

Windows 2000 Server

Windows 2000 Server

Windows 2000 Server

Windows 2000 Server

Windows 2000 Server

Windows 2000 Server

Windows 2000 Server

Windows 2000 Server

Windows 2000 Server

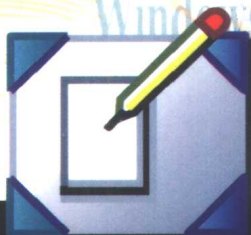
Windows 2000 Server

Windows 2000 Server

Windows

2000

Server



实用组网技术

(中文版)

许书明 等 ● 编著



华航Z0174196



电子工业出版社

Publishing House of Electronics Industry
URL: <http://www.phei.com.cn>

Windows 2000 Server

实用组网技术 (中文版)

许书明 等编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 提 要

本书以通俗易懂的方式,在介绍Windows 2000中文版各项新增功能及其涉及到的各种网络与通信原理的基础上,阐述了Windows 2000组网的基础技术,详细论述了组网时遇到的实际问题、具体步骤及解决方案,并重点介绍了基于Windows 2000 Server组网时的网络资源共享、网络安全性等一系列用户较关心的技术问题。全书共分12章,首先介绍了Windows 2000 Server中文版的新特色、Windows 2000的安装、Windows 2000的操作与维护、Windows 2000组网技术基础、网络用户账号及组账号的管理、分布式文件系统、网络打印的共享与管理、Windows 2000网络设计、网络的维护与检修、数据的管理与保护、Windows 2000的安全性,最后介绍了Internet信息服务器的创建和管理。

本书内容翔实、技术分析透彻,适合于对Windows操作系统有一定应用基础的中高级用户阅读,也可供从事Windows 2000网络集成与网络管理的用户参考。

图书在版编目(CIP)数据

Windows 2000 Server实用组网技术(中文版)/许书明等编著.-北京:电子工业出版社,2000.8
ISBN 7-5053-6123-6

I. W... II. 许... III. 计算机网络-操作系统(软件), Windows 2000 IV. TP393

中国版本图书馆CIP数据核字(2000)第68096号

书 名: Windows 2000 Server实用组网技术(中文版)

编 著: 许书明 等

责任编辑: 春 丽

印 刷 者: 北京天竺颖华印刷厂

装 订 者: 三河金马印装有限公司

出版发行: 电子工业出版社 URL: <http://www.phei.com.cn>

北京市海淀区万寿路173信箱 邮编: 100036 电话: 68279077

北京市海淀区翠微东里甲2号 邮编: 100036 电话: 68207419

经 销: 各地新华书店

开 本: 787×1092 1/16 印张: 17.5 字数: 420 千字

版 次: 2000年8月第1版 2000年8月第1次印刷

书 号: ISBN 7-5053-6123-6

TP·3266

定 价: 27.00元

凡购买电子工业出版社的图书,如有缺页、倒页、脱页请向购买书店调换,若书店售缺,请与本社发行部联系。

前 言

Windows 2000是微软公司集十几年的软件开发经验而推出的最新成果，也是历史上最大的一个商用操作系统家族。它凝聚了许多优秀的软件开发人员的智慧和心血，继承了Windows NT 4.0和Windows 98的优点，并几乎集成了当前Windows系统平台的所有功能，可以广泛地支持各种硬件设备和流行软件。

最新推出的Windows 2000家族包括了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，其中Windows 2000 Server将是服务器版本中最重要、应用最广泛的产品。

作为面向网络应用的新一代服务器主流操作系统，Windows 2000 Server提供了网络文件和打印服务、应用软件服务、Web通信服务、Internet信息服务等一系列完善的网络服务。例如，它不仅在网络的稳定性和可用性等方面进行了重大的改进，使基于Windows 2000的网络具有更高的安全性和可靠性；而且采用了基于Internet标准的活动目录服务接口，建立了一套全面的、分布式的底层服务结构。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Windows 2000的基础上编写了本书。本书内容围绕构建Windows 2000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的各项新功能和有关网络与通信原理方面的理论知识的介绍，又注重通过实际的操作过程让读者了解基于Windows 2000活动目录的用户和组管理、网络文件和打印的共享与管理等常用操作的机理。

本书是集体劳动的结晶，参加本书编写的人员除封面署名外，孔祥丰、邱丽、曹木军、王维、胡辰浩、王军、李万红、翟志强、张菊英、杜杰霞、刘春晓、张军、刘新、李文珍，李剑峰、刘秀英、李娟、曹峰以及杨浩等人也参加了本书的编写、整理和录排工作。由于创作时间紧迫，加之我们水平有限，书中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。

编 者

目 录

第1章 Windows 2000的新特色	1
1.1 Windows操作系统的发展过程	1
1.2 Windows 2000 Server简介	2
1.3 Windows 2000新增功能	3
第2章 Windows 2000 Server的安装	17
2.1 安装Windows 2000 Server的系统需求	17
2.2 安装前的准备工作	17
2.3 安装Windows 2000 Server	25
2.4 启动Windows 2000 Server	30
2.5 关闭Windows 2000 Server	32
第3章 系统的操作与维护	34
3.1 管理应用程序	34
3.2 使用Windows资源管理器	41
3.3 文件与文件夹的操作	50
3.4 使用回收站	56
第4章 Windows 2000组网技术基础	59
4.1 网络基础知识	59
4.2 网络结构	71
4.3 配置Windows 2000网络	75
4.4 添加网络域控制器	81
第5章 网络用户账户及组账户的管理	90
5.1 管理用户账户	90
5.2 管理组账户	97
5.3 管理组织单位	103
5.4 系统策略管理	106
第6章 分布式文件系统	113
6.1 理解分布式文件系统	113
6.2 分布式文件系统的优点	115
6.3 创建分布式文件系统	116
6.4 管理分布式文件系统	125

第7章 网络打印共享与管理	128
7.1 网络打印概述	128
7.2 安装Windows 2000打印设备	132
7.3 设置打印属性	141
7.4 管理打印作业	147
第8章 Windows 2000的网络设计	152
8.1 RAS的原理	152
8.2 配置远程访问服务器	154
8.3 配置拨号网络	164
8.4 跨域管理	170
第9章 网络检修与维护	175
9.1 计算机不能访问网络的原因	175
9.2 瓶颈问题的确定	176
9.3 故障的排除	181
9.4 使用网络监视器	183
9.5 使用性能监视器	189
第10章 数据的管理与保护	196
10.1 备份和还原	196
10.2 文件系统的维护	205
10.3 磁盘管理器	207
10.4 维护磁盘	211
10.5 使用磁盘配额	215
10.6 Windows2000的故障恢复	219
第11章 Windows 2000的安全特性	222
11.1 安全特性	222
11.2 影响网络的安全因素	226
11.3 账户和组的安全性	228
11.4 域的安全性	230
11.5 文件系统的的天性	235
11.6 IP安全性管理	239
第12章 创建Internet信息服务	243
12.1 IIS概述	243
12.2 使用IIS	248
12.3 管理IIS	261

第1章 Windows 2000的新特色

Windows 2000是微软公司的新一代操作系统。它是在Windows NT 4.0操作系统的基础上开发的,集Windows NT的技术和Windows 9x的优点于一身,并在此基础上开发了许多新功能和特性,而且提供了更高层次的安全性、稳定性和系统性能。Windows 2000将取代Windows 9x成为标准的桌面系统,它不仅适合个人办公和联网的台式机,而且还适合工作小组甚至用于整个公司运作的服务器。

1.1 Windows操作系统的发展过程

从DOS 1.0、Windows 3.1、Windows 95/98到Windows 2000的演变,不仅是一部微软公司从依附在IBM之下的小公司到世界第一大软件巨人的进化史,也是一个由计算机软硬件和使用者互动发展的过程。下面我们将就微软公司操作系统的演变过程,谈谈计算机软硬件领域的相应变革以及给用户带来的影响。

1.1.1 MS-DOS

从1981年DOS 1.0到1997年隐藏在Windows 95下的DOS 7.0,操作系统的发展历经16个年头,其功能也逐渐地从基本的磁盘I/O功能发展到拥有网络连线和存储器管理。然而,DOS的指令一直是许多刚接触电脑的人的噩梦:一大堆的内部、外部命令要死记硬背,出现操作错误系统只会告诉用户“Bad command or file not found”而没有具体的误操作提示。虽然DOS的使用不容易掌握,对于硬件限制也很多,但是简单的基本架构和多样化的应用软件,都使得DOS在电脑进化的过程中,仍然保留有它的一席之地。

1.1.2 Windows 3.x

Windows 3.x是微软公司图形化操作系统的一大进展,在此之前的Windows 1.0/2.0由于支持的应用软件很少,都没有被广泛使用。Windows 3.x虽然只能算是一个附属在DOS下的操作系统,但是图形化的界面与图标、文件管理等,让一般的用户都为之耳目一新。原本需要输入指令的动作变得简单了许多,只需鼠标移一移、点几下就能完成。此时也正好是图形化的Internet与World Wide Web刚开始兴起的时候,当别人都还在使用纯文字的Telnet上BBS浏览Web时,Windows 3.x却可以用Mosaic浏览器看到图文并茂的网站。而且当时的多媒体网页并不多,网页元素也不是很庞大,因此浏览的速度还不算慢。有了这些优势,微软公司的Windows 3.x为日后Windows家族的长足发展奠定了坚实的基础。

1.1.3 Windows 95

1995年,微软公司发布了划时代的Windows 95操作系统。从技术角度来看,Windows 95是一个32位的操作系统;从使用者角度来看,它则是一个完整的图形化操作系统。Windows

95的出现,使得硬件设备的需求向前迈进一大步。Windows 95可以算是一个完全脱离DOS文字模式的操作系统,“开始”菜单、工具栏等Windows系列的创举在当时令许多用户感到惊奇不已。

1.1.4 Windows 98

虽然Windows 98是许多人期待的操作系统,发行时间也由预定的1997年延至1998年,而且一般认为Windows 98与Windows 95之间的差异并不大,但它还是在许多方面做了改进:更加易用、支持新的硬件标准、提高了程序运行效率以及与Internet的完全集成。

微软公司在1998年10月底公布了下一代Windows操作系统NT 5.0的新名称——Windows 2000,正式将操作系统带入21世纪。微软公司早在1988年就成立了Windows NT开发部门,并于1993年7月23日成功推出Windows NT第一版:Windows NT 3.1和Windows NT 3.1 Advanced Server。长期以来,Windows NT系统给人的感觉就是给专业技术人员使用的操作平台。虽然微软公司在推出Windows NT Workstation时其主要设计思想就是面向一般终端用户,但是实际上许多人仍然期待Windows 98的上市。

这次微软公司推出的Windows 2000大胆地抛开了NT的包袱,把新一代操作系统的名称由原来预定的Windows NT 5.0改为了Windows 2000,目的是希望能让所有用户都知道,Windows 2000不只适用于高级工作站,也适用于一般用户。

1.2 Windows 2000 Server简介

微软公司发行了三种版本的Windows 2000 Server: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部门服务器的Windows 2000 Advanced Server、用于运行核心业务的数据中心服务器系统Windows 2000 Datacenter Server。下面我们简单分析一下这三种版本各自的特性。

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)的新系统。

Windows 2000 Advanced Server (以前的Windows NT Server 5.0企业版)是较强大的针对部门和应用程序的服务器,它集众多网络操作系统和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密集型的工作,而且把群集及负载均衡相集成以便提供优秀的系统和应用程序的稳定性。

Windows 2000 Datacenter Server将是微软公司所提供的功能最强的服务器操作系统。它支持多达32路的SMP系统及64GB物理内存(取决于系统构造)。与Windows 2000 Advanced Server一样,群集和负载均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事务处理。

无论哪种Windows 2000 Server,它们都有其突破性的特点:

- 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重要的Internet服务集成,Windows 2000 Server系列使建立并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规模性。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。

- 强大的端对端管理

Windows 2000 Server为你的服务器、网络和基于Windows的客户系统提供综合的管理服务, 这使得管理诸如Windows NT Workstation或Windows 2000 Professional等的系统更加简单容易。

1.3 Windows 2000新增功能

随着Internet和Intranet的迅速发展和各种硬件配置的增强, 人们对网络操作系统提出了越来越高的要求。Windows 2000 Server采用了先进的体系结构, 支持多种类型的CPU和对称的多处理结构, 并融合了许多具有使用价值的新技术和新功能。Windows 2000 Server提供的网络功能, 使其不仅可以作为网络邮件服务器和打印服务器, 它还包括文件服务器、网络和防火墙功能, 而受到了大家的喜爱。同时, Windows 2000 Server还可以轻松完成诸如桌面操作、文件管理、环境设置, 以及系统的维护和性能的优化、磁盘和文件系统的管理、用户账号的管理、网络访问等功能, 充分体现了对Internet支持的优势。

1.3.1 终端服务

终端服务戏剧性地改变了用户使用Windows客户机和服务器的传统方式, 不管对于前台还是后台的系统来说, 它都是一个巨大改变。微软公司的Windows NT Server 4.0 Terminal Server Edition是一个在技术上有重大突破的技术, 它能够让微软公司Windows NT Server操作系统支持基于Windows的终端, 也能够把Windows操作系统系列扩展到超级瘦客户端上。这一新技术带来了企业客户一个基于Windows计算环境的全新扩展, 其中包括更低的总拥有成本, 熟悉的32位Windows用户界面, 强大而多样的Windows操作系统系列产品。

客户机和服务器通过TCP/IP协议和标准的局域网构架联系。终端客户端把客户机的鼠标、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, 它们相互之间作为不同的会话(Session)是隔离的。

在Windows 2000 Server中, 终端服务器已经成为一个标准的服务, 用户可以在标准的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, 可以同时察看和编辑多国语言。

终端服务的特点

Windows NT Server Terminal Server版是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操作系统和运行基于Windows的应用程序的体验。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, 访问16位或32位基于Windows的应用程序;

- 基于Windows的终端 (Windows-Based Terminal, WBT)，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Windows 3.11操作系统的16位基于Windows的桌面。处理同上。
- X-based Terminals、Apple Macintosh、MS-DOS、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WinCE的ROM、网卡和显示卡的三合一或二合一PCI卡，可以改造无盘工作站，使之迅速提升到能够运行Windows NT的水平。

Windows 2000 Sever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，除了多国语言支持之外，改进之处还包括：

- 支持本地的打印机：这是微软公司在Terminal server Edition 4.0发布之后，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，本地打印是一个必须的功能。因此，Windows 2000的终端服务加强了对本地打印的支持，这是通过“虚拟通道”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，指导它来完成特定任务。微软公司的技术中已经有两种方式实现远程控制：Systems Management Server 2.0和NetMeeting 3.0。微软公司把这种远程控制的机制做到了终端服务中，只要管理员权限足够，他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。
- 嵌入在Web浏览器中的终端客户端。微软公司计划在发布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了。

终端服务的价值

Windows 2000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，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，使得WBT客户端没有办法上载数据，保证不受病毒的侵害；不能下载数据，保证了资料不至于被复制流失而泄密。
- 先进的32位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和使用经验。这有利于比竞争对手领先一步，提供更好的客户服务或为企业自身服务，获得先机。

- 对于软件开发企业来说, 内部的开发人员可以在安装了Office的终端服务器上处理办公事务, 而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作实际演示。甚至可以为用户在Internet上架设终端服务器。
- 对于移动办公的用户来说, 可以通过远程拨号上网, 启动Terminal客户端, 访问办公室桌上的OutLook来读取邮件, 这比用远程客户机上的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, 而是直接在局域网上的桌面上打开, 仅仅传递屏幕显示, 因而速度会有很大改善。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, Terminal Service提供了对服务器的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), 由于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, 而成为网络管理员强有力的工具。

1.3.2 活动目录

Windows 2000 Server最核心的技术是它的活动目录技术, 微软公司在改进“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”集成在系统中并采用了Internet的标准技术, 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, 并使用户能更容易地找到企业网为他们提供的资源。

活动目录的发展过程

微软公司在Windows NT Server 4.0中就已经贯彻了目录服务的思想。NT的“域(domain)”的概念是目录服务的一个基本单元。“单次登录(Single Logon)”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、Email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, 进一步发展了“活动目录(Active Directory)”。活动目录充分体现了微软公司产品的“ICE”, 即集成性(Integration)、深入性(Comprehensive)和易用性(Ease of Use)等优点。活动目录完全是一个可扩展、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外联网的需要。

活动目录是从一个数据存储开始的。它采用的是Exchange Server的数据存储, 称为: 可扩展的存储服务(Extensible Storage Service)。其特点是不需要事先定义数据库的参数, 而可以做到动态地增长, 性能非常优良。在这个数据存储之上已建立索引, 因此可以方便快速地搜索和定位。活动目录的分区是“域(Domain)”, 一个域可以存储上百万的对象。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, 微软公司建立了一个对象模型以构成活动目录。这一对象模型支持LDAP, 还可以管理和修改Schema。Schema包括了在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, 并且在整个域森林中是惟一的。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、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服务。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; 同时不管用户从何处访问或信息处在何处, 都可对用户提供统一的视图。

活动目录的集成性

微软公司的活动目录生动地结合了三个方面的管理内容: 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服务都集成在一起, 提供了具有变革性的价值。

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、个人主页地址、在公司中的职位关系等, 可以在活动目录中用右键单击用户对象发送邮件和访问其个人主页等。其职位关系可以在公司的内部网上以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。在活动目录中, 支持全局性的查找, 比如查找在整个网络中的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@hch.kb.com或User@kb.com的快捷方式来表征, 以便登录网络等。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, 从而构成一棵域树。如果你的公司兼并了另外一家公司, 你的域树可以和它们的域树workgroup.com建立起整个的域森林来。DNS (domain name service, 域名服务) 在此充当了名字解析功能, 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, 微软活动目录这种基于Internet标准的做法, 给用户带来了几乎无穷的益处。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第五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) 是微软公司和思科公司共同提出来的, 旨在提高网络可管理性和提高网络服务质量。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, 并支持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平台上的新一代应用程序。应用程序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service绑定信息, 通过Group Policy配置应用程序, 进行Just In Time应用下载和应用改变的自动通知等。比较典型的一个基于目录的应用例子是NetMeeting。在活动目录的环境中, 用户只要在NetMeeting中敲入同事的Email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。

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极少的几个对象, 也可以存储上亿万的对象。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。一个目录存储中仅仅包括了这个域中的所有对象。当域树建立起来之后, 每个域都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, 响应最好。域的目录存储还可以有很多的副本, 副本之间自动地完成同步, 并进一步提高响应速度和服务可获得性。

这种域树和域森林的方法, 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, 或者成为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不仅可以解决很多管理上令人头疼的问题, 并且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, 并且借助全局目录 (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可以在现有的Windows NT 4.0的环境中工作, 保护现有的投资; 微软公司也提供一系列的工具帮助4.0的用户迁移到Windows 2000的目录环境中。微软公司提供DirectoryConnector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, 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, 保证及时更新并且更新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, 并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。

活动目录的易用性

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

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的命令特别安装。目录服务还可以卸载, 而不用像在安装Windows NT 4.0那样, 一开始就要定终身: 区分是域控制器还是Member Server, 这两者之间不可转换。

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, 非常方便。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，以便于实施策略管理等。

在活动目录安装之后，主要有三个活动目录的微软公司管理界面（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站点管理，可以把域控制器置于不同的站点。一般局域网的范围内为一个站点，站点内的域控制器之间的复制是自动进行的；站点间的域控制器之间的复制，需要由管理员设定，以优化复制流量，提高可伸缩性。从活动目录管理界面还可以对SDOU（站点、域和组织单元的统称）右键单击，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。右键单击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于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进入安全模式来进行目录服务的恢复，保证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进行关键业务的用户，只有他们才能在实践中体会活动目录的优势。

1.3.3 网络服务

现代企业在其内部架设网络，已经成为一种时尚，而文件和打印的共享服务往往是企业架设网络的原始动机。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，成了一个新兴的热门话题。接下来我们就介绍Windows 2000 Server在这三个方面的新特性。

在当代的企业中，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，文件都要打印出来才能分发到相关的人员和部门中；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经费，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，如何在提高信息处理效率的同时降低存储的成本。而所有这些问题，就是Windows 2000文件/打印/存储服务要解决的重点。

完善的文件服务

Windows 2000 Server在Windows NT Server 4.0的高效文件服务基础上，加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中已经存在的一个文件服务, 但是在Windows 2000中得到了增强。它的作用是不管文件的物理分布情况如何, 就可以把文件组织成为树状的分层次逻辑结构, 便于用户访问网络文件资源、加强容错能力和均衡网络负载等。Windows 2000、Windows NT 4.0和Windows 98系统中都已安装了带有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微软公司管理界面 (MMC) 中创建一个DFS的根, 推荐将其建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存放共享文件夹; 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, 新进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, 而再不会迷失方向, 也无需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的文件系统, 它在NTFS 4的基础上, 增加了两个新的特别访问权限: 权限改变和拥有所有权。“权限改变”的访问权限, 与常用的“完全控制”的访问权限相比, 只可以改变某些文件/文件夹的权限属性, 而不能够增加或删除文件, 因而使管理更加细致。“拥有所有权”的访问权限可以用在一个员工离开公司后, 接替他的员工需要拥有其所拥有的文件的场合。

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问题: 磁盘配额。磁盘配额是Windows NT 4.0的用户要求增加的最为迫切的一项特性。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, 可以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的方式。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、对于攻击有防御能力, 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、落入不法分子手中, 即使不法分子重新安装操作系统, 原有的文件业务也无法访问, 这就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私钥丢失的情况下, 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定位, 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, 并且默认支持全文本的搜索。一旦安装之后, 所有的更新和索引创建/优化工作都是全自动的。在Windows 2000中建立索引的控制也更好, 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。

磁盘管理是为用户的磁盘存储器管理提供了许多新功能的图表工具, 它主要包括:

- 支持新的动态卷。有了动态卷导向的磁盘系统，用户就不需要再忍受每个磁盘只能有四个分区的限制了。
- 联机磁盘管理。用户不需要关闭系统或中断就可以完成管理员的任务。大多数配置的更改几乎立刻就能生效。
- 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。

强大的打印服务

用户在自己家的电脑上安装了Windows 2000 Server之后，当把自己的打印机连接到计算机，从控制面板的打印机中增添一台打印机时，会发现Windows 2000可以对本地打印机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，但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，用户只需找到此打印机，右键单击，选择“连结”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，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：开设在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，必须运行微软公司的Internet Information Server或者Personal Web Server，这些都支持标准的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。查找打印机的选项卡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，可以输入是否双面打印或按特殊分辨率打印等信息。一旦运行了查找打印机之后，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。

崭新的存储服务

随着Internet和Intranet的发展，网络用户数量迅猛增长，多媒体数据、内容导向的数据和32/64位计算的普及，造成了对于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。微软公司在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。同时也提供了自我描述的磁盘、简化的任务和直观的用户界面。

微软公司在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一个不能启动或装载Windows 2000的系统。顺便提一句,管理员通常可以在系统启动时按F8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,能够不增加磁盘就可以在服务器上增加新的自由空间。RSS自动地监测在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CDROM等比硬盘每兆空间更便宜的介质,这种存储的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在文件系统中加入对文件在远程存储上的位置的指针,文件系统可以依据这一信息来获得文件。这一切对于应用和用户来说都是透明的,很容易使用。

Windows 2000也支持先进的数据传输协议,比如I2O、光纤通道和1394等,数据传输性能的提高,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卡一种特性;光纤通道支持超过每秒1GB的传输速率和超过10公里的光纤长度,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。

除了上述光纤通道支持之外,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,能够方便地把可移动存储(如CDROM塔、磁带等)Mount或Dismount,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,自动地按照设定的规则,在介质池中移动文件。

Windows 2000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。

Internet信息服务

熟悉微软公司Windows NT Server 4.0的用户,都知道Internet Information Server 4.0(简称IIS 4)。在Windows 2000中,微软公司更新了IIS的版本,推出了IIS 5.0。IIS 5.0比4.0提供了更方便的安装与管理,增强的应用环境,基于标准的发布协议,改进的性能表现和扩展性,以及更好的稳定性和高可用性。

IIS 5.0的一个特点是不再需要特别安装,当用户安装了Windows 2000 Server之后, IIS 5.0就已经安装好了。微软公司还提供了很多的管理向导,比如“权限设置向导”来帮助设定和协调Web访问和NTFS文件的访问权限,“服务器证书向导”来给服务器安装电子证书等。IIS 5.0作为一个应用环境,还有对ASP增强的支持,比如无脚本ASP页面的快速处理、HTTP和HTTPS(安全通道访问方式)共享状态等。

IIS 5.0的设计目标中有一条:便于企业用户在一个基于Web的环境中共享和发布信息。所以,用户可以通过桌面上的“网上邻居”属性中的“添加网上邻居”来使某个网络位置用