HZ BOOKS

Windows 2000 Server Architecture and Planning, 2nd Edition

Windows 技术丛书

Windows 2000 Server

(美) Morten Strunge Nielsen 著
汪洲 刘砚 龚建 等译

Windows 2000 Server 体系结构与规划

机械工业出版社 China Machine Press
CORIOLIS

Windows 技术丛书

Windows 2000 Server 体系结构与规划

（美） Morten Strunge Nielsen 著

汪 洲 刘 砚 龚 建 等译

机械工业出版社
China Machine Press

本书完全涵盖了 Windows 2000 的主要特征，同时还提供了许多有关设计的实例、指导和警告。另外，本书还对如何从 Windows NT 迁移到 Windows 2000，如何同 Exchange Server 5.5、Exchange 2000 Server 和当前其他应用程序集成，以及如何同将来的集成活动目录应用程序集成进行了精深的探讨。

本书内容全面、深入浅出，从设计和计划的角度为读者全面理解 Windows 2000 提供了指导。

本书版权登记号：图字：01 - 2001 - 3943

图书在版编目（CIP）数据

Windows 2000 Server 体系结构与规划/（美）尼尔森（Nielsen, M.S.）著；汪洲等译 . - 北京：机械工业出版社，2002.1

（Windows 技术丛书）

书名原文：Windows 2000 Server Architecture and Planning, 2nd Edition

ISBN 7 - 111 - 09485 - 9

Ⅰ.W… Ⅱ.①尼…②汪… Ⅲ.服务器 - 操作系统（软件），Windows 2000 Server Ⅳ.TP316.86

中国版本图书馆 CIP 数据核字（2001）第 078851 号

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）

责任编辑：王高翔 张鸿斌

北京忠信诚印刷厂印刷·新华书店北京发行所发行

2002 年 1 月第 1 版第 1 次印刷

787mm × 1092mm 1/16·41.25 印张

印数：0 001 - 4 000 册

定价：68.00 元

译 者 序

Windows 2000 不仅代表了 Microsoft 最新和最主要的为了商业应用而开发的 Windows 平台，它还代表了 Microsoft 欲在其上建构未来所有 Windows 版本的平台，而这对于 Microsoft 是否能够在新的时期保持它在桌面操作系统的根据地是至关重要的。

任何有 Windows NT 工作经验的人都会从本书提供的信息中获益。但请不要误会，这本书在主观上是为计算机专业人员而写的。IT 战略家、IT 规划师、IT 设计师以及有 Windows NT 工作知识的管理员——或者想获取这些知识的人——都将会从本书得到最大收益。

如果你想成为一名 Microsoft 认证系统工程师（MCSE），这本书能够使你受益，因为它涵盖了 Microsoft 认证专业考试“设计 Microsoft Windows 2000 目录服务基础结构”（70－219）和“从 Microsoft Windows NT 4.0 升级到 Microsoft Windows 2000”（70－222）的全部教程。

本书的权威性和专业水准对你学习 Windows 2000 架构以及参加认证考试是一个极大的激励。当我们拿到这本书的时候，并没有马上就动手翻译，而是首先全面地浏览了一下本书的内容。为什么呢？因为它的独到之处——对主题的详尽、全面、透彻的讲解。每部分都就某个专题进行详细讨论，紧紧把握知识重点；本书提供大量适合于教学方法的材料，使你能够较快地掌握所学的知识，同时能够加强实践。现在，我们很荣幸能够有机会承担本书的翻译工作，并且抱着认真的态度将这本书的中文版奉献给你，希望你能够从本书中有所收获，这是作者的初衷，也是我们良好的愿望！

本书由汪洲、刘砚、龚建组织翻译，万方工作室的全体同仁参加了本书的校正、输入等工作。其他具体参加本书翻译、录排、校对工作的人员有：张雅升、曹燕惠、强秀丽、韩存兵、龚志翔、龚超、尹建军、刘今朝、强秀丽、任宇飞、李红玲、白红利、金荣学、薛彪、叶哲、邓海燕、邢倩、王育红、李军、刘彬、钱斌、赵锁、姜南、李智、田韫、李林、张巧莉、陈曙晖、邓波、邓涛、李卓林、聂宛析、田敏、龚露娜、马军、马丽、田军、田野、田蕴哲、王小将、李素丽、天海鹏等。龚波同志对全书进行了认真的审核。本书的出版是集体劳动的结晶，在此特别感谢万方工作室的全体工作人员。

由于时间仓促，且译者经验和水平有限，译文难免有不妥之处，恳请读者批评指正！我们的联系方式网址是 wf _ studio@sina. com。

万方工作室

2001 年 8 月

前　言

并非仅是革命

你没有必要成为 Micsosoft 网页的热心冲浪者，或是了解 Windows 2000 Server 的技术爱好者。但是，Microsoft 和大部分 IT 新闻评论关于 Windows 2000 是 Windows NT 技术的革命性进步的声明决不是浅薄的促销言论。

Windows 2000 Server 对于你将是一次革命性的体验，如果你能充分发掘它的活动目录特性。而且，如历史所证明的那样，你想保持从容就不能只是接纳些许的革命性思想，无论在今天的和平环境里还是在你的工作中都是一样。

为什么活动目录如此重要

如果你习惯于工作在 Windows NT Server 类型的域中，目录服务确实会颠覆你的世界——而且肯定要花费你大量的时间来使事情各归本位。

但是你所有的努力将会有收获，因为你为你的团体为目录服务的未来做了准备。实际上，自从 X.500、NDS 和 Exchange Server 起，未来就开始向着目录服务的方向演进了。我仍然觉得当 Novell 的 NDS 在 1993 年发布时，人人都可以称其为一次计算的突破。只有一样宝贵的东西在 Novell 的目录服务中失落了：来自相当比例的客户、独立软件供应商（ISV）和硬件制造商的明确支持。

目录服务的全部意义在于方便各种各样公司的应用程序与平台的管理和集成。不幸的是，Novell 从未设法说服主要的应用程序开发商和操作系统供应商在他们的产品中建立必要的 NDS 链接，只有那样才能使整个目录服务的理念生辉。

我充满信心，因为我相信活动目录——还有 Windows 2000 Server ——将取得比你当前从销售数字中看到的更大的成功。Microsoft 稳固地控制着客户平台，它与如此众多的应用程序开发商和硬件组件厂商紧密结合，以至在未来几年内对活动目录非常广泛的支持将会进一步发展。正如来自第三方的支持被证明是 Novell 关于 NDS 的惨败之源，它也将被证明是 Windows 2000 成功的基石。

所以，请不要简单地看待我将在第 3 章介绍的目录服务的概念。实际上，更容易的用户管理只是目录服务众多好处之一。我十分肯定当目前占有重要百分比的 NT Server 4 安装向 Windows 2000 Server 迁移后，我们都会惊异于目录服务的力量和潜能。

知识很重要，但经验更重要

现在机会很好，你只是缺乏关于活动目录的知识和经验，正如我开始着手实现我第一个基于目录服务的大型网络时一样。当时我已经阅读了大量关于 Novell 的 NDS 及目录服务的一般性

资料，但是无一能让我真正为实际问题做好准备。

不论你对于 Windows NT Server 多么有经验，你都会如我曾经所处的情形那样感到被遗弃，因为你的 NT 经验并不适用于活动目录。如果你的部分环境仍然运行于 NT 4 之上，你现有的 NT 技能将有助于进行过渡。实际上，从当前的 NT 环境向活动目录迁移时，惟一有用的是来自你从 Exchange（或 Novell 的 NDS，或 Banyan 的 StreetTalk）获得的经验。即便如此，用于 Exchange Server 5.5 的技能集仍与活动目录所需的相距甚远。

因此，请接受一个人的经验之谈。首先在开始进入目录服务的世界之前，你需要理解活动目录，并获取你所能够得到的有关目录服务的所有经验。第二步，不能低估实践它的时间和复杂性，——这是 Windows 2000 Server 相对缓慢的起步，以及你应该从现在就开始而不要花上好几年来完成的原因。

我强烈地建议现在就对活动目录进行规划。当你进入到规划阶段，可能有必要在 IT 组织内实行一些相当巨大的调整或变动。从一开始就从事并解决这些问题是明智的，因为以后不会变得更容易。通过确信今天开始所做的决策都已经把活动目录基础考虑在内，你可能会避免一些最糟糕的由迁移所带来的不利情况，并得到目录服务为你的公司带来的所有回报。

实现时间预估

基于我以前对于目录服务的经验以及一些关于活动目录的工作，我估计一个中型团体（即有 1000 到 5000 客户）将花 4～9 个月的时间来培训、测试、验证和开始向活动目录迁移。一个大型团体将不得不花费至少 9 个月的时间，而且很可能是 12～18 个月的时间来完成同样的工作。当然，如果该团体非常易于模拟，并且所需的公司知识及技术都已准备好，就能够更快地完成这些工作。但是，以我对大型 IT 基础结构项目的经验来判断，由于内部冲突、有限的 IT 部门资源、缺乏活动目录技能等原因，这个迁移项目可能需要更长时间来完成。

从本书中最大限度地获益

任何有 Windows NT 工作经验的人都会从本书提供的信息中获益。但请不要误会，这本书尽管在主观上是为计算机专业人员而写的，但 IT 战略家、IT 规划师、IT 设计师以及有 Windows NT 工作知识的管理员，或者想获取这些知识的人，都将会从本书得到最大收益。

如果你想成为一名 Microsoft 认证系统工程师（MCSE），这本书能够有助于使你得到最大回报，因为它涵盖了 Microsoft 认证专业考试“设计 Microsoft Windows 2000 目录服务基础结构”（70－219）和“从 Microsoft Windows NT 4.0 升级到 Microsoft Windows 2000”（70－222）的全部教程。

注意 通过 MCP 考试 70－219 和 70－222 的相应课程为“设计 Microsoft Windows 2000 目录服务基础结构”（MOC 1561）和“设计 Microsoft Windows 2000 升级策略”（MOC 2010）。

然而，你应当理解本书主旨是为你提供一切安全通过活动目录设计和规划的理论和实际经验。因此，通过认真学习本书你就会在考试中取得较好的成绩。但是你最好对本书辅以相应的

Exam Crams，因为 Microsoft 经常不时地更新 MCP 考试——而 Exam Crams 能使你了解确切的教程，来面对大量可能出现的问题。

还有，本书实际上超出了那两门考试教程的范围，它们加起来共有五个课程日——是本书提供的与考试相关的基础信息。由于所有小的细节看起来操作性太强而不能被课程所包括，所以不需要了解本书的每个小细节你就可以通过这两项考试。

但是我愿意强调的是，留心贯穿本书所提的建议，这样会使你做得更好。因为这些建议是基于我将活动目录解决方案应用到实际的经验，而且当你以后需要将你自己的活动目录知识付诸实践时，它会显得特别有用。正如任何 MCP 都会知道的那样：通过考试是一回事，但成功设计和实现一个复杂架构方案却是另一回事。

理解本书

本书的目的是从设计和远景规划的观点出发，使你对 Microsoft Windows 2000 Server 有全面彻底的理解。其含意是：实质上我将深入探究的一切都是从活动目录的视角出发。

本书分为五部分：

- 第一部分："概览"——第 1 章和第 2 章给出所有 Windows 2000（从 Professional 到 Datacenter Server 的全部版本）的主要功能与特性的纲要，以及一些与 Windows 2000 相关的市场背景。
- 第二部分："规划"——第 3 章到第 13 章开始对 Windows 2000 Server 新的活动目录特性进行十分详尽的讨论，那些想要理解 Windows 2000 Server 体系架构精彩之处的读者会对此感兴趣。
- 第三部分："高级设计专题"——第 14 章到第 16 章包括对高级规划任务的讨论，比起其他人，企业规划师和安全专家对此可能会更感兴趣。
- 第四部分："测试"——第 17 章到第 20 章对于为了测试的目的安装 Windows 2000 Server 和实现活动目录提供一个引导。相信我：你一定想看第 20 章，因为其中包括了许多关于在各种情况下如何优化你的设计的建议。
- 第五部分："适应当前基础结构"——第 21 章到第 23 章（包括附录 B）的内容是关于目前如何规划 Windows 2000 Server、与 Windows 2000 Server 集成，以及全面或部分向 Windows 2000 迁移的高级讨论。此部分以一个附录作为结束，描述了 Windows 2000 Server迁移项目的基础。

引导你学习本书

正如我已经指出的那样，本书开始的两章阐述了 Windows 2000 所导入市场的概括性观点。第 1 章集中在市场态势，目前及未来的几年中这将被证明对于 Windows 2000 Server 和所有 IT 专业人员具有极大的重要性。第 2 章对 Windows 2000 Server 的所有功能与特性提供了一个全面的介绍。

在此之后，你将接触到本书核心内容的"导论"。尽管第 6 章到第 12 章真正构成本书的核心，并提供给你所有关于活动目录精彩细节的一切信息，可是第 3 章到第 5 章对于获得活动目

录的全面认识，进而随着对目录主要属性的规划深化，其价值是无法估量的。第 3 章给出了一般性的目录服务介绍；第 4 章和第 5 章将开始介绍活动目录的关键特性和构件。

提示： 如果你对活动目录已经入门就可以略过第 3 章到第 5 章，因为这些章只是为了在你进入各领域学习之前为你提供概略的认识。还有，你可能会注意到第 4 章和第 5 章读起来有一些难度：它们是活动目录的速成课程，所以不要不阅读这两章的内容。在此之后一切都会好起来（也更容易理解）。

通过第 6 章，你会获得与活动目录相关的“真实”的规划技能。第 6 章分析了活动目录的组织和物理设置，这对于实现任何成功的目录服务来说都是活力的源泉。

第 7 章讲述 DDNS 和 DHCP（和 WINS），它们是活动目录运转的重要先决条件。事实上我不得不还要和只有 PC 背景的人打交道，在 DNS 领域这是绝对的，这使得本章变得相当庞大。第 8 章是关于域结构（包括组织单元和管理授权）的规划；第 9 章把用户账户和组的规划推向实践。第 10 章深入探讨了新的管理授权和组策略特性。第 11 章重点集中于超过一个域以上（即包括若干域或域树的目录）的目录的规划。第 12 章着眼于物理基础结构的规划，这将确保活动目录不会在网络上运行失控。整个活动目录的“基础”规划部分以第 13 章收尾，其中提供了来自规划阶段不同部分的最重要课程和最佳实践的简短回顾。

第 14 章进一步研究许多新的安全特性和所面临的挑战，包括了对活动目录安全性、Kerberos、IPSEC、EFS 和证书服务（Certificat Services）的讨论。

第 15 章提供了怎样把 Exchange Server 5.5 集成到活动目录的信息——以及怎样由此过渡到 Exchange 2000 Server。

第 16 章提出了对于支持活动目录的应用程序问题的见解。尽管关于这个重要的问题可以讲解更多的内容，但本章将以你为核心来深入研究你的企业自身的重要应用程序。

此时你已进入了测试阶段。第 17 章对于安装 Windows 2000 Server 以及通过 OU（组织单元）和最通用的对象实现单一的活动目录域提供了必要的信息。而在第 18 章中，你将获得一些关于最实用的“高级”活动目录话题的速成教程，如创建站点、实现组策略和管理授权等等。

在第 19 章中你将学会怎样规划、准备和最终更改目录架构。第 20 章将讲授如何访问在活动目录环境中生成的数据库大小和复制负载，以及对于任何的 LAN 或 WAN 如何优化活动目录。

最后三章（第 21 章到第 23 章）集中于怎样使活动目录适应现有的架构。第 21 章论述了针对 Windows 2000 Server 和活动目录，怎样实现新的平台方案。第 22 章对于如何从当前的 NT Server 平台向活动目录迁移给出了详尽的说明。

第 23 章给出了与当今最流行的遗留服务器平台和客户平台短期或长期共存的几种可能性，特别强调了 DNS 和其他网络问题。

最后，附录 A 向你提供 Windows 2000 Server/活动目录的预规划、设计、原型、构造、测试和实现的项目规划纲要。附录 B 为你展现了一些真实的有教育性的活动目录设计案例，希望为你的设计增加一点灵感。附录 C 对下一版的 Windows 2000 Server —— Whistler 版做了极短的说明。

我已经有这本书了：有什么新内容吗？

实际上本书是第 2 版，这意味着我已经更正了原书中的一些细小的错误和疏漏的地方。而且我还更新了一些从 Windows 2000 beta 版到 Windows 2000 最终版（包括 Service Pack 1）已改变了的内容。

但这些并不是全部：本书还包含了大量新素材，其中很多都是基于我对活动目录的实践经验，大部分已经被收集到现有的章节中。而这决非装点门面，新的素料使本书比原来厚了三分之一。

为了使得一切购买了本书第 1 版的人更加容易阅读，以下是第 2 版《Windows 2000 Server 体系结构与规划》中的主要变动和新增内容的纲要：

第 7 章——为了正确实施 DNS 结构，本章包括了更多的实用的建议（包括关于如何处理集成活动目录的 DDNS 和 WINS 的信息）。

第 9 章和第 10 章——从以前的第 9 章扩展而来，提供了关于 Windows 2000 Server 安全基础的更多信息和关于组策略的更多规划和实践建议。

第 12 章——给出了关于相当重要的文件复制服务（File Replication Service，FRS）的更多信息，增加了分布式文件系统（Distributed File System，DFS）一节，通过对在实践中非常重要细节的敏锐观察，更加深入地讨论了活动目录复制。

第 14 章——新增的一章，向你提供关于所有 Windows 2000 Server 引入的高级安全选项（如 Kerberos、PKI、EFS 和 IPSEC）的深入研究。

第 15 章——新增的一章，向你提供如何与 Exchange 5.5 集成的所需信息，以及向 Exchange 2000 Server 迁移的重要性。

第 16 章——新增的一章，提供了由实现活动目录的应用程序而引起的几种可能情况的处理方法。这包括对 Microsoft 元目录服务（Microsoft Metadirectory Services，MMS）的探究，它注定在未来的几年中将成为 Windows 2000 不可或缺的一部分。

第 20 章——集中增进你对 Windows 2000 网络行为的理解，是新颖而独特的一章，其中包含了大量对缺省设置进行改进的建议。

第 22 章——包含了许多关于从 Windows NT Server 向 Windows 2000 Server 迁移的新信息。包括对可以从 Microsoft 免费获取的非常重要的活动目录迁移工具（Active Directory Migration Tool，ADMT）的深入研究。

第 23 章——包括关于迁移和与非 Microsoft 环境——特别是 Unix 和 Novell 共存的新信息。

附录 B——新增的附录，提供一些为大小各异的公司进行活动目录设计的非常有趣的实例。

附录 C——当向下一版 Windows 2000 Server（即 Whistler 版）前进时，希望对活动目录进行哪些类型变化的简单预览。

随着在研究深度以及广度上的大幅度提高，我相信这本书将成为设计和规划 Windows 2000 Server 的“圣经”，而且同样相信，许多人可能不会再找到其他能与本书相媲美的书。好了，说得够多的。让我们从本书开始学习吧。

结束语

如果你在本书中遇到了任何错误或缺点，请告知我。可以通过 morten@strunge.com 联系我。一些相关信息存在于 www.strunge.com。

对于所有在座的人来说，我希望你们能够享受阅读此书的乐趣，正如我（通常）在写作时一样。

Morten Strunge Nielsen

2000 年 12 月 3 日

目　录

译者序
前言

第一部分　概　览

第 1 章　市场概览 …… 1
1.1　Microsoft 无处不在 …… 1
1.2　NT 与 Windows 9x 对比 …… 2
1.3　面向高端的 Windows 2000 Server …… 5
1.4　追求新的商业机遇 …… 6
1.4.1　个人数字助理 …… 7
1.4.2　瘦客户 …… 7
1.4.3　集成电视 …… 8
1.5　理解新的 Microsoft 思想：数字神经系统 … 8
1.6　一切都导向 Windows 2000 Server …… 10
第 2 章　Windows 2000 概述 …… 11
2.1　Windows 2000 是一个庞大的新版本 …… 11
2.1.1　Windows 2000 Server 的文件、打印和 Web 服务 …… 12
2.1.2　Windows 2000 Server 的应用程序、基础结构和通信服务 …… 13
2.1.3　Windows 2000 Professional …… 14
2.1.4　理解 Windows 2000 …… 15
2.1.5　第一项革命：活动目录 …… 19
2.1.6　第二项革命：Microsoft 管理控制台 … 21
2.1.7　第三项革命：减轻桌面负担的 IntelliMirror 和其他技术 …… 23
2.1.8　第四项革命：真正的安全性 …… 26
2.1.9　第五项革命：为分布式未来做准备 …… 26
2.1.10　获得正确的观点 …… 28

第二部分　规　划

第 3 章　目录服务导论 …… 29
3.1　目录服务由什么组成 …… 29
3.1.1　为什么需要目录服务 …… 30
3.1.2　X.500 是共同的根基 …… 34
3.1.3　了解 LDAP …… 35
3.2　当今的目录服务 …… 37
3.2.1　NDS …… 38
3.2.2　活动目录 …… 39
3.2.3　逐渐发展的目录服务 …… 40
第 4 章　理解活动目录 …… 42
4.1　进入活动目录 …… 42
4.2　基本的目录服务定义 …… 43
4.2.1　对象和属性 …… 43
4.2.2　容器 …… 43
4.2.3　树 …… 43
4.2.4　名称空间 …… 44
4.2.5　命名上下文和分区 …… 44
4.2.6　名称 …… 45
4.2.7　名称解析 …… 46
4.3　域：目录的逻辑分区 …… 46
4.3.1　树 …… 47
4.3.2　森林 …… 47
4.4　组织单元——域的逻辑分区 …… 49
4.5　全局编目：活动目录的另一重要特点 …… 49
4.6　域控制器和站点：目录的物理部分 …… 50
4.6.1　域控制器 …… 50
4.6.2　站点 …… 51
4.7　关键的活动目录特性 …… 52
4.7.1　DNS 集成 …… 52
4.7.2　Kerberos 安全 …… 52
4.7.3　访问活动目录 …… 53
4.7.4　复制 …… 53
4.8　活动目录怎样适应 Windows 2000 Server 的体系结构 …… 54

4.9 活动目录摘要 …… 57
第5章 活动目录的关键概念 …… 59
5.1 域和组织单元 …… 59
5.1.1 域 …… 59
5.1.2 组织单元 …… 59
5.2 树和森林 …… 60
5.2.1 树 …… 60
5.2.2 森林 …… 61
5.2.3 比较树和森林 …… 62
5.3 把重要块集中在一起 …… 62
5.4 DNS 和 LDAP …… 66
5.4.1 动态 DNS …… 66
5.4.2 轻型目录访问协议 …… 67
5.5 全局编目 …… 68
5.6 物理方面：站点和 DC …… 69
5.7 关于复制的讨论 …… 72
5.8 活动目录名称类型和命名规范 …… 74
5.9 活动目录的逻辑结构单元 …… 76
5.10 活动目录安全特征 …… 77
5.10.1 对象保护 …… 77
5.10.2 授权 …… 77
5.10.3 继承 …… 78
5.10.4 信任关系 …… 78
5.11 继续 …… 78
第6章 确定组织的目录设置 …… 81
6.1 有关规划组的几个问题 …… 81
6.2 确定组织的特点 …… 82
6.2.1 确认组织的模型 …… 84
6.2.2 确定组织结构 …… 86
6.2.3 组织的图表 …… 90
6.2.4 确定地理的结构 …… 90
6.2.5 规划组织的变化 …… 91
6.2.6 确定安全需求 …… 92
6.2.7 分析企业网络基础结构 …… 92
6.3 你的需求及原因 …… 96
6.4 继续 …… 96
第7章 决定 DNS 的结构 …… 98
7.1 活动目录设置中的一个 DNS 例子 …… 98
7.2 从 WINS 到 DDNS …… 100
7.2.1 介绍域名系统 …… 101
7.2.2 理解 DNS …… 102
7.2.3 DNS Server …… 108
7.2.4 标准资源记录格式 …… 111
7.2.5 DNS 名称的注册和解析 …… 114
7.3 熟悉 DDNS 和其他 DNS 新特征 …… 115
7.3.1 讨论 DDNS …… 117
7.3.2 讨论 DNS－NOTIFY …… 118
7.3.3 讨论增量区域传输 …… 118
7.3.4 讨论 SRV RR …… 118
7.3.5 掌握集成活动目录的 DDNS …… 120
7.3.6 HDCP 集成和 WINS 互操作性 …… 122
7.4 设计 DNS …… 125
7.4.1 选择 DNS Server …… 125
7.4.2 如何选择 DNS 名 …… 131
7.4.3 聚焦组织的根域 …… 132
7.4.4 在内部和外部根名间选择 …… 134
7.4.5 聚焦 DNS 区域和复制 …… 137
7.4.6 WINS：类似“鸡肋”——几点建议 …… 139
7.5 设计 DNS 的推荐步骤 …… 140
7.6 开展业务 …… 142
第8章 规划域结构 …… 143
8.1 坚持 KISS …… 143
8.2 建立一个域 …… 145
8.3 OU 基本知识 …… 147
8.4 OU 概念的总结 …… 148
8.4.1 分配管理权 …… 149
8.4.2 替换资源域 …… 150
8.4.3 应用策略 …… 150
8.4.4 对象分组 …… 151
8.5 OU 与域 …… 151
8.6 设计 OU 结构 …… 153
8.7 典型的 OU 模型 …… 153
8.7.1 基于地域的 OU 模型 …… 154
8.7.2 基于部门的 OU 模型 …… 155
8.7.3 基于业务单元的 OU 模型 …… 155
8.7.4 基于项目的 OU 模型 …… 155

8.7.5 基于管理的 OU 模型 …… 156
8.7.6 基于对象的 OU 模型 …… 156
8.8 规划 OU 结构 …… 156
8.8.1 考虑实现哪种 OU 对象 …… 159
8.8.2 决定 OU 结构每一层应该是什么样 …… 160
8.8.3 决定 OU 的命名规范 …… 161
8.8.4 规划委托 OU 管理权 …… 161
8.9 关于 OU 设计的一些建议 …… 162
8.9.1 第一层 …… 162
8.9.2 第二层 …… 163
8.9.3 其他层 …… 163
8.10 OU 设计的例子 …… 163
8.10.1 一个小组织的例子 …… 163
8.10.2 一个州政府的例子 …… 164
8.10.3 一个国际性企业的例子 …… 165
8.11 最好的实践经验 …… 166
8.12 总结 …… 168
第 9 章 规划用户和组管理方式 …… 169
9.1 用户账号管理简介 …… 169
9.2 用户账号 …… 174
9.2.1 何时超出域的范围 …… 179
9.2.2 其他用户账号选项 …… 180
9.3 组账号介绍 …… 181
9.3.1 掌握组 …… 183
9.3.2 其他组的新特征 …… 185
9.3.3 组范围概述 …… 186
9.3.4 理解域模式和组 …… 187
9.4 缺省组 …… 187
9.4.1 内置组 …… 188
9.4.2 预定义组 …… 191
9.4.3 理解缺省组 …… 192
9.4.4 特殊组 …… 193
9.4.5 可信任域组 …… 195
9.4.6 用户权限 …… 195
9.5 组策略 …… 199
9.6 最好的实践经验 …… 205
9.7 简述用户和组 …… 206
第 10 章 规划组策略和管理委托 …… 208
10.1 管理委托 …… 208
10.2 理解组策略 …… 211
10.3 深入探讨组策略 …… 216
10.3.1 软件设置——软件安装 …… 219
10.3.2 Windows 设置——安全设置 …… 220
10.3.3 Windows 设置——文件夹重定向 …… 222
10.3.4 Windows 设置——脚本 …… 222
10.3.5 管理模板 …… 222
10.4 开始做计划 …… 223
10.5 管理范围 …… 224
10.5.1 分层设计与整体设计 …… 224
10.5.2 单一策略类型的设计与多策略类型的设计 …… 225
10.5.3 功能角色与协同设计 …… 226
10.5.4 集中式或分布式控制 OU 委托 …… 229
10.5.5 更实际的问题 …… 229
10.6 性能优化 …… 232
10.7 管理优化 …… 233
10.8 最好的实践经验 …… 234
10.9 组策略小结 …… 236
第 11 章 规划域树和森林 …… 237
11.1 使用单个域 …… 237
11.2 介绍域树和森林 …… 238
11.2.1 域树说明 …… 239
11.2.2 森林说明 …… 240
11.3 准备好了么——好了 …… 240
11.4 开始设计域结构 …… 243
11.5 确定组织所需要的域数量 …… 245
11.5.1 设法满足单个域 …… 245
11.5.2 决定添加更多的域 …… 245
11.5.3 安排域树中的域 …… 246
11.5.4 安排森林中的域 …… 247
11.5.5 创建其他森林 …… 248
11.6 定义域名称空间 …… 248
11.6.1 根 …… 249
11.6.2 第一层 …… 249
11.6.3 第二层 …… 250
11.6.4 第三层及其他 …… 251

11.7 域设计举例 …… 252
11.7.1 单个域解决方案 …… 252
11.7.2 域树解决方案 …… 253
11.7.3 森林解决方案 …… 253
11.8 最好的实践经验 …… 254
11.9 总结 …… 255
第 12 章 物理结构规划 …… 257
12.1 介绍 DC、GC 和站点 …… 257
12.1.1 域控制器 …… 257
12.1.2 全局编目 …… 258
12.1.3 站点 …… 258
12.2 深入研究复制 …… 260
12.2.1 站点内部复制 …… 261
12.2.2 站点之间复制 …… 261
12.3 如何进行复制 …… 262
12.3.1 确定要复制的改动：更新传播 …… 262
12.3.2 防止不必要的复制：循环传播 …… 265
12.3.3 解决更新冲突：冲突检测 …… 266
12.3.4 多主机复制的一个小例外：FSMO …… 271
12.3.5 另一个例外：紧急复制触发器 …… 272
12.4 深入研究 DC 和 GC …… 273
12.4.1 理解 DC …… 274
12.4.2 理解 GC …… 275
12.5 深入研究站点 …… 278
12.5.1 站点的定义 …… 278
12.5.2 站点的含义 …… 280
12.5.3 深入研究站点内部的选项 …… 280
12.5.4 深入研究站点之间的选项 …… 283
12.5.5 选择复制拓扑 …… 287
12.6 不要忽略时间服务 …… 288
12.7 其他复制拓扑：DFS 和 FRS …… 291
12.7.1 感受 FRS …… 291
12.7.2 不要忽视 DFS 特征 …… 295
12.8 如何设计物理属性 …… 298
12.8.1 站点设计简介 …… 298
12.8.2 检查位置 …… 299
12.8.3 确定连通性及可用带宽 …… 299
12.8.4 设立站点结构 …… 299
12.8.5 确定站点属性 …… 301
12.8.6 决定放置 DC 和 GC 的地点 …… 303
12.8.7 放置 FSMO …… 304
12.8.8 优化不同场景 …… 305
12.8.9 优化 DFS 复制拓扑 …… 308
12.8.10 一些例子 …… 309
12.9 最好的实践经验 …… 312
12.10 总结 …… 314
第 13 章 结果评定 …… 315
13.1 理解目录服务 …… 315
13.2 了解活动目录 …… 317
13.3 核心活动目录概念 …… 318
13.3.1 动态 DNS …… 318
13.3.2 域 …… 319
13.3.3 组织单元 …… 319
13.3.4 域树和森林 …… 321
13.3.5 组 …… 322
13.3.6 域控制器 …… 323
13.3.7 站点 …… 323
13.3.8 全局编目 …… 324
13.4 规划：从误解到清楚 …… 325
13.5 规划活动目录逻辑结构 …… 326
13.6 规划活动目录物理结构 …… 331
13.7 不要忘记安全 …… 333
13.8 总结 …… 334

第三部分 高级设计专题

第 14 章 高级安全主题 …… 337
14.1 安全基础结构的基本原理 …… 337
14.1.1 SSPI …… 338
14.1.2 CryptoAPI …… 339
14.2 基本验证系统：Kerberos …… 342
14.2.1 工作原理 …… 344
14.2.2 Kerberos 是如何安全保护本地区域的 …… 345
14.2.3 Kerberos 是如何安全保护全局区域的 …… 346
14.2.4 人无完人 …… 348
14.3 两种选择：PKI 和智能卡 …… 348
14.3.1 了解公共密钥加密 …… 349

14.3.2 PKI 里是什么 …… 350
14.4 网络层安全：IPSEC …… 353
14.4.1 使用 IPSEC …… 354
14.4.2 IPSEC 选项 …… 355
14.4.3 IPSEC 内幕 …… 357
14.5 磁盘层安全：EFS …… 357
14.6 实现安全 …… 360
14.6.1 了解安全配置工具包 …… 360
14.6.2 理解安全模板 …… 362
14.6.3 使用安全模板 …… 362
14.6.4 如何配置和分析安全设置 …… 365
14.7 一种有很少缺陷的真正伟大的解决方案 …… 365
第 15 章 如何设计 Exchange Server …… 367
15.1 Exchange Server 互操作 …… 367
15.1.1 从 Windows NT Server 移植到 Windows 2000 Server …… 368
15.1.2 保持目录同步 …… 369
15.2 Exchange 2000 Server 介绍 …… 382
15.2.1 活动目录的美好前景 …… 382
15.2.2 几点综述 …… 384
15.2.3 新增的主要目录对象 …… 384
15.3 升级到 Exchange 2000 Server …… 385
15.3.1 Exchange 2000 Server 设计 …… 386
15.3.2 迁移到 Exchange 2000 Server …… 387
15.4 最好的实践经验 …… 389
15.5 这就是 Exchange …… 391
第 16 章 如何设计支持活动目录的应用程序 …… 393
16.1 什么是集成 …… 393
16.1.1 服务连接点 …… 394
16.1.2 使用现有目录对象 …… 395
16.1.3 服务主体名 …… 396
16.1.4 单次登录 …… 397
16.1.5 全部或部分目录集成 …… 398
16.2 当前情况 …… 398
16.3 通用集成 …… 400
16.3.1 MMS 简介 …… 401
16.3.2 MMS 基本原理 …… 402
16.4 这仅仅（希望）是开始 …… 404

第四部分 测 试

第 17 章 实现活动目录 …… 407
17.1 安装 Windows 2000 Server …… 407
17.1.1 选择合适的文件系统 …… 409
17.1.2 为活动目录准备服务器 …… 412
17.1.3 安装活动目录 DC …… 416
17.1.4 完成 DNS 的最后细节工作 …… 425
17.1.5 使用集成活动目录的 DNS …… 429
17.1.6 完成活动目录的最后细节 …… 431
17.1.7 管理活动目录 …… 433
17.2 到目前为止一切顺利 …… 443
第 18 章 高级活动目录实现专题 …… 444
18.1 高级选项 …… 444
18.2 为管理授权和策略创建 OU …… 445
18.2.1 管理授权 …… 446
18.2.2 组策略 …… 449
18.3 创建站点并定义复制属性 …… 453
18.3.1 创建子网和站点 …… 453
18.3.2 创建复制拓扑结构 …… 455
18.3.3 将 DC 转换成 GC …… 460
18.4 使用 Windows 2000 Server 进行灾难预防 …… 460
18.4.1 容错卷 …… 460
18.4.2 备份活动目录 …… 464
18.5 关键域和森林属性的使用 …… 466
18.5.1 改变域运行模式 …… 468
18.5.2 管理 UPN 后缀 …… 468
18.5.3 FSMO 介绍 …… 469
18.6 主要的活动目录工具 …… 471
18.6.1 ADSI 编辑器 …… 472
18.6.2 CLONEPR …… 473
18.6.3 DCDIAG …… 473
18.6.4 DSACLS …… 473
18.6.5 DSASTAT …… 473
18.6.6 活动目录管理工具 …… 473
18.6.7 活动目录对象管理器 …… 474
18.6.8 网络连通性测试器 …… 475

18.6.9 Windows 2000 域管理器 …… 475
18.6.10 NLTEST …… 475
18.6.11 NTDSUTIL …… 476
18.6.12 复制诊断工具 …… 476
18.6.13 活动目录复制监视器 …… 477
18.6.14 安全管理工具 …… 478
18.7 杂货袋 …… 478
第 19 章 模式管理 …… 480
19.1 模式概览 …… 480
19.2 最重要的活动目录对象类 …… 482
19.2.1 用于选择的大量对象 …… 482
19.2.2 类定义对象 …… 484
19.2.3 属性定义对象 …… 486
19.3 何时修改模式 …… 488
19.3.1 决定如何修改模式 …… 489
19.3.2 如何处理模式修改 …… 489
19.4 修改模式 …… 490
19.4.1 移去安全互锁以修改模式 …… 491
19.4.2 添加类 …… 492
19.4.3 修改类 …… 494
19.4.4 添加属性 …… 495
19.4.5 修改属性 …… 496
19.4.6 对模式添加和修改进行系统检查 …… 500
19.4.7 与修改模式相关的问题 …… 501
19.5 如何进行大量数据输入 …… 503
19.5.1 导出和导入目录信息的命令行工具 …… 503
19.5.2 处理活动目录大量数据的简单方法 …… 504
19.6 最好的实践经验 …… 508
19.7 对模式更新保持冷静 …… 508
第 20 章 估计活动目录大小的艺术 …… 511
20.1 活动目录技术内幕 …… 511
20.1.1 认识数据表 …… 512
20.1.2 理解数据库的工作原理 …… 513
20.2 活动目录数据库大小估计和优化 …… 517
20.2.1 自己进行测试以确定数据库大小 …… 517
20.2.2 体验数据库大小 …… 517
20.2.3 单一对象加载 …… 518
20.2.4 团体方案加载 …… 521
20.3 活动目录的复制负载 …… 522
20.3.1 站点内 DC 复制 …… 523
20.3.2 站点内 GC 复制 …… 525
20.3.3 站点间 DC 复制 …… 525
20.3.4 站点间 GC 复制 …… 526
20.4 理解和优化网络行为 …… 527
20.4.1 客户登录情况 …… 527
20.4.2 服务器复制 …… 529
20.4.3 减轻 WAN 的网络负载 …… 531
20.4.4 注意慢速 WAN …… 535
20.4.5 提高 DC/GC 的性能：给网络增加更重的负载 …… 536
20.5 最好的实践经验 …… 537
20.6 总结 …… 539

第五部分 适应当前基础结构

第 21 章 使用活动目录实现 NT Server 4 …… 541
21.1 设计 NT Server 4 解决方案的重要建议 …… 542
21.2 枯燥的 TCP/IP 细节 …… 543
21.2.1 DHCP、WINS 和 DNS 简介 …… 543
21.2.2 客户机和服务器 …… 545
21.3 选择域模式 …… 548
21.4 关键的组和用户学习课程 …… 549
21.5 Exchange Server …… 550
21.6 最好的实践经验 …… 551
21.7 总结 …… 551
第 22 章 迁移到活动目录 …… 553
22.1 纵观升级 …… 553
22.2 预计划：检查当前的 NT Server 结构 …… 554
22.3 决定如何迁移 NT 域 …… 555
22.3.1 理解 clean - sheet 方式 …… 556
22.3.2 理解现场方式 …… 557
22.3.3 单域模式 …… 559
22.3.4 单主控域模式 …… 559

22.3.5 多主控域模式 …… 560
22.3.6 完全信任模式： …… 562
22.3.7 了解你的工具 …… 563
22.4 制定恢复计划 …… 564
22.5 决定何时迁移到本地模式 …… 566
22.6 迁移及域合并基础 …… 567
22.6.1 关于森林之间的迁移 …… 568
22.6.2 关于森林内部的迁移和域合并 …… 569
22.7 掌握工具 …… 570
22.7.1 Active Directory Migration Tool …… 571
22.7.2 ClonePrincipal …… 573
22.7.3 MoveTree …… 573
22.7.4 NetDom …… 574
22.7.5 SIDWalker …… 574
22.8 Clean－sheet 方式的迁移 …… 574
22.9 现场方式的升级 …… 575
22.9.1 决定如何形成活动目录域 …… 575
22.9.2 决定如何升级 DC …… 576
22.9.3 域的重建和合并 …… 581
22.10 最好的实践经验 …… 584
22.11 实施一个真正的升级 …… 584
第 23 章 非微软环境的迁移和共存 …… 586
23.1 理解微软集成策略 …… 586
23.2 第一个目标：提供单次登录 …… 588
23.2.1 使用 Kerberos 协议实现 SSO …… 590
23.2.2 使用公共密钥的 SSO …… 592
23.2.3 通过 Host Integration Server 实现 SSO …… 593
23.3 第二个目标：提供更紧密的集成 …… 594
23.4 事件的当前状态 …… 596
23.4.1 Novell NetWare 互操作和迁移 …… 596
23.4.2 Unix 的互操作和迁移 …… 600
23.4.3 其他流行操作系统的互操作和迁移 …… 605
23.4.4 主机系统互操作性 …… 606
23.5 迄今为止的迁移和共存 …… 608

附 录

附录 A Windows 2000 Server 项目实施指南 …… 611
附录 B 活动目录设计案例 …… 626
附录 C Whistler：Windows 的下一个版本 …… 640