高级技术培训教材系列

计划、实现和维护 Windows Server 2003 活动目录结构

北京希望电子出版社　总策划
韩立刚　杨洪振　编　写

红旗出版社

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

高级技术培训教材系列

计划、实现和维护 Windows Server 2003 活动目录结构

北京希望电子出版社　总策划
韩立刚　杨洪振　编　写

红旗出版社

北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

图书在版编目（CIP）数据

计划、实现和维护 Windows Server 2003 活动目录结构 /
韩立刚，杨洪振编著. —北京：红旗出版社，2005.2
（高级技术培训系列教材）
ISBN 7-5051-1092-6

Ⅰ. 计… Ⅱ. ①韩… ②杨… Ⅲ. 服务器—操作系统
（软件），Windows Server 2003—技术培训—教材
Ⅳ. TP316.86

中国版本图书馆 CIP 数据核字（2004）第 118620 号

内 容 简 介

本书是 Windows Server 2003 培训教材之一。

全书共分为 12 章，内容包括：Windows Server 2003 活动目录，实现活动目录林和域结构，实现组织单元结构以及管理，实现用户组和计算机帐号，实现组策略，利用组策略管理用户环境，使用组策略部署和管理软件，使用站点管理活动目录复制，实现域控制器的规划，管理操作主控，维护活动目录数据库，实现活动目录基础结构。每章都提供典型模拟试题的分析用来强化相应章节知识点。

书中包含真实的背景资料，图文并茂，实践操作性强，并在课程中加入了众多的案例分析，给读者提供一个真实的场景实践。

本书内容新颖全面，是系统全面学习 Windows Server 2003 的网管人员、技术爱好者的很好的辅助教材，同时也可以作为参加 Windows Server 2003 系统工程师认证（对应 MCSE 课程号 2279，考试号 70-294）的很好的参考资料。

需要本书或技术支持的读者，请与北京中关村 083 信箱（邮编 100080）发行部联系，电话：010-82702660 010-82702658，010-62978181（总机）转 103 或 238，传真：010-82702698，E-mail：tbd@bhp.com.cn.

系 列 名	高级技术培训系列教材
书 名	计划、实现和维护 Windows Server 2003 活动目录结构
主 编	韩立刚 杨洪振
总 策 划	北京希望电子出版社
责 任 编 辑	安源 雷 铎
出 版	红旗出版社 北京希望电子出版社
发 行	北京希望电子出版社
地 址	红旗出版社 北京市沙滩北街 2 号（100727） 电话：（010）64037138 北京希望电子出版社 北京市海淀区上地三街 9 号金隅嘉华大厦 C 座 610
经 销	各地新华书店 软件连锁店
排 版	希望图书输出中心 娄艳
印 刷	北京市媛明印刷厂
版次 / 印次	2005 年 2 月第 1 版 2005 年 2 月第 1 次印刷
开本 / 印张	787 毫米×1092 毫米 1/16 22.875 印张
字 数	525 千字
印 数	1～5000 册
书 号	ISBN 7-5051-1092-6
定 价	38.00 元

总 序

“Windows 团队有 5000 个成员，加上额外的 5000 个合作伙伴，于是生产了超过 5000 万行的 Windows Server 2003 代码。所有人员遵从统一的领导制造代码，生成他们的工作结果，编译并连接为可执行程序或其他组件，最后组成一个 Windows 的 CD。这个过程持续 12 到 13 小时，每一天都在进行，这是曾经尝试过的最大的软件工程任务，没有其他软件项目可与之相比”。

——Mark Lucovsky（Windows Server 的设计师）

从微软公司推出 Windows Server 2003 beta 版本以来，我们就一直对它密切跟踪着。随着产品的发布，人们对它的兴趣也越来越浓。为了让广大读者、技术爱好者能找到一本专业的教材，我们集中了多名对 Windows Server 2003 感兴趣的工程师，他们都是处在微软教学第一线 MCT（Microsoft Certified Trainer）的教员，以及对微软产品有着深厚经验技术的爱好者，这样大家就开始了对 Windows Server 2003 技术的研究学习。针对这套知识体系以及微软公司新推出的面向 Windows Server 2003 的考试，我们策划编写了这一套丛书，希望通过它可以帮助大家对 Windows Server 2003 技术进行全面地了解，并对参加 MOC 考试有所帮助。现在这套教材经过我们的不懈努力，终于与大家见面。

在这套丛书中，每一章的开始都简单介绍章节的主要内容和学习目标，以便读者在学习过程中作为参照。每章都包含部分的案例研究分析，从读者的角度去理解案例，可以大大加深读者的学习效果。结尾处均包含相关 MCSE 考试的模拟试题和答案分析。这些模拟试题能有效地帮助读者在学习具体知识的同时备战 MCSE 考试。

本套丛书注重理论联系实际，所有内容采用图文并茂的形式帮助读者理解，每一张截图都是作者从实际网络环境中精心准备得来。每章都设计了实践操作部分，让读者不仅仅可以学到理论知识，而且能在书中的指导下进行实践操作。丛书是想系统全面学习 Windows Server 2003 的网管人员、技术爱好者很好的辅助教材，其中的典型模拟试题的分析更是希望参加微软 Windows Server 2003 系统工程师认证（MCSE）的很好的参考资料。

丛书中我们介绍了一些使用经验和心得，难免有不当之处，或者还有更好的方法欢迎赐教。如果有需要交流的地方可与作者联系，欢迎与您的真诚交流。

一件作品的完成是众人智慧与努力的结晶，在此特别感谢北京希望电子出版社。感谢编辑栾大成先生的努力工作，他的幽默风趣的言谈，踏实的工作态度让我记忆深刻。没有他用专业的眼光和细节的关注，这一系列的出版不能如此顺利。同时感谢在本书的编写过程中曾给予我帮助的朋友们：我的挚友刘春田、李明清，以及身边的众多给予帮助的朋友，你们带给了我启发和欢笑，愿你们可以完成心中所愿。给予我心灵上支持的杨蓉：带给你祝福，坚持下去，你的愿望一定会实现。谢谢你们的大力支持。

MCT（微软认证讲师）——杨洪振

前 言

Windows Server 2003 是继 Windows 2000 之后微软公司推出的新一代操作系统。本书详细讲解了 Windows servers 2003 最大的基础应用——活动目录的基础知识，创建办法，以及在企业信息化环境中的应用。书中包含真实的背景资料，图文并茂，实践操作性强，并在课程中加入了众多的案例分析，给读者提供一个真实的场景实践。

全书共分 12 章内容，系统地介绍了一个完整活动目录的学习过程。内容以读者的学习需求为主线，详细讲解了活动目录中各种的基本概念，具体的内容包括：关于活动目录中的物理组件；活动目录中的逻辑组件；实现活动目录林和域结构；OU 的实现和管理；活动目录中用户帐号和组的使用；组策略的实现；利用组策略去管理用户的环境，例如用户桌面的配置，实现重定向文件夹等；利用组策略为客户端部署软件，实现管理分发的软件；利用站点实现活动目录复制；由于性能和容错的原因，域中域控制器的安装策略；操作主控的管理，即主控角色的夺取、传递；活动目录数据库的维护管理。而且在最后一章，以案例为主线，对全书的知识进行了总结。

全书结构清晰，内容详尽，通过实例分析和课后练习来帮助学习者理解和掌握所学习的知识、概念和操作技巧。本书内容新颖全面，是系统全面学习 Windows Server 2003 的网管人员、技术爱好者的很好的辅助教材，同时也可以作为参加 Windows Server 2003 系统工程师认证（对应 MCSE 课程号 2279，考试号 70-294）的很好的参考资料。

由于时间仓卒，编写者水平有限，书中介绍的使用经验和心得难免有不当之处，或者还有更好的方法，恳请读者指正。

韩立刚：微软认证讲师（MCT），就职于国内一家著名的 CTEC，担任主讲教师。理论知识扎实，长期从事于微软课程的教学工作，对微软平台的产品有深入研究，从早期的 Windows NT 4，到 Windows 2000，到现在的 Windows server 2003。并且对微软平台其它产品也很熟悉，精通 Exchange server，ISA server。同时参与了多个项目的部署实施，如中国上安电厂的邮件系统部署，迁移方案，河北移动的 Windows 2000 基础平台部署。

杨洪振：资深 MCT（Microsoft Certified Trainer），MCSE，MCDBA MLC 讲师，曾长时间从事系统技术支持，系统集成项目以及讲授相关产品课程等工作。对于 Microsoft 系列产品有深入研究，在基于微软平台的网络系统，服务器应用以及网络安全等方面具有丰富经验，包括 Windows 2000、Exchange Server，ISA Server，SharePoint Portal Server，BizTalk Server，Small Business Server 并是国内第一批使用和研究 Windows Servers 2003，Exchange Server 2003 的技术人员。

作者

出版说明

Windows Server 2003 推出已经有 2 年时间了，但这种有史以来最强大的服务器操作系统却迟迟未能普及，很大的原因是缺乏相应的系统完整的教材和培训。为此，我们特组织优秀的微软认证讲师（MCT）编写了本套 Windows Server 2003 高级技术培训教材，以帮助你快速系统地掌握 Windows Server 2003 的相关技术和技巧，同时本书也可以作为获得微软最新的 MCSE/MCSA 认证的参考资料及自学培训教材。

全套教材共 6 本：

序号	书　名
1	管理 Windows Server 2003 环境
2	维护 Windows Server 2003 环境
3	实现 Windows Server 2003 网络基础结构：网络主机
4	实现和维护网络基础结构：网络服务
5	计划和维护 Windows Server 2003 网络基础结构
6	计划、实现和维护 Windows Server 2003 活动目录结构

本套培训教材都由第一线的微软认证高级技术培训中心讲师（MCT）编写，凝聚了 MCT 们多年实践和教学的经验，教材的每章都有学习重点，在必要章节附有实验供读者练习。另外，本套教材还包括大量的模拟试题，所有模拟试题都加入了试题分析和知识点解析以适应读者在各种环境中的实践能力。力求通过学习本套教材，即可成为一名优秀的 Windows Server 2003 系统管理人员，与此同时你将具备参加 MCSE/MCSA 考试的各种相关知识。

本套教材既可供系统管理员，广大网络技术人员和爱好者学习、参考使用 Windows Server 2003 系统，也可以作为微软认证 MCSE/MCSA 的自学参考教材。

编　者

目 录

第 1 章 Windows Server 2003 活动目录.....1
1.1 活动目录基础结构.....1
1.1.1 活动目录的作用.....1
1.1.2 活动目录逻辑结构.....2
1.1.3 活动目录的物理结构.....3
1.1.4 操作主控.....4
1.2 活动目录的工作方式.....5
1.2.1 目录服务.....5
1.2.2 架构.....6
1.2.3 全局目录.....7
1.2.4 标识符和相对标识符.....8
1.2.5 活动目录如何实现一次登录.....9
1.3 检测活动目录.....12
1.3.1 活动目录管理.....12
1.3.2 活动目录管理插件和工具.....13
1.3.3 实验：检测活动目录.....14
1.3.4 练习：检测活动目录结构.....16
1.4 活动目录设计、计划和实现过程.....16
1.4.1 活动目录设计、计划、实现概述.....17
1.4.2 活动目录设计过程.....17
1.4.3 活动目录计划过程.....18
1.4.4 活动目录实现过程.....18
1.5 模拟试题分析.....19
第 2 章 实现活动目录林和域结构.....21
2.1 创建林和域结构.....21
2.1.1 活动目录的安装要求.....21
2.1.2 安装活动目录.....22
2.1.3 创建林和域结构.....23
2.1.4 添加附加的域控制器.....25
2.1.5 如何重命名域控制器.....26
2.1.6 如何从活动目录中删除域控制器.....27
2.1.7 如何验证活动目录的安装.....28
2.1.8 如何诊断安装过程中的故障.....29
2.1.9 如何将计算机加入到域.....30
2.1.10 练习：创建域结构.....31
2.2 检测 DNS 活动目录集成区.....35
2.2.1 DNS 和活动目录名称空间.....35
2.2.2 活动目录集成区.....36
2.2.3 SRV 记录.....37
2.2.4 由域控制器注册的 SRV 记录.....37
2.2.5 如何检测由域控制器注册的 SRV 记录.....39
2.2.6 客户计算机如何利用 DNS 定位域控制器和服务.....40
2.2.7 练习：检测 SRV 记录.....41
2.3 提升目录林和域的功能级别.....41
2.3.1 林和域的功能级别.....41
2.3.2 启用新增的 Windows Server 2003 特征要求.....44
2.3.3 如何升级功能级别.....44
2.3.4 练习：升级域功能级别.....44
2.4 创建域之间的信任关系.....45
2.4.1 信任的类型.....45
2.4.2 信任域对象.....48
2.4.3 信任关系如何在目录林中工作.....48
2.4.4 信任如何穿越目录林.....49
2.4.5 何时以及如何创建信任.....51
2.4.6 验证和撤销信任.....54
2.4.7 练习 创建信任的快捷方式.....57
2.5 实验：实现活动目录.....58
练习 1 创建目录林中的第一个域.....58
练习 2 在 Test.net 域中创建附加的域控制器.....59
练习 3 创建目录林林中的一个子域.....59
练习 4 提升域和林功能级别.....59
练习 5 创建林信任.....60
2.6 模拟试题分析.....61
第 3 章 实现组织单元结构以及管理.....67
3.1 创建和管理组织单元.....67
3.1.1 介绍管理组织单元.....67
3.1.2 创建和管理组织单元的方法.....68
3.1.3 如何使用活动目录服务工具创建和管理组织单元.....69

3.1.4 如何使用 Ldifde 工具创建和管理组织单元 70
3.1.5 使用 Windows 脚本主机创建组织单元 71
3.1.6 练习：创建组织单元 71
3.2 活动目录中的对象安全性 72
3.2.1 活动目录安全组件 72
3.2.2 随机和系统访问控制列表 73
3.2.3 访问控制项 74
3.2.4 继承（Inheritance） 76
3.2.5 登录进程 76
3.2.6 访问令牌 77
3.2.7 Windows Server 2003 如何授权对资源的访问 78
3.3 活动目录对象的访问控制 79
3.3.1 活动目录权限 79
3.3.2 权限继承控制 81
3.3.3 设置活动目录权限 82
3.3.4 对象所有权 83
3.3.5 改变对象所有权 83
3.4 委派对组织单元的管理控制 84
3.4.1 什么是委派管理控制 84
3.4.2 组织单元的管理任务 85
3.4.3 如何委派管理控制 85
3.4.4 如何验证委派权限 87
3.4.5 练习：为组织单元委派管理控制 89
3.5 设计组织单元的策略 89
3.5.1 组织单元设计过程 90
3.5.2 影响组织单元结构的部门组织因素 90
3.5.3 组织单元结构设计指南 91
3.5.4 委派管理控制指导方针 92
3.5.5 练习：设计组织单元结构 93
3.6 试验：设计组织单元结构 95
练习 1 创建组织单元 95
练习 2 委派管理控制 95
练习 3 验证委派控制 96
3.7 模拟试题分析 96
第 4 章 实现用户组和计算机账号 99
4.1 账号 99
4.1.1 账号的类型 99
4.1.2 组的类型 100
4.1.3 什么是域本地组 102
4.1.4 全局组 103
4.1.5 通用组 104
4.2 创建和管理多用户账号 105
4.2.1 创建和管理多用户账号的工具 105
4.2.2 使用 Csvde 工具创建用户账号 106
4.2.3 使用 Ldifde 工具创建和管理用户账号 107
4.2.4 使用 Windows 脚本主机创建和管理用户账号 108
4.2.5 练习：创建用户账号 109
4.3 实现用户登录主名后缀 110
4.3.1 用户主名 110
4.3.2 用主名登录身份验证过程 112
4.3.3 用户登录主名如何在网络上路由 112
4.3.4 名称后缀冲突如何检测以及如何解决 114
4.3.5 创建和删除一个 UPN 后缀 115
4.3.6 如何启用和禁用名称后缀在林信任环境中路由 116
4.3.7 练习：创建 UPN 后缀 117
4.4 在活动目录中移动对象 118
4.4.1 SID 历史 118
4.4.2 移动对象的实质 118
4.4.3 在域内移动对象 119
4.4.4 在域之间移动对象 120
4.4.5 使用 LDP 查看被移动对象属性 122
4.4.6 练习：移动对象 124
4.5 设计用户，组和计算机账号策略 124

4.5.1 命名用户账号的方针 125
4.5.2 设置密码策略的方针 125
4.5.3 身份验证，授权和管理账号的方针 127
4.5.4 使用组的方针 128
4.5.5 练习：设计一个账号策略 129
4.6 设计活动目录审核策略 130
4.6.1 为什么需要审核对活动目录的访问 130
4.6.2 监视活动目录更改的指导方针 131
4.7 实验：实现一个账号和审核策略 131
练习 1 设计一个账号和审核策略 132
练习 2 使用 csvde 工具创建用户账号 132
练习 3 创建一个 UPN 后缀 133
练习 4 移动一个用户组 133
4.8 模拟试题分析 133
第 5 单元 实现组策略 136
5.1 组策略介绍 136
5.2 组策略结构 137
5.2.1 组策略设置的类型 137
5.2.2 组策略对象 138
5.2.3 计算机和用户的组策略设置 139
5.2.4 组策略对象和活动目录容器 140
5.3 处理组策略对象 140
5.3.1 创建已连接的组策略对象 141
5.3.2 创建未连接的组策略对象 142
5.3.3 连接一个已存在的组策略对象 142
5.3.4 指定管理组策略对象的域控制器 144
5.4 组策略设置如何应用于活动目录中 145
5.4.1 组策略继承性 145
5.4.2 如何处理组策略 146
5.4.3 控制组策略的处理 147
5.4.4 组策略和慢速网络连接 149
5.4.5 组策略中的回送处理模式设置 150
5.4.6 解决组策略之间的冲突 151
5.5 修改组策略的继承性 152
5.5.1 启用阻止继承 152
5.5.2 启用 No Override“禁止替代” 153
5.5.3 筛选组策略设置 154
5.5.4 Windows 管理规范（WMI）过滤器 155
5.5.5 使用 WMI 过滤器过滤组策略 156
5.5.6 练习：更改组策略继承 157
5.6 实验 A：实现组策略 158
练习 1 创建和连接组策略对象 158
练习 2 检验组策略设置 158
练习 3 阻止组策略继承 159
练习 4 强制执行组策略继承 159
练习 5 筛选组策略 159
5.7 管理组策略 160
5.7.1 拷贝 161
5.7.2 拷贝 GPO 161
5.7.3 备份 163
5.7.4 备份一个 GPO 164
5.7.5 还原 165
5.7.6 还原 GPO 165
5.7.7 导入 166
5.7.8 将设置导入 GPO 166
5.7.9 练习：管理组策略 167
5.8 监控和组策略冲突问题解决 168
5.8.1 实现组策略时常见问题 168
5.8.2 使用组策略模拟向导确认组策略设置 169
5.8.3 使用组策略结果验证组策略设置 172
5.8.4 练习：监控和组策略冲突问题解决 174
5.9 委派组策略的管理控制 174
5.9.1 委派组策略的管理控制 175
5.9.2 为站点、域或组织单元委派组策略控制 176
5.9.3 委派 WMI 过滤器的管理控制 178

5.10 实验 B:委派组策略管理.....179
练习 1 委派组策略管理.....180
5.11 实现组策略注意事项.....180
5.12 模拟试题分析.....181
第 6 章 利用组策略管理用户环境.....186
6.1 管理用户环境.....186
6.2 管理模板介绍.....187
6.2.1 管理模板.....187
6.2.2 计算机如何应用管理模板设置.....188
6.3 使用组策略中的管理模板.....189
6.3.1 管理模板设置的类型.....189
6.3.2 锁定桌面设置.....190
6.3.3 锁定用户访问网络资源的设置.....191
6.3.4 锁定用户访问管理工具和应用程序的设置.....192
6.3.5 执行管理模板.....193
6.3.6 练习：利用管理模板分配基于注册表的组策略.....194
6.4 用组策略分配脚本（Script）.....198
6.4.1 组策略脚本设置.....199
6.4.2 用组策略实现脚本设置的过程.....199
6.4.3 分配组策略脚本设置.....200
6.4.4 练习：利用组策略把脚本分配给用户和计算机.....200
6.5 利用组策略重定向文件夹.....201
6.5.1 文件夹重定向.....202
6.5.2 选择重定向的文件夹.....202
6.5.3 把文件夹重定向到服务器位置上..203
6.5.4 练习：把文件夹重定向到服务器位置上.....204
6.6 利用组策略确保用户环境安全.....206
6.6.1 账户策略.....206
6.6.2 账户锁定策略.....208
6.6.3 Kerberos 策略.....208
6.6.4 本地策略.....209
6.6.5 受限制的组.....213
6.6.6 利用组策略实现安全设置.....214
6.6.7 练习：利用组策略实现安全设置..215
6.7 解决用户环境管理过程中出现的问题...216
6.8 管理用户环境经验总结.....217
6.9 案例分析.....218
第 7 章 使用组策略部署和管理软件.....220
7.1 介绍软件部署.....220
7.1.1 软件安装和维护过程.....220
7.1.2 Windows 安装程序.....221
7.2 部署软件.....222
7.2.1 软件部署概述.....222
7.2.2 创建软件分发点.....222
7.2.3 分配软件.....223
7.2.4 发布软件.....223
7.2.5 使用组策略部署软件包.....224
7.2.6 设置软件安装默认值.....226
7.3 配置软件部署.....227
7.3.1 使用软件修改.....227
7.3.2 创建软件类别.....229
7.3.3 关联文件扩展名和应用程序.....230
7.4 维护已部署的软件.....231
7.4.1 升级部署的软件.....231
7.4.2 重新部署软件.....232
7.5 删除已部署的软件.....233
7.6 实验：升级和删除软件.....233
练习 1 部署应用程序升级.....234
练习 2 测试应用程序升级.....234
练习 3 删除部署的软件.....234
7.7 软件部署的常见问题.....234
7.7.1 使用组策略部署软件常见的问题.....234
7.7.2 判断产生问题的原因.....235
7.8 软件部署经验.....237
7.9 模拟试题分析.....237
第 8 章 使用站点管理活动目录复制.....239
8.1 活动目录复制介绍.....239

8.1.1 站点内复制 240
8.1.2 解决复制冲突问题 241
8.1.3 目录分区 244
8.1.4 复制拓扑（Replication Topology） 245
8.1.5 自动复制拓扑的产生 246
8.1.6 使用连接对象（Connection Objects） 247
8.1.7 全局目录服务器和复制分区 248
8.1.8 练习：检测活动目录复制 249
8.2 实验 A：跟踪活动目录复制 250
练习 1 检查多主控复制的数据冲突 250
8.3 利用站点优化活动目录复制 254
8.3.1 站点（Sites）和子网对象 254
8.3.2 站点连接 255
8.3.3 复制协议 256
8.3.4 站点内复制和站点间复制 257
8.3.5 创建和配置站点和子网 258
8.3.6 建立和配置站点连接 260
8.3.7 建立站点连接桥 261
8.4 管理站点拓扑 263
8.4.1 桥头服务器 264
8.4.2 站点间拓扑生成器 264
8.4.3 指定桥头服务器 265
8.4.4 刷新复制拓扑 265
8.4.5 通过站点间连接强制复制 266
8.5 实验 B：利用站点管理活动目录复制 266
练习 1 建立 IP 子网和站点对象 267
练习 2 配置站点连接和站点连接桥 267
8.6 监控复制通信 268
8.6.1 常见的复制问题 268
8.6.2 复制监控器 269
8.6.3 配置复制监控器 269
8.6.4 Repadmin 工具 272
8.6.5 DCdiag 工具 273
8.6.6 确定产生问题的原因 273
8.6.7 解决复制问题 274
8.6.8 练习：诊断复制失败 275
8.7 模拟试题分析 275
第 9 单元 实现域控制器的规划 281
9.1 布置全局目录服务器 281
9.1.1 全局目录概述 281
9.1.2 创建全局目录服务器 283
9.1.3 何时自定义全局目录服务器 283
9.1.4 如何自定义全局目录服务器存储哪些属性 283
9.1.5 通用组成员资格缓存 285
9.1.6 为一个站点启用通用组的成员资格缓存 285
9.1.7 练习：在活动目录中实现全局目录服务器 286
9.2 确定活动目录中域控制器的部署 286
9.2.1 域控制器容量规划的概述 286
9.2.2 活动目录容量规划的使用参数 287
9.2.3 收集设计信息 288
9.2.4 判断所需的域控制器数目 289
9.2.5 判断磁盘空间需求 290
9.2.6 判断最少的磁盘空间需求 290
9.2.7 判断内存需求 292
9.2.8 如何使用活动目录规划程序 292
9.3 设计活动目录中域控制器的规划 295
9.3.1 规划域控制器 295
9.3.2 规划全局目录服务器建议 296
9.3.3 启用通用组成员资格缓存建议 296
9.3.4 部署于活动目录集成的 DNS 服务建议 297
9.4 模拟试题分析 297
第 10 单元 管理操作主控 299
10.1 操作主控 299
10.1.1 架构主控 300
10.1.2 域命名主控 300
10.1.3 PDC 仿真器 300

10.1.4 RID 主控 301
10.1.5 基础结构主控 302
10.1.6 操作主控默认位置 303
10.2 传送和争夺操作主控角色 304
10.2.1 确定操作主控角色的保持者 304
10.2.2 传送操作主控角色 305
10.2.3 争夺操作主控角色 309
10.2.4 练习：传送操作主控角色 310
10.3 计划操作主控的部署 310
10.3.1 部署操作主控的建议 311
10.3.2 部署架构操作主控的建议 311
10.3.3 部署域命名主控的建议 312
10.3.4 部署 PDC 仿真器指导方针 312
10.3.5 部署 RID 主控的指导方针 313
10.3.6 部署基础结构主控的指导方针 313
10.3.7 争夺操作主控角色的指导方针 313
10.4 实验：管理操作主控 315
练习 1 确定操作主控 315
练习 2 传送基础结构主控角色 315
练习 3 争夺 PDC 仿真器角色 316
练习 4 使用 ntdsutil 传送操作主控角色 316
10.5 模拟试题分析 317
第 11 单元 维护活动目录数据库 319
11.1 维护活动目录数据库介绍 319
11.1.1 活动目录中的文件以及活动目录更改过程 320
11.1.2 垃圾收集处理 321
11.2 移动活动目录数据库和整理活动目录数据库碎片 321
11.2.1 移动活动目录数据库和日志文件 322
11.2.2 活动目录数据库碎片整理 323
11.2.3 练习：移动和碎片整理活动目录数据库 324
11.3 备份活动目录 326
11.3.1 系统状态数据的组件 326
11.3.2 备份系统状态数据 326
11.4 恢复活动目录 328
11.4.1 活动目录恢复的方法 328
11.4.2 执行原始恢复 329
11.4.3 执行正常恢复 330
11.4.4 执行授权恢复 331
11.5 实验：维护活动目录 332
练习 1 备份活动目录 332
练习 2 恢复活动目录 333
11.6 模拟试题分析 333
第 12 单元 实现活动目录基础结构 336
12.1 商业场景 336
12.2 活动目录基础结构的要求 337
12.3 实现活动目录基础结构 338
12.3.1 安装和配置 DNS 338
12.3.2 安装活动目录 339
12.3.3 创建站点和站点连接 340
12.3.4 设置打印机位置 341
12.3.5 建立 OU 结构和委派管理控制 342
12.3.6 建立用户和组 343
12.3.7 实现组策略 345
12.4 实验：实现活动目录基础结构 346
练习 1 计划实现活动目录基础结构的方案 347
练习 2 安装并配置 DNS 348
练习 3 安装活动目录 349
练习 4 建立站点和站点连接 349
练习 5 发布打印机和利用打印机位置 ...350
练习 6 建立 OU 结构和委派管理控制 ...350
练习 7 建立用户和组 351
练习 8 实现组策略 351
练习 9 验证实现 352

第 1 章　Windows Server 2003 活动目录

- 活动目录基础结构
- 活动目录如何工作
- 检测活动目录
- 活动目录设计、计划和实现过程
- 模拟试题分析

本章介绍活动目录目录服务的逻辑结构和物理结构以及活动目录的作用。还介绍了插件，命令行工具，用 Windows 脚本主机管理活动目录组件和活动目录设计，计划和实现过程。

学习目标

- 描述活动目录基础结构
- 描述活动目录如何工作
- 使用 MMC 插件检查活动目录组件
- 描述活动目录设计，计划，和实现过程

1.1　活动目录基础结构

- 活动目录的作用
- 活动目录逻辑结构
- 活动目录物理结构
- 操作主控

活动目录存储关于用户，计算机和网络资源并且使网络资源能够被用户和应用程序访问这些资源，它提供规范化的名称、描述、定位、访问、管理方法和保护这些资源信息。

1.1.1　活动目录的作用

活动目录提供下列功能：

- **活动目录功能**　活动目录提供目录服务功能，包括一种集中组织、管理和控制网络资源访问的方法。活动目录使物理网络拓扑和协议透明化，这样网络上的用户可以访问任何资源，而不需要知道资源在什么地方或物理上它是如何连接到网络上的。打印机就是这种类型的资源的一个例子。
- **集中的控制网络资源**　一个运行 Windows 2000 的服务器在活动目录中存储系统配置、用户配置文件和应用程序的信息。与组策略相结合，活动目录可以使管理员使用同样的管理界面在中心位置管理分布式桌面、网络服务和应用程序。通过集中的控制活动目录中的服务器，共享文件夹和打印机等网络资源，只允许授权用户的访问。

- **实现用户一次登录访问整个网络** 用户登录到域后，访问整个网络将不再需要重新输入帐号和密码。
- **集中的委派资源的管理** 管理员能够在一个中心位置使用管理接口管理分散的客户计算机，网络服务器和应用程序，或者通过委派管理控制委派某些资源的管理权限给其他管理员。
- **在逻辑结构中安全的存储对象** 活动目录以安全的，层次化的逻辑结构中存储所有的对象资源。
- **可扩展** 活动目录组织成一个一个的块，每个块可以存储大量对象。因此，活动目录可以扩展，这样，一个只有一台服务器和几百个对象的组织可以扩展成拥有几千台服务器和几百万个对象。
- **优化网络流量** 活动目录的物理结构将使你高效的使用带宽，例如当用户登录到网络，身份验证将使用离用户最近的域控制器，这样将降低网络流量，加快登录过程。

1.1.2 活动目录逻辑结构

活动目录以层次化的逻辑结构安全地存储对象信息。活动目录对象代表用户和资源，比如计算机和打印机，有些对象是其他对象的容器。

活动目录逻辑结构包括下列组件：

- **对象** 逻辑结构中最基本的组件。对象类是你能够在活动目录中创建的各种对象的模板和蓝图。每一种对象类由一组属性定义，这些属性定义了你能为对象赋予的可能的值。每个对象是属性值的唯一组合。
- **组织单元** 出于管理目的，你使用这些容器对象安排其他的对象。通过使用组织单元管理对象，你可以很容易地定位和管理对象。你也可以委派其他用户管理组织单元。组织单元能够嵌套其他的管理单元，这将大大简化对象的管理。
- **域** 域是活动目录中逻辑结构的核心单元。域是一个出于管理而定义的对象的集合，一个域包含许多台计算机，它们由管理员设定，共用一个目录数据库，安全策略，和其他域的信任关系。一个域有一个唯一的名字，给那些由域管理员集中管理的用户账户和组账户提供访问目录。域提供下列 2 个功能：
  - 对象的管理边界：在 Windows Server 2003 网络中，域起着安全边界的作用。安全边界的作用就是保证域的管理员只能在该域内有必要的管理权限，除非管理员得到其它域的明确授权。每个域都有自己的安全策略和与其它域的安全关系。
  - 复制单元：域同时也是一个复制单元。在域中，作为域控制器的计算机包含活动目录的副本。在一个特定域中，所有域控制器都能够得到活动目录中的变化信息，并把这些变化复制给该域中的其它控制器。
- **域树** 以层次结构组织在一起的域被称为域树。当你添加第二个域到树，它将成为树根域的子域。子域连接的域成为父域。子域可以有自己的子域。子域的名称连接父域的名组成自己的唯一的 DNS 名称。例如 corp.nwtraders.msft.一个树有相同的名称空间。
- **林** 林是活动目录的完全的实例。它包含一个或多个域树，目录林是一个或几个域目

录树。目录林中的域目录树并不共用连续的名字空间。然而，目录林中的域目录树共用共同的架构和全局目录。一个不与其它域目录树相联系的单一目录树形成只有一个域目录树的目录林。这样，每个域目录树的根域与目录林根域之间存在着传递信任关系。目录林根域的名字用来指向一个给定的目录林。

目录林中的每个域目录树都有它自己的唯一的名字空间。比如，Contoso,Ltd 创建一个称为 Northwind Traders 的独立组织。Contoso,Ltd 决定为该组织 Northwind Traders 建立一个新的活动目录域名，称为 nwtraders.msft。尽管这两个组织并不共用同样的名字空间，但是在现存的目录林中可以添加一个作为新域目录树的新的活动目录域，这就使这两个组织可以共用资源和管理功能。整个目录林将是活动目录实例包含的信息的安全边界。

1.1.3 活动目录的物理结构

在一个域中添加多个域控制器，这样如果一个出现故障后，该域中的其他域控制器可以提供容错。要实现容错，域控制器间要活动目录需要复制。如果一个域跨越了多个局域网，局域网之间用满速的广域网链路连接，控制活动目录的复制时间段，以避免和用户的数据流争用带宽。因为域中有多个域控制器，用户登录身份验证使用和自己在同一个局域网中的域控制器，登录速度将大大加快。

活动目录逻辑结构是用来管理和和组织资源的。于逻辑结构相比，物理结构是用来优化用户登录网络和活动目录复制产生的网络流量。为优化活动目录复制使用的带宽，你必须理解物理结构。物理结构组成：

- **域控制器** 运行 Windows Server 2003 或 Windows 2000 Server 和活动目录。每个域控制器具备存储和复制功能。一个域控制器只支持一个域。确保活动目录的高可用性，每一个域应该有至少两个域控制器。
- **活动目录站点** 站点有高速连接多个子网上的计算机组成。当你建立站点，在同一站点的域控制器通信频繁。频繁的复制通信将最小化站点内的延迟，即在一个域控制器上做的改变将很快的复制到其他的域控制器。你创建站点来优化不同位置的域控制器带宽的使用。
- **活动目录分区** 每一个域控制器包含下列活动目录分区。
  - 目录分区：目录分区存储域控制器所在域的所有对象副本，目录分区只在同一域的域控制器之间复制。
  - 配置分区：配置分区包含目录林的拓扑。拓扑是目录林中所有的域控制器和它们之间的连接。
  - 架构分区：架构分区存储整个林的架构。一个目录林只有一个架构，所以同一个林中的所有域对不同对象的定义一致。架构分区在目录林中的所有域控制器之间复制。
  - 可选的应用程序分区：应用程序分区存储与安全无关的，一个或多个应用程序使用的对象，应用程序分区在林中指定的域控制器之间复制。应用程序目录分区的好处之一就是其中的数据可复制到林中不同的域控制器，以提供冗余、可用性和容错。

1.1.4 操作主控

当对一个域进行改变时，改变将复制到域中所有的域控制器。有些改变，比如更改架构，将复制到目录林中所有的域控制器。这种复制成为多主控复制。

当多主控复制时，如果原始更新发生在不同的域控制器上的同一个对象属性，复制冲突将发生。为避免复制冲突，你使用单主控复制，即在一个域中只能在一个域控制器上做某种改变。这样，改变不能在同一时刻发生在网络中不同位置。活动目录为重要的改变使用单主控复制，比如添加一个新域，或更改整个目录林的架构。

使用单主控的操作在域中或林中整理成不同的角色。这些角色称为操作主控角色，对于每一中操作主控角色，只有角色拥有者才能做相应的目录的更改，负责某种角色的域控制器成为那种角色的操作主控。活动目录存储关于哪个域控制器是哪种角色的操作主控的信息。

活动目录定义五种操作主控角色，每种有一个默认位置。操作主控有域范围的和目录林范围的。

- 林范围的角色林中唯一，它们是：
  - 架构主控：控制所有的架构更新。架构包含对象类和属性的定义。用户用来创建所有活动目录对象，比如，计算机、用户、组、打印机。
  - 域命名主控：控制在目录林中添加和删除域。当你向目录林中添加新域，只有是域命名主控的域控制器能够添加。

只有架构主控和域命名主控在目录林范围唯一。

- 域范围的角色目录林中的每个域中唯一，它们是：
  - 主域控制器仿真器（PDC）：充当 Windows NT 4.0 PDC,支持运行在混合模式域备份域控制器（BDC）。混合模式指的是域中有运行 Windows NT 4.0 的域控制器。主域控制器仿真器默认是你创建新域的第一个域控制器。
  - 相对标识符（RID）主控：当你创建新的安全主体时，域控制器创建新的安全标识来代表对象指定对象唯一的安全标识（SID）。SID 包含域的 SID（用来唯一标识目录林中的域，同一域中的对象有相同的域 SID），和相对标识符（RID），RID 在安全主体创建的域中唯一。RID 主控分配 RID 块给域中的其他的域控制器，这样在域中的任何域控制器上创建安全主体时，将会在被授予的 RID 块中指派的 RID。这样在任何一个域控制器上创建的安全主体的 SID，将在整个目录林中唯一。
  - 基础结构主控：在任何时候，每个域中只能有一个域控制器作为结构主机。结构主机负责更新从它所在的域中的对象到其他域中对象的引用。比如：其他域中的全局组添加到本域中的域本地组，如果该全局组更改显示名，或移动到其他域，基础结构主控，负责更改域本地组对改全局组的引用。结构主机将其数据与全局编录的数据进行比较。全局编录通过复制操作定期接受所有域中对象的更新，从而使全局编录的数据始终保持最新。如果结构主机发现数据过时，则它从全局编录申请更新的数据。结构主机然后将这些更新的数据复制到域中的其他域控制器。

目录林中的每个域都有自己的 PDC 仿真器，RID 主控，和基础结构主控。

1.2　活动目录的工作方式

- 活动目录服务
- 架构
- 全局目录
- 标识名和相对标识名
- 活动目录如何实现一次登录
- 检测活动目录结构

本节介绍活动目录作为目录服务的作用。理解活动目录如何工作将会帮助你管理资源和解决资源访问出现的问题。

1.2.1　目录服务

在一个大的网络环境中的资源由许多用户和应用程序共享。为使用户和应用程序访问资源和信息，你需要用一致的方式去命名、描述、定位、管理和保证这些信息的安全。活动目录能起到这种作用。如图 1-1。

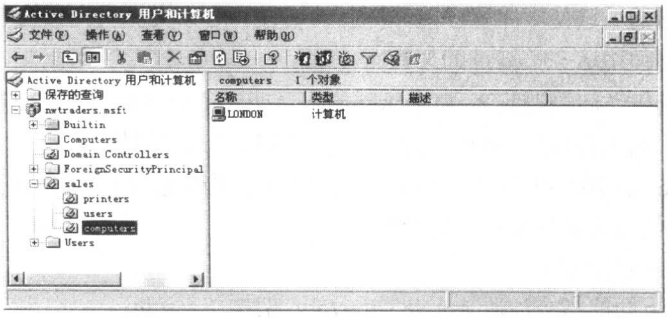

图 1-1　活动目录储存域中的资源

目录服务是一种结构化的关于组织中人和资源信息存储。在 Windows Server 2003 网络，目录服务是活动目录。

活动目录有下列功能：

- **使用户和应用程序访问对象的信息**　这些信息以属性值的方式存储。你可以基于对象的类，属性，属性值，活动目录中结构中的位置查找对象。
- **使网络的物理拓扑和协议透明**　这样，网络中的用户能访问任何资源，例如打印机，不用知道资源在哪，物理上如何连接到网络上的。
- **允许存储大量的对象**　因为存储在活动目录分区中，活动目录能够随着组织点增长而扩展。例如：目录能够从一个有几百个对象的服务器，扩展到成千个服务器和百万个对象。
- **能够作为非操作系统服务**　活动目录应用程序模式（AD/AM）是 Microsoft 活动目录的新增功能，能够扩展使用目录服务的应用程序使用场景。AD/AM 运行为非操作系统服务，不需要必须部署在域控制器上。作为非操作系统服务意味着多个 AD/AM 实例能够同时运行在一个域控制器上，每个实例被独立配置。