



Microsoft® Press



内附光盘

# 构建Active Directory服务

## —— 业内专家经验笔录

[美]Microsoft Corporation 著

东方人华 译

规划和实施Active Directory服务的经验之谈

Microsoft咨询服务  
部门的最佳惯例

IT Professional

清华大学出版社

<http://www.tup.tsinghua.edu.cn>



# 构建 Active Directory 服务——业内专家经验笔录

[美] Microsoft Corporation 著  
东方人华 译

清华大学出版社

(京)新登字 158 号

## 内 容 简 介

远在本书出版之前,包括 Microsoft Consulting Services、Microsoft Program Management 和众多 Windows 2000 测试版用户在内的许多组织和个人为如何高效地部署和运用 Windows 2000 Active Directory,实现从多种异构网络操作环境到 Windows 2000 的迁移、降低信息管理成本和增强网络环境的安全性等做出了许多探索性的实践。本书汇集了许多企业在这些方面的成功范例。对于当今和未来的企业经营者和 IT 部门主管来说,本书的参考价值是不言而喻的。

对于打算部署 Exchange 2000 Server 的企业用户来说本书具有很高的参考价值。

Building Enterprise Active Directory Services Notes from the Field

Copyright (2000) by Microsoft Corporation.

Original English language edition Copyright © (2000) by (Microsoft Corporation).

All rights published by arrangement with the original publisher, Microsoft Press, a division of Microsoft Corporation, Redmond, Washington, U.S.A.

北京市版权局著作权合同登记号: 图字 01-2000-4395 号

版权所有, 盗版必究。

本书贴有清华大学出版社激光防伪标签, 无标签者不得销售。

书 名: 构建 Active Directory 服务——业内专家经验笔录

作 者: Microsoft Corporation

译 者: 东方人华

责任编辑: 王青松

出 版 者: 清华大学出版社(北京清华大学学研大厦, 邮编 100084)

<http://www.tup.tsinghua.edu.cn>

印 刷 者: 北京市清华园胶印厂

发 行 者: 新华书店总店北京发行所

开 本: 787×960 1/16 印张: 28.25 字数: 614 千字

版 次: 2001 年 4 月第 1 版 2001 年 4 月第 1 次印刷

书 号: ISBN 7-900631-40-2

印 数: 0001~5000

定 价: 59.00 元 (含 1 张光盘)

# 引 言

欢迎使用业内专家经验笔录系列丛书的第七卷——《构建 Active Directory 服务——业内专家经验笔录》。在本卷中将介绍那些成功地实现 Windows 2000 Active Directory 的企业最佳作法。业内专家手记系列丛书中手记的特色在于，该系列中的每一卷都是以共享业内操作经验和实际使用情况为目的而编写的。本书是许多机构共同努力的结果，它们是：Microsoft Consulting Services、Microsoft Program Management，以及许多和我们通力合作的众多用户，当 Windows 2000 还处于开发中时，他们就在自己的业务中使用了 Active Directory。

Active Directory 被视为 Microsoft 分布式服务的一个更具完整性的组件。其他许多组件为了配置、管理和使用上的便利都要借助 Active Directory。使用计划周密的 Active Directory 可以产生非常显著的经济效益，因为它结合了许多 IT 专家管理的经营要素。

《构建 Active Directory 服务——业内专家经验笔录》是对 Microsoft Windows 2000 产品文档的一个补充。另外 Microsoft Windows 2000 Server Resource Kit (Microsoft Press 出版，2000) 也具有这样的功能。该书详细地介绍了 Active Directory 以及 Windows 2000 的结构细节和实施设置。

本书包含 12 章，共分成 3 个部分。

## 第 I 部分：建立基础

第 1 章总体介绍了大型分散企业的 Active Directory 设计。该章详细介绍了如何在所研究的环境中进行需求评价、过程设计以及使用 Active Directory。该章的作者仔细分析了许多设计准则，例如 DNS(域名系统)名称空间、Active Directory 域、WAN 链接和拨号连接的配置。

第 2 章或许是 Active Directory 复制方面可以利用的最直观、最有参考价值的文档。这一章全面介绍了 Active Directory 复制、布局设计的各种技巧，以及如何正确选择连接企业各个位置的传输工具。该章集中介绍 Compaq Computers 的企业设计，它是由 Compaq 公司专门从事公司联合开发项目 (Joint Development Program) 的高级顾问编写的。

第 3 章深入分析数据在 Active Directory 中的保存方式，以及如何正确地计算硬件要求。此章还介绍数据在 Active Directory 上的物理保存方式以及 Active Directory 存储的组织方式。本章的内容有助于读者确定域控制器和全局目录服务器的大小并设计适当的 Active Directory 分区创建方法和放置方法。

第 2 章详细介绍了复制的运行方式，而第 4 章，则详细介绍这些复制的数据在网上

——您的网络基础结构中——的形态。该章还详细分析了复制关于带宽使用的诸多方面。本章给读者提供了解 Active Directory 复制及其对企业潜在作用的翔实情况。此外，本章还介绍了网络端口的详细资料以及使用 NETMON 分析复制通信量的操作方式。

第 5 章逐条详述了 Active Directory 客户程序的网络和目录应用。在设计 Active Directory 基础结构时，这一点的重要性不亚于复制通信量。请注意，复制通信量是在编写或者修改对象时生成的，而客户程序通信量在用户每次登录到网络或者使用应用程序时都会产生。

## 第 II 部分：升级和集成情况

第 6 章详细介绍域的升级和强化策略。该章介绍了各种工具及其使用时间，还详细介绍了将企业从 WindowsNT 环境更换到 Windows 2000 的操作方式。另外，本章介绍了与下一级集成的问题。

第 7 章深入介绍了 Windows 2000、Active Directory 与 Unix 平台及客户程序的结合方式。本章分析了各种可以使用的工具及方法，讨论了各设计要素及其使用。

第 8 章对于那些使用已有的 Exchange 基础结构运行 Active Directory 的用户而言非常重要。本章分析了升级过程、Exchange 和 Active Directory 之间的集成与同步以及 Exchange 环境的崩溃与重建。

第 9 章分析了 Novells 的 NDS 与 Active 在结构上的一些关键差异。然后，分析了在 Netware 目录与 Active Directory 目录之间同步化对象的不同方法。这一章从管理与系统工程的角度对这两个产品进行了比较，因而对那些已经熟悉了 NetWare 的用户而言，这一章是了解 Active Directory 的极好起点。

## 第 III 部分：管理与安全

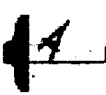
第 10 章是 Microsoft Consulting Services 中的一位 Active Directory 经验极其丰富的用户编写的。该作者介绍了 Active Directory 的脚本环境，包括 ADSI、ASP、Windows Scripting Host 和 Windows 管理规范（WMI）。

虽然 Windows 2000 域仍然可以用来在公司内分割管理权限，但这一技巧与运用 Active Directory 中的管理委托相比——从管理的角度来说——就显得非常浪费了。第 11 章研究了这一特性是如何将一个域划分成更易于管理的组织单位（Organizational Units, OU），选定的管理员可以通过这种方式获得各种授权。

第 12 章集中介绍分布式和异构型计算机的关键性技术——公钥基础结构（Public Key Infrastructures, PKI）。在这些环境中，拥有提供验证、保密和认可服务的坚固的安全防范系统是关键。这一章介绍了公钥基础结构的相关背景资料，包括它的使用目的、如何将它用作 Windows 2000 Active Directory 的一部分，以及 Windows 2000 PKI 的各个组件。

## 本书所用的提示图标

这些附加的图标起简单的提醒作用：

| 图标                                                                                | 说明                                                |
|-----------------------------------------------------------------------------------|---------------------------------------------------|
|  | <b>警告</b> 为了避免潜在的故障，建议您采取或者取消特定的动作。               |
|  | <b>注意</b> 正文中所强调、补充或者限制的要点。                       |
|  | <b>最佳操作或者操作指南</b> 突出提示经过检验的操作、技术或者 MCS 真实经验的操作过程。 |
|  | <b>工具</b> 指明样本代码、WindowsNT 公用程序、或者本书配套光盘上提供的各种工具。 |

## 配套光盘上的内容

您可以在本书配套光盘上找到——出于版面考虑——无法安排到书中的文档，以及许多有用的工具、脚本和公用程序。

下面按主题列举其中包含的内容：

## Active Directory 名称空间设计

- **Windows 2000 的应用模板。**该模板是 Microsoft 项目模板。它给出主要的设计步骤、任务和在网络中应用 Windows 2000 所必需的资源。模板可以根据公司的大小创建一个包括所有的依存、时间安排和重大事件在内的项目计划。请见光盘上的 Deployment Template 文件夹。

## 容量安排

- **为容量设计和 Active Directory 数据库大小增加 Active Directory 的工具。**这些工具允许用户在实验室环境中重新处理数据库的大小以及重新进行复制通信量测试。并提供脚本和注册文件以完全自动化进行各增量测试，包括 Active Directory 目录数据库的碎片合并。参见光盘上的 Capacity Planning Tools 文件夹。
- **生成 Exchange 2000 邮件和可以使用邮箱的用户、组、和联系人的工具。**在对 Active Directory 进行了增加之后，您可能想知道 Exchange 何时进入到 Active Directory。在

- 实验室环境中安装 Exchange 后，这些工具就可以用于创建用户的邮箱了。Active Directory 大小上的影响是可以测量出来的。参见光盘上的 CapacityPlanningTool 文件夹。
- **LDAP 工具、脚本和公用程序。**就网络通信量测试而言，许多小型工具和公用程序可用于创建典型的 LDAP 搜索操作。这些脚本可用于重新创建实验室中的各项测试。参见光盘上的 Capacity Planning Tools 文件夹。
- **复制通信量电子表格。**安装域控制器时，复制将每天运行一次。您可以使用这个 Micro softExcel 电子表格计算每天通过网络的通信量。参见光盘上的 Replication 文件夹。
- **复制通信量计算表。**不仅计算网络中生成的复制通信量非常重要，而且估计信息的发送时间也非常重要。不论您是在慢速连接还是在高速连接的环境中操作，这些表格都有助于准确地处理这些任务。参见光盘上的 Replication 文件夹。
- **附加文档。**本书中没有足够的版面介绍在 Exchange 2000 中进行客户登录操作、架构机修改等的每一个细节。您可以在光盘上找到这些内容的详细介绍，包括业内专家手记系列第六卷 Optimizing Network Traffic (Microsoft Press 出版, 1999) 里的 3 章内容。请参见光盘上的 Document 文件夹。

## Active Directory 管理

- **使用 ADSI 的 Sample Active Server Pages (Active 服务器页样本)。**Windows 2000 管理工具可以访问所有的配置和用户信息。不过，有些管理员需要获得更大的灵活性。本书中的脚本一章就是这方面的一个指导手册，它介绍如何创建简单的但功能强大的脚本以检索各种 Active Directory 配置信息，包括复制配置和 GlobalCatalog (全局编录) 配置信息。为了您使用的方便，光盘中包括了使用这些脚本的许多 ASP 页面。它们能用作 (也是) 功能强大的监控工具。请参见光盘上的 DSInfo 文件夹。
- **在多域环境中加强安全的工具。**大型公司常常希望限制 Domain Administrators (域管理员) 的性能，使之不能在整个树林的范围内影响架构或者在配置容器中的配置修改。本书中的第 12 章介绍了增强安全的方式。光盘中有一个工具 (DnProtect.exe) 允许您保护不同容器内的单独对象。请见光盘上的 DNProtect 文件夹。

## 如何使用配套光盘

要使用配套光盘，请将磁盘插入您的光驱中。启动菜单会自动出现。如果这个菜单没有出现，请运行 CD 根目录中的 StartCD.exe。

启动菜单是提供光盘上文件和模板的运行起点。它也能够让您安装查看光盘上 Optimizing Network Traffic (优化网络通信量) 中 3 章内容所需的软件。不过，要运用我们提供的所有脚本、公用程序和工具，您还是要一个一个单独地浏览各文件夹，并参看每

个文件夹适当的 Readme.doc。

## 系统技术要求

系统技术要求定义使用本书配套光盘上可利用资源所需的最小系统配置。该技术要求列在本书索引结束后的页面上。

## 深致谢意

在此，我们特意花上一些时间向那些在 Windows 2000 开发中帮助 Microsoft 公司进行特色功能鉴定、软件测试和在经营中实际使用 Windows 2000 软件测试版的用户致以深深的谢意。JDP 和 RDP 程序用户对于 Microsoft 公司了解各个用户的需求以及用户对软件特色功能的要求都非常重要。我们视各位用户为产品开发中的合作伙伴，他们是促使我们将软件做得更好的合作伙伴。在此，谨代表 Microsoft 公司所有人，感谢各位用户为使 Windows 2000 做得更好所花费的时间，进行的努力，提供的建议以及做出的各种贡献。

## 重要说明

本书中描述的公司、组织、产品、人员和事件例子纯属虚构。它们和任何真实的公司、组织、产品、人员或者事件没有任何的联系。特此说明。

# 目 录

## 第 I 部分 建立基础

|                                                     |           |
|-----------------------------------------------------|-----------|
| <b>第 1 章 Windows 2000 Active Directory 设计</b> ..... | <b>3</b>  |
| 1.1 Woodgrove 银行总体设计过程 .....                        | 3         |
| 1.1.1 阶段与交付 .....                                   | 3         |
| 1.1.2 小组 .....                                      | 4         |
| 1.1.3 高标准设计目标 .....                                 | 5         |
| 1.2 Windows NT 4.0 现行环境评估 .....                     | 6         |
| 1.2.1 现行网络结构 .....                                  | 6         |
| 1.2.2 现行国内 Windows NT 4.0 域结构 .....                 | 7         |
| 1.2.3 现行国际 Windows NT 4.0 域结构 .....                 | 8         |
| 1.3 Windows 2000 设计 .....                           | 10        |
| 1.3.1 Active Directory 的业务要求 .....                  | 10        |
| 1.3.2 Woodgrove 银行 Active Directory 的设计 .....       | 11        |
| 1.3.3 单一的国内域和独立的国际域 .....                           | 12        |
| 1.3.4 下一代 INTL 设计 .....                             | 40        |
| 1.4 小结 .....                                        | 42        |
| <b>第 2 章 Compaq 的 Windows 2000 站点拓扑设计</b> .....     | <b>44</b> |
| 2.1 Active Directory 复制基础 .....                     | 45        |
| 2.1.1 域控制器 .....                                    | 45        |
| 2.1.2 触发复制 .....                                    | 46        |
| 2.1.3 更新类型 .....                                    | 46        |
| 2.1.4 命名上下文 .....                                   | 47        |
| 2.1.5 站点 .....                                      | 48        |
| 2.1.6 桥头堡服务器 .....                                  | 49        |

|              |                                       |           |
|--------------|---------------------------------------|-----------|
| 2.1.7        | 复制传输.....                             | 49        |
| 2.1.8        | 知识一致性检测器.....                         | 50        |
| 2.1.9        | 连接对象.....                             | 50        |
| 2.1.10       | 全局编录复制.....                           | 51        |
| 2.1.11       | Compaq 的公司名称空间.....                   | 52        |
| 2.2          | 网络基础结构.....                           | 53        |
| 2.2.1        | 全局网 (GlobalNet) .....                 | 53        |
| 2.2.2        | 地址分配考虑.....                           | 55        |
| 2.2.3        | 遗留网络.....                             | 56        |
| 2.3          | 站点拓扑设计.....                           | 56        |
| 2.3.1        | 站点内复制与站点间复制.....                      | 57        |
| 2.3.2        | 创建复制拓扑.....                           | 58        |
| 2.3.3        | 站点拓扑.....                             | 59        |
| 2.3.4        | 服务器位置.....                            | 62        |
| 2.4          | 小结.....                               | 66        |
| <b>第 3 章</b> | <b>Active Directory 数据库规模评估 .....</b> | <b>68</b> |
| 3.1          | Active Directory 数据库结构和组件.....        | 68        |
| 3.1.1        | 总体结构.....                             | 69        |
| 3.1.2        | 数据库结构.....                            | 70        |
| 3.1.3        | 数据库的更改.....                           | 70        |
| 3.1.4        | 无用单元收集.....                           | 72        |
| 3.2          | Active Directory 数据库规模测试——单个对象.....   | 74        |
| 3.2.1        | 计算增长值和对象大小.....                       | 74        |
| 3.2.2        | 单个对象类型装载.....                         | 74        |
| 3.2.3        | 用户对象.....                             | 74        |
| 3.2.4        | 增加属性.....                             | 76        |
| 3.2.6        | 组织单元.....                             | 78        |
| 3.2.7        | 组.....                                | 79        |
| 3.2.8        | 联系人.....                              | 83        |
| 3.2.9        | 在 Active Direcoty 中存储公钥证书.....        | 84        |
| 3.2.10       | 打印机和卷.....                            | 85        |
| 3.2.11       | 在 Active Directory 中存储 BLOBS.....     | 87        |
| 3.3          | Active Directory 数据库规模测试——样本公司.....   | 88        |
| 3.3.1        | 带有最小属性的样本公司.....                      | 88        |
| 3.3.2        | 带有自定义属性的样本公司.....                     | 89        |

|                                                    |            |
|----------------------------------------------------|------------|
| 3.3.3 访问控制项.....                                   | 90         |
| 3.3.4 回收数据库中的空间.....                               | 92         |
| 3.4 数据库规模测试小结.....                                 | 94         |
| 3.5 Active Directory 数据库规模测试——全局编录服务器.....         | 95         |
| 3.5.1 样本公司全局编录服务器.....                             | 95         |
| 3.5.2 全局编录服务器和有通用组的样本公司.....                       | 96         |
| 3.5.3 用单个对象进行全局编录规模评估.....                         | 97         |
| 3.5.4 全局编录小结.....                                  | 99         |
| 3.6 添加 Microsoft Exchange 2000.....                | 100        |
| 3.6.1 用 Exchange 2000 扩展架构.....                    | 100        |
| 3.6.2 为用户添加邮箱.....                                 | 101        |
| 3.6.3 可用邮件组.....                                   | 103        |
| 3.6.4 可用邮件联系人.....                                 | 105        |
| 3.6.5 有 Exchange 2000 的样本公司.....                   | 106        |
| 3.6.6 有无 Exchange 2000 时的 Active Directory 小结..... | 108        |
| 3.7 小结.....                                        | 109        |
| <b>第 4 章 Active Directory 复制通信量分析.....</b>         | <b>110</b> |
| 4.1 为何要测量复制通信量?.....                               | 110        |
| 4.2 复制通信量的类型.....                                  | 112        |
| 4.2.1 复制方案.....                                    | 113        |
| 4.2.2 如何测量复制通信量.....                               | 114        |
| 4.3 站点内复制.....                                     | 114        |
| 4.3.1 RepAdmin.....                                | 116        |
| 4.3.2 MMC 强制复制.....                                | 117        |
| 4.3.3 复制选项小结.....                                  | 118        |
| 4.3.4 建立复制通信量模型.....                               | 119        |
| 4.3.5 全局编录、域内复制与域间复制的比较.....                       | 120        |
| 4.3.6 单个属性更改.....                                  | 120        |
| 4.3.7 站点内域对象复制.....                                | 124        |
| 4.3.8 站点内 GC 复制.....                               | 129        |
| 4.4 站点间复制.....                                     | 133        |
| 4.4.1 站点间域复制.....                                  | 134        |
| 4.4.2 添加用户属性.....                                  | 138        |
| 4.4.3 密码更改的复制.....                                 | 141        |
| 4.4.4 更改组成员身份.....                                 | 142        |

|              |                                                          |            |
|--------------|----------------------------------------------------------|------------|
| 4.4.5        | 管理操作.....                                                | 143        |
| 4.4.6        | 全局编录服务器复制.....                                           | 152        |
| 4.4.7        | 添加用户对象.....                                              | 153        |
| 4.4.8        | 复制组.....                                                 | 154        |
| 4.4.9        | 打印机和卷.....                                               | 157        |
| 4.4.10       | 调整 SMTP 复制.....                                          | 159        |
| 4.4.11       | 站点间通信量计算表格.....                                          | 161        |
| 4.4.12       | 慢速链路的复制.....                                             | 161        |
| 4.5          | 小结.....                                                  | 163        |
| <b>第 5 章</b> | <b>Active Directory 客户机网络通信量</b> .....                   | <b>164</b> |
| 5.1          | Windows NT 4 客户机登录通信量.....                               | 165        |
| 5.1.1        | 概述.....                                                  | 165        |
| 5.1.2        | 工作站启动过程.....                                             | 167        |
| 5.1.3        | 用户登录.....                                                | 171        |
| 5.2          | Windows 2000 Professional 到 Active Directory 的登录通信量..... | 174        |
| 5.2.1        | 测试 Harness 设置.....                                       | 176        |
| 5.2.2        | 组成员身份对登录通信量的影响.....                                      | 176        |
| 5.2.3        | 组策略对登录通信量的影响.....                                        | 178        |
| 5.2.4        | IntelliMirror 技术 .....                                   | 185        |
| 5.2.5        | NetBIOS 通信量.....                                         | 190        |
| 5.2.6        | Windows 2000 Professional 工作站登录通信量的说明.....               | 190        |
| 5.3          | LDAP 概念、操作、通信量以及 Active Directory 的容量规划.....             | 191        |
| 5.3.1        | 信息模型.....                                                | 191        |
| 5.3.2        | 命名模型.....                                                | 193        |
| 5.3.3        | 功能模型.....                                                | 194        |
| 5.3.4        | 更多的概念.....                                               | 195        |
| 5.4          | Active Directory LDAP 通信量分析.....                         | 206        |
| 5.4.1        | 测试环境.....                                                | 206        |
| 5.4.2        | 分析询问.....                                                | 220        |
| 5.4.3        | 分析更新.....                                                | 227        |
| 5.4.4        | 没有涉及的问题.....                                             | 234        |
| 5.5          | 小结.....                                                  | 235        |

## 第 II 部分 迁移和集成的方案

|                                       |            |
|---------------------------------------|------------|
| <b>第 6 章 域迁移与合并</b> .....             | <b>239</b> |
| 6.1 环境.....                           | 239        |
| 6.1.1 Windows NT 4.0 域模型.....         | 239        |
| 6.1.2 建议的 Active Directory 模型.....    | 240        |
| 6.2 确定迁移方案.....                       | 242        |
| 6.3 创建 Active Directory 基础结构.....     | 242        |
| 6.3.1 根级域 NWT.INT.....                | 242        |
| 6.3.2 二级域 NA.NWT.INT.....             | 243        |
| 6.4 迁移英国 (UK) 域 (原地升级).....           | 244        |
| 6.4.1 为什么要原地升级.....                   | 244        |
| 6.4.2 升级的顺序.....                      | 244        |
| 6.4.3 升级过程.....                       | 245        |
| 6.4.4 维持互用性.....                      | 247        |
| 6.5 合并北美 (NA) 域.....                  | 248        |
| 6.5.1 合并原因.....                       | 248        |
| 6.5.2 Active Directory 迁移工具.....      | 248        |
| 6.5.3 迁移的顺序.....                      | 248        |
| 6.6 迁移的过程.....                        | 249        |
| 6.6.1 设计并测试一个取消迁移的计划.....             | 249        |
| 6.6.2 建立和应用一个双重名称策略.....              | 249        |
| 6.6.3 建立和应用唯一性策略.....                 | 249        |
| 6.6.4 识别并删除不用的全局组和本地组.....            | 250        |
| 6.6.5 建立必要的信任关系.....                  | 250        |
| 6.6.6 复制全局组到 Windows 2000 域中.....     | 251        |
| 6.6.7 将共享的本地组复制到 Windows 2000 域中..... | 253        |
| 6.6.8 将用户帐户复制到 Windows 2000 域中.....   | 254        |
| 6.6.9 将计算机帐户迁移到 Windows 2000 域中.....  | 255        |
| 6.6.10 将一个试验组迁移到 Windows 2000 域中..... | 255        |
| 6.6.11 将余下的域成员迁移到 Windows 2000 域..... | 256        |
| 6.6.12 迁移期间的互用性.....                  | 256        |

|              |                                                    |            |
|--------------|----------------------------------------------------|------------|
| 6.6.13       | 取代源域.....                                          | 257        |
| 6.6.14       | 使用 ClonePrinciple、Netdom 和 MoveTree.....           | 257        |
| 6.7          | 将来的计划.....                                         | 258        |
| 6.7.1        | 资源域 NWTRDUK.....                                   | 258        |
| 6.7.2        | 北美的资源域.....                                        | 259        |
| 6.7.3        | 分支机构.....                                          | 259        |
| 6.8          | 小结.....                                            | 259        |
| <b>第 7 章</b> | <b>Active Directory 与基于 Unix 的 DNS 环境集成 .....</b>  | <b>260</b> |
| 7.1          | 先决条件.....                                          | 261        |
| 7.2          | 基础结构和 DNS 策略.....                                  | 261        |
| 7.3          | 为什么使用完全 Unix 的 DNS 解决方案? .....                     | 263        |
| 7.4          | DNS 对 Active Directory 的要求.....                    | 263        |
| 7.5          | 比较 Bind 和 Windows 2000 的 DNS.....                  | 263        |
| 7.5.1        | Active Directory 存储和复制集成.....                      | 264        |
| 7.5.2        | 安全动态更新.....                                        | 264        |
| 7.5.3        | 缓存解析程序.....                                        | 265        |
| 7.5.4        | DNS 插入程序.....                                      | 265        |
| 7.5.5        | WINS 集成 .....                                      | 265        |
| 7.5.6        | 支持 UTF-8 (Unicode) 字符 .....                        | 266        |
| 7.5.7        | 支持 Aging/Scavenging.....                           | 266        |
| 7.5.8        | DNSCMD 命令行实用程序.....                                | 266        |
| 7.6          | Unix DNS 环境的升级选项.....                              | 266        |
| 7.7          | 配置一个完全 Unix DNS 环境.....                            | 268        |
| 7.7.1        | Unix 服务器配置.....                                    | 268        |
| 7.7.2        | Windows 2000 服务器配置 .....                           | 274        |
| 7.7.3        | Windows 2000 DHCP 服务器配置.....                       | 274        |
| 7.7.4        | 下级 DHCP 服务器.....                                   | 276        |
| 7.7.5        | Windows 2000 客户端 .....                             | 276        |
| 7.7.6        | 下级客户端.....                                         | 277        |
| 7.8          | 其他一些考虑.....                                        | 277        |
| 7.8.1        | Bind 4.x 和 8.1.2 服务器.....                          | 277        |
| 7.8.2        | Windows 2000 域控制器和 DHCP 服务器.....                   | 278        |
| 7.9          | 小结.....                                            | 279        |
| <b>第 8 章</b> | <b>Active Directory 与 Exchange Server 集成 .....</b> | <b>280</b> |

|        |                                                             |     |
|--------|-------------------------------------------------------------|-----|
| 8.1    | 升级策略概述.....                                                 | 281 |
| 8.2    | All-Terrain Trucking 公司简介.....                              | 281 |
| 8.3    | 将 Windows NT 4.0 域升级到 Windows 2000 .....                    | 287 |
| 8.3.1  | 帐户域升级小结.....                                                | 288 |
| 8.3.2  | EXCHANGE 资源域升级小结.....                                       | 290 |
| 8.4    | 压缩资源域.....                                                  | 291 |
| 8.5    | 目录复制与同步.....                                                | 297 |
| 8.5.1  | Active Directory Connector.....                             | 298 |
| 8.5.2  | 使用连接协议建立关系.....                                             | 299 |
| 8.5.3  | 复制.....                                                     | 299 |
| 8.5.4  | 同步.....                                                     | 300 |
| 8.6    | 安装与配置 Active Directory Connector .....                      | 301 |
| 8.6.1  | 第一步: 检查 Windows NT 域结构和 Exchange Server 站点拓扑.....           | 301 |
| 8.6.2  | 第二步: 确定哪个目录服务来管理对象同一性.....                                  | 302 |
| 8.6.3  | 第三步: 修改 Active Directory 架构.....                            | 303 |
| 8.6.4  | 第四步: 定义目录同步的对象.....                                         | 303 |
| 8.6.5  | 第五步: 将 Exchange Server 站点/容器映射到 Active Directory 域/OU ..... | 305 |
| 8.6.6  | 第六步: 确定 Active Directory 和 Exchange Server 之间的属性映射 .....    | 306 |
| 8.6.7  | 第七步: 设置 Active Directory Connectors .....                   | 307 |
| 8.6.8  | 第八步: 创建连接协议, 从 Exchange 填充 Active Directory .....           | 308 |
| 8.6.9  | 第九步: 确定目录复制和同步的时间表.....                                     | 309 |
| 8.6.10 | 第十步: 为保持目录同步创建连接协议.....                                     | 311 |
| 8.6.11 | 第十一步: 对目录服务保密以防止冲突和保持同一性.....                               | 314 |
| 8.6.12 | Active Directory Connector 小结.....                          | 316 |
| 8.7    | 为 Exchange 2000 做规划 .....                                   | 317 |
| 8.7.1  | Exchange 2000 使用 Active Directory .....                     | 317 |
| 8.7.2  | Exchange 2000 ADC 的升级 .....                                 | 318 |
| 8.7.3  | 升级到 Exchange 2000 之前 .....                                  | 318 |
| 8.8    | 小结.....                                                     | 319 |
| 第 9 章  | Active Directory 与 Novell NetWare DNS.....                  | 321 |
| 9.1    | 网络目录概述.....                                                 | 322 |
| 9.1.1  | 架构对象、类和属性.....                                              | 323 |
| 9.1.2  | 层次结构和容器.....                                                | 324 |
| 9.1.3  | 安全与授权.....                                                  | 325 |
| 9.1.4  | 复制与同步.....                                                  | 326 |

|                                           |     |
|-------------------------------------------|-----|
| 9.1.5 分区.....                             | 326 |
| 9.2 比较 NDS 和 Active Directory.....        | 327 |
| 9.2.1 容器对象.....                           | 327 |
| 9.2.2 编录.....                             | 331 |
| 9.2.3 复制概述.....                           | 333 |
| 9.2.4 多主机更新.....                          | 333 |
| 9.2.5 身份验证.....                           | 334 |
| 9.2.6 安全与继承.....                          | 335 |
| 9.2.7 Internet 标准.....                    | 335 |
| 9.3 在 Active Directory 和 NDS 中设计解决方案..... | 337 |
| 9.3.1 设计目录的准则.....                        | 337 |
| 9.3.2 关于 Northwind.....                   | 338 |
| 9.3.3 设计过程.....                           | 338 |
| 9.4 Active Directory 和 NDS 之间的同步.....     | 347 |
| 9.4.1 对同步的需要.....                         | 347 |
| 9.4.2 出版者、订阅者和对话.....                     | 347 |
| 9.4.3 配置 MSDSS.....                       | 348 |
| 9.4.4 同步类型.....                           | 351 |
| 9.4.5 管理.....                             | 351 |
| 9.5 小结.....                               | 352 |

## 第III部分 管理与安全

|                                                   |     |
|---------------------------------------------------|-----|
| 第 10 章 编写 Active Directory 脚本.....                | 355 |
| 10.1 基础知识.....                                    | 355 |
| 10.1.1 什么是 ADSI.....                              | 355 |
| 10.1.2 Windows 脚本编写主机.....                        | 357 |
| 10.1.3 Active Server Pages.....                   | 358 |
| 10.1.4 HTML 应用程序.....                             | 358 |
| 10.1.5 使用 Visual Basic 编写 Office 2000 中的应用程序..... | 359 |
| 10.2 ADSI 基础知识.....                               | 359 |
| 10.2.1 结构.....                                    | 359 |
| 10.2.2 连接到 Active Directory.....                  | 360 |
| 10.2.3 读取一个对象.....                                | 361 |

|                                             |            |
|---------------------------------------------|------------|
| 10.2.4 更新一个对象.....                          | 361        |
| 10.2.5 枚举(Enumerating)一个容器中的对象 .....        | 362        |
| 10.2.6 搜索.....                              | 362        |
| 10.3 管理域的信息 .....                           | 363        |
| 10.3.1 提取计算机的信息.....                        | 363        |
| 10.3.2 信任关系.....                            | 366        |
| 10.3.3 创建用户帐户.....                          | 368        |
| 10.3.4 创建组.....                             | 368        |
| 10.4 管理企业配置信息.....                          | 371        |
| 10.4.1 分区.....                              | 371        |
| 10.4.2 列出站点.....                            | 372        |
| 10.4.3 创建站点.....                            | 374        |
| 10.4.4 列出子网.....                            | 376        |
| 10.4.5 创建子网.....                            | 376        |
| 10.4.6 列出域控制器.....                          | 377        |
| 10.4.7 站间链路.....                            | 380        |
| 10.4.8 复制连接.....                            | 382        |
| 10.4.9 灵活单主机操作.....                         | 383        |
| 10.4.10 IADSTools 示例 .....                  | 385        |
| 10.5 Window 管理规范 .....                      | 387        |
| 10.6 小结 .....                               | 392        |
| <b>第 11 章 委派树/树林操作.....</b>                 | <b>393</b> |
| 11.1 委派：原因和结果.....                          | 393        |
| 11.2 背景 .....                               | 394        |
| 11.3 中央办公室.....                             | 395        |
| 11.3.1 根域管理.....                            | 395        |
| 11.3.2 架构管理.....                            | 396        |
| 11.3.3 子域的预创建过程.....                        | 396        |
| 11.3.4 站点管理.....                            | 400        |
| 11.3.5 站间链路管理.....                          | 401        |
| 11.3.6 DNS 根的管理.....                        | 402        |
| 11.3.7 其他 Windows 2000 服务 .....             | 402        |
| 11.3.8 安全.....                              | 403        |
| 11.4 小结 .....                               | 405        |
| <b>第 12 章 建立一个 Windows 2000 公钥基础结构.....</b> | <b>406</b> |