

 万水计算机技术实用大全系列

Windows Server 2003

深层解决方案

Microsoft Windows Server 2003 INSIDER SOLUTIONS

[美] Rand Morimoto Andrew Abbate Eric Kovach Ed Roberts 著

杜大鹏 岳丽君 杜 墨 李善茂 等 译

杜国梁 陶英华 审 校



中国水利水电出版社
www.waterpub.com.cn

万水计算机技术实用大全系列

Windows Server 2003 深层解决方案

Microsoft Windows Server 2003 INSIDER SOLUTIONS

[美] Rand Morimoto Andrew Abbate Eric Kovach Ed Roberts 著

杜大鹏 岳丽君 杜 墨 李善茂 等译

杜国梁 陶英华 审 校

中国水利水电出版社

内 容 提 要

本书选取了其他书籍忽视的视角, 重点介绍有关 Windows Server 2003 的技巧、窍门、快捷方式和行之有效的经验。

本书内容覆盖 802.11x 无线安全性、智能卡实现、组策略管理、远程管理和高级活动目录设计等方面。书中还包括从 Windows NT4 和 Windows 2000 迁移的技巧和行之有效的经验。本书重点介绍了将 Windows 2003 与 NetWare 和 Unix 集成的关键方法、瘦客户机终端服务、性能调节和优化、服务器可伸缩性和服务器合并、用户文件管理以及其他更多的内容。

本书特别适合已具有 Windows 2003 或 Windows 2000 的基本知识, 而现在特别想了解 Windows 2003 的内幕技巧的网络管理人员。对于正在学习网络课程有志于将来从事网络设计和建设、网络管理与维护工作的在校学生和其他人员也有较高的参考价值。

Authorized translation from the English language edition, entitled MICROSOFT WINDOWS SERVER 2003 INSIDER SOLUTIONS: SHORTCUTS AND BEST PRACTICES, 1st Edition, 0672326094 by MORIMOTO, RAND, published by Pearson Education, Inc, publishing as Que/Sams, Copyright © 2004 by Sams Publishing.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc. CHINESE SIMPLIFIED language edition published by CHINA WATERPOWER PRESS/BEIJING MULTI-CHANNEL ELECTRONIC INFORMATION CO., LTD., Copyright © 2005.

北京市版权局著作权合同登记号: 图字 01-2004-3823

图书在版编目 (CIP) 数据

Windows Server 2003 深层解决方案 / (美) 莫林莫托 (Morimoto, R.) 等著;
杜大鹏等译. —北京: 中国水利水电出版社, 2005

(万水计算机技术实用大全系列)

书名原文: Microsoft Windows Server 2003 Insider Solutions

ISBN 7-5084-2882-X

I. W… II. ①莫…②杜… III. 服务器—操作系统(软件), Windows Server 2003 IV. TP316.86

中国版本图书馆 CIP 数据核字 (2005) 第 044196 号

书 名	Windows Server 2003 深层解决方案
作 者	[美] Rand Morimoto Andrew Abbate Eric Kovach Ed Roberts 著
译 者	杜大鹏 岳丽君 杜 墨 李善茂 等译
审 校	杜国梁 陶英华
出版 发行	中国水利水电出版社 (北京市三里河路 6 号 100044) 网址: www.waterpub.com.cn E-mail: mchannel@263.net (万水) sales@waterpub.com.cn
经 售	电话: (010) 63202266 (总机)、68331835 (营销中心)、82562819 (万水) 全国各地新华书店和相关出版物销售网点
排 版	北京万水电子信息有限公司
印 刷	北京北医印刷厂
规 格	787mm×1092mm 16 开本 32.5 印张 786 千字
版 次	2005 年 7 月第 1 版 2005 年 7 月第 1 次印刷
印 数	0001—5000 册
定 价	48.00 元

凡购买我社图书, 如有缺页、倒页、脱页的, 本社营销中心负责调换

版权所有·侵权必究

译者序

每译一本新书我们都有不同的体会，也同时学到不少知识，除了技术方面的知识外，在英文水平上也要上一个新台阶。

由于受译者的能力与时间的限制，对像 Windows Server 2003 这样容量巨大的操作系统软件，不可能熟悉其每项功能，从而准确地将其翻译出来。同时计算机的某些术语的译法还没有规范可循，在不同的书籍与媒体中也有不同的译法，难以统一。

为了照顾英语不太熟练的读者的需要，我们采用了以下处理方法：

(1) 对于涉及面广，而且在中文中也有比较统一的译法的词语，都尽量使用中文。如 Windows Explorer 就直接写成资源管理器，Active Directory 就以活动目录直呼其名，Registry 现在都称为注册表，我们当然也不会例外。

(2) 一般组件、菜单命令、对话框以及各种选项等，为使用软件时对照方便起见，先给出原文，然后在其后括号内给出中文译文。如 Active Directory User and Computer，在译文中写成 Active Directory User and Computer（活动目录用户与计算机）。

(3) 对于一些极其明显的英语命令、对话框名、选项等就不再标注其汉译，如 Add、Next 等。

本书是多人努力的结晶。本书由杜大鹏、岳丽君、杜墨、李善茂等翻译，其中，杜大鹏翻译了第 I 至第 IV 部分，岳丽君翻译了第 V 至第 VI 两部分，杜墨翻译了第 VII 部分，李善茂翻译了第 VIII 部分，全书由杜国梁、陶英华审校并统稿。参加本书其余工作（录入、打印、校对、联络等）的人还有杜文华、魏永魁、任建畅、梁国珍、魏天超、迟春、刘发来、董明、马相生和杨天华等。在此对这些人对本书所作出的贡献表示感谢。

译者

2005 年 5 月

引 言

在着手编写这本书时，我们就不想把本书只写成另一本安装和迁移的书籍，而是要写成一本有关实现和支持关键的 Windows Server 2003 技术，且 Windows 专家可以从中发现技巧、窍门和有效经验的知识资源的指导性书籍。本书作者从 Windows 2000 代码刚刚锁定时就开始接触 Windows Server 2003（当时的开发代号为 Whistler）了，当时大多数机构才刚有第一次接触 Windows 2000 产品“芳容”的机会。本书作者根据三年多与 Whistler 的早期β版和产品实现的工作经验，向读者提供有助于使 Windows 2003 技术正常发挥作用的资源。一旦有了实现该技术不同方式的机会，读者就可翻阅本书，从中找到成功的现场实现的行之有效的经验。

本书由 8 个部分组成，每一部分都着重于一种核心技术解决方案。每一部分由几章组成。下面列出本书各个部分的内容：

- 第 I 部分：安全性解决方案——本部分着重于关键性的安全性领域，这是对管理人员使系统正常运转面临的最大的挑战。本部分有 3 章讲解保护 Windows Server 2003 环境、与无线环境有关的安全性以及在受保护的访问环境中使用智能卡方面行之有效的经验。
- 第 II 部分：管理与经营解决方案——本部分包括 6 章，专门用来介绍与管理及经营 Windows 2003 环境有关的关键提示、技巧和行之有效的经验。介绍的专题包括分布式管理、管理用户权限和许可、管理桌面以及远程管理 Windows 2003 服务器方面的有效经验。此外，这一部分还介绍组策略，以及发挥组策略对象（Group Policy Objects）、组策略管理控制台和在 Windows 2003 中执行集中管理任务方面的最佳方式。本部分还包括一整章，重点介绍使 Windows 2003 网络环境保持最佳操作状态的每天、每周和每月的维护实践。
- 第 III 部分：设计和实现解决方案——与 Windows 2003 和第二代活动目录一起发布的新工具还有用于规划、实现和管理 Windows 的活动目录。本部分着重介绍在最成功的 Windows 和活动目录设计与实现解决方案中可以学到的内幕解决方案和教训。本部分还包括一章专门介绍有关高级活动目录设计概念、用于实现 Windows 2003 和活动目录的特别提示、技巧以及实现 DNS、DHCP、WINS 和域控制器的有效经验。
- 第 IV 部分：迁移和集成解决方案——向 Windows 2003 和活动目录的迁移，既可以是艰难的也可以是简单的，这依赖于所使用的迁移方法而定。本部分重点介绍 Windows NT 4.0 和 Windows 2000 向 Windows 2003 的迁移以及在 Windows 2003 活动目录环境中集成 UNIX、LDAP 和 Novell Networks 的方法。
- 第 V 部分：远程和移动用户解决方案——重点介绍对环境的移动访问。包括 VPN 访问、与 Windows 2003 的拨号通信、对基于 Windows 2003 资源的 Web 访问以及内建于 Windows 2003 终端服务内的新组件，这些都有助于机构对 Windows 2003 联网环境提供远程和移动访问手段。
- 第 VI 部分：业务连续性解决方案——随着机构对其网络和网络通信系统的依赖性越来越

越强，对具有可恢复性的容错环境的需求变得极其重要。本部分中有一章用来介绍在主要的系统故障发生之前，对注意到的时隐时现的系统问题的主动监测及报警方法。本部分另外一章着重介绍在 Windows 2003 环境中创建容错机制的各种不同方法。

- 第 VII 部分：性能优化解决方案——虽然有些机构将性能优化看做合并服务器和系统的一种方法，但有一些机构却把性能优化看做提高系统操作运转效率的一种方法。本部分既讲述根据调控经验的系统优化，也讲述合并过程，从而减少联网环境中服务器系统的数目。有关存储区域联网设备的章节描述了用户如何对存储的信息提供更好的可伸缩性、冗余性和易管理性。
- 第 VIII 部分：业务效率解决方案——本书的最后部分着重介绍 Windows 2003 中的文件管理、索引和信息查询选项，这些选项可提升 Windows 2003 中的内置技术，从而满足提高业务运转效率的要求。

目 录

译者序
引言

第 I 部分 安全性解决方案

第 1 章 实现 Windows Server 2003 的安全性 2

- 1.1 改善 Windows 2003 的默认安全性 2
 - 1.1.1 对 Windows 2000 的改进 3
 - 1.1.2 Windows 2003 中引入的
新安全技术 3
- 1.2 安全性策划 5
 - 1.2.1 实现传输层安全性 5
 - 1.2.2 要求数字签名 6
 - 1.2.3 使用 PKI (公共密钥基础结构) ... 6
 - 1.2.4 安装证书服务 7
 - 1.2.5 维护物理安全的重要性 8
- 1.3 使用双因素认证来了解谁在连接 9
 - 1.3.1 使用智能卡 9
 - 1.3.2 使用生物方法加强安全性 10
- 1.4 使用模板改善使用和管理 11
 - 1.4.1 使用安全配置和分析工具 11
 - 1.4.2 使用安全模板 11
- 1.5 审核安全配置情况 11
 - 1.5.1 审核系统安全性 12
 - 1.5.2 使用 Microsoft Baseline
Security Analyzer 12
 - 1.5.3 使用漏洞扫描程序 13
 - 1.5.4 审核文件系统 13
- 1.6 实现文件系统的安全性 14
 - 1.6.1 通过 NTFS 锁定文件系统 14
 - 1.6.2 锁定用户组成员 15
 - 1.6.3 使用户处于重要的文件
区域之外 15
- 1.7 实现 Web 服务的安全性 15
 - 1.7.1 使用 SSL 15

- 1.7.2 扫描 Web 服务器中的易受
攻击的漏洞 16
- 1.7.3 跟踪使用最新补丁 16
- 1.7.4 锁定 IIS 17
- 1.8 使用 EFS 维护文件机密 17
 - 1.8.1 使用独立的 EFS 18
 - 1.8.2 加密文件系统实现中的
常见缺陷 18
- 1.9 高级别安全实现方案 19
- 1.10 本章小结 20

第 2 章 配置安全的无线网络 21

- 2.1 穿越性的工作特征 21
- 2.2 管理频谱以避免拒绝服务式攻击 24
 - 2.2.1 选择信道 24
 - 2.2.2 保护自己免受内部干扰 24
 - 2.2.3 保护无线网络 24
- 2.3 实现对安全的 802.1x 技术的支持 25
- 2.4 利用 Windows Server 2003 的安全特性 25
 - 2.4.1 配置无线网络 (IEEE 802.11)
策略 26
 - 2.4.2 选择适当的无线网络策略属性 27
 - 2.4.3 在无线网络安全实现中
使用证书 30
 - 2.4.4 配置证书服务 30
 - 2.4.5 配置因特网认证服务 (IAS) .. 31
 - 2.4.6 配置 EAP-TLS 认证 31
- 2.5 配置无线网络客户 32
- 2.6 通过隧道技术最大化无线网络安全 33
 - 2.6.1 外部网络特点 34
 - 2.6.2 VPN 通道的重要性 34

2.7 无线网络维护技术.....	34	3.3.6 智能卡管理工具	42
2.7.1 对行为、地点和事件进行跟踪...	34	3.3.7 让用户使用智能卡	42
2.7.2 与无线网络相关的 IEEE 标准...	34	3.3.8 提供安全报告	43
2.7.3 其他资源	35	3.4 保护网络访问的技巧和窍门	44
2.8 本章小结	35	3.4.1 使用物理安全性	44
第 3 章 综合使用智能卡技术与安全访问技术	36	3.4.2 使安全性规则简单易行	44
3.1 全面部署证书服务	36	3.4.3 了解自己的行踪	45
3.1.1 使用 Windows Server 2003 的更新功能	36	3.5 创建单一登录环境	45
3.1.2 选择 CA 角色	37	3.5.1 合并目录	45
3.1.3 结合使用智能卡	38	3.5.2 合并应用程序	45
3.2 实现证书服务的安全性	39	3.6 实现 Web 服务器和服务的安全访问 ..	45
3.2.1 锁定服务器	39	3.6.1 锁门	46
3.2.2 分离服务器角色	39	3.6.2 隐藏钥匙	46
3.2.3 委派管理角色	39	3.6.3 需要 SSL	46
3.3 充分利用智能卡	40	3.7 证书服务的灾难恢复	46
3.3.1 选择适当的智能卡	40	3.7.1 建立容错机制	46
3.3.2 内存需求	40	3.7.2 规划备份和恢复	46
3.3.3 智能卡角色	41	3.8 综合使用智能卡与个性化设备	47
3.3.4 智能卡的生命期望值	41	3.8.1 在手持 PC 上使用智能卡	47
3.3.5 智能卡读卡器	42	3.8.2 在智能电话上使用智能卡	48
		3.9 本章小结	48

第 II 部分 管理与经营解决方案

第 4 章 分布式管理	50	4.4.1 Windows 2000 混合域功能级别 ..	57
4.1 选择机构的最佳管理模式	50	4.4.2 Windows 2000 固有的功能级别 ..	57
4.1.1 集中式管理	50	4.4.3 Windows Server 2003 的 中间功能级别	57
4.1.2 分布式管理	51	4.4.4 Windows Server 2003 的功能级别	57
4.1.3 混合管理	51	4.4.5 域管理功能	58
4.1.4 应用管理模型	51	4.4.6 森林管理功能	58
4.2 为最佳委派采用基于角色的管理	51	4.5 执行域和企业管理任务	59
4.2.1 运营主管	52	4.5.1 管理 Domain Admins 组	59
4.2.2 安全管理员	52	4.5.2 管理 Enterprise Admins 组	60
4.2.3 网络管理员	52	4.6 设置影响管理任务的组策略	61
4.2.4 目录服务管理员	53	4.6.1 将组策略与适当的容器链接	61
4.3 使用控制委派向导	53	4.6.2 通过组策略强制使用 复杂的管理员密码	61
4.3.1 通过组织单元进行委派控制	53	4.6.3 限制管理组成员资格	62
4.3.2 委派简单的管理任务	54		
4.3.3 委派自定义任务	54		
4.4 使用功能级别加强管理	56		

4.6.4	用组策略委派权限	63	5.5.2	管理移动用户	82
4.7	测试管理访问权的级别	63	5.5.3	管理管理员使之具有 灵活性和安全性	83
4.7.1	在实验室环境中测试改变	63	5.6	本章小结	83
4.7.2	记载测试过程和结果	64	第 6 章 实现组策略	84	
4.7.3	组策略建模	64	6.1	使用组策略	84
4.7.4	策略结果集 (Resultant Set of Policy, RSoP)	65	6.1.1	设置计算机策略	84
4.8	审核管理活动	65	6.1.2	设置用户策略	84
4.8.1	域控制器上的审核设置	66	6.1.3	理解组策略刷新间隔	84
4.8.2	安全日志的收集和归档	66	6.2	组策略的部署	85
4.8.3	审核账户管理事件	67	6.2.1	以少胜多	85
4.8.4	设置安全日志的适当容量	67	6.2.2	了解策略结果集 (RSoP)	85
4.9	本章小结	67	6.2.3	组策略的继承顺序	85
第 5 章 管理用户权限和许可	68		6.2.4	了解低速链接探测的影响	86
5.1	使用域的本地、全局和通用组	68	6.2.5	委派组策略管理权限	86
5.1.1	选择适当的用户组类型	68	6.2.6	避免跨域的策略指定	86
5.1.2	选择适当的组范围	70	6.2.7	使用组策略命名约定	86
5.2	使用 NTFS 和活动目录集成 的文件共享	71	6.2.8	理解缺省域策略	87
5.2.1	使用 NTFS 设置许可	71	6.3	理解组策略继承和应用顺序	87
5.2.2	设置 NTFS 许可	73	6.3.1	组策略继承	87
5.2.3	使用活动目录集成的共享	73	6.3.2	理解组策略应用的顺序	87
5.2.4	使用允许/拒绝许可	74	6.3.3	修改组策略继承	88
5.2.5	指定用户权限和特权	74	6.3.4	配置组策略回送	89
5.3	使用组策略管理权限和许可	76	6.4	理解低速链接对组策略的影响	89
5.3.1	用组策略指定权限	76	6.4.1	低速链接对站点的影响	89
5.3.2	使用组策略授予对文件 的访问权	77	6.4.2	确定低速链接速度	90
5.3.3	使用组策略授予对注册表 设置的访问权	78	6.4.3	配置惟一的低速链接速度	90
5.3.4	使用组策略管理用户组	79	6.5	使用工具加速组策略应用	90
5.4	使用用户配置文件最大化安全性、 功能并降低总拥有成本	80	6.5.1	链接组策略	90
5.4.1	本地和漫游用户配置文件	80	6.5.2	配置组策略插件	91
5.4.2	所有用户和缺省配置文件	80	6.5.3	禁用配置设置	91
5.4.3	强制性配置文件	81	6.5.4	使用 Show Configured Policies Only (只显示配置后的策略) 设置查看组策略	92
5.4.4	临时配置文件	81	6.5.5	删除孤立组策略	93
5.5	管理特定用户类型的权限和许可	81	6.6	软件安装的自动化	94
5.5.1	管理高度托管的用户	82	6.6.1	软件安装方面行之有效的方法	94
			6.6.2	确定分发是否成功	95
			6.7	使用组策略管理控制台提高易管理性	95

6.7.1 GPO 操作: 备份、恢复、 复制和导入	95	7.1 桌面数据备份自动化	106
6.7.2 迁移表	96	7.2 使用工作站映像加快部署	110
6.7.3 跨森林支持组策略管理	96	7.2.1 无人值守安装	110
6.7.4 HTML 报告功能和 Settings 选项卡	97	7.2.2 使用系统准备工具 (Sysprep) 制作服务器映像	111
6.7.5 链接 WMI 过滤器	97	7.2.3 使用远程安装服务部署 服务器映像	111
6.7.6 在 GPMC 中搜索组策略	97	7.3 创建 Windows XP 映像	112
6.8 在 GPMC 中使用策略的结果集	97	7.3.1 安装桌面软件	113
6.8.1 使用策略的结果集为组 策略建模	98	7.3.2 标准化桌面	113
6.8.2 使用 RSOP 的日志模式查看 应用的策略	98	7.3.3 几件小事	113
6.9 使用组策略最大化安全性	98	7.4 软件安装自动化	113
6.9.1 预定义的安全模板	98	7.5 低速链接探测	115
6.9.2 所需的缺省域组策略设置	99	7.6 保护安全管理配置	115
6.9.3 受限组: 通过组策略 指定本地组	99	7.6.1 通过安全补丁减少易受 攻击的漏洞	115
6.10 使用 Intellimirror 增加容错功能	100	7.6.2 在桌面上最大化安全性	116
6.10.1 使用文件夹重定向	100	7.7 管理系统和配置	118
6.10.2 使用漫游配置文件	101	7.7.1 远程管理桌面	118
6.11 使用其他有用工具管理组策略	101	7.7.2 管理多用户桌面	118
6.11.1 使用 GPupdate 工具	101	7.7.3 管理移动计算机	119
6.11.2 使用 GPreult 工具	102	7.7.4 管理公共或信息亭工作站	120
6.11.3 使用 GPmonitor.exe 工具	102	7.7.5 管理管理员工作站	121
6.11.4 使用 GPOTool 工具	102	7.8 使用有效工具管理桌面	122
6.11.5 使用 FRSDiag.exe 工具	102	7.8.1 Flopplock	122
6.11.6 使用 Sonar.exe 工具	103	7.8.2 Netdom	122
6.12 使用管理模板	103	7.8.3 Con2prt	122
6.12.1 理解策略与优选项的区别	104	7.8.4 用户状态迁移工具 (USMT)	123
6.12.2 使用 Microsoft 的附加组 策略模板	104	7.9 本章小结	123
6.12.3 自定义管理组策略模板	104	第 8 章 远程管理 Windows Server 2003	124
6.13 寻找有关组策略的附加资源	104	8.1 使用远程桌面管理	124
6.13.1 Microsoft 有关组策略 技术的 Web 站点	105	8.1.1 使用远程桌面连接加强 远程管理	124
6.13.2 组策略白皮书	105	8.1.2 启用远程桌面管理	125
6.14 本章小结	105	8.1.3 用于远程桌面管理的 行之有效的经验	126
第 7 章 管理桌面	106	8.2 利用 Windows Server 2003 的管理工具	127
		8.2.1 安装管理工具包	127

8.2.2 使用方便的控制台	128	9.3.6 检查 DHCP 范围.....	145
8.2.3 自定义管理控制台	129	9.4 每月的任务	145
8.3 使用带外远程管理工具处理 应急情况.....	129	9.4.1 活动目录数据库完整性检查 ..	145
8.3.1 应急管理服务	130	9.4.2 执行 Scandisk.....	145
8.3.2 为 EMS 配置串行连接	130	9.4.3 重新引导系统	146
8.3.3 特殊管理控制台	131	9.4.4 对系统的碎片整理	146
8.4 使用及配置远程协助	132	9.4.5 检查 WINS 是否损坏	146
8.4.1 远程协助的需求	132	9.5 将合并服务器作为维护任务	146
8.4.2 发送远程协助邀请	133	9.5.1 Windows 系统资源管理器	146
8.5 保护和监测远程管理	135	9.5.2 虚拟服务器	147
8.5.1 保护远程管理	135	9.6 备份技巧和窍门	147
8.5.2 监测远程管理	135	9.6.1 利用专用的备份 VLAN 改善性能	147
8.6 远程管理的委派	136	9.6.2 缓存到磁盘然后再保存到磁带 ..	148
8.7 在 Windows Server 2003 中远程管理 IIS	136	9.6.3 祖、父、子策略和换带机	148
8.7.1 使用 IIS 管理器	137	9.6.4 使用合适的代理软件	149
8.7.2 使用终端服务	137	9.6.5 备份中应包括和排除什么	149
8.7.3 使用远程管理 (HTML) 工具 ..	138	9.7 使用自动系统还原	150
8.8 本章小结	139	9.8 在维护实践中使用脚本	151
第 9 章 维护实践和过程	140	9.8.1 使用命令行界面	152
9.1 维护不如实现新技术那样有趣	140	9.8.2 自定义 MMC 视图	153
9.2 每天需要进行的工作	140	9.8.3 确保与检查表的一致性	153
9.2.1 查看日志	140	9.9 为什么 5 个 9 还不是好事	153
9.2.2 检查系统资源	140	9.9.1 维护时间的重要性	154
9.2.3 确认备份	141	9.9.2 高可用性环境中的维护	154
9.3 每星期的任务	142	9.10 更新的自动化	155
9.3.1 检查系统更新	142	9.10.1 调节软件更新服务: 使用 NTFS 许可和机器组	155
9.3.2 确认活动目录复制	144	9.10.2 与 Systems Management Server 一起使用 SUS	155
9.3.3 审核管理组成员资格	144	9.10.3 使用组策略启用 SUS	155
9.3.4 执行试验恢复	144	9.11 本章小结	156
9.3.5 检查活动目录数据库的大小 ..	144		

第 III 部分 设计和实现解决方案

第 10 章 高级活动目录设计	158	10.1.4 合并域	160
10.1 或大或小的实现	158	10.1.5 理解多森林	161
10.1.1 单域就地升级	158	10.1.6 使用占位式根域	161
10.1.2 多域——子域	159	10.2 配置与重新配置域和组织单元	162
10.1.3 多域——不连续的	160	10.2.1 在域间移动对象	162

10.2.2 在组织单元间移动对象	163	11.2.1 提供产品序列号	180
10.3 站点和新的知识一致性检查器	163	11.2.2 选择许可模式	180
10.3.1 汇总站点	164	11.2.3 激活 Windows Server 2003	181
10.3.2 站点“收养”	164	11.3 用远程安装服务自动化部署	182
10.3.3 使用 DNS 控制站点认证	165	11.3.1 RIS 的系统需求	182
10.4 有效使用跨森林信任	165	11.3.2 创建远程安装准备向导 (RIPrep) 映像	183
10.4.1 账户/资源森林	167	11.3.3 保护服务器映像	185
10.4.2 公司收购	167	11.3.4 充分利用 RIS 部署工具	185
10.5 森林间的同步	167	11.4 使用 Sysprep 保持服务器的 最大一致性	186
10.5.1 使用 GALSync 使目录同步 ..	168	11.4.1 Sysprep 如何工作	186
10.5.2 Microsoft 的身份信息服务	168	11.4.2 利用新的 Sysprep 特性	187
10.6 使用活动目录迁移工具的 行之有效的经验	168	11.5 使用 Unattend.txt 和安装管理器 的自定义安装	187
10.6.1 使用 ADMT 迁移资源	168	11.5.1 使用安装管理器的加强功能 ...	187
10.6.2 SID 历史记录的含义	169	11.5.2 使用 Unattend.txt 的完全 自动化安装	188
10.6.3 清除 SID 历史记录	169	11.6 创建快速部署的自定义 可引导光盘	188
10.6.4 ADMT 2.0 中的改进	169	11.6.1 创建自定义安装光盘 所需的工具	189
10.7 有效使用 Microsoft 元目录服务	169	11.6.2 使用 WinPE	189
10.8 域控制器的放置	171	11.7 优化标准服务器配置	189
10.8.1 从 Windows NT 4.0 迁移的 复制流与认证流的对比	171	11.7.1 最佳性能设置	189
10.8.2 确定本地域控制器的价值	172	11.7.2 优化安全设置	191
10.8.3 在 WAN 连接性上投资与 在域控制器上投资的对比	172	11.7.3 开始例行操作	191
10.9 全局编录的放置	172	11.8 使用设置向导自定义服务器	191
10.9.1 全局编录的作用	172	11.8.1 配置服务器角色	192
10.9.2 GC 复制流量与查找 流量的对比	172	11.8.2 管理服务器	193
10.9.3 确定全局编录故障的影响	173	11.9 使用 Windows 注册表控制基础	193
10.10 复制改善带来的好处	174	11.9.1 注册表编辑器	193
10.11 活动目录功能级别	174	11.9.2 保护注册表	193
10.12 本章小结	175	11.9.3 维护注册表	194
第 11 章 实现 Microsoft Windows Server 2003	177	11.10 本章小结	194
11.1 成功部署服务器的行之有效的经验 ..	177	第 12 章 实现 Microsoft 的活动目录	195
11.1.1 规划部署	177	12.1 利用功能级别	195
11.1.2 测试部署	178	12.1.1 Windows 2000 混合域 功能级别	195
11.1.3 执行部署	179		
11.2 序列号和激活 Windows Server 2003..	180		

12.1.2	Windows 2000 固有功能级别 ..	195	13.1.3	使用活动目录集成管理 地址信息	215
12.1.3	Windows Server 2003 的过渡功能级别	195	13.1.4	Windows Server 2003 中网络服务的变化	215
12.1.4	Windows Server 2003 功能级别	196	13.2	活动目录环境中的 DNS	217
12.2	改善域控制器的安装	196	13.2.1	DNS 对活动目录的影响	217
12.2.1	提升成员服务器	196	13.2.2	在非 Microsoft DNS 实现中的活动目录	217
12.2.2	使域控制器降级	197	13.2.3	在活动目录环境中使用 辅助区域	218
12.2.3	根据介质创建副本	198	13.2.4	在 DNS 中指定 SRV 记录 和站点解析	218
12.3	充分利用全局编录服务器	199	13.3	域名系统 (DNS) 的深入讨论	219
12.3.1	全局编录的放置	199	13.3.1	对 DNS 的需求	219
12.3.2	通用组缓存	200	13.3.2	DNS 框架	220
12.3.3	自定义全局编录	201	13.3.3	理解 DNS 的命名空间	220
12.4	最大化操作主机角色	202	13.4	使用配置服务器向导安装 DNS	220
12.4.1	正确放置操作主机角色	202	13.5	配置 DNS 指向自身	223
12.4.2	转移操作主机角色	203	13.6	在 Windows 2003 环境中使用 资源记录	223
12.5	通过森林和域间互连扩展企业	204	13.6.1	DNS 中的 Start of Authority (SOA)记录	224
12.5.1	建立跨森林信任	205	13.6.2	DNS Host (A)记录	224
12.5.2	授予跨森林权限	206	13.6.3	Name Server (NS)记录	225
12.5.3	认证防火墙	206	13.6.4	增加 DNS 信息的 Service (SRV)记录	225
12.6	增加域更名的灵活性	207	13.6.5	定义电子邮件传送的 Mail Exchanger (MX)记录	226
12.6.1	理解限制	207	13.6.6	用于反向 DNS 查询的 Pointer (PTR)记录	226
12.6.2	满足先决条件	208	13.6.7	用于别名信息的 Canonical Name (CNAME)记录	226
12.6.3	为域更名的过程	208	13.6.8	保存信息的其他 DNS 记录 ..	226
12.7	管理活动目录架构	209	13.7	建立并实现 DNS 区域	227
12.7.1	使用活动目录服务界面 编辑工具	210	13.7.1	正向查找区域	227
12.7.2	使用活动目录架构插件	210	13.7.2	反向查找区域	228
12.7.3	架构失活	211	13.7.3	主区域	228
12.8	使用应用程序分区改善复制	212	13.7.4	辅区域	228
12.8.1	创建应用程序分区	212	13.7.5	占位区域	229
12.8.2	创建一个副本	212			
12.8.3	管理复制	213			
12.9	本章小结	213			
第 13 章	建立牢固的基础设施	214			
13.1	聚焦 Windows Server 2003 的基础设施组成	214			
13.1.1	作为设施基础的网络寻址 ..	214			
13.1.2	使用名称解析简化地址查找 ..	214			

13.8 在 DNS 中创建区域转移	230	13.16.1 用于 DHCP 容错的 50/50 故障恢复方法	246
13.8.1 完全区域转移	231	13.16.2 用于 DHCP 容错的 80/20 故障恢复方法	247
13.8.2 增量区域转移 (IXFR)	231	13.16.3 用于 DHCP 容错的 100/100 故障恢复方法	247
13.9 理解 DNS 查询的重要性	232	13.16.4 备用范围方法	248
13.9.1 递归查询	232	13.16.5 DHCP 服务器集群	248
13.9.2 迭代查询	232	13.17 高级 DHCP 概念	249
13.10 其他 DNS 组件	233	13.17.1 DHCP 的超级范围	249
13.10.1 动态 DNS (DDNS)	233	13.17.2 DHCP 多点广播范围	249
13.10.2 存活期 (TTL)	233	13.17.3 DHCP 管理委派	249
13.10.3 源更新	234	13.17.4 NetSh 命令行实用工具	250
13.11 DNS 的维护、更新和清除	234	13.18 通过适当维护优化 DHCP	250
13.11.1 根提示	235	13.19 保护 DHCP 实现	251
13.11.2 转发器	235	13.19.1 DHCP 授权	251
13.11.3 使用 WINS 查找	236	13.19.2 DHCP 和域控制器的安全性	252
13.12 DNS 的故障诊断	237	13.20 继续使用 Windows 因特网命名服务	252
13.12.1 使用 DNS 事件查看器 诊断问题	237	13.20.1 传统的 Microsoft NetBIOS 解析方案	252
13.12.2 使用性能监视器监视 DNS	237	13.20.2 集成 WINS 和 DNS	253
13.12.3 客户端缓存和 HOST 解析问题	237	13.20.3 Windows Server 2003 WINS 中的变化	254
13.12.4 使用 NSLOOKUP 命令行实用工具	238	13.21 安装并配置 WINS	254
13.12.5 使用 IPCONFIG 命令行工具	238	13.21.1 安装 WINS	254
13.12.6 使用 TRACERT 命令行工具	239	13.21.2 配置推/拉伙伴	255
13.12.7 使用 DNSCMD 命令行工具	239	13.21.3 WINS 复制	255
13.13 深入讨论动态主机配置 协议 (DHCP)	240	13.21.4 NetBIOS 客户解析和 LMHOSTS 文件	256
13.13.1 DHCP 客户服务	240	13.22 WINS 规划、迁移和维护	256
13.13.2 自动的专有 IP 编址 (APIPA)	240	13.22.1 设计 WINS 环境	256
13.13.3 DHCP 中继代理	241	13.22.2 升级 WINS 环境	257
13.13.4 DHCP 和动态 DNS	242	13.22.3 WINS 数据库维护	258
13.14 Windows Server 2003 中 DHCP 的变化	242	13.23 全局编录域控制器 (GC/DC) 的放置	258
13.14.1 DHCP 数据库备份和 恢复的自动化	242	13.24 战略性放置 GC 和 DC 的需求	259
13.14.2 Windows XP 客户中的 DHCP	243	13.24.1 通用组缓存	259
13.15 安装 DHCP 并创建新有效范围	244	13.24.2 全局编录/域控制器放置	260
13.16 创建 DHCP 冗余	245	13.25 本章小结	260

第 IV 部分 迁移和集成解决方案

第 14 章 从 Windows NT 4.0 迁移.....262

14.1 向可伸缩的 Windows 2003 Server

环境迁移 262

14.1.1 规划将来的硬件需求 262

14.1.2 使用系统兼容性检查器 263

14.1.3 支持第三方软件 263

14.1.4 使用兼容性工具箱分析器 264

14.1.5 向灵活的活动目录森林迁移 .. 264

14.2 撤消和故障恢复..... 265

14.2.1 恢复 SAM 数据库的简单方法.. 265

14.2.2 从失败的账户迁移中还原 266

14.3 使网络停工时间最短的技巧 266

14.3.1 通过服务器冗余避免停机 266

14.3.2 配置冗余的全局编录 267

14.4 在迁移时规划并实现域名解析 267

14.4.1 理解 Windows 2003

的域名解析 268

14.4.2 在混合模式环境中实现 WINS . 268

14.4.3 安装 WINS..... 268

14.4.4 使 Windows 2003 的

WINS 退役 269

14.5 规划并升级文件系统与磁盘分区 ... 270

14.5.1 镜像卷 270

14.5.2 卷集、条带卷集和带奇偶

校验的条带卷集 270

14.6 在服务器升级期间避免失败和中断.. 271

14.6.1 规划出故障的硬件 271

14.6.2 Windows NT 的升级路径

和服务包 271

14.7 使 Windows 服务器跟上

Windows Updates 的步伐 272

14.8 利用 Windows Update

完成服务器升级..... 272

14.9 在并存期间支持 Windows 客户 273

14.9.1 域认证的负载平衡 273

14.9.2 在 Windows 2003 域

控制器上配置 PDC 模拟器... 273

14.9.3 支持 Windows 95、98

和 NT 4.0 客户系统 274

14.10 实现并保护密码迁移 275

14.11 在迁移桌面时发现权限问题 277

14.11.1 了解桌面迁移要求 278

14.11.2 本地桌面权限 278

14.11.3 配置桌面权限的提示 278

14.11.4 创建桌面迁移账户 278

14.11.5 配置多个桌面权限的提示... 278

14.11.6 利用域管理员组 278

14.11.7 使用 Net Add User 命令..... 279

14.12 维护及管理并存的行之

有效的经验 279

14.12.1 合并网络服务 279

14.12.2 使用 SID 历史记录保持

对资源的访问权 279

14.12.3 迁移 SID 历史记录..... 280

14.12.4 迁移并存的附加工具 280

14.13 域和服务器退役时常见的错误 280

14.13.1 Windows NT 4.0 域

服务器的退役 281

14.13.2 迁移时区分服务器的

角色顺序 281

14.13.3 删除许可 281

14.13.4 使用活动目录系统

编辑器 ADSI..... 282

14.14 本章小结 282

第 15 章 从 Windows 2000 迁移..... 283

15.1 准备迁移..... 283

15.1.1 准备要迁移的 Windows 2000

服务器 283

15.1.2 考虑活动目录硬件需求 285

15.1.3 计划升级类型 288

15.2 Windows Server 2003 应用程序

兼容性 288

15.3 使用应用程序兼容性工具箱 288

15.4 升级并安装 Windows Server 2003... 289

15.4.1	升级路径和要求	289	16.3.1	LDAP 与活动目录集成	307
15.4.2	执行干净安装而升级	290	16.3.2	使用元目录集成	310
15.4.3	升级 Windows 2000 域的技巧	291	16.4	使用密码同步	311
15.5	迁移网络服务	292	16.4.1	在 UNIX 和 NIS 中同步密码	311
15.5.1	迁移网络服务	292	16.4.2	同步 LDAP 中的密码	313
15.5.2	迁移域名系统服务	292	16.5	跨平台资源的集中管理	314
15.5.3	向 Windows 2003 迁移 DHCP	293	16.5.1	使用 Telnet 管理 UNIX 和 Windows	314
15.5.4	迁移 GPO	294	16.5.2	使用 Microsoft 管理控制台 (MMC)	314
15.6	迁移活动目录对象	294	16.5.3	配置 Active Directory Schema 插件	314
15.6.1	迁移安全性和分布组	295	16.6	基于 Windows 平台访问 UNIX	316
15.6.2	迁移用户账户	296	16.6.1	访问文件服务	316
15.7	故障恢复的行之有效的办法	297	16.6.2	在 UNIX 上访问打印机服务	318
15.7.1	备份活动目录	297	16.7	基于 UNIX 平台访问 Windows	319
15.7.2	从失败的升级中还原	297	16.7.1	使用 Telnet 访问 Windows	319
15.7.3	计划并避免网络停工	298	16.7.2	访问 Windows 文件服务	320
15.8	用 Windows Server 2003 支持客户	299	16.7.3	访问 Windows 打印服务	320
15.8.1	理解 Windows 2003 的客户兼容性	299	16.7.4	使用 LPD/LPR	321
15.8.2	启用传统客户支持	300	16.8	从一个平台向另一平台迁移资源	322
15.9	使 Windows 2000 退役	301	16.8.1	安置目录服务	322
15.9.1	使 Windows 2000 域和 域控制器退役	301	16.8.2	合并文件共享	322
15.9.2	使域成员服务器退役	301	16.8.3	合并打印机	322
15.9.3	在迁移期间区分服务器 角色的先后次序	301	16.9	本章小结	322
15.9.4	使用 ADSI 编辑器删除 服务器	302	第 17 章	Windows 2003 与 Novell Networks 的集成	323
15.10	提高 Windows 2003 功能级别	302	17.1	利用 Services for NetWare	323
15.10.1	域功能级别	302	17.1.1	使用 Gateway Services for NetWare 来桥接环境	323
15.10.2	提高功能级别	303	17.1.2	使用 File and Print Services for NetWare 替换服务器	324
15.11	本章小结	303	17.1.3	使用 Microsoft Directory Synchronization Service 集成目录	324
第 16 章	与基于 UNIX/LDAP 的系统集成	304	17.1.4	文件迁移实用工具 (FMU)	325
16.1	设计并规划平台集成	304	17.2	桥接 Novell 和 Windows 网络的方法	325
16.1.1	清点	304	17.2.1	使用双客户方法访问 多平台环境	325
16.1.2	创建集成/迁移计划	304			
16.2	创建集成的基础设施	305			
16.2.1	现共同的基础	305			
16.2.2	集成域名服务 (DNS)	306			
16.3	在不同环境之间集成目录	307			

17.2.2	在 Novell 环境中利用 Windows 的终端服务.....	326	17.4.2	同步目录作为共享登录方法....	330
17.2.3	使用 Web 服务来访问 Microsoft 技术	327	17.5	使 eDirectory/NDS 与活动目录同步 ...	330
17.3	安装 Microsoft Services for NetWare 工具	327	17.5.1	实现 MSDSS 的行之 有效的经验	331
17.3.1	准备 Services for NetWare 的基本配置	327	17.5.2	鉴别目录同步的限制	332
17.3.2	安装 File and Print Services for NetWare	328	17.5.3	备份和恢复 MSDSS 信息	332
17.3.3	安装 Microsoft 目录同步服务..	329	17.6	用 Windows 服务器替换 NetWare 服务器	333
17.4	创建单一登录环境.....	330	17.6.1	使 Windows 服务器模拟 Novell NetWare 服务器.....	333
17.4.1	双客户认证访问方法的 有效性	330	17.6.2	桥接 Novell 和 Microsoft 网络环境	334
			17.6.3	使用文件迁移向导来迁移文件	335
			17.7	本章小结	337

第 V 部分 远程和移动用户解决方案

第 18 章 VPN 和拨号解决方案 339

18.1	选择正确的 VPN 解决方案	339
18.1.1	Windows 2003 的路由 和远程访问服务	339
18.1.2	考察基于防火墙的 VPN	340
18.1.3	考察基于硬件的 VPN	340
18.1.4	确定何时从软件改变到硬件 ..	340
18.2	保护 L2TP 的行之有效的经验	341
18.2.1	与防火墙一起使用 L2TP	342
18.2.2	与防火墙串接使用 L2TP	342
18.2.3	L2TP 客户需求	343
18.2.4	利用远程接入策略	343
18.3	保护 PPTP 的行之有效的经验	344
18.3.1	与防火墙并行使用 PPTP	344
18.3.2	与防火墙串接使用 PPTP	345
18.3.3	PPTP 客户需求	345
18.3.4	利用远程接入策略	346
18.4	利用因特网认证服务	346
18.4.1	使用终端服务访问 IAS 服务器	347
18.4.2	使用 IPSec 加密保密数据	347
18.5	使用无线 VPN	348
18.6	部署 VPN 和拨号服务	348

18.6.1	利用 Microsoft 的连接 管理器	349
18.6.2	利用软调制解调器	351
18.6.3	将线路与较大电路合并	351
18.6.4	利用 RADIUS	351
18.6.5	使用 GPO 管理远程用户	353
18.7	使用站点到站点的 VPN	353
18.8	使用负载均衡增加伸缩性和弹性 ...	355
18.9	本章小结	355

第 19 章 使用 Web 访问 Windows

Server 2003 资源	357
19.1 向因特网公布 Web 共享的 行之有效的经验	357
19.1.1 保护边界	357
19.1.2 保护服务器内容	358
19.1.3 跟随 HTTP 认证请求	358
19.1.4 允许受信任网络	358
19.1.5 创建虚拟目录	359
19.1.6 设定虚拟目录权限	360
19.1.7 选择适当的用户访问控制	361
19.2 使用 SSL 保护对资源的访问	362
19.3 在 Web 服务器目录上启用 SSL	362
19.4 启用并保护因特网打印	365