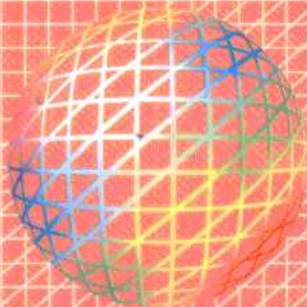


15



文已盡而意未盡

高效配置与管理

Windows 2000 Server

[美] Matthew Strebe 著

邱仲潘 译

每周 7 天,

每天 24 小时

保证网络全天候运转

使你成为

真正的网管专家

seven

電子工業出版社

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



TP316.86 193
S81



网络管理技术丛书

seven Windows 2000 Server

高效配置与管理 Windows 2000 Server

〔美〕 Matthew Strebe 著

邱仲潘 译

电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 提 要

本书详细介绍Windows 2000 Server的配置与管理技术,包括操作系统工作管理、网络计划、日常维护、查错与优化等内容,总结了作者多年的网络管理经验,是Windows 2000网管员的必备资料,也是深入学习Windows 2000管理的宝贵资料。



Copyright©2001 SYBEX Inc., 1151 Marina Village Parkway Alameda, CA 94501. World rights reserved. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without the prior agreement and written permission of the publisher.
本书英文版由美国SYBEX公司出版,SYBEX公司已将中文版独家版权授予中国电子工业出版社和北京美迪亚电子信息有限公司。未经许可,不得以任何形式和手段复制或抄袭本书内容。

图书在版编目(CIP)数据

高效配置与管理Windows 2000/(美)斯特伯(Strebe, M.)著;邱仲潘等译.一北京:电子工业出版社,2001.7

书名原文:Windows 2000 Server 24 Seven

ISBN 7-5053-6830-3

I. 高… II. ①斯… ②邱… 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047298号

书 名: 高效配置与管理Windows 2000 Server

著 者: [美] Matthew Strebe

译 者: 邱仲潘

责任编辑: 马振萍

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: 68252397

经 销: 各地新华书店

开 本: 787×1092 1/16 印张: 24.5 字数: 630千字

版 次: 2001年7月第1版 2001年7月第1次印刷

书 号: ISBN 7-5053-6830-3

TP·3858

定 价: 42.00元

版权贸易合同登记号 图字: 01-2001-1195

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调换。



前言

Windows 2000是个惊人的操作系统，同时也是个烦人的操作系统。如果计划得当，则支持Windows 2000相当容易，但如果计划不当，则网络体系结构可能无法满足网络增长的需求，从而使你不知所措。本书帮你进行Windows 2000网络的正确决策，并指出管理员（包括我自己）经常遇到的陷阱。Windows 2000是目前最高级也最复杂的软件，是全球最大的软件开发公司推出的标志性产品。其复杂性既好又坏，但只要正确管理，就可以兴利抑弊。本书将介绍如何正确管理Windows 2000。

尽管Windows 2000的用户界面与Windows 98相似，但它实际上是Windows NT的升级产品。事实上，Windows 2000在Beta测试阶段前一直称为Windows NT 5。尽管Windows 2000基于Windows NT，但在操作系统内部进行了巨大的改进与升级，管理界面也焕然一新。NT 4与NT 3.51的主要差别在于桌面用户界面，大多数管理工具都是相似的，只要熟悉Start菜单和Windows Explorer，这两个操作系统的管理差别就不大了。Windows 2000中的每个管理工具都大有不同。所有管理工具被改写成Snap-in，建立了Microsoft Management Console层次式管理工具，提供一致的外观和样子，有标准配置名字空间，便于文档中（和本书）使用。此外，操作系统还增加了许多新的服务与特性，网络堆栈从上到下作了改变，具有新的驱动器模型，改进了网络层传输，可以安全升级与改进Windows网络组件，并增加了Active Directory资源地址服务。

关于本书

本书实际上包含了本人在各种Windows管理与维护方面的六年顾问经验，包括成功的经验和失败的教训。本书的编排注重简明易懂，使本书不是Windows 2000方面的百科全书，而是个操作员手册，主要介绍作者遇到的对多个客户有影响的问题。本书不准备介绍每种奇怪的Windows 2000故障，而是介绍如何避免这些问题。本书不是按Microsoft路线走，而是以实地测试的方法使用Windows 2000。书中包括重大问题（如服务器切换和网络设计）以及小型问题（如确定多宿服务器中的物理适配器）的解决方法。书中会介绍Microsoft文档中遗漏或没有明确说明的问题。

Microsoft公司的TechNet信息光盘是我做顾问工作中的随身必备光盘，也是本书创作过程中的随身必备光盘，也应当成为你日常工作中的随身必备光盘。如果没有预订TechNet，请赶紧预订。没有操作系统制造商提供的权威性技术信息，你遇到奇怪的问题时就只能在黑暗中摸索，不管你有多长的Windows 2000使用经验。本书应配合TechNet光盘使用，而不能取代TechNet光盘。

此外，本书应是Microsoft Resource Kits的补充，而不是Microsoft Resource Kits的竞争者。配置软件时，我不准备重述Microsoft的建议，而只介绍与Microsoft建议不同的部分。什么时候会出现不同的情形呢？在管理超大或超小规模网络时，就可能会出现不同的情形，因为Microsoft公司的建议针对中型网络。我重点介绍小型网络，因为这些用户的手头资源最

少，又不太可能聘请专家帮助。

最后，我几乎每天访问support.microsoft.com，但愿你也如此。我遇到的问题中，几乎80%已经解决，并在这里作了说明。问题看上去越荒唐，就越可能在这里找到答案。

本书的读者

本书适用于Windows NT或Windows 2000系统管理员或想成为系统管理员的人。尽管本书是为自认为已经熟悉Windows NT或Windows 2000的管理员编写的，但本书的读者并不需要已经是个专家。但是，你至少应通过MCSE中的一门课或有相应的Windows 2000知识，因为我要求读者对Windows 2000网络体系结构、网络协议和一般网络有所了解。要充分利用本书，还应在公司中运行Windows 2000。本书适用于大小公司的所有用户。

假设

本书主要针对Windows 2000 Server，介绍旧版操作系统（Windows NT）中的相同部分，同时介绍其他Windows 2000版本中与Windows 2000 Server相似的服务，并说明不同版本的不同特性。通常，这在查错时已经足够了，因为不同Windows 2000版本有极大的相似性，只是包括的服务和几个注册表设置有所不同而已。

我还假设你在Intel平台上运行Windows 2000。我在Alpha服务器方面的经验不多，不能多作介绍。其他平台已经过时，应尽快移植到Intel平台。

Service Pack 1在本书创作期间推出，书中内容如有变动之处，请看www.sybex.com站点中本书的勘误表（称为service packs errata）。

本书的组织

本书分四个部分，涵盖Windows 2000的不同服务周期。第一部分“深入Windows 2000”，介绍Windows 2000技术。第二部分“Windows 2000网络计划”，介绍部署Windows 2000之前要计划的问题和Windows 2000联机时可能遇到的问题。第三部分“Windows 2000日常工作”，介绍Windows 2000与支持组织的日常维护。第四部分“查错与优化”，介绍修复Windows 2000的过程。

本书由以下部分组成，通过它可以使你找到相关内容。

第一部分“深入Windows 2000”

这个部分介绍网络环境中Windows 2000的设计与使用，重点是正确计划和设计体系结构，便于理解本书其他部分。

第1章“Windows 2000核心技术”，介绍Windows 2000的一般体系结构，是读者理解操作系统而不是熟悉Windows 2000的指南。

第2章“正确安装Windows 2000”，介绍如何在最困难的环境中方便快捷地安装或升级Windows 2000。

第3章“存储与容错”，介绍如何用海量存储设备存储与存档。本章还介绍Windows 2000的内部容错机制，介绍哪些更实用，哪些不实用。

第4章“网络协议”，介绍网络协议与路由，以及交换与路由网络体系结构的差别。

第5章“网络服务”，介绍Windows 2000所带的服务，特别是要使用的服务及使用原因。

第6章“Windows 2000安全”，介绍Windows 2000内部安全机制和安全措施。

第7章“路由与远程访问”，介绍将网络与外部世界连接。

第二部分“Windows 2000网络计划”

这个部分介绍网络计划与设计的各个方面，包括物理层到服务器应用程序。重点介绍事先计划如何消除后面的系统故障。

第8章“网络设计”，详细介绍网络设计。包括网络计划与设计的各个方面，以及根据支持的网路使用类型确定需要多少服务器和多少冲突域，同时介绍各种网络技术。

第9章“设计Windows 2000网络”，介绍Active Directory计划与设计，重点介绍实际设计和灵活选项，包括Active Directory快捷实现方法和出现新用途时定期回溯的需求。

第10章“部署Windows 2000”，提供在网络中发布Windows 2000 Professional与Server的模板。

第11章“将网络升级到Windows 2000”，可以从Windows NT或旧版网络操作系统升级到Windows 2000的方法。

第三部分“Windows 2000日常工作”

这个部分介绍网络与网络支持操作的长期维护。

第12章“支持客户机”，介绍如何管理网络中的客户计算机，不管数量有多少，种类有多少。本章介绍建立四层支持结构，迅速响应和解决客户计算机问题。

第13章“支持服务器”，介绍如何管理网络中的多个服务器，深入介绍域管理、高可用性问题。

第14章“信息技术管理”，介绍IT支持组织及如何查错，保证计算机顺利运行。

第四部分“查错与优化”

这个部分介绍处理各种问题的方法，包括查错与优化的理论和实践。

第15章“性能优化”，不仅介绍性能优化理论，而且介绍哪些性能优化最有意义。

第16章“查错理论”，介绍查错基本术语，适用于所有系统。

第17章“查错实务”，是针对Windows 2000的查错指南，可以帮助找出问题和解决问题。

第18章“注册表”，介绍Windows 2000注册表的内容及利用Windows 2000注册表的工具。

附录——有用的注册表键

这个附录包含最常用的Windows 2000注册表中的键，对Windows 2000管理员非常有用。我们加亮显示重要注册表键，以便于查找。

本书（《高效配置与管理Windows 2000 Server》）Web站点www.24sevenbook.com提供了更新材料以及提示和技巧，请来访问！



第一部分 深入Windows 2000

包括:

- Windows 2000体系结构
- Windows 2000版本
- Windows 2000服务
- Windows 2000安装选项
- Windows 2000引导过程
- 使用Windows 2000修复过程
- Windows 2000磁盘存储
- Windows 2000磁盘加密
- 管理存储
- 实现容错
- 核心Windows 2000网络技术
- 选择网络协议
- 网络服
- Windows 2000安装模型
- 组策略
- 实现网络安全
- Internet访问
- 虚拟专用网

第1章 Windows 2000核心技术

Windows 2000是个惊人的操作系统，是迄今为止最复杂也最有用的操作系统。最令人惊奇的是Windows 2000基本体系结构的相对简单性。几个简单的设计决策造就了这个操作系统，几乎能够在任何处理器体系结构的单机上的多个处理器间运行最复杂的软件。

在深入介绍Windows 2000复杂性之前，下面先介绍所有Windows 2000复杂服务所基于的简单概念。了解Windows 2000体系结构之后，一些不可理喻的现象就不难理解了。

本章是针对从Unix等操作系统移植的管理员编写的，但以简明扼要的方式介绍Windows 2000内部工作，即使最老练的Windows NT管理员也会喜欢。我还建立了本书的环境，介绍书中使用的术语。

本书应和Microsoft公司的正式Windows 2000 Resource Kits（资源工具库）一起使用。Resource Kits中包含要执行的每个任务的详细管理过程和管理员工具箱中的各种实用程序。但是，这个资源工具库只面向Microsoft公司的网络世界，因此没有全面介绍管理技术；没有介绍Windows 2000服务中的问题；也没有介绍Microsoft世界之外的任何重大实际案例。

可以把本书看成Microsoft Resource Kits的校订本。

本书主要针对Windows 2000最主要的软件包：Windows 2000 Server。但是，几乎本书的所有内容都适用于Windows 2000的所有软件包，因此本书中Windows 2000一词可以

指Windows 2000的任何当前版本, 包括Windows 2000 Professional。对于只在Windows 2000 Advanced Server或Windows 2000 Datacenter Server等具体产品中才有的特性, 书中将一一指出。

Windows 2000设计目标

Windows 2000是Windows NT的最新版本, Microsoft公司用Windows NT产品直接在文件服务器和小型应用程序服务器市场中与OS/2、NetWare与Unix竞争。Windows 2000在Beta阶段称为Windows NT 5, 但Microsoft将其更名为Windows 2000, 减少从基于MS-DOS的Windows 9x升级的用户心头的困惑(有趣的是, Northern Telecom公司拥有网络市场中的NT商标, 这可能也与改名一事有关)。

从那以来, 微处理器的功能已经可以和传统的大型机处理器相媲美, 小型机和大型机市场已经被运行Windows 2000的微型计算机取代, 因此, Windows 2000也已成为一个应用程序服务器。

从早期Windows NT以来, 网络操作系统市场已经大有改变, OS/2已经不再是竞争对手; Novell NetWare迅速失去市场, 使Novell公司这几年惨淡经营。但是, 尽管NT在商业性竞争对手面前取得了惊人的成功, 但却在普通的竞争者面前失去了Internet服务商场, 那些竞争者就是Linux和开放源代码运动。Linux从一个学生课题演变成对软件商业化拥有权的一场革命, 迅速成为Windows NT在几乎每个方面的强大竞争对手。尽管NT目前支持更自然的服务和非常容易配置与管理, 但Linux急起直追, 取得了巨大的行业支持。Linux的发展表明, 不仅可以利用分散无管理的开发工作, 而且分散性也许是超大市场操作系统与应用程序的最佳模型。

为了在强大的竞争者面前成为成功的网络操作系统, Microsoft公司在Windows 2000中支持一些重要的计算技术。这些核心技术包括:

- 多处理
- 多线程
- 巨型应用
- 平台独立性
- 强大安全性
- 向下兼容性

Windows 2000的许多功能实际上是在这个基本体系结构之上运行的服务功能和驱动程序, 如磁盘安全性和网络连接。这些功能见本章稍后“Windows 2000体系结构”一节。

多处理

多处理就是在一台计算机上使用多个微处理器, 换句话说, 就是所有微处理器连接一个内存总线。这个功能使多个微处理器可以处理同一问题, 而不发生网络通信开销过大的问题。这对处理要求很高的任务(如图形绘制或轨道计算)和对高负荷应用程序服务器(如Web与数据库服务器)提供更多处理功能非常有用。Windows 2000实现对称多处理(SMP, symmetrical multiprocessing), 即所有处理器负荷均匀。本章稍后“Windows 2000版本”

一节的表1.1中将介绍Windows 2000变体与多处理器支持之间的关系。

多线程

多线程（Multithreading）使多个程序可以同时运行，使一个程序（进程）可以同时执行多个线程。多线程的详细介绍见本章稍后“Windows 2000体系结构”一节。

实际校验：多线程应用程序

Internet Information Server (IIS) 的Web服务是多线程应用程序的典型例子。启动Web服务器时，一个线程中运行的代码监听TCP端口80的连接。Web浏览器发出连接请求时，这个监控线程立即派生一个新线程，运行回答连接的代码。这样就使监控线程可以继续收听新连接，而不受中断，并提供每个Web服务器连接的专用线程。多线程使服务器应用程序很容易编写，Windows 2000中的所有多用户服务都是这样工作的。

大地址空间

有效使用巨量内存的巨型应用程序需要“平台”或线性的32位内存空间（或4GB）。但是，Windows 2000将高位用于区别内核方式与用户方式，因此用户进程实际上只能使用31位（2GB）。

Windows NT（Windows 2000所基于的产品）开发人员没有想到应用程序会需要超过32位地址空间。开发Windows NT时，2GB硬盘还不存在，更不用说对一台机器提供4GB内存的动态内存模块。但是，新的软件开发总是会利用新硬件开发提供的资源，Windows 2000能很好地适用巨量内存。由于这两点，Windows 2000的Terminal Service功能和一些企业应用程序可能利用比Windows 2000提供的内存空间更大的空间，一些大型公司用户开始抱怨Windows 2000的2GB局限。

Windows NT Server 4企业版中提供了这个问题的临时补救方法。boot.ini文件中可以增加新的/3GB开关，将内核配置成用头两位内存将用户空间与系统空间分开，3/4为用户空间，1/4为系统空间。这样就使应用程序可以利用3GB空间，但会有少量性能影响。这个开关也适用于Windows 2000 Advanced Server版本。

Windows 2000 Advanced Server与Windows 2000 Datacenter Server解决了这个问题，通过让Intel公司对x86处理器的地址窗口扩展（AWE，Address Windowing Extensions）来扩展内存管理方案。

MS-DOS有640KB限制，原因是什么呢？8086处理器将内存分为16个64KB的内存条，总共1MB，因为16位处理器只能寻址16位地址空间（64KB字节）。Intel增加4位“页”寄存器（16个惟一值），表示计算机当前处理的64KB内存条。条间交换需要特殊的处理器指令，任何其他处理器指令都不能寻址当前内存条以外的内存。这是程序开发人员的头痛之事，代码必须在单个64KB内存条内运行，否则要正确处理条间交换。前10个64KB内存条是用户内存专用的（640KB），后六个64KB内存条（384KB）是BIOS ROM例程和插入ISA总线的I/O硬件专用的。80286体系结构增加另外4位页空间，将可用内存增加到16MB，仍然分成64KB内存条。

Windows 2000的平台内存体系结构解决了这些奇怪的问题,但仍然只限于32位地址空间(4GB)。尽管这个内存量好像已经很大,但有些应用程序可以利用更多内存。Windows 2000 Advanced Server与Windows 2000 Datacenter Server用相同的内存条寄存器机制分别寻址8GB和64GB。各个线程仍然限于32位地址空间,需要特殊处理器指令进行条间交换。换句话说,应用程序需要4GB以上地址空间时,需要像MS-DOS程序解决64KB内存条边界一样解决4GB局限。本章稍后表1.1将介绍不同Windows 2000版本提供的内存量。

Windows 2000目前正在针对使用64位字宽的Intel Itanium系列处理器开发。真正64位的Windows 2000允许应用程序把巨大的内存当作平面内存空间,而不是分为4GB段。新的Windows API、Win64可能对巨型应用程序迅速取代段间交换,保证段间交换很快就会退出历史舞台。值得一提的是,Microsoft公司还对Alpha发布Win64(已经是个64位处理器,在32位方式中运行Windows 2000),并对AMD公司的Sledgehammer处理器发布Win64,在标准x86系列上增加64位扩展。

平台独立性

平台独立性使Microsoft公司可以迅速将新出现的机器作为Windows 2000平台,不受特定制造商(如Intel)的限制。Windows 2000在抽象虚拟机(硬件抽象层,HAL)中运行,将Windows 2000的硬件访问变为硬件机器要求的内容。这个特性使Microsoft可以迅速移植到任何机器体系结构,只要对新的目标机器创建惟一HAL,然后对该机器使用的微处理器重新编译Windows 2000即可。

说明: Windows 2000实际上只支持Intel微处理器使用的以小尾字节顺序操作的微处理器。尾(Endian)指存储32位字的字节顺序:将最显著字节存放在前面的是大尾,将最显著字节存放在后面的是小尾。大多数现代处理器(除了Intel处理器)都可以在大尾与小尾方式之间切换,但实际计算机可能在硬件中限于一种方式。例如,尽管PowerPC处理器可在大尾与小尾方式之间切换,但Apple Macintosh计算机上通常固定为大尾方式,从而无法将Windows 2000移植到这个平台。

目前,Microsoft支持Windows 2000的前身Windows NT的四种微处理器体系结构:

MIPS NT最初是在MIPS计算机上开发的,但此后MIPS不再发展。

Intel 32位体系结构 这个体系结构包括过时的386与486、Pentium和Pentium Pro处理器,以及当前Intel的Celeron、Pentium II、Pentium III和Xeon处理器以及AMD 6x86与Athlon处理器。

Digital Alpha 由于Compaq拥有这个处理器,因此前途未卜。Hitachi公司是Alpha处理器的第二大供应商,继续沿Digital发展路线发展。Microsoft公司对Alpha处理器开发了Windows 2000测试版,但还没有发布最后版本,也许永远不会发布最后版本了。

IBM公司的PowerPC PowerPC开发已经停止,因为IBM公司不再生产基于PowerPC的工作站。目前只有Apple Power Macintosh工作站使用PowerPC微处理器。

Microsoft公司不再对Windows 2000支持MIPS和PowerPC微处理器,因为已经没有这方面的市场需求。Alpha处理器的未来因Compaq拥有Digital的半导体而前途未卜,因此Windows 2000可能不再支持Alpha处理器。针对Itanium的下一版Windows 2000正在测试阶段,但是,

尽管与Intel处理器关系密切，但Microsoft的平台独立性承诺仍然很有成效。

强大的安全性

强大的安全性提供的应用程序环境可以保证数据不被同一机器上另一应用程序修改。同一机器上运行的应用程序不会破坏另一应用程序的内存空间，从而防止意外崩溃和恶意窃取数据。尽管Windows 2000的安全性方面已经被发现存在奇怪的缺陷，但这个体系结构仍然是安全的，Windows 2000的安全性绝不逊于任何其他市场影响力大的高级操作系统。但是，厂家（包括Microsoft）经常在Windows 2000内核之上运行的服务与应用程序的安全实现方法中出现错误。这些问题是所有操作系统共有的，Windows 2000的安全体系结构实际上能防止许多缺陷。

实际校验：Windows 2000安全

Microsoft公司平均每周两次提供操作系统的安全热修复，使Windows NT与Windows 2000安全的Microsoft路线很难跟踪。但是，Linux也同样频频推出安全热修复，说明这些操作系统正受到更多黑客和安全研究人员的攻击，因为Internet无处不在。

向下兼容性

Windows 2000支持与现有标准和应用程序的向下兼容性，还支持各种向旧版Microsoft和第三方操作系统提供向下兼容性的应用程序子系统。各种子系统向下兼容性范围包括：

- DOS (Windows 2000 Virtual DOS Machine, NTVDM)
- 16位Windows应用程序 (Windows on Windows, WoW)
- OS/2 1.3 (OS/2子系统)
- POSIX (POSIX子系统)
- OpenGL (OpenGL API)
- Win32

针对这些规范编写的程序如果不直接访问硬件或通过驱动器服务直接访问硬件，则应在Windows 2000中顺利运行。OS/2子系统已经过时，大多数用户并不使用POSIX子系统。Windows 2000 Professional用户经常使用MS-DOS与Windows on Windows子系统，Win32子系统是Windows 2000操作所需要的，因此有时不作为子系统。

强大的Internet连接

Windows 2000利用了Windows NT的组网改进技术。第一版Windows NT不包括TCP/IP堆栈，而最终的Windows 2000则包括了比任何其他操作系统多的Internet连接特性，超过UNIX与Linux，并将其作为操作系统的一部分。与Windows NT不同的是，TCP/IP是Windows 2000操作系统不可缺省的部分，不能删除。Internet连接特性包括：

- 高度优化的TCP/IP堆栈
- RIP、OSPF和其他路由协议的路由支持
- 无状态分组过滤
- 网址转换 (NAT)

- 基于TCP/IP负荷平衡
- TCP/IP-based Quality of Service带宽分配
- IPSec (IP Security)
- Point-to-Point与Layer-2 Tunneling协议
- HTTP、FTP、NNTP与SMTP服务器
- Secure Socket Layer支持
- PPP与Remote Access Server
- 一流Web浏览器

这些改进在Windows NT 4中以松散形式存在,而现在则使Windows 2000成为Internet服务器市场的强大竞争者,可以从Windows 2000客户机无缝连接Internet。

Windows 2000体系结构

Windows 2000是个优先式多任务操作系统,即可以同时做多件事情,不管各个进程是否相互协作。

这些不同进程的调度是内核的事,内存分配和与输入/输出(I/O)设备的通信也是内核的事。内核管理计算机的三个基本组件:内存、处理器时间和I/O。

Windows 2000的物理实现方法是引导过程中装入一系列系统文件。例如,基本内核服务包含在文件ntoskrnl.exe中,而机器的硬件抽象层包含在文件hal.dll中。每个特定系统服务或驱动器有自己的相关文件。对依赖于其他服务的服务(如cdfs.sys光盘文件系统依赖于cdrom.sys设备驱动器),如果相关设备驱动器还没有运行,则这些模块无法启动。服务或驱动器的相关性体现在控制该服务的注册表键中。

内核和所有驱动器共享一个内存地址空间,防止其他进程影响,但并不相互隔离。这个进程内存空间称为内核方式。大多数内核是不分页的,即总是在内存中提供,不能分页到磁盘中。这是因为,这些内核包含控制分页和磁盘驱动器的代码,而且能保证优化性能,因为内核是经常使用的。执行方式中的服务和驱动器是分页的(除非配置成不分页),因为它们不经常使用,对分页功能不重要。

说明: 由于驱动器与内核共享相同的保护空间,因此可能使Windows 2000崩溃。驱动程序编的不好的驱动器和驱动不良硬件的驱动器可能造成蓝屏幕崩溃。

内核分成下列不同组件:

进程管理器 根据请求创建线程和进程。进程就是由一个或几个线程构成的惟一虚拟地址空间。线程就是进程中的惟一执行链,表示Windows 2000中的基本调度实体。线程有自己的内核堆栈、用户堆栈和环境变量(堆栈就是线程计算期间快速存储和读取数据的区域)。

中断处理器 在页故障或I/O调用之类的硬件事件调用时起作用。内核对每个中断调用建立一个中断处理器。内核本身处理一些中断,内核空间的驱动器处理其他中断。

硬件抽象层 使所有计算机在Windows 2000看来是一样的,不管其基于行业标准PC体系结构、高级RISC计算(ARC)体系结构,还是任何其他体系结构。硬件厂家提供

用于非标准PC机器的HAL。

提示：可以把HAL看成计算机主板的设备驱动器。

对象管理器 提供Windows 2000中不同组件的名字空间，如文件、端口、进程和线程，以及系统要跟踪的各种项目。进程可以用对象管理器的服务引用系统中的其他对象。

提示：利用Performance控制台可以浏览对象管理器管理的许多对象。

虚拟内存管理器 控制内存向磁盘分页。除了典型处理功能外，所有新型微处理器都有一个内存管理单元（MMU），对优先式多任务操作系统（包括Windows 2000）的体系结构至关重要。内存管理单元具有三大功能：

地址抽象 对每个进程创建惟一地址空间。每个进程只看到从地址0开始到请求内存长度为止的自由连续内存空间，不管进程是否实际存放在RAM中。这样进程就可以进行整个计算机内存空间的控制而不与另一进程的内存发生冲突。

页保护 防止进程访问对另一进程分配的内存（造成非法访问错误消息）。这就保证一个进程不会使机器上的其他进程崩溃。

虚拟内存 使操作系统可以通过记录I/O设备（如硬盘驱动器）中的内存页和访问这些内存时重调这些页，将I/O存储作为内存使用。这个操作对进程是完全透明的，计算机显示出更多的内存。

提示：用Control Panel中的System小程序指定计算机上如何设置虚拟内存。单击Advanced标签，单击Performance按钮并单击Change按钮。

进程间通信管理器 提供本地过程调用（LPC）功能，在进程之间传递消息。由于进程无法破坏另一进程的地址空间，因此要用LPC功能传输信息。LPC功能就是内核方式与用户方式之间的接口，和远程过程调用（RPC）服务一起使用，后者提供与网络上远程计算机进程的接口所需的抽象。

I/O管理器 表示所有驱动器可以连接的统一接口。I/O管理器处理设备驱动器之间数据和消息的传递，类似于LPC机制进行进程间通信。驱动器通过相关性层依赖于其他驱动器的服务。例如，直接与硬件通信的基本驱动器称为设备驱动器，NTFS文件系统之类的高级驱动器依赖于硬盘设备驱动器存储数据。这种驱动器分层使驱动器可以按特定目的进行抽象。例如，不同存储媒介可以使用相同的文件系统，多个文件系统可以使用相同的存储媒介。

提示：System Control Panel小程序中的Device Manager可以控制I/O管理器功能。

缓存管理器 优化文件访问，用RAM存储经常访问的文件。缓存管理器很像文件系统驱动器与用户级进程间的驱动器层。用户请求的文件在缓冲区时，缓存管理器返回这个文件，而不是访问低速存储媒介。缓存管理器和Virtual Memory Manager一起配合，使用未用的RAM。Virtual Memory Manager需要内存时，先分配缓存内存之后再将活动进程分页到磁盘中。

驱动器 通过基本驱动器之上的相关性分层系统提供I/O设备接口。下节将详细介绍驱动器。

安全引用监视器 限制哪个对象能访问其他对象，从而强制执行安全性。对象请求访问其他对象时，Security Reference Monitor检查访问对象提供的安全标识符和引用对象的访问控制表。如果引用对象的访问控制表中没有这个对象的安全标识符，则拒绝访问。利用这种机制，可以在整个Windows 2000中实现用户级安全性。第6章详细介绍这种机制。

即插即用管理器 控制即插即用驱动器，必要时发出停止和启动命令，支持热可交换硬件与设备探测和安装。

电源管理器 控制电源相关事件和消息的中心，负责监视电池状态，启动、停止和暂停硬件资源以节省电源，控制操作系统的休眠与准备特性。

图形设备界面 提供屏幕上表示图形的界面，包括Window Manager组件，提供基于内容的高级区域（窗口）。在Windows NT 4之前，这个组件在内核之外。Windows 2000将其放进内核中，减少处理器开销和提高操作系统图形性能。

驱动器

驱动器控制硬盘、串口、显示等I/O设备。每个能在Windows 2000中使用的硬件都带有让Windows 2000控制该设备的软件（此外，Windows 2000还有几个公用设备的驱动器）。

驱动器使Windows 2000可以控制各种类型的I/O设备，而不只是编写Windows 2000时存在的设备。驱动器还提供了各种低级服务的抽象，例如，计算机可以通过文件系统驱动器用多种数据结构进行文件存储，以更适合特定设备的特征。

驱动器的体系结构大致相同，但一些重要驱动器类对Windows 2000的操作至关重要：

设备驱动器 直接控制硬件，包括硬盘控制器驱动器、显示设备驱动器等。

文件系统驱动器 控制存储设备中存储数据的结构，允许按指定名称引用数据块（称为文件）。文件系统驱动器控制存储设备的设备驱动器，从而达到这个功能。

网络驱动器 进行数据链上传输数据所需要的各种功能。这些分层功能包括将数据分解为寻址分组，提供命名存储读取和驱动网络适配器。

在Windows 2000早期部署期间，Microsoft公司推出Windows驱动器模型（WDM）规范，使制造商能建立Windows 98和Windows 2000支持的设备驱动器。Windows 2000要求WDM驱动器支持电源管理特性，以便使设备置于准备状态或关闭设备，实现热交换功能。Windows NT中的有些设备驱动器（如声卡驱动器）与Windows 2000在不需要支持电源管理特性时是兼容的。

提示：如果找不到特定设备的Windows 2000驱动器（除了网络适配器），可以试用Windows 98或Windows NT驱动器。这通常是行不通的，但如果可行，则可继续使用本该扔掉的设备。

服务

服务就是没有直接用户界面的应用程序，由操作系统自动启动。服务运行就像按定义用户安全环境登录时一样。服务的配置通常用Control Panel小程序或Microsoft Management Console (MMC) snap-in管理。服务与驱动器的差别在于它们在内核之外，因此不直接影响

Windows 2000的操作（当然，理论上Windows 2000的版本是无缺陷的），只能调用内核。许多服务在引导时自动启动，具有相应的各种安全权限。有些服务是实时启动的。服务用Computer Management控制台中的Service snap-in管理。

服务在执行的保护方式安全环境中操作，但不属于内核。不运行任何服务时，操作系统也可以实际引导和操作。

Windows 2000版本

Microsoft公司目前维护五种Windows 2000版本，但只有四种已成为产品：Windows 2000 Terminal、Windows 2000 Professional、Windows 2000 Server和Windows 2000 Advanced Server。到本书编写时，Windows 2000 Datacenter Server还没有发布。

表1.1比较每个软件包的关键特性。

表1.1 Windows 2000产品选项

产品	可用内存	处理器	群集支持
Terminal	共享	共享	N/A
Professional	4GB	2	N/A
Server	4GB	4	N/A
Advanced Server	8GB	8	2个结点
Datacenter Server	64GB	32	4个结点

Windows 2000 Terminal

Windows 2000 Terminal是Windows 2000 Server的Terminal Services提供的客户机环境，提供与Windows 2000 Professional相似的服务，在瘦客户机和Microsoft Terminal Services客户机中使用。

Windows 2000 Professional

Windows 2000 Professional是Microsoft公司的业务类桌面操作系统，是Windows 95衍生的基于MS-DOS的Win32系列操作系统之后的下一代家庭操作系统。由于Windows 2000在显示游戏和多媒体市场上并不像Windows 95/98/ME那么出色（由于其图形绘制子系统开销很大），因此Microsoft公司还没有合并这两个操作系统系列。

Windows 2000 Professional的重要服务包括：

文件与打印共享 文件共享服务是网络操作系统的基础，使服务器可以作为大型共享硬盘，从而使许多客户机可以访问巨量共享存储空间。用户可以在公司任何地方共享文件，具有基本多用户应用程序的平台。打印共享服务将文档从几个客户机传输到服务器中排队，一次一个文档进行打印。

NetMeeting远程桌面共享 这个服务使IT管理员和培训人员可以连接Windows 2000 Professional用户桌面和进行远程控制，解决问题和介绍软件用法。但是，尽管控制器，但只能识别控制者的输入，而不能像AT&T的免费VNC（Virtual Network

Computing) 工具一样识别双方用户的输入。此外, 这个服务不让用户将桌面控制“发送”给管理员, 使网址转换网络之外的管理员很难访问网址转换网络内部。此外这个服务的性能和特征与VNC极为相近。NetMeeting使用H.323视频远程会议协议, 许多防火墙也无法转换。从好的方面看, NetMeeting允许网络声音、白板使用和其他同时协作。利用NetMeeting远程控制桌面和Terminal Services远程控制服务器之后, Microsoft公司终于为企业中的所有操作系统提供了完整的远程控制服务。

Windows Installer Windows Installer提供描述应用程序安装的标准化格式。通过将描述应用程序安装的格式标准化(用.msi安装包文件), Microsoft提供了远程安装和控制改变的基础。但是, 目前支持Windows Installer的应用程序只有Office 2000组件。除非要安装的每个应用程序都使用.msi安装包文件, 否则要创建自己的.msi包或用其他方法进行远程安装。除非大部分应用程序开发人员都支持Windows Installer, 否则Windows Installer对管理帮助不大。

Windows 2000带有Veritas(原名Seagate) Software公司的WinINSTALL.msi包装工具。这个软件保存计算机文件系统与注册表“前”瞬像并在安装应用程序之后取得“后”瞬像, 将前后瞬像进行比较。然后程序创建安装包, 将前后瞬像之间不同的文件与注册表键复制。重新包装现有应用程序不是特别方便, 特别是需要排除文件时。需要用清洁的计算机(或虚拟机器)创建瞬像。包装器在安装地址方面也不够灵活, 不能启用或关闭部分应用程序安装。除非应用程序带有.msi包, 否则这个方法只在超大型环境中才实用。

即插即用 即插即用是一组设备驱动器, 使操作系统可以管理计算机硬件、重新配置设备资源分配和管理电源。加上支持电源管理的设备驱动器, 许多外设可以实现热交换(不必关闭计算机而从系统中增加与删除)。据我所见, 这是Windows 2000对Windows NT的主要改进之处, 对客户机和服务器提供了大量新的管理渠道。即插即用可以支持全新的技术(如USB与Firewire), 并对现有PCMCIA与CardBus设备大大改进支持。此外, Windows 2000在桌面运行的Microsoft操作系统中消耗的待机电量最少。

Internet连接共享 这个服务是Windows 2000 Server的路由与远程访问服务(RRAS)中网址转换(NAT)组件的简单版本, 提供一个非常简单的界面, 使普通用户可以指定两个网络连接中哪一个“共享”。然后这个服务自动配置该接口上的NAT、DHCP与DNS代理服务, 使连接的计算机可以接收DHCP地址, 只用一个公用IP地址无缝连接Internet。

Windows 2000 Server

Windows 2000 Server是Microsoft的主线服务器操作系统, 给大小公司的网络提供文件、打印、终端、Web和应用程序服务。

Windows 2000 Server可以在一般服务器硬件上运行, 不需要特殊化, 不必与工作站硬件有所不同。能够支持各种硬件使这个操作系统可以用于, 从一天处理几个连接的小部门服务器到处理成千上万连接的海量多处理Internet服务器。

Windows 2000 Server是Microsoft公司最著名的服务器操作系统Windows NT Server 4的直接后代。到Windows NT Server 4发布时, Microsoft占有服务器市场的4%份额, 而到

Windows 2000 Server发布时, Microsoft已经占有服务器市场的50%份额, 80%的新安装都使用Microsoft产品。Windows NT 4已经完全战胜Novell NetWare、OS/2 Warp和大多数专属Unix版本, 只有Solaris与Linux还有一定的市场地位。

Windows 2000 Server希望把余下的空白抹平。Microsoft密切关注目前的主要操作系统对手Linux, 要保证: Linux能做的, Windows 2000 Server都能做, 而且做得更好。Windows 2000 Server中增加的网络服务清单是令人难忘的: Active Directory支持LDAP目录、操作系统集成DNS、Kerberos安全验证、IPSec (这是Linux所不支持的)、网络地址转换与各种路由协议、以及多用户终端对话。Windows NT在管理用户的安全性和便利性方面一直是优秀的。在许多站点中, Unix只用于作为廉价邮件服务, 因为Microsoft没有在操作系统中提供轻量级POP3与SMTP邮件工具。

Active Directory Active Directory实际上是个层次式数据库, 存储配置与网络资源的信息, 如计算机、用户和组。Microsoft将这个简单数据库集成到大多数服务中, 在中央管理地址存放所需的信息和其他相关数据。重要的是Active Directory的服务集成, 而不是数据库本身。Microsoft和第三方创建使Active Directory管理更直观的工具之后, Windows 2000 Server将更加没有对手。

Intellimirror Intellimirror是Microsoft公司的文件复制服务, 改头换面之后集成到Active Directory中。Intellimirror组件可以在不同计算机之间自动复制文件和Active Directory对象, 使信息、应用程序和数据文件发布可以自动化。但这个服务也有一定的局限性, 从而限制其在许多环境中的使用。

组策略 Microsoft扩展Windows NT 4安全策略概念, 使多个不仅影响安全的策略可以根据不同安全组的关联影响同一用户, 从而大大提高管理员的能力, 可以微调控制各个用户对计算机和网络服务的使用。

Kerberos Kerberos验证机制最初是为了实现Unix系统安全性, 对用户验证问题采用加密的概念。Microsoft公司的自然NT挑战与响应验证机制只使用用户口令, 很容易攻破, 特别是集成Internet Explorer时。地球上的任何Web站点都可以悄悄用你的账号名, 试出你计算机上的口令。Kerberos验证提供表示身份的短期“门票”或验证密钥, 只在短时间内有效, 即使黑客能够获取, 得到的也只是过时和一文不值的东西。这样就有效阻止了口令窃取和伪装。

公用密钥结构 (PKI) Microsoft的PKI服务使NTFS Encrypting File Service之类的系统服务可以使用任何PKI兼容的加密算法, 支持许多不同的用户验证方法。这种可扩展安全系统使公司可以在一定管理层选择相应的安全程度, 而不是利用操作系统服务所带的通常不够充分的安全性。PKI对IPSec、Certificate Manager、Secure Socket Layer、验证与登录服务、磁盘加密和操作系统其他加密相关服务提供加密服务。

Macintosh客户机的文件与打印服务 这个服务是早期Windows NT的产物, 因为Apple并没有真正推出强大的服务器操作系统 (尽管进行了许多努力)。Microsoft实现Apple的AppleTalk网络协议, 将其包装在向Macintosh客户机提供文件与打印服务的服务中。由于这个服务仿真Apple文件共享, 因此在Macintosh客户机上不需要安装软件。为此, Windows 2000是大多数Macintosh客户机中的优选网络操作系统。