

精通 Windows XP 管理与配置

周明涛 编著



机械工业出版社
China Machine Press

精通 Windows XP 管理与配置

周明涛 编著



机械工业出版社
China Machine Press

本书详细介绍了 Windows XP 的管理、配置和实现原理。从 MMC 的操作和管理,到 Windows XP 的网络配置,基本涵盖了 Windows XP 中常见的中高级操作知识。

本书在介绍 Windows XP 管理和配置操作的同时,也对其底层所进行的工作进行了必要、全面的描述,这有助于帮助读者更加深入地理解 Windows XP 的核心机制以及实现原理。

本书适合于那些已经基本掌握 Windows XP 的常规操作,并希望更深入地了解 Windows XP 的管理和配置知识的读者。

版权所有,侵权必究。

图书在版编目 (CIP) 数据

精通 Windows XP 管理与配置/周明涛编著. - 北京:机械工业出版社, 2003.2
ISBN 7-111-11622-4

I. W… II. 周… III. 窗口软件, Windows XP IV. TP316.7

中国版本图书馆 CIP 数据核字 (2003) 第 009743 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:于杰琼 李 炎

北京市密云县印刷厂印刷·新华书店北京发行所发行

2003 年 2 月第 1 版第 1 次印刷

787mm × 1092mm 1/16 · 30.75 印张

印数: 0 001-4 000 册

定价: 48.00 元

凡购本书,如有倒页、脱页、缺页,由本社发行部调换

前言

2001年10月25日，微软公司在全球商业中心——纽约举行了隆重的发布会，庆祝微软历史上最优秀的操作系统——Windows XP的诞生。微软公司的董事长兼首席软件设计师比尔·盖茨在这个产品发行会上发表了主题演讲，PC业的众多前沿人物，以及超过50位微软的合作伙伴，都在这个发布会上经历了这一具有历史意义的时刻。在电脑软件的发展历史上，很少有一种软件的地位能够同操作系统相媲美。而在操作系统发展的历史上，Windows XP无疑是当前这个舞台上最受争议也是最引人注目的明星。

正如以前的各种操作系统一样，在经历了市场的惯性和用户逐渐认可之后，直至2002年的年中，Windows XP才真正的流行起来。而在这一年多的时间里，对Windows XP的各种评论就从来没有中断过。从Windows XP的稳定性和易用性，直到Windows XP中最受人诟病的“激活”机制，没有哪个操作系统在发布过后的这么长的时间内，围绕它还能有如此热烈和长久不衰的讨论。

就笔者看来，Windows NT是微软的第一个“稳定”的操作系统；Windows 2000是微软的第一个既“稳定”又“好用”的操作系统，而Windows XP则是微软的第一个既“好用”又“稳定”的操作系统。显然，无论微软是否承认，在给笔者的印象中，Windows XP正试图淡化微软NT系列操作系统在人们心中“稳定而不好用”的印象，淡化“NT内核”的宣传（而这种宣传，在当年推出Windows 2000时比比皆是——看看Windows 2000的启动画面就知道了），而鼓励普通用户将工作的重点全面放到Windows XP上，换句话说，Windows XP是第一个面向普通用户（而不仅仅只是商业用户）的“稳定”的操作系统，它的目标除了希望取代在商业环境中早已经风行的Windows 2000之外，更希望取代在普通用户桌面久驻不去的已经成为神话的Windows 98。在Windows XP的发布会上，比尔·盖茨曾经自豪地说：“随着Windows XP的面世，我们进入了一个全新的、令人振奋的个人计算时代。新版Windows向用户提供了更多令人激动的改进，它充分释放了个人电脑的潜在力量，使人们真正体验到数字世界的极致。”在距离Windows XP的发布已经1年多，Service Pack1也已经及时推出的今天，可以说，Windows XP的确当得起这种评价。Windows XP在“稳定”的基础上，将“好用”的特性发挥到极致，甚至已经远比Windows 98要好用。

虽然Windows XP毫无疑问可以胜过Windows 98，但是它毕竟同Windows 98有着显著的差别，如果仅将Windows XP当做Windows 98来使用，未免显得有些暴殄天物（虽然这可能正是微软针对普通用户的初衷）。要充分发挥Windows XP的高级特性，了解Windows XP的一些核心操作技术是很有必要的。本书的目的就是帮助读者全面掌握Windows XP的高级管理和配置技术。

本书不仅介绍了Windows XP中管理和配置的实际操作方法，也同时深入介绍了在操作底

层所发生的事情。这样读者在学习操作的过程中，同时也可以更深入地了解操作背后的原理和技术。让读者不仅知其然，也知其所以然，这正是笔者撰写本书的出发点之一。当然，Windows XP 是一个博大精深的操作系统，笔者在这方面的尝试可能还比较肤浅。但是应该说，这种尝试对现在渴望深入了解 Windows XP 的读者来说是比较有用的。

本书的另一个特点是不仅介绍了图形界面下的 Windows XP 的管理和配置操作，而且也介绍了如何在命令行下实现类似的任务。Windows XP 是一个非常复杂的操作系统，很多管理任务都只能在命令行下进行。掌握 Windows XP 的命令行操作和管理，无疑能够让您在通往 Windows XP 的专家之途中更加顺利。

除了介绍 Windows XP 本身的管理和配置操作之外，本书也对 Windows XP 的启动和维护进行了比较详细的介绍。特别是故障恢复控制台，这是很多读者可能会感觉困惑的环境之一。本书全面介绍了 Windows XP 的故障恢复控制台的使用，可以确保读者在 Windows XP 的启动排错方面，做到彻底的心中有数。

Windows XP 不仅是一个单机操作系统，也是一个网络操作系统，离开了网络，Windows XP 的很多特色都无从发挥。本书在 Windows XP 的网络方面也有比较深入的介绍。另外，本书也简要（但很全面）地介绍了网络的基础知识，这对于那些已经熟识单机环境，而希望进入网络世界的读者来说是非常有用的。

本书不是一本操作入门书，因此那些诸如如何打开文件夹、使用画图或写字板程序，以及如何利用控制面板安装和删除程序之类的操作都不会包含在本书中。本书针对的是已经会用 Windows XP，但是希望更深入地了解 Windows XP 的核心特性，最终成为 Windows XP 专家的部分读者。对于希望通过微软认证考试 70-210 科目（《安装、配置和管理 Windows 2000 Professional》）的读者，这本书也可以起到一定的参考作用。

本书由个人独立撰写，限于水平，书中的错误和纰漏在所难免，希望广大读者予以批评指正。我的联系地址是 mtzhou@263.net，如果您对本书有什么问题或建议，可以将电子邮件发送到这个地址上，我必将尽力进行答复。

感谢在本书撰写过程中给予我帮助的朋友们，是他们的督促和帮助，才使本书可以尽早呈现在广大读者面前。

周明涛

2003 年 1 月 1 日

目 录

前 言

第 1 章 了解 MMC	1
1.1 MMC 概述	1
1.1.1 MMC 和管理单元	1
1.1.2 认识 MMC 窗口	2
1.1.3 MMC 的访问模式	3
1.1.4 MMC 的简要历史	4
1.2 启动 MMC	4
1.2.1 直接启动 MMC	5
1.2.2 打开现有的 MMC 控制台	5
1.2.3 了解启动 MMC 的命令行参数	7
1.3 添加和删除管理单元	8
1.3.1 添加和删除管理单元	8
1.3.2 定制任务板视图	12
1.4 保存控制台文件	14
1.4.1 设置控制台文件的访问模式	14
1.4.2 设置控制台文件的名称和图标	15
1.4.3 保存控制台文件	15
1.4.4 通过管理工具文件夹管理自定义 控制台文件	16
1.5 使用 MMC	16
1.5.1 创建新的 MMC 窗口	16
1.5.2 定制 MMC 显示方式	18
1.5.3 控制细节窗格显示的列项目	19
1.5.4 导出细节窗格的内容	20
1.5.5 查看属性页关联的管理单元 和项目	20
1.5.6 使用收藏夹列表	21
1.5.7 磁盘清理	21
1.5.8 发布消息	22
第 2 章 Windows XP 的命令行解释器 ..	25
2.1 命令行操作概述	25

2.1.1 Windows 中的命令行解释环境	25
2.1.2 在 Windows 的命令行解释环境下 可以实现的功能	25
2.2 启动和配置命令行解释器	26
2.2.1 启动命令行解释器	26
2.2.2 命令提示符窗口基本使用方法	28
2.2.3 命令行解释器的嵌套	30
2.2.4 配置命令提示符窗口	31
2.2.5 cmd.exe 的命令行参数	32
2.2.6 使用 start.exe 命令	36
2.3 了解环境变量	37
2.3.1 环境变量概述	37
2.3.2 了解环境变量的种类	38
2.3.3 了解环境变量的优先级别	38
2.3.4 设置环境变量	39
2.3.5 Windows XP 中常见的环境变量	43
2.4 常规的命令行操作	46
2.4.1 获取命令行帮助	46
2.4.2 认识 Windows 保留的文件名称	48
2.4.3 命令的重定向	49
2.4.4 管道操作和筛选器	51
2.5 批量执行命令	53
2.5.1 批处理文件概述	53
2.5.2 批处理文件常用命令	53
2.5.3 在批处理文件中使用参数	56
2.5.4 在批处理文件中使用环境变量	59
2.5.5 控制批处理文件的流程	60
第 3 章 启动过程和启动故障排除	65
3.1 了解 Windows XP 的启动过程	65
3.1.1 一些术语和基本知识	65
3.1.2 电源开启自检过程	69
3.1.3 初始化启动过程	69
3.1.4 引导程序载入过程	69

3.1.5 检测和配置硬件过程	70	4.2.3 设置自动登录	126
3.1.6 内核加载过程	71	4.3 本地用户和组	127
3.1.7 用户登录过程	75	4.3.1 了解用户和组	127
3.1.8 即插即用设备的检测过程	77	4.3.2 认识内置的用户和用户组	128
3.2 多重操作系统的启动问题	77	4.3.3 以其他用户身份操作计算机	133
3.3 使用多个硬件配置文件	78	4.3.4 利用控制面板中的“用户帐户” 小程序管理用户	135
3.3.1 管理硬件配置文件	79	4.3.5 利用“本地用户和组”管理 单元管理用户	137
3.3.2 修改硬件配置文件对应的硬件设置	80	4.3.6 用“本地用户和组”管理单元 管理用户组	140
3.4 认识 Windows XP 启动时的高级 选项菜单	81	4.3.7 以命令行方式管理用户和 用户组	141
3.4.1 Windows XP 的高级选项菜单	81	4.4 创建和修改用户配置文件	145
3.4.2 最后一次正确的配置	81	4.4.1 用户配置文件的类型	145
3.4.3 安全模式	82	4.4.2 用户配置文件中包含的内容	145
3.4.4 其他几种启动方式	85	4.4.3 管理用户配置文件	146
3.5 认识 boot.ini 文件	86	4.4.4 创建漫游配置文件	147
3.5.1 boot.ini 文件的结构	87	4.4.5 指派强制用户配置文件	149
3.5.2 了解 boot.ini 中的 ARC 语法	88	4.4.6 为配置文件指派登录脚本	149
3.5.3 了解 boot.ini 中的操作系统 启动参数	90	4.4.7 为配置文件指定主文件夹	149
3.5.4 编辑 boot.ini 的方法	92	4.5 其他一些相关操作	150
3.6 启动时临时禁用应用程序和服务	95		
3.6.1 利用 Shift 键临时禁用启动 应用程序	95	第 5 章 资源的访问控制模型	151
3.6.2 利用组策略管理启动方案	96	5.1 访问控制概述	151
3.6.3 使用系统配置实用程序	97	5.1.1 几个术语	151
3.7 系统恢复控制台	100	5.1.2 访问控制原理	153
3.7.1 利用 Windows XP 的光盘进入 系统恢复控制台	100	5.1.3 安全描述符	154
3.7.2 在硬盘上安装系统恢复控制台	101	5.1.4 认识权限	155
3.7.3 系统恢复控制台的常用命令	102	5.1.5 了解 SID	157
第 4 章 用户登录和身份认证	113	5.2 认识安全组类型	160
4.1 概述	113	5.2.1 安全组的内涵和外延	160
4.1.1 几个术语	113	5.2.2 本地组	161
4.1.2 认识 Windows XP 的登录类型	115	5.2.3 全局组	161
4.1.3 Windows XP 在安全机制方面 的新特性	117	5.2.4 通用组	162
4.2 认证原理	120	5.2.5 内置安全性原则	162
4.2.1 认证的两个基本过程	121	5.2.6 Everyone 和 Anonymous Logon	164
4.2.2 交互式登录原理	121	5.3 编辑访问控制设置	165
		5.3.1 为对象设置访问控制机制	165
		5.3.2 控制权限项目的继承	166

5.3.3 精确定制 ACL	168	6.4.4 在单机环境中包含 EFS 认证	197
5.3.4 审核安全主体在对象上的行为	169	6.4.5 由企业 CA 来颁发证书	197
5.3.5 管理对象的所有者	170	6.4.6 更新证书密钥	200
5.3.6 查看对象上安全主体所拥有的 有效权限	173	6.4.7 将自签名的证书替换为 CA 颁发 的证书	201
5.4 深入理解权限的含义	173	6.5 授权多个用户访问加密文件	201
5.4.1 基本的文件和文件夹权限	173	6.5.1 如何授权多个用户访问加密 文件	201
5.4.2 高级的文件和文件夹权限	174	6.5.2 多用户共享加密文件的内部 机制	203
5.4.3 基本权限和高级权限之间的 对应关系	175	6.6 数据恢复	203
5.4.4 对象的移动复制时权限的变化	176	6.6.1 证书和私钥的备份和恢复	204
5.5 使用 cacls 命令	177	6.6.2 数据恢复代理	207
第 6 章 加密文件系统	179	6.6.3 备份和恢复加密文件和文件夹	210
6.1 加密文件系统概述	179	6.6.4 系统还原功能对 EFS 的影响	210
6.1.1 什么是加密文件系统	179	6.7 其他的相关操作	211
6.1.2 哪些对象可以被加密	179	6.7.1 使用密码重设磁盘	211
6.1.3 加密文件系统的简要工作特性	180	6.7.2 激活启动时的密钥保护	213
6.1.4 Windows XP 中 EFS 的新特性	180	6.7.3 激活 3DES	214
6.1.5 为您的环境配置 EFS	180	6.7.4 利用 EFSINFO 工具查看加密 文件信息	215
6.2 EFS 的工作原理	181	6.7.5 禁用 EFS	216
6.2.1 几个名词	181	第 7 章 组策略	219
6.2.2 了解加密文件系统组件	182	7.1 组策略概述	219
6.2.3 被加密文件的结构	182	7.1.1 什么是组策略	219
6.2.4 加密过程概述	183	7.1.2 Windows XP 中的组策略的新 特性	220
6.2.5 解密过程概述	184	7.1.3 组策略能够完成哪些工作	220
6.3 进行 EFS 操作	185	7.1.4 组策略和本地安全策略的关系	221
6.3.1 在资源管理器中进行 EFS 操作	185	7.2 深入了解组策略	222
6.3.2 使用 cipher 命令行工具进行 EFS 操作	187	7.2.1 认识组策略对象	222
6.3.3 激活快捷菜单中的 EFS 选项	189	7.2.2 本地组策略对象的存储	222
6.3.4 加密和解密脱机文件	189	7.2.3 组策略的继承	223
6.3.5 在文件共享环境中进行远程 EFS 操作	190	7.2.4 组策略的优先级	225
6.3.6 在 Web 文件夹中进行远程 EFS 操作	192	7.3 操作组策略	225
6.4 传递 EFS 证书	195	7.3.1 打开组策略管理单元	225
6.4.1 EFS 如何使用证书	195	7.3.2 打开本地安全策略管理单元	226
6.4.2 检测 EFS 证书是否存在	195	7.3.3 使用组策略对象	226
6.4.3 了解证书和密钥的存储	196	7.3.4 使用管理模板	227

7.3.5 配置组策略.....	229	8.4.2 导入模板.....	261
7.3.6 刷新组策略.....	229	8.4.3 进行安全性分析.....	261
7.4 使用本地安全策略.....	232	8.4.4 修改分析结果.....	262
7.4.1 定义组策略中的帐户策略.....	232	8.4.5 导出模板.....	262
7.4.2 定义组策略中的本地策略.....	233	8.4.6 进行安全性配置.....	263
7.4.3 定义组策略中的公钥策略.....	233	8.4.7 查看日志.....	263
7.4.4 定义组策略中的软件限制策略.....	233	8.5 使用 secedit 命令.....	263
7.4.5 定义组策略 IP 安全策略.....	233	8.5.1 利用 secedit 命令进行安全性 分析.....	263
7.5 软件限制策略.....	233	8.5.2 利用 secedit 命令进行安全性 配置.....	264
7.5.1 软件限制策略概述.....	234	8.5.3 利用 secedit 命令从数据库中 导出模板.....	265
7.5.2 创建规则.....	236	8.5.4 利用 secedit 命令验证导入模板 的语法.....	265
7.5.3 配置软件限制策略.....	239		
7.6 策略的结果集.....	240	第 9 章 审核.....	267
7.6.1 登录模式和计划模式.....	241	9.1 审核概述.....	267
7.6.2 启动策略的结果集管理单元.....	241	9.1.1 什么是审核.....	267
7.6.3 在 HTML 页面中查看策略的 结果集.....	242	9.1.2 审核可以完成什么工作.....	267
7.6.4 利用 gpresult 命令查询组策略的 结果集.....	243	9.1.3 审核同事件日志的关系.....	268
7.7 其他相关操作.....	244	9.1.4 如何规划审核方案.....	268
7.7.1 定制启动脚本和关机脚本.....	244	9.2 设置审核策略.....	269
7.7.2 维护 Internet Explorer.....	245	9.2.1 设置审核策略.....	269
		9.2.2 了解安全策略中的审核选项.....	270
第 8 章 安全模板与安全配置分析.....	247	9.3 配置审核操作.....	271
8.1 安全模板概述.....	247	9.3.1 审核对象访问.....	271
8.2 操作安全模板.....	247	9.3.2 审核帐户登录事件.....	274
8.2.1 认识预定义的安全模板.....	248	9.3.3 审核登录事件.....	274
8.2.2 定义新的安全模板.....	251	9.3.4 审核过程追踪.....	275
8.2.3 编辑安全模板.....	253	9.3.5 审核目录服务访问.....	275
8.2.4 复制安全模板.....	257	9.3.6 审核特权使用.....	275
8.2.5 导出安全模板列表.....	257	9.3.7 审核系统事件.....	275
8.2.6 删除安全模板.....	258	9.3.8 审核帐户管理.....	276
8.2.7 在组策略中应用安全模板.....	258	9.3.9 审核策略更改.....	276
8.3 安全配置和分析工具概述.....	258	9.4 事件查看器原理.....	276
8.3.1 安全性分析.....	258	9.4.1 启动事件查看器.....	276
8.3.2 安全性配置.....	259	9.4.2 理解事件查看器查看的事件 日志类型.....	277
8.3.3 安全配置和分析工具的使用流程.....	259	9.4.3 配置事件查看器.....	278
8.4 操作安全配置和分析工具.....	259		
8.4.1 创建和打开安全配置分析数 据库.....	260		

9.4.4 安全模板中的事件查看器策略	279	11.1.1 相比 Windows 2000 改进的部分	307
9.4.5 了解事件日志的访问权限	281	11.1.2 相比 Windows NT 4.0 改进的内容	308
9.4.6 Event Log 服务	281	11.2 管理动态磁盘	308
9.5 使用事件查看器	283	11.2.1 基本磁盘和动态磁盘	308
9.5.1 查看事件日志	283	11.2.2 了解动态卷的类型	310
9.5.2 操作事件日志	284	11.2.3 启动磁盘管理器	313
9.5.3 管理事件日志	286	11.2.4 将基本磁盘转换为动态磁盘	315
9.5.4 查看其他计算机上的日志	289	11.2.5 添加、移动和删除磁盘	318
9.6 用命令行管理事件查看器	290	11.3 管理动态卷	322
9.6.1 eventcreate.exe 命令	290	11.3.1 新建卷	322
9.6.2 eventquery.vbs 脚本	291	11.3.2 格式化卷	324
9.6.3 eventtriggers.exe 命令	293	11.3.3 扩展卷	325
第 10 章 服务	295	11.3.4 修改驱动器盘符和路径	326
10.1 服务概述	295	11.3.5 删除卷	328
10.1.1 服务概述	295	11.4 在 diskpart 命令下管理磁盘	328
10.1.2 了解启动计算机时服务的加载时间	295	11.4.1 进入 diskpart 命令解释环境	328
10.1.3 服务登录时所使用的帐户身份	296	11.4.2 在 diskpart 解释环境中选择操作焦点	329
10.1.4 服务的访问权限	296	11.4.3 在脚本中使用 diskpart 命令	330
10.2 使用服务管理器	298	11.5 使用 fsutil 命令控制 NTFS 高级特性	330
10.2.1 查看服务的基本属性	299	11.5.1 NTFS 文件系统高级特性概述	330
10.2.2 配置服务的启动方式	300	11.5.2 控制文件系统行为	334
10.2.3 开始、停止、暂停和恢复服务	300	11.5.3 管理卷的坏区	335
10.2.4 选择运行服务的帐户	301	11.5.4 根据安全标识符操作文件	335
10.2.5 为硬件配置文件启用和禁用服务	302	11.5.5 列出驱动器和卷信息	336
10.2.6 设置当服务失败时的故障恢复机制	302	11.5.6 创建硬连接	337
10.2.7 查看服务的依存关系	303	11.5.7 管理对象标识符	338
10.3 在系统配置实用工具中管理服务的启动状态	304	11.5.8 管理磁盘配额	339
10.4 利用 net 命令控制服务	304	11.5.9 查询或删除装入点	340
10.5 sc 命令	305	11.5.10 管理稀疏文件	340
10.5.1 利用 sc 命令启动、暂停、恢复和停止服务	305	11.5.11 管理更改日志	341
10.5.2 利用 sc 命令配置服务的启动类型	305	11.5.12 管理卷	343
第 11 章 磁盘管理和 NTFS 文件系统	307	11.6 其他的磁盘存储特性概述	343
11.1 Windows XP 的磁盘管理的新特性	307	11.6.1 可移动存储	343
		11.6.2 磁盘压缩	344
		11.6.3 磁盘配额	346
		11.6.4 文件备份	348

第 12 章 Windows XP 网络基础	349	13.2.5 共享打印机	386
12.1 网络概述	349	13.3 管理网络连接	386
12.1.1 什么是网络	349	13.3.1 访问网络共享资源	386
12.1.2 网络架构	350	13.3.2 了解网络登录	388
12.1.3 网络的拓扑结构	351	13.3.3 管理网络登录密码	388
12.2 数据传输和网络标准模型	353	13.3.4 映射驱动器	390
12.2.1 网络访问方法	353	13.3.5 从 Windows 98 访问 Windows XP ...	391
12.2.2 网络如何发送数据	355	13.3.6 管理共享	393
12.2.3 网络标准 OSI 模型	356	13.4 使用脱机文件	397
12.2.4 Windows NT/2000/XP 和 OSI 模型	358	13.4.1 启用计算机上的脱机文件特性 ...	397
12.3 TCP/IP 协议	358	13.4.2 设置共享文件夹的脱机访问 方式	398
12.3.1 TCP/IP 概述	358	13.4.3 设置文件夹的脱机访问	398
12.3.2 TCP/IP 体系架构	359	13.4.4 同步脱机项目	399
12.3.3 TCP/IP 的应用层	359	13.4.5 设置脱机文件选项	404
12.3.4 TCP/IP 的传输层	360	13.4.6 同脱机文件操作有关的组 策略选项	405
12.3.5 TCP/IP 的 Internet 层	362	13.5 利用 net 命令管理网络连接	406
12.3.6 TCP/IP 的网络接口层	369	13.5.1 net view 命令	406
12.4 网络连接设备	369	13.5.2 net share 命令	407
12.4.1 中继器	369	13.5.3 net use 命令	408
12.4.2 集线器	370	13.5.4 net session 命令	409
12.4.3 交换机	370	13.5.5 net file 命令	410
12.4.4 桥接器	371	13.5.6 net config 命令	411
12.4.5 路由器	372	13.5.7 net statistics 命令	412
12.4.6 网关	374	第 14 章 配置 TCP/IP	415
12.5 在 Windows XP 中构建局域网	374	14.1 Windows XP 的网络配置概述	415
12.5.1 了解 Microsoft 网络环境	374	14.1.1 Windows XP 中的 TCP/IP 特性 ...	415
12.5.2 加入到网络环境	376	14.1.2 认识 Windows XP 的 NWLink 网络协议	416
第 13 章 资源共享和网络连接	381	14.1.3 配置协议绑定顺序	416
13.1 资源共享概述	381	14.2 配置 TCP/IP	417
13.1.1 资源共享的目的	381	14.2.1 验证 TCP/IP 配置	418
13.1.2 资源共享的方式	381	14.2.2 使用 netsh 工具来配置和监视 计算机	422
13.1.3 确保共享的实施	382	14.2.3 配置桥接	426
13.2 资源共享的基本操作	382	14.2.4 配置本地 IP 路由	427
13.2.1 设置文件夹共享	382	14.3 配置 IP 地址	436
13.2.2 了解共享访问权限同 NTFS 访问 权限的关系	384	14.3.1 配置 DHCP	436
13.2.3 隐藏共享	385		
13.2.4 删除共享	385		

14.3.2	配置 APIPA	438	15.1	常见的网络攻击方式	455
14.3.3	手工配置 IP 地址	439	15.2	IPSec	457
14.3.4	配置备用 IP	439	15.2.1	IPSec 能够提供的安全服务	457
14.3.5	了解多宿主环境	440	15.2.2	IPSec 是如何防范攻击的	458
14.4	配置 TCP/IP 名字解析	441	15.2.3	IPSec 协议类型	459
14.4.1	名字解析的过程	441	15.2.4	IPSec 组件	459
14.4.2	选择合适的名字解析方法	441	15.2.5	IPSec 的工作流程	460
14.4.3	了解计算机的命名规范	442	15.2.6	IPSec 标准	461
14.4.4	了解 DNS 查询和解析过程	445	15.3	部署 IPSec	461
14.4.5	配置 DNS 客户端	446	15.3.1	启动 IPSec 管理单元	461
14.4.6	编辑 hosts 文件	447	15.3.2	了解三个默认的 IPSec 策略	462
14.4.7	配置 NetBIOS 名字解析	447	15.3.3	指派策略	462
14.5	TCP/IP 常用命令行工具	449	15.3.4	新建 IPSec 策略	462
14.5.1	getmac	449	15.3.5	编辑 IPSec 策略	463
14.5.2	hostname	450	15.3.6	编辑安全规则	465
14.5.3	nslookup	450	15.3.7	管理 IP 筛选器列表	468
14.5.4	netstat	450	15.3.8	管理筛选器操作	470
14.5.5	nbstat	451	15.3.9	IPSec 策略的其他操作	472
14.5.6	arp	452	15.3.10	在命令行下管理 IPSec	472
14.5.7	tracert	452	15.4	使用 IP 安全监视器	473
14.5.8	pathping	453	15.5	TCP/IP 筛选	474
14.5.9	在支持工具包中的其他工具	454	15.6	配置 Internet 防火墙	475
第 15 章	网络安全	455	15.6.1	启用 Internet 防火墙	476
			15.6.2	配置 Internet 防火墙	476

第 1 章 了解 MMC

要深入掌握 Windows XP 的使用和管理，MMC 是不可忽略的工具。MMC 是 Microsoft Management Console（微软管理控制台）的首字母缩写，是微软公司针对多种管理需求，为各种管理工具专门设计的一个统一的、规范的操作平台。

在 Windows XP 中，大多数的管理和配置工具都可以融入 MMC 的大旗之下，我们经常使用的诸如“设备管理器”、“事件查看器”等实用工具，实际上都是在 MMC 的帮助下同用户进行交互的，在阅读完本章之后，读者不仅能够了解这些实用工具实际的组织方法，而且还可以根据自己的需求，自定义相应的工具组合。

尽管 MMC 这三个字母已经包含了“控制台”的含义，但是为便于叙述，在本书中仍然在很多地方使用“MMC 控制台”这样的描述方式。虽然在语法上有些不通，但是可能更便于读者的理解。这是有先例的，微软在 Windows 2000 的启动画面上也使用了“NT 技术”这样的词语（NT 是 New Technology ——新技术的含义）。

1.1 MMC 概述

MMC 是 Microsoft Management Console（微软管理控制台）的首字母缩写，顾名思义，它是一个专门用于管理的控制台，其设计目标主要用于为 Windows 管理员提供一个统一的、规范的管理接口和操作平台。任何管理工具，只要符合 MMC 的编程规范，就能够融入 MMC 的控制台中，让用户采用同操作其他管理工具类似的方法来操作当前的管理工具。

1.1.1 MMC 和管理单元

可能出乎读者的意料，MMC 本身并不能完成任何管理操作，换句话说，它并不是一个真正的实用工具，MMC 只是根据某种操作规范提供了一个工具框架，它更像是一个工具箱，凡是符合这个工具箱管理规范的工具都可以放入到这个工具箱中以供用户操作。在 Windows 中，所有可以放入到 MMC 中进行使用的工具称作“管理单元”（Snap-In），MMC 同这些管理单元的关系如图 1-1 所示。

在 Windows 中，人们可以直接使用的很多管理工具实际上都已经融入到 MMC 中，例如“事件查看器”。读者可以通过打开“开始”菜单，选择“运行”，然后输入“eventvwr.msc”命令来启动它，如图 1-2 所示。

通过在一个 MMC 窗口中添加管理单元，就可以在一个 MMC 窗口中对计算机的多项配置进行管理。例如，假设希望在一个 MMC 窗口中既使用“事件查看器”，也使用其他一些管理工具例如“磁盘管理”，可以通过对 MMC 进行操作，构建一个包含“事件查看器”和“磁盘管理”的 MMC 管理工具集来实现。如图 1-3 所示。具体的操作方法在后面介绍。

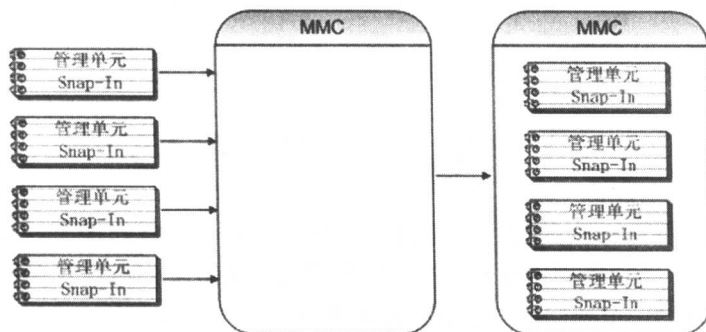


图 1-1 管理单元同 MMC 的关系

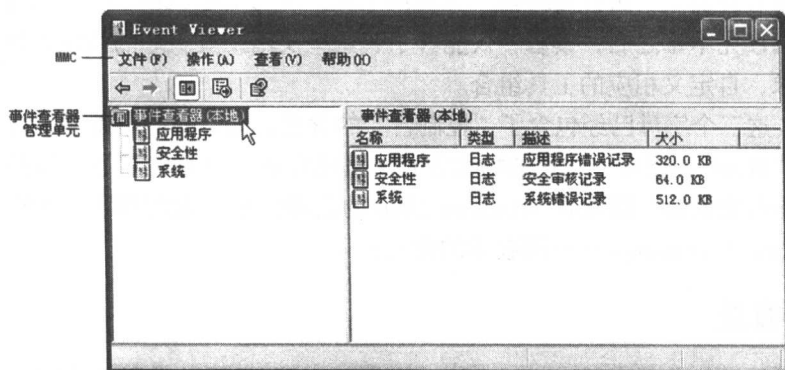


图 1-2 MMC 和事件查看器管理单元

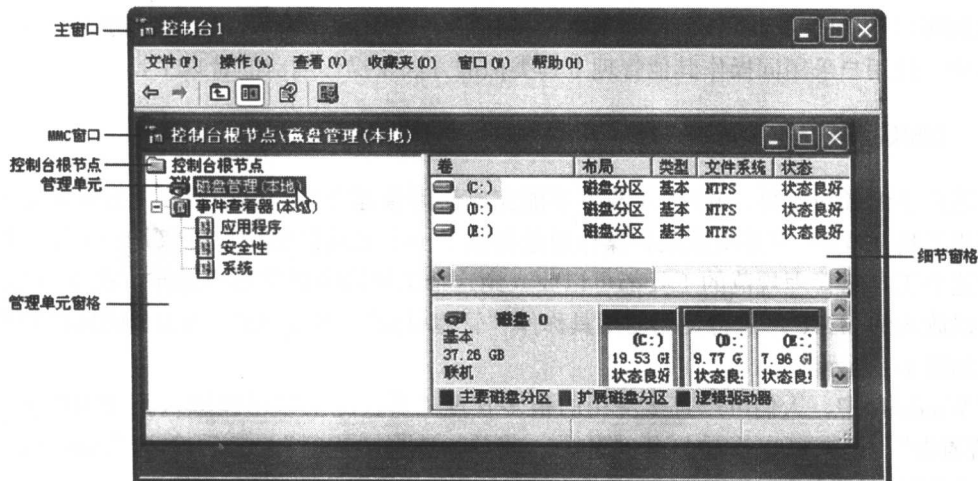


图 1-3 包含“事件查看器”和“设备管理器”的 MMC

1.1.2 认识 MMC 窗口

从图 1-3 中可看到，一个典型的 MMC 控制台由一个主窗口（也即程序窗口）和多个

MMC 窗口组成。每个 MMC 窗口中包含两个窗格。左边窗格称作管理单元窗格，其中显示控制台树，最顶端称作“控制台根节点”，所有添加到控制台的管理单元，都将以树的形式显示在控制台树上，右边的窗格称作细节窗格，用于显示左方管理单元对应的信息和有关功能。随着在左方管理单元窗格中选择管理单元的不同，右方细节窗格中的内容也会随之不同。

控制台的菜单项包含“文件”、“操作”、“查看”、“收藏夹”等，其中一些菜单项是所有管理单元可共用的，而另一些菜单项则随着所选管理单元的不同而不同。例如，假设在 MMC 中添加了“磁盘管理”和“事件查看器”这两个管理单元，那么在左方窗格分别选中这两个管理单元项时，在“操作”菜单中显示的菜单命令也各不相同，如图 1-4 所示。

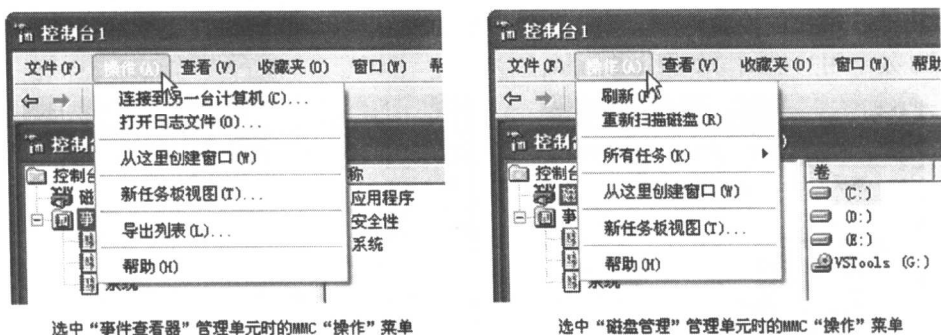


图 1-4 MMC 的菜单会随管理单元的不同而变化

1.1.3 MMC 的访问模式

通过对 MMC 控制台进行定制，可以构建符合自己需要的管理工具集合。通过对 MMC 控制台设置访问模式，也可以控制用户管理和编辑 MMC 的权限。

在 MMC 中包含两种主要的访问模式即“作者模式”和“用户模式”。“作者模式”允许用户对控制台进行全方位的控制，进行诸如添加或删除管理单元、定制任务板视图和任务等多种选项；而“用户模式”则对用户的可操作能力进行限制。

在 MMC 中有三种类型的用户模式，加上“作者模式”，MMC 总共有四种控制模式，如下所示：

- **作者模式** 在这种模式下，用户拥有对 MMC 控制台进行全部控制的权限。例如可以添加或删除管理单元、创建新窗口、创建任务板视图及任务、向收藏夹列表添加项目，以及查看控制台树等。
- **用户模式 - 完全访问** 在这种模式下，用户可以在 MMC 中执行所有的窗口管理的命令（如创建新窗口等），并且可以对 MMC 本身进行完全地控制。如果其中的管理单元可以管理不同的计算机，则用户还可以为管理单元选择要管理的计算机。但是在这种模式下，用户不能添加或删除管理单元。
- **用户模式 - 受限访问，多窗口** 在这种模式下，用户不能修改控制台属性，也不能添加或删除管理单元，但是可以创建多个窗口来查看管理单元选项。

- 用户模式 – 受限访问，单窗口 在这种模式下，用户不能修改控制台，也不能添加或删除管理单元，但是可以创建多个窗口来查看管理单元选项。

MMC 控制台的访问模式，可以通过打开 MMC 的“文件”菜单，选择“选项”命令来完成。在后面会介绍相关操作。

通过检查 MMC 控制台中的菜单命令是否包含相关的操作信息，可以简单判断当前的 MMC 处于何种访问模式。例如，新建一个 MMC 控制台，并向其中添加“计算机管理”管理单元，打开 MMC 的“文件”菜单，若可以看到诸如“添加/删除管理单元”这样的菜单项，这表明当前的 MMC 处于作者模式。如果打开控制面板的“管理工具”中的“计算机管理”，会看到一个非常精简的控制台“文件”菜单，里面没有“添加/删除管理单元”命令，表明当前的 MMC 处于用户模式。如图 1-5 所示。

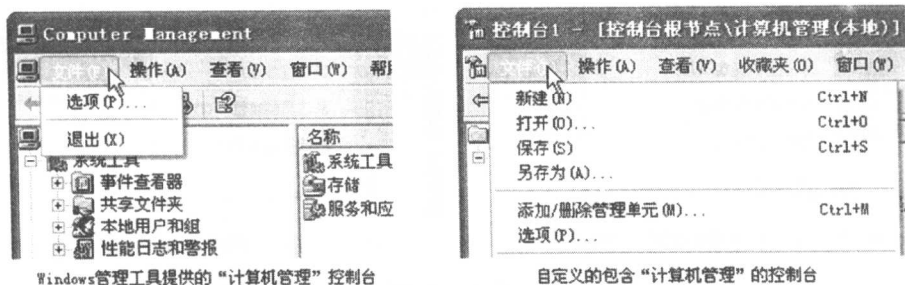


图 1-5 控制台的不同访问模式

1.1.4 MMC 的简要历史

实际上，MMC 不是 Windows XP 独有的东西，早在 Windows NT 4.0 下，通过安装 NT Option Pack，就附带将 MMC 1.0 安装到系统中，那时微软就已经开始推荐软件开发者根据 MMC 的规范创建管理程序。随着 SQL Server 7 等工具的发布，MMC 1.1 也随之流行，在 MMC 1.1 中添加了一些接口，并且修改了一些规范。

一直到 Windows 2000，MMC 才开始大行其道，这时候的 MMC 版本已经是 1.2 了。几乎所有的 Windows 2000 管理工具，如“设备管理器”、“磁盘碎片整理程序”、“系统信息”等，以及其他一些元素，如 ActiveX 控件、指向网页的链接、文件夹、任务板视图和任务等，都可以被放置到 MMC 中进行操作和管理。

在 Windows XP 中，包含的 MMC 版本是 2.0。这是一个全新的、符合微软 .NET 规范的管理控制台，但是它的更新主要在底层接口和组件的应用上，对于编程人员来说，编写新的 MMC 2.0 管理单元更加容易，也更加规范，但是对于一个 Windows 管理员来说，新的 MMC 2.0 操作方法并不比 MMC 1.0 复杂多少。所以，如果读者有在 Windows NT 或 Windows 2000 下使用 MMC 的经验，那么这一章的内容大可忽略不看了。

1.2 启动 MMC

前面了解了 MMC 的概念，现在学习如何启动 MMC。

1.2.1 直接启动 MMC

启动 MMC 非常简单, 打开“开始”菜单, 选择“运行”, 然后在“运行”对话框中输入“MMC”, 单击“确定”按钮, 即可启动 MMC。新启动的 MMC 是一个不包含任何管理单元的空的管理控制台, 如图 1-6 所示。

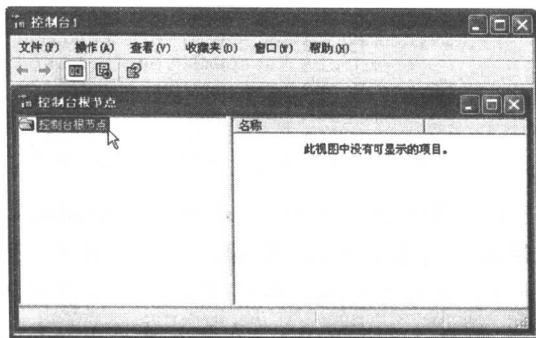


图 1-6 新启动的 MMC 控制台窗口

1.2.2 打开现有的 MMC 控制台

所谓现有的 MMC 控制台, 在大多数情况下指的就是原先已经配置好的、包含管理单元和必要的任务板视图和任务的 MMC 控制台。这些配置信息保存在所谓的控制台文件中, 文件采用 .msc 扩展名。打开现有的 MMC 控制台, 实际就是打开相关的 .msc 控制台文件。

大家知道 Windows 本身提供的很多现成的管理工具, 如“事件查看器”或“磁盘管理”等实际上都是 MMC 的控制单元, 在打开这些程序进行管理时, 实际上就是打开了相应的 .msc 控制台文件。例如, 在控制面板中的“管理工具”中, 运行“事件查看器”, 这实际上等同于打开了位于 Windows 的 System32 目录下的 eventvwr.msc 控制台文件。如果利用 Windows 的搜索功能在系统中搜索带有 .msc 扩展名的文件, 还可以找到很多。这些都是微软事先创建好的 MMC 控制台。

1. 打开 MMC 控制台的基本方法

要打开现有的 MMC 控制台, 只需找到相关的 .msc 文件, 然后双击它就可以了。

如果要打开的 MMC 控制台文件位于系统路径中 (也即其路径在 PATH 环境变量中被设置), 如 Windows 内置的一些 MMC 控制台, 则可以直接在命令行上执行该 MMC 控制台文件名, 譬如, 可以在“开始”菜单的“运行”对话框中直接输入该控制台文件的名称, 再单击“确定”按钮来打开它。例如要打开计算机管理, 可以直接在“运行”对话框中输入“compmgmt.msc”, 并确认操作。

下面是一些 Windows 中现有的 .msc 文件的路径和名称:

证书管理
索引服务

%SystemRoot%\system32\certmgr.msc
%SystemRoot%\system32\ciadv.msc