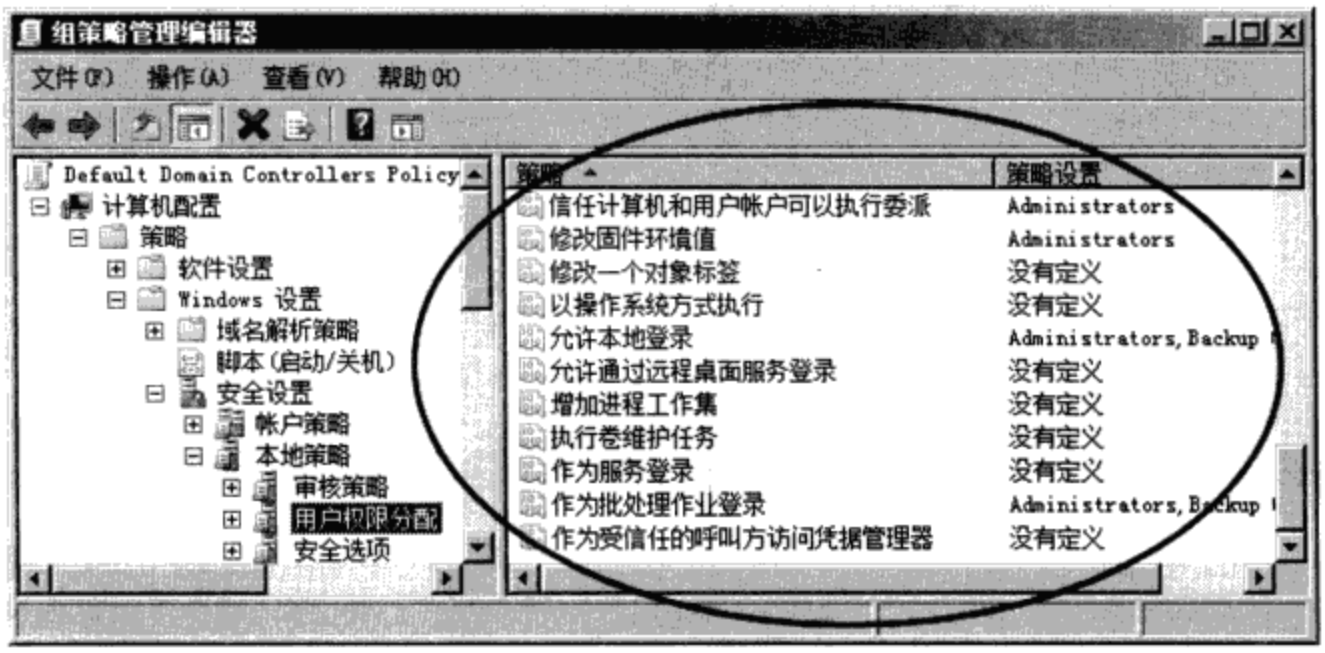


图4-61

要分配图 4-61右方的任何一个权限给用户时，请使用【双击该权限➲在图 4-62中单击添加用户或组按钮➲选择用户或组】的方法进行操作。

Download at http://www.pin5i.com/

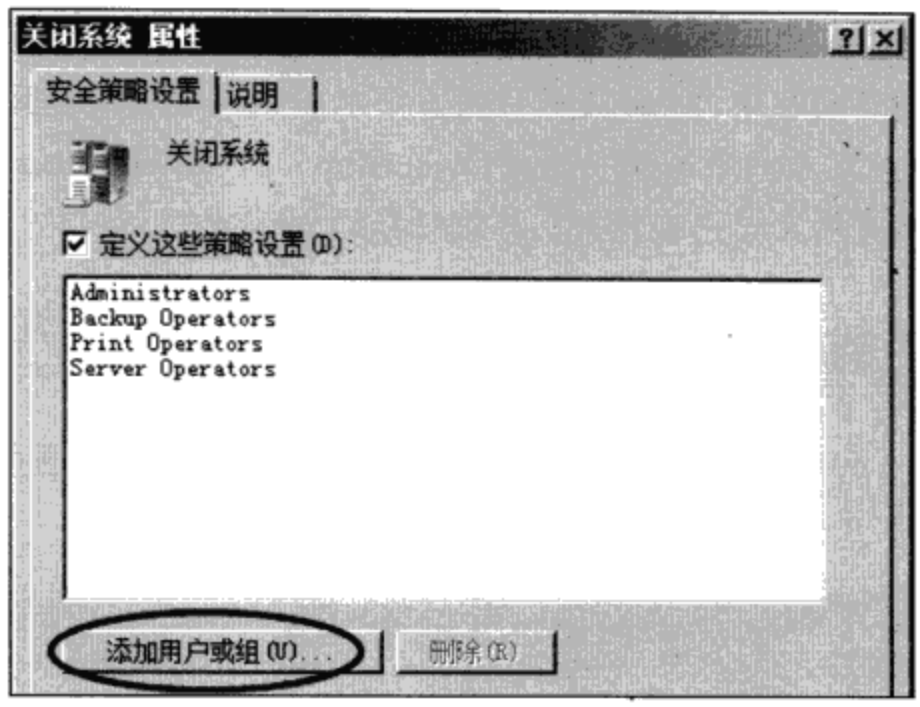


图 4-62

下面列举几个常用的权限策略进行说明。

- 允许本地登录（Allow Log On Locally）：允许用户直接在计算机上单击Ctrl + Alt + Del键登录。
- 拒绝本地登录（Deny Log On Locally）：拒绝用户直接在计算机上单击Ctrl + Alt + Del键登录。这个权限优先于**允许本地登录**的权限。
- 将工作站添加到域（Add Workstations To Domain）：允许用户将计算机加入到域。

提示

每一个域用户账户默认已经有10次将计算机加入域的机会，不过一旦拥有**将工作站添加到域**的权限后，其次数就没有限制。

- 关闭系统（Shutdown The System）：允许用户将此计算机关机。
- 从网络访问此计算机（Access This Computer From The Network）：允许用户通过网络上的其他计算机连接、访问此计算机内的资源。
- 拒绝从网络访问这台计算机（Deny Access This Computer From The Network）：拒绝用户通过网络上的其他计算机连接、访问此计算机内的资源。这个权限优先于**从网络访问此计算机**权限。
- 从远程系统强制关机（Force Shutdown From A Remote System）：允许用户从远程计算机来将这台计算机关机（可通过shutdown.exe程序）。
- 备份文件和目录（Backup Files And Directories）：允许用户备份硬盘内的文件和文件夹。
- 还原文件和目录（Restore Files And Directories）：允许用户还原所备份的文件和文件夹。
- 管理审核和安全记录（Manage Auditing And Security Log）：允许用户指定要审核的事件，也允许用户查询和清除安全记录。
- 更改系统时间（Change The System Time）：允许用户更改计算机的系统日期与时间。

Download at http://www.pin5i.com/

- 加载和卸载设备驱动程序（Load And Unload Device Drivers）：允许用户加载和卸载设备（设备）的驱动程序，也就是允许用户添加和删除硬设备的驱动程序。
- 取得文件或其他对象的所有权（Take Ownership Of Files Or Other Objects）：允许夺取其他用户所拥有的文件、文件夹或其他对象的所有权。

4-5-5 安全选项策略

您可以通过如图 4-63所示的**安全选项**来启用计算机的一些安全性设置。图中以**测试用的GPO**为例，并列举以下几个安全选项策略。

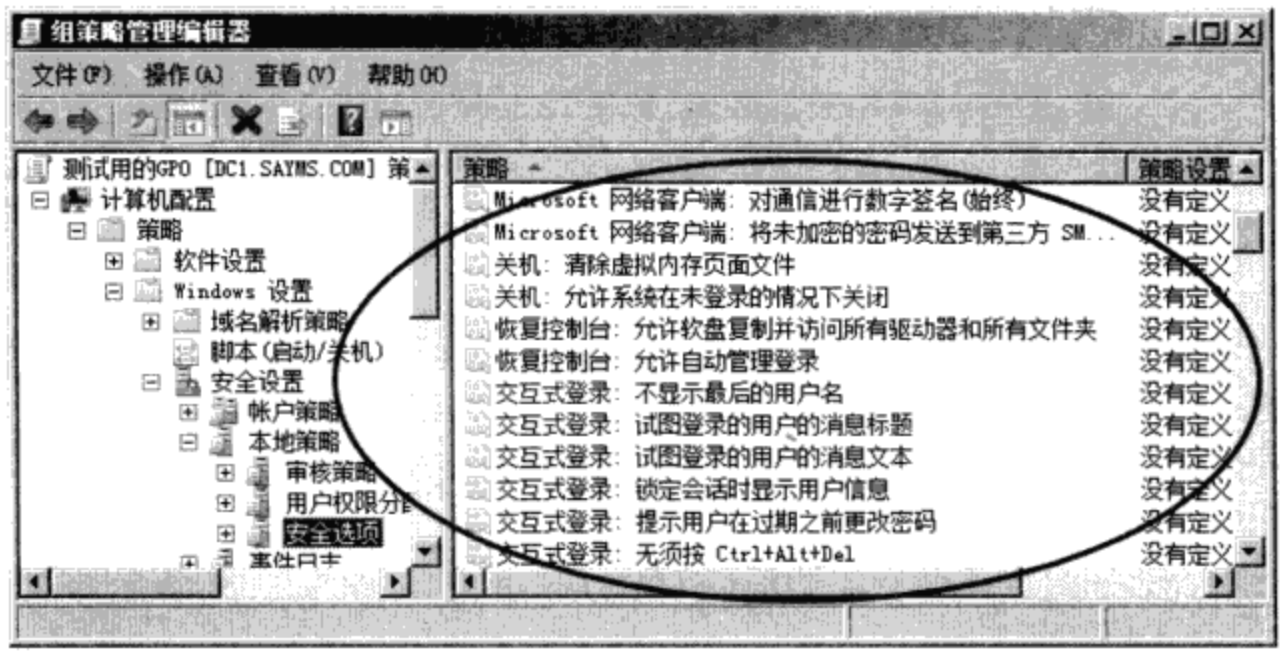


图4-63

- 交互式登录：无须按Ctrl + Alt + Del键。让登录界面不要再显示**按**Ctrl + Alt + Del**登录**窗口。
- 交互式登录：不要显示上次登录的用户名。每一次用户按Ctrl + Alt + Del键后都会自动显示上一次登录者的用户名，然而通过此选项可以让其不显示。
- 交互式登录：域控制器无法使用时，要缓存先前的登录次数。域用户登录成功后，其账户和密码会被存储到用户计算机的缓存区，若之后此计算机因故无法与域控制器连接的话，该用户还是可以通过缓存区的账户数据来验证其身份进行登录。您可以通过此策略来限制缓存区内账户数据的数量，默认为记录10个登录用户的账户数据。若此值为0，表示禁用此缓存功能；若此值超过50，则最多只会缓存50个账户信息。
- 交互式登录：在密码过期之前提示用户更改密码。用来设置在用户的密码过期之前几天，提示用户更改密码。
- 交互式登录：给出登录用户的信息本文、登录用户的信息标题。若用户在登录时按Ctrl + Alt + Del键后，界面上能够显示希望用户看到的信息的话，请通过这两个选项来设置，其中一个用来设置信息标题文字，另一个用来设置信息本文。
- 关机：允许不登录就将系统关机。让登录界面能够显示关机图标或按钮，以便在不需要登录的情况下就可以直接通过此图标或按钮将计算机关机。

Download at http://www.pin5i.com/

4-5-6 登录/注销、启动/关机脚本

您可以让域用户登录时，其系统就自动运行**登录脚本**（Script），而当用户注销时，就自动运行**注销脚本**；另外也可以让计算机在开机启动时自动运行**启动脚本**，而关机时自动运行**关机脚本**。

1. 登录/注销脚本的设置

以下使用文件名为**logon.vbs**的文件来练习登录脚本。您可以自行使用**记事本**（Notepad）来创建此文件，其内只有一行用来在屏幕上显示字符串的命令：

```
wscript.echo"您好！这是登录脚本测试"
```

同时也请创建文件名为**logoff.vbs**的文件来练习注销脚本，其内也只有一行用来在屏幕上显示字符串的命令：

```
wscript.echo"再见！这是注销脚本测试"
```

以下我们使用组织单位**业务部**的**测试用的GPO**来说明。

STEP 1 选择【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑】。

STEP 2 如图 4-64所示，通过【展开**用户配置**➲策略➲Windows设置➲脚本（登录/注销）➲双击右方的**登录**➲单击显示文件按钮】的方式进行操作。

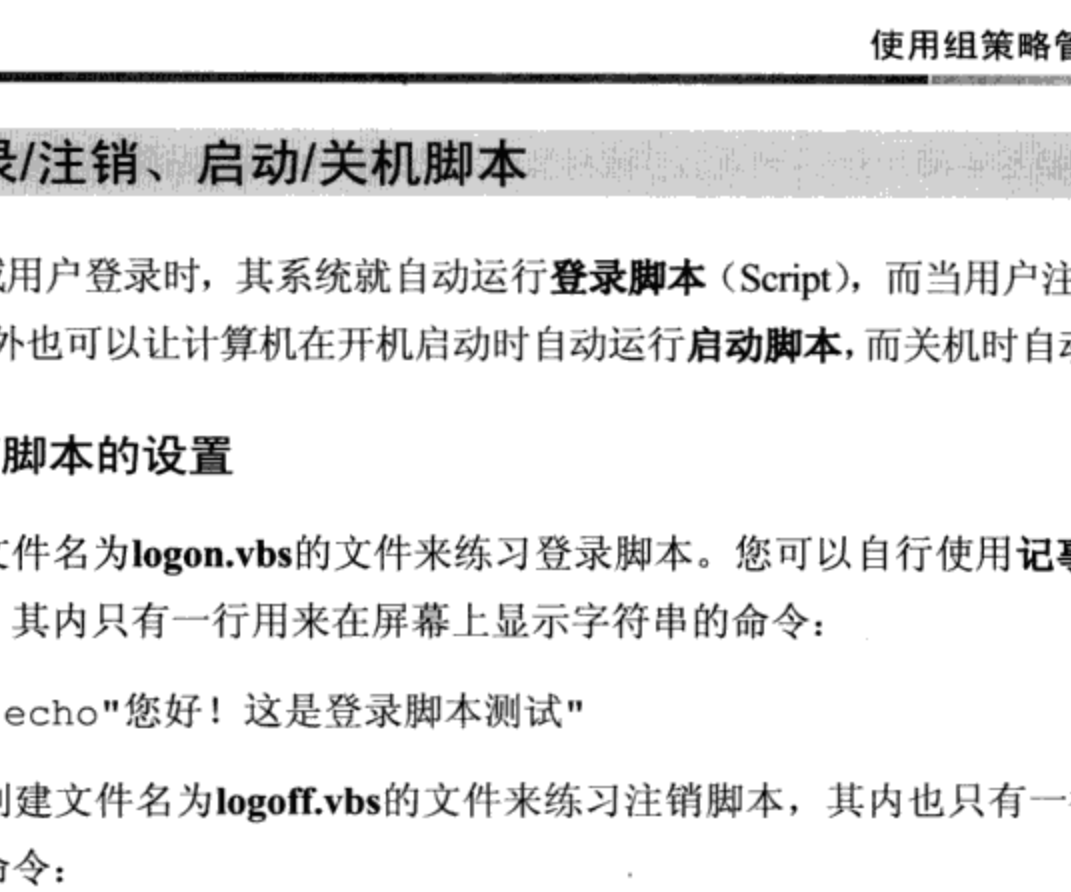


图 4-64

Download at http://www.pin5i.com/

STEP 3 出现如图4-65所示的界面时，请将登录脚本logon.vbs粘贴到界面中的文件夹内，此文件夹是位于域控制器的SYSVOL文件夹内，其完整路径为（其中的GUID是**测试用的GPO**的GUID）：

```
%systemroot%\SYSVOL\sysvol\域名\Policies\{GUID}\User\Scripts
\Logon
```

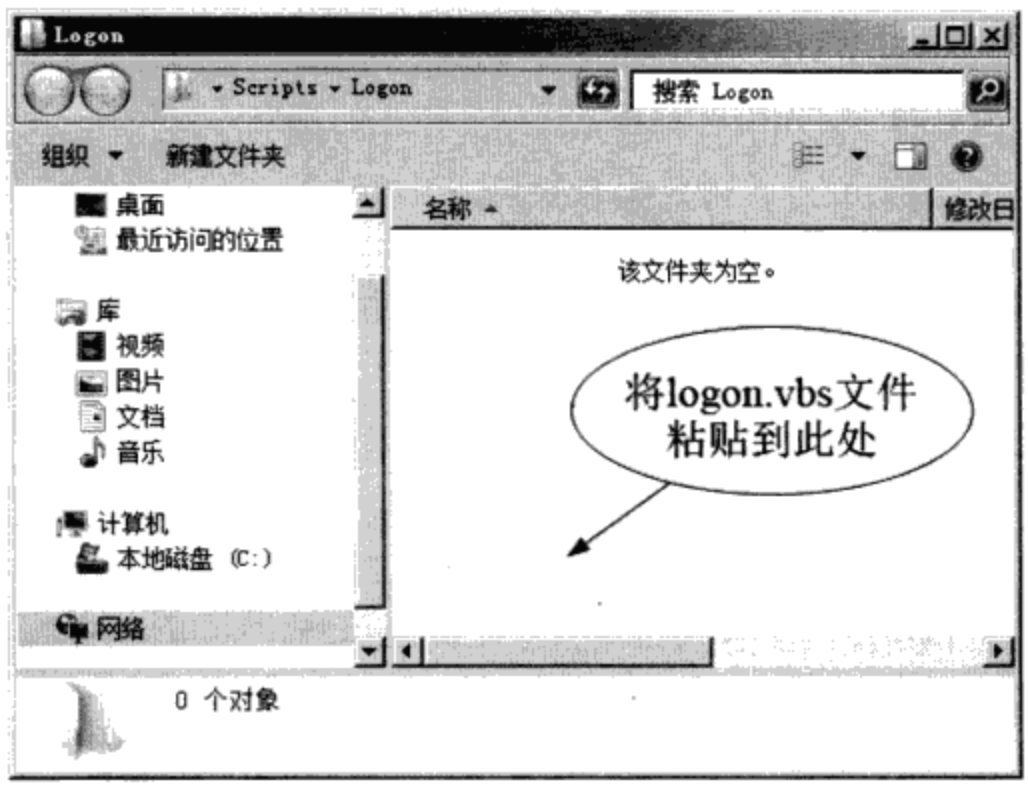


图4-65

STEP 4 请关闭图4-65，返回到图4-64，单击**添加**按钮。

STEP 5 在图4-66中通过**浏览**按钮来从图4-65的文件夹内选择登录脚本文件**logon.vbs**。完成后单击**确定**按钮。

提示

如果您所设计的脚本需要输入参数的话，请在**脚本参数**文本框中输入该参数，例如**//I**或**//Logo**等。

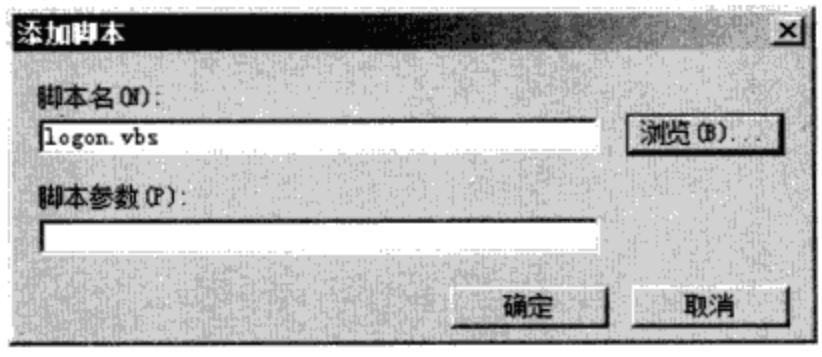


图4-66

STEP 6 返回到图4-64，单击**确定**按钮。

Download at http://www.pin5i.com/

STEP 7 双击图4-64右方的**注销**按钮，然后重复相同的步骤来设置**注销脚本 logoff.vbs**。

STEP 8 完成设置后，组织单位**业务部**内的所有用户登录与注销时，系统会分别自动运行登录脚本（**logon.vbs**）与注销脚本（**logoff.vbs**），也就是说组织单位**业务部**内的用户登录与注销时，屏幕上会分别出现如图 4-67所示的对话框。



图4-67

2. 启动/关机脚本的设置

以下将使用文件名为**startup.vbs**的文件来练习启动脚本，其内只有一行用来在屏幕上显示字符串的命令：

```
wscript.echo"您好！ 这是启动脚本测试"
```

同时也将使用文件名为**shutdown.vbs**的文件来练习关机脚本，其内也只有一行用来在屏幕上显示字符串的命令：

```
wscript.echo"再见！ 这是关机脚本测试"
```

我们将以图 4-68中组织单位**业务部**的**测试用的GPO**为例进行说明，而且要以图中计算机名称为Win7PC1的计算机来练习启动/关机脚本。如果您要练习的计算机不是位于组织单位**业务部**内，而是位于容器Computers内，则您需要通过域级别的GPO来练习（例如Default Domain Policy GPO），或是将计算机账户移动到组织单位**业务部**。



图4-68

Download at http://www.pin5i.com/

系统运行脚本的方式分为**同步**与**异步**两种模式，在您指定多个脚本时，这两种模式的运行有所不同。

- 同步模式：它会等前一个脚本运行完成后才运行下一个脚本。
- 异步模式：不等前一个脚本运行完成，就立即运行下一个脚本。

登录脚本、注销脚本与关机脚本默认都是采用**同步**方式，而启动脚本在Windows Vista以前的系统也是采用**同步**方式，不过从Windows Vista开始默认采用**异步**方式，这将使得我们所设计的启动脚本**startup.vbs**在Win7PC1计算机上运行时，无法将**您好！这是启动脚本测试**文字显示在屏幕上（见**异步执行启动脚本**策略内的说明），因而无法验证我们的实验是否成功，所以请先通过组策略来将其改为**同步**模式。由于我们的测试计算机Win7PC1是位于组织单位**业务部**内，因此请通过其内的**测试用的GPO**来设置：如图 4-69所示【展开**计算机配置**➲策略➲管理模板➲系统➲脚本➲将右方的**异步运行启动脚本**设置为**已禁用**】。

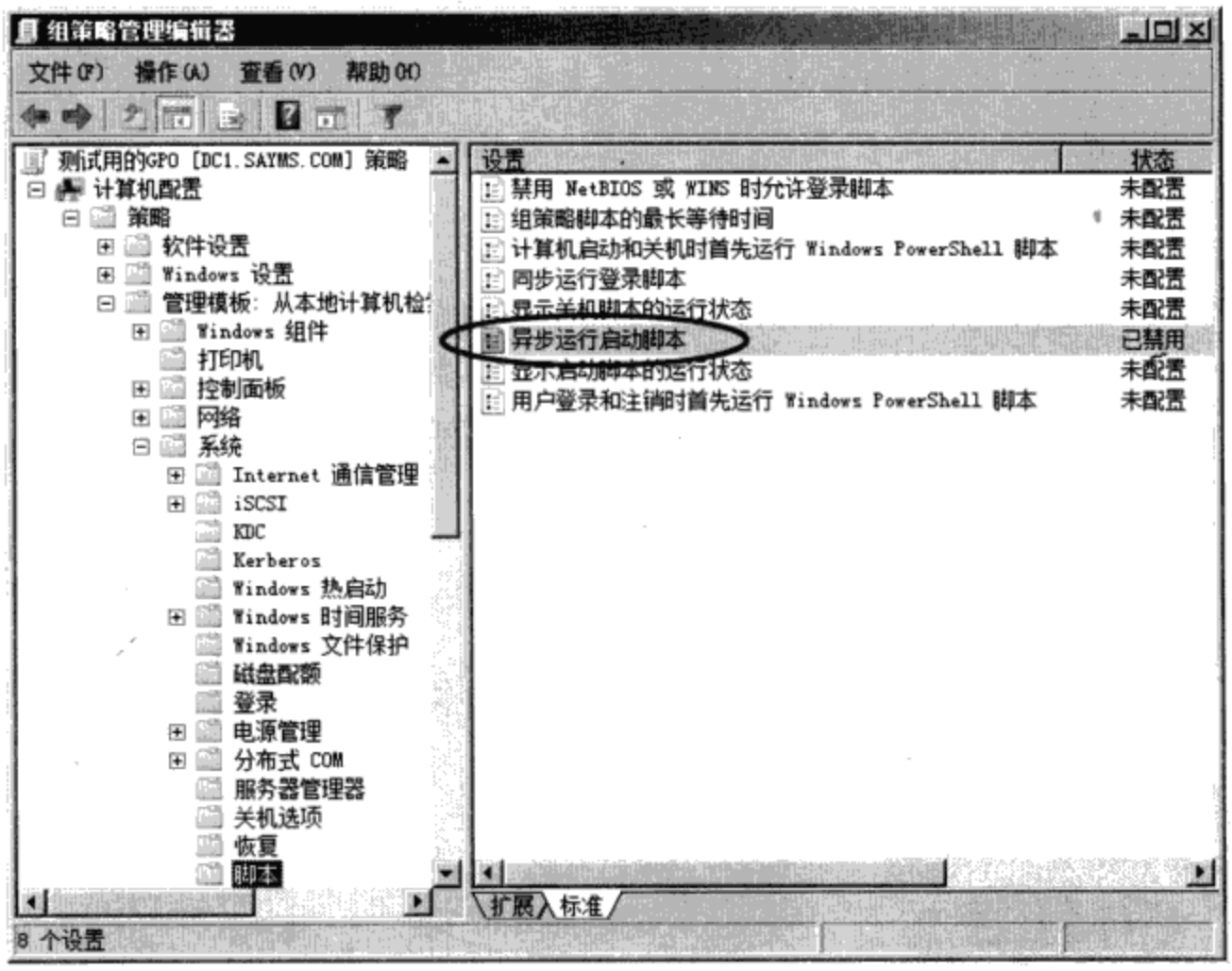


图 4-69

由于此部分的练习与登录/注销脚本几乎完全相同，故此处不再重复，不过您需要通过更改图 4-70中**计算机配置**处的**脚本（启动/关机）**来设置。

Download at http://www.pin5i.com/

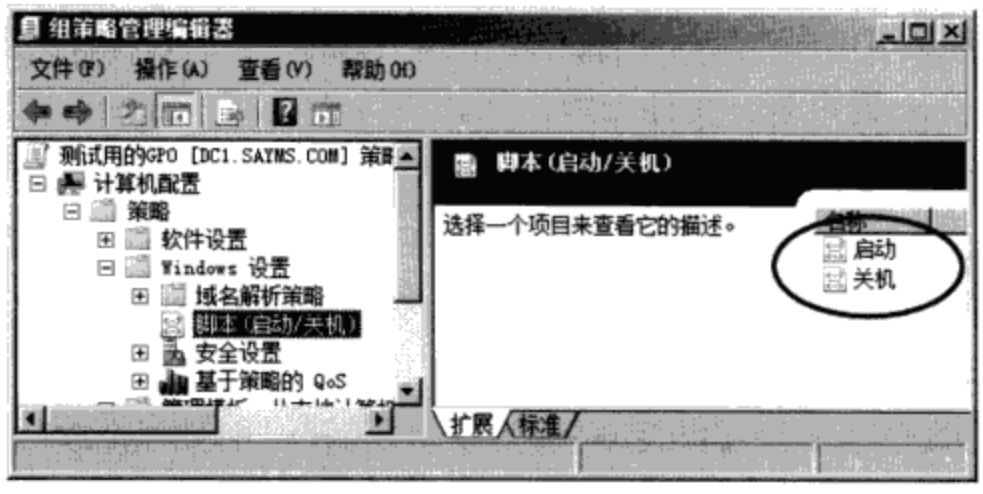


图4-70

完成后，组织单位**业务部**内的计算机Win7PC1重新启动与关机时，屏幕上会分别出现如图4-71所示的对话框。

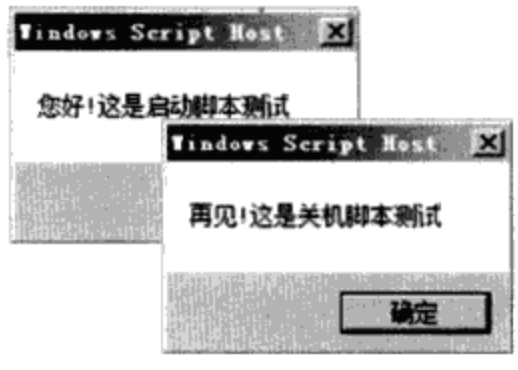


图4-71

4-5-7 文件夹重定向

您可以使用组策略来将用户的某些文件夹的存储位置，重定向到网络共享文件夹内，这些文件夹包含**我的文档**、**我的图片**、**我的音乐**等，如图 4-72所示，此图为用户**刘彼得**（peter）在Windows 7计算机上的个人文件夹，用户**刘彼得**可以通过【开始➲计算机➲单击**桌面**➲单击右方的**刘彼得**】的方式来取得此界面。



图4-72

Download at http://www.pin5i.com/

这些文件夹平常是存储在本地用户配置文件内，也就是**%SystemDrive%\用户\用户名**（或**%SystemDrive%\Users\用户名**）文件夹内，例如图 4-73为用户peter（此处显示其登录账户peter，不是其显示名称**刘彼得**）的本地用户配置文件的文件夹，因此用户换到另外一台计算机登录的话，就无法访问到这些文件夹，而如果能够将其存储地点改为（重定向到）网络共享文件夹的话，则用户到域内的任何一台计算机登录时，都可以通过此共享文件夹来访问这些文件夹内的文件。

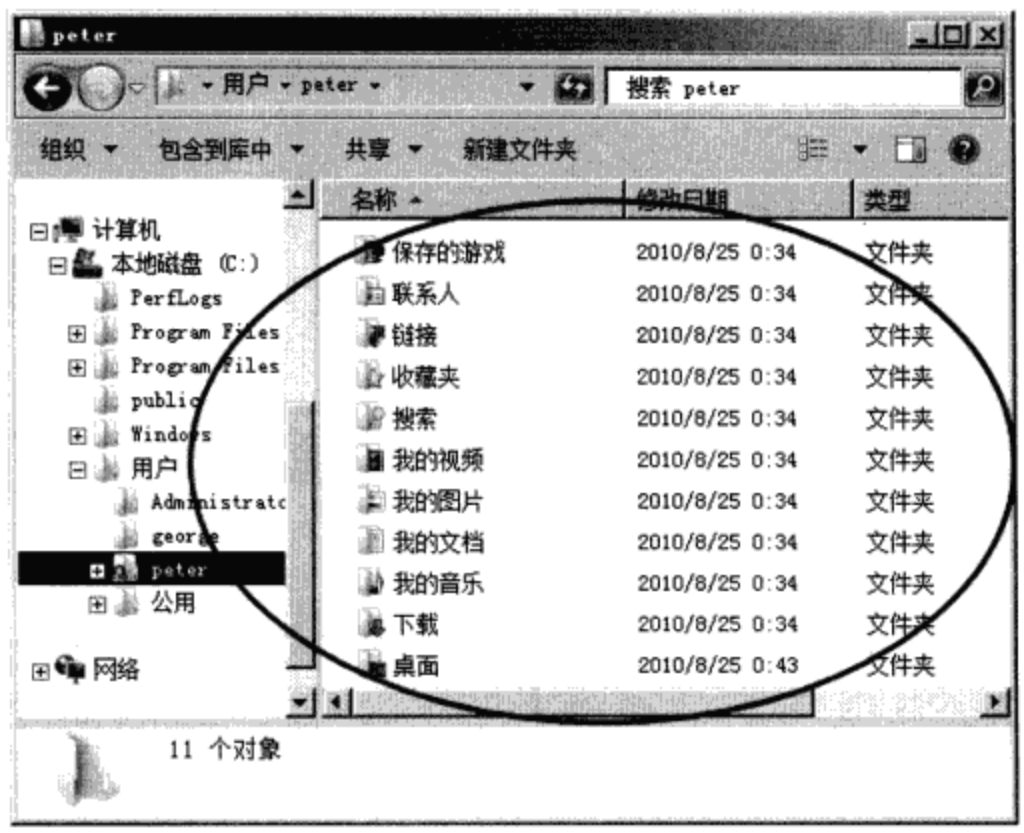


图4-73

1. 可以被定向的文件夹

表 4-1中列出了在Windows Server 2008 R2、Windows Server 2008、Windows 7、Windows Vista与旧版Windows 系统内可被定向的文件夹。

表 4-1

Windows Server 2008 R2 与Windows 7	Windows Server 2008 与Windows Vista	旧版Windows系统中对应的文件夹
AppData（Roaming）	AppData（Roaming）	Application Data
联系人	联系人	无
桌面	桌面	无
我的文档	文档	我的文档
下载	下载	无
收藏夹	收藏夹	无
链接	链接	无
我的音乐	音乐	无

Download at http://www.pin5i.com/

（续表）

Windows Server 2008 R2 与Windows 7	Windows Server 2008 与Windows Vista	旧版Windows系统中对应的文件夹
我的图片	图片	我的图片
保存的游戏	保存的游戏	无
搜索	搜索	无
开始菜单	**开始**菜单	**开始**菜单
我的视频	视频	无

2. 将我的文档重定向

用户**刘彼得**（peter）可以通过【对着图 4-72中的**我的文档**单击右键➲属性➲如图 4-74所示】的方法来获取**我的文档**当前是存储在本地用户配置文件文件夹C:\Users\Peter之下。

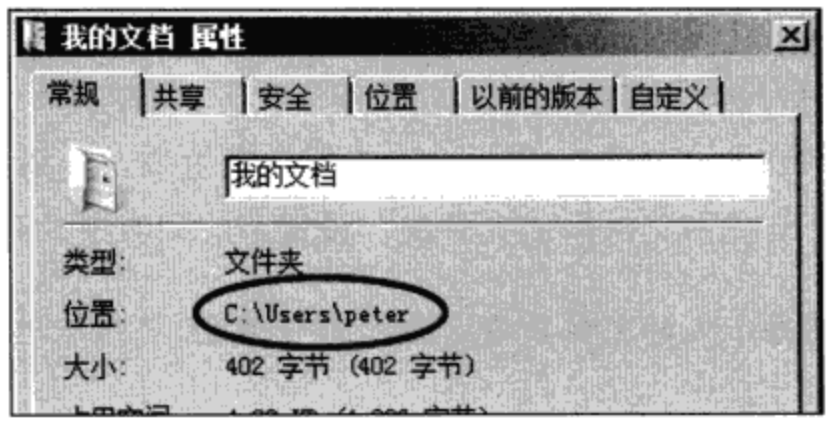


图4-74

我们使用将组织单位**业务部**内所有用户（包含peter）的**我的文档**文件夹重定向来说明如何将文件夹定向到另外一台计算机上的共享文件夹。

STEP 1 请到域内任何一台成员计算机上创建一个文件夹，例如我们将在服务器dc1上创建文件夹C:\DocStore，然后要将组织单位**业务部**内所有用户的**我的文档**文件夹定向到此文件夹内。

STEP 2 将此文件夹设置为**共享文件夹**，赋与Everyone**读取/写入**权限（系统会同时将**完全控制**的共享权限与NTFS权限赋予Everyone）。

> **提示**
>
> 其共享名默认为文件夹名称DocStore，建议将共享文件夹隐藏起来，也就是将共享名最后一个字符设置为：$，例如DocStore$。

STEP 3 请到域控制器上选择【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑】。

STEP 4 如图4-75所示，通过【展开**用户配置**➲策略➲Windows设置➲文件夹重定向➲对着**文档**单击右键➲属性】的方式进行操作。

Download at http://www.pin5i.com/

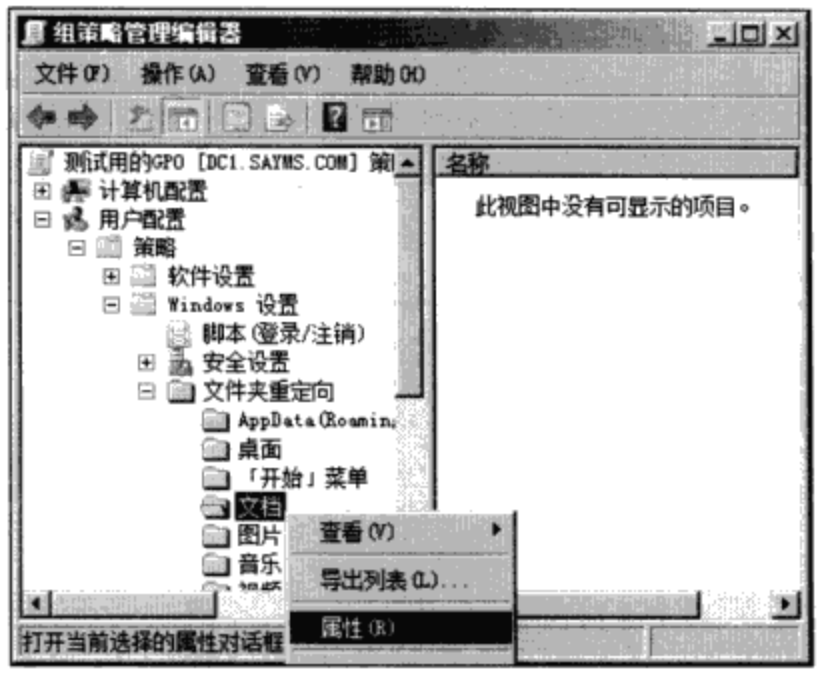


图4-75

STEP 5 参照图 4-76进行设置，完成后单击确定按钮。图中的**根路径**指向我们所创建的共享文件夹\\dc1\DocStore，系统会在此文件夹之下自动为每一位登录的用户分别创建一个专属文件夹，例如账户名为peter的用户登录后，系统会自动在\\dc1\DocStore之下，创建一个名称为peter的文件夹。**设置**下拉列表中共有以下几种选择。

- **基本－将每个人的文件夹重定向到同一位置**：将组织单位业务部内所有用户的文件夹都重定向。
- 高级－为不同的用户组指定位置：将组织单位业务部内隶属于指定组内的用户的文件夹重定向。
- 未配置：也就是不重定向。

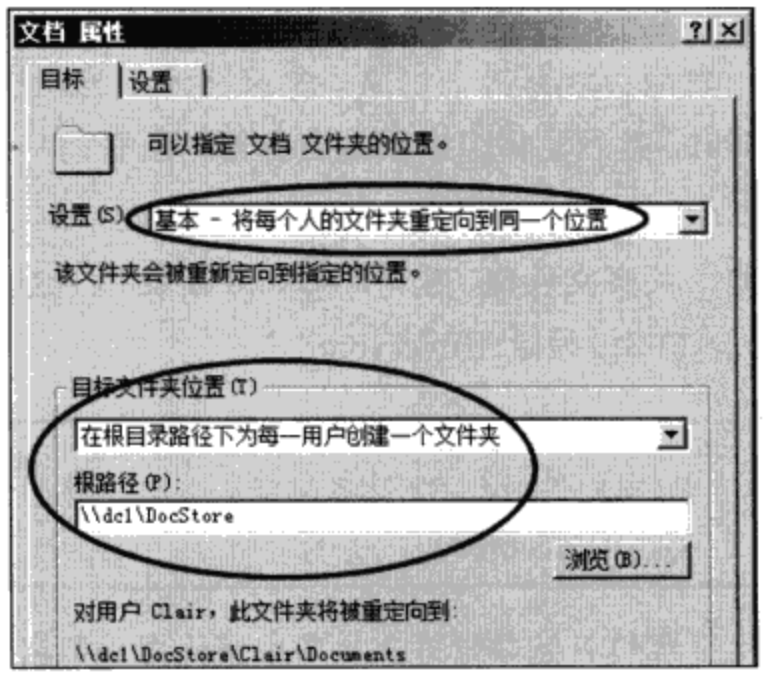


图4-76

另外图中的**目标文件夹位置**共有以下的选择：

Download at http://www.pin5i.com/

- 重定向到用户的主目录：若用户账户内有指定主目录的话，则此选择可将文件夹定向到其主目录。
- 在根目录路径下为每一用户创建一个文件夹：如前面所述，它让每一个用户各有一个专属的文件夹。
- 重定向到下列位置：将所有用户的文件夹定向到同一个文件夹。
- 重定向到本地用户配置文件位置：定向回原来的位置。

STEP 6 我们需另外设置才能够将定向策略应用到旧版Windows系统，但此时我们尚未配置，故会出现如图4-77所示的对话框，请直接单击**是（Y）**按钮继续（后面会介绍如何将定向策略应用到旧版Windows系统）。

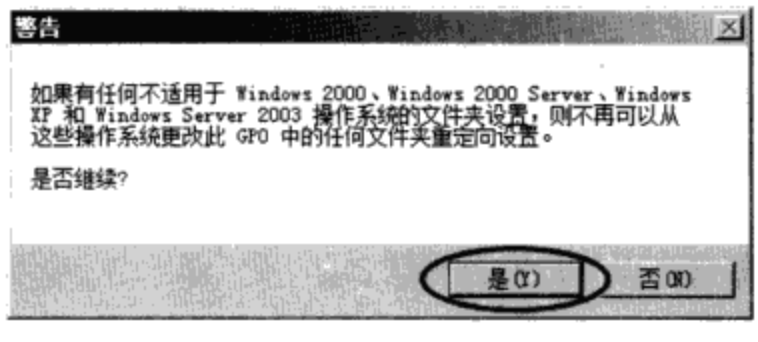


图4-77

STEP 7 请使用组织单位**业务部**内的任何一个用户账户到域成员计算机（当前需要至少是Windows Vista，以Windows 7为例）登录，例如peter（假设其显示名称为**刘彼得**），则peter的**我的文档**文件夹将被定向到\\dc1\DocStore\peter\documents 文件夹（也就是\\dc1\DocStore\peter**我的文档**文件夹）。您可以通过【开始➲单击**刘彼得**➲如图4-78所示对着**我的文档**单击右键➲属性】的方法来得知**我的文档**文件夹位于定向后的新位置\\dc1\DocStore\peter。

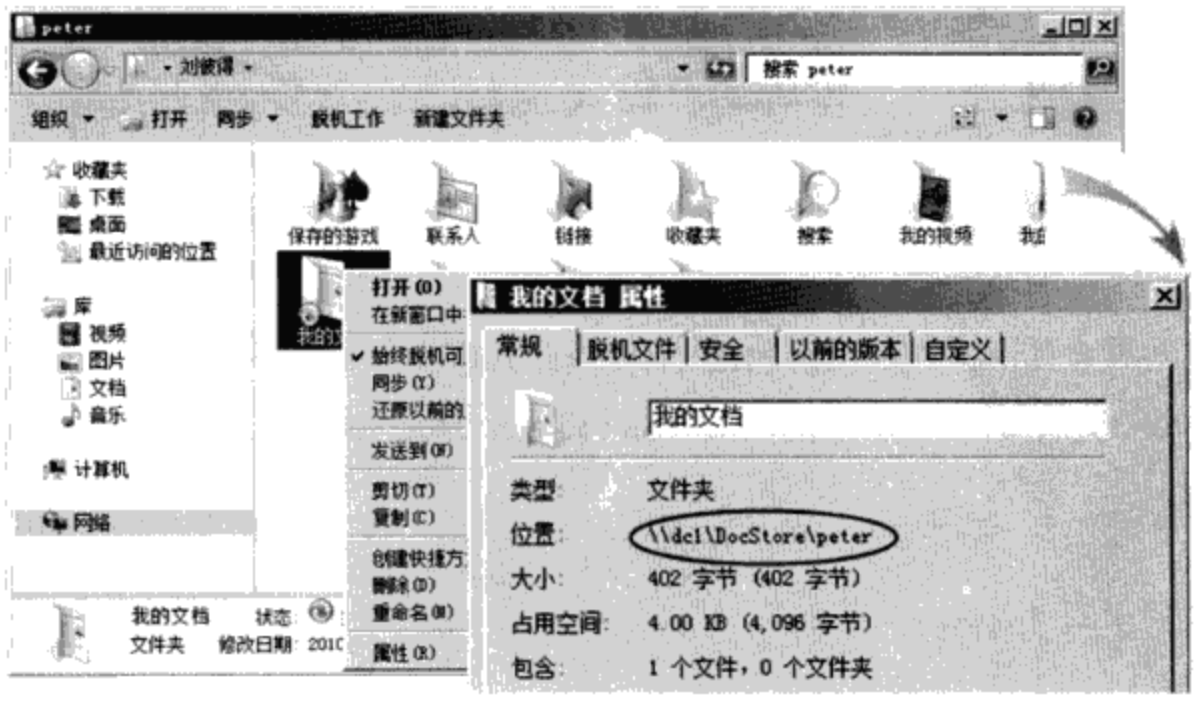


图4-78

Download at http://www.pin5i.com/

注意

用户可能需要登录两次后，文件夹才会被成功定向：为了让用户登录更快速，因此用户登录时，系统默认并不会等待网络启动完成后再通过域控制器来验证用户，而是直接读取本地缓存区内的账户数据来验证用户，让用户登录。之后等网络启动完成，系统就会自动在后台应用策略。不过因为**文件夹重定向**策略与**软件安装**策略必须在登录时才有作用，因此可能需要登录两次才有作用。若用户账户内有被指定使用漫游用户策略文件、主目录或登录脚本的话，则该用户登录时，系统会等网络启动完成才让用户登录。若用户第1次在此计算机登录的话，因缓存区内没有该用户的账户数据，故必须等网络启动完成，才可以取得最新的组策略设置值。通过组策略来更改客户端默认值的方法为：【计算机配置➲策略➲管理模板➲系统➲登录➲永远在计算机启动及登录时等待网络启动】。

由于用户的**我的文档**文件夹已经被重定向，因此用户原本位于本地用户配置文件内的**我的文档**文件夹将被删除，例如图 4-79中为用户peter的本地用户配置文件的内容，其内已经看不到**我的文档**文件夹。



图4-79

您可以到共享文件夹所在的服务器dc1上检查此共享文件夹之下，是否已经自动创建用户peter专属的文件夹，如图 4-80所示的C:\DocStore\Peter \Documents文件夹就是peter的**我的文档**的新存储位置。

Download at http://www.pin5i.com/

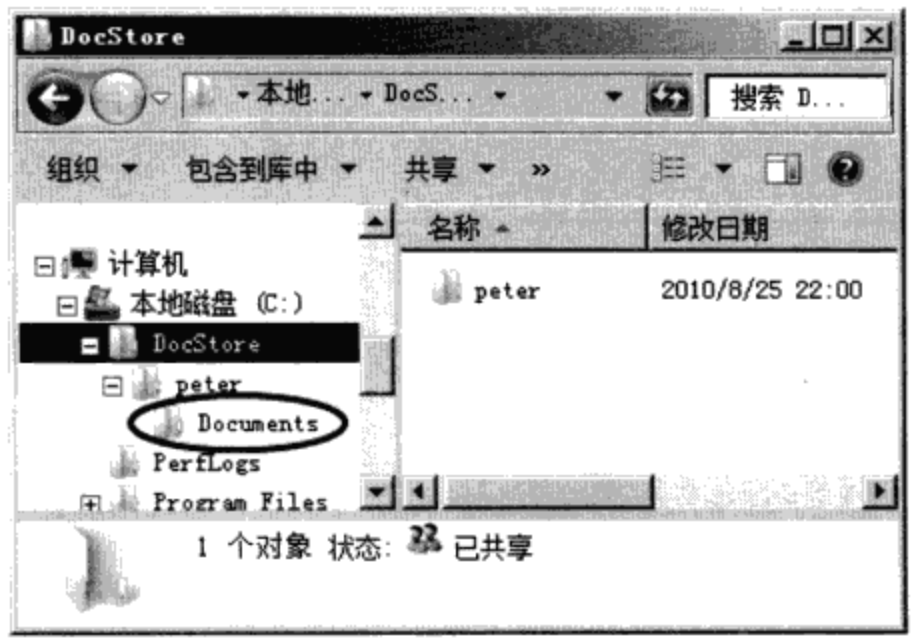


图 4-80

3. 文件夹重定向的好处

将用户的**我的文档**文件夹（或其他文件夹）重定向到网络共享文件夹后，便可以具备以下优点与特点：

- 用户到网络上任何一台计算机登录域时，都可以访问到此文件夹。
- 使用漫游用户配置文件的用户，其**我的文档**文件夹被重定向后，在漫游用户配置文件文件夹内就不会存储**我的文档**，所以用户登录、读取漫游用户策略文件时，或注销、存储漫游用户策略文件时，因为不需要加载、存储**我的文档**，故用户登录、注销的效率较好。
- **我的文档**文件夹被重定向到服务器网络共享文件夹后，其内的文件可通过信息部门的服务器定期备份工作来让用户的文件多了一份保障。
- **我的文档**文件夹被重定向到服务器的网络共享文件夹后，系统管理员可通过**磁盘配额**设置来限制用户的**我的文档**在服务器内可使用的磁盘空间。
- **我的文档**文件夹默认是与操作系统在同一个磁盘内，在将其重定向到其他磁盘后，即使操作系统磁盘被格式化、重新安装，也不会影响到**我的文档**内的文件。

4. 文件夹重定向的其他设置

您可通过图 4-81中的**设置**标签来设置以下选项（以**我的文档**文件夹为例）：

- 授予用户对文档的独占权限：只有用户自己与系统对重定向后的新文件夹具备完全控制的权限，其他用户都无任何权限，系统管理员也没有权限。若未选择此选项，则会继承其父文件夹的权限。
- 将文档的内容移到新位置：它会将原文件夹内的文件移动到重定向后的新文件夹内。若未选择此选项，则文件夹虽然会被重定向，但是原文件夹内的文件仍然会被留在原地。

Download at http://www.pin5i.com/

提示

如果您取消选择此选项的话，则用户原本位于本地用户配置文件内的**我的文档**文件夹会被保留。

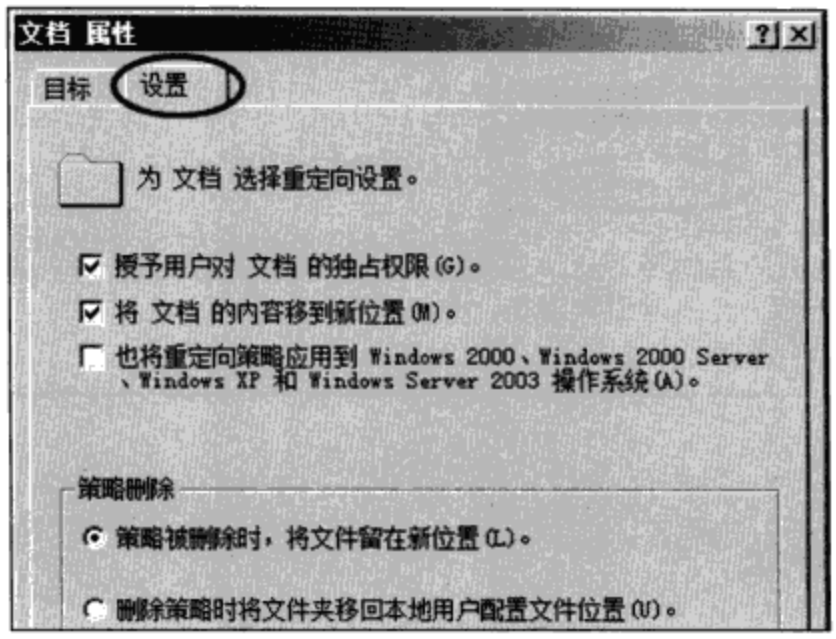


图4-81

- 也将重定向策略应用到Windows 2000、Windows 200 Server、Windows XP及Windows Server 2003操作系统：重定向策略默认只会被应用到Windows Server 2008 R2、Windows Server 2008、Windows 7与Windows Vista，但选择此选项后，就可以将策略应用到Windows 2000等旧系统。
- 策略删除：用来设置当组策略删除后（例如GPO被删除或禁用），是否要将文件夹定向回原来的位置，默认是不会，也就是仍然留在新文件夹。

4-6 使用组策略来限制访问可移动存储设备

系统管理员可以使用组策略来限制用户访问**可移动存储设备**（Removable Storage Device，例如USB移动硬盘），以免企业内部员工轻易地通过这些存储设备将重要数据带离公司。

以组织单位来说，若您是针对**计算机配置**来设置这些策略的话，则任何域用户只要在这个组织单位内的计算机登录，就会受到限制；若您是针对**用户配置**来设置这些策略的话，则所有位于此组织单位内的用户到域内任意一台计算机登录时，就会受到限制。

注意

这些策略设置仅对使用Windows Vista、Windows 7、Windows Server 2008 与Windows Server 2008 R2等新版操作系统的计算机有效。

系统提供了如图 4-82所示的策略设置（图中以**用户配置**为例）。

Download at http://www.pin5i.com/

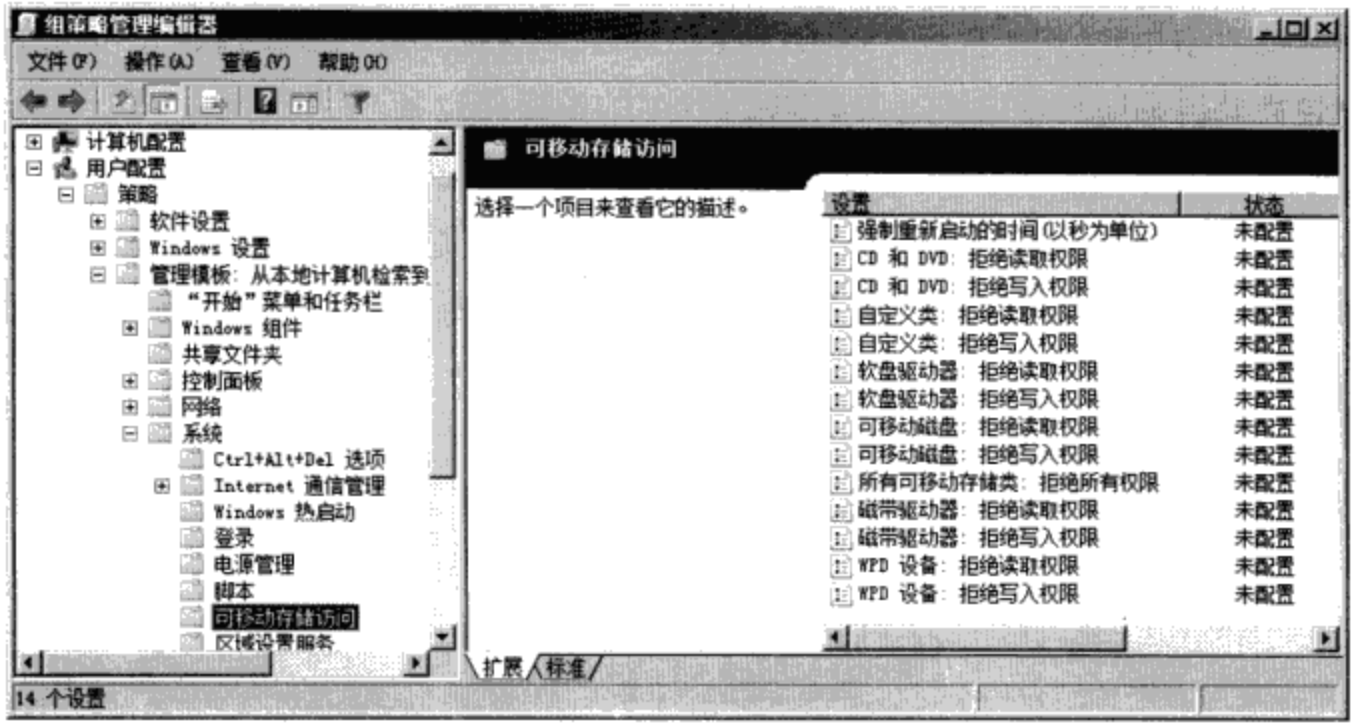


图 4-82

1. 强制重新启动的时间（以秒为单位）

有些策略设置必须重新启动计算机才会应用，而若您如图 4-83所示启用这个**强制重新启动的时间（以秒为单位）**策略的话，则系统就会在图中指定的时间到达时自动重新启动计算机。

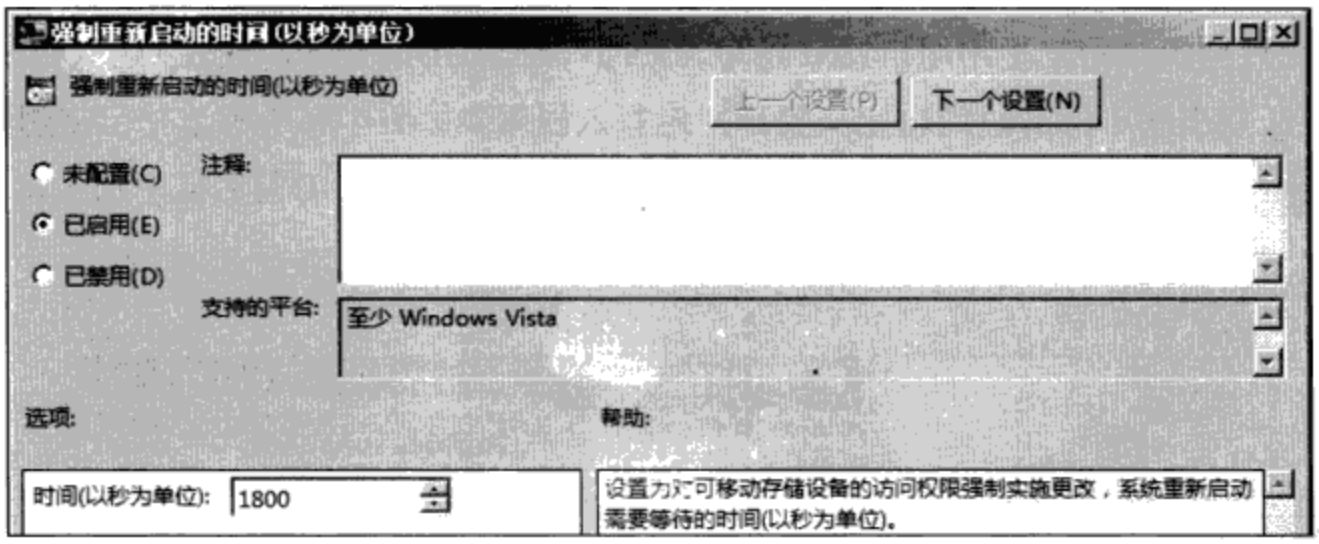


图 4-83

4. CD 和 DVD：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入隶属于CD和DVD类别的设备，包含通过USB连接的设备。

5. 自定义类：拒绝读取权限、拒绝写入权限

属于同一类型的设备会拥有相同的**设备安装类**（Device Setup Class），例如所有的CD光驱都是隶属于**CD-ROM设备安装类**，它们都是采用相同的安装和设置方式。**设备安装类**代码是

Download at http://www.pin5i.com/

采用32个字符的GUID格式（也就是xxxxxxxx-xxxx-xxxx-xxxx- xxxxxxxxxxxx），因此您可以通过**设备安装类**来拒绝用户读取或写入到拥有此GUID的存储设备。

您可通过**设备管理器**来查询设备的GIUD，以Windows 7内的光驱为例：【开始➲对着**计算机**单击右键➲管理➲如图 4-84所示单击**设备管理器**➲展开右边的**DVD/CD-ROM驱动器**➲双击光驱设备➲在弹出的对话框中单击**详细信息**标签➲在**属性**列表中选择**设备类 GUID**➲从**值**文本框可知其GUID】。

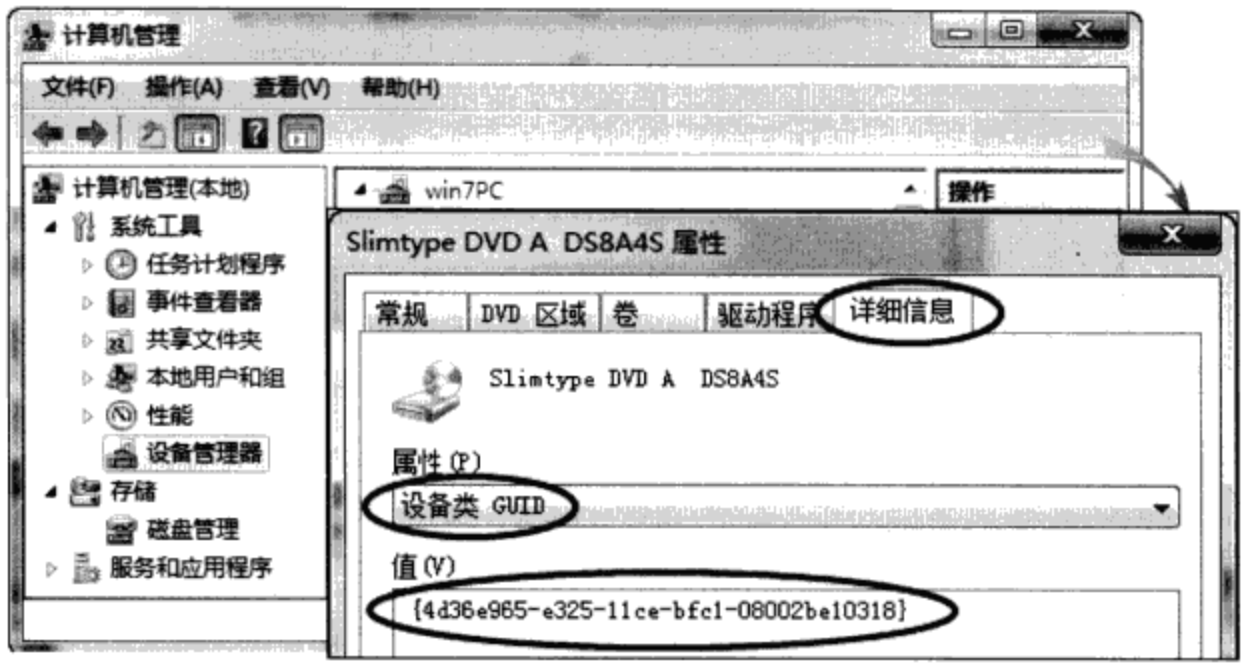


图 4-84

接下来使用组策略来拒绝用户读取或写入到拥有此GUID的设备，假设要拒绝用户写入此存储设备：【双击图 4-85右边的**自定义类：拒绝写入权限**➲如图 4-86所示选择**已启用**单选按钮➲单击显示按钮➲输入此设备的GUID后单击确定按钮】，注意GUID前后需附加大括号{}。

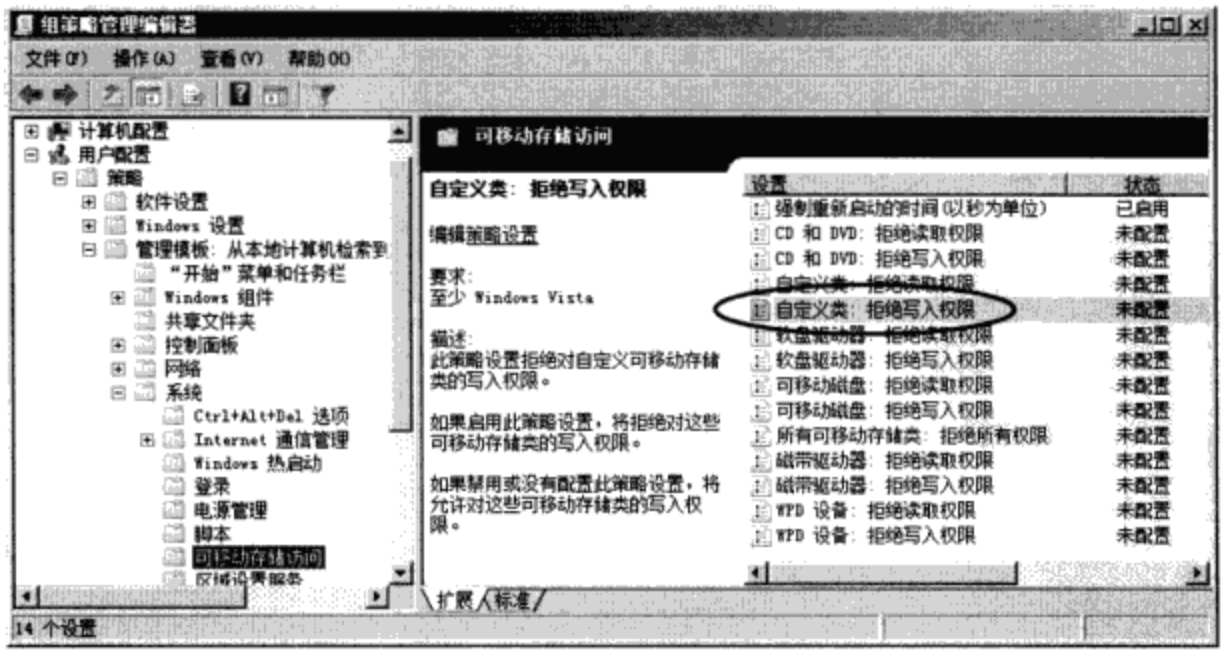


图 4-85

Download at http://www.pin5i.com/

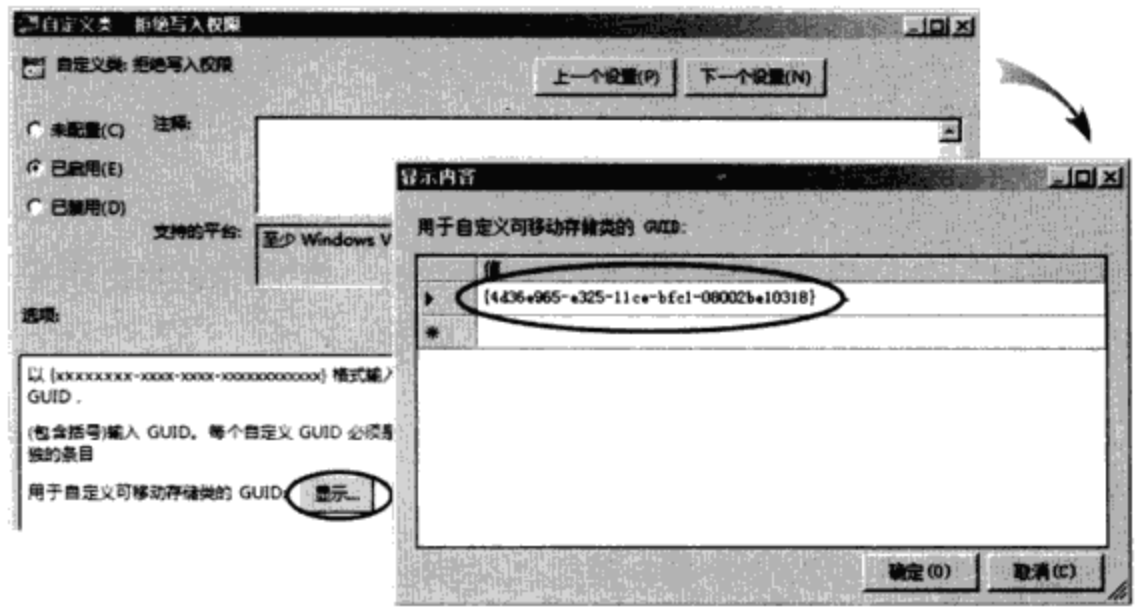


图4-86

5. 软盘驱动器：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入隶属于软盘驱动器类的设备，包含通过USB连接的设备。

6. 可移动磁盘：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入隶属于可移动磁盘类的设备，例如USB移动硬盘或外接式USB硬盘驱动器。

7. 所有可移动存储类：拒绝所有权限

拒绝用户访问所有的可移动存储设备，此策略设置的优先权高于其他策略，因此若您启用此策略的话，则不论其他策略设置为何，都会拒绝用户读取与写入到可移动存储设备。如果您已禁用或未配置此策略的话，则用户是否可以读取或写入到可移动存储设备，由其他策略的设置来决定。

8. 磁带驱动器：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入隶属于磁带驱动器类的设备，包含通过USB连接的设备。

9. WPD 设备：拒绝读取权限、拒绝写入权限

拒绝用户读取或写入隶属于WPD（Windows Portable Device）的设备，例如移动电话、媒体播放器、Windows CE等设备。

Download at http://www.pin5i.com/

4-7 WMI筛选器

若将GPO链接到组织单位后，则该GPO的设置值默认会被应用到此组织单位内的所有用户与计算机，如果要改变这个默认值的话，可以有以下两种选择：

- 通过**过滤组策略设置**中的**委派**标签来选择要应用此GPO的用户和计算机。
- 通过本节所介绍的**WMI筛选器**来设置。

举例来说，假设您已经在组织单位**业务部**内创建**测试用的GPO**，并通过它来让此组织单位内的计算机自动安装您所指定的软件（后面章节会介绍），不过您却只想让Windows 7计算机安装此软件，其他操作系统的计算机并不需要安装，此时可以通过以下的**WMI筛选器**设置来进行操作。

STEP 1 如图 4-87所示，通过【对着**WMI筛选器**单击右键➲新建】的方式进行操作。



图4-87

STEP 2 在图 4-88中的**名称**和**描述**文本框中分别输入适当的文字说明后单击添加按钮。图中将名称设置为**Windows 7专用的筛选器**。

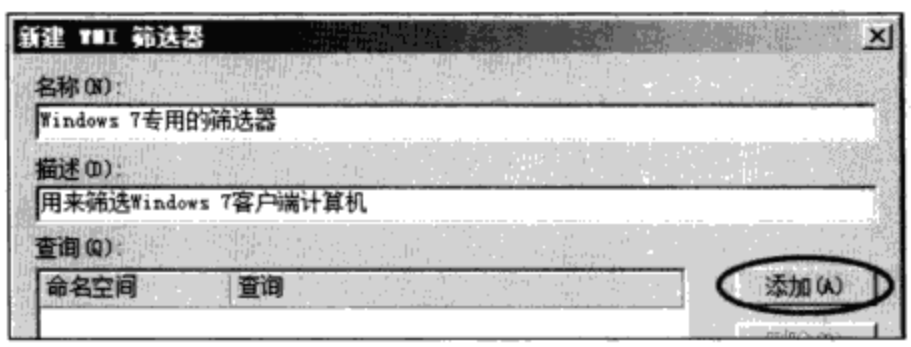


图4-88

STEP 3 在图 4-89中的**命名空间**文本框中选择默认的**root/CIMv2**，然后在**查询**文本框输入

Download at http://www.pin5i.com/

以下的查询命令（后述）后单击确定按钮：

```
Select * from Win32_OperatingSystem where Version like "6.1%"
and ProductType = "1"
```

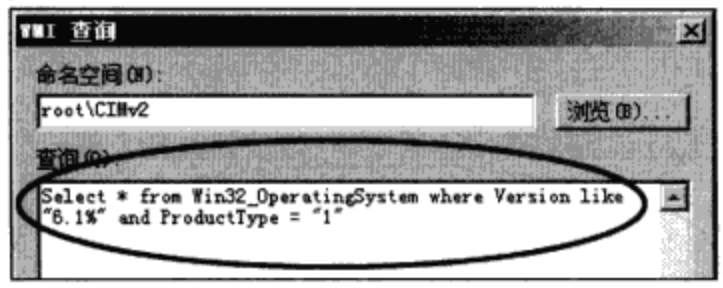


图 4-89

STEP 4 在图 4-90中单击保存按钮。

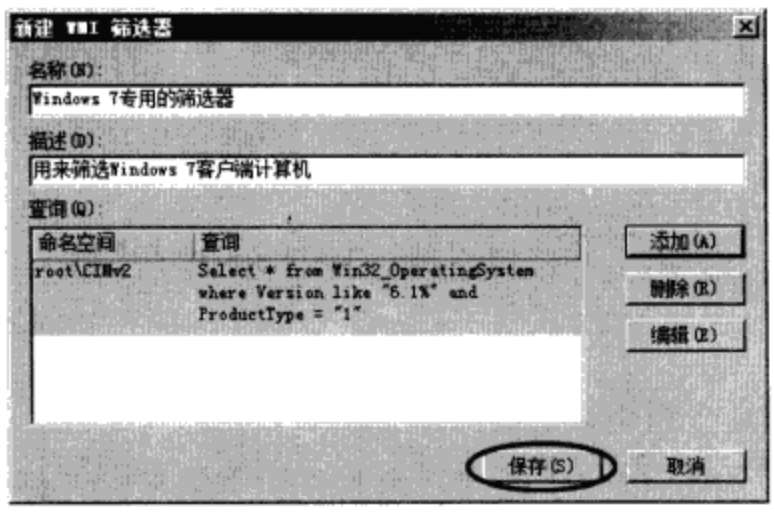


图 4-90

STEP 5 在图 4-91中**测试用的GPO**右下方的**WMI筛选**处选择刚才所创建的**Windows 7专用的筛选器**即可。

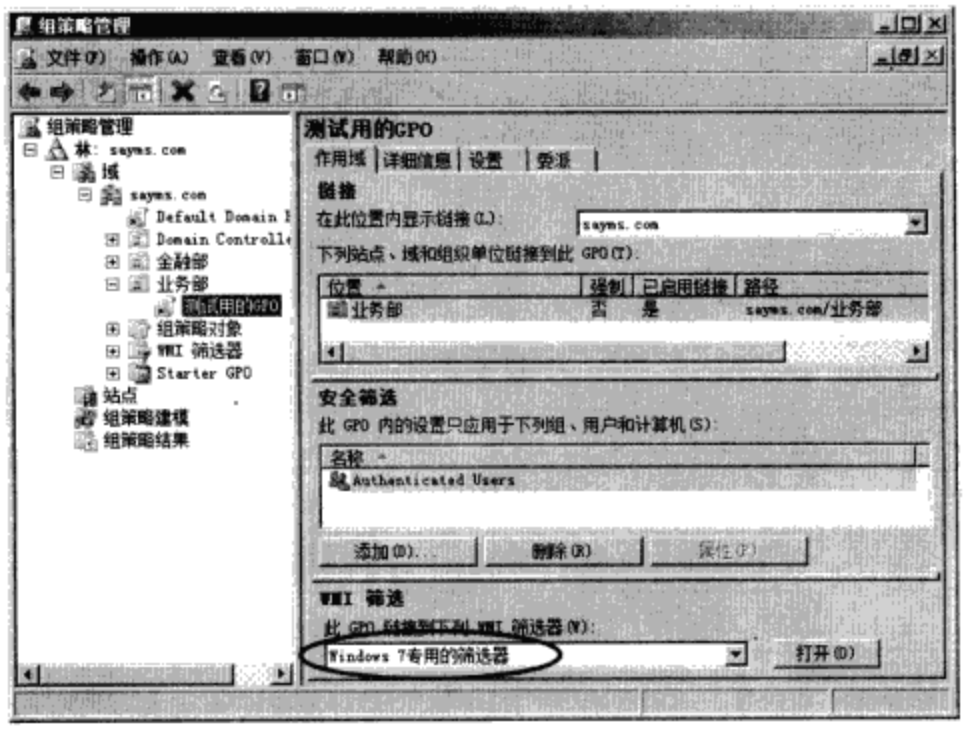


图 4-91

Download at http://www.pin5i.com/

组织单位**业务部**内所有的Windows 7客户端都会应用**测试用的GPO**策略设置，但是其他Windows系统并不会应用此策略。您可以到客户端计算机上通过运行**gpresult /r**命令来查看应用了哪些GPO，如图 4-92所示为在一台位于**业务部**内的Windows Server 2008 R2客户端上使用**gpresult /r**命令所查看到的结果，因为**测试用的GPO**搭配了**Windows 7专用的筛选器**，故Windows Server 2008 R2计算机不会应用此策略（被WMI筛选器拒绝）。

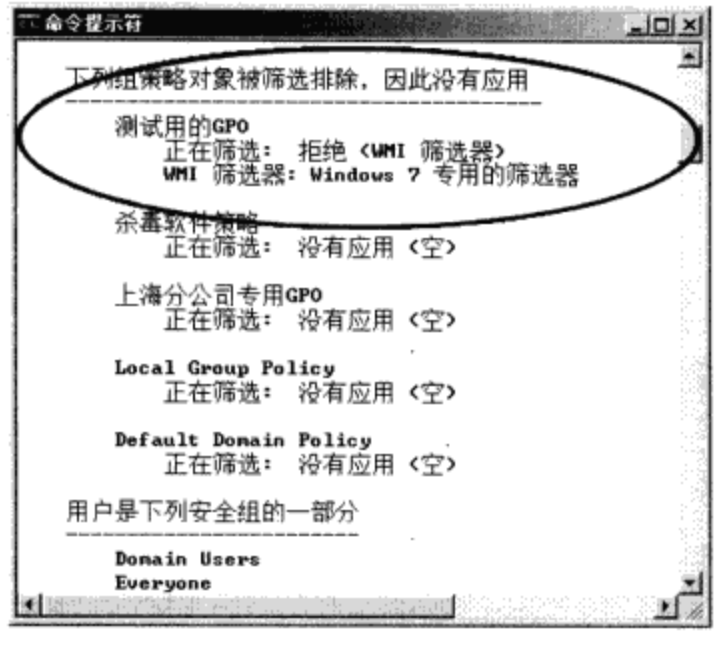


图 4-92

图 4-89中的**命名空间**是一组用来管理环境的类（Class）和实例（Instance）的集合，系统内包含着各种不同的命名空间，以便于通过其内的类和实例来管理各种不同的环境，例如命名空间**CIMv2**内所包含的是与Windows环境有关的类和实例。

图 4-89中的**查询**字段内需要输入WMI 查询语言（WQL）来执行过滤操作，其中的**Version like**后面的数字所代表的意义如表 4-2所示。

表 4-2

操作系统 / 版本	Windows Server 2008 R2与Windows 7	Windows Server 2008与Windows Vista	Windows Server 2003	Windows XP	Windows 2000
Version	6.1	6.0	5.2	5.1	5.0

而ProductType右边的数字所代表的意义如表 4-3所示。

表 4-3

ProductType	所代表的意义
1	客户端级别的操作系统，例如Windows 7、Windows Vista
2	服务器级别的操作系统，且是域控制器
3	服务器级别的操作系统，但不是域控制器

综合以上两个表格的说明后，下面列举几个可以用来过滤客户端的WQL命令，如表 4-4所示。

Download at http://www.pin5i.com/

表 4-4

要过滤的客户端	可用的WQL命令
Windows 7	select * from Win32_OperatingSystem where Version like "6.1%" and ProductType="1"
Windows Server 2008 R2成员服务器	select * from Win32_OperatingSystem where Version like "6.1%" and ProductType="3"
Windows 7与Windows Server 2008 R2	select * from Win32_OperatingSystem where Version like "6.1%"
Windows Server 2008 R2域控制器	select * from Win32_OperatingSystem where Version like "6.1%" and ProductType="2"
Windows Vista	select * from Win32_OperatingSystem where Version like "6.0%" and ProductType="1"
Windows Server 2008成员服务器	select * from Win32_OperatingSystem where Version like "6.0%" and ProductType="3"
Windows Vista 与 Windows Server 2008成员服务器	select * from Win32_OperatingSystem where Version like "6.0%" and ProductType<>"2"
Windows Server 2003成员服务器	select * from Win32_OperatingSystem where Version like "5.2%" and ProductType="3"
Windows Server 2003 与 Windows Server 2008成员服务器	select * from Win32_OperatingSystem where (Version like "5.2%" or Version like "6.0%") and ProductType="3"
Windows 7、Windows Vista、Windows Server 2008 R2 与 Windows Server 2008 （成员服务器）	select * from Win32_OperatingSystem where Version like "6.%" and ProductType<>"2"
Windows XP	select * from Win32_OperatingSystem where Version like "5.1%"
Windows XP Service Pack 3	select * from Win32_OperatingSystem where Version like "5.1%" and ServicePackMajorVersion=3
Windows XP Service Pack 2（含）以上	select * from Win32_OperatingSystem where Version like "5.1%" and ServicePackMajorVersion>=2

4-8 组策略建模与组策略结果

您可以通过**组策略建模**（Group Policy Modeling）来针对用户或计算机模拟可能的状况，例如某用户账户当前是位于甲组织单位内，某计算机账户当前是位于乙容器内，而我们想要知道将来若该用户或计算机账户被移动到其他容器时，该用户到此计算机上登录后，其用户或计算机策略的设置值。另外在当前现有的环境之下，若想要知道用户在某台计算机登录之后，其用户与计算机策略设置值的话，可通过**组策略结果**（Group Policy Result）来提供这些信息。

1. 组策略建模

我们将使用图 4-93中的环境来练习**组策略建模**。图中用户账户**刘彼得**（peter）与计算机

Download at http://www.pin5i.com/

账户WIN7PC1当前都是位于组织单位**业务部**内，而如果将来用户账户**刘彼得**（peter）与计算机账户WIN7PC1都被移动到组织单位**金融部**，这个时候若用户**刘彼得**（peter）到计算机WIN7PC1上登录的话，其用户与计算机策略设置值可以通过**组策略建模**来事先模拟得知，操作步骤如下。



图4-93

STEP 1 在图 4-94中，通过【对着**组策略建模**右击➲**组策略建模向导**】的方式进行操作。



图4-94

STEP 2 当出现**欢迎使用组策略建模向导**界面时单击下一步按钮。

STEP 3 由于必须指定一台Windows Server 2003或新版本的域控制器来执行模拟工作，因此请通过图 4-95来选择域控制器，图中系统可自行挑选一台域控制器。

Download at http://www.pin5i.com/

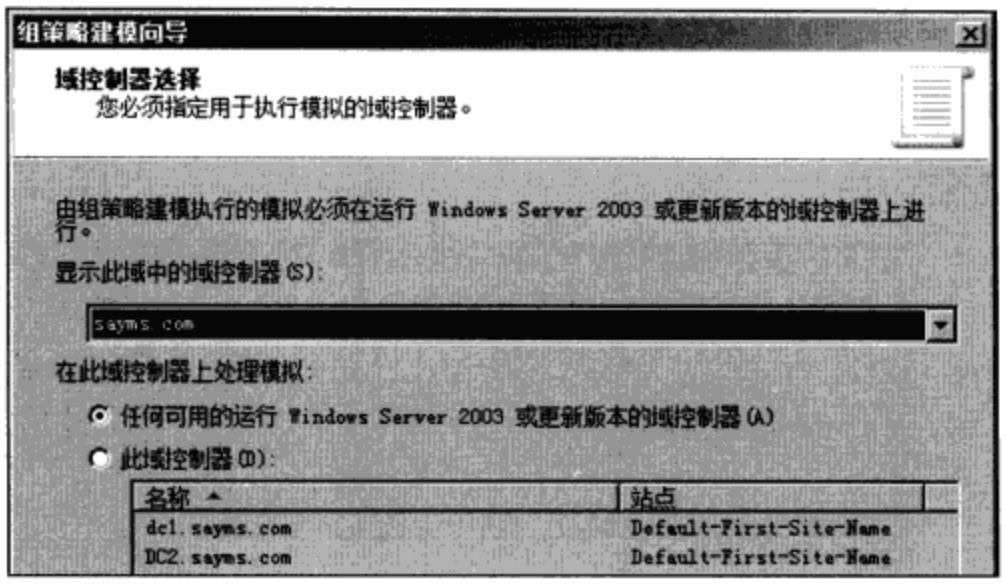


图 4-95

STEP 4 在图 4-96中分别选择我们要练习的用户账户peter与计算机账户WIN7PC1后单击**下一步**按钮。

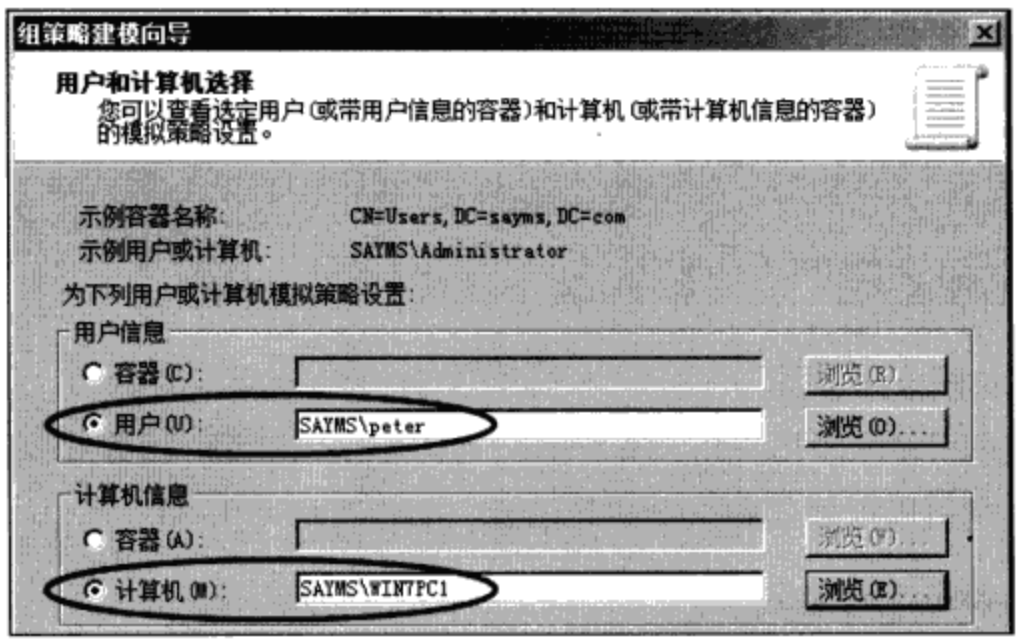


图 4-96

STEP 5 在图 4-97中选择**慢速网络连接**或**环回处理模式**复选框等，完成后单击**下一步**按钮。

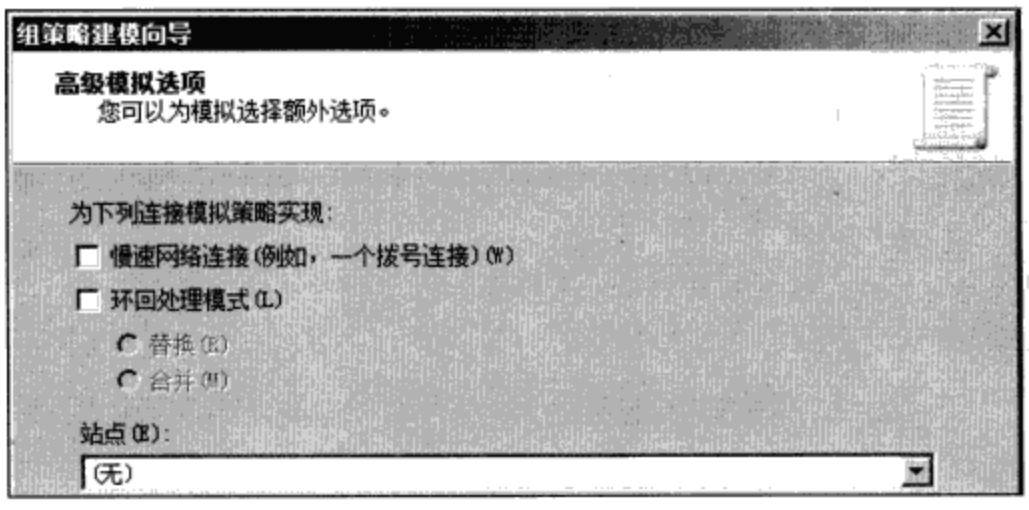


图 4-97

Download at http://www.pin5i.com/

STEP 6 由图 4-98可知用户账户**刘彼得**（peter）与计算机账户WIN7PC1当前都是位于组织单位**业务部**，请通过浏览按钮来将其模拟到将来的位置，也就是组织单位**金融部**，单击下一步按钮。

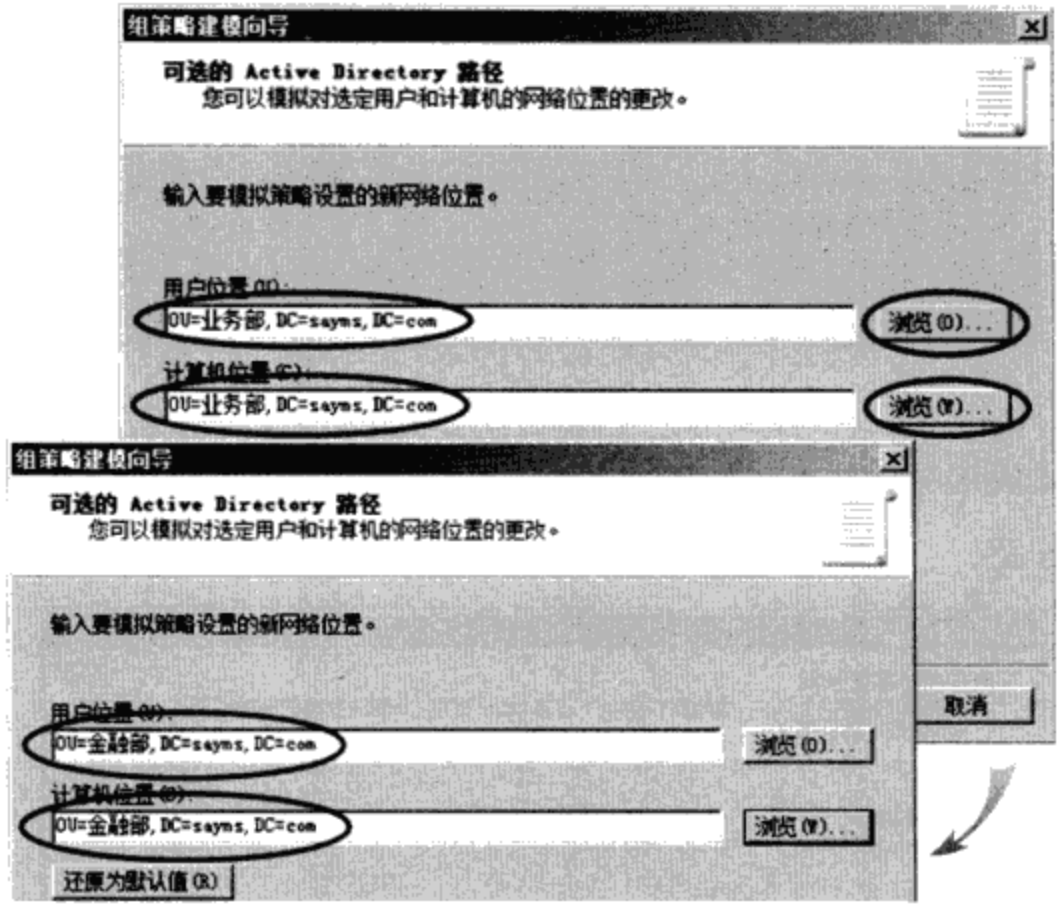


图 4-98

STEP 7 图 4-99分别显示了用户与计算机账户当前所隶属的组，如有需要的话，可通过单击添加按钮来模拟他们将来会隶属的组，单击下一步按钮。

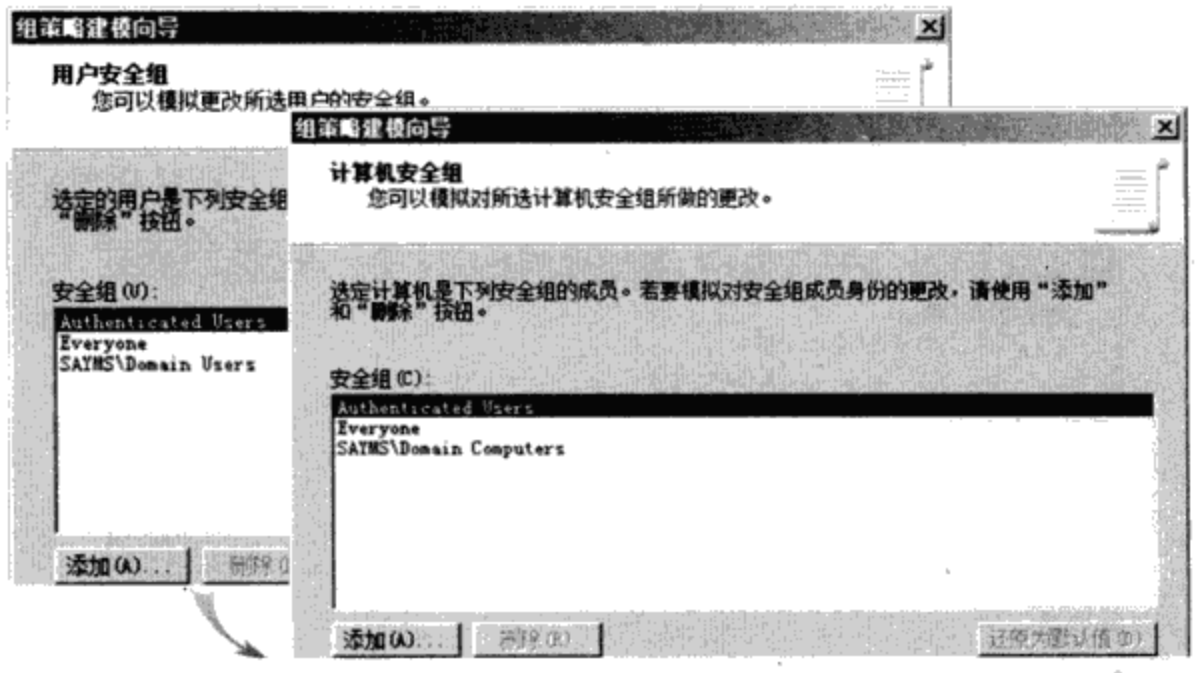


图 4-99

STEP 8 图 4-100分别显示了用户与计算机账户当前所应用的**WMI筛选器**，如有需要的话，

Download at http://www.pin5i.com/

可通过单击添加按钮来模拟他们将来会应用的**WMI筛选器**，单击下一步按钮。

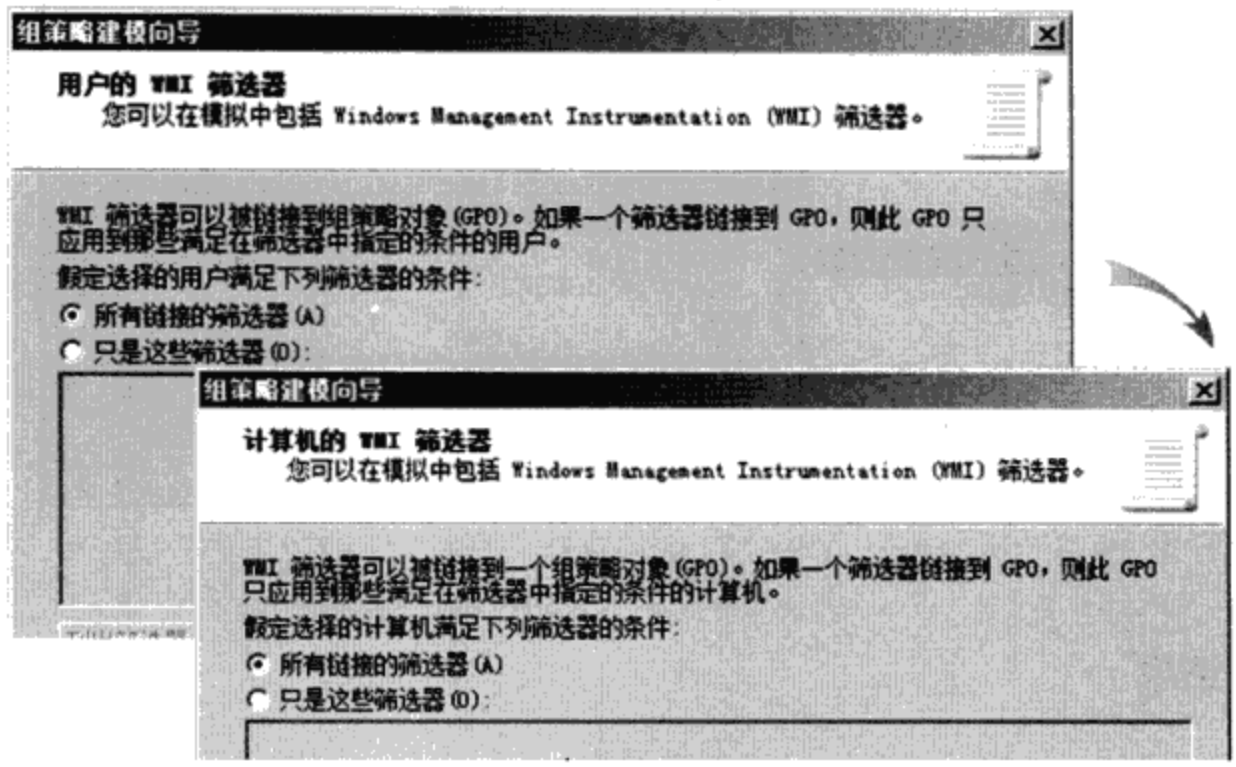


图4-100

STEP 9 确认图 4-101的设置无误后单击下一步按钮。

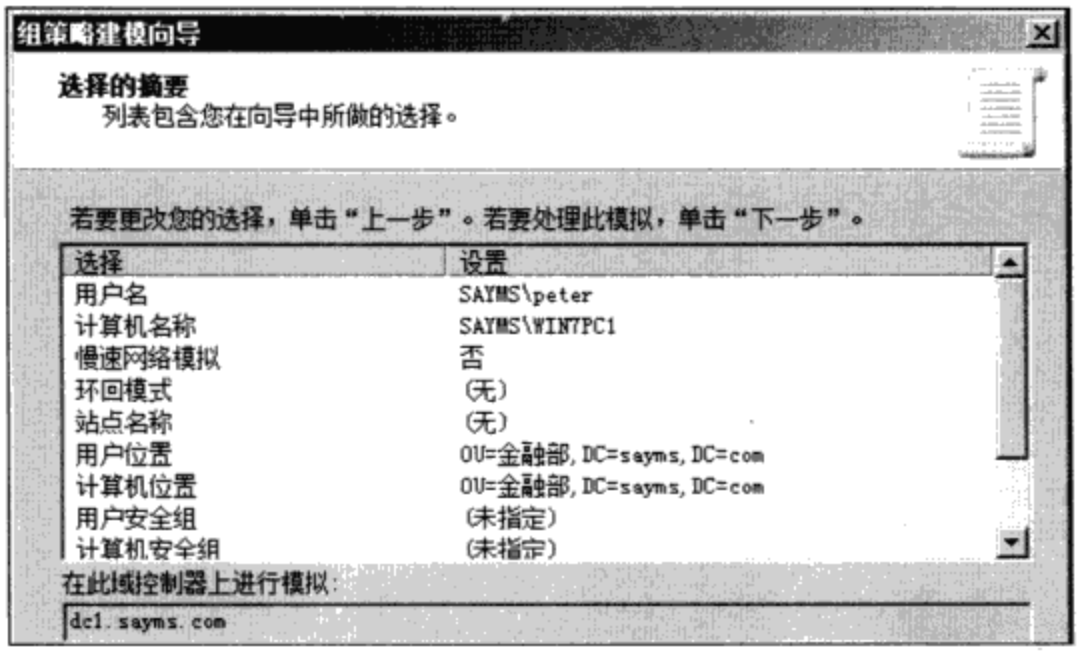


图4-101

STEP 10 当出现**正在完成组策略建模向导**界面时单击完成按钮。

STEP 11 设置完成后，可通过图 4-102右边的3个标签来查看模拟的结果。

Download at http://www.pin5i.com/

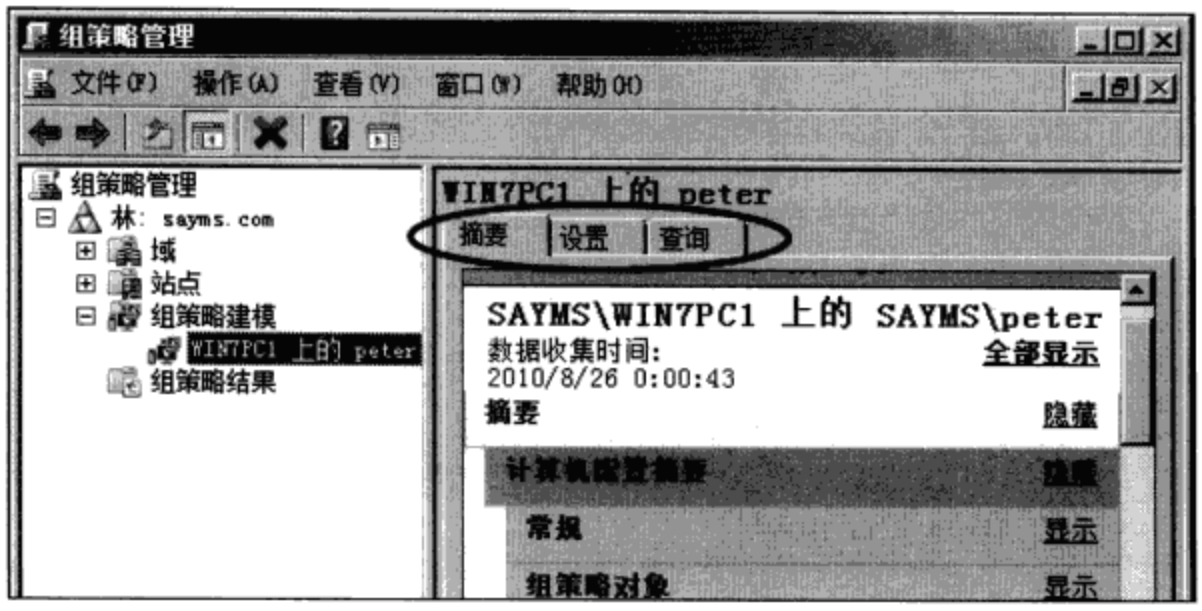


图4-102

2. 组策略结果

我们将使用图4-103的环境来练习**组策略结果**。我们想要知道图中用户账户**刘彼得**（peter）到计算机WIN7PC1登录后的用户与计算机策略的设置值。

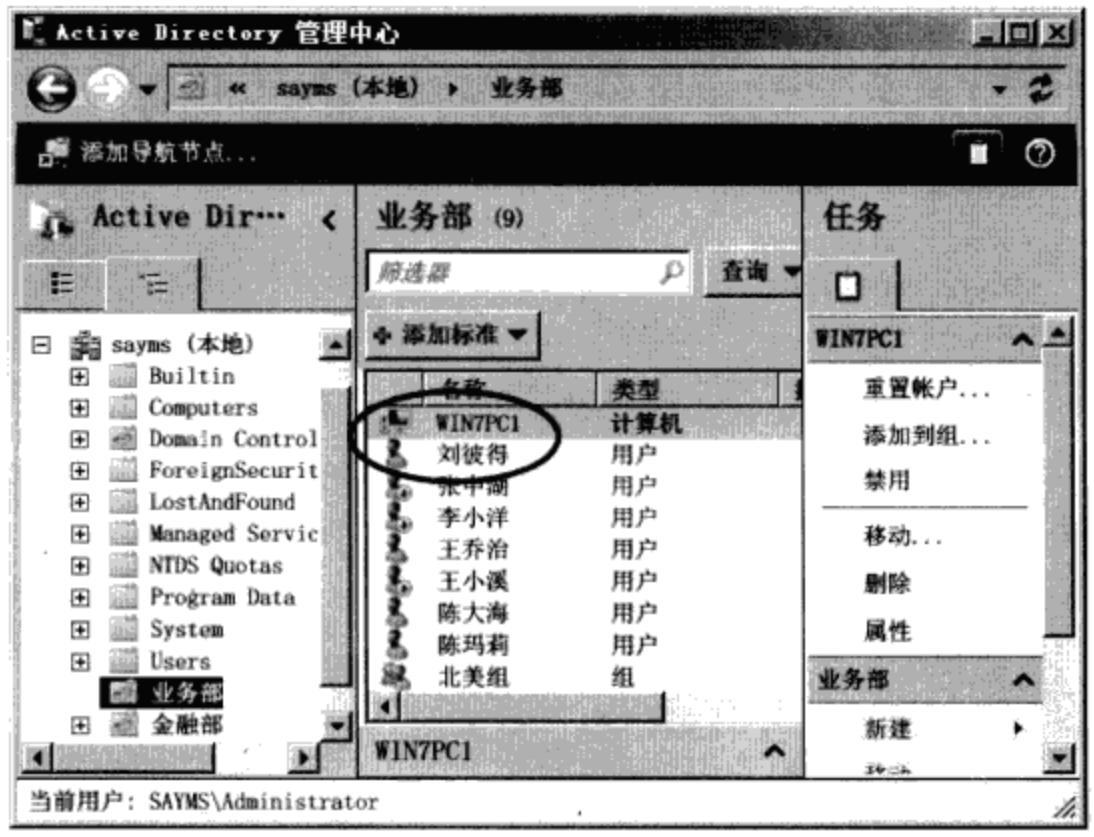


图4-103

STEP 1 若用户**刘彼得**（peter）未曾到计算机WIN7PC1登录的话，请先登录。

STEP 2 请到域控制器上以系统管理员的身份登录、运行**组策略管理**，如图4-104所示，通过【对着**组策略结果**单击右键➲组策略结果向导】的方式进行操作。

Download at http://www.pin5i.com/

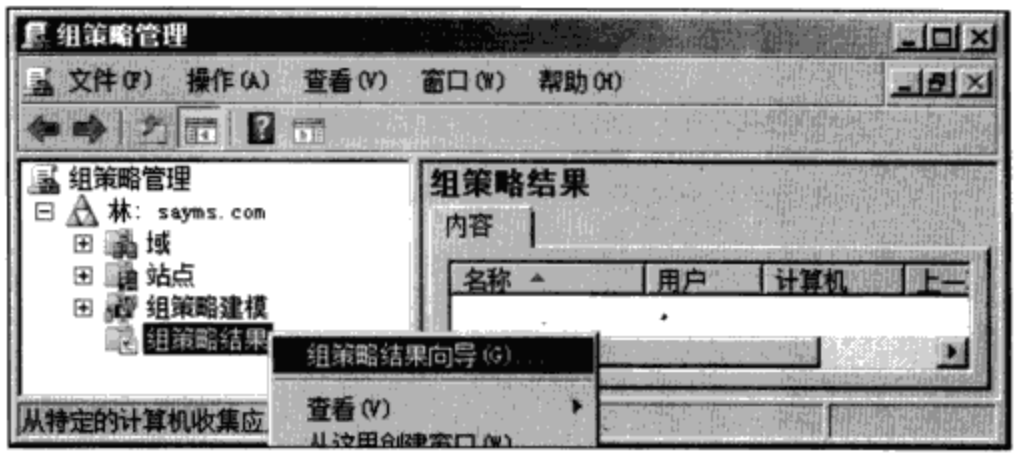


图 4-104

STEP 3 当出现**欢迎使用组策略结果向导**界面时单击下一步按钮。

STEP 4 在图 4-105中选择要查看的域计算机WIN7PC1后单击下一步按钮。

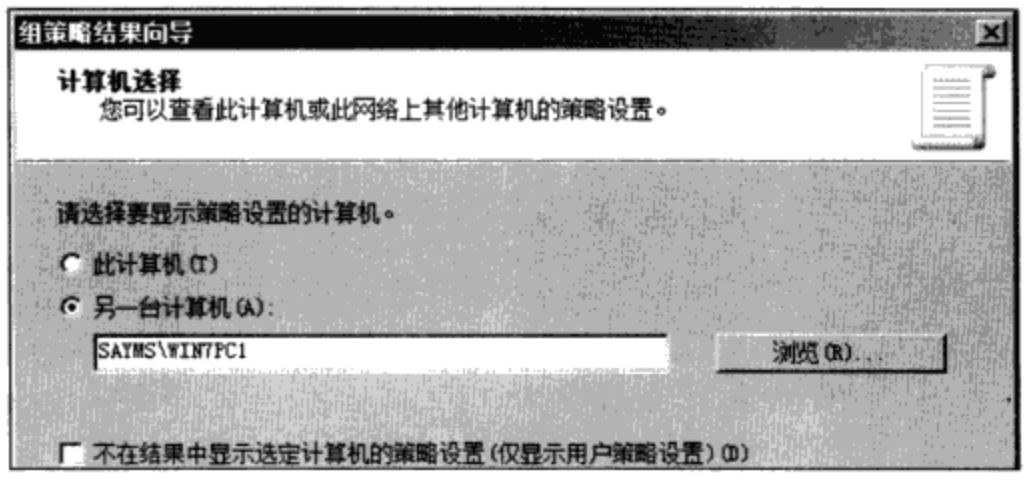


图 4-105

注意

请先将此域成员计算机的**Windows防火墙**关闭，否则无法连接此计算机。

STEP 5 在图 4-106中选择域用户peter（**刘彼得**）后单击下一步按钮。只有当前登录的用户与曾经登录过的用户账户可以被选择。

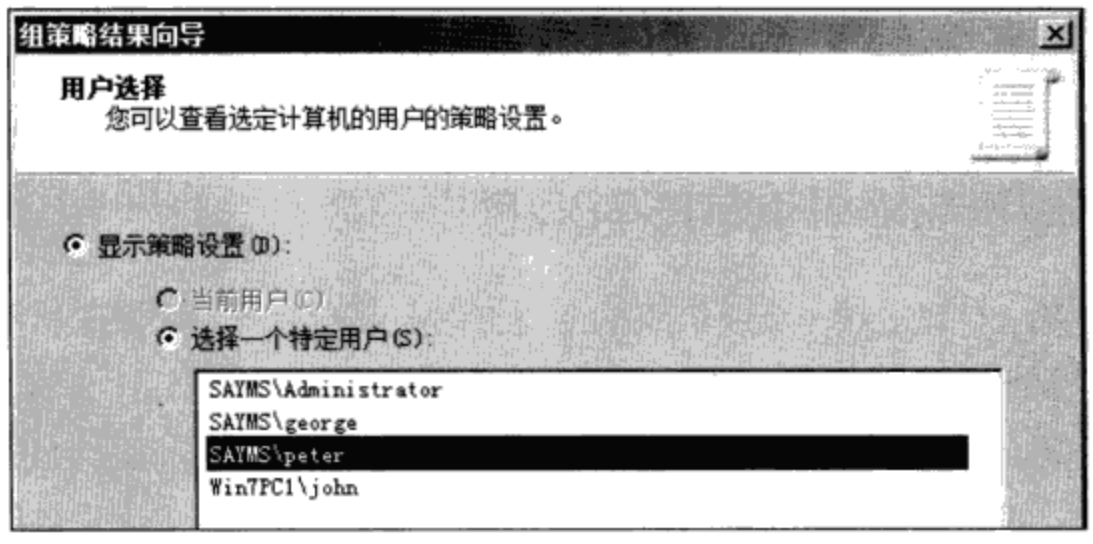


图 4-106

Download at http://www.pin5i.com/

STEP 6 请确认图 4-107中的设置无误后单击下一步按钮。

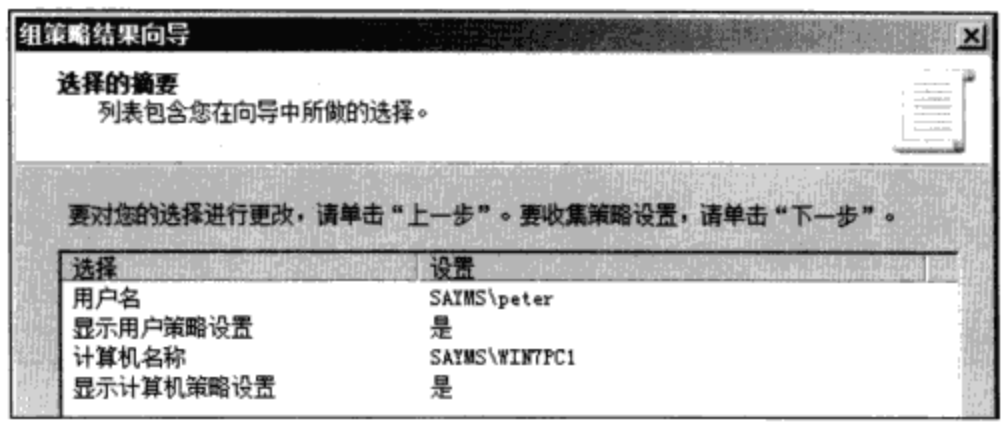


图 4-107

STEP 7 当出现**正在完成组策略结果**界面时单击完成按钮。

STEP 8 可通过图 4-108右边的3个标签来查看结果。

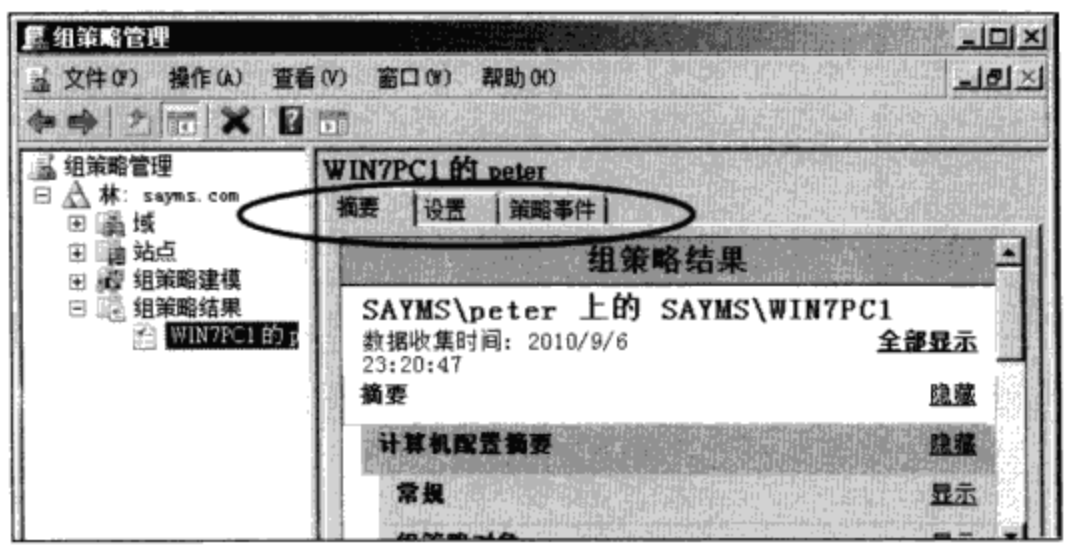


图 4-108

4-9 组策略的委派管理

您可以将GPO的链接、添加与编辑等管理工作，分别委派给不同的用户来负责，以分散和减轻系统管理员的管理负担。

4-9-1 站点、域或组织单位的GPO链接委派

您可以将链接GPO到站点、域或组织单位的工作委派给不同的用户来执行，以组织单位**业务部**为例，可以如图 4-109所示单击组织单位**业务部**后，通过**委派**标签来将链接GPO到此组织单位的工作委派给用户，由图中可知默认是Administrators、Domain Admins或Enterprise Admins组内的用户才拥有此权限。还可以通过界面中的**权限**下拉列表来设置**执行组策略建模分析**和**读取组策略结果数据**这两个权限。

Download at http://www.pin5i.com/

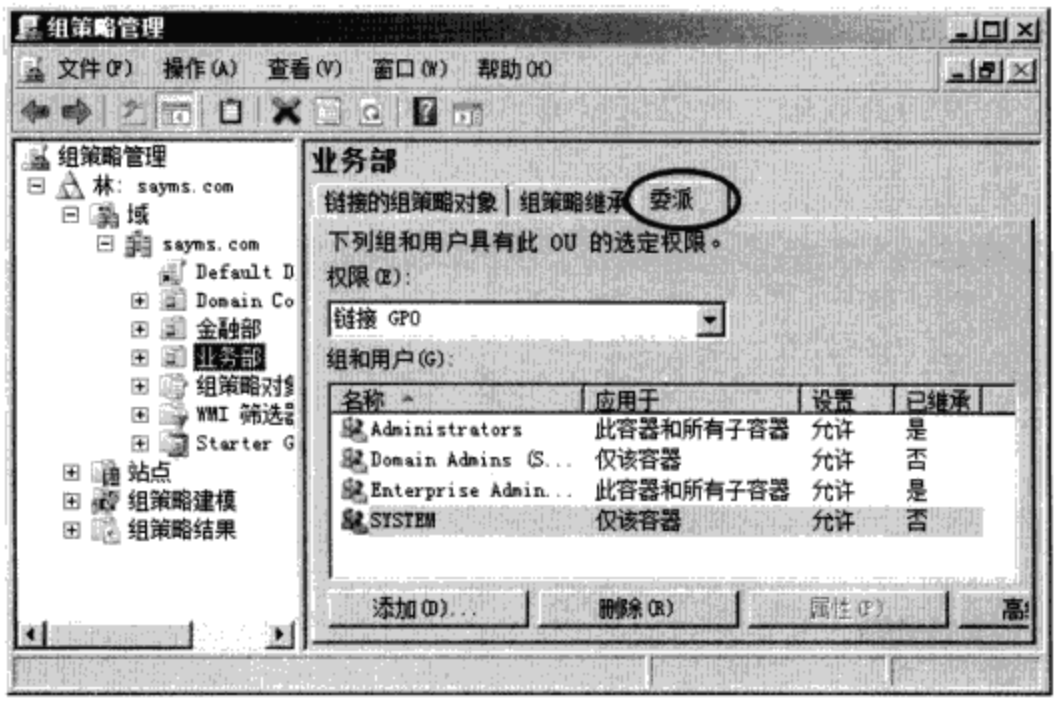


图 4-109

4-9-2 编辑GPO的委派

默认是Administrators、Domain Admins或Enterprise Admins组内的用户才有权限编辑GPO，如图 4-110所示为**测试用的GPO**的默认权限列表，您可以通过此界面来赋予其他用户权限，这些权限包含**读取**、**编辑设置**与“**编辑设置，删除、修改安全性**”等3种。

图 4-110

4-9-3 添加GPO的委派

系统默认是Domain Admins与Group Policy Creator Owners组内的用户才有权限添加GPO，如图 4-111所示，您也可以通过此界面来将此权限赋予其他用户。

Download at http://www.pin5i.com/

Group Policy Creator Owners组内的用户在添加GPO后，他就是这个GPO的所有者，因此他对这个GPO拥有完全控制的权限，所以可以编辑这个GPO的内容，不过他却无权限编辑其他的GPO。

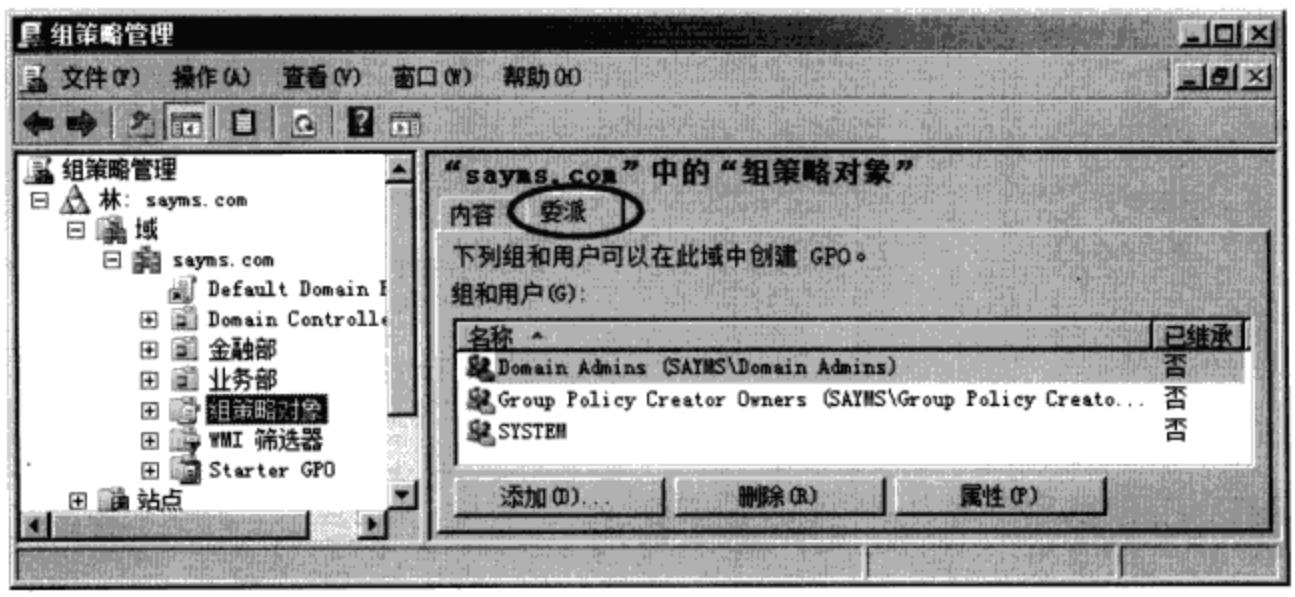


图4-111

4-9-4 WMI筛选器的委派

系统默认是Domain Admins与Enterprise Admins组内的用户才有权限在域内创建新的WMI筛选器，并且可以修改所有的WMI筛选器，如图4-112所示的**完全控制**权限。而Administrators与Group Policy Creator Owners组内的用户也可以创建新的WMI筛选器和修改其自行创建的WMI筛选器，不过却不可以修改其他用户所创建的WMI筛选器，如图4-112所示的**CreatorOwner**权限。您也可以通过此界面来将权限赋予其他用户。

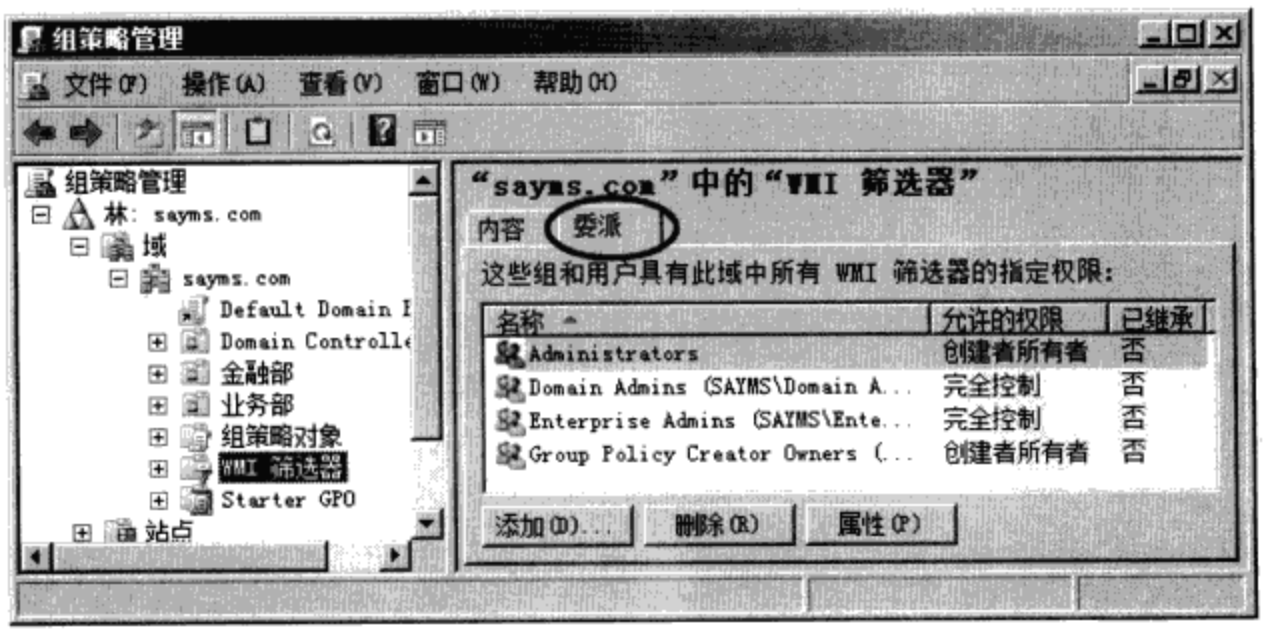


图4-112

Group Policy Creator Owners组内的用户，在添加WMI筛选器后，他就是此WMI筛选器的所有者，因此他对此WMI筛选器拥有完全控制的权限，所以可以编辑此WMI筛选器的属性，

Download at http://www.pin5i.com/

不过他却无权限编辑其他的WMI筛选器。

4-10 Starter GPO的设置和使用

Starter GPO内仅包含**管理模板**的策略设置，您可以将经常用到的**管理模板**策略设置值创建到**Starter GPO**内，然后在创建一般GPO时，就可以直接将**Starter GPO**内的设置值导入到这个一般GPO内，如此便可以节省创建一般GPO的时间。创建**Starter GPO**的步骤如下所示。

STEP 1 如图 4-113所示，通过【对着**Starter GPO**单击右键➲新建】的方式进行操作。

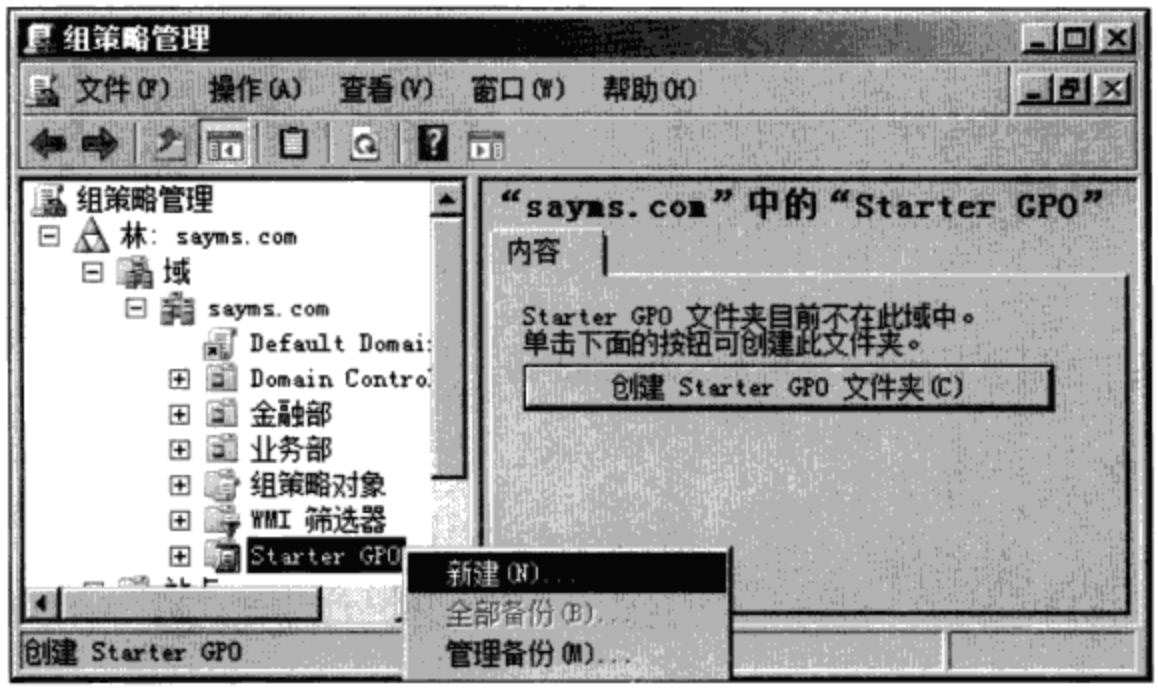


图4-113

提示

可以不需要单击界面右方的**创建 Starter GPO 文件夹**按钮，因为在您创建第1个**Starter GPO**时，它也会自动创建此文件夹，此文件夹的名称是StarterGPOs，它是位于域控制器的sysvol共享文件夹之下。

STEP 2 在图 4-114中为此**Starter GPO**设置名称和输入注释后单击**确定**按钮。

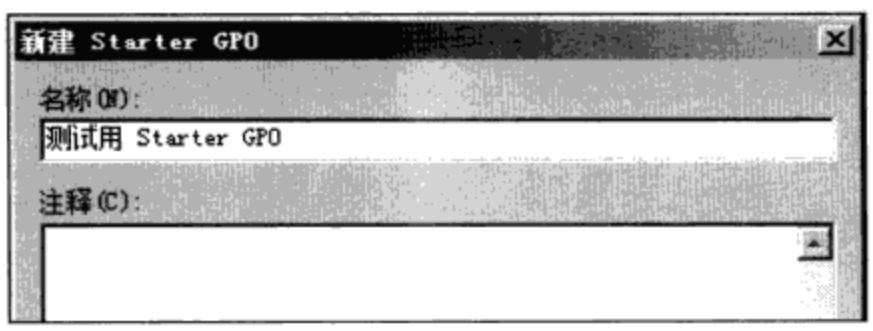


图4-114

STEP 3 在图 4-115中，通过【对着此Starter GPO单击右键➲编辑】的方式进行操作。

Download at http://www.pin5i.com/

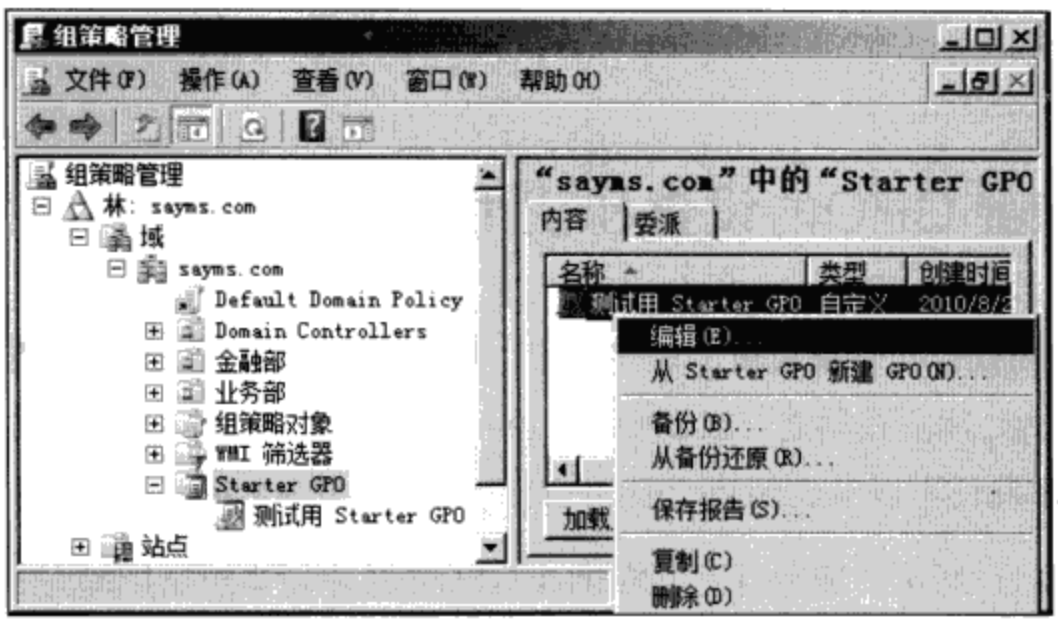


图4-115

STEP 4 通过图 4-116来编辑计算机和用户配置的**管理模板**策略。

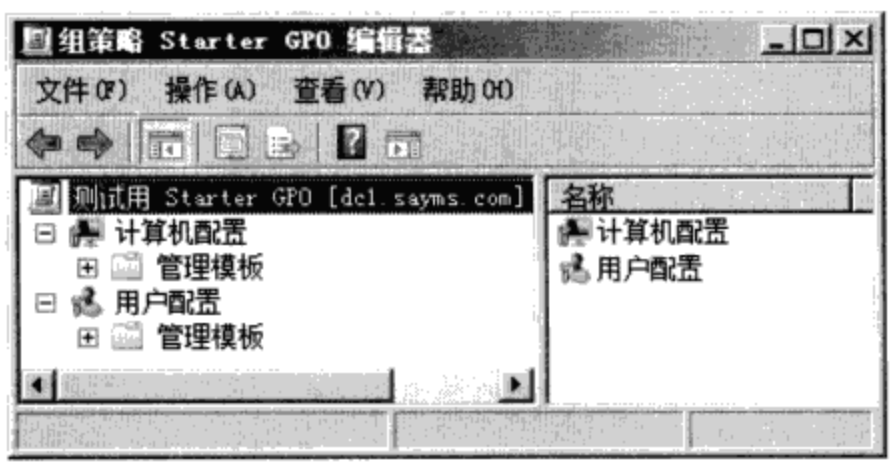


图4-116

完成**Starter GPO**的创建和编辑后，在创建一般GPO时，就可以如图4-117所示选择从这个**Starter GPO**来导入其**管理模板**的设置值。

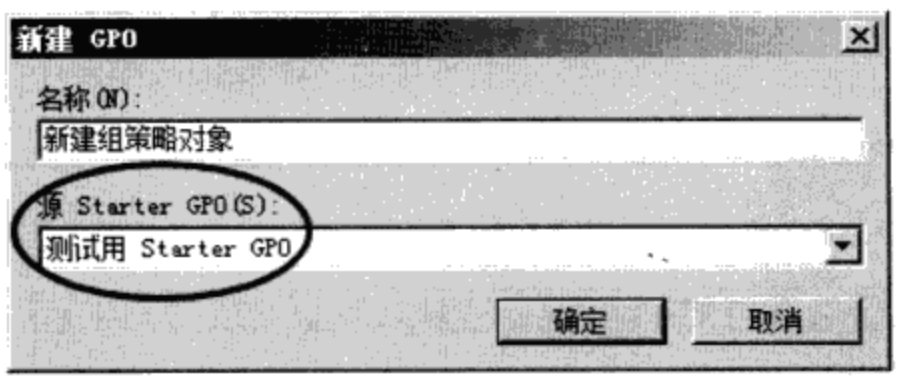


图4-117

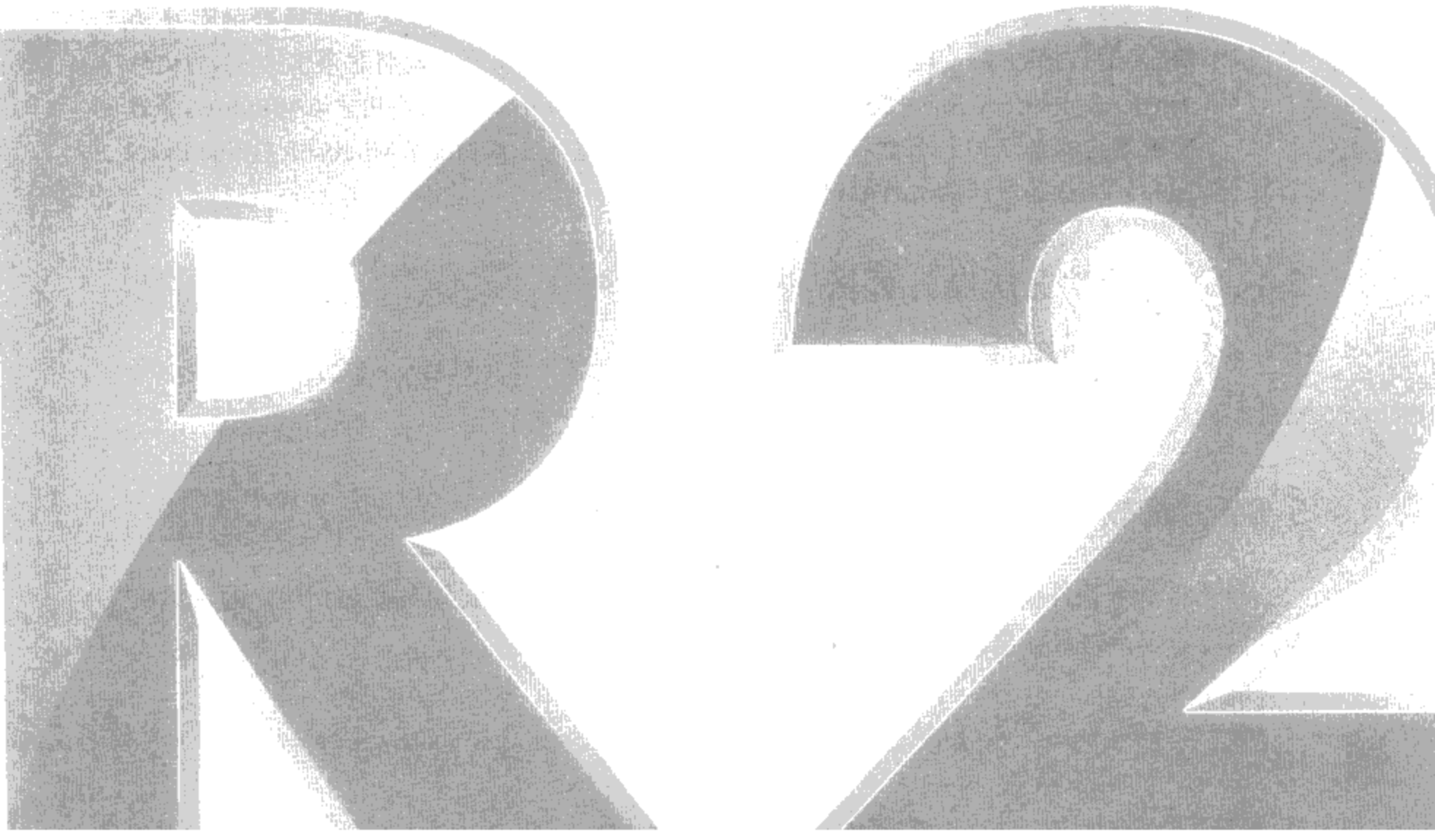
Download at http://www.pin5i.com/

第5章

使用组策略部署软件

可以通过AD DS组策略来为企业内部计算机部署（Deploy）软件，也就是自动为这些计算机安装、维护和删除软件。

- 软件部署概述
- 将软件发布给用户
- 将软件分配给用户或计算机
- 将软件升级和重新部署
- 部署Microsoft Office
- 发布ZAP应用程序
- 软件部署的其他设置
- 将软件重新封装成MSI应用程序



Download at http://www.pin5i.com/

5-1 软件部署概述

可以通过组策略来将软件部署给域内的计算机，也就是用户登录或计算机启动时会自动安装或很容易安装所部署的软件，而软件部署分为**分配**（Assign）和**发布**（Publish）两种。一般来说，这些软件需为**Windows Installer Package**，也就是这些软件内包含着扩展名为.msi的安装文件，例如Microsoft Office 2007就是Windows Installer Package。客户端计算机是使用Windows Installer service来安装Windows Installer Package。

> **提示**
>
> 也可以部署扩展名为.zap或msp的软件，或是将其他类型的软件封装成为.msi的Windows Installer Package（后述）。

5-1-1 将软件分配给用户

当您将一个软件通过组策略分配给域用户后，用户在域内的任何一台计算机登录时，这个软件都会被**通告**（Advertised）给该用户，但是此软件并没有完全安装，而只是安装了与这个软件有关的部分信息而已，例如可能会在【开始➲所有程序】中自动创建该软件的快捷方式。用户的计算机会在以下两种情况之下来安装此软件。

- 用户开始运行此软件：例如用户通过【开始➲所有程序➲选择该软件的快捷方式】或双击桌面上的快捷方式后，就会自动安装此软件。
- 使用**文件启动**功能（Document Activation）：举例来说，假设这个被**通告**的程序为Microsoft Office Excel 2003，则用户登录时，他的计算机会自动将扩展名为.xls的文件和Microsoft Office Excel 2003关联在一起（Associate），此时只要用户在**Windows资源管理器**内双击任何一个扩展名为.xls的文件，系统就会自动安装Microsoft Office Excel 2003，这就是所谓的**文件启动**功能。

5-1-2 将软件分配给计算机

当您将一个软件通过组策略分配给域成员计算机后，这些计算机启动时就会自动安装这个软件，而且任何用户登录都可以使用此软件。

5-1-3 将软件发布给用户

当您将一个软件通过组策略发布给域用户后，此软件并不会自动被安装到用户的计算机内，而是由用户自行使用以下两种方式来安装此软件。

Download at http://www.pin5i.com/

- 通过**控制面板**来安装。Windows Server 2008 R2或Windows 7客户端（需加入域才有以下选项）：选择【开始➲控制面板➲单击**程序**处的**获取程序**】；Windows Server 2008或Windows Vista客户端（需加入域才有以下选项）：选择【开始➲控制面板➲单击**程序**➲单击**获取新程序**处的**从网络安装程序**】；Windows Server 2003或Windows XP客户端：选择【开始➲控制面板➲添加或删除程序➲添加新程序】。
- 使用**文件启动**功能（Document Activation）。举例来说，假设这个被发布的软件为Microsoft Office Excel 2003，则在AD DS内会自动将扩展名为.xls的文件和Microsoft Office Excel 2003关联在一起（Associate），然而用户登录时，他的计算机并不会将扩展名为.xls的文件和Microsoft Office Excel 2003关联在一起，也就是对此计算机来说，扩展名为.xls的文件是一个**未知的文件类型**，不过只要用户在**Windows资源管理器**内双击任何一个扩展名为.xls的文件，他的计算机就会通过AD DS得知扩展名为.xls的文件是与Microsoft Office Excel 2003关联在一起的，因此会自动安装Microsoft Office Excel 2003。

注意

您无法将软件发布给计算机，只能够分配给计算机。如果用户的计算机内已经安装其他版本Microsoft Office Excel，例如Microsoft Office Excel 2007，则此时.xls的文件应该已经与Microsoft Office Excel 2007关联在一起，因此对此计算机来说，扩展名为.xls的文件并不是**未知的文件类型**，故用户在**Windows资源管理器**内双击扩展名为.xls的文件时，系统会执行Microsoft Office Excel 2007来打开此文件，而不会通过AD DS来自动安装Microsoft Office Excel 2003。

5-1-4 自动修复软件

被发布或分配的Windows Installer Package可以具备自动修复的功能，也就是客户端在安装完成后，若此软件程序内有关键性的文件损毁、丢失或不小心被用户删除的话，则在用户运行此软件时，其系统会自动检测到此不正常现象，并重新安装这些文件。

5-1-5 删除软件

一个被发布或分配的软件，在用户将其安装完成后，若您之后不想再让用户来使用此软件的话，可在组策略内从发布或分配的软件列表中将此软件删除，并设置下次用户登录或计算机启动时，自动将这个软件从用户的计算机中删除。

Download at http://www.pin5i.com/

5-2 将软件发布给用户

以下我们沿用前几章的组织单位**业务部**中的**测试用的GPO**为例来练习将软件（Windows Installer Package）发布给此组织单位内的用户，并让用户通过**控制面板**来安装此软件。若您还没有创建组织单位**业务部**与**测试用的GPO**的话，请先使用**Active Directory管理中心**（或**Active Directory用户和计算机**）和**组策略管理**来创建，并在此组织单位内新建几个用来练习的用户账户。

5-2-1 发布软件

以下步骤将先创建**软件发布点**（Software Distribution Point，也就是用来存储Windows Installer Package的共享文件夹），接着设置软件默认的存储位置，最后再将软件发布给用户。

> **提示**
>
> 以下将使用一个免费的文字编辑软件**AkelPad374**来练习，它原本是**非MSI应用程序**，不过笔者已经将其重新封装成扩展名为.MSI的Windows Installer Package。

STEP 1 请在域中的任何一台服务器内（假设为dc1）创建一个用来作为**软件发布点**的文件夹，例如C:\Packages，它将用来存储Windows Installer Package，例如我们要用来练习的**AkelPad374**。

STEP 2 将此文件夹设置为**共享文件夹**，赋予Everyone**读取**权限（系统会同时将**读取**的共享权限和NTFS权限赋予Everyone）。

> **提示**
>
> 其共享名默认为文件夹名称Packages，建议将共享文件夹隐藏起来，也就是将共享名最后一个字符设置为**$**符号，例如Packages$。

STEP 3 在共享文件夹内新建用来存放**AkelPad374**的子文件夹，然后将**AkelPad374**复制到此文件夹内，如图 5-1所示。

Download at http://www.pin5i.com/



图 5-1

STEP 4 接着设置软件默认的存储位置：请在域控制器上选择【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑➲在图 5-2中展开**用户配置**➲策略➲软件设置➲软件安装➲单击上方的**属性**图标】。

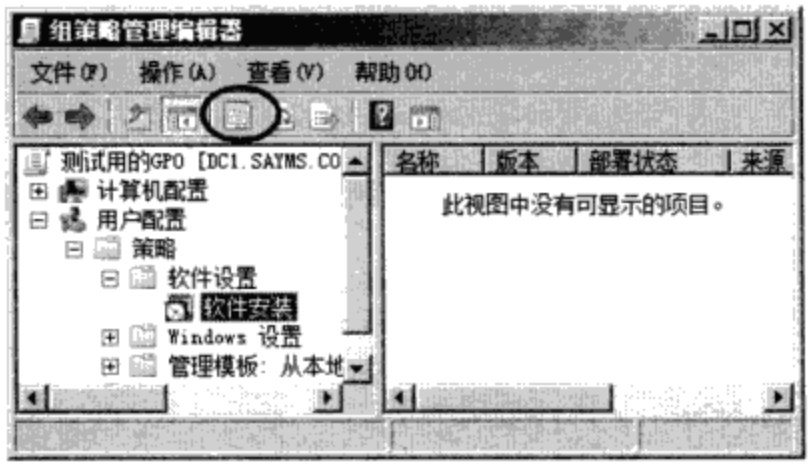


图 5-2

STEP 5 在图 5-3中的**默认程序数据包位置**文本框中输入软件的存储位置，注意必须是UNC网络路径，例如\\dc1\Packages。完成后单击确定按钮。

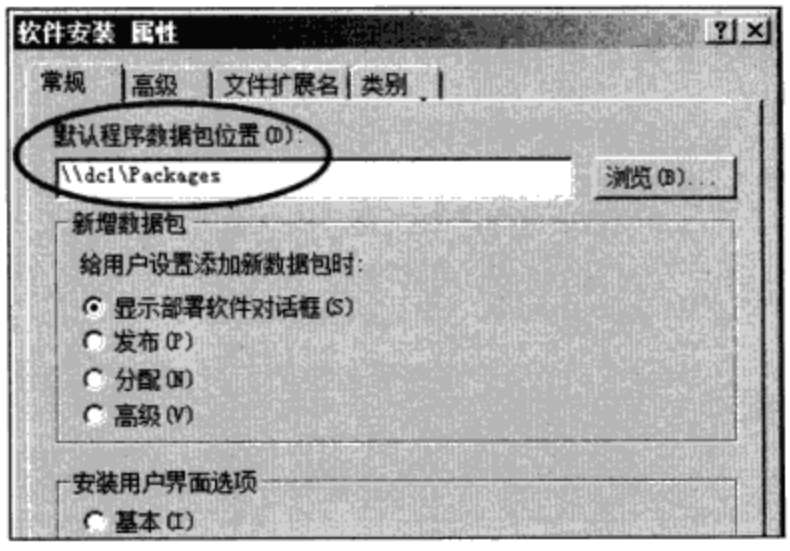


图 5-3

Download at http://www.pin5i.com/

STEP 6 如图 5-4所示，通过【对着**软件安装**单击右键➲新建➲数据包】的方式进行操作。

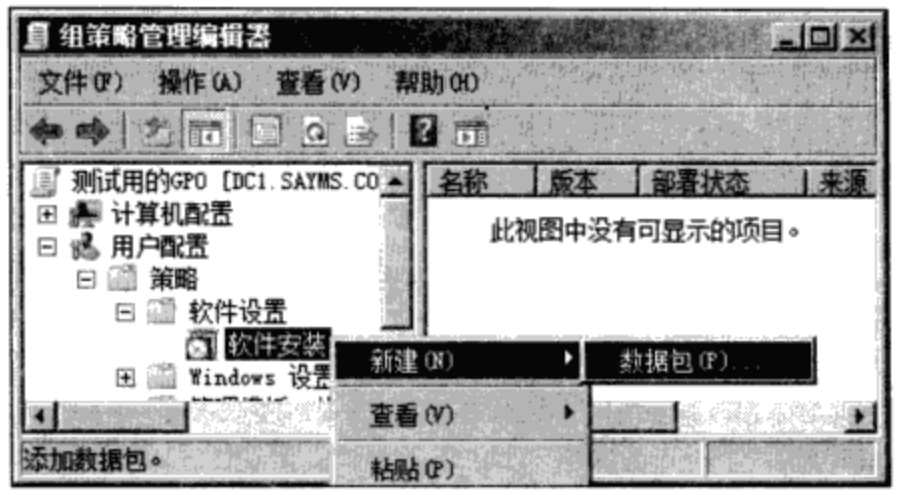


图 5-4

STEP 7 在图 5-5中选择要用来练习的Windows Installer Package，也就是选择AkelPad374文件夹中的AkelPad374.msi（扩展名.msi默认会被隐藏），然后单击打开按钮。

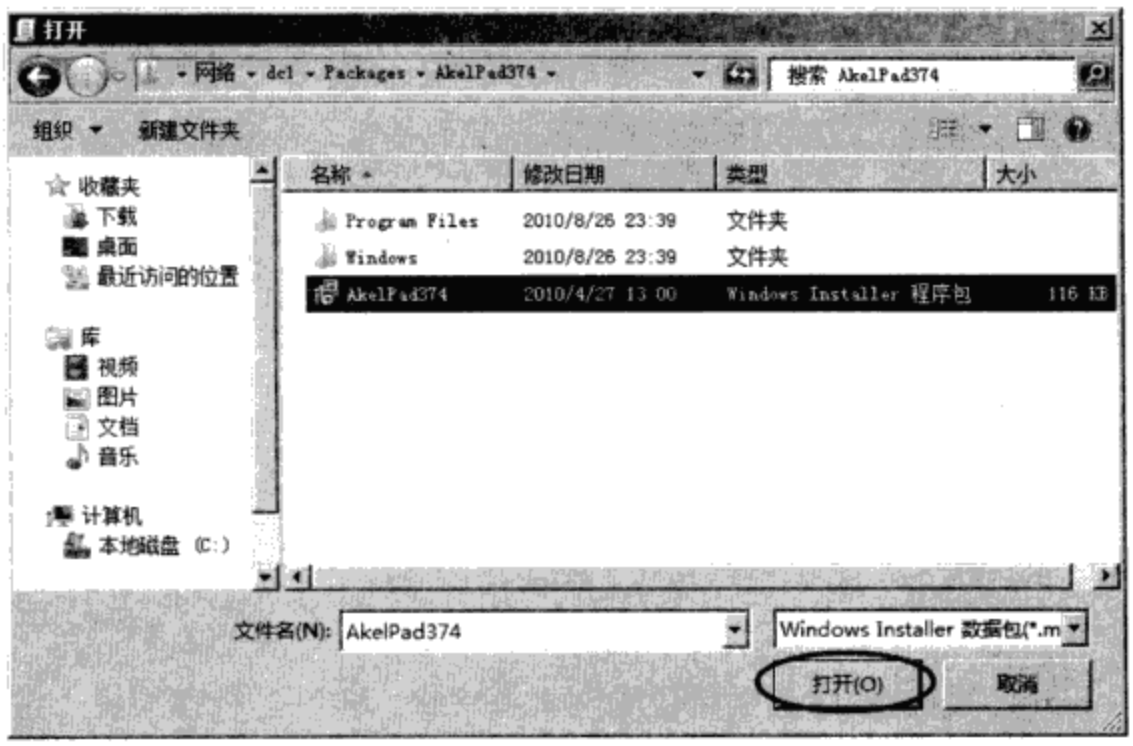


图 5-5

STEP 8 在图 5-6中选择**已发布**单选按钮，然后单击确定按钮。

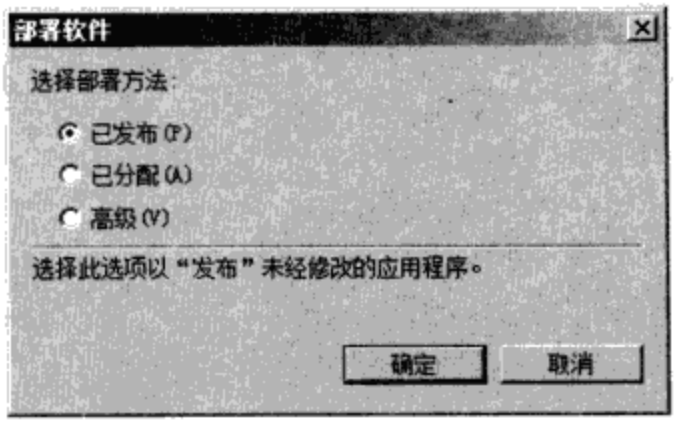


图 5-6

Download at http://www.pin5i.com/

STEP 9 由图 5-7右方可知AkelPad 374已被成功发布。

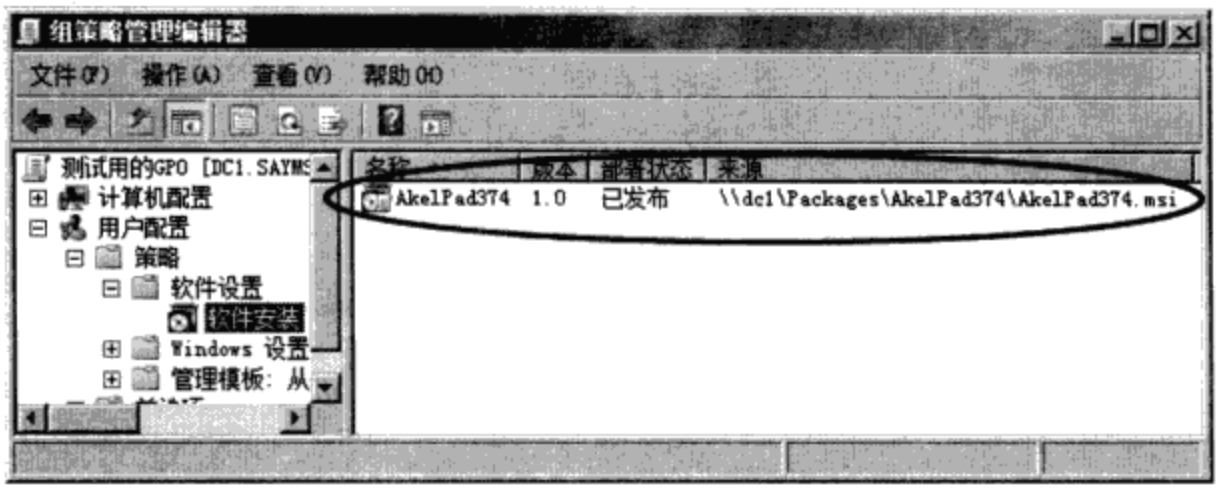


图 5-7

5-2-2 客户端安装被发布的软件

我们将在域成员计算机上通过**控制面板**来练习安装上述被发布的软件。

注意

我们所使用的应用程序AkelPad默认并未和任何扩展名有关联性，故无法通过**文件启动**的方式来安装此程序。

STEP 1 请到域中的任何一台计算机上使用组织单位**业务部**中的用户账户（例如peter）登录域，假设用户的计算机为Windows 7。

STEP 2 选择【开始➲控制面板➲如图 5-8所示单击**程序**处的**获得程序**】。

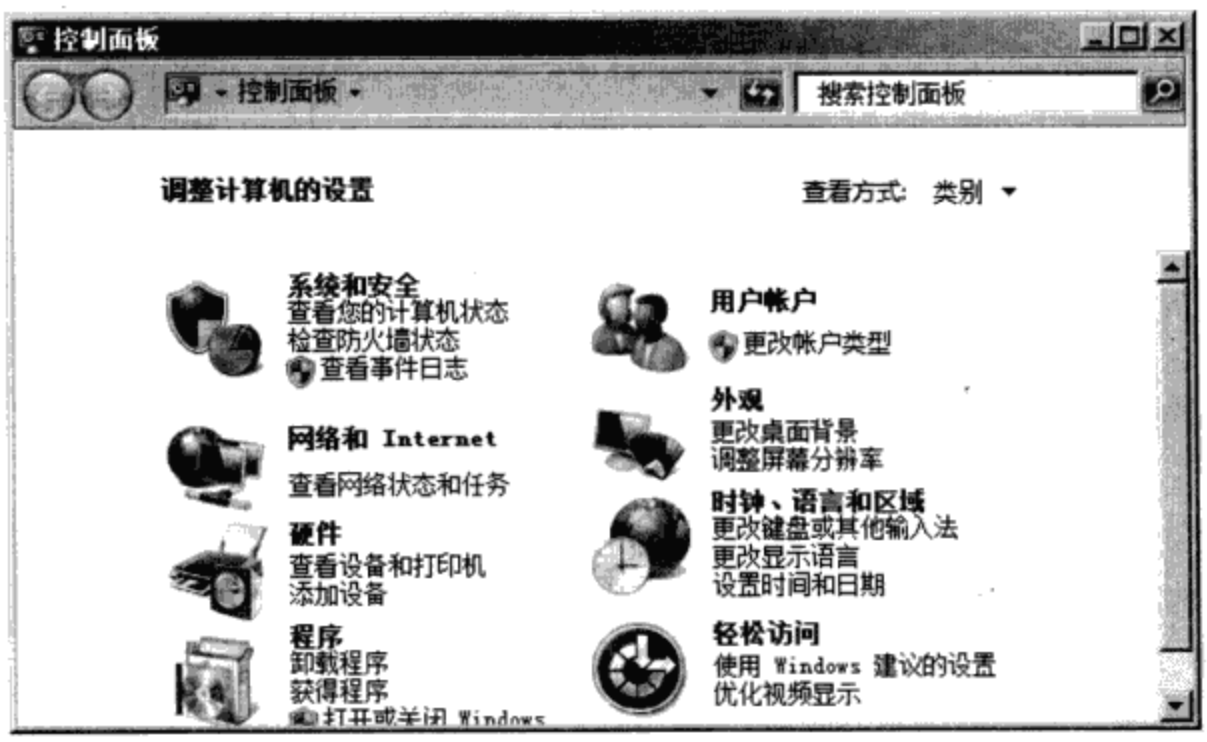


图 5-8

STEP 3 选择图 5-9中已发布的软件**AkelPad374**后单击上方的**安装**按钮。

Download at http://www.pin5i.com/

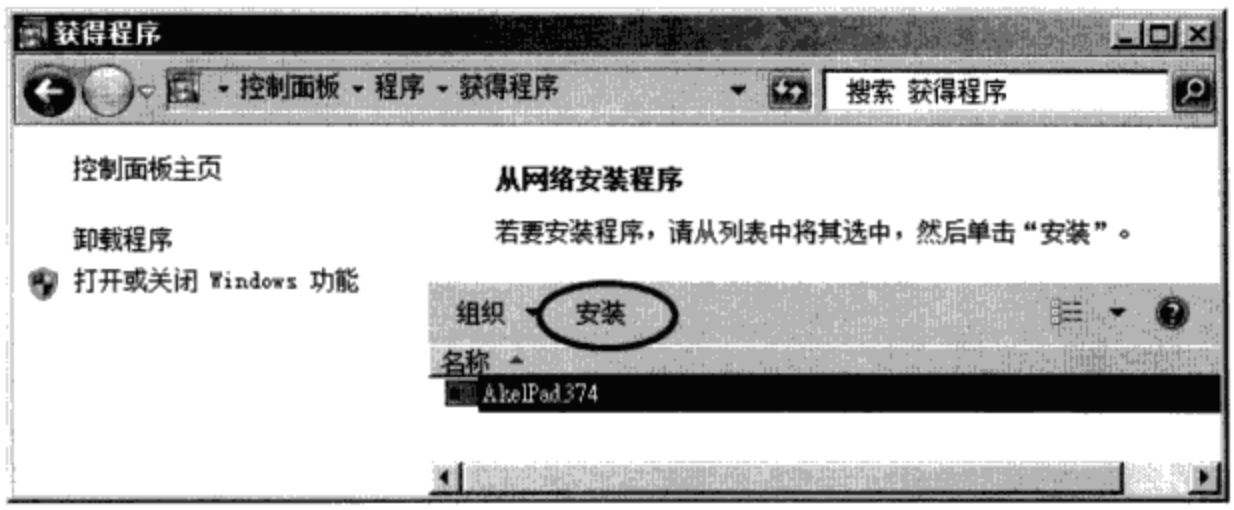


图 5-9

STEP 4 完成后在【开始➲所有程序➲AkelPad】内会看到AkelPad的相关快捷方式。试着运行这个程序来测试此程序是否可以正常运行。

5-2-3 测试自动修复软件的功能

我们要将安装好的软件AkelPad374的某个文件夹删除，以便测试当系统发现此文件夹丢失时，是否会自动重新安装此文件夹和其内的文件。当前登录的用户仍然是用户peter。

STEP 1 请如图 5-10所示将C:\Program Files\AkelPad\AkelFiles文件夹删除，出现确认界面时单击 是 (Y) 按钮。

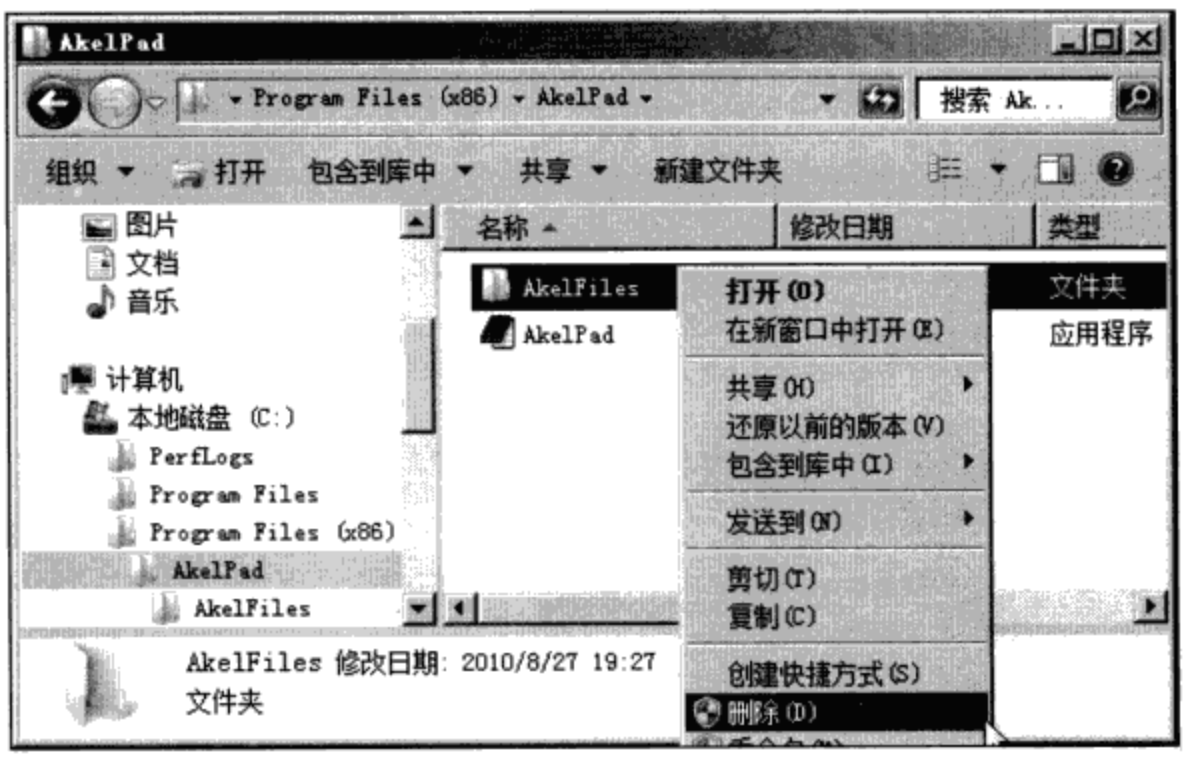


图 5-10

STEP 2 由于当前登录的用户peter并没有权限删除此文件夹，故请在图 5-11中输入系统管理员的账户和密码后单击 是 (Y) 按钮。

Download at http://www.pin5i.com/



图 5-11

STEP 3 接下来再运行AkelPad来测试自动修复功能：选择【开始➲所有程序➲AkelPad➲AkelPad】，此时因为系统检测到AkelFiles文件夹已经不见了，故会自动重新安装此文件夹和其内的文件。

提示

若您是使用Windows XP的话，请先注销peter，改用系统管理员身份登录、删除文件夹，注销后再改用peter登录，运行AkelPad，系统就会自动重新安装被删除的文件夹和其内的文件。

5-2-4 取消已发布的软件

若要取消已经被发布的软件，如图5-12所示，通过【对着该软件单击右键➲所有任务➲删除】的方式进行操作，然后有以下两种选择。



图 5-12

- 立即从用户和计算机中卸载软件：当用户下次登录时或计算机启动时，此软件就会自动被删除。

Download at http://www.pin5i.com/

- 允许用户继续使用软件，但阻止新的安装：用户已经安装的软件不会被删除，可以继续使用它，不过新用户登录时，就不会有此软件可供选择与安装。

5-3 将软件分配给用户或计算机

将软件分配给用户或计算机的步骤，与前一小节将软件发布给用户类似，本节仅列出区别。

5-3-1 分配给用户

您可以将软件分配给整个域或某个组织单位内的用户，其详细的操作步骤请参照前一节，不过需要如图 5-13所示改为选择**已分配**。

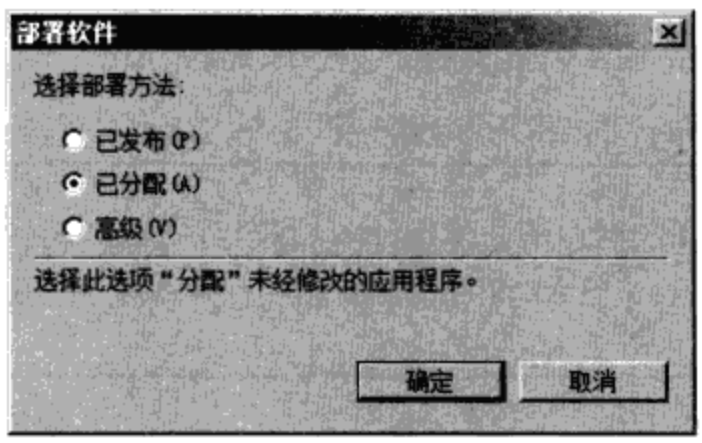


图 5-13

您也可以将一个已经发布的软件直接改为**已分配**，如图 5-14所示通过【对着此软件单击右键➲分配】的方式进行操作。



图 5-14

被分配此软件的用户，当他们登录后，系统就会创建该软件的快捷方式，将相关扩展名和此软件之间创建起关联关系，不过此软件事实上并还没有真正的被安装完成，此时只要用户选择此软件的快捷方式，系统就会自动安装此软件；用户也可以使用**文件启动**的方式来安装此

Download at http://www.pin5i.com/

软件，详见**将软件分配给用户**的相关说明。

5-3-2 分配给计算机

当您将软件分配给整个域或组织单位内的计算机后，这些计算机在启动时就会自动安装此软件。分配的步骤与前一节相同，不过请注意以下几点事项。

- 请按如图 5-15所示通过**计算机配置**来设置，而不是**用户配置**。

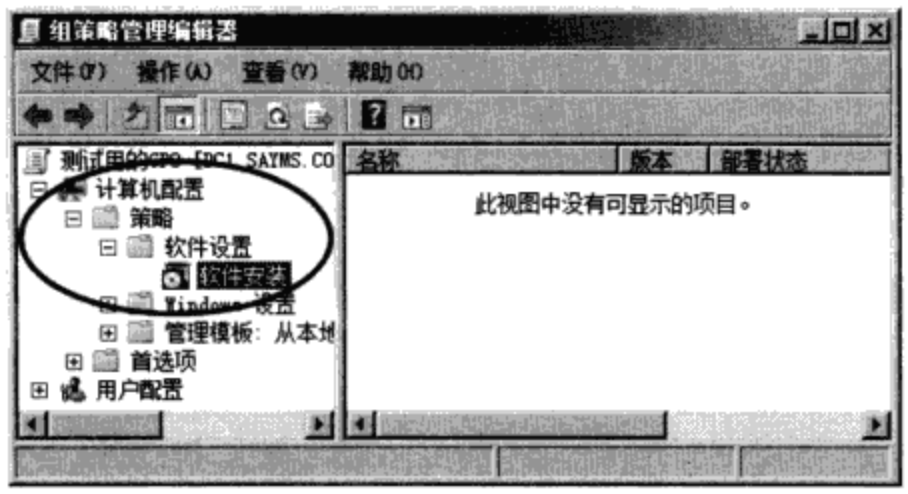


图 5-15

- 请设置软件默认的存储位置:【对着图 5-15中的**软件安装**单击右键➲属性➲默认程序数据包位置】。
- 在图 5-16中选择**已分配**。由图可看出只能**分配**给计算机，无法**发布**给计算机。

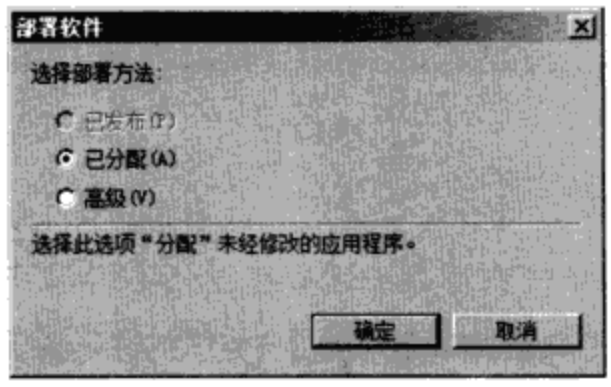


图 5-16

5-4 软件升级和重新部署

我们可以通过软件部署来将旧版的软件升级或安装更新程序。

5-4-1 软件升级

您可以将已经部署给用户或计算机的软件，升级到较新的版本，而升级的方式有以下两种：

Download at http://www.pin5i.com/

- 强制升级：此时不论是发布或分配新版的软件，原来旧版的软件都会被自动升级，不过事实上只是安装新版软件的快捷方式而已，用户必须选择此快捷方式或需要运行此软件时，系统才会开始完整的安装这个新版本的软件。
- 选择性升级：此时无论是发布或分配新版的软件，原来旧版的软件都不会被自动升级，用户必须通过**控制面板**来安装这个新版本的软件。

提示

分配给计算机的软件，只可以选择**强制升级**。

以下将说明如何部署新版本软件（假设是AkelPad443），以便将用户的旧版本软件（假设是AkelPad374）升级，同时假设是要针对组织单位**业务部**内的用户，而且是通过**测试用的GPO**来练习。

STEP 1 先将新版软件复制到软件发布点内，如图 5-17所示的**AkelPad443**文件夹。

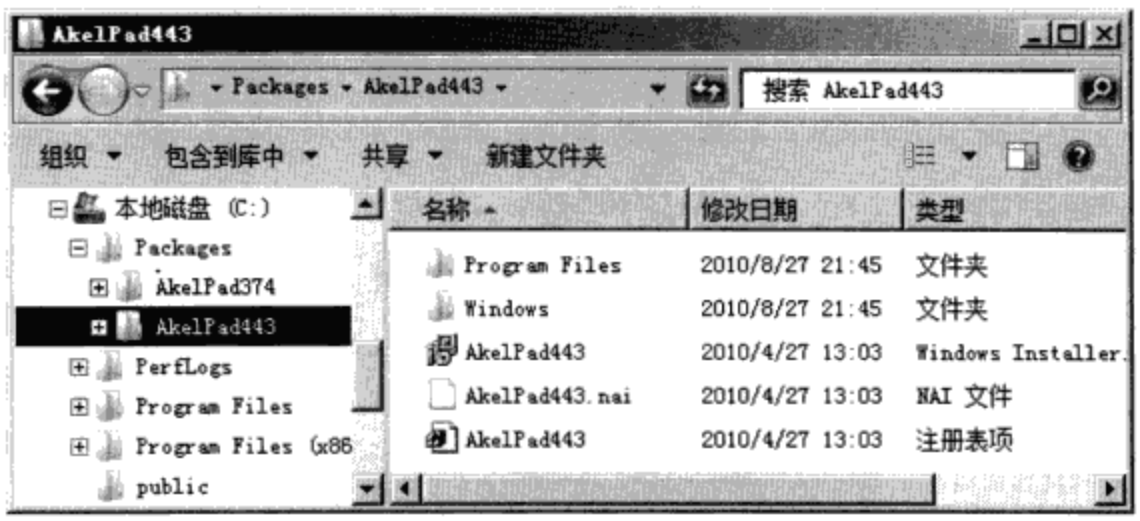


图 5-17

STEP 2 请在域控制器上，通过【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑➲在图 5-18中展开**用户配置**➲策略➲**软件设置**➲对着**软件安装**右击➲**新建**➲**数据包**】的方式进行设置。

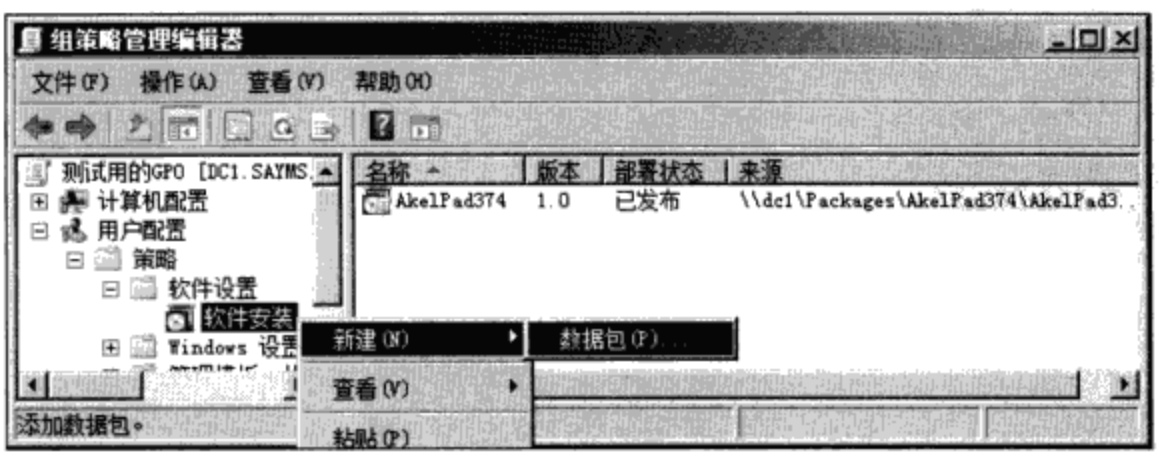


图 5-18

STEP 3 在图 5-19中选择新版本的Windows Installer Package，也就是AkelPad443.msi（扩展

Download at http://www.pin5i.com/

名.msi默认会被隐藏），然后单击打开按钮。

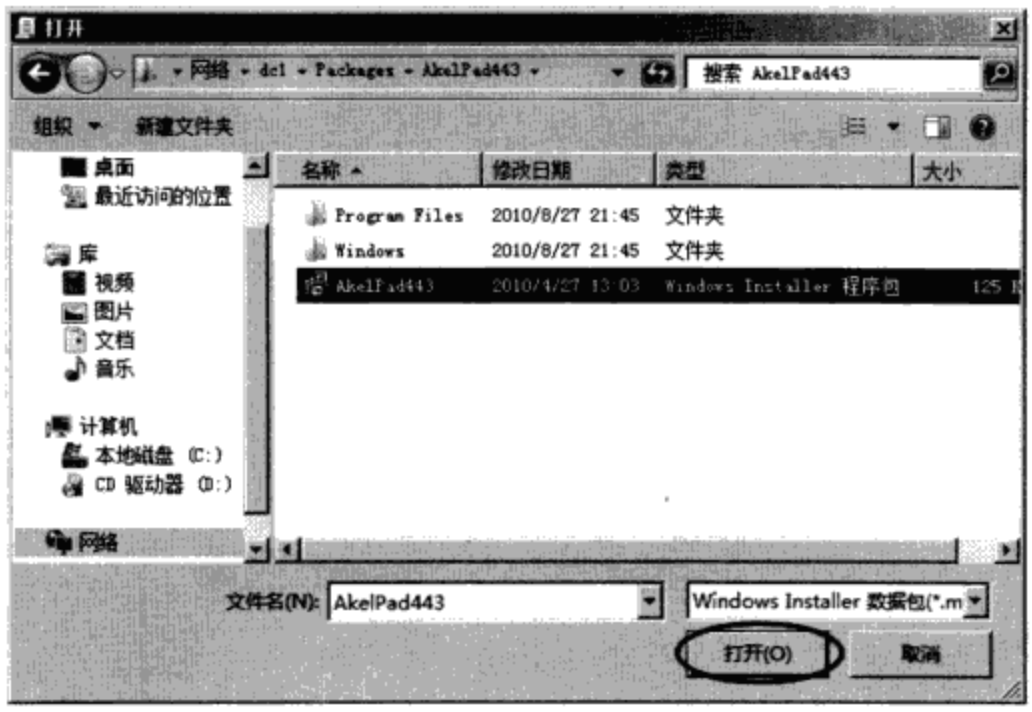


图 5-19

STEP 4 在图 5-20中选择**高级**单选按钮后单击确定按钮。

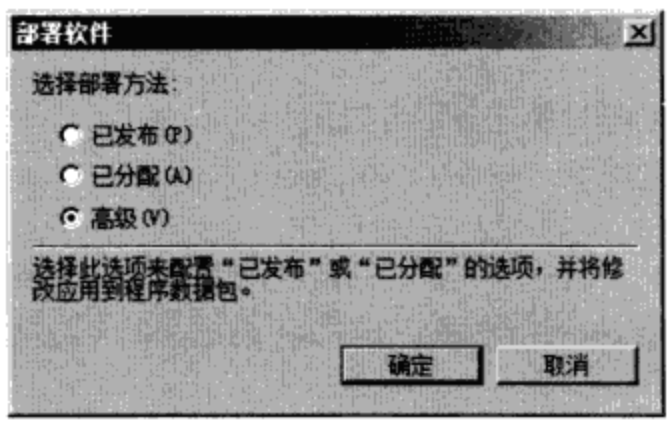


图 5-20

STEP 5 在图 5-21中单击**升级**标签，如果要强制升级的话，请选择**现有程序包所需的升级**复选框，否则直接单击添加按钮即可。

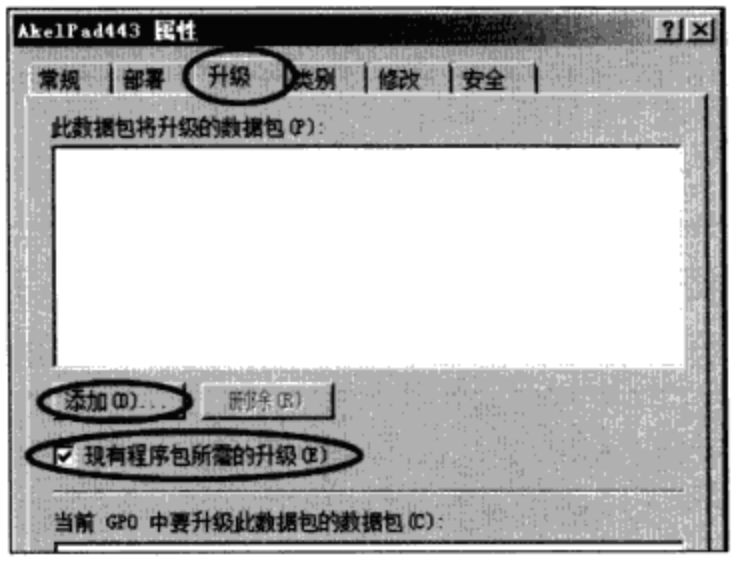


图 5-21

Download at http://www.pin5i.com/

STEP 6 在图 5-22中选择要被升级的旧版软件AkelPad374后单击确定按钮。

提示

在图中您也可以选择将其他GPO所部署的旧软件升级。另外还可以通过对话框的最下方来选择先卸载旧版软件，再安装新版软件，或是直接将旧版软件升级。

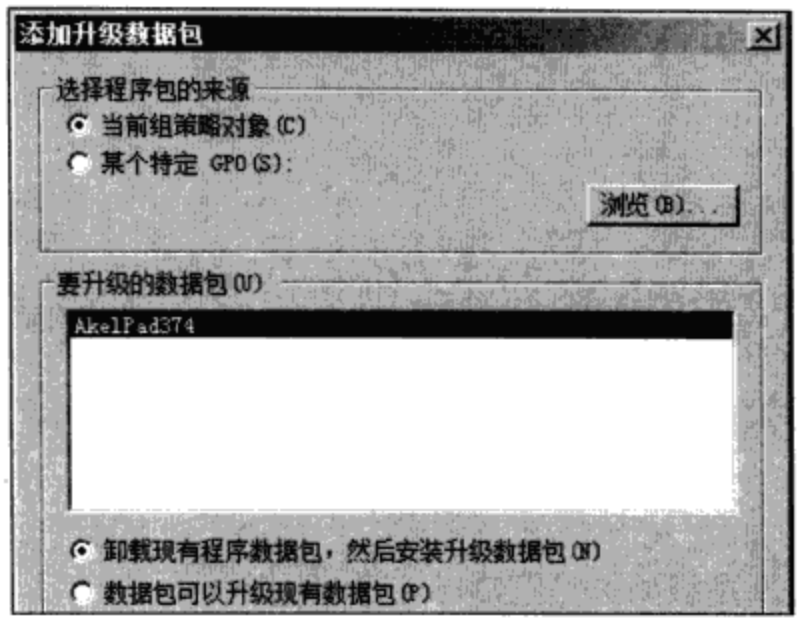


图 5-22

STEP 7 返回到前一个对话框时单击确定按钮。

STEP 8 图 5-23为完成后的界面，其中AkelPad443左边的向上箭头，表示它是用来升级的软件。

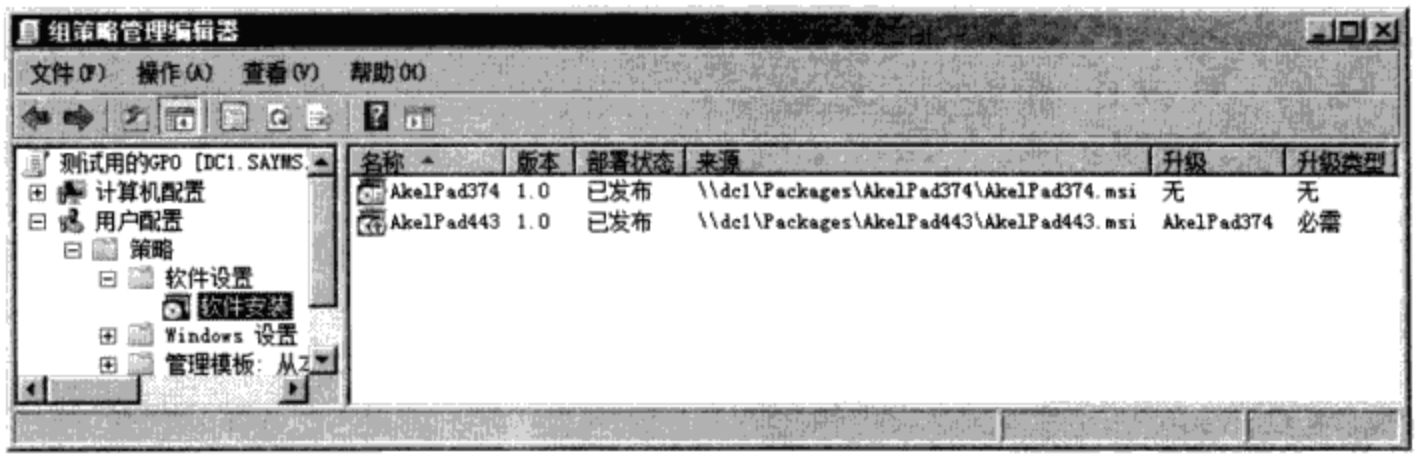


图 5-23

提示

从右边的**升级**和**升级类型**列也可知道它是用来将AkelPad374强制升级，不过默认并不会显示这两列，必须通过【单击上方的**查看**菜单➲添加/删除列】的方法来添加这两列。

STEP 9 由于我们是选择强制升级，所以当用户选择【开始➲所有程序➲AkelPad➲AkelPad】来运行此程序时，其计算机便会自动将AkelPad374升级为AkelPad443。

Download at http://www.pin5i.com/

5-4-2 重新部署

一个已部署的软件，如果之后软件厂商有发布Service Pack（服务包）或修补程序的话，则您可以通过**重新部署**来为此软件安装Service Pack或修补程序。

如果已经部署的软件因为感染计算机病毒或其他因素而无法正常运行的话，也可以通过**重新部署**来让客户端重新安装已部署的软件。

如果要将Service Pack或修补程序重新部署的话，请先更新软件发布点内的Windows Installer Package文件夹内的文件，而更新方法需视Service Pack或修补程序的文件类型而定。

- Windows Installer Package，也就内含附文件名为.msi的安装程序：则请直接将这些文件复制到软件发布点的Windows Installer Package文件夹内，也就是将旧的文件覆盖掉即可。
- Windows Installer Patch，也就是附文件名为.msp的修补文件：则请运行以下命令来更新软件发布点的Windows Installer Package文件夹内的文件：

  `msiexec /p .msp 文件的路径和文件名 /a .msi 文件的路径和文件名`

  例如修补文件是存储在 C:\Test 文件夹内，文件名为 Patch.msp，而 Windows Installer Package 是存储在 C:\Packages\AkelPad443 文件夹内，文件名为 AkelPad443.msi，则所需运行的命令为：

```
Msiexec /p C:\Test\Patch.msp /a C:\Packages\AkelPad443\AkelPad443.msi
```

完成文件更新后，请如图 5-24所示，通过【对着该软件单击右键➲所有任务➲重新部署应用程序】的方式进行操作即可。

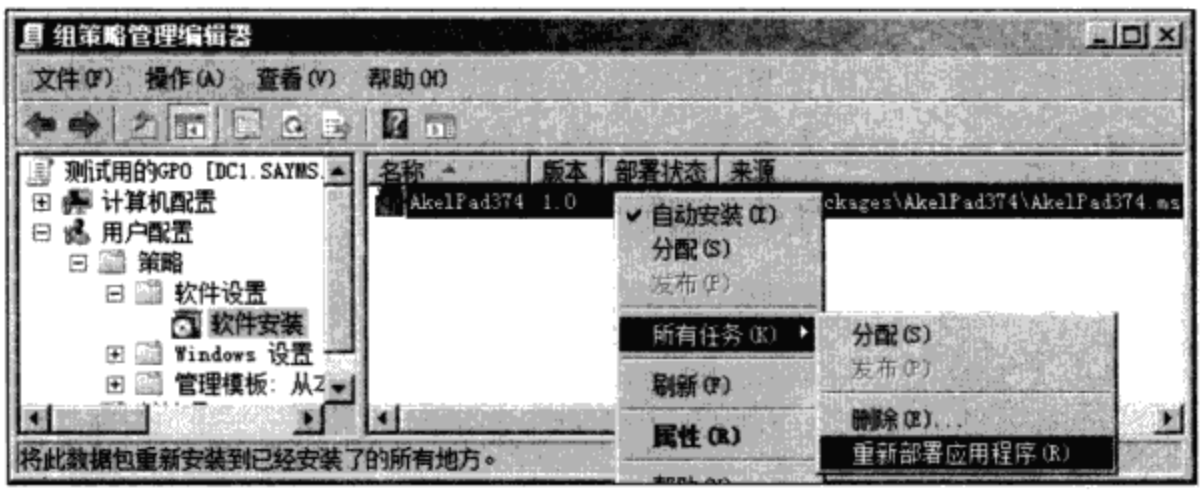


图 5-24

重新部署软件后，用户的计算机何时才会安装该Service Pack或修补程序呢？可分为以下三种情况：

- 若该软件是分配给用户，则下一次用户登录时，该软件的快捷方式和注册表都会被更

Download at http://www.pin5i.com/

新，不过需等用户再次运行此软件时，才会开始安装。

- 若该软件是分配给计算机，则下一次计算机重新启动时就会安装。
- 若该软件是发布给用户，而且用户也已经安装了此软件，则下一次用户登录时，该软件的快捷方式和注册都会被更新，不过需等用户再次运行此软件时才会安装。

5-5 部署Microsoft Office

以下将分别说明如何部署Microsoft Office 2003和Microsoft Office 2007。

5-5-1 部署Microsoft Office 2003

我们可以将整套Office 2003部署给用户或计算机，也可以通过**转型文件**（Transform File）来仅部署其中的Word、PowerPoint、Excel等个别软件。**转型文件**的扩展名为**.mst**，又称为**软件修正文件**（Software Modifications File）。

1. 将 Microsoft Office 2003 安装文件复制到软件发布点

请使用以下步骤来将Microsoft Office 2003 CD内的安装文件复制到软件发布点（例如我们前面所使用的C:\Packages）。

提示

您也可以直接使用**Windows资源管理器**将文件复制到软件发布点，不过用户在安装时需要自行输入**公司名称**和**产品标识符**。

STEP 1 请到存放**软件发布点**的计算机上确定存储软件发布点的磁盘具有足够的空间。

STEP 2 选择【开始➲运行➲单击浏览按钮➲浏览到Office 2003 CD➲双击SETUP.EXE➲如图 5-25所示附上**/a**参数➲单击确定按钮】。

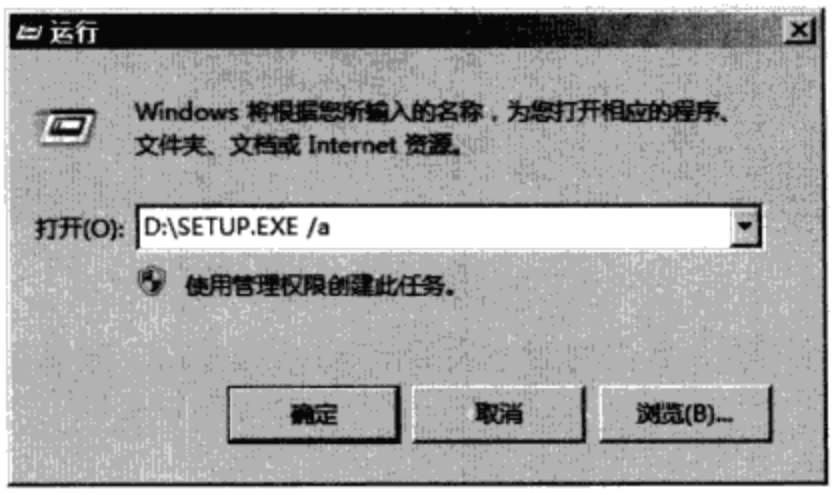


图 5-25

Download at http://www.pin5i.com/

STEP 3 在图 5-26中输入单位、安装位置、产品密钥等相关数据后单击下一步按钮。

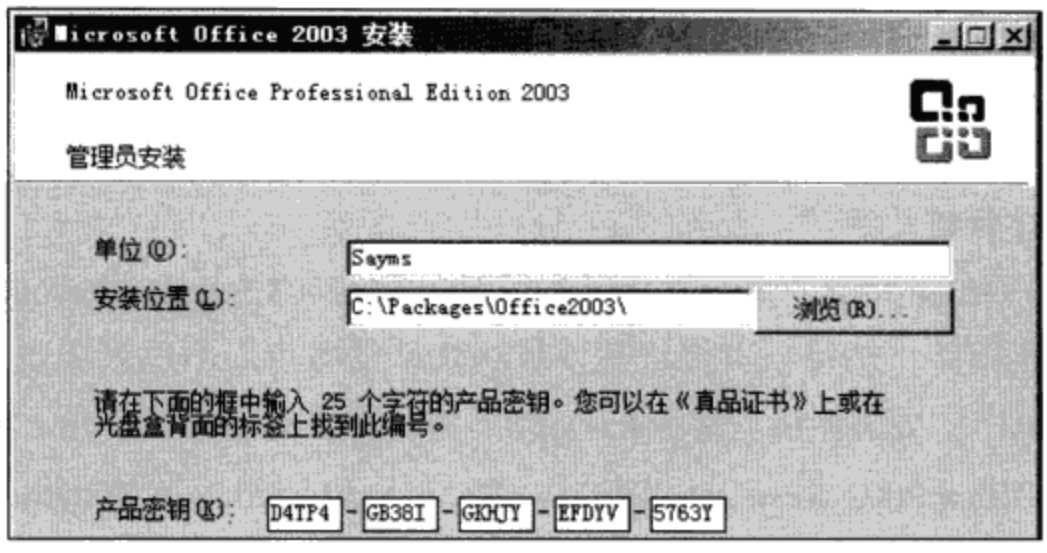


图 5-26

提示

此处输入适当的产品密钥后，用户在安装Office 2003时，就不会显示要求输入产品密钥的界面，同时也不需要激活（Activate）此产品。图中的产品密钥是随意设置的。

STEP 4 出现最终用户许可协议界面时选择**我接受《许可协议》中的条款**后单击安装按钮。

STEP 5 之后安装程序便会将Microsoft Office 2003的安装文件复制到软件发布点，如图 5-27所示为完成后的界面。

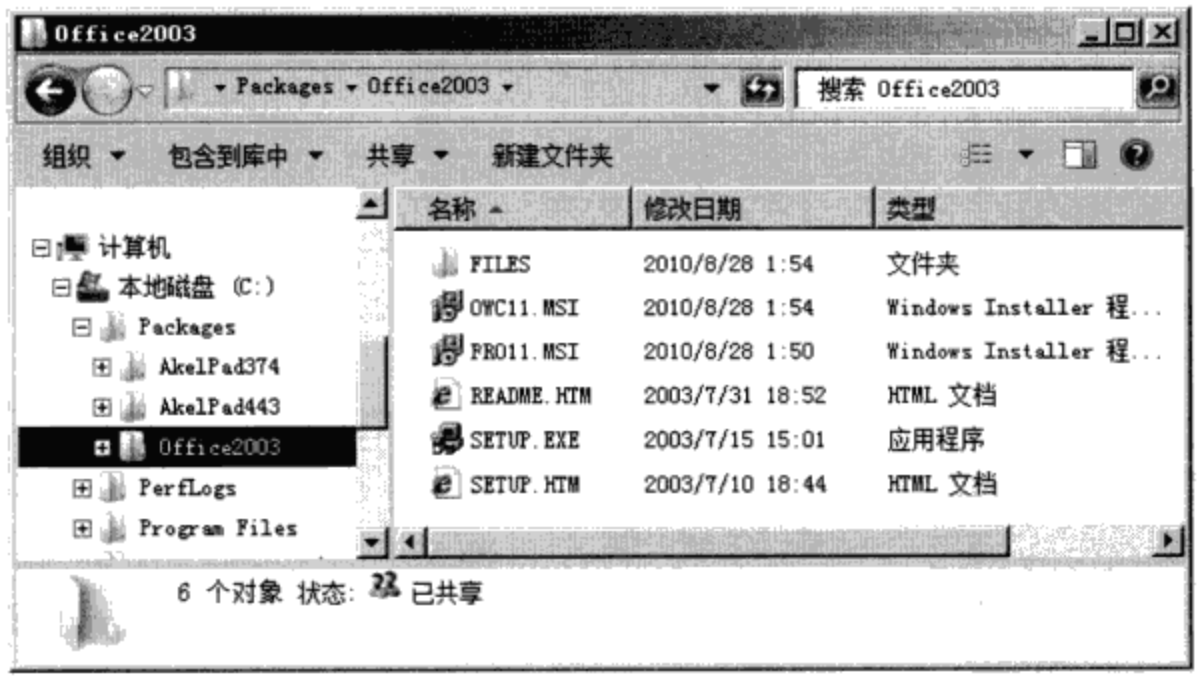


图 5-27

2. 部署整套 Microsoft Office 2003

要部署整套Office 2003的话，请选择将图 5-27中的PRO11.MSI（扩展名.msi默认会被隐藏）部署给用户或计算机即可，由于其部署方法与前面部署一般Windows Installer Package相同，故此处不再重复说明。

Download at http://www.pin5i.com/

3. 部署 Microsoft Office 2003 中的个别软件

以下将说明如何创建一个限定用户只能够安装PowerPoint 2003的**.mst转型文件**，然后将搭配此**转型文件**的Microsoft Office 2003部署给用户。

（1）创建.mst 转型文件

创建Microsoft Office 2003的**.mst**文件需要用到Office 2003 Editions Resource Kit Tools，请到微软网站下载此程序。您可以直接将其安装到软件发布点，不过只需安装其中的Custom Installation Wizard即可。安装完成后选择【开始➲所有程序➲ Microsoft Office ➲Microsoft Office Tools➲Microsoft Office 2003 Resource Kit Tools➲Custom Installation Wizard】。以下仅针对创建**.mst转型文件**的步骤做必要的说明，其他步骤都采用默认值。

> **提示**
>
> 我们可以在**.mst转型文件**内做更多的详细设置，例如选择安装文件夹、是否要额外安装其他文件、新建或删除快捷方式等。

STEP 1 请在图 5-28中输入或浏览到Office 2003的**.msi**文件，它被我们存储在软件发布点内，而且**.msi**的文件名是PRO11.MSI，然后选择**Create a new MST file**单选按钮。

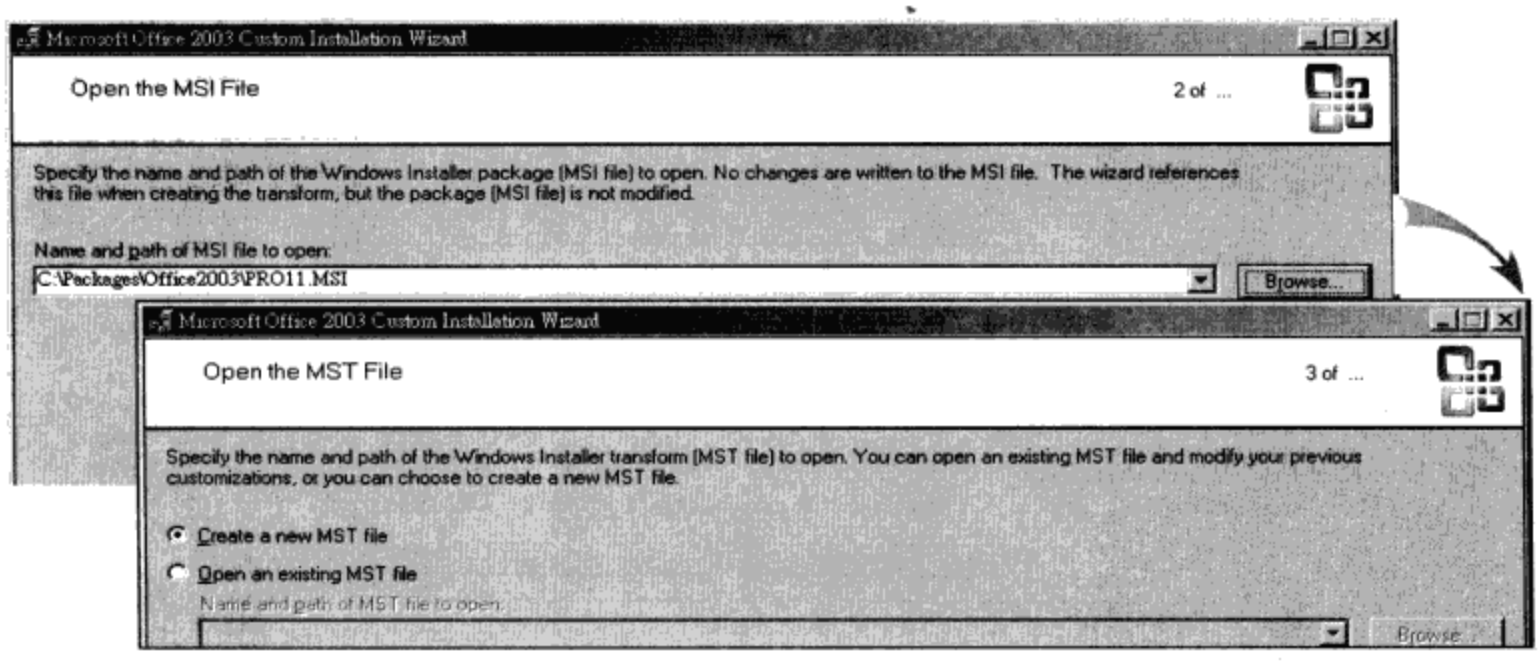


图 5-28

STEP 2 在图 5-29中设置**.mst转型文件**的文件名和路径，图中我们将其文件名设置为PowerPointOnly.MST，并将其存储到软件发布点内。

Download at http://www.pin5i.com/

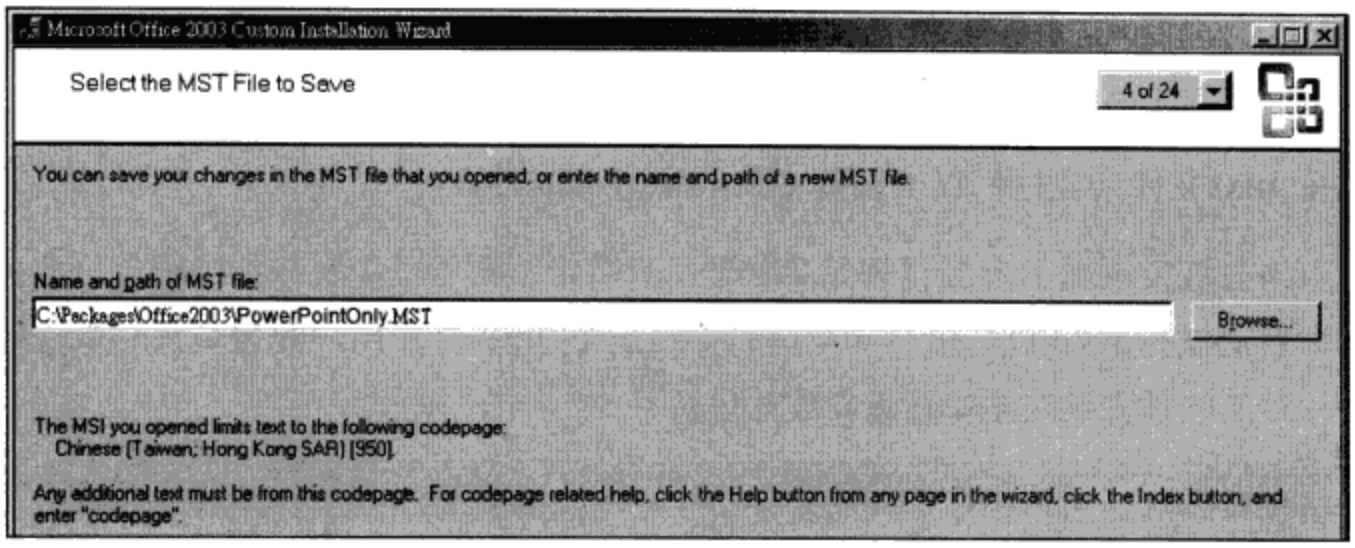


图 5-29

STEP 3 在图 5-30中只选择安装Microsoft Office PowerPoint、Office工具和Office共享的功能，其他的选择不安装、隐藏和锁定。

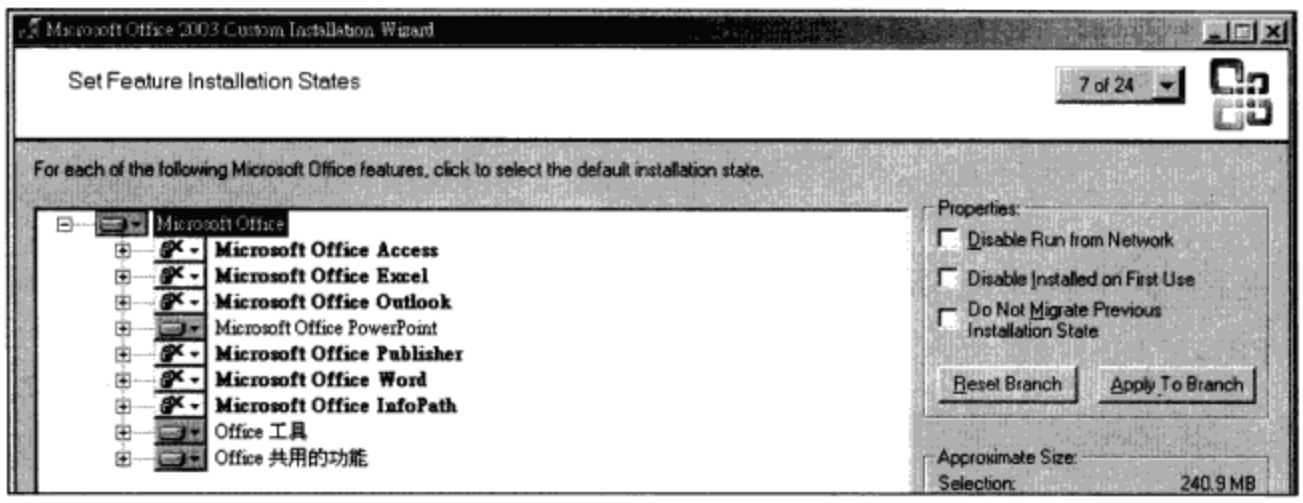


图 5-30

STEP 4 图 5-31中的PowerPointOnly.MST为所创建的**.mst转型文件**。

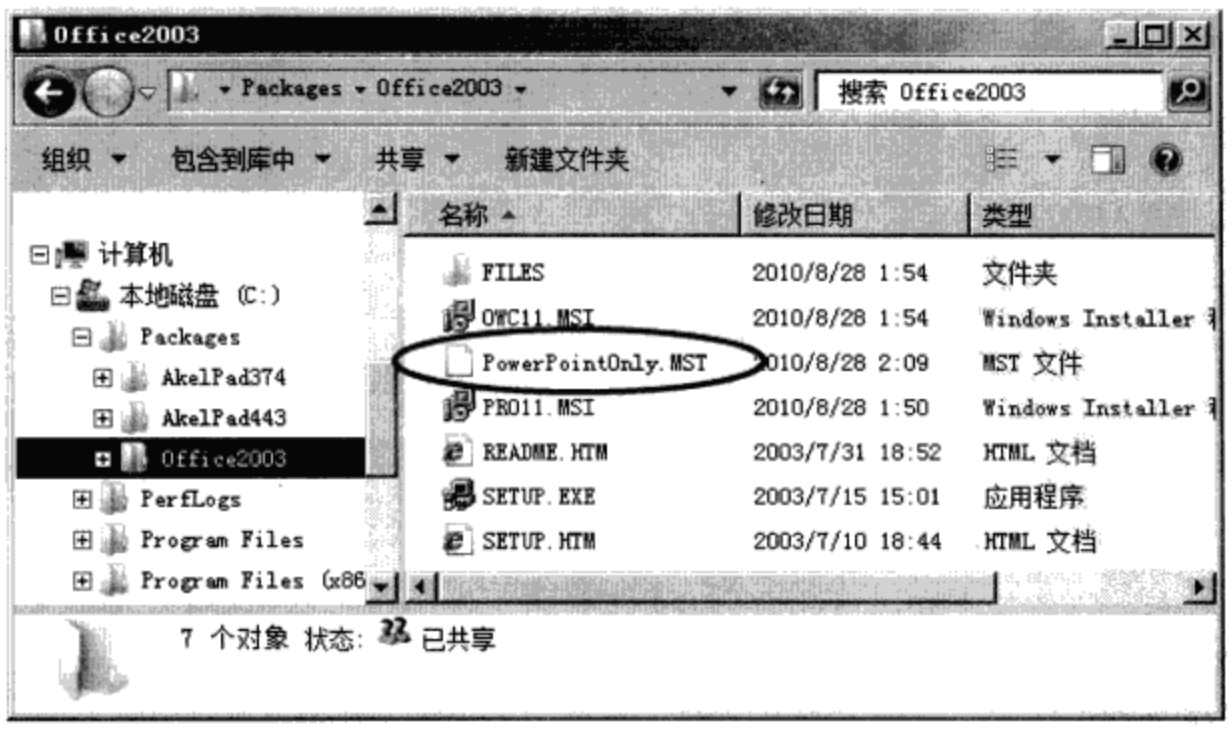


图 5-31

Download at http://www.pin5i.com/

（2）通过转型文件来部署 PowerPoint 2003

我们要通过之前的**测试用的GPO**来将Microsoft Office 2003发布给组织单位**业务部**中的用户，并搭配**.mst**文件来让他们仅安装其中的PowerPoint 2003。

STEP 1 请在域控制器上选择【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑➲在图 5-32中展开**用户配置**➲策略➲软件设置➲对着**软件安装**右击➲新建➲数据包】。

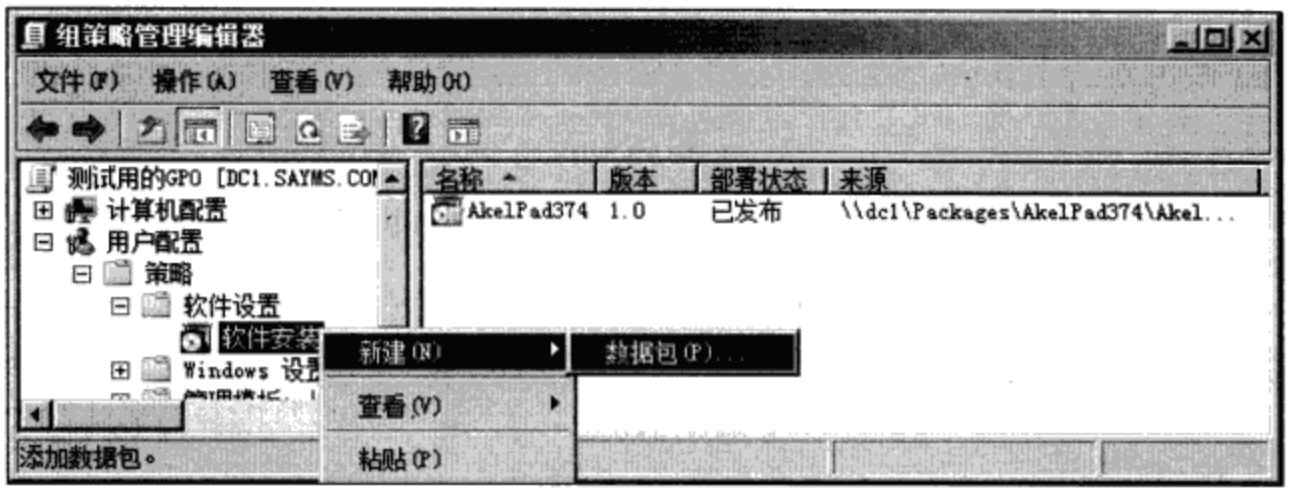


图 5-32

STEP 2 在图 5-33 中选择Microsoft Office 2003 中Windows Installer Package的安装文件PRO11.MSI（扩展名.msi默认会被隐藏），然后单击打开按钮。

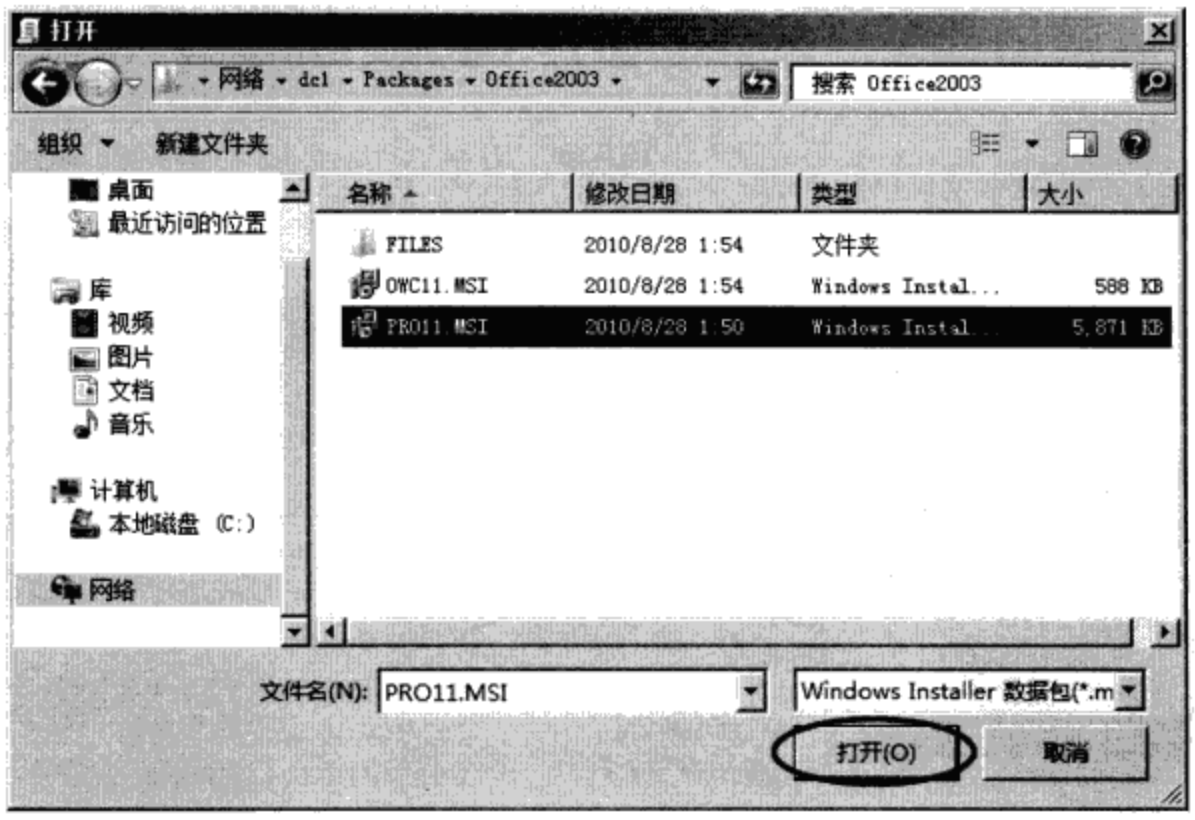


图 5-33

STEP 3 在图 5-34中选择**高级**单选按钮后单击确定按钮。

Download at http://www.pin5i.com/

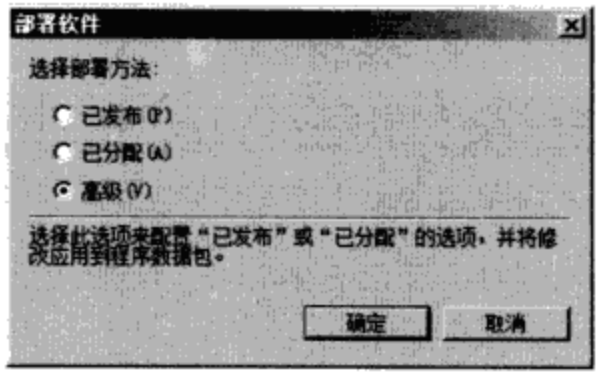


图 5-34

注意

您必须在此时选择**高级**单选按钮，因为一旦部署后就无法更改。

STEP 4 单击图 5-35中**修改**标签之下的添加按钮。

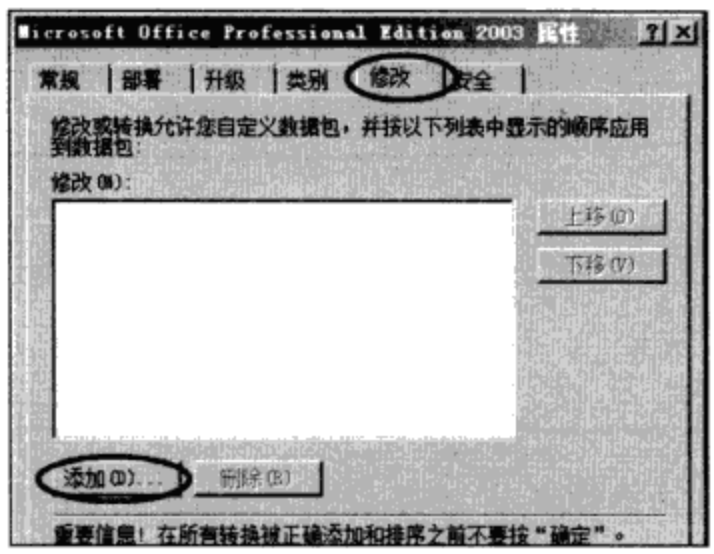


图 5-35

STEP 5 在图 5-36中选择我们所创建的**PowerPointOnly.mst**文件后单击打开按钮。

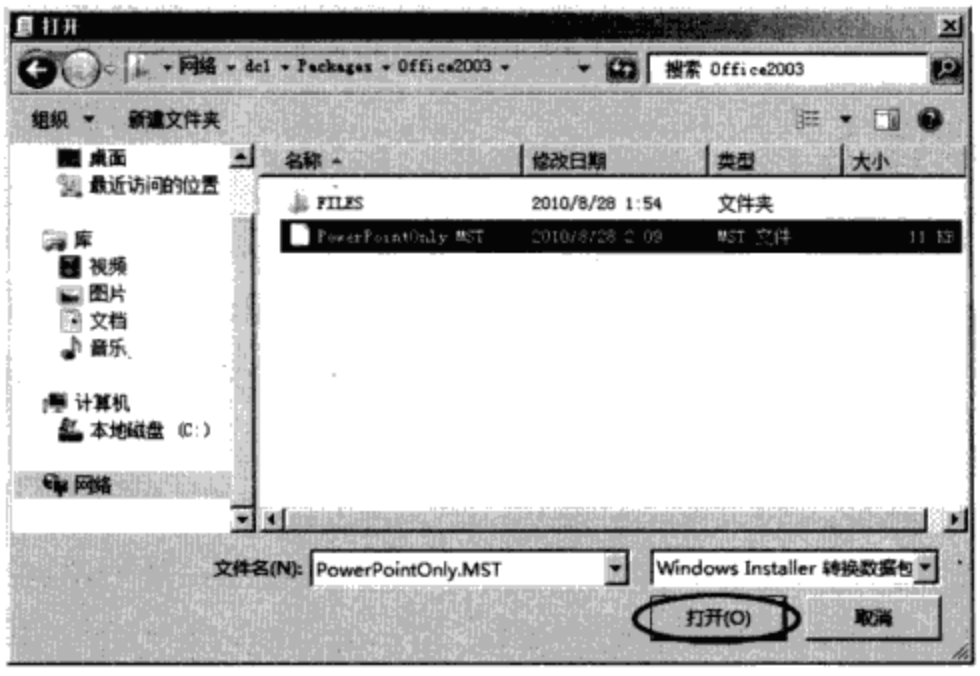


图 5-36

Download at http://www.pin5i.com/

STEP 6 返回到图 5-37的对话框时单击**确定**按钮。

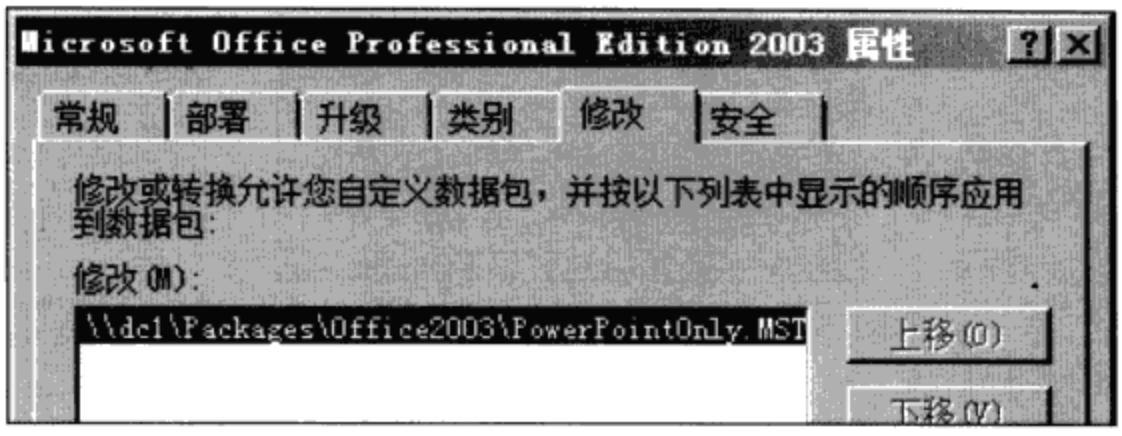


图 5-37

STEP 7 图 5-38为设置完成后的界面。

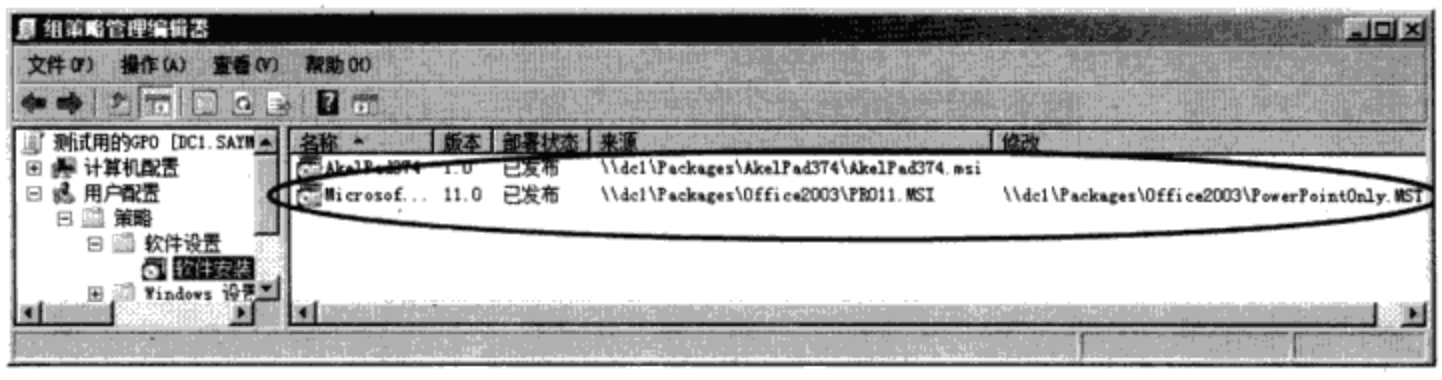


图 5-38

提示

默认并不会显示图中右边的**修改**列，您必须通过【单击上方的**查看**菜单➲添加/删除列】的方法来添加此列。

STEP 8 请使用组织单位**业务部**内的用户账户登录，然后通过**控制面板**来练习安装这个搭配**.mst转型文件**的Microsoft Office 2003，用户只能够安装PowerPoint，其他的会被锁定、无法选择。

5-5-2 部署Microsoft Office 2007

由于Microsoft Office 2007内的个别应用程序，例如Word、PowerPoint、Excel等，都是单独的Windows Installer Package，因此我们可以直接部署这些个别软件，不需要搭配**.mst转型文件**。

Microsoft Office 2007仅支持分配给计算机，不支持分配与发布给用户，如果您将Microsoft Office 2007分配或发布给用户的话，用户将无法安装。将Microsoft Office 2007分配给计算机后，这些计算机启动时就会自动安装分配的软件，但是部分的安装与设置程序必须等用户登录后才会运行。以下假设您所使用的是Microsoft Office 2007中文版DVD。

Download at http://www.pin5i.com/

> **提示**
>
> 若您是通过Microsoft Office 2007多国语言版来部署，而且不是部署U.S English版，例如部署中文版的话，则仍然需要搭配光盘内的**ShellUI.MST转型文件**。除了**ShellUI.MST转型文件**外，Microsoft Office 2007已经不再支持其他的**转型文件**。

1. 将 Microsoft Office 2007 安装文件复制到软件发布点

请在软件发布点内为Microsoft Office 2007创建一个专属文件夹，然后将Microsoft Office 2007 DVD内所有文件夹和文件复制到此文件夹内，如图 5-39所示我们将其复制到Office 2007文件夹内。

> **提示**
>
> 若有Microsoft Office 2007更新文件的话，请将这些扩展名为.msp的更新文件复制到此文件夹之下的Updates文件夹内。



图 5-39

2. 将 Microsoft Office 2007 分配给计算机

如果您要部署整个Office 2007的话，请部署图 5-39中文件夹Enterprise.WW内的Enterprise.WW.msi文件；如果仅要部署Office 2007中个别软件的话，请部署该软件所在文件夹

Download at http://www.pin5i.com/

内的.msi文件，例如若要部署PowerPoint 2007的话，请部署PowerPoint.WW\PowerPoint.msi文件。

您可以通过配置文件Config.xml来自定义部署项目，例如安装界面的显示级别（完整、基本、无）、选择安装文件夹、输入产品密钥等。整套Office 2007的配置文件位于Enterprise.WW\Config.xml；而每一套个别软件的文件夹内都各自有一个Config.xml文件，举例来说，PowerPoint 2007的配置文件是位于PowerPoint.WW文件夹之内。

> **提示**
>
> Config.xml文件的详细说明可到微软下载相关文件，请使用关键字Config.xml file in the 2007 Office system来查找。

我们要通过之前的**测试用的GPO**来将Microsoft Office 2007中32位版的PowerPoint 2007分配给组织单位**业务部**中的计算机。

STEP 1 为了让用户在第一次运行PowerPoint 2007时不需要输入产品密钥，因此请先将产品密钥输入到PowerPoint 2007的Config.xml配置文件内：请到存储软件发布点的计算机上使用记事本打开Office2007\PowerPoint.WW\Config.xml文件，然后如图 5-40所示将PIDKEY前后的批注符号 <!-- 与 --> 删除，将BCDFGHJKMPQRTVWXY2346789B字符串替换成您的产品密钥（图中产品密钥是随意输入的范例，实际上您必须输入有效的产品密钥才可以部署）。

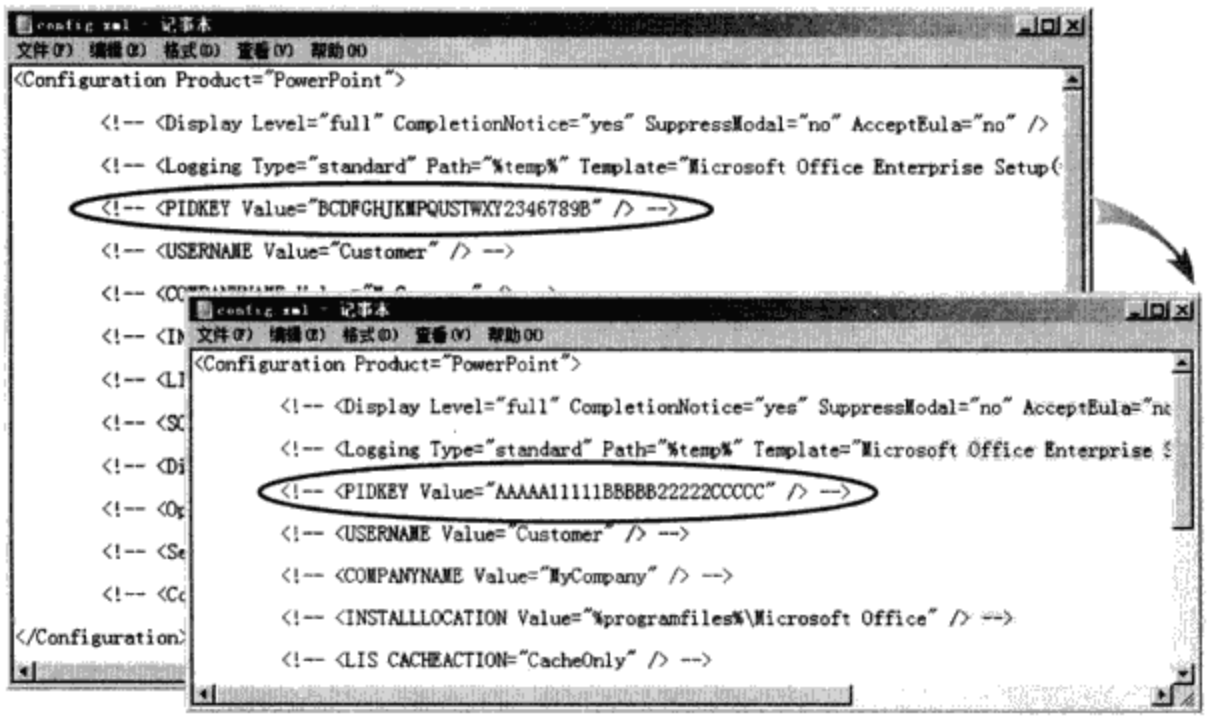


图 5-40

STEP 2 请在域控制器上选择【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑➲在图 5-41中展开**计算机配置**➲策略➲软件设置➲对着**软件安装**右击➲新建➲数据包】。

Download at http://www.pin5i.com/

注意

Office 2007仅支持分配给计算机，不支持发布和分配给用户。

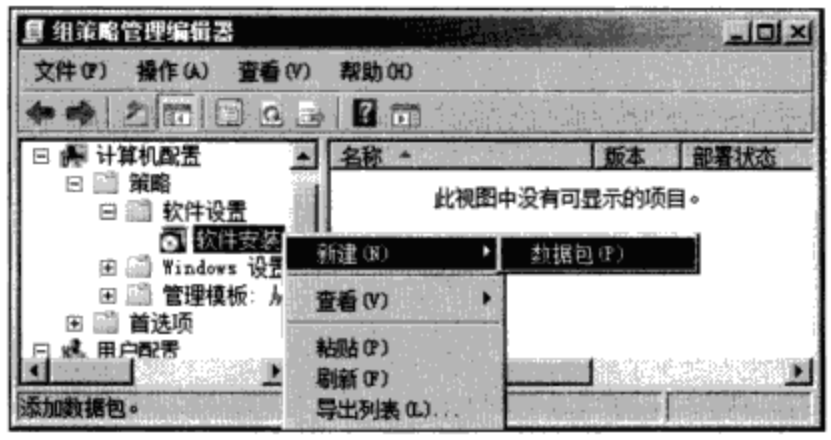


图 5-41

STEP 3 在图 5-42中选择Office2007\PowerPoint.WW文件夹内的Windows Installer Package PowerPointWW.msi（扩展名.msi默认会被隐藏），然后单击打开按钮。

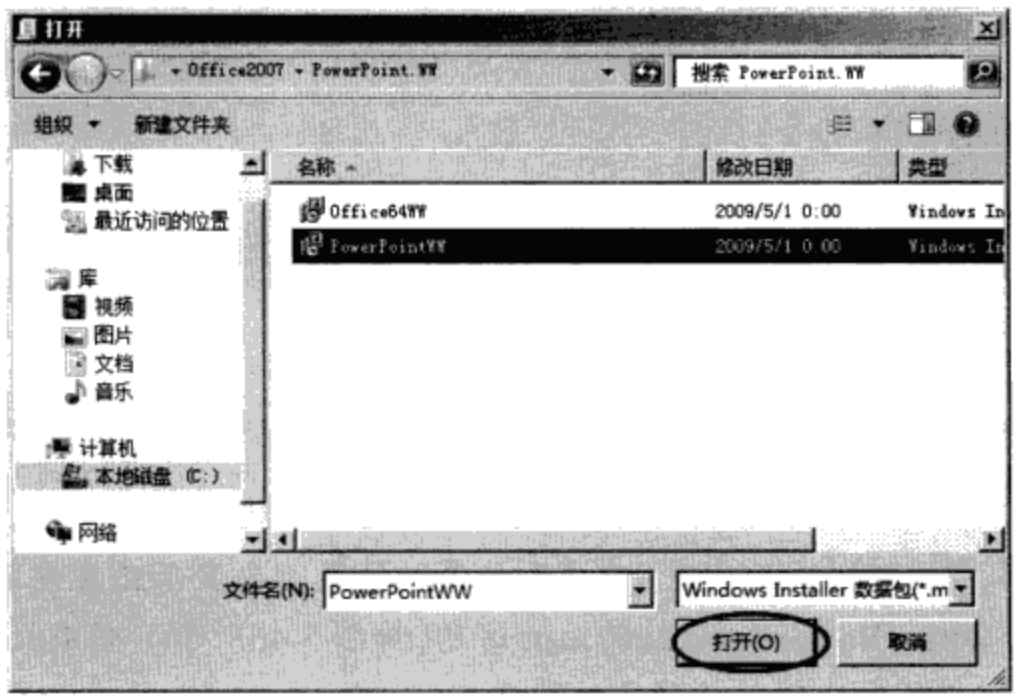


图 5-42

STEP 4 在图 5-43中选择**已分配**单选按钮后单击确定按钮。

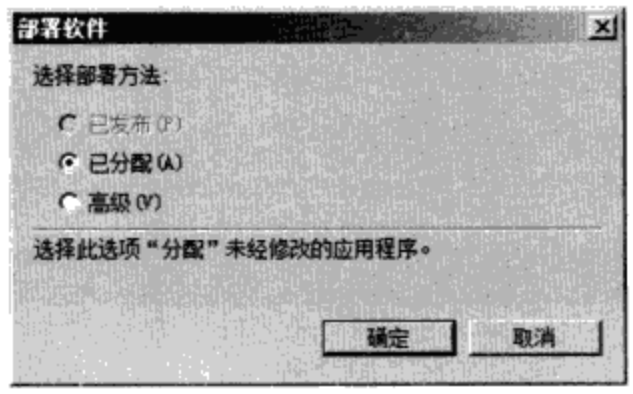


图 5-43

Download at http://www.pin5i.com/

注意

若在Office2007\PowerPoint.WW\Config.xml配置文件内输入错误的产品密钥的话，则此时会出现如图 5-44所示的对话框。

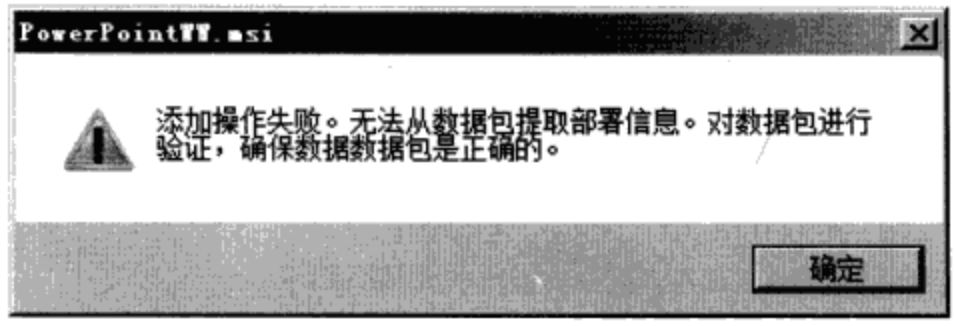


图 5-44

STEP 5 图 5-45为完成后的界面。

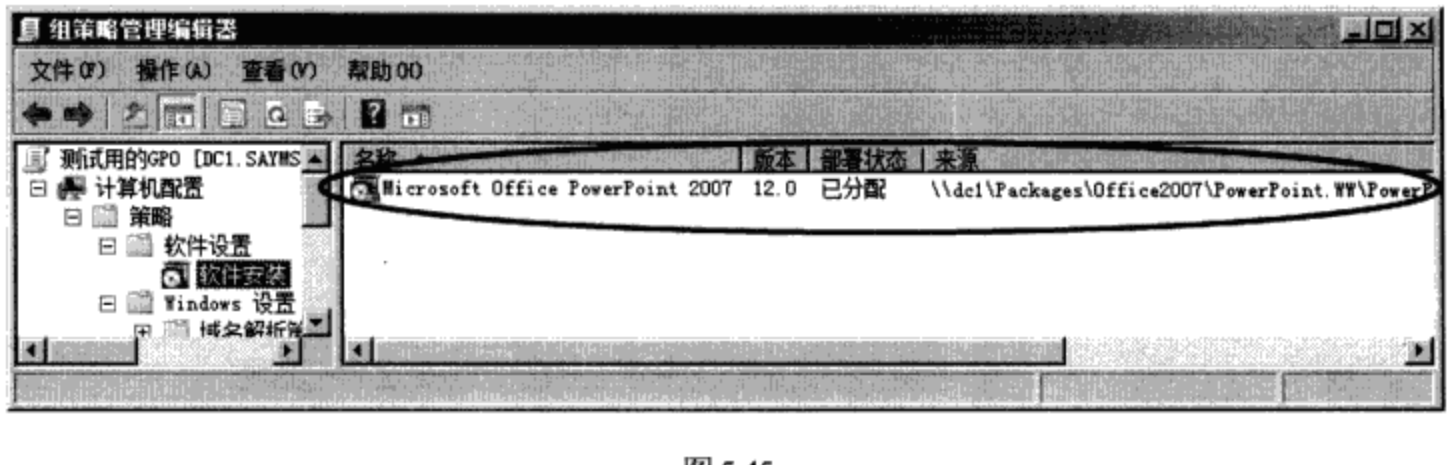


图 5-45

完成分配后，请到组织单位**业务部**内的任何一台计算机上做测试，也就是将此计算机重新启动（可能需要重新启动多次）。

- 如果此计算机是Windows XP：则应用计算机设置时会显示**正在安装经过管理的软件 Microsoft Office PowerPoint 2007...**的信息（如图 5-46所示）。完成此阶段的安装后（需等一段时间）便会出现请求登录的界面。



图 5-46

- 如果此计算机是Windows 7或Windows Vista：则应用计算机设置时会安装PowerPoint

Download at http://www.pin5i.com/

2007，并显示**请稍候...** 信息，完成此阶段的安装后（需等一段时间）便会出现要求登录的界面。

用户登录后，安装程序会继续完成后面的设置工作，而用户在开始第一次使用某些功能时，系统也会在此时安装这些功能。

5-6 发布ZAP应用程序

您可以通过创建一个扩展名为**.ZAP**的文件来将一般非Windows Installer Package（非.msi）的软件部署给用户。在部署**.ZAP**文件时请注意以下事项：

- 它只能够被发布给用户，无法分配给用户与计算机。
- 不具备自动修复等Windows Installer Package才有的特色。
- 因为它不是Windows Installer Package，故不是通过具备安装权限的Windows Install Services来安装，因此若该应用程序的安装程序会更改系统设置的话（例如更改注册表），则用户必须具备系统管理员权限。
- 不支持.mst转型文件。
- 用户第一次开始使用尚未安装的功能时，系统也无法自动安装此功能。
- 若客户端为64位系统，而您要部署的应用程序为32位的话，请确认该程序可以在64位系统上正常的安装和运行，因为32位**.ZAP**应用程序在64位系统上无法正常使用的概率较高。
- 除非另外设置（后述），否则32位的**.ZAP**应用程序并不会出现在64位系统的**控制面板**的**添加/删除程序**或**程序**内。

此处我们以AkelPad 4.4.3为例来说明如何将非Windows Installer Package的软件发布给用户。AkelPad 4.4.3的执行文件为AkelPad-4.4.3-setup.exe。假设我们要针对组织单位**业务部**内的**测试用的GPO**来设置。

STEP 1 请先在软件发布点内为AkelPad 4.4.3创建一个文件夹，例如AkelPad443ZAP，然后将其安装文件AkelPad-4.4.3-setup.exe复制到此文件夹内。

STEP 2 使用**记事本**创建一个扩展名为**.ZAP**的文件，其内容如图 5-47所示。

- 第一行请输入[Application]。
- FriendlyName: 为此应用程序设置一个名称，并在前后附加双引号。
- SetupCommand: 输入AkelPad 4.4.3执行文件的路径和文件名，注意前后请附加重复的双引号。

Download at http://www.pin5i.com/

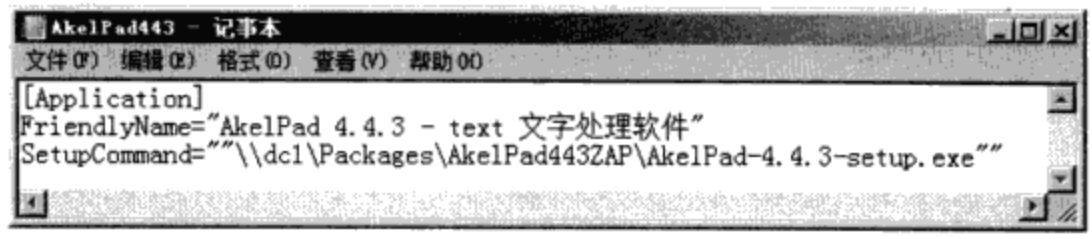


图5-47

提示

1. 若应用程序需附加参数的话，则使用一组双引号即可，例如：

```
SetupCommand = "\\dc1\Packages\Test\Setup.exe" /q
```

2. 若.ZAP文件和软件安装文件（AkelPad-4.4.3-setup）是位于同一个文件夹内的话，则在SetupCommand处直接输入软件安装文件名即可，可以不需要输入路径，例如：

```
SetupCommand = "AkelPad-4.4.3-setup.exe"
```

STEP 3 使用**另存为**来存储此文件，请如图5-48所示直接将文件存储到软件发布点，图中我们将文件名设置为AkelPad443.ZAP，注意扩展名必须是.ZAP，因此请在文件名前后附加双引号，否则**记事本**会自动在文件名后另外加上.txt，也就是AkelPad443.ZAP.txt，而不是我们所需要的AkelPad443.ZAP。

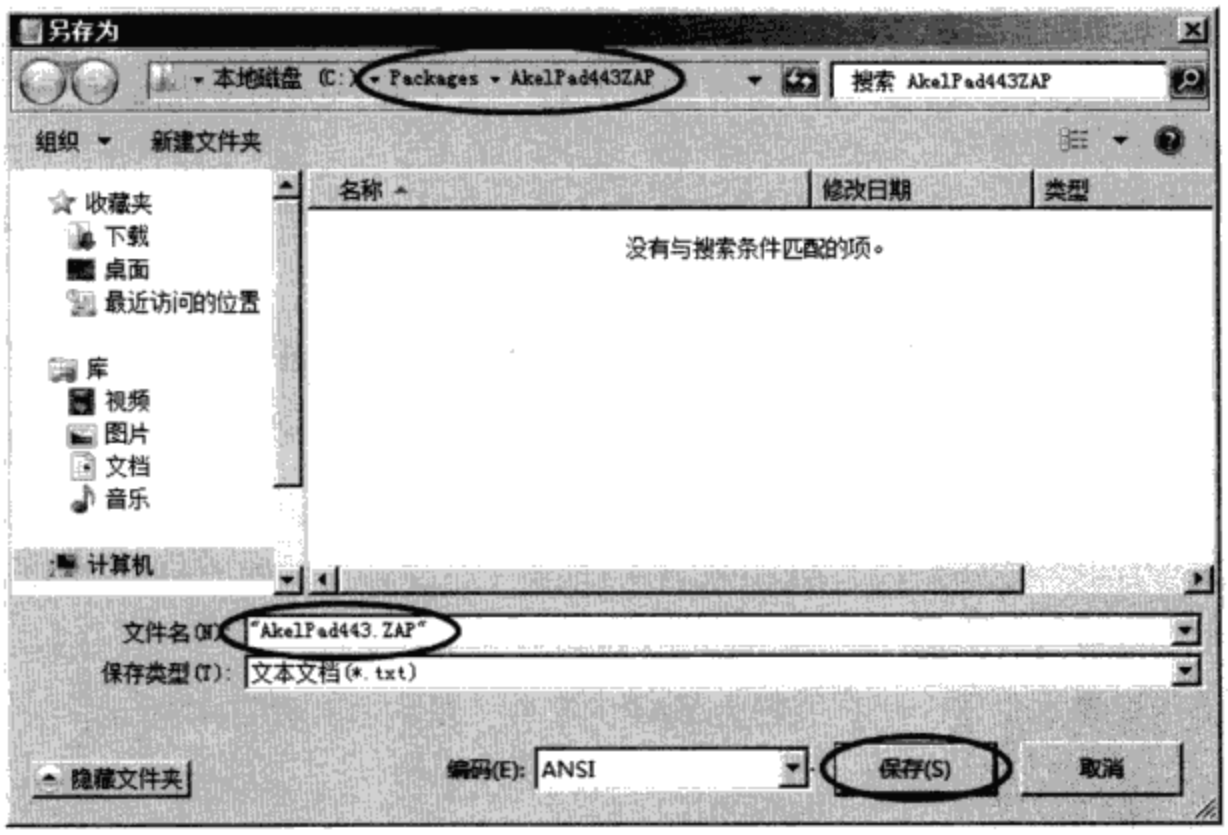


图5-48

STEP 4 如图5-49所示确认软件发布点内已经包含.ZAP文件和安装文件。

Download at http://www.pin5i.com/

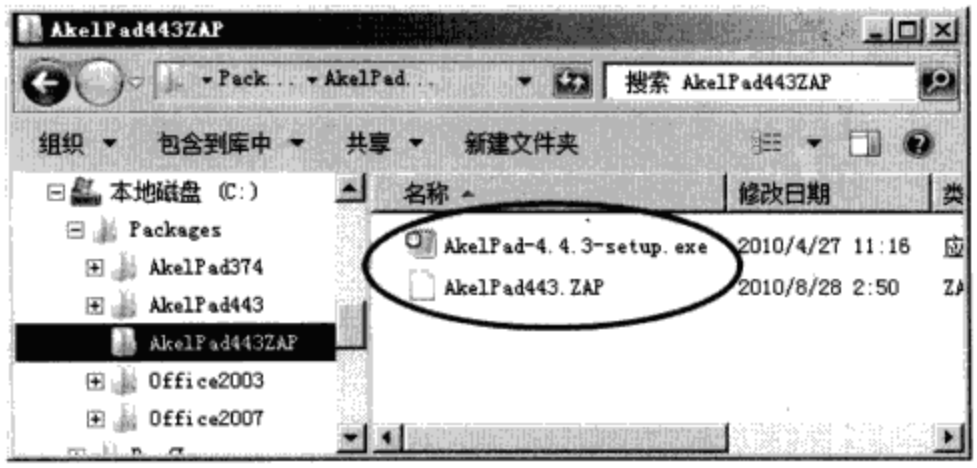


图 5-49

STEP 5 请在域控制器上通过【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑➲在图 5-50中展开**用户配置**➲策略➲软件设置➲对着**软件安装**右击➲新建➲数据包】的方式进行操作。



图 5-50

STEP 6 先在图 5-51右下角选择**ZAW早期版本应用程序数据包 (*.zap)**，然后选择我们所创建的.ZAP文件AkelPad443.ZAP，单击打开按钮。

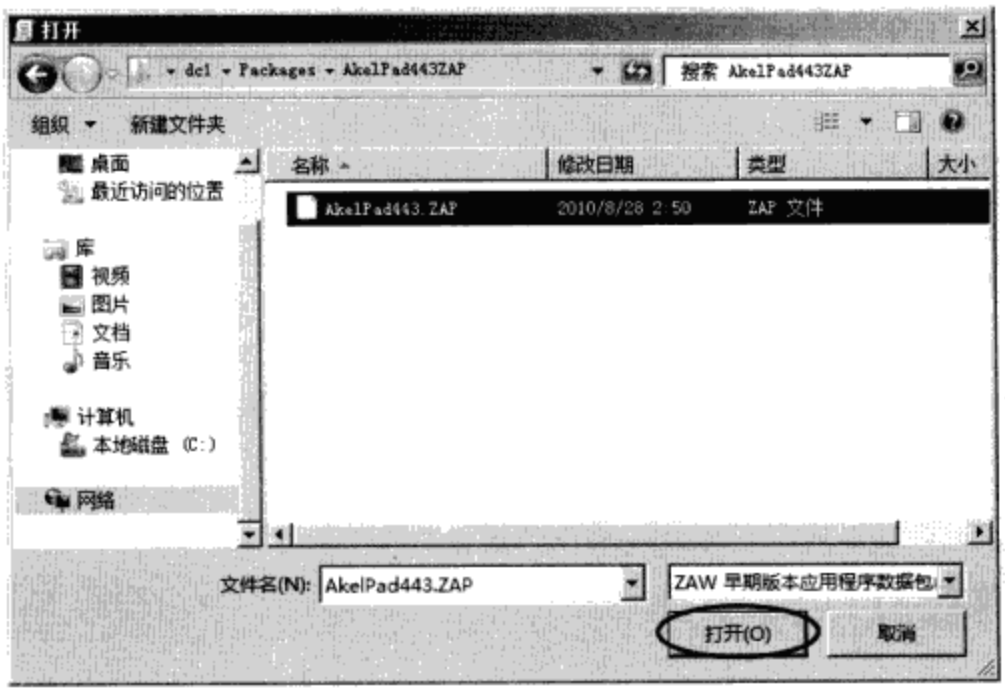


图 5-51

Download at http://www.pin5i.com/

STEP 7 在图 5-52中选择**已发布**单选按钮后单击确定按钮。

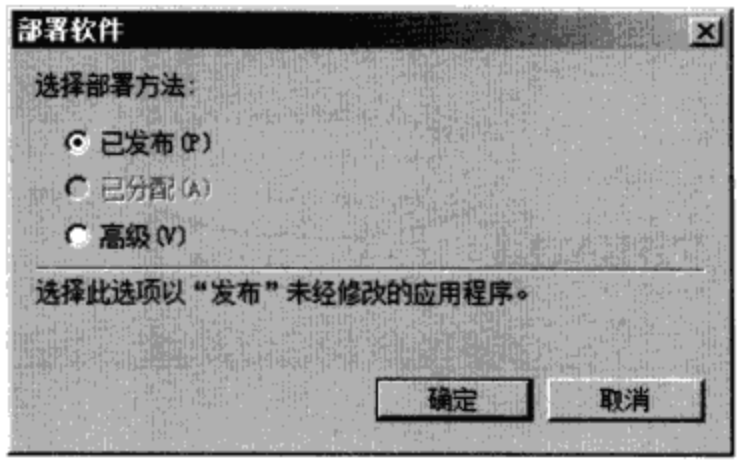


图 5-52

STEP 8 图 5-53为完成后的界面。

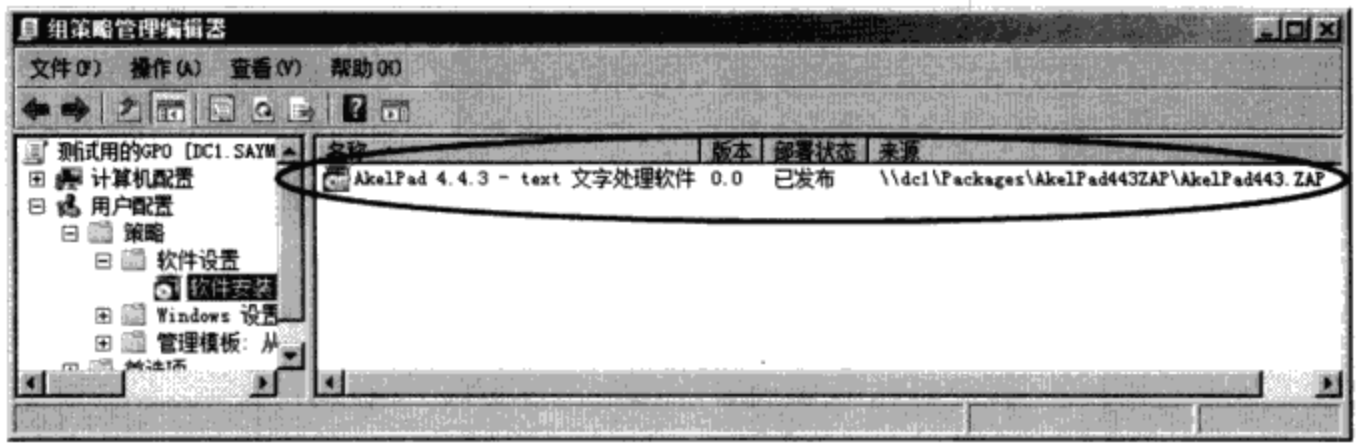


图 5-53

请使用组织单位**业务部**内的用户来登录，但是因为此时AkelPad 4.4.3需要由具备系统管理员权限的用户才可以安装，故若该用户没有系统管理员权限的话，则在Windows 7或Windows Vista计算机上安装时，系统会要求提供系统管理员的账户和密码才允许安装。在Windows XP计算机上安装的话，若用户不具备系统管理员权限就无法安装，因此请先将用户加入到Domain Admins组后再来练习。

5-7 软件部署的其他设置

您可以更改软件部署的默认值，以便让以后所新建的软件自动采用这些默认值。您也可以更改已经部署的软件相关设置值。

5-7-1 更改部署默认值

以**用户配置**来说，在通过【对着图 5-54中的**软件安装**单击右键➲属性】的方式进行操作

Download at http://www.pin5i.com/

后，便可以通过前图来更改以下的默认值。

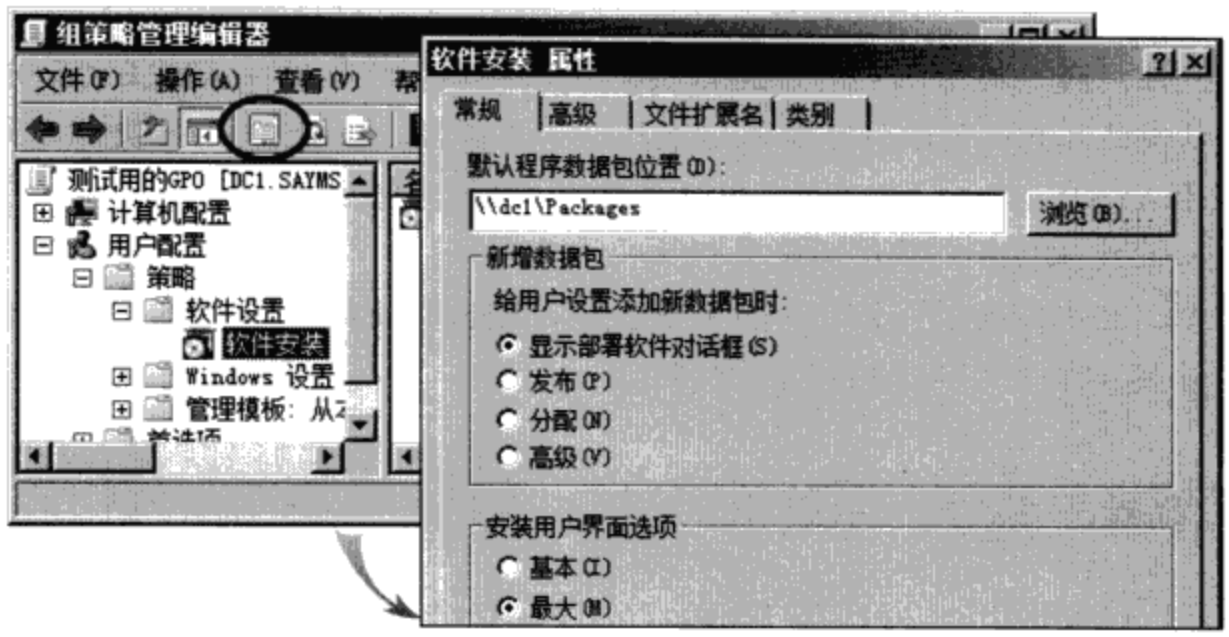


图 5-54

- **默认程序数据包位置**：前面已经介绍过了，这里不再赘述。
- **新增数据包**：用来设置新建软件时的默认部署方式。
- **安装用户界面选项**：让用户通过基本安装界面或完全安装界面来安装此软件（此软件需具备基本和完全安装界面的选择功能）。

注意

若要更改已部署软件的相关设置的话，请通过【对着该软件右击➲属性】的方法进行操作。

5-7-2 更改高级部署设置

您可以通过单击图 5-55中的**高级**标签来设置以下的默认值。

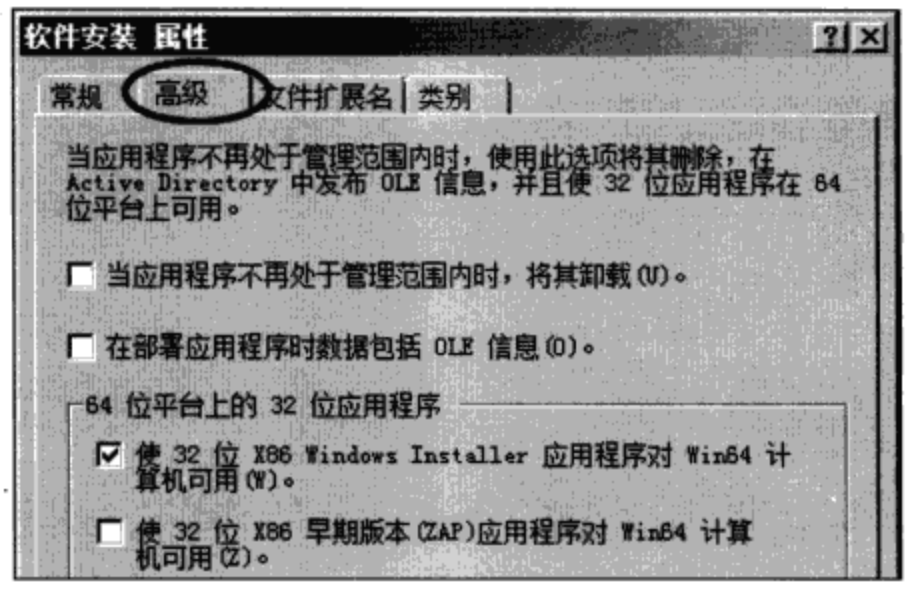


图 5-55

Download at http://www.pin5i.com/

- 当应用程序不再处于管理范围内时，将其卸载：若用户账户被移动到其他组织单位或GPO被禁用、删除等的话，则用户下次登录时，此软件就会被自动删除。
- 在部署应用程序时数据包含OLE信息：是否要部署与应用程序有关的COM组件的信息，以便让客户端的软件可以通过这些信息来安装这些组件（有点类似于**文件启动**）。
- 使32位X86 Windows Installer应用程序对Win64计算机可用：是否要让32位应用程序发布或分配给64位操作系统的计算机。
- 使32位X86早期版本（ZAP）应用程序对Win64计算机可用：是否要让32位的.ZAP应用程序发布给使用64位操作系统的用户。

5-7-3 扩展名和软件关联的优先级

如果您将Microsoft Office 2003中的PowerPoint 2003分配给计算机的话，则系统会在AD DS内将扩展名**.ppt**与PowerPoint 2003之间创建起关联关系。

如果您在同一个GPO内也设置了将Microsoft Office XP中的PowerPoint 2002发布给用户，则系统也会在AD DS内将扩展名**.ppt**和PowerPoint 2002之间创建起关联关系。请问此时如果用户使用**文件启动**的方式来安装PowerPoint时，到底是会安装PowerPoint 2003，还是PowerPoint 2002呢?这需要通过应用程序优先级来决定。

您可以如图 5-56所示通过**文件扩展名**标签来设置应用程序的优先级，例如图中的Office 2003 优先级较高，故用户使用**文件启动**的方式来安装PowerPoint时，会安装Office 2003的PowerPoint 2003。

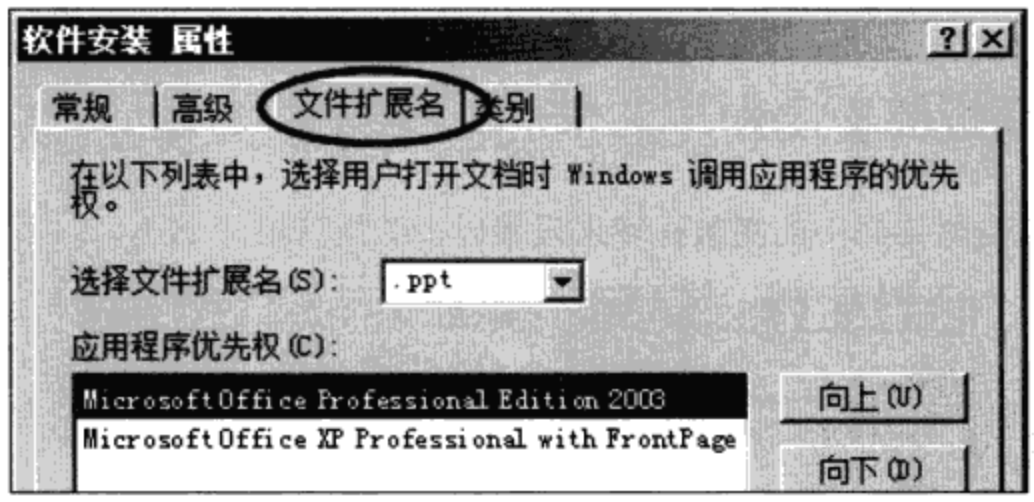


图5-56

5-7-4 软件分类

将所部署的软件分类后，用户在安装软件时，便可以根据软件类别来选择软件。首先请创建软件类别，然后再将所部署的软件归纳到适当的类别。

创建软件类别的方法为【单击图 5-57的**类别**标签后，通过添加按钮来创建】，图中的文字

Download at http://www.pin5i.com/

处理、电子表格、绘图软件等类别为完成创建后的范例。

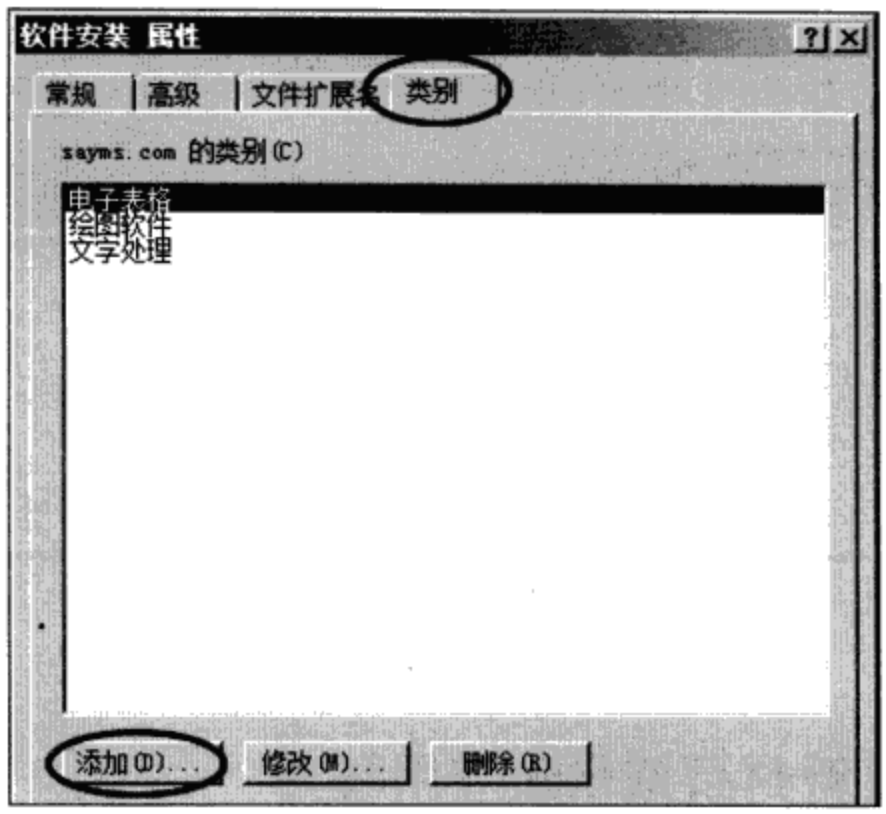


图 5-57

将所部署的软件归纳到适当类别的方法为：【如图 5-58所示对着已部署的软件右击➲属性➲通过图中的**类别**标签来设置】，图中我们已经将AkelPad 4.4.3归类到**文字处理**。

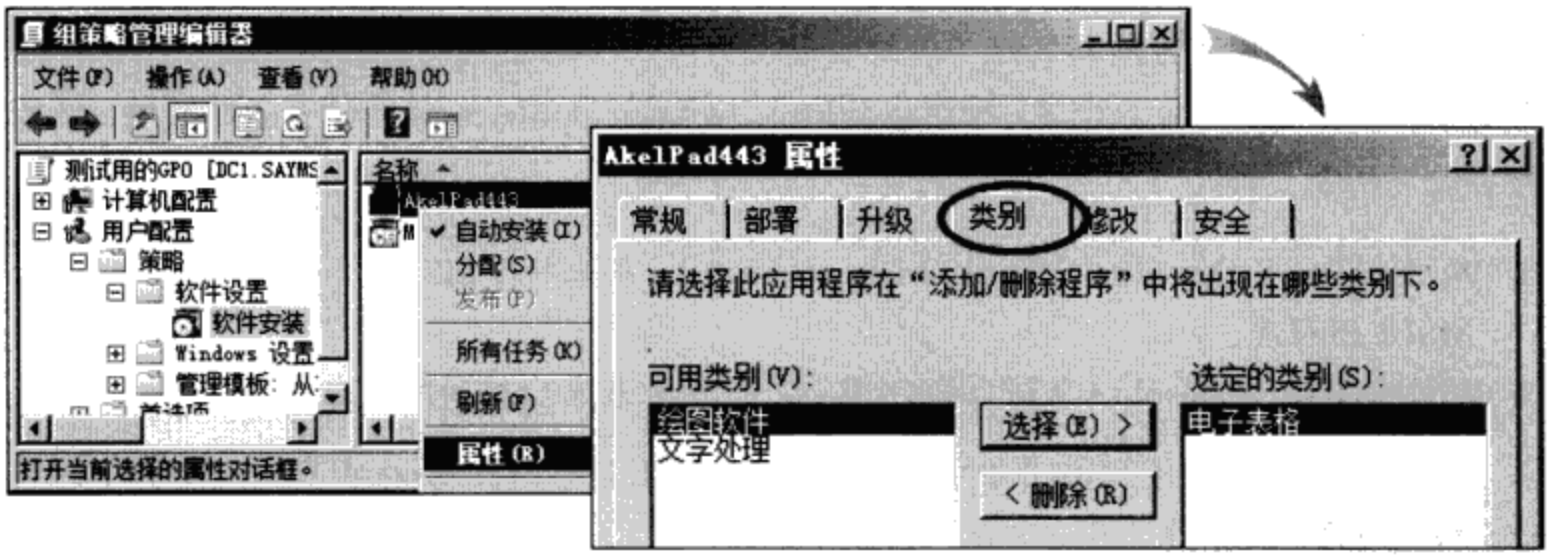


图 5-58

而用户在Windows XP计算机上通过**控制面板**来安装软件时，就可以根据类别来选择软件，如图 5-59所示为用户在选择类别（例如**文字处理**）后，界面上只会显示隶属于此类别的软件（例如AkelPad443）。

Download at http://www.pin5i.com/

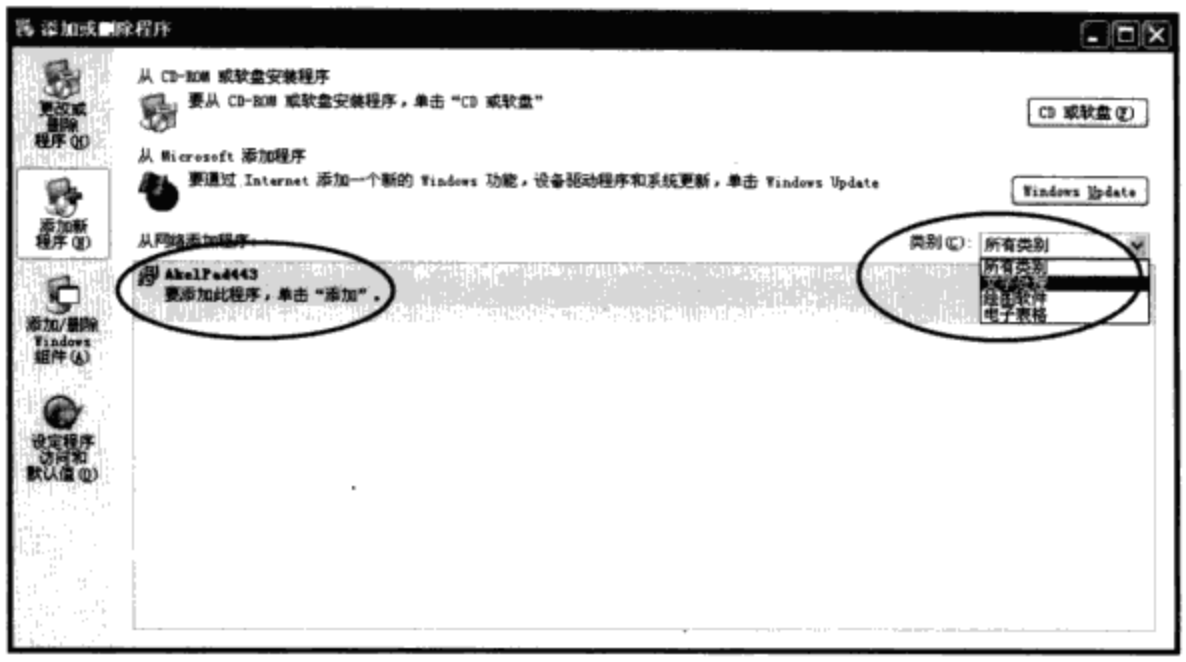


图 5-59

5-8 将软件重新封装成MSI应用程序

如果您所使用的应用程序为**非MSI应用程序**（非Windows Installer Package），但是却想要将它通过组策略部署给用户或计算机的话，此时您还可以通过**软件重新封装**（Software Repackaging）程序来将此应用程序重新封装成为**MSI应用程序**（Windows Installer Package）。

市面上有不少的**软件重新封装**程序，其中Scalable Software公司所提供的WinINSTALL LE是一个简单、容易使用的免费程序，您可以到**http://www.scalable.com/** 网站下载此程序，此程序包含着以下两个工具。

- WinINSTALL Discover Wizard （Discover.exe）：用来将非MSI应用程序重新封装成为MSI应用程序。
- WinINSTALL Console（WICONSOLE.exe）：用来查看和编辑**MSI应用程序**。

以下通过图 5-60为例进行说明如何使用WinINSTALL Discover Wizard 来将应用程序封装成为**MSI应用程序**。

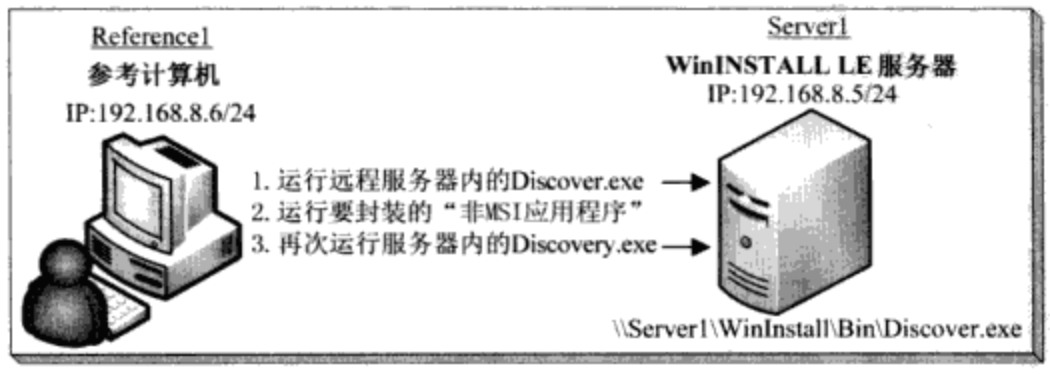


图 5-60

STEP 1 请先准备一台计算机，它被称为**参考计算机**（如图 5-60所示中左边的Reference1），

Download at http://www.pin5i.com/

注意为了确保能够将应用程序封装成为正确无误的**MSI应用程序**，因此在这台计算机内安装Windows系统后，请不要另外在这台计算机上安装其他应用程序，也就是说它必须是一台**clean computer（纯净的计算机）**。

提示

建议先将要重新封装的**非MSI应用程序**的安装文件复制到本地磁盘内。

STEP 2 将Scalable Software的WinINSTALL LE安装到另外一台计算机（如图 5-60所示中右边的Server1），假设我们将其称为**WinINSTALL LE服务器**，此程序默认会被安装到 %SystemDrive%\Program Files\Scalable\WinINSTALL 或 %SystemDrive%\Program Files（x86）\Scalable\WinINSTALL文件夹内，且会自动被设置为共享文件夹，其共享名默认为WinINSTALL。注意请不要将此软件安装到左边的**参考计算机**。

提示

如果这台计算机是Windows Server 2008 R2、Windows Server 2008、Windows 7或Windows Vista的话，则安装程序会自动例外开放**Windows防火墙**内的**文件和打印机共享**，以便让**参考计算机**可以进行连接。

STEP 3 到图 5-60中左边的**参考计算机**Reference1上，确认已经关闭所有的应用程序，通过网络连接到右边Server1的共享文件夹WinINSTALL，运行其内的Bin\Discover.exe程序，此时它会创建**Before快照**（Before Snapshot），其内包含着此**参考计算机**在安装**非MSI应用程序**之前的环境，包含当前磁盘内有哪一些文件、登录设置值与其他设置值等。

STEP 4 运行此程序时需指定封装后的**MSI应用程序**的文件名和存储路径（默认是**WinINSTALL LE服务器**的WinINSTALL共享文件夹之下的\Bin\Packages文件夹），选择存储的磁盘、要扫描的磁盘、要排除的文件和文件夹、要排除的登录路径等。完成创建**Before快照**后，Discover.exe程序会引导您继续在**参考计算机**Reference1上安装要被重新封装成为**MSI应用程序**的**非MSI应用程序**，其安装程序的扩展名一般是**.exe**。您也可以使用前面所使用的软件**AkelPad**来练习。

STEP 5 完成**非MSI应用程序**的安装后，继续在**参考计算机**Reference1上再次运行位于**WinINSTALL LE服务器**Server1上的Discover.exe程序。

STEP 6 此时它会创建**After快照**（After Snapshot），也就是读取**参考计算机**在安装完成此**非MSI应用程序**后的环境，然后使用**After快照**和**Before快照**两者之间的差异来创建一个**MSI应用程序**，这个**MSI应用程序**默认会被放置到**WinINSTALL LE服务器**的\\Server1\WinINSTALL\Bin\ Packages之内。

Download at http://www.pin5i.com/

如果您要编辑刚才制作的**MSI应用程序**，例如自行新建快捷方式、将卸载的快捷方式删除、更改安装文件夹、新建文件等，则请到**WinINSTALL LE服务器**Server1上运行WinINSTALL Console，其运行方法为【开始➲所有程序➲ Scalable WinINSTALL ➲ WinINSTALL LE】，其执行文件名称为WICONSOLE.EXE。

Download at http://www.pin5i.com/

第6章

限制软件的运行

我们可以通过**软件限制策略**（Software Restriction Policy，SRP）所提供的多种规则，来限制或允许用户可以运行的程序。

- 软件限制策略概述
- 启用软件限制策略



Download at http://www.pin5i.com/

6-1 软件限制策略概述

我们在前面的章节中曾经介绍过如何使用文件名来限制用户只能够或不可以运行指定的应用程序，然而若用户有权更改文件名的话，就可以绕过此限制，此时我们仍然可以通过本章的**软件限制策略**来控制管理。

软件限制策略的安全级别分为以下三种。

- 不受限（Unrestricted）：也就是所有登录的用户都可以运行指定的程序（只要用户拥有适当的访问权限，例如NTFS权限）。
- 不允许（Disallowed）：不论用户对程序文件的访问权限是什么，都不允许运行。
- 基本用户（Basic user）：允许以一般用户的权限（分配给users组的权限）来运行程序。

系统默认的安全级别是所有程序都**不受限**，也就是只要用户对要运行的程序文件拥有适当访问权限的话，就可以运行此程序。不过您可以通过**哈希规则**、**证书规则**、**路径规则**和**网络区域规则**等4 种规则来创建例外的安全级别，以便拒绝用户运行指定的程序。

6-1-1 哈希规则

由于**哈希**（Hash）是根据程序的文件内容所算出来的一连串字符，故不同程序有着不同的哈希值，所以系统可用它来识别程序。在您为某个程序创建**哈希规则**，并使用它限制用户不允许运行此程序时，系统就会为该程序创建一个哈希值。而当用户要运行此程序时，他的计算机就会比对其自行算出来的哈希值是否与软件限制策略中的哈希值相同，如果相同，表示它就是被限制的程序，因此会被拒绝运行。

即使此程序的文件名被改变或被移动到其他位置，也不会改变其哈希值，因此仍然会受到哈希规则的约束。

> **提示**
>
> 若客户端计算机的程序文件内容被更改的话（例如感染计算机病毒），此时因为用户的计算机所算出的哈希值，并不会与哈希规则中的哈希值相同，因此会认为它不是受限制的程序，故不会拒绝此程序的运行。

6-1-2 证书规则

软件发行公司可以使用证书（Certificate）来签署其所开发的程序，而软件限制策略通过此证书来识别程序，也就是说您可以创建**证书规则**来识别使用此证书所签署的程序，以便允

Download at http://www.pin5i.com/

许或拒绝用户运行此程序。

6-1-3 路径规则

您可以通过**路径规则**来允许或拒绝用户运行位于某个文件夹内的程序。由于是根据路径来识别程序，因此如果程序被移动到其他文件夹的话，此程序将不会再受到路径规则的约束。

除了文件夹路径外，您也可以通过**注册表**路径来限制，例如允许用户可以运行在注册表中所指定的文件夹内的程序。

6-1-4 网络区域规则

您可以使用网络区域规则来允许或拒绝用户运行位于某个区域内的程序，这些区域包含本地计算机、Internet、本地 Intranet、受信任的站点和受限制的站点。

除了本地计算机和Internet之外，您可以设置其他三个区域内所包含的计算机或网站：【打开网页浏览器Internet Explorer➲单击**工具**菜单➲Internet选项➲单击图 6-1中的**安全**标签➲选择要设置的区域后单击站点按钮】。

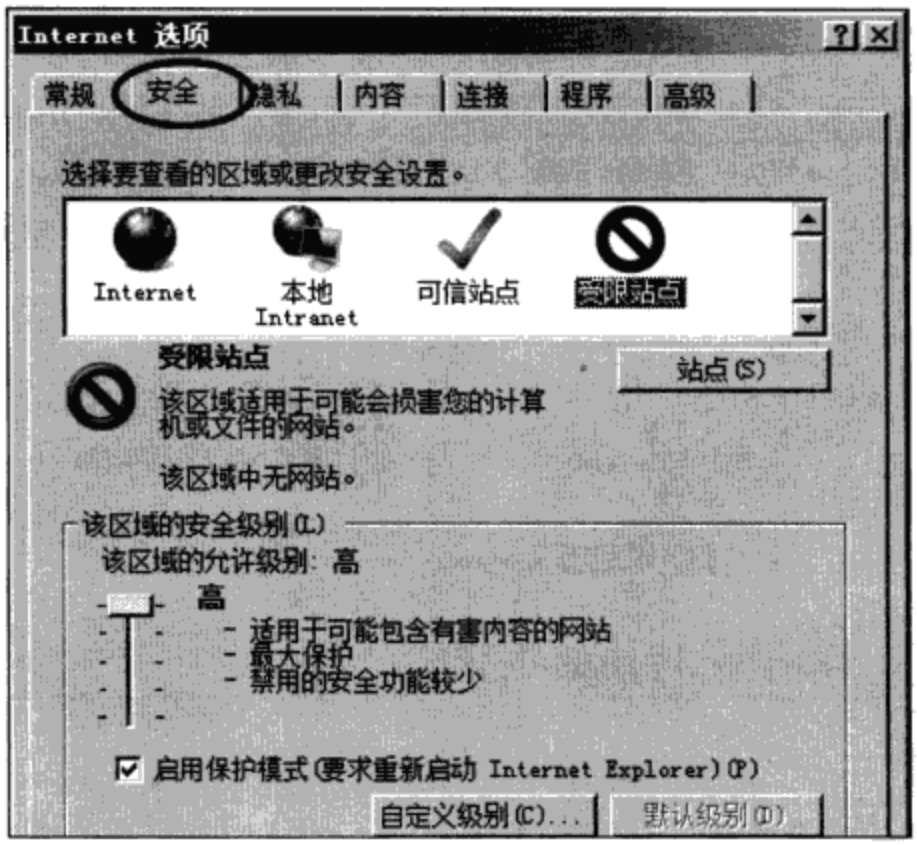


图 6-1

提示

网络区域规则目前只适用于扩展名为.msi的Windows Installer Package。

Download at http://www.pin5i.com/

6-1-5 规则的优先级

您可能会针对同一个程序设置不同的软件限制规则，而这些规则的优先级由高到低为：哈希规则、证书规则、路径规则、网络区域规则。

例如您针对某个程序设置了哈希规则，且设置其安全级别为**不受限**，然而您同时针对此程序所在的文件夹设置路径规则，且设置其安全级别为**不允许**，此时因为哈希规则的优先级高于路径规则，故用户仍然可以运行此程序。

6-2 启用软件限制策略

您可以通过本地计算机、站点、域和组织单位等4个不同的地方来设置软件限制策略。以下将使用前几章所使用的组织单位**业务部**内的**测试用的GPO**来练习软件限制策略（若尚未有此组织单位和GPO的话，请先创建）：请到域控制器上通过【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑➲在图 6-2中展开**用户配置**➲策略➲Windows设置➲安全设置➲对着**软件限制策略**单击右键➲创建软件限制策略】的方式进行操作。

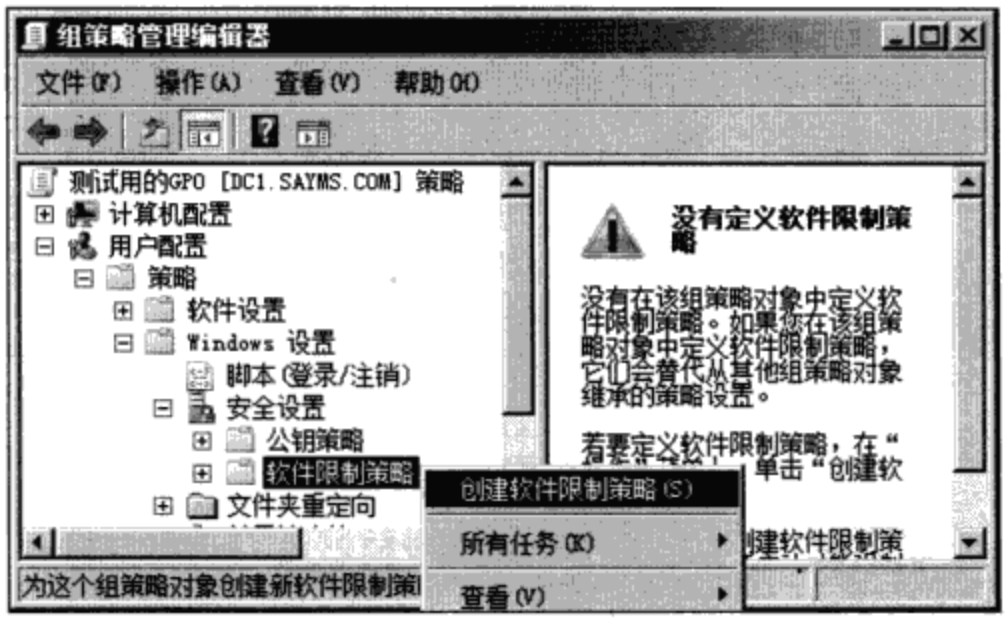


图 6-2

接着单击图 6-3中的**安全级别**，从右方**不受限**前面的打勾符号可知默认安全级别是所有程序都**不受限**，也就是只要用户对要运行的程序文件拥有适当访问权限的话，就可以运行该程序。

Download at http://www.pin5i.com/

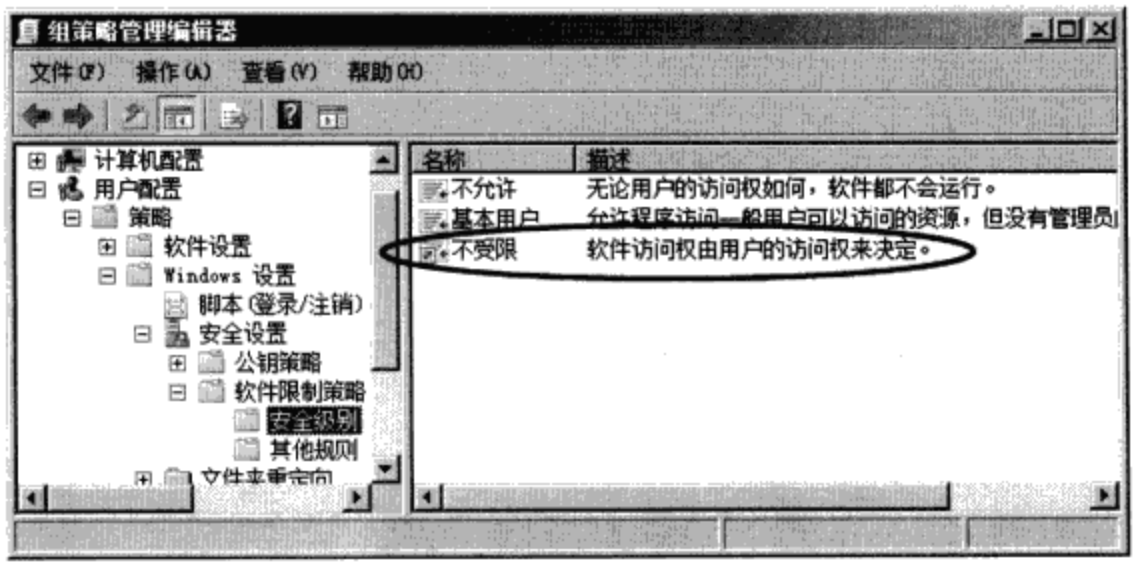


图 6-3

6-2-1 新建哈希规则

例如若要使用哈希规则来限制用户不可以安装Foxy 1.9.10简体中文版的话，则其步骤如下所示（假设其安装文件为Foxy.1.9.10.TC.Setup.exe）。

STEP 1 我们将到域控制器上设置，因此请先将Foxy 1.9.10简体中文版的安装文件Foxy.1.9.10.TC.Setup.exe复制到此计算机上。

STEP 2 如图 6-4所示，通过【对着**其他规则**单击右键➲新建哈希规则➲单击浏览按钮】的方式进行操作。

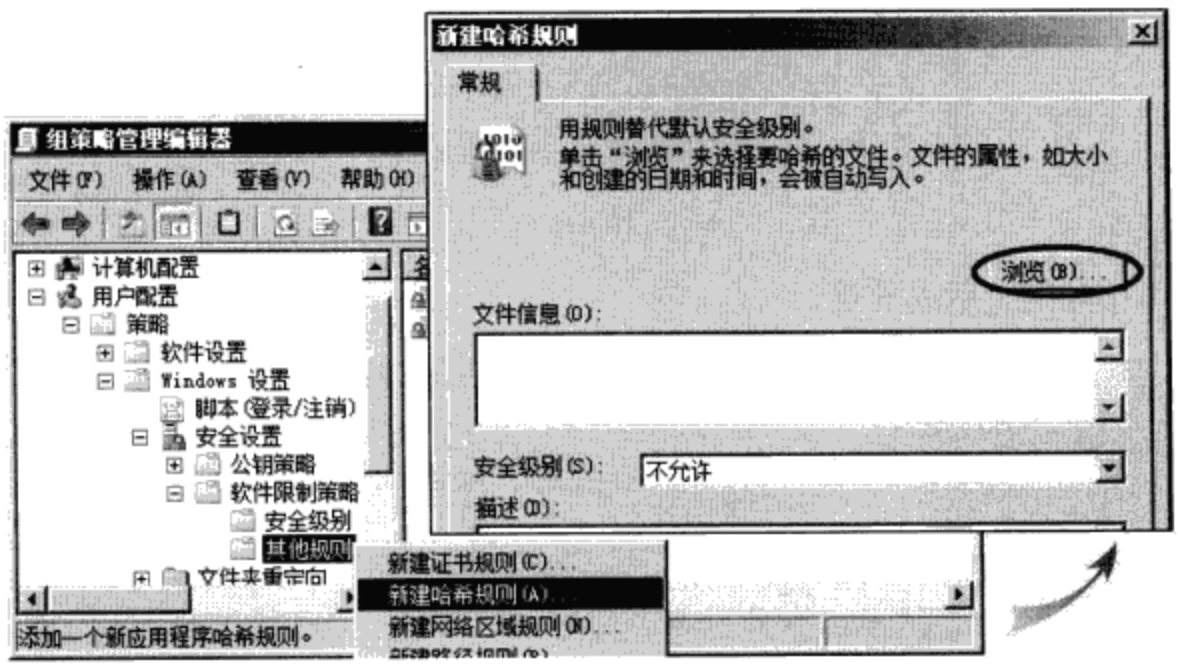


图 6-4

STEP 3 在图 6-5中浏览到Foxy 1.9.10安装文件的存储位置后选择Foxy.1.9.10.TC.Setup.exe，单击打开按钮。

Download at http://www.pin5i.com/



图 6-5

STEP 4 在图 6-6中选择**不允许**安全级别后单击确定按钮。

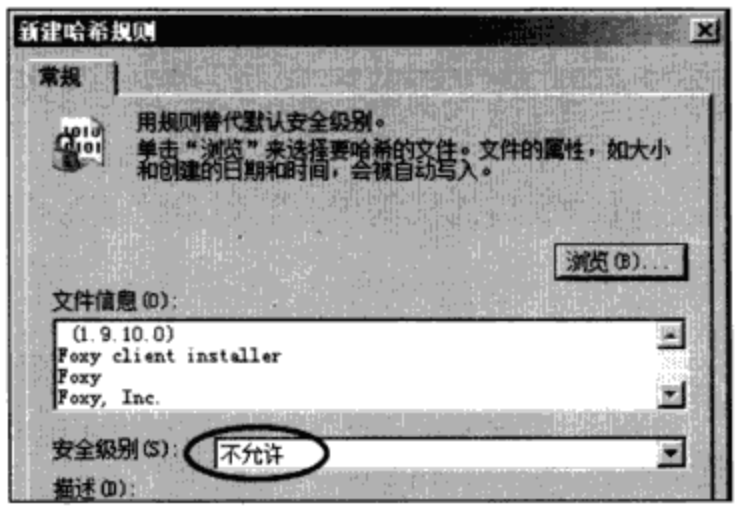


图 6-6

STEP 5 图 6-7为完成后的界面。

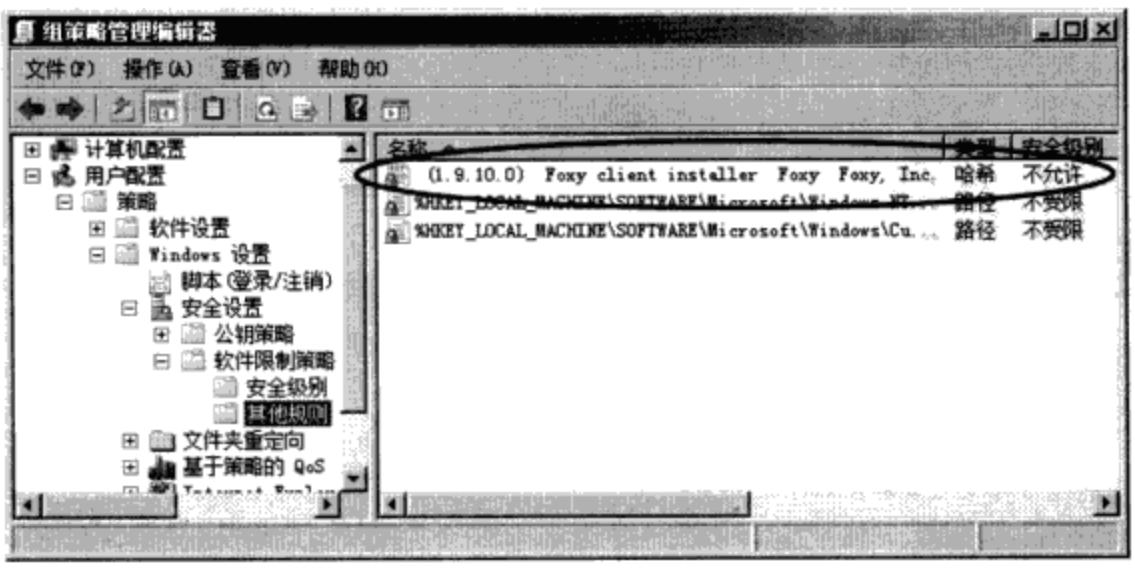


图 6-7

Download at http://www.pin5i.com/

位于组织单位**业务部**内的用户应用此策略后，在运行Foxy 1.9.10简体中文版的安装文件Foxy.1.9.10.TC.Setup.exe时会被拒绝，而且会出现如图 6-8所示的警告对话框。

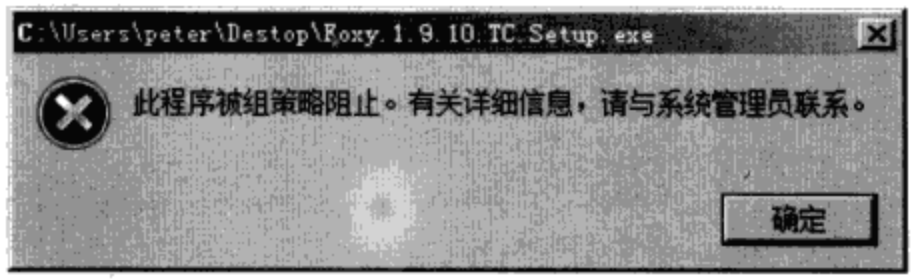


图6-8

注意

1. 不同版本的Foxy，其安装文件的哈希值也都不相同，因此若要禁止用户安装其他版本Foxy的话，则需要再针对它们创建哈希规则。
2. 为了加强阻挡的效果，建议也禁止用户运行Foxy文件，其设置方法为先在一台计算机安装Foxy，找出Foxy的运行文件（一般是Foxy.exe），针对此文件创建哈希规则来禁止用户运行此文件。

6-2-2 新建路径规则

路径规则分为一般文件夹路径规则和注册表路径规则两种。路径规则中可使用环境变量，例如%Userprofile%、%SystemRoot%、%Appdata%、%Temp%、%Programfiles%等。

1. 新建文件夹路径规则

举例来说，如果您要使用文件夹路径规则来限制用户不可以运行位于\\dc1\SystemTools共享文件夹内所有程序的话，则其设置步骤如下所示。

STEP 1 如图 6-9所示，通过【对着**其他规则**单击右键➲新建路径规则】的方式进行操作。

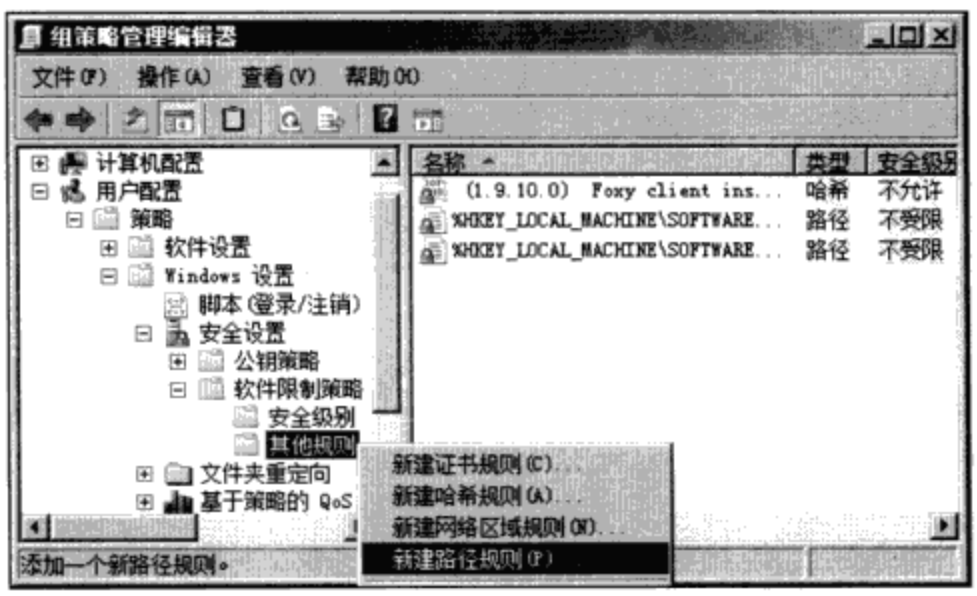


图6-9

Download at http://www.pin5i.com/

STEP 2 在图 6-10中输入或浏览到\\dc1\SystemTools，安全级别选择**不允许**，单击确定按钮。

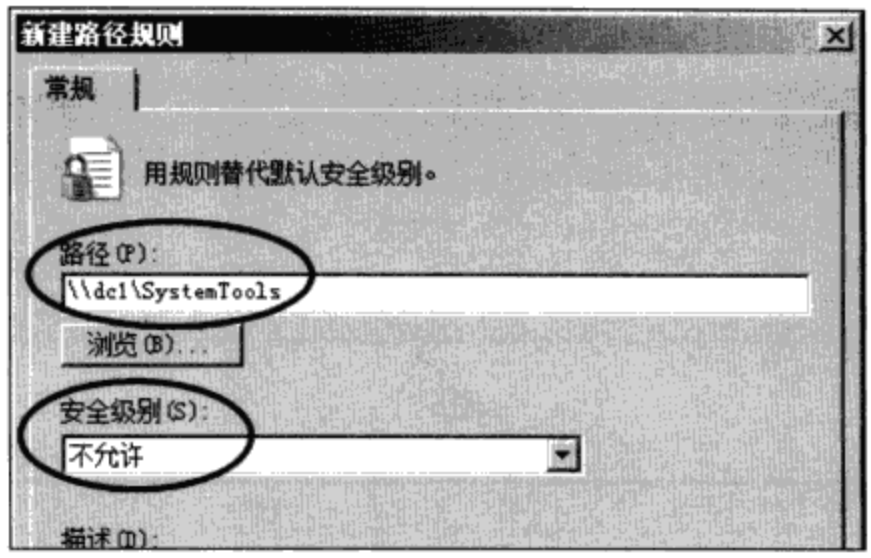


图 6-10

提示

若您只是要限制用户运行此路径内某个程序的话，请输入此程序的文件名，例如要限制的程序为flushgar.exe的话，则请输入\\dc1\SystemTools\flushgar.exe；若不论此程序位于何处，都要禁止用户运行的话，则直接输入程序名称flushgar.exe即可。

STEP 3 图 6-11为完成后的界面。

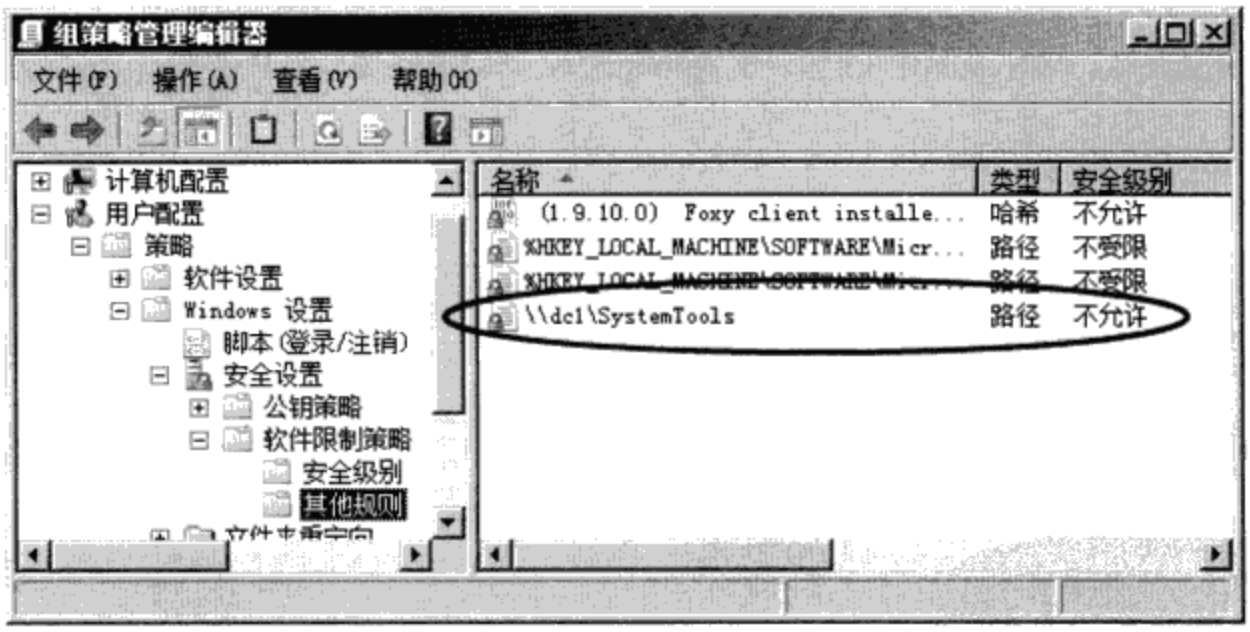


图 6-11

2. 新建注册表路径规则

您也可以通过**注册表**（Registry）路径来允许或禁止用户运行路径内的程序，由图 6-12中可看出系统已经内置了两个注册表路径。

Download at http://www.pin5i.com/

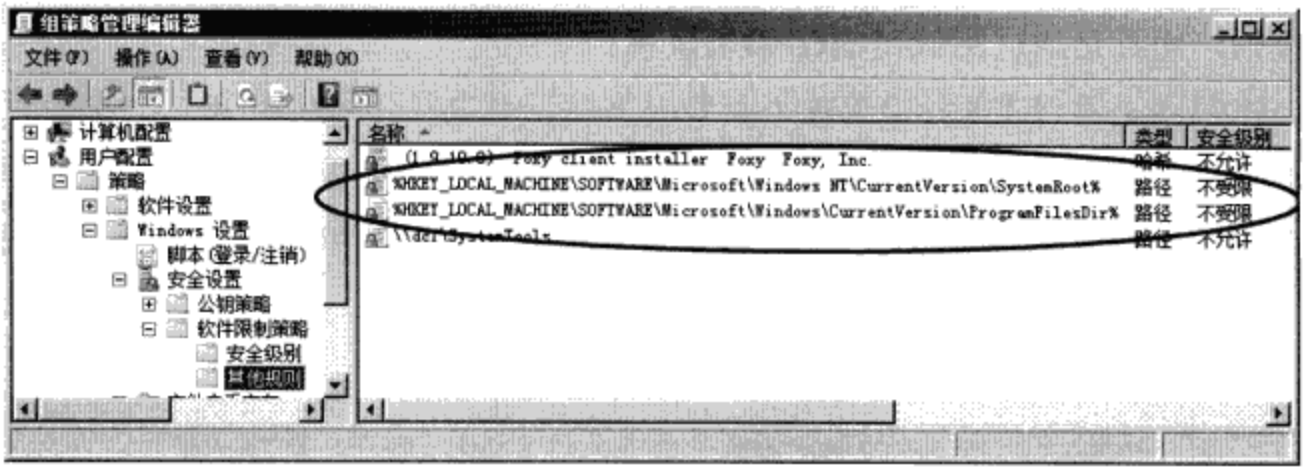


图6-12

其中第一个注册表路径是要允许用户可以运行位于以下注册表路径内的程序：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\
SystemRoot
```

而我们可以使用注册表编辑器（REGEDIT.EXE）来查看其所对应到的文件夹，如图 6-13 所示的C:\Windows，也就是说用户可以运行位于文件夹C:\Windows内的所有程序。

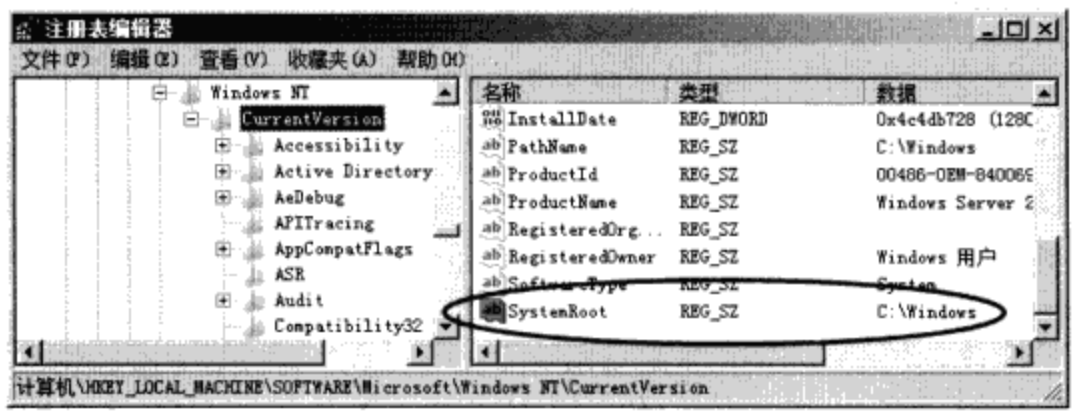


图6-13

若要编辑或新建注册表路径规则的话，记得在路径前后要附加**%**符号，例如：

```
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\
SystemRoot%
```

6-2-3 新建证书规则

由于客户端计算机默认并未启用证书规则，因此这些计算机在运行扩展名为.exe的运行文件时，并不会处理和证书有关的事宜。以下我们将先启用客户端的证书规则，然后再来创建证书规则。

1. 启用客户端的证书规则

证书规则的启用是通过组策略来设置，以下假设是要针对组织单位**业务部**内的计算机来

Download at http://www.pin5i.com/

启用证书规则，而且是通过**测试用的GPO**来设置。

请到域控制器上通过【开始➲管理工具➲组策略管理➲展开到组织单位**业务部**➲对着**测试用的GPO**单击右键➲编辑➲在图 6-14中展开**计算机配置**➲策略➲Windows设置➲安全设置➲本地策略➲安全选项➲将右边的**系统设置：将 Windows 可执行文件中的证书规则用于软件限制策略**设置为**已启用**】的方法进行操作。完成后，位于此组织单位**业务部**内的计算机在应用策略后便具备通过证书来限制程序运行的功能。

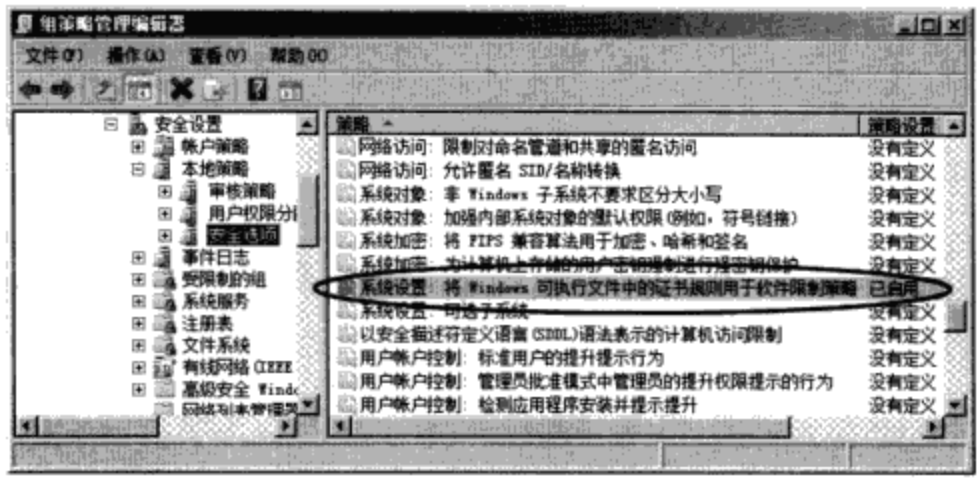


图 6-14

提示

若要启用本地计算机的证书规则，可通过【运行**GPEDIT.MSC**➲计算机配置➲Windows设置➲安全设置➲本地策略➲安全选项➲将**系统设置：将 Windows 可执行文件中的证书规则用于软件限制策略**设置为**已启用**】的方式进行操作，若此设置和域组策略设置有冲突时，则以域组策略的设置优先。

您也可以通过以下方法来启用客户端的证书规则：【在图 6-15中展开**计算机配置**➲策略➲Windows设置➲安全设置➲软件限制策略➲双击右边的**强制**选项➲选择**强制证书规则**单选按钮】。

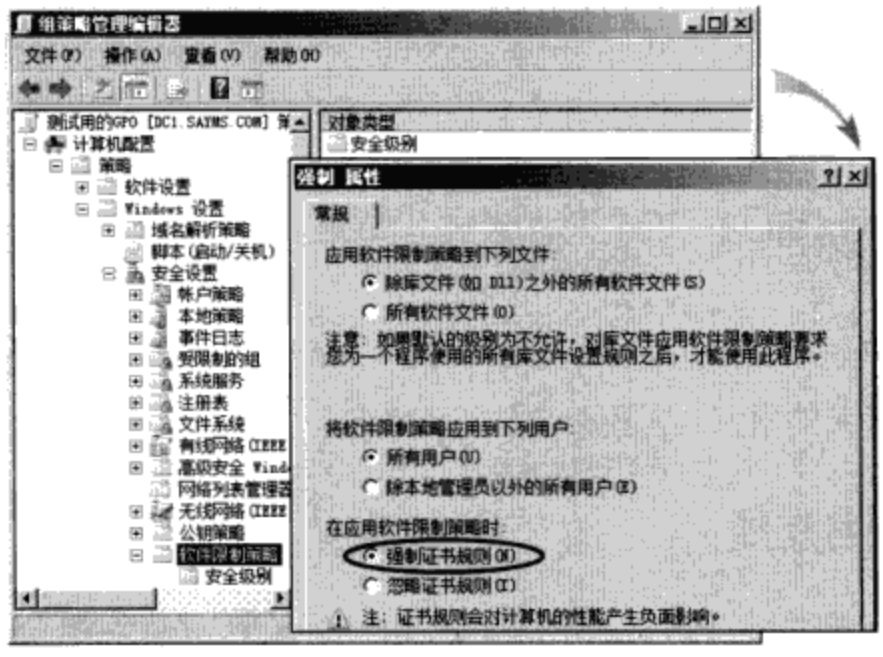


图 6-15

Download at http://www.pin5i.com/

2. 新建证书规则

以下假设在组织单位**业务部**内默认的安全级别是**不允许**，也就是此组织单位内的用户无法运行所有程序，但只要程序经过Sayms公司所申请的**程序代码签署证书**签署的话，该程序就允许运行，假设此证书的证书文件为SaymsCert.cer。

> **提示**
>
> 您可以通过自行架设的CA来练习，其步骤为：架设CA（例如独立根CA），使用Internet Explorer来向此CA申请**程序代码签署证书**（记得选择**标记密钥**为**可导出**），下载和安装证书，使用Internet Explorer将证书导出保存（通过【单击**工具**菜单➲Internet选项➲内容➲证书➲选择证书➲导出】的方法进行操作）。

STEP 1 对着图 6-16中的**其他规则**右击➲新建证书规则➲单击**浏览**按钮。

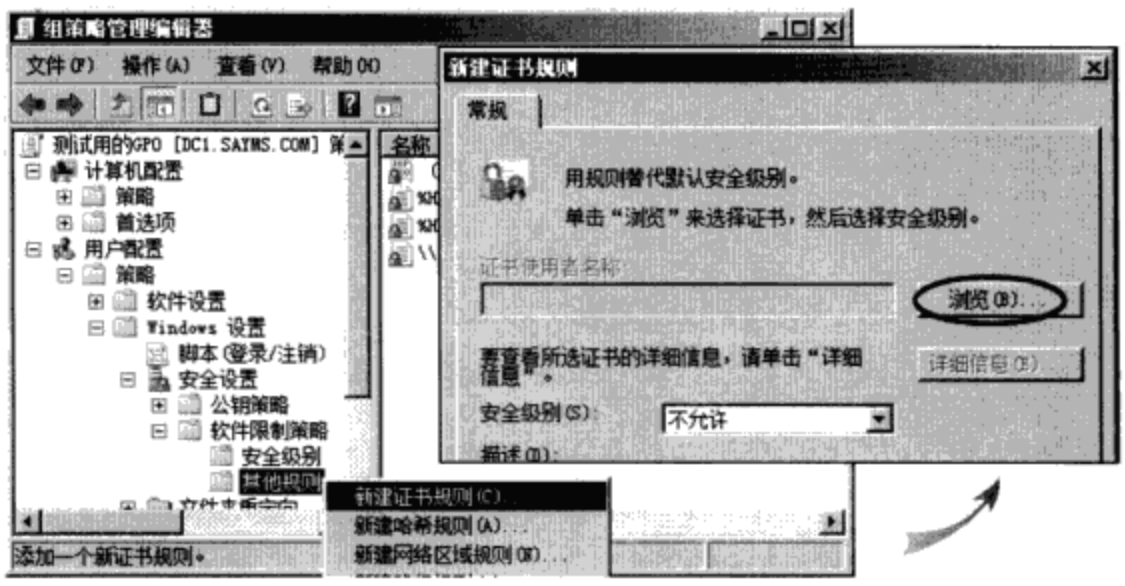


图 6-16

STEP 2 在图 6-17中浏览到证书文件SaymsCert.cer后单击**打开**按钮。



图 6-17

Download at http://www.pin5i.com/

STEP 3 在图 6-18中选择**不受限**后单击确定按钮。

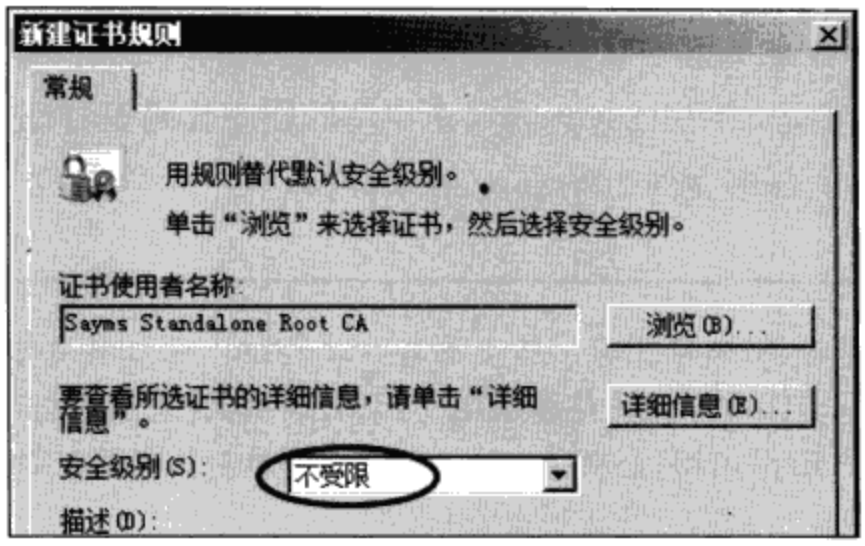


图6-18

STEP 4 图 6-19为完成后的界面。位于组织单位**业务部**内的用户应用此策略后，在运行所有经过Sayms证书签署的程序时，都会被允许。

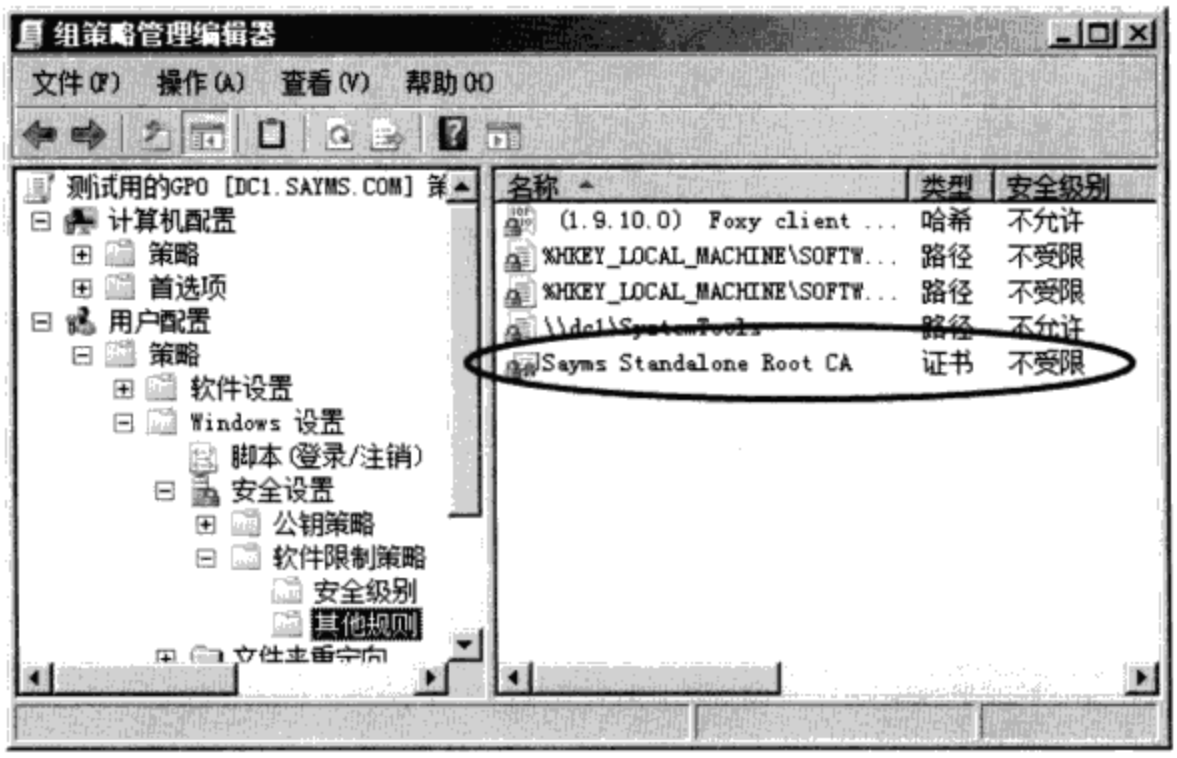


图6-19

6-2-4 新建网络区域规则

您也可使用**网络区域规则**来允许或拒绝用户运行位于某个区域内的程序，这些区域包含本地计算机、Internet、本地 Intranet、受信任的站点和受限制的站点。

创建网络区域规则的方法和其他规则很类似，也如图 6-20所示，可通过【对着**其他规则**单击右键➲新建网络区域规则➲在**网络区域**下拉列表中选择区域➲选择安全级别】的方式进行操作，图6-21表示只要是位于**受限制的站点**内的程序都不允许运行。

Download at http://www.pin5i.com/

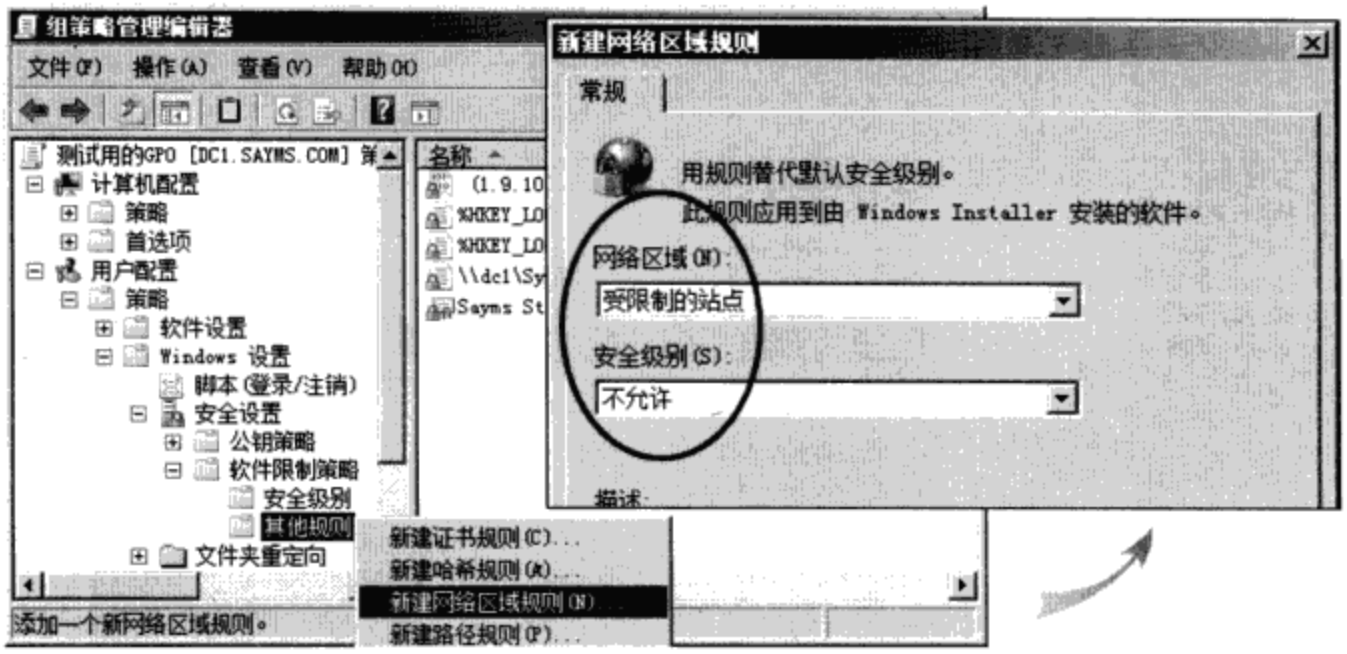


图 6-20

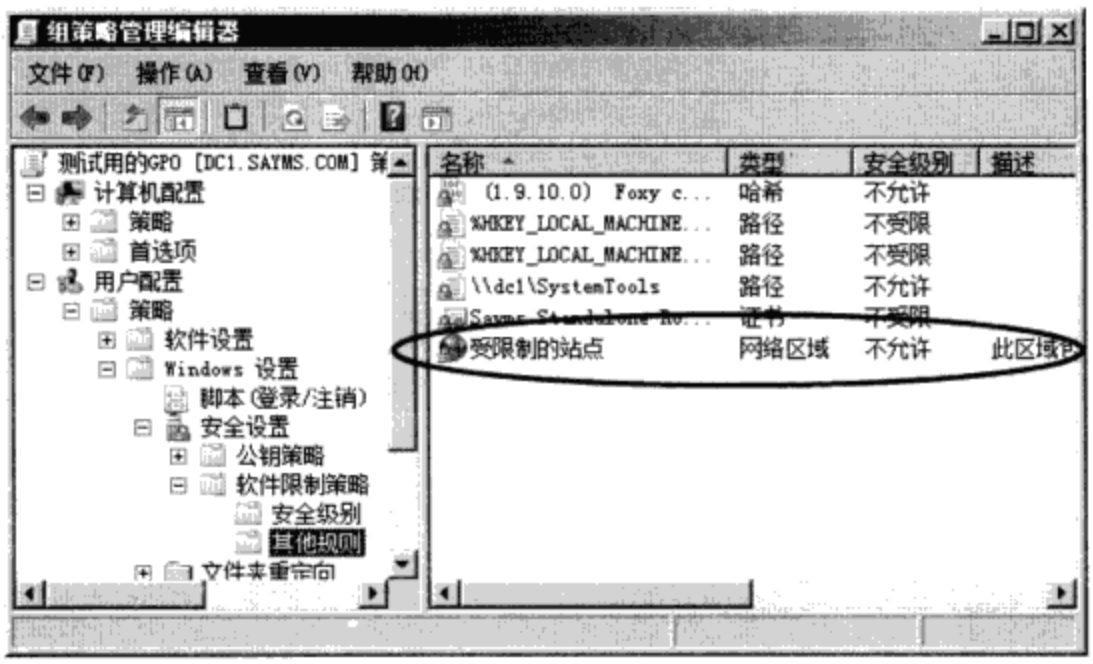


图 6-21

6-2-5 不要将软件限制策略应用到本地系统管理员

若不想将软件限制策略应用到本地系统管理员（Administrators）的话，可以如图 6-22所示，通过【双击**软件限制策略**右边的**强制**选项➲在**将软件限制策略应用到下列用户**选项组中选择**除本地管理员以外的所有用户**单选按钮➲单击确定按钮】的方式进行操作。

Download at http://www.pin5i.com/

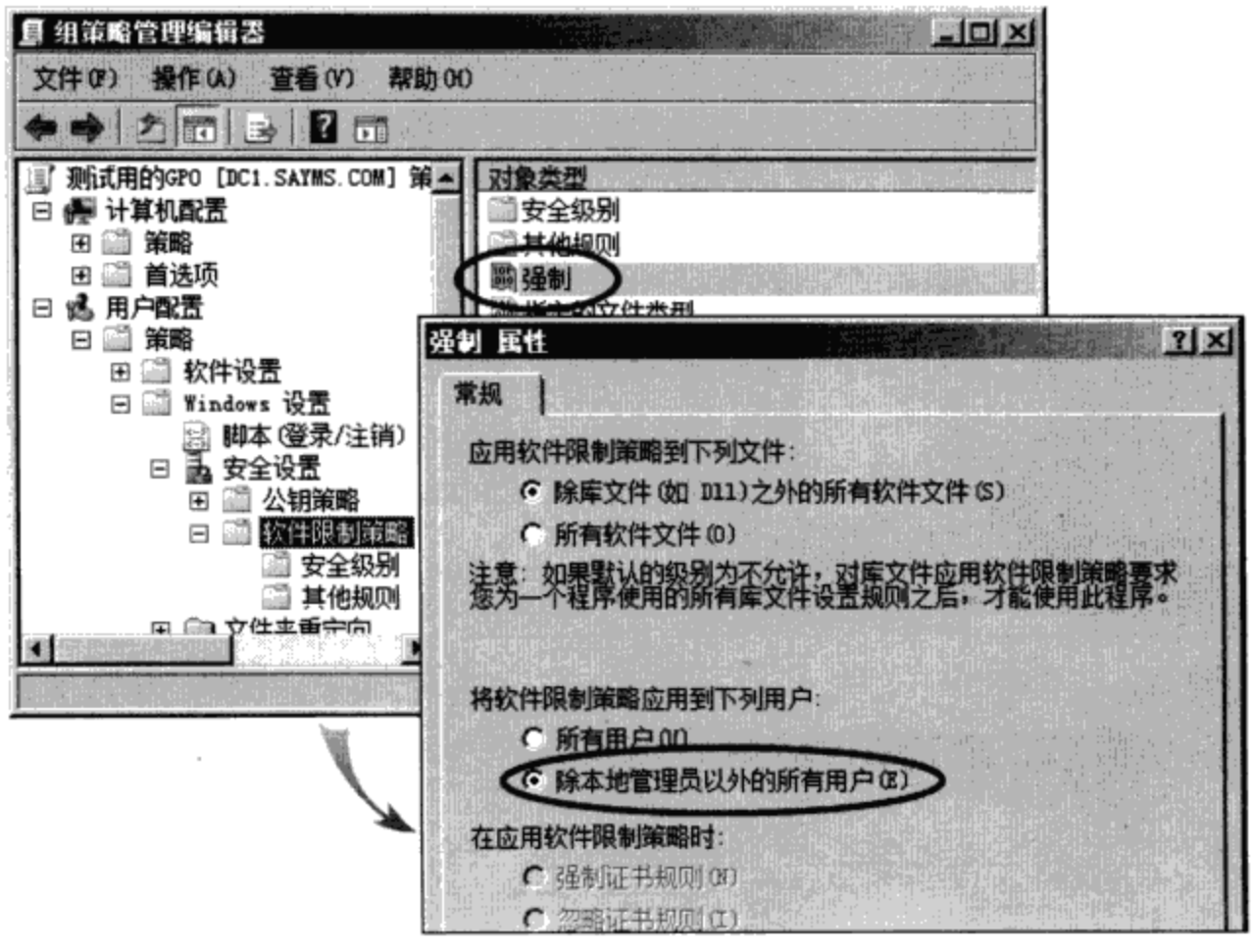


图 6-22

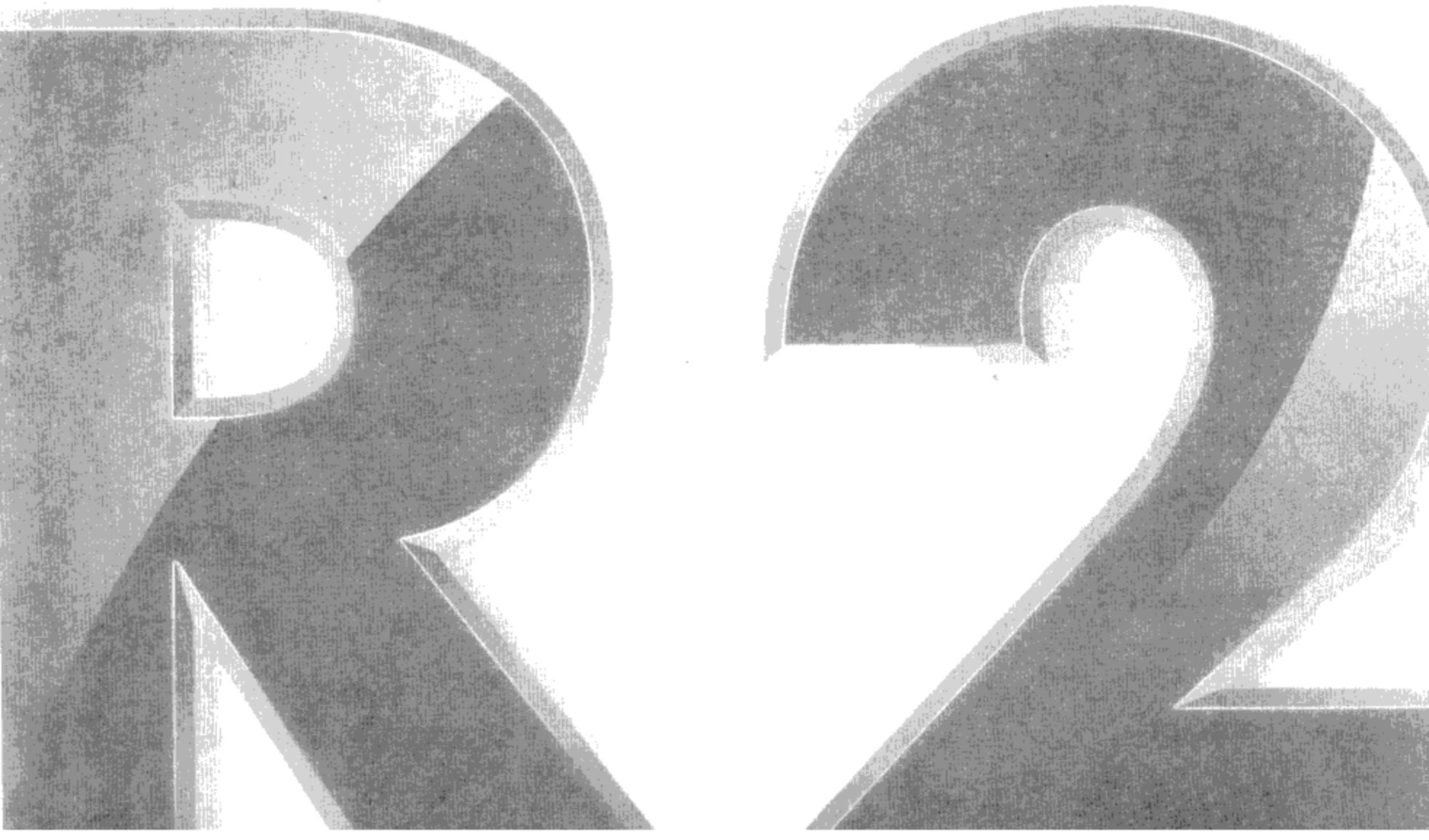
Download at http://www.pin5i.com/

第7章

创建域树和林

我们在第2章已经介绍过如何创建单一域的网络环境，本章将更进一步介绍如何创建完整的**域树**（Domain Tree）与**林**（Forest）。

- 创建第一个域
- 创建子域
- 创建林中的第2个域树
- 删除子域和域树
- 更改域控制器的计算机名称



Download at http://www.pin5i.com/

7-1 创建第一个域

在开始创建域树和林之前，若您对**Active Directory域服务**（AD DS）概念还不是很清楚的话，请先参考第1章的说明。以下使用图 7-1中的林来解说，此林内包含左右两个域树。

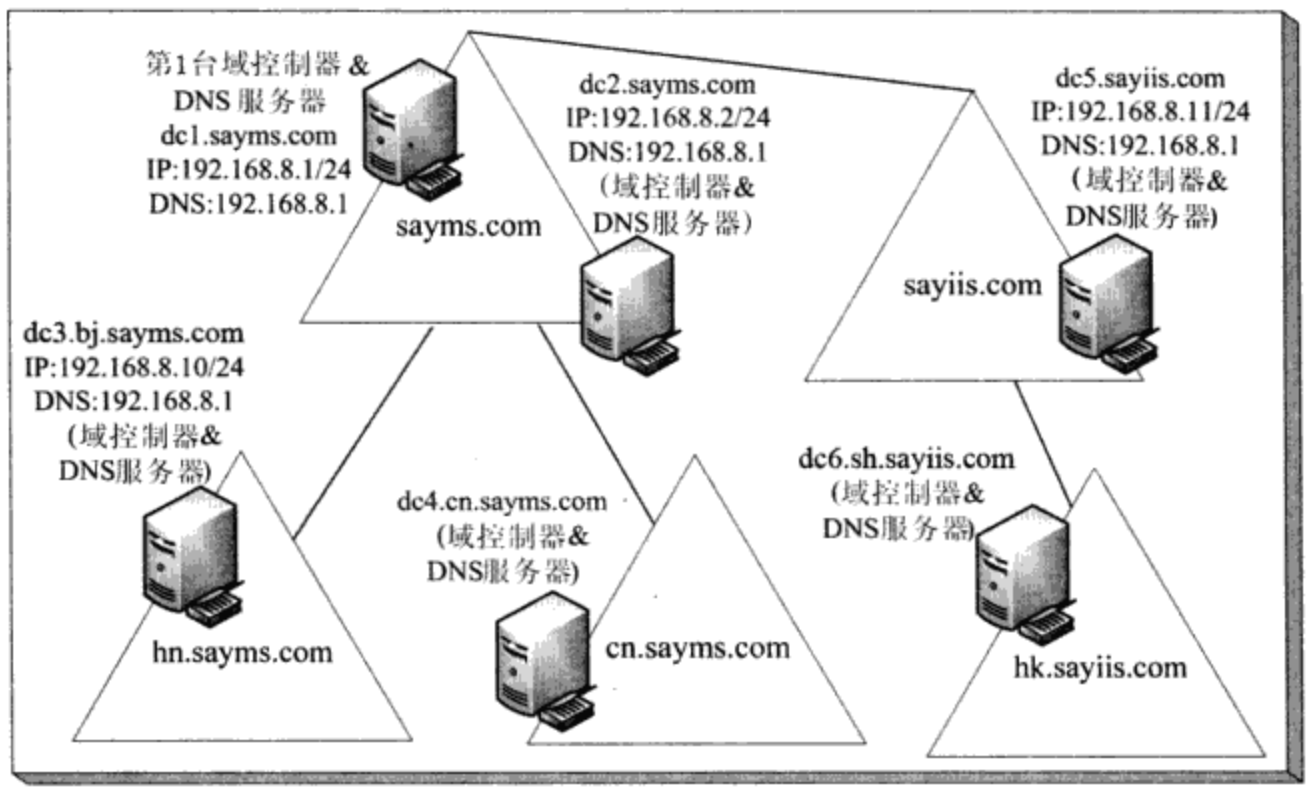


图 7-1

- 左边的域树：它是这个林内的第1 个域树，其根域的域名为sayms.com。根域之下有两个子域，分别是hn.sayms.com和cn.sayms.com。林名称是以第1个域树的根域名称来命名，所以这个林的名称就是sayms.com。
- 右边的域树：它是这个林内的第2 个域树，其根域的域名为sayiis.com。根域之下有一个子域hk.sayiis.com。

创建域之前的准备工作和如何创建图中第1个域sayms.com的方法，都已经在第2章内介绍过了。本章将只介绍如何来创建子域（例如图中的hn.sayms.com）与第2个域树（例如图右边的sayiis.com）。

7-2 创建子域

请先确定图7-1中的根域sayms.com已经创建完成，我们将在此域之下创建子域hn.sayms.com。

Download at http://www.pin5i.com/

7-2-1 使用Windows窗口来创建子域

以下通过将图 7-1 中的 dc3.hn.sayms.com 升级为域控制器的方式来创建子域 hn.sayms.com，这台服务器可以是独立服务器或隶属于其他域的现有成员服务器。

STEP 1 请先在图 7-1左下角的服务器dc3.hn.sayms.com上安装Windows Server 2008 R2，将其计算机名设置为dc3，IPv4地址等依照图示来设置（图中采用TCP/IPv4）。注意将计算机名设置为dc3即可，等升级为域控制器后，就会自动改为dc3.hn.sayms.com。

STEP 2 在这台服务器上选用以下两种方式之一来安装 **Active Directory 域服务**（AD DS）：

- 单击左下角的服务器管理器图标：此时请跳到**STEP 3**。
- 通过【开始➲运行➲输入dcpromo后单击确定按钮】的方法：此时它会自动运行**STEP 3** ~ **STEP 9**的安装AD DS步骤，故请直接跳到**STEP 10**。

STEP 3 单击左边的**角色**，单击**添加角色**。

STEP 4 在出现**开始之前**界面时单击下一步按钮。

STEP 5 在图 7-2中选择**Active Directory域服务**复选框，在弹出的对话框中单击**添加必需的功能**，单击下一步按钮。



图 7-2

STEP 6 在Active Directory域服务界面中单击下一步按钮。

STEP 7 在**确认安装选择**界面中单击安装按钮。

STEP 8 在出现**安装结果**界面时单击关闭按钮。

STEP 9 如图7-3所示，通过【单击左边角色处的Active Directory域服务➲单击**运行Active Directory域服务安装向导 (dcpromo.exe)**】的方法进行操作。

Download at http://www.pin5i.com/

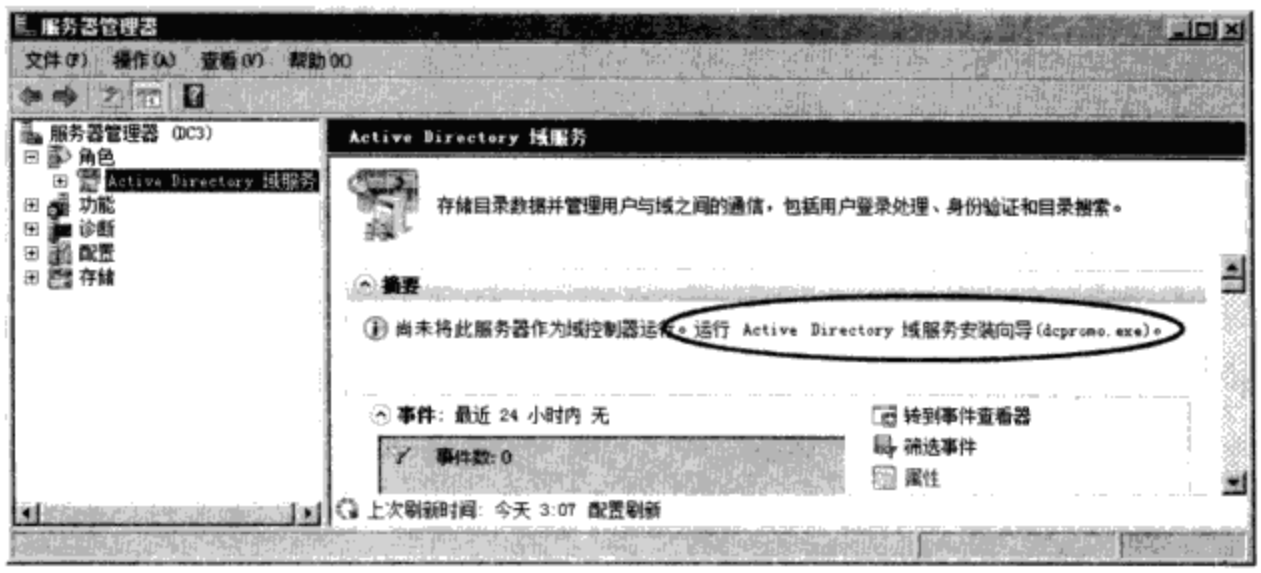


图 7-3

STEP 10 如图 7-4所示选择**使用高级模式安装**复选框后单击下一步按钮。

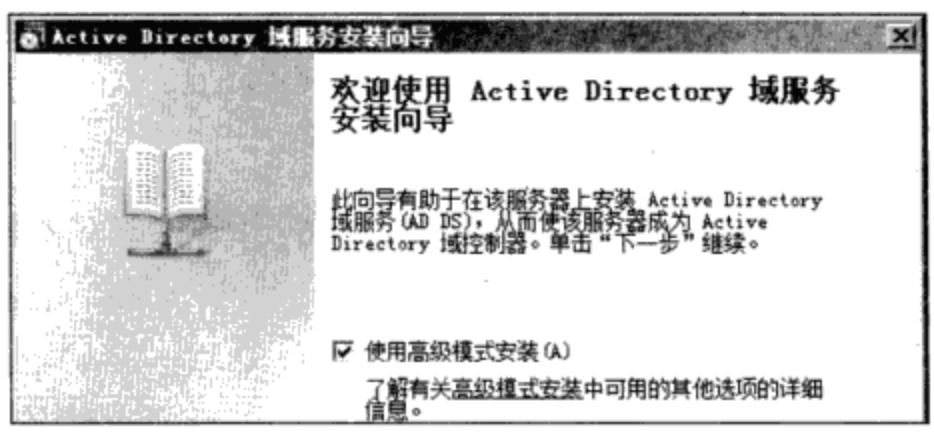


图 7-4

提示

您也可以不选择**使用高级模式安装**复选框，此时有一些设置会自动采用默认值，因此安装过程中与这些设置有关的界面不会出现。

STEP 11 当出现**操作系统兼容性**界面时单击下一步按钮。

STEP 12 如图 7-5所示选择**现有林**之下的**在现有林中新建域**单选按钮后单击下一步按钮。

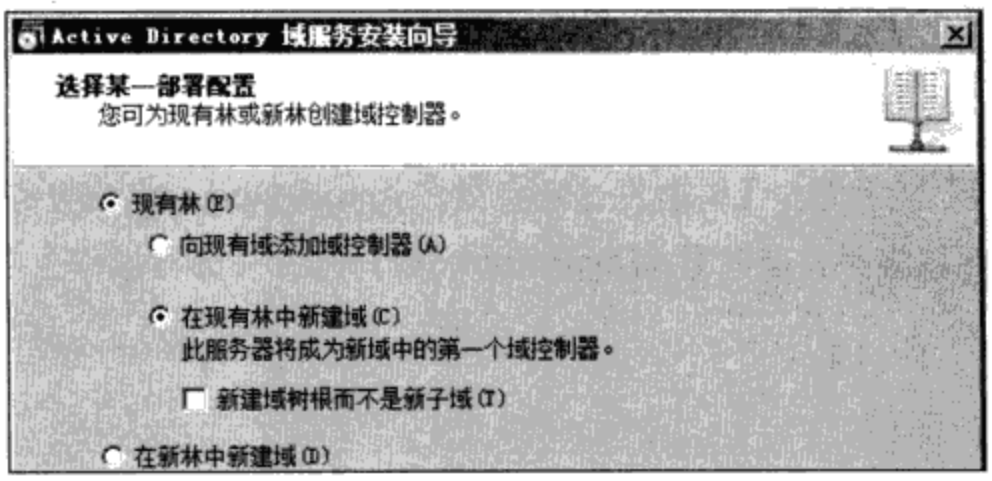


图 7-5

Download at http://www.pin5i.com/

STEP 13 在图 7-6中【输入域名sayms.com➲单击设置按钮➲输入Administrator和其密码后单击确定按钮➲单击下一步按钮】。

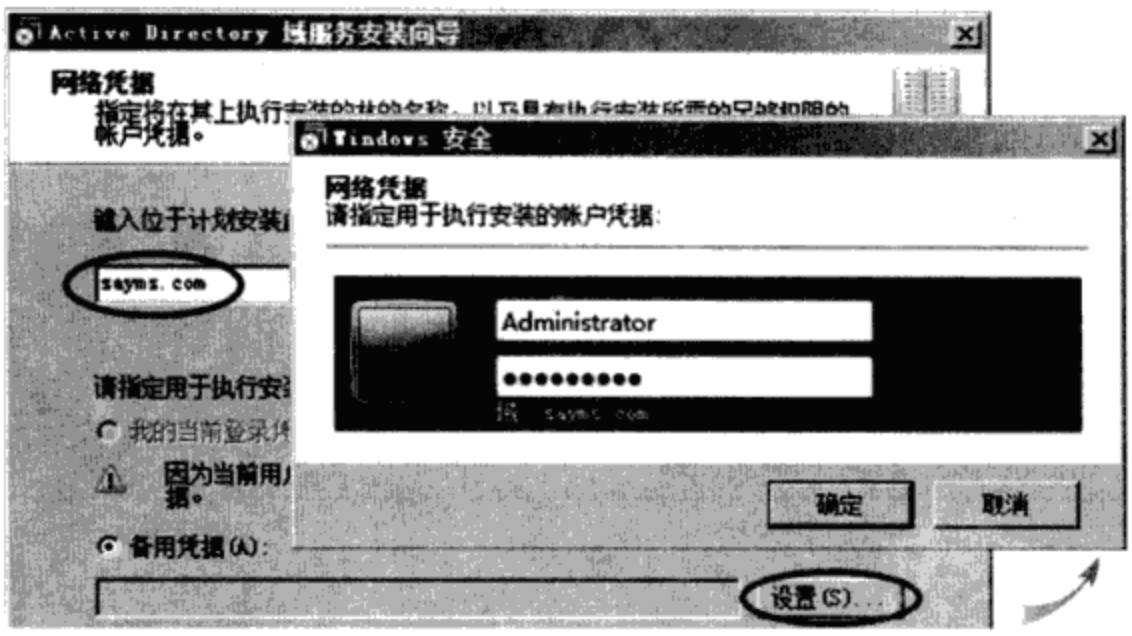


图 7-6

注意

图中输入林中任何一个域名都可以，安装向导只是要使用它来取得这个林中有哪一些域存在的信息。只有Enterprise Admins组内的用户有权限创建子域，若您现在所登录的账户不是隶属于此组的话（例如现在的登录账户为本地Administrator），就需要通过**备用凭据**来另外指定有权限的用户账户。

STEP 14 在图 7-7中的**父域的FQDN**文本框中输入sayms.com，在**子域的单标签DNS名称**文本框中输入hn，单击下一步按钮。

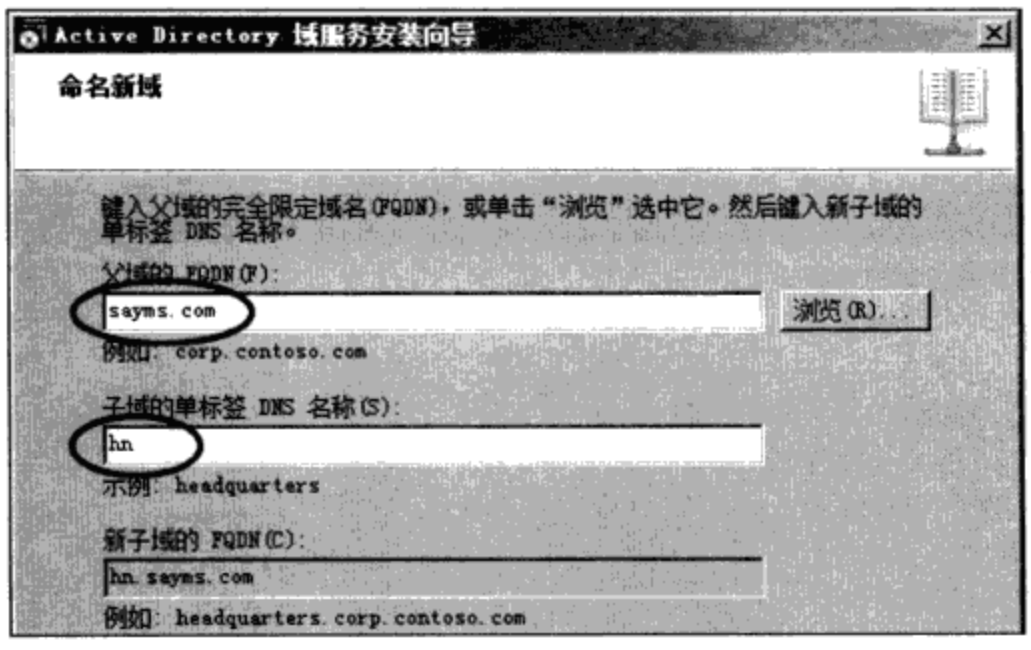


图 7-7

STEP 15 在图 7-8中单击下一步按钮。图中安装向导会为此子域设置一个NetBIOS格式的域

Download at http://www.pin5i.com/

名（不分大小写），它让Windows NT等不支持DNS域名的旧系统可以使用NetBIOS名称来访问此域的资源。默认的NetBIOS域名为DNS域名中第1个句点左边的文字，例如DNS名为hn.sayms.com，则NetBIOS名称为HN。

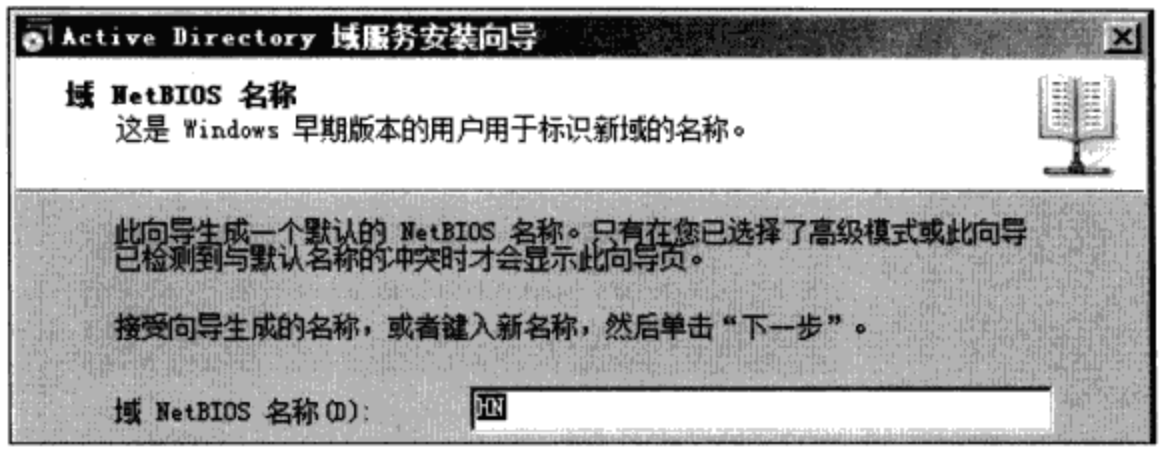


图7-8

STEP 16 在图 7-9中选择新域控制器所在的AD DS站点，目前只有一个默认的站点Default-First-Site-Name。请直接单击下一步按钮。

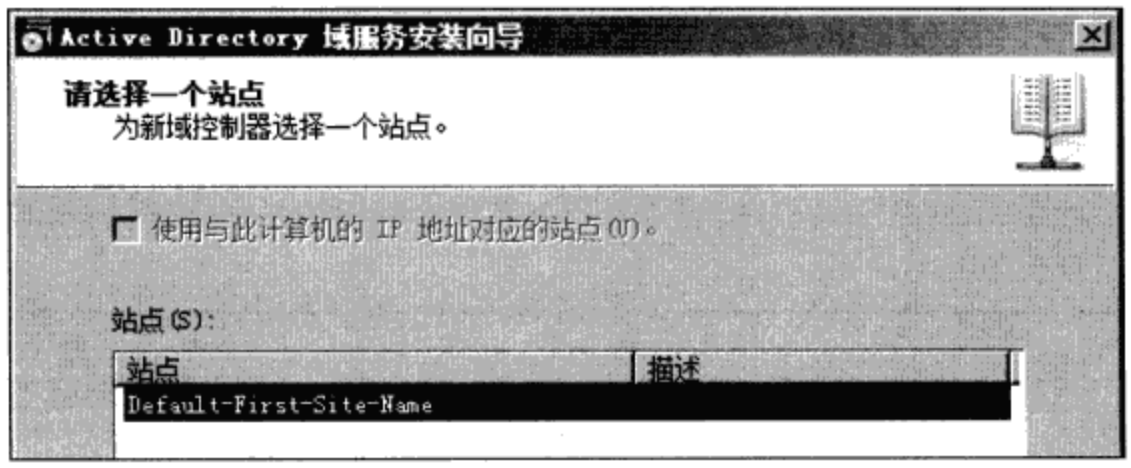


图7-9

STEP 17 在图 7-10中直接单击下一步按钮。由图中可知默认会在这台服务器上安装DNS服务器。

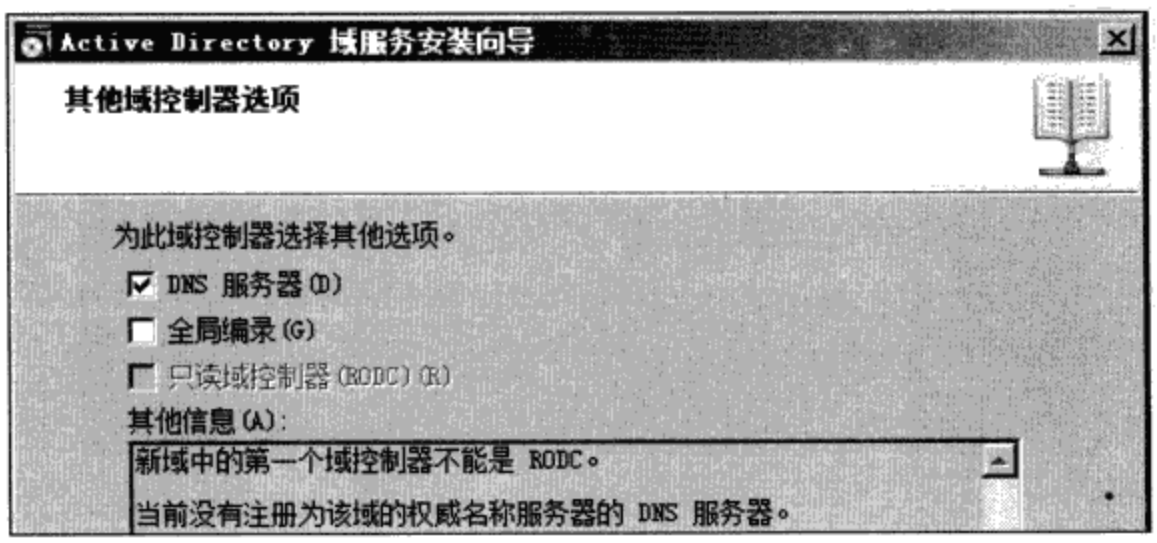


图7-10

Download at http://www.pin5i.com/

STEP 18 在图 7-11中单击下一步按钮来让向导自动选择AD DS数据库中的来源域控制器(或手动选择特定的域控制器)。



图 7-11

STEP 19 当出现数据库、日志文件和SYSVOL的位置界面时直接单击下一步按钮。

STEP 20 设置**目录服务还原模式**的系统管理员密码，完成后单击下一步按钮。注意密码必须符合复杂性需求，且至少7个字符。

STEP 21 在图 7-12中直接单击下一步按钮。

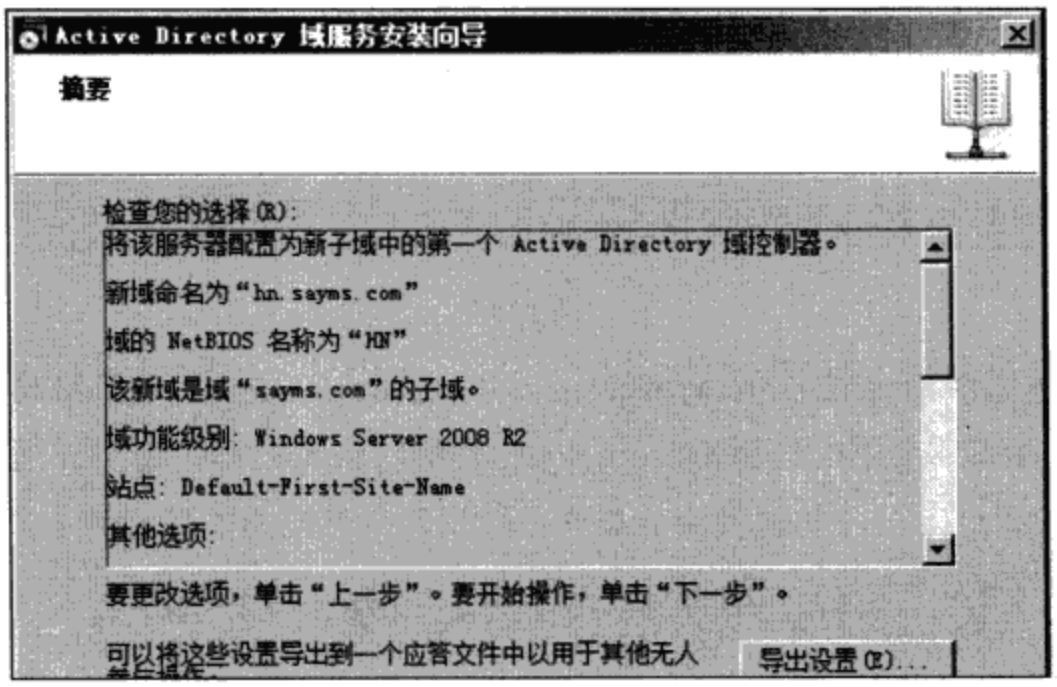


图 7-12

提示

您可以单击导出设置按钮来将设置存储为**应答文件**（Answer File），它可供利用dcpromo.exe来安装域控制器时使用，不过安装向导并不会将**目录服务还原模式**的系统管理员的密码存储到此文件。

STEP 22 可在图 7-13中选择**完成后重新启动**复选框或完成后手动重新启动。

Download at http://www.pin5i.com/

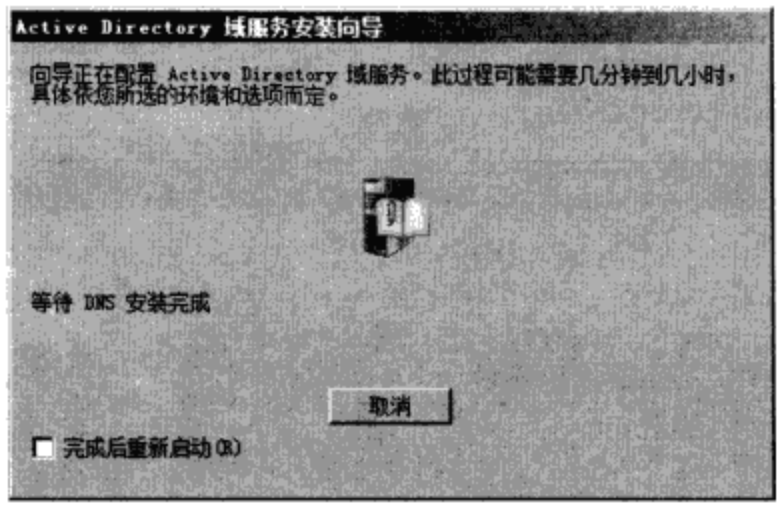


图 7-13

完成域控制器的安装后，因为它是此域中的第1台域控制器，故原本这台计算机内的本地用户账户会被移动到AD DS数据库内。由于这台域控制器同时也安装了DNS服务器，因此其内会自动创建如图 7-14所示的区域hn.sayms.com，用来提供此区域的查询服务。

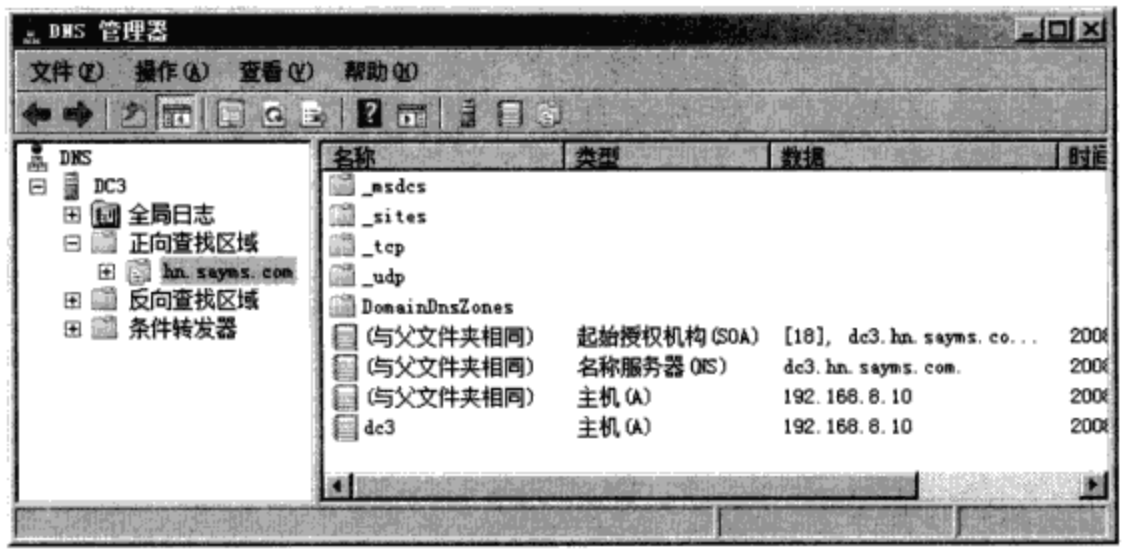


图 7-14

同时此台DNS服务器会将非hn.sayms.com域（包含sayms.com）的查询请求，通过**转发器**转给sayms.com的DNS服务器dc1.sayms.com（192.168.8.1）来处理，您可以通过【如图 7-15所示单击服务器DC3➲单击上方的**属性**图标➲单击**转发器**标签来查看此设置】的方法进行操作。

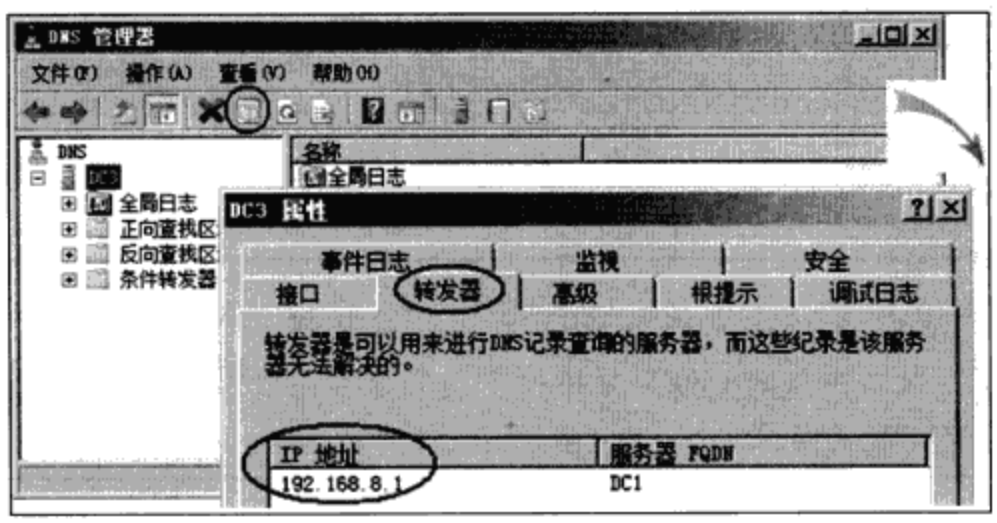


图 7-15

Download at http://www.pin5i.com/

另外这台服务器的**首选DNS服务器**会如图 7-16所示被改为指向自己，**备用DNS服务器**指向sayms.com的DNS服务器dc1.sayms.com（192.168.8.1）。

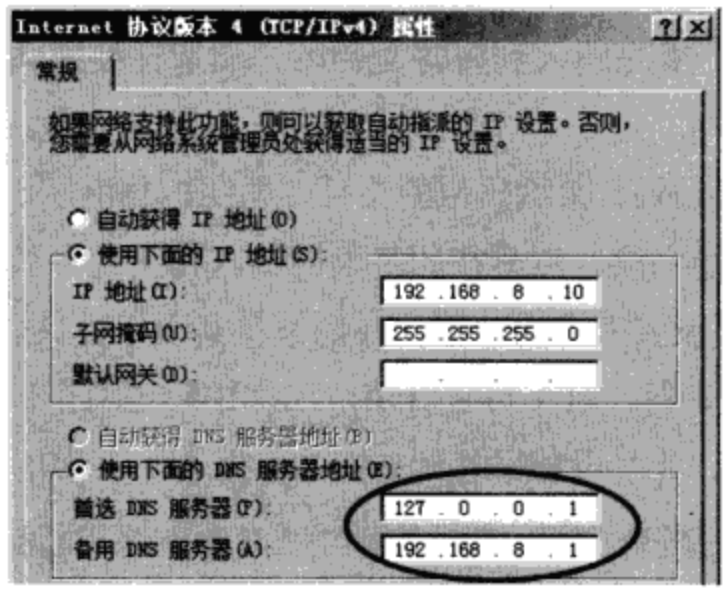


图 7-16

同时在sayms.com的DNS服务器dc1.sayms.com内也会自动在区域sayms.com之下创建如图7-17所示的委派域（hn）和名称服务器日志（NS），以便当它接收到查询hn.sayms.com的请求时，可以将此查询请求转给dc3.hn.sayms.com这台服务器来处理。

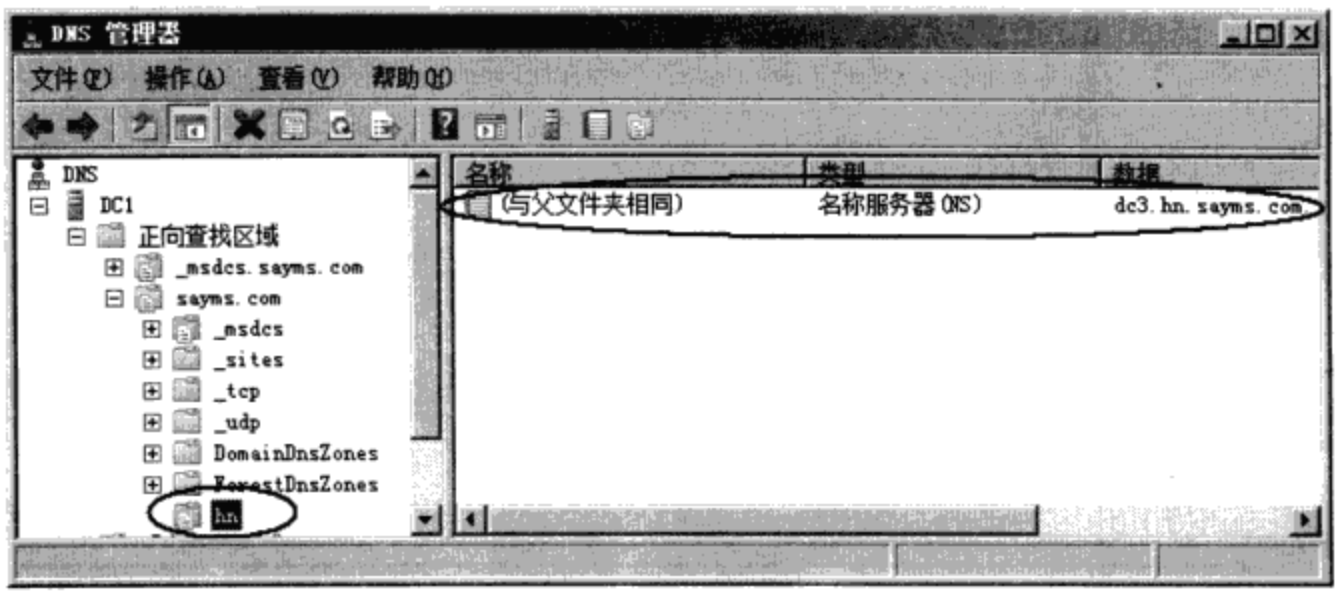


图 7-17

Q 根域sayms.com的用户，是否可以在隶属于子域hn.sayms.com的成员计算机上登录？子域hn.sayms.com的用户，是否可以在隶属于根域sayms.com的成员计算机上登录？

A 都可以，所有域内的用户，默认都可以在任何一个域内的成员计算机上登录，不过域控制器除外，因为默认只有隶属于Enterprise Admins组（位于林根域sayms.com内）的用户才有权限在所有域内的域控制器上登录，而每一个域的系统管理员（Domain Admins），虽然可以在所属域的域控制器上登录，但却不可以在其他域的域控制器上登录，除非另外被赋予**允许本地登录**的权限。

Download at http://www.pin5i.com/

7-2-2 使用应答文件来创建子域

在您通过将服务器升级为域控制器的方式来创建子域hn.sayms.com时，可以将升级时所必须提供给安装向导的数据，事先输入到**应答文件**内，然后让安装向导直接从应答文件来读取这些数据。

请使用**记事本**（notepad.exe）来编辑应答文件，如图 7-18所示，图中我们必须在此文件内创建一个名称为**DCInstall**的字段，然后在此字段内输入相关的参数和参数值，图中的参数说明请参考表 7-1。其中需要设置密码的参数，我们都将其设置为111aaAA，它符合域密码策略的要求，也就是：至少7个字符，且不可包含用户名称中超过两个以上的连续字符，还有至少要包含A～Z、a～z、0～9、非字母数字（例如!、$、#、%）等4组字符中的3组。



图 7-18

提示

其他更多的参数请参考微软网站的文件说明。

表 7-1

参数值	说明	参数值可为
ReplicaOrNewDomain	创建新域中的第1台域控制器、现有域中只读域控制器（RODC）或现有域中的其他域控制器	Domain、ReadOnlyReplica或Replica
NewDomain	指定新域的种类	Forest（新林的根域）、Tree（新树状目录的根域）、Child（现有林中的子域）
ParentDomainDNSName	父域的域名（FQDN）	例如sayms.com

Download at http://www.pin5i.com/

（续表）

参数值	说明	参数值可为
ChildName	子域的单标签域名	例如hn
DomainNetBiosName	NetBIOS域名	例如hn
DomainLevel	域功能级别	0（Windows 2000）、2（Windows Server 2003）、3（Windows Server 2008）、4（Windows Server 2008 R2）
SiteName	域控制器所在的站点名称	若未另外创建站点的话，则目前只有内置的第1个站点，站点名称为Default-First-Site-Name
InstallDNS	是否要安装DNS服务器	Yes或No
ConfirmGc	是否要将其设置为全局编录服务器	Yes或No
CreateDNSDelegation	是否要在上层创建委派域	Yes或No
DNSDelegationUserName	使用此账户和密码在上层域创建此子域的委派域	若未指定的话，则使用运行AD DS安装向导的用户账户和密码
DNSDelegationPassword		
UserDomain	使用此账户身份来将服务器升级为域控制器，此处包含用户的域、用户账户名称和密码	
UserName		
Password		
DatabasePath	设置AD DS数据库的存储路径	例如C:\Windows\NTDS，可使用环境变量，如%systemroot%\NTDS
LogPath	设置AD DS记录文件的存储路径	
SYSVOLPath	设置SYSVOL文件夹的路径	
SafeModeAdminPassword	安全模式（目录服务还原模式）的系统管理员密码	不可以为空白密码
RebootOnCompletion	安装完成后是否重新启动计算机	Yes或No

完成应答文件的创建后，请通过以下命令（参考图 7-19）来安装域控制器和创建子域，假设应答文件的文件名为answer.txt，且是位于C:\Test文件夹内：

```
dcpromo  /unattend:"C:\Test\answer.txt"
```

提示

dcpromo.exe读取到应答文件中所有的密码后，会自动将这些密码清除后再保存到应答文件内。



图 7-19

Download at http://www.pin5i.com/

7-2-3 使用命令行来创建子域

您可以通过【开始➲命令提示符】或单击左下角的**Windows PowerShell**图标，然后运行如下所示的**dcpromo.exe**命令来创建子域内的第一台域控制器（参考图 7-20）：

```
dcpromo /unattend /replicaOrNewDomain:domain /newDomain:child
/ParentDomainDNSName:sayms.com /childName:hn
/DomainNetbiosName:HN /domainLevel:4
/SiteName:Default-First-Site-Name /InstallDns:yes /confirmGC:no
/createDNSDelegation:yes
/DNSDelegationUserName:sayms.com\administrator
/DNSDelegationPassword:111aaAA /UserDomain:sayms.com
/UserName:sayms.com\administrator /Password:111aaAA
/databasePath:"%SystemRoot%\NTDS" /logPath:"%SystemRoot%\NTDS"
/sysvolpath:"%SystemRoot%\SYSVOL"
/safeModeAdminPassword:111aaAA /rebootOnCompletion:yes
```

提示

您可以使用 **dcpromo /?:Promotion** 来查看此命令的详细语法。



图 7-20

7-3 创建林中的第2个域树

在现有**林**中新建第2个（或更多个）**域树**的方法为：先创建此域树中的第一个域，而创建第一个域的方法是通过创建第一台域控制器的方式来实现。

假设我们要新建一个如图 7-21所示的域sayiis.com，由于这是该域树中的第一个域，所以它是这个新域树的根域。我们要将sayiis.com域树加入到林sayms.com中（sayms.com是第1个域

Download at http://www.pin5i.com/

树的根域的域名，也是整个林的林名称）。

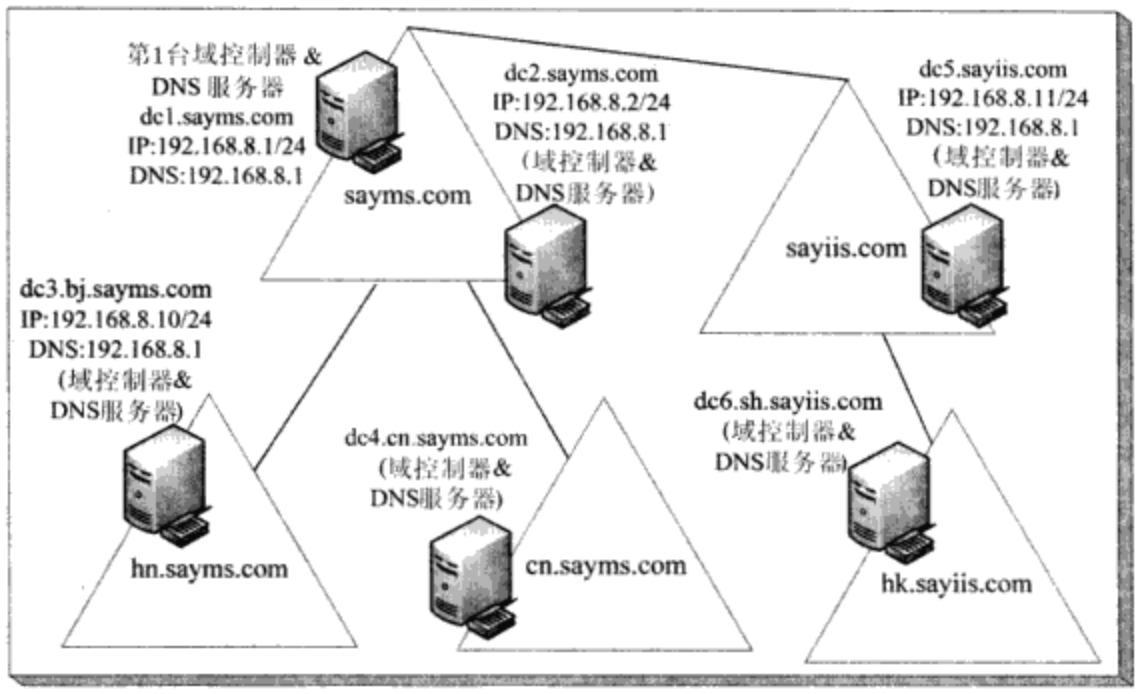


图 7-21

以下我们将通过创建图 7-21中域控制器dc5.sayiis.com的方式来创建第2个域树。

7-3-1 选择适当的DNS架构

若要将sayiis.com域树加入到林sayms.com中的话，就必须在创建域控制器dc5.sayiis.com时能够通过DNS服务器来找到林中的**域命名操作主机**（Domain Naming Operations Master），否则无法创建域sayiis.com。**域命名操作主机**默认是由林中第1台域控制器所扮演（详细说明见第10章），以图 7-21为例，它就是dc1.sayms.com。

还有在DNS服务器内必须有一个名称为sayiis.com的**主要查找区域**，以便让域sayiis.com的域控制器能够将自己注册到此区域内。域sayiis.com和sayms.com可以使用同一台DNS服务器，也可以各自使用不同的DNS服务器。

1. 使用同一台 DNS 服务器

请在这台DNS服务器内另外创建一个名为sayiis.com的主要区域，并启用动态更新功能。此时这台DNS服务器内同时拥有sayms.com和sayiis.com两个区域，如此sayms.com和sayiis.com内的计算机和域控制器都可以通过此台DNS服务器来找到对方。

2. 各自使用不同的 DNS 服务器，并通过区域传送来复制日志

请在此台DNS服务器（见图 7-22右半部）内创建一个名为sayiis.com的主要区域，并启用动态更新功能，您还需要在此台DNS服务器内另外创建一个名为sayms.com的辅助区域，此区域内的日志需要通过**区域传送**功能从域sayms.com的DNS服务器（图 7-22左半部）复制过来，

Download at http://www.pin5i.com/

它让域sayiis.com内的计算机和域控制器可以找到域sayms.com内的计算机和域控制器。

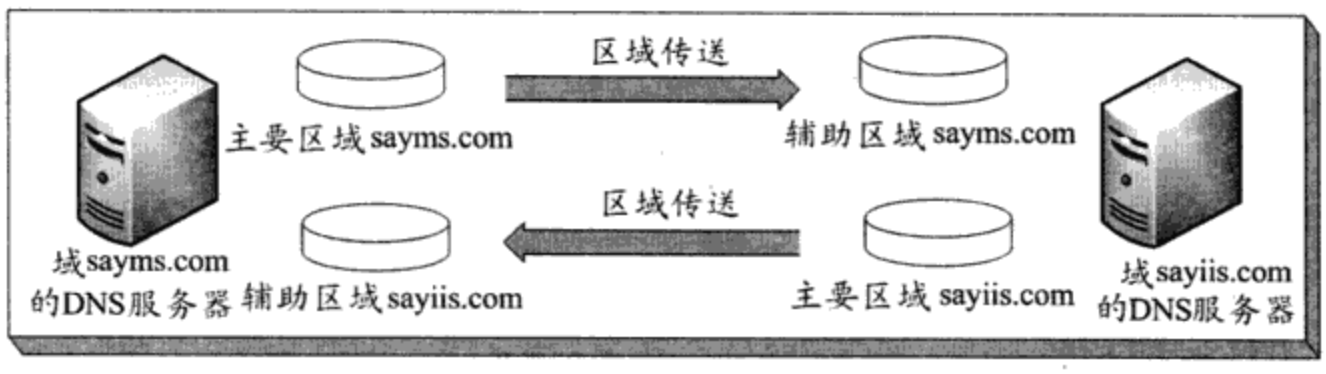


图 7-22

同时您也需要在域sayms.com的DNS服务器内另外创建一个名为sayiis.com的辅助区域，此区域内的日志也需要通过**区域传送**功能从域sayiis.com的DNS服务器复制过来，它让域sayms.com内的计算机和域控制器可以找到域sayiis.com内的计算机和域控制器。

3. 其他情况

我们前面所搭建的sayms.com域环境是将DNS服务器直接安装到域控制器上，因此其内会自动创建一个DNS区域sayms.com（如图 7-23所示中左边的Active Directory集成区域sayms.com），接下来当您要安装sayiis.com的第1台域控制器时，其默认也会在这台服务器上安装DNS服务器，并自动创建一个DNS区域sayiis.com（如图 7-23所示中右边的Active Directory集成区域sayiis.com），而且还会自动设置转发器来将其他区域（包含sayms.com）的查询请求转给图中左边的DNS服务器，因此sayiis.com内的计算机和域控制器可以通过右边的DNS服务器来同时查询sayms.com和sayiis.com区域内的计算机和域控制器。

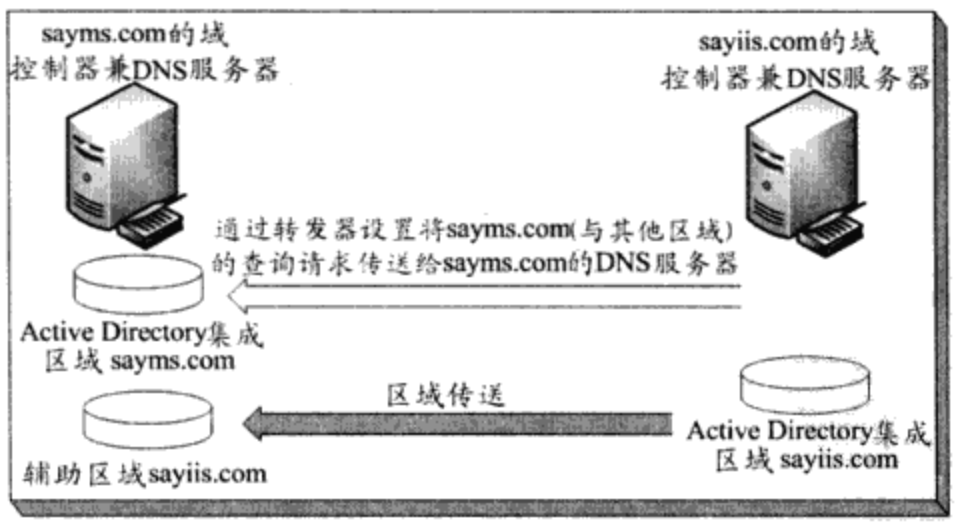


图 7-23

不过您还必须在左边的DNS服务器内自行创建一个sayiis.com辅助区域，此区域内的日志需要通过**区域传送**从右边的DNS服务器复制过来，它让域sayms.com内的计算机和域控制器可以找到域sayiis.com内的计算机和域控制器。

Download at http://www.pin5i.com/

> **注意**
>
> 您也可以在左边的DNS服务器内，通过**条件转发器**只将sayiis.com的查询转给右边的DNS服务器，如此就可以不需要创建辅助区域sayiis.com，也不需要区域传送。注意由于右边的DNS服务器已经使用**转发器**设置将sayiis.com之外的所有其他区域的查询，转发给左边的DNS服务器，因此左边DNS服务器请使用**条件转发器**，而不要使用一般的**转发器**，否则除了sayms.com和sayiis.com两个区域之外，其他区域的查询将会在这两台DNS服务器之间循环。

7-3-2 使用Windows窗口来创建第2个域树

以下采用如图 7-23所示的DNS架构来创建林中第2个域树sayiis.com，并且是通过将图 7-21中的dc5.sayiis.com升级为域控制器的方式来创建域树sayiis.com，这台服务器可以是独立服务器或隶属于其他域的现有成员服务器。

STEP 1 请先在图 7-21右上角的服务器dc5.sayiis.com上安装Windows Server 2008 R2，将其计算机名设置为dc5，IPv4地址等依照图示来设置（图中采用TCP/IPv4）。注意将计算机名设置为dc5即可，等升级为域控制器后，它就会自动被改为dc5.sayiis.com。还有**首选DNS服务器**的IP地址请指定到192.168.8.1，以便通过它来找到林中的**域命名操作主机**（也就是第一台域控制器dc1），等dc5升级为域控制器和安装DNS服务器后，系统会自动将其**首选DNS服务器**的IP地址改为自己（127.0.0.1）。

STEP 2 在这台服务器上选择以下两种方式之一来安装**Active Directory域服务**（AD DS）。

- 单击左下角的服务器管理器图标：此时请跳到**STEP 3**。
- 通过【开始➲运行➲输入dcpromo后单击确定按钮】的方法：此时它会自动运行**STEP 3** ~ **STEP 9**的安装AD DS步骤，故请直接跳到**STEP 10**。

STEP 3 单击左边的**角色**，单击**添加角色**。

STEP 4 当出现**开始之前**界面时单击下一步按钮。

STEP 5 在图 7-24中选择**Active Directory域服务**，在弹出的界面中单击**添加必需的功能**，单击下一步按钮。



图 7-24

Download at http://www.pin5i.com/

STEP 6 在**Active Directory域服务**界面中单击下一步按钮。

STEP 7 在**确认安装选择**界面中单击安装按钮。

STEP 8 当出现**安装结果**界面时单击关闭按钮。

STEP 9 如图 7-25所示，通过【单击左边角色处的**Active Directory域服务**选项➲单击右边的**运行Active Directory域服务安装向导（dcpromo.exe）**】的方法进行操作。

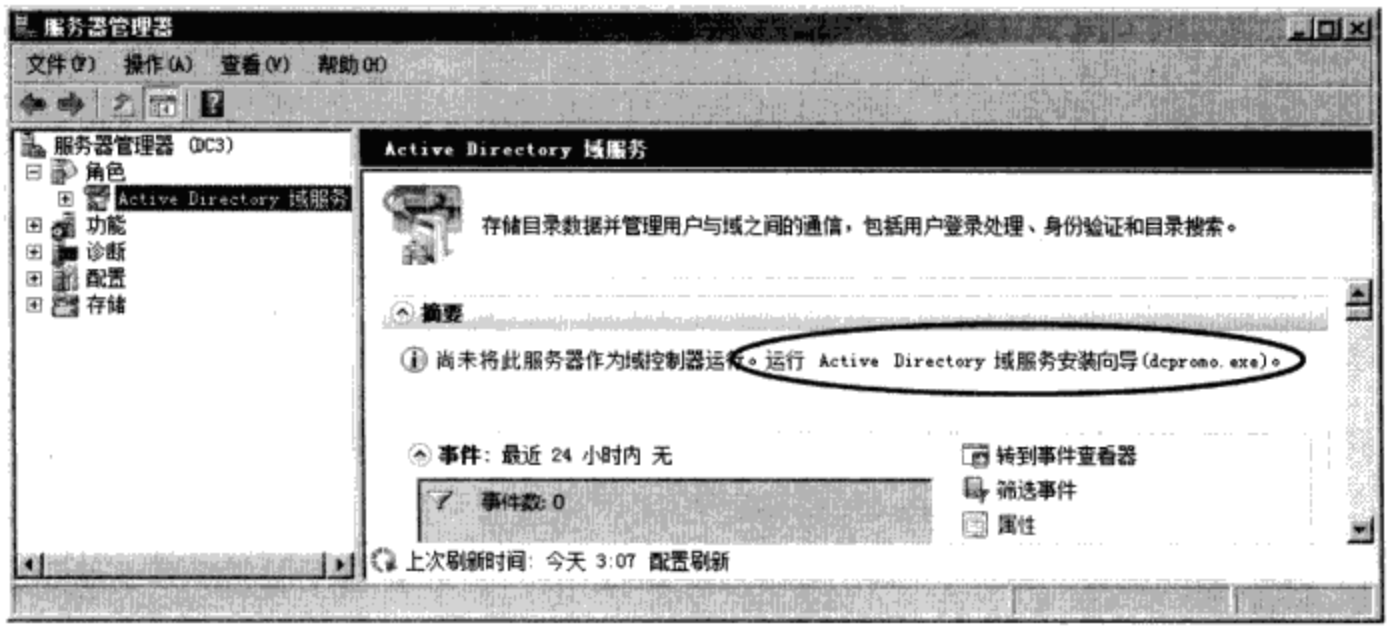


图 7-25

STEP 10 如图 7-26所示选择**使用高级模式安装**复选框后单击下一步按钮。

> **提示**
>
> 您也可以不选择**使用高级模式安装**复选框，此时有一些设置会自动采用默认值，因此安装过程中和这些设置有关的界面不会出现。

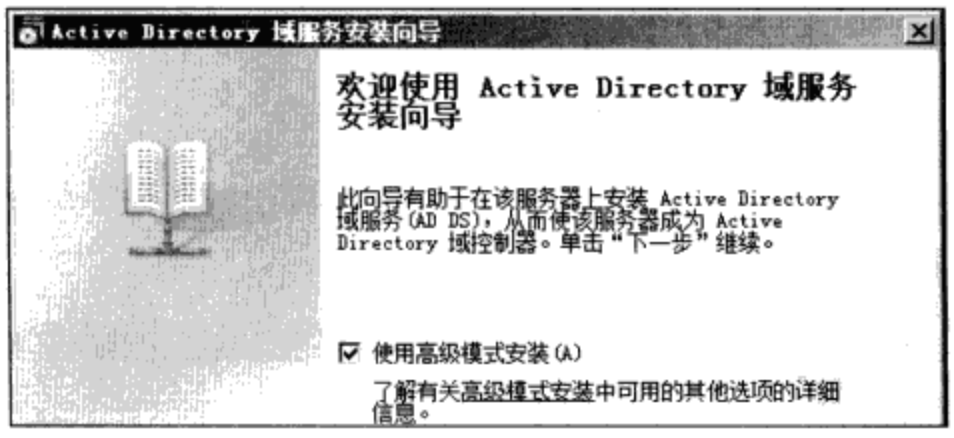


图 7-26

STEP 11 当出现**操作系统兼容性**界面时单击下一步按钮。

STEP 12 如图 7-27所示选择**现有林**之下的**在现有林中新建域**单选按钮，选择**新建域树根而不是新子域**复选框，单击下一步按钮。

Download at http://www.pin5i.com/

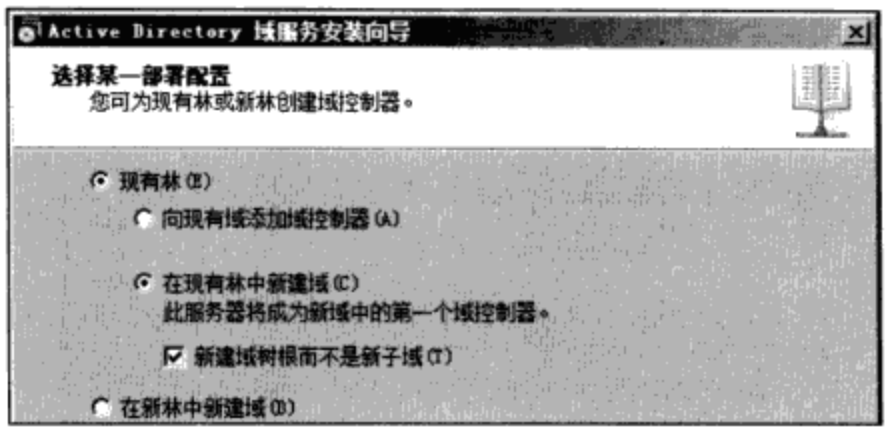


图 7-27

STEP 13 在图 7-28中，通过【输入域名sayms.com➲单击设置按钮➲输入Administrator和其密码后单击确定按钮➲单击下一步按钮】的方式进行操作。

注意

图中输入林中任何一个域名都可以，安装向导只是要使用它来取得这个林中有哪一些域存在的信息。只有Enterprise Admins组内的用户有权限创建新域树，若您现在所登录的账户不属于此组的话（例如现在登录的账户为本地Administrator），就需要通过**备用凭据**来另外指定有权限的用户账户。



图 7-28

STEP 14 在图 7-29中输入新域树的根域的域名sayiis.com后单击下一步按钮。

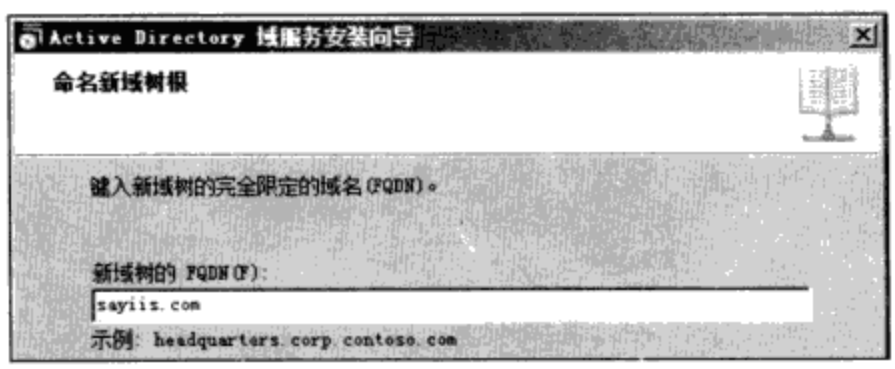


图 7-29

Download at http://www.pin5i.com/

STEP 15 在图 7-30中安装向导会为此域设置一个NetBIOS格式的域名（不分大小写），默认的NetBIOS域名为DNS域名sayiis.com中第1个句点左边的文字，也就是SAYIIS。



图 7-30

STEP 16 在图 7-31中选择新域控制器所在的AD DS站点，目前只有一个默认的站点Default-First-Site-Name，请直接单击 下一步 按钮。

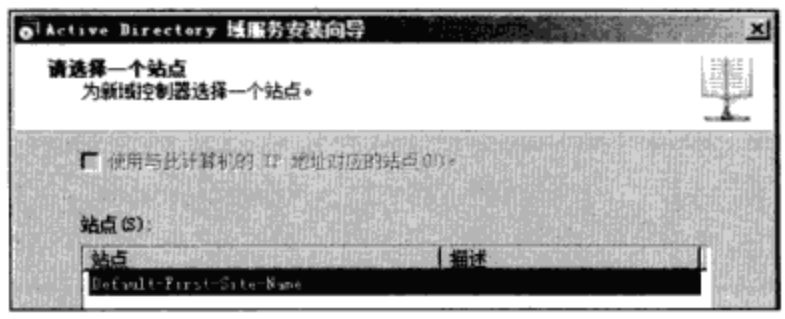


图 7-31

STEP 17 在图 7-32中直接单击 下一步 按钮来采用默认值（安装DNS服务器）。

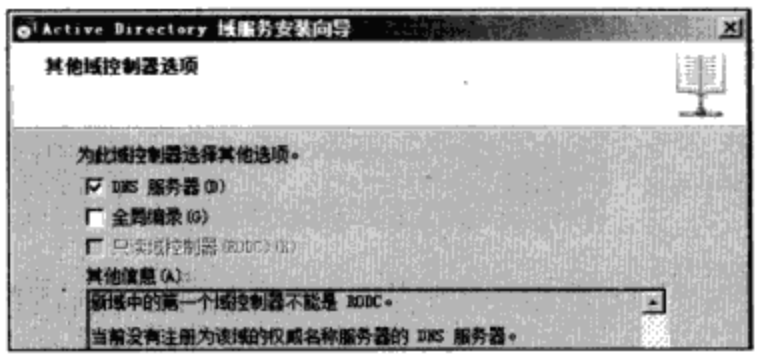


图 7-32

STEP 18 若出现如图7-33所示的对话框的话，表示安装向导找不到父域，因而无法设置父域将查询sayiis.com的工作分配给此台DNS服务器，然而此sayiis.com为根域，它并不需要通过父域来分配，故请直接单击 是（Y） 按钮即可。

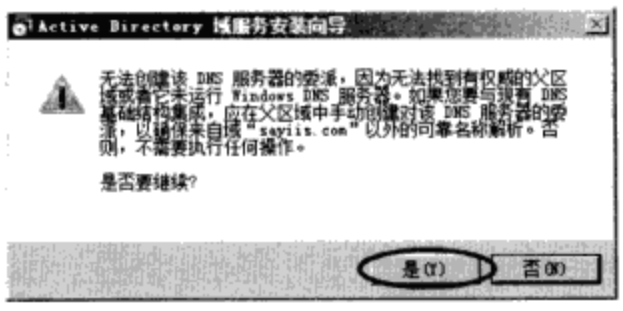


图 7-33

Download at http://www.pin5i.com/

STEP 19 在图 7-34中单击下一步按钮来让向导自动选择AD DS数据库的源域控制器（或手动选择特定的域控制器）。



图 7-34

STEP 20 当出现数据库、日志文件和SYSVOL的位置界面时直接单击下一步按钮。

STEP 21 设置**目录服务还原模式**的系统管理员密码，完成后单击下一步按钮。注意密码必须符合复杂性需求，且至少7个字符。

STEP 22 在图 7-35中直接单击下一步按钮。

提示

您可以单击导出设置按钮来将设置存储为**应答文件**（Answer File），它可供利用dcpromo.exe来安装域控制器时使用，不过安装向导并不会将**目录服务还原模式**的系统管理员的密码存储到此文件。

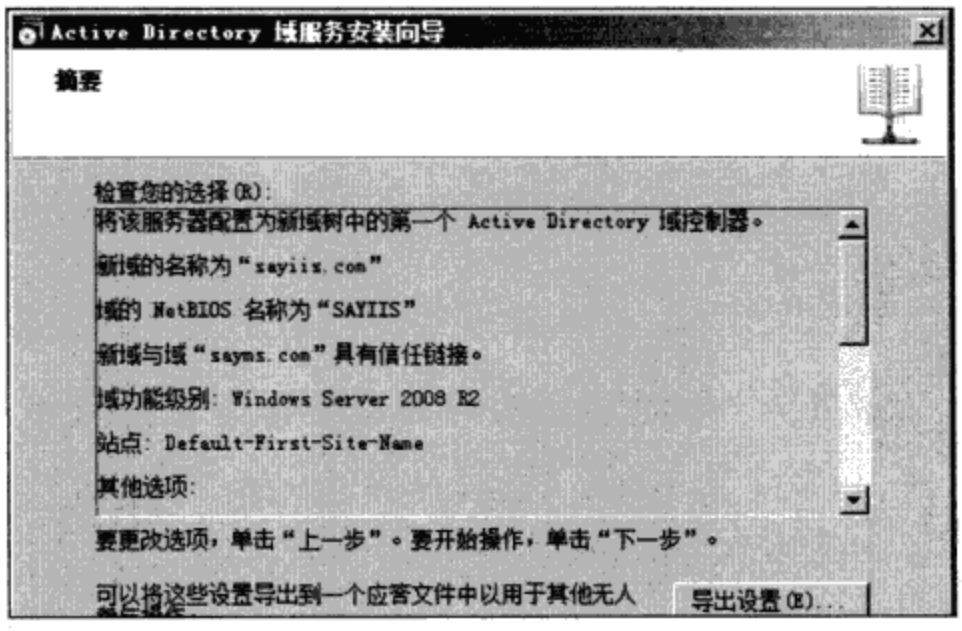


图 7-35

STEP 23 可在图 7-36中选择**完成后重新启动**复选框或完成后手动重新启动。

Download at http://www.pin5i.com/

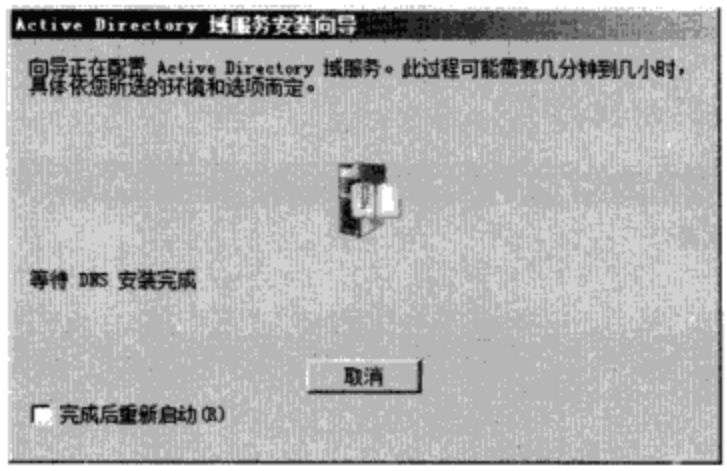


图 7-36

完成域控制器的安装后，因为它是此域中的第1台域控制器，故原本这台计算机内的本地用户账户会被移动到AD DS数据库内。另外它同时也安装了DNS服务器，其内会自动创建如图7-37所示的区域sayiis.com，用来提供此区域的查询服务。

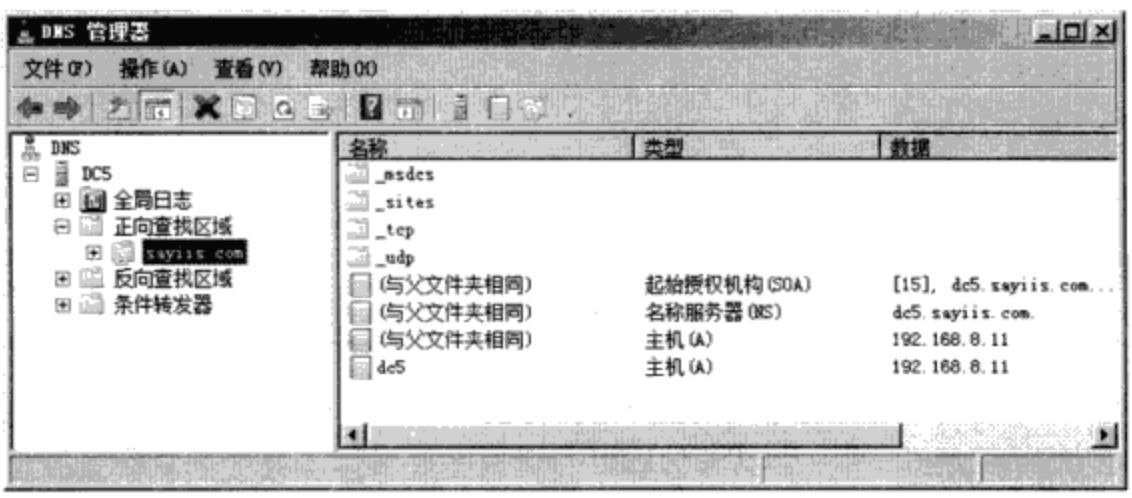


图 7-37

此DNS服务器会将非sayiis.com的所有其他区域（包含sayms.com）的查询请求通过**转发器**传送给sayms.com的DNS服务器（IP地址为192.168.8.1），而您可以在DNS管理控制面板内通过【如图7-38所示单击服务器DC5➲单击上方的**属性**图标➲单击**转发器**标签】的方式来查看此设置。

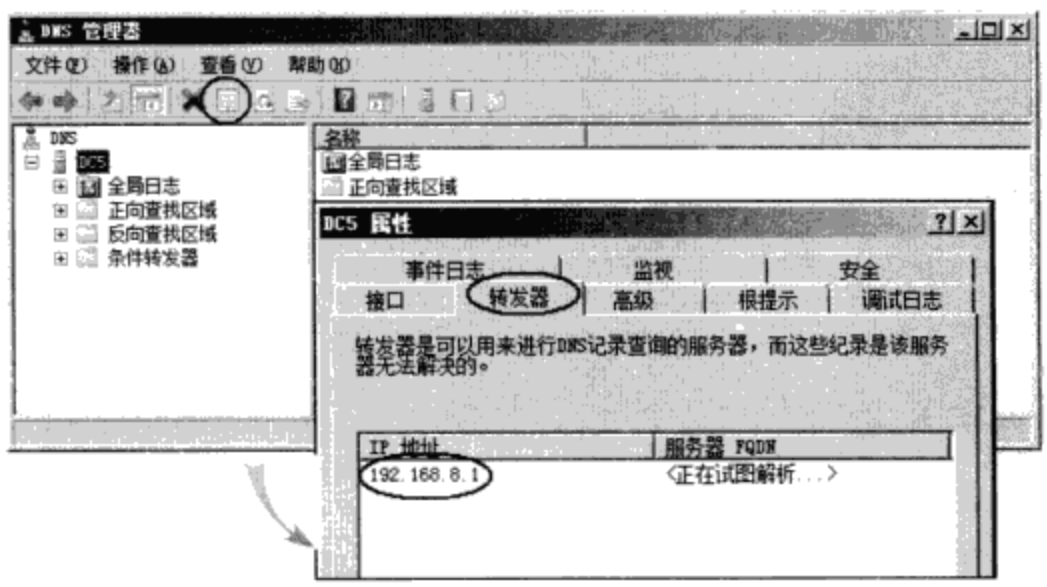


图 7-38

Download at http://www.pin5i.com/

这台服务器的**首选DNS服务器**的IP地址如图7-39所示，被自动改为指向自己（127.0.0.1），而原本位于**首选DNS服务器**的IP地址（192.168.8.1）会被设置在**备用DNS服务器**。

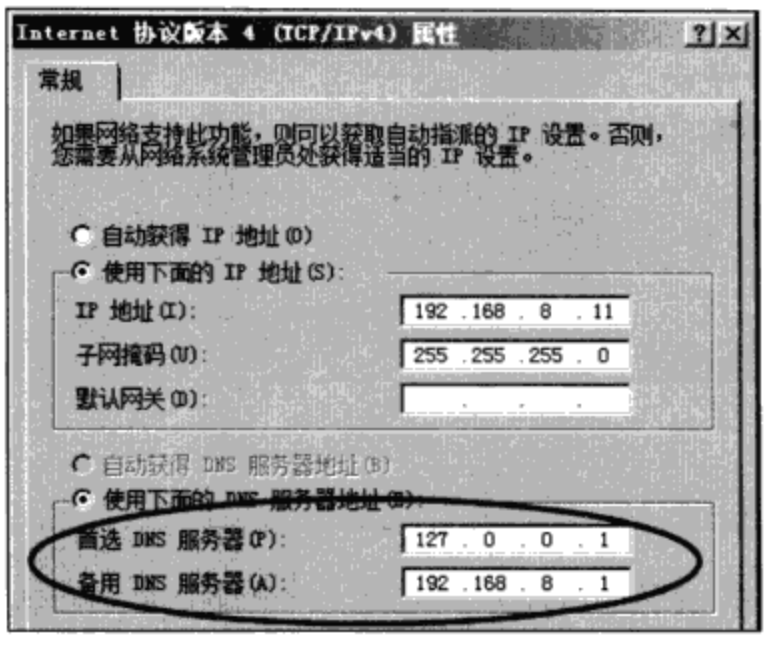


图 7-39

然后要到DNS服务器dc1.sayms.com内创建一个辅助区域sayiis.com，以便让域sayms.com内的计算机可以查找到域sayiis.com内的计算机。此区域内的记录是通过**区域传送**功能从dc5.sayiis.com复制过来，不过我们需要先在dc5.sayiis.com中设置允许此区域内的日志可以**区域传送**给dc1.sayms.com （192.168.8.1），如图 7-40所示：【单击区域sayiis.com➲单击上方的**属性**图标➲单击**区域传送**标签】来设置。

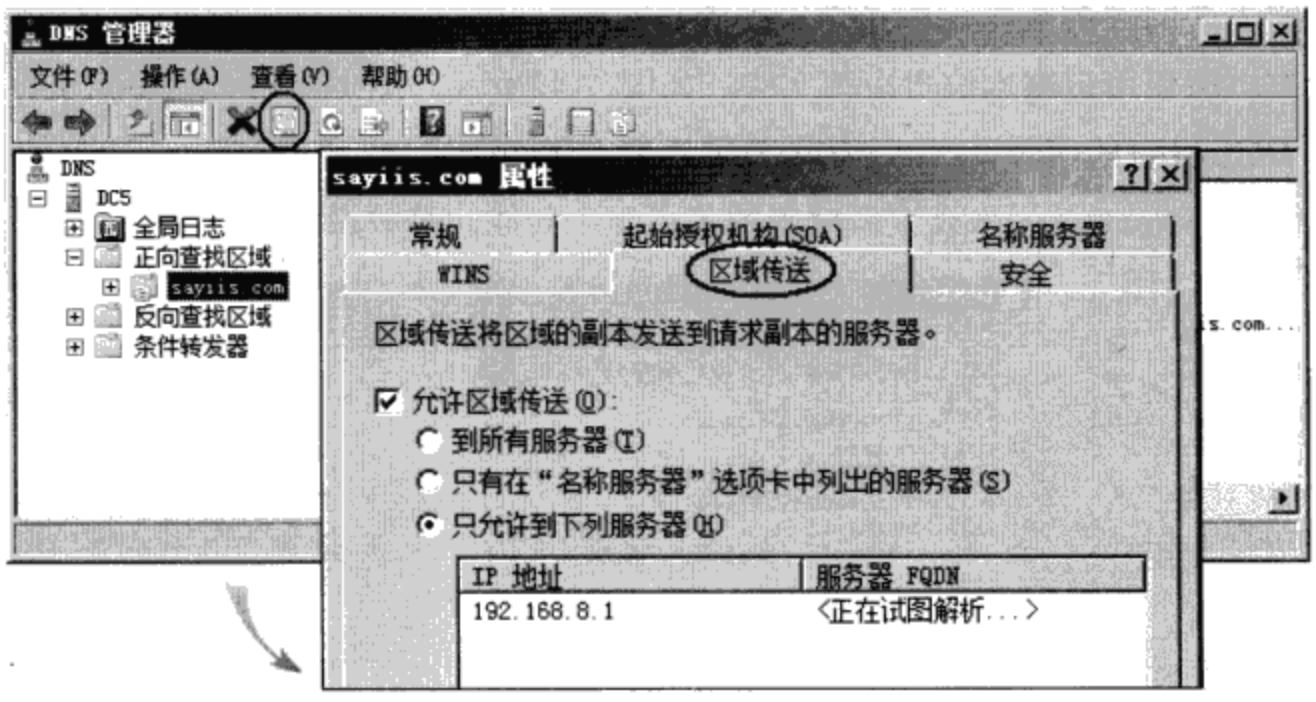


图 7-40

接下来到dc1.sayms.com这台DNS服务器上新建正向辅助区域sayiis.com，并选择从dc5.sayiis.com（192.168.8.11）来运行**区域传送**操作，也就是其**主机服务器**是dc5.sayiis.com（192.168.8.11），图 7-41为完成后的界面。

Download at http://www.pin5i.com/

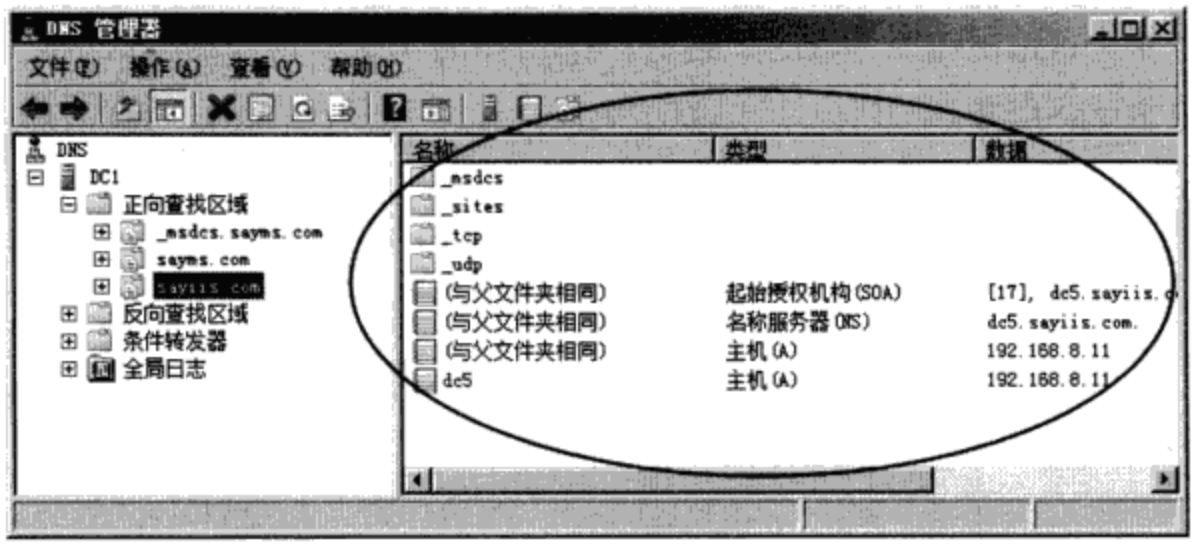


图 7-41

提示

1. 若区域sayiis.com前出现红色X符号的话，请先确认dc5.sayiis.com已允许区域传送给dc1.sayms.com，然后【对着sayiis.com区域右击➲选择**从主服务器传送**或**从主服务器加载**】。
2. 若要在sayiis.com之下创建子域hk.sayiis.com的话，请将dc6.hk.sayiis.com的**首选DNS服务器**指定到dc5.sayiis.com （192.168.8.11）。

7-3-3 使用应答文件来创建第2个域树

在您通过将服务器升级为域控制器的方式来创建第2个域树sayiis.com时，可以将升级时所必须提供给安装向导的数据，事先输入到**应答文件**内，然后让安装向导直接从应答文件来读取这些数据。请使用**记事本**编辑应答文件，如图 7-42所示，图中我们必须在此文件内创建一个名称为**DCInstall**的字段，然后在此字段内输入相关的参数和参数值，图中的参数除了NewDomainDNSName是用来设置新域的域名之外，其他的参数说明请参考前面的表 7-1。



图 7-42

Download at http://www.pin5i.com/

完成应答文件的创建后，请通过以下命令（参考图 7-43）来安装域控制器和创建第2个域树，假设应答文件的文件名为answer.txt，且此文件位于C:\Test文件夹内：

```
dcpromo  /unattend:"C:\Test\answer.txt"
```

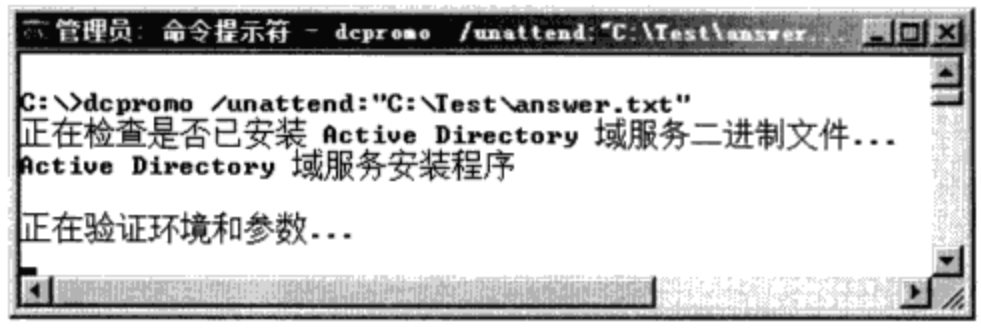


图 7-43

提示

dcpromo.exe读取到应答文件中所有的密码后，会自动将这些密码清除后再保存到应答文件内。其他关于转发器与在dc1.sayms.com中创建辅助区域的说明，请参考前一小节的内容。

7-3-4 使用命令行来创建第2个域树

您可通过【开始➲命令提示符】或单击左下角的**Windows PowerShell**图标，然后运行如下所示的**dcpromo.exe**命令来创建第2个域树（参考图 7-44）：

```
dcpromo /unattend /replicaOrNewDomain:domain /newDomain:tree
/NewDomainDNSName:sayiis.com /DomainNetbiosName:SAYIIS
/domainLevel:4 /SiteName:Default-First-Site-Name /InstallDns:yes
/confirmGC:no /createDNSDelegation:no /UserDomain:sayms.com
/UserName:sayms.com\administrator /Password:111aaAA
/databasePath:"%SystemRoot%\NTDS" /logPath:"%SystemRoot%\NTDS"
/sysvolpath:"%SystemRoot%\SYSVOL"
/safeModeAdminPassword:111aaAA /rebootOnCompletion:yes
```



图 7-44

Download at http://www.pin5i.com/

7-4 删除子域和域树

我们将使用图 7-45中左下角的域hn.sayms.com来说明如何删除子域，同时使用右边的域sayiis.com来说明如何删除域树。删除的方式是将域中的最后一台域控制器降级，也就是将AD DS 从该域控制器删除。至于如何删除额外域控制器dc2.sayms.com与域sayms.com的说明已经在第2章介绍过了，此处不再重复。

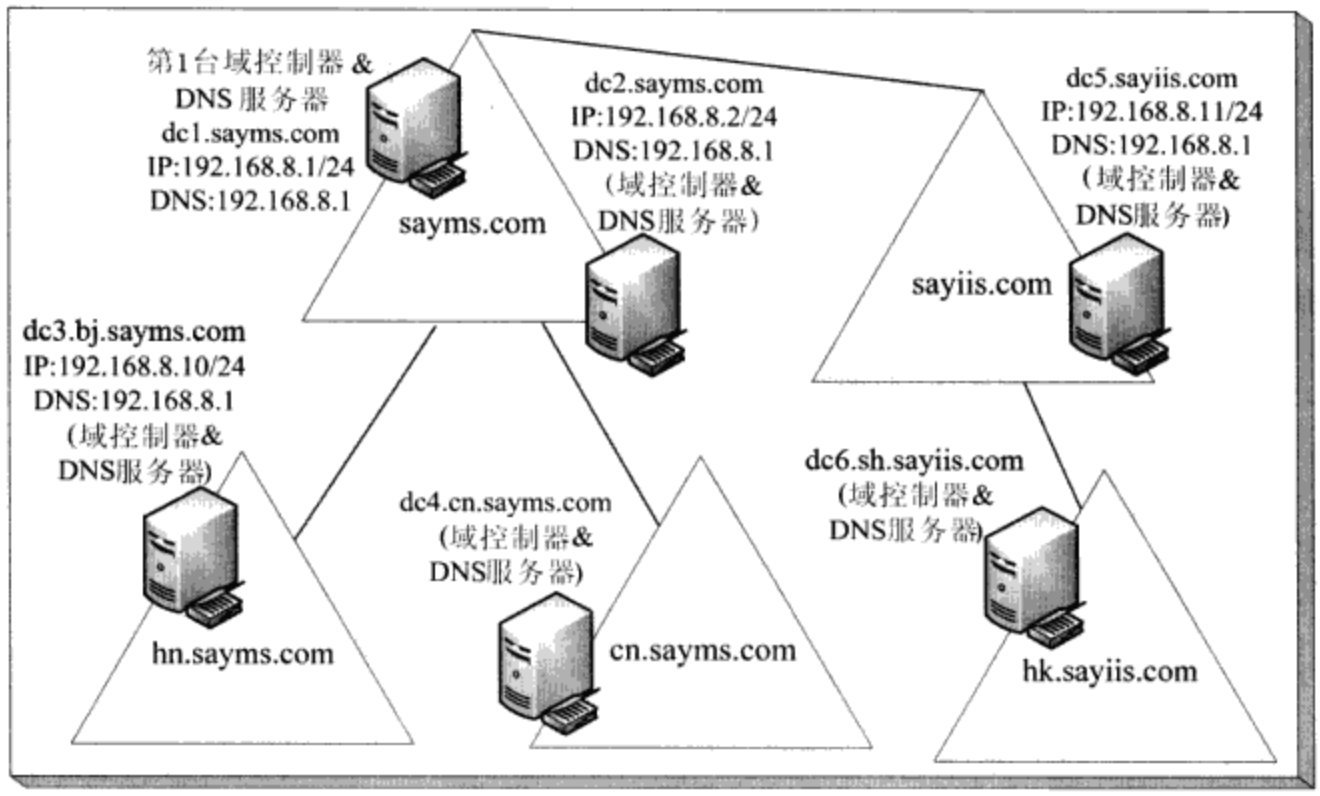


图 7-45

7-4-1 使用Windows窗口来删除子域或域树

必须是Enterprise Admins组内的用户才有权限删除子域或域树。由于删除子域和域树的步骤相似，因此以删除子域hn.sayms.com为例进行说明，而且假设图中的dc3.hn.sayms.com是这个域中的最后一台域控制器。

> **注意**
>
> 若删除（降级）失败的话，可参考第10-5节的说明。

STEP 1 请到图 7-45中的域控制器dc3.hn.sayms.com上登录，然后选择【开始➲运行➲输入**dcpromo**后单击确定按钮】。

STEP 2 在**欢迎使用Active Directory域服务安装向导**对话框中直接单击下一步按钮。

STEP 3 若出现如图 7-46所示对话框的话（表示这台域控制器是**全局编录服务器**），请直接单击确定按钮。

Download at http://www.pin5i.com/

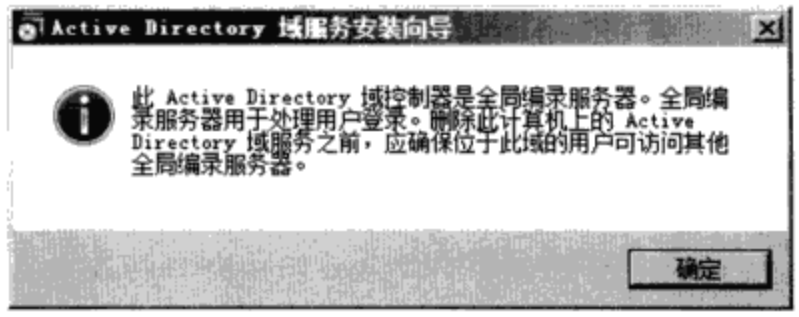


图 7-46

STEP 4 在图 7-47中选择**删除该域，因为此服务器是该域中的最后一个域控制器**复选框后单击下一步按钮，降级后这台服务器将变成独立服务器。

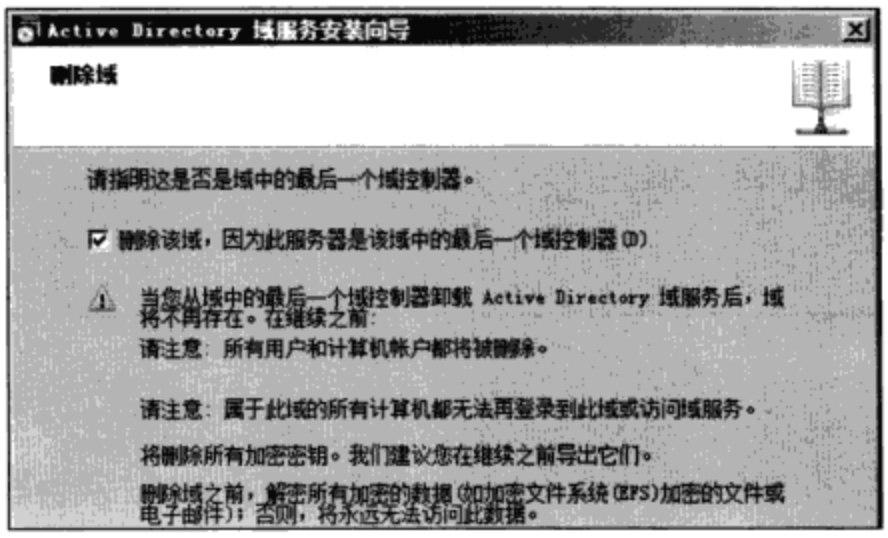


图 7-47

STEP 5 如果没有出现如图 7-48所示对话框的话，请直接跳到**STEP 9**。图 7-48表示这台域控制器内含可写入的Active Directory集成DNS区域（不包含RODC的只读DNS区域），安装向导会将此区域的**应用程序目录分区**删除。若此界面出现其他应用程序所创建的**应用程序目录分区**的话，请尽量先使用该应用程序所提供的工具程序（如果有的话）来删除此**应用程序目录分区**，单击下一步按钮。

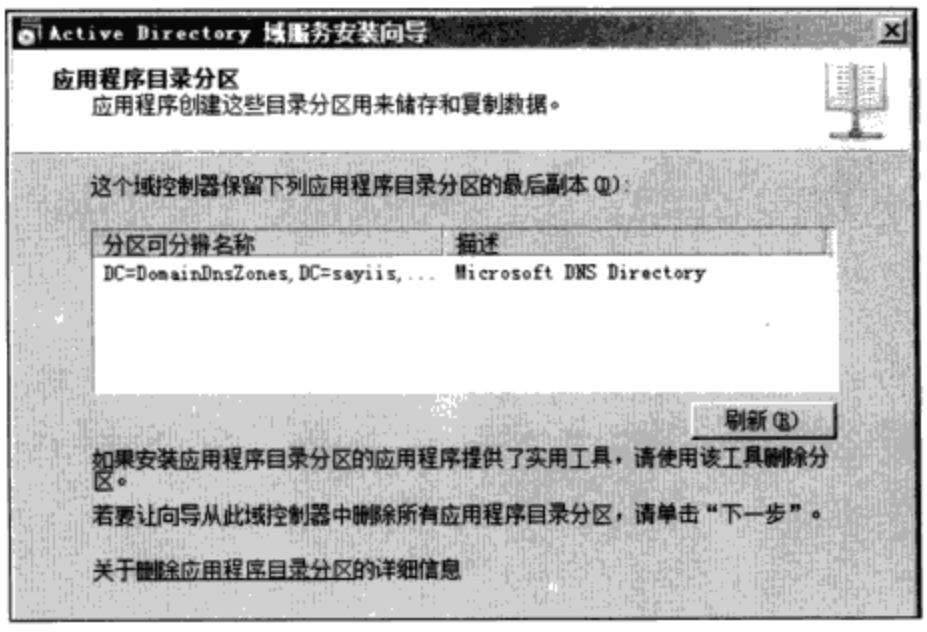


图 7-48

Download at http://www.pin5i.com/

STEP 6 选择图 7-49中的选项后单击下一步按钮。它会将此域控制器中所有的**应用程序目录分区**删除。

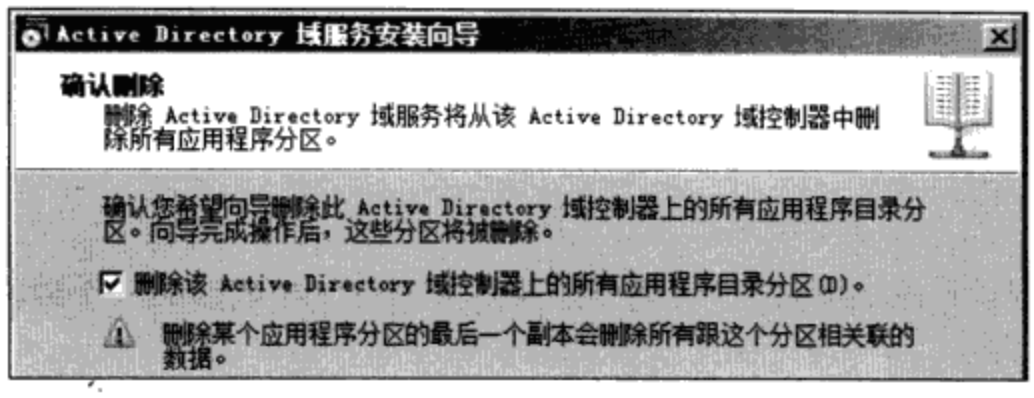


图 7-49

STEP 7 在图 7-50中，通过【输入域名sayms.com➲单击设置按钮➲输入Administrator和其密码后单击确定按钮➲单击下一步按钮】的方式进行操作。

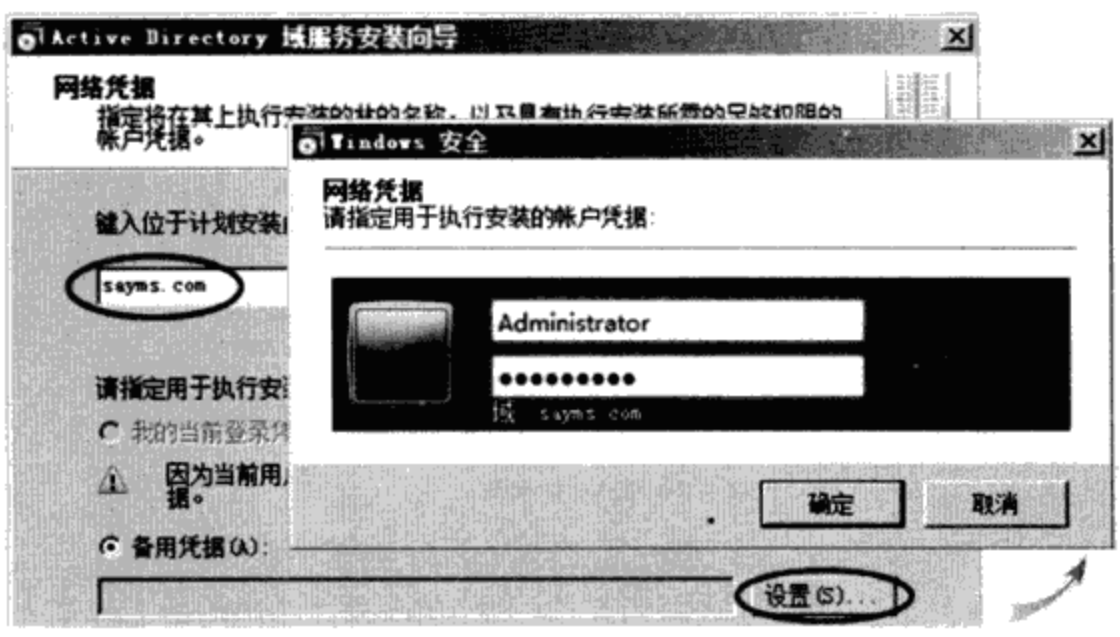


图 7-50

STEP 8 由于此Active Directory集成DNS区域即将被删除，因此请将父域（sayms.com）内的DNS委派区域（hn，参见图 7-17）一并删除，也就是选择图 7-51中的选项后单击下一步按钮。

注意

只有Enterprise Admins组内的用户有权限删除子域或域树，若您现在所登录的账户不是属于此组的话（例如我们现在所登录的账户是域HN的Administrator），就需要在**备用凭据**处另外指定用户账户（位于Sayms.com中Enterprise Admins组内的用户账户）。

Download at http://www.pin5i.com/

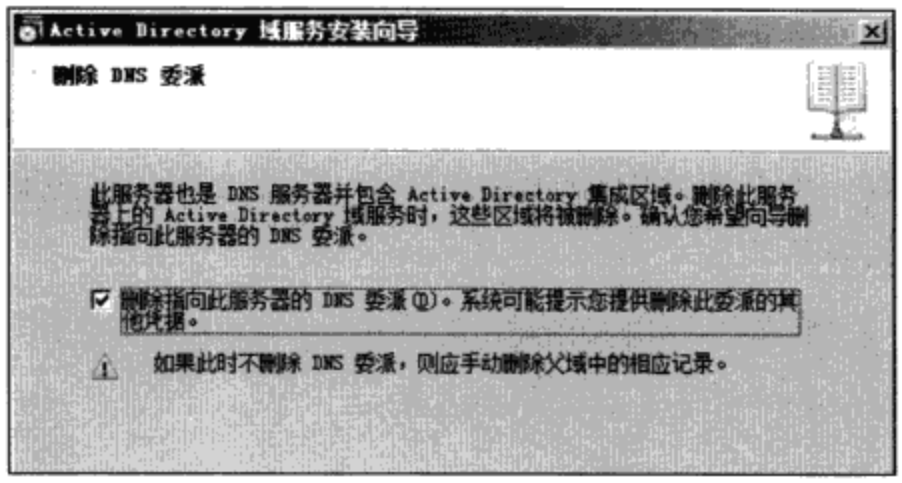


图 7-51

提示

若您没有权限删除父域的DNS委派区域的话，则接下来会要求您输入账号和密码，不过因为前一个步骤我们已经输入父域sayms.com的Administrator账户和密码，故不会再要求您输入账户和密码。

STEP 9 在图 7-52中为这台即将被降级为独立服务器的计算机，设置其本地Administrator的新密码（需符合复杂性要求，且至少7个字符），完成后单击下一步按钮。

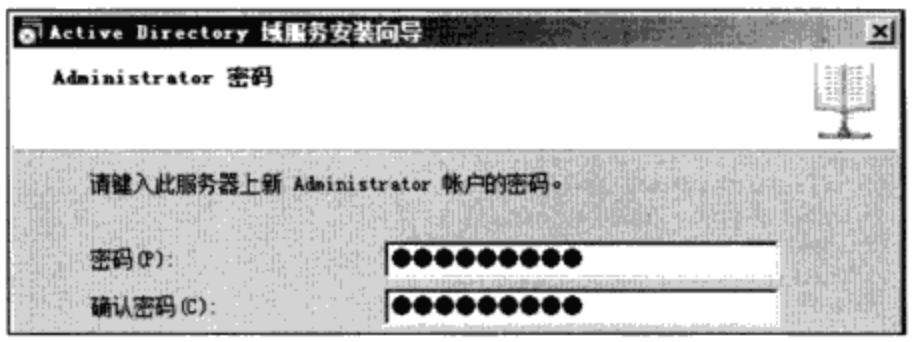


图 7-52

STEP 10 当出现**摘要**界面时，请直接单击下一步按钮。

STEP 11 完成后，重新启动计算机。

虽然这台服务器已经不再是域控制器了，不过其**Active Directory域服务**组件仍然存在，并没有被删除，因此以后若要再升级为域控制器的话，只需要运行**dcpromo.exe**即可，不需要再通过添加角色的方式来安装**Active Directory域服务**。还有虽然Active Directory集成DNS区域的**应用程序目录分区**已删除，但是DNS服务器组件仍然存在。

若想要删除**Active Directory域服务**或**DNS服务器**的话，可通过【单击左下角的**服务器管理器**图标➲单击角色➲选择**Active Directory域服务**或**DNS服务器**➲**单击右边的删除角色**】的方式进行操作。

7-4-2 使用应答文件来删除子域或域树

您可以将删除子域或域树时所必须提供给安装向导的数据，事先输入到**应答文件**内，然

Download at http://www.pin5i.com/

后让安装向导直接从**应答文件**来读取这些数据。请使用**记事本**来编辑应答文件，如图 7-53所示为删除子域hn.sayms.com的应答文件，而图 7-54为删除域树sayiis.com的应答文件，图中我们必须在此文件内创建一个名称为**DCInstall**的字段，然后在此字段内输入相关的参数和参数值，各参数的说明请见表 7-2。



图 7-53



图 7-54

表 7-2

参数值	说明	参数值可为
RetainDCMetadata	是否在域中保留域控制器的metadata，以供RODC删除AD DS时使用	Yes或No（默认为No）
IsLastDCInDomain	是否为此域内的最后一台域控制器	Yes或No（默认为No）
RemoveApplicationPartitions	是否删除应用程序目录分区	Yes或No（默认为No）
AdministratorPassword	设置本地Administrator的密码	
RemoveDNSDelegation	是否删除父域内的委派域	Yes或No（默认为Yes）
DNSDelegationUserName	使用此身份来删除父域内的委派域，此处包含账户名称和密码	若未指定的话，则使用运行AD DS安装向导的账户和密码
DNSDelegationPassword		
UserDomain	使用此账户的身份来删除子域或域树	
UserName		
Password		

Download at http://www.pin5i.com/

完成应答文件的创建后，请通过以下命令（参考图 7-55）来删除子域或域树，假设应答文件的文件名为answer.txt，且此文件位于C:\Test文件夹内：

```
dcpromo /unattend:"C:\Test\answer.txt"
```

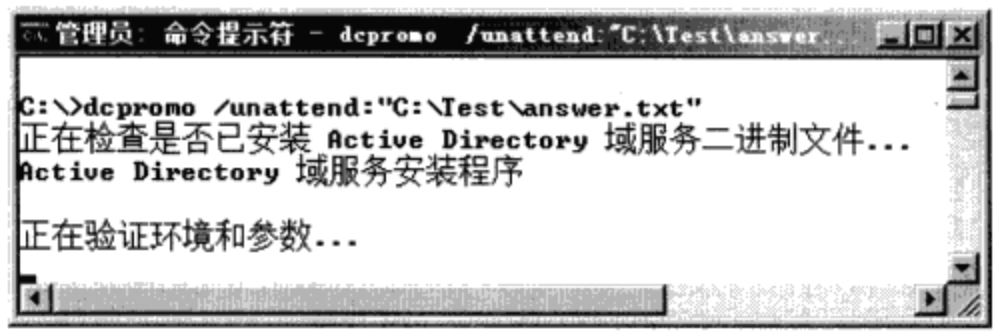


图 7-55

7-4-3 使用命令行来删除子域或域树

您可以通过【开始➲命令提示符】或单击左下角的**Windows PowerShell**图标，然后运行**dcpromo.exe**命令来删除子域或域树。例如以下命令可用来删除子域（参考图 7-56）：

```
dcpromo /unattend /RetainDCMetadata:no /IsLastDCInDomain:yes
/RemoveApplicationPartitions:yes /AdministratorPassword: 111aaAA
/RemoveDNSDelegation:yes    /DNSDelegationUserName:sayms.    com\
administrator
/DNSDelegationPassword:111aaAA /UserDomain:sayms.com
/UserName:sayms.com\administrator /Password:111aaAA
```



图 7-56

而以下命令可用来删除域树：

```
dcpromo /unattend /RetainDCMetadata:no /IsLastDCInDomain:yes
/RemoveApplicationPartitions:yes /UserDomain:sayms.com
/UserName:sayms.com\administrator  /Password:111aaAA
```


Download at http://www.pin5i.com/

```
/AdministratorPassword:111aaAA /RemoveDNSDelegation:no
```

提示

您可以使用 **dcpromo /?:Promotion** 来查看此命令的详细语法。

7-5 更改域控制器的计算机名称

若因为公司组织更改或为了让管理工作更为方便，而需要更改域控制器的计算机名的话，此时可以使用Netdom.exe程序，不过请先确认此域的**域功能级别**已经提升为**Windows Server 2003**（含）。您必须至少是隶属于Domain Admins组内的用户，才有权限更改域控制器的计算机名。操作步骤如下：

STEP 1 请选择【开始➲命令提示符】或单击左下角的**Windows PowerShell**图标。

STEP 2 运行以下命令：

```
netdom computername  目前的旧计算机名  /add:新计算机名
```

其中**目前的旧计算机名**（主要计算机名）和**新计算机名**都必须是FQDN。此命令会为这台计算机另外新建一个计算机名，并更新此计算机账户在AD DS中的SPN（Service Principal Name）属性，也就是在这个SPN属性内同时拥有当前的旧计算机名和新计算机名。此命令也会使用新计算机名来更新在DNS服务器内的日志。注意新计算机名和旧计算机名的后缀需相同，例如都是sayms.com。

提示

SPN（Service Principal Name）是一个包含多重设置值（Multivalue）的名称，它是根据DNS主机名来创建的。SPN用来代表某台计算机所支持的服务，其他计算机可以通过SPN来与这台计算机的服务通信。

STEP 3 请等候一段时间，以便让SPN属性复制到此域内的所有域控制器，而且管辖此域的所有DNS服务器都接收到更新日志后，再继续以下删除旧计算机名的步骤，否则因为有些客户端通过DNS服务器所查询到的计算机名可能是旧的，同时其他域控制器可能仍然是通过旧计算机名来与这台域控制器通信，故若您先运行以下删除旧计算机名步骤的话，则它们使用旧计算机名来与这台域控制器通信时会失败，因为旧计算机名已经被删除，因而会找不到这台域控制器。

STEP 4 运行以下命令，此命令会将新计算机名称设置为主要计算机名。

```
netdom computername 旧计算机名 /makeprimary:新计算机名
```


Download at http://www.pin5i.com/

STEP 5 重新启动计算机。

STEP 6 选择【开始➲命令提示符】或单击左下角的**Windows PowerShell**图标，然后运行以下命令，此命令会将目前的旧计算机名删除，在您删除此计算机名之前，客户端计算机可以同时通过新、旧计算机名来找到这台域控制器。

```
netdom computername 新计算机名 /remove:旧计算机名
```

您也可以通过【开始➲对着**计算机**单击右键➲属性➲单击**更改设置**➲如图 7-57所示单击**计算机名**标签中的更改按钮】的方法来更改计算机名，然而这种方法会将目前的旧计算机名直接删除，换成新计算机名，也就是新旧计算机名不会并存一段时间。这个计算机账户的新SPN属性与新DNS记录，会延迟一段时间后才复制到其他域控制器与DNS服务器，因而在这段时间内，有些客户端在通过这些DNS服务器或域控制器来查找这台域控制器时，仍然会使用旧计算机名，但是因为旧计算机名已经被删除，故找不到这台域控制器，因此建议您还是采用**netdom**命令来更改域控制器的计算机名。

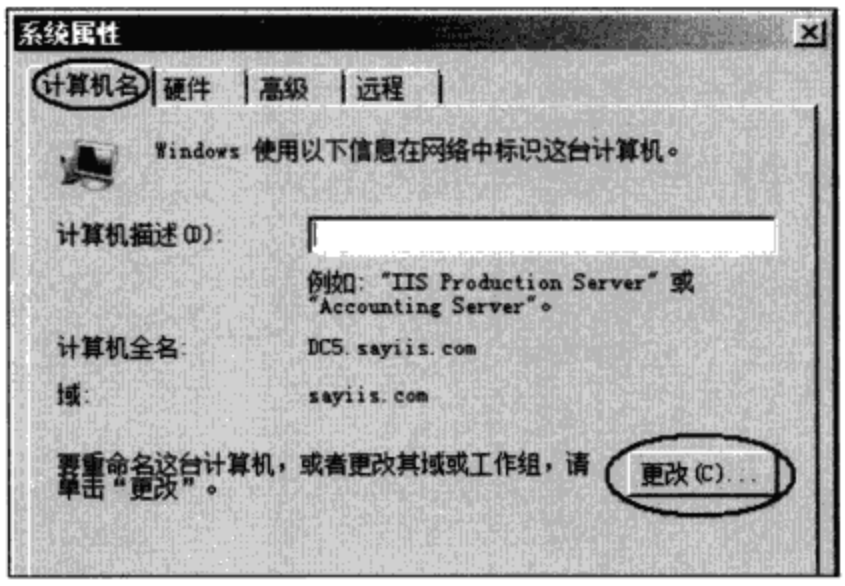


图 7-57

提示

Windows Server 2008 R2、Windows Server 2008也支持使用Rendom.exe等相关命令来更改域名，不过步骤较复杂，有需要的话，请参考微软网站上的说明文件。

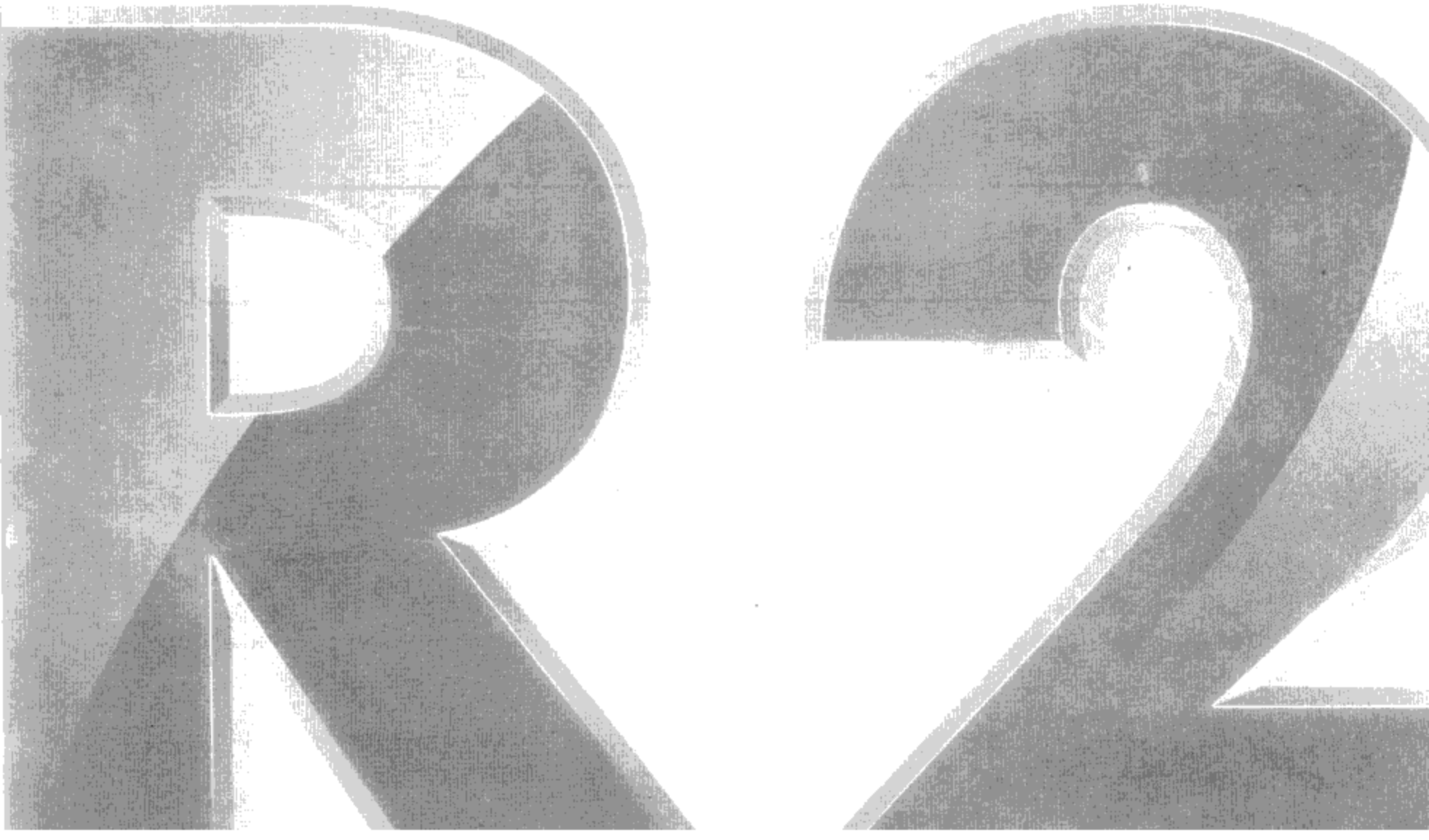
Download at http://www.pin5i.com/

第8章

管理域和林信任

两个域之间在具备信任关系后，双方的用户便可以访问对方域内的资源，使用对方域的计算机登录。

- 域和林信任概述
- 创建**快捷方式信任**
- 创建**林信任**
- 创建**外部信任**
- 管理和删除信任



Download at http://www.pin5i.com/

8-1 域和林信任概述

信任（Trust）是两个域之间通信的桥梁，两个域相互信任之后，双方的用户便可以访问对方域内的资源，使用对方域的计算机登录。

8-1-1 信任域和受信任域

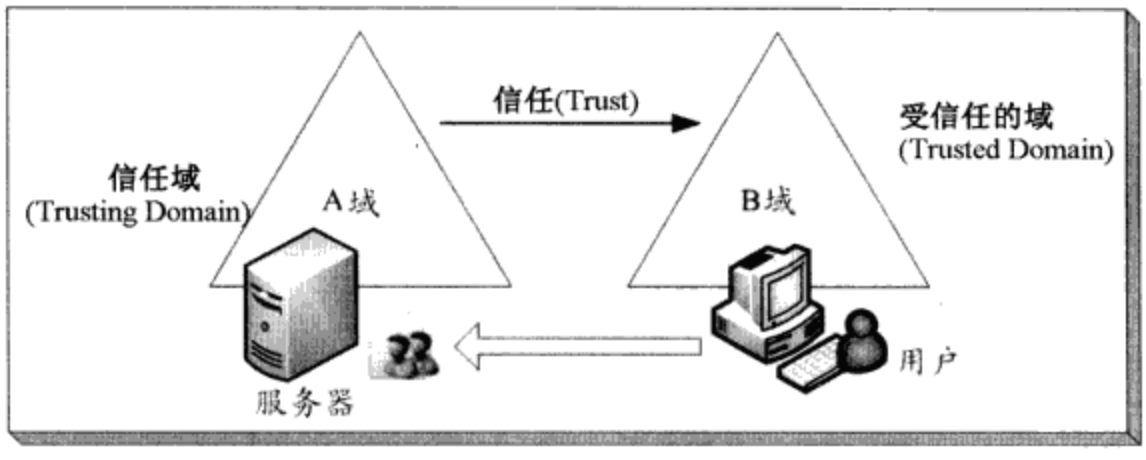


图 8-1

以图 8-1为例，当A域**信任**B域后：

- A域被称为**信任域**（Trusting Domain），而B域被称为**受信任域**（Trusted Domain）。
- B域的用户只要具备适当的权限，就可以访问A域内的资源，例如文件、打印机等，因此A域又被称为**资源域**（Resources Domain），而B域又被称为**账户域**（Accounts Domain）。
- B域的用户可以到A域内的计算机上登录。

注意

A域的用户却不可以访问B域内的资源，也不可以到B域的计算机上登录，除非B域也信任A域。

- 图中的信任关系是**A域信任B域**的**单向信任**（One-way Trust），如果B域也同时信任A域的话，则我们将其称为**双向信任**（Two-way trust），此时双方都可以访问对方的资源，也可以使用对方的计算机登录。

8-1-2 跨域访问资源的流程

当用户在某台计算机登录时，系统必须验证用户身份，而在验证身份的过程中，除了需确认用户名和密码无误外，系统还会为用户创建一个**Access Token**（访问令牌），其内包含着该

Download at http://www.pin5i.com/

用户账户的SID（Security Identifier）、用户所隶属的所有组的SID等数据。用户取得这个Access Token后，当他要访问本地计算机内的资源时（例如文件），便会出示Access Token，而系统会根据Access Token内的SID数据来决定用户拥有何种权限。

> **提示**
>
> 负责验证用户身份的服务是Local Security Authority（LSA），而验证用户身份的方法分为Kerberos与NTLM两种。

同理当用户连接网络上其他计算机时，这台计算机也会为该用户创建一个Access Token，而当用户要访问此网络计算机内的资源时（例如共享文件夹），便会出示Access Token，这台网络计算机便会根据Access Token内的SID数据，来决定用户拥有何种访问权限。

> **注意**
>
> 由于Access Token是在登录（本地登录或网络登录）时创建的，因此如果您在用户登录成功之后，才将用户加入到组的话，此时该Access Token内并没有包含这个组的SID，因此用户也不会具备该组所拥有的权限。用户必须注销再重新登录，以便重新创建一个包含这个组SID的Access Token。

图 8-2为一个域树，图中父域（sayms.com）和两个子域（hn.sayms.com和cn.sayms.com）之间有着双向信任关系。我们使用此图来解释域信任和用户身份验证之间的关系，而且是要通过**子域cn.sayms.com信任根域sayms.com**、**根域sayms.com信任子域hn.sayms.com**这条信任路径（Trust Path），来解释当位于子域hn.sayms.com内的用户George要访问另外一个子域cn.sayms.com内的资源时，系统是如何来验证用户身份和如何来创建Access Token的。

图中George是子域hn.sayms.com的用户，而ServerA位于另外一个子域cn.sayms.com内，当George要访问共享文件夹\\ServerA\tools时，George的计算机必须先取得一个用来和ServerA通信的**Service Ticket**（服务票）。George的计算机取得Service Ticket并与ServerA通信成功后，ServerA会发放一个Access Token给George，以便让George使用这个Access Token来访问位于ServerA内的资源。以下详细说明其流程（请参照图 8-2中的数字）。

STEP 1 George使用所属域hn.sayms.com内的用户账户登录。当George在工作站A登录时，会由其所属域的域控制器DC1来负责验证George的用户名和密码，同时发放一个**Ticket-Granting-Ticket**（TGT，索票凭证）给George，以便让George使用TGT来索取一个用来和ServerA通信的Service Ticket。用户George登录成功后，开始访问共享文件夹**\\ServerA\tools**。

> **提示**
>
> 您可以将TGT视为**通行证**，用户必须拥有TGT后，才可以索取Service Ticket。

Download at http://www.pin5i.com/

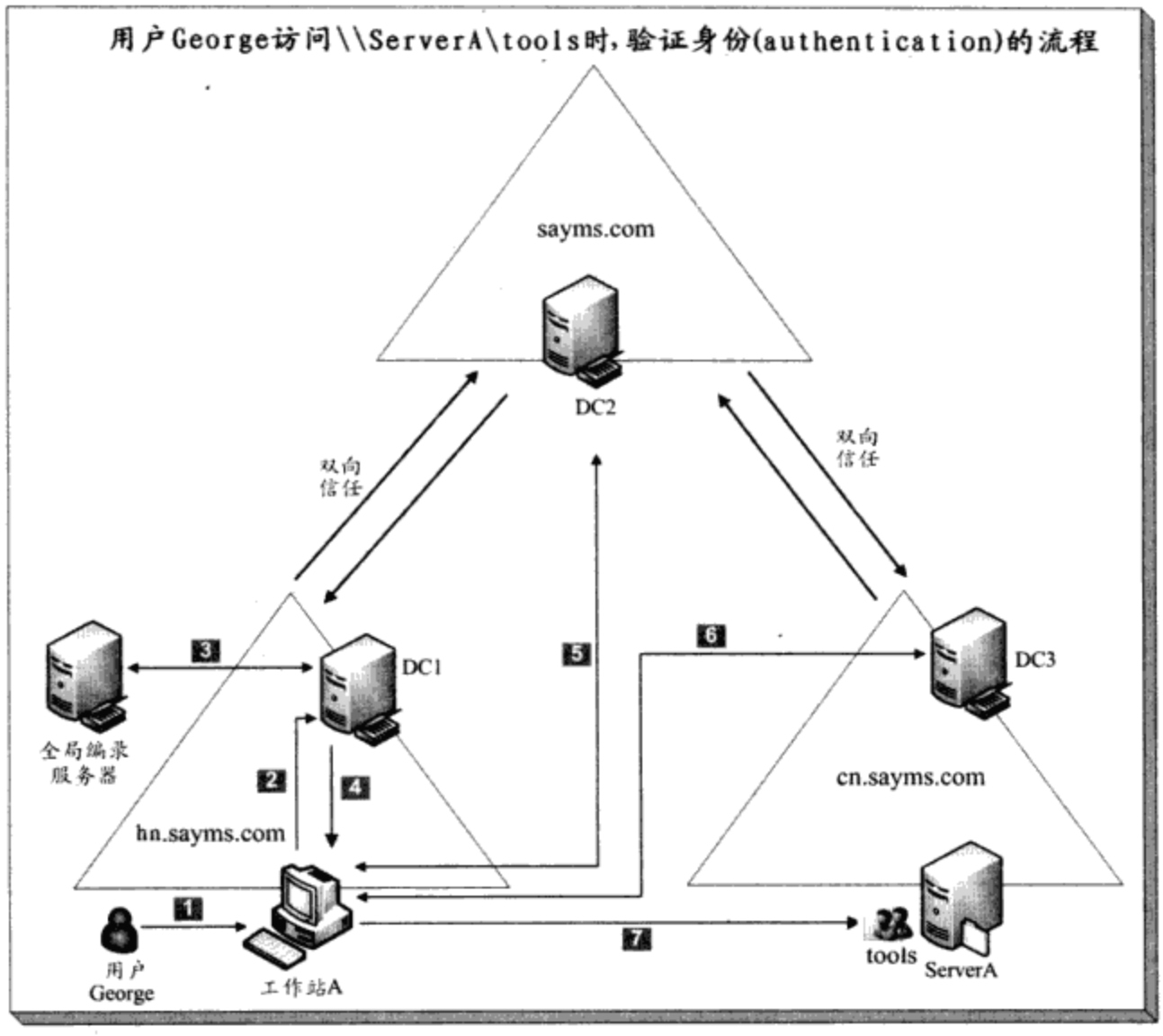


图 8-2

STEP 2 工作站A会向所属域内扮演**Key Distribution Center**（KDC）角色的域控制器DC1，索取一个用来与服务器ServerA通信的Service Ticket。

STEP 3 域控制器DC1检查其数据库后，发现ServerA并不在它的域内（hn.sayms.com），因此转向**全局编录服务器**询问ServerA是位于哪一个域内。**全局编录服务器**根据其AD DS数据库的日志，得知服务器ServerA是位于子域cn.sayms.com内，便将此信息告知域控制器DC1。

STEP 4 域控制器DC1得知ServerA是位于域cn.sayms.com后，它会根据信任路径，通知工作站A去找**信任域**sayms.com的域控制器DC2。

STEP 5 工作站A向域sayms.com的域控制器DC2查询域cn.sayms.com的域控制器。域控制器DC2通知工作站A去找域控制器DC3。

STEP 6 工作站A向域控制器DC3索取一个能够与ServerA通信的Service Ticket。域控制器DC3发放Service Ticket给工作站A。

STEP 7 工作站A取得Service Ticket后，它会将Service Ticket传送给ServerA。ServerA读取Service Ticket内的用户身份数据后，会根据这些数据来创建Access Token，然后将Access Token传给用户George。

Download at http://www.pin5i.com/

从上面的流程可知，当用户要访问另外一个域内的资源时，系统会根据信任路径，依序跟每一个域内的域控制器通信后，才能够取得Access Token，并依据Access Token 内的SID数据来决定用户拥有何种权限。

8-1-3 信任的种类

总共有6 种类型的信任关系，如表 8-1所示，其中前面2种是在您使用**Active Directory域服务安装向导（dcpromo.exe）**创建域时，由系统自动创建的，其他4种必须手动创建。

表8-1

信任类型名称	转移性	单向或双向
父-子 （Parent-Child）	是	双向
树状-根目录 （Tree-Root）	是	双向
快捷方式 （Shortcut）	是（部分）	单向或双向
林 （Forest）	是（部分）	单向或双向
外部 （External）	否	单向或双向
领域 （Realm）	是或否	单向或双向

1. 父-子信任（Parent-Child Trust）

同一个域树中，父域和子域之间的信任关系称为**父-子信任**，例如图 8-3中的sayms.com和hn.sayms.com之间、sayms.com和cn.sayms.com之间、sayiis.com和hk.sayiis.com之间，这个信任关系是自动创建的，也就是说当您在域树内创建任何一个AD DS子域后，此子域会自动信任其上一层的父域，同时父域也会自动信任这个新的子域，而且此信任关系具备**双向转移性**（相关说明可参考第1章）。

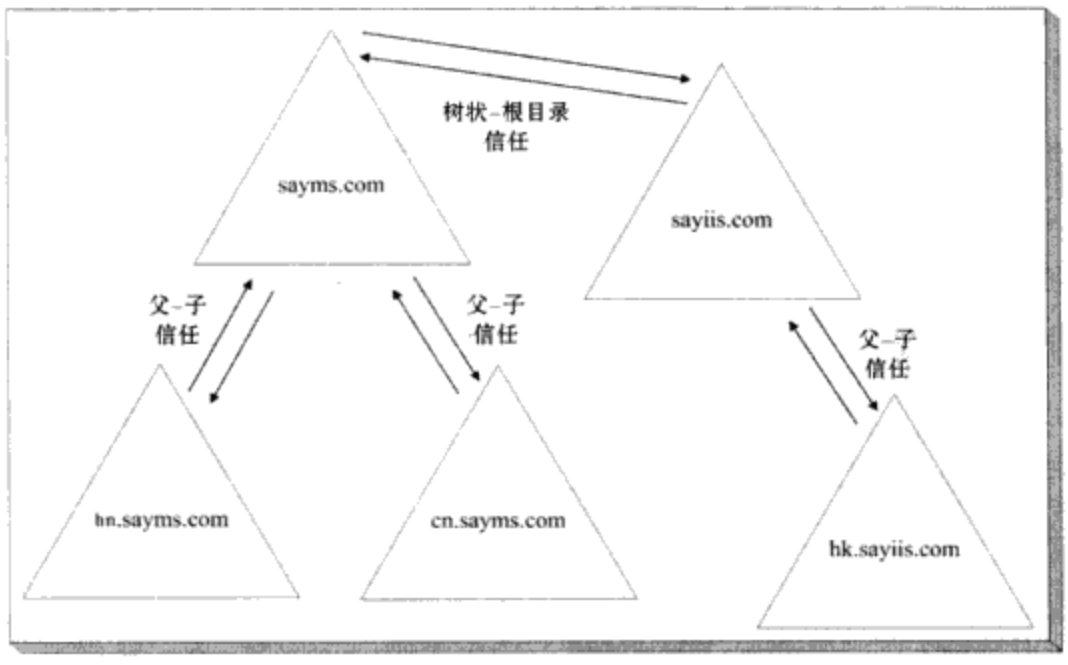


图 8-3

Download at http://www.pin5i.com/

2. 树状-根目录信任（Tree-Root Trust）

同一个林中，林根域（Forest Root Domain，如图 8-3所示的sayms.com）和其他域树的根域（Tree Root Domain，如sayiis.com）之间的信任关系被称为**树状-根目录信任**。

此信任关系是自动创建的，也就是说当您在现有林中创建一个域树后，**林根域**和这个新的**域树根域**之间会自动相互信任对方，而且这些信任关系具备**双向转移性**，因此双方的所有域之间都会自动双向信任。

3. 快捷方式信任（Shortcut Trust）

快捷方式信任可以缩短验证用户身份的时间。例如若图 8-4中域cn.sayms.com 内的用户经常需要访问域hk.sayiis.com内的资源，如果按照一般验证用户身份所走的信任路径，就必须浪费时间经过域sayiis.com和sayms.com，然后再传给cn.sayms.com的域控制器来验证，此时如果我们在域cn.sayms.com和hk.sayiis.com之间创建一个**快捷方式信任**，也就是让域hk.sayiis.com直接信任cn.sayms.com，则域hk.sayiis.com的域控制器在验证域cn.sayms.com的用户身份时，就可以跳过域sayiis.com和sayms.com，也就是直接传给域cn.sayms.com的域控制器来验证，如此便可以节省验证身份所花费的时间。

您可以自行决定要创建单向或双向**快捷方式信任**，例如图中的**快捷方式信任**是单向的，也就是**域 hk.sayiis.com 信任域 cn.sayms.com**，它让域 cn.sayms.com 的用户在访问域hk.sayms.com内的资源时，可以走**快捷方式信任**的路径来验证用户的身份。由于是单向**快捷方式信任**，因此反过来域hk.sayiis.com的用户在访问域cn.sayms.com内的资源时，却无法走这个**快捷方式信任**的路径，除非域cn.sayms.com也**快捷方式信任**域hk.sayiis.com。

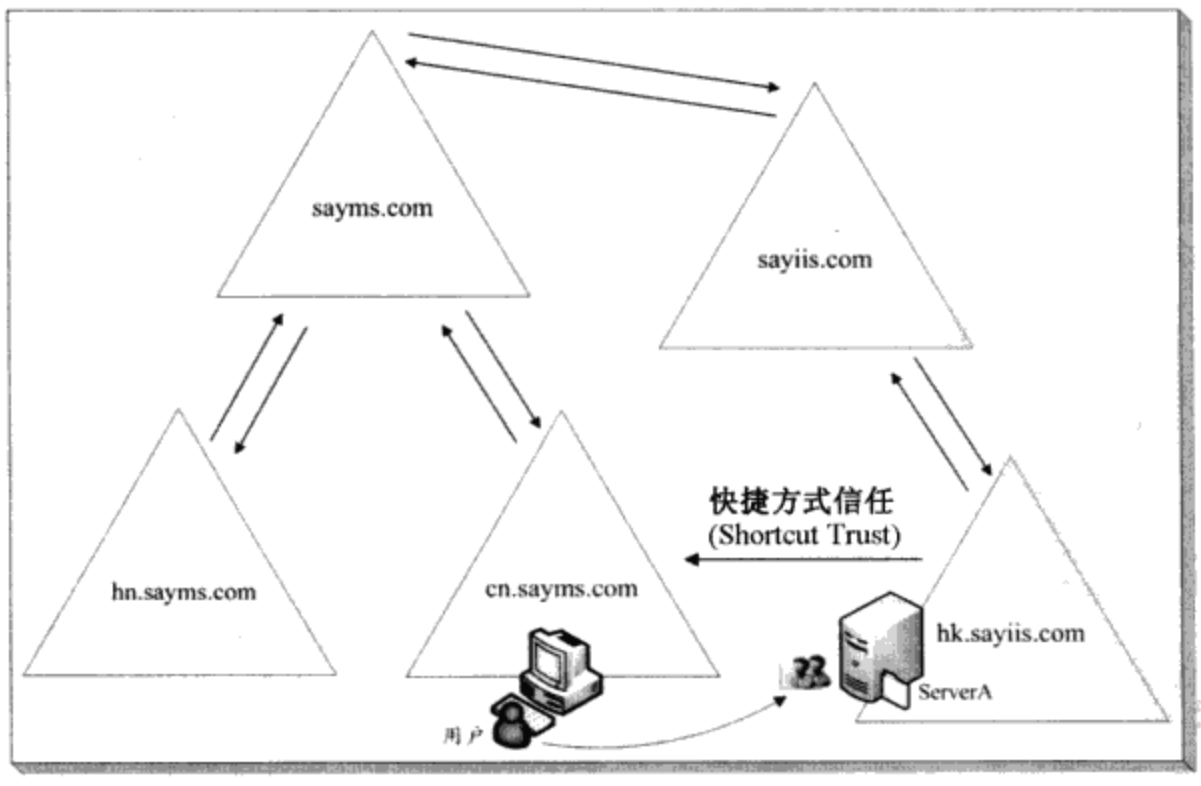


图 8-4

Download at http://www.pin5i.com/

注意快捷方式信任仅有部分转移性，也就是只会向下扩展，不会向上扩展，以图8-5为例，图中在D域创建一个**快捷方式信任**到F域，这个快捷方式信任会自动向下扩展到G域，因此D域的域控制器在验证G域的用户身份时，可以走【D域→F域→G域】的快捷方式路径。然而D域的域控制器在验证E域的用户身份时，仍然必须走【D域→A域→E域】的路径，也就是通过**父-子信任**【D域→A域】和**树状-根目录信任**【A域→E域】的路径。

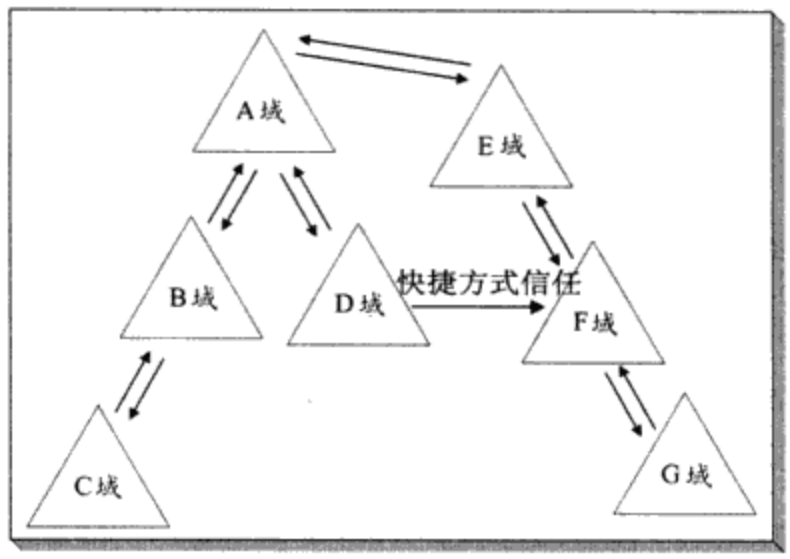


图8-5

4. 林信任（Forest Trust）

两个林之间可以通过**林信任**来创建信任关系，以便让不同林内的用户可以相互访问对方的资源。您可以自行决定要创建单向或双向的信任关系，例如图8-6中我们在两个林sayms.com和sayisa.com之间创建了双向信任关系，由于**林信任**具备**双向转移性**的特性，因此会让两个林中的所有域之间都相互信任，也就是说所有域内的用户都可以访问其他域内的资源，不论此域是位于哪一个林内。

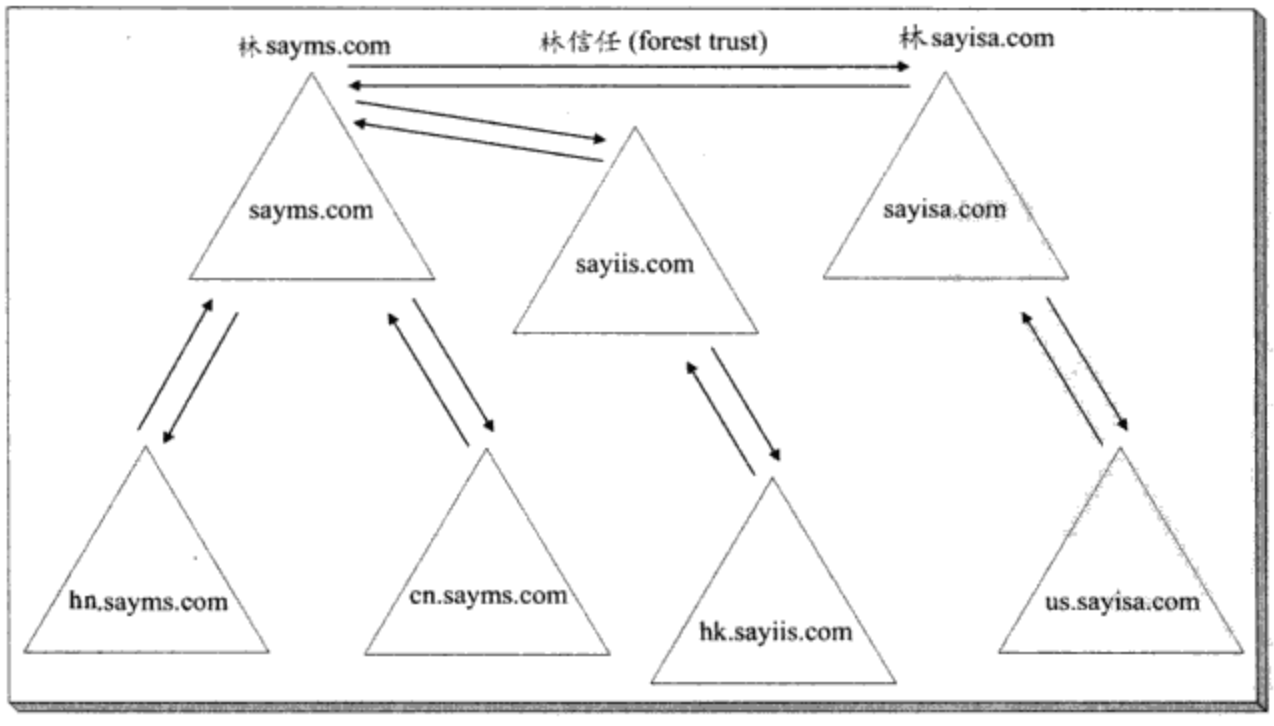


图8-6

Download at http://www.pin5i.com/

注意林信任仅有部分转移性，也就是说两个林之间的**林信任**关系并无法自动地扩展到其他第3个林，例如虽然您在林A和林B之间创建了**林信任**，同时也在林B和林C之间创建了**林信任**，但是林A和林C之间并不会自动有信任关系。

5. 外部信任（External Trust）

分别位于两个林内的域之间可以通过**外部信任**来创建信任关系，另外AD DS域也可以通过**外部信任**来与Windows NT 4.0域创建信任关系。您可以自行决定要创建单向或双向信任关系，例如图 8-7中两个林sayms.com和sayexg.com之间并没有信任关系，但是我们在域sayiis.com和域sayexg.com之间创建了双向的**外部信任**关系，同时也在uk.sayexg.com和Windows NT 4.0域human之间创建了双向的**外部信任**关系。由于**外部信任**并不具备**转移性**，因此除了图中的sayiis.com和sayexg.com之间，还有uk.sayexg.com和human之间外，其他域之间并不具备信任关系。

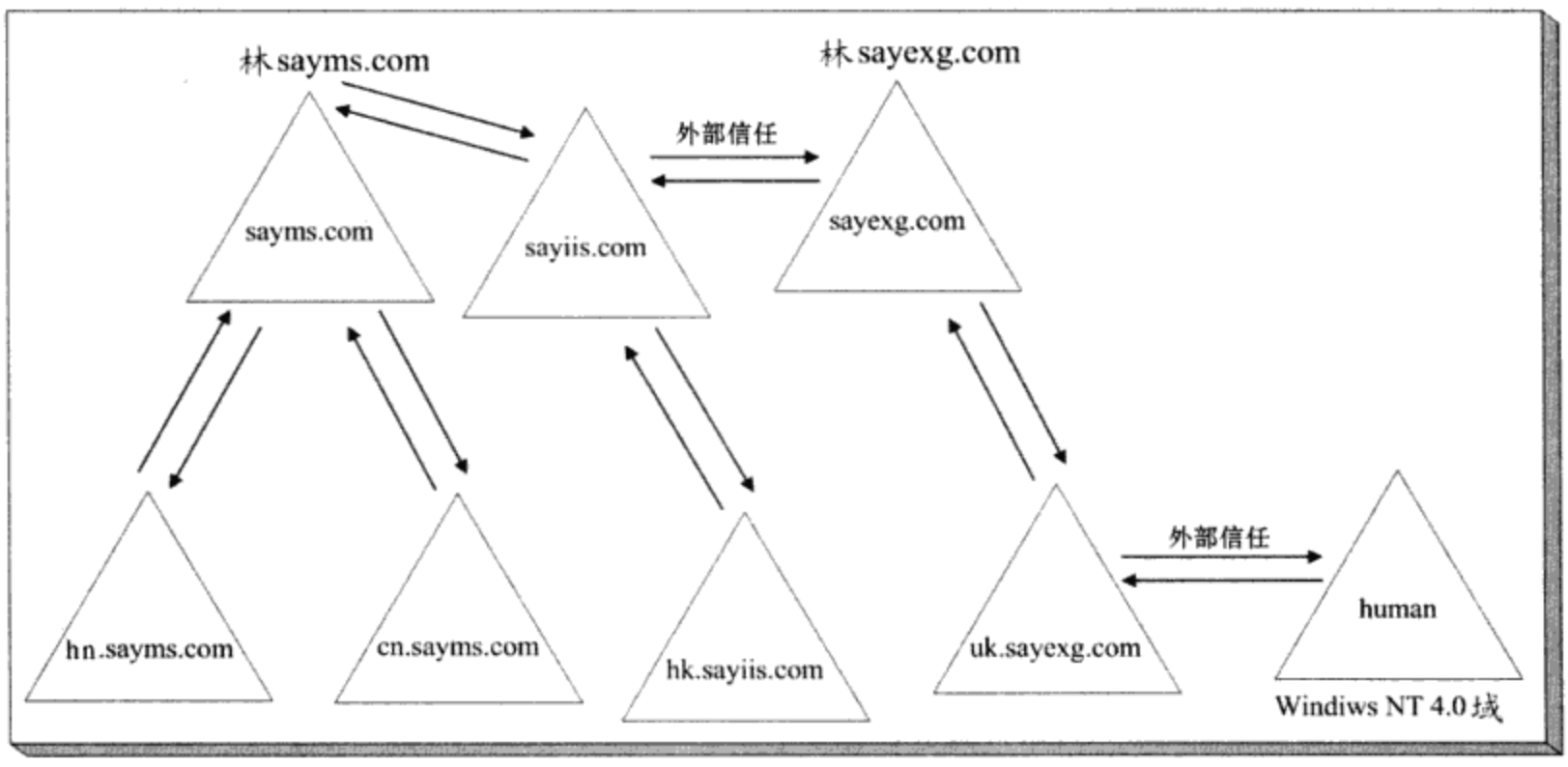


图8-7

6. 领域信任（Realm Trust）

AD DS域可以和**非Windows系统**（例如UNIX）的Kerberos领域之间创建信任关系，这个信任关系称为**领域信任**。这种跨平台的信任关系，让AD DS域能够和其他Kerberos系统相互通信。**领域信任**可以是单向或双向，而且可以从**转移性**切换到**非转移性**，也可以从**非转移性**切换到**转移性**。

Download at http://www.pin5i.com/

8-1-4 创建信任前的注意事项

前面的6种信任关系中，**父-子信任**是在创建子域时自动创建的，而**树状-根目录信任**则是在创建域树时自动创建的，其他的4种信任关系必须手动创建。请先了解以下事项，以减少在创建信任关系时的困扰。

- 创建信任就是在创建两个不同域之间的通信桥梁，从域管理的角度来看，两个域各需要有一个拥有适当权限的用户，在各自域中分别做一些设置，以完成双方域之间信任关系的创建工作。其中**信任域**一方的系统管理员，需要为此信任关系创建一个**传出信任**（Outgoing Trust）；而**受信任域**一方的系统管理员，则需要为此信任关系创建一个**传入信任**（Incoming Trust）。**传出信任**和**传入信任**可视为此一信任关系的两个端点。
- 以创建图 8-8中**A域信任B域**的单向信任来说，我们必须在A域创建一个**传出信任**，相对的也必须在B域创建一个**传入信任**。也就是说在A域创建一个**传出到**B域的信任，同时相对的，在B域创建一个让A域**传入**的信任。

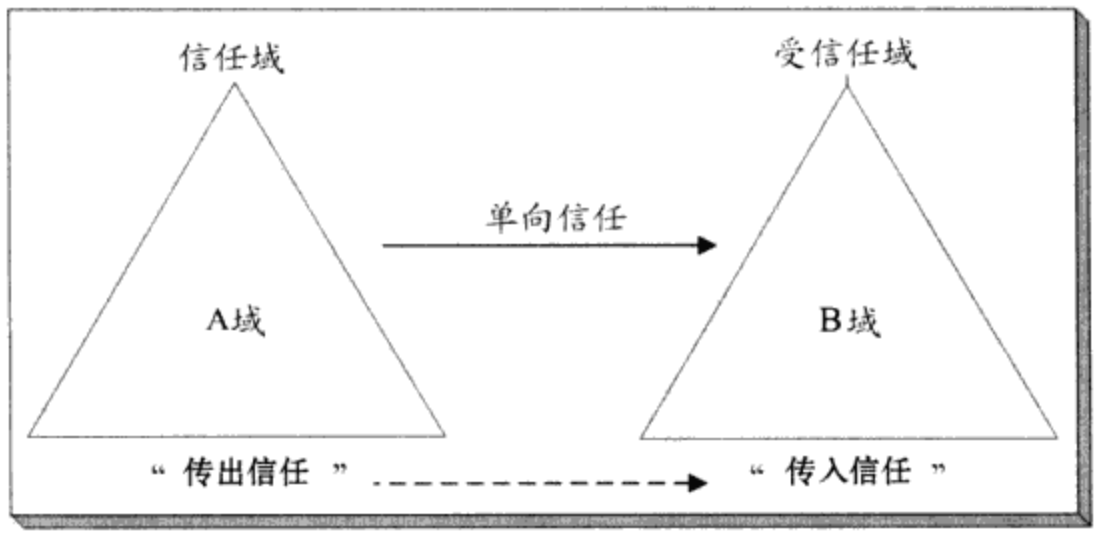


图8-8

- 在您使用**新建信任向导**来创建图中的单向信任关系时，您可以选择先单独创建A域的**传出信任**，然后再另外单独创建B域的**传入信任**；或是选择同时创建A域的**传出信任**和B域的**传入信任**：如果是分别单独创建这两个信任的话，则需要在A域的**传出信任**和B域的**传入信任**设置相同的信任密码；如果是同时创建这两个信任的话，则在信任过程中并不需要设置信任密码，但您需要在这两个域都拥有适当权限，系统默认是Domain Admins或Enterprise Admins组的成员拥有此权限。
- 以创建图 8-9的**A域信任B域，同时B域也信任A域**的双向信任来说，我们必须在A域同时创建**传出信任**和**传入信任**，其中的**传出信任**是用来信任B域，而**传入信任**是要让B域可以信任A域。相对的也必须在B域创建**传入信任**和**传出信任**。在使用**新建信任向导**来创建图中的双向信任关系时，您可以单独先创建A域的**传出信任**和**传入信任**，然后再另外单独创建B域的**传入信任**和**传出信任**；或选择同时创建A域和B域的

Download at http://www.pin5i.com/

传入信任、传出信任：如果是分别单独创建A域和B域的**传出信任、传入信任**的话，则需要在A域和B域设置相同的信任密码；如果是同时创建A域和B域的**传出信任、传入信任**的话，则在信任过程中并不需要设置信任密码，但您需要在这两个域都拥有适当的权限，系统默认是Domain Admins或Enterprise Admins组的成员拥有此权限。

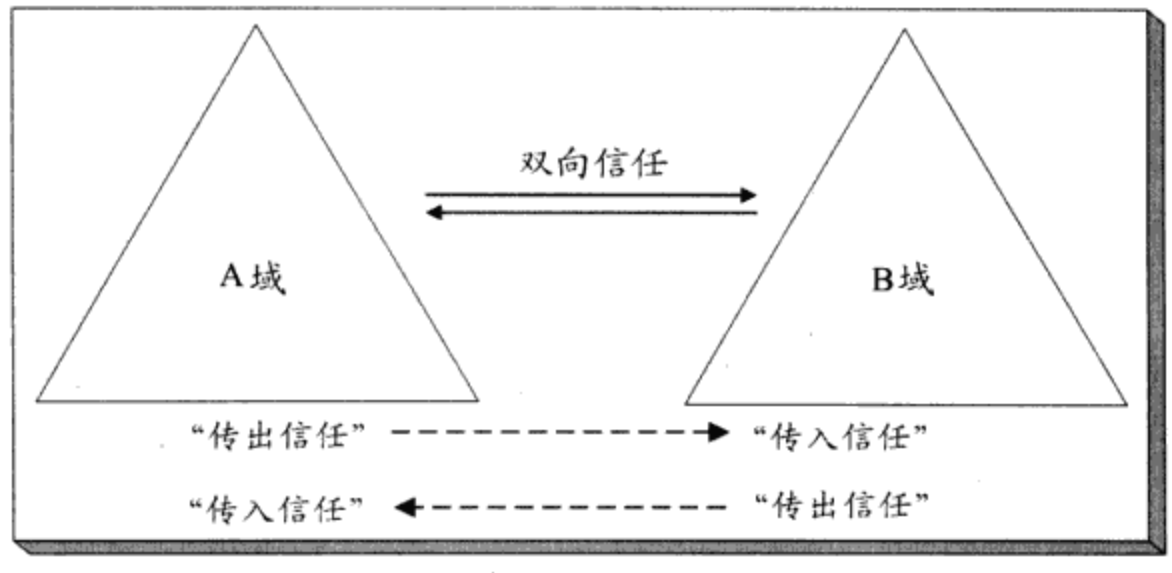


图8-9

- 两个域之间在创建信任关系时，相互之间可以使用DNS名称或NetBIOS名称来指定对方的域名：如果是使用DNS域名，则相互之间需通过DNS服务器来查询对方的域控制器；如果是使用NetBIOS域名，则可以通过广播或WINS服务器来查询。但是广播消息无法跨越到另外一个网络，因此若通过广播来查询的话，则两个域的域控制器必须位于同一个网络内。如果是通过WINS服务器来查询的话，则两个域的域控制器可以不需要在同一个网络内。
- 除了使用**新建信任向导**来创建两个域或林之间的信任外，您也可以使用**netdom trust**命令来新建、删除或管理信任关系。

8-2 创建快捷方式信任

本节以创建图 8-10中域hn.sayiis.com信任域cn.sayms.com的单向**快捷方式信任**为例进行说明。请务必先参考创建信任前的注意事项的说明后，再继续以下的步骤。

Download at http://www.pin5i.com/

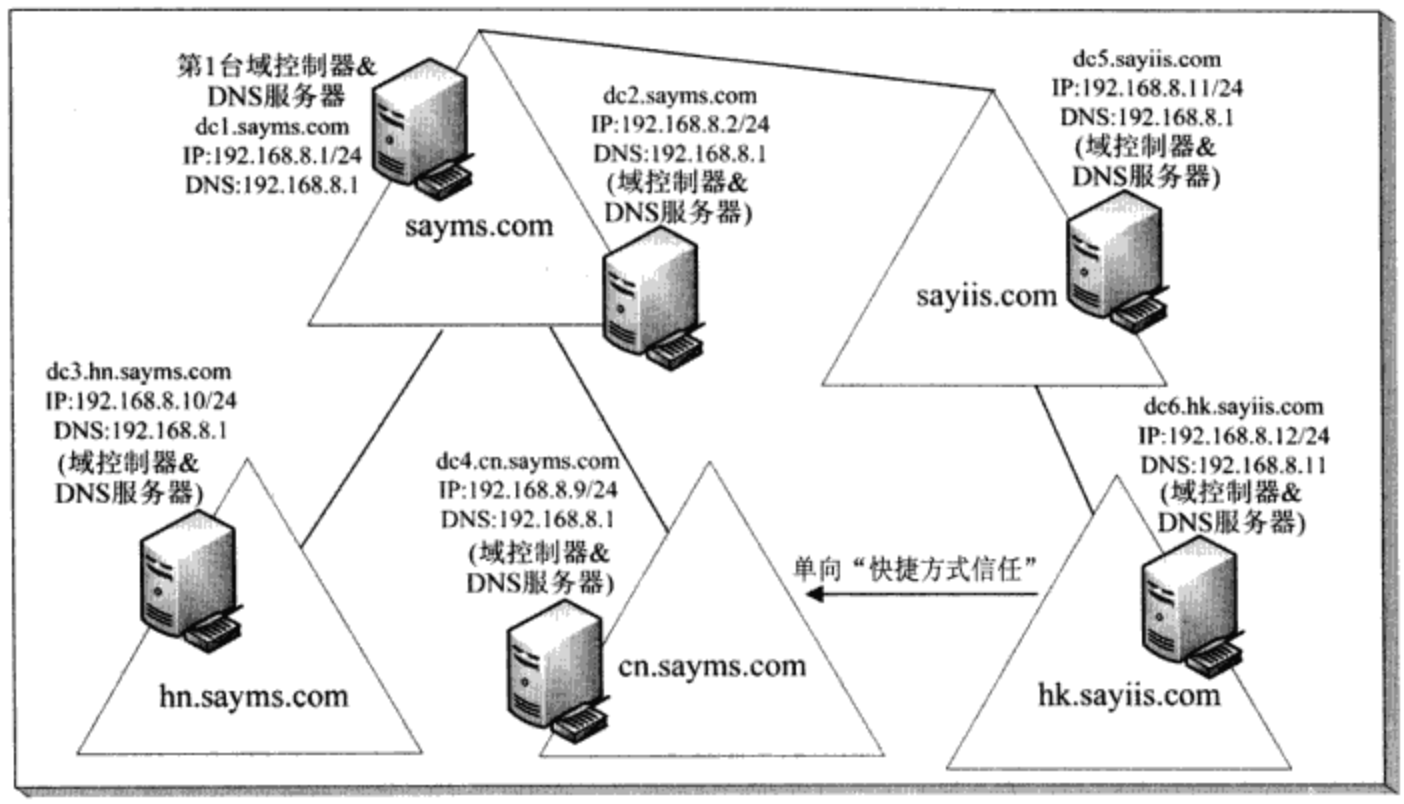


图 8-10

我们将图重新简化为图 8-11，图中我们必须在域hk.sayiis.com中创建一个**传出信任**，相对的也必须在域cn.sayms.com中创建一个**传入信任**。我们以同时创建域hk.sayiis.com的**传出信任**和域cn.sayms.com的**传入信任**为例进行说明。

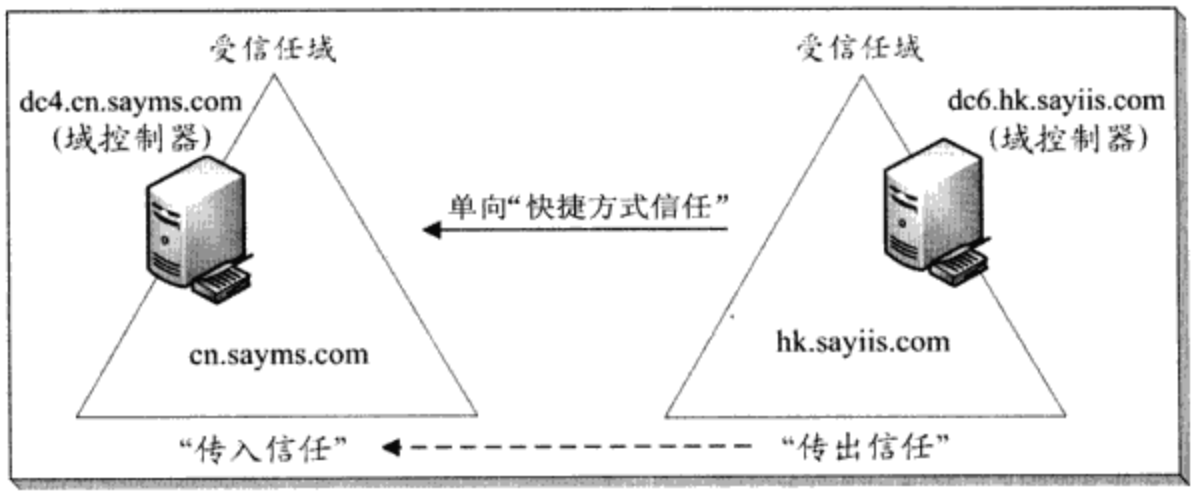


图 8-11

STEP 1 以下假设是要在左边受信任域cn.sayms.com的域控制器dc4.cn.sayms.com 上，使用 Domain Admins（cn.sayms.com）或Enterprise Admins（sayms.com）组内的用户登录和创建信任。

STEP 2 选择【开始➲管理工具➲Active Directory域和信任关系】。

STEP 3 如图 8-12所示，通过【单击域cn.sayms.com➲单击上方的**属性**图标】的方式进行操作。

Download at http://www.pin5i.com/

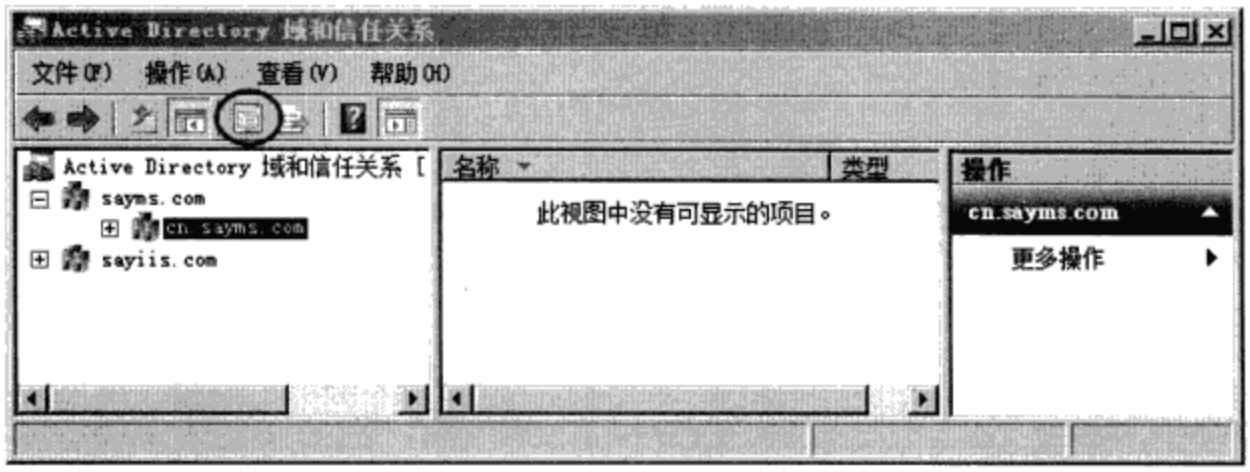


图 8-12

STEP 4 在图 8-13中的**信任**标签中单击新建信任按钮。

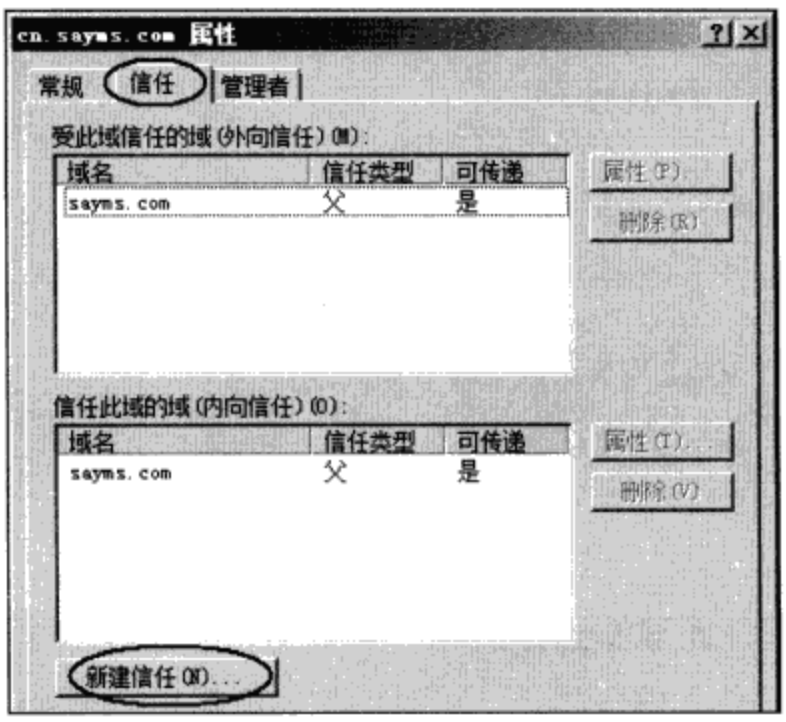


图 8-13

> **提示**
>
> 由图中的上半部分可看出域cn.sayms.com已经信任其父域sayms.com，同时从下半部分可看出，域cn.sayms.com也已经被其父域sayms.com所信任。也就是说域cn.sayms.com和其父域sayms.com之间已经自动具有双向信任关系，它就是**父-子信任**。

STEP 5 当出现**欢迎使用新建信任向导**界面时单击下一步按钮。

STEP 6 在图 8-14中输入对方域的DNS域名hk.sayiis.com（或NetBIOS域名HK）。

Download at http://www.pin5i.com/

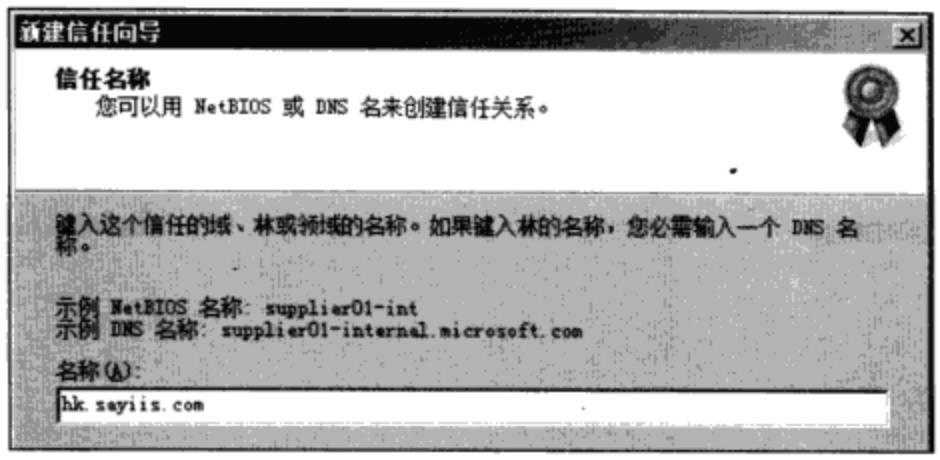


图8-14

STEP 7 在图8-15中选择**单向：内传**单选按钮，表示我们要创建如图8-11所示的单向快捷方式信任中左方域cn.sayms.com的**传入信任**。

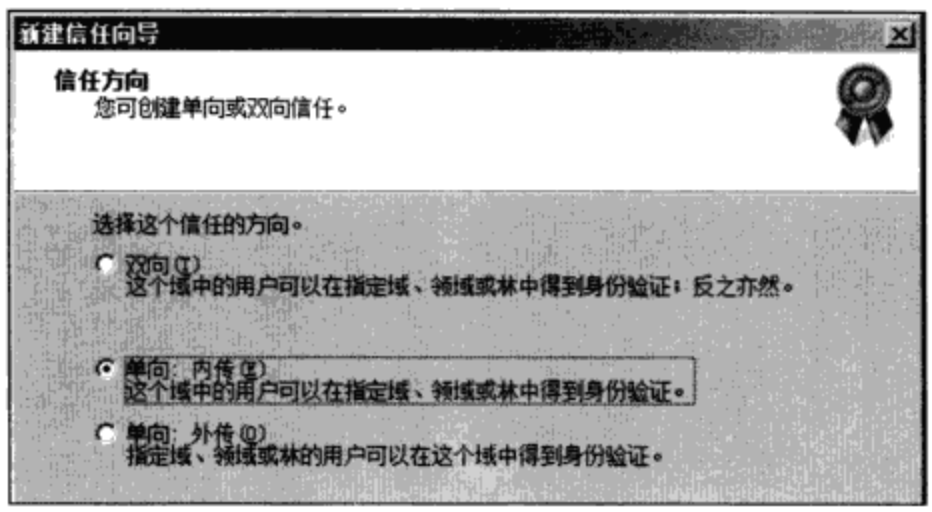


图8-15

STEP 8 在图8-16中选择**此域和指定的域**单选按钮，也就是除了要创建图8-11中左方域cn.sayms.com的**传入信任**之外，同时也要创建右方域hk.sayiis.com的**传出信任**。

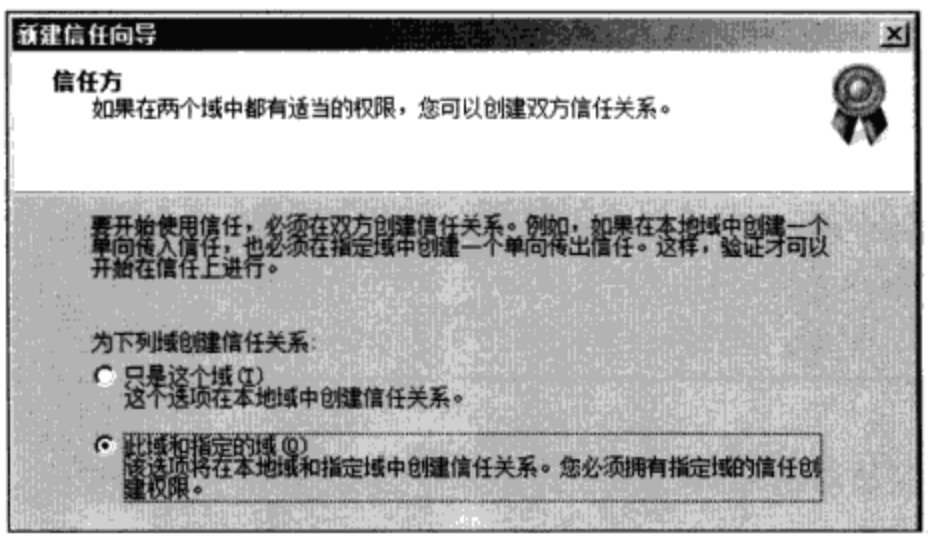


图8-16

注意

如果您选择**只是这个域**单选按钮的话，则您必须事后另外再针对域hk.sayiis.com创建一个传出到域cn.sayms.com的**传出信任**。

Download at http://www.pin5i.com/

STEP 9 在图 8-17中输入对方域（hk.sayms.com）的Domain Admins组内的用户名和密码，或Enterprise Admins组内的用户名和密码。

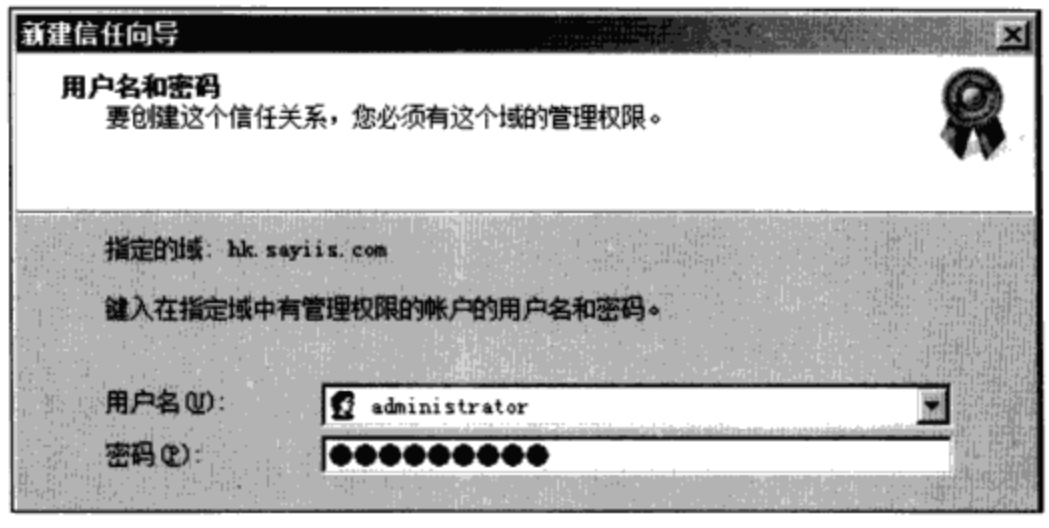


图 8-17

提示

如果要输入Enterprise Admins组内的用户账户的话，请在用户名之前输入林根域的域名，例如sayms\administrator或sayms.com\administrator，其中的sayms为林根域的NetBIOS域名，而sayms.com为其DNS域名。

STEP 10 在图 8-18中单击下一步按钮。

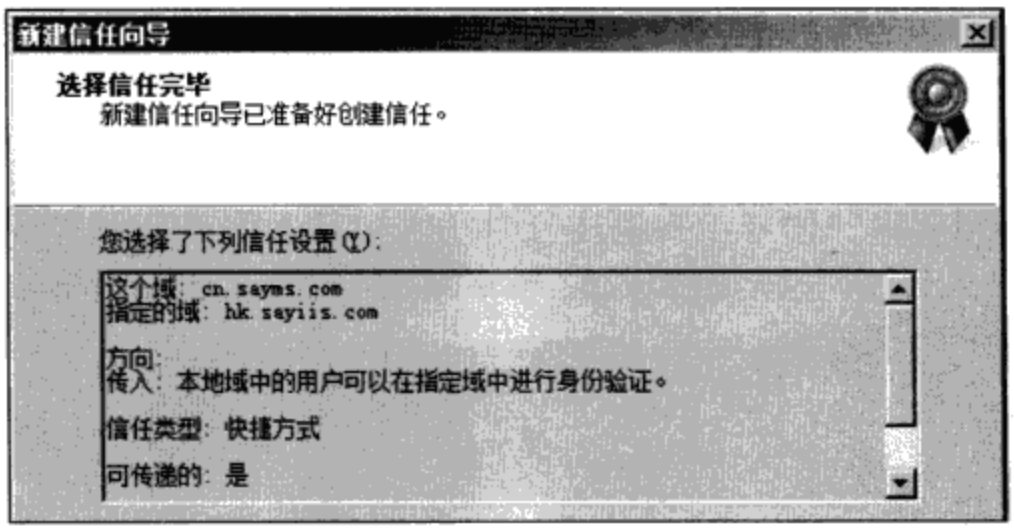


图 8-18

STEP 11 在图 8-19中单击下一步按钮。

Download at http://www.pin5i.com/

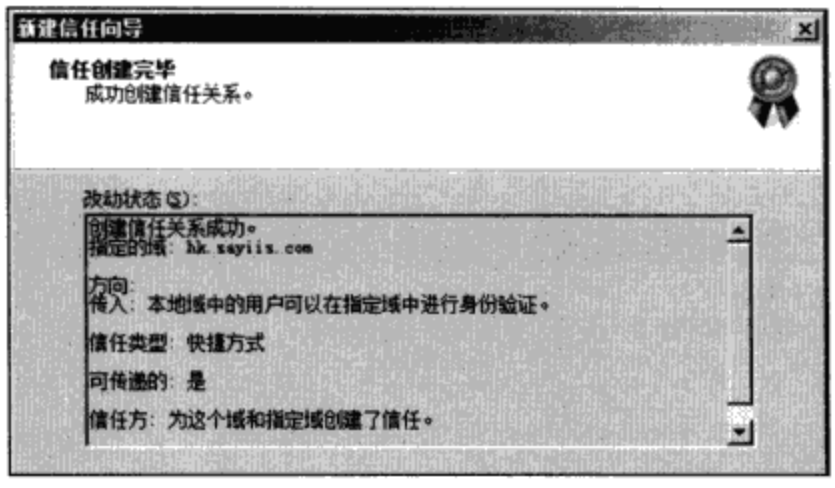


图8-19

STEP 12 您可以在图8-20中选择**是，确认传入信任**单选按钮，以便确认cn.sayms.com的**传入信任**和hk.sayiis.com的**传出信任**两者是否都已经创建成功，也就是要确认此**单向快捷方式信任**是否已经创建成功。

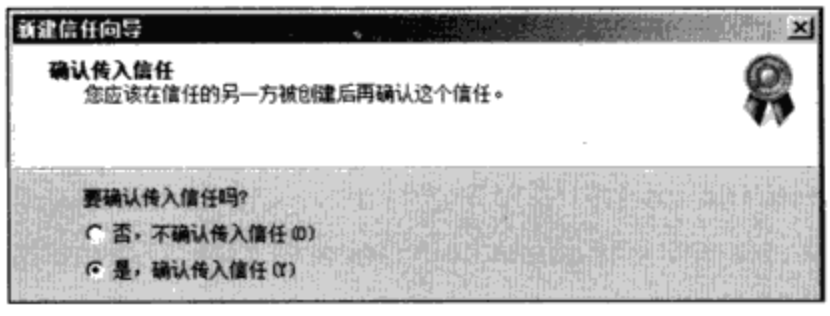


图8-20

提示

如果您是分别单独创建域cn.sayms.com的**传入信任**和域hk.sayiis.com的**传出信任**的话，请确认这两个信任关系都已经创建完成后，再选择**是，确认传入信任**单选按钮。

STEP 13 当出现**完成新建信任向导**界面时单击完成按钮。

图8-21为完成创建单向快捷方式信任后的界面，表示在域cn.sayms.com中有一个从域hk.sayiis.com中的**传入信任**，也就是说域cn.sayms.com是被域hk.sayiis.com信任的**受信任域**。

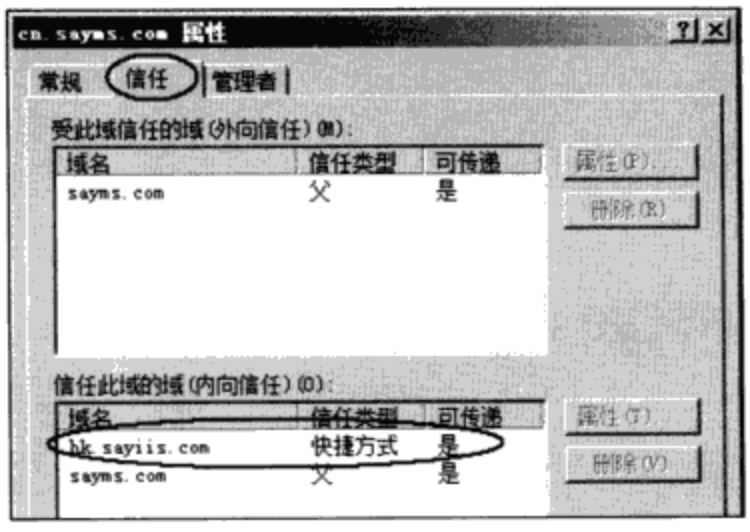


图8-21

Download at http://www.pin5i.com/

同时在域hk.sayiis.com中也会有一个连接到域cn.sayms.com的**传出信任**，也就是说域hk.sayiis.com是域cn.sayms.com 的**信任域**，您可以通过【如图 8-22所示右击sayiis.com之下的域hk.sayiis.com➲**属性**➲单击**信任**标签】的方法来查看此设置。

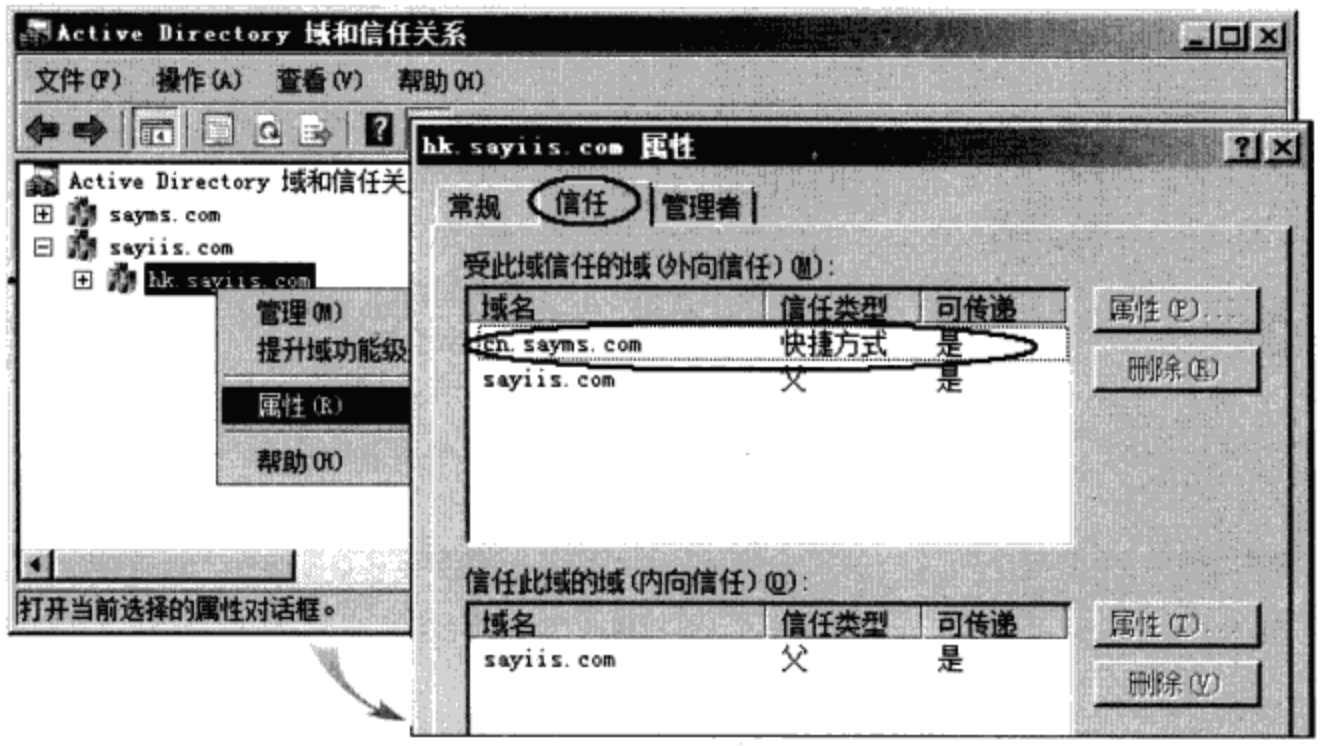


图 8-22

8-3 创建林信任

本节将以创建图 8-23中林sayms.com和林sayisa.com之间的双向**林信任**进行说明。

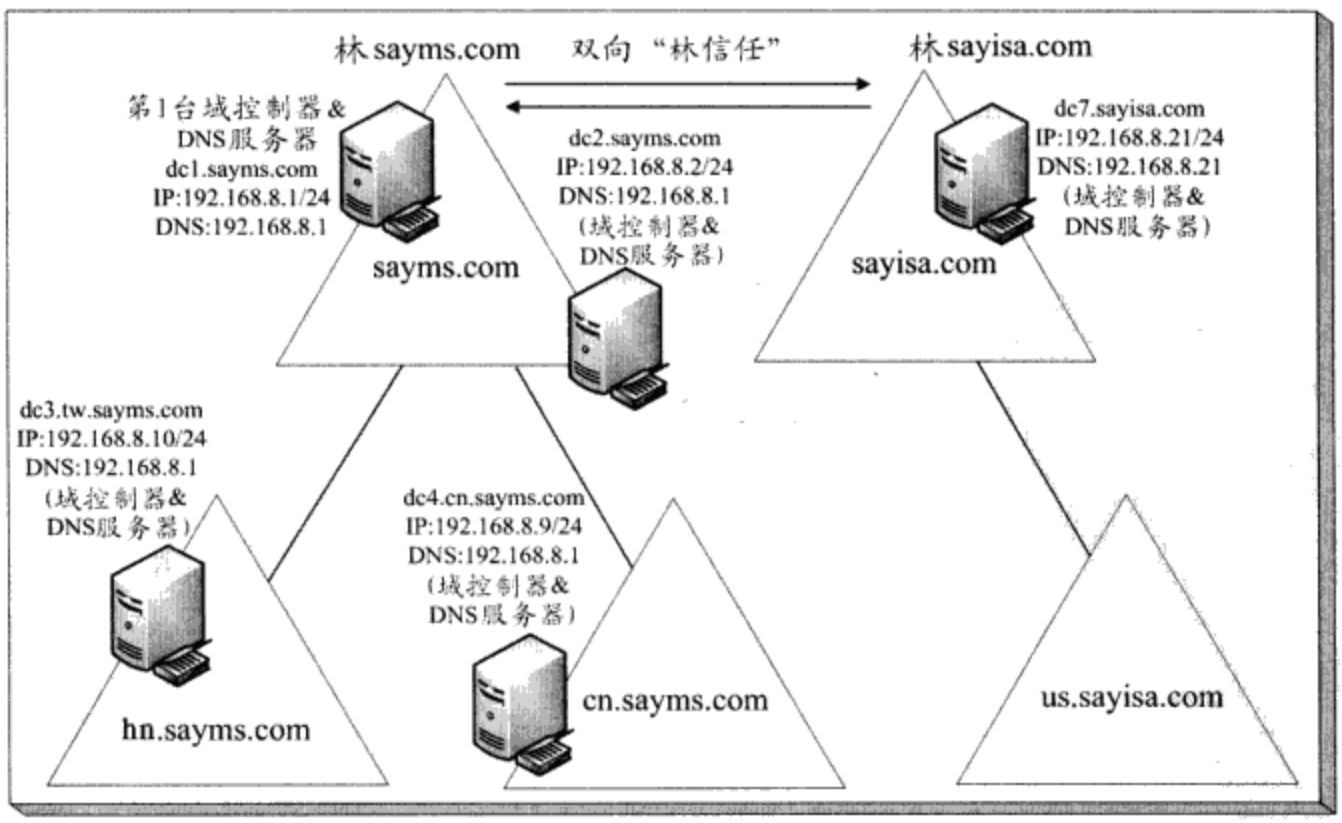


图 8-23

Download at http://www.pin5i.com/

我们将图重新简化为图 8-24，图中我们需要在林根域sayms.com创建**传出信任**和**传入信任**，相对的也需要在林根域sayisa.com创建**传入信任**和**传出信任**。

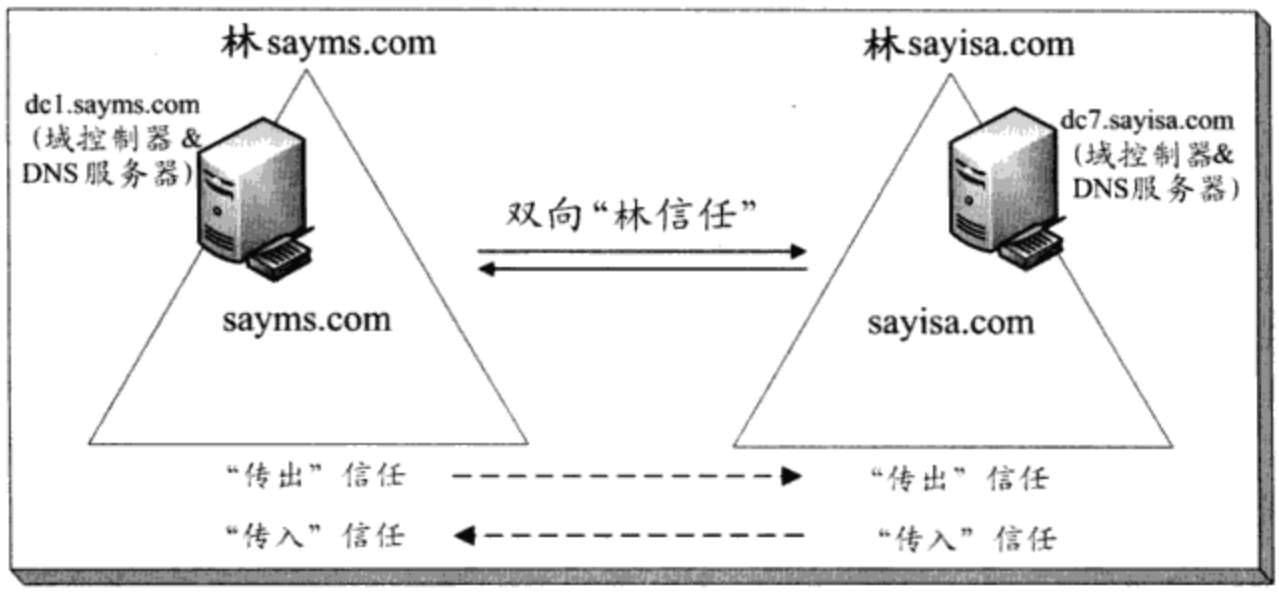


图 8-24

8-3-1 创建林信任前的注意事项

在创建**林信任**之前，请先注意以下事项：

- 请先了解创建信任前的注意事项。
- 两个林之间需要通过DNS服务器来找到对方林根域的域控制器。以图 8-24为例，您必须确定在域sayms.com中可以通过DNS服务器找到域sayisa.com的域控制器，同时在域sayisa.com中可以通过DNS服务器找到域sayms.com的域控制器：若两个林根域使用同一台DNS服务器，也就是此DNS服务器内同时有sayms.com和sayisa.com区域，则双方都可以通过此DNS服务器来找到对方的域控制器；若两个林根域不是使用同一台DNS服务器，则您可以通过**条件转发器**（Conditional Forwarder）来进行设置，例如在sayms.com的DNS服务器中指定将sayisa.com的查询要求，转给sayisa.com的DNS服务器（参见图 8-25，图中假设域sayisa.com的DNS服务器的IP地址为192.168.8.21），同时也请在sayisa.com的DNS服务器中指定将sayms.com的查询请求，转给sayms.com的DNS服务器。若两个林根域不是使用同一台DNS服务器的话，则还可以通过**辅助区域**进行设置，例如在sayms.com的DNS服务器创建一个名称为sayisa.com的辅助区域，其数据是从sayisa.com的DNS服务器通过**区域传送**复制过来；同时也在sayisa.com的DNS服务器创建一个名称为sayms.com的辅助区域，其数据是从sayms.com的DNS服务器通过**区域传送**复制过来。

Download at http://www.pin5i.com/

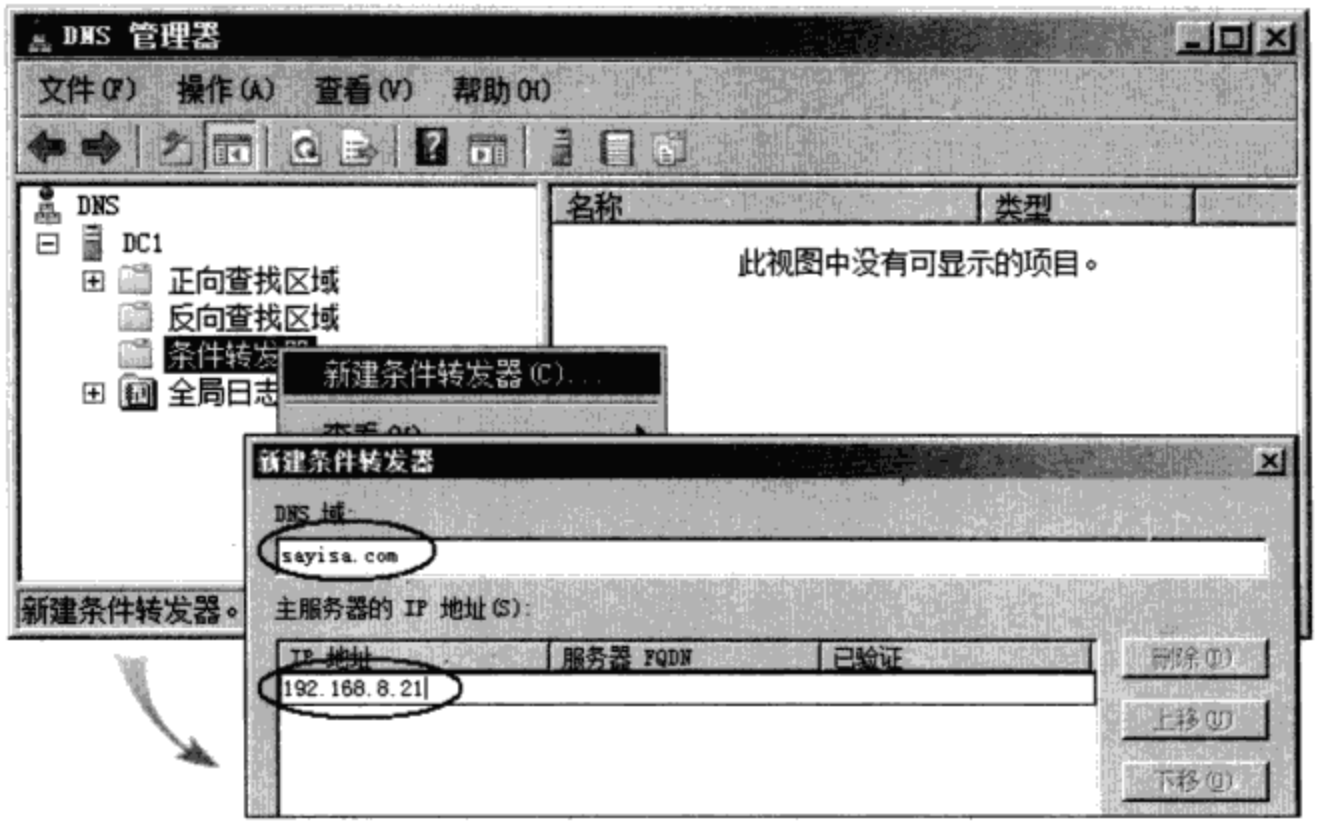


图 8-25

提示

请先完成**条件转发器**的设置，再分别到sayms.com和sayisa.com的域控制器上，使用ping对方区域内主机的方式来测试**条件转发器**的功能是否正常。

确定两个林的**林功能级别**都已经提升为**Windows Server 2003**（含）以上。有关**林功能级别**的详细内容，请参考第1章；如何提高林功能级别的说明，请参考第2章。

8-3-2 开始创建林信任

我们将在林sayms.com和sayisa.com之间创建一个双向的**林信任**，也就是说我们将为林sayms.com创建**传出信任**和**传入信任**，同时也为林sayisa.com创建相对的**传入信任**和**传出信任**。请先确认DNS服务器的设置已经完成，同时林功能级别已升级为**Windows Server 2003**（含）以上。

STEP 1 以下假设是要在图 8-24中林根域sayms.com的域控制器上dc1.sayms.com，使用Domain Admins或Enterprise Admins组内的用户登录与创建信任。

STEP 2 选择【开始➲管理工具➲Active Directory域和信任关系】。

STEP 3 如图 8-26所示，通过【单击域sayms.com➲单击上方的**属性**图标】的方式进行操作。

Download at http://www.pin5i.com/

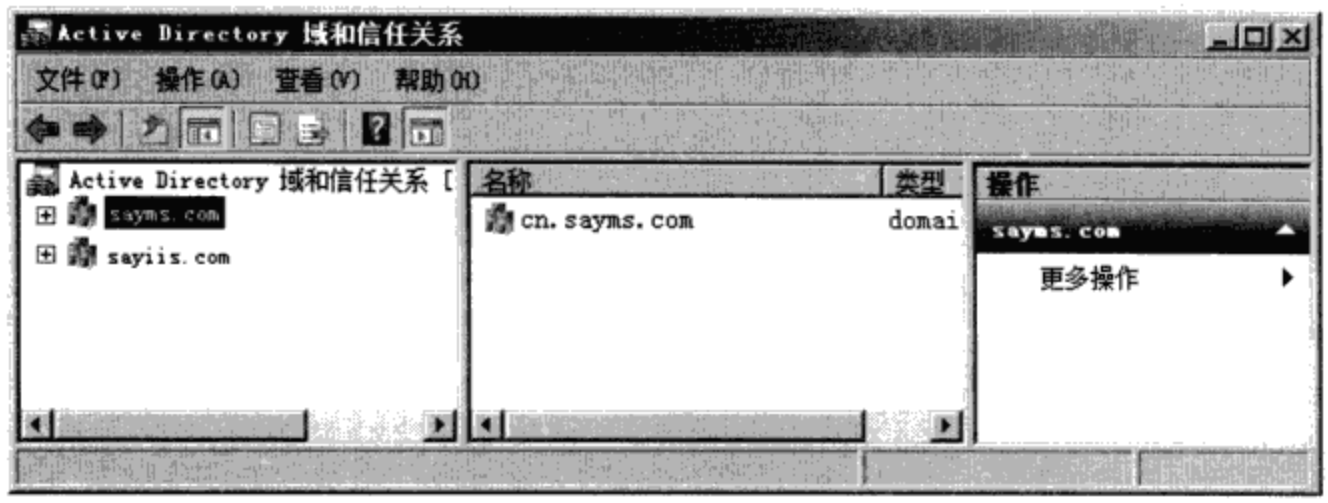


图 8-26

STEP 4 选择图 8-27中的**信任**标签，单击新建信任按钮。

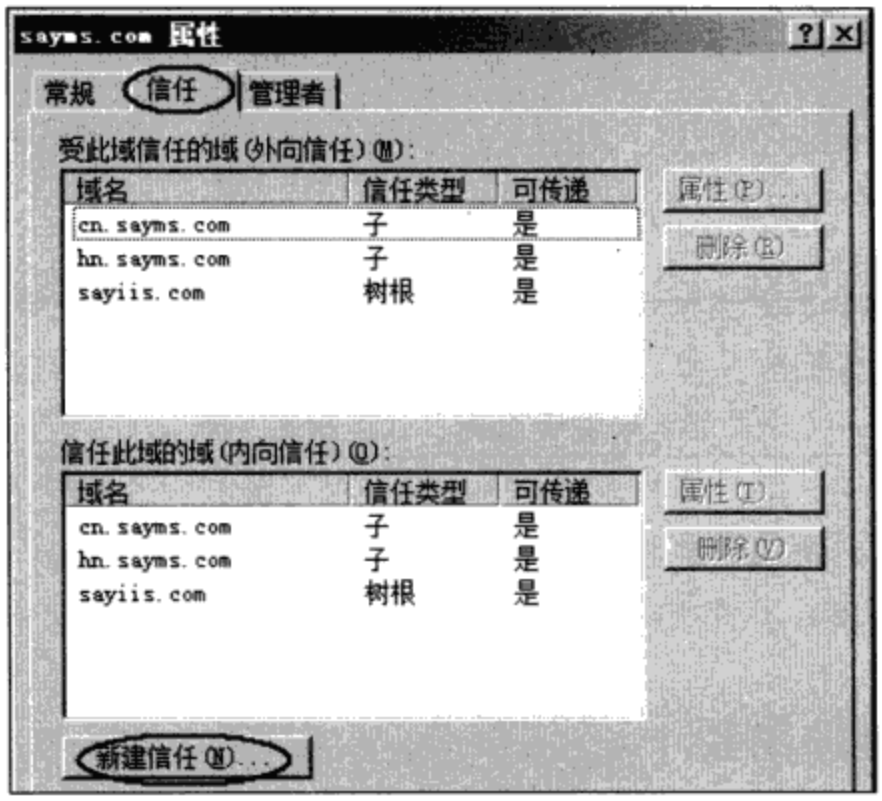


图 8-27

提示

由图中上半部分可看出，域sayms.com已经信任其子域cn.sayms.com和hn.sayms.com，同时也信任了另一个域树的根域sayiis.com；从图中的下半部分可看出，域sayms.com已经被其子域cn.sayms.com和hn.sayms.com所信任，同时也被另外一个域树的根域sayiis.com所信任。也就是说，域sayms.com和其子域之间已经自动存在双向**父-子信任**关系。还有域sayms.com和域树sayiis.com之间也已经自动存在双向**树状-根目录信任**关系。

STEP 5 在图 8-28中单击下一步按钮。如果图中没有**另一个林**这一行的话，表示**林功能级别**尚未提升为**Windows Server 2003**（含）以上。

Download at http://www.pin5i.com/

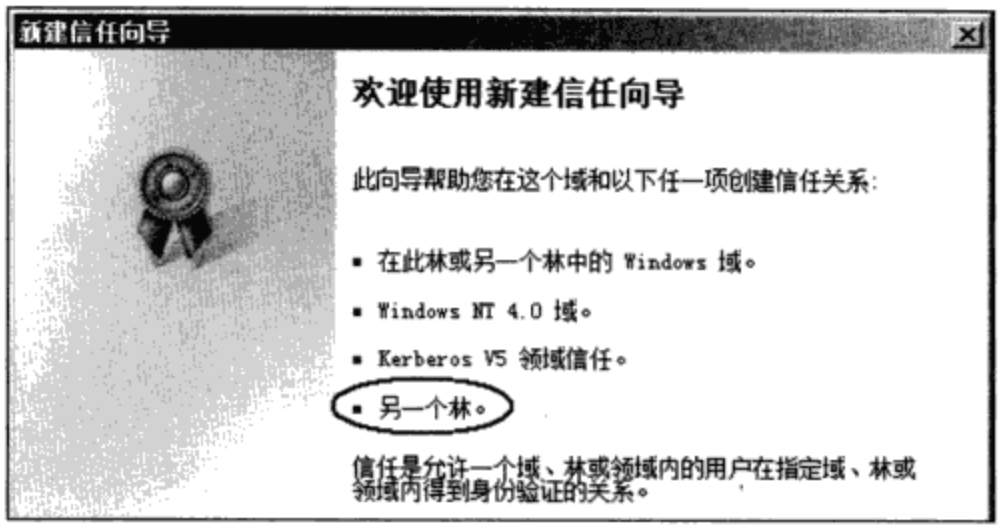


图 8-28

STEP 6 在图 8-29中输入对方域的DNS域名sayisa.com（或NetBIOS域名SAYISA），单击下一步按钮。

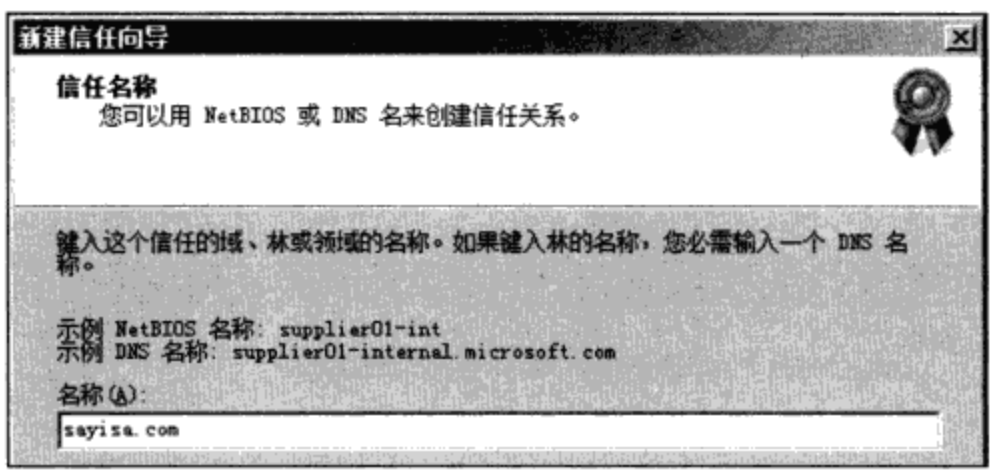


图 8-29

STEP 7 在图 8-30中选择**林信任**单选按钮后单击下一步按钮。

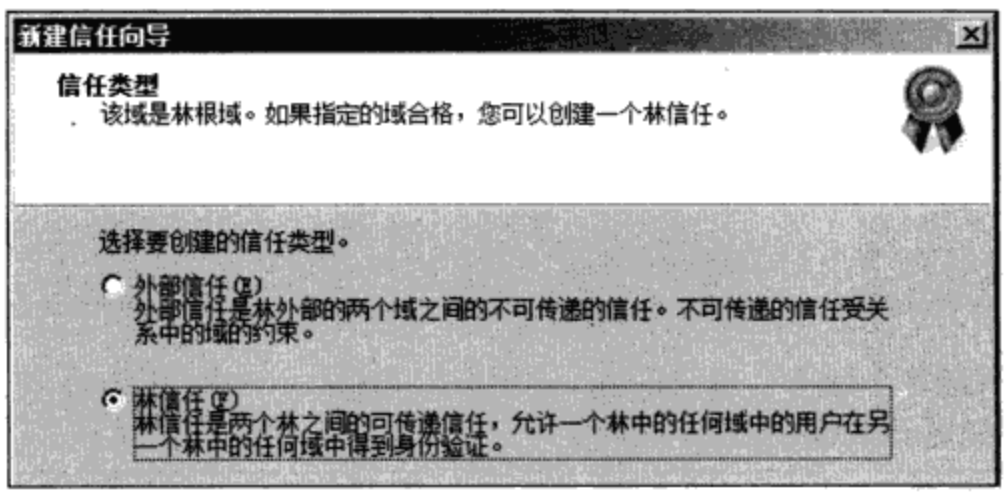


图 8-30

提示

若图中选择**外部信任**单选按钮的话，也可以让sayms.com和sayisa.com之间创建信任关系，不过它不具有**转移性**，然而**林信任**具有**转移性**。

Download at http://www.pin5i.com/

STEP 8 在图 8-31中选择**双向**单选按钮后单击 下一步 按钮，表示我们要同时创建图 8-24中左方域sayms.com的**传出信任**和**传入信任**。

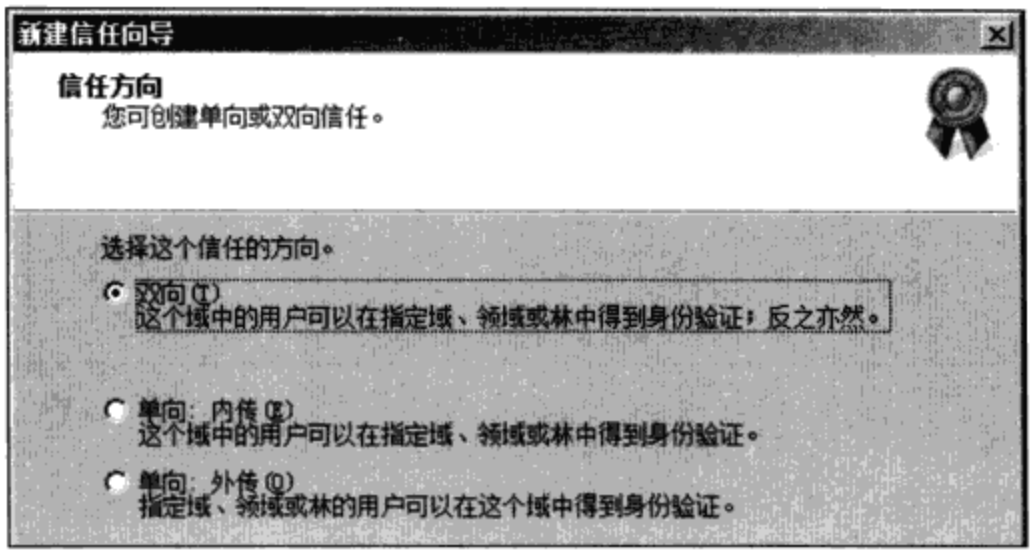


图 8-31

STEP 9 在图 8-32中选择**此域和指定的域**单选按钮，也就是除了要创建如图8-24所示的sayms.com的**传出信任**和**传入信任**之外，同时也要创建sayisa.com的**传入信任**和**传出信任**。

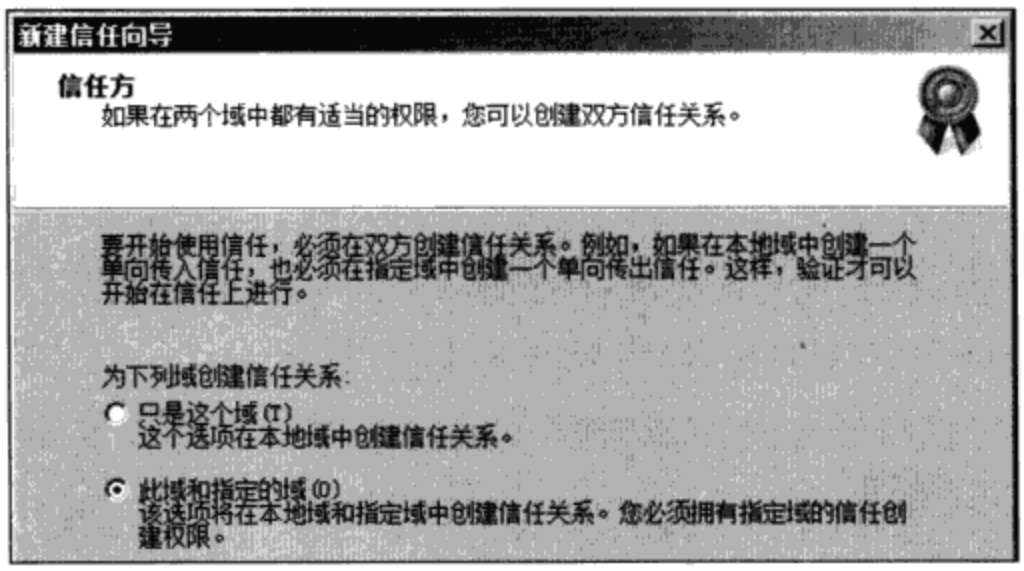


图 8-32

注意

如果您选择**只是这个域**单选按钮的话，则您必须事后另外再针对域sayisa.com来创建和域sayms.com之间的**传入信任**和**传出信任**。

STEP 10 在图 8-33中输入对方林根域（sayisa.com）内Domain Admins或Enterprise Admins组内的用户名和密码后单击 下一步 按钮。

Download at http://www.pin5i.com/

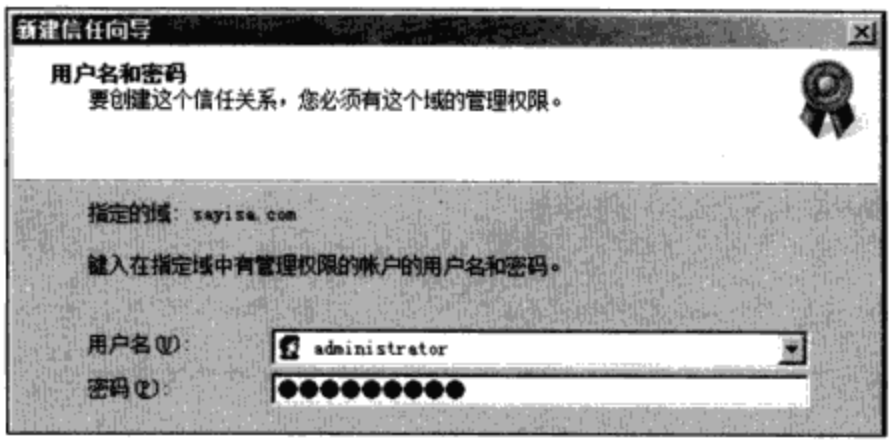


图 8-33

STEP 11 如图 8-34所示为如何验证另一个林（sayisa.com）的用户身份。

- 全林性身份验证：表示要验证另一个林内（sayisa.com）所有用户的身份。用户只要经过验证成功，就可以在本林内（sayms.com）访问他们拥有权限的资源。
- 选择性身份验证：此时另一个林内只有被选择的用户（或组）才会被验证身份，其他用户会被拒绝。被选择的用户只要经过验证成功，就可以在本林内访问他们拥有权限的资源。

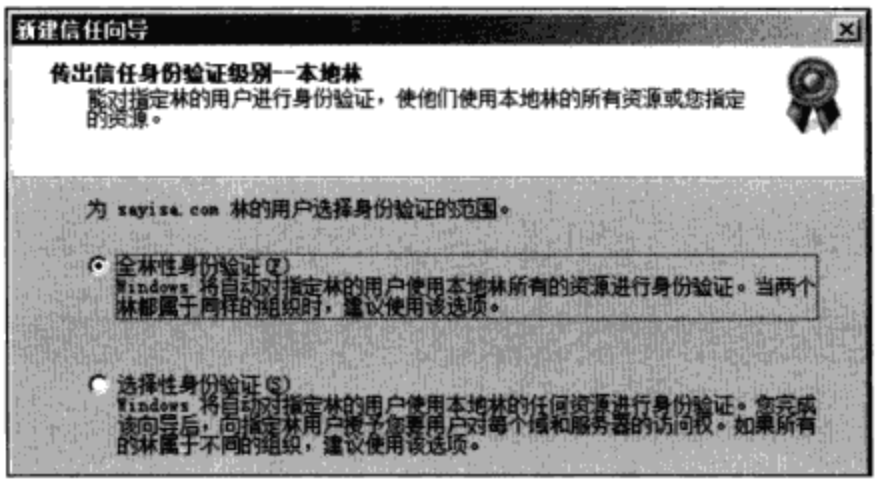


图 8-34

STEP 12 图 8-35是用来设置当本地林（sayms.com）中的用户要访问另外一个林（sayisa.com）内的资源时，如何来验证用户身份。

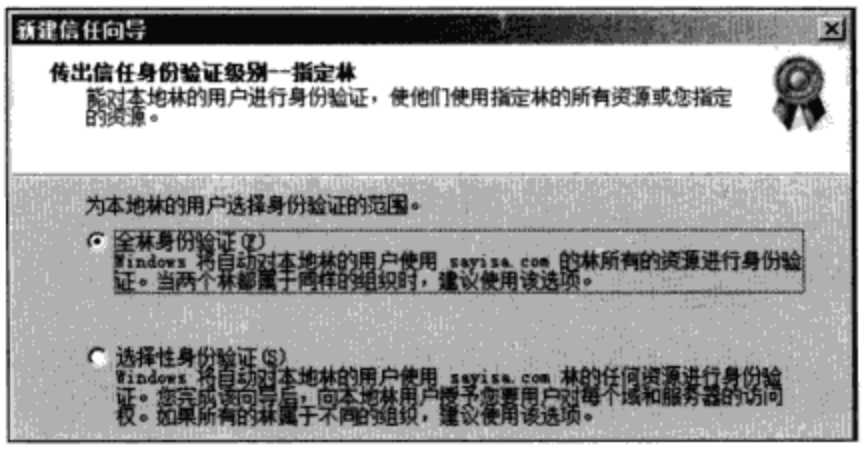


图 8-35

Download at http://www.pin5i.com/

STEP 13 在图 8-36中单击下一步按钮。

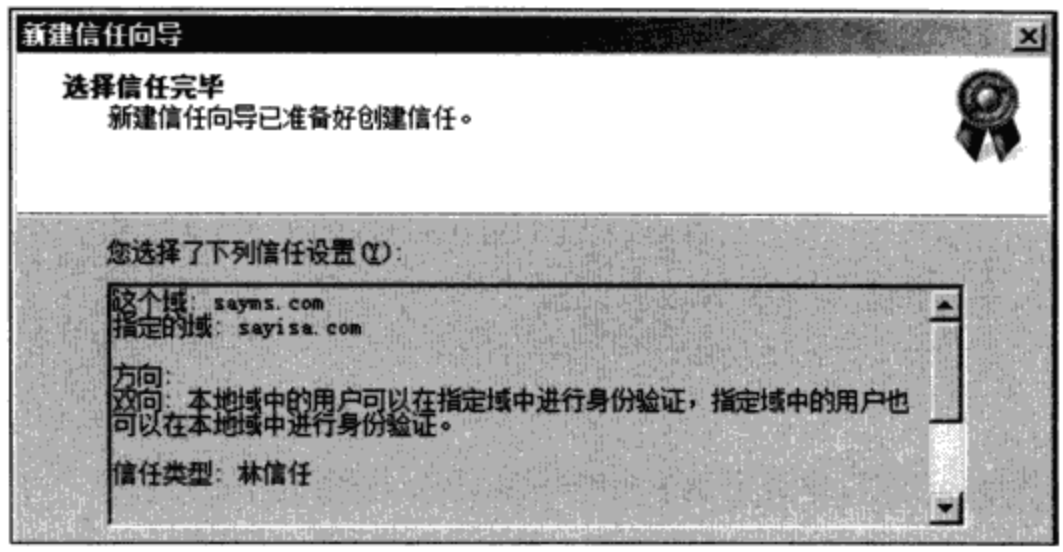


图 8-36

STEP 14 在图 8-37中单击下一步按钮。**路由名称后缀**（Routing Name Suffixes）是什么呢？图中显示本林会负责验证的后缀为sayms.com和sayiis.com，因此当本林中的用户使用UPN名称（例如george@sayms.com）在对方林中登录或访问资源时，对方就会将验证用户身份的工作转发到本林来执行，也就是根据后缀来将验证用户身份转到（路由到）本林。图8-37表示本林支持*.sayiis.com和*.sayms.com后缀，也就是sayms.com、hn.sayms.com、cn.sayms.com、sayiis.com、hk.sayiis.com等都是本林所支持的后缀，用户的UPN后缀只要是上述之一，则验证工作就会转给本林来执行。若不想让对方林将特定后缀的验证转到本林的话，可在图中取消选择该后缀。

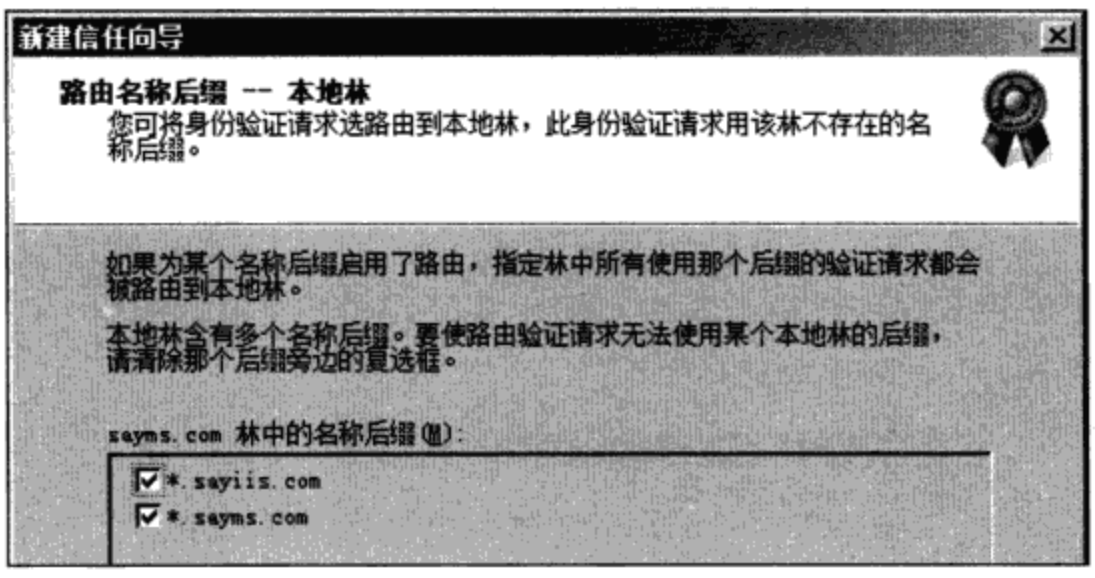


图 8-37

STEP 15 在图 8-38中单击下一步按钮。

Download at http://www.pin5i.com/

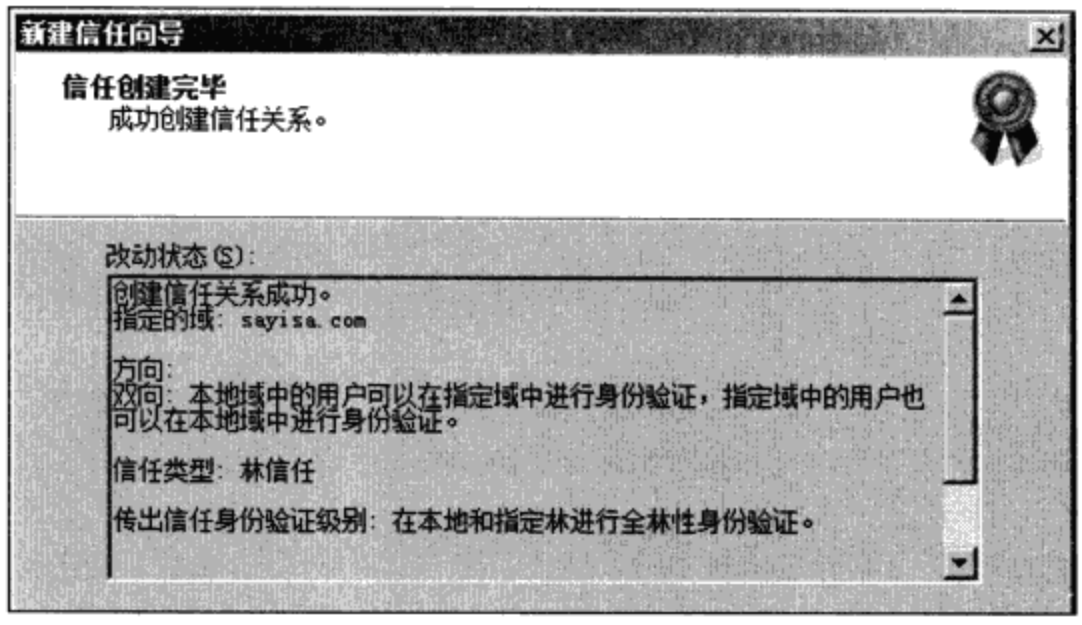


图 8-38

STEP 16 您可以在图 8-39中选择**是，确认传出信任**单选按钮，以便确认在图 8-24中sayms.com的**传出信任**和sayisa.com的**传入信任**这一组单向的信任是否创建成功。

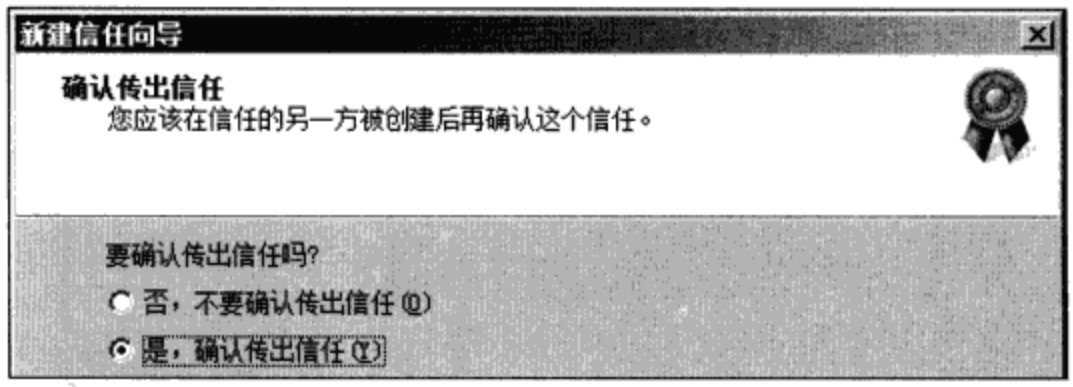


图 8-39

提示

如果您是分别单独创建域sayms.com的**传出信任**和域sayisa.com的**传入信任**的话，请确认这两个信任关系都已经创建完成后，再选择**是，确认传出信任**单选按钮。

STEP 17 您可以在图 8-40中选择**是，确认传入信任**单选按钮，以便确认在图 8-24中sayms.com的**传入信任**和sayisa.com的**传出信任**这一组单向的信任是否创建成功。

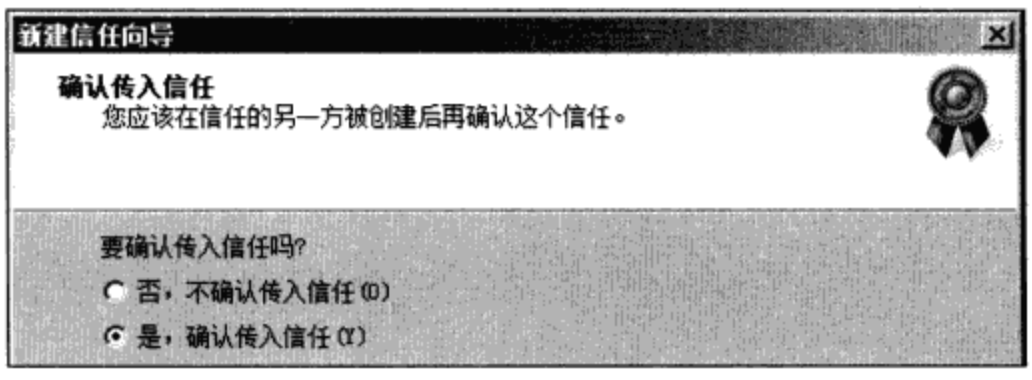


图 8-40

Download at http://www.pin5i.com/

STEP 18 在图 8-41中单击完成按钮。



图 8-41

图 8-42为完成创建双向**林信任**后的界面，图上方表示在域sayms.com中有一个传出到域sayisa.com的传出信任，也就是说域sayms.com信任域sayisa.com；图下方表示在域sayms.com中有一个从域sayisa.com来的传入信任，也就是说域sayms.com被域sayisa.com所信任。

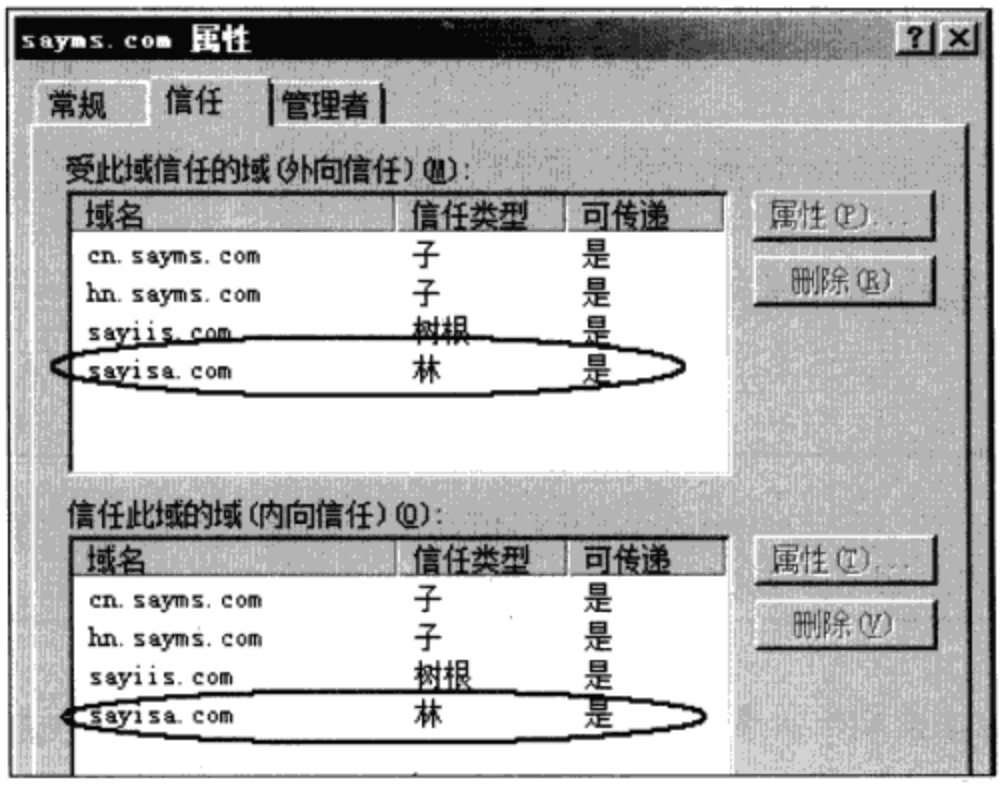


图 8-42

您也可以到林sayisa.com的域控制器上通过【开始➲管理工具➲ Active Directory域和信任关系➲如图 8-43所示对着sayisa.com单击右键➲属性➲**信任**标签】的方式来查看此双向信任。图上方表示在域sayisa.com中有一个传出到域sayms.com的传出信任，也就是说域sayisa.com信任域sayms.com；图下方表示在域sayisa.com中有一个从域sayms.com来的传入信任，也就是说域sayisa.com被域sayms.com所信任。

Download at http://www.pin5i.com/

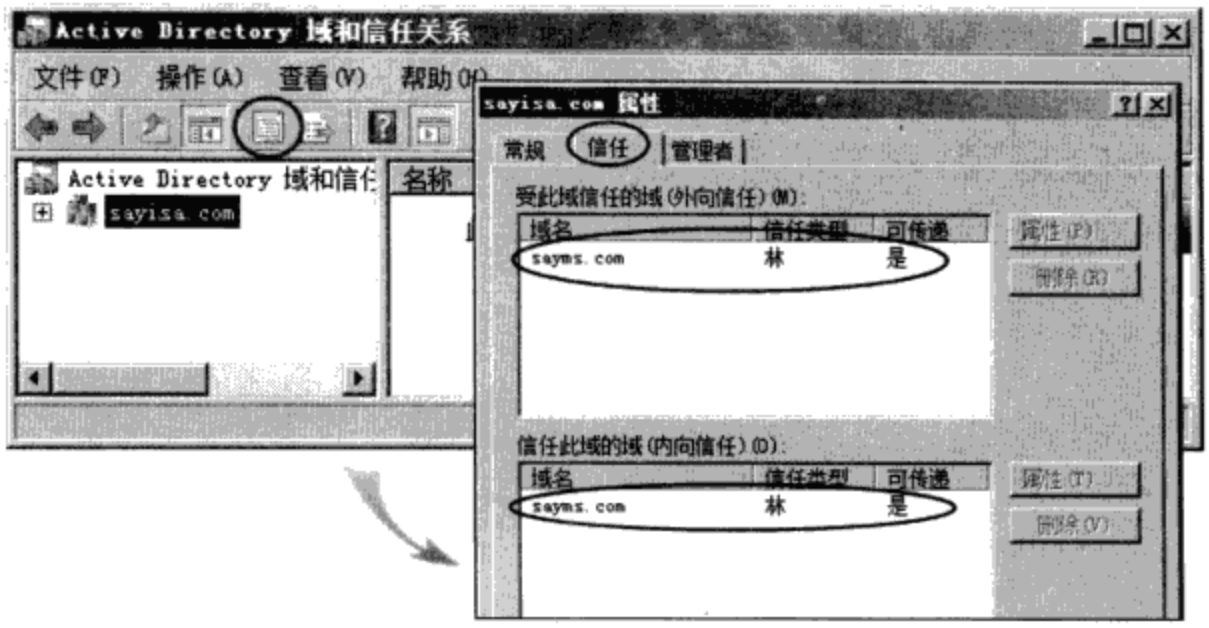


图 8-43

8-3-3 设置选择性身份验证

如果您在图 8-34中选择**选择性身份验证**单选按钮的话，则您需要在本林内的计算机上，将**允许身份验证**（Allowed to Authenticate）权限授予另外一个林内的用户（或组），只有拥有**允许身份验证**权限的用户来连接此计算机时才会被验证身份，而在经过验证成功后，该用户便有权限来访问此计算机内的资源。以下假设**信任林**（Trusting Forest）为sayms.com，而**受信任林**为sayisa.com。

STEP 1 请到**信任林**（sayms.com）内的域控制器dc1.sayms.com上选择【开始➲管理工具➲Active Directory管理中心➲如图 8-44所示双击要设置的计算机账户（假设是Win7PC1）】。

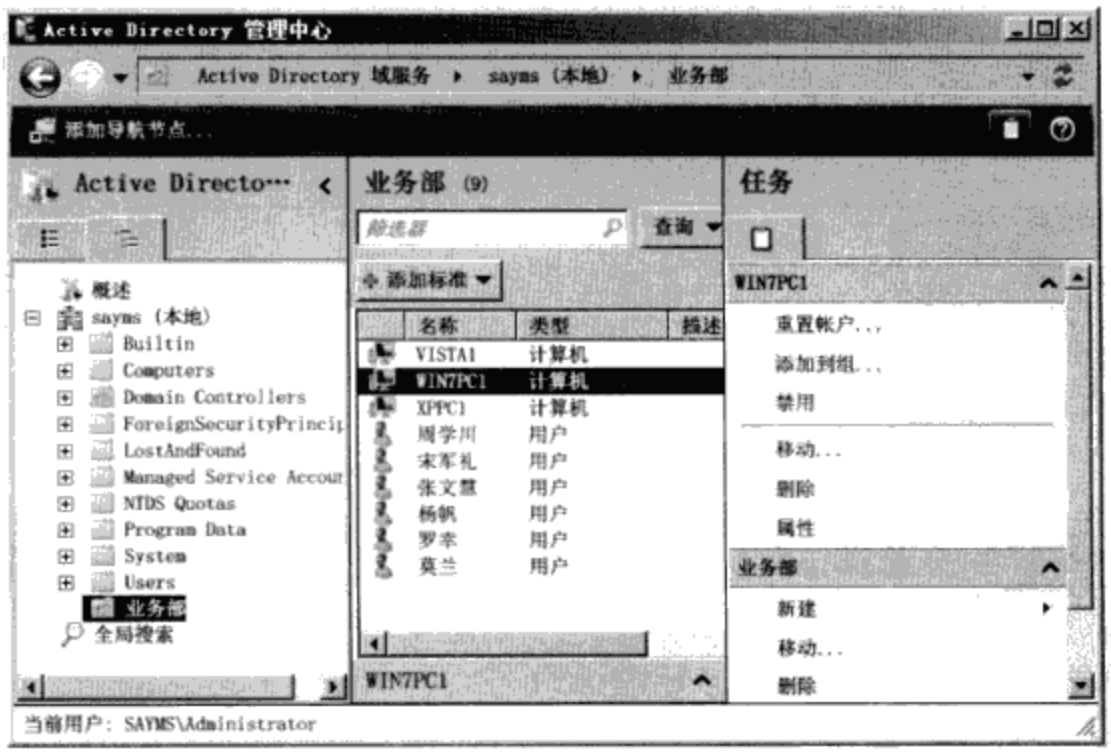


图 8-44

Download at http://www.pin5i.com/

STEP 2 如图 8-45所示单击**安全**标签下的添加按钮。

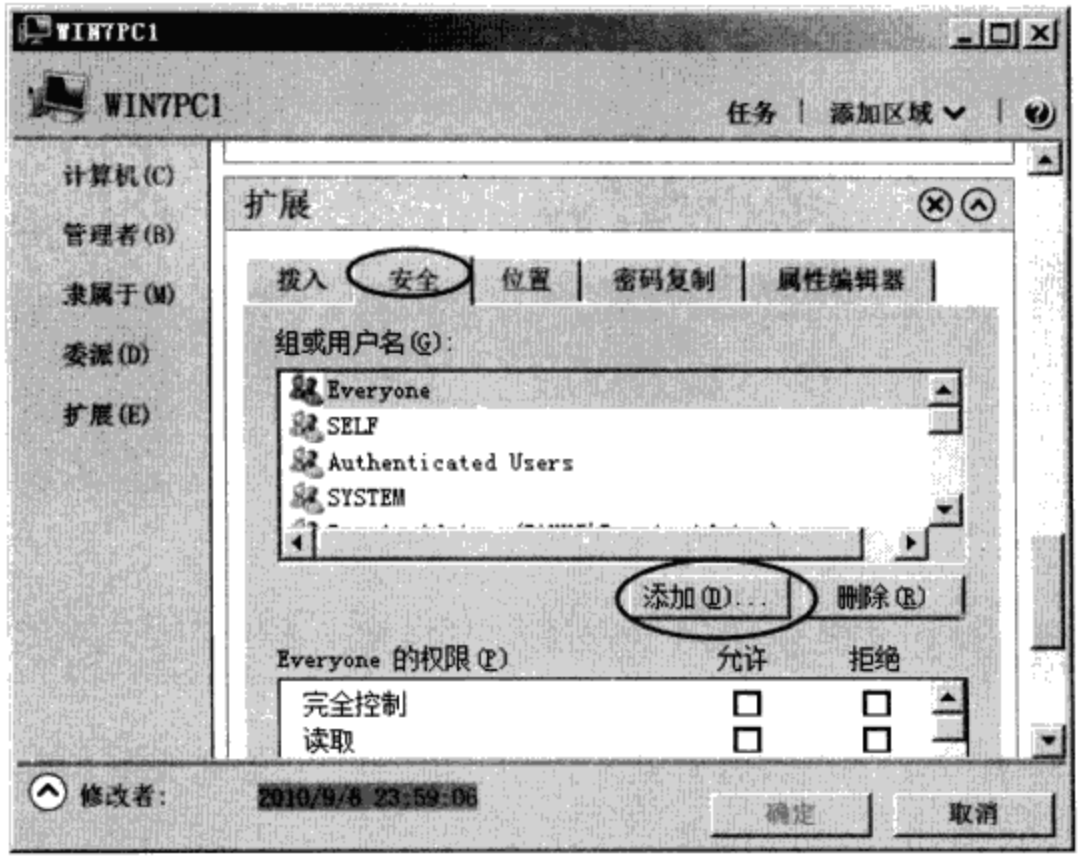


图 8-45

STEP 3 在图 8-46中单击位置按钮，选择对方林sayisa.com后单击确定按钮。

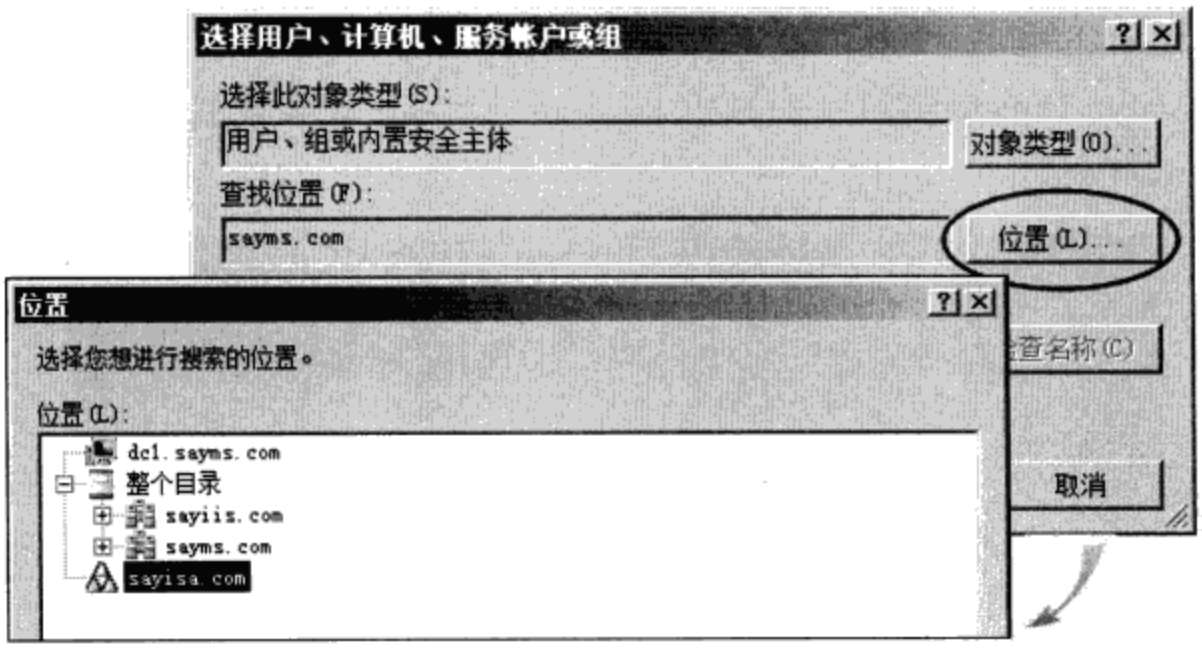


图 8-46

STEP 4 由图 8-47可知**查找位置**已被改为sayisa.com，接着请通过单击高级按钮来选择sayisa.com内的用户或组，图中是已经完成选择后的界面，而所选的用户为Robert，单击确定按钮。

Download at http://www.pin5i.com/

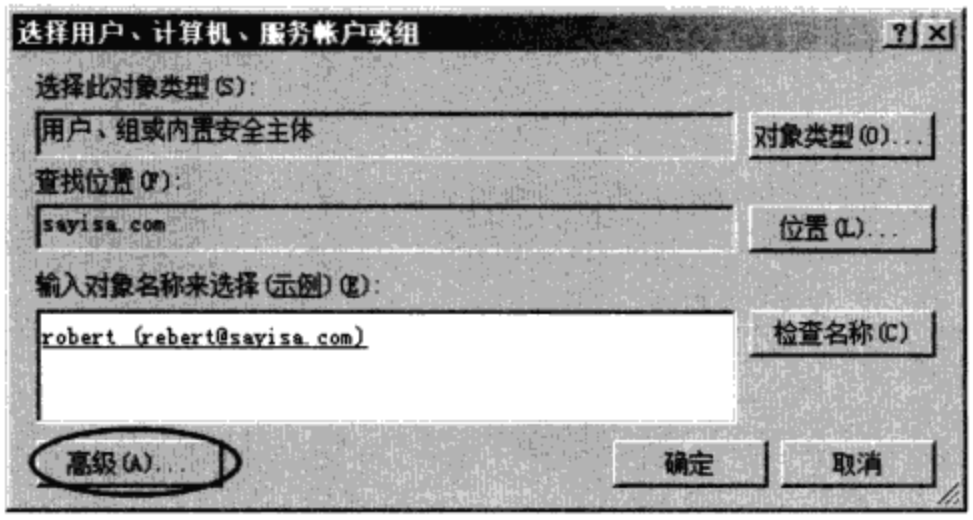


图 8-47

STEP 5 如图 8-48所示在**允许身份验证**右边选择**允许**后单击确定按钮。

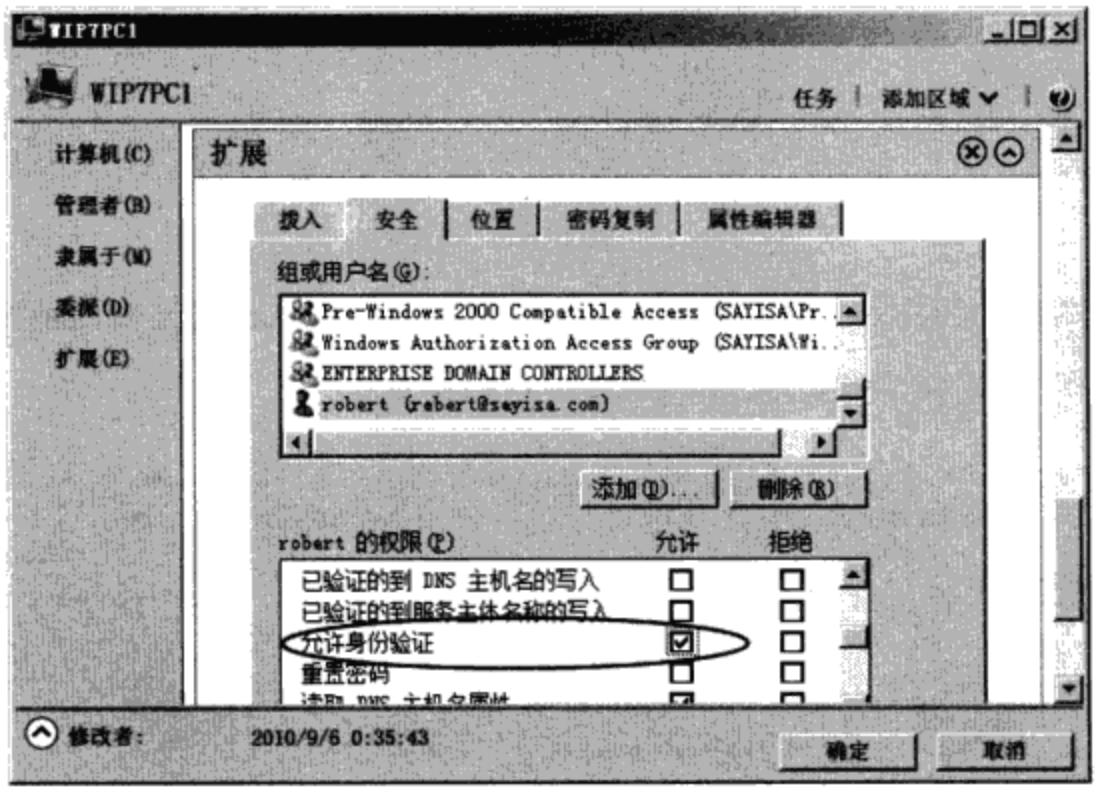


图 8-48

8-4 创建外部信任

本节以创建图 8-49中林sayms.com和林sayexg.com之间的双向**外部信任**为例进行说明。

Download at http://www.pin5i.com/

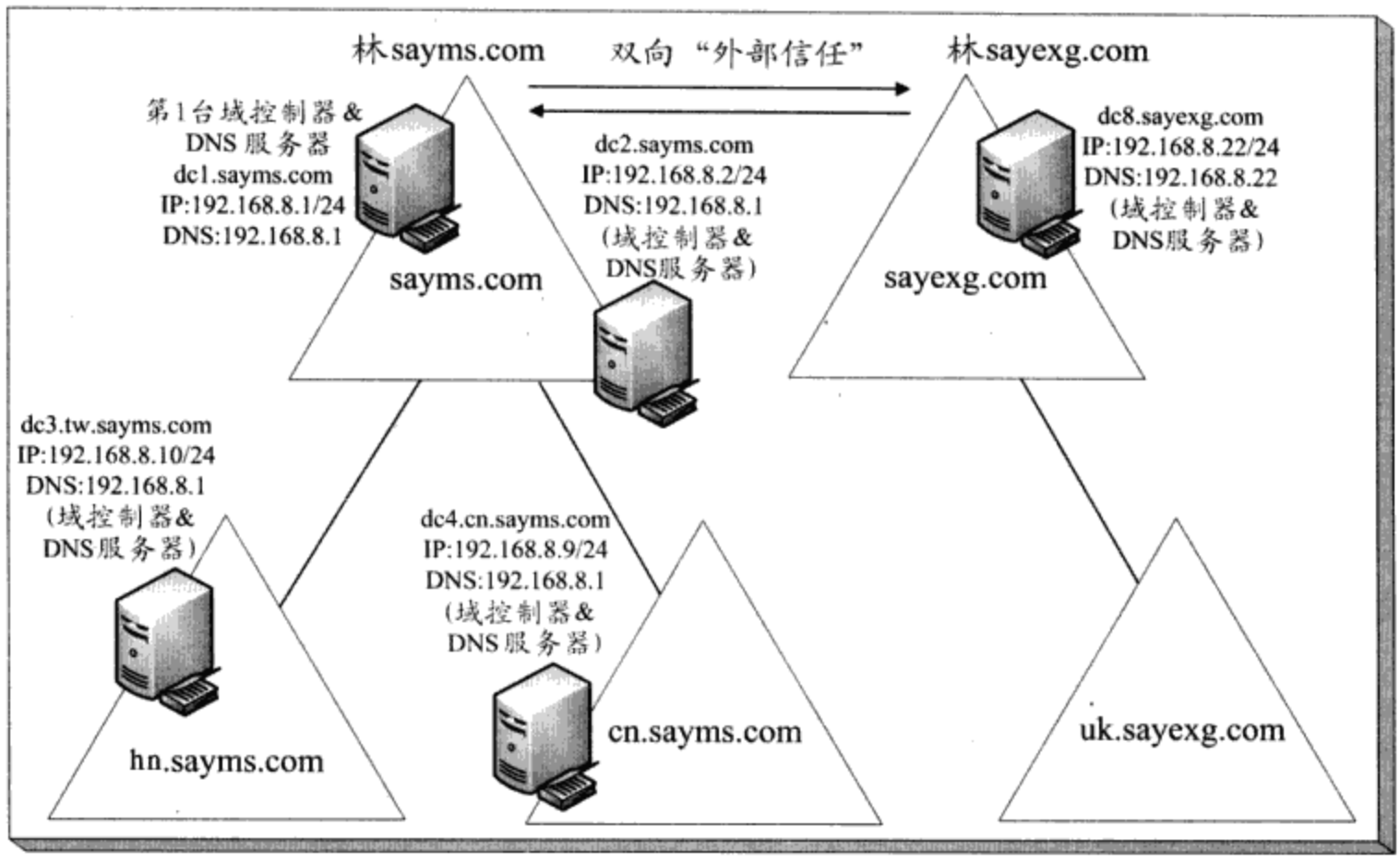


图8-49

我们将图重新简化为图 8-50，图中我们要在林根域sayms.com创建**传出信任**和**传入信任**，相对的也要在林根域sayexg.com创建**传入信任**和**传出信任**。

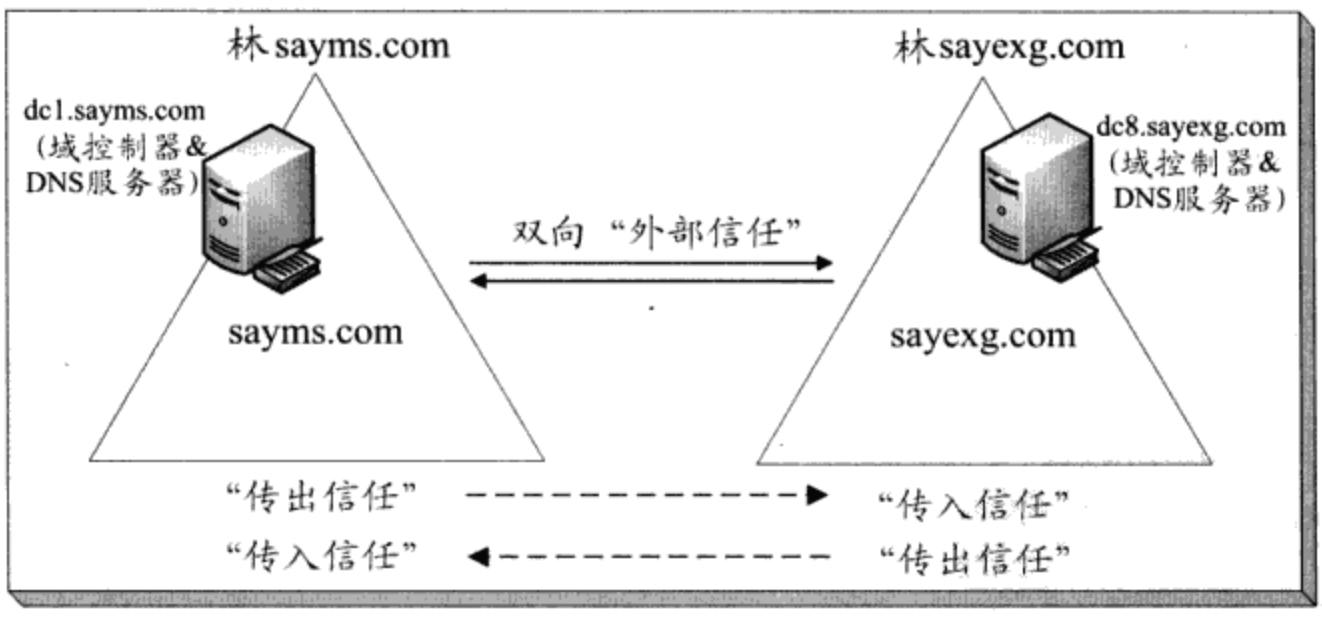


图8-50

外部信任的注意事项、DNS服务器设置、创建步骤等和**林信任**相同，此处不再重复，不过在创建**外部信任**时需在如图 8-51所示的对话框中选择**外部信任**单选按钮。

Download at http://www.pin5i.com/

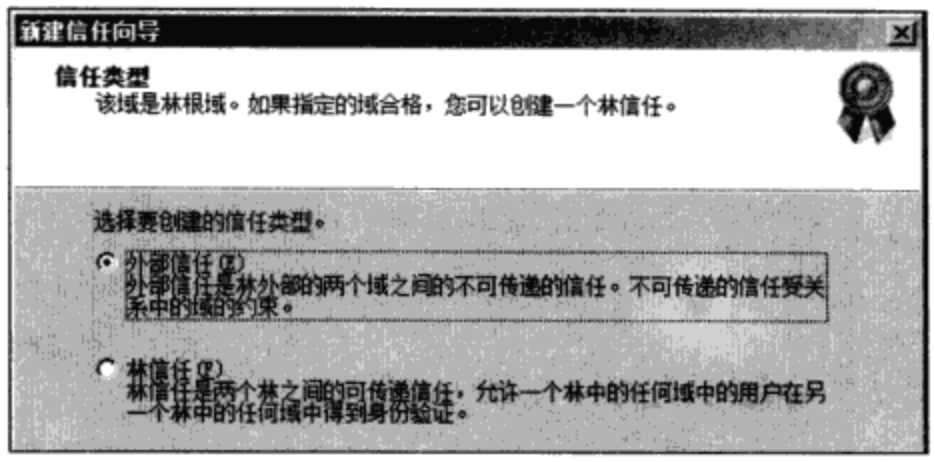


图 8-51

还有会另外显示如图8-52所示的对话框，表示系统默认会自动启用**SID筛选**（SID Filter Quarantining）功能，以便增加安全性：若外部**受信任域**的域控制器被入侵的话，它可能会在**SID历史**（SID History）内插入**信任域**的系统管理员的SID，如此会让入侵者在**信任域**内拥有系统管理员的权限，而这个**SID筛选**功能会将不属于用户域（Home Domain）的SID删除，避免入侵者通过**SID历史**取得**信任域**内不该拥有的权限。

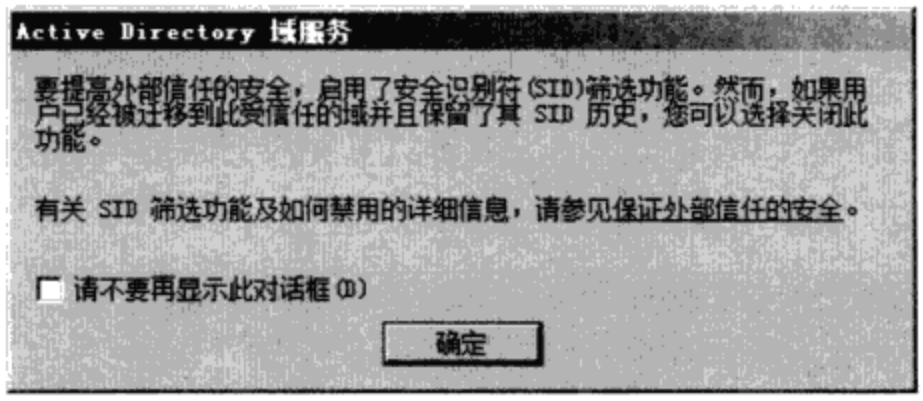


图 8-52

图 8-53为完成**外部信任**创建后，在**信任域**sayms.com所看到的界面；而图 8-54为在**受信任域**sayexg.com所看到的界面。

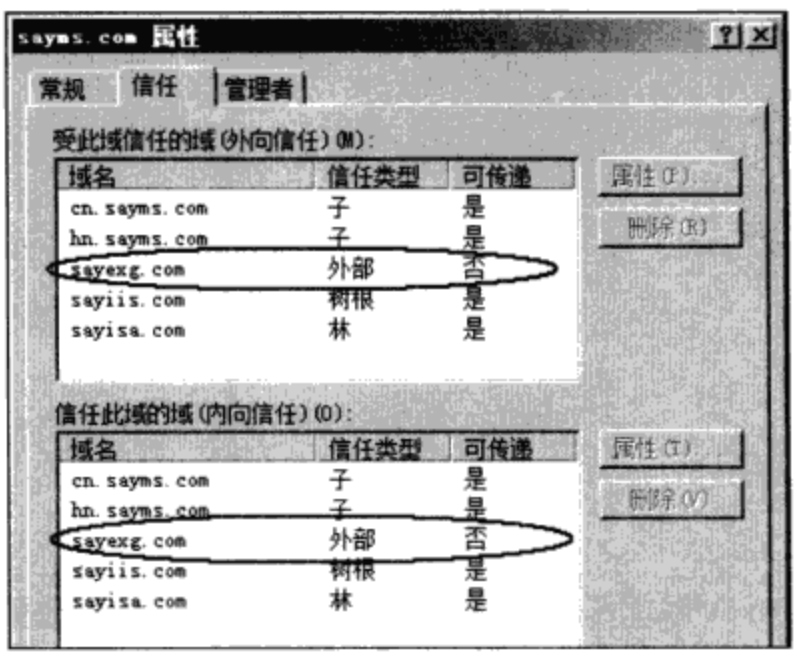


图 8-53

Download at http://www.pin5i.com/

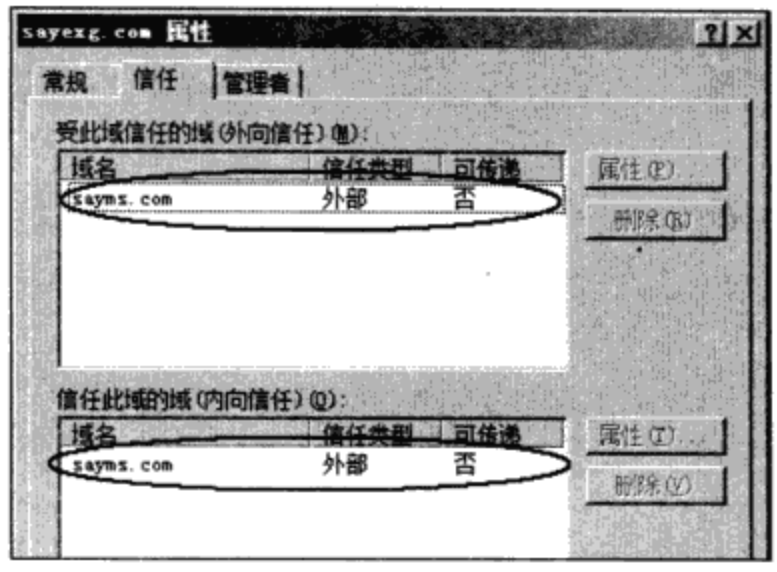


图 8-54

8-5 管理和删除信任

8-5-1 信任的管理

若要更改信任设置的话，只要如图 8-55所示【选择要管理的传出或传入信任➲单击**属性**按钮】，然后通过弹出的对话框来管理信任关系。

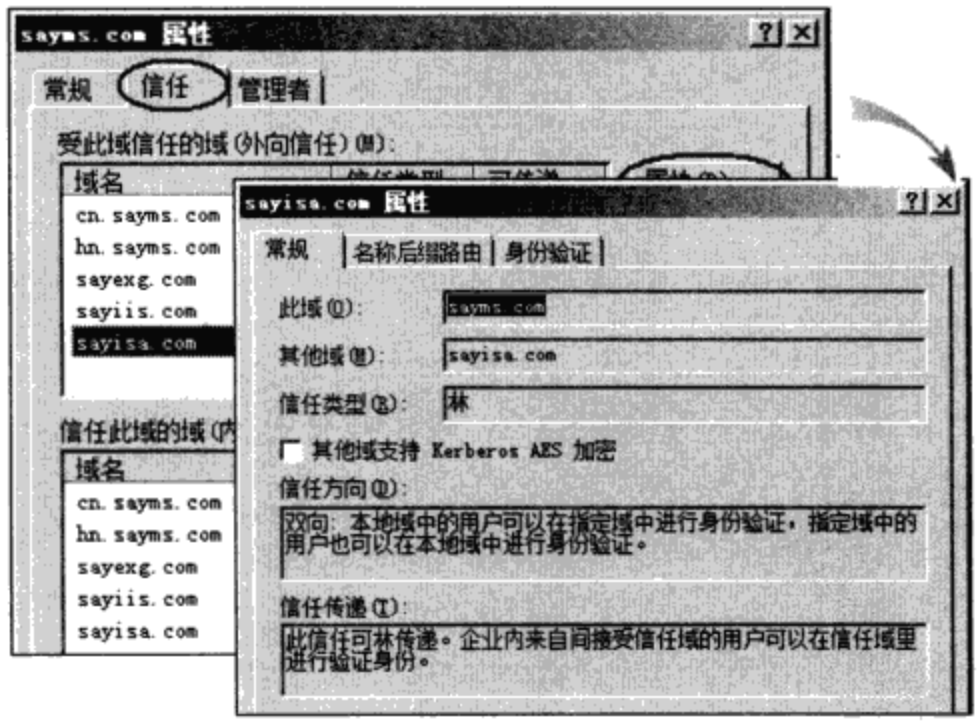


图 8-55

1. 验证信任关系

若对方域支持Kerberos AES加密的话，则可选择图 8-55中的**其他域支持Kerberos AES加密**复选框。若要重新确认和对方域或林之间的信任关是否仍然有效的话，请单击**验证**按钮。若

Download at http://www.pin5i.com/

对方域或林内有新子域的话，此验证也可同时更新**名称后缀路由**（Name Prefix Routing，详见图 8-37的说明）的信息。

2. 更改名称后缀路由设置

当用户的UPN（例如george@sayisa.com）后缀是隶属于此指定林时，则用户身份的验证工作会转给此林的域控制器。图 8-56中的**名称后缀路由**标签用来更改所选林的名称后缀路由状态，例如要停止将后缀为sayisa.com的验证转给林sayisa.com的话，请在图 8-56中单击该林后缀后单击禁用按钮。

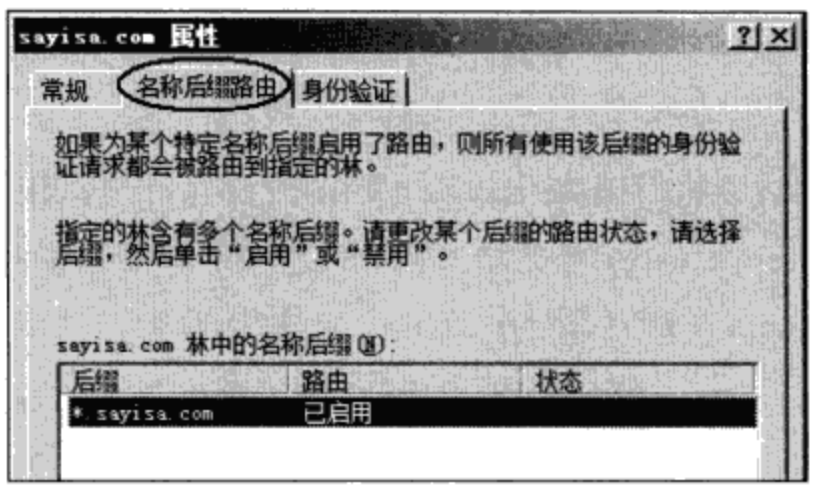


图 8-56

如果该林内包含多个后缀，例如sayisa.com、us.sayisa.com，而您只是要停止将其中部分后缀验证工作转给该林的话，请【单击图 8-56中的编辑按钮➲在图 8-57中选择要禁用的名称后缀（例如us.sayisa.com）➲单击禁用按钮】。

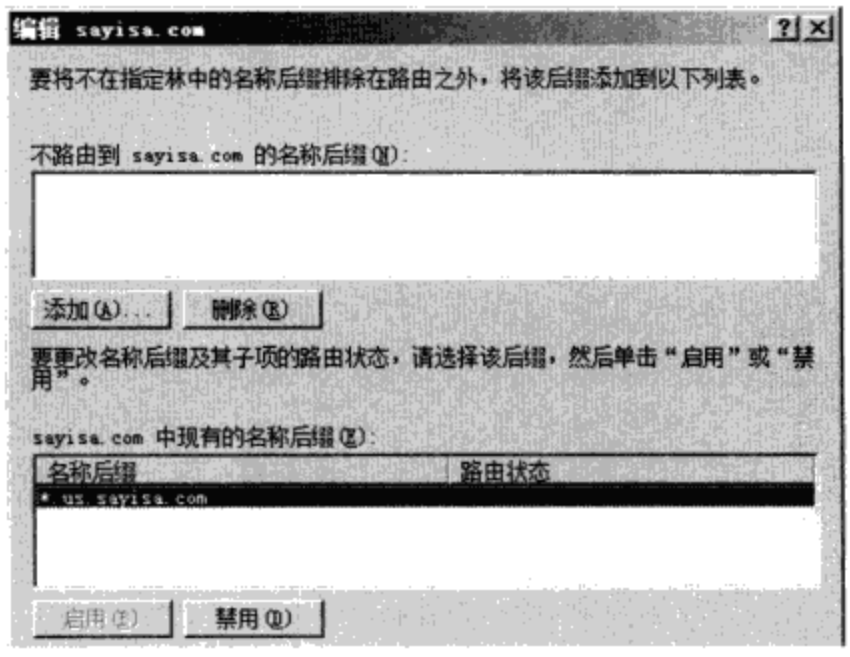


图 8-57

另外为了避免**后缀名称冲突**现象的发生，此时您可以通过图 8-57上方的添加按钮来将后缀排除。何谓**后缀名称冲突**现象？举例来说，图 8-58中林sayms.com和林sayisa.com之间创建了

Download at http://www.pin5i.com/

双向林信任、林sayisa.com和林jp.sayisa.com（注意是林，不是子域）之间也创建了双向林信任、林sayms.com和林jp.sayisa.com之间创建了单向林信任。

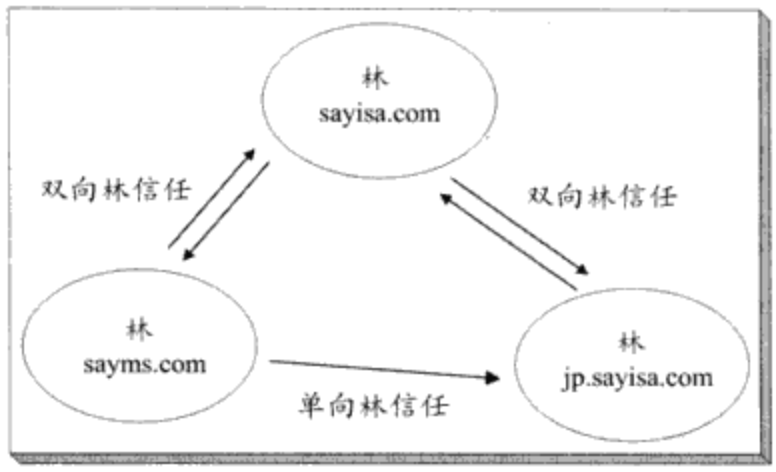


图8-58

图中林sayms.com默认会将后缀为*.sayisa.com的身份验证工作转给林sayisa.com来运行，包含后缀sayisa.com和jp.sayisa.com，可是因为两个林之间的**林信任**关系并无法自动的扩展到第3个林，因此当林sayisa.com收到后缀为jp.sayisa.com的身份验证要求时，并不会将其转给林jp.sayisa.com。

解决上述问题的方法为在林sayms.com中将后缀jp.sayisa.com排除，也就是【编辑信任关系sayisa.com➲在图 8-59中单击添加按钮➲输入后缀jp.sayisa.com➲单击确定按钮】，如此林sayms.com就不会将后缀是jp.sayisa.com的身份验证要求转给林sayisa.com，而是直接转给林jp.sayisa.com（因为图 8-59中林sayms.com和林jp.sayisa.com之间有单向林信任）。

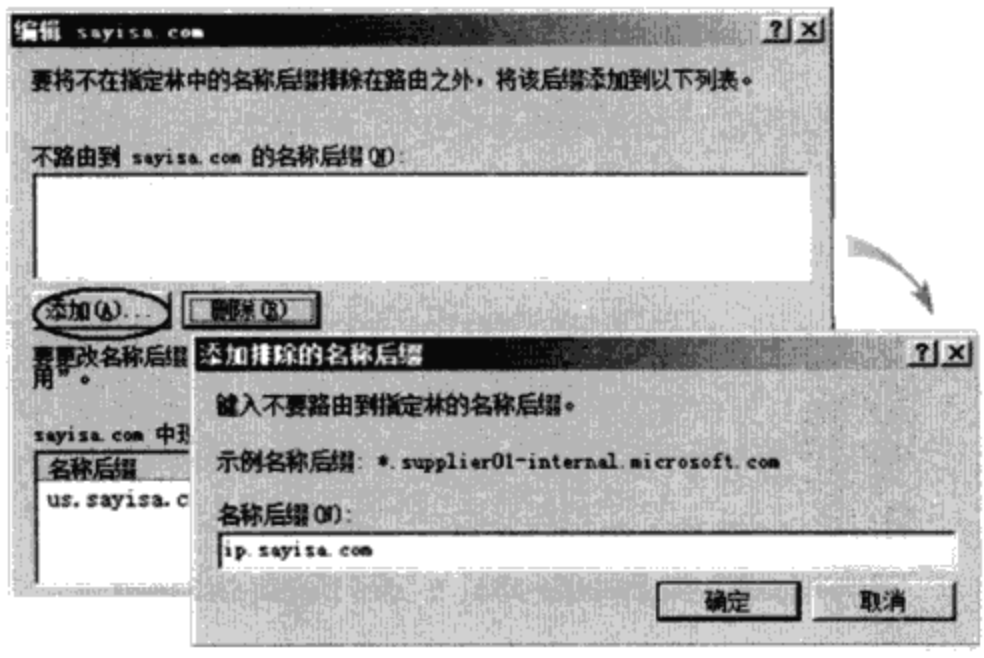


图8-59

3. 更改验证方法

若要更改身份验证方法的话，请通过图 8-60中的**身份验证**标签来设置，图中两个身份验证方法的说明请参考图 8-34。

Download at http://www.pin5i.com/

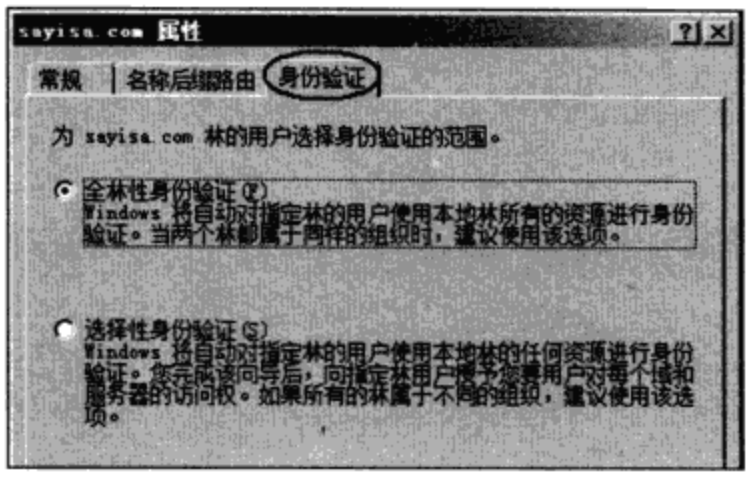


图 8-60

8-5-2 信任的删除

您可以将**快捷方式信任**、**林信任**、**外部信任**、**领域信任**等自行创建的信任删除，然而系统自动创建的**父-子信任**和**树状-根目录信任**不可以删除。

我们以图 8-61为例来说明如何删除信任，而且是要删除图中**林sayms.com信任sayisa.com**这个单向的信任，但是保留**林sayisa.com信任sayms.com**。

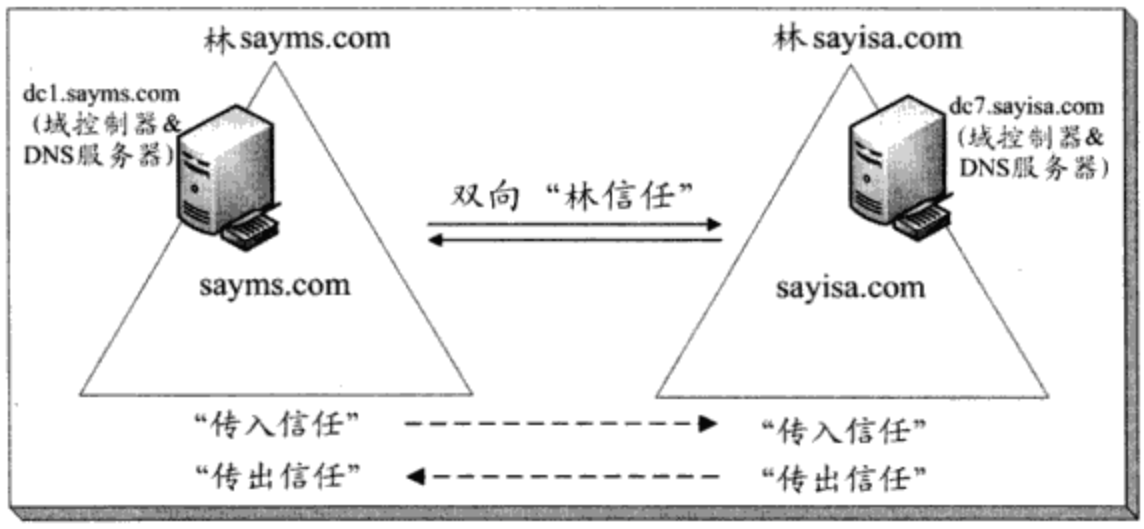


图 8-61

STEP 1 如图 8-62所示，通过【单击域sayms.com➲单击上方的**属性**图标】的方式进行操作。

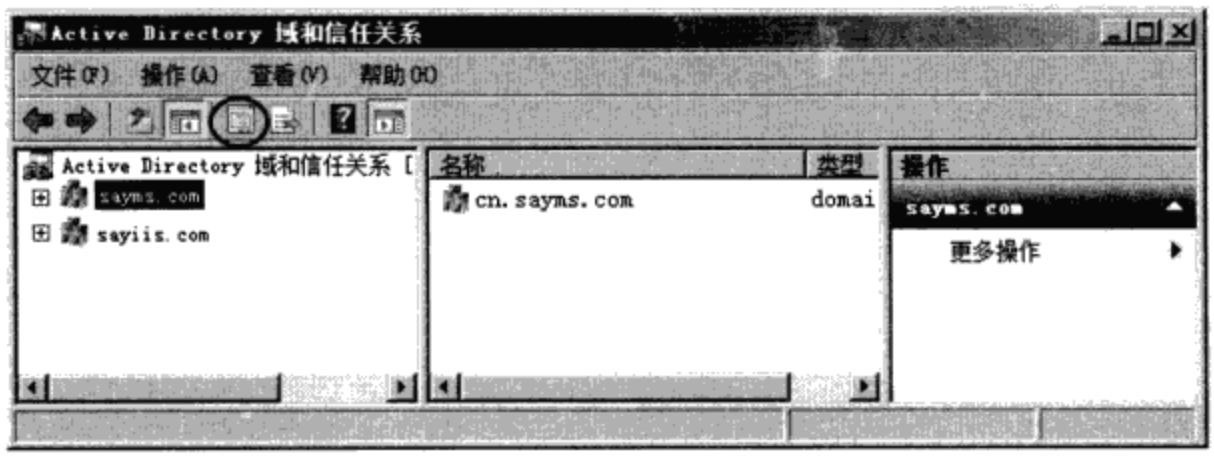


图 8-62

Download at http://www.pin5i.com/

STEP 2 在图 8-63中，通过【单击**信任**标签➲选择**受此域信任的域（外向信任）**之下的域sayisa.com】的方式进行操作，也就是选择图 8-61中sayms.com的**传出信任**，然后单击删除按钮。

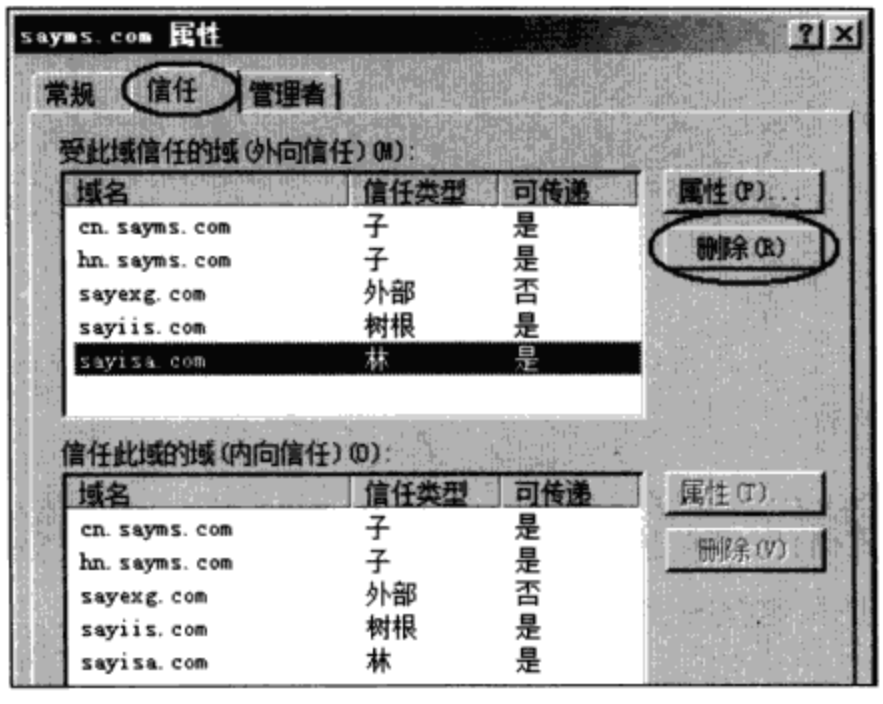


图 8-63

STEP 3 在图 8-64中可以选择的项目如下。

- 不，只从本地域删除信任：也就是只删除图 8-61中的sayms.com的外向信任。
- 是，从本地域和另一个域中删除信任：也就是同时删除图 8-61中的sayms.com的外向信任和sayisa.com的内向信任。若选择此选项的话，则您必须输入对方域sayisa.com的Domain Admins或Enterprise Admins组内的用户名和密码。

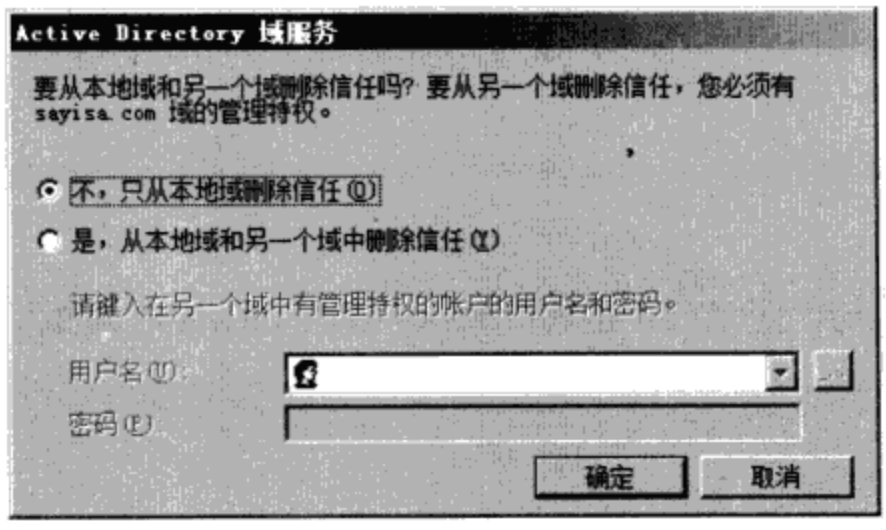


图 8-64

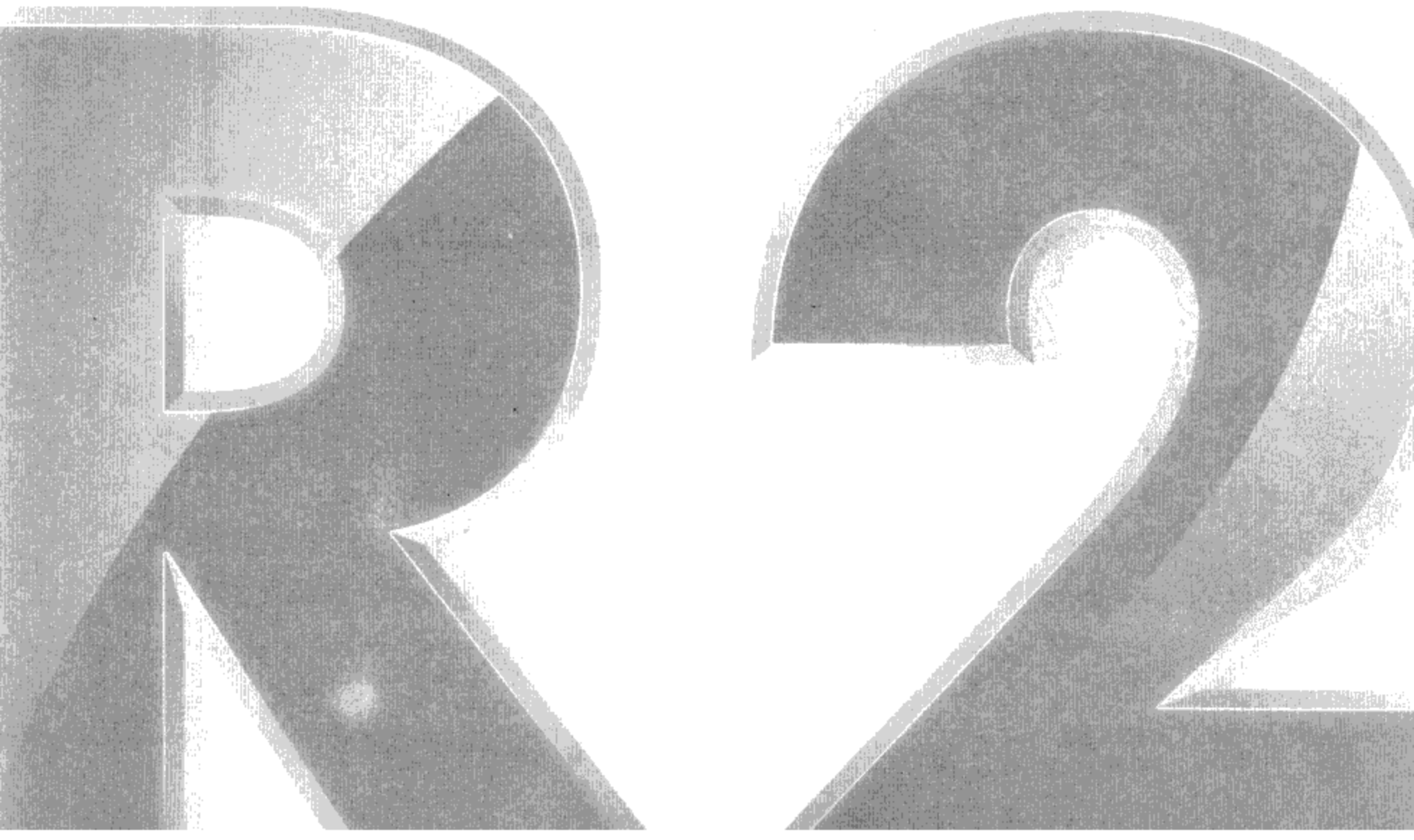
Download at http://www.pin5i.com/

第9章

Active Directory 数据库的复制

对拥有多台域控制器的**Active Directory域服务**（AD DS）来说，如何更高效地复制Active Directory数据库、如何提高AD DS的可用性与如何让用户能够快速的登录，是身为系统管理员的您必须了解的重要课题。

- 站点与Active Directory数据库的复制
- 默认站点的管理
- 利用站点来管理Active Directory复制
- 管理全局编录服务器
- 解决Active Directory复制冲突的问题



Download at http://www.pin5i.com/

9-1 站点与Active Directory数据库的复制

站点（Site）是由一个或多个IP子网（Subnet）所组成，这些子网之间通过**高速且可靠的连接**串接起来，也就是这些子网之间的连接速度要够快且稳定、符合您的需要，否则您就应该将它们分别规划为不同的站点。

一般来说，一个LAN（局域网）之内各个子网之间的连接都符合速度快且高可靠度的要求，因此可以将一个LAN规划为一个站点；而WAN（广域网）内各个LAN之间的连接速度一般都不快，因此WAN之中的各个LAN应分别规划为不同的站点，如图 9-1所示。

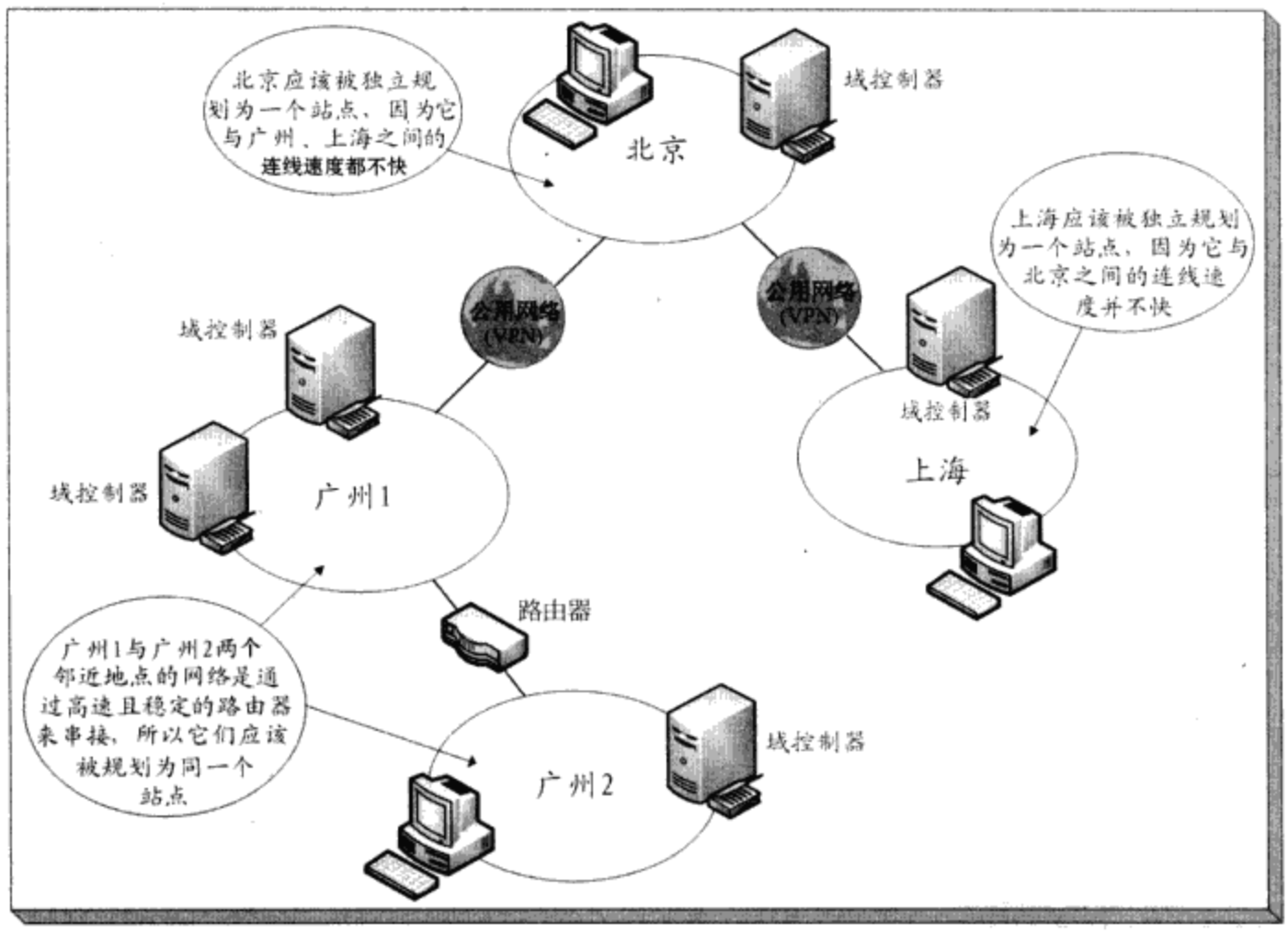


图9-1

AD DS内大部分数据是利用**多主机复制模式**（Multi-Master Replication Model）来复制。在这种模式之中，您可以直接更新任何一台域控制器内的Active Directory对象，之后这个更新对象会被自动复制到其他域控制器，例如当您在任意一台域控制器的Active Directory数据库内新建一个用户账户后，这个账户会自动被复制到域内的其他域控制器。

站点与Active Directory数据库的复制之间有着重要的关系，因为这些域控制器是否在同一个站点内，会影响到域控制器之间Active Directory数据库的复制操作。

Download at http://www.pin5i.com/

9-1-1 同一个站点之间的复制

由于同一个站点内的域控制器之间是通过快速的连接串接在一起，因此在复制Active Directory数据库时，可以有效的、快速的复制，而且不会压缩所发送的数据。

同一个站点内的域控制器之间的Active Directory复制是采用**更改通知**（Change Notification）的方式，也就是当某台域控制器（以下将其称为**源域控制器**）的Active Directory数据库内有一条数据变动时，默认它会等15s后，就通知位于同一个站点内的其他域控制器。收到通知的域控制器如果需要这条数据的话，就会发出**更新数据**的请求给**源域控制器**，这台**源域控制器**收到请求后，便会开始复制的程序。

1. 复制伙伴

源域控制器并不是直接将变动数据复制给同一个站点内的所有域控制器，而是只复制给它的**直接复制伙伴**（Direct Replication Partner），而哪些域控制器是其**直接复制伙伴**呢？每一台域控制器内都有一个被称为Knowledge Consistency Checker（KCC）的程序，它会自动创建最有效率的**复制拓扑**（Replication Topology），也就是决定哪一些域控制器是它的**直接复制伙伴**，而哪些域控制器是它的**转移复制伙伴**（Transitive Replication Partner），换句话说，**复制拓扑**是复制Active Directory数据库的逻辑连接路径，如图 9-2所示。

以图中域控制器DC1来说，域控制器DC2是它的**直接复制伙伴**，因此DC1会将变动数据直接复制给DC2，而DC2收到数据后，会再将它复制给DC2的**直接复制伙伴**DC3，依次类推。

对域控制器DC1来说，除了DC2与DC7是它的**直接复制伙伴**外，其他的域控制器（DC3、DC4、DC5、DC6）都是**转移复制伙伴**，它们用于间接获得由DC1复制来的数据。

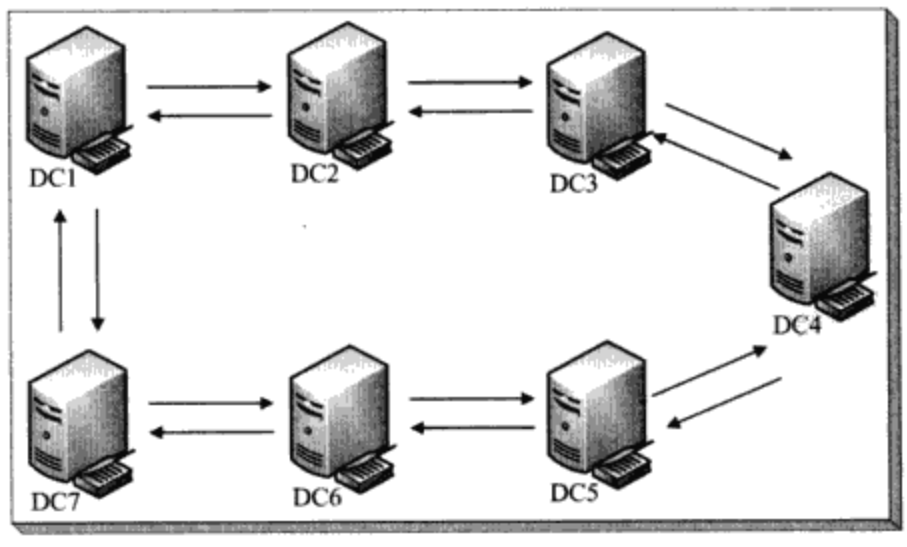


图 9-2

2. 如何减少复制延迟时间

为了减少复制的延迟时间（Replication Latency），也就是从**源域控制器**内的Active Directory

Download at http://www.pin5i.com/

数据有变动开始，到这些数据被复制到所有其他域控制器之间的间隔时间不要太长，因此KCC在创建**复制拓扑**时，会让数据从**源域控制器**发送到**目的域控制器**时，其所跳跃的域控制器数量（Hop Count）不超过3台，以图 9-2来说，从DC1到DC4跳跃了3台域控制器（DC2、DC3、DC4），而从DC1到DC5也只跳跃了3台域控制器（DC7、DC6、DC5）。换句话说，KCC会让**源域控制器**与**目的域控制器**之间的域控制站数量不超过2台。

> **提示**
>
> 为了避免**源域控制器**负担过重，因此**源域控制器**并不是同时通知其所有的**直接复制伙伴**，而是会间隔3s，也就是先通知第1 台**直接复制伙伴**，间隔3s后再通知第2台，依次类推。

当有新域控制器加入时，KCC会重新创建**复制拓扑**，而且仍然会遵照**跳跃的域控制器数量不超过3台**的策略，例如当图 9-2中添加了一台域控制器DC8后，其**复制拓扑**就会有变化，图 9-3为可能的**复制拓扑**之一，图中KCC将域控制器DC8与DC4设置为**直接复制伙伴**，否则DC8与DC4之间，无论是通过【DC8→DC1→DC2→DC3→DC4】或【DC8→DC7→DC6→ DC5→DC4】的途径，都会违反**跳跃的域控制器数量不超过3台**的策略。

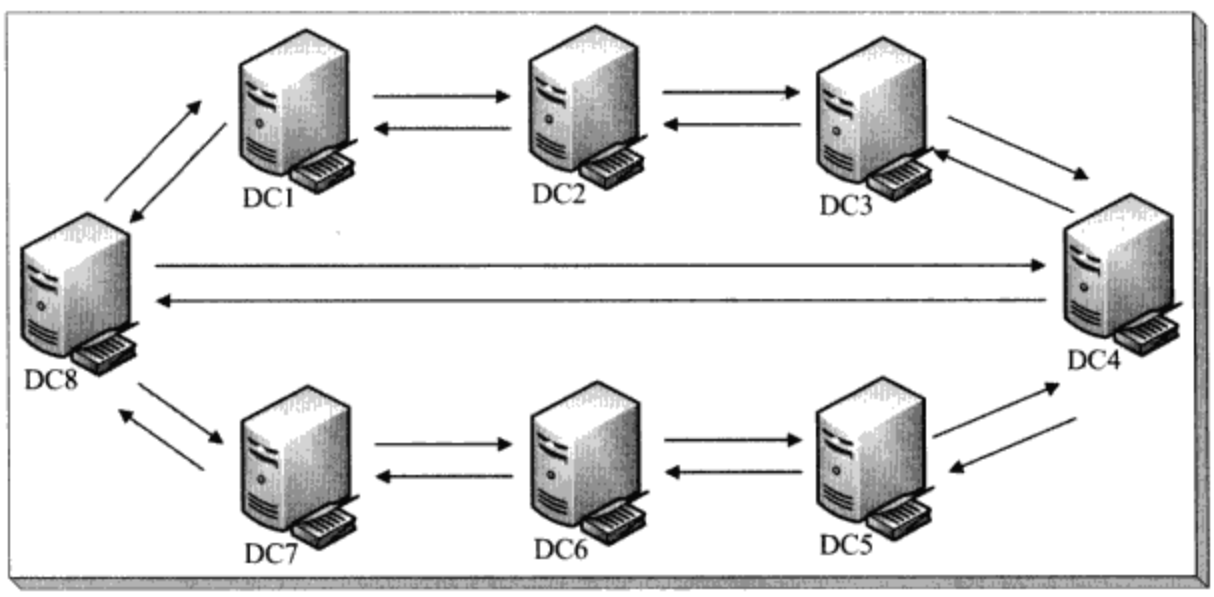


图 9-3

3. 紧急复制

对某些重要的更新数据来说，系统并不会等15s才通知**直接复制伙伴**，而是立即通知，这个操作被称为**紧急复制**。这些重要的更新数据包含用户账户被锁定、账户锁定策略有变动、域的密码策略有变动等。

9-1-2 不同站点之间的复制

由于不同站点之间的连接速度不够快，因此为了降低对连接带宽的影响，故站点之间的

Download at http://www.pin5i.com/

Active Directory数据在复制时会被压缩，而且数据的复制是采用**日程安排**（Schedule）的方式，也就是在安排时间内才会进行复制工作。原则上应该尽量安排在站点之间连接的非高峰时期才执行复制工作，同时复制频率也不要太高，以避免复制时占用两个站点之间的连接带宽，影响两个站点之间其他数据的传输效率。

不同站点的域控制器之间的**复制拓扑**，与同一个站点的域控制器之间的**复制拓扑**是不相同的。每一个站点内都各有一台被称为**站点间拓扑生成器**的域控制器，它负责创建**站点之间的复制拓扑**，并从其站点内挑选一台域控制器来扮演**bridgehead服务器**（桥接头服务器）的角色，例如图 9-4中SiteA的DC1与SiteB的DC4，两个站点之间在复制Active Directory数据时，是由这两台**bridgehead服务器**负责将该站点内的Active Directory变动数据复制给对方，这两台**bridgehead服务器**得到对方的数据后，会再将它们复制给同一个站点内的其他域控制器。

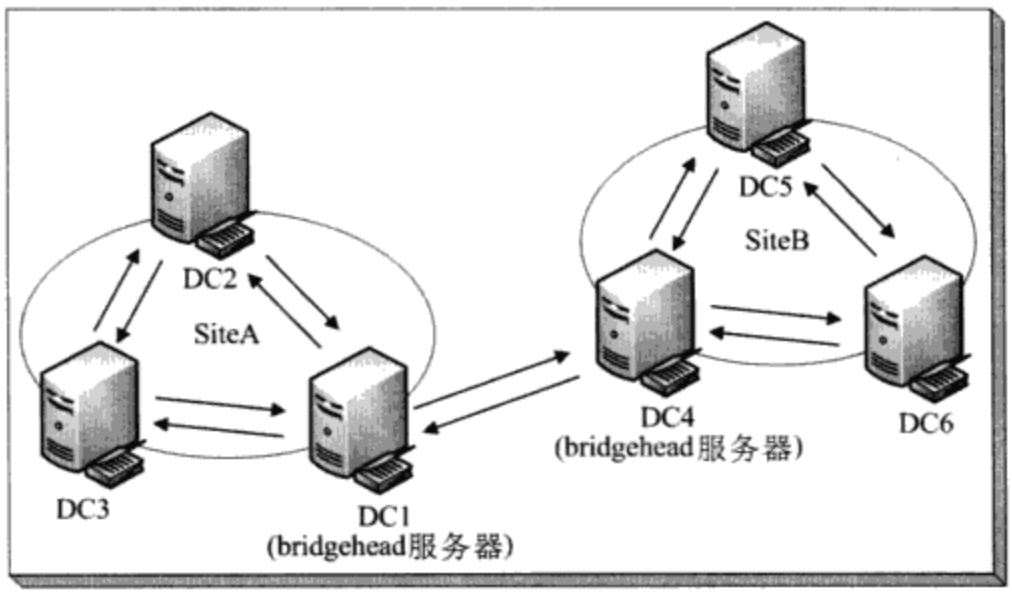


图9-4

两个站点之间Active Directory复制的其他细节，包含**站点链接**（Site Link）、开销、复制计划、复制频率等都会在后面章节另外说明。

9-1-3 目录分区与复制拓扑

Active Directory数据库被逻辑地分为以下多个目录分区（详见第1章）：**架构目录分区**、**设置目录分区**、**域目录分区**与**应用程序目录分区**。

KCC在创建**复制拓扑**时，并不是整个Active Directory数据库只采用一种**复制拓扑**，而是不同的**目录分区**各有其不同的**复制拓扑**，例如DC1在复制**域目录分区**时，可能DC2是它的**直接复制伙伴**，但是在复制**设置目录分区**时，DC3才是它的**直接复制伙伴**。

9-1-4 复制协议

域控制器之间在复制Active Directory数据时，其所使用的复制协议分为以下两种：

Download at http://www.pin5i.com/

- RPC over IP（Remote Procedure Call over Internet Protocol）：无论是同一个站点之间或不同站点之间，都可以利用RPC over IP来执行Active Directory数据库的复制操作。为了确保数据在发送时的安全性，RPC over IP会执行验证身份与数据加密的工作。

提示

在**Active Directory站点和服务**对话框中，同一个站点之间的复制协议RPC over IP会被改用IP来代表。

- SMTP（Simple Mail Transfer Protocol）：SMTP只能够用来执行不同站点之间的复制。若不同站点的域控制器之间无法直接通信，或之间的连接质量不稳定时，就可以通过SMTP的邮件方式来发送。不过这种方式有些限制，例如：只能够复制架构目录分区、设置目录分区与应用程序目录分区，不能够复制域目录分区；必须向**企业CA**（Enterprise CA）申请证书，因为在复制过程中，需要用证书来验证身份。

9-2 默认站点的管理

在您创建第1个域时，系统就会自动创建一个默认站点，以下介绍如何来管理这个默认的站点。

9-2-1 默认的站点

您可以利用【开始➲管理工具➲Active Directory站点和服务】的途径来管理站点，如图9-5所示。

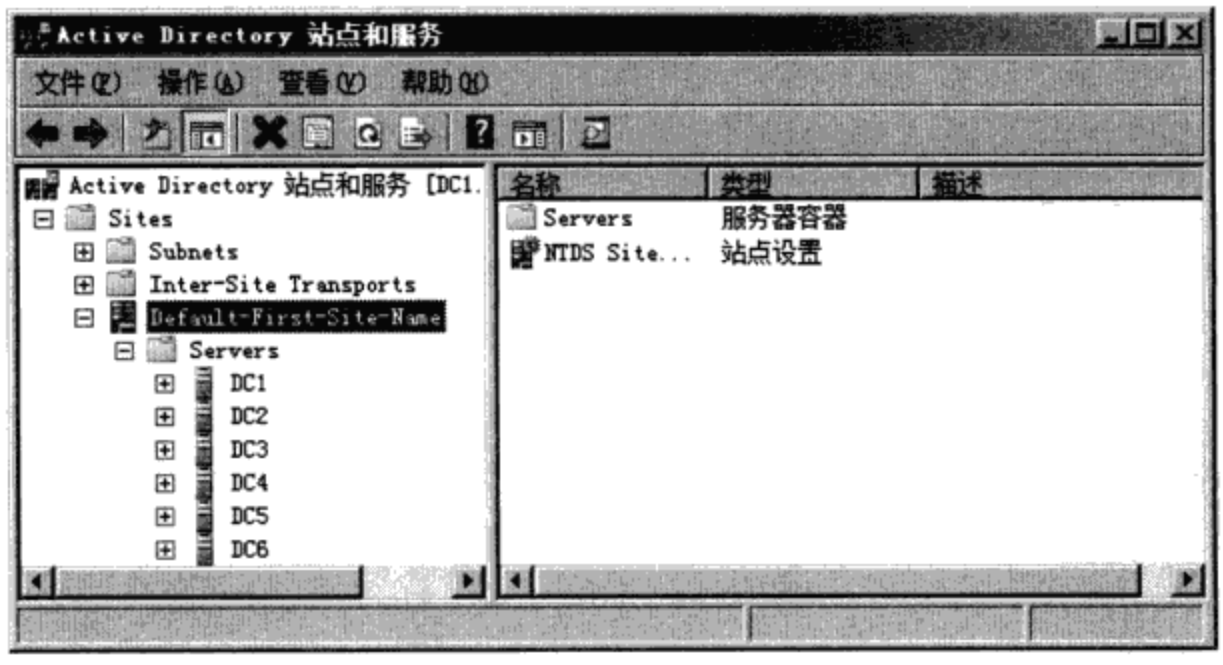


图9-5

Download at http://www.pin5i.com/

- Default-First-Site-Name: 这是默认的第1个站点，它是在您创建AD DS林时由系统自动创建的站点，您可以更改这个站点的名称。
- Servers: 其内记录着位于此Default-First-Site-Name 站点内的域控制器，还有这些域控制器的设置值。
- Inter-Site Transports: 记录着站点之间的IP与SMTP这两个复制协议的设置值。
- Subnets: 您可以通过此处在AD DS内创建多个IP子网，并将子网划入到所属的站点内。

假设您在AD DS内已经创建了多个IP子网，此时您在安装域控制器时，若此域控制器是位于其中某个子网内（从IP地址的网络ID来判断），则此域控制器的计算机账户就会被放到此子网所隶属的站点内。

然而在您创建AD DS林时，系统默认并没有在AD DS内创建任何的子网，因此您所创建的域控制就不属于任何一个子网，此时这台域控制器的计算机账户会被放到Default-First-Site-Name站点内，例如图 9-5中的DC1，DC2，…，DC6等域控制器都是在此站点内。

9-2-2 Servers文件夹与复制设置

图 9-5中的Servers文内记录着位于Default-First-Site-Name站点内的域控制器，而在选择图中的任意一台域控制器后（例如DC1），将出现如图 9-6所示的对话框。



图9-6

图中的NTDS Settings内包含5个由KCC所自动创建的**连接对象**（Connection Object），其名称都是**自动生成**的，这5个**连接对象**分别来自DC2～DC6，表示DC1会直接接收由这5台域控制器所复制过来的Active Directory数据，也就是说这5台域控制器都是DC1的**直接复制伙伴**。同

Download at http://www.pin5i.com/

理在选择DC2~DC6中任何一台域控制器时，也可以看到它们与**直接复制伙伴**之间的**连接对象**。

这些在同一个站点内的域控制器相互之间的**连接对象**，都会由KCC负责自动创建与维护，而且是双向的。您也可视需要来手动创建**连接对象**，例如假设图 9-7中DC3 ~ DC4之间原本并没有**连接对象**存在，也就是它们并不是**直接复制伙伴**，但是您可以手动在它们之间创建单向或双向的**连接对象**，以便让它们之间可以直接复制Active Directory数据库，例如图中手动创建的**连接对象**是单向的，也就是只有DC3可以直接从DC4来复制Active Directory数据库。

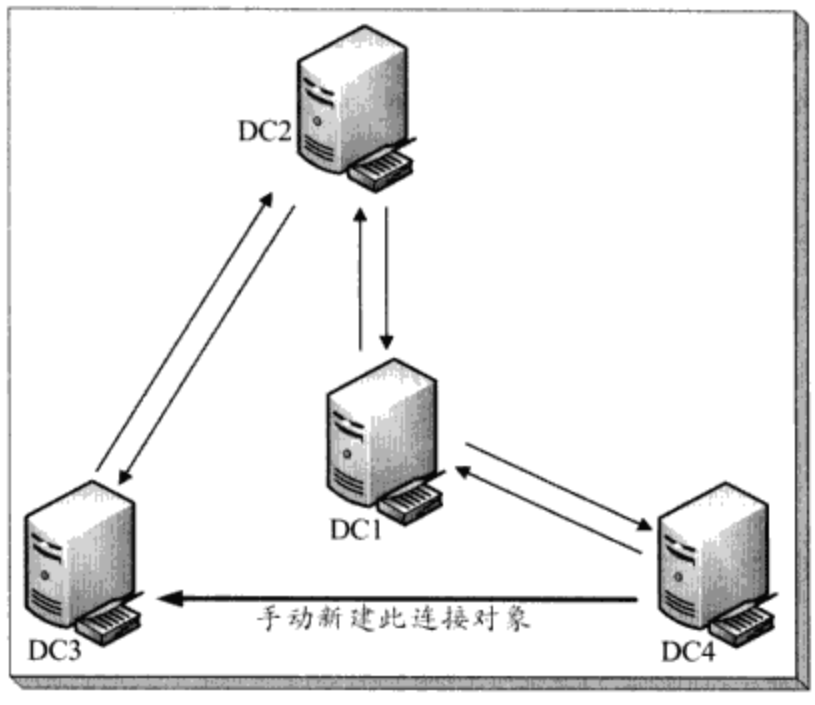


图9-7

创建此单向连接对象的途径为：【如图 9-8所示对着DC3之下的**NTDS Settings**单击右键➲新建Active Directory域服务连接➲选择DC4➲…】。

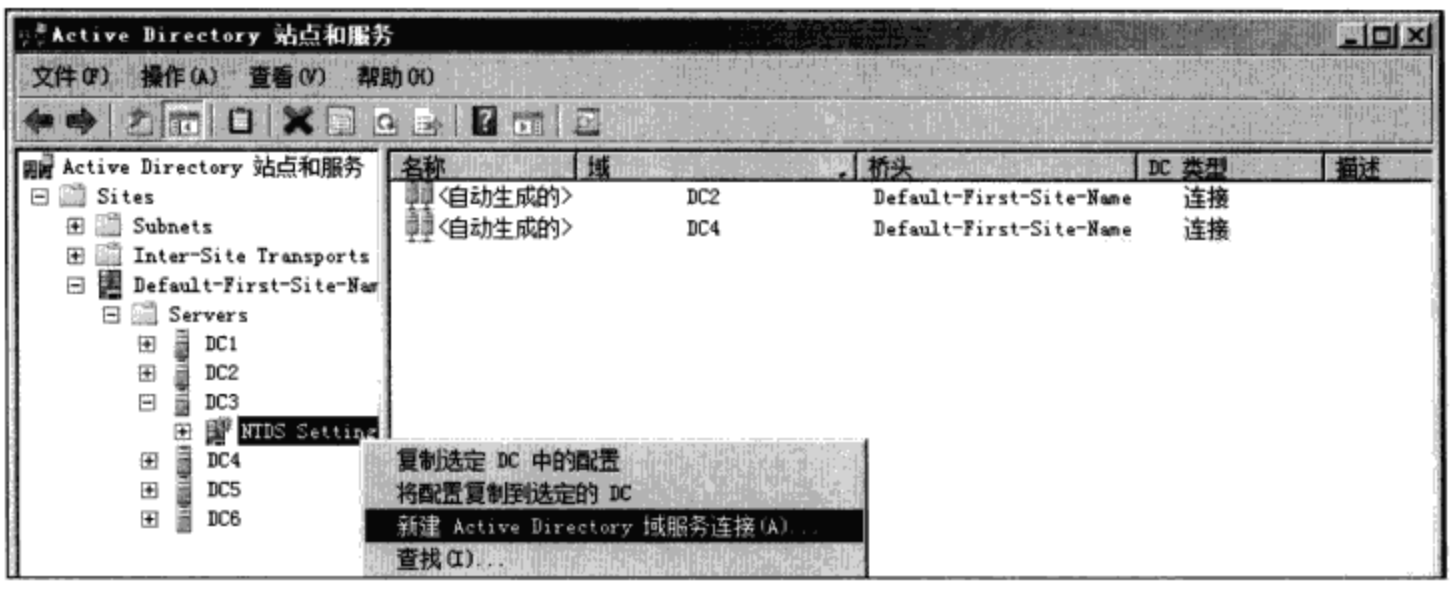


图9-8

在双击图 9-6中的任何一个**连接对象**后(例如**源服务器**为DC2的连接对象)，将出现如图 9-9所示的对话框。您可以单击图中**服务器**右方的更改按钮，来改变复制的源服务器。

Download at http://www.pin5i.com/

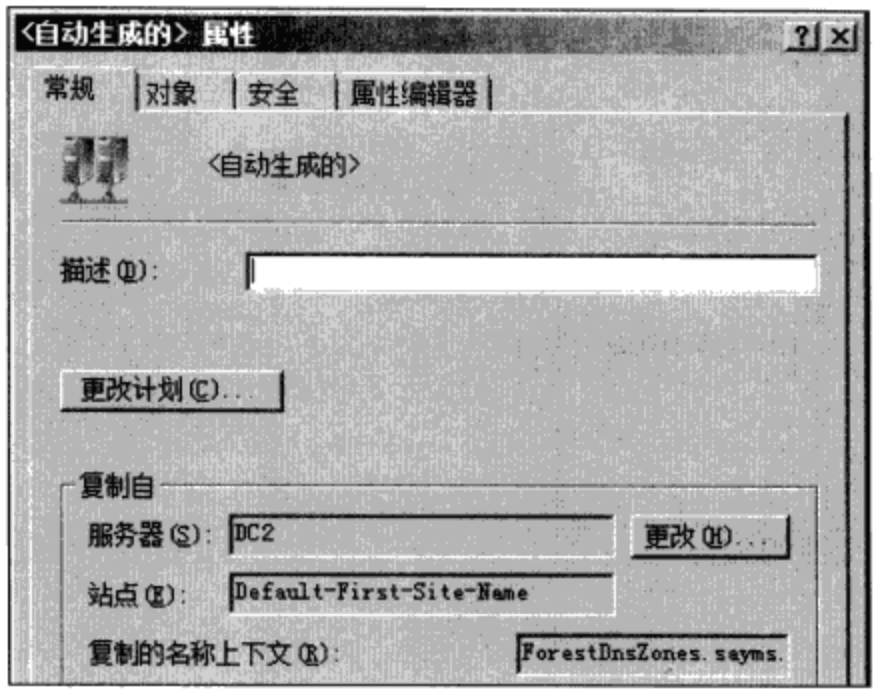


图 9-9

若域控制器内的Active Directory数据有变动时（例如新建用户账户），则其默认是15s后会通知同一个站内的**直接复制伙伴**，以便将数据复制给它们。即使没有变动数据，默认也会每隔一小时执行一次复制工作，以确保没有遗失任何应该复制的数据，您可以通过图 9-9中的更改计划按钮来查看与改变此间隔时间，如图 9-10所示。

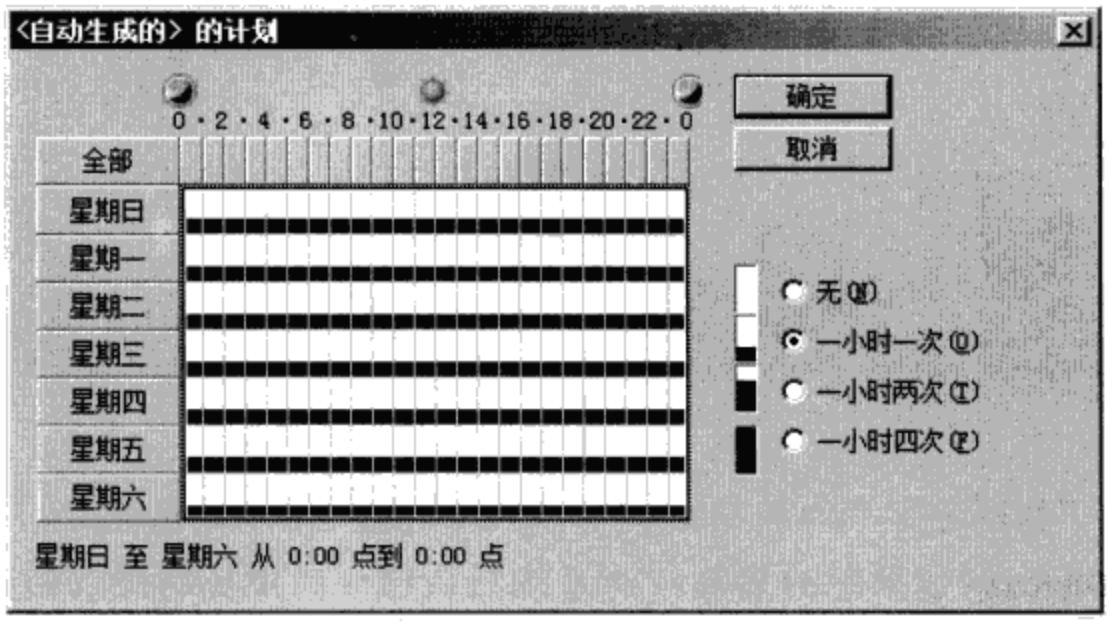


图 9-10

如果您想要立刻复制的话，请自行以手动的方式来完成，方法是：【先选择图 9-11左方的目的服务器（例如DC1）➲单击**NTDS Settings**➲对着右边的复制源服务器单击右键➲立即复制副本】，即可从DC6复制到DC1。

Download at http://www.pin5i.com/

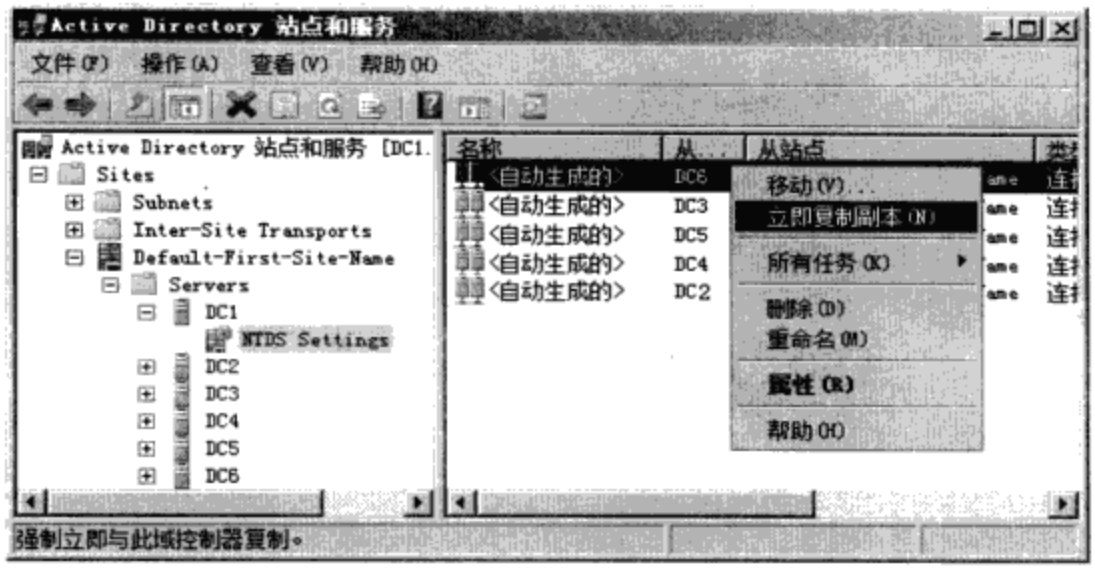


图9-11

9-3 利用站点来管理Active Directory复制

以下将先利用图 9-12来说明如何创建多个站点与IP子网，然后再说明站点之间的Active Directory复制设置。

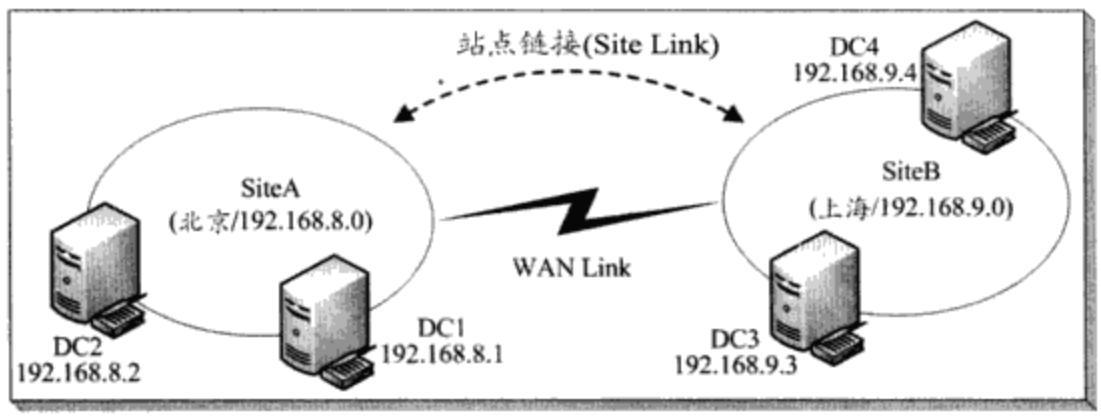


图9-12

站点之间除了物理连接（WAN Link）外，还必须创建逻辑的**站点链接**（Site Link）才可以进行Active Directory数据库的复制，而系统默认已经为IP复制协议创建一个名称为DEFAULTIPSITELINK的站点链接，如图 9-13所示。

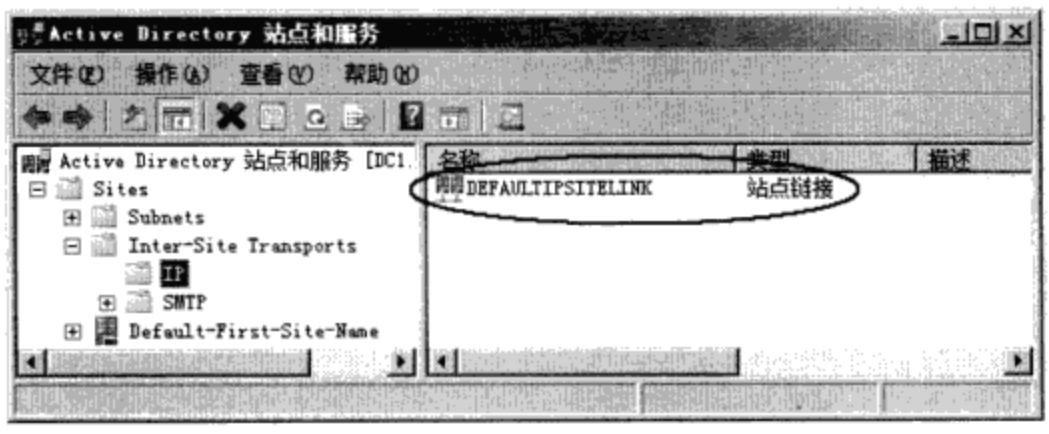


图9-13

Download at http://www.pin5i.com/

我们在创建图 9-12中的SiteA与SiteB时，必须通过**站点链接**将这两个站点逻辑地连接在一起，它们之间才可以进行Active Directory数据库的复制。

9-3-1 创建站点与子网

以下将先创建新站点，然后创建隶属于此站点的IP子网。

1. 创建新站点

下面将说明如何创建图 9-12中的SiteA与SiteB。

STEP 1 选择【开始➲管理工具➲Active Directory站点和服务➲如图 9-14所示对着**Sites**单击右键➲新站点】。



图 9-14

STEP 2 在图 9-15中设置站点名称（例如SiteA），并将此站点归纳到适当的**站点链接**后单击 确定 按钮。图中因为目前只有一个默认的**站点链接**DEFAULTIPSITELINK，故只能够暂时将其归纳到此默认的**站点链接**。只有隶属于同一个**站点链接**的站点之间才可以进行Active Directory数据库的复制。

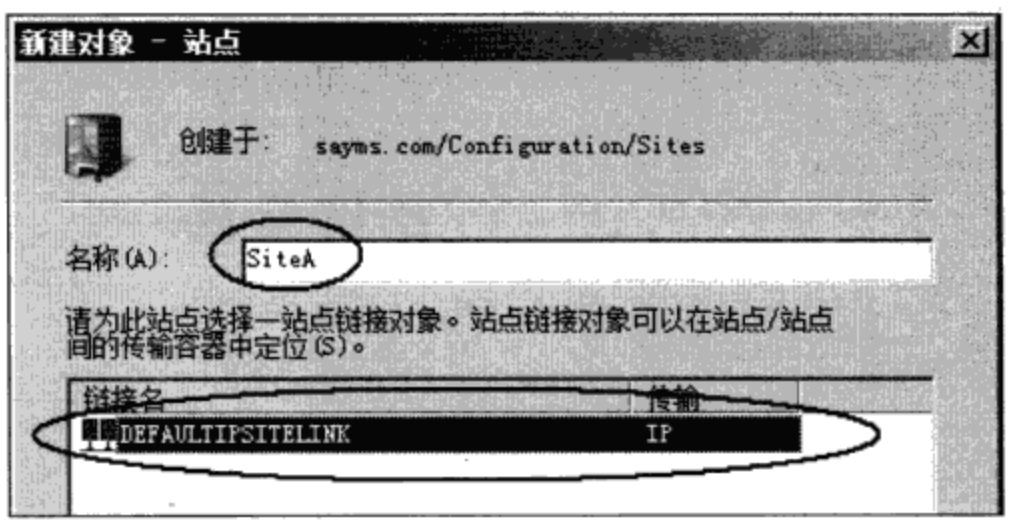


图 9-15

Download at http://www.pin5i.com/

STEP 3 在图 9-16中直接单击确定按钮。

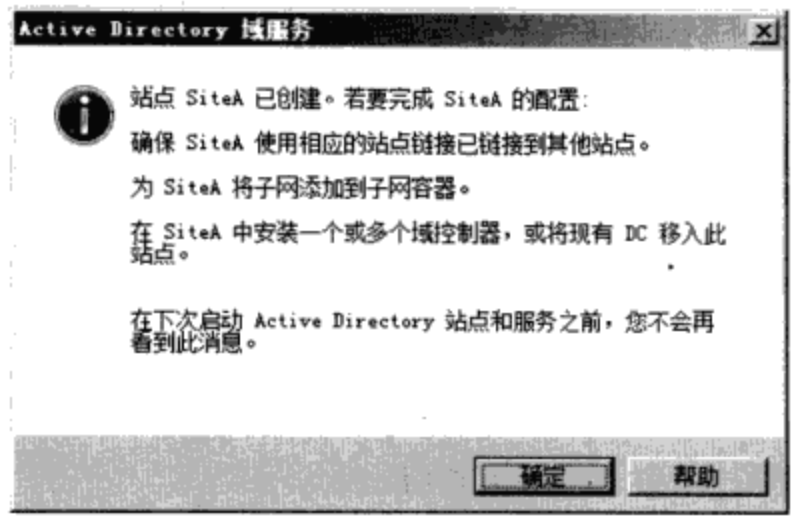


图 9-16

STEP 4 请重复**STEP 1** ~ **STEP 3**来创建SiteB，图 9-17为完成后的界面。

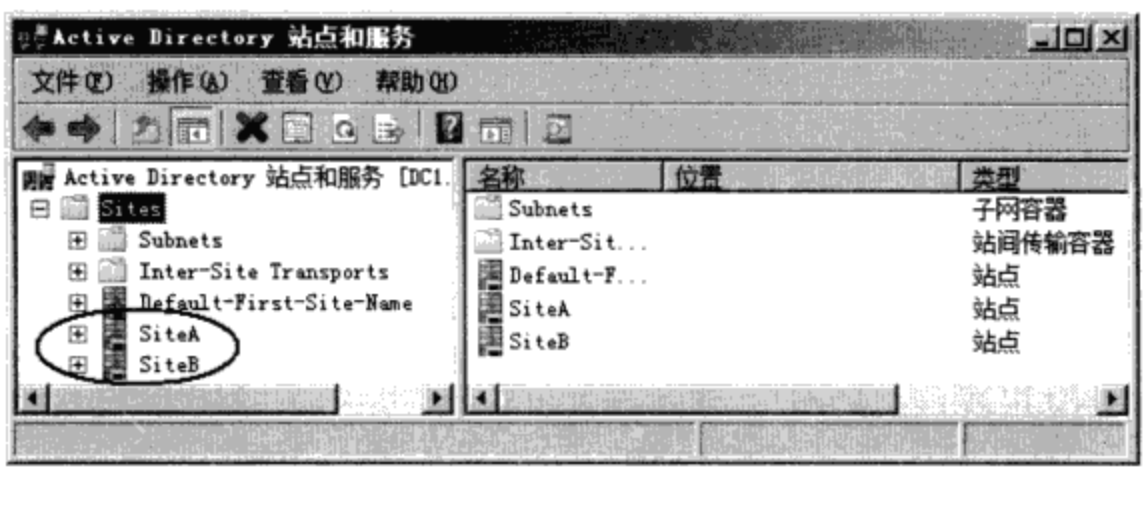


图 9-17

2. 创建 IP 子网

以下将说明如何创建图 9-12中的IP子网192.168.8.0与192.168.9.0，并将它们分别划入到SiteA与SiteB内。

STEP 1 如图 9-18所示，通过【对着**Subnets**单击右键➲新建子网】的方式进行操作。



图 9-18

Download at http://www.pin5i.com/

STEP 2 在图 9-19中的**前缀**文本框中输入192.168.8.0/24，其中的192.168.8.0为网络ID，而24表示子网掩码为255.255.255.0（二进制中为1的位共有24个），并将此子网划入站点SiteA内。

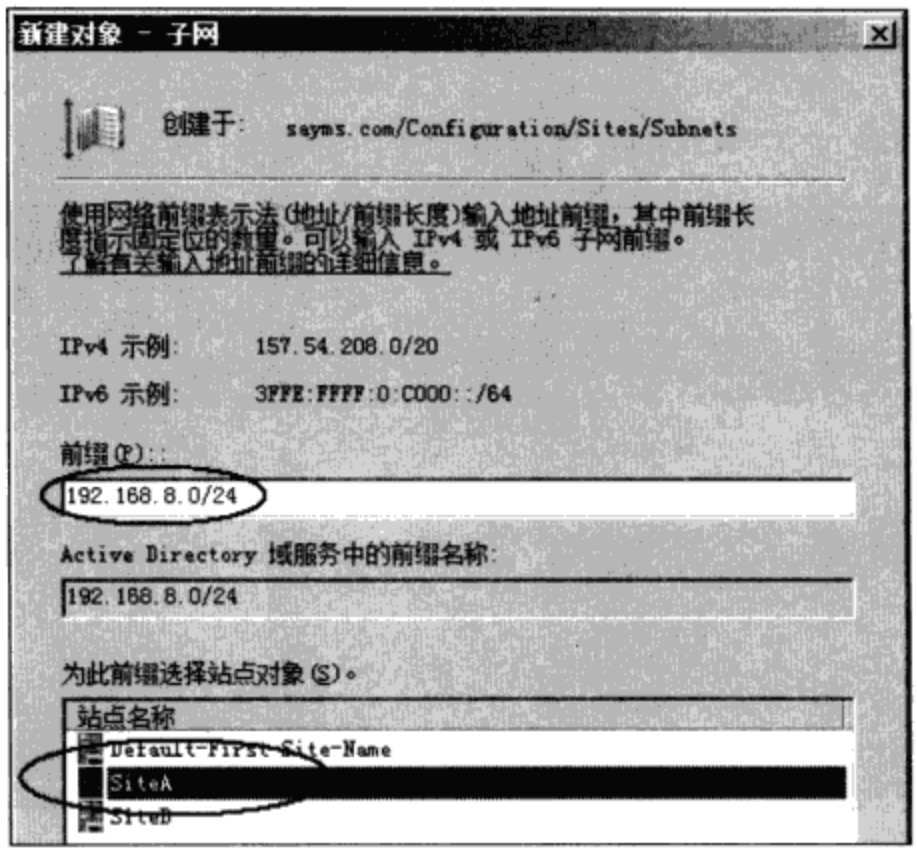


图 9-19

STEP 3 重复前两个步骤来创建IP子网192.168.9.0，并将其划入站点SiteB。图 9-20为完成后的界面。

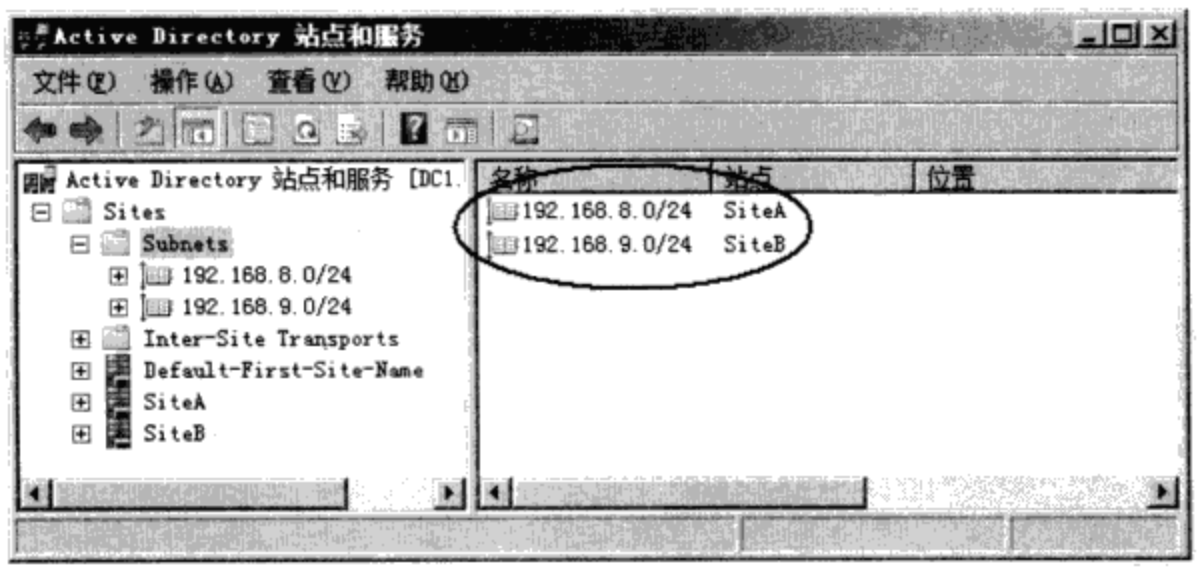


图 9-20

9-3-2 创建站点链接

以下将说明如何创建图 9-12中的**站点链接**，并将此**站点链接**命名为SiteLinkAB。我们利用IP复制协议来进行说明。

Download at http://www.pin5i.com/

注意

由于我们在前面创建SiteA与SiteB时，都已经将SiteA与SiteB归纳到DEFAULTIPSITELINK这个**站点链接**，也就是说这两个站点已经通过DEFAULTIPSITELINK逻辑的连接在一起了。我们通过以下练习来将其改为通过SiteLinkAB来连接。

STEP 1 请按如图 9-21所示进行操作【对着**IP**单击右键➲新站点链接】。

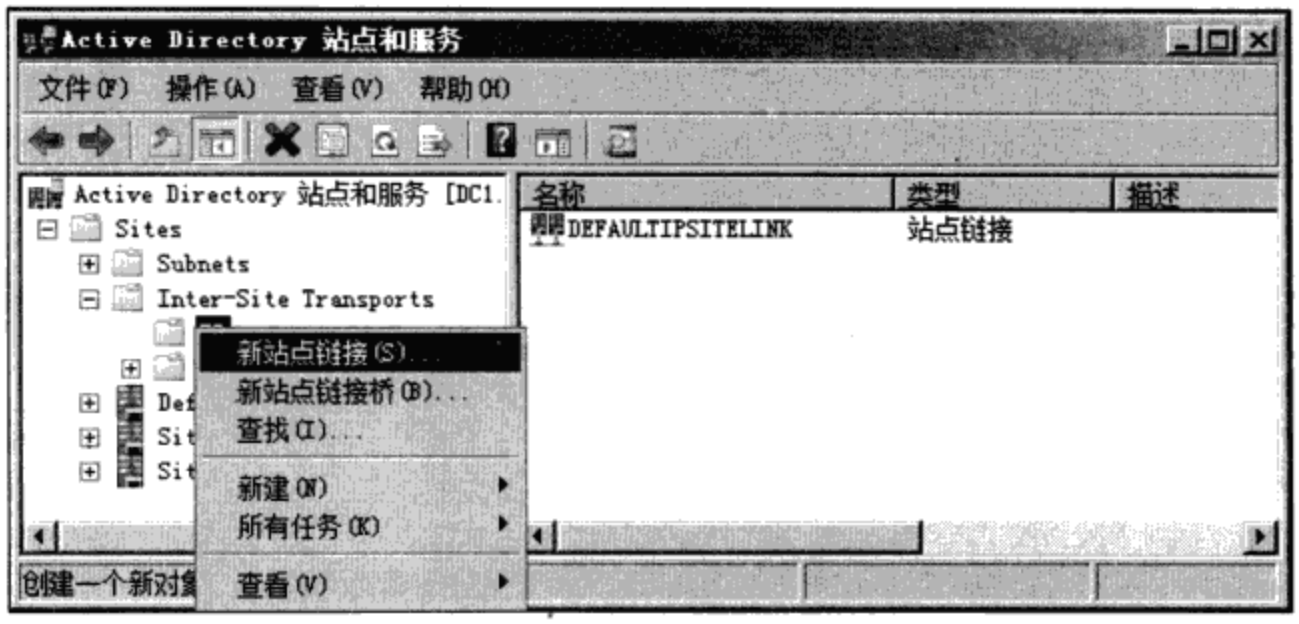


图 9-21

STEP 2 在图 9-22中，通过【设置站点链接名称（SiteLinkAB）➲选择SiteA与SiteB后单击添加按钮➲单击确定按钮】的方式进行操作。之后SiteA与SiteB便可根据**站点链接**SiteLinkAB内的设置来复制Active Directory数据库。

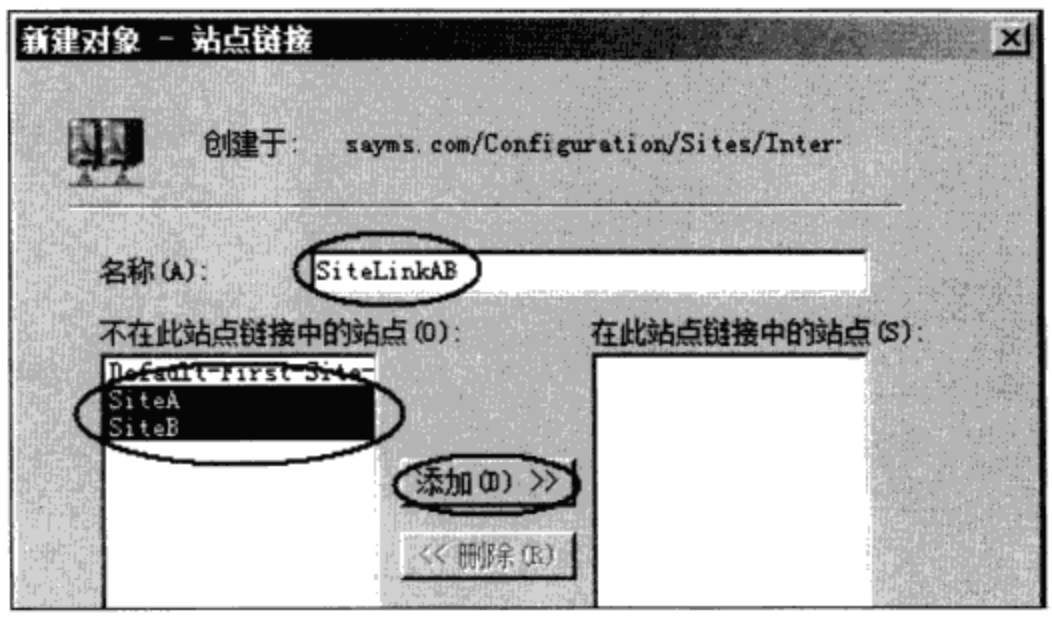


图 9-22

STEP 3 图 9-23为完成后的界面。

Download at http://www.pin5i.com/

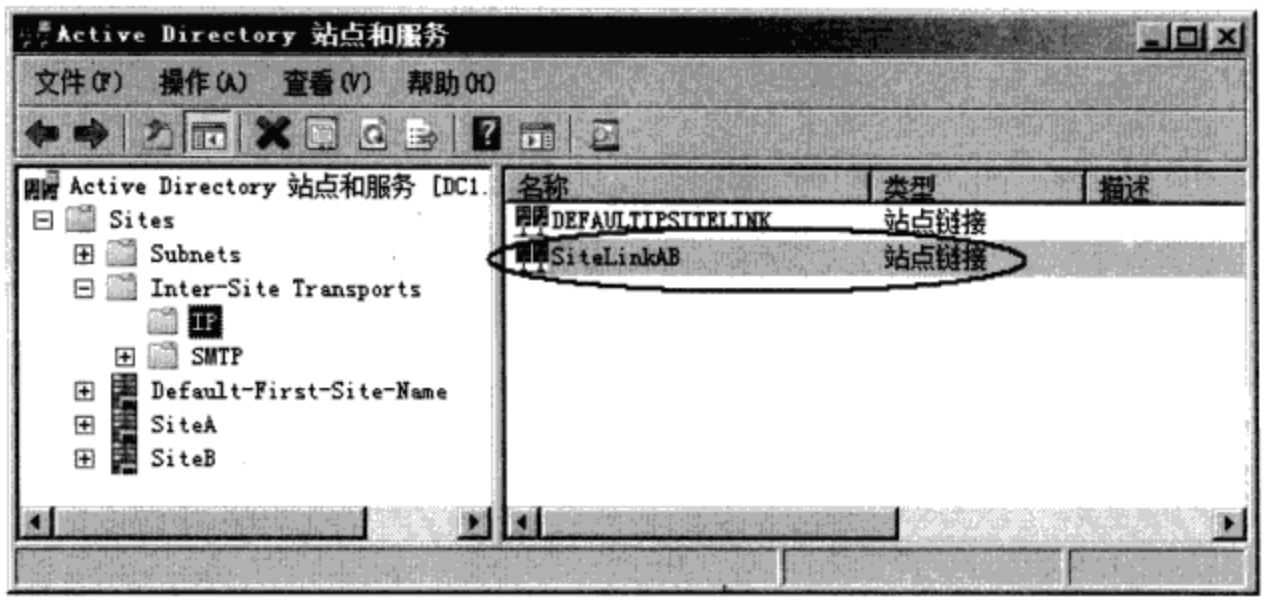


图 9-23

9-3-3 将域控制器转移到所属的站点

目前所有的域控制器都是被放置到Default-First-Site-Name站点内，而在完成新站点的创建后，我们应该将域控制器转移到正确的站点内。以下假设域控制器DC1与DC2的IP地址的网络ID都是192.168.8.0（如图 9-24所示），故我们需要将DC1与DC2转移到站点SiteA；同时假设DC3与DC4的IP地址的网络ID都是192.168.9.0，故我们需要将DC3与DC4转移到站点SiteB。

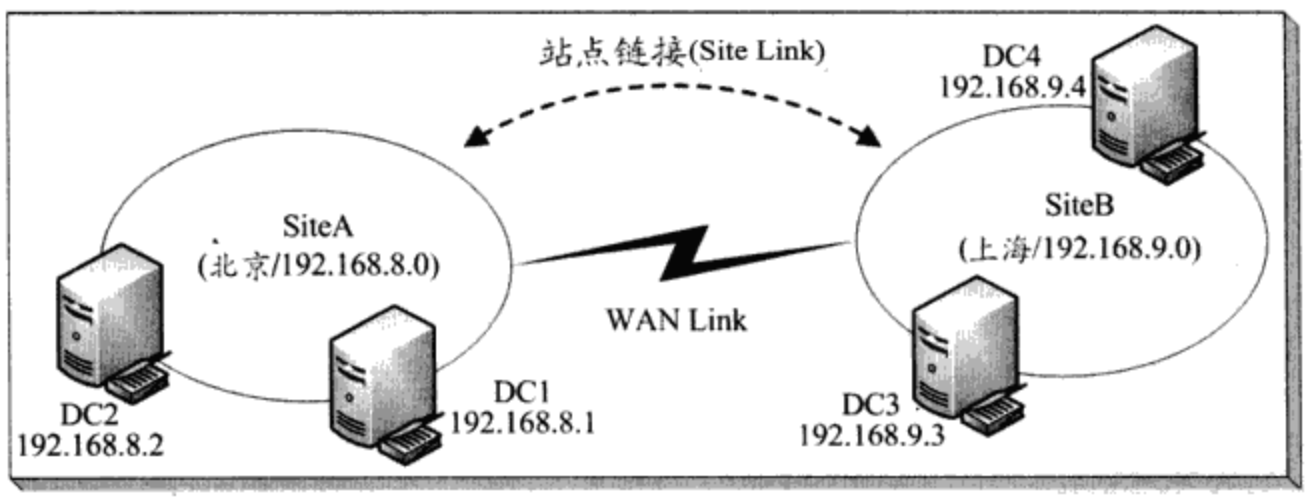


图 9-24

注意

以后若您在图 9-24中的**北京**网络内安装新域控制器的话，则该域控制器的计算机账户会自动被放置到SiteA内，同理在**上海**网络内所安装的新域控制器，其计算机账户会自动被放到SiteB内。

STEP 1 如图 9-25所示，通过【展开Default-First-Site-Name站点➲单击Servers➲对着要被移动的服务器（例如DC1）单击右键➲移动】的方式进行操作。

Download at http://www.pin5i.com/

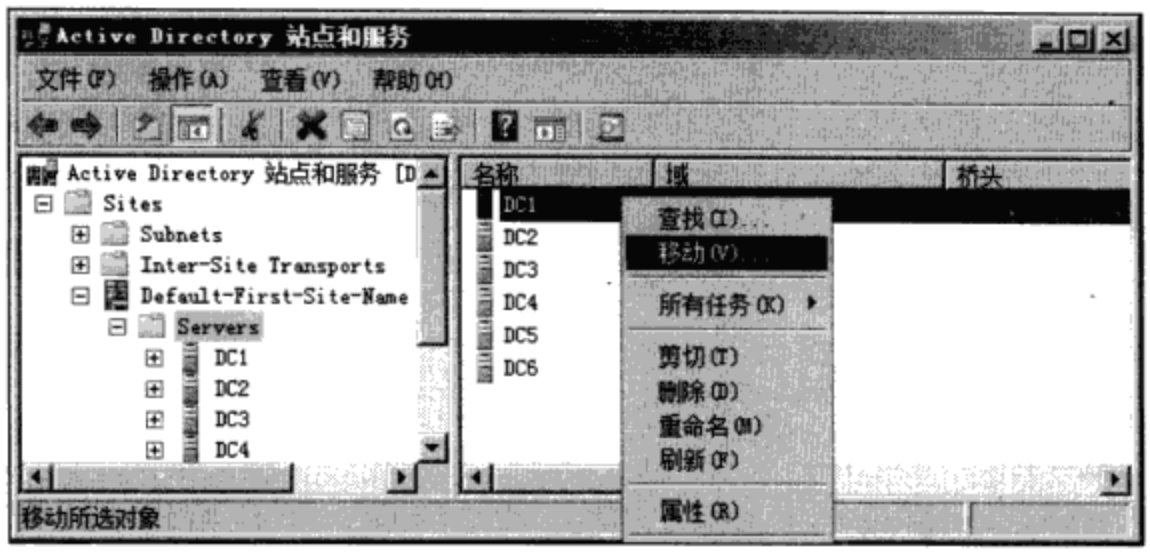


图 9-25

STEP 2 在图 9-26中选择目的地站点SiteA后单击确定按钮。

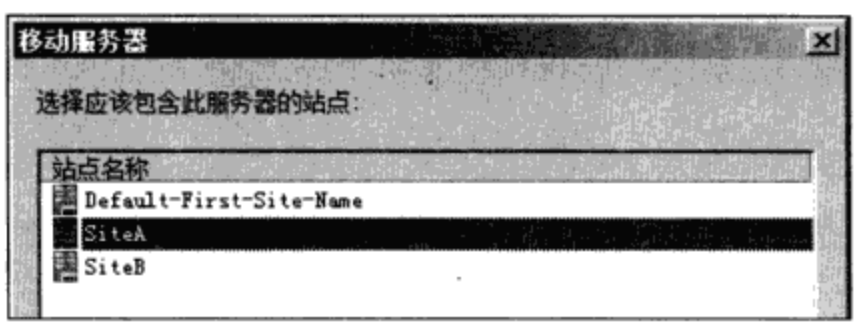


图 9-26

STEP 3 重复以上步骤将DC2转移到SiteA、将DC3与DC4转移到SiteB。图 9-27为完成后的界面。

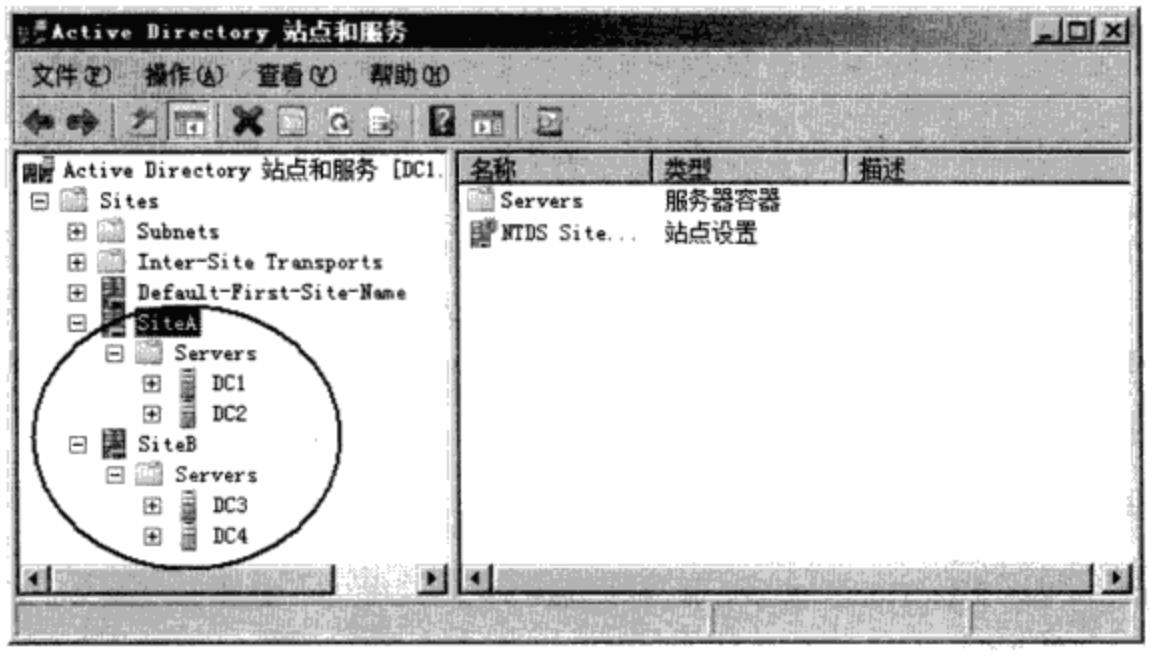


图 9-27

9-3-4 指定首选的bridgehead服务器

前面说过每一个站点内都各有一台被称为**站点间拓扑生成器**的域控制器，它负责创建**站**

Download at http://www.pin5i.com/

点之间的复制拓扑，并从其站点内挑选一台域控制器来扮演**bridgehead服务器**的角色，例如图9-28中SiteA的DC1与SiteB的DC4，两个站点之间在复制Active Directory数据时，是由这两台**bridgehead服务器**负责将该站点内的Active Directory变动数据复制给对方，这两台**bridgehead服务器**得到对方的数据后，会再将它们复制给同一个站点的其他域控制器。

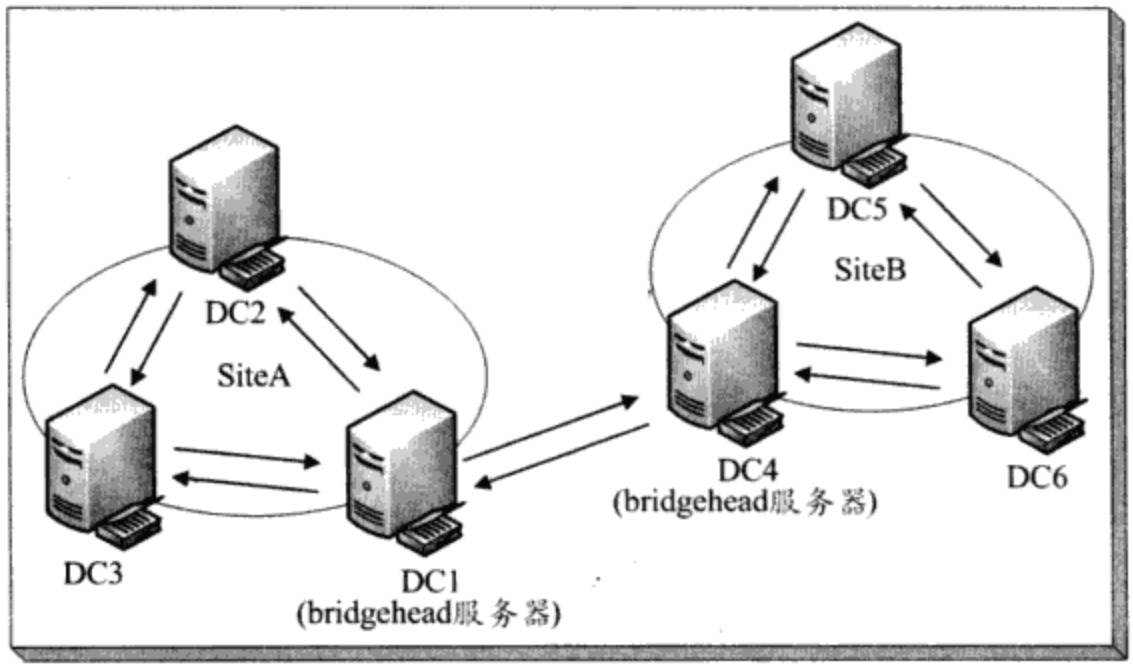


图 9-28

您也可以自行选择扮演**bridgehead服务器**的域控制器，它们被称为**首选的bridgehead服务器**（Preferred Bridgehead Server）。例如若您要将SiteA内的域控制器DC1指定为**首选的bridgehead服务器**的话，请如图 9-29所示，通过【展开站点SiteA➲单击Servers➲选择域控制器DC1➲单击上方的**属性**图标➲选择复制协议（例如IP）➲单击添加按钮】的方式进行操作。

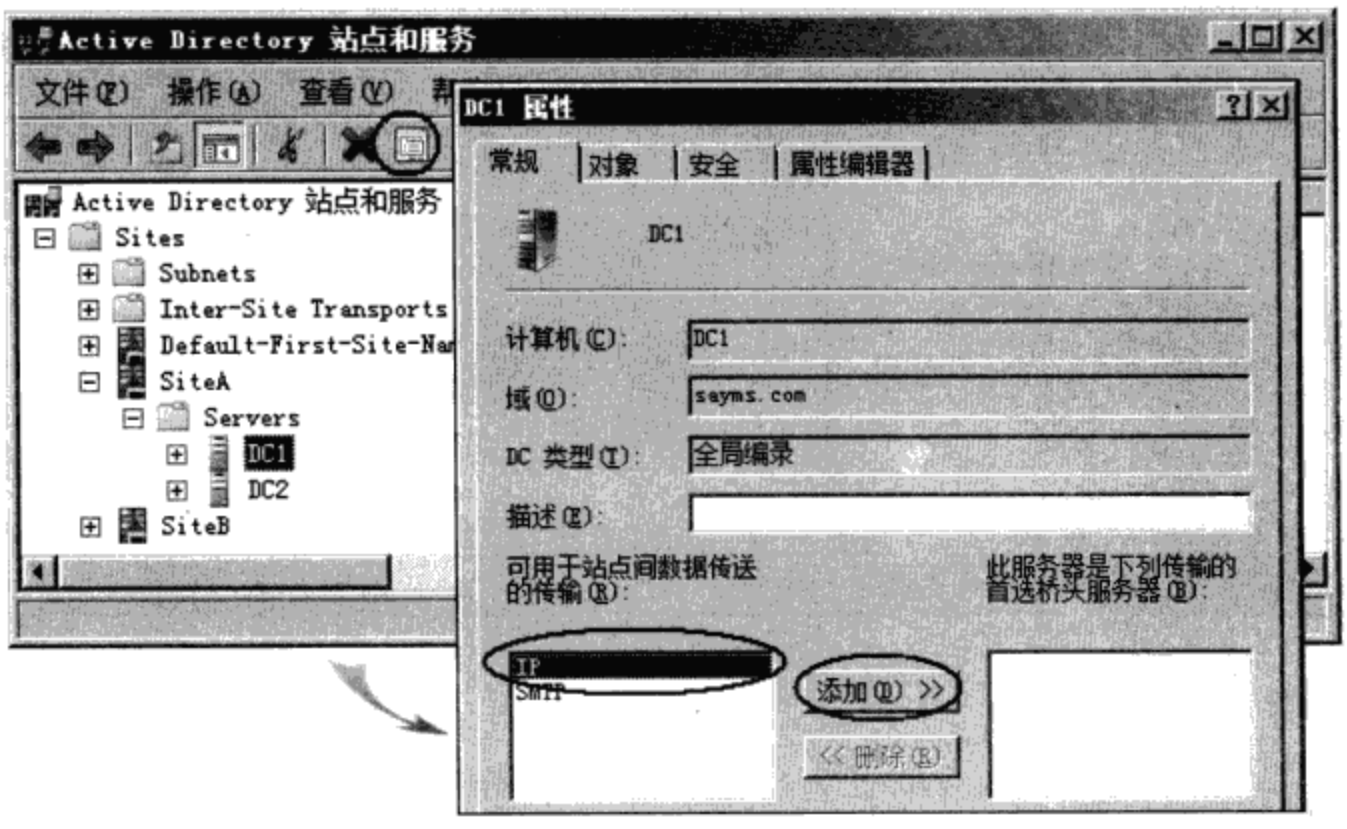


图 9-29

Download at http://www.pin5i.com/

您可以重复以上的步骤来将多台的域控制器设为**首选的bridgehead服务器**，但是AD DS一次只会从其中挑选一个来复制数据，如果这一台故障了，它会再挑选其他的**首选的bridgehead服务器**。

若要查看**首选的bridgehead服务器**列表的话，可选择【展开Inter-Site Transports➲对着IP右击➲属性➲单击**属性编辑器**标签➲单击筛选器按钮➲选择显示只读属性处的反向链接➲双击属性列表中的bridgeheadServerListBL】。

> **注意**
>
> 请不要自行指定首选的**bridgehead服务器**，因为它会让KCC停止自动挑选**bridgehead服务器**，因此若您所选择的**首选的bridgehead服务器**都故障时，KCC并不会再自动挑选**bridgehead服务器**，如此将没有bridgehead服务器可供使用。若您要将扮演**首选的bridgehead服务器**的域控制器转移到其他站点的话，请先取消其**首选的bridgehead服务器**的角色后再转移。

9-3-5 站点链接与Active Directory数据库的复制设置

两个站点之间是通过**站点链接**的设置来决定如何复制Active Directory数据库：【如图9-30所示对着站点链接（例如SiteLinkAB）单击右键➲属性➲通过如图 9-31所示的界面进行设置】。



图 9-30

Download at http://www.pin5i.com/



图9-31

- **不在/在此站点链接中的站点**：您可以在界面中将其他的站点加入到此**站点链接**SiteLinkAB内，也可以将站点从这个**站点链接**中删除。
- **开销**：如果两个站点之间有多个实际的WAN Link，则它们之间就可以有多个逻辑的站点链接，而每一个站点链接可以有着不同的开销（默认值为100）。这里的**开销**是一个用来与其他**站点链接**相比较的相对值。每一个**站点链接**的开销计算，需要考虑到实际WAN Link的连接带宽、稳定性、延迟时间与费用，例如若开销考虑是以WAN Link的连接带宽为依据的话，则您应该将带宽较宽的**站点链接**的开销值设得较低，假设您将带宽较低的**站点链接**的开销设置为默认的100，则带宽较宽的**站点链接**的开销值应该要比100小。KCC在创建**复制拓扑**时，会选择**站点链接**开销较低的域控制器来当作**直接复制伙伴**。另外用户在登录时，若其计算机所在的站点内没有域控制器可以提供服务的话（例如域控制器因故脱机），则用户的计算机会到其他站点去查找域控制器，此时它会通过**站点链接**开销最低的连接去查找域控制器，以便让用户能够较快速地登录。
- **复制频率**、**更改计划**：**复制频率**是用来设置隶属于这个**站点链接**的站点之间，每隔多久复制一次Active Directory数据库，默认是180分钟。但并不是时间到了就一定会执行复制的工作，因为还需视**站点链接**的设置是否允许在此时间复制而定，可单击更改计划按钮，然后用图 9-32来更改计划。系统默认是一个星期7天、1天24小时的任何时段都允许进行复制，可以更改此计划，例如改为在高峰时期不允许复制，不过它会增加复制的延迟时间。

Download at http://www.pin5i.com/

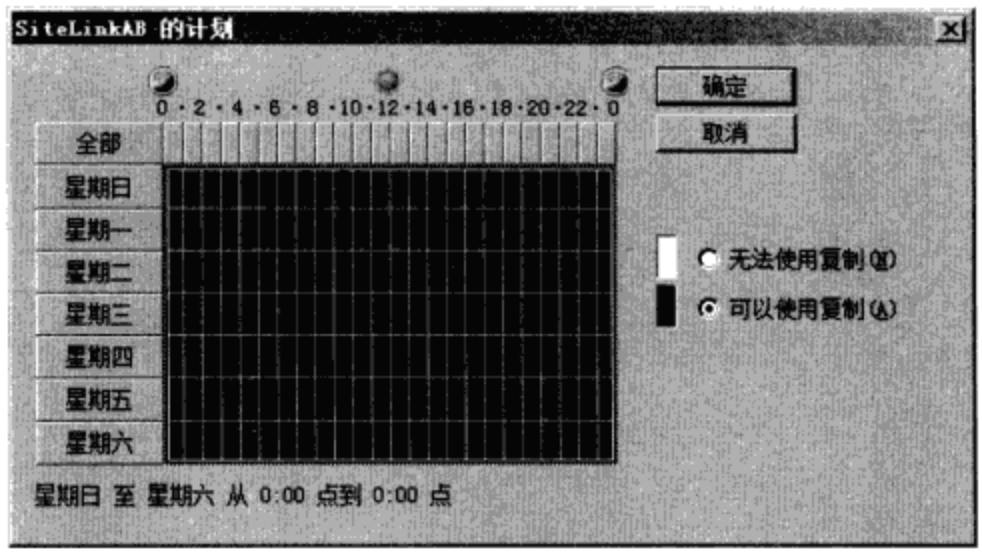


图 9-32

9-3-6 站点链接桥

站点链接桥（Site Link Bridge）是由两个或多个**站点链接**所组成，它让这些**站点链接**具备**转移性**（Transitive），如图 9-33所示的SiteA与SiteB之间已经创建了一个**站点链接**SiteLinkAB，而SiteB与SiteC之间也创建了一个**站点链接**SiteLinkBC，则**站点链接桥**SiteLinkBridgeABC让SiteA与SiteC之间具备着隐性的**站点链接**，也就是说KCC在创建**复制拓扑**时，可以将SiteA的域控制器DC1与SiteC的域控制器DC3设置为**直接复制伙伴**，让DC1与DC3之间可以通过两个WAN Link的物理线路来直接复制Active Directory数据，不需要由SiteB的域控制器DC2来转发。

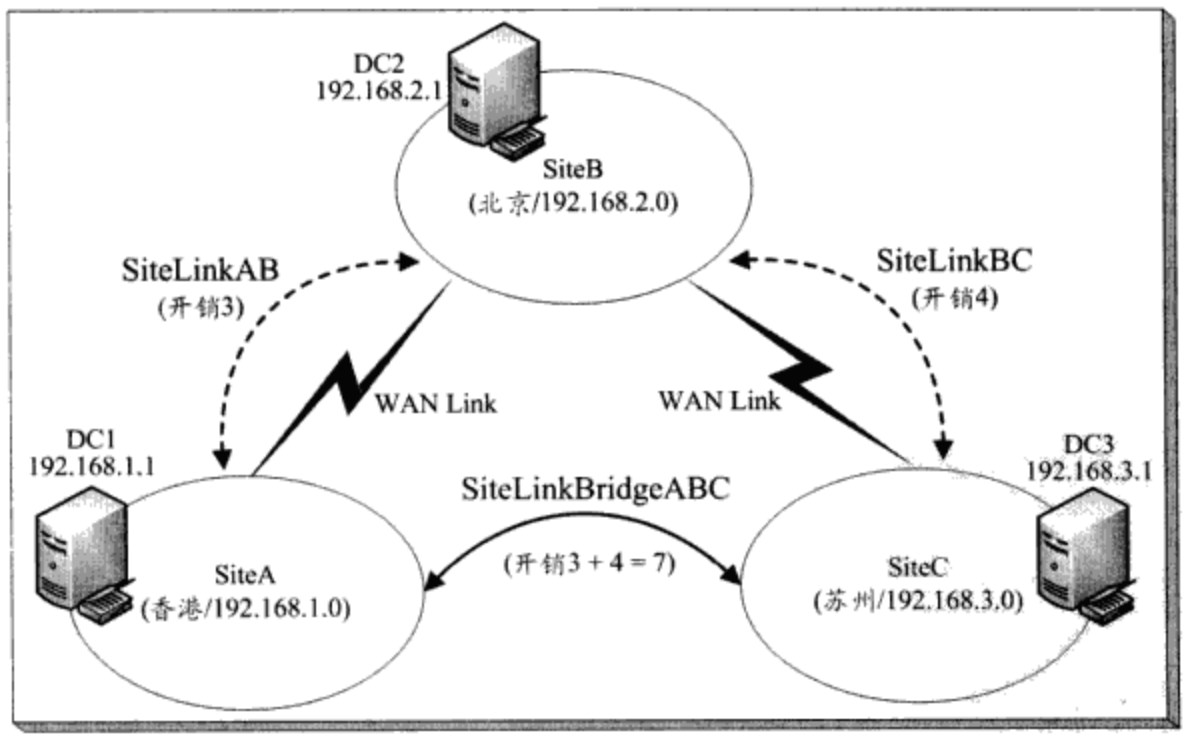


图 9-33

图中SiteLinkAB的开销为3、SiteLinkBC的开销为4，因此SiteLinkBridgeABC的开销为3 + 4 = 7，由于这个开销高于SiteLinkAB的开销3与SiteLinkBC的开销4，因此KCC在创建**复制拓扑**时，默认并不会在DC1与DC3之间创建**连接对象**，也就是不会将DC1与DC3设为**直接复制伙**

Download at http://www.pin5i.com/

伴，除非是DC2无法使用（例如计算机故障、脱机）。

系统默认会自动桥接所有的**站点链接**，而您可以如图 9-34所示，通过【展开**Inter-Site Transports**➲单击**IP**文件夹➲单击上方的**属性**图标➲选择或取消**为所有站点链接搭桥**复选框】的途径来更改其设置值。

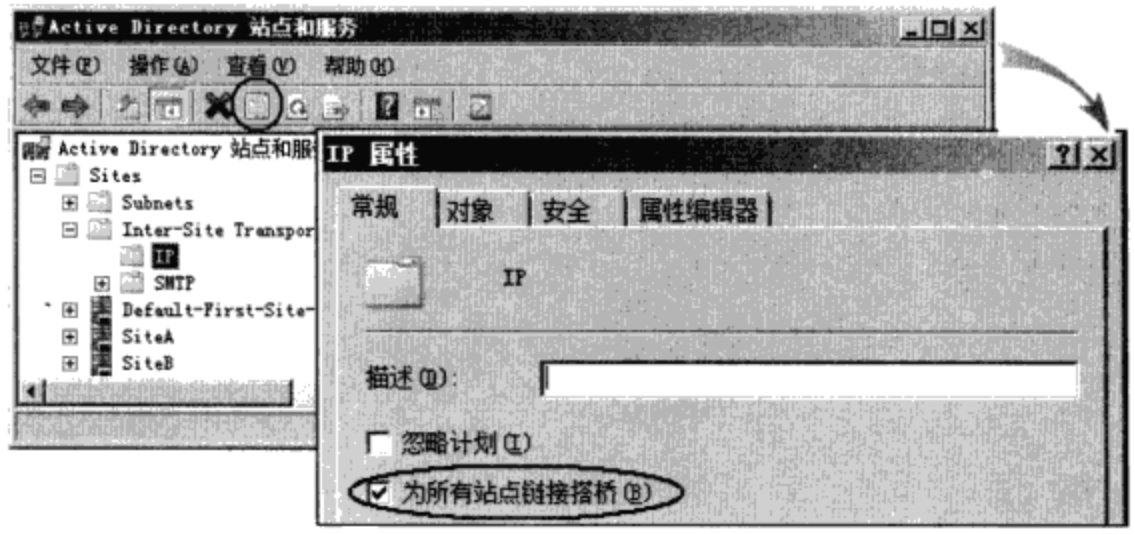


图 9-34

由于系统默认已经自动桥接所有的**站点链接**，因此您不需要另外自行创建**站点链接桥**，除非您想要控制Active Directory数据复制的方向或两个站点之间受到限制无法直接通信，例如在图 9-33的SiteB架设防火墙，并通过防火墙限制SiteA的计算机不可与SiteC的计算机通信，则图中的SiteLinkBridgeABC就没有意义了，因为SiteA将无法直接与SiteC进行Active Directory数据库复制，此时如果SiteA还可以通过另外一个站点SiteD来与SiteC通信的话，我们就没有必要让KCC浪费时间创建SiteLinkBridgeABC，或浪费时间尝试通过SiteLinkBridgeABC来复制Active Directory数据库，也就是说您可以先取消选择图 9-34中的**为所有站点链接搭桥**复选框，然后如图 9-35所示自行创建SiteLinkBridgeADC，以便让SiteA的计算机与SiteC的计算机直接选择通过SiteLinkBridgeADC来通信。

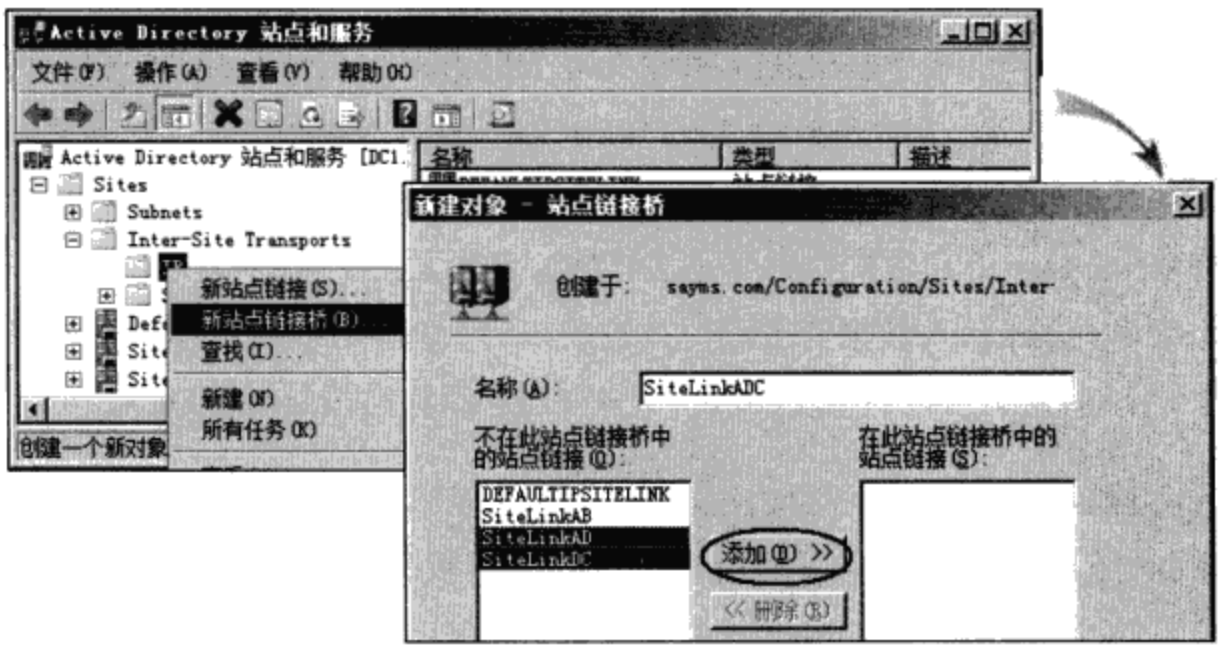


图 9-35

Download at http://www.pin5i.com/

9-3-7 站点链接桥的两个示例讨论

本节我们通过两个实例来探讨**站点链接桥**的应用。

1. 站点链接桥示例一

图 9-36中SiteA与SiteB之间、SiteB与SiteC之间分别创建了**站点链接**，且分别有着不同的复制计划与复制间隔时间，请问DC1与DC3之间何时可以复制Active Directory数据库（以下针对**域目录分区**来进行说明）？

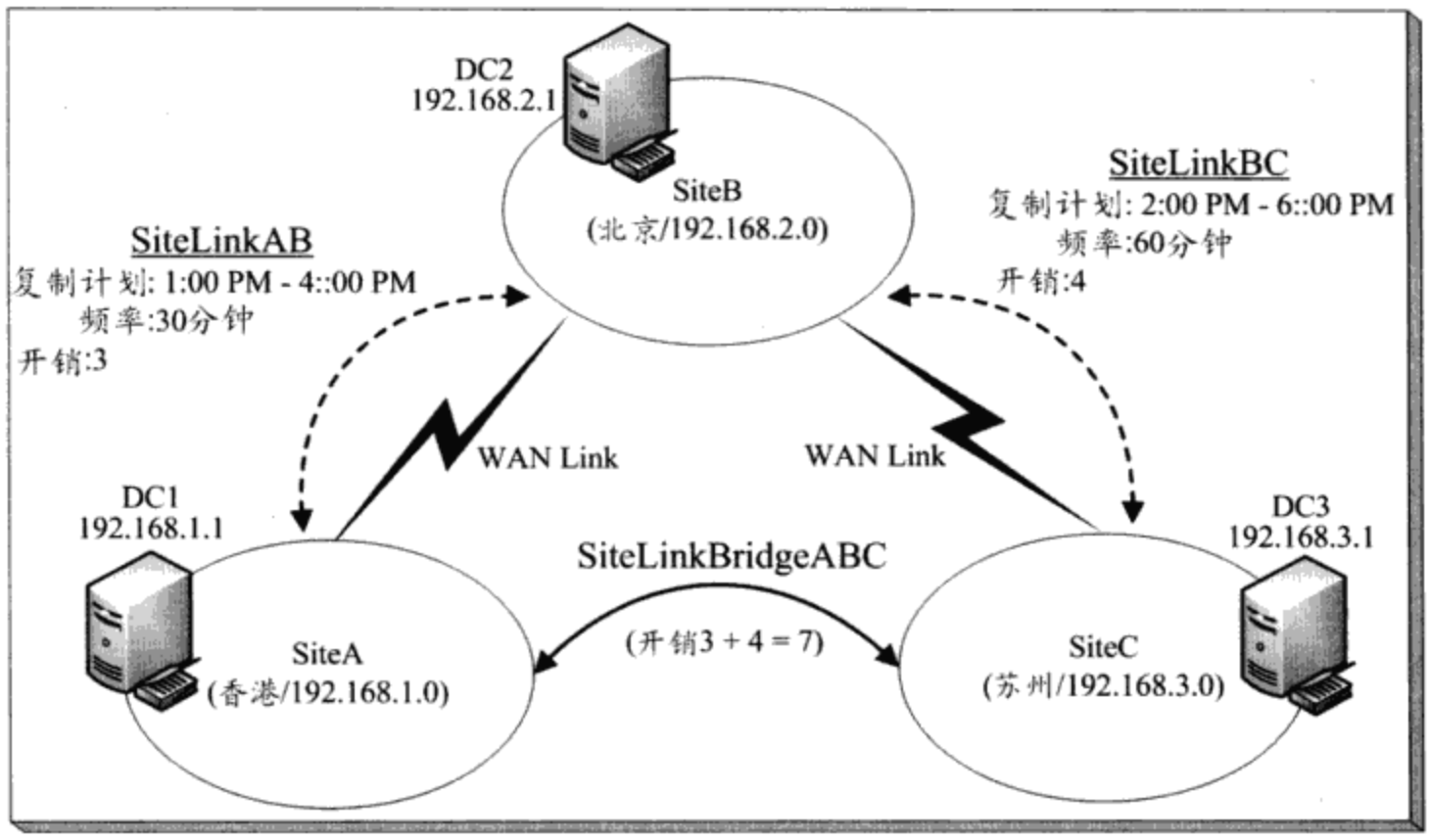


图9-36

（1）若 DC2 正常工作，且 DC1、DC2 与 DC3 隶属于同一个域

图中SiteLinkAB开销为3、SiteLinkBC开销为4，因此SiteLinkBridgeABC开销将是3 + 4 = 7，由于这个开销高于SiteLinkAB的开销3与SiteLinkBC的开销4，因此KCC在创建**复制拓扑**时，并不会在DC1与DC3之间创建**连接对象**，也就是不会将DC1与DC3设为**直接复制伙伴**，所以DC1与DC3在复制Active Directory数据库时必须通过DC2来转发。

当DC1的Active Directory数据有变动时，它可以在1:00 PM ~ 4:00 PM之间将数据复制给DC2，而DC2在收到数据后，会在2:00 PM ~ 6:00 PM之间将数据复制给DC3。

（2）若 DC2 脱机，或 DC2 与 DC1/DC3 不是隶属于同一个域

此时因为DC2无法提供服务（或不会存储另外一个域的Active Directory数据），因此DC1与DC3之间必须直接复制Active Directory数据库，此时KCC在创建**复制拓扑**时，因为SiteA与SiteC之间有**站点桥接链接器**，所以会在DC1与DC3之间创建**连接对象**，也就是将DC1与DC3

Download at http://www.pin5i.com/

设置为**直接复制伙伴**，让DC1与DC3之间可以直接复制。

但何时DC1与DC3之间才会直接复制Active Directory数据库呢？它们只有在两个**站点链接**的复制计划中有重叠的时段才会进行复制工作，例如SiteLinkAB复制计划是1:00 PM ~ 4:00 PM，而SiteLinkBC是2:00 PM ~ 6:00 PM，因此DC1与DC3之间会复制的时段为2:00 PM ~ 4:00 PM。

另外DC1与DC3之间的复制间隔时间为两个**站点链接**的最大值，例如SiteLinkAB为30分钟，SiteLinkBC为60分钟，则DC1与DC3两个站点链接的复制间隔时间为60分钟。

注意

在DC2故障或脱机（或DC2不是与DC1/DC3同一个域）的情况下，虽然可以通过**站点桥接链接器**让DC1与DC3直接复制Active Directory数据库，但是如果两个站点链接的复制计划中没有重叠时段的话，则DC1与DC3之间还是无法复制Active Directory数据库。

2. 站点链接桥示例二

若图 9-37中SiteA与SiteB之间、SiteB与SiteC之间分别创建了站点链接，但是您却取消选择图 9-34中的**为所有站点链接搭桥**复选框，而且并没有自行创建**站点链接桥**，则DC1与DC3之间是否可以进行Active Directory复制呢（以下针对**域目录分区**来进行说明）？

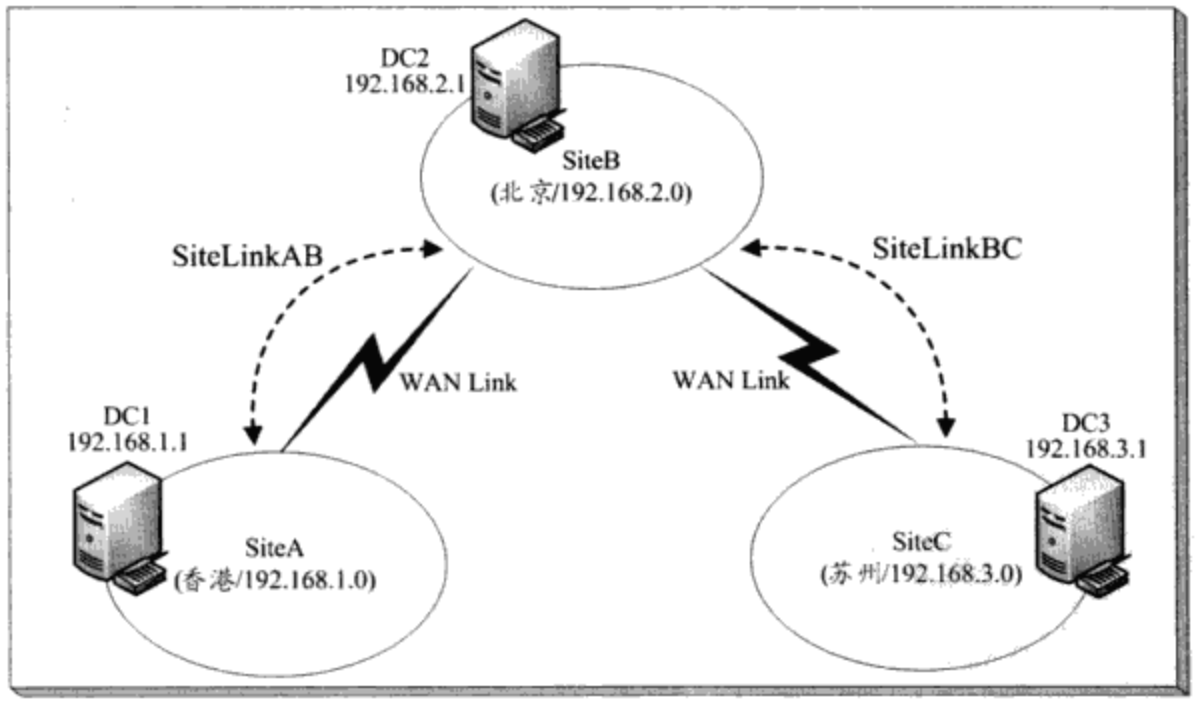


图 9-37

（1）若 DC2 正常工作，且 DC1、DC2 与 DC3 隶属于同一个域

此时由于SiteA与SiteC之间没有**站点桥接链接器**，因此KCC在创建**复制拓扑**时，不会在DC1与DC3之间创建**连接对象**，也就是不会将DC1与DC3设为**直接复制伙伴**，因此DC1与DC3之间只能够通过DC2来转发Active Directory数据。

Download at http://www.pin5i.com/

（2）若 DC2 脱机，或 DC2 与 DC1/DC3 不是隶属于同一个域

此时DC2无法接收与存储DC1与DC3的Active Directory数据，因此DC1与DC3必须直接复制Active Directory数据，但是因为SiteA与SiteC之间并没有**站点链接桥**，因此KCC无法在DC1与DC3之间创建**连接对象**，也就是无法将DC1与DC3设为**直接复制伙伴**，所以DC1与DC3之间将无法复制Active Directory数据。

9-4 管理全局编录服务器

全局编录服务器（Global Catalog Server，GC）也是一台域控制器，其内的**全局编录**存储着林中所有的Active Directory对象，如图 9-38所示。

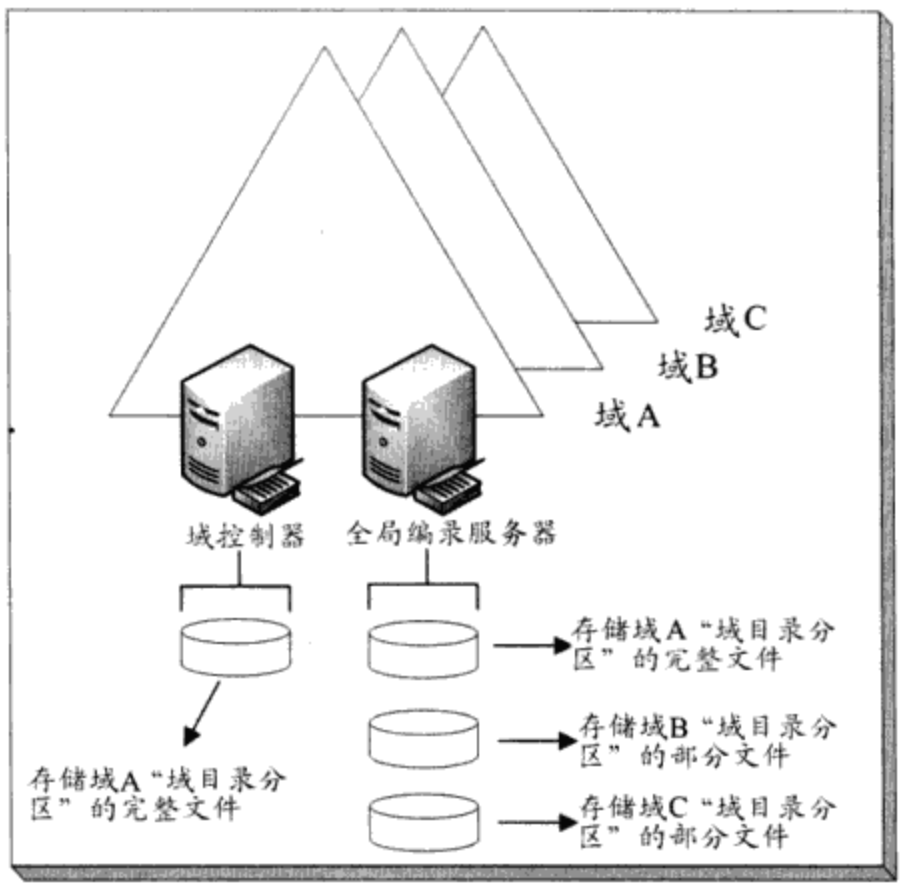


图9-38

图中的一般域控制器内只会存储所属域内**域目录分区**的完整数据，但是**全局编录服务器**还会存储林中所有其他域的**域目录分区**的对象的部分属性，让用户可以通过**全局编录**内的这些属性，快速地找到位于其他域内的对象。系统默认会将用户常用来搜索的属性加入到**全局编录**内，例如登录账户名、UPN、电话号码等。

9-4-1 添加属性到全局编录内

您也可以自行利用**Active Directory架构**控制台来将其他属性加入到**全局编录**内，不过可

Download at http://www.pin5i.com/

能需要在域控制器上先运行**regsvr32 schmmgmt.dll**命令来登录**schmmgmt.dll**，然后再通过【开始➲运行➲输入**MMC**后单击**确定**按钮➲选择**文件**菜单➲添加/删除管理单元➲选择**Active Directory架构**➲单击**添加**按钮】来创建此控制台。

若您要将其他属性加入到**全局编录**中的话，请通过【如图 9-39所示单击左边的**属性**文件夹➲双击右边要加入的属性➲选择**将此属性复制到全局编录**复选框】的方式进行操作。

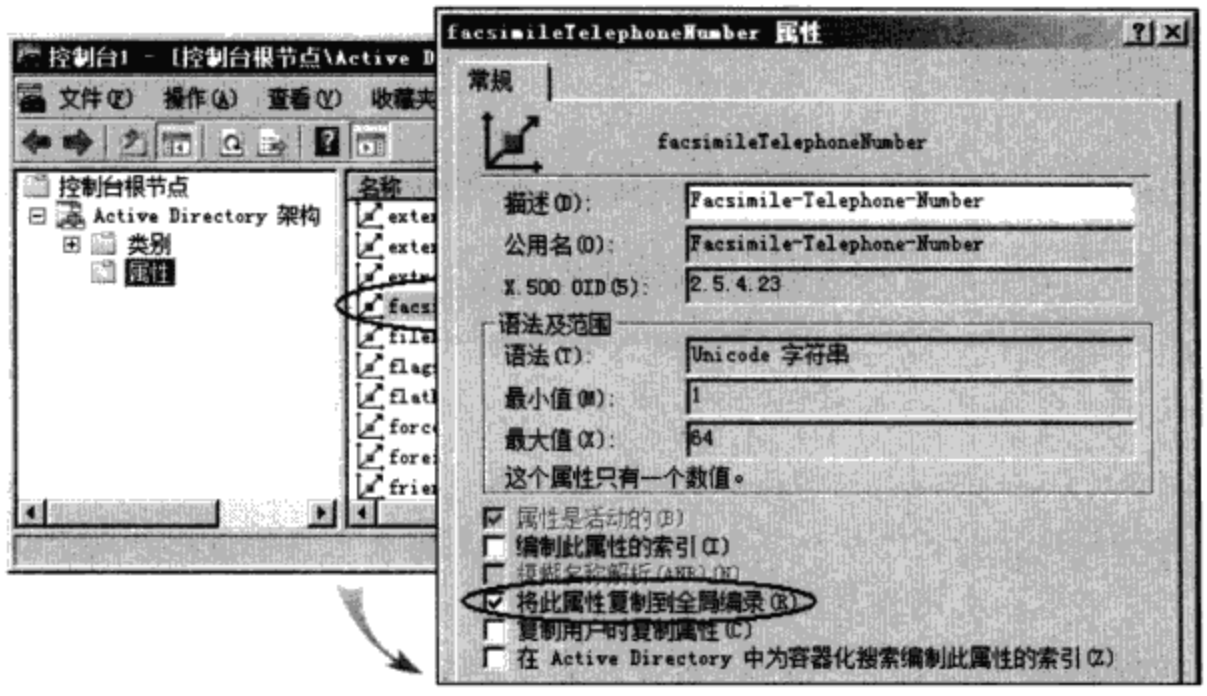


图 9-39

9-4-2 全局编录的功能

全局编录主要提供以下功能。

- **快速查找对象**：由于**全局编录**内存储着林中所有域的**域目录分区**对象的部分属性，用户可以利用这些属性快速地找到位于其他域的对象。举例来说，系统管理员可以通过【开始➲管理工具➲Active Directory管理中心➲如图 9-40所示单击**全局搜索**➲将**范围**下拉列表中选择**全局编录搜索**】的途径来利用**全局编录**快速地查找对象。

提示

全局编录的TCP端口号为3268，因此若用户与**全局编录服务器**之间被防火墙隔开的话，请在防火墙开放此端口。

Download at http://www.pin5i.com/

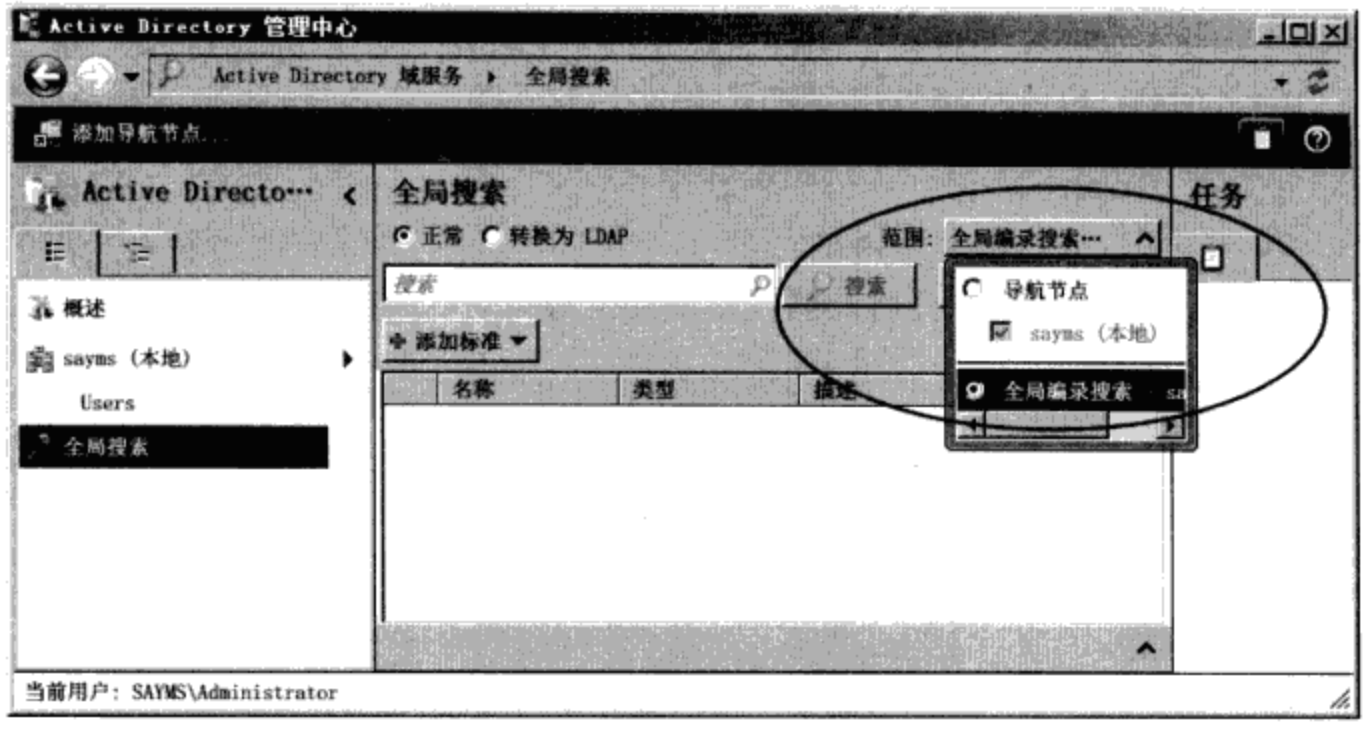


图9-40

- **提供UPN（User Principal Name）的验证功能**：当用户利用UPN登录时，若负责验证用户身份的域控制器无法从其Active Directory数据库来得知该用户是隶属于哪一个域的话，它可以向**全局编录服务器**询问。例如用户到域hk.sayiis.com的计算机上利用其UPN george@sayms.com账户登录时，由于域hk.sayiis.com的域控制器无法得知此george@sayms.com账户是位于哪一个域内（见Q&A），因此它会向**全局编录**查询，以便完成验证用户身份的工作。

Q 若用户的UPN为george@sayms.com，则该用户账户就一定是在域sayms.com的Active Directory数据库吗?

A 不一定! 虽然用户账户的UPN后缀默认就是账户所在域的域名，但是后缀可以更改，而且用户账户被转移到其他域时，其UPN并不会改变，也就是说UPN后缀不一定就是其域名。

- **提供通用组的成员数据**：当用户登录时，系统会为用户创建一个Access Token，其内包含着用户所隶属组的SID，也就是说用户登录时，系统必须得知该用户隶属于哪一组，不过因为通用组的成员信息只存储在**全局编录**，因此当用户登录时，负责验证用户身份的域控制器，需向**全局编录服务器**查询该用户所隶属的通用组，以便创建Access Token、让用户完成登录的程序。

当用户登录时，如果找不到**全局编录服务器**的话（例如故障、脱机），则用户是否可以登录成功呢?

- 如果用户之前曾经在这台计算机成功登录过，则这台计算机仍然能够利用存储在其**缓存区**（Cache）内的用户身份数据（Credentials）来验证用户的身份，因此还是可以登录成功的。

Download at http://www.pin5i.com/

↘ 如果用户之前未曾在这台计算机登录过，则这台计算机的**缓存区**内就不会有该用户的身份数据，故无法验证用户身份，因此用户无法登录。

提示

如果用户是隶属于Domain Admins组的成员，则无论**全局编录**是否在线，他都可以登录。

若要将某台域控制器设置为**全局编录服务器**的话，请按如图 9-41所示进行操作【单击该域控制器➲单击**NTDS Settings**➲单击上方的**属性**图标➲选择**全局编录**复选框】。

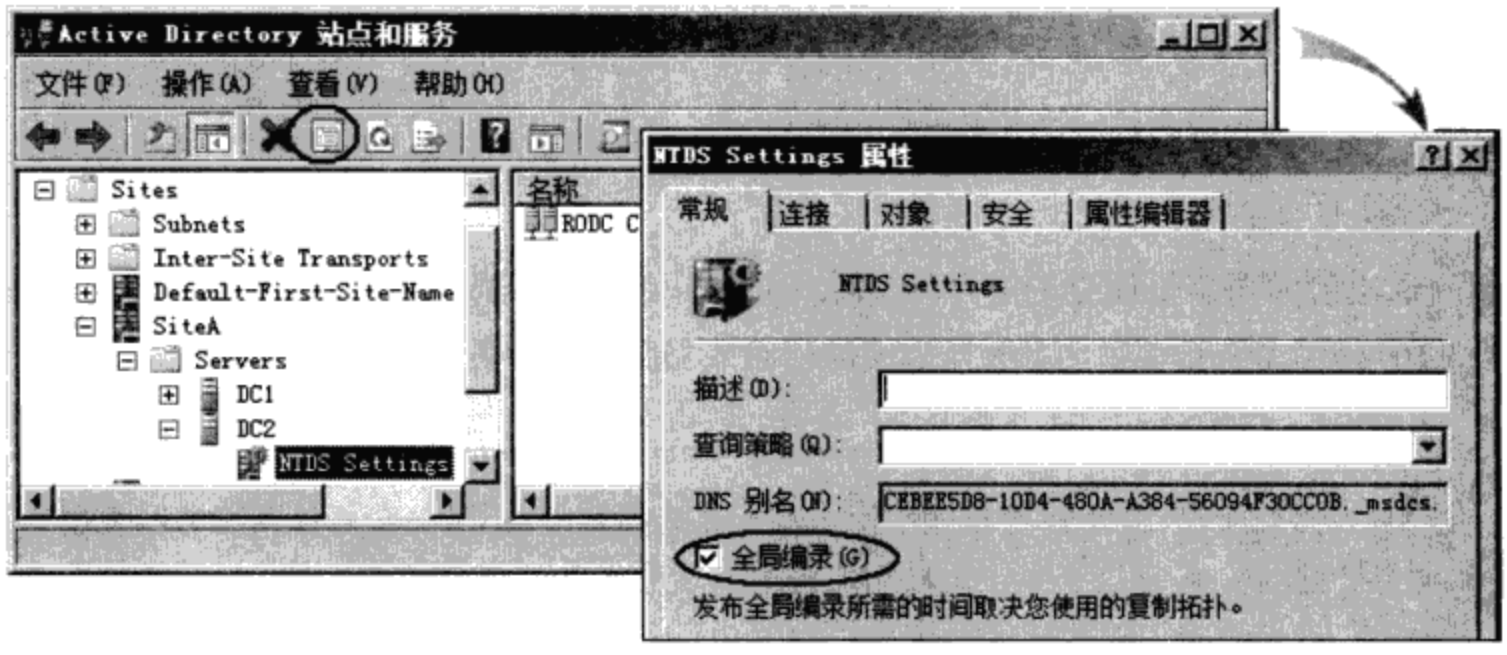


图9-41

9-4-3 通用组成员身份缓存

虽然您应该在每一个站点内启用一台**全局编录服务器**，但是对一个小型站点来说，因为硬件配备有限、经费短缺、带宽不足等因素的影响，所以架设一台**全局编录服务器**可能有困难。此时您可以通过**通用组成员身份缓存**来解决此问题。

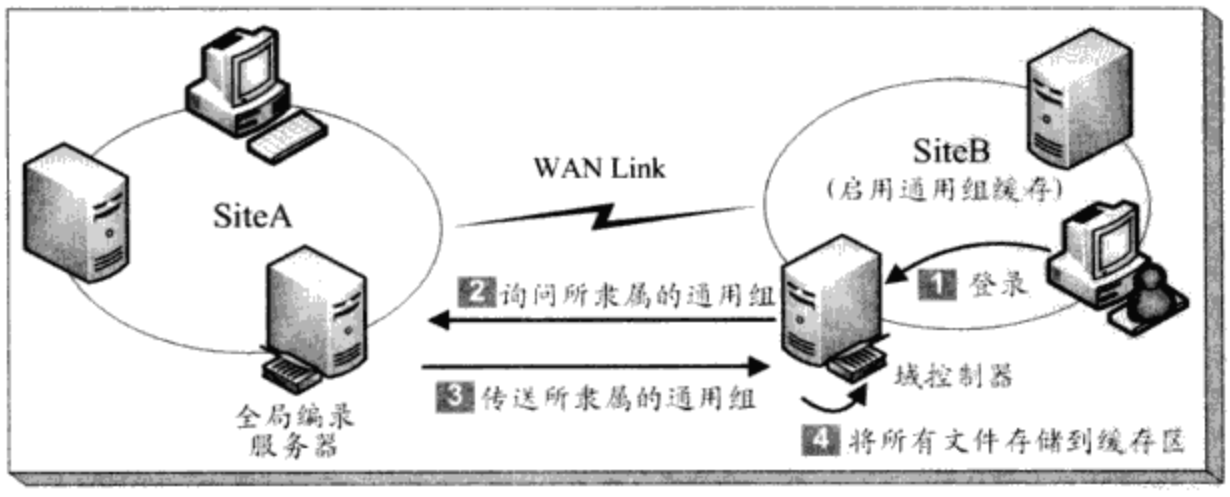


图9-42

例如图 9-42中若SiteB启用了**通用组成员身份缓存**，则当用户登录时，SiteB内的域控制器

Download at http://www.pin5i.com/

会向SiteA的**全局编录服务器**查询用户是隶属于哪一通用组，该域控制器得到这些数据后，便会将这些数据存储到其缓存区内，以后当这个用户再登录时，这台域控制器就可以直接从缓存区内得知该用户是隶属于哪一通用组，而不需要再向**全局编录**查询。**通用组成员身份缓存**拥有以下的好处：

- 加快用户登录的速度，因为域控制器不需要再向位于远程另外一个站点的**全局编录**查询。
- 现有域控制器的硬件不需要升级。由于**全局编录**的负担比较重，因此需要比较好的硬设备，然而站点启用**通用组成员身份缓存**后，该站点内的域控制器就可以不需要将硬件升级。
- 减轻对网络带宽的负担，因为不需要与其他站点的**全局编录**来复制林中所有域内的所有对象。

启用**通用组成员身份缓存**的途径为：【如图 9-43所示选择站点（例如SiteB）➲对着右边的**NTDS Settings**单击右键➲属性➲选择**启用通用组成员身份缓存**复选框】。



提示

域控制器默认会每隔8小时更新一次缓存区，也就是每隔8小时向**全局编录服务器**索取一次最新的数据，而它是从哪一个站点的**全局编录服务器**来更新缓存数据呢？这可从图中最下方的**在站点全局编录中刷新缓存**（Refresh Cache from）来选择。

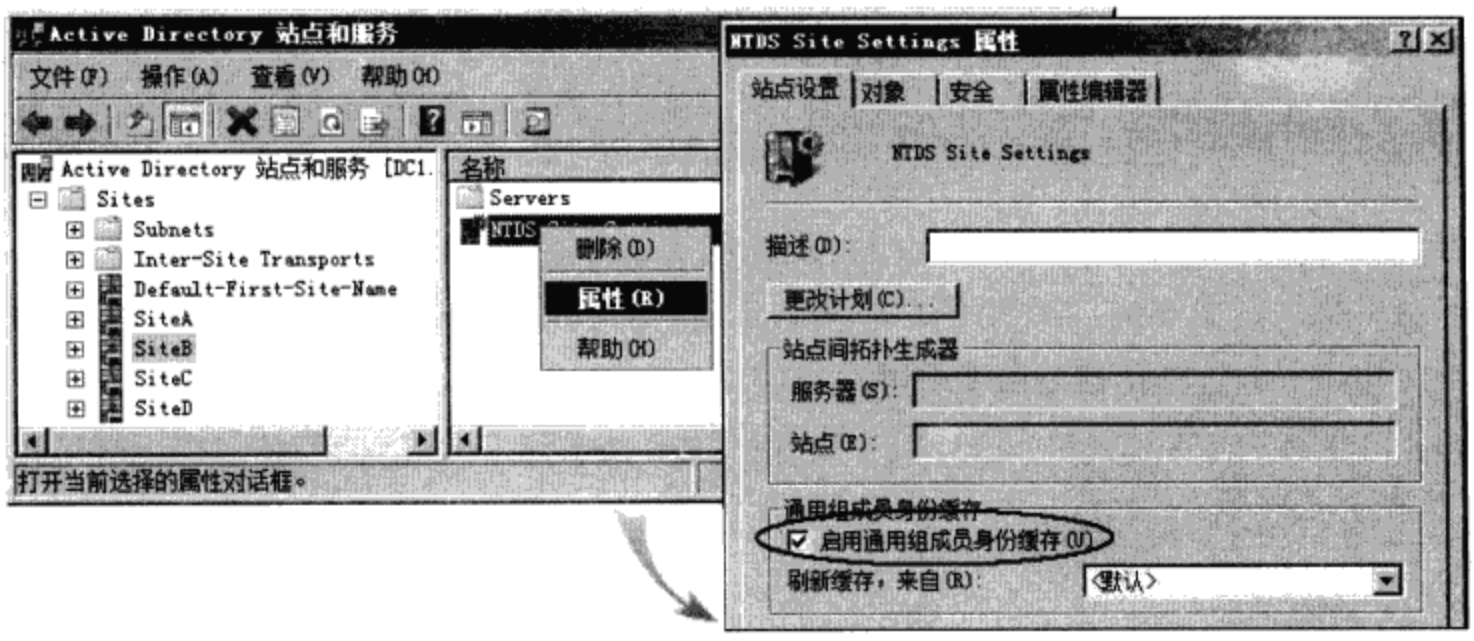


图 9-43

9-5 解决Active Directory复制冲突的问题

Active Directory数据库内的大部分数据是利用**多主机复制模式**来复制的，因此您可以直接更新任意一台域控制器内的Active Directory对象，之后这个更新对象会被自动复制到其他域控制器。

Download at http://www.pin5i.com/

但是若两个系统管理员同时分别在两台域控制器中创建相同的对象，或是修改相同对象的话，则之后双方开始相互复制这些对象时，就会有冲突发生，此时系统该如何来解决这个问题呢？

9-5-1 属性戳记

AD DS使用**戳记**（Stamp）来作为解决冲突的依据。当您修改了Active Directory某个对象的属性数据后（例如修改用户的地址），这个属性的戳记数据就会改变。这个戳记是由三个数据所组成的。

版本号	修改时间	域控制器的GUID

- 版本号（Version Number）：每一次修改对象的属性时，属性的版本号都会增加，初始值是1。
- 修改时间（Timestamp）：对象属性被修改的原始时间。
- 域控制器的GUID：发生对象修改行为的源域控制器的GUID。

AD DS在解决冲突时，是以戳记值最高的优先，换句话说版本号较高的优先；若版本号相同，则以修改时间较后的优先；若修改时间还是相同（机率非常小），再比较源域控制器的GUID，GUID数值较高者优先。

9-5-2 冲突的种类

Active Directory对象共有以下三种不同种类的冲突情况，而不同种类的冲突，其解决冲突的方法也不同：

- 属性值相冲突。
- 在某容器内添加对象或将对象转移到此容器内，但是这个容器已经在另外一台域控制器内被删除。
- 名称相同。

1. 属性冲突的解决方法

如果是属性值有冲突，则以戳记值最高的优先。举例来说，假设用户**王乔治**的**显示名称**属性的版本号目前为1，而此时有两个系统管理员，分别在两台域控制器上修改了**王乔治**的**显示名称**（如图 9-44所示），则在这两台域控制器内，**显示名称**属性的版本号都会变为2。因为版本号相同，故此时需要以**修改时间**（Timestamp）来决定以哪一个系统管理员所修改的数据优先，也就是以修改时间较晚的优先。

Download at http://www.pin5i.com/

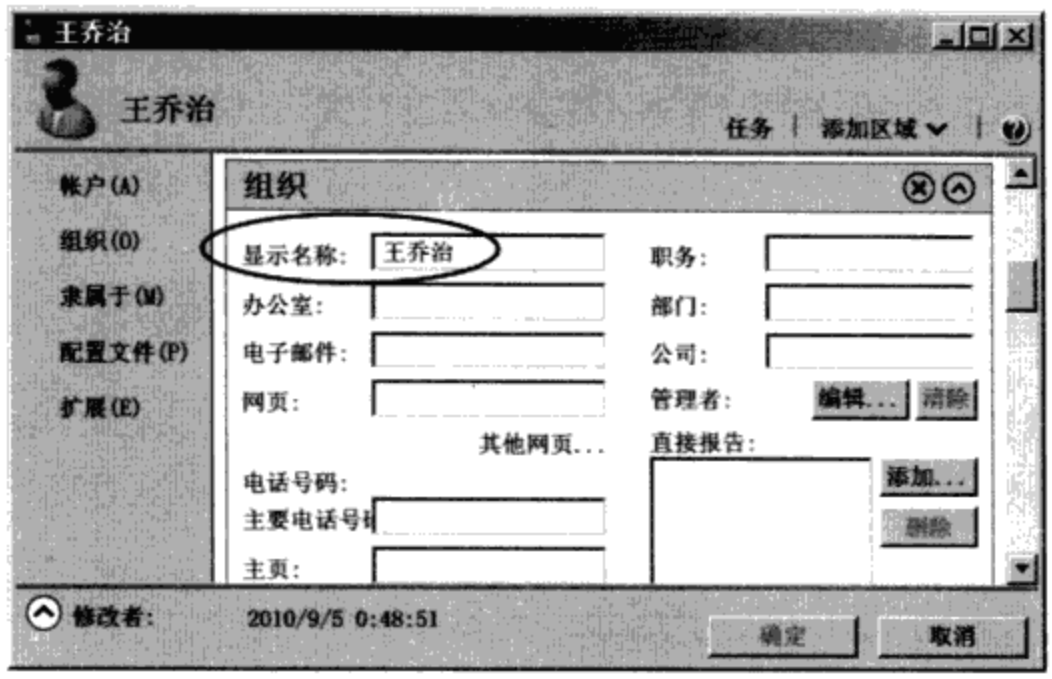


图9-44

您可以利用以下的**repadmin**程序来查看版本号，如图9-45所示。

```
repadmin /showmeta CN=王乔治,OU=业务部,DC=sayms,DC=com
```

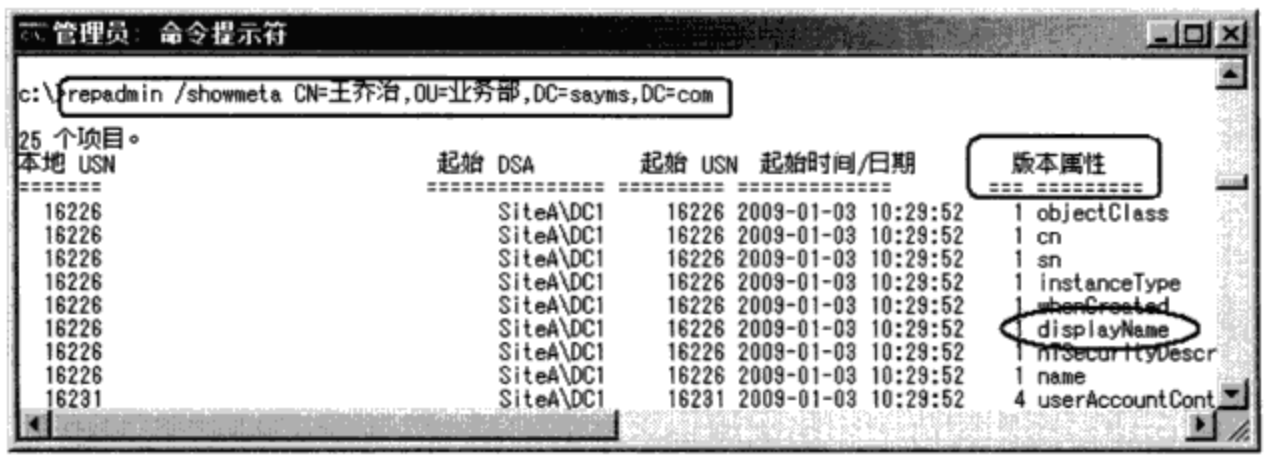


图9-45

提示

Repadmin.exe还可以用来查看域控制器的**复制拓扑**、创建**连接对象**、手动执行复制、查看复制信息、查看域控制器的GUID等。

2. 对象存放容器被删除的解决方法

例如某个系统管理员在第1台域控制器上将图9-46中的组织单位**业务部**删除，但是同时在第2台域控制器上却有另外一个系统管理员在组织单位**业务部**内添加一个用户账户**高丽黛**。请问两台域控制器之间开始复制Active Directory数据库时，会发生什么情况呢？

Download at http://www.pin5i.com/

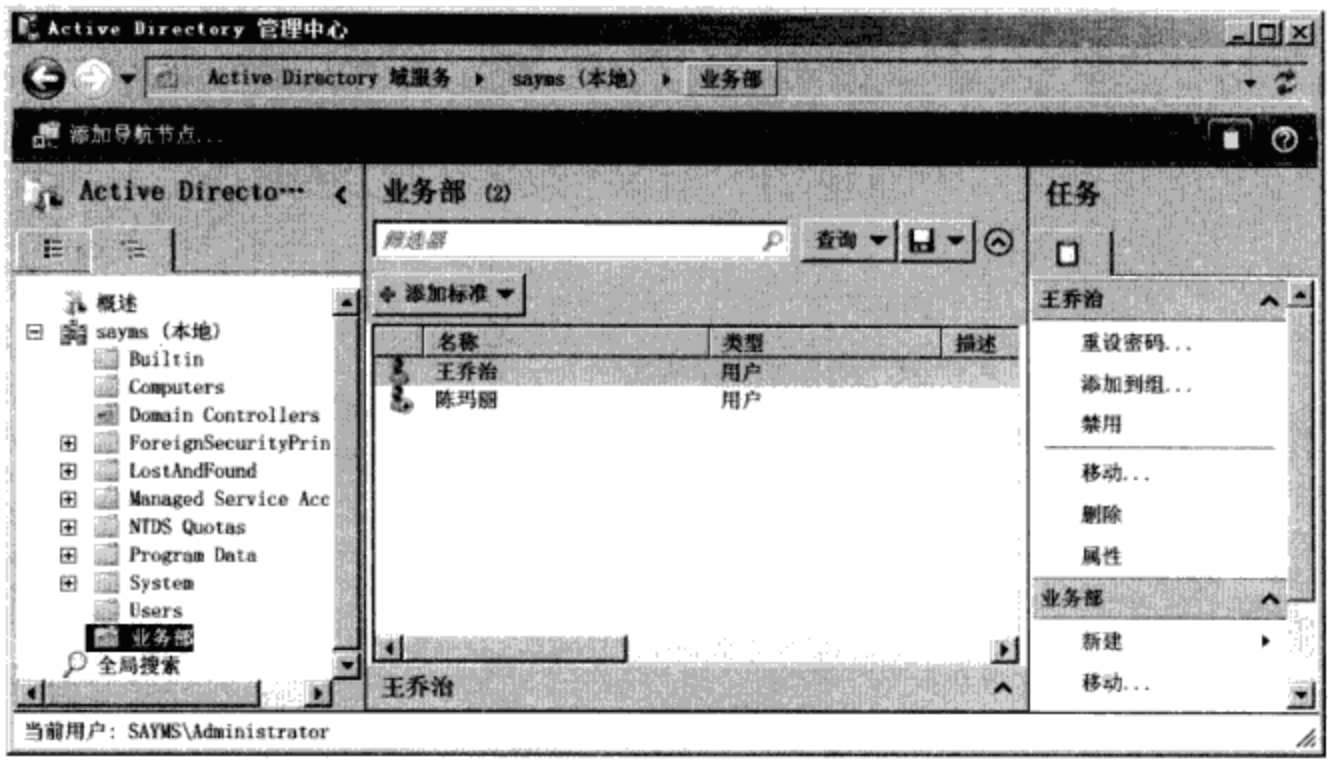


图 9-46

此时所有域控制器内的组织单位**业务部**都会被删除，但是用户账户**高丽黛**会被放置到LostAndFound文件夹内，如图 9-47所示。这种冲突现象并不会使用到戳记来解决问题。



图 9-47

提示

若需要验证上述理论的话，请先让两台域控制器之间的网络无法通信，然后分别在两台域控制器上操作，再让两台域控制器能够通过网络正常通信，手动复制Active Directory数据库。不过在您删除组织单位**业务部**时会被拒绝，这是因为系统默认会保护组织单位，避免被意外删除，除非您先执行以下步骤【打开Active Directory管理中心➲对着组织单位**业务部**单击右键➲属性➲如图 9-48所示单击**组织单位**选项➲取消选择**防止意外删除**复选框】。

Download at http://www.pin5i.com/

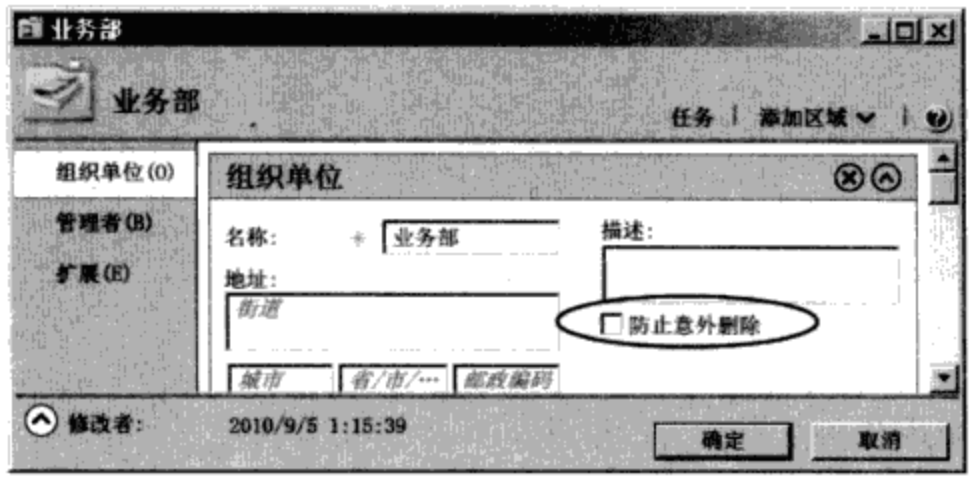


图 9-48

3. 名称相同

如果对象的名称相同，则两个对象都会被保留，此时戳记值较高的对象名称会维持原来的名称，而戳记值较低的对象名称会被改变为：

对象的RDN CNF：对象的GUID

例如在两台域控制器上同时添加一个名称相同的用户**赵日光**，但是分别有不同的属性设置，则在两台域控制器之间进行Active Directory数据库复制后，其结果为：如图 9-49所示的两个账户都被保留，但其中一个被改名。

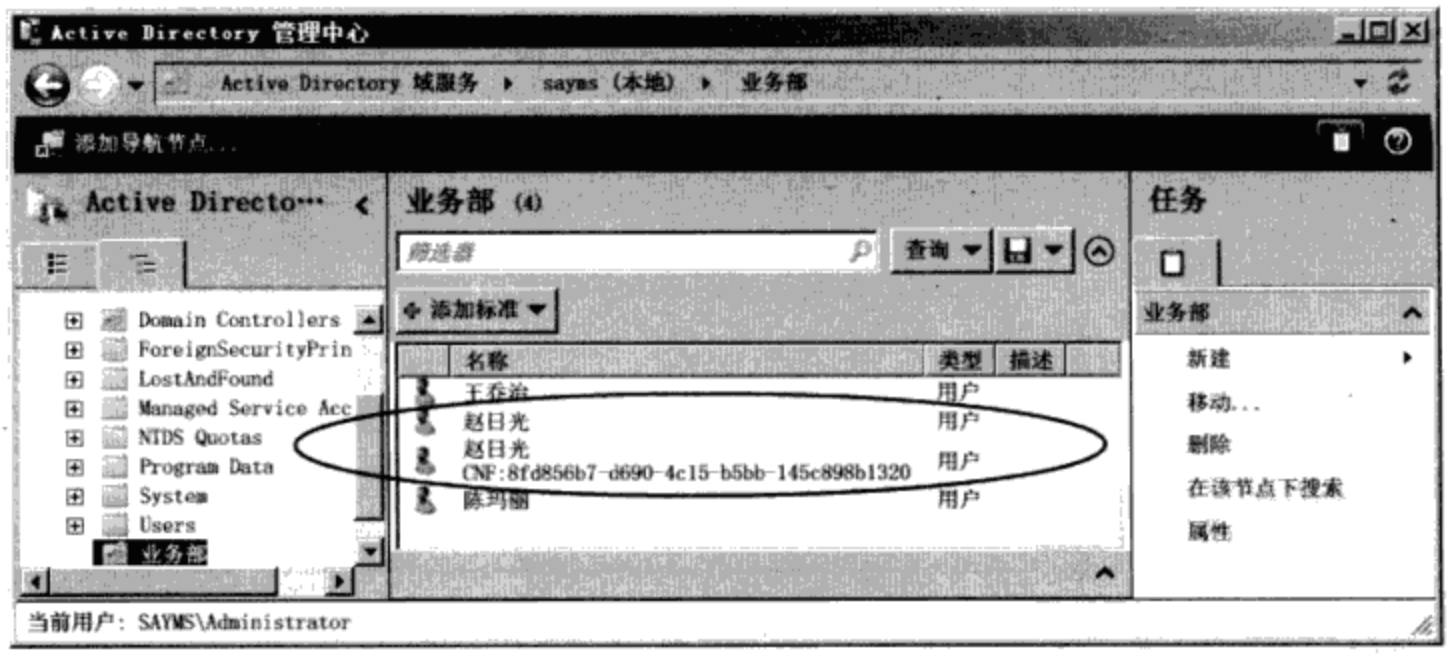


图 9-49

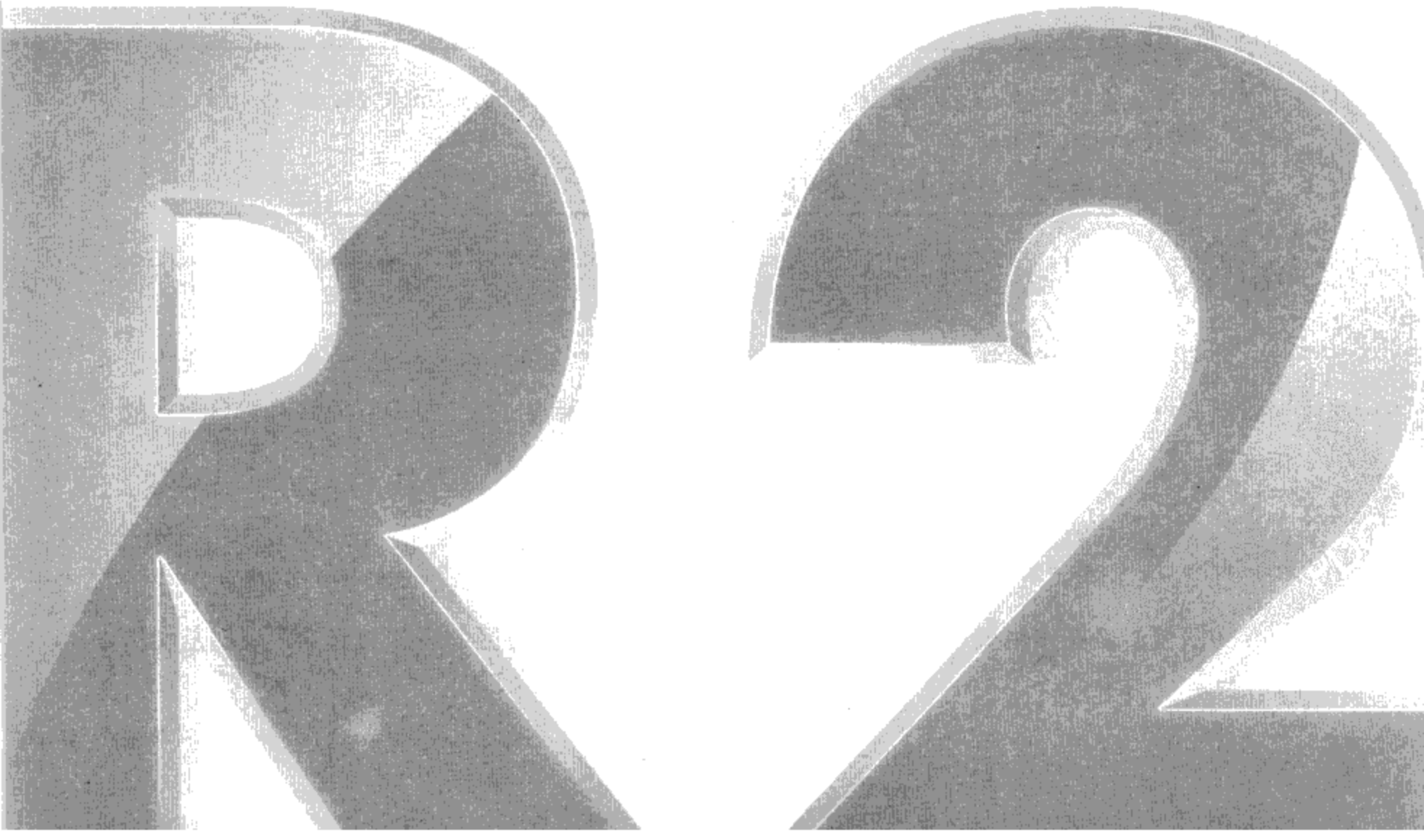
Download at http://www.pin5i.com/

第10章

操作主机的管理

在AD DS内有一些数据的维护与管理是由**操作主机**（Operations Master）来负责的，身为系统管理员的您必须彻底了解它们，才能够充分控制与维持域的正常运行。

- 操作主机概念
- 操作主机的放置优化
- 找出扮演操作主机角色的域控制器
- 转移操作主机角色
- 夺取操作主机角色



Download at http://www.pin5i.com/

10-1 操作主机概述

Active Directory数据库内绝大部分数据的复制是采用**多主机复制模式**（Multi-master Replication Model），也就是您可以直接更新任何一台域控制器内绝大部分的Active Directory对象，之后这个对象会被自动复制到其他域控制器。

然而有少部分数据的复制是采用**单主机复制模式**（Single-master Replication Model）。在此模式下，当您提出更改对象的要求时，会由其中一台被称为**操作主机**的域控制器负责接收与处理此请求，也就是说该对象是先被更新在这台操作主机内，再由这台操作主机将其复制到其他域控制器。

Active Directory域服务（AD DS）内总共有5个操作主机角色：

- 架构操作主机（Schema Operations Master）。
- 域命名操作主机（Domain Naming Operations Master）。
- RID操作主机（Relative Identifier Operations Master）。
- PDC模拟器操作主机（PDC Emulator Operations Master）。
- 基础结构操作主机（Infrastructure Operations Master）。

一个林中只有一台**架构操作主机**与一台**域命名操作主机**，这2个林级别的角色默认都是由林根域内第1台域控制器所扮演。而每一个域拥有自己的**RID操作主机**、**PDC模拟器操作主机**与**基础结构操作主机**，这3个域级别的角色默认是由该域内第1台域控制器所扮演。

提示

1. 操作主机角色（Operations Master Roles）也被称为Flexible Single Master Operations（FSMO）Roles。
2. **只读域控制器**（RODC）无法扮演操作主机的角色。

10-1-1 架构操作主机

扮演**架构操作主机**角色的域控制器，负责更新与修改**架构**（Schema）内的对象种类与属性数据。隶属于Schema Admins组内的用户才有权限修改**架构**。一个林中只能够有一台**架构操作主机**。

10-1-2 域命名操作主机

扮演**域命名操作主机**角色的域控制器，负责林内**域目录分区**的添加与删除，也就是负责

Download at http://www.pin5i.com/

林内的域添加与删除工作。它也负责**应用程序目录分区**的添加与删除。一个林中只能够有一台**域命名操作主机**。

10-1-3 RID操作主机

每一个域内只能够由一台域控制器扮演**RID操作主机**角色，而其主要的工作是发放RID（Relative ID）给其域内的所有域控制器。RID有何用途呢？当域控制器内新建了一个用户、组或计算机等对象时，域控制器必须指派一个唯一的安全标识符（SID）给这个对象，此对象的SID是由域SID与RID所组成的，也就是说**对象SID = 域SID + RID**，而RID并不是由每一台域控制器自己产生的，它是由**RID操作主机**来统一发放给其域内的所有域控制器。每一台域控制器需要RID时，它会向**RID操作主机**获取一些RID，RID用完后再向**RID操作主机**获取。

由于是由**RID操作主机**来统一发放RID，因此不会有RID重复的情况发生，也就是每一台域控制器所获得的RID都是唯一的，因此对象的SID也是唯一的。如果是由每一台域控制器各自生成RID的话，则可能不同的域控制器会生成相同的RID，因而会有对象SID重复的情况发生。

10-1-4 PDC模拟器操作主机

每一个域内只能够由一台域控制器扮演**PDC模拟器操作主机**角色，而它所负责的工作如下。

1. 支持旧客户端计算机

用户在域内的旧客户端计算机（例如Windows NT 4.0）上更改密码时，这个密码数据是会被更新在PDC（Primary Domain Controller）上，而AD DS通过**PDC模拟器操作主机**来扮演PDC的角色。

另外若域内有Windows NT Server 4.0 BDC（Backup Domain Controller）的话，它会要求从Windows NT Server 4.0 PDC来复制用户账户与密码等数据，而AD DS通过**PDC模拟器操作主机**来扮演PDC的角色。

2. 减少因为密码复制延迟所造成的问题

当用户的密码更改后，需要一点时间这个密码才会被复制到其他所有的域控制器，如果在这个密码还没有被复制到其他所有域控制器之前，用户利用新密码登录，则可能会因为负责检查用户密码的域控制器内还没有用户的新密码数据，因而无法登录成功。

AD DS采用以下方法来减少这个问题发生的机率：当用户的密码更改后，这个密码会优先

Download at http://www.pin5i.com/

被复制到**PDC模拟器操作主机**，而其他域控制器仍然是依照一般复制程序，也就是需要等一段时间后才会收到这个最新的密码。如果用户登录时，负责验证用户身份的域控制器发现密码不对时，它会将验证身份的工作转送给拥有新密码的**PDC模拟器操作主机**，以便让用户可以登录成功。

3. 负责整个域时间的同步

域用户登录时，如果其计算机时间与域控制器不一致的话，将无法登录，而**PDC模拟器操作主机**就是负责整个域内所有计算机时间的同步工作。AD DS的时间同步程序请参考图10-1。

- 图中林根域sayms.com内的**PDC模拟器操作主机**DC1与外部的时间服务器同步。
- 所有其他域的**PDC模拟器操作主机**的计算机时间会自动与林根域sayms.com内的**PDC模拟器操作主机**同步，例如图中的DC2、DC4、DC5、DC6会与DC1同步。
- 各域内的其他域控制器都会自动与该域的**PDC模拟器操作主机**时间同步，例如DC3会与DC2同步。
- 域内的成员计算机会与验证其身份的域控制器同步，例如图中tw.sayms.com内客户端计算机会与DC3同步。

由于林根域sayms.com内的**PDC模拟器操作主机**的计算机时间会影响到林内所有计算机的时间，因此请确保此台**PDC模拟器操作主机**的时间正确性。

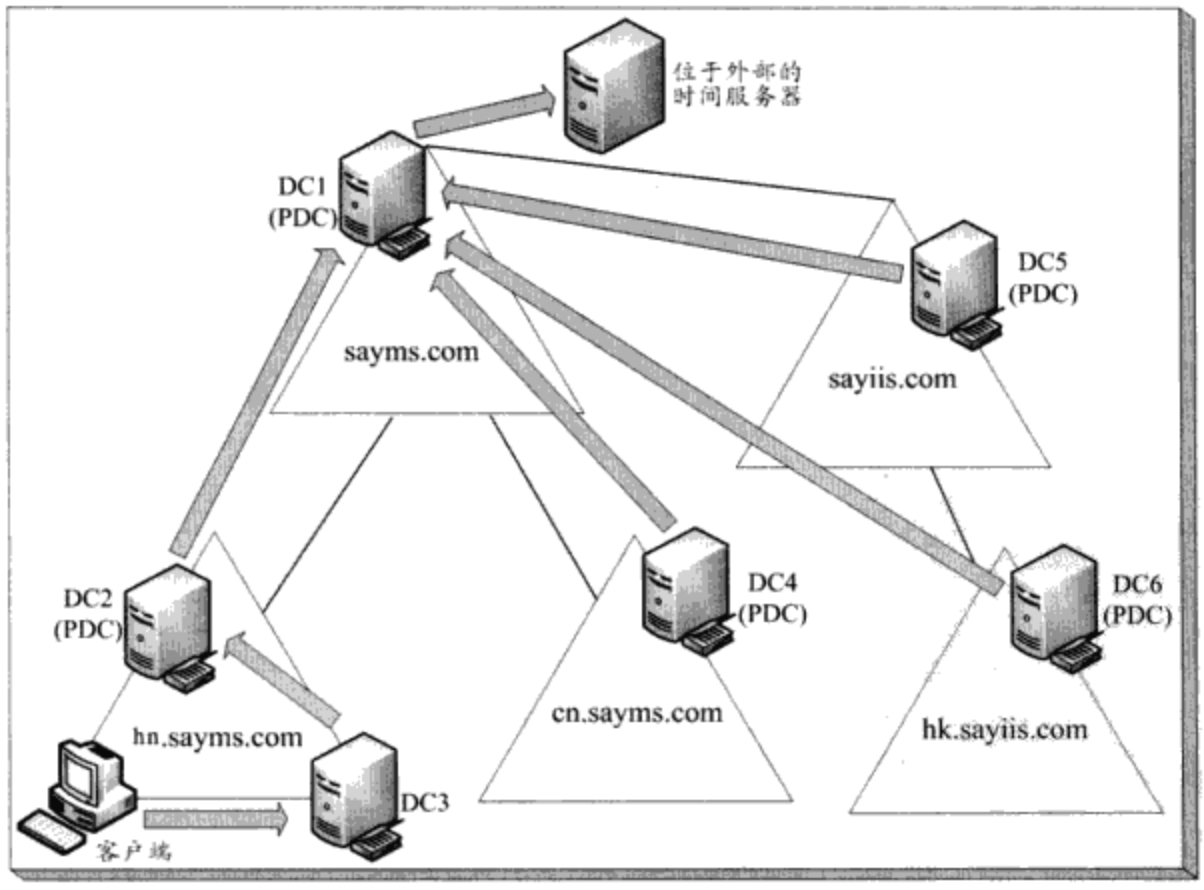


图 10-1

客户端计算机可以通过**w32tm /query /configuration**命令来查看时间同步的设置，而我们可以从此命令的结果界面（参考图 10-2）的**Type**字段来判断此客户端计算机时间的同步方式。

Download at http://www.pin5i.com/

提示

上述命令适用于Windows Server 2008 R2、Windows 7、Windows Server 2008与Windows Vista，若是旧版Windows系统的话，可用**net time /querysntp**命令，不过仅能够显示有限的信息。

- NoSync：表示客户端不会同步时间。
- NTP：表示客户端会从外部的时间服务器来同步，而所同步的服务器会显示在图中**NtpServer**字段，例如图中的**time.windows.com**。
- NT5DS：表示客户端是通过前面图 10-1的域架构方式来同步时间。
- AllSync：表示客户端会选择所有可用的同步机制，包含外部时间服务器与域架构方式。

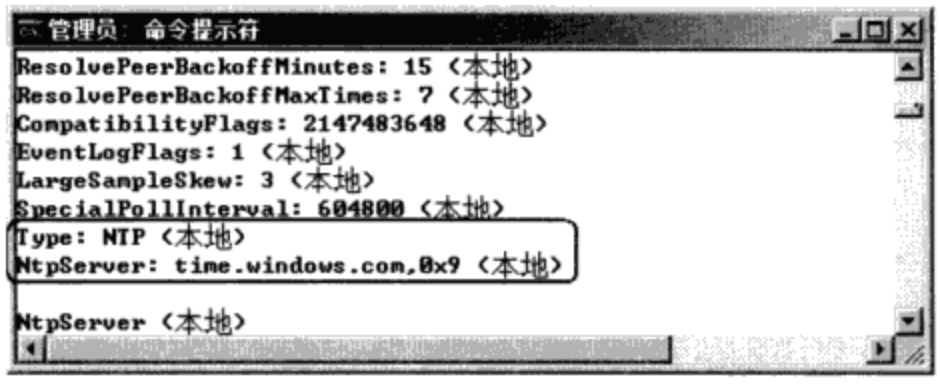


图 10-2

提示

未加入域的客户端计算机可能需要先启动**Windows Time**服务，再来执行上述程序，而且必须以系统管理员的身份来执行此程序。

如果客户端计算机是通过图 10-1中的域架构方式来同步时间的话，则执行 **w32tm /query /configuration**命令后的**Type**字段如图 10-3所示为NT5DS。而您也可以通过如图 10-4所示的**w32tm /query /source**命令来得知其目前所同步的时间服务器，例如图中的dc1.sayms.com，它就是前面图 10-1中域sayms.com内的PDC。

提示

时间同步所使用的协议为SNTP（Simple Network Time Protocol），其端口号为UDP 123。

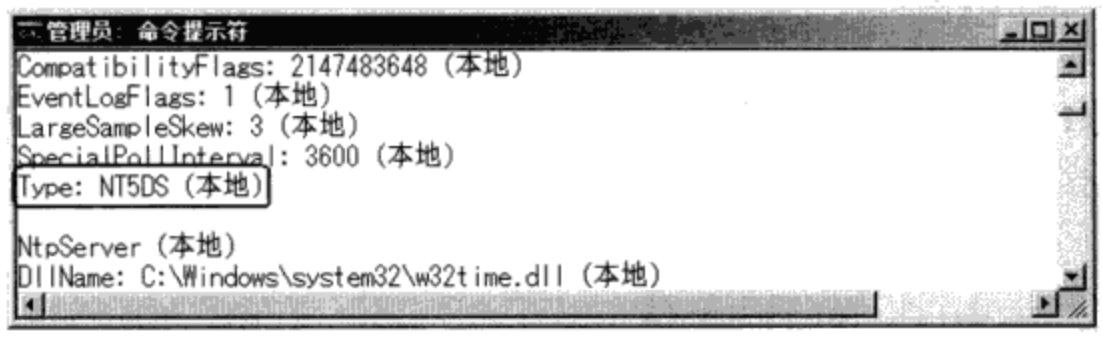


图 10-3

Download at http://www.pin5i.com/

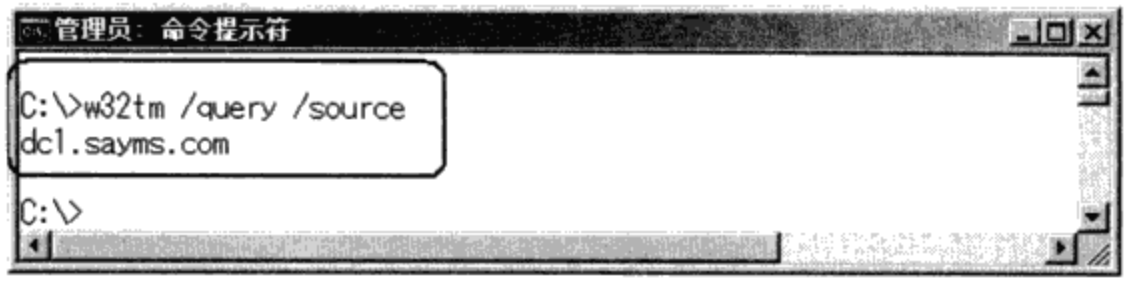


图 10-4

未加入域的计算机，其时间默认会自动与微软的时间服务器 **time.windows.com**同步，若要更改这个设置或执行手动同步的话，以Windows Server 2008 R2或Windows 7计算机来说，可以在这些计算机上选择【开始➲控制面板➲设置日期和时间➲如图 10-5所示单击**Internet时间**标签➲单击更改设置按钮➲通过弹出的对话框进行设置】或用**w32tm /resync**命令手动同步。



图 10-5

10-1-5 基础结构操作主机

每一个域内只能够由一台域控制器来扮演**基础结构操作主机**的角色。如果域内有对象参考到其他域的对象时，**基础结构操作主机**会负责更新这些参考对象的数据，例如本域内有一个组的成员包含另外一个域的用户账户，当这个用户账户有变动时，**基础结构操作主机**便会负责来更新这个组的成员信息，并将其复制到同一个域内的其他域控制器。

基础结构操作主机是通过**全局编录服务器**来得到这些参考数据的最新版本，因为**全局编录服务器**会收到由每一个域所复制来的最新变动数据。

10-2 操作主机的放置优化

为了提高运行效率、减轻系统管理的负担与减少问题发生的机率，因此如何适当的放置操

Download at http://www.pin5i.com/

作主机便成为不可忽视的问题。

10-2-1 基础结构操作主机的放置

由于**基础结构操作主机**与**全局编录**并不兼容，因此请勿将**基础结构操作主机**放置到**全局编录服务器**上，除非是以下的情况。

- 所有的域控制器都是**全局编录服务器**：由于**全局编录服务器**会收到由每一个域所复制来的最新变动数据，故此时由哪一台域控制器来扮演**基础结构操作主机**都无所谓。
- 只有一个域：如果整个林中只有一个域，则**基础结构操作主机**就没有作用了，因为没有其他域的对象可供参考，此时不需要理会**基础结构操作主机**是由哪一台域控制器来扮演。

为了便于管理，建议将域级别的**RID操作主机**、**PDC模拟器操作主机**与**基础结构操作主机**都放置到同一台域控制器上。

> 提示
>
> 如果域中有**只读域控制器**（RODC）的话，则**PDC模拟器操作主机**必须由Windows Server 2008或Windows Server 2008 R2域控制器来扮演。

10-2-2 PDC模拟器操作主机的放置

PDC模拟器操作主机经常需要与网络上的其他系统通信，它的负担比其他操作主机来得重，故此台计算机的设备性能应该是最好、最稳定的，以确保能够应付较重的负担与提供较高的可用性。

如果要降低**PDC模拟器操作主机**的负担的话，可以在DNS服务器内调整它的**权重**（Weight）。当客户端需要查找域控制器来验证用户身份时，客户端会向DNS服务器查询域控制器，而DNS服务器会将客户端转到（Refer To）指定的域控制器，由这台域控制器来负责验证用户身份，而由于所有域控制器默认的**权重**是相同的（100），因此每一台域控制器被转移的机率也是相同的。如果您将**PDC模拟器操作主机**的**权重**降低的话，例如降为一半（50），则客户端被转移到这台**PDC模拟器操作主机**的机率就会降低一半，如此便可以降低它的负担。

假设**PDC模拟器操作主机**为dc1.sayms.com，而您要调整其**权重**的话，请【打开**DNS管理器**控制台➲如图 10-6所示展开到区域sayms.com下的_tcp文件夹➲双击右边的dc1.sayms.com➲修改图 10-7中的**权重**值】。

Download at http://www.pin5i.com/

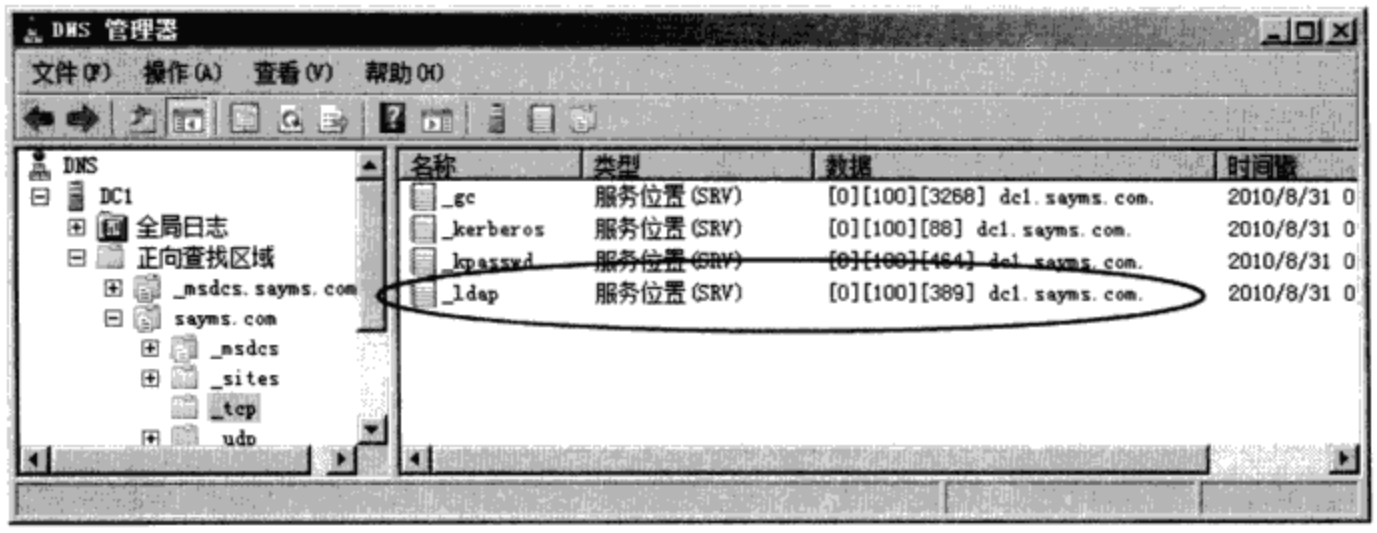


图 10-6

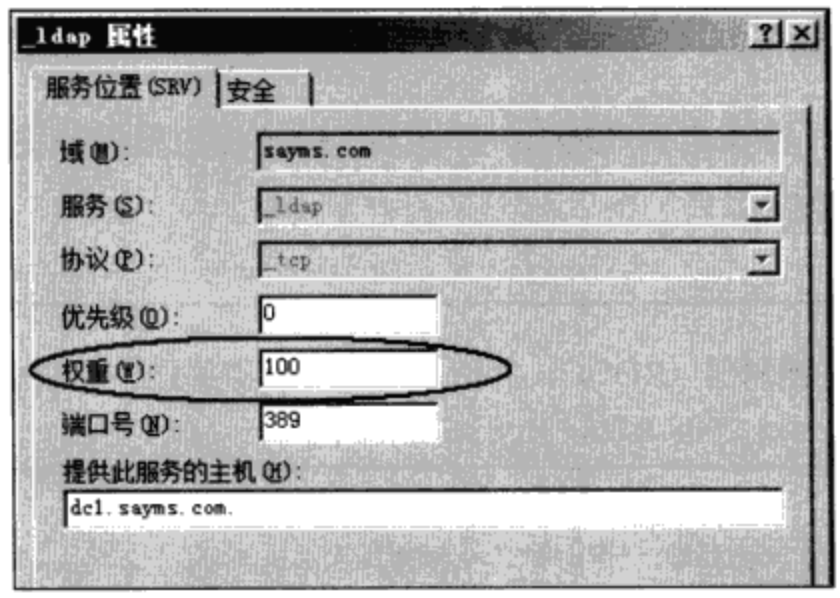


图 10-7

若网络内旧版系统（Windows 2000之前的版本）数量较多的话，则 **PDC模拟器操作主机** 会使用比较多的RID，此时若将**PDC模拟器操作主机**与**RID操作主机**放在同一台域控制器上的话，也可以让这两个角色的通信更有效率。

10-2-3 林级别操作主机的放置

林中第1台域控制器会自动扮演林级别的**架构操作主机**与**域命名操作主机**的角色，它同时也是**全局编录服务器**。这两个角色并不会对域控制器造成太大负担，它们也与**全局编录**兼容，而且即使将这两个角色移到其他域控制器也不会改善运行性能，因此为了便于管理与执行备份、还原工作，故建议将这两个角色继续保留由这台域控制器来扮演。

10-2-4 域级别操作主机的放置

每一个域内的第1台域控制器会自动扮演域级别的操作主机，以林根域中的第1台域控制器为例，它同时扮演2个林级别与3个域级别的操作主机，同时也是**全局编录服务器**，不过因为

Download at http://www.pin5i.com/

其中的**基础结构操作主机**与**全局编录**并不兼容，因此除非所有的域控制器都是**全局编录服务器**或林中只有一个域，否则请将**基础结构操作主机**的角色转移到其他域控制器，为了便于管理，请将**RID操作主机**与**PDC模拟器操作主机**也一并转移到这台域控制器。

除了林根域之外，其他域请将3台域级别的操作主机保留由第1台域控制器来扮演，但不要将这台域控制器设置为**全局编录服务器**，除非所有域控制器都是**全局编录服务器**或林中只有一个域。除非工作负担太重，否则请尽量将这3台操作主机交由同一台域控制器来扮演，以减轻管理负担。

10-3 找出扮演操作主机角色的域控制器

在您新建AD DS域时，系统会自动选择域控制器来扮演操作主机，我们将在本节介绍如何找出扮演操作主机的域控制器。不同的操作主机角色可以利用不同的Active Directory管理控制台来检查，如表 10-1所示。

表 10-1

角色	管理控制台
架构操作主机	Active Directory架构
域命名操作主机	Active Directory域和信任
RID操作主机	Active Directory用户和计算机
PDC模拟器操作主机	Active Directory用户和计算机
基础结构操作主机	Active Directory用户和计算机

10-3-1 找出架构操作主机

我们可以利用**Active Directory架构**来找出目前扮演**架构操作主机**角色的域控制器，操作步骤如下。

STEP 1 您需要到域控制器上登录，然后登录**schmmgmt.dll**，才可以使用**Active Directory架构**控制台，若尚未登录**schmmgmt.dll**的话，请执行以下命令，并在出现登录成功界面后，再继续以下的步骤。

```
regsvr32  schmmgmt.dll
```

STEP 2 选择【开始➲运行➲输入**MMC**后单击**确定**按钮➲选择**文件**菜单➲添加/删除管理单元➲在图 10-8中选择**Active Directory架构**选项➲单击**添加**按钮➲单击**确定**按钮】。

Download at http://www.pin5i.com/

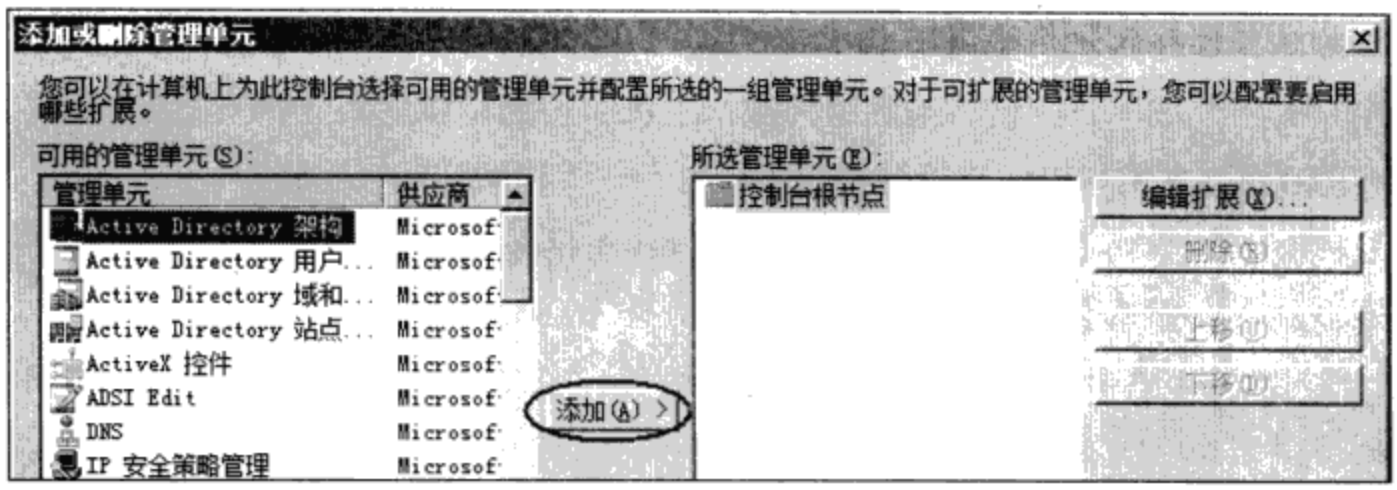


图 10-8

STEP 3 如图 10-9所示，通过【对着**Active Directory架构**单击右键➲操作主机】的方式进行操作。



图 10-9

STEP 4 从图 10-10中可知当前**架构主机**为dc1.sayms.com。

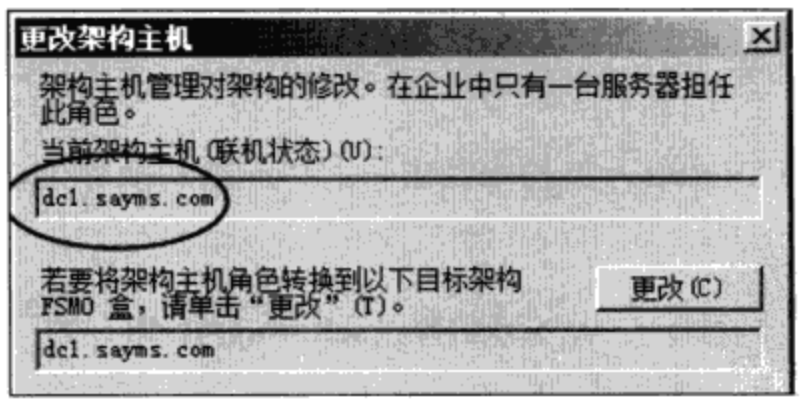


图 10-10

10-3-2 找出域命名操作主机

找出目前扮演**域命名操作主机**角色的域控制器的途径为：【开始➲管理工具➲ Active Directory域和信任关系➲如图 10-11所示对着**Active Directory域和信任关系**单击右键➲操作主机➲从图10-11中可知**域命名操作主机**为dc1.sayms.com】。

Download at http://www.pin5i.com/

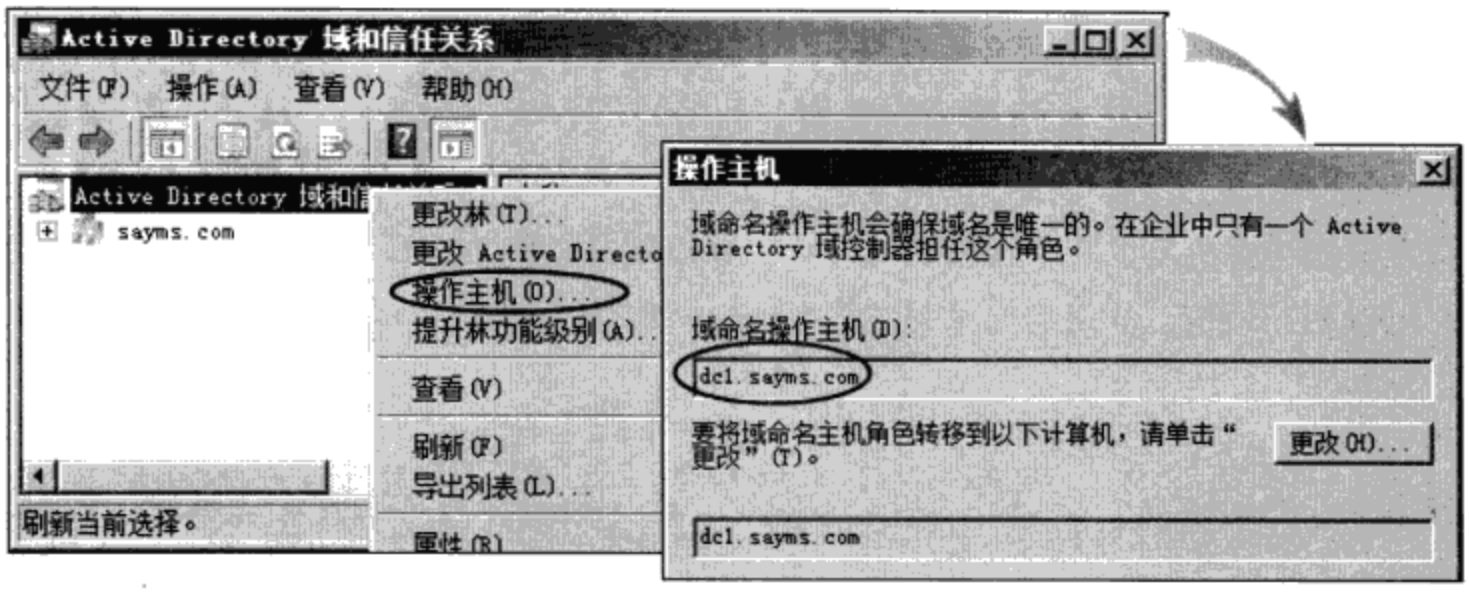


图 10-11

10-3-3 找出RID、PDC与基础结构操作主机

找出目前扮演这3个操作主机角色的域控制器的途径为：【开始➲管理工具➲ Active Directory用户和计算机➲如图 10-12所示对着域名（sayms.com）单击右键➲操作主机➲从弹出的对话框中可知扮演**RID操作主机**角色的域控制器为dc1.sayms.com】，您还可以从图中的**PDC**与**基础结构**标签来得知扮演这两个角色的域控制器。

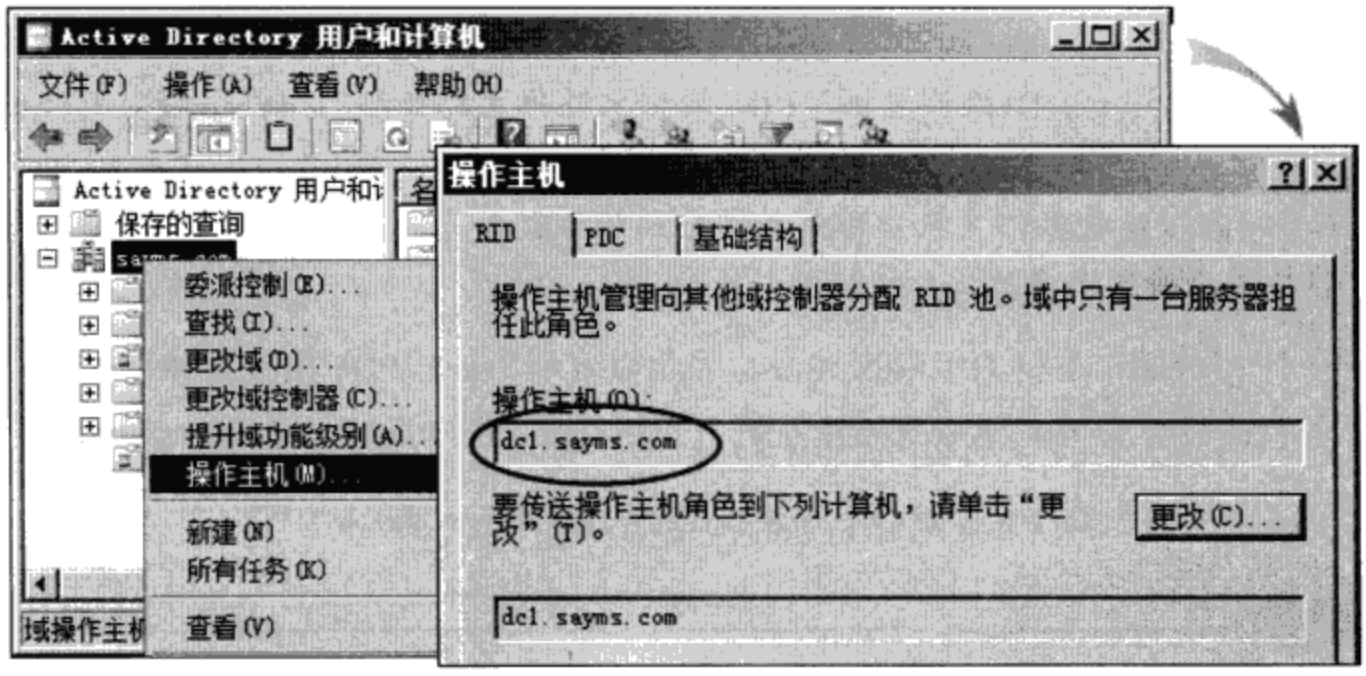


图 10-12

10-4 转移操作主机角色

在您新建AD DS域时，系统会自动选择域控制器来扮演操作主机，而在您要将扮演操作主机角色的域控制器降级为成员服务器时，系统也会自动将其操作主机角色转移到另外一台适当的域控制器，因此在大部分的情况下，您并不需要自行转移操作主机角色。

Download at http://www.pin5i.com/

不过有时候您可能需要自行转移操作主机角色，例如域架构更改或原来扮演操作主机角色的域控制器负荷太重，而您想要将其转移到另外一台域控制器，以便降低原操作主机的负荷。

请在将操作主机角色安全转移到另外一台域控制器之前，先确定两台域控制器都已经连上网络，可以相互通信，同时您必须是隶属于表 10-2中的组或被委派权限，才有权执行转移的工作。

表 10-2

角色	有权限的组
架构操作主机	Schema Admins
域命名操作主机	Enterprise Admins
RID操作主机	Domain Admins
PDC模拟器操作主机	Domain Admins
基础结构操作主机	Domain Admins

在执行安全转移动作之前，请注意以下事项：

- 转移角色的过程中并不会有数据丢失。
- 可以将林级别的**架构操作主机**与**域命名操作主机**转移到同一个林中的任何一台域控制器。
- 可以将域级别的**RID操作主机**与**PDC模拟器操作主机**转移到同一个域中的任何一台域控制器。
- 不要将**基础结构操作主机**转移到兼具**全局编录服务器**的域控制器，除非所有域控制器都是**全局编录服务器**或林中只有一个域。

转移任何一种操作主机的步骤都类似，因此以下利用转移**PDC模拟器操作主机**为例来进行说明，并且假设要将**PDC模拟器操作主机**由dc1.sayms.com转移到dc2.sayms.com。

STEP 1 选择【开始➲管理工具➲Active Directory用户和计算机】。

> **提示**
>
> 转移PDC模拟器操作主机、RID操作主机与基础结构操作主机都是使用Active Directory用户和计算机控制台，而转移架构操作主机是使用Active Directory架构控制台，转移域命名操作主机是使用Active Directory域和信任控制台。

STEP 2 如果您目前所连接的域控制器就是即将扮演操作主机的dc2.sayms.com（如图 10-13所示），则请跳到**STEP 5**，否则请继续以下的步骤。

Download at http://www.pin5i.com/

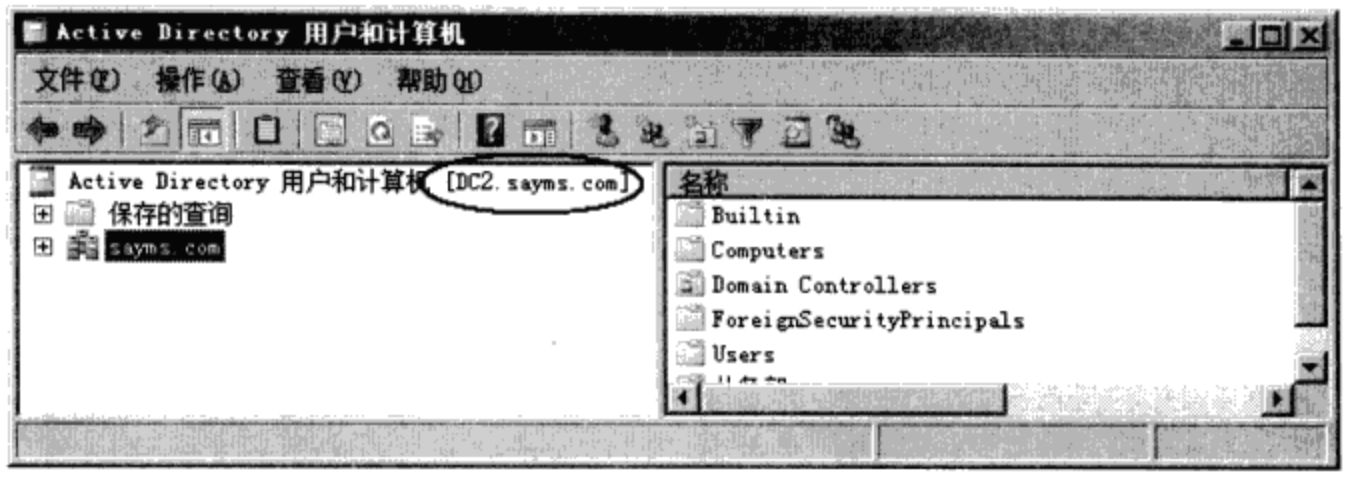


图 10-13

STEP 3 如图 10-14所示，通过【对着**Active Directory用户和计算机**单击右键➲更改域控制器】的方式进行操作（当前所连接到的域控制器为dc1.sayms.com）。

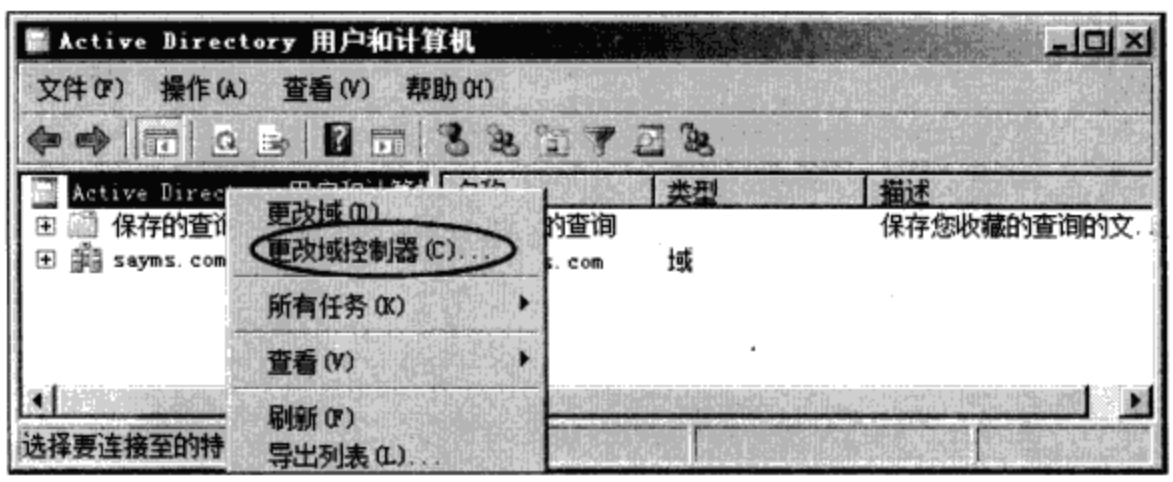


图 10-14

STEP 4 在图 10-15中选中即将扮演操作主机角色的域控制器dc2.sayms.com后，单击**确定**按钮。

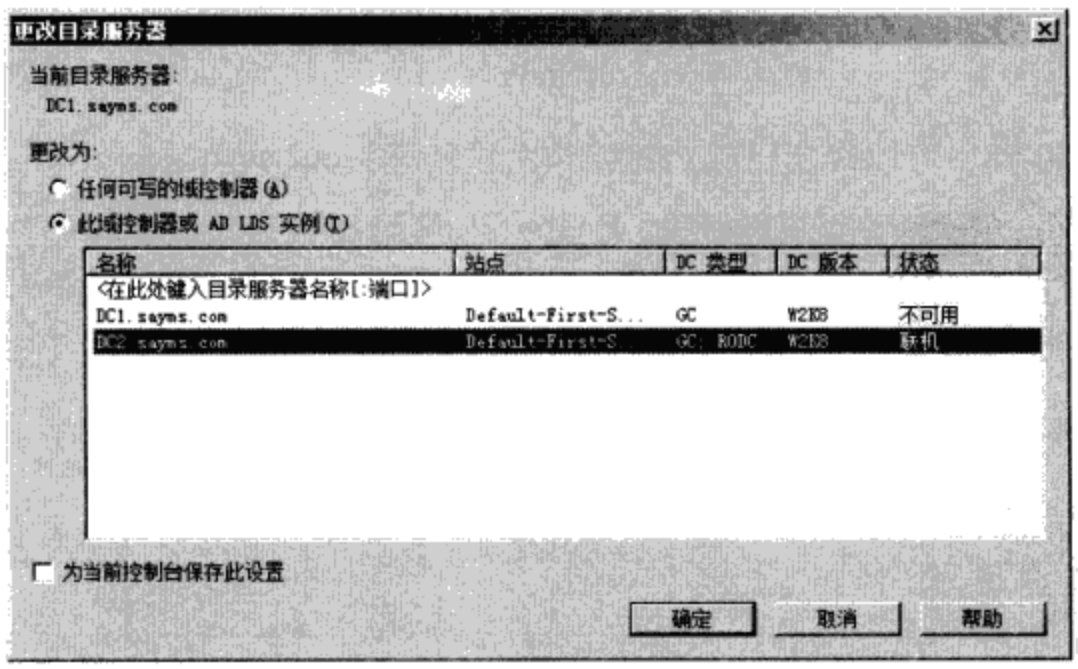


图 10-15

STEP 5 如图 10-16所示，通过【对着域名sayms.com单击右键➲操作主机】的方式进行操作。

Download at http://www.pin5i.com/

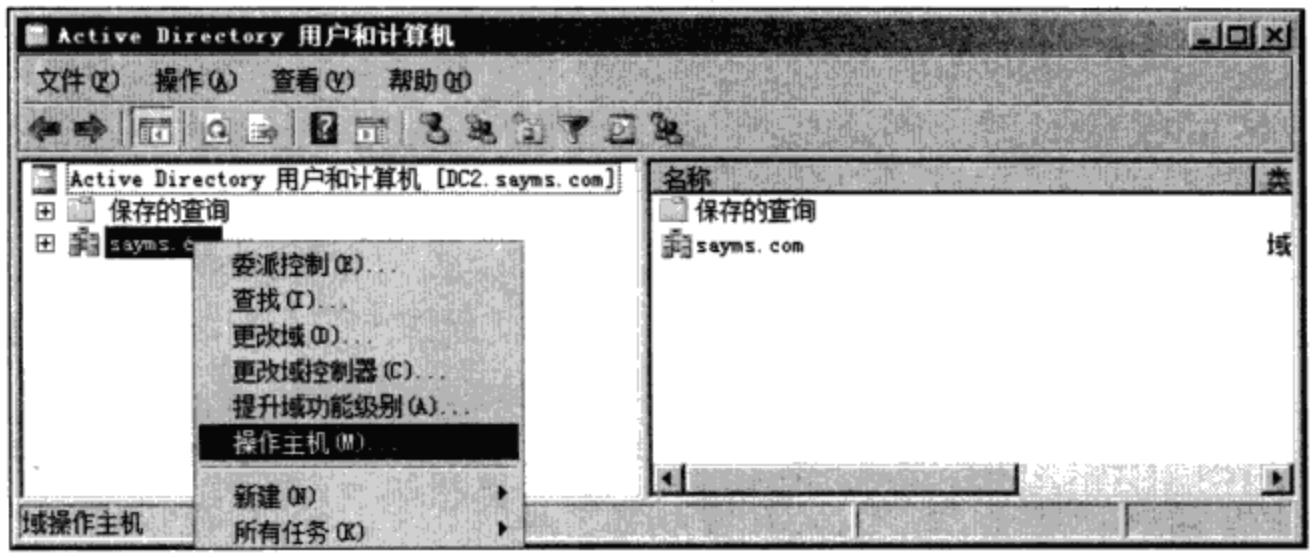


图 10-16

STEP 6 如图10-17所示，通过【单击**PDC**标签➲确认目前所连接的域控制器是dc2.sayms.com➲单击更改按钮➲单击是（Y）按钮➲单击确定按钮】的方式进行操作。

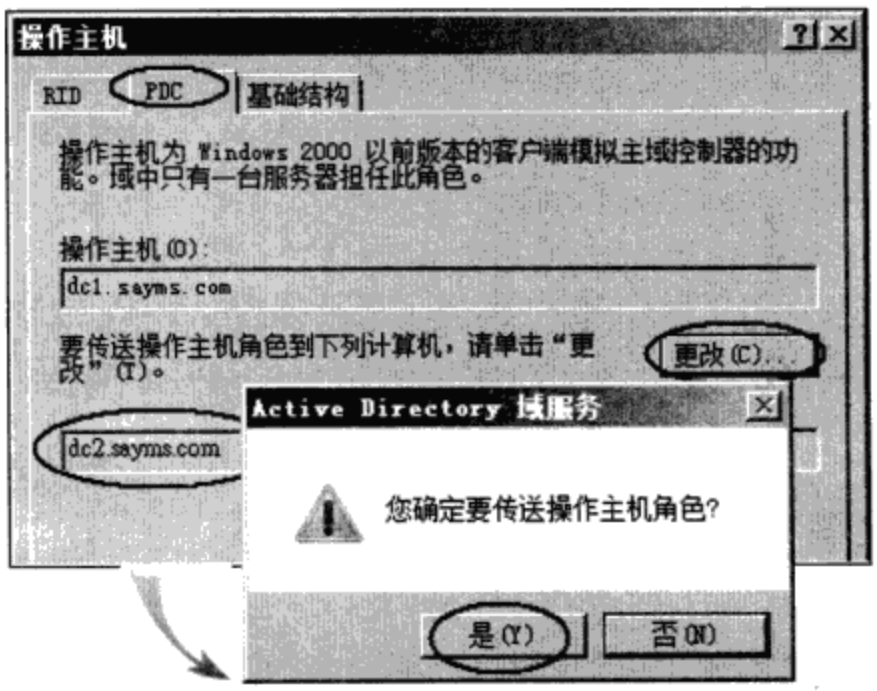


图 10-17

STEP 7 从图 10-18中可以确定已成功将操作主机转移到dc2.sayms.com。

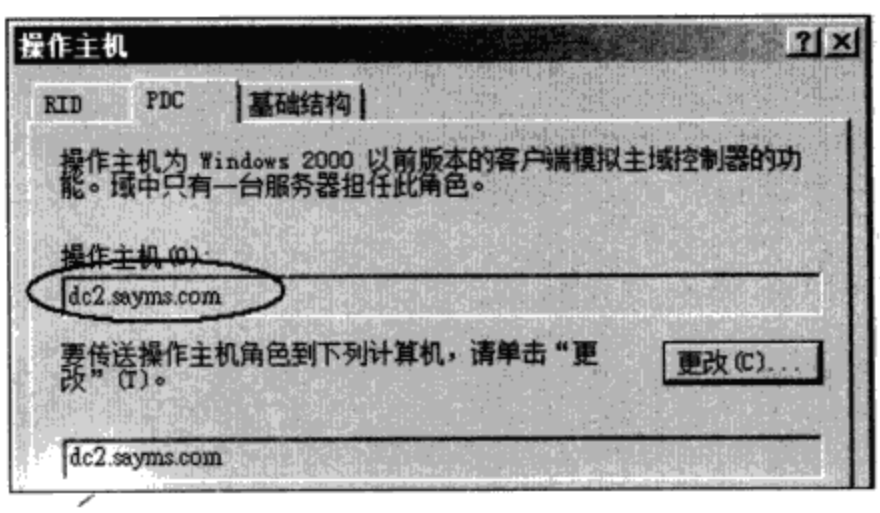


图 10-18

Download at http://www.pin5i.com/

10-5 夺取操作主机角色

如果扮演操作主机角色的域控制器故障或网络有问题时，则您可能需要采用**夺取**（Seize）的方式来将操作主机角色强迫转移到另外一台域控制器。



注意

只有在无法安全转移的情况下，才使用夺取的方法。

10-5-1 操作主机关机所造成的影响

有的操作主机故障时，短时间内就会对网络造成明显的影响，然而有的却不会，因此请参考以下说明来决定是否要尽快夺取操作主机角色。

由于新操作主机是根据其内的Active Directory数据库来运行，因此为了减少数据丢失，请在执行夺取步骤之前等待一段时间（至少等所有域控制器之间完成一次Active Directory复制所需的时间），让这台即将成为新操作主机的域控制器完整接收到从其他域控制器复制来的变动数据。

由于夺取操作主机时并未与原操作主机通信协调，因此一旦夺取操作主机角色后，请不要再启动原扮演操作主机角色的域控制器，否则会出现两台域控制器都各自认为是操作主机，因而会影响到AD DS的运行，严重的话，可能会损毁Active Directory数据库。



注意

一旦**架构操作主机**、**域命名操作主机**或**RID操作主机**的角色被夺取后，请**永远不要**将原来扮演这些操作主机角色的域控制器再连接到网络上。建议将这台域控制器的硬盘格式化。

1. 架构操作主机关机时

由于用户并不会直接与**架构操作主机**通信，因此若**架构操作主机**暂时无法提供服务的话，对用户并没有影响；而对系统管理员来说，除非他们需要访问架构内的数据，例如要安装一个会修改架构的应用程序（例如Microsoft Exchange Server），否则也暂时不需要使用到**架构操作主机**，所以请等**架构操作主机**修复后重新上线即可，不需要执行夺取的步骤。

如果**架构操作主机**关机的时间太久，以致于影响到系统运行时，则您应该夺取操作主机角色，以便改由另外一台域控制器来扮演。由于夺取是非常的手段，因此请确认有其必要性后，再执行夺取的步骤。

Download at http://www.pin5i.com/

2. 域命名操作主机关机时

域命名操作主机暂时无法提供服务的话，对网络用户并没有影响，而对系统管理员来说，除非他们要添加或删除域，否则也暂时不需要使用到**域命名操作主机**，所以请等**域命名操作主机**修复重新上线即可，不需要执行夺取的步骤。

如果**域命名操作主机**关机的时间太久，以致于影响到系统运行时，则您应该夺取操作主机角色，改由另外一台域控制器来扮演。由于夺取是非常的手段，因此请确认有其必要性后，再执行夺取的步骤。

3. RID 操作主机关机时

RID操作主机暂时无法提供服务，对网络用户并没有影响，而对系统管理员来说，除非他们要在域内新建对象，同时他们所使用的域控制器之前所索取的RID已经用完，否则也暂时不需要使用到**RID操作主机**，所以可以不需要执行夺取的步骤。

如果**RID操作主机**关机的时间太久，以致于影响到系统运行时，则您应该夺取操作主机角色，改由另外一台域控制器来扮演。由于夺取是非常的手段，因此请确认有其必要性后，再执行夺取的步骤。

4. PDC 模拟器操作主机关机时

由于**PDC模拟器操作主机**无法提供服务时，网络用户可能会很快察觉到，例如旧客户端将因为无法与**PDC模拟器操作主机**通信而不能更改密码。若密码已经过期，也会因为无法更改密码而无法登录，因此您应该尽快修复**PDC模拟器操作主机**，若无法在短期内修复的话，则需要尽快执行夺取步骤。

PDC模拟器操作主机的角色被夺取后，若原来扮演**PDC模拟器操作主机**的域控制器修复后，还是可以连接到网络上，不过因为角色已被夺取，故它会自动放弃**PDC模拟器操作主机**角色。它会通过从其他域控制器复制来的Active Directory变动数据得知扮演新**PDC模拟器操作主机**角色的域控制器。您还是可以将角色再转移到原来的域控制器。

5. 基础结构操作主机关机时

基础结构操作主机暂时无法提供服务的话，对网络用户并没有影响，而对系统管理员来说，除非他们最近搬移大量账户或改变大量账户的名称，否则也不会察觉到**基础结构操作主机**已经关机，所以暂时可以不需要执行夺取的步骤。

若**基础结构操作主机**关机的时间太久，以致于影响到系统运行时，则应该夺取操作主机角色，改由另外一台不是**全局编录服务器**的域控制器来扮演。

基础结构操作主机的角色被夺取后，若原来扮演**基础结构操作主机**的域控制器修复后，

Download at http://www.pin5i.com/

还是可以连接到网络上，不过因为角色已被夺取，故它会自动放弃**基础结构操作主机**角色。它会通过从其他域控制器复制来的Active Directory变动数据得知扮演新**基础结构操作主机**角色的域控制器。您还是可以将角色再转移到原来的域控制器。

10-5-2 夺取操作主机角色实例演练一

我们利用以下的范例来解说如何夺取操作主机角色，以便让域能够继续正常的运行。

> **注意**
>
> 只有在无法利用**转移**方法的情况下，才使用**夺取**方法。您必须是隶属于适当的组才可以执行**夺取**的操作（参见表 10-2）。

假设网络内只有一个域，而且是采用默认值，也就是说5 个操作主机角色都是由默认的第1台域控制器所扮演，如图 10-19所示的dc1.sayms.com，现在这台域控制器却因故永远无法使用了，因此您需要夺取这5个操作主机角色，改由另外一台域控制器来扮演，如图中的dc2.sayms.com。

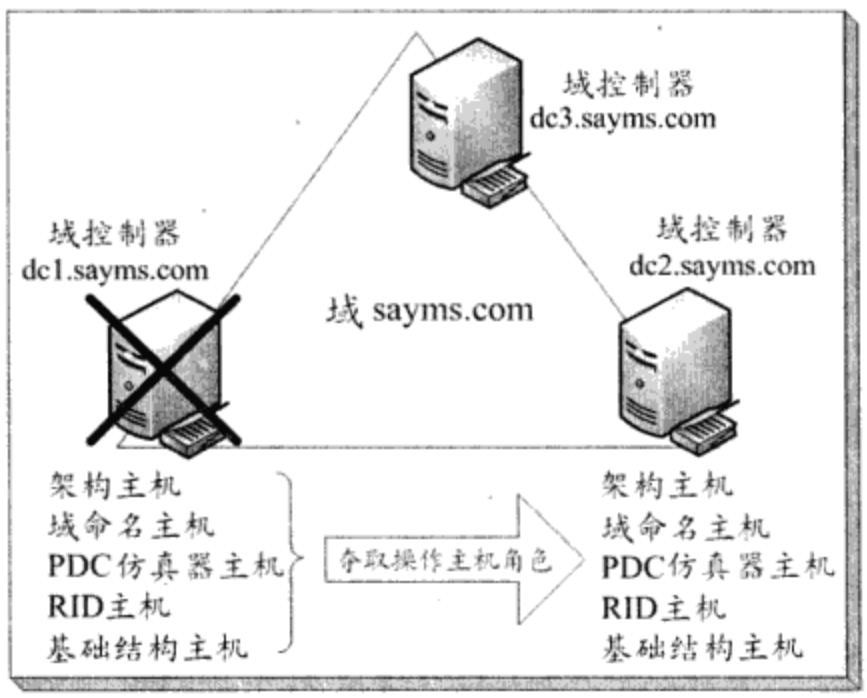


图 10-19

STEP 1 到一台仍然正常的域控制器上利用域系统管理员身份登录。

STEP 2 选择【开始➲命令提示符】或单击左下角的**Windows PowerShell**图标，然后执行命令ntdsutil。

STEP 3 在ntdsutil提示符下，执行命令roles。

> **提示**
>
> 您可以在每一个提示字符下利用 **?** 来查询命令的用法。

Download at http://www.pin5i.com/

STEP 4 在fsmo maintenance提示符下，执行命令connections。

> **提示**
>
> 您所输入的命令都可以缩写，例如connections可缩写为conn、con或co，一直到系统无法识别为止。

STEP 5 在server connections提示符下，执行以下命令来连接到要扮演操作主机角色的域控制器（例如dc2.sayms.com）：connect to server dc2.sayms.com。

STEP 6 在server connections提示符下，执行以下命令：quit。

> **提示**
>
> 若要查询目前扮演5大操作主机的域控制器的话，请在此时输入select operation target，然后输入list roles for connected server，查询完成后输入quit命令。

STEP 7 在fsmo maintenance提示符下，执行命令：seize pdc。

STEP 8 当出现如图 10-20所示的界面时单击 是（Y） 按钮。

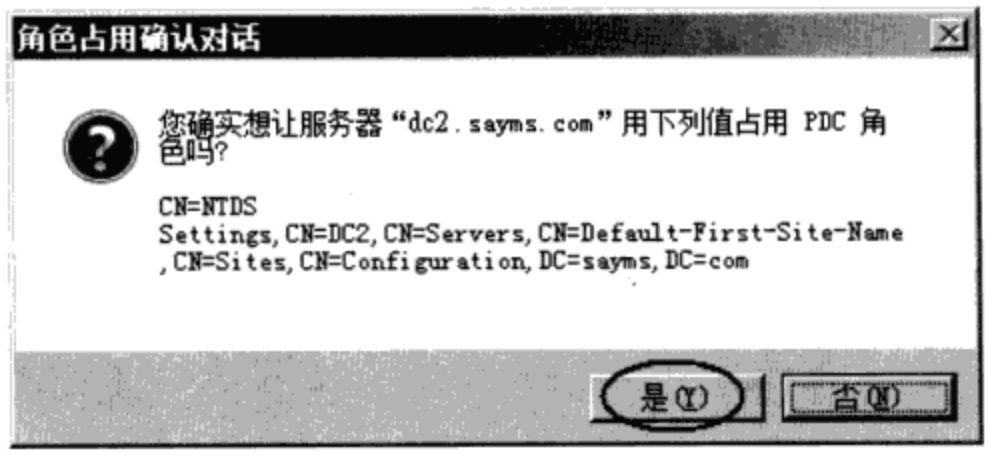


图 10-20

STEP 9 图 10-21为前面几个步骤的完整过程，图中系统会先尝试转移角色，若失败再夺取。从图中可知已经成功夺取**PDC模拟器操作主机**的角色，并改由域控制器dc2.sayms.com来扮演。

Download at http://www.pin5i.com/

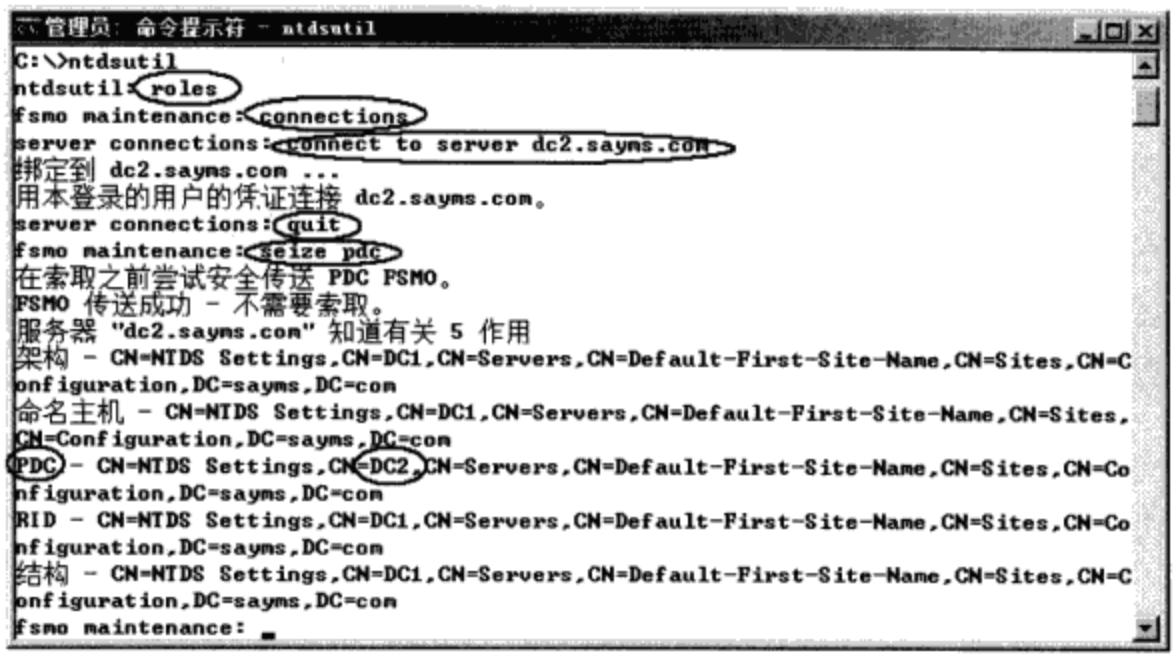


图 10-21

STEP 10 请继续执行以下4个命令来夺取其他4个操作主机角色：

```
seize schema master
seize naming master
seize RID master
seize infrastructure master
```

注意

一旦**架构操作主机**、**域命名操作主机**或**RID操作主机**的角色被夺取后，请**永远不要**将原来扮演这些操作主机角色的域控制器再连接到网络上，建议将这台域控制器的硬盘格式化。

10-5-3 夺取操作主机角色实例演练二

假设网络内只有一个域，而且是采用默认值，也就是5个操作主机角色都是由默认的第1台域控制器所扮演，如图 10-22所示中的dc1.sayms.com。

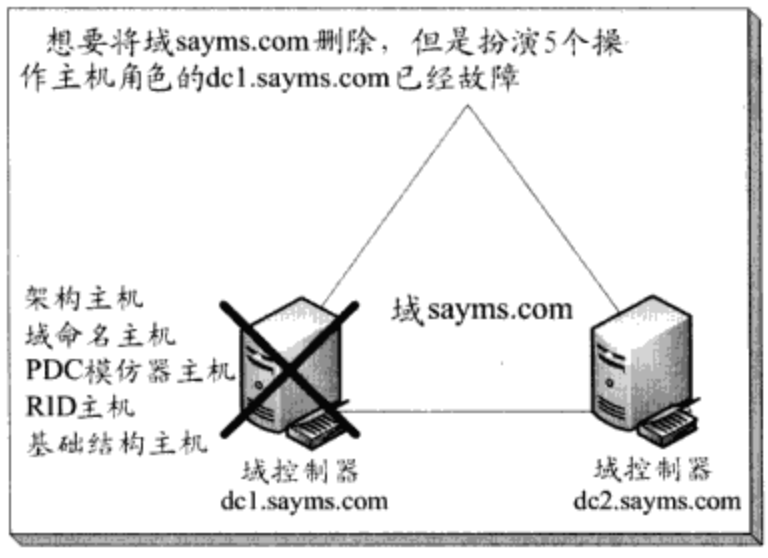


图 10-22

Download at http://www.pin5i.com/

现在扮演这5个操作主机角色的域控制器dc1.sayms.com却因故障永远无法使用，此时想要将此域删除，也就是要将AD DS从第2台域控制器dc2.sayms.com内删除。

若希望能够保留dc2.sayms.com内的Windows Server 2008 R2操作系统，也就是并没有要重新安装Windows Server 2008 R2操作系统，因此想要采用降级的方式来删除第2台域控制器dc2.sayms.com内的AD DS，但是却失败，因为在执行降级程序时，无论在图10-23中是否选择**删除该域，因为此服务器是该域中的最后一个域控制器**复选框，都无法将dc2.sayms.com降级。

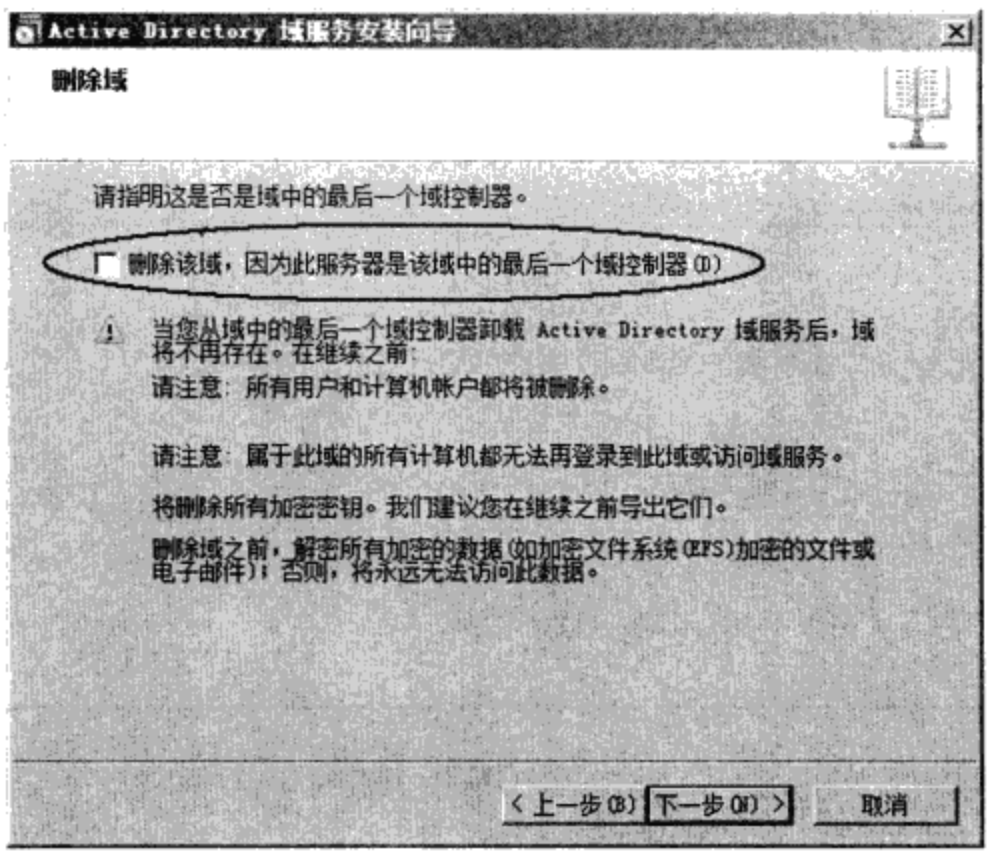


图10-23

若您选择**删除该域，因为此服务器是该域中的最后一个域控制器**复选框的话，则会出现如图 10-24所示的对话框，因为在Active Directory数据库中记录着还有另外一台域控制器dc1.sayms.com存在。

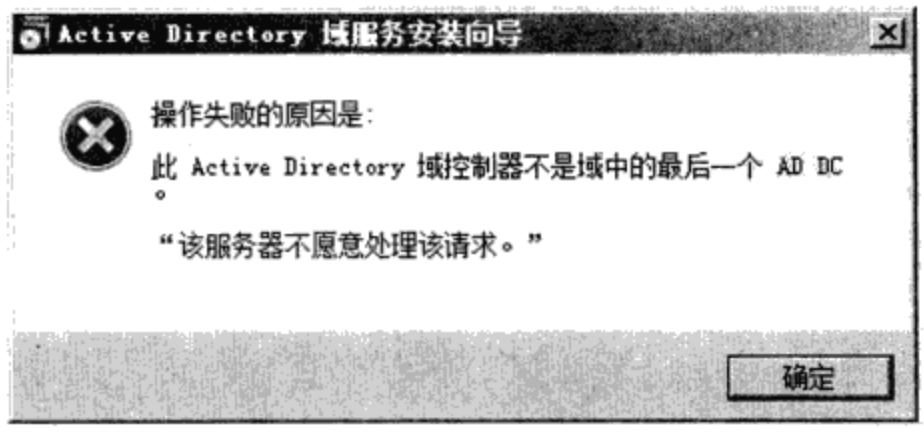


图10-24

若您不选择**删除该域，因为此服务器是该域中的最后一个域控制器**复选框的话，则会出现如图 10-25所示的对话框，因为系统找不到另外一台域控制器dc1.sayms.com。

Download at http://www.pin5i.com/

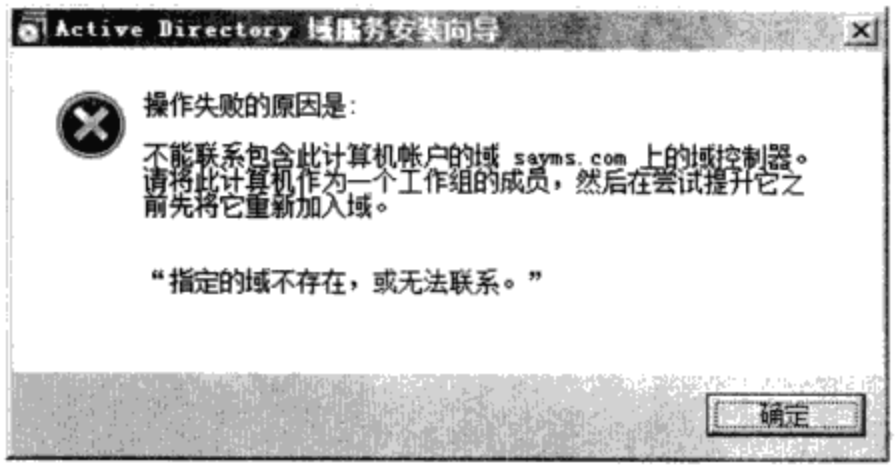


图 10-25

此时您可以通过执行**dcpromo /forceremoval**命令来强制将AD DS从域控制站dc2.sayms.com内删除。

也可以先利用**Active Directory站点和服务**将域控制器dc1.sayms.com的**NTDS Setting**删除，然后再执行**dcpromo**来将AD DS从域控制器dc2.sayms.com内删除，这种方法的步骤如下所示。

STEP 1 选择【开始➲管理工具➲Active Directory站点和服务➲如图 10-26所示展开到DC1➲单击**NTDS Setting**➲单击上方的**删除**图标➲在弹出的对话框中单击 是(Y) 按钮】。



图 10-26

STEP 2 选择图 10-27中的选项后单击 删除 按钮。

Download at http://www.pin5i.com/

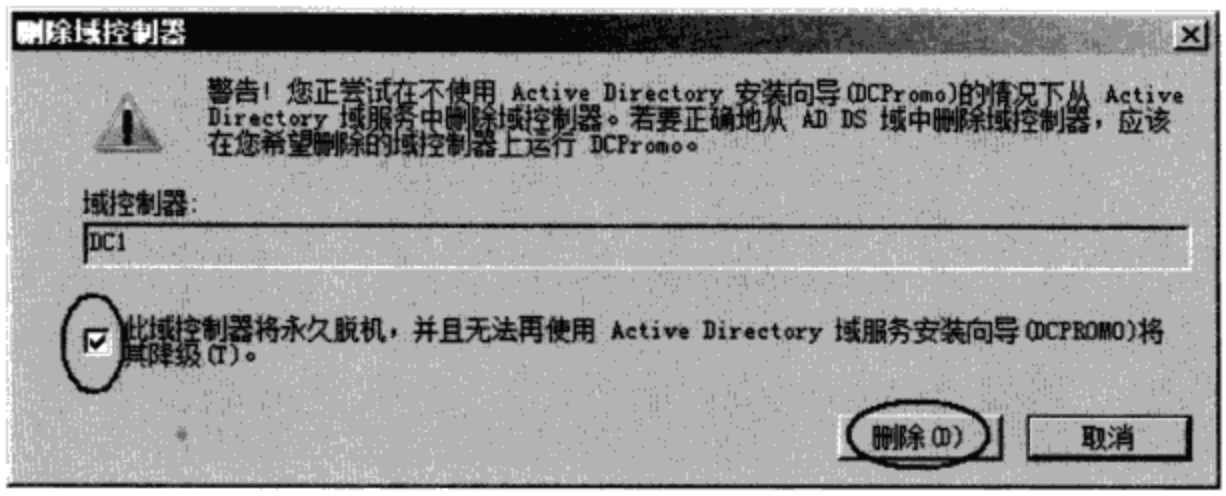


图 10-27

STEP 3 若出现图 10-28的话，表示此域控制器是**全局编录服务器**，请单击是（Y）按钮。

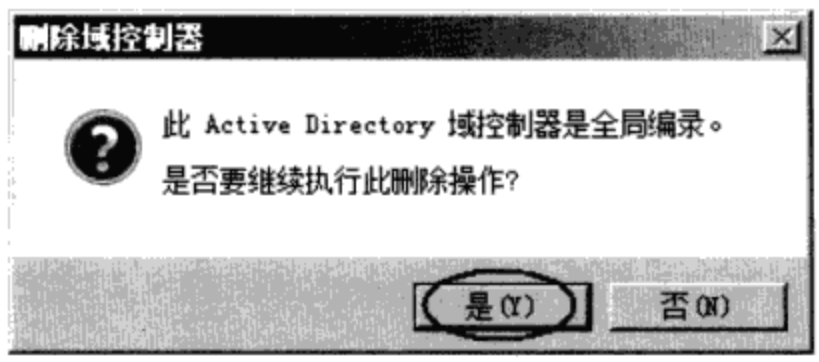


图 10-28

STEP 4 在图 10-29中单击确定按钮，以便将原本由dc1.sayms.com所扮演的5个操作主机角色移动到dc2.sayms.com。

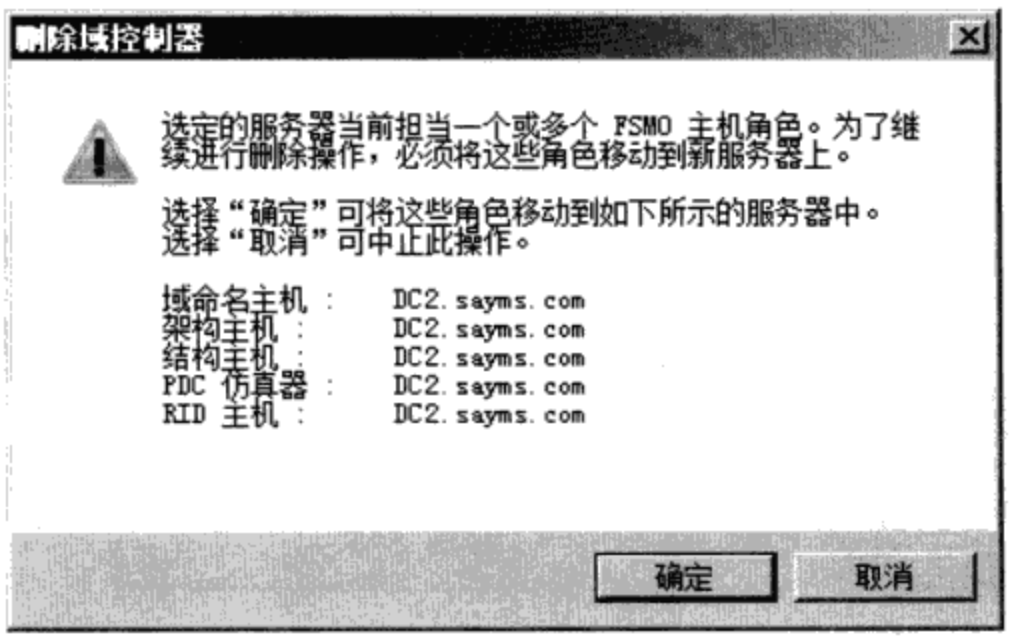


图 10-29

STEP 5 执行**dcpromo.exe**命令来将AD DS从域控制器dc2.sayms.com内删除（降级），并在图10-23中选择**删除该域，因为此服务器是该域中的最后一个域控制器**复选框，降级完成后，此域也会被删除。

Download at http://www.pin5i.com/

第11章

AD DS的维护

为了保证域环境的正常运行，应该定期备份AD DS（Active Directory域服务）的相关数据。同时为了保持AD DS的运行性能，也应该充分了解Active Directory数据库。

- 系统状态概述
- 备份AD DS
- 还原AD DS
- Active Directory数据库的转移与重新整理
- 重设**目录服务还原模式**的系统管理员密码
- 更改**可重新启动的AD DS**的登录设置
- Active Directory回收站



Download at http://www.pin5i.com/

11-1 系统状态概述

Windows Server 2008 R2服务器的系统状态（System State）内所包含的数据，视服务器所安装的角色种类而有所不同，例如其内可能包含着以下的数据。

- 注册值。
- COM+ 类别注册数据库（Class Registration Database）。
- 启动文件（Boot Files）。
- Active Directory证书服务（AD CS）数据库。
- Active Directory数据库（Ntds.dit）。
- SYSVOL文件夹。
- 群集服务信息。
- Microsoft Internet Information Services（IIS） metadirectory。
- 受Windows Resource Protection保护的系统文件。

11-1-1 Active Directory数据库

AD DS内的组件主要分为Active Directory数据库文件与SYSVOL文件夹，其中Active Directory数据库文件默认是位于%systemroot%\NTDS文件夹内，如图 11-1所示。

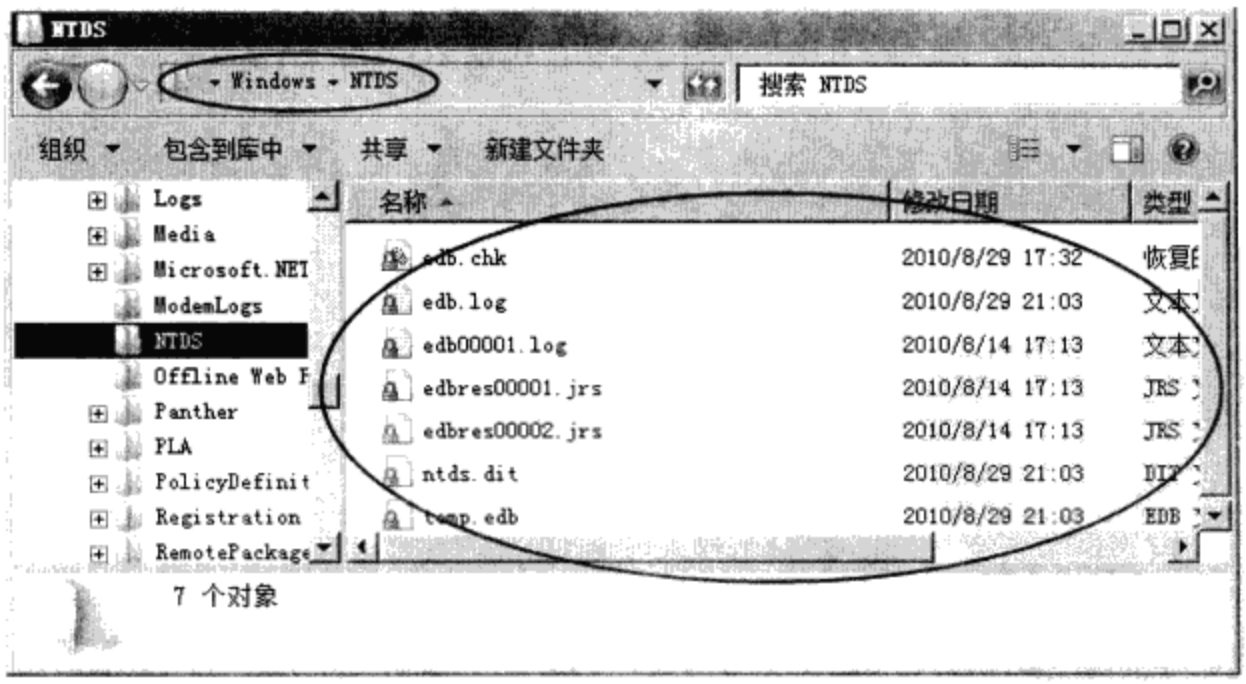


图 11-1

- ntds.dit: 是Active Directory数据库文件，存储着这台域控制器的Active Directory内的对象。
- edb.log: ebd.log是Active Directory事务日志（扩展名.log默认会被隐藏），容量大小为

Download at http://www.pin5i.com/

10 MB。当您要更改Active Directory内的对象时，系统会先将变动数据写入到内存（RAM）内，然后等系统空闲或关机时，再根据内存内的记录来将更新数据写入Active Directory数据库（ntds.dit）。这种先在内存内处理的方式，可以提高Active Directory的运行效率。系统也会将内存内的数据变动过程写到事务日志内（edb.log），若系统不正常关机（例如断电），以致于内存内尚未被写入，Active Directory数据库的更新数据丢失时，系统就可以根据事务日志来推算出不正常关机前，在内存内的更新记录，并将这些记录写入Active Directory数据库。如果事务日志填满了数据，则系统会将其更名，例如Edb00001.log，Edb00002.log，……，并重新新建一个事务日志。

- edb.chk：它是**检查点**（Check Point）文件。每一次系统将内存内的更新记录写入Active Directory数据库时，都会一并更新edb.chk，它会记载事务日志的检查点。如果系统不正常关机，以致于内存内尚未被写入，Active Directory数据库的更新记录丢失的话，则下一次开机时，系统便可以根据edb.chk来得知需从事务日志内的哪一个变动过程开始，来推算出不正常关机前内存内的更新记录，并将它们写入Active Directory数据库。
- edbres00001.jrs与edbres00002.jrs：这两个是预留文件，未来如果硬盘的空间不够时可以使用这两个文件，每一个文件都是10 MB。

11-1-2 SYSVOL文件夹

SYSVOL文件夹是位于**%systemroot%**内，此文件夹内存储着以下的数据：**脚本文件**（Scripts）、**NETLOGON共享文件夹**、**SYSVOL共享文件夹**与**组策略相关配置**。

11-2 备份AD DS

您应该定期备份域控制器的系统状态，以便在域控制器的AD DS损毁时，可以通过备份数据来还原域控制器。

11-2-1 安装Windows Server Backup功能

首先您需要添加Windows Server Backup功能：【单击左下角的**服务器管理器**图标➲单击**功能**➲单击右边的**添加功能**➲展开图 11-2中的Windows Server Backup功能➲选择图中的Windows Server Backup复选框➲单击下一步按钮、安装按钮】。

Download at http://www.pin5i.com/

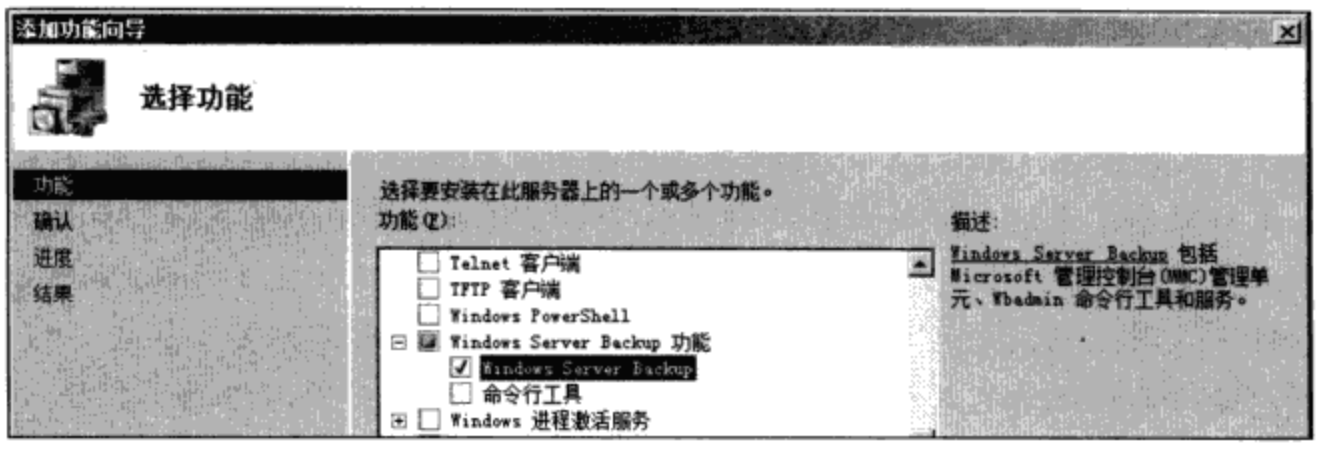


图 11-2

提示

如果您想要利用Windows PowerShell所提供的命令来编写脚本（Scripts），以便通过此脚本来执行备份工作的话，请选中图中的**命令行工具**复选框。

11-2-2 备份系统状态

我们将通过备份**系统状态**的方式来备份AD DS，系统状态的文件是位于安装Windows Server 2008 R2的磁盘内，一般是C磁盘，这个磁盘我们将它称为备份的源磁盘，然而备份目标磁盘默认是不可以包含源磁盘，所以您无法将系统状态备份到源磁盘C，因此您需将其备份到另外一个磁盘、DVD或其他计算机内的共享文件夹。必须隶属于Administrators或Backup Operators组才有权限执行备份系统状态的工作，而且必须有权限将数据写入目标磁盘或共享文件夹。

提示

若要开放可以备份到源磁盘的话，请在以下注册路径中添加一条名称为AllowSSBToAnyVolume的数值，其类型为DWORD：

```
HKLM\SYSTEM\CurrentControlSet\Services\wbengine\SystemStateBackup
```

其值为1表示开放，为0表示禁止。建议不要开放，否则可能会备份失败，而且需要使用比较多的磁盘空间。

以下假设我们要将系统状态数据备份到网络共享文件夹**\\dc2\backup**内（请先在dc2计算机上新建此共享文件夹）：

STEP 1 选择【开始➲管理工具➲Windows Server Backup➲如图 11-3所示单击**一次性备份…**】。

Download at http://www.pin5i.com/

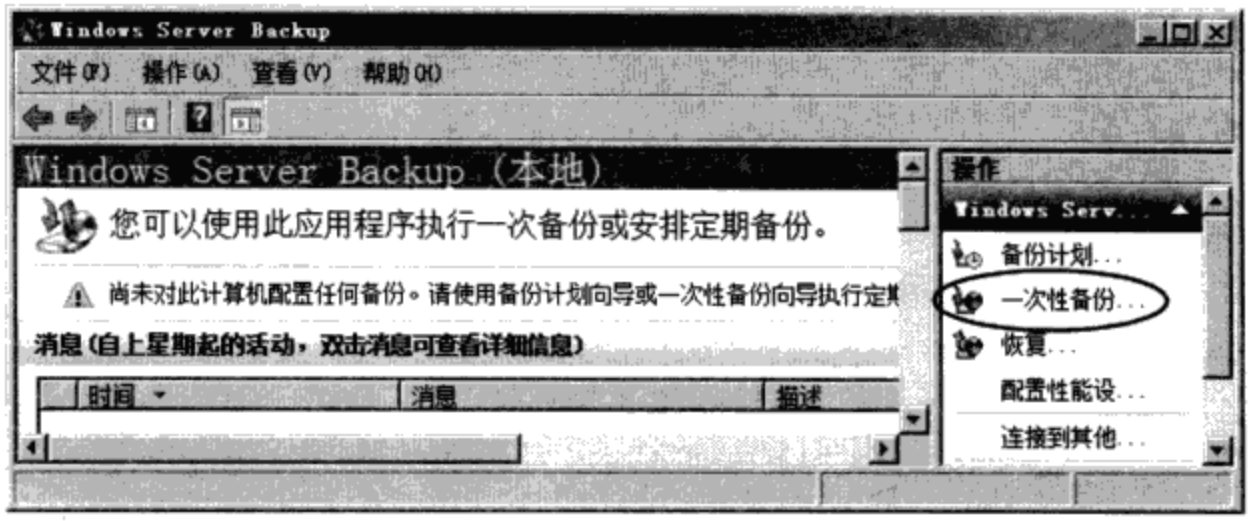


图 11-3

STEP 2 如图 11-4所示选择**其他选项**单选按钮后单击下一步按钮。

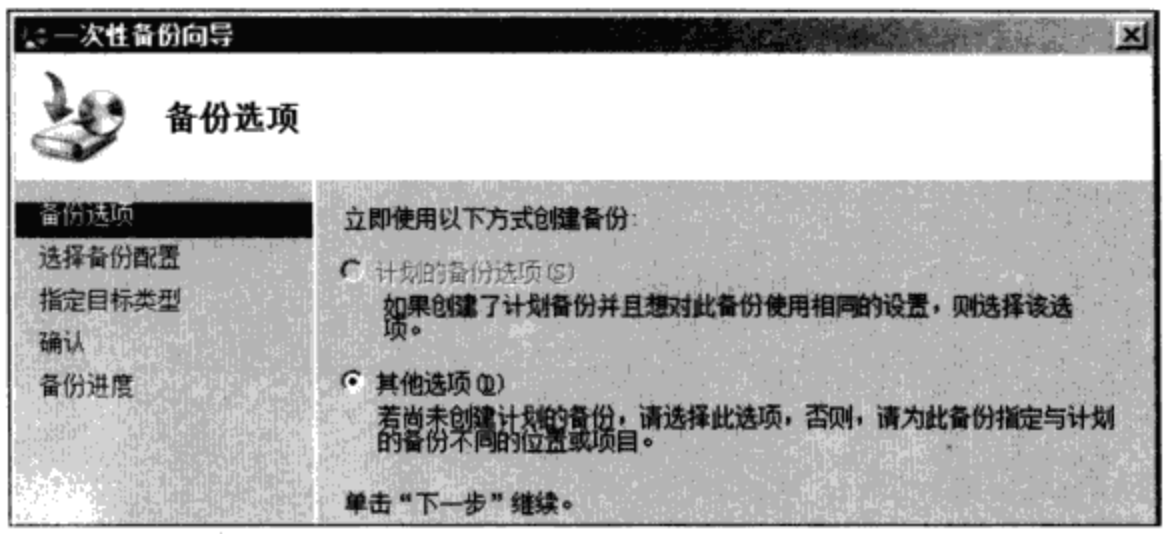


图 11-4

STEP 3 在图 11-5中选择**自定义**单选按钮后单击下一步按钮。

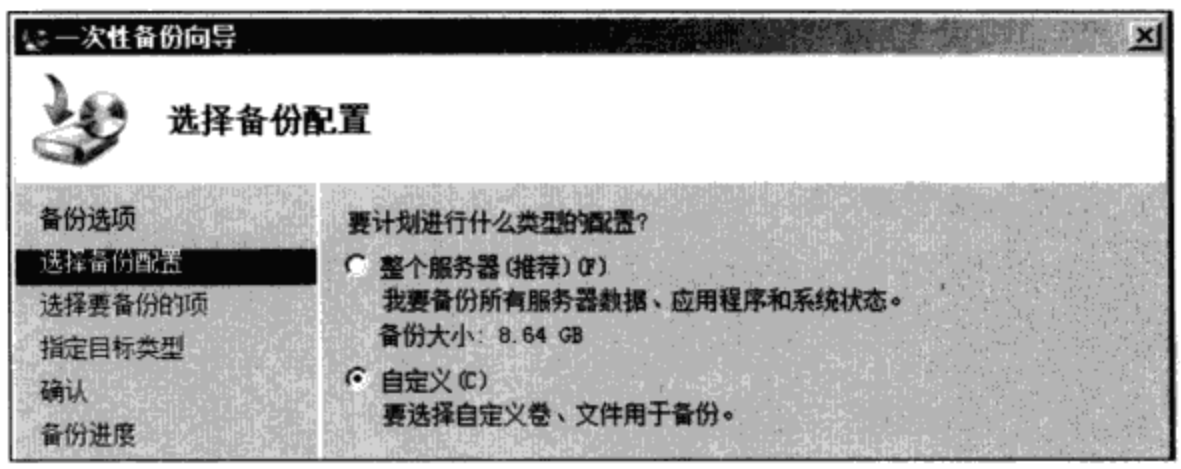


图 11-5

提示

您也可以通过选择**整个服务器**单选按钮的方式来备份整台域控制器内的所有数据，它包含系统状态。

STEP 4 如图 11-6所示单击添加项按钮。

Download at http://www.pin5i.com/

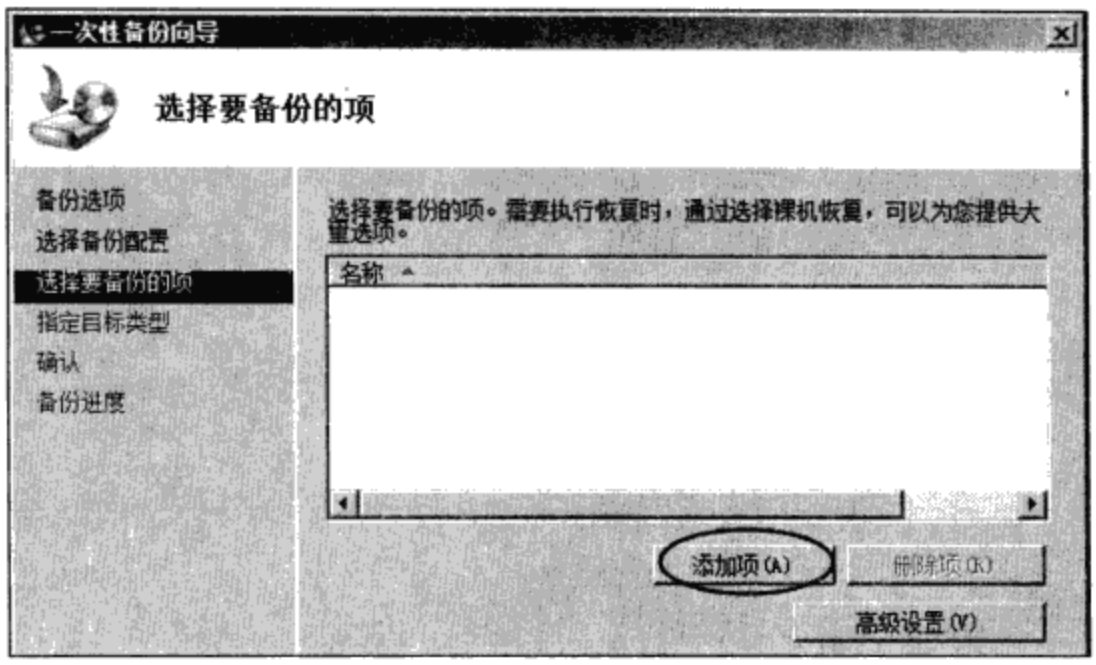


图 11-6

STEP 5 如图 11-7所示选择**系统状态**复选框后单击确定按钮。

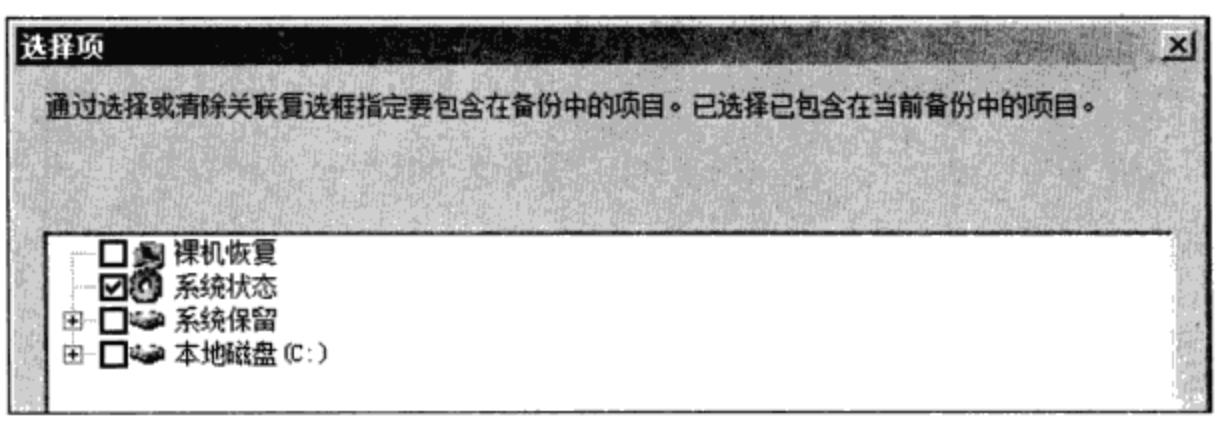


图 11-7

STEP 6 返回到**选择要备份的项**对话框后单击下一步按钮。

STEP 7 如图 11-8所示选择**远程共享文件夹**单选按钮后，单击下一步按钮。

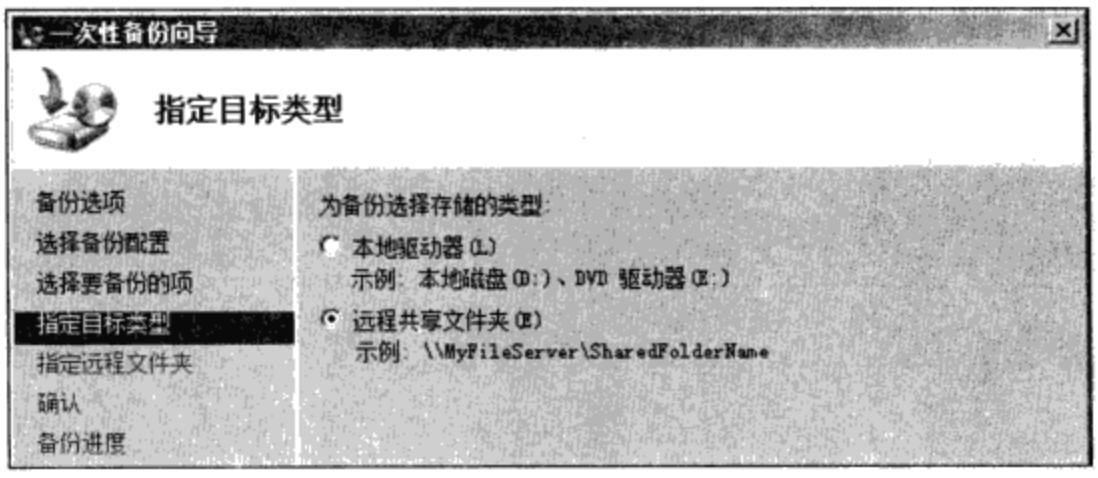


图 11-8

STEP 8 如图 11-9所示，在**位置**文本框中输入**\\dc2\backup**后单击下一步按钮。

Download at http://www.pin5i.com/

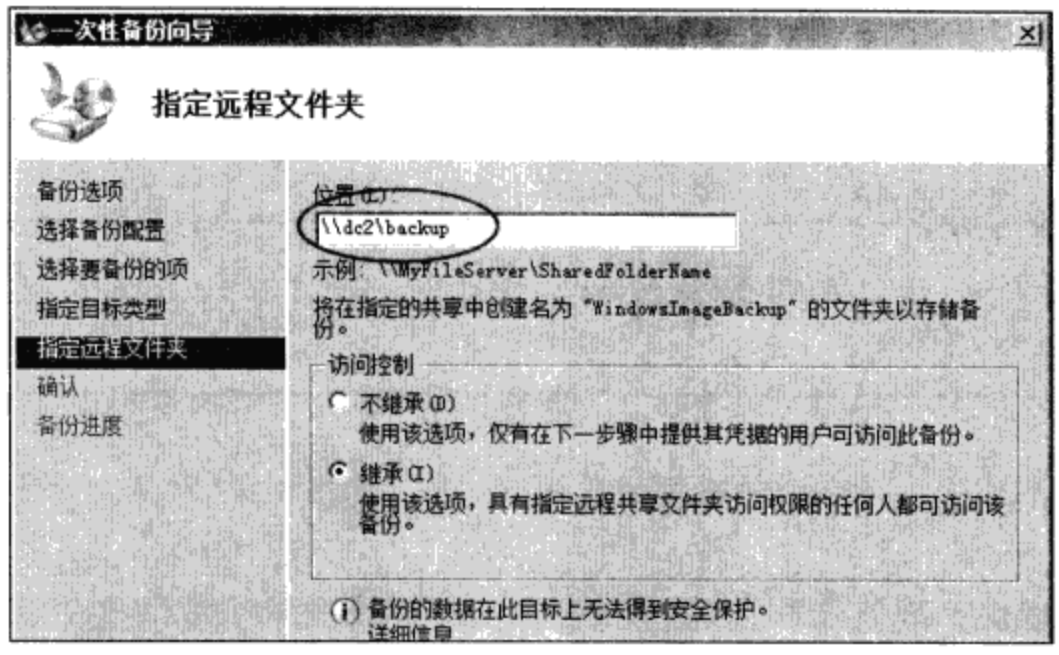


图 11-9

STEP 9 在**确认**对话框中单击备份按钮。

提示

您也可以通过**wbadmin**命令来备份系统状态，例如：

```
wbadmin start systemstatebackup -backuptarget:\\dc2\backup
```

此范例假设是要备份到网络共享文件夹**\\dc2\backup**。

11-3 还原AD DS

在系统状态备份完成后，若AD DS数据损毁的话，您就可以通过执行**非授权还原**（Nonauthoritative Restore）的程序来修复AD DS。您必须进入**目录服务还原模式**（Directory Services Restore Mode，DSRM），然后利用之前的备份来执行**非授权还原**的工作。

提示

若系统无法启动的话，则您应该运行完整服务器的还原程序，而不是执行**非授权还原**程序。

11-3-1 进入目录服务还原模式的方法

您可以通过按F8键或运行Bcdedit.exe两种方式来进入**目录服务还原模式**。

1. 按 F8 键进入目录服务还原模式

操作步骤如下：

Download at http://www.pin5i.com/

STEP 1 将域控制器重新启动，并在完成自我测试后、系统启动初期立刻按F8键（多按几次，以免错过可按F8键的时机）。

提示

若计算机内安装了多个Windows系统的话，则您可以在出现操作系统选择列表（默认会等待30s）时再按F8键。

STEP 2 如图 11-10所示选择**目录服务还原模式**后按Enter键，之后将出现**目录服务还原模式**的登录界面。

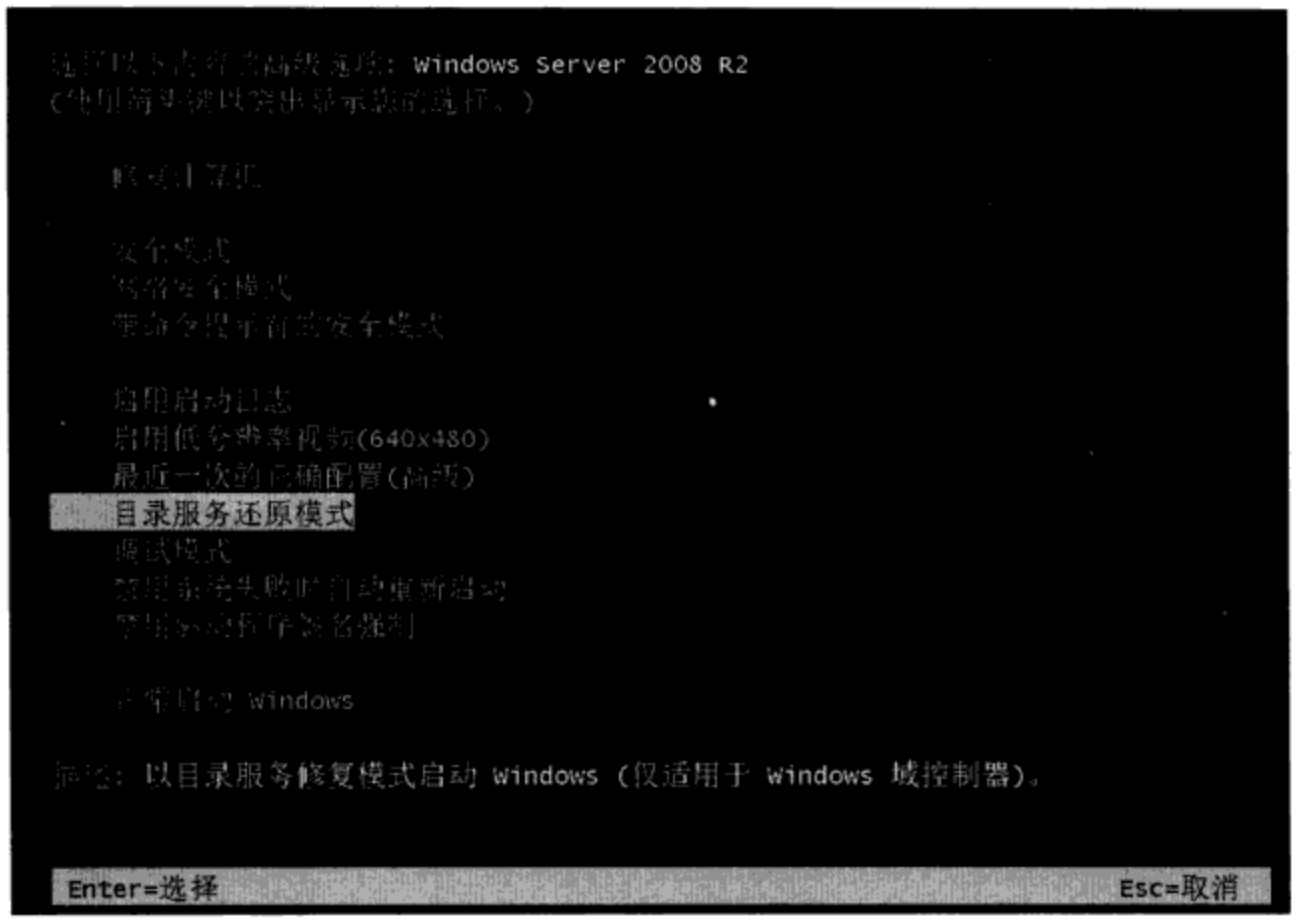


图 11-10

STEP 3 请执行AD DS的**非授权还原**。

2. 执行 Bcdedit.exe 程序进入目录服务还原模式

虽然可以通过按F8键的方式来进入**目录服务还原模式**，但是却不容易抓住按F8键的时机，而通过Bcdedit.exe程序就可以避免此困扰。

STEP 1 打开命令提示符窗口或单击左下角的Windows PowerShell图标，然后输入以下命令：**bcdedit /set safeboot dsrepair**。

STEP 2 重新启动计算机，之后将出现**目录服务还原模式**的登录界面。

Download at http://www.pin5i.com/

提示

以后启动计算机时，都会出现**目录服务还原模式**的登录界面，因此在您完成AD DS还原程序后，请在**命令提示符**窗口下执行以下命令：

```
bcdedit  /deletevalue  safeboot
```

重新启动计算机时，便会重新以一般模式来启动系统。

STEP 3 请继续执行AD DS的非授权还原步骤。

11-3-2 执行AD DS的非授权还原

接下来需要利用**目录服务还原模式**的系统管理员账户与密码登录，并执行AD DS的标准还原程序，也就是**非授权还原**。以下假设之前制作的系统状态备份是位于网络共享文件夹**\\dc2\backup**内。

STEP 1 请在**目录服务还原模式**的登录界面中单击切换用户按钮，单击其他用户按钮，然后如图 11-11所示输入**目录服务还原模式**的系统管理员的用户名与密码，其中用户名称可输入**.\Administrator**或**计算机名\Administrator**。

提示

若域内还有其他域控制器在线的话，也可以利用域用户账户来登录，不过却无法执行还原操作，您必须利用**目录服务还原模式**的系统管理员账户与密码来登录，才有权限执行域控制器的还原操作。

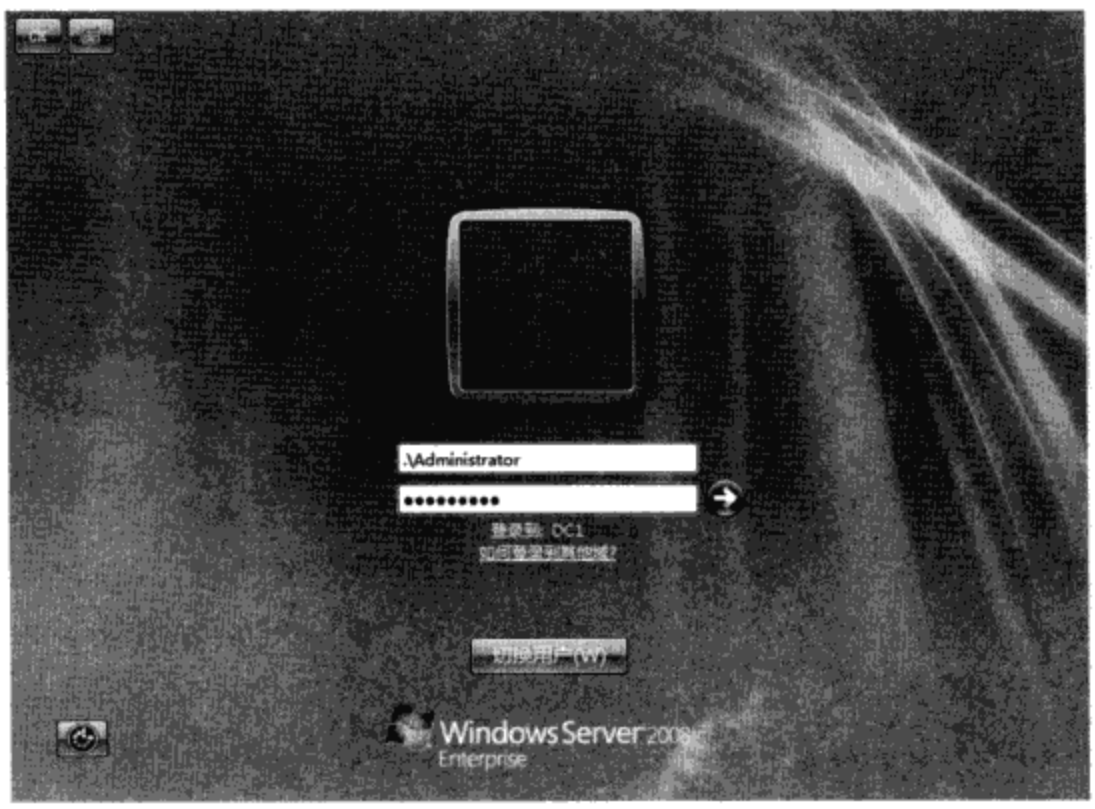


图 11-11

Download at http://www.pin5i.com/

STEP 2 选择【开始➲管理工具➲Windows Server Backup➲单击图 11-12中的**恢复…**】。

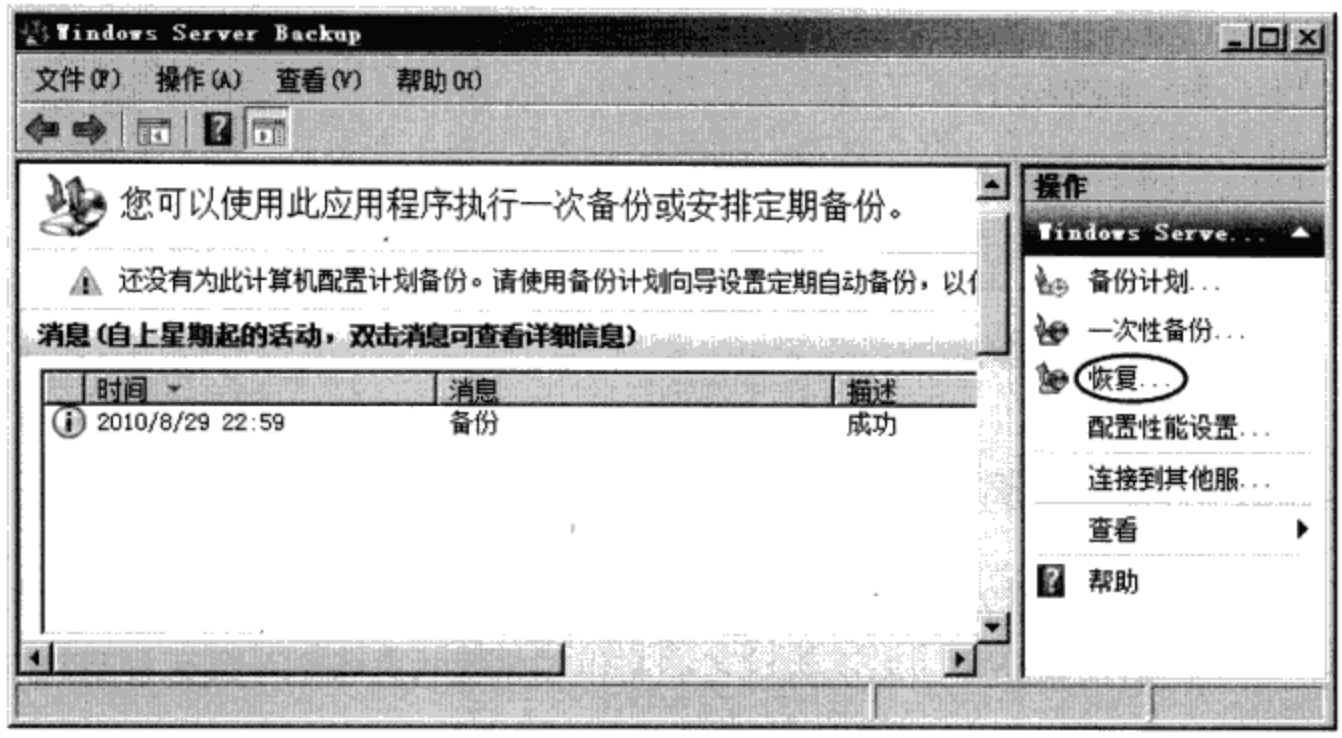


图 11-12

STEP 3 如图 11-13所示选择**在其他位置存储备份**单选按钮后单击 下一步 按钮。

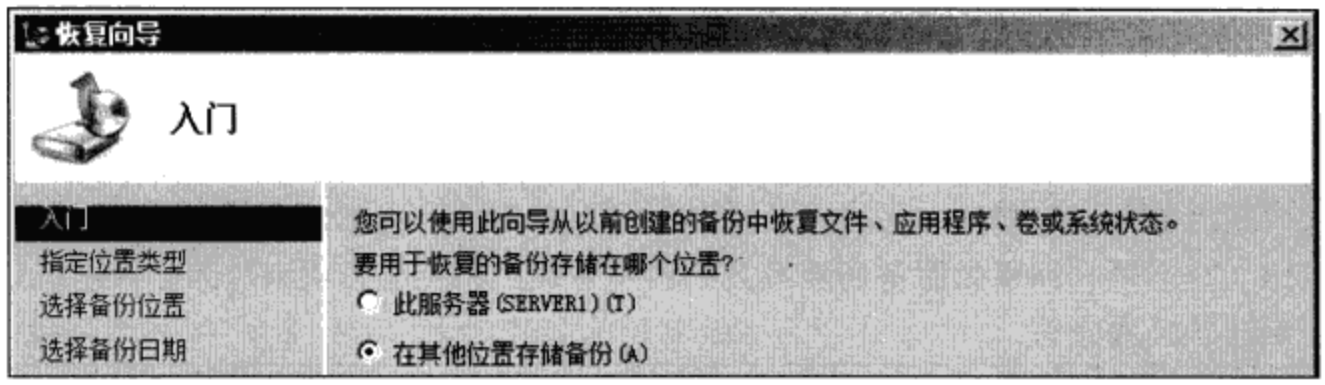


图 11-13

STEP 4 如图 11-14所示选择**远程共享文件夹**单选按钮后单击 下一步 按钮。

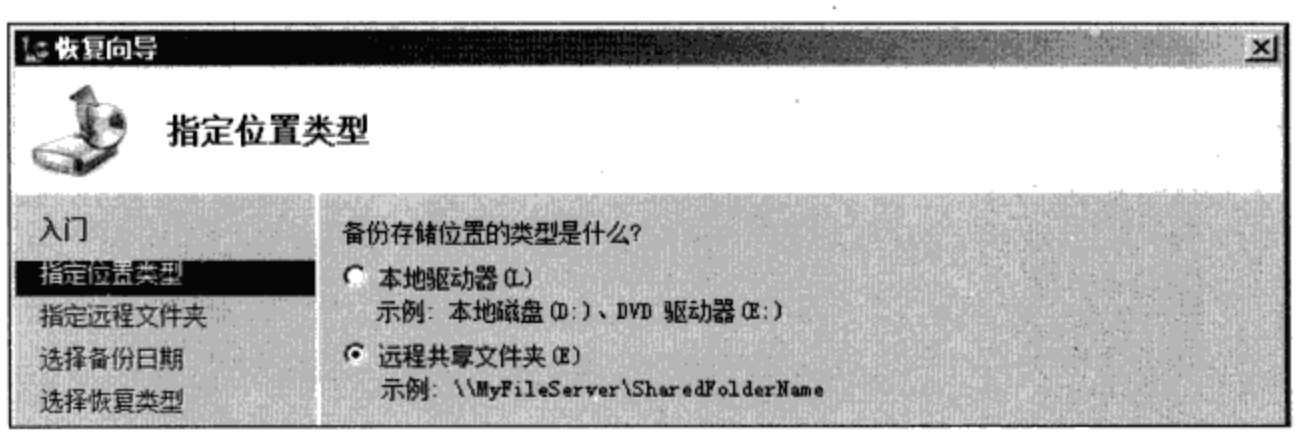


图 11-14

STEP 5 如图 11-15所示输入共享文件夹的路径**\\dc2\backup**后单击 下一步 按钮。

Download at http://www.pin5i.com/

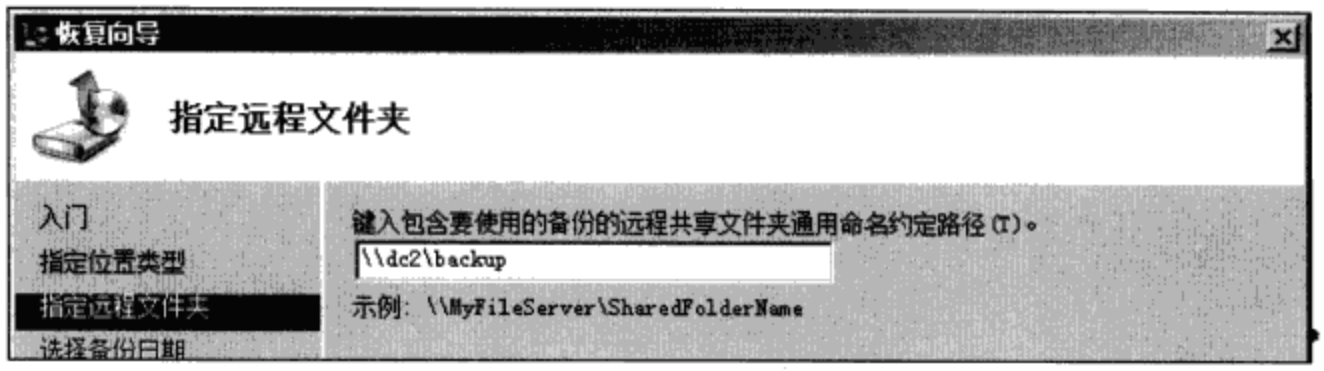


图 11-15

STEP 6 在图 11-16中选择备份的日期与时间后单击下一步按钮。

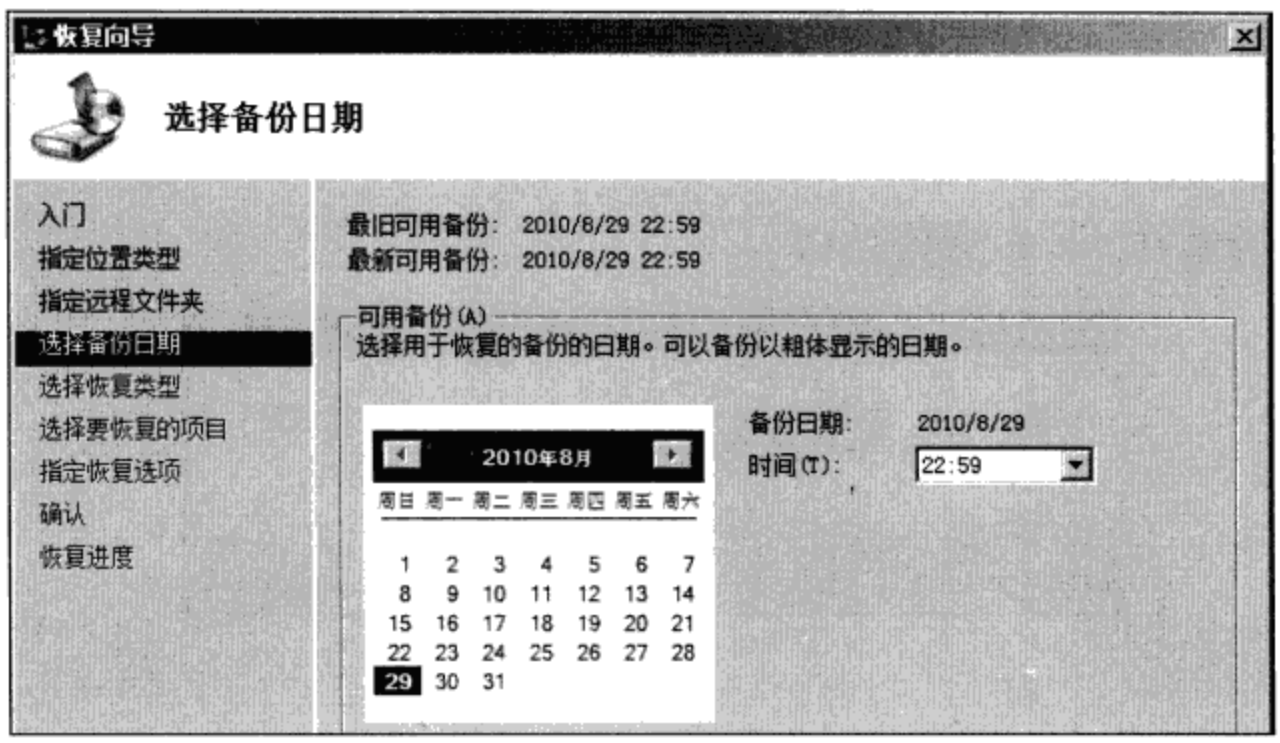


图 11-16

STEP 7 如图 11-17所示选择**系统状态**单选按钮后单击下一步按钮。

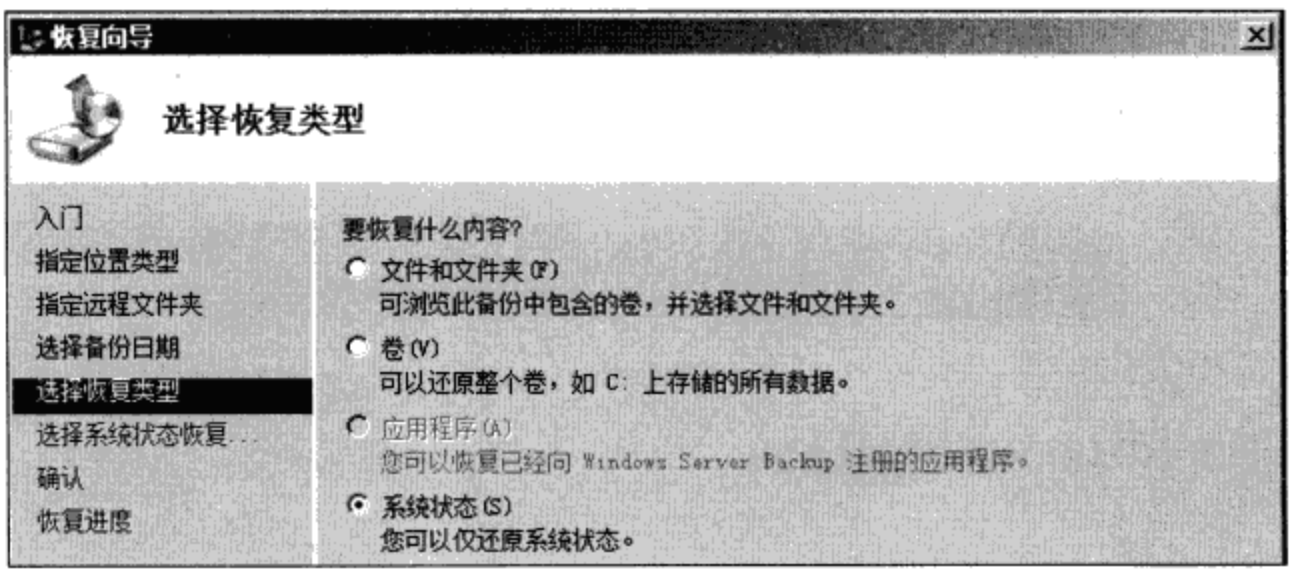


图 11-17

STEP 8 如图 11-18所示选择**原始位置**单选按钮后单击下一步按钮。

Download at http://www.pin5i.com/

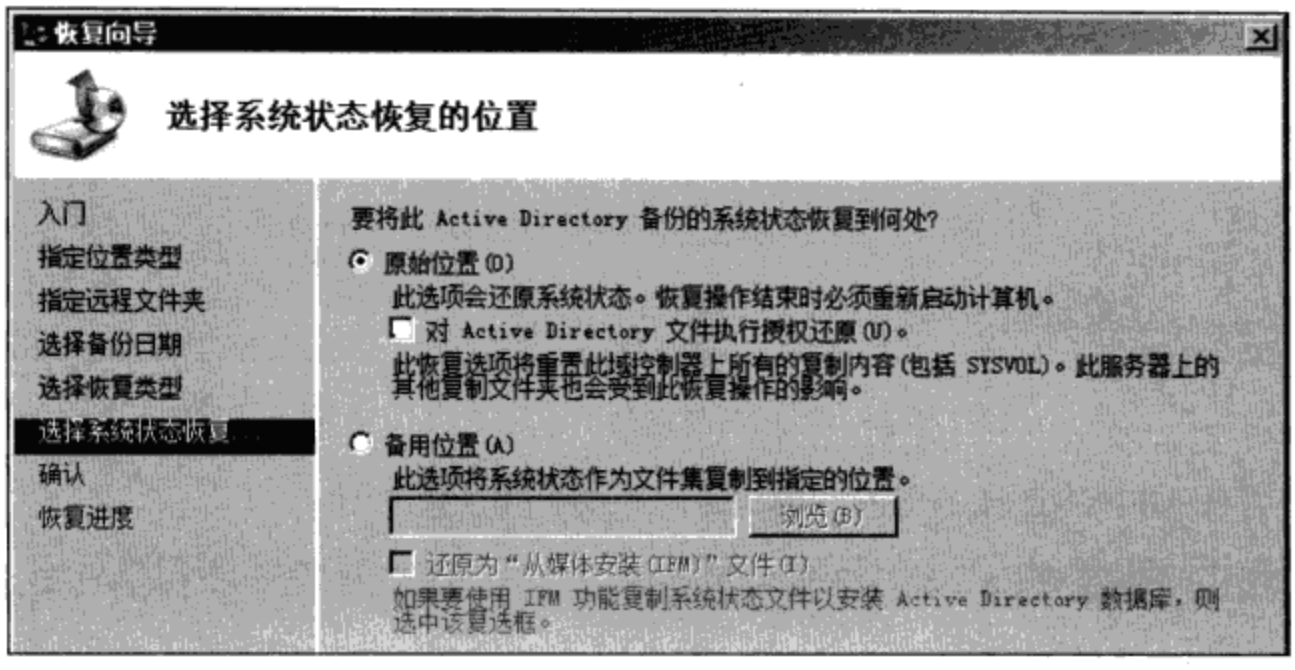


图 11-18

STEP 9 在图 11-19中单击确定按钮。

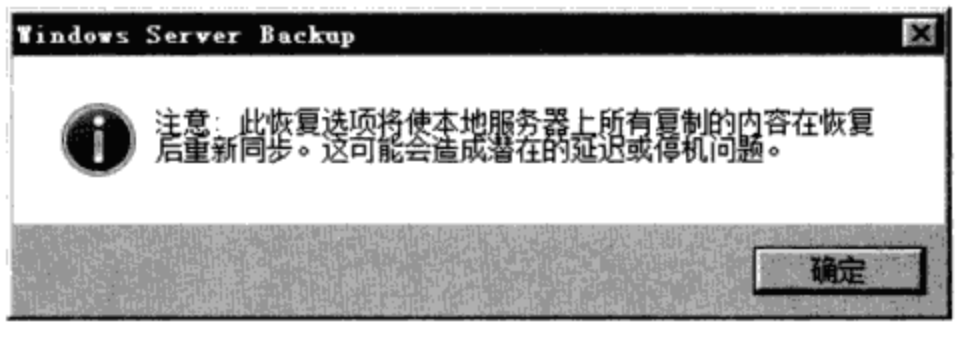


图 11-19

STEP 10 参考图 11-20中的说明后单击确定按钮。

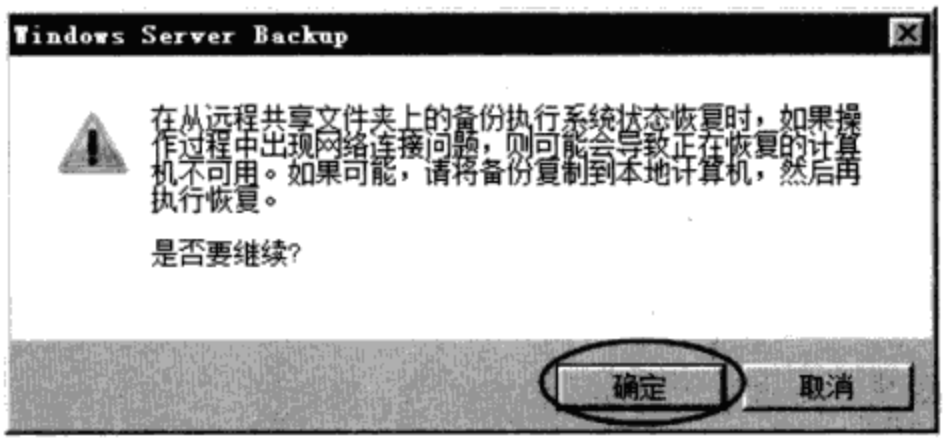


图 11-20

STEP 11 如图 11-21所示单击恢复按钮。

Download at http://www.pin5i.com/

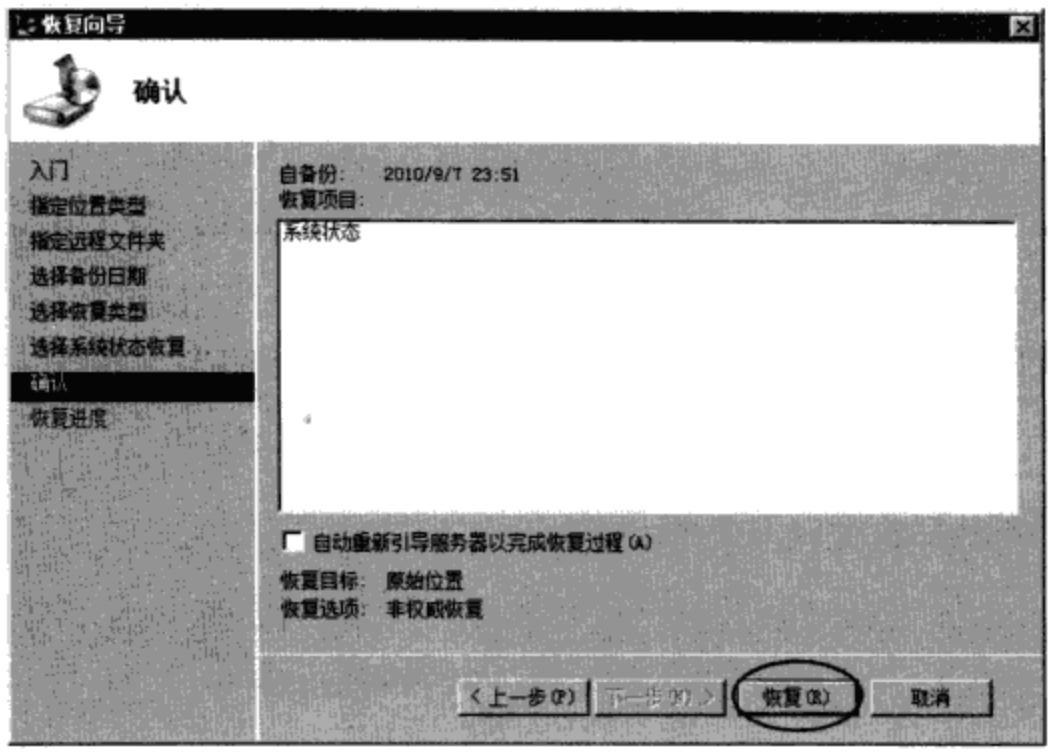


图 11-21

STEP 12 在图 11-22中单击 是（Y） 按钮。

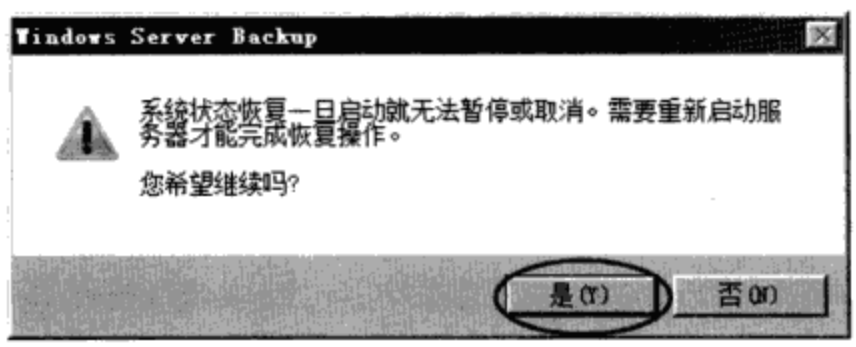


图 11-22

STEP 13 完成还原后，请如图 11-23所示单击 重新启动 按钮。



图 11-23

提示

若您是利用**bcdedit /set safeboot dsrepair**命令进入目录服务还原模式的话，可先执行**bcdedit /deletevalue safeboot**，以便让系统重新以一般模式来启动。

若您是通过wbadmin.exe程序来还原系统状态的话，请先执行以下命令：

Download at http://www.pin5i.com/

```
wbadmin get versions -backuptarget:\\dc2\backup
```

它用来读取备份的版本号，其中的**-backuptarget**用来指定存储备份的位置。



提示

若在存储备份的位置内存储着多台服务器的备份的话，则您可以指定要读取的服务器，例如欲读取属于服务器DC1的备份的话，可增加**-machine:dc1** 这个参数。

请记下要用来还原的备份版本，它是位于**版本识别源**处的字符串（假设是**05/07/2010-14:38**），然后执行以下命令：

```
wbadmin start systemstaterecovery -version: 05/07/2010-14:38 -
backuptarget:\\dc2\backup
```

11-3-3 针对被删除的AD DS对象执行授权还原

如果域内只有一台域控制器，那么只需要执行**非授权还原**即可，但是如果域内有多台的域控制器的话，则只执行**非授权还原**可能还不够，必须搭配**授权还原**。

例如域内有两台域控制器DC1与DC2，而且您曾经备份域控制器DC2的系统状态，可是却不小心利用**Active Directory管理中心**控制台将用户账户**王乔治**删除，之后这个变动数据会通过Active Directory的复制机制被复制到域控制器DC1，因此在域控制器DC1内的**王乔治**账户也会被删除。



注意

当您将用户账户删除后，此账户并不会立刻从Active Directory数据库内删除，而是被转移到Active Directory数据库内一个名为Deleted Objects的隐藏式文件夹内，同时这个用户账户的版本号会被加1。Windows Server 2008 R2默认是180天后才会将其从Active Directory数据库内删除（从Windows Server 2003 SP1开始为180天，之前的版本是60天）。

若要找回被不小心删除的**王乔治**账户，您可能会在域控制器DC2上利用标准的**非授权还原**来将之前已经备份的旧**王乔治**账户还原，可是虽然在域控制器DC2内的**王乔治**账户已被还原了，但是在域控制器DC1内的**王乔治**却是被标记为**已删除**的账户，下一次DC1与DC2之间执行Active Directory复制程序时，将会有什么样的结果呢？

答案是在DC2内刚被还原的**王乔治**账户会被删除，因为对系统来说，DC1内被标记为**已删除**的**王乔治**的版本号较高，而DC2内刚还原的**王乔治**是旧的数据，其版本号较低。我们在第9章内已经介绍过两个对象有冲突时，系统会以**戳记**（Stamp）来作为解决冲突的依据，因此版本号较高的对象会覆盖掉版本号较低的对象。

Download at http://www.pin5i.com/

若要避免上述现象发生的话，请另外再执行**授权还原**。当您在DC2上针对**王乔治**账户另外执行过**授权还原**后，这个被还原的旧**王乔治**账户的版本号将被增加，而且是从备份当天开始到执行**授权还原**为止，每天增加100,000，因此当DC1与DC2开始执行复制工作时，由于位于DC2的旧**王乔治**账户的版本号会比较高，所以这个旧**王乔治**会被复制到DC1，将DC1内被标记为**已删除**的**王乔治**覆盖掉，也就是说旧**王乔治**被还原了。

以下练习假设上述用户账户**王乔治**是新建在域sayms.com的组织单位**业务部**内，我们需要先执行**非授权还原**，然后再利用**ntdsutil**命令来针对用户账户**王乔治**执行**授权还原**。您可以按照以下的顺序来练习：

- 在第1台域控制器上新建组织单位**业务部**，然后在其内新建用户账户**王乔治**。
- 等**王乔治**账户被复制到第2台域控制器（请检查第2台域控制器上是否已经有**王乔治**账户）。
- 在第2台域控制器上备份**系统状态**。
- 在第2台域控制器上将用户账户**王乔治**删除（此账户会被转移到隐藏文件夹**Deleted Objects**内）。
- 等这个被删除的**王乔治**账户被复制到第1台域控制器，也就是等第1台域控制器内的**王乔治**也被删除（默认是等15s）。
- 在第2台域控制器上先执行**非授权还原**，然后再执行**授权还原**，它便会将被删除的**王乔治**账户还原。

以下仅针对最后一个步骤来说明，也就是先执行**非授权还原**，然后再执行**授权还原**。

STEP 1 请执行**非授权还原**步骤，也就是执行**AD DS的非授权还原** **STEP 1** ~ **STEP 12**，注意不要执行**STEP 13**，也就是完成还原后，不要重新启动计算机。

STEP 2 继续在**命令提示符**下输入以下命令后按Enter键：**ntdsutil**。

STEP 3 在**ntdsutil**提示符下，输入以下命令后按Enter键：**activate instance ntds**。表示要将域控制器的Active Directory数据库设置为活动。

STEP 4 在**ntdsutil**提示符下，输入以下命令后按Enter键：**authoritative restore**。

STEP 5 在**authoritative restore**提示符下，针对域sayms.com的组织单位**业务部**内的用户**王乔治**执行**授权还原**，其命令如下所示：**restore object CN=王乔治,OU=业务部,DC=sayms,DC=com**。

> **提示**
>
> 如果您要针对整个Active Directory数据库执行**授权还原**的话，请运行**restore database**命令；如果您要针对组织单位**业务部**执行**授权还原**的话，请运行以下命令（可输入**?**来查询命令的语法）：restore subtree OU=业务部,DC=sayms,DC=com。

STEP 6 在图 11-24中单击**是（Y）**按钮。

Download at http://www.pin5i.com/

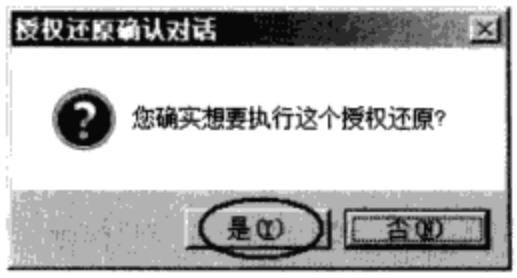


图 11-24

STEP 7 图 11-25为前面几个步骤的完整操作过程。

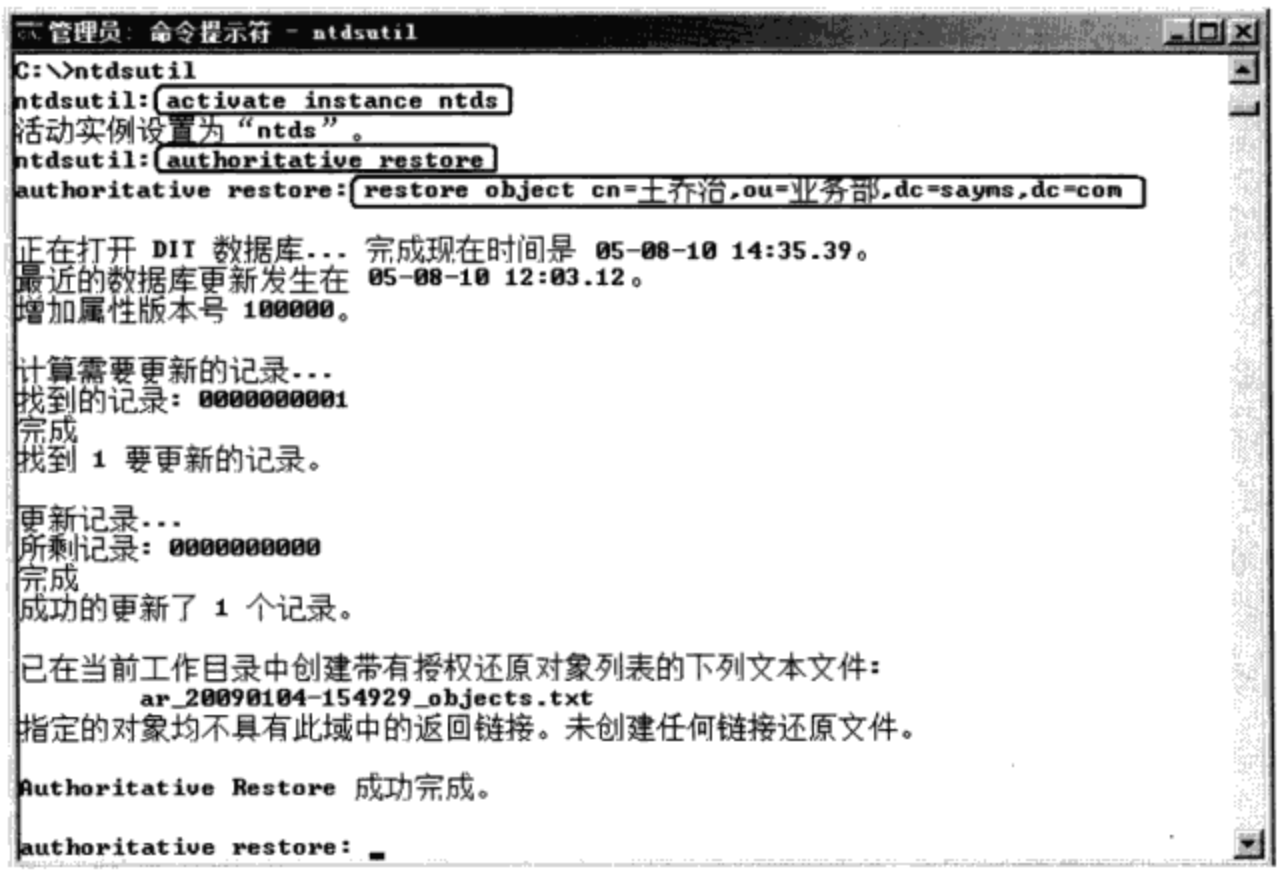


图 11-25

STEP 8 在**authoritative restore**提示符下，输入quit命令。

STEP 9 在**ntdsutil**提示符下，输入quit命令。

STEP 10 重新用正常模式启动系统。

STEP 11 等域控制器之间的Active Directory自动同步完成，或利用Active Directory站点和服务手动同步，或执行以下命令来手动同步 :**repadmin /syncall dc2.sayms.com /e /d /A /P**。其中**/e**表示包含所有站点内的域控制器，**/d**表示信息中以Distinguished Name（DN）来识别服务器，**/A**表示同步此域控制器内的所有目录分区，**/P**表示同步方式是将此域控制器（dc2.sayms.com）的变动数据传送给其他域控制器。

完成同步工作后，可利用**Active Directory管理中心**来验证用户账户王乔治已经被还原，而您也可以通过以下命令来验证**王乔治**账户的属性版本号确实被增加了100,000，如图 11-26所示中的**版本**字段。

```
repadmin /showmeta CN=王乔治,OU=业务部,DC=sayms,DC=com
```


Download at http://www.pin5i.com/

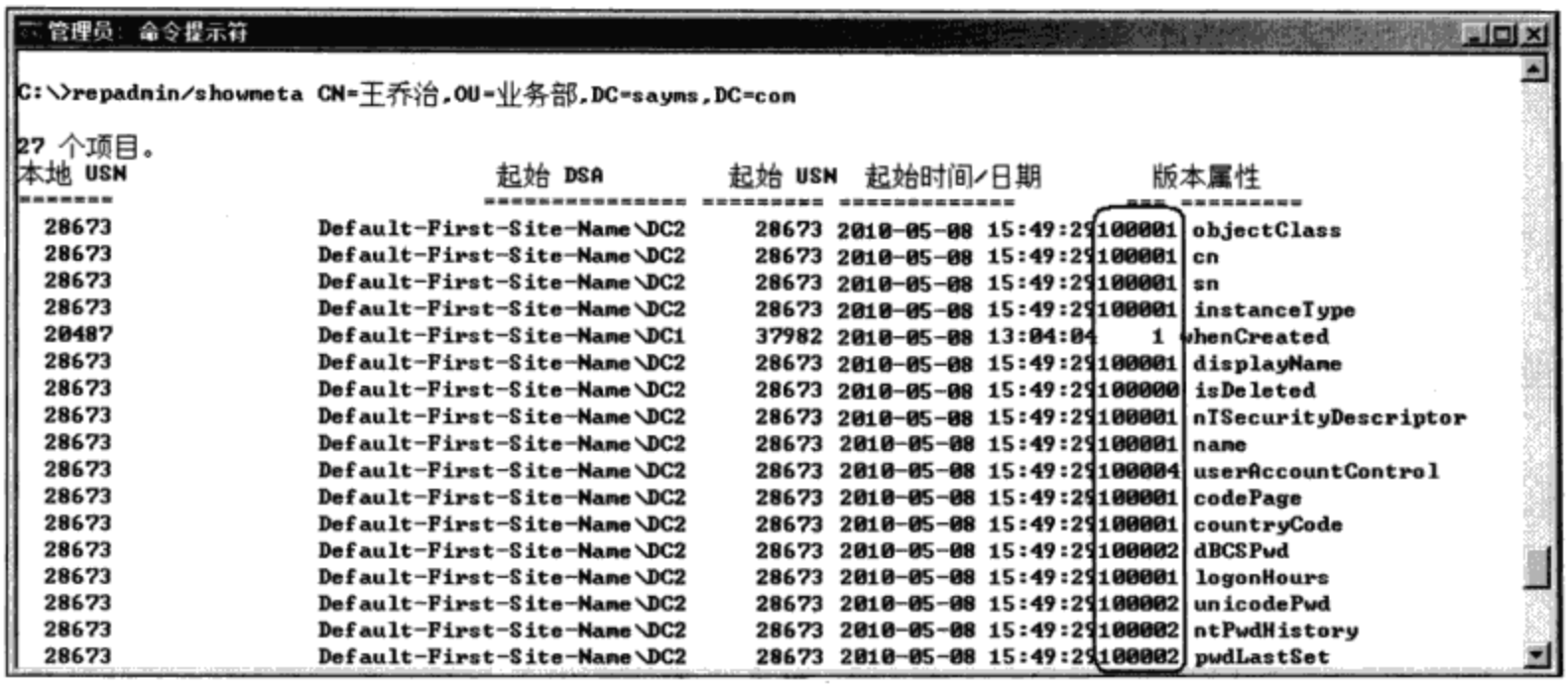


图 11-26

提示

如果您要针对SYSVOL文件夹执行**授权还原**的话，请在前面执行**非授权还原**时，增加**-authsysvol**参数，例如：wbadmin start systemstaterecovery –其他参数 –authsysvol。

11-4 Active Directory数据库的转移与重组

Active Directory数据库与事务日志的存储位置默认是在**%systemroot%\NTDS**文件夹内，然而一段时间以后，若硬盘存储空间不够或为了提高工作效率的话，则您可能需要将Active Directory数据库转移到其他地点或重组。

11-4-1 可重新启动的AD DS（Restartable AD DS）

在旧版Windows Server 2003域控制器内，若要进行Active Directory数据库维护工作的话，例如安装安全性更新、转移Active Directory数据库、数据库脱机重组等，就必须重新启动计算机，然后进入到**目录服务还原模式**内来执行这些维护工作。

如果这台域控制器也同时提供其他网络服务的话，例如它同时也是DHCP服务器，则重新启动计算机将造成这些服务会暂时停止对客户端服务。

除了进入**目录服务还原模式**之外，Windows Server 2008 R2（Windows Server 2008）域控制器还提供新的**可重新启动的AD DS**功能，此时只需要将AD DS服务停止，就可以执行Active Directory数据库的维护工作，不需要重新启动计算机来进入**目录服务还原模式**，如此不但可让Active Directory数据库的维护工作更容易、更快地完成，且其他服务也不会被中断。完成维护工作后再重新启动AD DS服务。

Download at http://www.pin5i.com/

在AD DS服务停止的情况下，若要利用**dcpromo.exe**将AD DS从域控制器删除的话，需要改用**dcpromo /forceremoval**命令。

在AD DS服务停止的情况下，只要还有其他域控制器在线，则您仍然可以在这台AD DS服务已经停止的域控制器上利用域用户账户来登录。若没有其他域控制器在线的话，则在这台AD DS服务已停止的域控制器上，默认只能够利用**目录服务还原模式**的系统管理员账户来进入**目录服务还原模式**。

11-4-2 转移Active Directory数据库文件

在此我们不采用进入**目录服务还原模式**的方式，而是利用将AD DS服务停止的方式来进行Active Directory数据库文件的转移工作，此时您必须至少是隶属于Administrators组的成员才有权限进行以下的操作。

我们需要利用**ntdsutil.exe**来转移Active Directory数据库与事务日志，以下假设要将它们都转移到E:\NewNTDS文件夹。

提示

1. 您不需要手动新建此文件夹，因为**Ntdsutil.exe**会自动新建。若您要事先新建此文件夹的话，请确认SYSTEM与Administrators对此文件夹拥有**完全控制**的权限。
2. 若要更改SYSVOL文件夹的存储位置的话，方法为：删除AD DS、重新安装AD DS、在安装过程中指定新的存储位置。

STEP 1 打开**命令提示符**对话框（或单击左下角的**Windows PowerShell**图标）。

STEP 2 如图 11-27所示执行以下命令来停止AD DS服务：**net stop ntds**。接着输入**Y**后按Enter键，它也会将其他相关服务停止。



图 11-27

STEP 3 在**命令提示符**下，输入以下命令后按Enter键（参考图 11-8）：**ntdsutil**。

STEP 4 在ntdsutil提示符下，输入以下命令后按Enter键：**activate instance ntds**。表示要将

Download at http://www.pin5i.com/

域控制器的Active Directory数据库设置为活动。

STEP 5 在**ntdsutil**提示符下，输入以下命令后按Enter键：**files**。

STEP 6 在**file maintenance**提示符下，输入以下命令后按Enter键：**info**。它可以查看Active Directory数据库与事务日志目前的存储位置，由图 11-28可知它们目前都是位于C:\Windows\NTDS文件夹内。

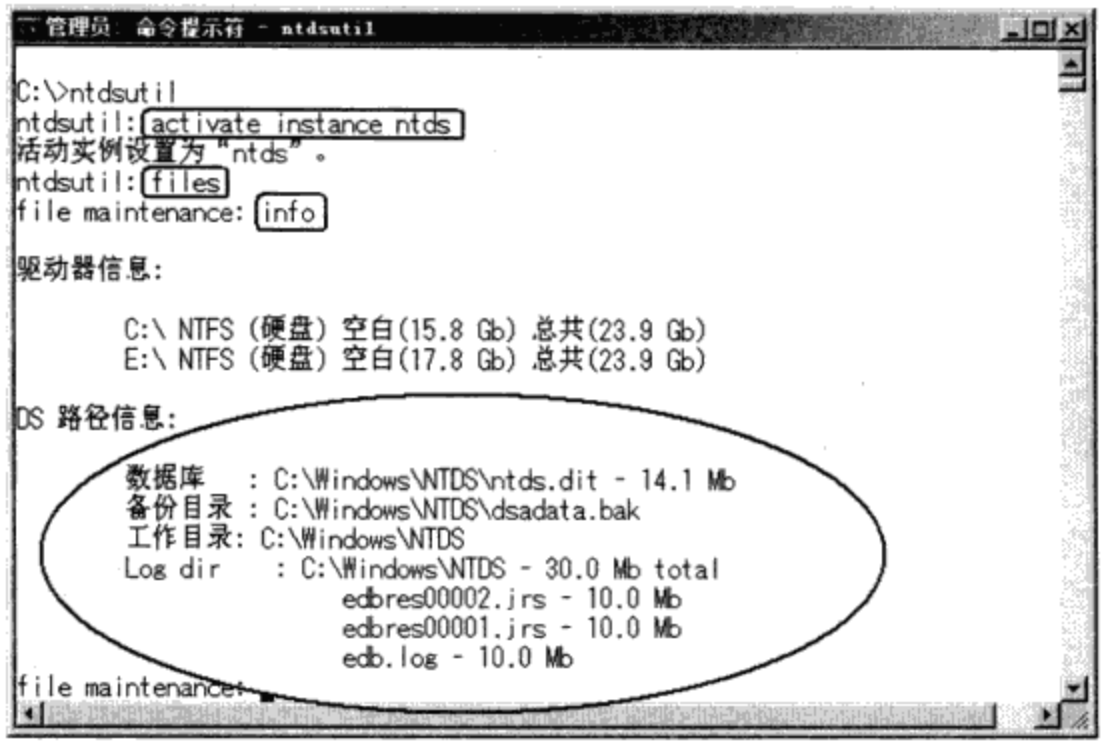


图 11-28

STEP 7 在**file maintenance**提示符下，如图 11-29所示输入以下命令后按Enter键，以便将数据库文件转移到E:\NewNTDS：**move db to E:\NewNTDS**。

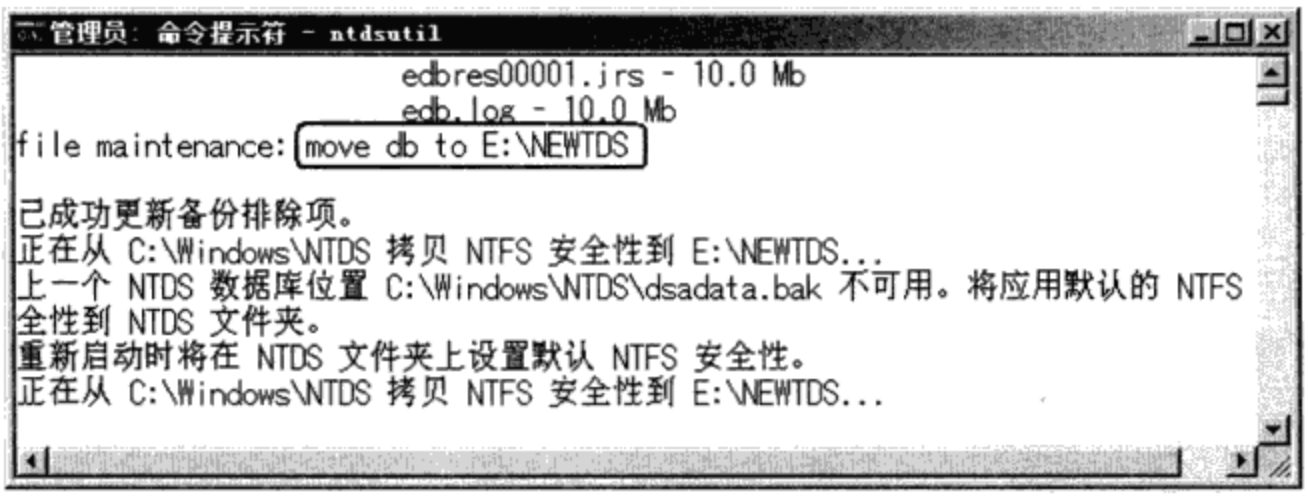


图 11-29

STEP 8 在**file maintenance**提示符下，如图 11-30所示输入以下命令后按Enter键，以便将事务日志也转移到E:\NewNTDS：**move logs to E:\NewNTDS**。由图中可知数据库与事务日志都已经正确地被转移到新地点E:\NewNTDS。

Download at http://www.pin5i.com/

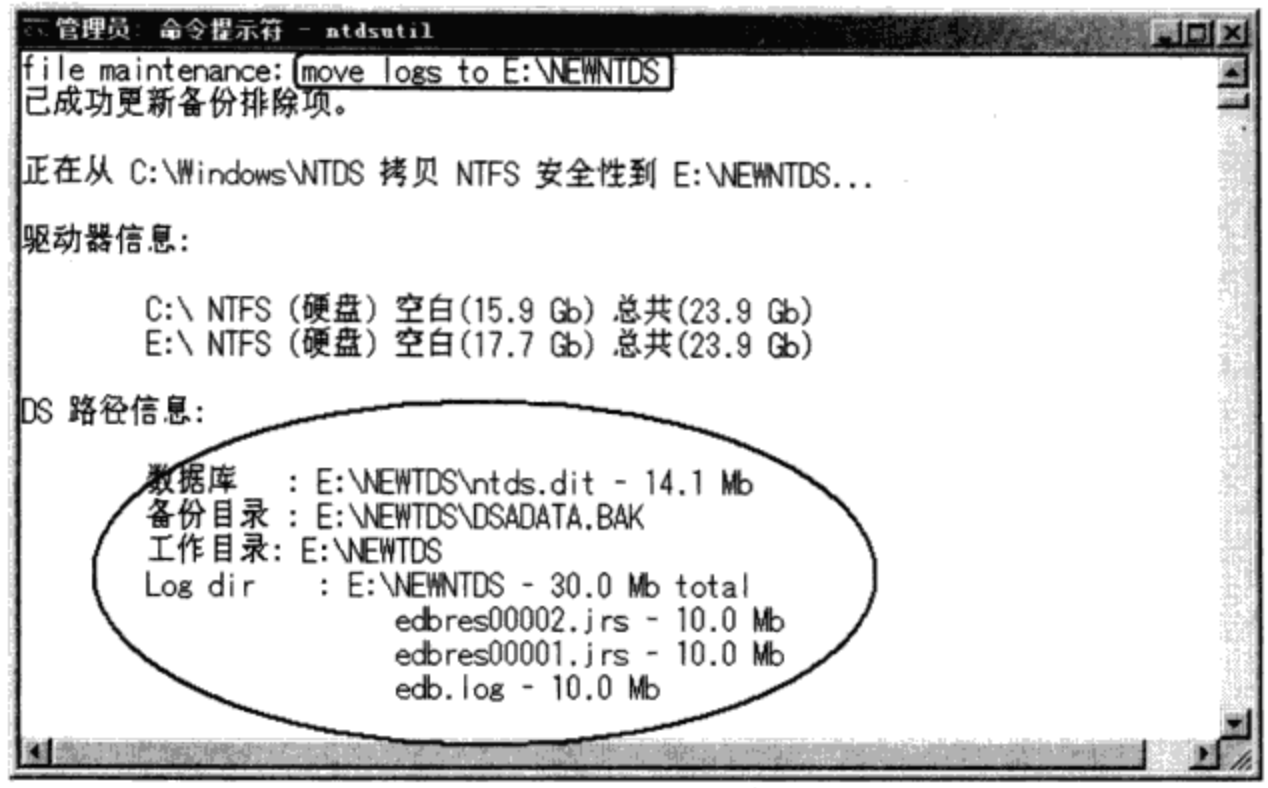


图 11-30

STEP 9 在**file maintenance**提示符下，如图 11-31所示输入以下命令后按Enter键，以便执行数据库的完整性检查：**integrity**。由图中的文字Integrity check successful可知完整性检查成功。

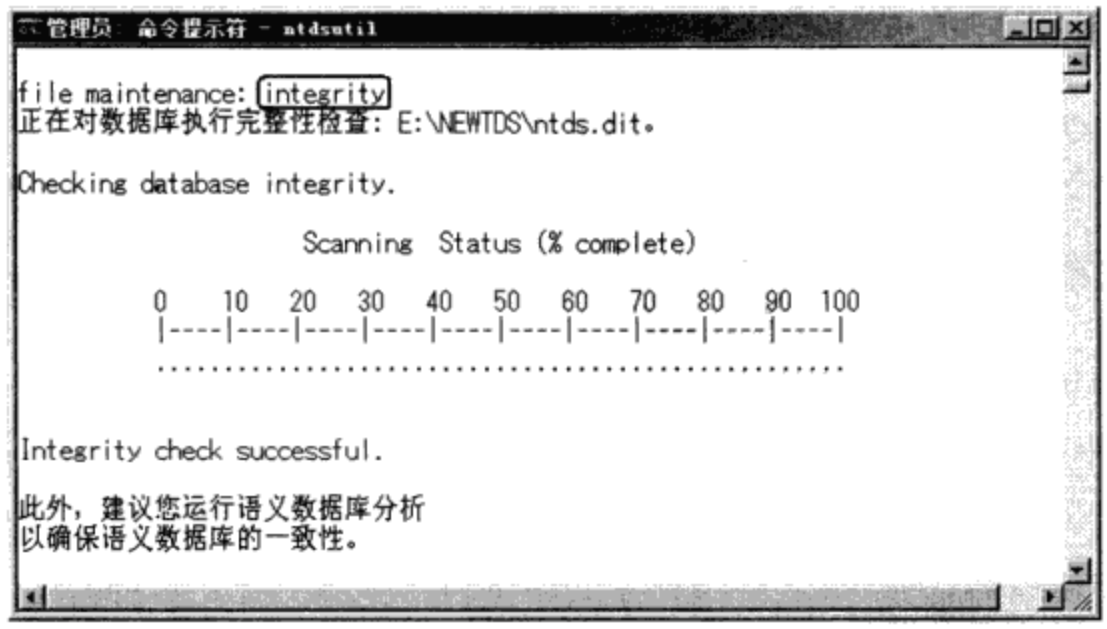


图 11-31

STEP 10 在**file maintenance**提示符下，输入以下命令后按Enter键：**quit**。

STEP 11 若完整性检查成功的话，可跳到**STEP 20**，否则请继续以下的步骤。

STEP 12 在**ntdsutil**提示符下，输入以下命令后按Enter键（参考图 11-32）：**semantic database analysis**。

Download at http://www.pin5i.com/

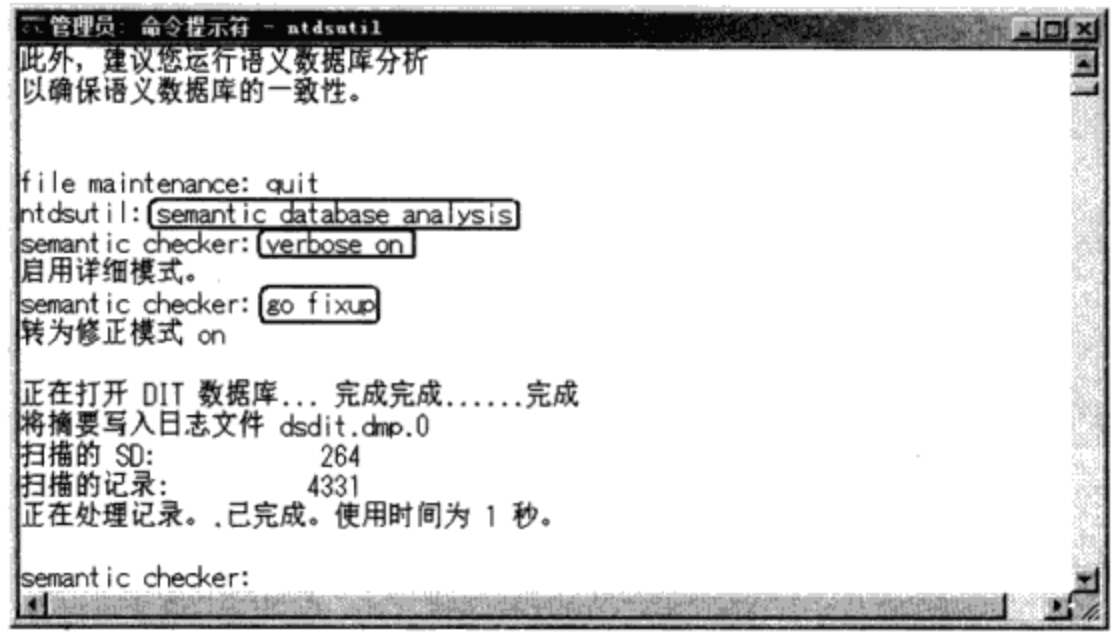


图 11-32

STEP 13 在**semantic checker**提示符下，输入以下命令后按Enter键，以便启用详细信息模式：**verbose on**。

STEP 14 在**semantic checker**提示符下，输入以下命令后按Enter键，以便执行语义数据库分析工作：**go fixup**。

STEP 15 在**semantic checker**提示符下，输入以下命令后按Enter键：**quit**。

STEP 16 若语义数据库分析没有错误的话，可跳到**STEP 20**，否则请继续以下的步骤。

STEP 17 在**ntdsutil**提示符下，输入以下命令后按Enter键（参考图 11-33）：**files**。

STEP 18 在**file maintenance**提示符下，输入以下命令后按Enter键，以便修复数据库：**recover**。



图 11-33

STEP 19 在**file maintenance**提示符下，输入以下命令后按Enter键：**quit**。

STEP 20 在**ntdsutil**提示符下，输入以下命令后按Enter键：**quit**。

Download at http://www.pin5i.com/

STEP 21 返回到**命令提示符**下，输入以下命令后按Enter键，以便重新启动AD DS服务：net start ntds。

11-4-3 重组Active Directory数据库

Active Directory数据库的重组操作（Defragmentation），会将数据库内的数据排列的更整齐，让数据的读取更快速，可以提升AD DS运行效率。Active Directory数据库的重组分为以下两种。

1. 在线重组（Online Defragmentation）

每一台域控制器会每隔12小时自动执行所谓的**垃圾收集程序**（Garbage Collection Process），这个程序会重组Active Directory数据库。**在线重组**并无法减少Active Directory数据库文件（ntds.dit）的大小，而只是将数据有效率地重新整理、排列。由于此时Active Directory还在运行中，因此这个重组操作被称为**在线重组**。

另外我们曾经说过一个被删除的对象，并不会立刻被从Active Directory数据库内删除，而是被转移到一个名称为**Deleted Objects**的隐藏文件夹内，这个对象在180天以后才会被自动清除，而这个清除操作也是由**垃圾收集程序**所负责。虽然对象已被清除，不过腾出的空间并不会还给操作系统，也就是数据库文件的大小并不会减少。当您新建新对象时，该对象就会使用腾出的可用空间。

> **提示**
>
> 从Windows Server 2003 SP1开始，已删除的对象会在180天后被删除，Windows Server 2003 SP1以前的版本则是60天。

2. 脱机重组（Offline Defragmentation）

脱机重组必须在AD DS服务停止或**目录服务还原模式**内手动进行，脱机重组会新建一个全新的、整齐的数据库文件，并会将已删除的对象所占用的空间还给操作系统，因此可以腾出可用的硬盘空间给操作系统或其他应用程序来使用。

> **提示**
>
> 在一个内含多个域的林中，若有一台域控制器曾经兼具**全局编录服务器**，但现在已经不再是**全局编录服务器**的话，则这台域控制器经过**脱机重组**后，新的Active Directory数据库文件会比原来的文件小很多，也就是说可以腾出很多的硬盘空间给操作系统。

以下将介绍如何来执行**脱机重组**的步骤。请确认当前存储Active Directory数据库的磁盘内有足够大的可用空间来存储**脱机重组**所需的暂存盘，请至少保留数据库文件大小的15%可用空

Download at http://www.pin5i.com/

间。还有重组后的新文件的存储位置，也需保留至少与原数据库文件大小的可用空间。以下假设原数据库文件是位于C:\Windows\NTDS文件夹，而我们要将重组后的新文件放到E:\NTDSTemp文件夹。

提示

1. 您不需手动新建E:\NTDSTemp文件夹，**Ntdsutil.exe**会自动创建。
2. 如果您要将重组后的新文件存储到网络共享文件夹的话，请开放Administrators组拥有权限来访问此共享文件夹，并先利用网络驱动器来连接到此共享文件夹。

STEP 1 打开命令提示符（或单击左下角的Windows PowerShell图标）。

STEP 2 如图 11-34所示执行以下命令来停止AD DS服务：**net stop ntds**。接着输入**Y**后按Enter键。它也会将其他相关服务停止。

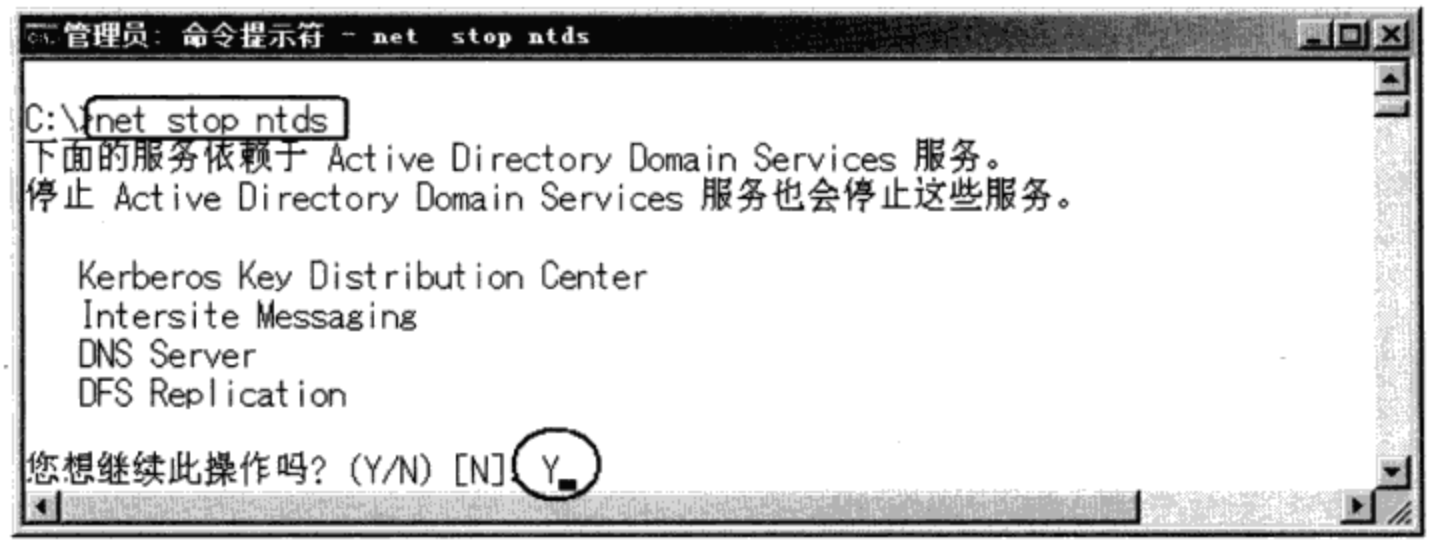


图 11-34

STEP 3 在**命令提示符**下，输入以下命令后按Enter键（参考图 11-35）：**ntdsutil**。

STEP 4 在ntdsutil提示符下，输入以下命令后按Enter键：**activate instance ntds**。表示要将域控制器的Active Directory数据库设定为使用中。

STEP 5 在**ntdsutil**提示符下，输入以下命令后按Enter键：**files**。

STEP 6 在**file maintenance**提示符下，输入以下命令后按Enter键：**info**。它可以查看Active Directory数据库与事务日志目前的存储位置，由图 11-35可知道它们当前都是位于C:\Windows\NTDS文件夹内。

Download at http://www.pin5i.com/

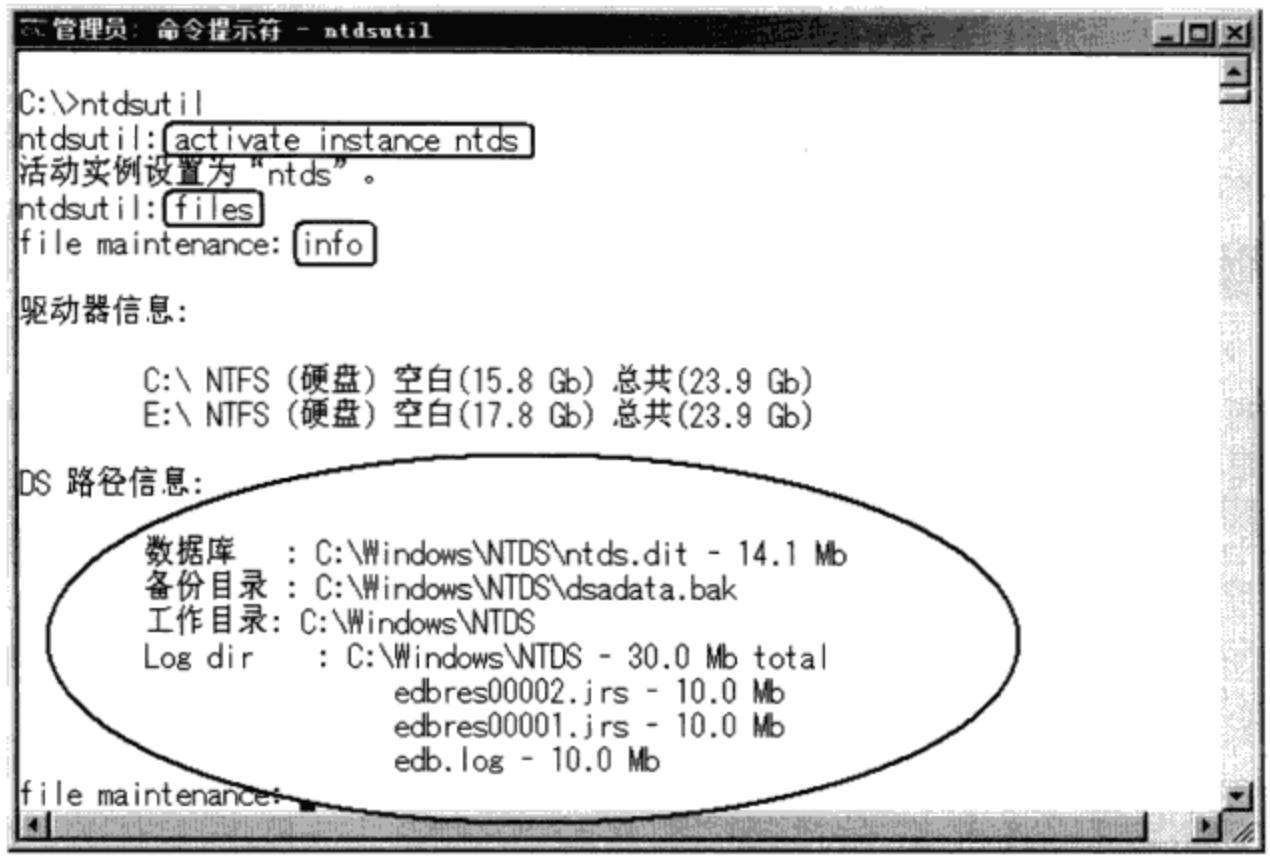


图 11-35

STEP 7 在**file maintenance**提示符下，如图 11-36所示输入以下命令后按Enter键，以便重组数据库文件，并将所生成的新数据库文件放到E:\NTDSTTemp文件夹内（新文件的名称还是**ntds.dit**）：**compact to E:\NTDSTemp**。



图 11-36

Download at http://www.pin5i.com/

提示

1. 若所输入的路径中有空格符的话，请在路径前后加上双引号，例如“E:\New Folder”。
2. 若要将新文件放到网络驱动器的话，例如K:，请用以下命令：**compact to K:**。

STEP 8 暂时不要离开**ntdsutil**程序，打开**Windows资源管理器**后执行以下几项操作：

- 将原数据库文件C:\Windows\NTDS\ntds.dit备份起来，以备不时之需。
- 将原事务日志C:\Windows\NTDS*.log删除。
- 将重组后的新数据库文件E:\NTDSTemp\ntds.dit复制到C: \Windows\NTDS文件夹，并覆盖原数据库文件。

STEP 9 继续在**ntdsutil**程序的**file maintenance**提示符下，如图 11-37所示输入以下命令后按Enter键，以便执行数据库的完整性检查：**Integrity**。由图下方所显示的Integrity check successful可知完整性检查成功。



图 11-37

STEP 10 在**file maintenance**提示符下，输入以下命令后按Enter键：**quit**。

STEP 11 在**ntdsutil**提示符下，输入以下命令后按Enter键：**quit**。

STEP 12 返回到**命令提示符**下，输入以下命令后按Enter键，以便重新启动AD DS服务：**net start ntds**。若无法启动AD DS服务的话，请试着采用以下途径来解决问题：

- 利用**事件查看器**来查看**目录服务**日志文件，若有事件标识符为1046或1168的事件记录的话，请利用备份来还原AD DS。

Download at http://www.pin5i.com/

- 再重复执行数据库完整性检查（Integrity），若完整性检查失败的话，请将之前备份的数据库文件ntds.dit复制回原数据库的存储位置，然后重复数据库重组的操作，这个操作中的数据库完整性检查若还是失败的话，请执行语义数据库分析工作（Semantic Database Analysis），若失败的话，请执行修复数据库的操作（Recover）。

11-5 重设目录服务还原模式的系统管理员密码

如果忘记了**目录服务还原模式**的系统管理员密码，以致于无法进入**目录服务还原模式**时该怎么办呢？此时您可以在正常模式下，利用**ntdsutil**程序来重设**目录服务还原模式**的系统管理员密码，其步骤如下所示：

STEP 1 请到域内的任意一台计算机上利用域系统管理员账户登录。

STEP 2 打开**命令提示符**（或单击左下角的**Windows PowerShell**图标），输入以下命令后按Enter键（完整的操作界面如图 11-38所示）：**ntdsutil**。

STEP 3 在**ntdsutil**提示符下，输入以下的命令后按Enter键：**set DSRM password**。

STEP 4 在**重设DSRM系统管理员密码**提示符下，执行以下的命令：**reset password on server dc2.sayms.com**。以上命令假设要重设域控制器dc2.sayms.com的**目录服务还原模式**的系统管理员密码。

注意

要被重设密码的域控制器，其AD DS服务必须是启动中。

STEP 5 输入与确认新密码。

STEP 6 连续输入**quit**命令以便离开**ntdsutil**程序，图 11-38为以上几个主要步骤的操作界面。

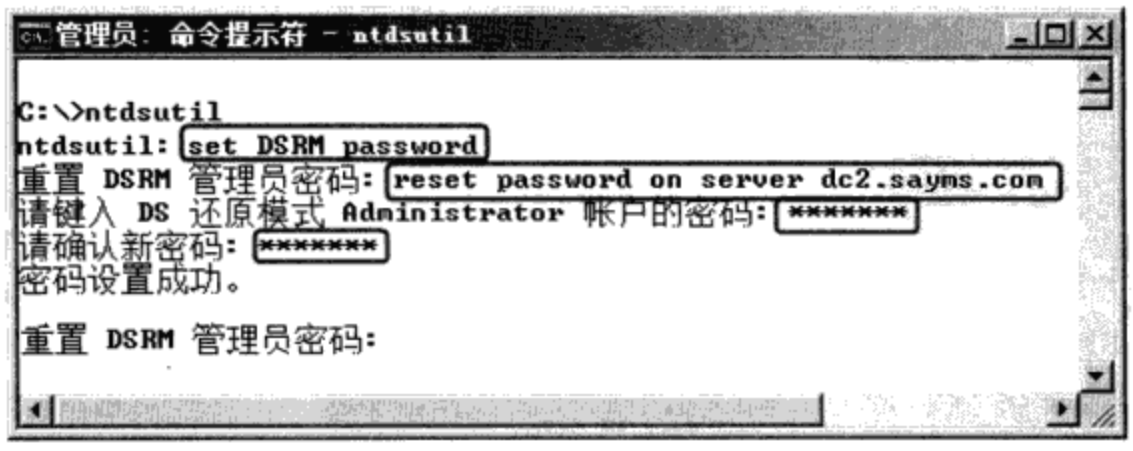


图 11-38

Download at http://www.pin5i.com/

11-6 更改可重新启动的AD DS的登录设置

在AD DS服务停止的情况下，只要还有其他域控制器在线，则您仍然可以在这台AD DS服务已经停止的域控制器上利用域用户账户来登录。

若没有其他域控制器在线的话，则在这台AD DS服务已停止的域控制器上，默认只能够利用**目录服务还原模式**（DSRM）的系统管理员账户来进入**目录服务还原模式**，然而这种运行方式可能会造成困扰，例如：

- 在域控制器上利用域系统管理员的身份登录。
- 将AD DS服务停止。
- 受密码保护的屏幕保护程序被启动。

此时若您要继续使用这台域控制器的话，则必须输入域系统管理员账户来解开屏幕保护的锁定，不过因为AD DS服务已经停止，而且网络上也没有其他域控制器在线，因此无法验证域系统管理员身份，也就无法解开屏幕保护的锁定。如果要更改默认登录设置的话，就可以在这个时候利用**DSRM系统管理员**账户来解除锁定。更改登录设定的方法为：运行注册表编辑器REGEDIT.EXE，然后修改或添加以下的注册值：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\DSRMAdmi
nLogonBehavior
```

DSRMAdminLogonBehavior的数据类型为REG_DWORD，它用来决定在这台域控制器以正常模式启动、但AD DS服务停止的情况下，**DSRM系统管理员**是否可以登录。

- 0：不可以登录，**DSRM系统管理员**只能够登录到**目录服务还原模式**，这是默认值。
- 1：**DSRM系统管理员**可以在AD DS服务停止的情况下登录，不过**DSRM系统管理员**不受密码策略设置的约束。在域中只有一台域控制器的情况下，或某台域控制器是在一个隔离的网络等状况下，此时或许您比较希望能够将此参数改为这个设置值。
- 2：在任何情况之下，也就是不论AD DS服务是否启动、不论是否在**目录服务还原模式**下，都可以使用**DSRM系统管理员**来登录。不建议您采用此方式，因为**DSRM系统管理员**不受密码策略设置的约束。

11-7 Active Directory回收站

在旧版的Windows系统中，系统管理员可能会因不小心将Active Directory对象删除，因而造成不少困扰，尤其是误删组织单位的话，其内所有对象都会不见。虽然系统管理员可进入

Download at http://www.pin5i.com/

目录还原模式来找回被误删的对象，不过比较耗费时间，且在**目录还原模式**这段期间内，域控制器会暂时停止对客户端提供服务。

因此在Windows Server 2008 R2中便针对此事稍作改进，例如您可以在新建用户与组账户等对象时，选择**防止意外删除**复选框（如图 11-39所示）。如果您是新建组织单位的话，系统甚至默认就会自动选择**防止意外删除**复选框。除此之外，Windows Server 2008 R2还另外添加了**Active Directory回收站**（Active Directory Recycle Bin），它让系统管理员不需要进入**目录还原模式**，就可以快速找回被删除的对象。

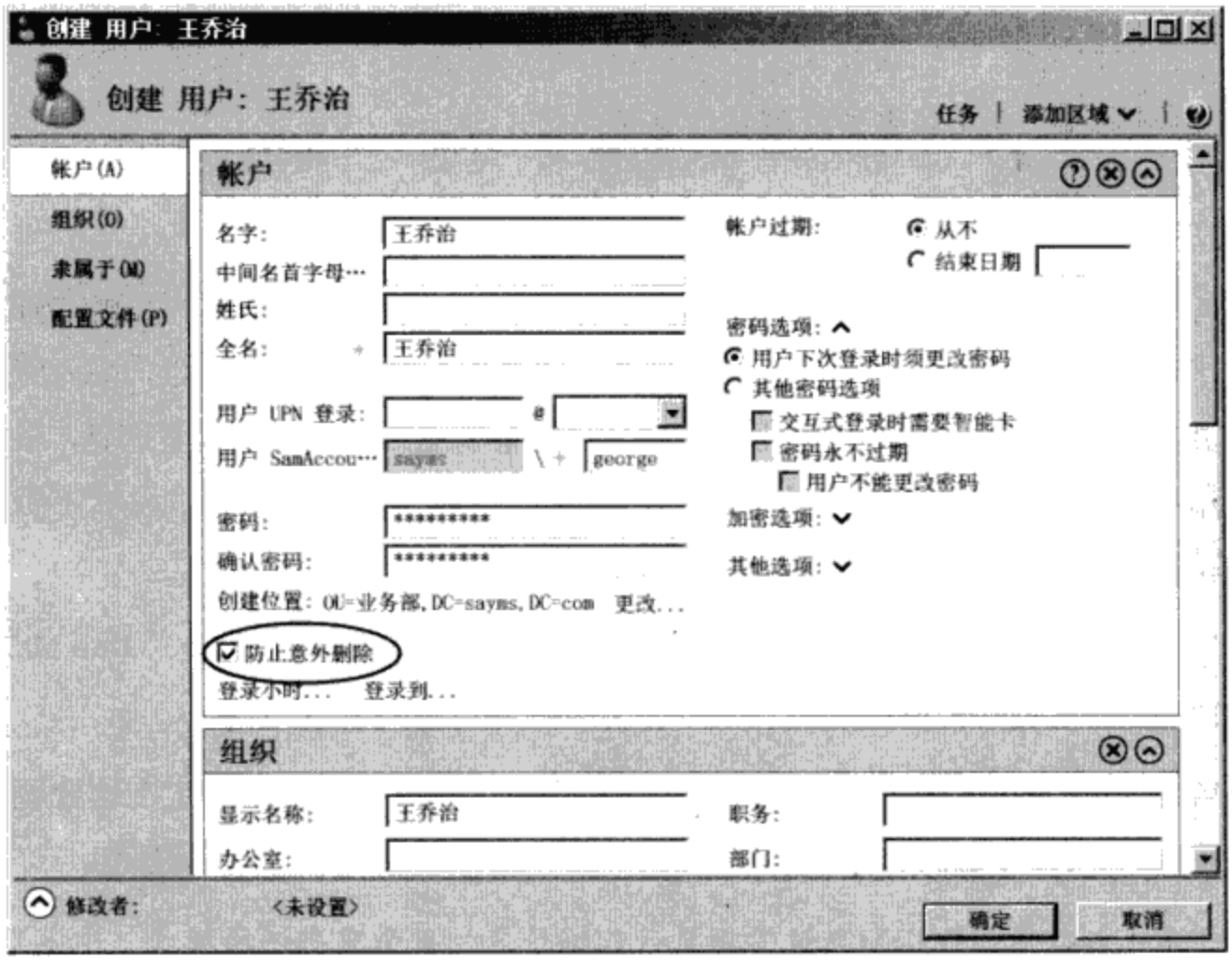


图 11-39

本节将以实例来说明如何通过**Active Directory回收站**功能来找回被删除的Active Directory对象。目前**Active Directory回收站**并未提供较友善的图形界面，因此有些工作需要通过命令来完成。

11-7-1 Active Directory回收站的系统需求

Active Directory回收站要求林功能级别必须是Windows Server 2008 R2，因此林中的所有域控制器都必须是Windows Server 2008 R2，同时所有域的域功能级别也都必须是Windows Server 2008 R2。若您的林与域功能级别尚未符合要求的话，请参考第2章的说明来提高功能级别。

Download at http://www.pin5i.com/

11-7-2 启用Active Directory回收站

我们将利用Windows PowerShell的Active Directory模块所提供的cmdlet命令来启用Active Directory回收站，不过需注意一旦启用**Active Directory回收站**后，就无法再停用，因此域与林功能级别也都无法再被降级。

STEP 1 请到一台可写的域控制器上利用系统管理员的身份登录。

STEP 2 选择【开始➲管理工具➲Windows PowerShell的Active Directory模块】。

STEP 3 如图 11-40所示执行以下命令后按Y键和Enter键，其中假设林根域的域名为sayms.com：

```
Enable-ADOptionalFeature 'Recycle Bin Feature' -scope ForestOrConfigurationSet -
Target 'sayms.com'
```

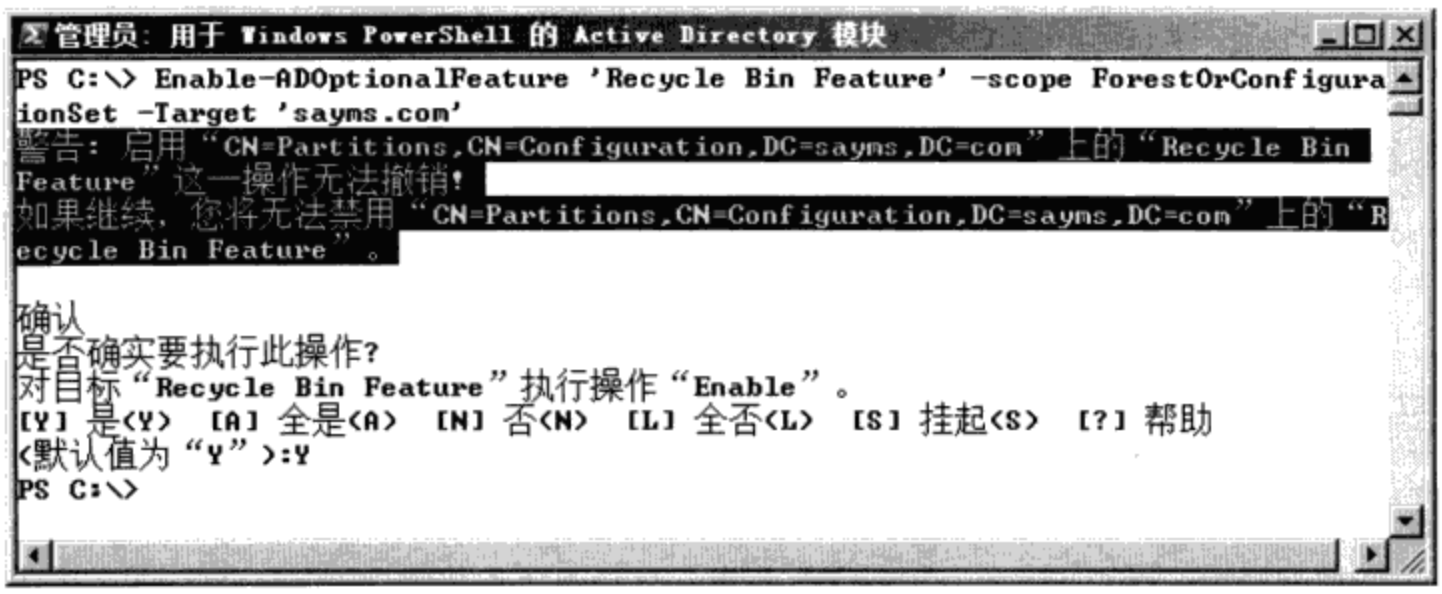


图 11-40

11-7-3 还原被删除的对象

为了便于验证**Active Directory回收站**的功能，因此请先通过**Active Directory管理中心**来删除一个用户账户（以下假设所删除的用户账户为位于**业务部**组织单位内的**王乔治**），完成后再继续以下的步骤。您可以通过以下两种方法之一来还原被删除的对象：

- 利用Windows PowerShell的Active Directory模块。
- 利用ldp.exe程序。

1. 利用 Windows PowerShell 的 Active Directory 模块来还原被删除的对象

STEP 1 到域控制器上利用系统管理员身份登录。

STEP 2 选择【开始➲管理工具➲Windows PowerShell的Active Directory模块】。

Download at http://www.pin5i.com/

STEP 3 如图 11-41所示运行以下命令来查看被删除的对象，从运行结果可看到被删除对象的显示名称为**王乔治**：

```
Get-ADObject -ldapFilter:"(msDS-LastKnownRDN=*)" -Include
DeletedObjects
```



图 11-41

STEP 4 如图 11-42所示运行以下命令来还原用户账户**王乔治**：

```
Get-ADObject -Filter {displayName -eq "王乔治"} -IncludeDeleted
Objects | Restore-ADObject
```

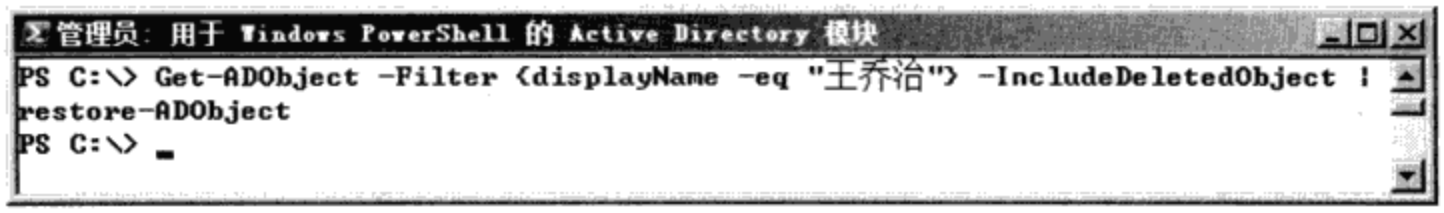


图 11-42

STEP 5 利用**Active Directory管理中心**来验证用户账户**王乔治**是否已被还原，而且这个被还原的账户也会被复制到其他的域控制器。

2. 利用 ldp.exe 程序来还原被删除的对象

STEP 1 请到域控制器上利用系统管理员的身份登录。

STEP 2 选择【开始➲运行➲输入**ldp.exe**后单击确定按钮】。

STEP 3 如图 11-43所示选择**连接**菜单中的**连接**命令。

Download at http://www.pin5i.com/

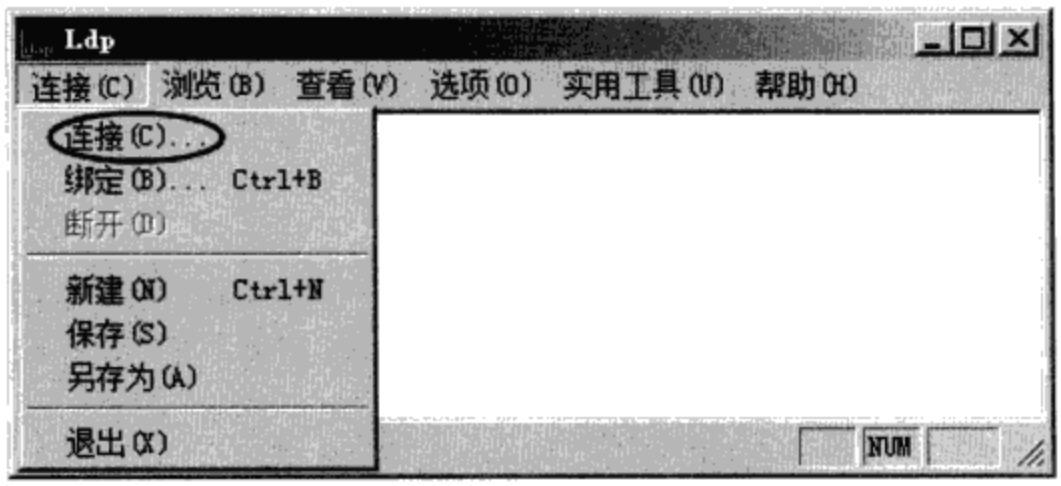


图 11-43

STEP 4 在图 11-44中的**服务器**文本框中输入林根域内的域控制器的计算机名后单击**确定**按钮，图中假设计算机名为server1。

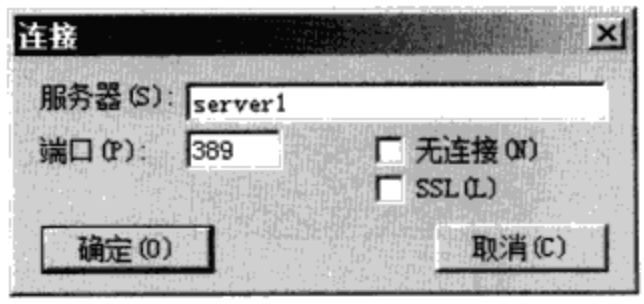


图 11-44

STEP 5 如图 11-45所示选择**连接**菜单中的**绑定**命令。



图 11-45

STEP 6 在图 11-46中直接单击**确定**按钮。

Download at http://www.pin5i.com/

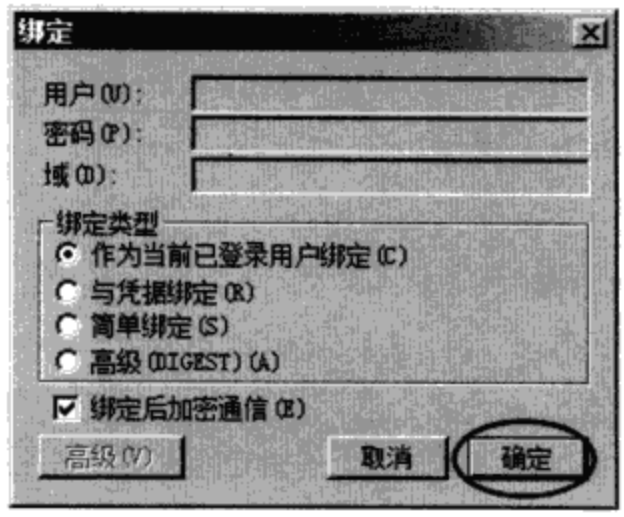


图 11-46

STEP 7 如图 11-47所示选择**查看**菜单中的**树**命令。

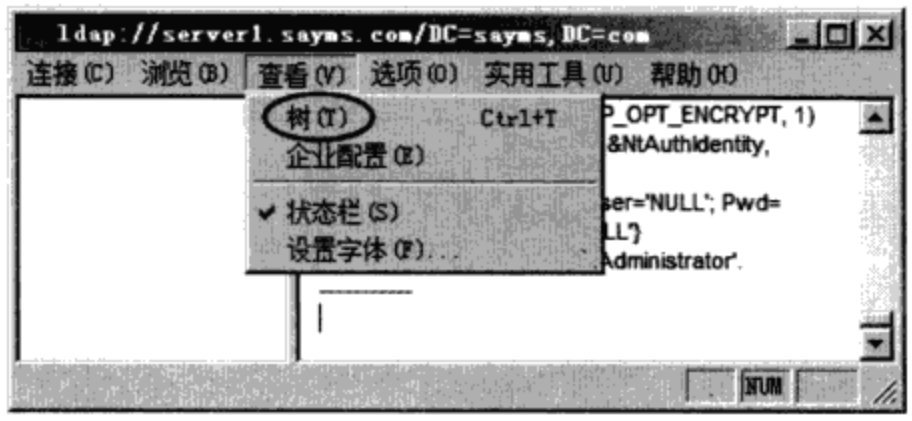


图 11-47

STEP 8 在图 11-48中输入林根域的Distinguished Name（DN）后单击确定按钮，例如我们的林根域是sayms.com，则其DN为**DC=sayms,DC=com**。

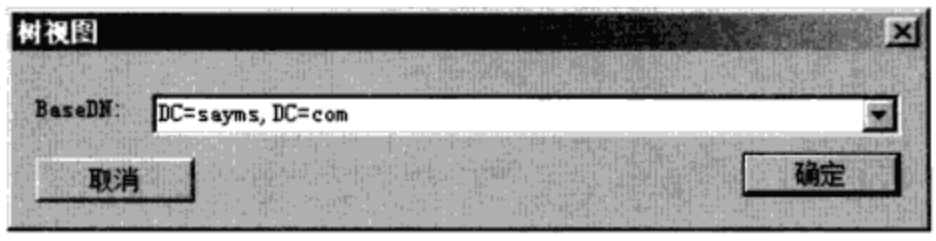


图 11-48

STEP 9 如图 11-49所示选择**选项**菜单中的**控制**命令。

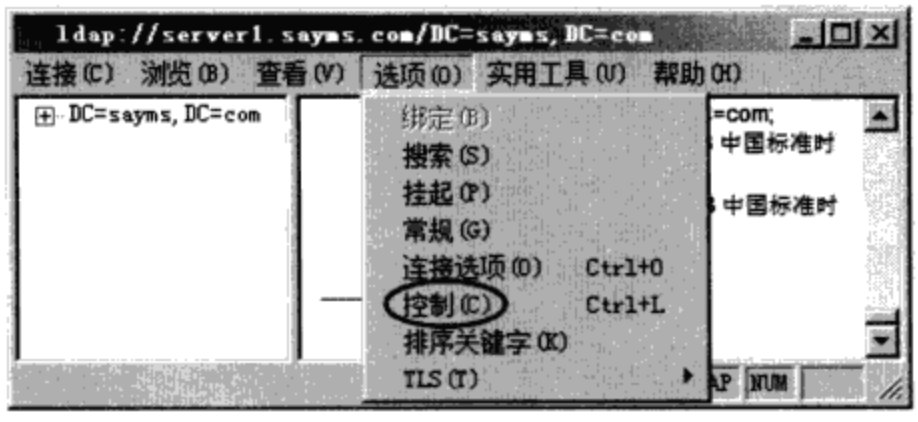


图 11-49

Download at http://www.pin5i.com/

STEP 10 如图 11-50所示选择**Return deleted objects**后单击确定按钮。

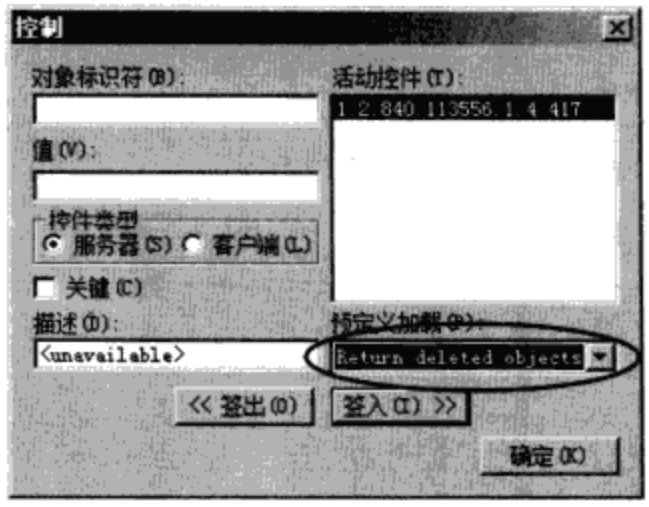


图 11-50

STEP 11 从图 11-51中可看到被删除的用户账户**王乔治**。

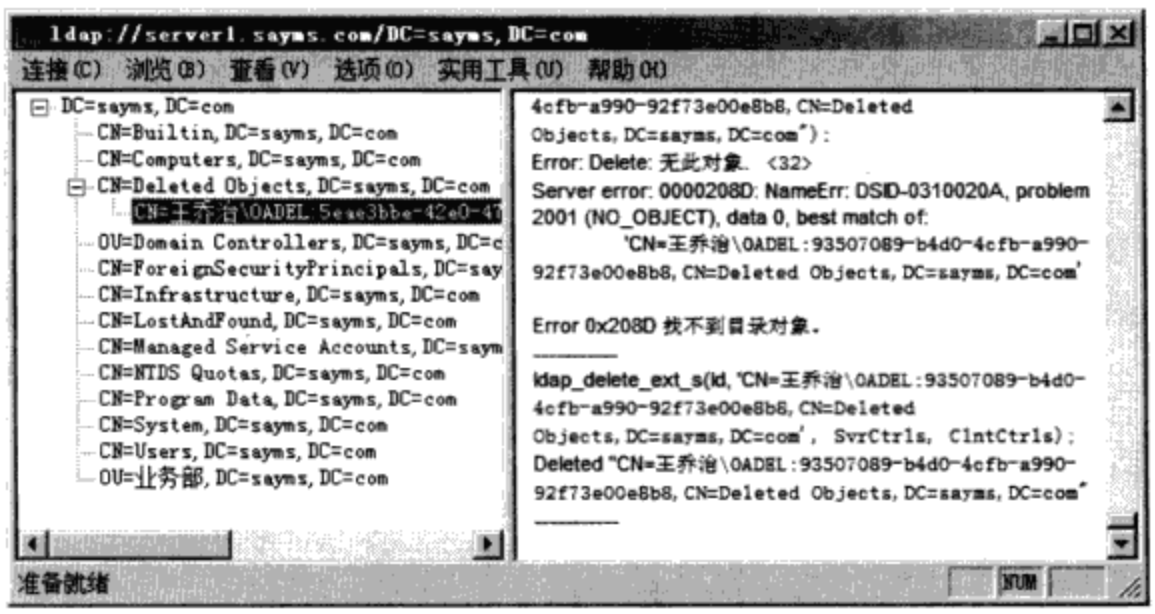


图 11-51

STEP 12 如图 11-52所示，通过【对着此用户账户单击右键➲修改】的方式进行操作。

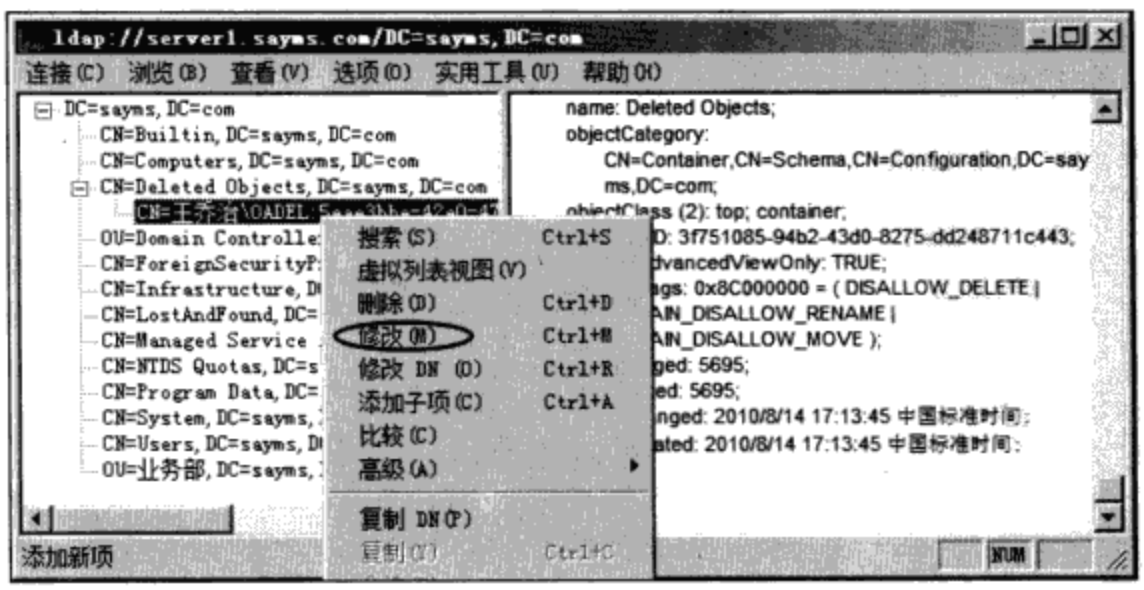


图 11-52

Download at http://www.pin5i.com/

STEP 13 在图 11-53中依照箭头编号顺序来操作，其中**属性**文本框中请输入**isDeleted**。

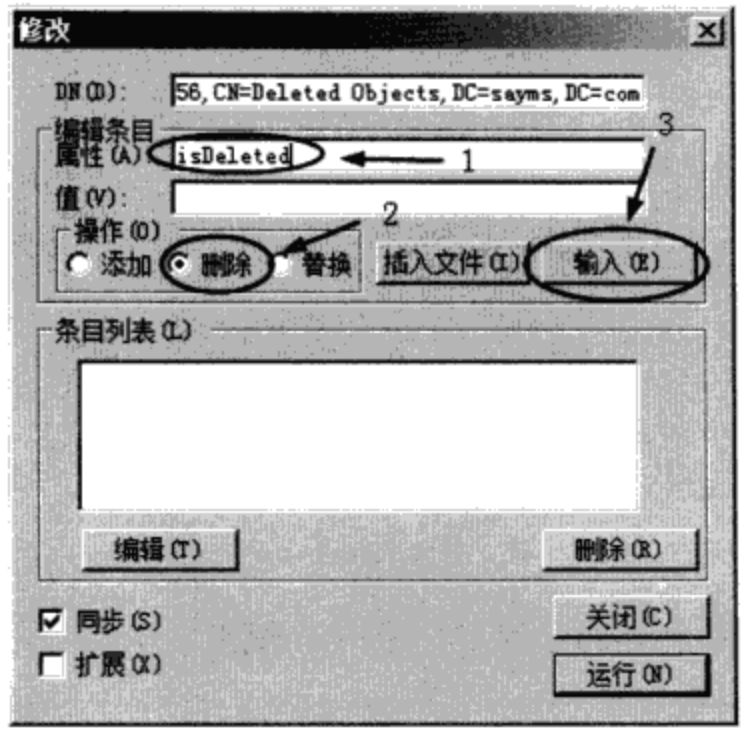


图 11-53

STEP 14 参照图 11-54中的1、2、3号箭头来设置后，单击4号箭头处的输入按钮。其中**属性**文本框中请输入**distinguishedName**，**值**文本框中请输入用户账户**王乔治**在Active Directory内原来的DN，例如图中的**cn=王乔治,ou=业务部,dc=sayms,dc=com**。

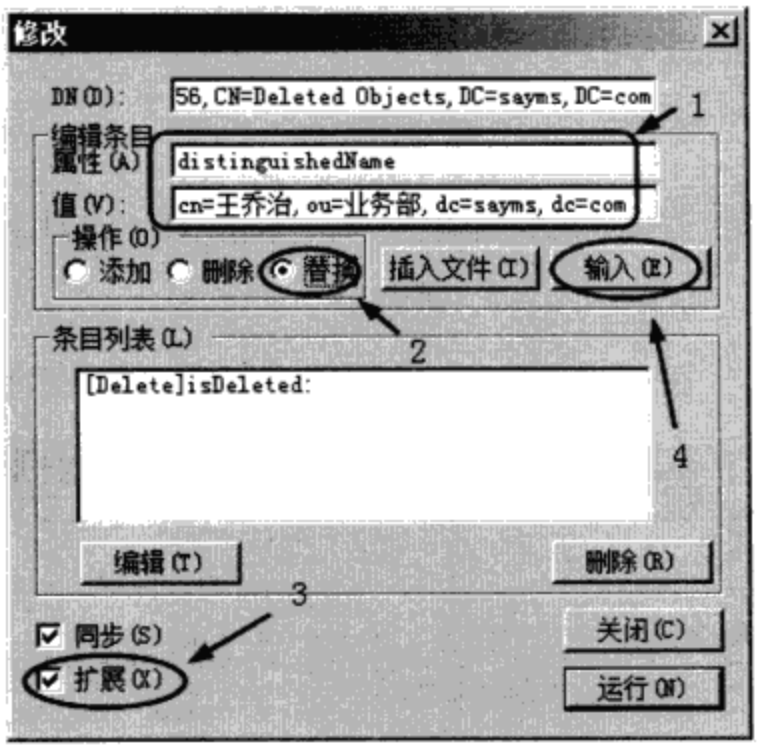


图 11-54

STEP 15 在图 11-55中单击运行按钮后就可以还原用户账户**王乔治**。

Download at http://www.pin5i.com/



图 11-55

STEP 16 利用**Active Directory管理中心**来验证用户账户**王乔治**是否已被还原，而且这个被还原的账户也会被复制到其他的域控制器。

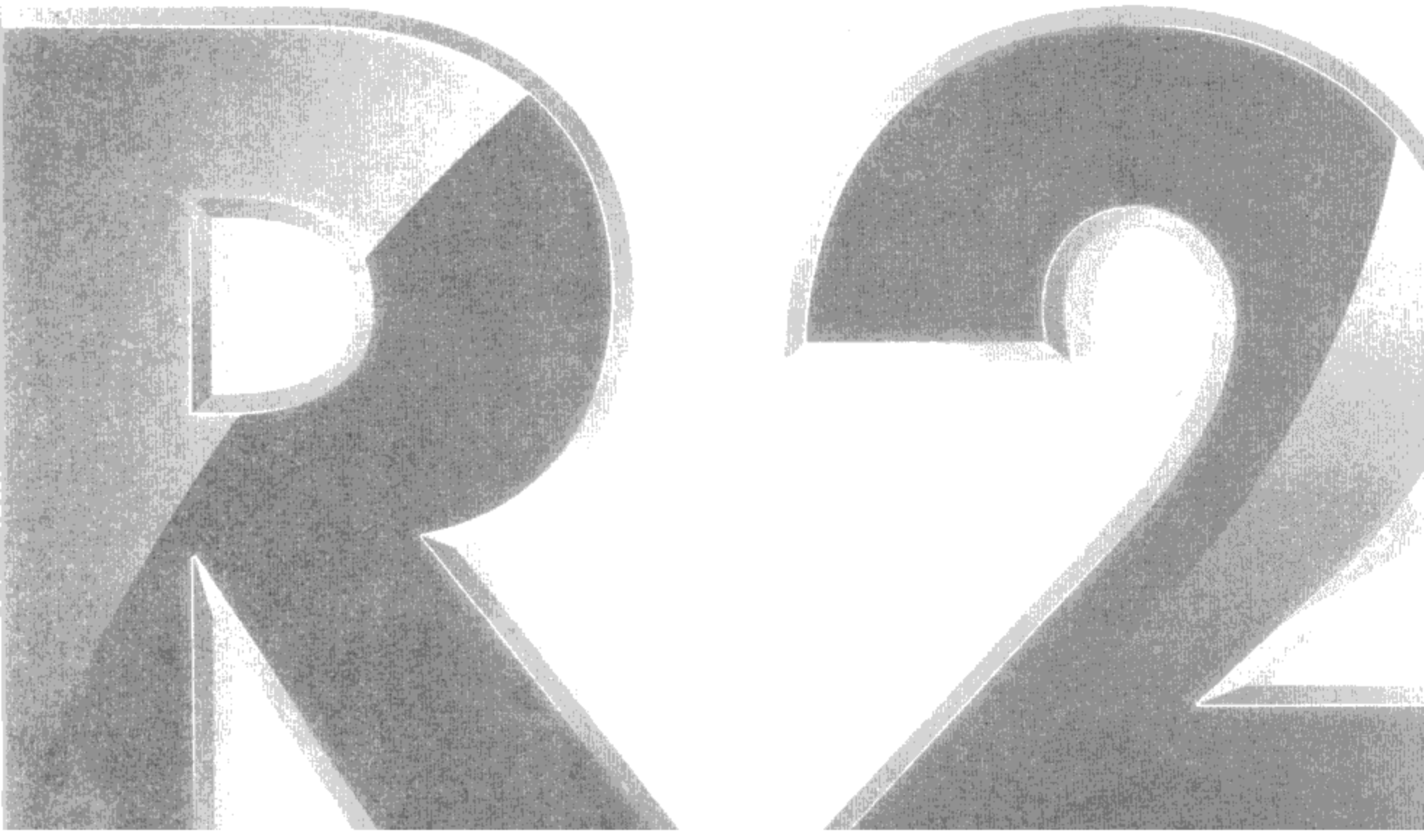
Download at http://www.pin5i.com/

第12章

将资源发布到 AD DS

将资源发布（Publish）到**Active Directory域服务**（AD DS）后，域用户便能够很方便地找到这些资源。可以被发布的资源包含用户账户、计算机账户、共享文件夹、共享打印机与网络服务等，其中有的是在新建对象时就会自动被发布，例如用户与计算机账户，而有的需要手动发布，例如共享文件夹。

- 将共享文件夹发布到AD DS
- 查找AD DS内的资源
- 将共享打印机发布到AD DS



Download at http://www.pin5i.com/

12-1 将共享文件夹发布到AD DS

将共享文件夹发布到**Active Directory域服务**（AD DS）后，域用户便能够很容易地通过AD DS找到、访问这个共享文件夹。您必须是Domain Admins或Enterprise Admins组内的用户，或是被委派权限，才可以执行发布共享文件夹的工作。

以下假设要将服务器DC1内的共享文件夹**C:\图库**，通过组织单位**业务部**来发布。请先利用**Windows资源管理器**将此文件夹设置为共享文件夹，同时假设其共享名为**图库**。

12-1-1 利用Active Directory用户和计算机控制台

STEP 1 选择【开始➲管理工具➲Active Directory用户和计算机➲如图 12-1所示对着组织单位**业务部**单击右键➲新建➲共享文件夹】。



图 12-1

STEP 2 在图 12-2中的**名称**文本框中为此共享文件夹设置名称，在**网络路径**文本框中输入此共享文件夹所在的路径**\\DC1\图库**，单击确定按钮。

Download at http://www.pin5i.com/

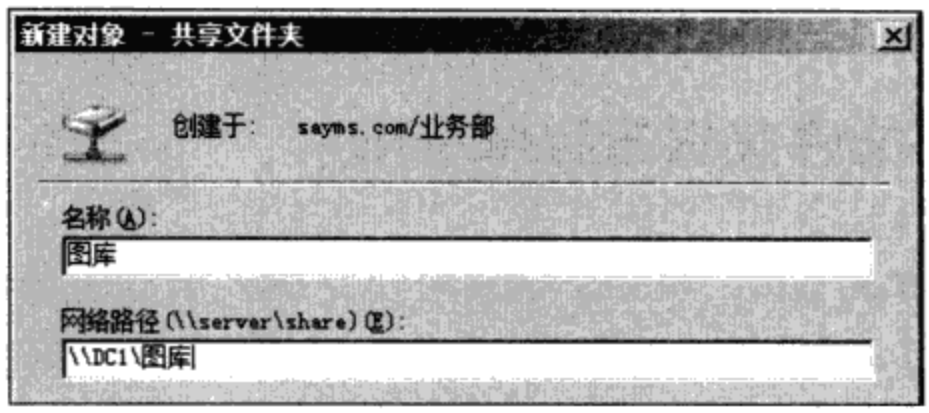


图 12-2

STEP 3 在图 12-3中双击刚才新建的对象——**图库**。

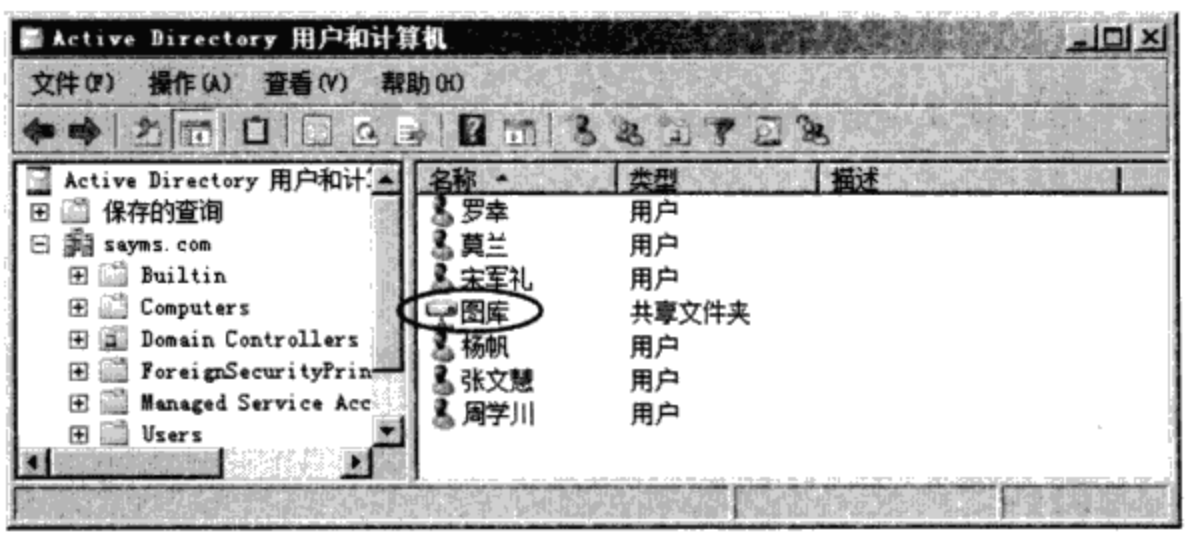


图 12-3

STEP 4 单击图 12-4中的关键字按钮。

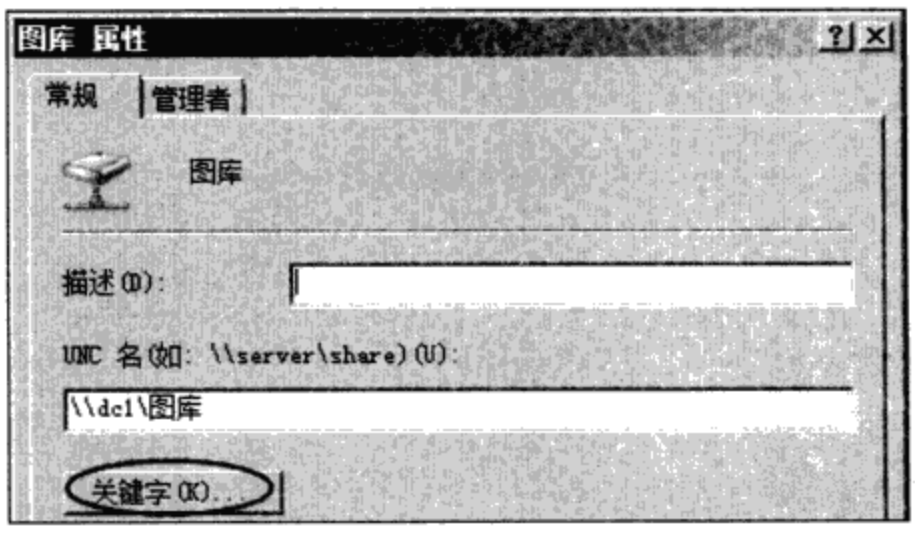


图 12-4

STEP 5 通过图 12-5来将此共享文件夹内的关键字（例如**Facebook符号**、**网络图形**等）添加到此处，让用户可以通过关键字来查找此共享文件夹，完成后单击确定按钮。

Download at http://www.pin5i.com/

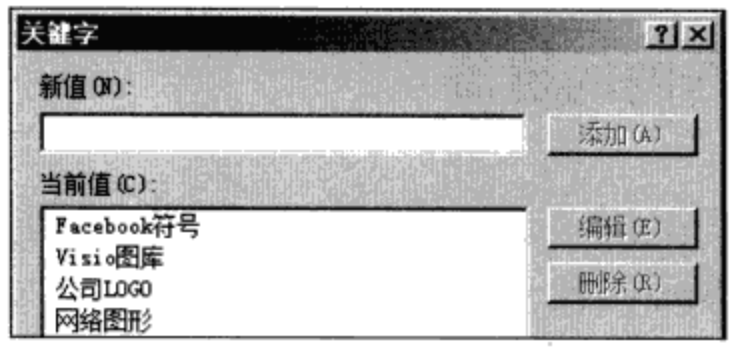


图 12-5

12-1-2 利用**计算机管理**控制台

STEP 1 请到共享文件夹所在的计算机（DC1）上选择【开始➲管理工具➲计算机管理】。

STEP 2 如图 12-6所示，通过【展开**系统工具**➲共享文件夹➲共享➲单击中间的共享文件夹**图库**➲单击上方的**属性**图标】的方式进行操作。

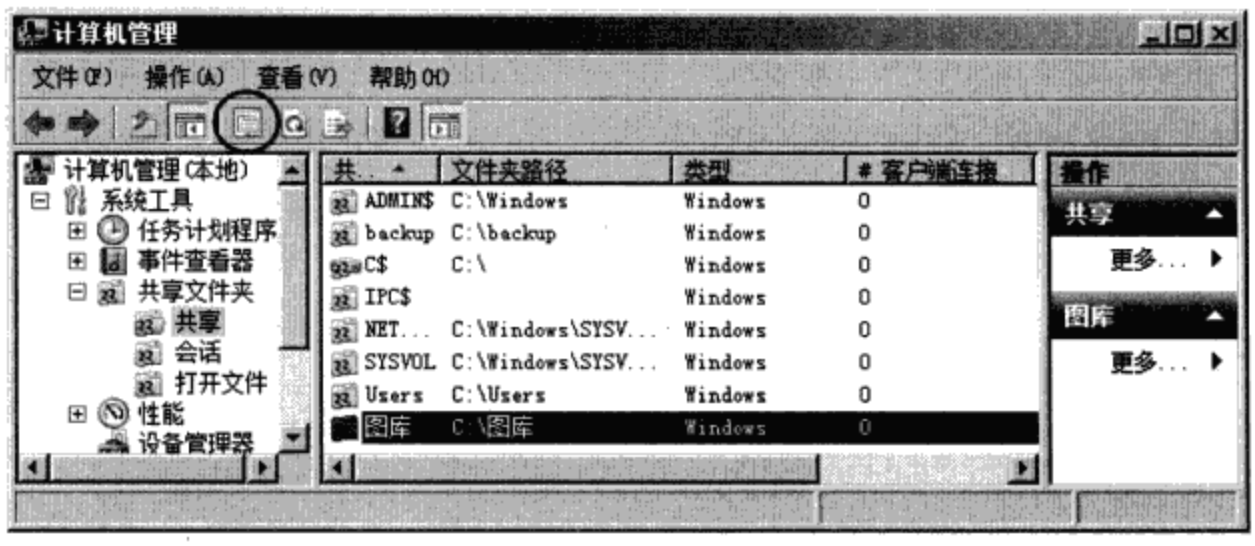


图 12-6

STEP 3 如图 12-7所示，通过【选择发布标签➲选择**将这个共享在Active Directory中发布**复选框➲单击确定按钮】的方式进行操作。您也可通过图右下方的编辑按钮来添加关键字。

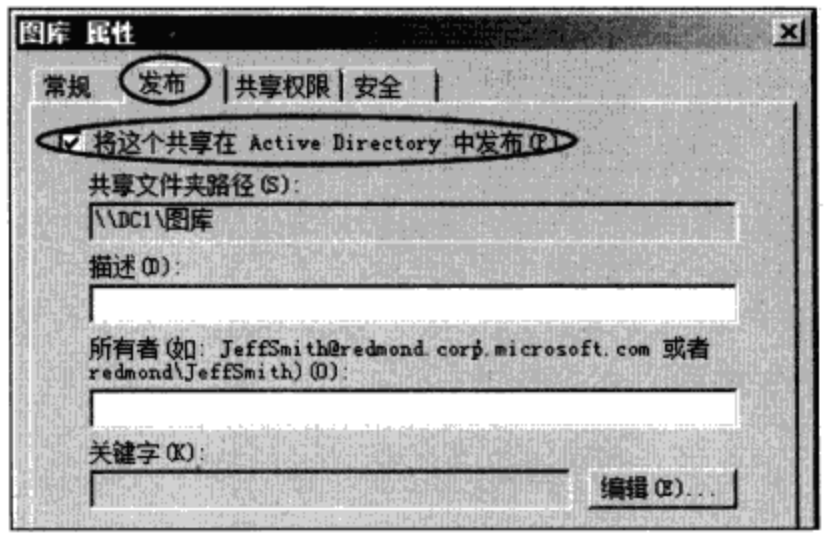


图 12-7

Download at http://www.pin5i.com/

12-2 搜索AD DS内的资源

系统管理员或用户可以通过多种途径来搜索发布在AD DS内的资源，例如可以通过网络或**Active Directory用户和计算机**控制台进行操作。

12-2-1 通过网络

以下将分别说明如何在Windows 7、Windows Vista、Windows Server 2008 R2、Windows Server 2008、Windows XP与Windows Server 2003等域成员计算机内，通过网络来搜索AD DS内的共享文件夹。

1. Windows 7、Windows Vista、Windows Server 2008 R2 与 Windows Server 2008

若是Windows 7或Windows Server 2008 R2计算机的话，请先选择【开始➲计算机➲网络】；若是Windows Vista或Windows Server 2008计算机的话，请先选择【开始➲网络➲如图 12-8所示单击**搜索Active Directory**➲在**查找**下拉列表中选择**共享文件夹**➲设置查找的条件（例如图中利用**关键字**进行设置）➲单击开始查找按钮】。

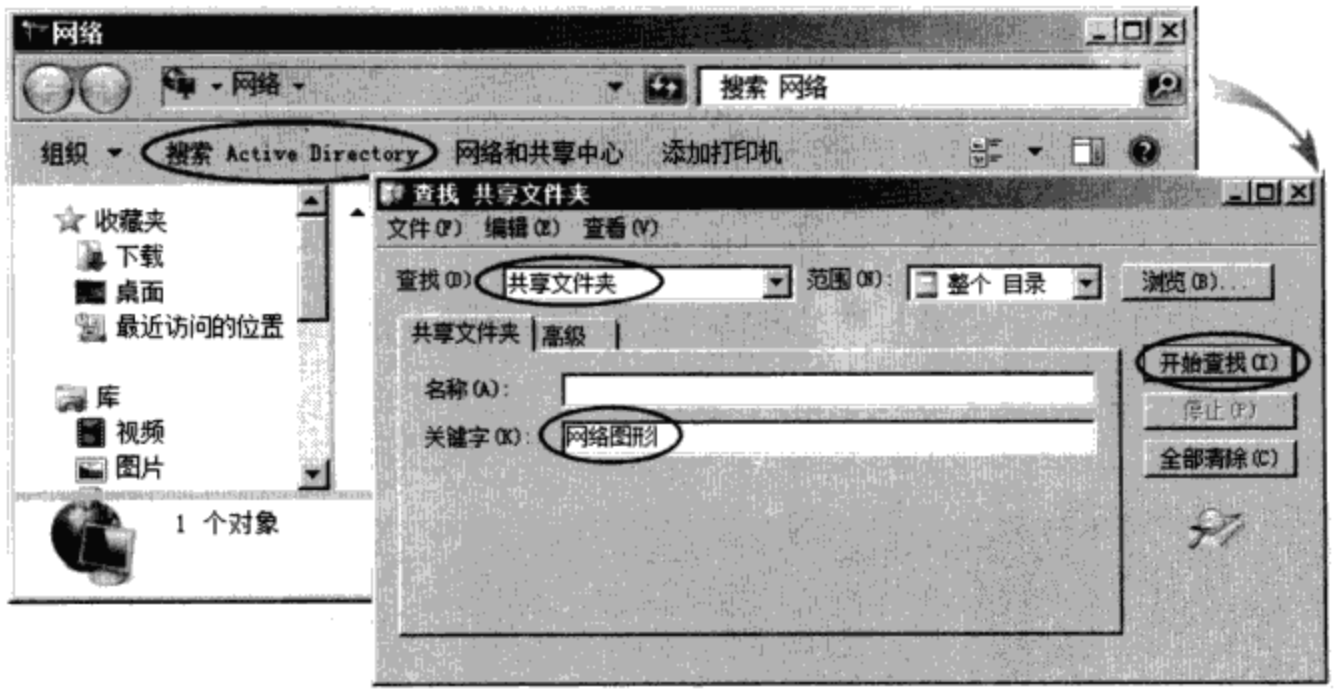


图 12-8

如图 12-9所示为搜索到的共享文件夹，您可直接双击此文件夹来访问其内的文件，或通过对着此共享文件夹单击右键的方式来管理、访问此共享文件夹。

Download at http://www.pin5i.com/

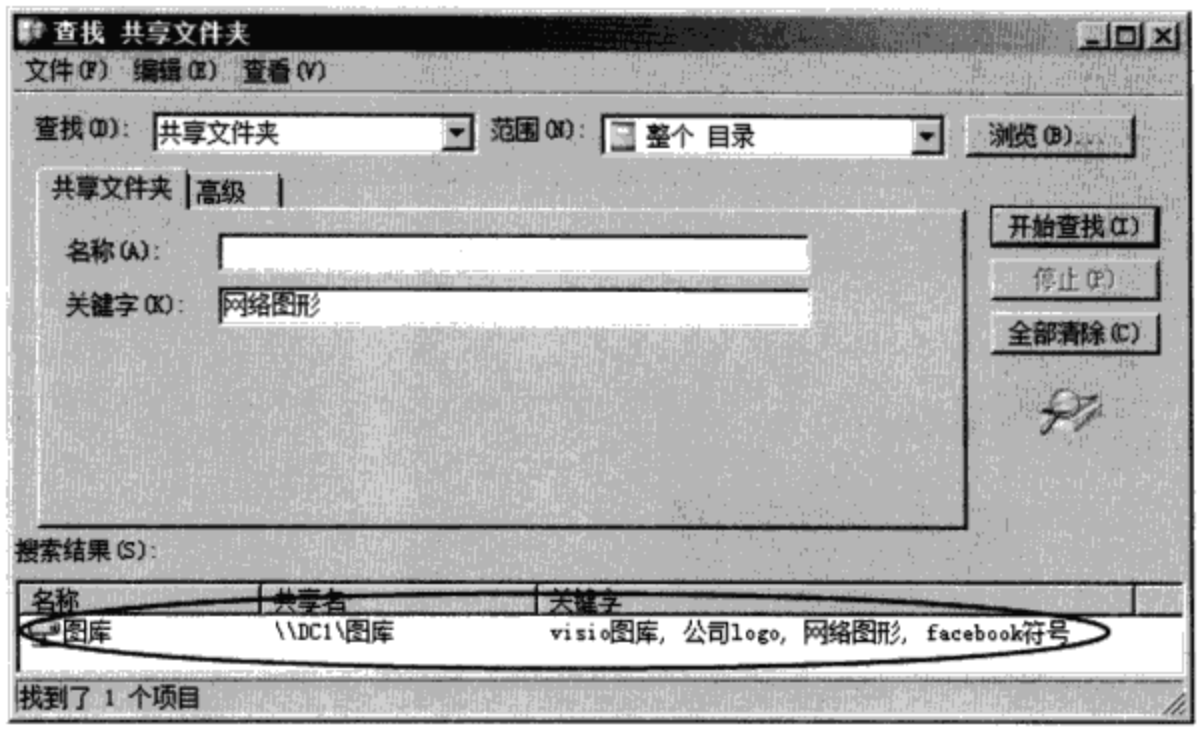


图 12-9

2. Windows Server 2003 与 Windows XP

若是Windows Server 2003的话，请通过【打开**Windows资源管理器**➲选择**工具**菜单➲文件夹选项➲在图 12-10中选择**在文件夹中显示常见任务**单选按钮➲单击确定按钮】的方式进行操作。图中的设置是Windows XP的默认值，故Windows XP不需另外设置。

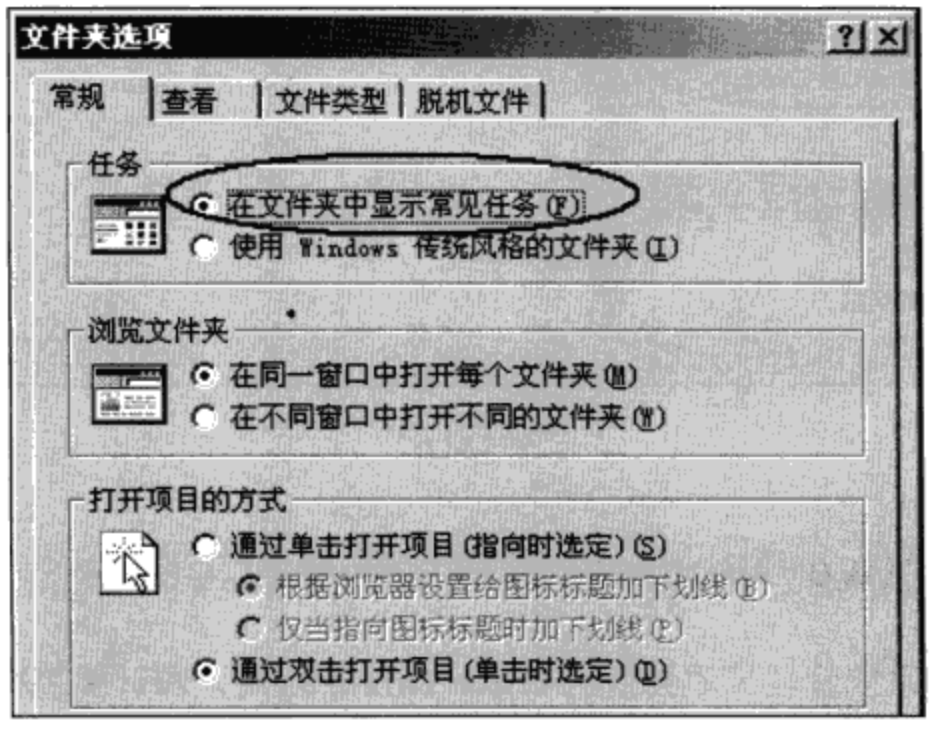


图 12-10

接着如图 12-11所示，通过【对着**网上邻居**单击右键➲打开➲然后如图 12-12所示通过单击**搜索Active Directory**来搜索共享数据】的方式进行操作。

Download at http://www.pin5i.com/

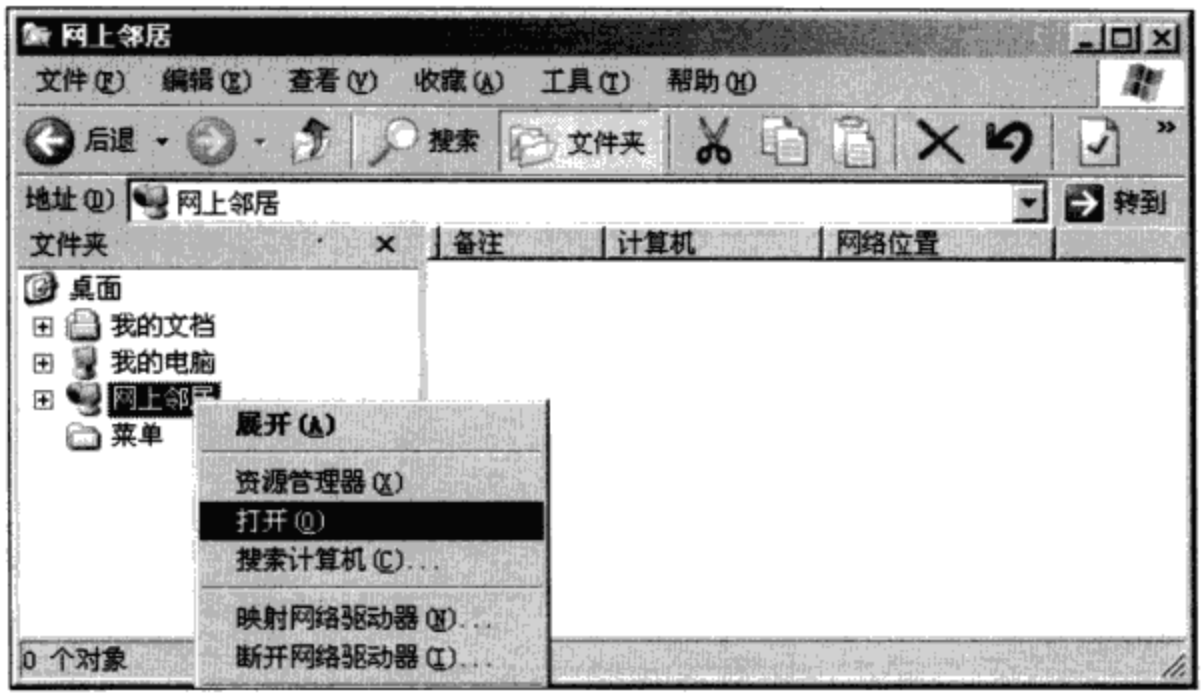


图 12-11

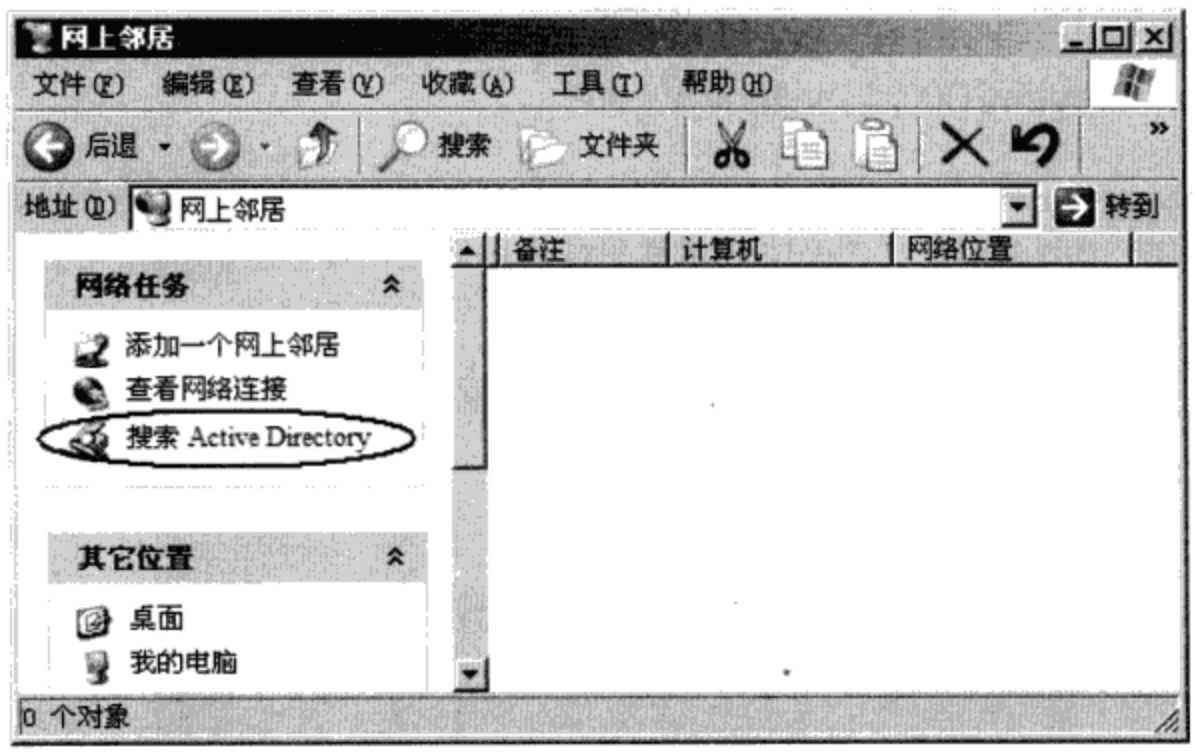


图 12-12

12-2-2 通过Active Directory用户和计算机控制台

一般来说，只有系统管理员才会使用**Active Directory用户和计算机**控制台。而这个控制台是位于【开始➲管理工具】内，不过此控制台默认只存在于域控制器，其他成员计算机需另外安装或添加。

1. 安装 Active Directory 用户和计算机控制台

在Windows Server 2008 R2、Windows 7、Windows Server 2008与Windows Vista上可以通过安装AD DS管理工具，来使用**Active Directory用户和计算机**控制台，其安装说明请参

Download at http://www.pin5i.com/

考第2-8节。

在Windows Server 2003成员服务器上可通过以下途径来使用**Active Directory用户和计算机**控制台：【开始➲运行➲输入**MMC**后单击确定按钮➲选择**文件**菜单➲添加/删除管理单元➲单击添加按钮➲如图 12-13所示选择**Active Directory用户和计算机**控制台➲单击添加按钮➲…】，完成后就可以在【开始➲管理工具】中选择**Active Directory用户和计算机**控制台。

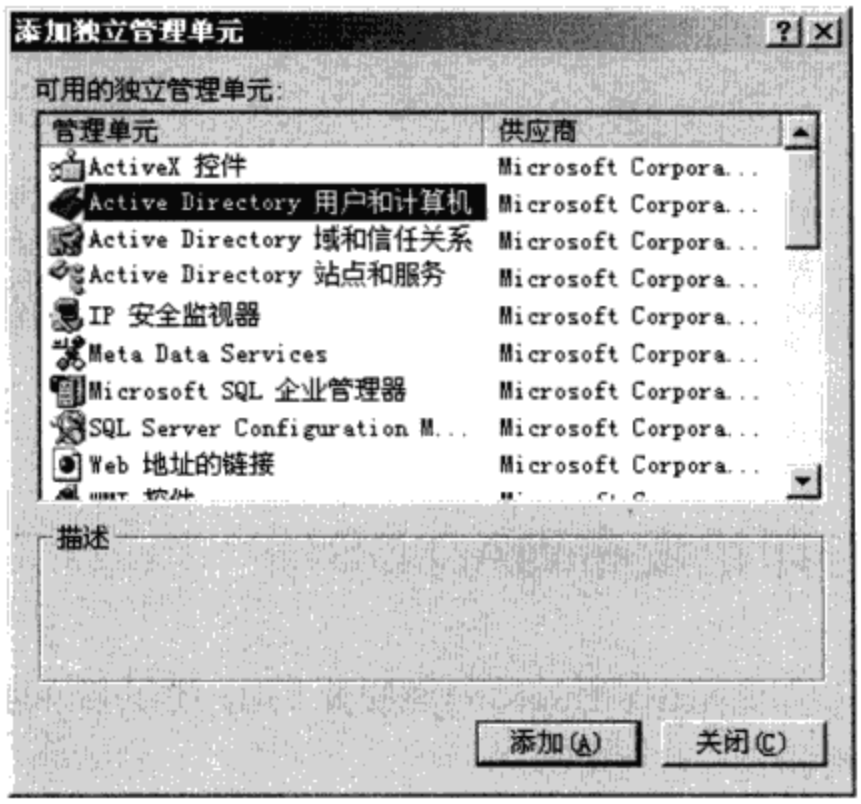


图 12-13

在Windows Server 2003成员服务器上还可以通过运行ADMINPAK.MSI来拥有**Active Directory用户和计算机**控制台，此程序位于Windows Server 2003 CD的 i386文件夹内。

加入域的Windows XP Professional也可以通过运行位于Windows Server 2003 CD的 i386文件夹内的ADMINPAK.MSI来使用**Active Directory用户和计算机**控制台。运行完成后，就可以在【开始➲管理工具】中选择**Active Directory用户和计算机**控制台。

2. 搜索共享文件夹

想要通过**Active Directory用户和计算机**控制台来查找共享文件夹的话，请如图 12-14所示进行操作：【对着域名sayms.com单击右键➲查找➲在**查找**下拉列表中选择**共享文件夹**➲设置查找的条件（例如图中利用**关键字**进行设置）➲单击立即查找按钮】。

Download at http://www.pin5i.com/

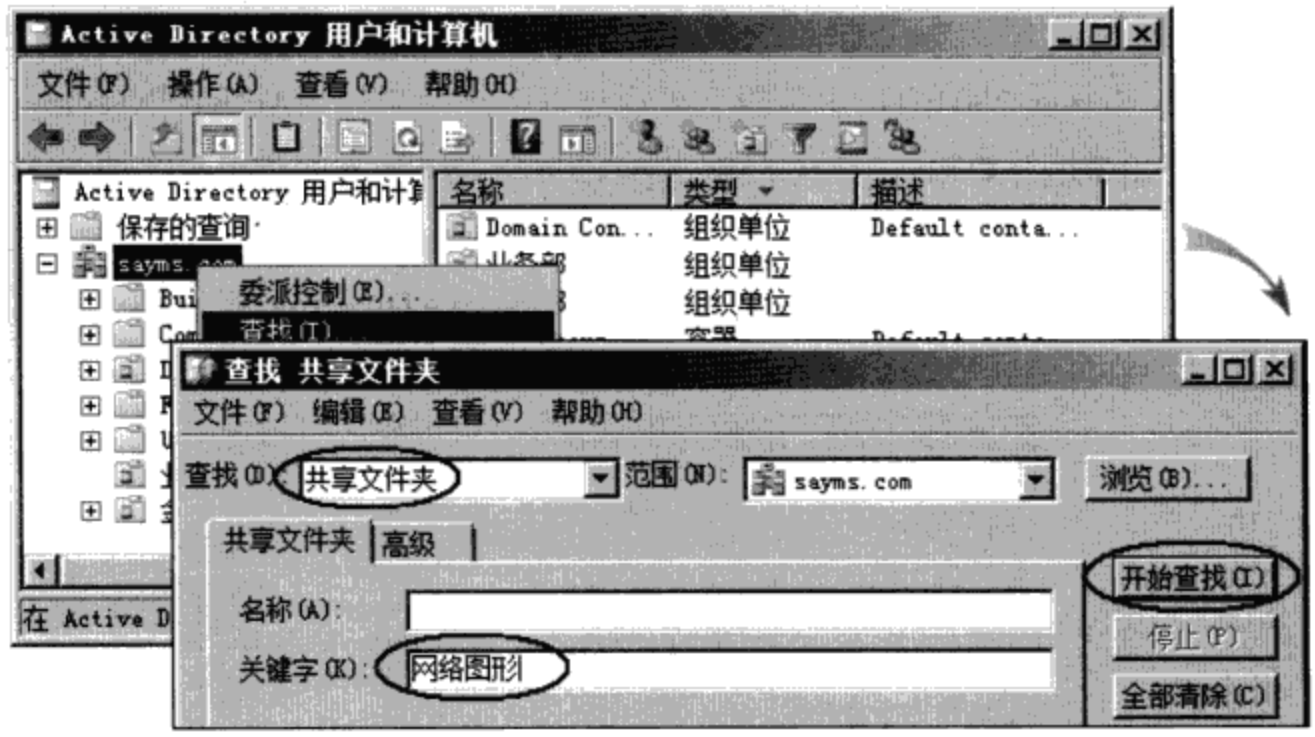


图 12-14

12-3 将共享打印机发布到AD DS

当您将共享打印机发布到**Active Directory域服务**（AD DS）后，便可以让域用户很容易地通过AD DS来找到与使用这台打印机。

12-3-1 发布打印机

域内的Windows成员计算机，有的默认会自动将共享打印机发布到AD DS，然而有的默认却需要您自行手动发布。

1. 发布 Windows Server 2008 R2、Windows 7 的共享打印机

若要将隶属于域的Windows Server 2008 R2或Windows 7内的共享打印机发布到AD DS的话，请选择【开始➲设备和打印机➲对着已经共享的打印机单击右键➲打印机属性➲如图 12-15所示单击**共享**标签➲选择**列入目录**复选框】。

Download at http://www.pin5i.com/

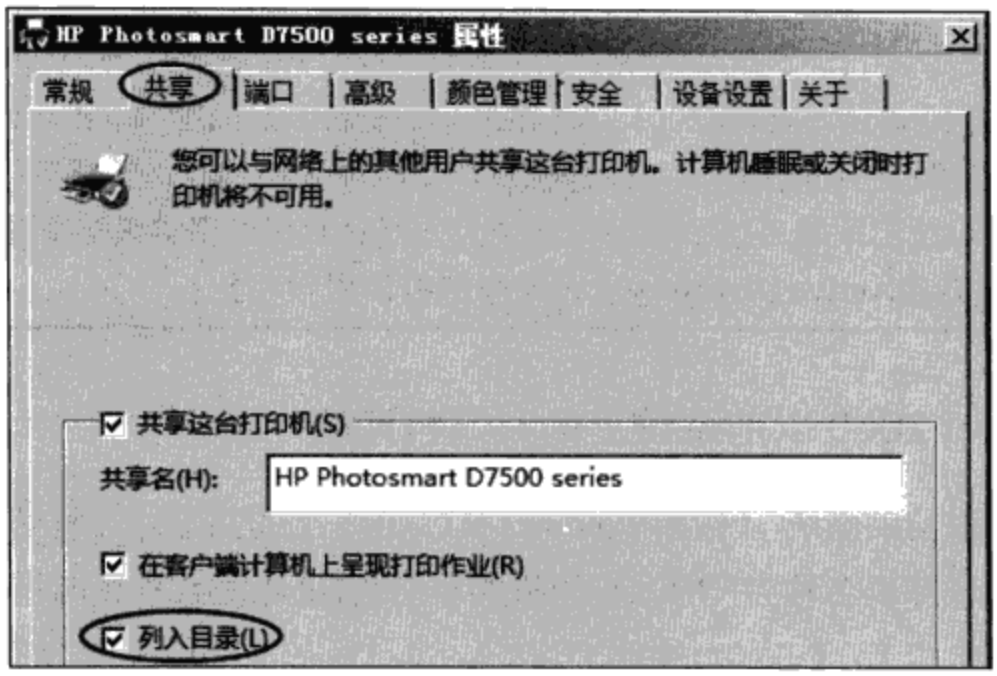


图 12-15

2. 发布 Windows Server 2008、Windows Vista 的共享打印机

若要将隶属于域的Windows Server 2008或Windows Vista内的共享打印机发布到AD DS的话，请选择【开始➲控制面板➲打印机➲对着已经共享的打印机单击右键➲属性➲如图 12-16所示单击**共享**标签➲选择**列入目录**复选框】。

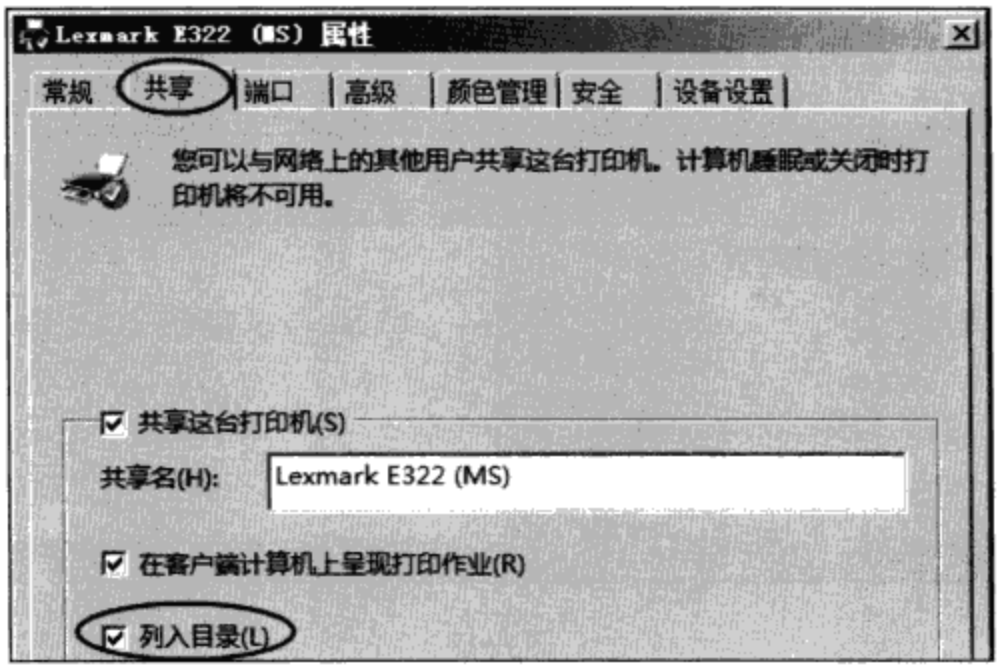


图 12-16

3. 发布 Windows Server 2003、Windows XP 的共享打印机

Windows Server 2003、Windows XP Professional或Windows 2000计算机上的共享打印机默认会自动被发布到AD DS，不需要另外发布。若要自行决定是否要发布的话，以Windows Server 2003为例，可以利用【开始➲打印机和传真➲对着已经共享的打印机单击右键➲属性➲单击**共享**标签➲选择或取消**列入目录**复选框】的方法进行操作。

Download at http://www.pin5i.com/

提示

如果您要禁用Windows Server 2003、Windows XP Professional或Windows 2000等计算机自动发布共享打印机的功能的话，可以通过域组策略或本机计算机策略来设置，以Windows Server 2008 R2域组策略来说，其设置途径为：【计算机配置➲策略➲系统管理模板➲打印机➲禁用**自动在Active Directory上公布新的打印机**策略】。

4. 发布 Windows 2000 以前系统上的共享打印机

Windows 2000以前的系统（例如Windows NT 4.0）上的共享打印机必须手动发布，举例来说，如果您要将计算机名称为NT4、打印机共享名为HP4L的共享打印机发布到组织单位**业务部**的话，其操作步骤为：【开始➲管理工具➲Active Directory用户和计算机➲如图 12-17所示对着组织单位**业务部**单击右键➲新建➲打印机➲输入共享打印机的网络路径**\\NT4\HP4L**】。

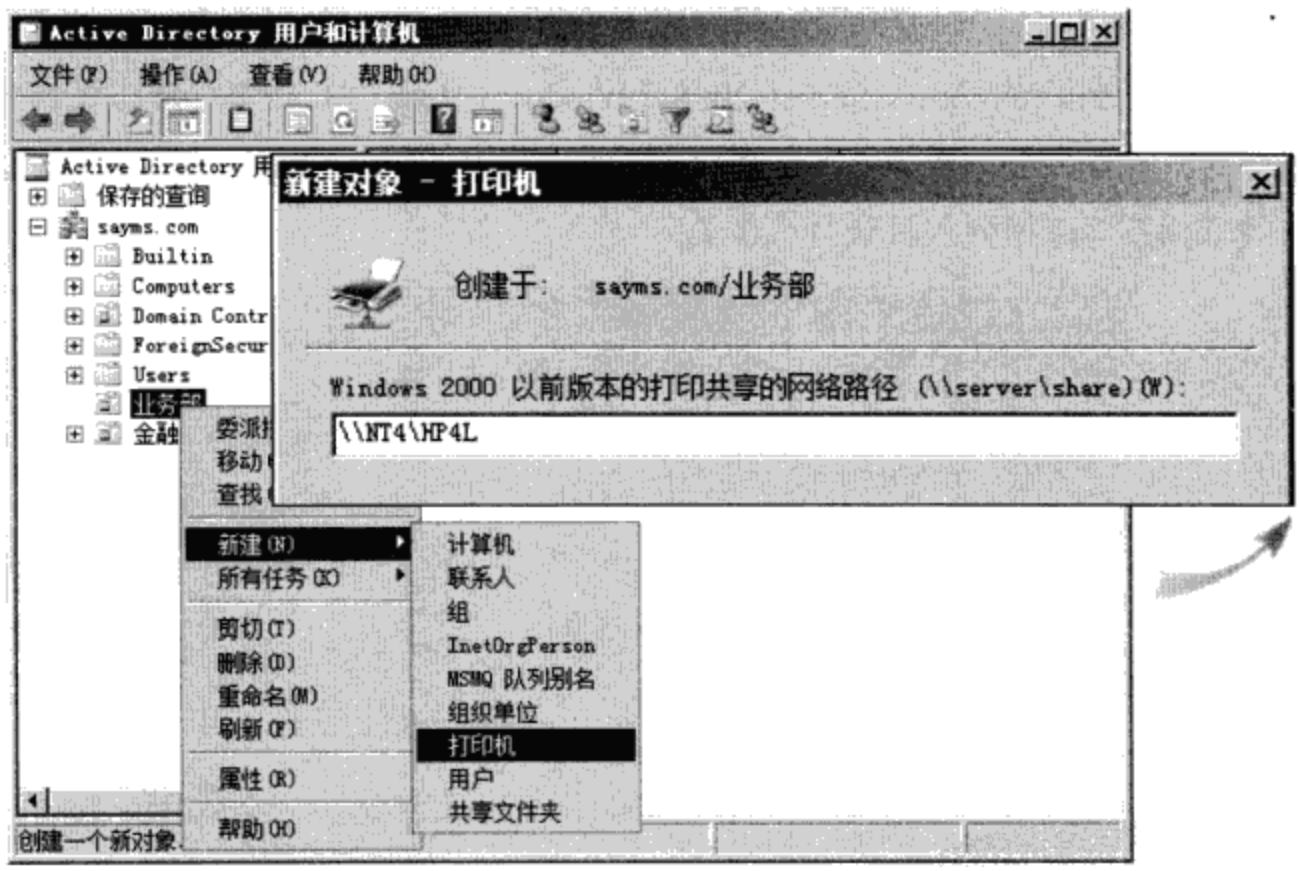


图 12-17

提示

您也可以利用**pubprn.vbs**脚本文件来将Windows NT 4.0系统上的打印机发布到AD DS，例如：

```
pubprn    \\NT4\HP4L  "LDAP://OU=业务部,DC=sayms,DC=com"
```

以Windows Server 2008 R2简体中文版为例，**Pubprn.vbs**位于**%Systemroot%\ System32\ Printing_Admin_Scripts\zh-CN**文件夹。

Download at http://www.pin5i.com/

5. 查看发布到 AD DS 的共享打印机

您可以通过**Active Directory用户和计算机**来查看已被发布到AD DS的共享打印机，如图12-18所示，通过【选择**查看**菜单➲用户、联系人、组和计算机作为容器】的方式进行操作。

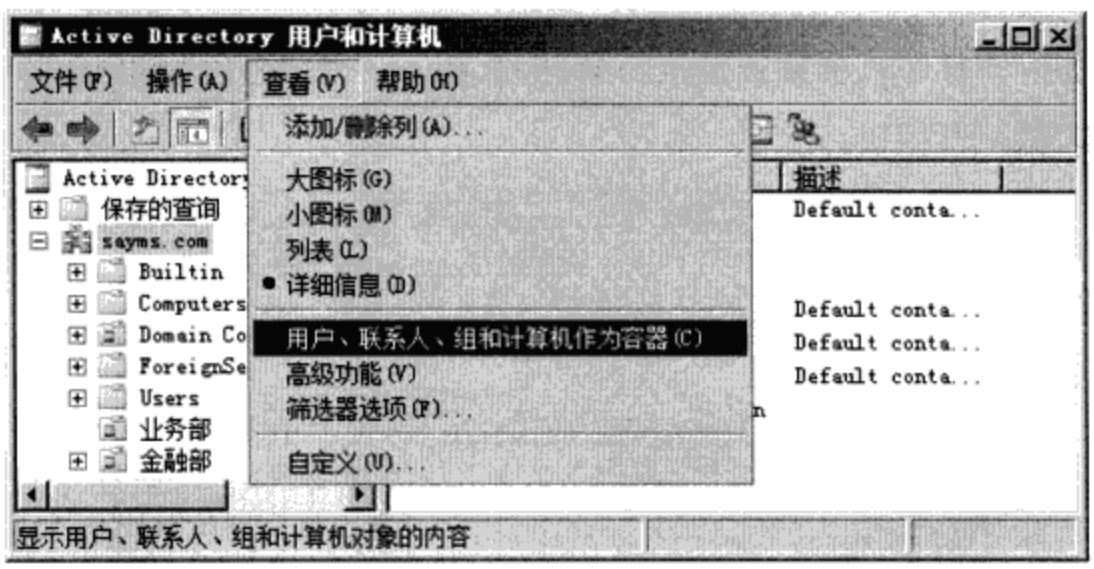


图 12-18

接着在**Active Directory用户和计算机**中选择拥有打印机的计算机后就可以看到被发布的打印机，如图 12-19所示，图中的打印机对象名称是由计算机名称与打印机名称所组成，您可以自行更改此名称。

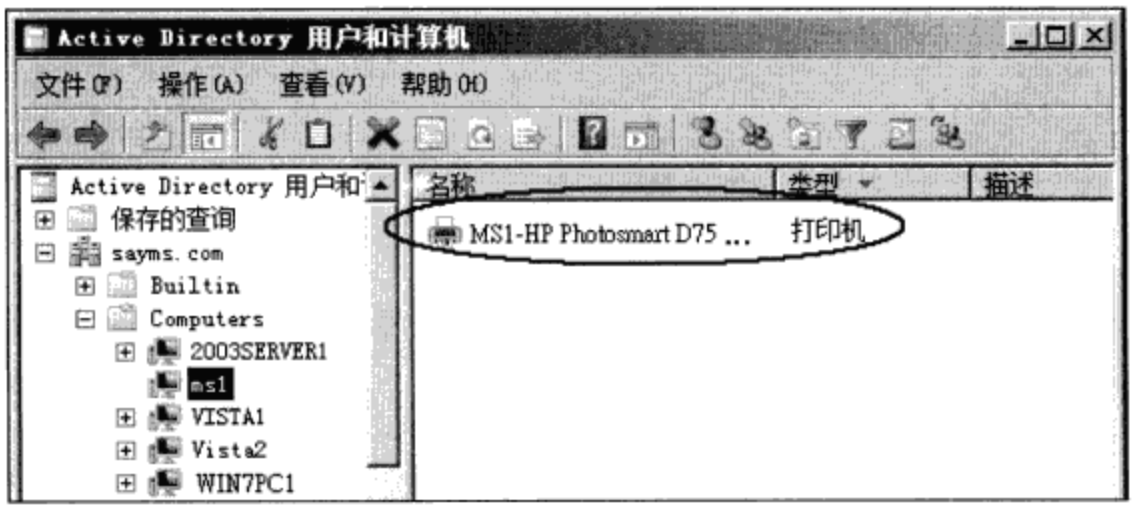


图 12-19

12-3-2 通过AD DS搜索共享打印机

系统管理员或用户利用AD DS来搜索打印机的方法，与搜索共享文件夹的方法类似，请参考**搜索AD DS内的资源**的相关说明。

12-3-3 利用打印机位置来搜索打印机

若AD DS内拥有多个站点，且每个站点内都有许多已被发布到AD DS的共享打印机的话，

Download at http://www.pin5i.com/

则通过**打印机位置**可让用户来搜索适合其使用的共享打印机。

1. 一般的打印机位置搜索功能

若您为每一台打印机都设置**位置**的话，则用户可以通过**位置**来搜索位于指定**位置**的打印机，例如图 12-20中的打印机**位置**被设置为**第1栋大楼**，则用户可以如图 12-21所示利用**位置**来查找位于**第1栋大楼**的打印机。

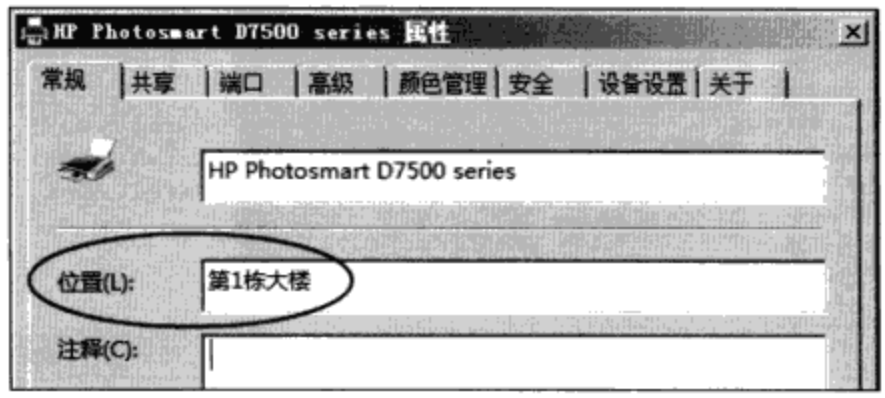


图 12-20

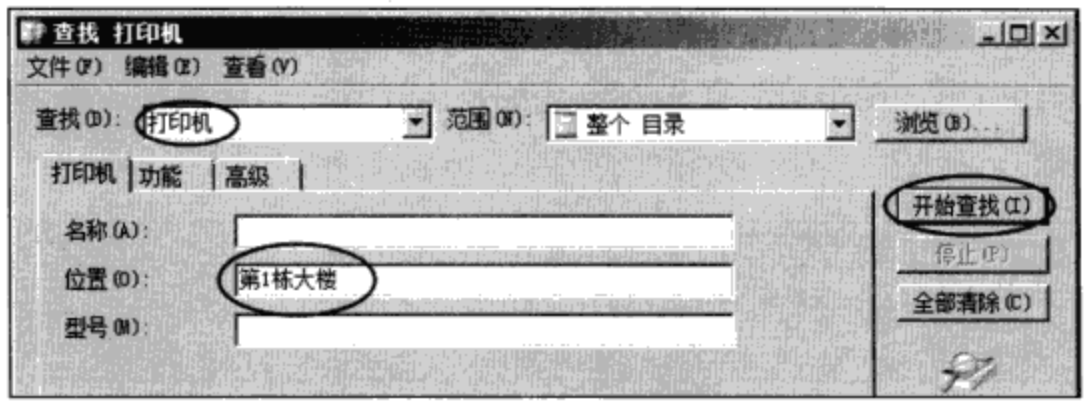


图 12-21

建议在打印机的**位置**文本框中的文字采用类似**北京/第1栋大楼**、**北京/第2栋大楼**的格式，它让用户在搜索打印机时更为方便：

- 若用户要搜索位于**北京/第1栋大楼**内的打印机时，可以在**位置**文本框中输入**北京/第1栋大楼**。
- 若用户需要同时搜索位于**北京/第1栋大楼**与**北京/第2栋大楼**的打印机时，只需要在**位置**文本框中输入**北京**即可，系统会同时搜索位于**北京/第1栋大楼**与**北京/第2栋大楼**的打印机。

2. 高级的打印机位置搜索功能

用户在利用图 12-20中的**位置**文本框来搜索打印机时，必须自行输入**北京/第1栋大楼**这些文字，如果我们能够事先做适当设置的话，就可以让系统自动为用户在**位置**文本框中输入**北京/第1栋大楼**，让用户更方便地搜索适合的打印机。

要达到上述目的的话，您就必须为每一个Active Directory站点设定**位置**，同时也为每一台

Download at http://www.pin5i.com/

打印机设定**位置**，以图 12-22为例进行说明。

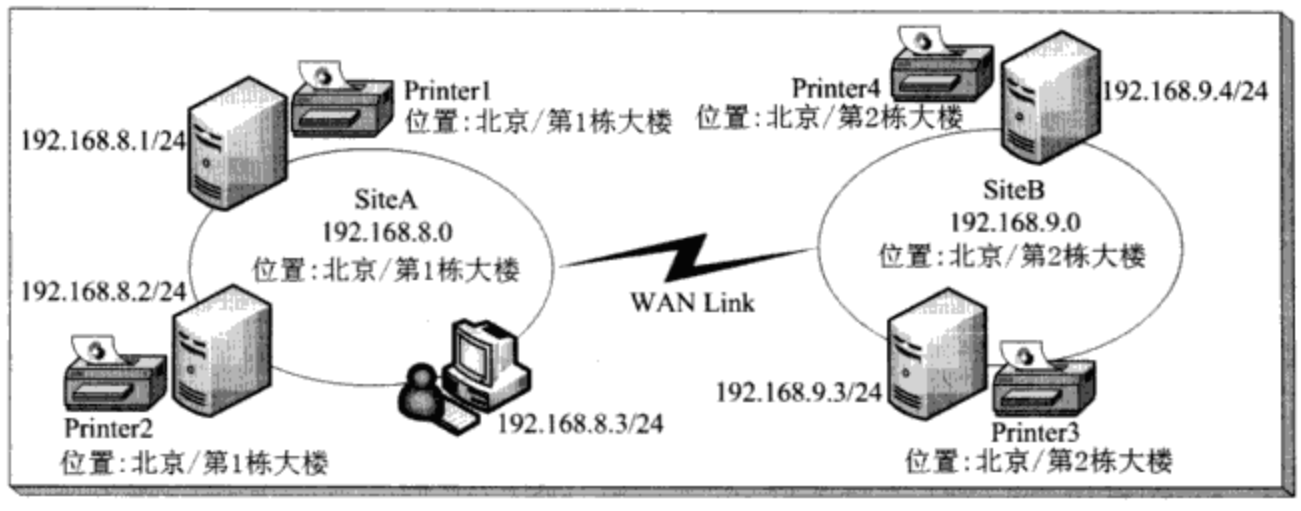


图 12-22

- 站点SiteA的**位置**被设为**北京/第1栋大楼**，同时这个站点内的每一台打印机（Printer1与Printer2）的**位置**也被设为**北京/第1栋大楼**。
- 站点SiteB的**位置**被设为**北京/第2栋大楼**，同时这个站点内的每一台打印机（Printer3与Printer4）的**位置**也都被设为**北京/第2栋大楼**。
- 由于站点SiteA内用户的计算机（IP地址192.168.8.3/24）是位于SiteA内，而SiteA的**位置**为**北京/第1栋大楼**，因此当这个用户在搜索打印机时，系统便会自动在搜索打印机的界面中的**位置**文本框中输入**北京/第1栋大楼**，不需要用户自行输入，让用户在搜索打印机时更为方便。

以上功能被称为**打印机位置追踪**（Printer Location Tracking），而这个功能的设置分为以下4大步骤。

（1）利用组策略启用**打印机位置追踪**功能

您可以针对整个域内的所有计算机或某个组织单位内的计算机来启用这个功能：【计算机配置➲策略➲管理模板➲打印机➲如图 12-23所示启用**预设打印机搜索位置文本**】，图中是利用Default Domain Policy GPO来针对域内的所有计算机来设置。

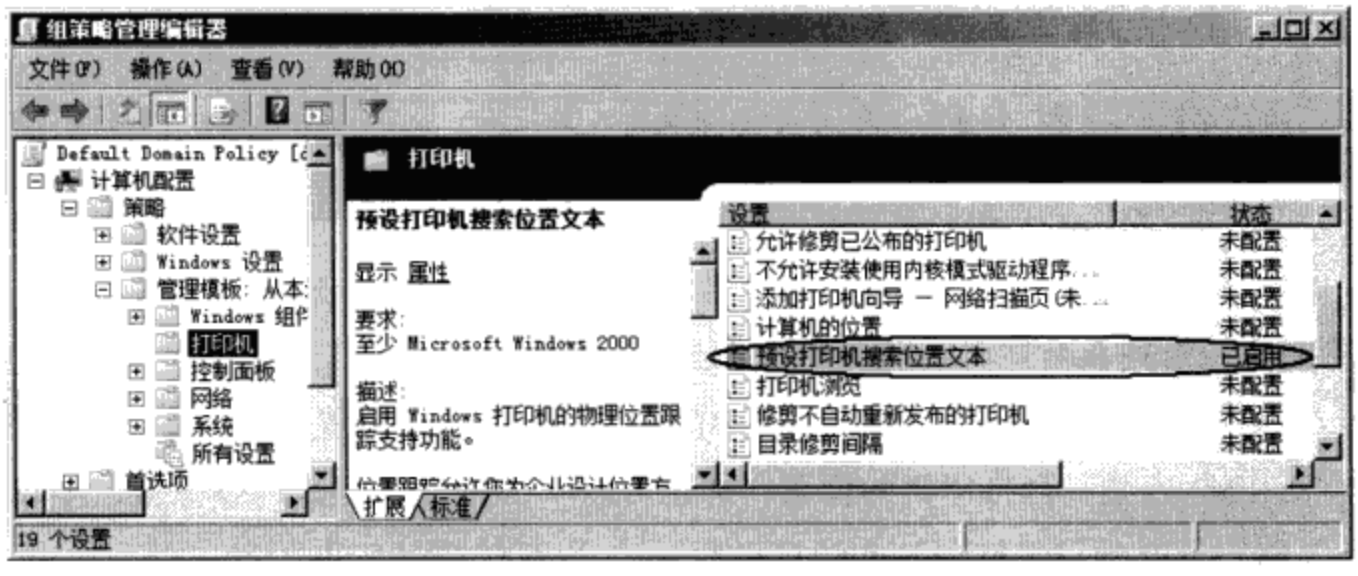


图 12-23

（2）利用 Active Directory 站点和服务新建 IP 子网

例如图 12-24中新建了192.168.8.0与192.168.9.0两个IP子网，它们分别被包含在SiteA与SiteB内。

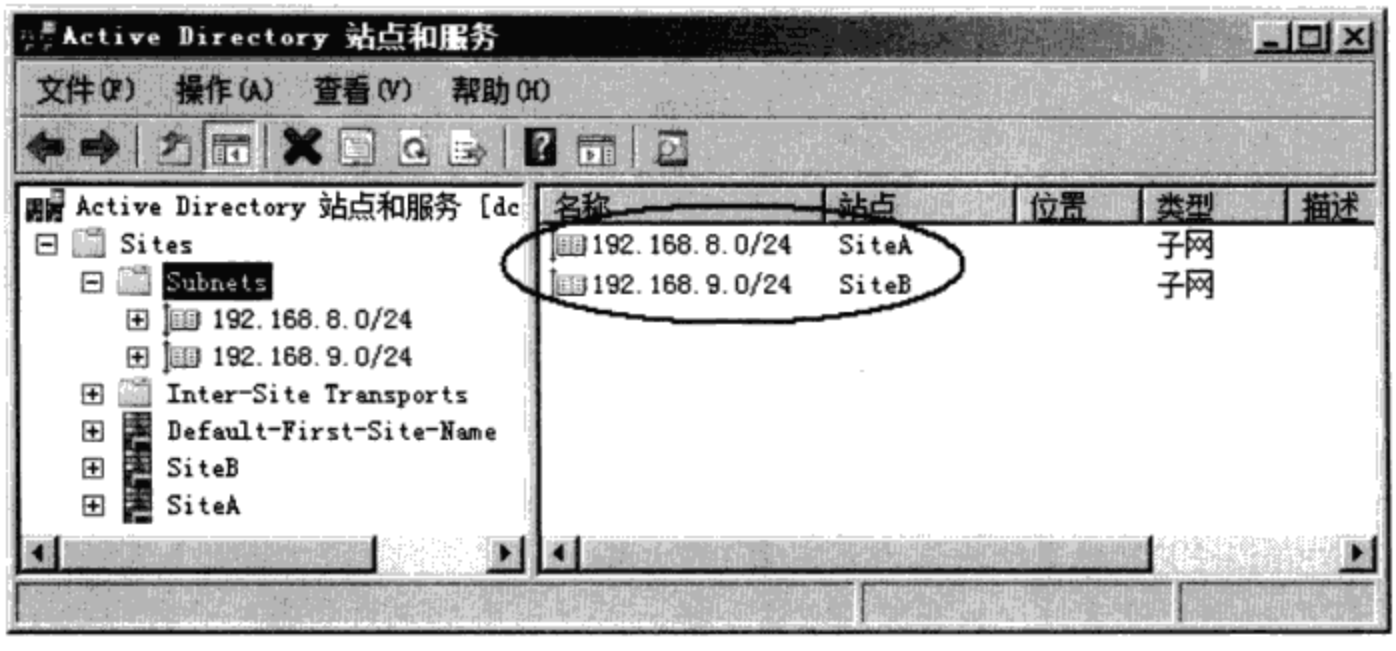


图 12-24

（3）设置每一个 IP 子网的位置

如图 12-25所示，通过【单击192.168.8.0子网➲单击上方的**属性**图标➲选择**位置**标签➲在**位置**文本框中输入**北京/第1栋大楼**】。继续将第2个子网192.168.9.0的**位置**设置为**北京/第2栋大楼**。



图 12-25

（4）到每一台连接打印机的计算机上设置打印机的位置

方法为：【对着打印机单击右键➲属性➲如图 12-26所示在**位置**文本框中输入其位置字符串】，图中为SiteA内某一台打印机的**位置**。您也可以单击浏览按钮来选择**位置**，不过第1个步骤中的组策略设置必须已经应用到此计算机后，才会出现浏览按钮。

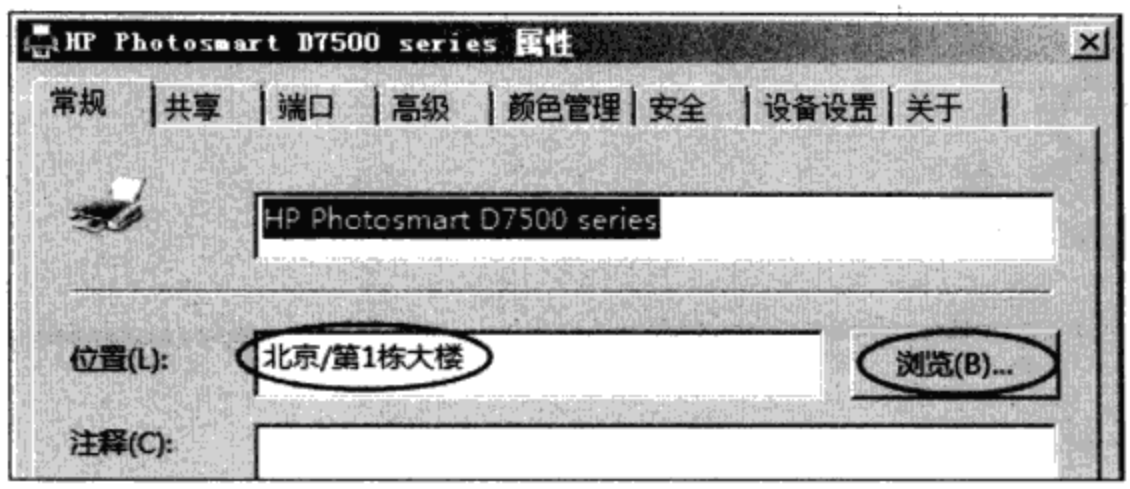


图 12-26

提示

您也可以通过Windows Server 2008 R2的**打印管理**控制台来集中设置每一台打印机的**位置**，而您可以通过安装**打印和文件服务**角色的方式来拥有**打印管理**控制台。安装完成后，可通过【开始➲管理工具➲打印管理】来使用此控制台。

完成以上设置后，用户在搜索打印机时，系统就会自动为用户在**位置**文本框中输入正确的位置字符串，如图 12-27所示。

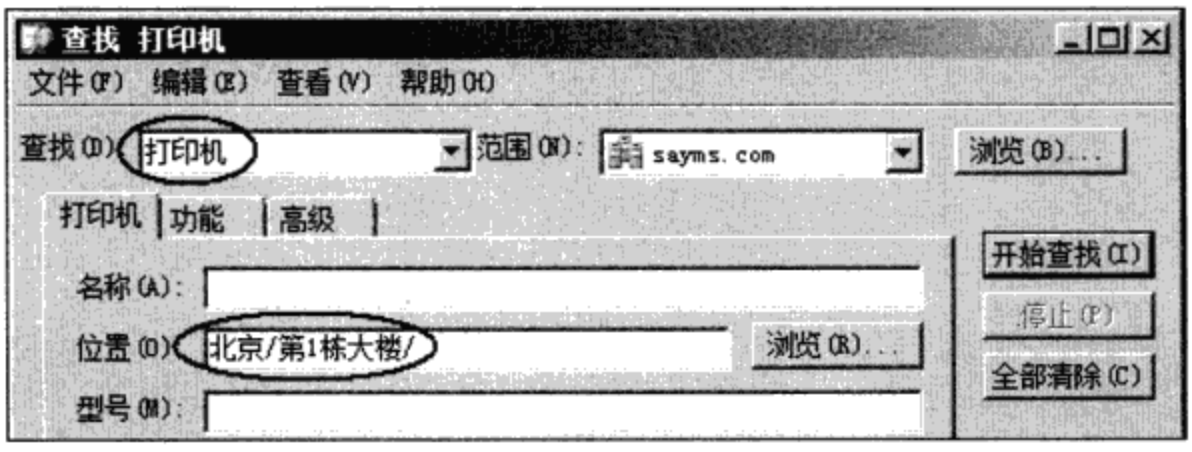


图 12-27

第13章

自动信任根 CA

在PKI（Public Key Infrastructure 公钥基础结构）的架构下，企业可以通过向CA（Certification Authority，证书颁发机构）所申请到的证书，来确保数据在网络上传送的安全性，然而用户的计算机需要信任发放证书的CA。本章将介绍如何通过AD DS的组策略，来让域内的计算机自动信任指定的**根CA**（Root CA）。

- 自动信任CA的设置准则
- 自动信任内部的独立CA
- 自动信任外部的CA



13-1 自动信任CA的设置准则

您可以通过AD DS组策略（Group Policy），来让域内所有计算机都自动信任指定的根CA，也就是自动将这些根CA的证书发送、安装到域内所有的计算机：

- 如果是企业根CA（Enterprise Root CA），则您不需要另外设置组策略，因为AD DS会自动通过组策略将企业根CA的证书发送到域内所有计算机，也就是说域内所有计算机都会自动信任企业根CA。
- 如果是安装在成员服务器上的独立根CA（Stand-alone Root CA），而且是由具备访问AD DS权限的域系统管理员所安装的，则您也不需要另外设置组策略，因为AD DS会自动通过组策略将此独立根CA的证书发送到域内所有计算机。
- 如果是安装在独立服务器的独立根CA，或是安装在成员服务器上的独立根CA，但执行安装工作的用户不具备访问AD DS的权限，则您需要另外通过**受信任的根证书颁发机构**（Trusted Root Certificate Authority Policy）策略，来将此独立根CA的证书自动发送到域内所有计算机。
- 如果不是架设在公司内部的独立根CA，而是外界的独立根CA，则需要另外通过**企业信任**（Enterprise Trust Policy）策略，来将此独立根CA的证书自动发送到域内所有计算机。

提示

Windows计算机只要信任了根CA，它们默认就会自动信任根CA之下所有的子级CA（Subordinate CA）。

我们将针对后面两种情况，说明如何利用**受信任的根证书颁发机构**策略与**企业信任**策略，来让域内的计算机自动信任我们所指定的独立根CA。

13-2 自动信任内部的独立CA

若公司内部的独立根CA是利用Windows Server 2008 R2（或Windows Server 2008）Active Directory 证书服务或Windows Server 2003 Certificate Services所架设的，而且是安装在独立服务器，或安装在成员服务器，但执行安装工作的用户不具备访问AD DS权限的话，则您需要通过**受信任的根证书颁发机构**策略来将此独立根CA的证书，自动发送到域内的计算机，也就是让域内的计算机都自动信任此独立根CA。我们将利用以下两大步骤来练习将独立根CA **MS1-Standalone Root CA**的证书，自动发送到域内的所有计算机：

- 下载独立根CA的证书并存档。
- 将独立根CA的证书导入到**受信任的根证书颁发机构**策略。

13-2-1 下载独立根CA的证书并保存

STEP 1 请到域控制器或任何一台计算机上运行网页浏览器Internet Explorer，并输入以下的URL路径：

```
http://CA的主机名、计算机名或IP地址/certsrv
```

以下利用IP地址来举例，并假设CA的IP地址为192.168.8.11。

> **提示**
>
> 如果运行Internet Explorer的计算机为Windows Server 2008 R2或Windows Server 2008的话，可暂时先将其**Internet Explorer增强的安全配置**（IE ESC）禁用，否则系统会阻挡连接CA网站：【单击左下角的**服务器管理器**图标➲单击**配置IE ESC**➲选择**管理员**处的**关闭**】选项。

STEP 2 在图 13-1中单击**下载CA证书、证书链或CRL**链接。

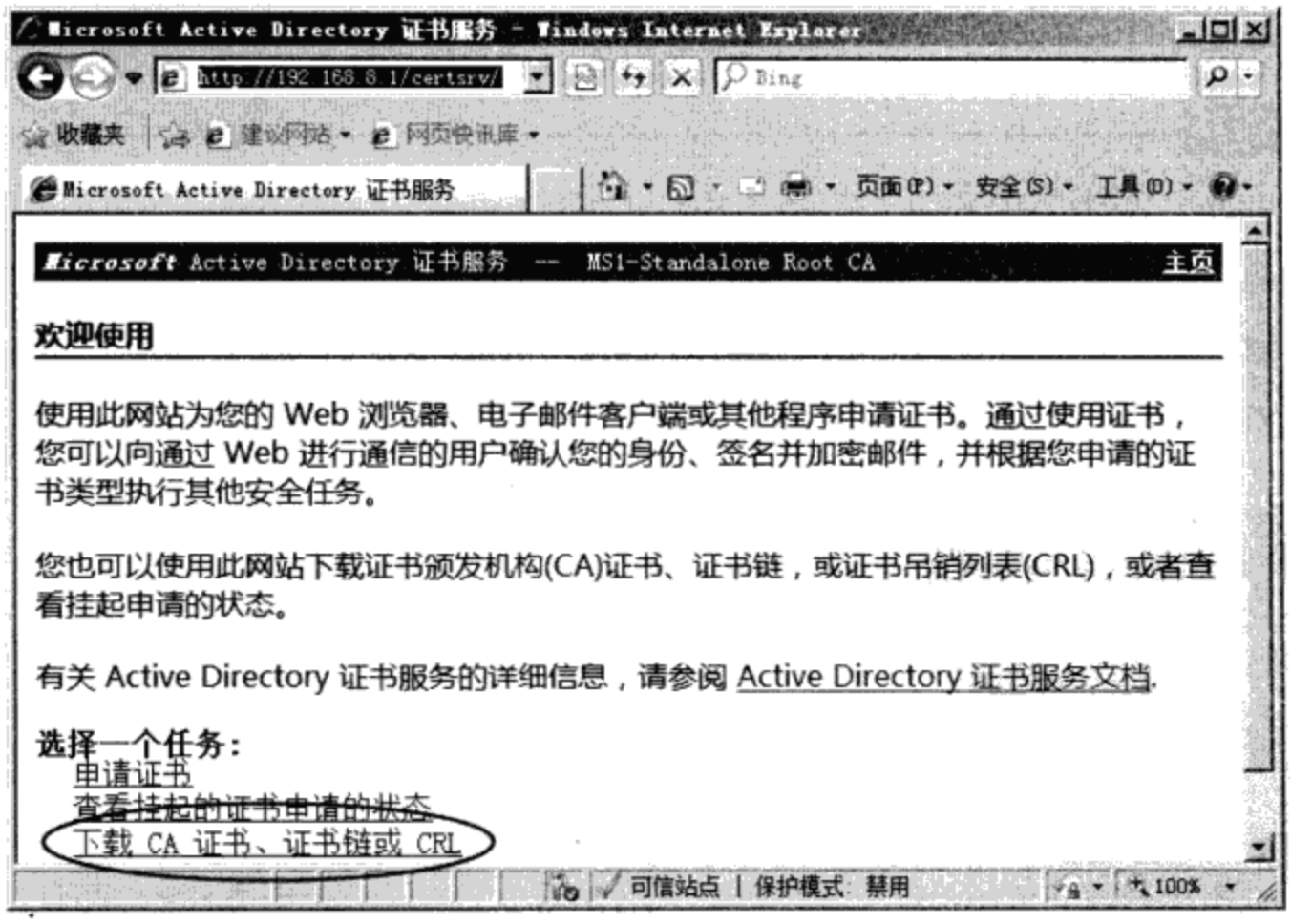


图 13-1

STEP 3 在图 13-2中**单击下载CA证书**或**下载CA证书链接**。

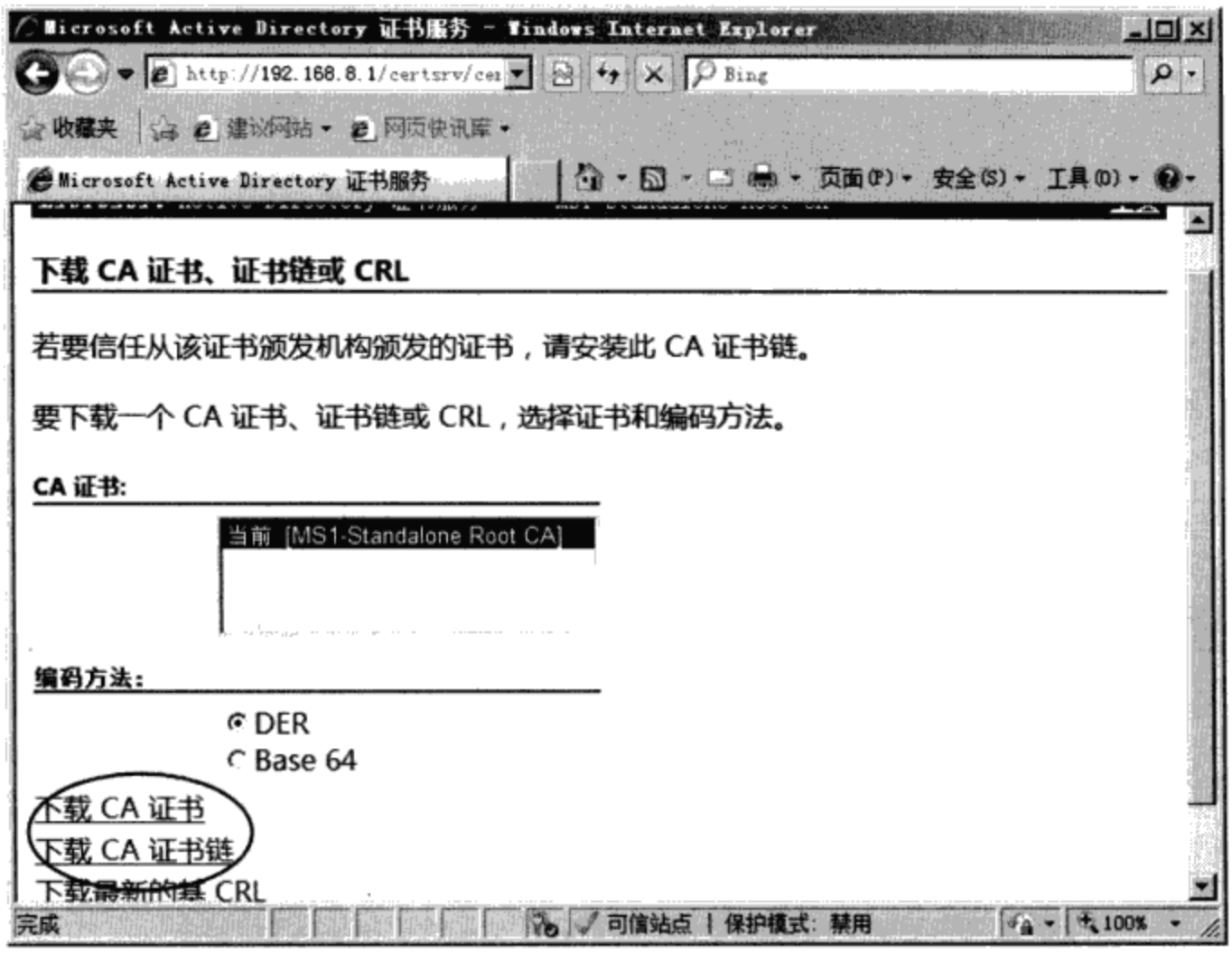


图 13-2

STEP 4 若前一个步骤中单击**下载CA证书**，则请通过图 13-3中的保存按钮来将CA证书保存为扩展名是.cer的文件（内含证书）。若前一个步骤中单击**下载CA证书链**，则请通过图 13-4中的保存按钮将CA证书保存为扩展名是.p7b的文件（包含证书与证书路径）。

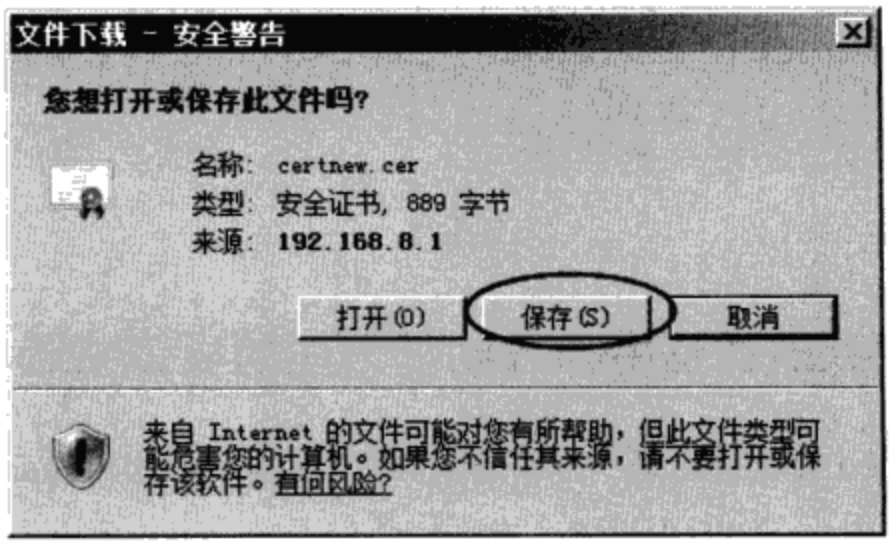


图 13-3

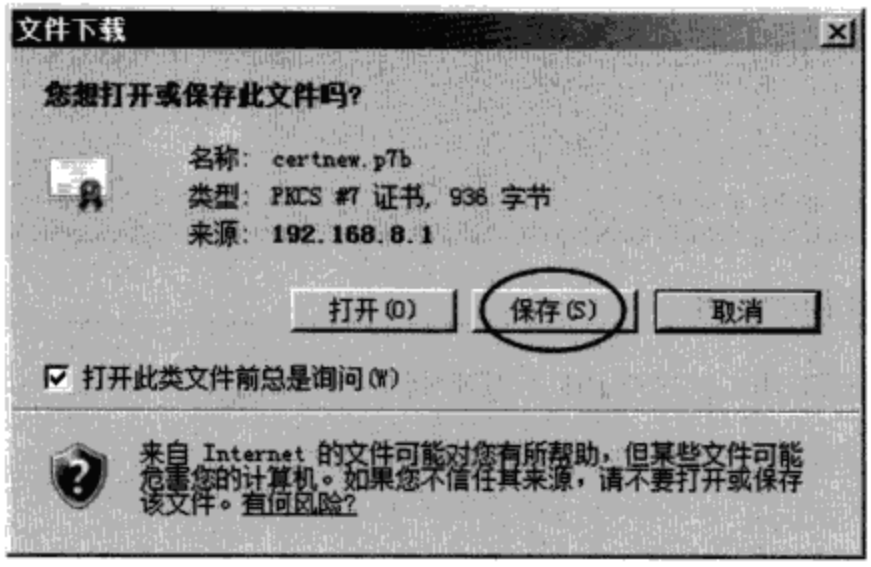


图 13-4

提示

如果计算机的**根证书存储区**（Root Store）内已经有该CA的证书，也就是计算机已经信任此CA的话，则可以利用另外一种方式来将CA的证书保存：【运行浏览器Internet Explorer➲选择**工具**菜单➲Internet选项➲选择**内容**标签➲单击证书按钮➲如图13-5所示选择**受信任的根证书颁发机构**标签➲选择CA的证书➲单击导出按钮】。

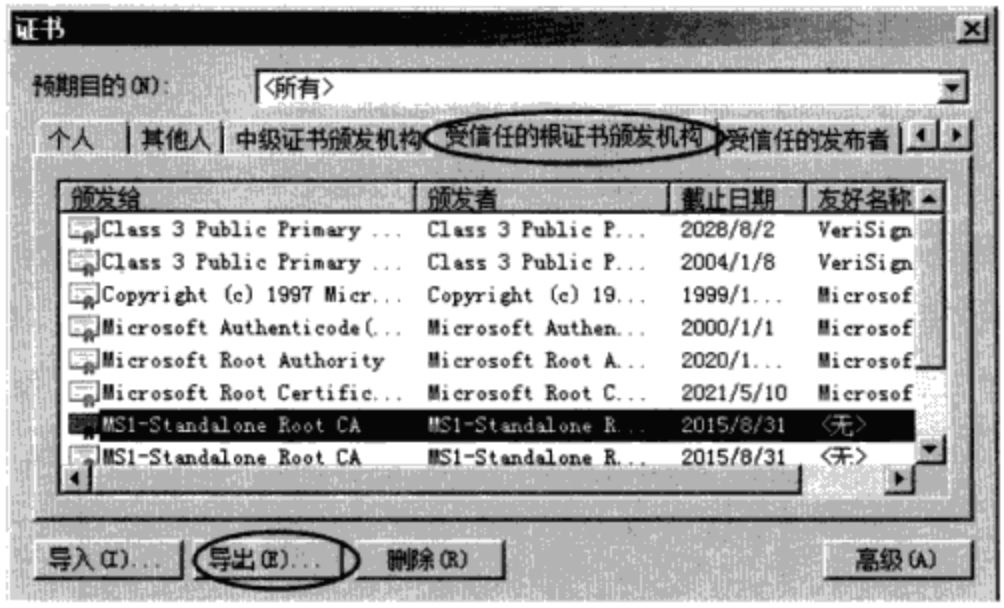


图 13-5

13-2-2 将独立根CA的证书导入到受信任的根证书颁发机构策略

假设要让域内所有计算机都自动信任前述的独立根CA：**MS1-Standalone Root CA**，而且要通过Default Domain Policy GPO来设置，操作步骤如下。

提示

若您仅是要让某个组织单位内的计算机来信任独立根CA的话，请通过该组织单位的GPO来设置。

STEP 1 请到域控制器上选择【开始➲管理工具➲组策略管理➲如图 13-6所示展开到域sayms.com➲对着Default Domain Policy单击右键➲编辑】。

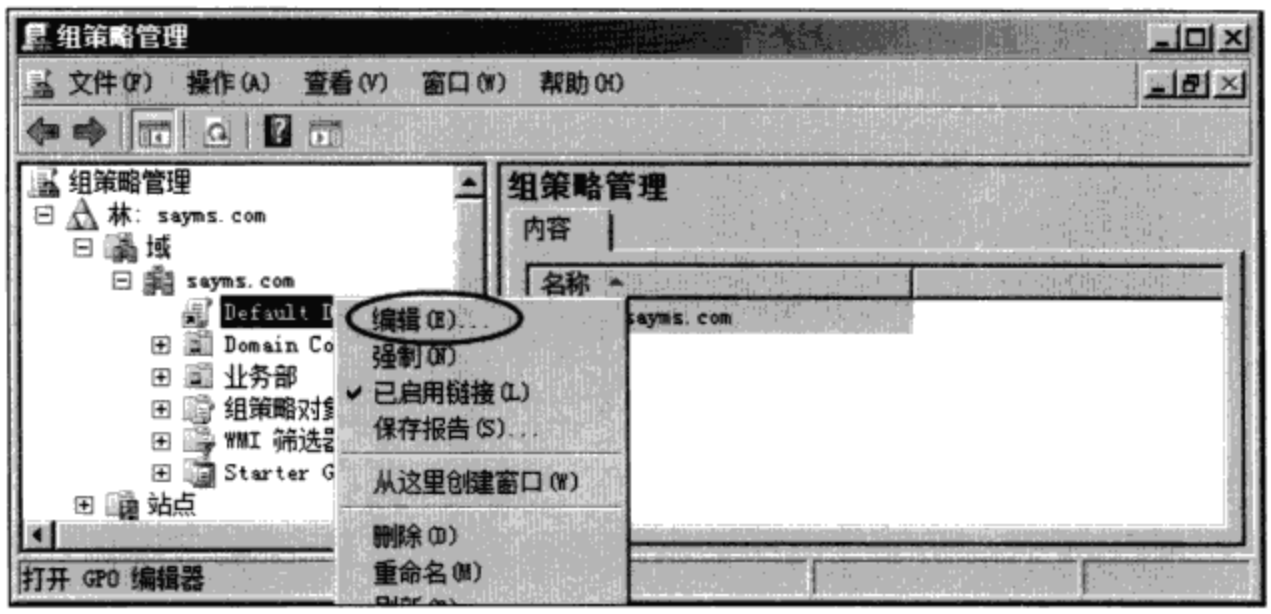


图 13-6

STEP 2 如图 13-7所示，通过【展开**计算机配置**➲策略➲Windows设置➲安全设置➲公钥策略➲对着**受信任的根证书颁发机构**单击右键➲导入】的方式进行操作。

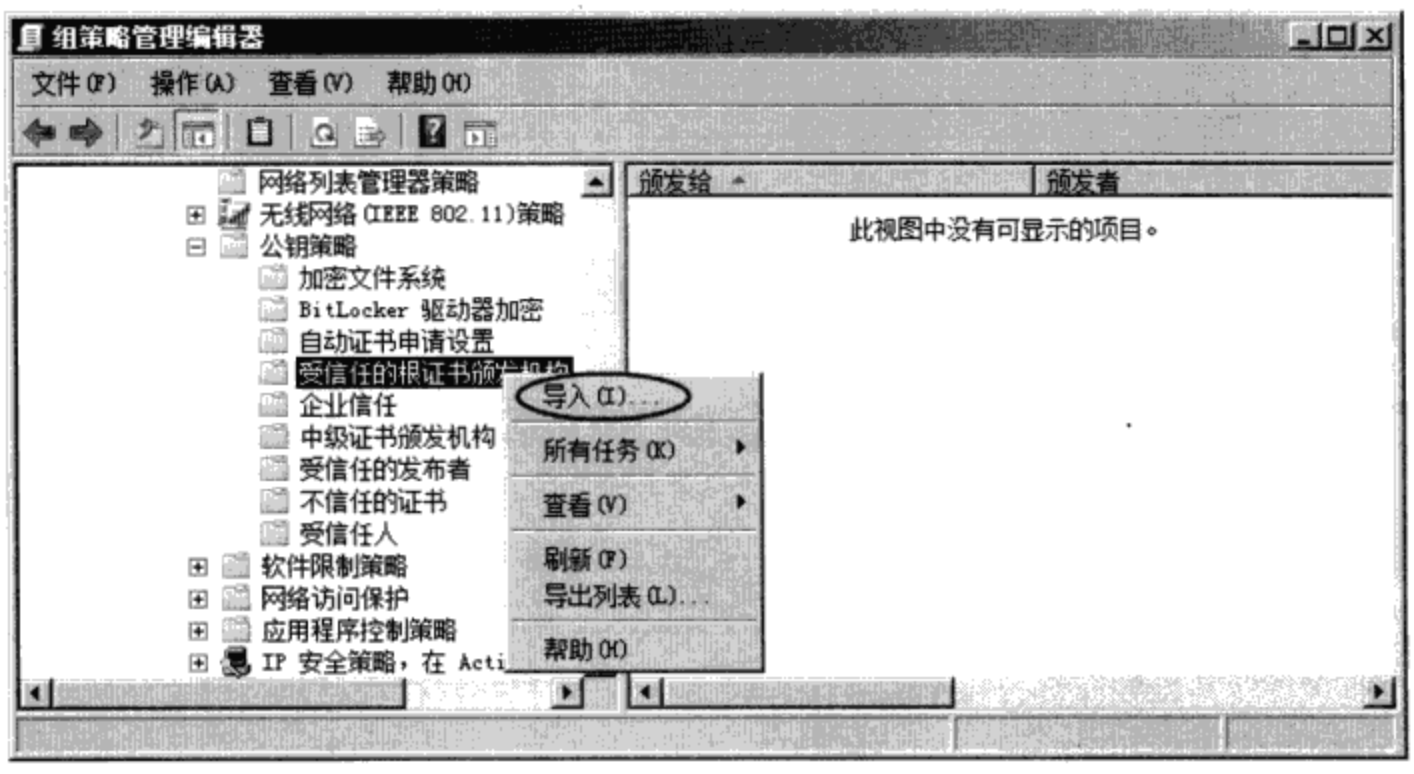


图 13-7

STEP 3 当出现**欢迎使用证书导入向导**界面时单击下一步按钮。

STEP 4 在图 13-8中选择之前下载的CA证书文件后单击下一步按钮，图中我们选择包含证书与证书路径的.p7b文件。

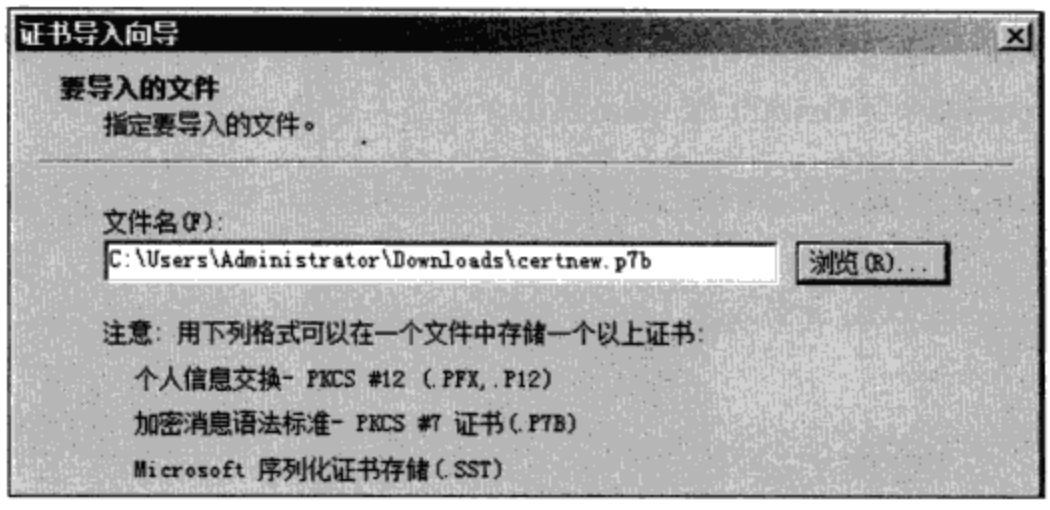


图 13-8

STEP 5 在图 13-9中单击下一步按钮。

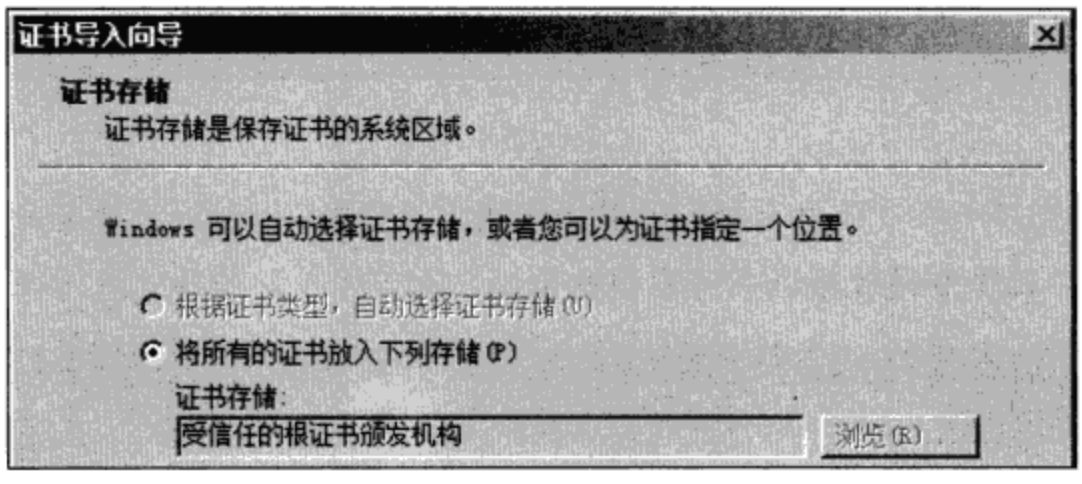


图 13-9

STEP 6 当出现**完成证书导入向导**界面时单击完成按钮。

STEP 7 图 13-10为完成后的界面。

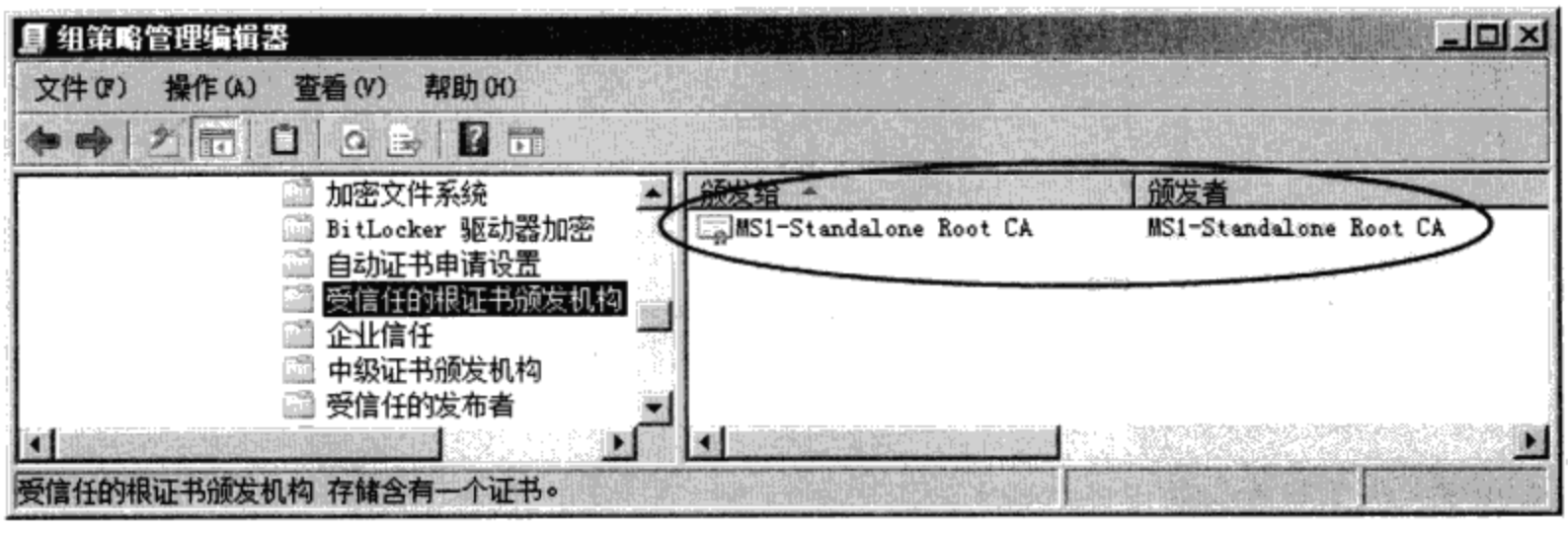


图 13-10

完成以上步骤后，域内所有计算机在应用这个策略后，它们都会自动信任上述的独立根CA。您可以在每一台计算机上执行**gpupdate /force**命令来快速应用此策略，然后通过以下途径来检查这些计算机是否已经信任名称为**MS1-Standalone Root CA**的独立根CA：【运行Internet

Explorer➲单击**工具**菜单➲Internet选项➲单击**内容**标签➲单击证书按钮➲如图 13-11所示单击**受信任的根证书颁发机构**标签】，由图中可知此计算机已经信任此独立根CA。

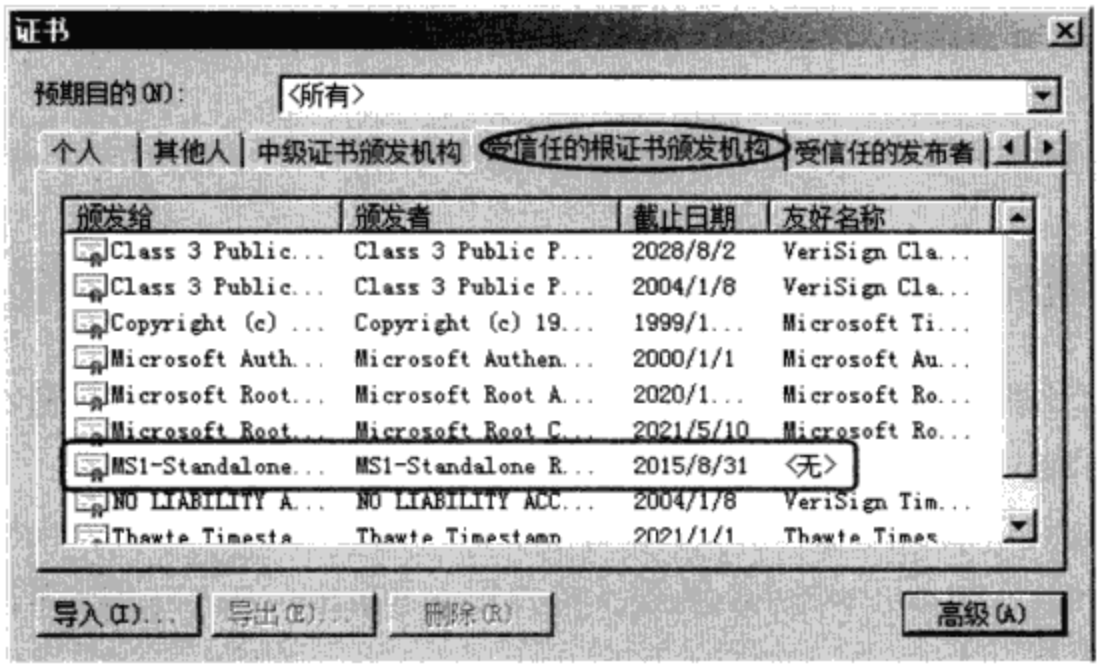


图 13-11

13-3 自动信任外部的CA

也可以让域内所有计算机都自动信任位于外部的根CA，其方法是先新建**证书信任列表**（Certificate Trust List，CTL），然后通过**企业信任**策略来将**证书信任列表**内的所有根CA的证书发送到域内所有计算机，也就是让域内所有计算机都自动信任这些根CA。

虽然外界的根CA可以发放各种不同用途的证书，例如用来保护电子邮件的证书、服务器验证的证书等，可是有时候您只希望信任此根CA所发放的证书仅能够用在单一用途上，例如保护电子邮件，其他用途一概拒绝信任，这些设置也一并通过**证书信任列表**来完成。

以下将建立一个**证书信任列表**来让域内所有计算机都自动信任名称为**External Standalone Root CA**的独立根CA，仅信任其用在**服务器验证**的单一用途上。

首先我们必须取得此独立根CA的证书，然后因为**证书信任列表**必须经过签名，因此必须申请一个可以用来为**证书信任列表**签名的证书。我们将通过以下三大步骤来练习：

- 下载独立根CA的证书并保存。
- 申请可以为**证书信任列表**签名的证书。
- 新建**证书信任列表**（CTL）。

13-3-1 下载独立根CA的证书并保存

下载名称为**External Standalone Root CA**的独立根CA的证书并保存，假设其文件名为

ExtCertnew.p7b：

- 若这台独立根CA是利用Windows Server 2008 R2（Windows Server 2008） **Active Directory证书服务**或Windows Server 2003 **Certificate Services**所架设的，则其操作方法与前一节**下载独立根CA的证书并保存**相同。
- 若这台根CA是利用其他软件所架设，则请参考与该软件相关的文件进行操作。

13-3-2 申请可以为证书信任列表签名的证书

由于**证书信任列表**必须经过签名，因此必须申请一个可以为**证书信任列表**签名的证书。假设要向名称为Sayms Enterprise Root CA的企业根CA申请此证书。

我们将在扮演域控制器的Windows Server 2008 R2中来向上述CA申请证书，不过在Windows 7、Windows Vista、Windows Server 2008 R2与Windows Server 2008等计算机上利用浏览器向CA网站申请上述证书时需要采用以下两种方式之一，否则申请证书会失败：

- 利用https方式来链接CA网站，但需将CA网站加入到**信任的网站**区域内。
- 利用http方式来链接CA网站，但请暂时将网页浏览器Internet Explorer的**本地Intranet**的安全级别降为**低**级别，同时将CA网站加入到**本地Intranet**。

由于第1种方法的CA网站必须申请与安装SSL证书，比较麻烦，因此以下我们采用第2种方法来申请证书。

STEP 1 请到域控制器上登录，然后暂时将网页浏览器Internet Explorer的**本地Intranet**的安全级别降为**低**级别：【打开Internet Explorer➲选择**工具**菜单➲Internet选项➲如图13-12所示单击**安全**标签➲单击**本地Intranet**➲将安全级别降为**低**】。

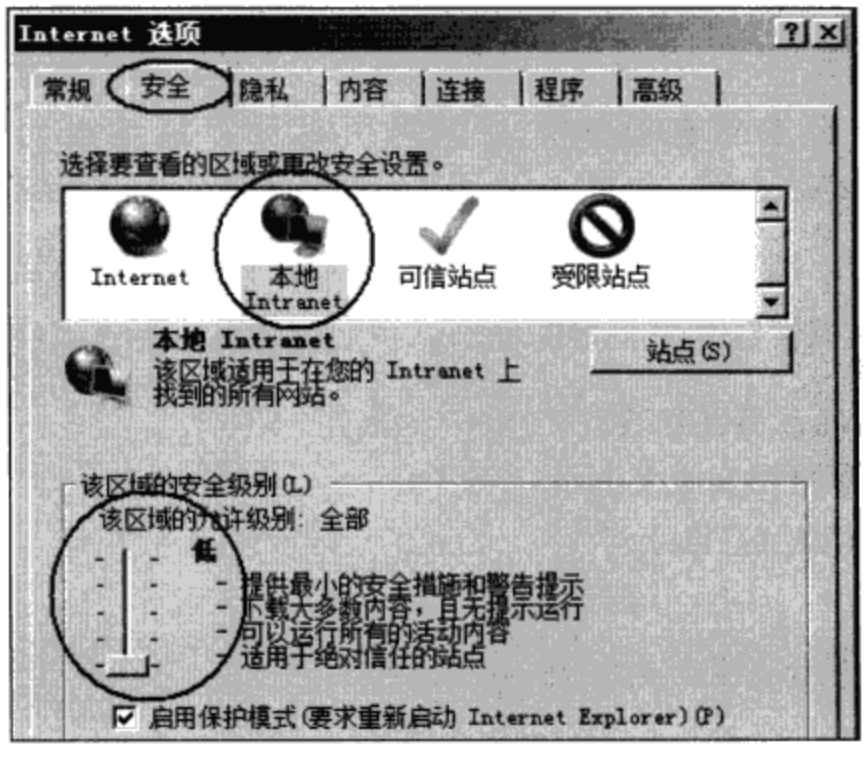


图 13-12

STEP 2 假设要向企业根CA（Sayms Enterprise Root CA）申请用来将**证书信任列表**签名的证书，因此请将此企业根CA网站加入到**本地Intranet**：【单击图 13-12中的站点按钮➲单击图 13-13中的高级按钮➲在弹出的对话框中将**http://192.168.8.1/**加入此区域后单击关闭按钮以及确定按钮】，假设192.168.8.1是企业根CA的IP地址。

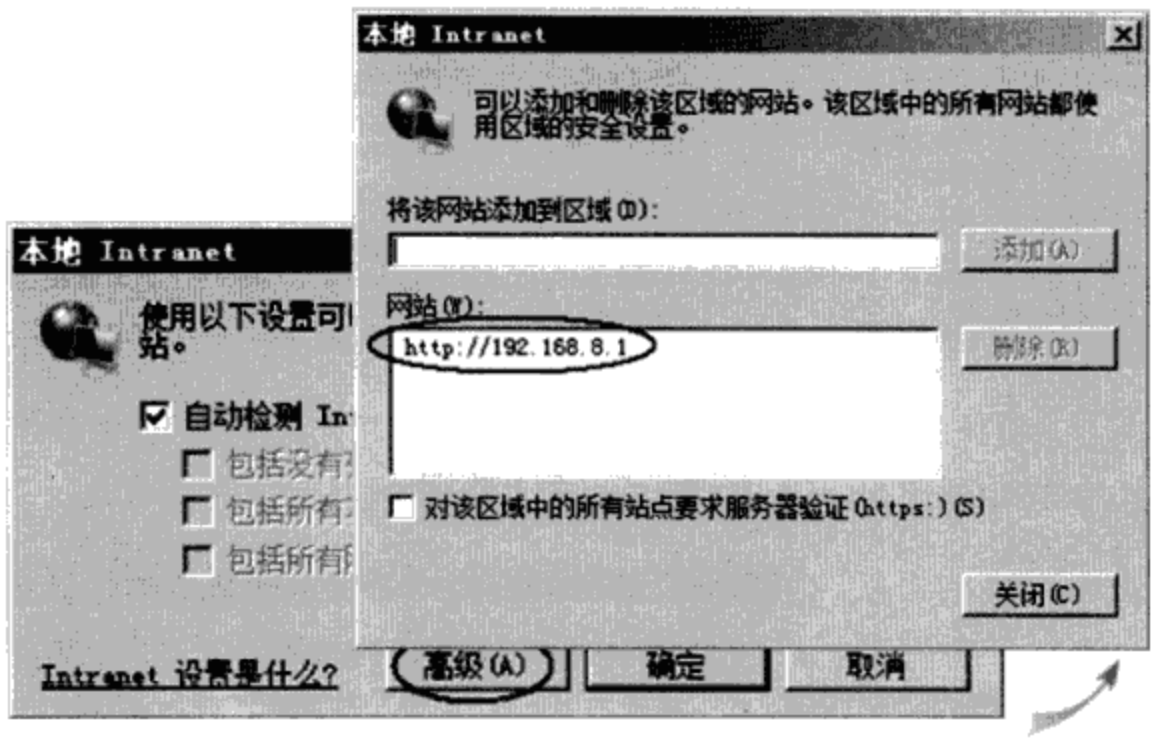


图 13-13

STEP 3 在Internet Explorer内输入网址 **http://192.168.8.1/certsrv/**。

STEP 4 若出现如图13-14所示对话框的话，请输入**域系统管理员**的用户名（sayms\administrator）与密码后单击确定按钮。



图 13-14

STEP 5 在图 13-15中选择**申请证书**、**高级证书申请**、**创建并向此CA提交一个申请**。



图 13-15

STEP 6 在图 13-16中的两个对话框中都单击**是（Y）**按钮。

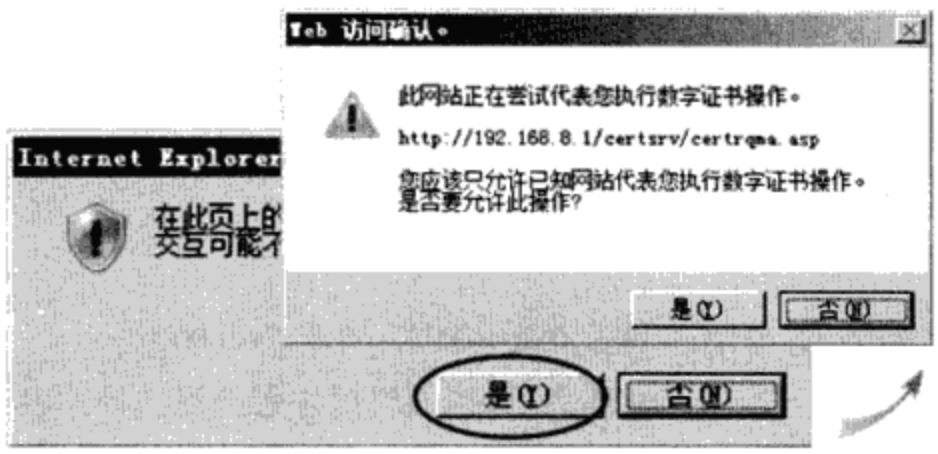


图 13-16

STEP 7 在图 13-17中的**证书模板**下拉列表中选择**系统管理员**后单击**提交**按钮。

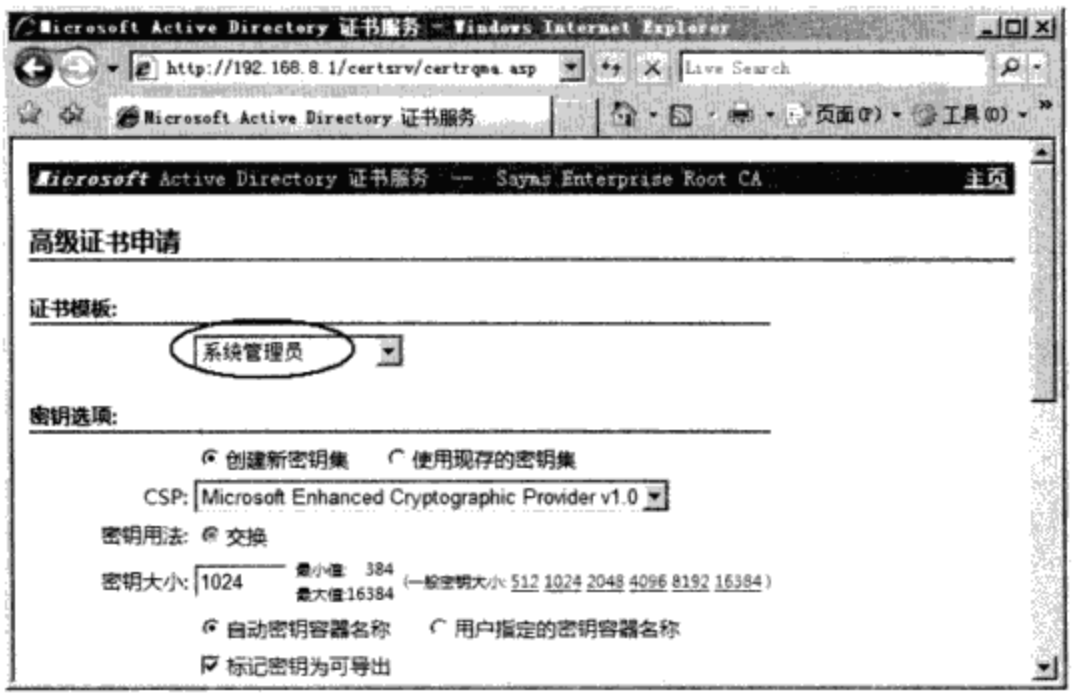


图 13-17

STEP 8 在图 13-18中的两个对话框中都单击**是（Y）**按钮。

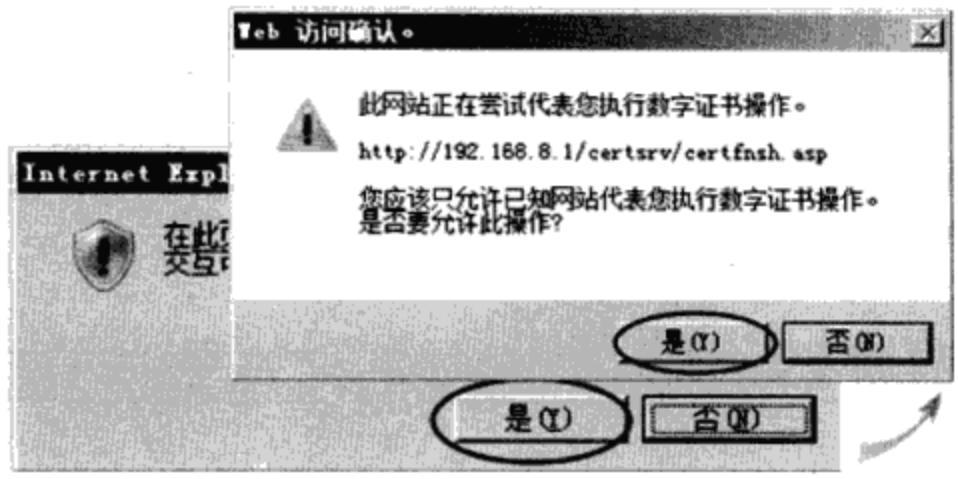


图 13-18

STEP 9 在图 13-19中单击**安装此证书**。

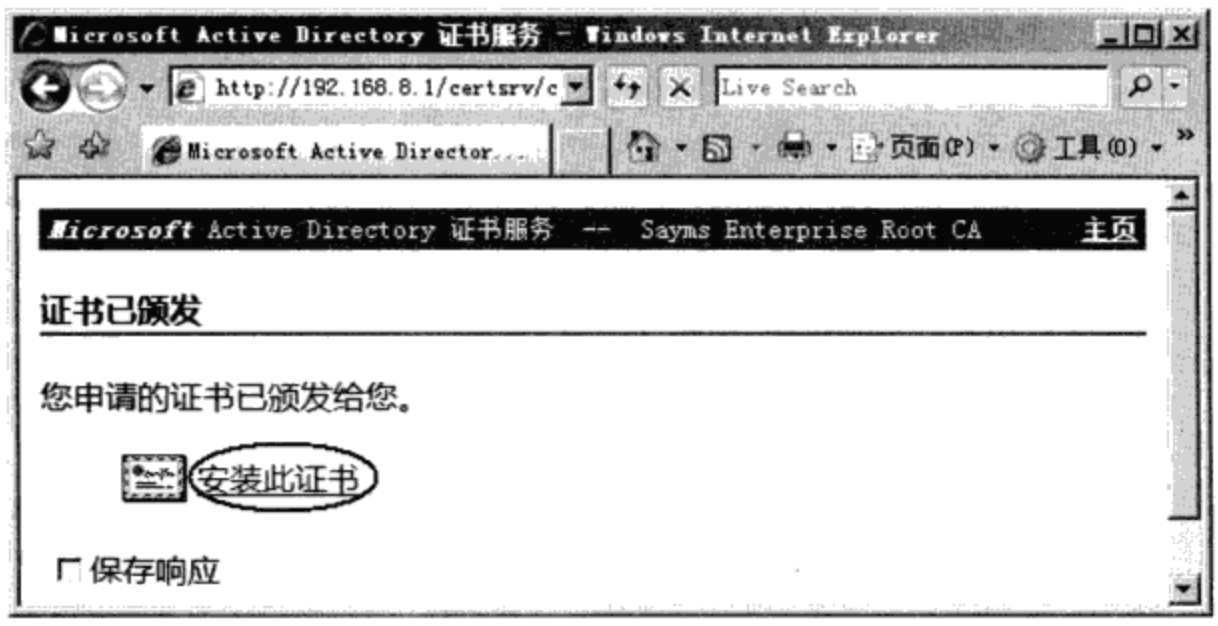


图 13-19

STEP 10 将**本地Intranet**的安全级别恢复为原级别（默认为**中低**）。

13-3-3 创建证书信任列表（CTL）

以下所要创建的**证书信任列表**（CTL）内包含着外部独立根CA（External Standalone Root CA）的证书，也就是要让域内所有计算机都自动信任此独立根CA，而我们将通过Default Domain Policy GPO来设置。

STEP 1 请到域控制器上选择【开始➲管理工具➲组策略管理➲如图 13-20所示展开到域sayms.com➲对着Default Domain Policy单击右键➲编辑】。

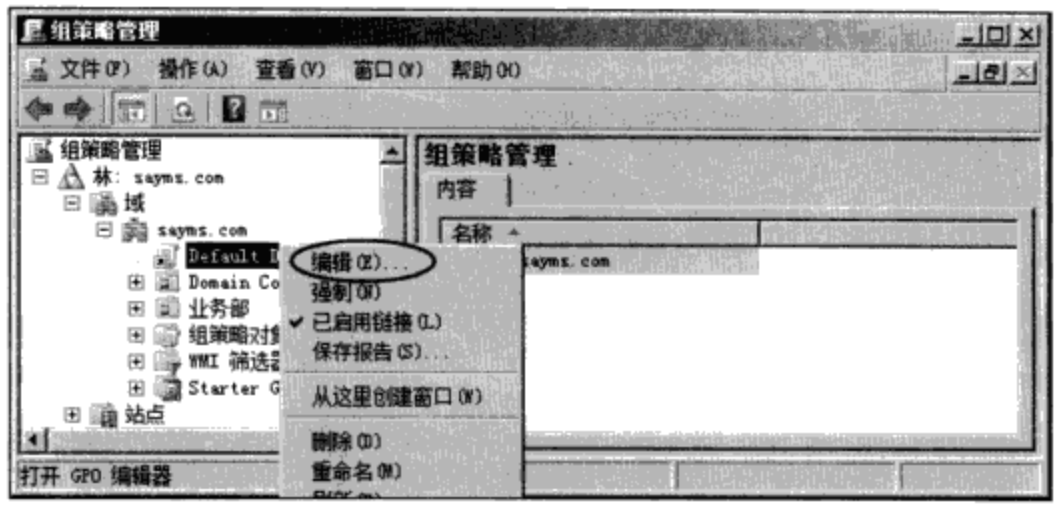


图 13-20

STEP 2 展开**计算机配置**➲策略➲Windows设置➲安全设置➲公钥策略➲如图 13-21所示对着**企业信任**单击右键➲新建➲证书信任列表。

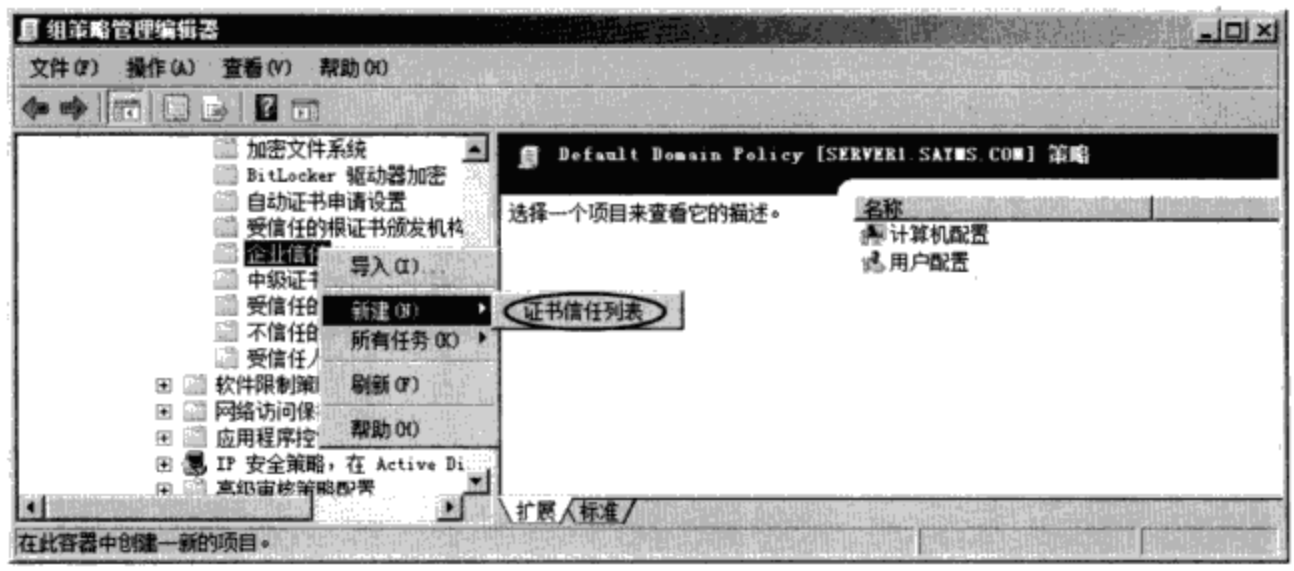


图 13-21

STEP 3 当出现**欢迎使用证书信任列表向导**对话框时单击下一步按钮。

STEP 4 在图 13-22中选择CTL的用途（**服务器验证**）后单击下一步按钮。

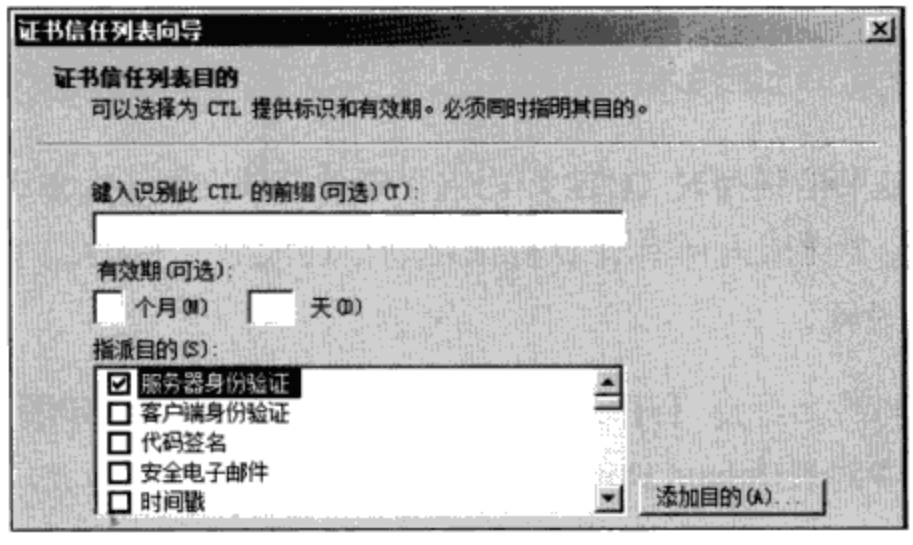


图 13-22

STEP 5 在图 13-23中单击**从文件添加**按钮。

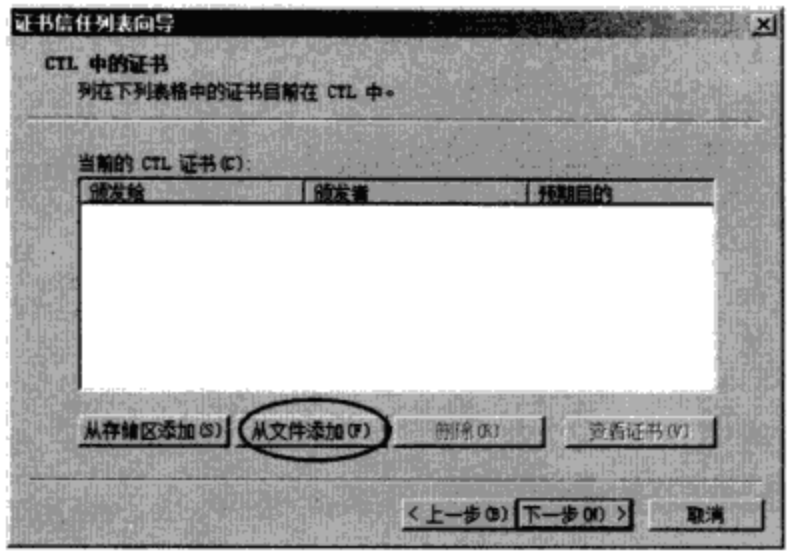


图 13-23

STEP 6 在图13-24中选择外部独立根CA（External Standalone Root CA）的证书文件后单击打开按钮。



图 13-24

STEP 7 返回到如图 13-25所示的对话框时单击下一步按钮。

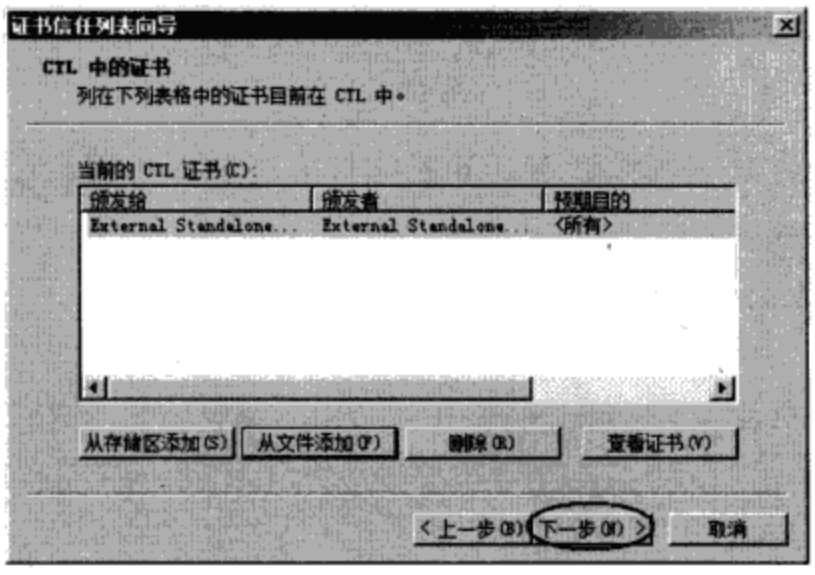


图 13-25

STEP 8 在图 13-26中【单击从存储区选择按钮➲选择我们在前面申请用来将CTL签名的证书➲单击确定按钮】。

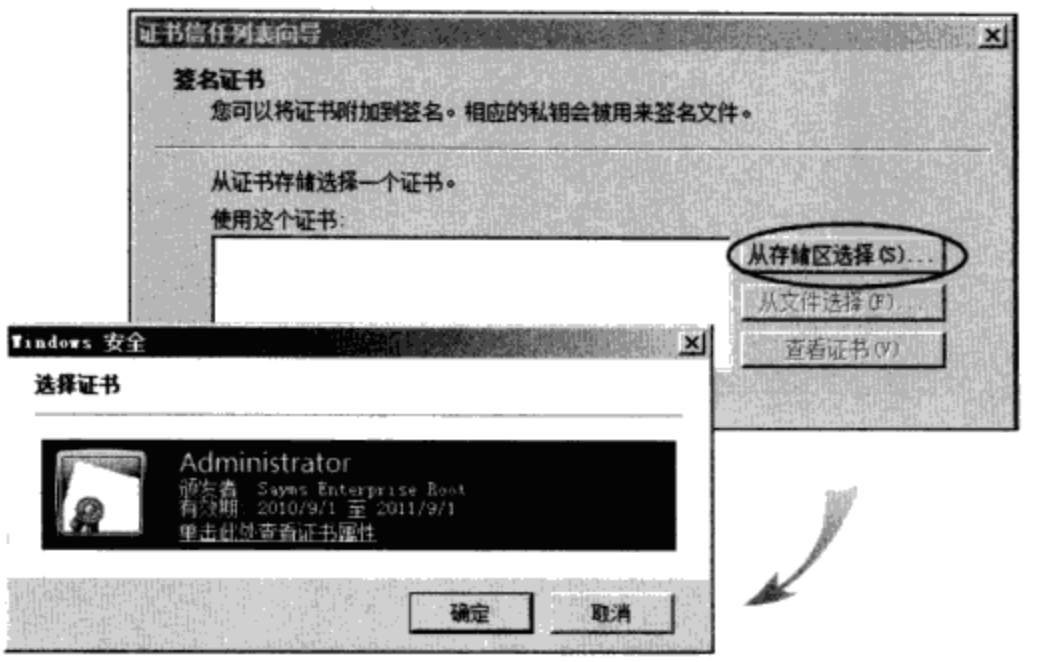


图 13-26

STEP 9 在图 13-27中的两个对话框中都直接单击下一步按钮。

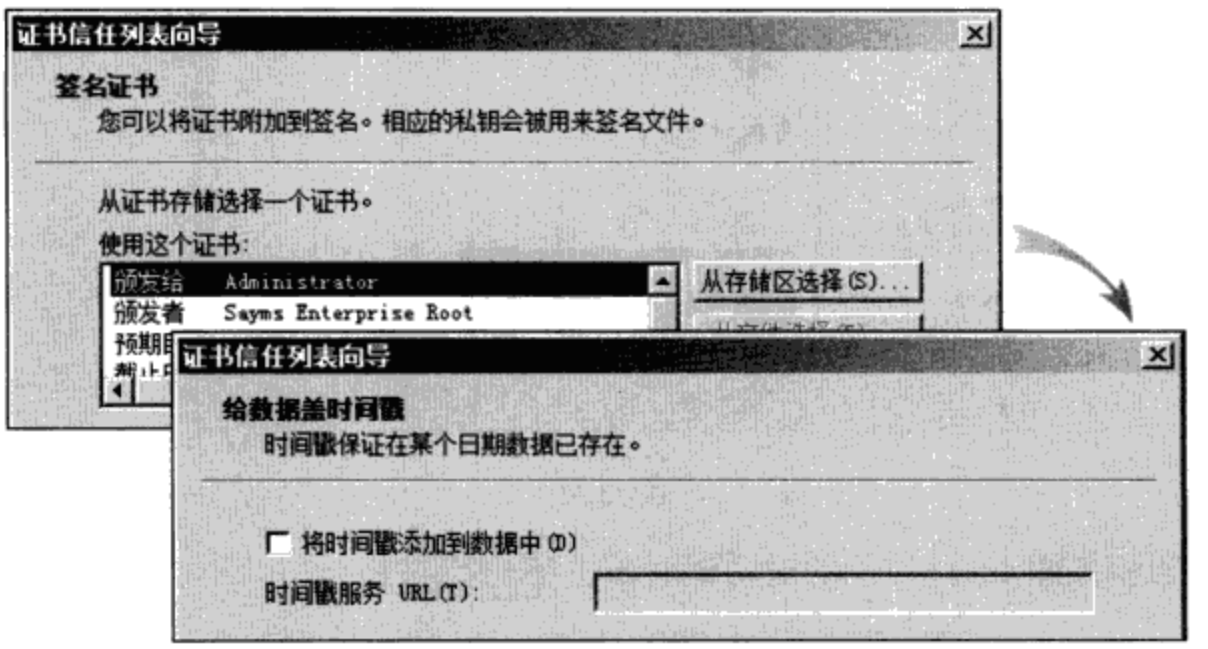


图 13-27

STEP 10 在图 13-28中为此列表设置友好的名称与描述后单击下一步按钮。

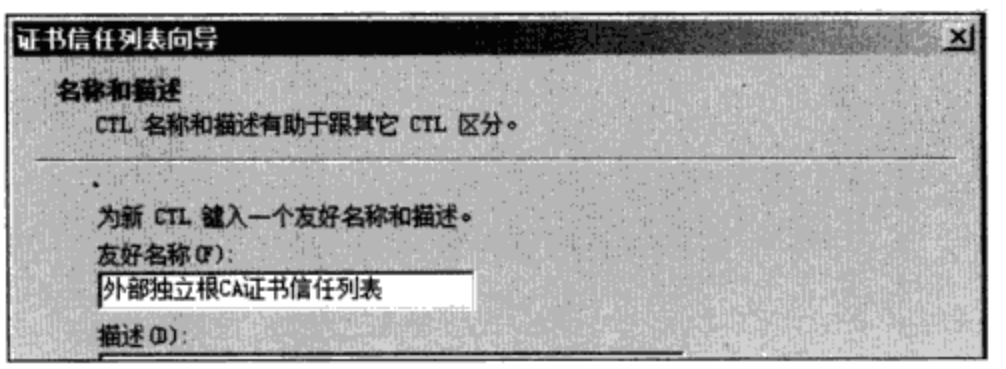


图 13-28

STEP 11 当出现**正在完成证书信任列表向导**对话框时单击完成按钮以及单击确定按钮。

STEP 12 图 13-29为完成后的界面。

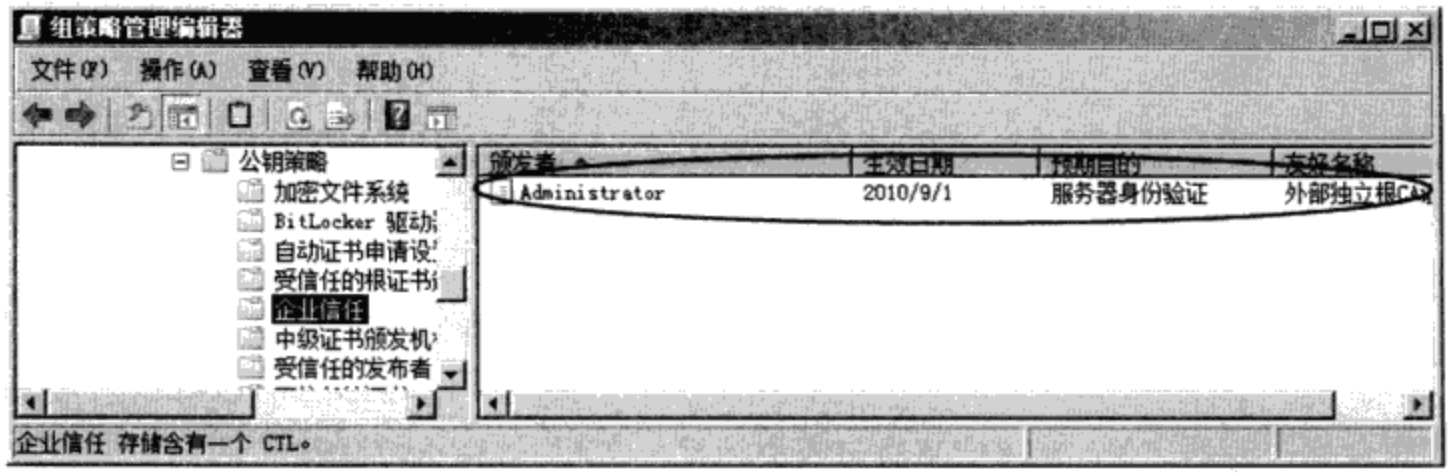


图 13-29

完成以上步骤后，域内所有计算机在应用这个策略后，都会自动信任上述的外部独立根CA。您可以到每一台计算机上执行**gpupdate /force**命令来快速应用此策略。应用完成后，可在这些计算机上通过自定义本地计算机的**证书**管理控制台来检查它们是否已经取得这个证书信任列表，如图 13-30所示为已经成功取得此列表的界面。

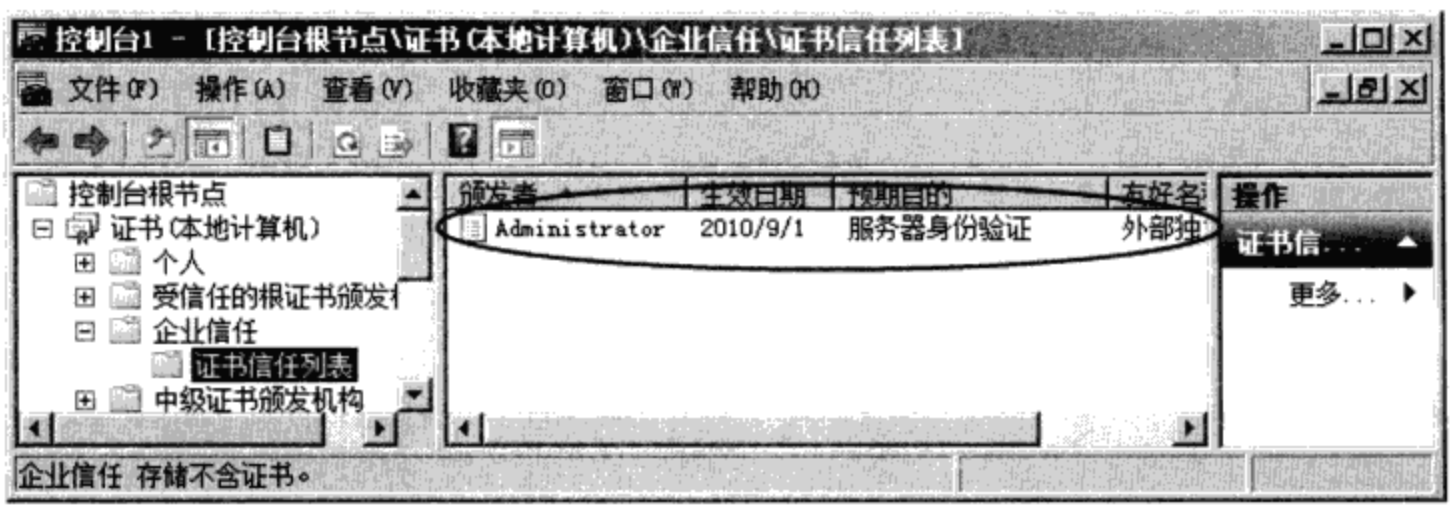


图 13-30

提示

通过**证书信任列表**所信任的CA证书，并不会显示在用户计算机的**受信任的根证书颁发机构**存储区。

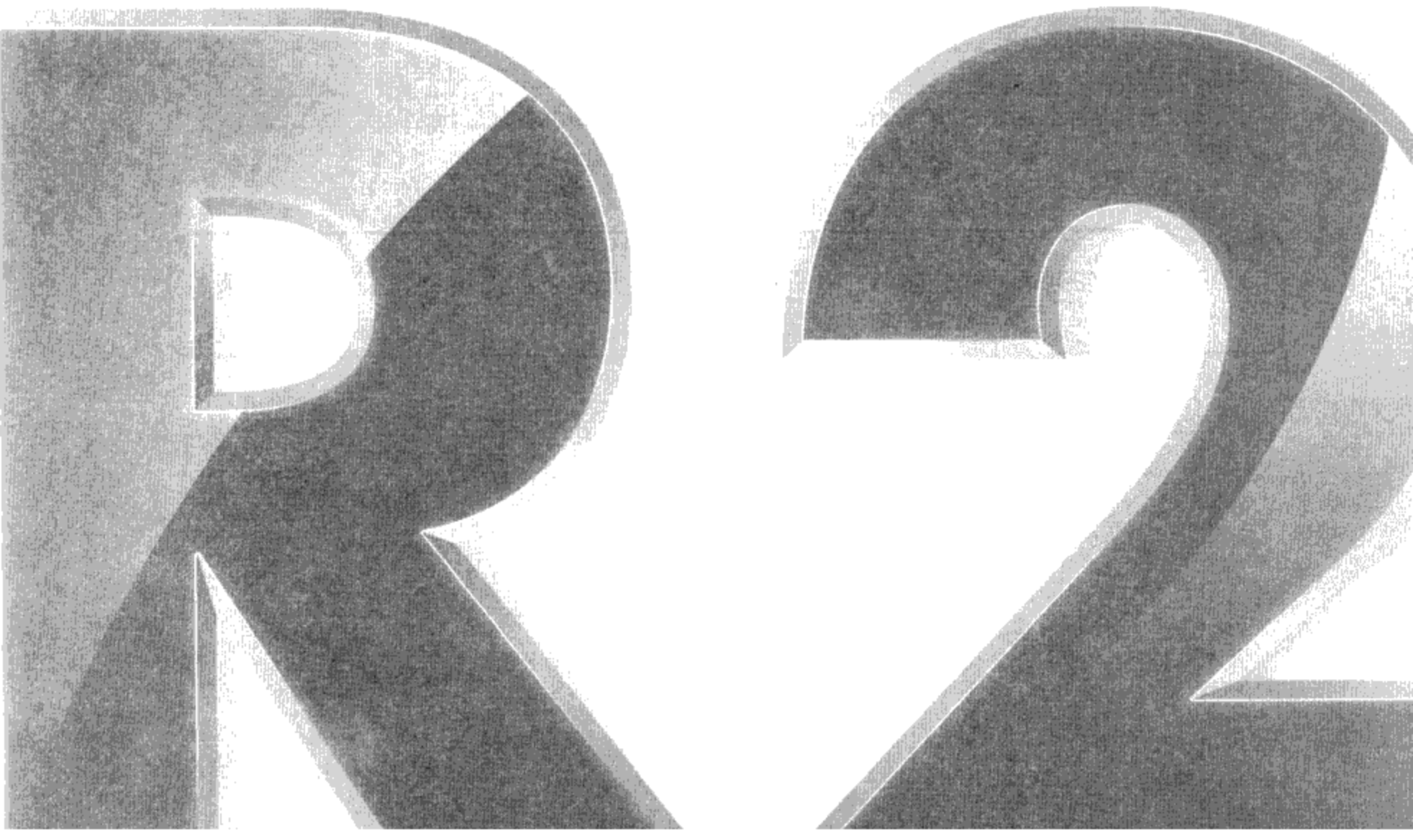
您可以将此CTL导出保存，其方法为【对着此CTL单击右键➲所有任务➲导出】，以后有需要时可以再通过【对着**企业信任**单击右键➲导入】的方法来将其导入。

附录A

AD DS与防火墙

若两台域控制器之间，或域控制器与成员计算机之间，被防火墙隔离的话，则如何让Active Directory数据库复制、用户身份验证、网络资源访问等行为通过防火墙的阻挡，便成为了系统管理员必须了解的重要课题。

- AD DS相关的端口
- 限制动态RPC端口的使用范围
- IPSec与VPN端口



A-1 AD DS相关的端口

不同的网络服务会使用到不同的TCP或UDP端口（port），如果防火墙没有开放相关端口的话，将造成这些服务无法正常运行。我们先在表 A-1中列出AD DS （Active Directory域服务）相关的服务与其所占用的TCP/UDP端口号，然后再说明这些服务的使用场合。

表 A-1

服务	TCP端口	UDP端口
RPC Endpoint Mapper	135	
Kerberos	88	88
LDAP	389	389
LDAPS （LDAP over SSL）	636	636
LDAP GC （LDAP Global Catalog）	3268	
LDAPS GC （LDAP Global Catalog over SSL）	3269	
SMB （Microsoft CIFS）	445	
DNS	53	53
Network Time Protocol （NTP）		123
Active Directory数据库复制、文件复制服务（FRS）、分布式文件系统（DFS）等服务	使用动态端口：需限制端口范围或更改为静态端口	
NetBIOS Name Service		137
NetBIOS Datagram Service		138
NetBIOS Session Service	139	

提示

若为了降低开放端口的复杂性与确保所有与AD DS相关的工作都能够正常运行的话，可以将以下所提到的端口全部开放。

A-1-1 用户登录时会用到的端口

将客户端计算机加入域以及在用户登录时会用到以下的服务，因此若客户端计算机与域控制器之间被防火墙隔离的话，请在防火墙开放以下的端口。

- Microsoft CIFS：445/TCP。
- Kerberos：88/TCP、88/UDP。
- DNS：53/TCP、53/UDP。
- LDAP：389/TCP、389/UDP。

- Netlogon服务: NetBIOS Name Service（137/UDP）/NetBIOS Datagram Service（138/UDP）/ NetBIOS Session Service（139/TCP）与SMB（445/ TCP）。

A-1-2 计算机登录时会用到的端口

计算机登录到域控制器时会用到以下的服务，因此如果域成员计算机与域控制器之间是被防火墙隔离的话，请在防火墙开放以下的端口。

- Microsoft CIFS: 445/TCP。
- Kerberos: 88/TCP、88/UDP。
- LDAP: 389/UDP。
- DNS: 53/TCP、53/UDP。

A-1-3 创建域信任时会用到的端口

位于不同林的域之间在创建快捷方式信任、外部信任等**显性的信任**（Explicit Frust）关系时，会用到以下的服务，因此如果这两个域的域控制器之间是被防火墙隔离的话，请在防火墙开放以下的端口。

- Microsoft CIFS: 445/TCP。
- Kerberos: 88/TCP、88/UDP。
- LDAP: 389/TCP、389/UDP。
- LDAPS: 636/TCP（如果使用SSL的话）。
- DNS: 53/TCP、53/UDP。

A-1-4 验证域信任时会用到的端口

不同域的域控制器之间在验证信任关系时会用到以下的服务，因此若这些域控制器之间是被防火墙隔离的话，请在防火墙开放以下的端口。

- Microsoft CIFS: 445/TCP。
- Kerberos: 88/TCP、88/UDP。
- LDAP: 389/TCP、389/UDP。
- LDAPS: 636/TCP（如果使用SSL的话）。
- DNS: 53/TCP、53/UDP。
- Netlogon服务: NetBIOS Name Service（137/UDP）/NetBIOS Datagram Service（138/UDP）/ NetBIOS Session Service（139/TCP）与SMB（445/ TCP）。

A-1-5 访问文件资源时会用到的端口

访问文件资源时所使用的服务为SMB （445/TCP）或NetBIOS Name Service（137/UDP）/ NetBIOS Datagram Service（138/UDP）/NetBIOS Session Service（139/TCP），因此若用户的计算机与资源所在的计算机是被防火墙隔离的话，请在防火墙开放这些服务的端口。

A-1-6 运行DNS查询时会用到的端口

如果要通过防火墙来向DNS服务器提出查询请求的话，例如查询域控制器的IP地址，就需要开放DNS服务的端口：53/TCP与53/UDP。

A-1-7 运行Active Directory数据库复制时会用到的端口

两台域控制器之间在进行Active Directory数据库复制时会用到以下服务，因此若这两台域控制器之间被防火墙隔离的话，请在防火墙开放以下端口。

- Active Directory数据库复制：它不是使用静态RPC（Remote Procedure Call）端口，而是使用动态RPC端口（1024~65535之间），此时我们要如何来开放端口呢？动态RPC端口可以被限制在一段较小的范围内，因此我们只要在防火墙开放这一小段范围的TCP端口即可，也可以自行指定一个静态的端口。
- RPC Endpoint Mapper：135/TCP。使用动态RPC端口时，需要搭配RPC Endpoint Mapper服务，因此请在防火墙开放此服务的端口。
- Kerberos：88/TCP、88/UDP。
- LDAP：389/TCP、389/UDP。
- LDAPS：636/TCP（如果使用SSL的话）。
- DNS：53/TCP、53/UDP。
- Microsoft CIFS：445/TCP。

A-1-8 文件复制服务（FRS）会用到的端口

若域功能级别是Windows Server 2008以下的话，则同一个域的域控制器之间在复制SYSVOL文件夹时，会使用FRS（File Replication Service）。FRS也是采用动态RPC端口，因此若将动态RPC端口限制在一段较小范围内的话，则我们只要在防火墙开放这段范围的TCP端口即可。但是使用动态RPC端口时，需要搭配RPC Endpoint Mapper服务，因此请在防火墙开放RPC Endpoint Mapper：135/TCP，也可以自行指定一个静态的端口。

A-1-9 分布式文件系统（DFS）会用到的端口

若域功能级别为Windows Server 2008（含）以上的话，则Windows Server 2008 R2（Windows Server 2008）域控制器之间在复制SYSVOL文件夹时需使用**DFS复制服务**（DFS Replication Service），因此若这些域控制器之间是被防火墙隔离的话，请在防火墙开放以下的端口。

- LDAP：389/TCP、389/UDP。
- Microsoft CIFS：445/TCP。
- NetBIOS Datagram Service：138/UDP。
- NetBIOS Session Service：139/TCP。
- Distributed File System（DFS）。
- RPC Endpoint Mapper：135/TCP。

A-1-10 其他可能需要开放的端口

- LDAP GC、LDAPS GC：3268/TCP、3269/TCP（如果使用SSL的话）。假设用户登录时，负责验证用户身份的域控制器需要通过防火墙来向**全局编录服务器**查询用户所隶属的通用组数据时，您就需要在防火墙开放端口3268或3269。若Microsoft Exchange Server需要访问位于防火墙另外一端的**全局编录服务器**的话，也需要开放端口3268或3269。
- Network Time Protocol（NTP）:123/UDP。用于时间的同步。
- NetBIOS的相关服务：137/UDP、138/UDP、139/TCP。开放这些端口，以便通过防火墙来使用NetBIOS服务，例如支持旧客户端来登录、浏览网上邻居等。

A-2 限制动态RPC端口的使用范围

动态RPC端口是如何运行的呢？以Microsoft Office Outlook（MAPI客户端）与Exchange Server之间的通信为例：客户端Outlook先连接Exchange Server的RPC Endpoint Mapper（RPC Locator Services，TCP端口135）、RPC Endpoint Mapper再将Exchange Server所使用的端口（动态的，范围在1024~65535之间）通知客户端、客户端Outlook再通过此端口来连接Exchange Server。

Active Directory数据库的复制、Outlook与Exchange Server之间的通信、文件复制服务（File Replication Service，FRS）、分布式文件系统（Distributed File System，DFS）等默认都是使用动态RPC端口，也就是没有固定的端口，这将造成在防火墙设置上的困扰。

A-2-1 限制所有服务的动态RPC端口范围

以下将说明如何将计算机所使用的动态RPC端口限制在指定的范围内。建议从端口号5000开始，而且因为可能有多个应用程序会使用RPC端口，因此应至少包含20个以上的端口。端口号最大为65535。

我们需要使用修改注册表（Registry）的方式来将动态RPC端口限制在指定范围内。请到要限制动态端口范围的计算机上运行注册表编辑器REGEDIT.EXE，然后通过以下路径来设置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc
```

STEP 1 在上述路径之下添加一个名称为**Internet**的项（图 A-1为整个步骤完成后的界面）。

STEP 2 在**Internet**选项下添加如表 A-2所示的三个数值。

表 A-2

数值名称	数据类型	数值
Ports	REG_MULTI_SZ（多字符串值）	自定义，例如5000~5020
PortsInternetAvailable	REG_SZ（字符串值）	Y
UseInternetPorts	REG_SZ（字符串值）	Y

STEP 3 图 A-1为设置完成后的界面。

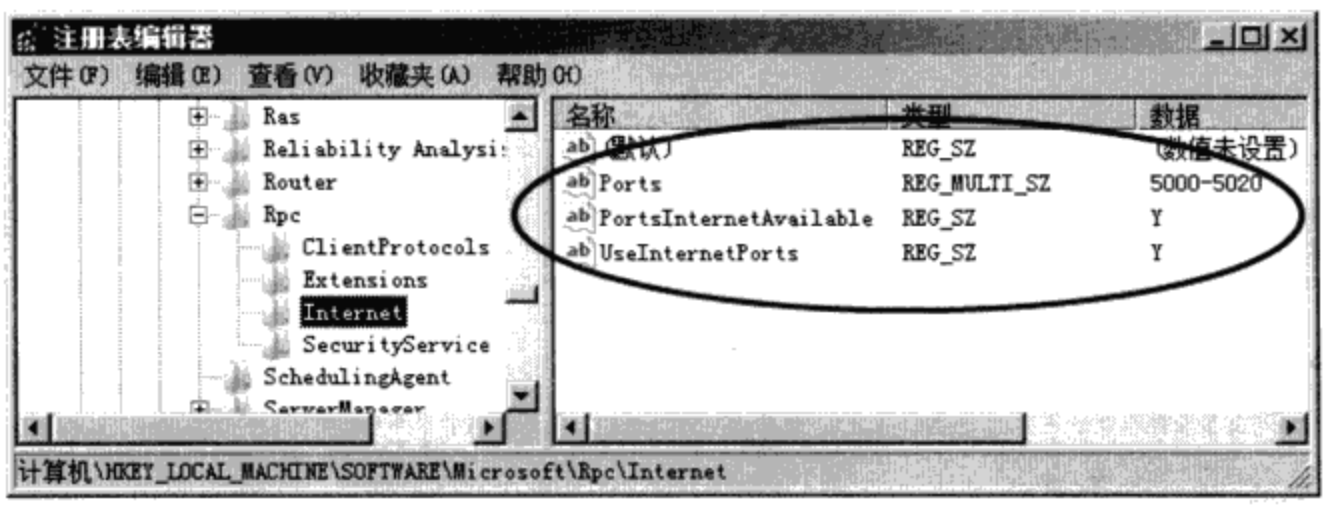


图 A-1

STEP 4 重新启动计算机后，所有会用到动态RPC端口的程序，都会使用5000～5020之间的端口号。

如果您要修改域控制器的注册表的话，请任意找一台域成员计算机来与这台域控制器通信，然后在这台域控制器上打开**命令提示符**窗口、运行**netstat -n**命令来查看此域控制器当前所使用的端口，此时应该可以看到某些服务所使用的端口是在我们所限制的范围5000 ～ 5020内，如图 A-2所示。

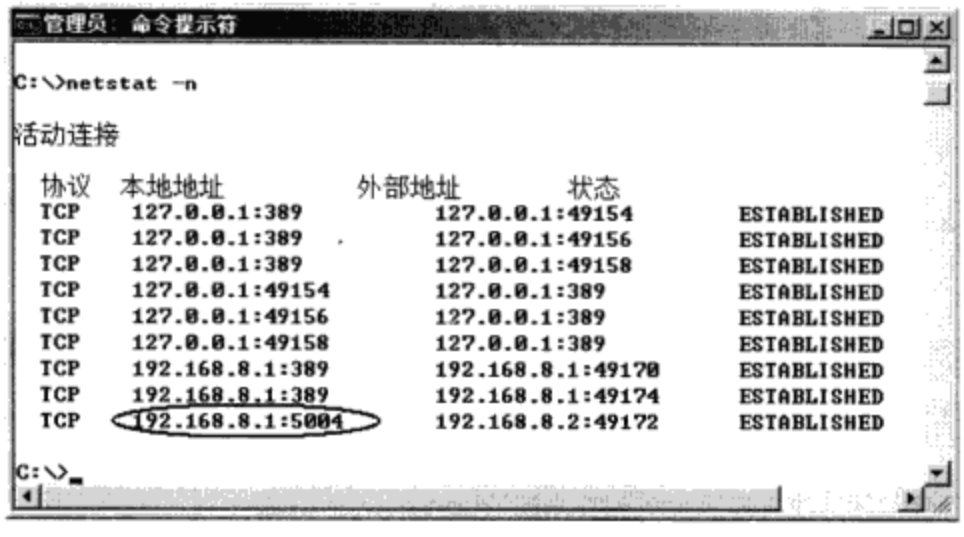


图 A-2

A-2-2 限制Active Directory数据库复制时指定的静态端口

域控制器运行Active Directory数据库复制工作时，默认是使用动态RPC端口，但是我们也可以自行指定一个静态的端口。请到域控制器上运行注册表编辑器REGEDIT.EXE，然后通过以下路径来设置：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
```

请在上述路径之下添加一个如表 A-3所示的数值，图 A-3为完成后的界面，图中我们将端口号设置为56789（十进制），注意此端口不可以与其他服务所使用的端口相同。

表 A-3

数值名称	数据类型	数值
TCP/IP Port	REG_DWORD	自定义，例如56789

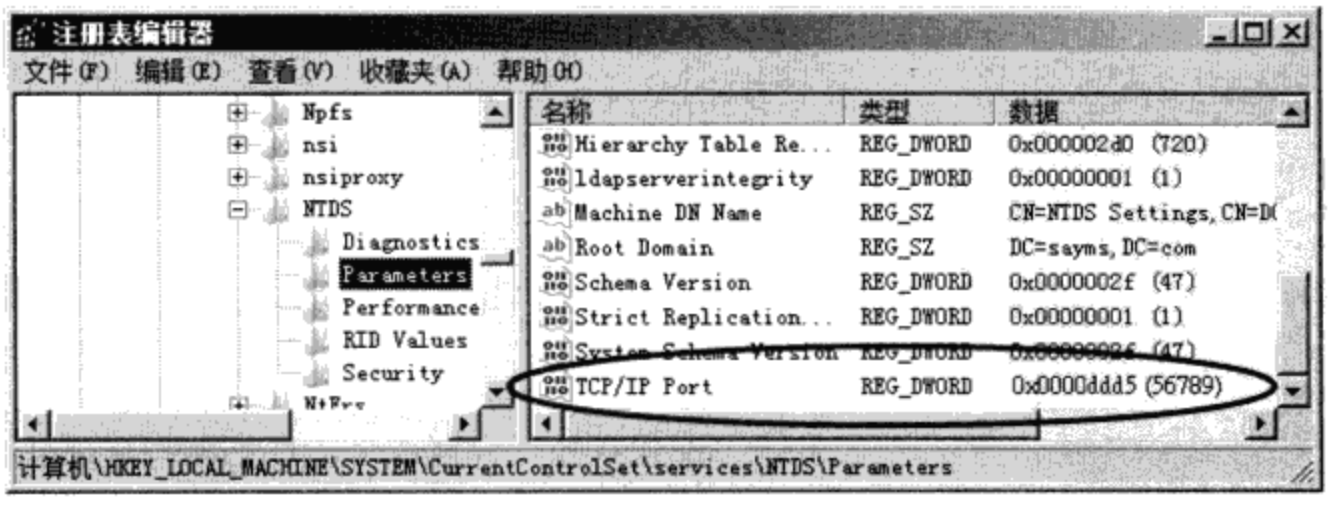


图 A-3

完成后重新启动，以后这台域控制器在运行Active Directory数据库复制时所使用到的端口将会是56789。您可以先使用**Active Directory站点和服务**来手动与其他域控制器之间运行

Active Directory数据库复制的工作，然后在这台域控制器上打开**命令提示符**窗口、运行**netstat -n**命令来查看其所使用的端口，如图 A-4所示可看到指定的端口56789。

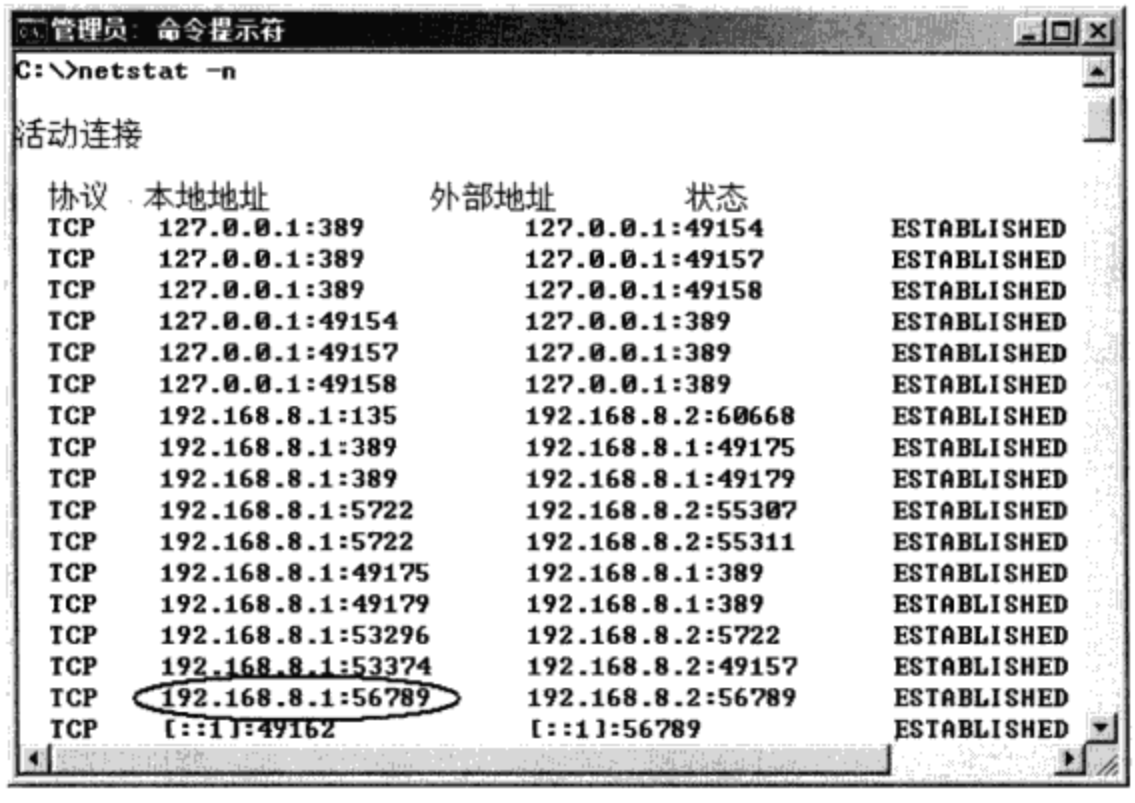


图 A-4

A-2-3 限制FRS使用指定的静态端口

若域功能级别为Windows Server 2008以下的话，则同一个域的域控制器之间在复制SYSVOL文件夹时，会使用FRS（File Replication Service）。FRS默认也是采用动态RPC端口，但是我们也可以自行指定一个静态的端口。请到域控制器上运行注册表编辑器REGEDIT.EXE，然后通过以下路径来设置：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters
```

请在上述路径之下添加一个如表 A-4所示的数值，表中我们将端口号设置为45678（十进制），注意此端口不可以与其他服务所使用的端口相同，完成后重新启动。以后这台域控制器的FRS服务所使用的端口将会是45678。

表 A-4

数值名称	数据类型	数值
RPC TCP/IP Port Assignment	REG_DWORD	自定义，例如45678

A-2-4 限制DFS使用指定的静态端口

若域功能级别为Windows Server 2008（含）以上的话，则Windows Server 2008 R2（Windows

Server 2008）域控制器之间在复制SYSVOL文件夹时需使用**DFS复制服务**，而它也是采用动态RPC端口，但是可以使用DFSRDIAG.EXE程序来将其绑定到一个静态的端口。请到域控制器上打开**命令提示符**窗口，然后运行以下命令（如图 A-5所示，图中假设将端口绑定到34567）：

```
DFSRDIAG StaticRPC /Port:34567
```

注意此端口不可以与其他服务所使用的端口相同。完成后，重新启动这台域控制器，以后其**DFS复制服务**所使用的端口将会是34567。

提示

从Windows Server 2003 R2开始提供此DFSRDIAG.EXE程序。



图 A-5

您可以先使用**Active Directory站点和服务**来手动与其他域控制器之间执行AD DS复制工作（它也会复制SYSVOL文件夹），然后在这台域控制器上打开**命令提示符**窗口、运行**netstat -n**命令来查看其所使用的端口，如图 A-6所示可看到指定的连接34567。

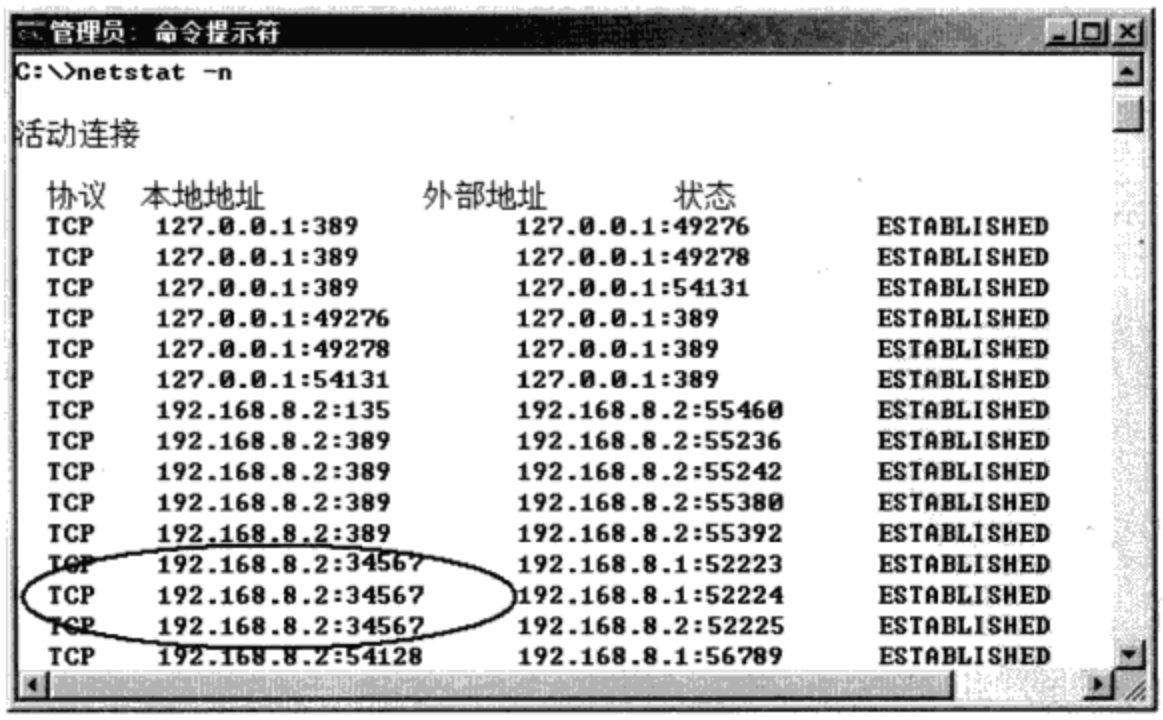


图 A-6

A-3 IPSec与VPN端口

如果域控制器之间，或域控制器与成员计算机之间，不但被防火墙隔离，而且所传送的数据还经过IPSec的处理，或经过PPTP、L2TP等VPN安全传输通道来传送的话，则还有一些协议或端口需要在防火墙开放。

A-3-1 IPSec所使用的协议与端口

IPSec除了用到UDP协议外，还会用到ESP与AH协议，因此我们需要在防火墙开放相关的UDP端口与ESP、AH协议。

- Encapsulation Security Payload （ESP）：协议号为50。
- Authentication Header （AH）：协议号为51。
- Internet Key Exchange （IKE）：所使用的UDP端口号为500。

A-3-2 PPTP VPN所使用的协议与端口

除了TCP协议外，PPTP VPN还会使用到GRE协议。

- General Routing Encapsulation （GRE）：协议号为47。
- PPTP：所使用的TCP端口号为1723。

A-3-3 L2TP/IPSec所使用的协议与端口

除了UDP协议外，L2TP/IPSec还会用到ESP协议。

- Encapsulation Security Payload （ESP）：协议号为50。
- Internet Key Exchange （IKE）：所使用的UDP端口号为500。
- NAT-T：所使用的UDP端口号为4500，用于使IPSec可以穿越NAT。



提示

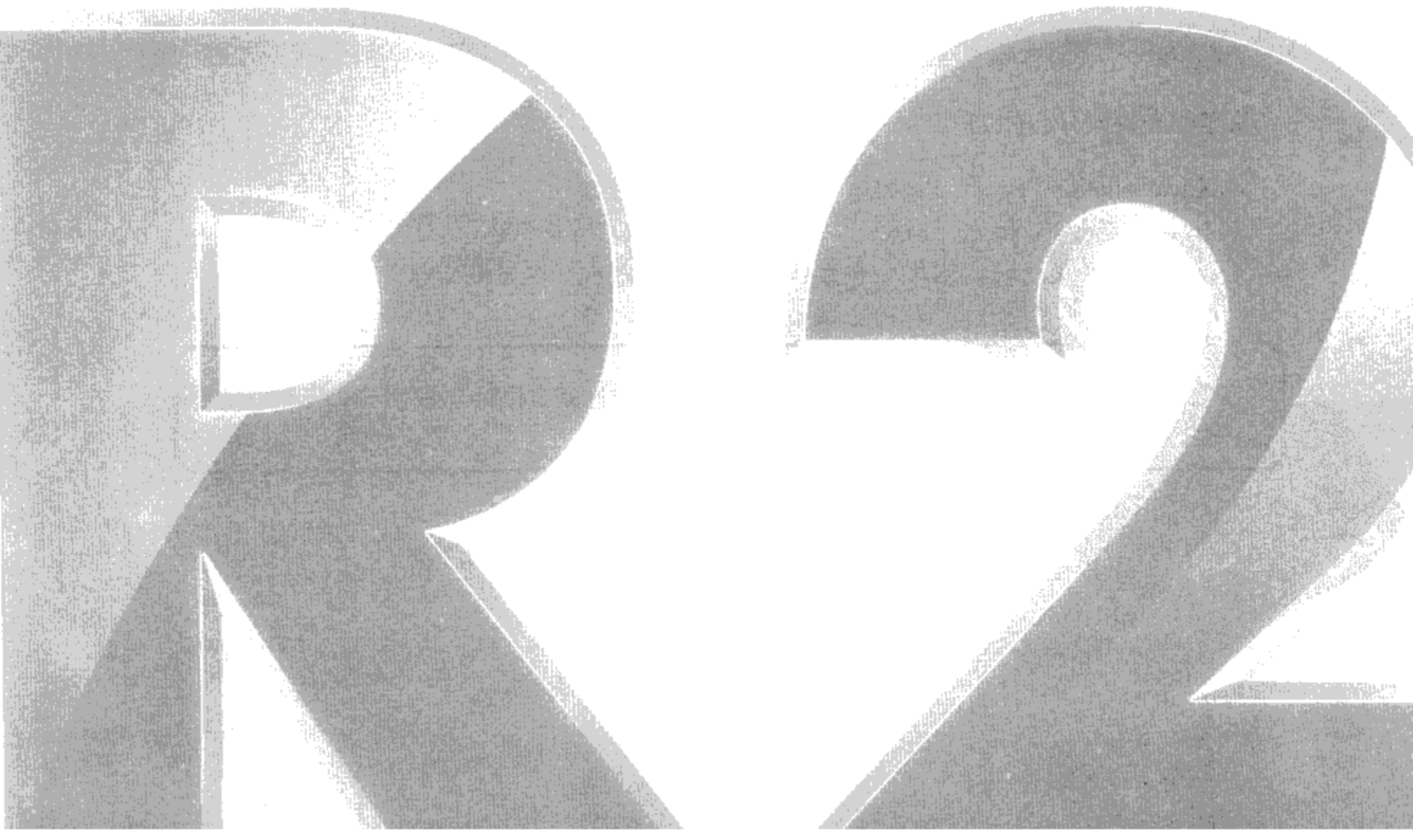
虽然L2TP/IPSec还会使用到UDP 端口1701，但它是被封装在IPSec数据包内，因此不需要在防火墙开放此端口。

附录 B

服务器核心安装的管理

在安装Windows Server 2008 R2时可以选择一个被称为**服务器核心安装**的新选项，它提供一个最小化的环境，可以降低系统维护与管理需求、减少使用硬盘容量、减少被攻击威胁。

- **服务器核心安装**概述
- **服务器核心安装**的基本设置
- 在**服务器核心安装**内安装服务器角色
- 在**服务器核心安装**内安装功能
- **服务器核心安装**的远程管理
- 常用命令列表

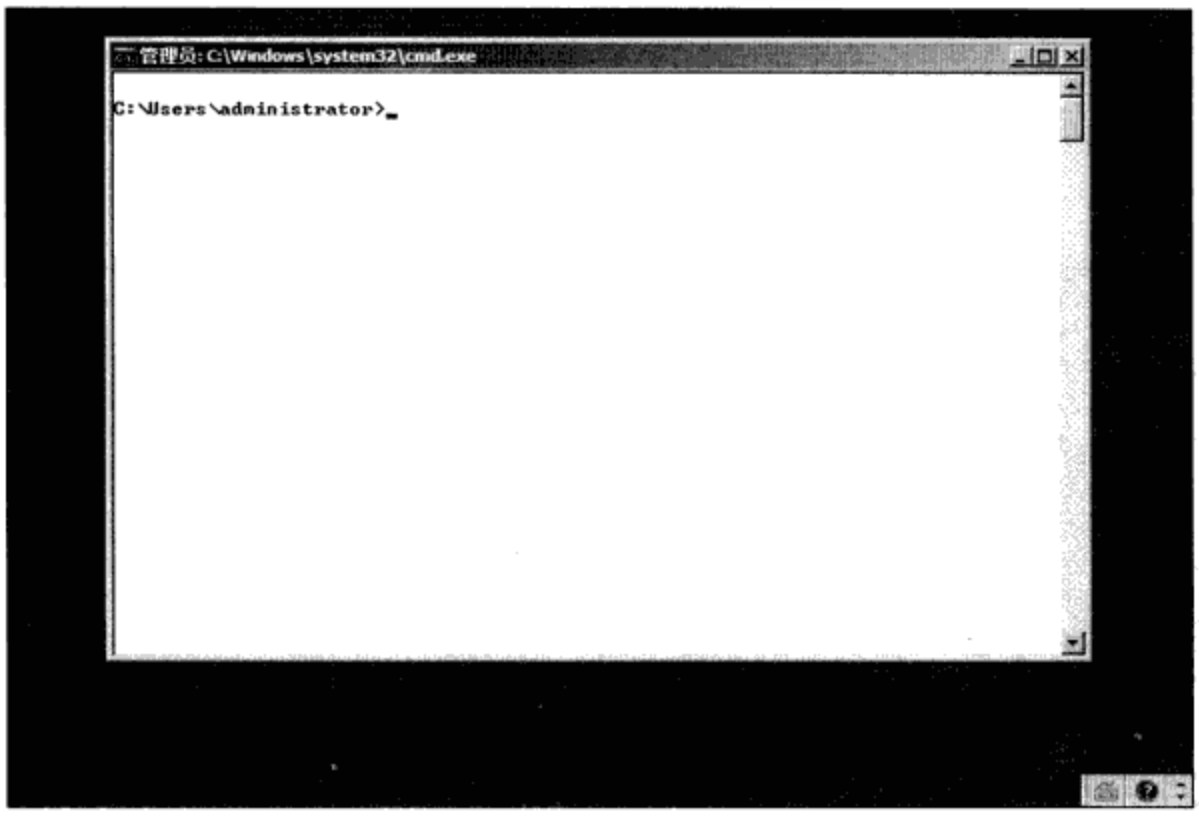


B-1 服务器核心安装概述

服务器核心安装提供一个最小化的运行环境来支持部分特定角色，它可以降低系统维护与管理需求、减少硬盘的使用量、减少被攻击的威胁。Windows Server 2008 R2 **服务器核心安装**支持以下服务器角色：

- Active Directory证书服务（AD CS）。
- Active Directory域服务（AD DS）。
- Active Directory轻型目录服务（AD LDS）。
- DHCP服务器。
- DNS服务器。
- 文件服务（包含文件服务器资源管理器）。
- Hyper-V。
- 打印服务。
- 流媒体服务。
- Web服务器（包含支持ASP.NET子集）。

服务器核心安装只会安装上述角色所需的二进制文件，它并不提供Windows窗口管理界面，因此在您登录**服务器核心安装**后的管理界面为**命令提示符**（如图 B-1所示），您需要在此环境下使用命令来管理**服务器核心安装**或通过另外一台Windows Server 2008 R2完全安装的计算机来管理**服务器核心安装**。



图B-1

服务器核心安装内也不会显示启用Windows的提示信息、更新程序的提示信息与密码过期提示信息等，因为这些功能都是**Windows资源管理器**的一部分，然而**服务器核心安装**内并不会安装**Windows资源管理器**。

> **注意**
>
> 若您不小心将**命令提示符**窗口关闭的话，可使用注销再重新登录或【按 Ctrl + Alt + Del 键➲启动任务管理器➲选择**文件**菜单➲新建任务➲输入**cmd.exe**➲单击 确定 按钮】的方法来重新打开此窗口。

在Windows Server 2008 R2内提供了一个名为**Sconfig.cmd**的程序，它使系统管理员可更容易地设置**服务器核心安装**。

> **提示**
>
> Internet上还有一个名为**Core Configurator**的程序，它提供图形界面让系统管理员更容易管理**服务器核心安装**，例如更改设置、安装服务器角色、安装功能等，不过此程序并不完全适用于中文版的**Windows Server 2008 R2 服务器核心安装**。

B-2 服务器核心安装的基本设置

本节将说明如何更改**服务器核心安装**的计算机名、IP地址、DNS服务器的IP地址、启用**服务器核心安装**与加入域等基本设置。

B-2-1 更改计算机名

您可以先使用**hostname**或**ipconfig /all**命令来查看此台服务器当前的计算机名（主机名）。假设当前的计算机名为ServerCoreBase，同时假设我们要将其更改为ServerCore1，因此请通过以下命令来运行计算机名称的更改操作：

```
netdom renamecomputer ServerCoreBase /NewName:ServerCore1
```

接下来通过以下命令来重新启动计算机，以便让此更改生效：

```
shutdown /r /t 0
```

您也可以使用**Sconfig**程序来更改计算机名称：运行**Sconfig**，然后在图 B-2中选择**计算机名称**后单击 Enter 键。

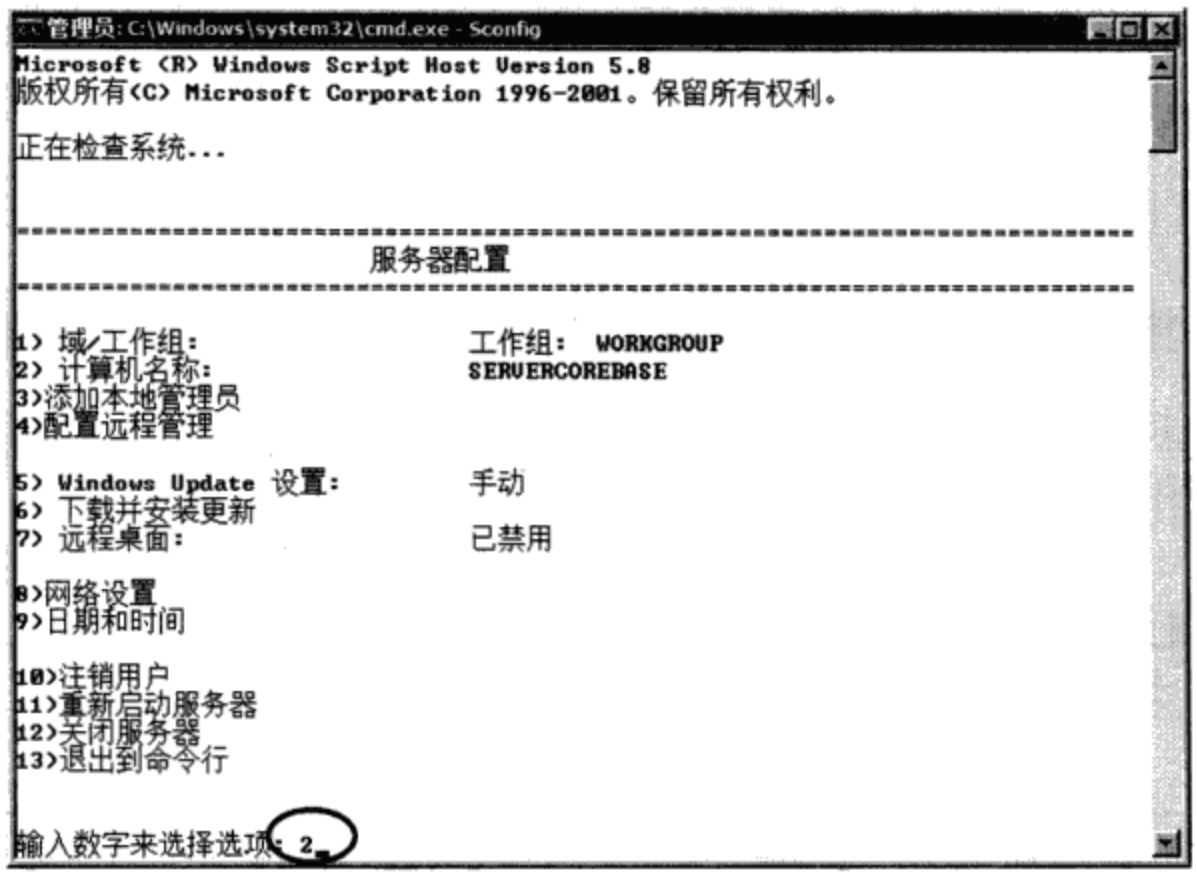


图 B-2

B-2-2 更改IP地址

此计算机的IP地址等设置默认是动态获取，而假设我们要将其更改为以下的配置：IP地址为192.168.8.41、子网掩码为255.255.255.0、默认网关为192.168.8.254、首选DNS服务器的IP地址为192.168.8.1，操作步骤如下。

STEP 1 在**命令提示符**下，运行以下命令：

```
netsh  interface  ipv4  show  interfaces
```

STEP 2 找出网卡的Idx代号，如图 B-3所示的Idx代号为3。

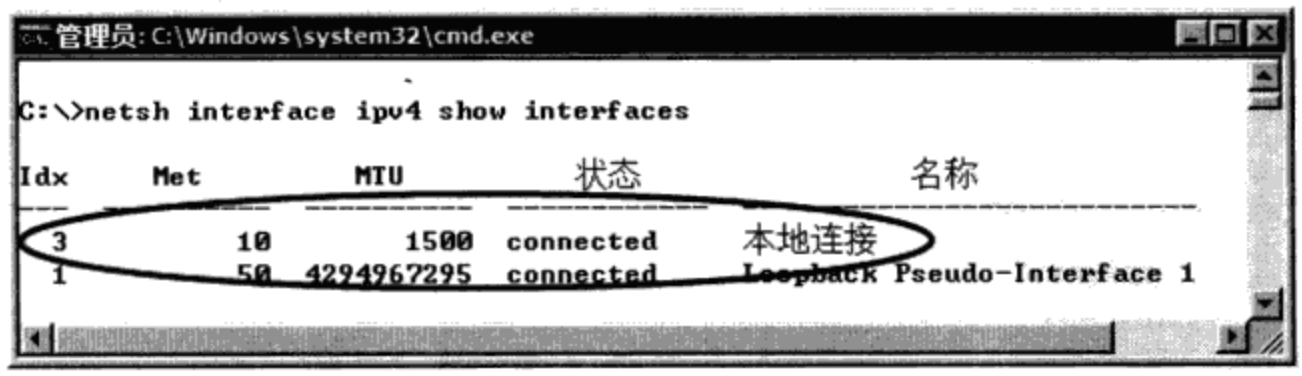


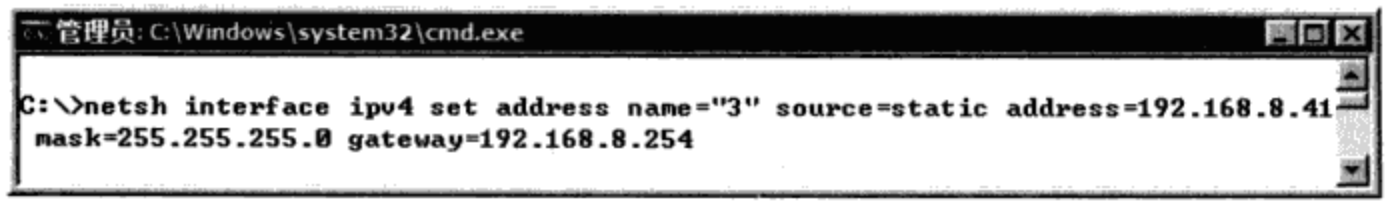
图 B-3

STEP 3 在**命令提示符**下，运行以下命令（如图 B-4所示）：

```
netsh  interface  ipv4  set  address  name="3"
```

```
source=static address=192.168.8.41  mask=255.255.255.0
gateway=192.168.8.254
```

其中的3为Idx代号。



图B-4

提示

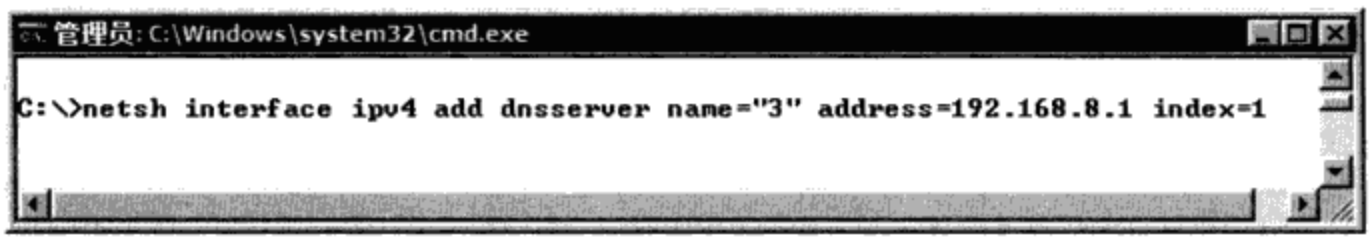
若要改回动态获取IP设置的话，请运行以下命令：

```
netsh  interface  ipv4  set  address  name="3"  source=dhcp
```

STEP 4 在**命令提示符**下，运行以下命令（如图 B-5所示）：

```
netsh  interface  ipv4  add  dnsserver  name="3"
address=192.168.8.1  index=1
```

其中**index=1**表示要设置第1台DNS服务器（首选DNS服务器）。



图B-5

提示

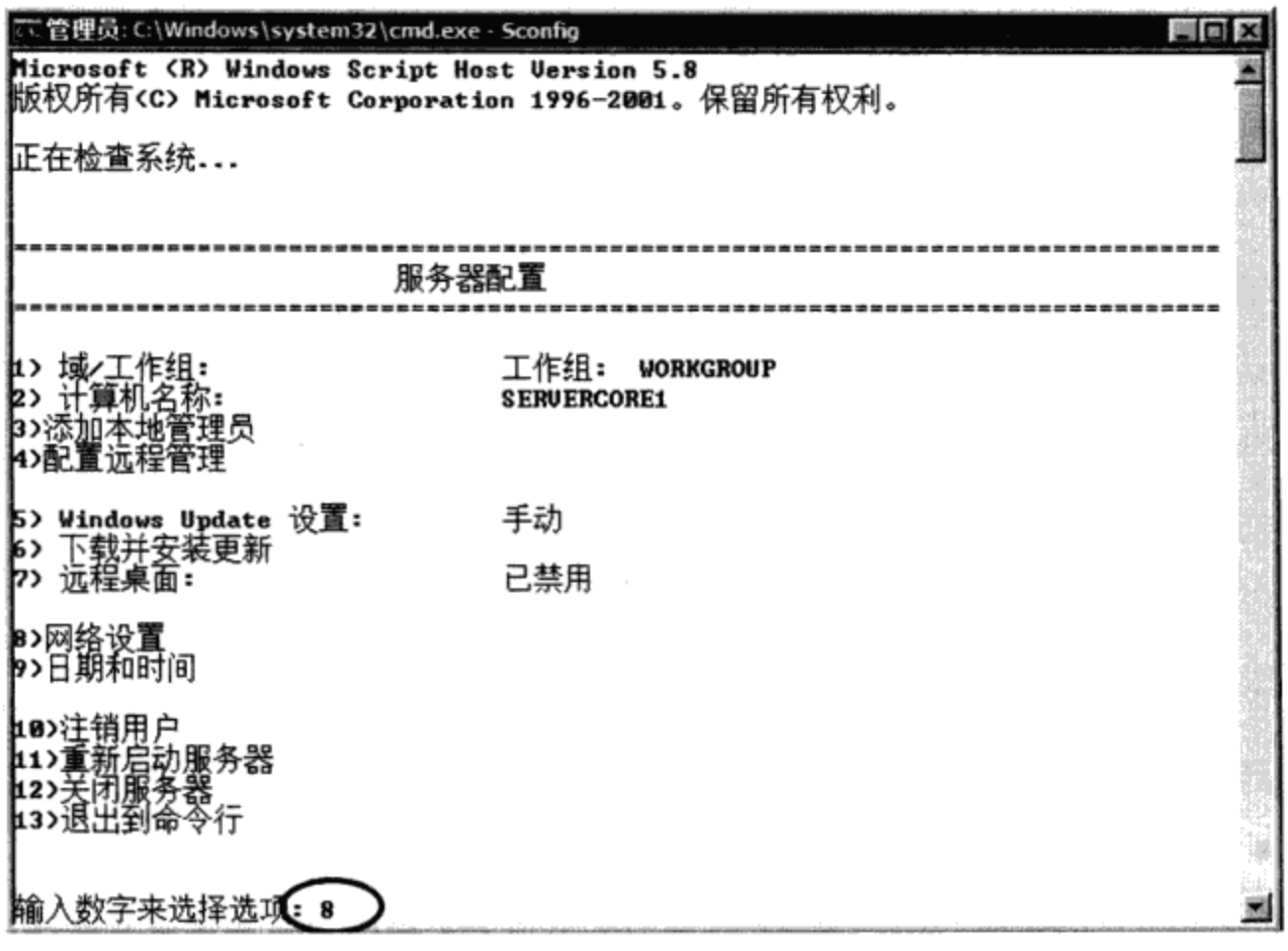
若要删除DNS服务器IP地址的话，请运行以下命令：

```
netsh interface ipv4 delete dnsserver name="3" address=192.168.8.1
```

STEP 5 有需要的话，可以重复**STEP 4**的步骤，以便设置多台DNS服务器，不过index数值必须依序增加。

STEP 6 使用**ipconfig /all**命令来查看上述设置是否正确。

您也可以使用**Sconfig**程序来更改IP地址等网络设置：运行**Sconfig**，然后在图 B-6中选择**网络设置**后单击Enter键。



图B-6

B-2-3 启用服务器核心安装

您可以通过以下步骤来启用**服务器核心安装**。请先运行以下命令来输入产品密钥：

```
Slmgr.vbs -ipk  <25个字符的密钥字符串>
```

完成后，再运行以下的命令来启用**服务器核心安装**：

```
Slmgr.vbs  -ato
```

屏幕上并不会显示启用成功的信息，但是会显示失败的信息。

您也可以到另外一台Windows Server 2008 R2、Windows Server 2008、Windows 7或Windows Vista计算机上打开**命令提示符**窗口，然后通过以下命令来启用**服务器核心安装**：

```
cscript \Windows\System32\slmgr.vbs ServerCore1 <用户名> <密码> -ato
```

其中假设**服务器核心安装**的计算机名为ServerCore1（或输入IP地址），而后请输入系统管理员账户Administrator及其密码。

B-2-4 加入域

假设此**服务器核心安装**的计算机名为ServerCore1，而且我们要使用域Administrator的身份

（假设其密码为111aaAA）来将其加入AD DS域sayms.com。请运行以下命令：

```
netdom join ServerCore1 /domain:sayms.com /userD:administrator
/passwordD:111aaAA
```

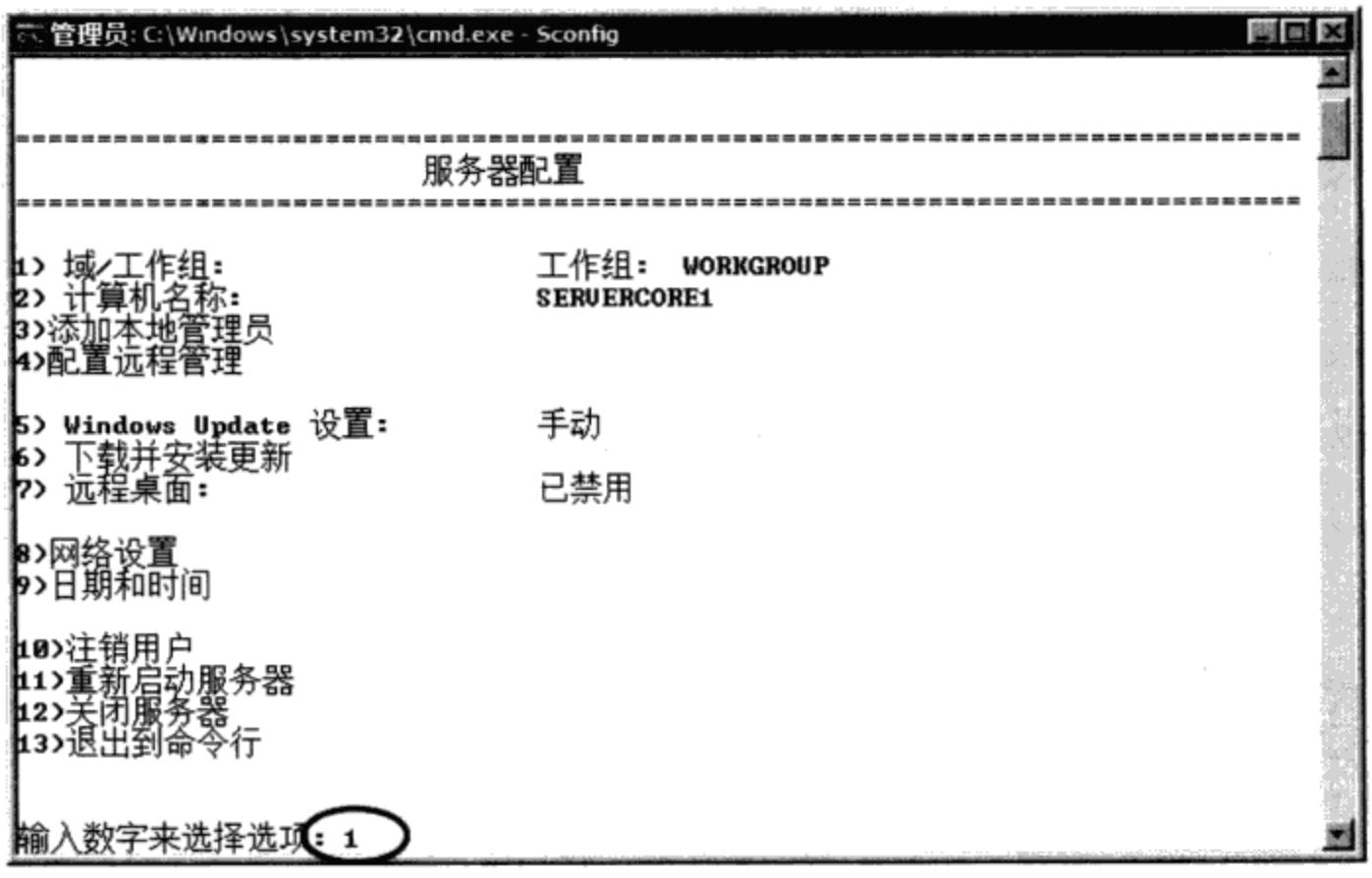
若担心输入密码时被旁人看到的话，可改为运行如下命令：

```
netdom join ServerCore1 /domain:sayms.com /userD:administrator
/passwordD:*
```

之后根据界面上的要求来输入密码，此时密码不会显示在屏幕上。
接下来通过以下命令来重新启动计算机，以便让此更改生效：

```
shutdown /r /t 0
```

您也可以通过运行**Sconfig**命令来将此计算机加入域：【如图 B-7所示选择**域/工作组**后单击Enter键➲输入**D**键后单击Enter键➲输入域名sayms.com后单击Enter键➲输入域系统管理员账户Administrator后单击Enter键➲输入此账户的密码后单击Enter键➲……】。



图B-7

B-2-5 将域用户加入本地Administrators组

您也可以将域用户账户加入到本地系统管理员组Administrators，例如若您要将域sayms.com用户peter加入到本地Administrators组的话，请运行以下的命令：

```
net localgroup administrators /add sayms.com\peter
```

您也可以通过运行**Sconfig**来将上述域用户Peter加入此计算机的本地Administrators组：【在图B-7中选择**添加本地管理员**后单击Enter键➲输入用户账户**sayms.com\Peter**后单击Enter键】。

B-2-6 更改日期与时间、地区及语言选项

若要更改日期与时间的话，请运行以下命令：

```
control timedate.cpl
```

您也可以通过运行**Sconfig**命令来更改日期与时间：【在图 B-7中选择**日期和时间**后单击Enter键➲……】。

若要更改地区及语言选项的话，请运行以下命令：

```
control intl.cpl
```

若要查看系统的版本信息的话，请运行以下命令：

```
systeminfo.exe
```



提示

在**服务器核心安装**内不支持使用winver.exe程序来查看版本信息。

B-3 在服务器核心安装内安装服务器角色

完成**服务器核心安装**的基本设置后，接下来可以安装服务器角色（Server Role）。在**服务器核心安装**内仅支持部分的服务器角色，可使用**dism.exe**程序来安装这些角色。

B-3-1 查看现有的角色与功能

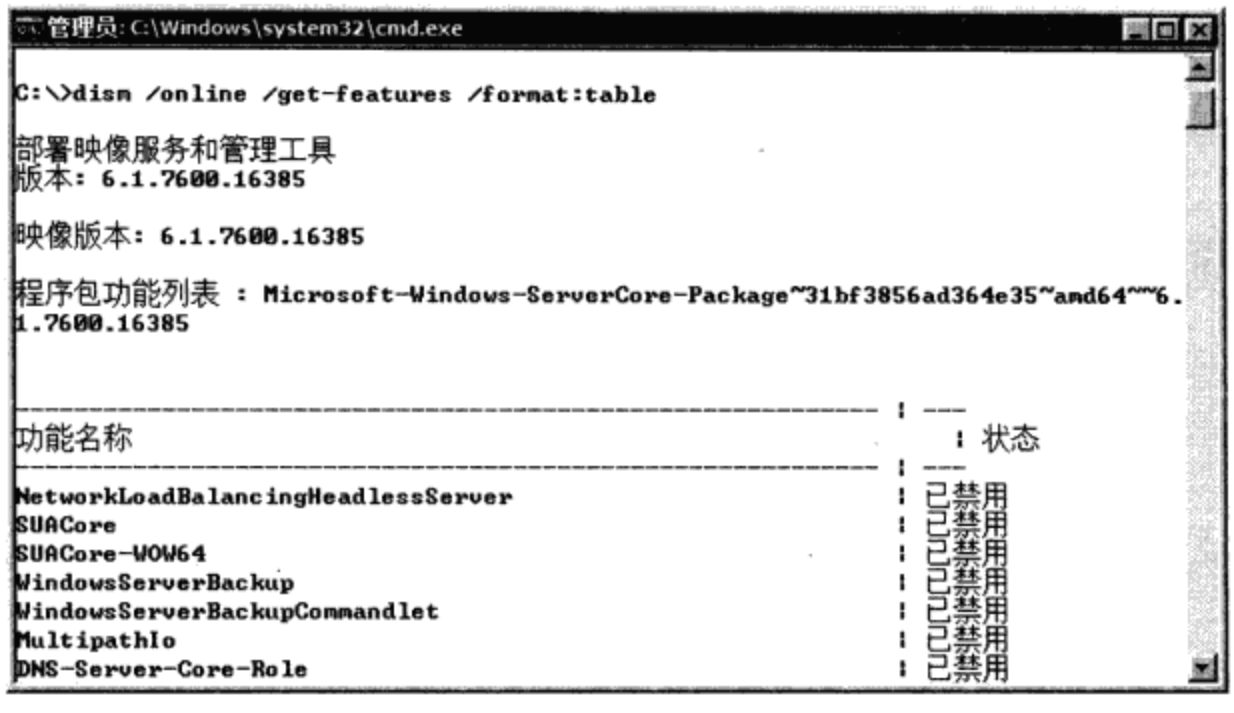
您可以先使用以下的**Dism.exe**命令来查看这台**服务器核心安装**内可以被安装的服务器角色与功能、查看当前已经安装的角色与功能，如图B-8所示。

```
Dism /online /get-features /format:table
```



提示

Windows Server 2008 **服务器核心安装**是使用**oclist**来查看可安装的、已经安装的、尚未安装的角色与功能。



B-8

B-3-2 DNS服务器角色

请运行以下命令来安装DNS服务器角色：

```
Dism /online /enable-feature /featurename:DNS-Server-Core-Role
```

注意**Dism.exe**命令中的参数大小写是有差异的（Case-Sensitive），因此**DNS-Server-Core-Role**字符串必须大小写都正确。

您可以在安装完成后，使用**dnscmd**命令或在其他计算机上通过DNS MMC主控制台来管理此台DNS服务器。

之后若要删除DNS服务器角色的话，请运行以下的命令：

```
Dism /online /disable-feature /featurename:DNS-Server-Core-Role
```

提示

其他角色的删除方法也是使用**/disable-feature**参数。Windows Server 2008 **服务器核心安装**是使用**ocsetup.exe**来安装角色与功能，例如安装DNS服务器的命令如下所示：

```
start  /w  ocsetup  DNS-Server-Core-Role
```

若要删除此角色的话，请在后面增加**/uninstall**参数。

B-3-3 DHCP服务器角色

请运行以下命令来安装DHCP服务器角色：

```
Dism /online /enable-feature /featurename:DHCPServerCore
```

您可以在安装完成后，使用**netsh**命令或在其他计算机上通过DHCP MMC主控制面板来管理此台DHCP服务器。如果它是架设在AD DS域环境中的话，则还需要经过授权的程序。

由于此DHCP服务器默认并不会自动启动，因此若要将其改为自动启动的话，请通过以下命令（注意**start=**与**auto**之间需空一格）：

```
sc config dhcpserver start= auto
```

若要手动启动的话，请运行以下的命令：

```
net start dhcpserver
```

B-3-4 文件服务角色

系统默认已经安装文件服务角色以提供共享管理功能，若要安装**文件服务**的其他功能的话，请运行以下命令：

- 安装**文件复制服务**（File Replication Service，FRS）

  Dism /online /enable-feature /featurename:FRS-Infrastructure

- 安装**分布式文件系统服务**（Distributed File System，DFS）

  Dism /online /enable-feature /featurename:DFSN-Server

- 安装**分布式文件系统复制服务**（DFS Replication Service）

  Dism /online /enable-feature /featurename:DFSR-Infrastructure- ServerEdition

- 安装Services for Network File System（NFS）

  Dism /online /enable-feature /featurename:ServerForNFS-Base

  Dism /online /enable-feature /featurename:ClientForNFS-Base

B-3-5 Hyper-V角色

请运行以下命令来安装Hyper-V角色：

```
Dism /online /enable-feature /featurename:Microsoft-Hyper-V
```

安装完成后，请在其他计算机上通过Hyper-V管理工具来管理，例如在Windows Server 2008 R2安装内通过**Hyper-V Manager**控制面板，而您可以通过安装**Hyper-V工具**这个角色管理工具来操作**Hyper-V Manager**控制台。

B-3-6 打印服务角色

请运行以下命令来安装与打印服务角色相关的服务：

- 安装打印服务器角色服务

  Dism /online /enable-feature /featurename:Printing-ServerCore-Role

- 安装Line Printer Daemon（LPD）服务

  Dism /online /enable-feature /featurename:Printing-LPDPrintService

若要在这台打印服务器上添加打印机的话，请到另外一台Windows Server 2008 R2、Windows Server 2008、Windows 7或Windows Vista计算机上使用**打印管理**（Print Management）控制面板。

B-3-7 Active Directory证书服务（AD CS）角色

请运行以下命令来安装AD CS角色：

```
Dism /online /enable-feature /featurename:CertificateServices
```

B-3-8 Active Directory轻型目录服务（AD LDS）角色

请运行以下命令来安装AD LDS角色（需要先安装**NetFx3-ServerCore**）：

```
Dism /online /enable-feature /featurename:NetFx3-ServerCore
Dism /online /enable-feature /featurename:DirectoryServices-ADAM-
ServerCore
```

B-3-9 Active Directory域服务（AD DS）角色

请运行以下命令来安装**Active Directory域服务**（AD DS）角色：

```
dcpromo /unattend:<应答文件>
```

B-3-10 Stream Media Services角色

请通过以下步骤来安装Stream Media Services（流媒体服务）：

STEP 1 使用另外一台计算机连接微软网站、下载Stream Media Services的安装文件（例如

Windows Media Services 2008 for Windows Server 2008 R2，其文件后缀名为.msu）。

STEP 2 将此安装文件复制到**服务器核心安装**计算机（可通过USB移动硬盘或CD/DVD），并运行上述安装文件。

STEP 3 运行以下命令：

```
Dism /online /enable-feature /featurename:MediaServer
```

STEP 4 到另外一台计算机上通过Stream Media Services MMC控制面板来管理此Stream Media Services角色。

> **提示**
>
> 您可以到另外一台已经安装Stream Media Services的Windows Server 2008 R2计算机上，使用**Windows Media Service**控制面板来管理**服务器核心安装**上的Stream Media Services。

B-3-11 Web服务器（IIS）角色

若要采用默认安装选项来安装**Web服务器（IIS）**的话，请运行以下命令：

```
start /w pkgmgr /iu:IIS-WebServerRole;WAS-WindowsActivationService;
WAS-ProcessModel
```

若要安装所有选项的话，请运行以下命令：

```
start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;
IIS-CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;
IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-HttpRedirect;
IIS-ApplicationDevelopment;IIS-ASP;IIS-CGI;IIS-ISAPIExtensions;
IIS-ISAPIFilter;IIS-ServerSideIncludes;IIS-HealthAndDiagnostics;
IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;
IIS-HttpTracing;IIS-CustomLogging;IIS-ODBCLogging;IIS-Security;
IIS-BasicAuthentication;IIS-WindowsAuthentication;
IIS-DigestAuthentication;IIS-ClientCertificateMappingAuthentication;
IIS-IISCertificateMappingAuthentication;IIS-URLAuthorization;
IIS-RequestFiltering;IIS-IPSecurity;IIS-Performance;
IIS-HttpCompressionStatic;IIS-HttpCompressionDynamic;
IIS-WebServerManagementTools;IIS-ManagementScriptingTools;
IIS-IIS6ManagementCompatibility;IIS-Metabase;
IIS-WMICompatibility;IIS-LegacyScripts;IIS-FTPPublishingService;
```

```
IIS-FTPServer;WAS-WindowsActivationService;WAS-ProcessModel
```

提示

若要删除**Web服务器（IIS）**的话，请运行以下命令：

```
start /w pkgmgr /uu:IIS-WebServerRole;
WAS-WindowsActivationService;WAS-ProcessModel
```

B-4 在服务器核心安装内安装功能

在**服务器核心安装**的基本设置完成，且服务器角色也安装、设置完成后，接着您可以开始安装功能（Feature）选项。您可以先通过以下的**dism.exe**命令来查看这台**服务器核心安装**内可以安装的功能：

```
Dism /online /get-features /format:table
```

要安装功能的话，请运行以下的命令：

```
Dism /online /enable-feature /featurename:<功能名称>
```

若要删除功能的话，请运行以下的命令：

```
Dism /online /disable-feature /featurename:<功能名称>
```

其中**<功能名称>**的大小写是有差异的，而它们可以是如下选项。

- 故障转移群集：FailoverCluster-Core。
- 网络负载平衡：NetworkLoadBalancingHeadlessServer。
- UNIX应用程序子系统：SUACore。
- UNIX应用程序32位子系统：SUACore-WOW64。
- Windows Server Backup：WindowsServerBackup。
- 多路径IO：MultipathIo。
- 可移动存储管理器：Microsoft-Windows-RemovableStorageManagementCore。
- Bitlocker磁盘驱动器加密：BitLocker。

提示

若要允许通过远程来管理此BitLocker的话，请在这台**服务器核心安装**内运行以下命令：

```
Dism /online /enable-feature /featurename:BitLocker-RemoteAdminTool
```

- SNMP服务：SNMP-SC。
- WINS服务器：WINS-SC。

- QWAVE：QWAVE。
- Telnet客户端：TelnetClient。
- Branch Cache：PeerDist、PeerDistHashP与SMBHashGeneration。
- .NET Framework 2.0：NetFx2-ServerCore。若要支持32位的话，请使用NetFx2-ServerCore-WoW64。
- .NET Framework 3.0与3.5：NetFx3-ServerCore。若要支持32位的话，请同时使用NetFx2-ServerCore-WoW64与NetFx3-ServerCore- WoW64。
- Windows PowerShell：MicrosoftWindowsPowerShell。
- Windows PowerShell Server Manager cmdlets：ServerManager-PSH-Cmdlets。
- Windows PowerShell Best Practices Analyzer cmdlets：BestPractices-PSH-Cmdlets。
- WoW64（默认已经安装）：ServerCore-WOW64。
- Input Method Editor 32-bit support：ServerCore-EA-IME-WOW64。
- Windows Server Migration Tools：ServerMigration。
- IIS Management Service：IIS-ManagementService。



提示

完成安装IIS Management Service后，若要启用远程管理功能的话，请将注册表**EnableRemoteManagement**设置为1，它位于以下注册路径：

```
HKLM\Software\Microsoft\WebManagement\Server
```

接下来通过运行以下命令来启动IIS Management Service：

```
net  start  wmsvc
```

B-5 服务器核心安装的远程管理

您可以在其他计算机中（以下将其称为**源计算机**）通过以下几种途径来远程管理**Windows Server 2008 R2 服务器核心安装**：

- 远程桌面。
- RemoteApp。
- MMC管理控制台。
- 服务器管理器。
- Windows Remote Shell。



提示

您还可以通过**scregedit.wsf**脚本文件来运行其他管理工作，此脚本文件的使用方法可通过以下命令来查询：

```
cscript  C:\Windows\System32\scregedit.wsf  /cli
```

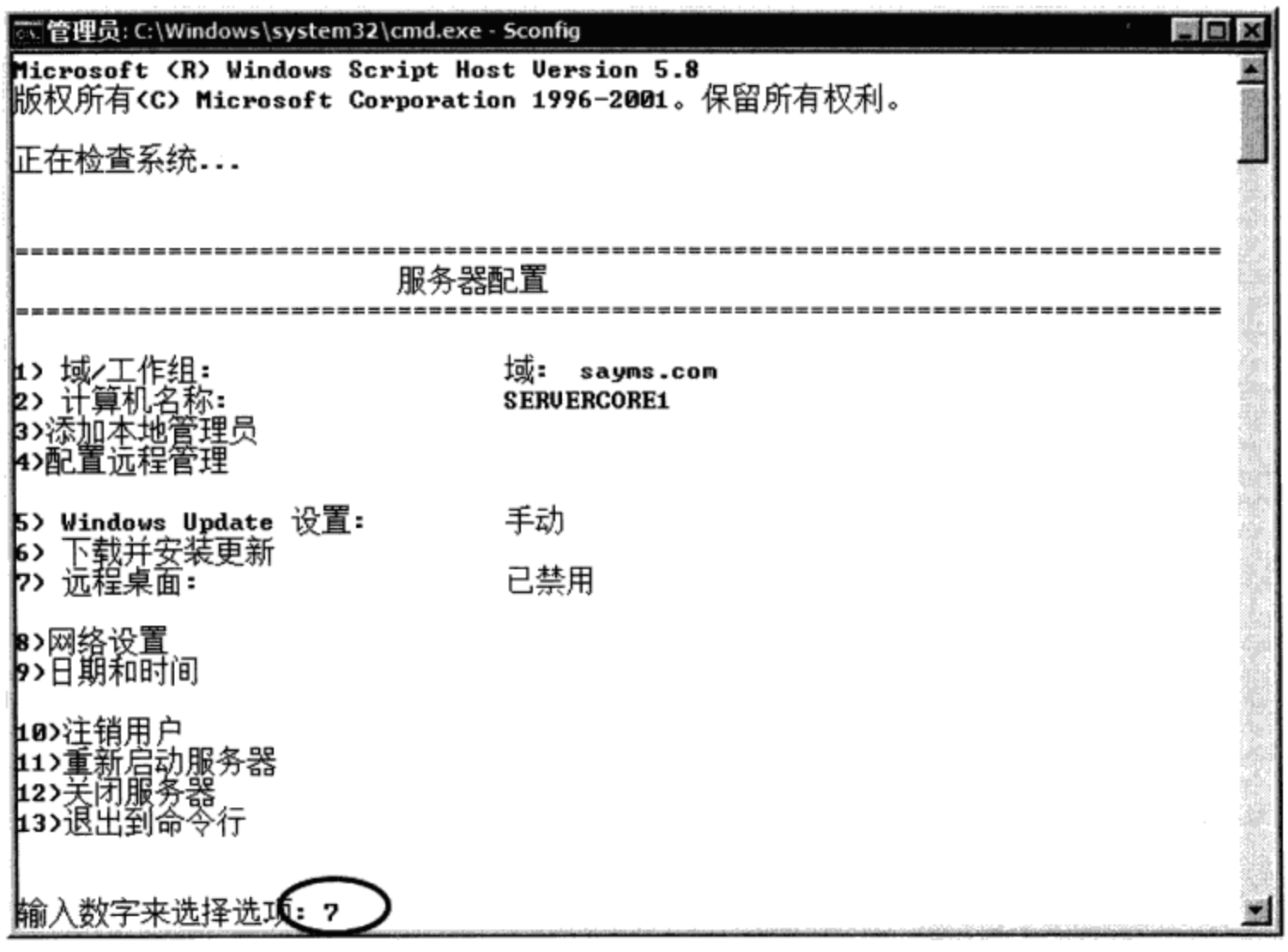
B-5-1 通过远程桌面来管理服务器核心安装

我们需要先在**服务器核心安装**上启用**远程桌面**，然后通过源计算机的**远程桌面连接**来连接与管理**服务器核心安装**。

STEP 1 请在**服务器核心安装**上运行以下命令：

```
cscript  C:\Windows\System32\Scregedit.wsf  /ar  0
```

其中的**/ar 0**表示启用**远程桌面**，若输入**/ar 1**表示禁用、**/ar /v**用来查看**远程桌面**当前的启用状态。也可以通过运行**Sconfig**命令来启用**远程桌面**：【如图 B-9所示选择**远程桌面**后单击Enter键➲输入**E**键后单击Enter键➲输入**1**或**2**后单击Enter键➲...】。



图B-9

STEP 2 到源计算机上选择【开始➲运行➲输入**mstsc**➲单击确定按钮】。

STEP 3 如图 B-10所示，通过【输入**服务器核心安装**的IP地址（或主机名）➲单击连接按钮➲输入Administrator与其密码➲单击确定按钮】的方式进行操作。



图 B-10

STEP 4 接下来便可通过**命令提示符**来管理此**服务器核心安装**。

STEP 5 完成管理工作后，请输入**logoff**命令以便结束此连接。

B-5-2 通过 RemoteApp来管理服务器核心安装

我们需要在一台安装Windows Server 2008 R2的源计算机上安装**远程桌面会话主机工具**、创建RemoteApp 的RDP封装、通过此封装来管理**服务器核心安装**，操作步骤如下。

STEP 1 请先确认**服务器核心安装**计算机已经启用**远程桌面**。

STEP 2 请到另一台安装Windows Server 2008 R2的源计算机上：【单击左下角的**服务器管理器**图标➲功能➲添加功能➲展开**远程服务器管理工具**➲角色管理工具➲远程桌面服务工具➲选择**远程桌面会话主机工具**➲…】。

STEP 3 选择【开始➲运行➲输入MMC后单击确定按钮➲选择**文件**菜单➲添加/删除管理单元➲选择**RemoteApp管理器**➲单击添加按钮➲如图 B-11所示选择**另一台计算机**➲输入**服务器核心安装**的IP地址（假设是192.168.8.41）➲单击两次确定按钮】。

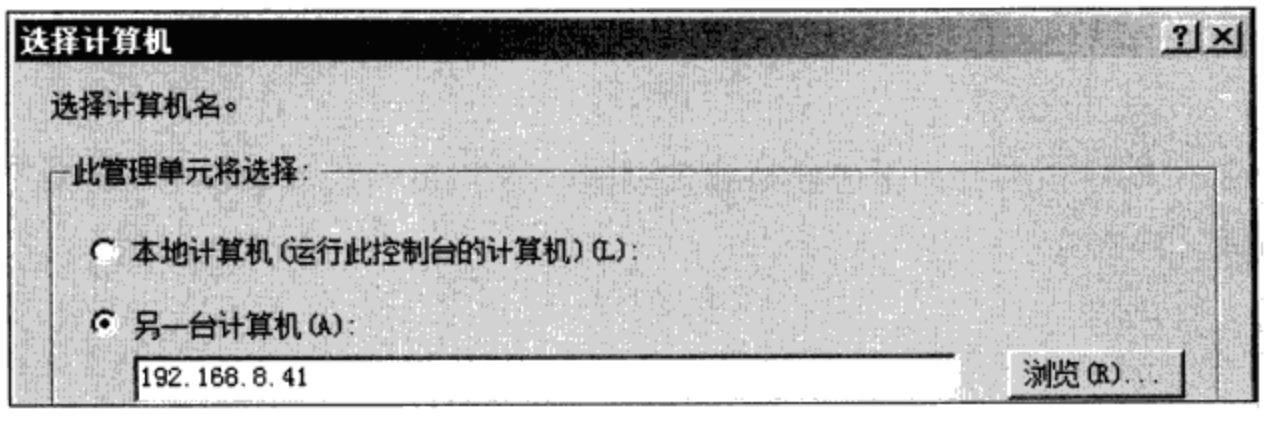


图 B-11

STEP 4 如图 B-12所示，通过【单击**RemoteApp管理器**选项➲单击**添加 RemoteApp程序**选项】的方式进行操作。

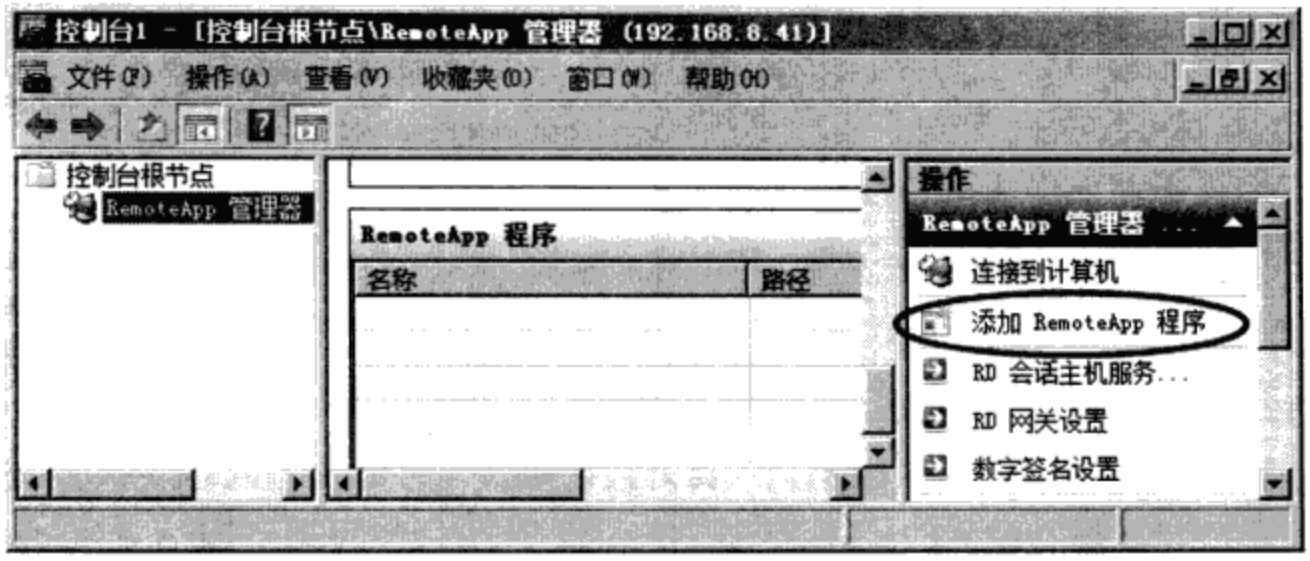


图 B-12

STEP 5 当出现欢迎使用RemoteApp的向导界面时单击 下一步 按钮。

STEP 6 在图 B-13中单击 浏览 按钮。

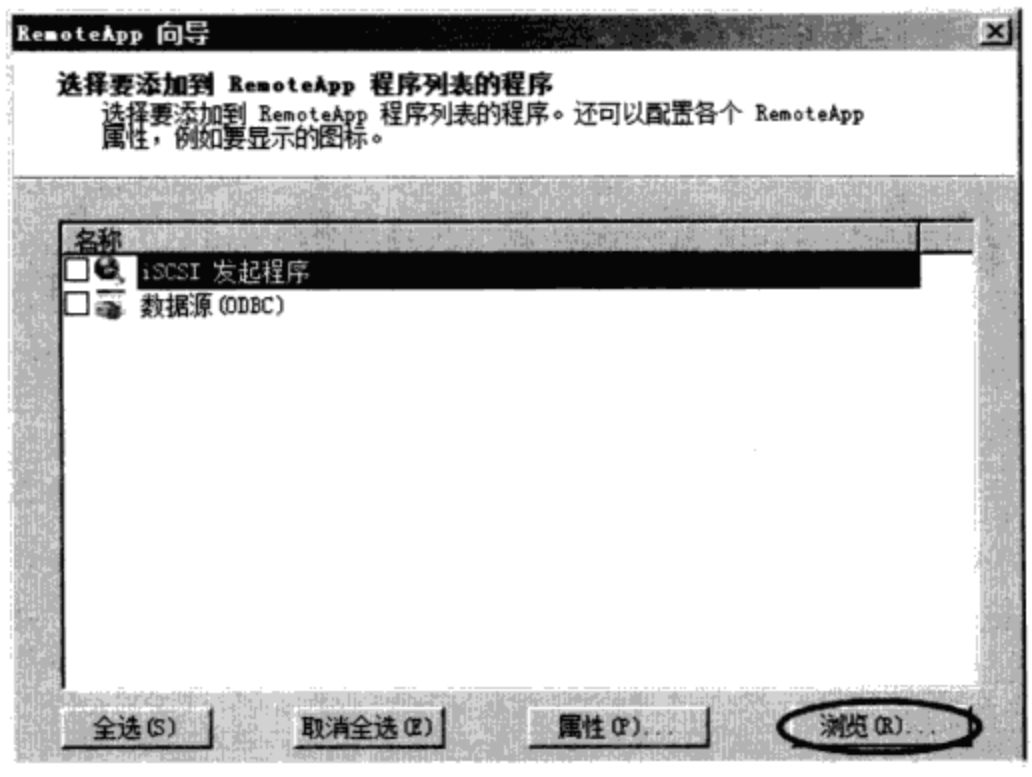


图 B-13

STEP 7 在图 B-14中浏览到**服务器核心安装**的C$\Windows\System32 \cmd.exe文件后单击 打开 按钮。

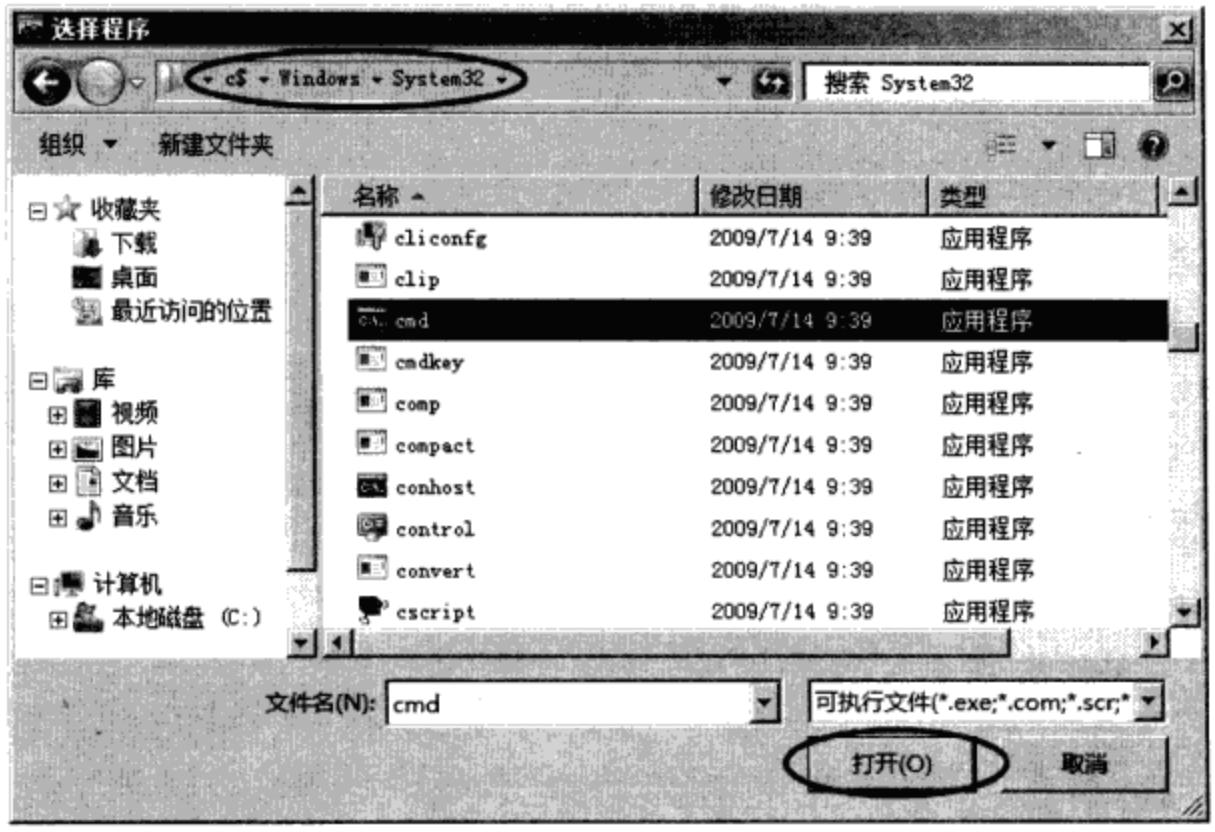


图 B-14

STEP 8 当在选择要添加到RemoteApp程序列表的程序界面中单击下一步按钮。

STEP 9 当出现**复查设置**界面时单击完成按钮。

STEP 10 如图 B-15所示，当**cmd.exe**程序出现在**RemoteApp程序**列表后【对着此程序右击➲**创建.rdp文件**】。

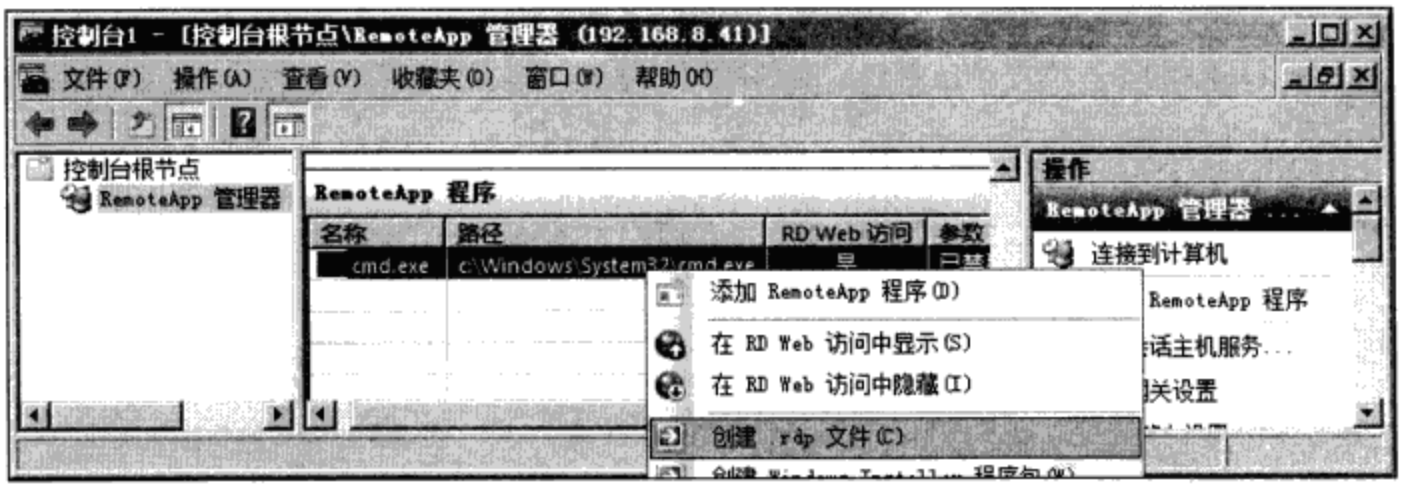
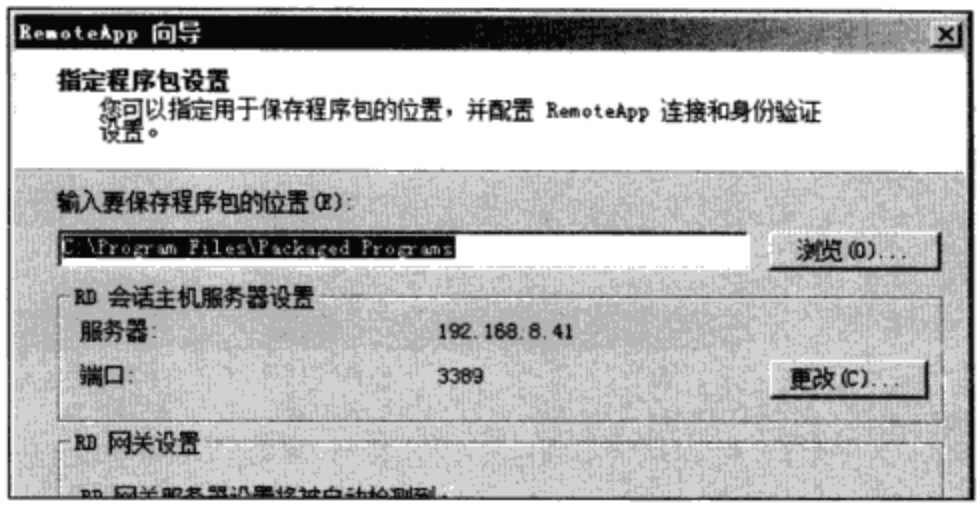


图 B-15

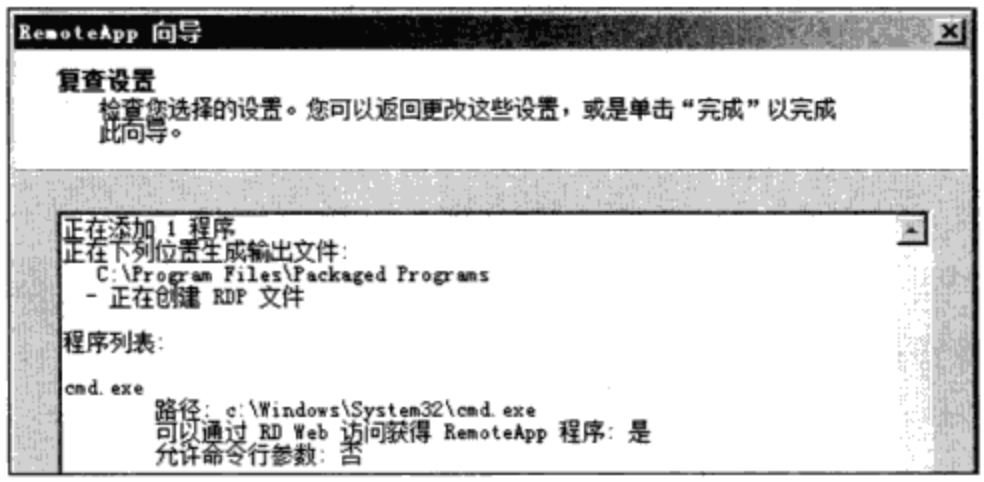
STEP 11 当出现欢迎使用RemoteApp向导界面时单击下一步按钮。

STEP 12 在图 B-16中输入此.rdp文件的存储地点后单击下一步按钮，图中我们采用默认存储位置。



图B-16

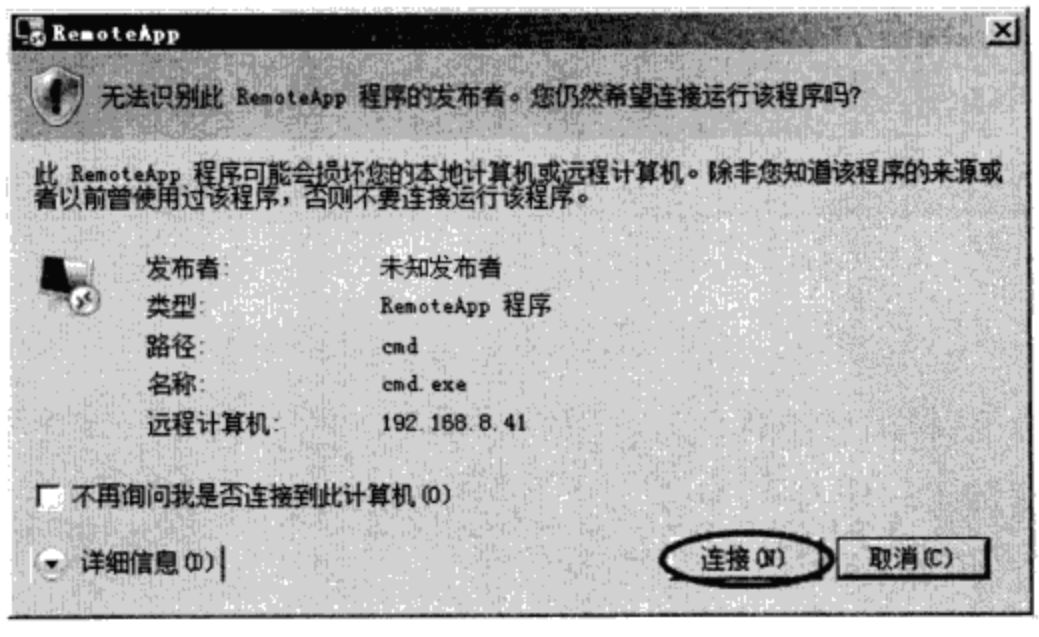
STEP 13 确认图 B-17中的设置无误后单击完成按钮。



图B-17

STEP 14 运行这个新创建的.rdp文件（位于C:\Program Files\Packaged Programs文件夹），它就会连接到**服务器核心安装**。

STEP 15 若出现图 B-18的话，请直接单击连接按钮。



图B-18

STEP 16 在图 B-19中输入Administrator账户和密码后单击确定按钮。

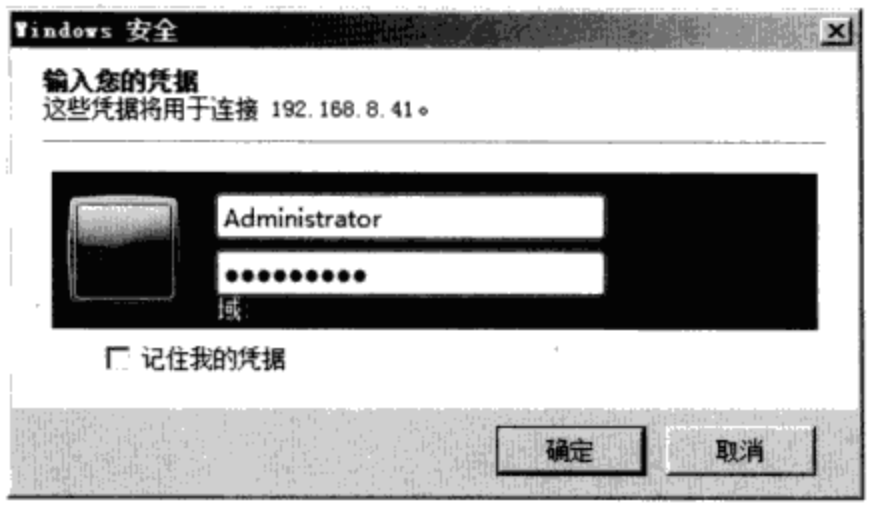


图 B-19

STEP 17 若出现图 B-20的话，请直接单击**是（Y）**按钮。

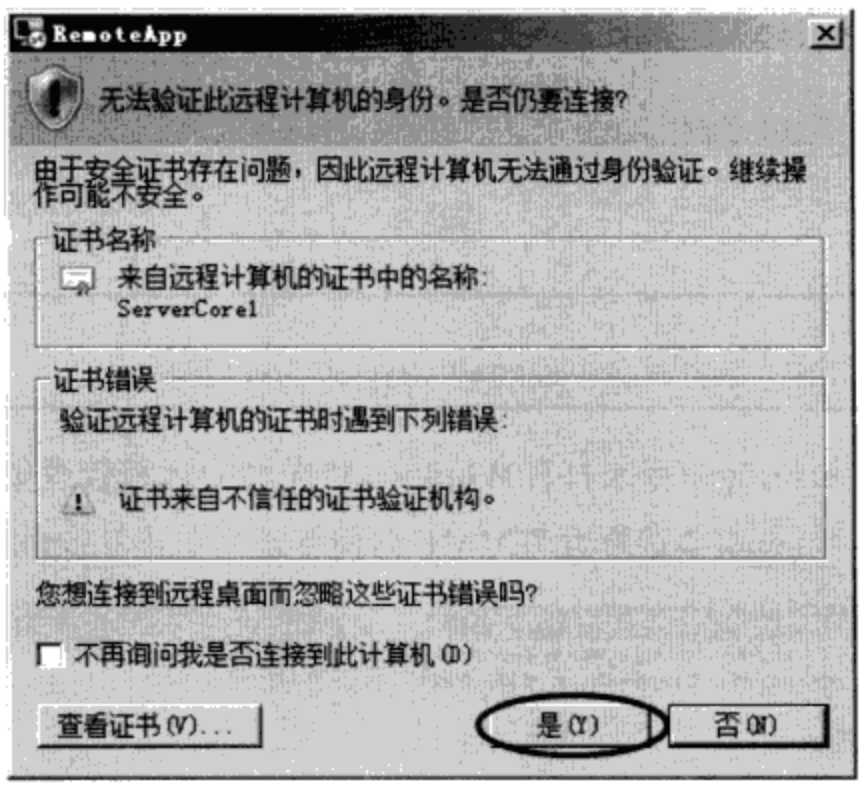


图 B-20

STEP 18 如图 B-21所示可通过**命令提示符**窗口来管理**服务器核心安装**计算机。

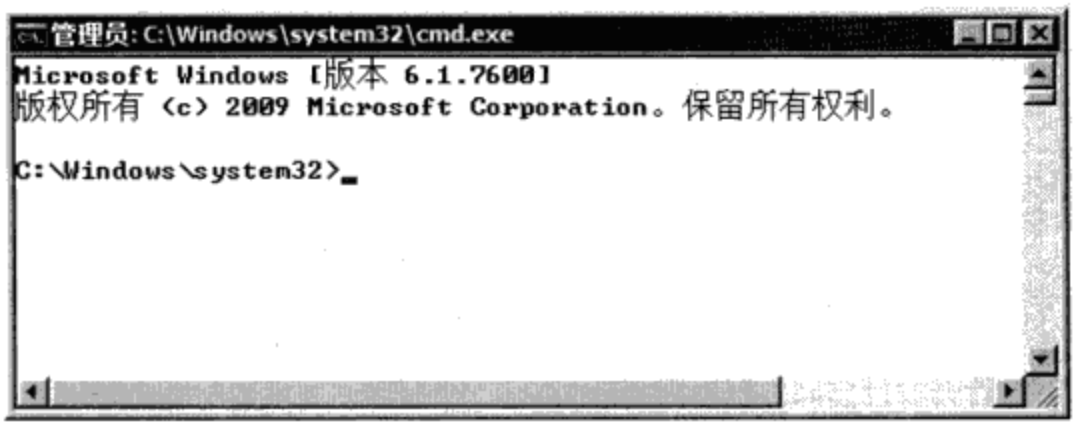


图 B-21

STEP 19 完成管理工作后，运行**exit**命令即可结束此连接。

B-5-3 通过MMC管理控制台来管理服务器核心安装

您可以通过现有的或自定义的MMC管理控制台来连接与管理**服务器核心安装**，以下假设源计算机与**服务器核心安装**都是AD DS域成员。

若要在源计算机上，使用MMC管理控制台（例如**计算机管理**控制台）来远程管理**服务器核心安装**的话，则您必须在**服务器核心安装**上通过以下命令来打开**Windows防火墙**的**远程管理**策略（参见图 B-22）：

```
netsh advfirewall firewall set rule group="远程管理"  new enable=yes
```

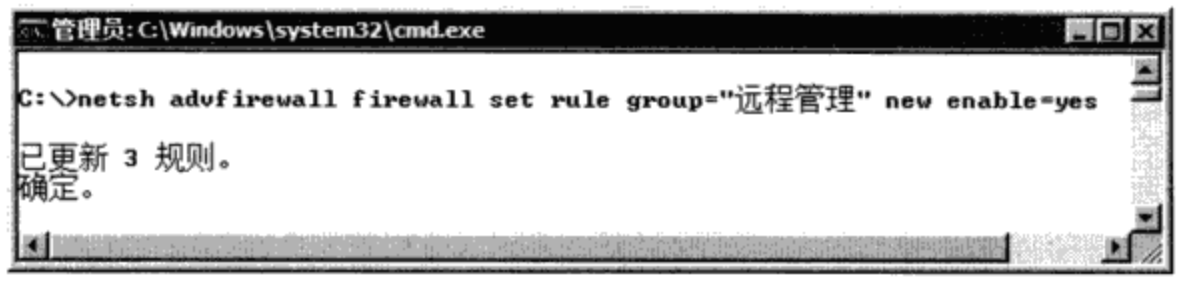


图 B-22

> **注意**
>
> 若要禁用此策略的话，请将命令中的**enable=yes**改为**enable=no**。

您也可以通过运行**Sconfig**命令来打开**Windows防火墙**的**远程管理**策略：【如图 B-23所示选择**配置远程管理**后单击Enter键➲选择**允许MMC远程管理**后单击Enter键】。

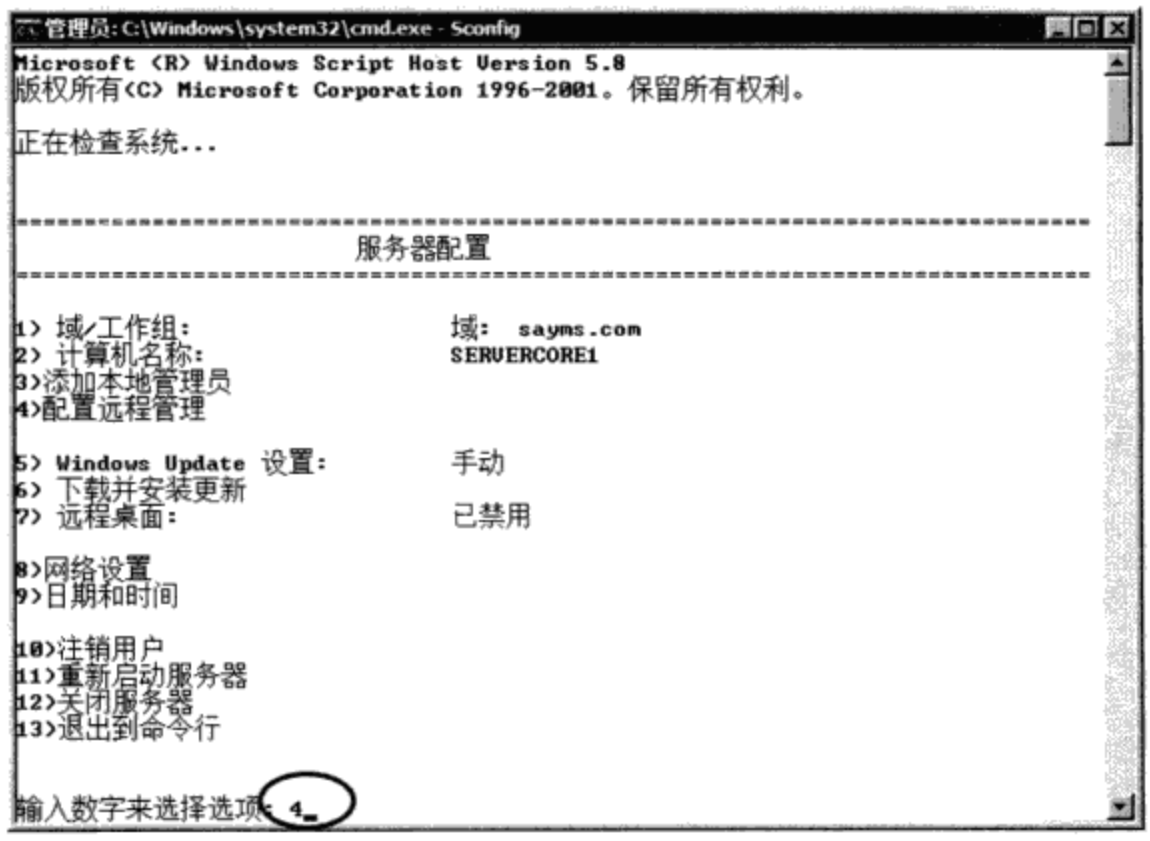
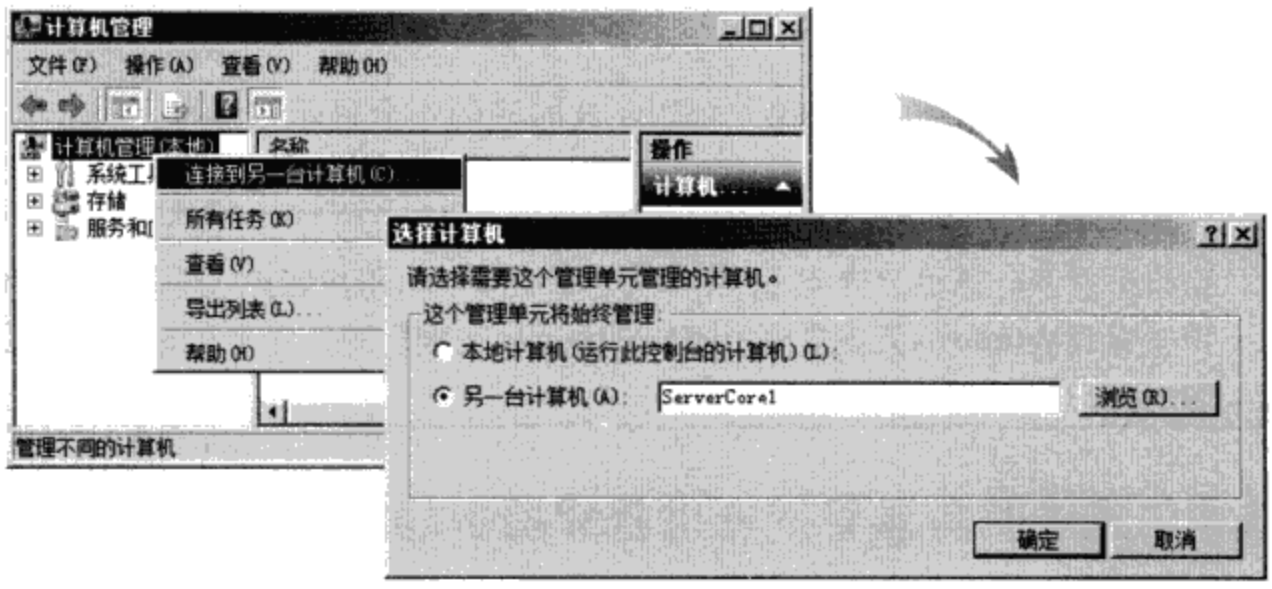


图 B-23

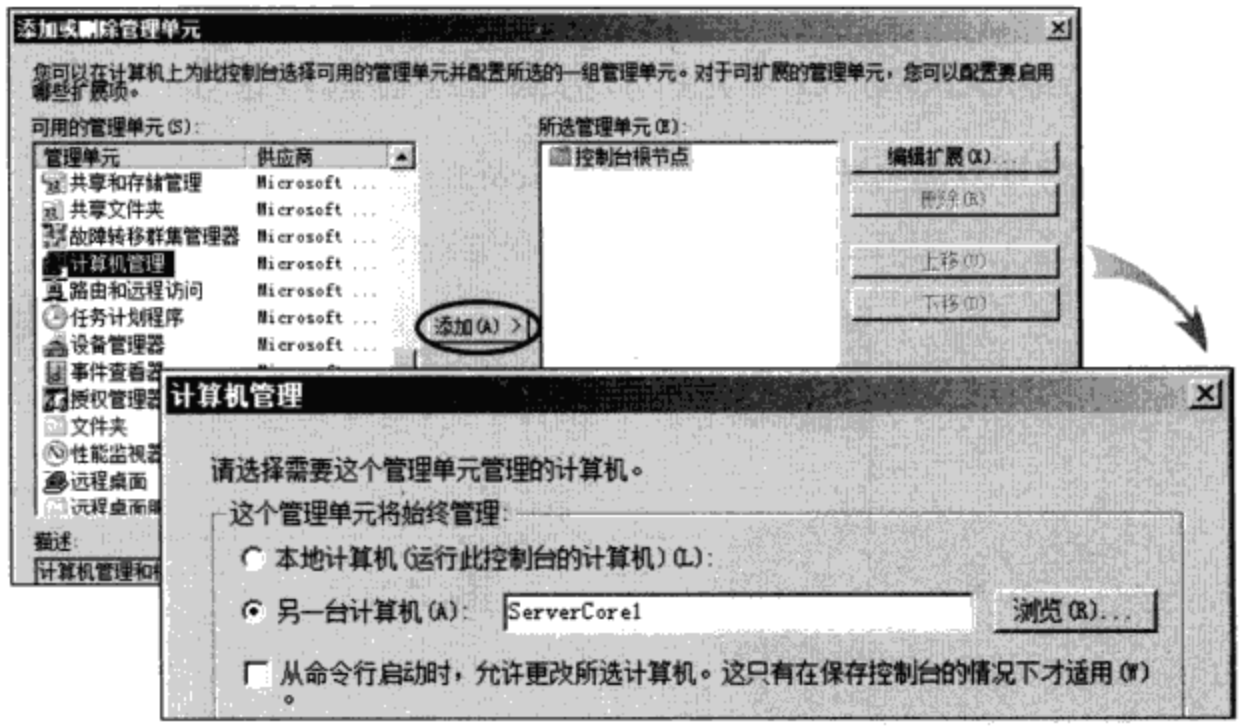
我们将在源计算机上，分别使用现有的与自定义的MMC管理控制台来进行说明：

- **现有的MMC管理控制台**：以**计算机管理**控制台为例，如图 B-24所示，通过【对着**计算机管理（本地）**单击右键➲连接到另一台计算机➲输入**服务器核心安装**的计算机名或IP地址】的方式来连接与管理**服务器核心安装**计算机。



图B-24

- **自定义的MMC管理控制台**：以自定义**计算机管理**控制台为例，通过【开始➲运行➲输入MMC后单击 确定 按钮➲选择**文件**菜单➲添加/删除管理单元➲如图 B-25所示选择**计算机管理**➲单击 添加 按钮➲输入**服务器核心安装**的计算机名（假设是ServerCore1）或IP地址➲单击 完成、确定 按钮】的方法进行操作。



图B-25

如果源计算机不是隶属于AD DS域的话，则您可能需要在源计算机上，先通过以下命令来指定用来连接**服务器核心安装**的用户账户，再通过MMC管理控制台来连接与管理**服务器核心安装**。以下假设要连接的**服务器核心安装**的计算机名为ServerCore1，要被用来连接的账户为Administrator（其他账户也可以，但必须隶属于**服务器核心安装**的本地Administrators组），其密码为111aaAA：

```
Cmdkey /add:ServerCore1 /user:Administerator /pass:111aaAA
```

若担心输入密码时被其他人看到的话，请运行以下命令：

```
Cmdkey /add:ServerCore1 /user:Administerator /pass
```

之后根据界面上的要求来输入密码，此时密码不会显示在屏幕上。

提示

您也可在源计算机上使用【开始➲控制面板➲单击**用户账户**（或**用户账户和家庭安全**）➲单击**管理Windows凭据**➲单击**添加Windows凭据**】的方法来指定用来连接**服务器核心安装**的用户账户与密码】。

B-5-4 通过服务器管理器来管理服务器核心安装

您可在一台安装Windows Server 2008 R2的源计算机上，通过**服务器管理器**来连接与管理**服务器核心安装**。假设源计算机与**服务器核心安装**都是AD DS域成员，且**服务器核心安装**的计算机名为ServerCore1。

您可以在**服务器核心安装**上，使用Sconfig或Windows PowerShell命令来允许源计算机通过服务器管理器来远程管理此**服务器核心安装**。

1. 使用 SCONFIG 来允许服务器管理器远程管理

STEP 1 在**服务器核心安装**上运行Sconfig。

STEP 2 如图 B-26所示选择**配置远程管理**后单击Enter键。

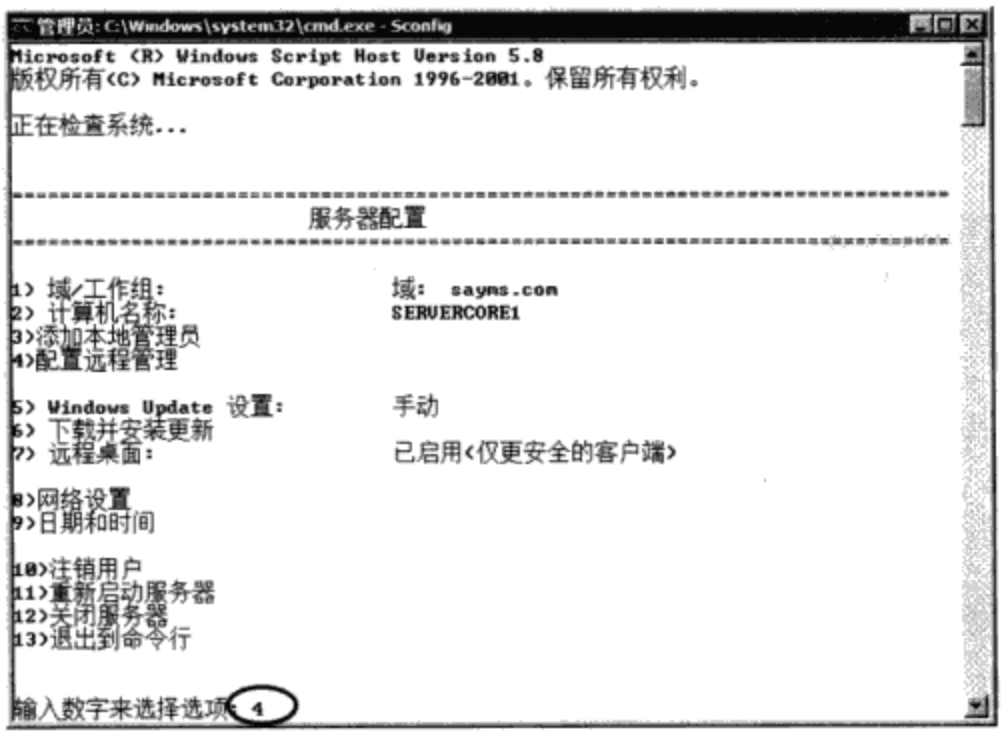


图 B-26

STEP 3 在图 B-27中选择**启用Windows PowerShell**后单击Enter键。

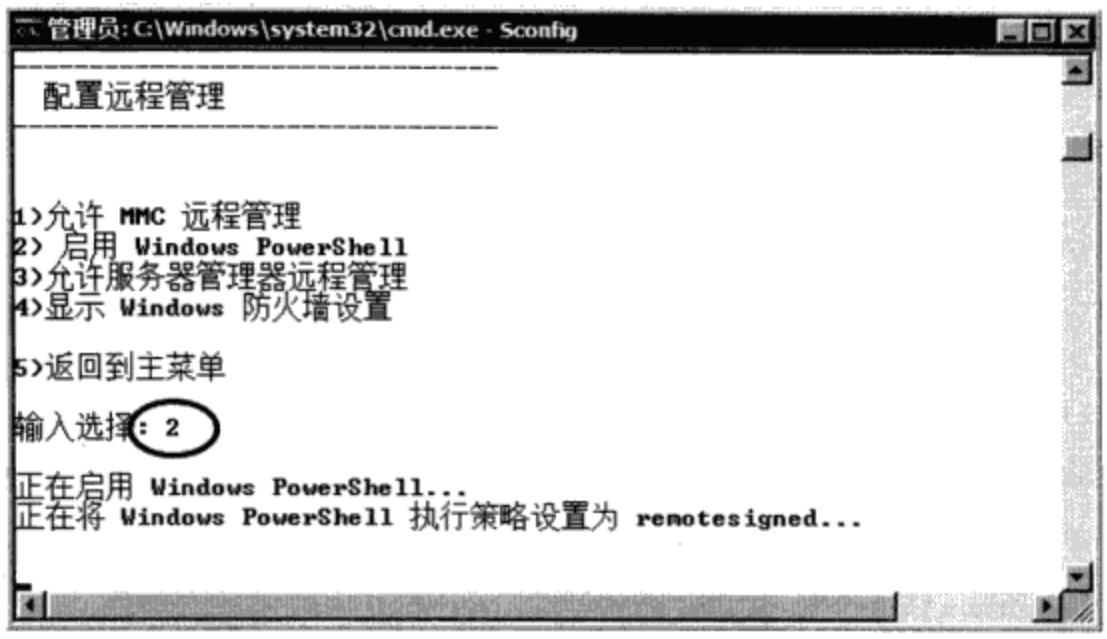


图 B-27

STEP 4 当出现如图 B-28所示的界面时单击是（Y）按钮以便重新启动计算机。

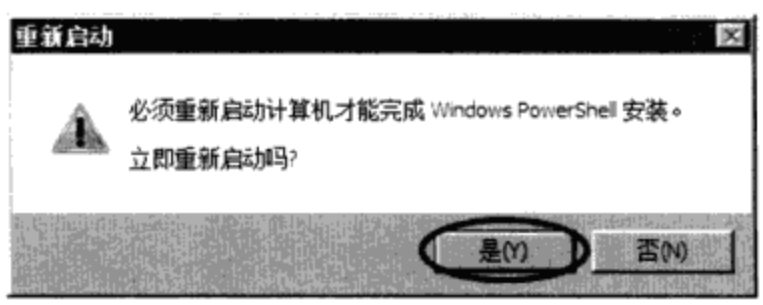


图 B-28

STEP 5 重新登录**服务器核心安装**。

STEP 6 运行**Sconfig**命令并选择**配置远程管理**后单击Enter键，如图 B-29所示，选择**允许服务器管理器远程管理**后单击Enter键】。

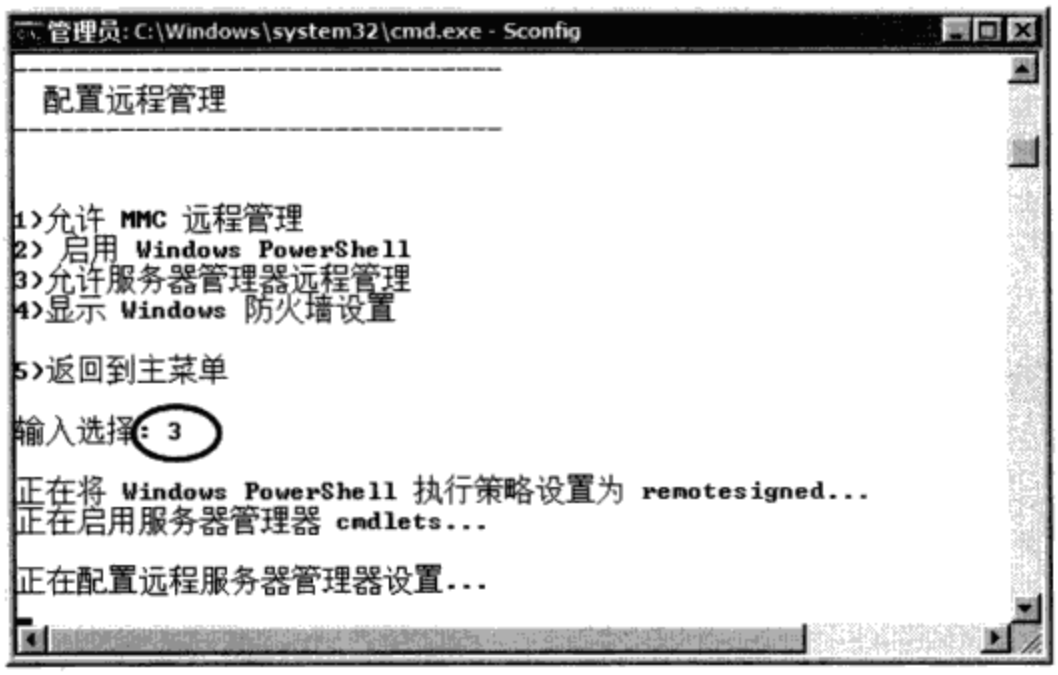


图 B-29

STEP 7 当出现**已启用**界面时单击确定按钮。

2. 使用 Windows PowerShell 命令来允许服务器管理器远程管理

STEP 1 在**服务器核心安装**上运行以下命令来安装所需功能：

```
Dism.exe/Online/Enable-Feature/FeatureName:NetFx2-ServerCore
/FeatureName:MicrosoftWindowsPowerShell/FeatureName:ServerMana
ger -PSH-Cmdlets /FeatureName: BestPractices-PSH- Cmdlets
```

STEP 2 运行**shutdown /r /t 0**命令来重新启动计算机，并以系统管理员的身份重新登录。有需要的话，可以使用**dism.exe**命令来确认上述功能是否已经安装成功。

STEP 3 启动Windows PowerShell，输入命令PowerShell后单击Enter键。

STEP 4 运行以下命令：

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

STEP 5 通过运行以下命令来允许通过服务器管理器远程管理：

```
Configure-SMRemoting.ps1 -force -enable
```

（1）到源计算机通过服务器管理器来管理服务器核心安装

STEP 1 到安装Windows Server 2008 R2的源计算机上，通过【单击**服务器管理器**图标➲如图 B-30所示对着**服务器管理器**右击➲连接到另一台计算机】的方式进行操作。

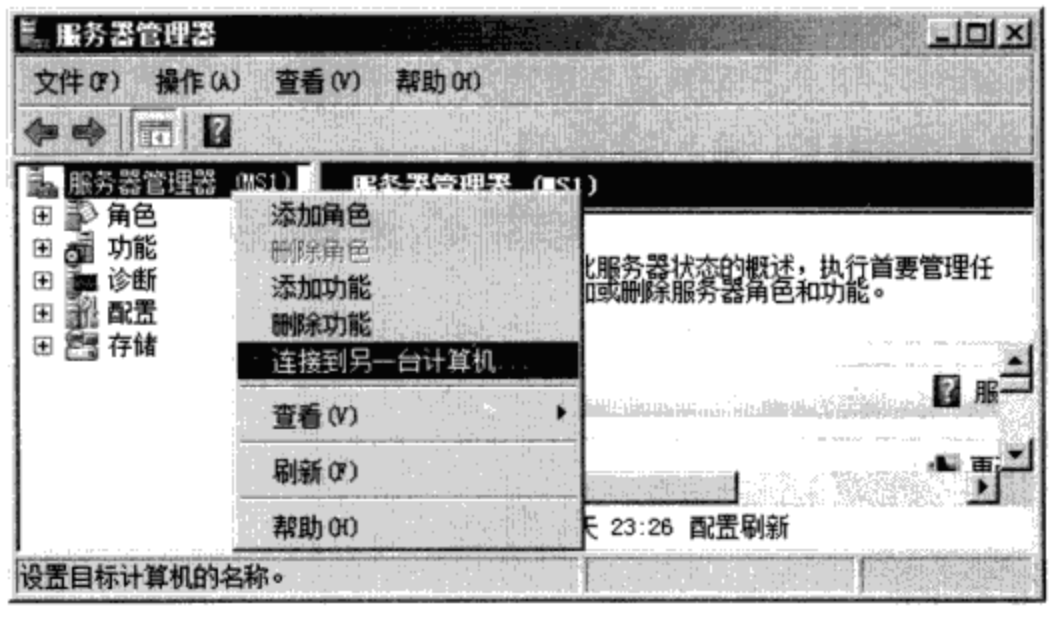


图 B-30

STEP 2 如图 B-31所示，通过【选择**另一台计算机**单选按钮➲单击浏览按钮或输入**服务器核心安装**的计算机名ServerCore1➲单击确定按钮】的方式进行操作。

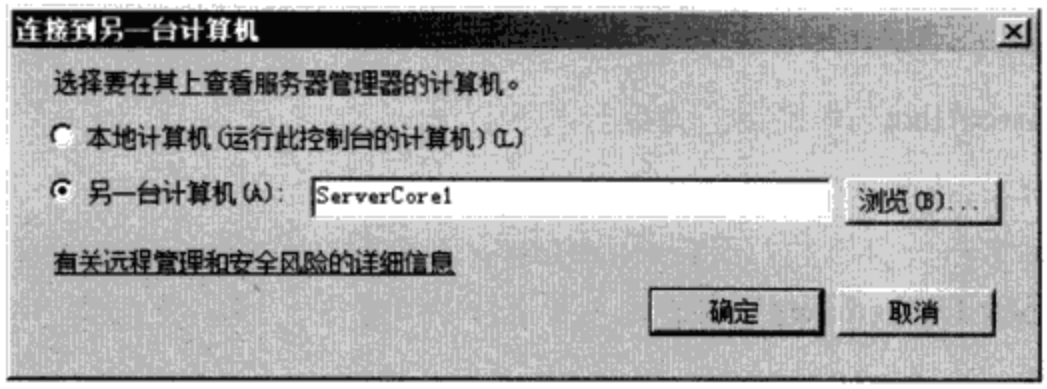


图 B-31

STEP 3 如图 B-32所示通过服务器管理器来管理**服务器核心安装**ServerCore1。

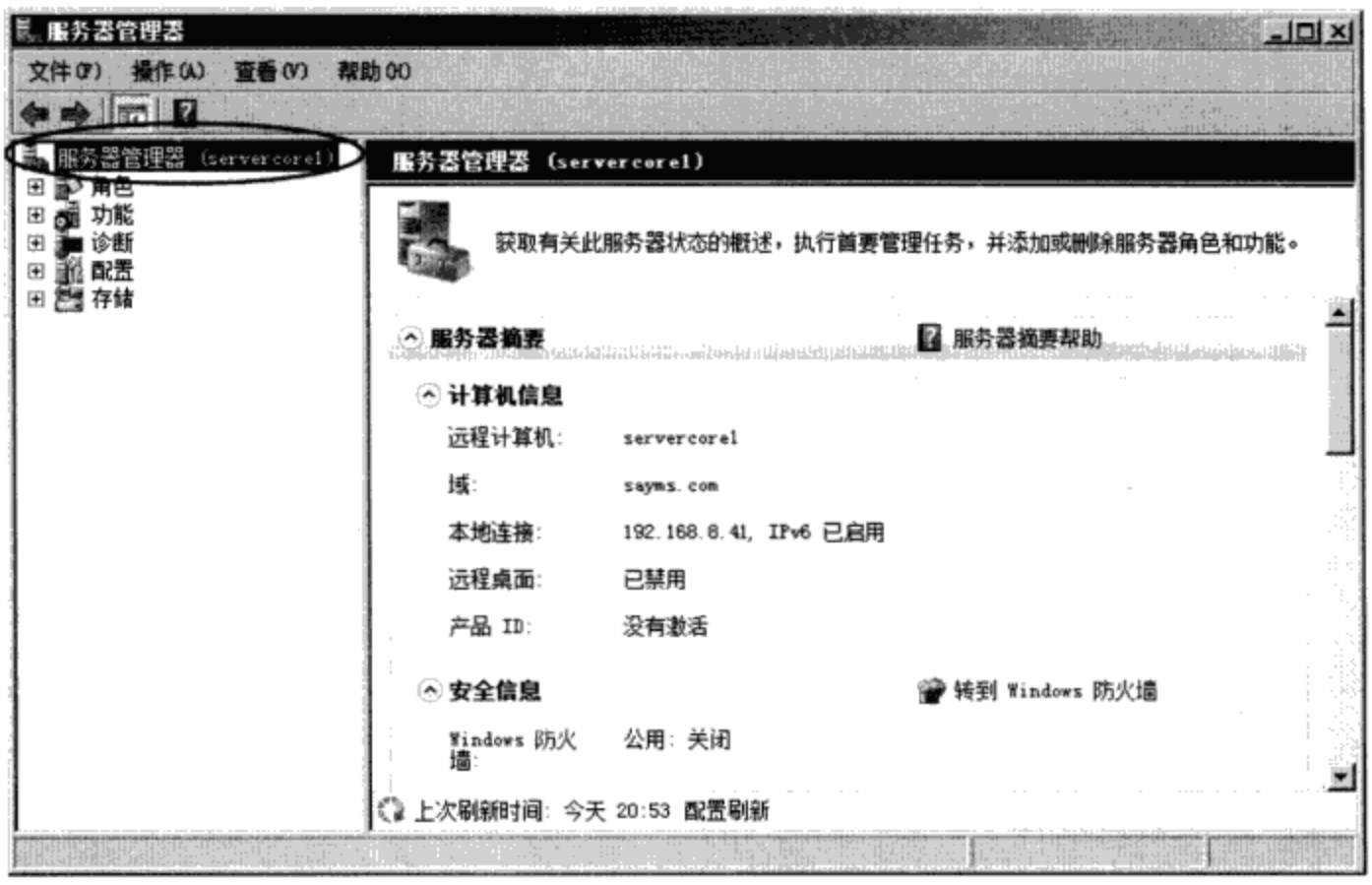


图 B-32

（2）源计算机非域成员

若源计算机为非域成员的话，则它也可以使用服务器管理器来远程管理**服务器核心安装**，不过您需要在源计算机上通过**winrm**命令来将**服务器核心安装**加入到**TrustedHost**列表内，例如若**服务器核心安装**的计算机名为ServerCore4.sayms.com，则请在源计算机上运行以下命令（参见图 B-33）：

```
winrm set winrm/config/client @{TrustedHosts="ServerCore4.sayms.com"}
```

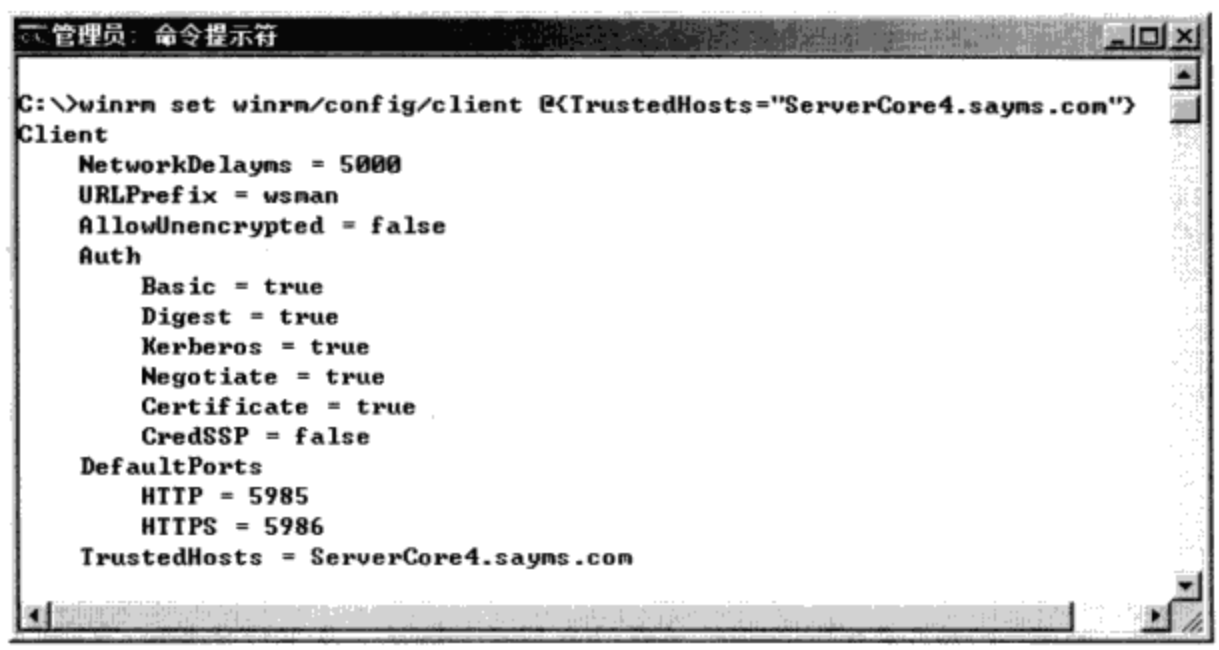
提示

若要查看**TrustedHost**列表的话，请运行以下命令：

```
winrm  get  winrm/config/client
```

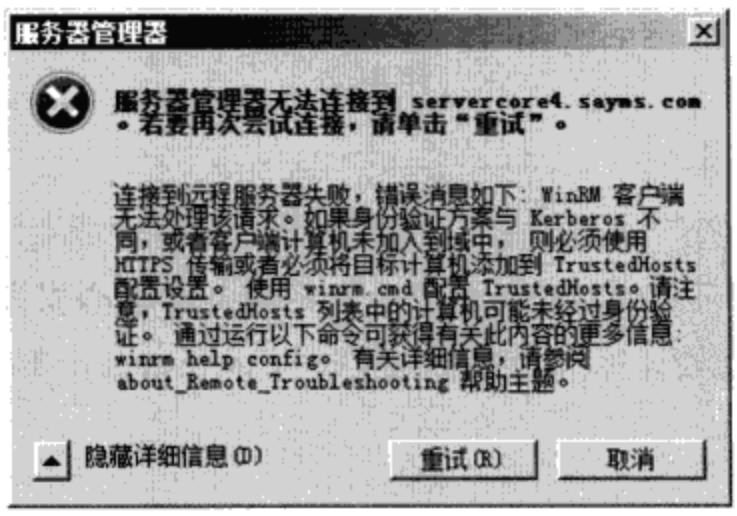
您可以同时将多台计算机加入到**TrustedHost**列表内，不过计算机名称之间要用逗号（,）隔开。若要删除**TrustedHost**列表的话，可运行以下命令：

```
winrm  set  winrm/config/client @{TrustedHosts=""}
```



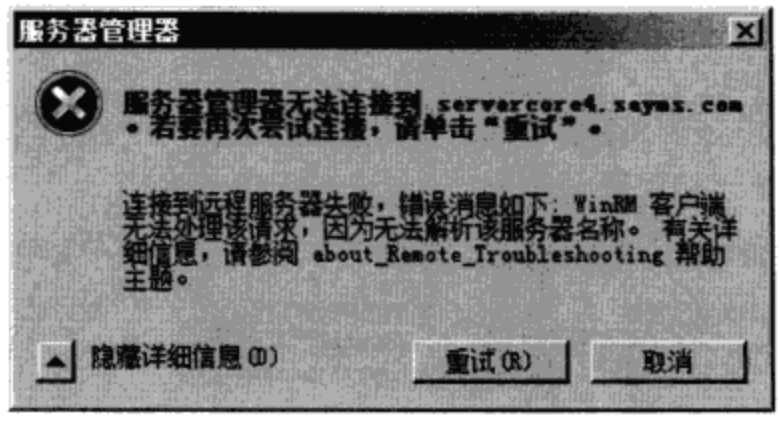
图B-33

若未将**服务器核心安装**加入到源计算机的**TrustedHost**列表内的话，则在源计算机上使用服务器管理器连接**服务器核心安装**时会失败，且会出现如图 B-34所示的警告界面（需单击**查看详细信息**才会显示无法连接的详细原因）。



图B-34

您还需要确认源计算机可以解析到**服务器核心安装**计算机名（Server4.sayms.com）的IP地址，否则在源计算机上使用服务器管理器连接**服务器核心安装**时会失败，且会出现如图 B-35所示的警告界面。



图B-35

您可以通过DNS服务器或源计算机的Hosts文件来解析**服务器核心安装**计算机名（Server4.sayms.com）的IP地址。

若您在源计算机上是通过IP地址来连接**服务器核心安装**的话，则请确认源计算机可以通过IP地址来反向解析到其计算机名，否则连接**服务器核心安装**时会失败，而且也会出现如图B-35所示的警告界面。

您还需要在源计算机上通过以下命令来指定用来连接**服务器核心安装**的用户账户，再通过**服务器管理器**来连接与管理**服务器核心安装**。以下假设要连接的**服务器核心安装**的计算机名为ServerCore4.sayms.com、要被用来连接的账户为Administrator（其他用户账户也可以，但必须隶属于**服务器核心安装**的本地Administrators组）、其密码为111aaAA：

```
Cmdkey /add:ServerCore4.sayms.com /user:Administerator /pass:111aaAA
```

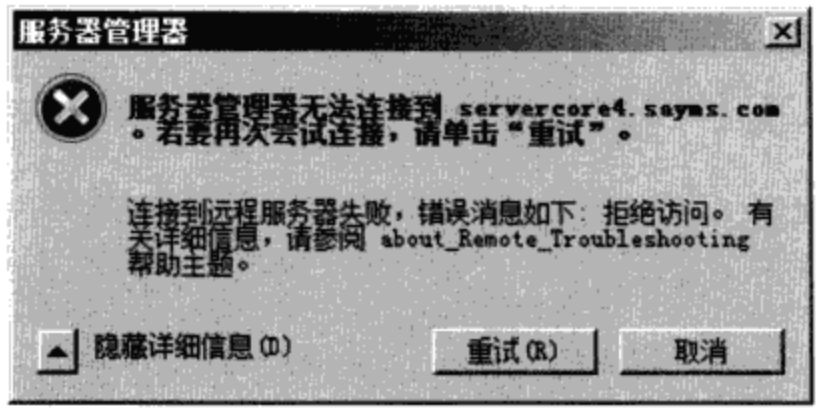
若担心输入密码时被其他人看到的话，请运行以下命令：

```
Cmdkey /add:ServerCore4.sayms.com /user:Administerator /pass
```

之后根据界面上的要求来输入密码，此时密码不会显示在屏幕上。

> 提示
>
> 您也可在源计算机上使用【开始➲控制面板➲单击**用户账户**（或**用户账户和家庭安全**）➲单击**管理Windows凭据**➲单击**添加Windows凭据**】的方法来指定用来连接**服务器核心安装**的用户账户与密码】。

若未通过上述步骤指定用户账户的话，则在源计算机上使用**服务器管理器**连接**服务器核心安装**时可能会失败，且会出现如图 B-36所示的警告界面。



图B-36

提示

若未通过上述步骤指定用户账户的话，则您登录源计算机的用户账户时，会被自动用来连接**服务器核心安装**，若**服务器核心安装**上也有相同名称与密码的本地用户账户且此账户隶属于Administrators组的话，则将自动使用此用户账户来连接与管理**服务器核心安装**。

3. 在 Windows 7 上通过服务器管理器来远程管理

若要在Windows 7计算机上通过服务器管理器来远程管理**服务器核心安装**的话，请先到微软网站下载与安装Remote Server Administration Tools for Windows 7，安装完成后选择【开始➲控制面板➲单击**程序**选项➲单击最上方的**打开或关闭Windows功能**➲展开**远程服务器管理工具**➲选择**服务器管理器**➲单击确定按钮】，之后便可通过【开始➲管理工具➲服务器管理器】的方法来远程管理**服务器核心安装**。

提示

若**管理工具**没有显示在**开始**菜单中的话，可通过【对着屏幕左下角的**开始**图形右击➲属性➲单击**「开始」菜单**右边的自定义按钮➲选择**系统管理工具**中的**在「所有程序」菜单和「开始」菜单上显示**】的方法进行操作。

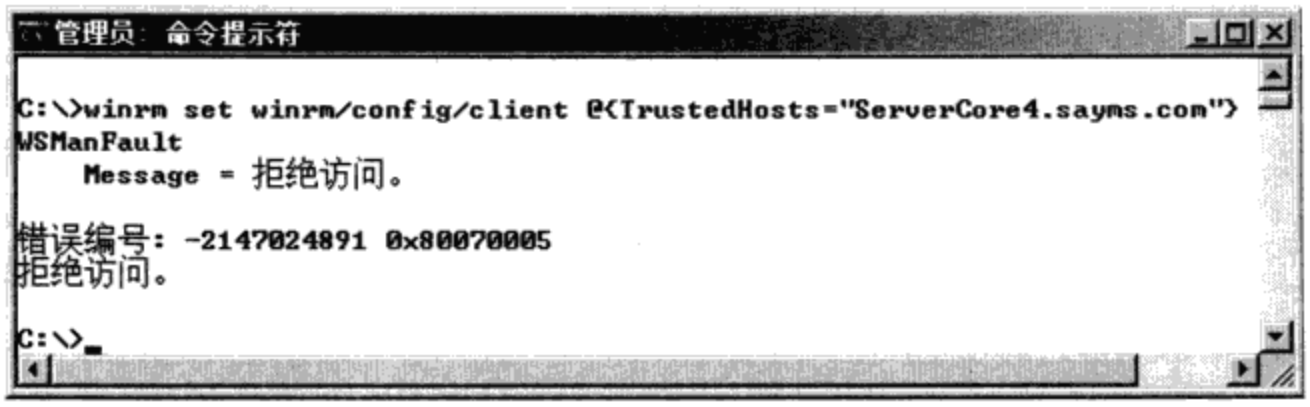
若此台Windows 7计算机未加入域的话，则同样需要通过**winrm**命令来将**服务器核心安装**加入到**TrustedHost**列表内，不过需要先运行**net start winrm**命令来启动Windows Remote Management服务。

您必须以系统管理员的身份来运行**net start winrm**命令，并将**服务器核心安装**加入到**TrustedHost**列表内。若您现在不是使用Administrator身份登录的话：

- 请注销并改用Administrator身份来登录，打开**命令提示符**窗口，执行上述两个操作，不过此账户默认被禁用，因此必须先启用。
- 可以不需注销，直接通过【开始➲所有程序➲附件➲对着**命令提示符**右击➲以管理员身份运行】的方式打开**命令提示符**窗口，然后执行上述两个操作。

注意

若系统管理员Administrator的密码是空的话，则运行将**服务器核心安装**加入到**TrustedHost**列表的工作时会失败，且会显示如图 B-37所示的**访问被拒绝**的提示信息。



图B-37

B-5-5 通过Windows Remote Shell来管理**服务器核心安装**

假设源计算机与**服务器核心安装**都是域的成员，首先需要在**服务器核心安装**计算机上运行以下命令来启用Windows Remote Shell：

```
winRM quickconfig
```

接下来到源计算机打开**命令提示符**窗口，然后使用**winrs.exe**命令来运行**服务器核心安装**内的命令，例如若要查看**服务器核心安装**的C:\Windows文件夹内的文件列表的话，请运行以下的命令：

```
Winrs -r:ServerCore1 dir C:\Windows
```

其中假设**服务器核心安装**的计算机名为ServerCore1。若源计算机为非域成员的话，则需要在源计算机上通过**winrm**命令将**服务器核心安装**加入到**TrustedHost**列表内，且需确认源计算机可以解析到**服务器核心安装**的IP地址。若源计算机是Windows 7的话，还需要先使用**net start winrm**命令来启动Windows Remote Management服务，再来执行将**服务器核心安装**加入到**TrustedHost**列表的工作。

B-5-6 安装硬件设备

如果所安装的硬件设备的驱动程序内含在Windows Server 2008 R2中的话，则将此硬件设备连接到计算机时，系统的即插即用（PnP）功能就会自动安装此驱动程序。

如果您所安装的硬件设备的驱动程序并没有内含在Windows Server 2008 R2中的话，而是需要另外提供的话，则请通过以下步骤来安装：

STEP 1 将驱动程序文件复制到**服务器核心安装**的一个临时文件夹内。

STEP 2 使用**cd**命令切换到此文件夹，然后运行以下的命令，其中的**驱动程序的inf文件**是扩展名为.inf的文件。

```
pnputil -i -a  <驱动程序的inf文件>
```

STEP 3 重新启动计算机。

您可以使用以下命令来查看**服务器核心安装**内已经安装的驱动程序：

```
sc query type= driver
```

注意**type=**与**driver**之间需要空一个空格。若要禁用某个服务的话，请通过以下的命令：

```
sc delete <服务名称>
```

此**<服务名称>**可通过前面的查询命令来获得。

B-5-7 其他注意事项

在源计算机中通过以下MMC管理控制台来管理**服务器核心安装**时，还必须额外做一些设置。

- **设备管理器**MMC管理控制台：您必须启用**服务器核心安装**的**允许远程访问即插即用接口**策略：在另一台Windows Server 2008 R2、Windows Server 2008、Windows 7或Windows Vista计算机上自定义**组策略对象编辑器**控制台，连接到**服务器核心安装**计算机，启用位于**计算机配置\策略\管理模板\系统\设备安装**的**允许远程访问即插即用接口**策略，最后重新启动计算机。若在源计算机中通过**设备管理器**MMC管理控制台来管理**服务器核心安装**的话，则它仅提供只读功能。
- **IP安全监视器**MMC管理控制台：您需要在**服务器核心安装**上运行以下命令来允许远程管理：

```
cscript C:\Windows\system32\scregedit.wsf /im 1
```

- **性能监视器**MMC管理控制台：不需要额外的设置，不过仅能监视性能数据，无法监视可靠性数据。

B-6 常用命令列表

本节将常规工作的管理命令按照分类给出列表，您可以通过这些命令在本地或远程管理**服务器核心安装**。

B-6-1 设置与安装命令

工作	命令
设置本地系统管理员的密码	net user administrator *
将计算机加入域	netdom join %computername% /domain:<域> /userD:<域\用户名> /passwordD:* 完成后重新启动计算机，并使用**set**命令来查看
将计算机脱离域	netdom remove %computername% /domain:<域> /userD:<域\用户名> /passwordD:* 完成后重新启动计算机，并使用**set**命令来查看
将用户加入本地Administrators组	net localgroup Administrators /add <域>\<用户名>
将用户从本地Administrators组删除	net localgroup Administrators /delete <域\用户名>
在本地计算机内添加用户账户	net user <用户名> /add *
在本地计算机内添加组账户	net localgroup <组名> /add
更改域成员计算机的计算机名	netdom renamecomputer %computername% /NewName:<新计算机名> /userD:<域\用户名> /passwordD:*
更改工作组计算机的计算机名	netdom renamecomputer %computername% /NewName:< 新计算机名>
禁用页面文件的管理	wmic computersystem where name="<计算机名>" set AutomaticManagedPagefile=False
设置页面文件	wmic pagefileset where name="<path/filename>" set InitialSize=<initialsize>,MaximumSize=<maxsize>
设置静态IP地址	①使用**ipconfig /all**查看相关信息 ②使用**netsh interface ipv4 show interfaces**查看idx代号 ③运行**netsh interface ipv4 set address name <idx代号> source=static address=<IP地址> gateway= <默认网关的IP地址>** ④使用**ipconfig /all**查看结果
设置静态DNS服务器的IP地址	netsh interface ipv4 add dnsserver name=<idx代号> address=<DNS服务器的IP地址> index=1 若要设置多台DNS服务器的话，请重复上述命令，但需依序增加index数值，例如**index=2**
将IP地址改为动态获取	netsh interface ipv4 set address name=<idx代号> source=dhcp
启用本地服务器	①slmgr.vbs –ato ②通过**slmgr –dli**来查看启用状态
启用远程服务器	cscript slmgr.vbs -ato <计算机名> <用户名> <密码>

B-6-2 网络与防火墙命令

工作	命令
让服务器使用代理服务器来连接Internet	netsh winhttp set proxy <服务器名>:<端口号> 无法通过需要输入密码的代理服务器来连接Internet
让服务器不要通过代理服务器来连接Internet	netsh winttp set proxy <服务器名>:<端口号> bypass-list="<local>"
查看或修改IPSEC设置	netsh ipsec
查看或修改NAP设置	netsh nap
查看或修改IP到物理地址的转换信息	arp
查看或设置路由表	route
查看或设置DNS服务器的设置	nslookup
查看协议统计信息与当前的TCP/IP网络连接状态	netstat
查看协议统计信息与当前的TCP/IP over NetBIOS的网络连接状态	nbtstat
查看网络连接跃点（hops）	pathping
追踪网络连接跃点	tracert
查看多点路由器的设置	mrinfo
启用通过远程来管理防火墙设置	netsh advfirewall firewall set rule group="Windows 防火墙远程管理"new enable=yes （其中**Windows**与**防火墙远程管理**之间有一个空格）

B-6-3 更新、错误报告与回应

工作	命令
安装更新程序	wusa <update>.msu /quiet
列出已安装的更新程序	运行systeminfo，然后通过hotfix字段来查看
删除更新程序	运行**expand /f:* <update>.msu c:\test** 使用记事本打开**c:\test\<update>.xml**文件，将install文字替换成remove并保存，运行**pkgmgr /n:<update>.xml**
设置自动更新	查看当前的设置：cscript scregedit.wsf /AU /v 启用自动更新：cscript scregedit.wsf /AU /4 停用自动更新：cscript scregedit.wsf /AU /1

（续表）

工作	命令
启用错误报告	查看当前的设置：serverWerOptin /query 自动传送详细的报告：serverWerOptin /detailed 自动传送摘要报告：serverWerOptin /summary 禁用错误报告：serverWerOptin /disable
参与客户经验改进计划（CEIP）	查看当前的设置：serverCEIPOptin /query 启用CEIP：serverCEIPOptin /enable 禁用CEIP：serverCEIPOptin /disable

B-6-4 服务、程序与性能

任务	命令
列出运行中的服务	sc query net start
启动一个服务	sc start <服务名称> net start <服务名称> 其中的<服务名称>可使用前面的sc query命令来查看
停止一个服务	sc stop <服务名称> net stop <服务名称>
列出运行中的应用程序与其相关信息	tasklist
强迫中止一个程序	先运行tasklist命令来取得程序标识符（PID），然后运行taskkill /PID <PID>
启动任务管理器	taskmgr
管理性能计数器与记录	Typeperf、logman、relog与tracerpt等

B-6-5 事件日志

任务	命令
列出事件日志文件	wevtutil el
查询指定日志文件中的事件	wevtutil qe /f:text <日志名称>
将事件日志文件导出	wevtutil epl <日志名称>
删除事件日志文件	wevtutil cl <日志名称>

B-6-6 磁盘与文件系统

任务	命令
管理磁盘分区	请使用**diskpart /?**来查看使用语法
管理软件RAID	请使用**diskraid /?**来查看使用语法
管理磁盘分区划分点	请使用**mountvol /?**来查看使用语法
重组一个磁盘分区	请使用**defrag /?**来查看使用语法
将磁盘分区转换成NTFS文件系统	convert <磁盘区代号> /FS:NTFS
压缩一个文件	请使用**compact /?**来查看使用语法
管理打开的文件	请使用**openfiles /?**来查看使用语法
管理VSS文件夹	请使用**vssadmin /?**来查看使用语法
管理文件系统	请使用**fsutil /?**来查看使用语法
验证文件的签署	请使用**sigverif /?**来查看使用语法
夺取文件或文件夹的拥有权	请使用**icacls /?**来查看使用语法

B-6-7 硬件设备驱动器

任务	命令
为新硬件设备安装驱动程序	将驱动程序文件复制到任何一个临时的文件夹内，使用**cd**命令切换到此文件夹，然后运行以下的命令： **pnputil –i –a** <驱动程序的inf文件> 其中的**<驱动程序的inf文件>**是扩展名为**.inf**的文件
删除硬件设备的驱动程序	使用**sc query type= driver**命令来查询驱动程序名称，运行**sc delete <驱动程序名称>**