Windows 2000 中文版实用组网技术

刘芝泉　赵玉双　等编著

清 华 大 学 出 版 社

需要全本请访问 www.ertongbook.com

(京) 新登字 158 号

内 容 简 介

本书在详细介绍 Windows 2000 中文版的各项新增功能和各种网络通信原理的基础上,重点讨论了 Windows 2000 中文版的网络安装、配置、管理、安全性等一系列专题。全书共分 14 章,首先介绍了 Windows 2000 中文版的新功能、安装事项、网络基础知识、TCP/ IP 协议及相关服务等,然后介绍了网络配置、配置 DNS、DHCP 和 WINS 服务器、活动目录、用户和计算机账户管理、资源共享和远程访问,最后介绍了网络性能优化和网络安全性等专题。

本书内容翔实、结构清晰、叙述流畅、技术分析透彻,适合于对 Windows 操作系统有一定了解的用户阅读,也可供从事 Windows 2000 网络集成与网络管理的用户参考。

版权所有,翻印必究。
本书封面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: Windows 2000 中文版实用组网技术
作　者: 刘芝泉 赵玉双 等
出版者: 清华大学出版社(北京清华大学校内,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: 787×1092 1/ 16　印张:20　字数:469 千字
版　次: 2000 年 5 月第 1 版　2000 年 5 月第 1 次印刷
书　号: ISBN 7-302-01128-1/ TP・418
印　数: 0001～6000
定　价: 28 .00 元

前　言

人们期待已久的新的操作系统 Windows 2000 终于在新世纪来临时推出了。Windows 2000 将 Microsoft 公司原有的 Windows 95/ 98 和 Windows NT 两大类操作系统统一在以下 4 个产品系列中:用于移动用户和台式终端的 Windows 2000 Professional,用于工作组和部门服务器的 Windows 2000 Server,用于应用程序服务器和更强劲的部门服务器的 Windows 2000 Advanced Server,以及用于核心业务海量数据处理中心服务器的 Windows 2000 Datacenter Server。Windows 2000 在桌面环境和基本操作方法等方面继承了 Windows 95/ 98 和 Windows NT 的风格,它主要在网络应用的可靠性、可用性、适应性、安全性等方面进行了重大的改进和增强。例如,Windows 2000 采用了基于 Internet 标准的活动目录,建立了一套全面的、分布式的底层服务,具有集成性、深入性、易用性等优点。另外,Windows 2000 还改进了终端服务,采用了新的 NTFS 5 文件系统,增强了远程安装和用户数据管理,完善了系统的分布式安全机制等。

为了让广大读者深入全面地了解 Windows 2000 在网络方面的各项功能及其应用,我们组织了一批多年从事网络管理和网络集成的专家,在认真细致地分析测试了 Windows 2000 的基础上编写了本书。本书内容围绕在组建 Windows 2000 在网络的过程中遇到的安装、配置、系统管理、安全性和性能优化等问题展开,既有对 Windows 2000 各项新功能和网络通信原理方面理论知识的介绍,又注重通过实际的操作过程让读者学会 DNS、DHCP、WINS 和 IIS 等服务器的安装和管理。

本书由康博创作室策划,参加本书编写的除封面署名外,还有赵培军、秦峥、张磊、庞斌、庞峥、潘勇、陈帆、孔祥丰、袁建华、张菊英、王玉娟、曹木军、和红杰、崔建营、马军霞、李瑞民、孙秀等人。由于创作时间紧迫,加之我们水平有限,本书难免会有各种疏漏和不足之处,欢迎广大读者和各界专家批评指正。

作　者

2000 年 3 月

第 1 章　Windows 2000 Server 新功能概述

Windows 2000 是 Microsoft 公司推出的新一代操作系统。为标志其在 Windows 95/ 98 基础上所进行的改进, Microsoft 公司将其命名为 Windows 2000。这个新命名方案的另一个理由是:Windows 98 是 Windows 9x 软件的最后版本,而以后的所有版本都是基于 NT 的。同时, Microsoft 重新命名 Windows NT 5 .0 为 Windows 2000 是为了简化其产品线。新的 Windows 2000 产品线由 4 个产品组成,其中包括 Windows 2000 Professional、Windows 2000 Server、Windows 2000 Advanced Server、Windows 2000 Datacenter Server。

在 Windows 2000 产品线中,Windows 2000 Server 是服务器操作系统系列中的主要产品。Windows 2000 Server 为形成商业优势而集成了最佳的网络、应用程序和 Web 服务。它提供了不断提高的可靠性和可扩展性,通过强大而又灵活的管理服务降低了用户的计算成本,并且它还为优秀的、需要执行重要任务的商业应用程序提供了最佳的运行环境。另外,Windows 2000 Server 为未来的商务计算重新定义了操作平台。这些都是 Windows 2000 Server 所具有的一些最重要的功能与特性,接下来我们将对 Windows 2000 Server 的 3 种不同版本有所侧重地进行简单的介绍。同时,本章将主要针对 Windows 2000 Server 中所采用的众多新技术和新功能进行详细的分类介绍,使读者能对它的主要功能和先进的服务器新创意有一个总体的了解,以便为学习本书后面章节的内容打下基础。

1 .1　Windows 2000 Server 简介

Microsoft 公司同时发行了 3 种版本的服务器操作系统。其中 Windows 2000 Server (以前的 Windows NT Server 5 .0) 最适用于中小型企业进行应用程序部署、建立 Web 服务器、支持工作组和分支机构。该版本将是最流行的 Windows 服务器操作系统,它能够支持两路对称多处理器(SMP)架构的新系统。

Windows 2000 Advanced Server(以前的 Windows NT Server 5 .0 企业版)是较强大的部门和应用程序服务器,它集众多网络操作和 Internet 服务于一身。由于该服务器可支持具有四路 SMP 的新系统,所以它更适合用于数据库密集型的工作,而且它把群集(Clustering)及负载平衡(Windows Load Balance Service, WLBS)相集成,以便提供系统的稳定性。

Windows 2000 Datacenter Server 是 Microsoft 公司所提供的功能最强的服务器操作系统,它支持高达 32 路的 SMP 系统及 64GB 物理内存(取决于系统结构)。与 Windows 2000 Advanced Server 一样,群集和负载平衡服务集成是其标准功能。该系统可用于大

型数据仓库、经济分析、科学及工程方面的大规模模拟,以及联机交易处理。

以上这些版本不仅有助于降低总体成本,而且提供了能增加商业竞争力的服务器基础架构。其突出特点如下:

全面的 Internet 和应用软件服务:通过与用于新一代数字化商业方式的 Internet 服务集成,Windows 2000 Server 系列使建立部署强大的电子商务、知识管理和其他商业方式更为容易。

增强的可靠性和可扩展性:与 Windows NT 4.0 相比,Windows 2000 Server 具有更高水平的整体系统可靠性和可扩展性。例如,系统已针对 32 位处理器进行了优化,支持最高达 64GB 的内存,并建立了更强大的系统体系结构。

强大的端对端管理:为降低成本,Windows 2000 Server 为服务器、网络和 Windows 客户系统提供综合的管理服务。例如,"活动目录"目录服务为管理 Windows 2000 Professional 系统提供了高效方法。

以上介绍了 3 种版本的 Windows 2000 Server,由于功能的侧重点各不相同,各自都有相应的使用环境和场所。用户可以根据工作或学习的实际需要来选择其中一个版本进行安装、配置与管理。

本书针对大多数用户的需求,将只对 Windows 2000 Server 的有关知识和组网技术进行介绍,关于其他版本的 Windows 2000 Server 请读者参考其他相关书籍。

1.2 终端服务

在 Windows 2000 Server 的众多新功能中,我们先来介绍终端服务(Terminal Service)和基于 Windows 的终端(Windows-based Terminal, WBT)。这样做的原因是:终端服务极大地改变了用户使用 Windows 客户机和服务器的传统方式,对于客户/服务器系统来讲,这是一个巨大改变。Windows Terminal 是 Windows 家族中的一个丰硕果实,要解释这个新技术,还要从 Windows NT Server 4.0 Terminal Server Edition 谈起。

1.2.1 终端服务的由来

Windows NT Server 4.0 Terminal Server Edition 是一个在技术上有重大突破的版本,它既能够让 Microsoft Windows NT Server 操作系统支持 Windows 终端,也能够把 Windows 操作系统系列扩展到超级瘦客户端上。这一新技术带给企业客户一个基于 Windows 计算环境的全新扩展,其中包括更低的总体成本、熟悉的 32 位 Windows 用户界面和强大而多样的 Windows 操作系统系列产品。

Windows NT Server 4.0 Terminal Server Edition 的工作原理是:客户机和服务器通过 TCP/IP 协议和标准的局域网构架联系。通过终端客户端,客户机的鼠标、键盘的输入传递到 Terminal Server 上,再把服务器上的显示传递回客户端。客户端没有计算能力,至多只提供一些缓存的能力。众多的客户端可以同时登录到服务器上,仿佛同时在服务器上工作一样,作为不同的会话(Session),它们相互之间是隔离的。

需要全本请访问 www.ertongbook.com

在 Windows 2000 Server 中,终端服务器已经成为一个标准的服务,用户在标准的 Windows 2000 Server 上选择安装作为 Windows 部件的终端服务,就可获得原来终端服务器的功能。该服务对中文的支持非常彻底,因为 Windows 2000 本身支持 Unicode,可以同时显示和编辑多国语言。

1.2.2　终端服务的特点

Windows NT Server 4.0 Terminal Server Edition 是 Windows NT Server 4.0 产品系列的一个扩展。在多用户的 Windows NT 环境中,一个超级瘦客户端能够让用户同时得到使用 Windows NT 操作系统和运行 Windows 应用程序的体验。Terminal Server 能够让用户从下列任何类型的桌面,通过标准的 TCP/IP 网络运行 16 位或 32 位 Windows 应用程序。

一种新的低成本的硬件,通常指基于 Windows 的终端,它能够由第三方的硬件供应商供应。其内核是嵌入式的 Windows CE 操作系统,预装了 Terminal Server 的可定制客户端。

任何现有的 32 位 Windows 桌面操作系统,如 Windows 95/98 或 Windows NT Workstation。只要运行基于软件的 Terminal 客户端即可,此软件非常小,效率很高。

旧的运行 16 位 Windows 3.11 操作系统的基于 Windows 的桌面。

X-based Terminals、Apple Macintosh、MS-DOS&reg、网络计算机,以及基于 UNIX 的桌面(通过第三方的附加产品实现)。

通过第三方提供的硬件板卡、集成 Windows CE 的 ROM、网卡和显示卡的三合一或二合一 PCI 卡的可改造无盘工作站。

1.2.3　Windows 2000 Server 终端服务的新特性

Windows 2000 的终端服务比 Windows NT Server 4.0 Terminal Server Edition 又有了很多的改进,除了支持多国语言之外,改进之处还包括:

支持本地打印机　这是 Microsoft 公司在发布 Terminal Server Edition 4.0 之后,用户需求最强烈的一个功能。通常使用 WBT 或软件终端客户端的用户,多是"任务工作者(Task Worker)",比如银行、证券公司和邮局等的柜台交易人员,本地打印是一个必需的功能。因此,Windows 2000 的终端服务增加了对本地打印的支持,它是通过一种虚拟通道(Virtual Channel)技术实现的。

支持会话重影(Session Shadowing)　在实际工作环境中,用户有时需要远程控制一个客户端来完成特定任务。Microsoft 已经有两种方式实现远程控制:Systems Management Server 2.0 和 NetMeeting 3.0。Microsoft 把这种远程控制的机制集成到了终端服务中,只要管理员权限足够,就可以控制某一个终端客户端的对话,双方可以同时工作在一个界面上。

支持嵌入在 Web 浏览器中的终端客户端　Microsoft 公司计划在发布 Windows 2000 之后,继续开发 ActiveX 形式的终端客户端。用户不再需要下载客户端,在本地安装之后再运行。只需打开 Internet Explorer,访问内嵌了终端客户端的网页,即可使

用终端访问的服务。

1.2.4 终端服务的业务价值

Windows 2000 Server 终端服务在降低总体管理成本、迅速部署业务应用等方面具有优势,为企业竞争能力的提高带来了简单性和灵活性。其价值主要体现在以下几方面:

桌面客户端真正做到傻瓜型,不需要任何的维护工作。同时,终端服务器能保持客户端的对话,即使客户端不慎掉电,只要重新开机和连接,就会恢复到原来的工作状态,没有损失数据之忧。可以通过设定让 WBT 客户端无法上载和下载数据,这样既保证了不受病毒的侵害,又保证了不至于因数据被复制而泄密。

先进的 32 位的 Windows 应用可以迅速在企业内部推广,无论客户端是硬件型的(WBT),还是软件型的(可以利用旧的 486/ Pentium 机器),都可以获得一致的界面。有利于企业领先于竞争对手,提供更好的客户服务或为企业自身服务。

对于软件开发企业来说,内部的开发人员可以在安装了 Office 的终端服务器上办公,不至于因为拆装自用机器做实验而影响办公效率。销售人员可以拨号回公司,通过笔记本上的终端客户端给用户做实际演示。甚至可以为用户在 Internet 上架设终端服务趋,在安装了应用软件之后,请用户试用或租赁。

对于移动办公的用户来说,可以通过远程拨号上网后,启动终端客户端运行办公室的桌面电脑上的 Outlook 来读取邮件,比运行远程客户机上的 Outlook 来读邮件要快很多。因为邮件不再需要通过低速的远程连接下载,便可直接在局域网上的桌面电脑上打开,仅仅传递屏幕显示,速度会有很大提高。终端服务还有专门为远程使用进行的设置,可以进行本地图片缓存,进一步提高速度。

对于网络管理员来说,与 Web、MMC 和 Script 的远程管理方法相比,终端服务提供了对服务器更为彻底的远程管理。Windows 2000 Server 中的终端服务和终端客户端(在\winnt\system32\client 目录下)可以跨越基本的基于活动目录的域管理模式,简单而灵活地连接到任何一台有权限的服务器上,是网络管理员的强有力的工具。

1.2.5 部署终端服务的考虑

对于希望在 Windows 2000 Server 终端服务上部署应用的用户来说,需要考虑下面几个问题:

应用程序的兼容性问题　　应用程序应该考虑到多用户的情形,把机器的数据和用户的数据彻底分开。Microsoft 公司在 http:// www .microsoft .com/ ntserver 网站上提供了有关这方面情况的白皮书。

应用程序的性能问题　　一般来说,每个客户端会话需占用 4～8MB 的服务器内存。在实际的测试中,一台双 350MHz Pentium Ⅱ CPU、512MB 内存的服务器,能支持 50 人的日常办公。在使用终端服务的环境里,一定要保证服务器的性能,并且做好日常性的维护工作。

如果用户的数量很多的话,建议用户采用双机集群或负载均衡方法。建立漫游客户(roaming user)并把个人配置文件放置在网络路径上,可以使用户无论从哪一点登录

到网络,都会得到同样的使用环境。

1.3　活 动 目 录

Windows 2000 Server 最核心的技术是“活动目录(Active Directory)”技术,它在改进“活动目录”目录服务技术的基础上,建立了一套全面的、分布式的底层服务。“活动目录”是集成在系统中的、采用了 Internet 标准的技术,是一套具有扩展性的多用途目录服务技术。它能有效地简化网络用户及资源的管理,并使用户更容易地访问网络资源。

1.3.1　活动目录的由来

在 Windows NT Server 4.0 中就已经贯彻了目录服务的思想。NT 的“域(domain)”概念是目录服务的一个基本单元。一次登录(Single Login)在 Windows NT Server 的环境下有了具体的应用,比如 Internet Information Server、Exchange Server、SQL Server 等都可以与 Windows NT Server 的账号验证集成起来,用户一次登录就可以获得 Web、E-maiL 和数据库等多种多样的网络服务。

Windows 2000 Server 在 Windows NT Server 4.0 的基础上,进一步扩展了活动目录。活动目录充分体现了 Microsoft 产品的 ICE,即集成性(Integration)、深入性(Comprehensive)和易用性(Ease of Use)等优点。活动目录是一个完全可扩展、可伸缩的目录服务,既能满足商业 ISP 的需要,又能满足企业内部网和因特网的需要。

活动目录是从数据存储开始的。它采用 Exchange Server 的数据存储技术,称为 Extensible Storage Service (ESS)。其特点是不需要事先定义数据库的参数,可以做到动态的增长,性能非常优良。在这个数据存储之上已建立索引,可以方便快速地搜索和定位。活动目录的分区是域,一个域可以存储上百万个对象。域之间还有层次关系,可以建立域树和域森林,无限地扩展。

在数据存储之上,Microsoft 建立了一个对象模型以构成活动目录。这一对象模型对 LDAP 有纯粹的支持,还可以管理和修改 Schema。Schema 包括了活动目录中的计算机、用户和打印机等所有对象的定义,其本身也是活动目录的内容之一,它在整个域森林中是唯一的。通过修改 Schema 的工具,用户或开发人员可以自己定义特殊的类和属性,来创建所需要的对象和对象属性。

活动目录包括两个方面:目录和与目录相关的服务。目录是存储各种对象的一个物理上的容器;而目录服务是使目录中所有信息和资源发挥作用的接口。活动目录是一个分布式的目录服务。信息可以分散在多台不同的计算机上,保证快速访问和容错;并且不管用户从何处访问或信息处在何处,目录服务都对用户提供统一的视图。

1.3.2　活动目录的集成性

活动目录结合了 3 个方面的管理内容:用户和资源管理、基于目录的网络服务,以及基于网络的应用管理。而且活动目录广泛地采纳了 Internet 标准,把众多的 Internet 服

务都集成了在一起。

目录管理的基本对象是用户和计算机,还包括文件、打印机等资源。举例来说,用户对象的属性非常丰富,不但有常见的账号名、口令等,还包括邮件信箱和个人主页地址、在公司中的职位关系等。可以在活动目录中右击用户对象发送邮件和访问其个人主页;其职位关系可以在公司的内部网上用 Web 组织结构图的方式动态地显示出来,也可以被内部采购、费用报销等应用程序利用来实施业务逻辑。活动目录,支持全局性的查找,比如查找整个网络中支持双面打印的彩色打印机等。

活动目录彻底地采用了 Internet 标准协议,比如用户账号可以用 User@hch .kb .com 或 User@kb .com 的快捷方式来表示并登录网络等。在此 hch .kb .com 和 kb .com 就是两个不同的域。但是这两个域之间有信任关系,因为 kb .com 是一个根域,hch .kb .com 是一个子域。子域之下还可以有子域,比如 works .hch .kb .com,相互之间都是可传递的信任关系,构成一棵域树。如果你的公司兼并了一家其他的公司,你的域树可以和他们的域树 workgroup .com 建立起整个的域森林来。DNS (Domain Name Service)在此充当了名字解析的功能,建议用户使用与活动目录集成的 DNS Server 来保证动态更新域名和提供更好的复制能力。整个域森林的所有对象,只要安全性管理许可,都可以用 LDAP 协议访问到。

在当今的 Internet 时代,活动目录这种基于 Internet 标准的做法,给用户带来了无穷尽的益处。活动目录集成了关键服务,如 DNS、MSMQ(消息队列服务);集成了关键应用,如电子邮件、网管、ERP 等;集成了关键数据访问,如 ADSI、OLE DB 等;还集成了关键的安全性,如 Kerberos 第 5 版本和公开密钥基础设施等。

基于活动目录的网络基础设施服务(Directory-Enabled Networking, DEN)是一种旨在提高网络可管理性和提高网络服务质量的协议。在 Windows 2000 活动目录中,可以完成根据不同的用户或应用分配网络带宽等高级的网络管理任务,以及支持 ATM 网络和 QoS 协议等。

基于活动目录的应用服务(Directory-Enabled Application)是在 Windows 2000 平台上的新一代的应用程序。应用程序开发员可以扩展活动目录的 Schema 和 UI,通过 ADSI/ ADO 编程,在活动目录中发布服务绑定信息,通过组策略配置应用程序,进行实时应用下载和应用改变的自动通知等。一个比较典型的基于活动目录应用的例子是 NetMeeting。在活动目录的环境中,用户只要在 NetMeeting 中键入同事的 E-mail 别名,就可以通过活动目录中的定位服务与其进行对话和桌面协作等,非常方便。

1.3.3 活动目录的深入性

活动目录的深入性体现在企业级的可伸缩性、安全性、互操作性、编程能力和升级能力上。活动目录既可以存储几个对象,也可以存储上亿万个对象。活动目录通过为每个域创建一个目录存储的方法来获得伸缩性。这一个目录存储中仅仅包括了该域的所有对象。当域树建立起来之后,每个域有能力搜索整个域树中所有的目录存储。这种划分整个域树的方法,使用户所需要的信息离用户最近,响应最快。域的目录存储还可以有很多副本,副本之间自动地进行同步,进一步提高了响应速度和服务的可用性。

这种域树和域森林的方法可以帮助活动目录使用容器层次来模拟一个企业的组织结构。组织中的不同部门可以成为不同的域,或者一个域中有层次结构的组织单元(Organizational Unit, OU),从而采用层次化的命名方法来反映组织结构和进行管理授权。顺着组织结构进行"颗粒化"的管理授权可以解决很多管理上的头疼问题,在加强中央管理的同时,又不失机动灵活性。

Windows NT 4.0 中的很多域都可以成为 OU,建立起更大的域和更简化的域关系,借助全局目录(Global Catalog),用户和管理员仍然能够迅速地找到对象和管理对象。Windows 2000 可以在现存的 Windows NT 4.0 的环境中工作,保护用户现有的投资;Microsoft 公司也提供了一系列的工具帮助 Windows NT 4.0 的用户迁移到 Windows 2000 的目录环境中。例如 Directory Connector 可以使活动目录与 Exchange Server 5.5、NDS 的目录服务同步,而 Exchange 6.0 干脆就采用了 Windows 2000 作为其目录服务。

在活动目录中,目录存储只有一种形式,即域控制器(Domain Controller),它包括了完整的域目录的信息,不再有主域控制器和备份域控制器的区别。所有的域控制器在用户访问和提供服务方面都是相同的。它们之间的同步采用了一种先进的多主复制的技术,称为 Update Sequence Numbers (USN)。每个服务器跟踪其复制伙伴的最新 USN 列表,保证及时更新并且不会有冲突或相互覆盖等。

Windows 2000 的安全性服务(如 Kerberos、PKI 和智能卡等)和活动目录紧密结合。活动目录存储了域安全政策的信息,比如域口令的限制政策、系统访问权限等,实施了基于对象的安全模型和访问控制机制。在活动目录中的每个对象都有一个独有的安全性描述,定义了浏览或更新对象属性所需要的访问权限。但是,当 LDAP 客户端访问活动目录时,操作系统会实施访问安全控制,而不是由活动目录来决定访问控制。Windows 2000 安全性和活动目录相辅相成,可以共同完成任务和协同管理。

1.3.4　活动目录的易用性

一个功能强大的目录服务如果不便于使用,也不是一个好的目录服务。活动目录的易用性,也是 Windows 2000 整体简洁性的一个体现。

先说一下活动目录的安装。Windows NT Server 4.0 的用户可能不习惯 Windows 2000 Server 的做法:所有的新安装都安装成为 Member Server,目录服务都需要事后用 Dcpromo 的命令专门特别安装。目录服务还可以卸载,而不用像安装 Windows NT 4.0 那样,一开始就要定终身:区分域控制器还是 Member Server,两者之间不可转换。

Dcpromo 是一个图形化的向导程序,引导用户一步一步地建立域控制器,可以新建一个域森林、一棵域树,或者仅仅是域控制器的另一个备份。很多其他的网络服务,比如 DNS Server、DHCP Server 和 Certificate Server 等,都可以在以后与活动目录集成安装,便于实施策略管理等。

在活动目录安装之后,主要有 3 个活动目录的 Microsoft 管理界面(MMC):一个是活动目录用户和计算机管理,主要用于实施对域的管理;一个是活动目录的域和域信任关系的管理,主要用于管理多域的关系;还有一个是活动目录的节点管理,可以把域控制器置于不同的节点。一般局域网的范围内为一个节点,节点内的域控制器之间的复制是自

动进行的;节点间的域控制器之间的复制,需要管理员设定,以优化复制流量,提高可伸缩性。在活动目录管理界面中,还可以右击 SDOU(节点、域和组织单元的统称),启动组策略(Group Policy)的管理界面,实施对对象的细致管理。

对于 SDOU,管理员还可以方便地进行管理授权。右击 SDOU 就可以启动管理授权向导,一步一步地设定哪些管理员对哪些对象有什么样的管理权限。比如说企业内部技术支持中心的管理员,只有复位用户口令的权限,没有创建和删除用户账号的权限。这种更细致的管理方法称为"颗粒化"。

另外,活动目录还充分地考虑到了备份和恢复目录服务的需要。Windows 2000 备份工具中有专门备份活动目录的选项,在出现意外事故的时候,可以在机器启动时按 F8 键,进入安全模式来进行目录服务的恢复,最大限度地减少灾难的恶性影响。

通过上述的介绍,相信读者对于活动目录的出色之处已经有了一个初步的了解。因此建议大型企业的大型网络使用 Windows 2000 Server 先进的目录服务功能。因为要发挥活动目录的企业级性能,需要有使用大型网络开展关键业务的用户,只有他们才能在实践中体会活动目录的优势。

1.4 文件、打印与存储服务

现代企业中架设网络已经成为一种时尚,而文件和打印服务的共享往往是企业架设网络的最初原因。从最早的局域网萌芽,到今天纷繁复杂的网络世界,文件/打印服务一直占据着重要的地位。同时,随着网络的发展,存储网络(Storage Area Network, SAN)也渐渐浮出海面,成为一个新兴的热门话题。接下来就来介绍 Windows 2000 Server 在这 3 个方面的新特性。

在现在的企业中,人们有时候会注意到这样的现象:企业里各个部门都配上了电脑,但是电脑只是用作打字机,文件都要通过打印出来才能分发到相关的人员和部门;每台电脑都配备了打印机,企业不知道采用网络打印服务可以大大节省购买打印机的开销,也便于加强统一管理;而且,企业也常常不知道如何存储海量的文件和数据信息,在提高信息处理效率的同时降低存储的成本。这些问题,就是 Windows 2000 文件、打印、存储服务要解决的重点。

1.4.1 功底深厚的文件服务

Windows 2000 Server 在 Windows NT Server 4.0 的高效文件服务基础上,增强或新增了分布式文件系统、用户配额、加密文件系统、磁盘碎片整理、索引服务、动态卷管理和磁盘管理等特性。

分布式文件系统(Distributed File System, DFS)是一个在 Windows NT Server 4.0 中已经存在的文件服务,在 Windows 2000 中得到了进一步增强。它的作用是不管文件的物理分布情况如何,都可以把文件组织成为树状的层次逻辑结构,便于用户访问网络文件资源、加强容错能力和网络负载均衡等。Windows 2000、Windows NT 4.0 和 Win-

需要全本请访问 www.ertongbook.com

dows 98 系统中都已安装了支持 DFS 的客户端,Windows 95 的 DFS 客户端需要另外下载安装。

启动分布式文件系统,首先需要安装 DFS 服务,然后从 DFS 的 Microsoft 管理界面(MMC)中创建一个 DFS 的根,推荐建立成为与活动目录相结合的根(这样有容错的能力),所以需要指定相应的域和服务器来寄宿共享文件夹,然后再命名即可。在 DFS 根之下,还可以生成叶节点和支节点,两者的区别是支节点还可以再包含叶节点。

建立了分布式文件系统之后,新入公司的员工可以从一棵按公司业务结构建立的文件树的根节点开始寻找文件,而不会迷失方向,也无须考虑文件的物理存储位置。即使文件的物理存储位置有变动,也不会影响用户的使用。这是一个透明的高扩展性的文件管理方案。

Windows 2000 采用了 NTFS 5 文件系统,在 NTFS 4 的基础上,增加了两个新的特别访问许可:权限改变和拥有所有权。权限改变的访问许可与常用的完全控制的访问许可相比,只能改变某些文件/ 文件夹的权限属性,而不能增加或删除文件,管理得更加细致。拥有所有权的访问许可可以用于在一个员工离开公司后,接替后的员工需要拥有前任员工所拥有的文件配置。

在 Windows 2000 的分布式网络环境中,用户多了一个新的工具来管理文件存储的增长带来的磁盘配额问题。磁盘配额是 Windows NT 4 .0 的用户要求增加的一项最为迫切的特性。它可以允许管理员根据文件或文件夹的所有权来向用户分配磁盘空间,还可以设定警报和观察用户所剩的磁盘空间。需要注意的是,这种磁盘配额的管理是以磁盘卷为基础的,只能在磁盘卷的属性中设定。

加密文件系统(Encrypting File System, EFS)是在磁盘上存储 NTFS 文件的一种新的加密存储方式。加密文件系统是以公用密钥为基础的,作为系统服务的一部分,容易管理,有防御攻击的能力,而且对于用户来讲是透明的。用户只需要在文件夹的高级属性中指定“加密内容以保护数据”,文件夹中的文件和子文件夹都会被加密。对于移动用户来说,假如笔记本丢失而落入不法分子手中,即使不法分子重新安装操作系统,原有的文件也无法访问,从而进一步提高了安全性。在 Windows 2000 的整体安全性设置中,可以指定“文件恢复代理”的管理员,以便在原有文件主人密钥丢失的情况下,仍然可以由管理员帮助恢复文件。

Windows 2000 中有一个索引服务(Index Service),可以帮助用户在浩如烟海的文件中快速找到所需要的文件。索引服务原来是设计用来搜索 Internet 或 Intranet 上的 Web 页面的,但是在 Windows 2000 中索引服务还可以搜索文件系统,并且默认时支持全文本的搜索。一旦安装之后,所有的更新和索引的创建和优化工作都是全自动的。在 Windows 2000 中建立索引控制也很方便,并且可以与远程存储服务相结合,搜索远程的文件和 Html 页面等。

动态卷管理功能允许用户不需要重新启动即可以管理服务器的存储器。例如,用户可以不重新启动系统而创建、扩充、映射卷或者添加磁盘。

磁盘管理为用户的磁盘存储器管理提供了拥有众多新功能的图表工具,这些功能主要包括:

支持新的动态卷　　有了支持新动态卷的磁盘系统,用户就不需要再忍受每个磁盘最多只能有 4 个分区的限制了。

联机磁盘管理　　用户不需要关闭系统或中断使用就可以完成管理员的任务。大多数配置的更改立即就能生效。

本地和网络驱动器管理　　作为管理员,用户可以管理任何运行 Windows NT 4.0 或 Windows 2000 的网络计算机。

卷的装配地点　　用户可以使用磁盘管理器在本地任何一个 NTFS 格式卷中的空文件夹上连接或装配本地驱动器。

1.4.2 出神入化的打印服务

用户在自己家中的电脑上安装了 Windows 2000 Server 之后,当把自己的打印机连接到计算机,从"打印机"窗口中增添一台打印机时,会发现 Windows 2000 可以自动地检测和安装驱动程序。这对于广大的普通用户来说,真是方便了许多。Windows 2000 还支持脱机打印,当打印机重新连接的时候,原来存储的打印任务就可以开始进行了。

对于网络打印机,用户只需找到此台打印机,右击,选择"连接"命令即可把它安装到本地,省却了提供打印驱动程序的过程。网络打印机还可以以一个 URL 的形式来表示,即所谓的 Internet 打印服务。Internet 打印是 Windows 2000 中的一个新特性,它提供了通过 Internet 将打印作业提交给打印机的方式。这方面的应用有:开设 Internet 上的快速印刷厂、酒店的商务中心打印,或者通过 Internet 打印代替 FAX 的功能等。

要想使 Windows 2000 处理包含 URL 的打印作业,必须运行 Microsoft 公司的 Internet Information Server 或者 Personal Web Server,来支持标准的 Web 访问安全机制。Internet 打印将 Internet 打印协议(IPP)作为低级协议使用,将其封装在作为载体使用的 HTTP 协议中。也可以通过浏览器来管理 Internet 或 Intranet 上的打印机。

通过活动目录,用户还可以查找打印机。查找打印机的选项提供输入不同类型搜索准则的方法:可以输入诸如名称、位置和打印机型号等信息,在附加搜索选项中,可以输入是否支持双面打印或按特殊分辨率打印等信息。在开始查找之后,还可以使用列标题对搜索结果窗格中列出的打印机进行分类和筛选。

1.4.3 崭露头角的存储服务

随着 Internet 和 Intranet 的发展,网络用户数量迅猛增长,多媒体和 32/64 位计算的普及,造成了对大量存储空间的要求,同时网络管理员也希望得到一个可提供快速存取、灵活增添任意数据类型的存储设备。并且可以减少管理负荷的网络系统,于是 SAN 作为新一代集中式存储解决方案就应运而生了。Windows 2000 的存储服务就考虑到 SAN 网络的需要,建立了一套基础服务,为存储市场上的创新提供了坚实的基础。

Windows 2000 中更容易使用的存储管理体现在动态磁盘卷管理、磁盘碎片整理和自动系统恢复等方面。Microsoft 公司在 Windows 2000 中集成了 VERITAS 公司的动态磁盘卷管理,提供了在线的磁盘卷创建、扩展或镜像,甚至增加新的磁盘,也不需要重新启动机器。同时它也提供了自我描述的磁盘、简化的任务和直观的用户界面。

Microsoft 公司在 Windows 2000 中加入了磁盘碎片整理工具,可以使得文件、目录和自由空间变得更加连续,提高文件的访问性能。自动系统恢复(Automated System Recover, ASR) 可以帮助管理员在 Windows 2000 安装程序的帮助下恢复不能启动或装载的 Windows 2000 系统。管理员通常可以在系统启动时按 F8 键,进入一个恢复控制台来进行系统的修补工作,比如关停一些系统服务等。

Windows 2000 也设计了通过层次性存储管理(Hierarchical System Management, HSM)、支持新兴存储访问协议等方法来降低存储的成本。层次性存储管理是建立在远程存储服务(Remote Storage Service, RSS)之上的,无须添加磁盘就可以在服务器上增加新的自由空间。RSS 自动地监测本地硬盘上的剩余空间的大小。如果在一个主要硬盘上的自由空间下降到一个事先设定的水平,RSS 自动把本地数据复制到远程存储上以腾出空间。

因为远程存储通常采用磁带或 CD-ROM 等比硬盘更便宜的介质,这种存储方法提供了很好的成本有效性。RSS 可以根据管理员事先设定的规则,把不经常使用的文件自动移动到远程存储上。同时 HSM 在文件系统中加入在文件所在远程存储上的位置指针,文件系统可以依据这一信息来获得文件。这一切对于应用程序和用户来说都是透明的。

Windows 2000 也支持先进的数据传输协议,比如 I2O、光纤通道和 1394 等,数据传输的性能提高,对于整体存储系统的响应能力有很大的改进。I2O 是存储卡或者 RAID 卡的一种特性;光纤通道支持超过每秒 1GB 的传输速率和超过 10KM 的光纤长度,并且可以通过 Hub 级联,容量无限增长;1394 是多媒体带宽的高速并行连接,适合于视频音频信号的传输。

除了支持上述光纤通道之外,Windows 2000 为了解决存储增长的瓶颈问题,还提供了可移动存储管理(Removable Storage Manager, RSM)。RSM 提供了通向介质转换器或介质库的一个标准接口,能够方便地进行可移动媒介(如 CDROM 塔、磁带等)的安装或卸载,并且提供了编目、跟踪、控制硬件的能力。RSM 把可移动介质组成不同的介质池,并自动地按照设定的规则在介质池中移动文件。

Windows 2000 对备份工具也作了修改,提供了新的向导程序,改变了原来以磁带备份为核心的做法,而以介质备份为核心。备份工具与 RSM 相结合,为管理员保护数据和扩展存储空间提供了几乎无限的能力。

1.5　远程安装与用户数据管理

对于网络管理员来讲,单纯管理几台客户端机器也许并不是什么大不了的工作,可是架不住用户有各自不同的口味、人员也三天两头地变化,网络管理员总是被巨大的工作负荷压迫着。Microsoft 在 Windows NT Server 4.0 平台上提供了 Microsoft Systems Management Server 2.0 系统管理解决方案,可以进行网络规划、配置和诊断。

在此基础上,Windows 2000 进一步加强了对变化和配置的管理,这一整套技术称为智能镜像 (Intellimirror)。而 Systems Management Server 仍然是针对 Windows 2000

平台的增值解决方案,提供比智能镜像更高级的一些管理服务。

智能镜像的主要内容包括 4 个方面:远程安装、用户数据管理、应用软件管理和用户设置管理。这些特性需要 Windows 2000 Professional 和 Windows 2000 Server 前后台相结合才能体现出来。Microsoft 设计智能镜像的基本思路是:使管理员把精力集中在管理使用电脑的用户上,而不是机器上。智能镜像可以降低整体拥有成本,使用户和管理员轻松地管理好数据、应用软件和设置等。这一切都是通过 Windows 2000 中彻底分离用户数据和机器数据的技术手段来实现的。

智能镜像与 Windows 2000 的其他技术紧密结合,比如活动目录、组策略(Group Policy)等。组策略是 Windows NT 系统策略的升级,它作用于某个特定的"容器",比如节点(Site)、域(Domain)和组织单元(Organizational Unit OU),简称 SDOU。一旦实施,组策略就对容器中的机器或用户起作用,实施智能镜像。

1.5.1 远程安装

人们在现代的公司环境中经常会遇到这样的情况:需要为新员工安装一台全新的计算机,或者需要彻底重新安装操作系统和应用软件。因为在日常的工作中,除了操作系统之外,还需要很多的应用软件和工具,比如 MS Office、WinZip 等,人们也会希望安装机器的时候能够把这些应用软件也一起装上,甚至把公司标准的桌面主题也一并设置好。采用 Windows 2000 智能镜像就可以轻松地做到这一点。为实现此功能用户需要进行以下几步操作:

(1) 首先需要在一台 Windows 2000 Server 上安装 DHCP 服务(动态 IP 地址分配)和远程安装服务(Remote Installation Service,RIS)。需要注意的是,在 Windows 2000 的活动目录环境中,安装 DHCP 服务之后,并不是总能启动的,只有管理员在活动目录中授权特定的 DHCP 服务之后才能启动。这个措施是为了防止未授权的 DHCP 服务捣乱网络环境。在安装了作为 Windows 2000 系统部件的远程安装服务后,可以从控制面板的"增加/删除软件"程序中进行 RIS 的配置,比如指定一个可以使用的 Image 文件供客户端安装(通常是 Windows 2000 Professional 的安装文件)。

(2) 然后用户就可以到客户端开机启动机器,注意一定要用网卡上的 BootROM 启动(如果网卡支持 PXE)或者是采用特制的软盘启动。这个软盘可用 RIS 服务器上的一个可执行文件 rbfg.exe 来制作。软盘支持的网卡也有限制,大概只有 20 多种,多为比较常见的网卡。

(3) 客户机器启动时,需要用户按 F12 键进入远程安装模式。客户机通过 DHCP 获得 IP 地址,然后在验证账号和口令之后,选择某一个 Image 文件开始安装。需要注意,用户登录用的账号必须拥有"增加一台工作站到域"的权限。如果事先把一个 Unattended.txt 文件与此 Image 文件建立联系的话,接下来的安装过程也可以做到无人值守。在 Windows 2000 的光盘上还提供了一个 Setup Manager 工具,可以帮助管理员来创建这样的 Unattended.txt 文件。

(4) 如果管理员希望在远程安装过程中把应用程序一并安装上的话,Microsoft 公司还提供了一个特别的工具,称为 Riprep。在管理员安装了一个标准的公司桌面操作系

统,并配置好应用软件和一些桌面设置之后,可以使用 Riprep 从这个标准的公司桌面系统制作一个 Image 文件。这个 Image 文件既包括了客户端的应用软件,又把每个桌面系统必须独占的安全 ID、计算机账号等删除了。管理员可以把它放到远程安装服务器上,供客户端远程启动进行安装时选用。

有了远程安装服务,企业用户在部署数以千计的 Windows 2000 Professional 时的困难就迎刃而解了。其实在 Windows NT Workstation 4 .0 中已经准备了类似的工具,称为 SysPrep,也可以做到通过复制 Image 文件的方式快速部署。企业桌面管理员只要给用户简单的指示或者再加一张启动软盘,就可以让用户快速完成一个标准企业桌面的安装和配置,省去不少精力和时间。

1 .5 2　用户数据管理

现代计算环境面临的另一个挑战是如何管理用户的数据。有的用户整天在路上工作,需要处理在线和离线两种环境下的数据和文件;有的用户没有自己的计算机,需要和别人合用,或者干脆见到哪台计算机空闲就用哪台计算机。传统的用软盘保存自己文件的做法,在数据和文件日益爆炸的今天,已经不能奏效了。

Windows 2000 在组策略中对用户的管理就有“ 文件夹重定向 ”一项,可以把文件夹定位到文件服务器上一个特定的目录中,还可以自动地为此目录加上存取权限。再配合“ 磁盘配额 ”的使用,管理员在为用户提供方便的同时,不至于以服务器超负载为代价。

正是因为文件是在服务器上的共享目录中,用户可以从任何一台计算机登录,获得同样的文件使用经验。如果用户需要离线处理的能力,用户或管理员可以指定此共享目录在离线时也可用。

1 .6　分布式安全性

信息安全对今天的网络系统来说,是一个非常重要又非常严重的问题,它涉及到从硬件到软件、从单机到网络的各个方面的安全性机制。而网络操作系统的安全性是整个网络系统安全体系中的基础环节。

在保护一个企业的信息技术方面,防火墙、加密设备和其他的许多相关部件都有着重要的作用。但是最重要的决定因素仍然是选择一个适当的网络操作系统。企业不但要考察网络操作系统所能够提供的安全特性,还要考虑达到适当安全水平所需要花费的成本,以及对企业业务和竞争力的影响。

今天,企业越来越向 Internet 开放,企业网络和 Internet 网络之间的区分已经不再明显。企业需要采用基于 Internet 的技术,与业务伙伴、供货商和顾客进行交互,安全性就成为在 Internet 和 Intranet 中控制资源访问权限的关键因素,同时企业也需要安全管理上的灵活性和简易性。

安全性技术也在快速的发展变化之中。在今天日益复杂的环境中,为了达到较高的安全程度,有两个领域发展很快,即公用密钥证书和动态口令。企业越来越多地面临着通

过公共网络进行远程访问、通过 Internet 进行企业间通信的问题。这是推动安全技术发展的动力。

1.6.1 Windows 2000 的安全性设计

作为新一代的企业级网络操作系统,Windows 2000 在安全特性方面的设计注重了以下 3 个方面:

对于基于 Internet 的新型企业的支持。帮助它们突破原有的企业网络和 Internet 的界限,满足移动办公、远程工作和随时随地接入 Internet 进行通信和电子商务的需要。新一代的 Extranet 应用由此应运而生。

在 Windows 2000 中提供的是一个安全性框架,并不偏重于任何一种特定的安全特性。新的安全协议、加密服务提供者或者第三方的验证技术,可以方便地结合到 Windows 2000 的"安全服务提供者接口"(Security Service Provider Interface SSPI)中,供用户选用。

Windows 2000 意识到用户对于向下兼容的需要,完全无缝地对 Windows NT 4.0 的网络提供支持,提供对 Windows NT 4.0 中采用的 NTLM(NT LAN Manager)安全验证机制的支持。用户可以依照自己的步调迁移到 Windows 2000 中替代 NTLM 的 Kerberos 安全验证机制。

1.6.2 Windows 2000 中的验证服务架构

通过安全服务提供者接口(Security Service Provider Interface, SSPI),Windows 2000 实现了应用协议和底层安全验证协议的分离。不管是 NTLM、Kerberos、Secure Channel (Web 访问的常用验证方法),还是 DPA(Distributed Password Authentication, 社团/内容网站常用的验证方法),它们对于应用层来说都是一致的。应用厂商还可以通过 Microsoft 公司提供的 Platform SDK 产品包中的 Security API 来开发自己的验证机制。

1.6.3 Kerberos 的验证机制

Kerberos 是在 Internet 上长期被采用的一种安全验证机制,它是基于共享密钥的验证机制。Kerberos 协议定义了一系列客户机、密钥发布中心(Key Distribution Center, KDC)和服务器之间进行的获得和使用 Kerberos 票证的通信过程。

当已被验证的客户机试图访问一个网络服务时,Kerberos 服务(即 KDC)就会向客户端发放一个有效期一般为 8 个小时的"会话票证"(Session Ticket)。网络服务不需要访问目录中的验证服务,就可以通过会话票证来确认客户端的身份,这种会话的建立过程比 Windows NT 4.0 中的速度要快许多。

Kerberos 加强了 Windows 2000 的安全特性,它拥有更快的网络应用服务验证速度,允许多层次的客户/服务器代理验证,并可以跨域验证,建立可传递的信任关系。可传递的信任关系的实现是因为每个域中的验证服务(KDC)信任都是由同一棵树中其他 KDC 所发放的票证,这就大大简化了大型网络中多域模型的域管理工作。

需要全本请访问 www.ertongbook.com