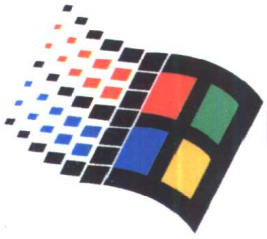

Windows 2000 用户管理

（美）Lori M.Sanders 著
齐舒创作室 译

机械工业出版社
China Machine Press

Windows 2000 用户管理

（美） Lori M.Sanders 著
齐舒创作室 译
毅 弘 审校

机 械 工 业 出 版 社

本书旨在给 Windows 2000 系统管理员提供综合的实际指导，使他们可以高效而可靠地对用户和桌面资源进行管理。书中介绍了 Windows 2000 为用户和资源管理所提供的新功能，详细地阐述了 Active Directory、域模型和安全性机制；讨论了用户管理的各个方面，包括用户的创建、工具、从其它目录结构的迁移、组和高效使用组的规划。最后，讨论了用户环境的管理，介绍了配置、组策略对象以及 Microsoft 成组并作为 IntelliMirror 营销的功能。本书适合于专门从事 Windows 2000 系统管理的用户使用。

本书版权登记号：图字：01－2000－1416

图书在版编目(CIP)数据

Windows 2000 用户管理/(美) 桑德(Sanders, L. M)著/齐舒创作室译. －北京：机械工业出版社，2000
ISBN 7－111－08658－9

Ⅰ. W… Ⅱ. ①桑…②齐… Ⅲ. 窗口软件，Windows 2000－系统管理 Ⅳ. TP316.7

中国版本图书馆 CIP 数据核字(2000)第 82578 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)
责任编辑：何文军 封面设计：姚毅
北京市密云县印刷厂印刷·新华书店北京发行所发行
2001 年 2 月第 1 版第 1 次印刷
797mm × 1092mm $^{1}/_{16}$ · 10.5 印张 · 257 千字
印数：5 000册
定价：18.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话(010)68993821、68326677－2527

引　言

本书的目的是提供一个综合的实际指导，来利用 Windows 2000 管理用户和他们的桌面环境。本书分为 3 个部分。第 1 部分概览 Windows 2000 为用户和资源管理所提供的新能力，以及可利用的 Active Directory、域模型和安全性机制。第 2 部分将阐述用户管理的所有方面：用户的创建、大多数工具、从其它目录结构的迁移、组和高效使用组的规划。第 3 部分讨论用户环境的管理，为此使用配置、组策略对象以及 Microsoft 成组并作为 IntelliMirror 营销的功能，如 Offline Files、Remote Operating System Installation(ROSI)服务和 Application Deployment。

随着 Windows 2000 的出现，在管理用户和管理用户的环境及桌面之间很难划一条清楚的界限。这是本书把这两个议题组合在一起的一个原因。现在，很难确定一个主题在哪里停止，下一个主题从哪里开始。这种困难在这个概要的框架中得到了反映。例如，现在难以准确地知道应该把有关组策略的章节放在哪里，因为有些功能明显地落在用户管理议题下，而其它功能同样清楚地是面向环境的。

第 1 部分　Windows 2000 基础

这个部分的主要内容是为了使读者能从本书后几部分得到最大的收益而必须掌握的背景知识。本部分将从对 Windows 2000 新特征的讨论开始，因为这些特征与用户和桌面管理有关。接着，对 Active Directory 体系结构组件、安全性机制、域模型和混合与本机模式操作。域的崩溃问题将从另一个角度来解决，以使用 Organizational Units(OUs)演示管理代表的内在益处。

第 2 部分　管理用户和组

在这个部分中，给读者提供了一个按步指导，以便使用不同的工具集在 Active Directory 中或本地机器 SAM 上创建用户和组。这里将讨论使用 User Interface(UI)和 Active Directory Services Interface(ADSI)脚本编程从头开始创建用户和组，同时，还将讨论用于从数据库、电子表格、早先的 NT 版本和 NetWare 环境加载用户的工具。这个部分将利用许多背景资源和脚本编程例子。

本部分将引导读者了解现存的组，规划创建新的安全性和发布产品，以及高效地使用组。将被包含在组相关章节中的其它议题是深层次的组嵌套、底层客户、混合模式操作以及多域树中的标记爆炸等问题。与其中每个议题相关联的问题也将予以考察。利用一个情节演示组的最高效的设计来在最大程度上减少企业重复通信信息，并以这个演示来结束本部分内容的学习。

第 3 部分　环境管理

本部分将阐述一个管理员可以在 Windows 2000 中用于管理用户和他们的日常计算环境的所有技术。讨论使用配置管理用户的桌面和可以利用的配置类型。本部分中的第 8 章将涉及组策略对象及它们可以在用户和环境管理方面所扮演角色的议题。每种类型的策略对象都被

予以详细讨论，同时还将讨论策略的传播和可以在域树中对它进行过滤的方式。第 9 章学习处理客户管理的剩余 IntelliMirror 组件，例如 Offline Files 和 ROSI 服务。

本书目的

本书的主要目标是打开读者的视野，让读者看到利用 Windows 2000 管理用户和环境的新的可能性，并让读者对那些可能性感兴趣。

笔者假设，本书的大多数读者都将是管理员（不是程序员）。在此基础上，将广泛地使用战争故事和真实的例子来理解正在讲述的要点。需要情节时，将使用单一的虚构组织。这种策略给读者在整个书的内容中提供了连续性，笔者感到，设法掌握新概念时，这是有好处的。例如，读者在设法学习 ADSI 脚本编程基础的同时，不必设法解释一个新的情节和命名约定。这种方法与前面提到的真实经历结合起来，以便读者从本书的学习中得到最大的收益。

此外，还假设读者将相当熟悉 Microsoft 环境的管理。因此，与人们可能会在针对新的 NT 管理员的文本中找到的内容相比，这里的说明层次稍微更加抽象一些。假设读者熟悉可在 NT 4 环境中利用的服务和掌握用于在 Windows 2000 中实现 Active Directory 结构的 TCP/IP 概念所需要的网络操作必备知识。

笔者尽力使本书内容清晰而简单。介绍产品的一些新接口和特征时，将使用屏幕快照引导读者理解更迟钝的界面。这个产品为管理性任务和用户任务都广泛地利用了向导（Wizard）。所以，一旦管理员开始使用 Windows 2000，就可以很快地完成许多内容的学习。当界面直观，但概念或服务是新的时，与在屏幕快照上花费的时间相比，笔者在理论和背景方面花费了更多的时间。笔者已经教过很多人使用了这个产品的 Beta 和预览版本，认为对管理员将在哪里存在问题有了一种体会。

译 者 序

随着 Windows 2000 的出现，该操作系统的多用户特征和网络能力得到了进一步的增强。用户和系统的管理水平直接关系着能否有效地发挥该操作系统的潜力。对用户管理问题的解决也影响着系统的使用效率和使用安全性。所以，作为一个管理员，必须深入探讨用户管理的内涵，掌握用户管理的技巧。

本书给 Windows 2000 系统管理员提供了一个综合的实际指导，使他们可以高效而可靠地对用户和桌面资源进行管理。书中介绍了 Windows 2000 为用户和资源管理所提供的新功能，详细地阐述了 Active Directory、域模型和安全性机制；讨论了用户管理的各个方面，包括用户的创建、工具、从其它目录结构的迁移、组和高效使用组的规划。最后，讨论了用户环境的管理，介绍了配置、组策略对象以及 Microsoft 成组并作为 IntelliMirror 营销的功能。本书适合于专门从事 Windows 2000 系统管理的用户使用。

本书是齐舒创作室集体劳动的结晶，参加本书翻译的还有吴杨、刘延、刘小明、李宏军、张世扬、赵天亮、吴齐、关汗羽、李治、李海涛、苏震、卢雪阳、张士华、陈辉、郑明峰、姚正思、沈毅明、汪宝川、高朴真、王立、顾仁、刘航、方东、许胜利、冯卫国、黄丽云和张梦天。由于我们使用 Windows 2000 操作系统的经验有限，在本书的翻译过程中难免会出现个别技术概念理解上的错误。敬请读者批评指正。

译者

目　录

第3部分 环境管理

第1部分　Windows 2000 基础

第 1 章　Windows 2000 内部概览

对商务世界来说，PC 的出现已经改变了我们从技术支持的观点接近桌面的方式。在那些过去的日子里，如果一个终端坏了，我们就叫主机修理人员来进行修理。它们通常带来一个新终端，将其连接上去，拆除旧终端。尽管我们经常被强烈地引诱对有问题的 PC 做同样的事情，但经济情况通常要求我们尽力修理机器，而不是扔掉它，买一台新的。由于很多公司都只了解购买一个新系统中的硬件和软件前面的成本，所以购买后的 PC 技术支持已经成为当今商务计算环境中的隐含成本之一。根据我们阅读一些企业分析家的报告，所有估计所有权的年总成本（TCO）可以介于每台 PC 略低于 4000 美元到略高于 12000 美元。把那些成本与我们单位的 PC 数目相乘，可以很容易地看出，为什么降低 PC 的 TCO 已经成了企业的一个主要目标。事实上，这可能是读者购买此书的原因之一。Microsoft 已经响应了人们所关心的问题，为此，把很多复杂的用户和环境管理工具合并在 Windows 2000 中。

当我们设法降低 TCO 时，有几件事情我们可以做。成功的关键之一是减少访问用户桌面的技术支持人员的数目。如何达到这个极高的目标呢？首先，我们将设法标识和去除引起最大麻烦的易变因素（不，我们不能删除用户！）。

谈到用户，可以找到一种方法，对用户进行保护，同时仍然允许他们对他们的环境有所控制，这不是很重要的吗？为他们的文档和文件提供自动容错又怎么样呢？如何能够创建重要资源的透明替代网络路径？让我们使那些网络资源看起来好像都位于用户的硬盘驱动器上一样，以便他们甚至不需要了解网络！让人不必照料用户管理性琐事不也很好吗？那些要求我们在用户数据库中改变它们的邮件地址或电话号码等事项。Windows 2000 将能完成所有这些事情及其它操作。

在笔者曾工作过的每个单位，都存在这种权力斗争。这个通用的、表面上看起来永恒的冲突中，所得到的奖赏是对桌面的控制。用户派别是提醒管理员 PC 中的“P”代表“个人（Personal）”的第一件事情。自然，管理同盟对于谁应该控制桌面持有一个相当不同的观点。不必因为我们是一组多疑的畸形控制人员（无论我们的用户社团怎么想），而只是因为一个更加标准化桌面被反复证明更容易支持，且更重要的是，为了避免出现灾难，无论是什么原因，都

需要重新构造桌面。Windows 2000将不会神奇地结束我们单位的这场斗争,但它将会走过一段很长的路,来给我们以一种健全的和受控的方式提供代表管理的能力,以便可以减轻两个派别之间的紧张状态。

无论需要对桌面进行什么级别的控制,以及是否要求为企业使用一个集中或分散管理模型,都可以定制Windows 2000来满足我们的需要。

用户

笔者已经知道的管理员或技术支持人员与他们的用户有着相同的爱/憎关系,笔者发现这很有意思。没有他们对帮助桌面的不断调用,我们将被解雇,或者至少感到负担很重。不过,我们不得不承认,他们提供了无休止的挑战和源源不断的重要挑战的故事来在会议和上课时讲述。其中大多数挑战和故事都出自难以置信的,为他们的机器所做的有创造力的事情,以及他们调用帮助桌面以报告事故时降临到他们头上的惊人健忘症。Windows 2000将不解决我们的全部用户问题,但它在限制用户的创造能力和把环境恢复到健忘症之前的状态的能力方面,走过了一段很长的路程。

1.1 Windows 2000中用户和桌面管理的新内容

我们将如何达到降低TCO、创建一个适当的管理模型以及根据需要委派管理任务的目标?Windows 2000添加了三项主要技术,笔者看到,它们作为核心技术,用于改进我们管理桌面和用户的方式。我们将在本书的后面更加详细地讨论其中的每项技术,但本节内容将给读者提供一个概念背景,以便将来讨论。三项新技术是:

- Active Directory(活动目录)
- Group Policy Objects(组策略对象)
- IntelliMirror Technologies(IntelliMirror技术)

尽管对Windows 2000来说,Active Directory完全是新内容,但组策略对象和IntelliMirror技术实际上是对现存Microsoft能力的进一步改进。例如,组策略对象是NT 4的系统策略的一个扩充(如果愿意,就是有关类固醇的策略)。IntelliMirror是ZAK和ZAW技术的一个发展。在Windows 2000中,组策略和IntelliMirror通过它们对Active Directory结构和机制的理解以工具的形式得到了它们真正的效力。所以,让我们从那里开始我们的讨论,确信我们也可以理解Active Directory为什么是这个新操作系统的一个如此重要的组件。

1.1.1 Active Directory

Microsoft网络操作系统以前版本的局限性之一是:缺省一种目录服务,来允许管理员创建一种三维的抽象目录树。这个能力存在于其它网络操作系统(NOS)中已有一段时间了。只要向任何Novell或Banyan Vines管理员进行咨询即可。Active Directory就是Microsoft对NDS、Banyan Vines和X.500目录服务的回答。

Active Directory可能是Windows 2000中最有影响的唯一新特征。它将改变网络管理员管理用户和资源的方式。这个特征为我们听说Windows 2000是"一场革命,不是一个发展"的所有谣传提供了燃料。那种说法的真实性是值得怀疑的,因为如果再更深地探究一下NT体系结构、注册表以及信任机制,将会发现NT 4和Windows 2000之间所存在区别很小。不要声称是"革命",也许我们可以更现实地声称Microsoft使这个产品产生了一个飞跃发展,类似于第一

种生物离开原始分泌物在陆地上行走。

尽管三维目录服务的好处是不可否认的，但笔者已经发现传统的 NT 和 LAN Manger 管理员不得不认真地重新调节他们的思维，以适应 Active Directory 的思想。从被连接到其中共享资源与某一特定服务器相关联的物理世界到三维目录服务的虚拟世界的切换会是一个很难的变化。不过笔者相信，一旦进行了这样的切换，就将回忆以前的 Microsoft 系统，把它们视作为原始的和有局限性的系统。相信我，这种切换是一种解放性的经历！在这种满怀希望的观点的支配下，让我们来更仔细地了解一下这种新的目录服务。

为什么使用三维目录服务?

所有的网络操作系统都必须利用某些形式的名称或目录服务，它们允许用户在网络上找到有用的共享资源。我们以一维、二维或三维的形式讨论这些服务。

一维名称服务要求用户在每台存在有他们需要访问的共享资源的服务器上都有一个帐户。一维名称服务的一个例子将是 NT 4 工作组。在这个模型中，用户只针对每台机器的 SAM 被予以鉴定，因为他们企图访问那台机器。所以，他们必须在每个 SAM 上都拥有有效的帐户。

使用二维模型时，针对中央权威机构对用户进行鉴定，并且只要求为他们希望访问的所有资源拥有一个帐户。听起来像 NT 4 一样，为任何其他人使用通过式(pass through)鉴定? 完全正确！NT 4 的域模型是二维名称服务的主要例子。如果读者进行过域之间的管理，就已经遇到过二维服务的一个缺点，即域界限。理论上，为任何用户只需要存在一个用户帐户，通过这个帐户可以在其它域中对他们进行鉴定，前提是在域之间建立了所要求的信任关系。不过实际上，出于安全性原因考虑，为相同的用户在不同的域中建立多个帐户更容易，或者更可取。

真正的三维目录服务有几个特点，其中第一个特点是供整个企业的所有网络资源使用的唯一登录。无论资源位于企业中的什么位置，假设已经准许用户访问所请求的资源，则他们应该能够使用他们的当前被登录的证书进行鉴定。三维服务的另一个特点是以一种分布形式保存有关网络环境的信息。几个服务器之间目录的重复增加了目录的容错能力。这种重复必须以保证目录数据流通这样的一种方式进行，以便对一个目录服务器的数据库进行更改时，所有其它服务器将很快得到更新，以便反映所做的变化。此外，用户应该能够按照某一具体的资源名称或者资源类型搜索一个目录。作为一个例子，笔者应该能够审查目录，以搜索“Accounting Dept. Color Laser Printer(审计部门彩色激光打印机)”或者只是搜索“color printers(彩色打印机)”。

最后，这些目录资源应该独立于它们的物理安装位置存在。这是对象抽象的概念。这是使我们老的 NT 管理员感到苦恼的概念。笔者不是需要知道在 PRINTSVR3 上安装了审计部门的彩色激光打印机，而是可以确定打印机的位置，从逻辑的意义上讲，该打印机可以存在于这个目录中，该位置可能与笔者找到所有那些出纳员的地方相同。

Windows 2000 为三维目录服务满足了所有这些要求，其中在 Windows 2000 中使用 Active Directory 服务。Active Directory 允许管理员创建和管理一个域树或域森林。我们将在下节的内容中进一步讨论那些概念。在那个目录结构内，可以成组资源，以反映组织结构，并通过委派减轻管理负担。用户只需要一个用户帐户来访问所有资源，数据被保存在分布于整个结构中的几个服务器上，并且每当发生变化时都进行重复，以确保数据流通。

目录服务和 X.500 规范

就像对于 Novell 的 NDS 和 Banyan Systems 的 Street Talk 一样，Microsoft 的 Active Directory 以

X.500 目录服务模型为基础,它不是 X.500 顺应的。尽管 X.500 目录服务规范在名义上听起来很重要,但就像很多 ISO 倡议一样,它被认为太复杂和笨拙,在现实世界中不能完整地实现。不过同时人们意识到,规范是描述的目录服务的潜在结构比较坚实,并给它们提供了可伸缩性、灵活性和容错性。因此,软件制造商认为他们所想的是 X.500 规范中最好的内容,并以他们自己独有的方式使其实现。同样,我们也受到企业标准非标准实现的折磨。

当前,存在有几个互用性倡议,它们由 Novell、Banyan 和 IBM 保证来把它们的目录服务移植到其它平台。例如,为 NT 4 存在有 NDS,而 Banyan 在几个其它平台上拥有以一种有限的方式实现的 ENS 目录服务。不过,这些解决办法有时会引起它们自己的问题,如需要一台 Novell 服务器在 NT 网络上运行 NDS,以及只有有限的目录服务为 UNIX 平台使用 Banyan VINES ENS。

Microsoft 正希望利用其 Active Directory 的实现及其支持服务和 API 达到当前在市场上各个目录服务之间的互用性。它们正在打算达到这种互用性,为此,在已经定义可互用服务(如目录和安全性服务)现存工业标准上创建 Active Directory。我们说 Active Directory 不是 X.500 顺应的一个原因是:Microsoft 不是使用 DAP 作为目录协议,而是选择 Lightweight Directory Access Protocol(LDAP)。Microsoft 几乎自从这个规范出现以来就投入了大量资金。除了使用 LDAP 标准在 Active Directory 的虚拟结构中定位和影响资源外,Active Directory 的域树结构还使用 DNS 命名约定。最后,一旦把一个目录完全转换到 Windows 2000,系统就可以使用 Kerberos 安全性系统进行鉴定服务。

使用 LDAP 命名约定,Microsoft 设计了叫做 LDAP 的一个基本目录接口,可以在脚本和程序中使用该接口,在 Windows 2000 Active Directory 中创建、修改和删除目录对象。将来,Microsoft 希望 ADSI 将是所选择的编程接口,来在所有的网络操作环境中修改目录。由于它使用 LDAP 并具有允许应用程序员只使用一个 API 访问不同网络环境中所有资源的附加优点,所以它们更有可能在那个希望中获得成功。

1.1.2 IntelliMirror

前面提到,IntelliMirror 是 Micrososft Zero Admin 初步(ZAK 和 ZAW)的一种自然发展。实际上,它是已经合并到 Windows 2000 中的一个技术集。其中有些技术已经整体或部分地存在于其它 Microsoft 软件包中。例如,SMS 系统的管理员将感到十分适应 Windows 2000 的应用程序发行特征,因为如果他们在 SMS 中使用过 Microsoft Installer 服务,则将已经熟悉那些特征。

IntelliMirror 的所有特征都被设计在万一出现致命崩溃时,可以更容易地恢复用户的工作站。Windows 2000 集体被称为 IntelliMirror 的特征是:

- Client Side Caching(客户侧高速缓存)
- Remote Boot(远程引导)
- Single Instance Storage(单一实例存储空间)
- Microsoft Installer for Automated Application Deployment(自动应用程序发行的 Microsoft 安装程序)
- Group Policies(组策略)

尽管笔者专门提供了第 9 章的内容,来对 IntelliMirror 进行完整讨论,因为能够利用其特征,对于我们能够有效地管理桌面是至关重要的,下面简要地对每个功能进行解释。

客户侧高速缓存

没有网络可供利用时，客户侧高速缓存允许使用基于服务器的文件。这项工作通过在客户的硬盘驱动器上建立一个高速缓存来完成。当用户访问服务器上的文件时，自动高速缓存文件和它们的容许权。如果由于某种原因网络变得不可利用，用户就以完全相同的方式访问文件，好像客户被连接了一样。Windows 2000 不是遵循指定的网络路径，而是把请求重定向到文档局部高速缓存的拷贝。当网络再次变得可以利用时，高速缓存中的文档被自动与服务器的拷贝同步。如果同时更改了两个拷贝，就要问用户他们想如何解决问题。

组策略对象

组策略对象有时被作为一个 IntelliMirror 特征列出，这取决于我们正在阅读哪篇 Microsoft 论文。我们将在 Windows 2000 内作为一个独立的功能讨论那些对象。我们将在下节内容中对它们进行讨论，在第 8 章的内容中对它们进行更深入的讨论。

远程引导

远程引导(Remote Boot)允许快速从网络上的一个中央位置重新安装操作系统。如果由于硬件问题需要重新加载操作系统，则接收一台新 PC 或者那些费解的软件故障之一的用户，即一个管理员，指定某一特定的用户或机器与某一特定的操作系统相关。使用一张自举协议软盘或者一个 PC98 BIOS 顺应系统，用户引导机器，从网络下载操作系统。如果我们在网络有什么信息，则也可以为 NetPC 使用这个特征。

单一实例存储空间(SIS)

用户安装软件包和使它们进行网络安装时，我们经常遇到问题，这导致服务器上受损包的几个拷贝占据宝贵的硬盘驱动器空间。SIS 允许我们克服这个问题。使用 SIS 时，管理员指定服务器存储空间的一个部分作为 SIS 区域。当把一个文件保存到那个服务器上时，服务器对照 SIS 区域中的其它文件检查文件。如果那个新文件等同于一个现存的文件，SIS 就不保存文件的第二个拷贝。相反，服务器只为那个文件创建一个目录项。

Microsoft 安装程序(MSI)

IntelliMirror 的应用程序发行特征使用 MSI 工具的一个组合来完成，利用这个工具可以管理安装机制和组策略对象，定义特定应用程序的接收者。这个工具可被用于从用户的机器发行、更新、修理和删除应用程序。可以对应用程序进行设置，来进行强制发行，或者可以发布它们，以便如果用户愿意就可以进行安装。通过及时使用安装，只有图标被实际放在桌面上。只要当用户第一次启动应用程序时，才实际安装所要求的文件。这阻止系统为这个特定的用户可能从来不需的软件安装不必要的应用程序文件。

1.1.3　组策略对象

组策略允许我们设定用户和机器设置，利用登录/注销和启动/关闭脚本、设置审计和口令策略这样的安全性策略、使用自动化的应用程序发行，以及把所要求的 URL 和文件发布到用户的桌面环境。这些策略对象可以由用户、机器、组或者组织在整个域中有选择性地发行。

本章的前面提到，组策略是可供 NT 4 系统的管理员利用的各个能力的扩展。我们在 NT 4 中作为系统策略讨论的内容在 Windows 2000 中被称为软件策略，且它们只是组策略的一个组

成部分。Widnows 2000中的五类组策略是：

- Software Policies(软件策略)
- User Documents and Settings(用户文档和设置)
- Scripts(脚本)
- Security Settings(安全性设置,供用户和机器使用)
- Application Deployment(应用程序发行)

尽管我们将在第8章中非常详细地讨论其中的每类策略,但笔者认为在这里进行一个简要介绍还是应该的。

软件策略

笔者提到,软件策略支配NT系统策略所影响的相同注册表设置。策略像它们在NT 4中一样,通过更改目标机器的注册表设置来影响客户。其中,软件策略可被用于限制用户更改桌面、配置某一特定机器的所有用户的桌面、恢复设置以及设置用户目录的缺省位置的能力。

用户文档和设置

我们可以使用这些设置把文件夹重定向到其它位置。例如,读者可能会把用户的My Document文件夹重定向到一个网络驱动器,来为它们的文件夹得到容错特征。也可以利用这些策略把URL分布到所有的用户和某一特定的组或组织单位(Organizational Unit,OU)。例如,读者可能想让所有的Windows 2000管理员拥有与Microsoft Knowledge Base或Windows 2000 Server主页的一个直接连接。

脚本

除了在NT 4中可以利用的登录脚本操作能力外,利用Windows 2000,现在可以为任何用户、组或者OU添加注销脚本。我们也可以为机器、机器组或者某一特定OU中的机器使用启动和关闭脚本。现在,这些策略的发行中完全支持Windows Scripting Host(WSH)。WSH是供32位的Windows环境使用的一个独立于语言的脚本主机,同时包含有VBScript和JScript引擎。Microsoft预言,其它软件公司将提供允许使用Perl、REXX、TCL和Python的引擎。我们将在以后的章节中对WSH花费更多的时间。

安全性设置

我们可以通过组策略对象在域中应用安全性设置。利用组策略编辑器(Group Policy Editor),可以设置帐户策略、局部策略(审计、用户权限和其它局部安全性选项)、事件日志设置,以及定义被限制组(如管理员、高级用户和服务器操作员)的成员资格,也可以控制系统设置,如系统服务配置、注册表文件安全性和文件系统安全性。

应用程序发行

从SMS继承是自动把软件包发布在桌面的能力。利用这些发行策略,可以为一个OU、特定用户或者一组机器分配、发布、修理、更新或者删除应用程序。MSI工具处理发行机制,但发行的选择性是通过组策略得到的。我们将在第8章中详细地考察这两个议题。

所有这些类型的组策略对象都可被予以继承,或者在域逻辑结构的任何级别上受到阻塞。这意味着管理员有能力设置将应用于整个域的一个策略,为此,在域的根处创建它,并指定沿着树向下继承它。管理员也可以通过选择策略的块继承从任何策略选择树的一部分。例如,

有人可能不想把缺省的域用户策略应用到管理员组织中。

组策略将是我们管理库中最强大的工具之一，用于达到为桌面降低 TCO 的难以捉摸的目标。它们将允许我们创建管理的桌面环境，可以对这些环境进行定制，来适应用户的作业职责和他们的 PC 教养程度。由于这个原因，笔者专门为这个主题提供了第 8 章的内容。

1.2　Active Directory 概览

构成 Active Directory 的信息被保存在许多数据库中，针对企业树或企业森林的不同部分可以对它们进行重复。Microsoft 经常在它们的说明文档中引用这些数据库作为命名上下文。

结构中的每个域都为它自己拥有一个数据库。这在 Active Directory 中经常被称为用户命名数据库或分区。这个数据库中的信息被重复到那个域中的所有域控制器。对树的剩余部分不对它进行重复。

有三个其它的命名上下文由 Active Directory 保存。它们是 Global Catalog(全局类别)、配置信息和概要。配置信息和概要被集体称为 Active Directory 元数据。所有这三个命名上下文都由整个目录结构共享，所以对于每个目录树或森林，都只有一个 Global Catalog 及单一的概要和配置定义。

由于这些信息由整个结构共享，所以元数据和全局类别被重复到企业中的每个域控制器。对这些通用命名上下文的任何变化都将在整个企业开始一个重复周期。除了重复通信外，还要记住，这个级别的一个错误将会是在整个企业重复的一个错误。将其视作为扰乱了注册表，但这件事情是发生在全局基础上的，每个人都知道这件事情！由于这些原因，建议对其中任何上下文进行更改都应该极其小心，并且预先要认真地进行思考。

不过，让我们开始在一个比较小的规模上考察这些组件。首先，让我们来在域级对 Active Directory 进行考察，然后继续进行到比较大的事情。

1.2.1　域

来自 NT 4 的域概念在 Windows 2000 中仍然占有一席之地。域是树或森林企业模型的构建块，我们将在下节的内容中对它们进行讨论。从管理、安全性和策略发布的角度来看，Windows 2000 中的域仍然用作为界限。

符合 NT 4 域的所有内容对 Windows 2000 中的域仍然有效。在一个独立的工作站上，域界限是工作站，且用户针对工作站 SAM 进行鉴定。如果一台机器是一个域的成员，其中有域控制器处于运作状态，则针对域数据库对用户进行鉴定。唯一区别是：在 Windows 2000 中，我们是针对 Active Directory 而不是域的 SAM 进行鉴定。

Active Directory 结构中的每个域都被称为分区。每个分区都有一个数据库，保存着有关那个分区中所有对象的信息。信息包括对象名称、被填充属性的所有实例以及那个对象实例的访问控制清单和它的属性。这个数据库在域中的所有域控制器上都进行了重复。主域控制器(PDC)和备份域控制器(BDC)的概念在 Windows 2000 中都已消失了。域控制器都是使用多主控(multimaster)重复机制达到同步目的的对等控制器。这意味着如果我们的 PDC 爆炸，或者有些傻瓜在其中撒上了咖啡，我们不再感到惊慌。只有至少还有一个其它的域控制器在分区中操作，则仍然对那个域有着完全的管理能力。现在，再没有用户打电话抱怨说，他们不能改变他们的口令，因为主域控制器拆下来送去修理了。

域概念仍然存在于Windows 2000的一个原因是为了与现存的NT 4域模型保持向后兼容。从现实的意义上来讲,Microsoft不期望我们把一个域控制器升级到Windows 2000服务器,我们还将把所有其它的内容迁移到组织中。由于意识到了这个现实,Windows 2000域服务器识别两种模式的域操作:混合模式(mixed)和本机模式(native)。

操作在本机模式的Windows 2000域假设所有的域控制器都被升级到了Windows 2000。在这种模式中,域控制器之间的多主控重复特征被打开,Kerberos成为缺省的鉴定机制,并且允许进行组的深层嵌套以及通用安全性组的识别。

新提升的域控制器的缺省模式是混合模式。在混合模式中,Windows 2000域控制器完全像NT 4主域控制器或备份域控制器一样操作,使用NTLM作为鉴定系统,应用NT 4的所有组规则,以及为NT 4域控制器使用主-从重复方法。W2K DC在混合模式下模仿PDC还是BDC取决于其在现存的NT 4域中的安装次序。如果它是域中升级的第一个W2K域控制器,就将进行接管,宣称它自己是新的域PDC。当升级了附加的域控制器时,它们将充当为NT 4 BDC,直到所有的DC被升级,管理员选择把域切换到本机模式操作为止。

1.2.2 树和森林

域被成组在一起,形成树或森林。在图1-1和图1-2中可以清楚地看到两种结构之间的区别。

在图1-1中看到,树之所以被这样命名,是因为它类似于一颗颠倒的树,根在顶部,枝向下延伸。结构中的所有域都按信赖关系被链接到一起。树中的所有子域所使用的名称都是从根的名称派生出来的,创建了一个连续的名称空间。

可以把两颗或三颗树链接到一起,形成一片森林。在图1-2中可以看到,名称空间是不连续的,其中每颗树都有它自己的根域名称。域的这种布置对于那些为它们的部门或附属部门有预先存在的公共DNS名称空间的公司来说是很方便的。如果两个公司合并为一个公司,这也是很方便的。

无论我们是创建了树还是森林结构,注意,离开根的子域使用DNS命名约定派生它们的名称。由树创建的名称空间可以是一个公共名称空间,它在Internet上是可以看得见的,如microsoft.com,或者可以是一个私有名称空间,这样的名称空间只能在组织的内部网上看到。

连接域的信赖关系再不必像在NT 4中那样手工创建和独立管理。当一个域加入到一颗现存的树和森林时,自动在域和其紧接着的父域之间自动创建双向信赖。此外,Windows 2000信赖关系是过渡的和含蓄的。我们将在第2章的内容中更多地讨论这些信赖关系。

笔者在本章的前面提到,每个分区都保存着存在于该分区中各对象的一个数据库。这些构成Active Directory的更大的结构也拥有必须在整个目录树或目录森林中共享的信息。记住,每颗树或森林都共享着一个通用的Global Catalog、配置信息和概要。我们将在接下来几小节内容中更多地讨论这三种命名上下文。

Global Catalog

Global Catalog的目的是使整个目录中资源的搜索更加容易和高效。用户不必知道某一特定的资源驻留在哪个域中,他可以对整个目录进行搜索,在树或森林的任何位置寻找资源。Active Directory搜索引擎同时支持白页和黄页类型的搜索,以便用户可以按照资源名称或者只是资源的类型进行搜索。