计算机安全技术丛书

Windows系统管理之道

——命令行脚本应用与解决方案

[美] Pawan K. Bhardwaj 编著

张 猛 译

在盲人岛上，即使是独眼龙，也能当国王。

- 从中国水利水电出版社网站上下载命令行语法
- 避免Windows管理上巨大的时间浪费
- 发现在理论和历史上都少有介绍的容易部署的方案

中国水利水电出版社
www.waterpub.com.cn

计算机安全技术丛书

Windows 系统管理之道
——命令行脚本应用与解决方案

[美] Pawan K. Bhardwaj 编著

张 猛 译

中国水利水电出版社

内 容 提 要

在众多 Windows 系统管理方面的图书中，本书是与众不同的一本，它从命令行的角度深入介绍了 Windows 系统管理。本书并未全面涉及命令行管理的所有方面，而是采用“最佳实践”的方式，就日常 Windows 管理中最常见的任务——命令行操作、计划任务、文件系统和磁盘管理、磁盘分区管理、服务管理、注册表管理、性能监视与优化、网络管理与维护——提供了非常详细的基于命令行的解决方案。因此，除了提高读者的理论水平，加深对 Windows 内幕的理解之外，书中的示例和解决方案可以直接用来解决日常的网络管理问题，提高工作效率。

本书适合于 Windows XP 和 Windows Server 2003 系统管理员阅读，尤其适合于非专职的、繁忙的、需要管理机器的 IT 人员阅读并作为手册参考。

本书所讨论的命令工具的某些语法和代码可以从中国水利水电出版社网站下载，网址为：http://www.waterpub.com.cn/softdown/。

北京市版权局著作权合同登记号：图字 01-2006-7279 号

图书在版编目（CIP）数据

Windows 系统管理之道：命令行脚本应用与解决方案 /（美）巴德瓦杰（Bhardwaj,P.K.）编著；张猛译．—北京：中国水利水电出版社，2008

（计算机安全技术丛书）

书名原文：How to cheat at Windows System Administration Using Command Line Scripts

ISBN 978-7-5084-5024-7

Ⅰ．W… Ⅱ．①巴…②张… Ⅲ．服务器—操作系统（软件），Windows—系统管理 Ⅳ．TP316.86

中国版本图书馆 CIP 数据核字（2007）第 155138 号

书　　名	Windows 系统管理之道——命令行脚本应用与解决方案
作　　者	（美）Pawan K. Bhardwaj　编著　　张　猛　译
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京市天竺颖华印刷厂
规　　格	787mm×1092mm　16 开本　24 印张　462 千字
版　　次	2008 年 1 月第 1 版　2008 年 1 月第 1 次印刷
印　　数	0001—4000 册
定　　价	38.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

译者序

用命令行把自己变得更强大！

2007 年初，我在一家资产数百亿的集团公司做培训，这家集团正在如火如荼地大上特上 SAP ERP 系统，但其公司内部的 SAP 顾问和信息技术人员的薪酬只有 IT 业的 1/3 左右。有一天，我所在公司的网络管理员逐个办公桌地询问每个人的 IP 地址。原来内网有一台桌面机不断地向外发包，估计是被病毒或黑客控制的肉鸡机器。于是我问他，为什么不查一下发包机器的 MAC 地址，然后根据计算机资产登记表中登记的 MAC 地址确认机器。原来他一是不知道有 MAC 地址这回事，二是没有做过登记。

2007 年 4 月初，我启动了一个“Java 企业级开发集训营”，同时在学校开设了一门《网络技术与应用》课程。在集训营第一天，当我要求学员配置 Java 环境变量时，几乎没有人知道命令提示符、批处理文件、环境变量。在学校，当我要求学生获得自己机器的 IP 地址、测试目标网络的连通性时，同样没有几个学生知道命令提示符、ping 命令。

开学之后有一天在系里，我懒得到另外一台机器上拷贝文件，就让同事把他机器上的防火墙打开。他奇怪地问，我没设置共享，你怎么就能访问呢。我说：因为我用命令行连接过去的，你们都不会吗？

所谓“成也萧何，败也萧何”。微软操作系统的界面非常友好，只要会用鼠标单击拖放，似乎就可以做系统管理员了。我也看到许多管理员，包括许多所谓的专家，都能对微软操作系统指指点点，说微软的操作系统不安全，说微软的操作系统不强大。但是，看看这么些系统管理员和专家，没有几个能越过友好的 GUI 界面，深入利用微软强大的命令行工具、脚本工具、自动管理工具、企业级管理工具。可以说，微软把用户变成傻子了。

但是，微软确实没有真的把用户变成傻子，每一版 Windows 操作系统，微软都对命令行、脚本、批处理、自动管理做了显著的增强，MCSE 认证课程的内容，从 NT 到 2000 一直到 2003，技术深度逐年递增。

那么如何能不被友好的 GUI 界面变成傻子，真正发挥微软操作系统的威力，使自己区别于那些鼠标管理员呢？我自己的成长历程也许可以作为一个参照：从 8086 时代的 DOS 3.0 开始使用，那时没有图形用户界面，只能用命令行；内存容量有限，所以要精研系统配置；因为不是学计算机专业的，所以恨不得所有参考资料的每个字都要认真研读。就这样，艰苦的环境、对效率的追求、充分地学习打下了使用命令行和键盘操作的基本功。直到今天，即使使用 Windows 2003/XP，我最喜欢用的还是输入 cmd 调出命令行，因为效率实在是太高了。

记得 1998 年学 MCSE 时，接触的案例就已经是在跨国公司，一个管理员管理数千台桌面机、几百台服务器的场景。因此，作一个系统管理员真的是可以拿到很高的薪水。而现在，许多公司一个系统管理员管理几十台机器都管理不过来。这样低下的生产力水平，怎么会不制约企业的发展呢？怎么能让企业提供优厚的待遇呢？

曼昆在《经济学原理》中指出：“各国生活水平的差异，都可以归于各国生产力水平

的差别。”这个原理，不仅适用于国家，还适用于企业和个人。企业的工资水平低、收益低，在于员工的生产力水平低，管理1000台机器的员工和管理50台机器的员工，效率不可同日而语。鼠标管理员的收入低、工作量大，同样在于自己只会用GUI界面做重复劳动，而不会利用微软提供的强大工具放大自己的能力。

所以，不论是对企业还是对个人，我都建议他们有必要学习本书，提高自己的系统管理水平和效率。这个建议适用于所有企业，因为现在所有的企业都已经离不开计算机系统。

如果说本书有什么不足之处，我想就是太过详细了，每一条命令、每个参数都有非常详细的解释、示例，甚至还要给出一些专家提示，对于我来说读起来实在是浪费时间。但转念一想，不就是因为许多人看了友好的用户界面，似懂非懂，而高校教师又只是提纲契领地大致讲讲，才制造出这么多生产力低下的鼠标管理员吗？所以，作者这种追求细致的作风也许正是我们所应该学习的。

本书由张猛翻译，在翻译过程中，得到了张波、欧阳宇、易磊、盛海燕、安晓梅、徐红霞、杜芳、武堂、黄湘情的帮助，其中张波审校了全文，在此一并致谢。

张 猛

2007年4月15日

于北京石油化工学院经管学院办公室

关于本书

主要作者

Pawan K. Bhardwaj（MCSE、MCT、Security+、Network+、I-Net+和 A+）是一名独立技术培训师和作者。他从 Windows NT 3.51 发布的时候起就积极从事 Windows 管理工作。在过去的 16 年里，他曾经在小型和中型公司不同的系统和网络支持级别上工作。他的一些主要项目包括为印度最大的新闻集团和美国最大的电子商务公司工作，在那里他积极参与了基于 Windows 技术的大型 LAN 和 WAN 解决方案的设计与实现。

Pawan 是 1997 年在印度获得 MCSE 认证的前 100 人之一。他讲授 Windows 管理和网络课程，并担任培训机构的顾问，编写和参与了 Syngress/McGraw Hill 出版社的 12 本以上的认证图书，另外还合著了 MCSE 2003 Electives Exams in a Nutshell（O'Reilly Media, Inc.，2006 年出版）。

技术编辑及审校

Kimon Andreou 是佛罗里达州迈阿密 Royal Caribbean International 的 IT 资产经理。他的专长有软件开发、软件质量保障、数据仓库和数据安全。Kimon 担任过 Secure Discovery Solutions（一家电子证据公司）的 CTO、S-doc（一家软件安全公司）的支持和质量保障经理、SPSS 公司 Enabling 技术部门的首席解决方案架构师。他曾经在亚洲、欧洲、北美和南美领导过项目。Kimon 拥有 American College of Greece 大学的商业管理科学学士学位和佛罗里达国际大学的管理信息系统科学硕士学位。

Kimon 撰写了本书的第 12 章。

合著者

Brian Barber（MCSE、MCP+I、MCNE、CNE-5、CNE-4、CNA-3、CNA-GW）是 Syngress 出版社的 Configuring Exchange 2000 Server（ISBN：1-928994-25-3）、Configuring and Troubleshooting Windows XP Professional（ISBN：1-928994-80-6）以及两门 Windows Server 2003 的 MCSE 课程（考试 70-296 [ISBN：1-932266-57-7]和 70-297 [ISBN：1-932266-54-2]）的合著者，是加拿大 Ottawa 的 Sierra 系统咨询公司的高级技术顾问。他的专业领域有 IT 服务管理和技术基础架构，特别是系统管理的多平台集成、目录服务和消息传递。他曾担任 MetLife Canada 的高级技术分析师和 LGS Group Inc.（现在是 IBM 全球服务的一部分）的高级技术协调师。

Brian 撰写了本书的第 11 章。

Dave Kleiman（CAS、CCE、CIFI、CISM、CISSP、ISSAP、ISSMP、MCSE）从 1990 年起就在信息技术安全领域工作。目前他是 SecurityBreachResponse.com 的所有者。他曾是佛

罗里达州的认证执法官员，其专业领域有诉讼支持、计算机渗透调查、紧急事件响应、入侵分析。他曾经开发了 Windows 操作系统的锁定工具 S-Lok（www.s-doc.com/products/slok.asp），这个工具全面超越了 NSA、NIST 和 Microsoft Common Criteria Guidelines。

Dave 是 Microsoft Log Parser Toolkit（Syngress 出版社出版，ISBN：1-932266-52-6）和 Security Log Management: Identifying Patterns in the Chaos（Syngress 出版社出版，ISBN：1-59749-042-3）的作者。他还是 Perfect Passwords: Selection, Protection, Authentication（Syngress 出版社出版，ISBN：1-59749-041-5）和 Winternals Defragmentation, Recovery, and Administration Field Guide（Syngress 出版社出版，ISBN：1597490792）的技术编辑。他经常在许多国家级安全会议上发表演讲，是与安全有关的新闻邮件、Web 站点和 Internet 论坛的投稿人。Dave 是许多专业安全组织的成员，包括国际反恐和安全专家协会（IACSP）、国际计算机渗透检查师（ISFCE）、信息系统审计和控制协会（ISACA）、高技术犯罪调查协会（HTCIA）、认证欺骗检查师协会（ACFE）、反恐听证委员会（ATAB）以及 ASIS 国际。他还是 FBI 的 InfraGard 的信息技术部门的领导以及国际信息系统渗透协会（IISFA）的培训总监。

Dave 撰写了本书的第 13 章。

Mahesh Satyanarayana 是印度 Shimoga 的 Visveswaraiah 理工大学的电子与通信工程专业的大四学生。他希望在今年夏天毕业，目前已经接受了在 Caritor 公司工作，这是一家 SEI-CMM 5 级的全球咨询和系统集成公司，总部位于 CA 的 San Ramon。Caritor 在全世界向各行业的客户提供 IT 基础设施和商业解决方案。Mahesh 将加入 Caritor 开发中心位于印度班加罗尔的架构和设计部门，将在那里为移动设备开发软件系统。其专业领域包括 Windows 安全和相关的 Microsoft 编程技术，且目前还在努力得到 Red Hat Linux 平台管理员级的认证。

Mahesh 撰写了本书的附录 A。

命令行工具的语法和代码下载

本书所讨论的命令工具的某些语法和代码可以从中国水利水电出版社网站下载，网址为：http://www.waterpub.com.cn/softdown/。

前　言

欢迎阅读《Windows 系统管理之道——命令行脚本应用与解决方案》一书。本书的设计目的是帮助读者理解 Windows 命令 Shell 的威力。计算机的发展史上有一个时代是没有图形用户界面（GUI）的，每项任务无论大小如何，都要使用命令和批处理文件才能执行。随着 Windows 不断推出新版本，Microsoft 试图添加越来越多的 GUI 或配置向导（对话框）层次来简化管理工作。虽然这些“向导”交互性很好，也能让管理员的工作更简单，但是它们并不总是完成日常管理任务最方便、最有效的方式。这些向导非常费时，而且很多时候看起来让人有点糊涂。当然，还有一种方法可以避免使用这些向导，即用操作系统中包含的命令行工具实现同样的任务。

假设要用 Windows 向导或 GUI 把一个用户添加到活动目录、为用户分配访问某些资源的合适许可、限制对其他资源的访问。要完成这些任务差不多要花上一个小时。但是如果使用命令行，那么只用一半时间就能完成相同的任务。这不仅节约了时间，还提高了管理员的生产力。

虽然不应就此而低估 Windows GUI 的作用，但是在提高效率、增进效能、节约时间方面，命令行工具确实有自己的重要性和用武之地。命令行工具既能解决问题，又能节约时间。现在已经没有多少管理员能使用这些工具。所以本书的目的主要是让管理员知道如何利用这些命令行工具完成每天的管理工作、解决重复出现的网络问题、提高他们的工作效率。

全书共 13 章，分为 5 个部分。第一部分介绍 Windows 命令 Shell、批处理文件和任务计划这些基础知识。第二部分介绍基本的 Windows 系统管理，包括文件和硬盘的管理。第三部分介绍系统服务、事件日志、性能和打印服务。第四部分介绍活动目录服务。第五部分介绍管理 Windows Server 2003 环境中的网络服务。

学习旅程从第 1 章的 Windows 命令 Shell 基础开始。在这一章将学习如何访问命令 Shell、如何定制 Shell 的属性，将学会用多种方式修改命令 Shell 属性来满足自己的需求。安装 Windows Server 2003 安装盘中包含的支持工具也在本章介绍，还将学到如何访问帮助和支持中心中的 Windows A～Z 命令参考。

在第 2 章，解释了如何用非管理员账户在命令行下安全地工作。在使用命令 Shell 时，有时需要指定查找命令或批处理文件的路径。将学习如何在命令提示符或者“系统属性”对话框中修改环境变量，改变命令路径。本章还解释了如何修改来自标准键盘的命令输入和到命令窗口的命令输出，如何处理命令生成的错误，讨论了如何创建批处理文件。在本章还将学习批处理文件中的常用命令以及如何在批处理文件内使用每条命令。

在第 3 章，讨论了任务计划程序服务、任务计划 GUI 和 schtasks 命令行工具。如果任务计划程序服务没有运行，则不能安排任何脚本或应用程序自动运行。任务计划向导是安排任务按照预定计划运行的完美工具，但是还可以使用 schtasks 工具执行相同的任务。这个工具代替了老的 AT 命令，虽然在 Windows XP 和 Windows Server 2003 中仍然支持 AT 命令。还将学习使用 schtask 工具不同的子命令创建、修改、删除、查询、运行或终止任务。

schtask 可以说是 Windows 中最复杂的命令集之一。

在第 4 章，讨论一些非常常见的用于管理和维护文件、文件夹和软盘的命令。深入了解这些命令、命令的语法以及它们的用法，在批处理文件或脚本中使用它们来简单管理任务的时候非常有帮助。传统的 Copy、Xcopy、Move 和 Del（Erase）命令在本章中都作了介绍，而且包含了它们的用法示例。然后讨论了使用 diskcopy 命令复制磁盘和使用 diskcomp 命令比较磁盘。其他与文件和文件夹管理有关的命令，如 Tree、MD（Mkdir）和 RD（Rmdir）也在本章中作了介绍。

第 5 章介绍了文件系统和硬盘的维护。本章介绍的最有意义的工具包括 Fsutil、Chkdsk 和 Defrag。其中 Fsutil 工具是新加入 Windows XP 和 Windows Server 2003 操作系统家族的。虽然读者可能有使用旧工具的经验，如 Chkdsk 和 Defrag，但还是需要对操作系统有透彻的了解才能在创建脚本的时候使用 Fsutil 命令及其子命令。本章还会讨论 Format、Convert 和 Compact 命令。

第 6 章专门讨论用来管理硬盘分区和卷的 diskpart 命令行工具。这个工具与其他命令行工具不同，它在 Windows 命令 Shell 内作为基于文本的命令解释器运行。这个工具包含多条命令，只能在 diskpart 解释器启动之后运行。可以用这个工具执行简单的与磁盘相关的任务，如创建和删除分区、卷，还可以执行复杂的任务，如创建、维护和管理容错卷。因为 diskpart 的工作方式比它的 GUI 同类“磁盘管理”管理单元更强大，所以它对选中的磁盘、分区或卷拥有更多控制。diskpart 支持脚本，也可以创建脚本自动执行重复的与磁盘有关的管理任务。diskpart 的错误码使得可以更精确地处理命令执行。

第 7 章解释了一些与维护 Windows 操作系统有关的关键问题，包括服务、驱动程序，以及最重要的 Windows 注册表。本章将讨论 SC 和 Reg 这两个命令行工具，它们提供了多套有助于配置和维护 Windows 操作系统的子命令。虽然很少需要在 GUI 或命令行下直接编辑 Windows 注册表，但是最好还是能理解如何查询、添加、删除、保存和恢复注册表项目。

第 8 章讨论一些监视和管理事件日志、进程及性能日志的命令行工具。监视是系统和网络管理的一个重要方面，切记不可忽视。本章介绍了与 Windows 事件日志管理有关的命令行工具，包括 EventCreate、Eventtriggers 和 EventQuery。本章将学习如何使用 TaskList 命令查看系统服务和应用程序，如何使用 TaskKill 命令终止不响应的进程。本章还包含一些监视和管理性能日志的命令行工具，这些工具包括在命令 Shell 窗口显示性能数据的 TypePerf 工具，在 Windows 注册表中注册新的性能计数器的 Lodctr 工具，以及提取和重新采样已经存储的性能数据的 Relog 工具。

第 9 章讨论用来管理打印机和打印作业的命令行工具。值得注意的是，多数命令只有非常简单的、易于使用的语法。在本章将学会使用 Prnmngr 命令安装打印机，用 Prncnfg 命令查看和配置已安装的打印机。本章讨论的其他命令包括 Prndrvr、Prnport、Prnqctl 和 Prnjobs，分别用来管理打印机驱动程序、创建和配置 TCP/IP 端口、管理打印队列以及管理打印作业。

第 10 章介绍了管理活动目录对象的目录服务（DS）命令的基本语法。将学习 DS 命令可以处理的对象类，包括计算机（桌面机和成员服务器）、联系人、用户、组、服务器（域控制器）、组织单元、站点、子网、配额和目录分区。将学习如何使用 DSQuery 命令及不同的对象类型在活动目录中搜索对象，如何使用 DSGet 命令显示指定对象的属性，如何用

DSAdd 和 DSRm 命令在目录数据库中添加和删除对象。解释了用 DSMod 命令修改指定对象属性，以及用 DSMove 命令把对象在域中从一个容器移动到另一个容器。

第 11 章把目录服务命令的讨论向前推进了一步。本章包含的一些示例有助于理解和使用那些看起来非常复杂的 DS 命令。

第 12 章介绍了执行基本网络故障排除任务的过程，讨论了 Windows 命令行工具中可以使用的标准网络工具的用法，讨论了 Net 命令及其相关子命令的用法。然后研究了其他许多网络诊断工具，如 Ping、IPConfig、Pathping、Finger 和 ARP。研究了一些更强大的工具的用法，如 Netstat 和 NBTStat，学习解读这些命令的结果。本章还介绍了功能全面的 DNS 查询命令行工具 NSLookup。最后，研究了如何与远程 UNIX 计算机以及它们使用的服务进行通信，这些服务通常很少在 Windows 计算机中看到。

在第 13 章将完成这次学习之旅。第 13 章讨论了 NETSH 命令，将学习如何用 NETSH 命令查看 Windows Server 2003 环境中的设置以及配置网络组件。NETSH 在 Windows 命令 Shell 内以独立的命令解释器运行，有自己的一大套子命令。虽然不能在本书范围内讨论每个 NETSH 命令或子命令，但我们尽力在本章解释了最常用的命令。

在 Windows XP 和 Windows Server 2003 中，Microsoft 对命令行的功能做了一些修改：添加了多条新命令，对其他一些命令的功能做了修改。与此同时，一些命令也从支持的命令列表中删除，其中有一些是从 MS-DOS 操作系统的时候就开始使用的命令。

本书的附录讨论了在 Windows XP 和 Windows Server 2003 的 32 位和 64 位版本中不再支持的 MS-DOS 命令。

本书的目的是向读者介绍 Windows XP 和 Windows Server 2003 操作系统中提供的强大的命令行工具。一旦对这些工具有了充分的理解，就会了解如何编写批处理文件。虽然本书不是脚本编程方面的书，但是编写脚本或批处理文件是读者掌握了基础知识之后要走的下一步。多数有经验的系统管理员都依赖预先配置好的批处理文件或脚本来管理网络服务。在 Web 上搜索有助于找到已经设计好的脚本。但是在生产服务器上使用这些脚本之前，一定要在测试服务器上试验这些免费得到的脚本。

编写这本书对于我们几个来说都是一项了不起的经历，我们希望作者、技术编辑团队以及 Syngress 出版社的编辑们共同努力的结果会为我们的读者带来能够增长知识、有所用途、令人欣慰的体验。我们洗耳恭听各位读者的建议与指正。

——Pawan Bhardwaj

MCSE、MCT、Security+、Networking+、A+

目　录

第二部分 基本的 Windows 管理

第三部分　管理 Windows 系统和打印机

第四部分 操作活动目录

第五部分 Windows 网络管理

第1部分

命令行入门

第 1 章　命令行基础

本章内容包括：

- Windows 命令 Shell 基础
- 启动 Windows 命令 Shell
- 命令 Shell 内部命令
- 命令历史
- 访问 Windows 命令参考
- 安装 Windows 支持工具

1.1　引言

多数系统管理员都认为管理基于 Windows 的网络的主要途径就是通过 Windows 图形用户界面（GUI）。在某种程度上确实如此。如果在中小型企业中工作，可以通过 Windows GUI 完成日常的多数管理任务。但是你可能没有认识到在 Windows 操作系统中还存在更强大的界面：命令行。多数管理员都认为命令行与编程有关，实际上并不是这样。Windows 命令行实际上是另一种管理工具，而且比向导和其他界面强大得多。

1.2　Windows 命令 Shell 基础

Microsoft 每次发行新版 Windows 的时候，都引入向导形式的新 GUI，试图简化管理操作系统的任务。结果连资深管理员都开始忘记命令提示符，曾几何时，这曾经是管理操作系统和应用程序的唯一途径。而且，许多新管理员从未打开过命令提示符窗口。当执行一项任务存在更容易的方法时，为什么还要在命令和命令的开关、语法上费力气呢？

随着 Microsoft 每次推出新版 Windows，Windows 命令 Shell 变得越来越多才多艺。当 Windows 的第一版在 20 世纪 90 年代初出现的时候，支持专家们就开始认为