Microsoft

微软技术丛书

MVP
Microsoft®
Most Valuable
Professional

Windows PowerShell 实用宝典

（美）William R. Stanek 著
陆晓珺 译

- IT专家解读Windows PowerShell的全新力作
- 全面、深入地剖析Windows PowerShell 2.0新特性
- 结构独特、实例丰富、操作性强

清华大学出版社

Microsoft

微软技术丛书

MVP
Microsoft®
Most Valuable
Professional

Windows PowerShell 实用宝典

（美）William R. Stanek 著
陆晓珺 译

清华大学出版社
北 京

内 容 简 介

本书由浅入深地介绍了 Windows PowerShell，内容涵盖 PowerShell 的运行环境的配置，别名、函数和对象的处理方式和方法，以及 PowerShell 在远程和网络环境中的各种应用，如计算机的盘点及文件和打印机管理等，这些都属于 Windows 服务器和 PC 客户端管理工作的基本任务。相比图形化的管理方式，PowerShell 更加小巧、稳定和灵活，能大大简化日常工作。本书含有大量实例操作指导和技巧提示，方便管理员的日常工作。

本书适合所有 Windows 管理员参考，对熟悉脚本语言和 UNIX/Linux Shell 环境的管理员来说，也有实用价值。

北京市版权局著作权合同登记号　图字：01-2009-6824

图书在版编目(CIP)数据

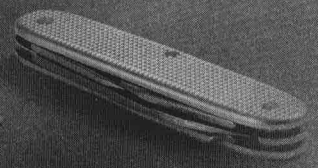
Windows PowerShell 实用宝典/(美)斯坦里克(Stanek, W. R.)著；陆晓珺译. —北京：清华大学出版社，2010.4
(微软技术丛书)
书名原文：Windows PowerShell 2.0 Administrator's Pocket Consultant
ISBN 978-7-302-22166-1

Ⅰ. W… Ⅱ. ①斯… ②陆… Ⅲ. 窗口软件，Windows Ⅳ. TP316.7

中国版本图书馆 CIP 数据核字(2010)第 033127 号

责任编辑：汤涌涛
装帧设计：杨玉兰
责任印制：王秀菊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：23　**字　数**：552 千字
版　　次：2010 年 4 月第 1 版　　**印　　次**：2010 年 4 月第1 次印刷
印　　数：1～4000
定　　价：49.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：(010)62770177 转 3103　　产品编号：032679-01



《微软技术丛书》出版前言

在黄昏里希冀皓月与繁星
在深夜希冀着黎明
在炎夏希冀凉秋
在严冬又希冀新春
这不断的希冀啊，
使我感触到世界的存在，
带给我多量的生命的力。
这样，
我才能跨过——
这黎明黄昏，黄昏黎明，春夏秋冬，秋冬春夏的茫茫的时间的大海啊。

——艾青

时间在流逝，技术也在迅猛发展。在希冀中，微软的.NET 战略早已经变成现实，带来全新、快速而敏捷的企业计算能力，也给软件开发商和软件开发人员提供了支持未来计算的高效 Web 服务开发工具。在希冀中，我们欣喜地看到，微软的每一个技术创新，都对中国开发人员产生巨大的推动作用，使得越来越多的人加入微软开发阵营。

微软出版社为了配合 Visual Studio 的推广和普及，邀请项目开发组的核心开发人员和计算机图书专业作家精心编写了微软 IT Pro 系列图书。该丛书自上市以来，在美国图书销量排行榜上一直高居前列，颇受读者好评，成为程序开发人员和网络开发人员了解微软技术的权威工具书。随着新的开发平台的发布，该系列得以大幅度扩充，在美国及欧洲图书市场广受好评。

从 2002 年开始，清华大学出版社为了满足中国广大程序开发人员、网络开发人员以及计算机用户学习最新技术的渴望，在微软出版社的配合下，先后推出了《微软.NET 程序员系列》和《微软.NET 程序设计系列》。这两套书阵容庞大，几乎涵盖.NET 技术及其应用的各个方面；也正因为如此，翻译和编辑加工的工作量也大得惊人。但为了保持国外优秀技术图书的魅力，同时使读者领会新技术的真谛，本丛书的翻译和编辑都是经过严格筛选的、具有很高的翻译水平或丰富编辑经验的技术人员。同时，我们还聘请微软公司相关产品组的技术专家审读每一本书，确保在技术上准确无误。

2005 年，随着微软新的开发平台的推出，我们将原有的两套丛书整合为《微软技术丛书》。这套丛书针对不同层次的读者，分为 5 个子系列：从入门到精通、技术内幕、高级编程、精通&宝典和认证考试教材。各系列特色如下：

★ **从入门到精通**

- 适合新手程序员的实用教程
- 侧重于基础技术和特征

- 提供范例文件

★ **技术内幕**

- 权威、必备的参考大全
- 包含丰富、实用的范例代码
- 帮助读者熟练掌握微软技术

★ **高级编程**

- 侧重于高级特性、技术和解决问题
- 包含丰富、适用性强的范例代码
- 帮助读者精通微软技术

★ **精通&宝典**

- 着重剖析应用技巧，以帮助提高工作效率
- 主题包括办公应用和开发工具

★ **认证考试教材**

- 提供完整的 Ebook(英文版)
- 提供实际场景、案例分析和故障诊断实验
- 完全根据考试要求来阐述每一个知识点

这套丛书延续以前严谨的编校风格，一切以保证图书内容和技术质量为核心，付出了大量心血。相信整合后的这套丛书必然会帮助程序开发人员、网络开发人员以及具有一定编程基础的中高级读者，快速、全面地掌握微软技术，为将来的技术生涯奠定扎实的基础，使之成为中国软件产业的栋梁！

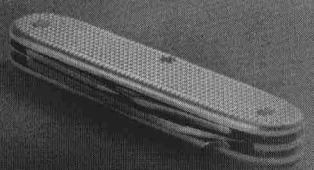
为增强本书的可读性，便于读者迅速定位关键术语的原文和快速根据索引来定位知识点(概念、函数等)的详细介绍，有些经典图书中在相应位置标注了原书页码(在当前行末尾用粗体方括号【】或椭圆形底纹 表示)，并在书后附上原书索引，以期能对大家提供更多的帮助。已经采用这一体系设计的图书有《Windows 核心编程(第 5 版)》、《Visual C# 2008 从入门到精通》、《ASP.NET 3.5 核心编程》、《Visual C# 2008 核心编程》和《精通 Windows 3D 图形编程》。

在此，感谢参与本丛书的翻译和审校人员，感谢他们付出的心血和时间。他们来自培训和实践前沿，具有深厚的技术底蕴和文化素养，善于用浅显易懂的语言阐述晦涩难懂的技术细节。同时也要感谢这一年来时刻关注这套书的读者朋友们。他们热心地提出自己的意见和建议，感谢他们的宽容和善意关爱。我们将和大家一样，时刻关注微软技术发展的最新动态，时刻保持自己的技术动力！

亲爱的读者朋友，期待着您把每一次看书的机会，都当成增进知识的时候。这个过程，绝对不是浅尝辄止，更非自认把书看过一两遍就可以了。深度的阅读是尽可能地把书本的知识转换为自己熟悉的，甚至读到自己内心的深处。同时，也请把您对这套书的感受告诉我们，我们期待着和您分享，联系信箱 coo@netease.com。

尽管我们注入大量心血，但疏忽纰漏之处在所难免，恳请读者朋友提出建议和批评。本丛书在创作、翻译和编辑过程中得到了微软(中国)公司的大力支持。本丛书能够顺利出版，更是倾注了无数幕后人员的汗水和心力。在此，对他们的辛勤劳动一并表示衷心感谢！

清华大学出版社



译 者 序

计算机的发展史迄今已有 60 多年。如今，生活、学习、办公越来越依赖于计算机。对于企业来说，越来越多的业务种类带来了越来越多的应用，越来越多的应用带来了越来越多的服务器，随之而来的压力就自然转嫁到服务器管理员身上。管理好服务器成为保障企业良好运营的一个重要基础。对于管理员来说，高效地管理好服务器能够避免给企业带来重大损失，甚至可以为企业创造效益。

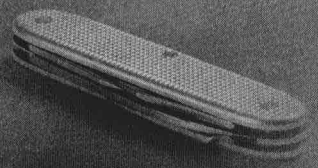
随着计算机的发展，计算机语言层出不穷，各种语言所针对的对象也有所不同。本书介绍的 Windows PowerShell 就是一种脚本语言。如果接触过 VBScript，或者是由 Linux 管理员转为 Windows 管理员，只要对 Linux Shell 有一定的了解，那么学习 PowerShell 就不是一件难事(事实上，从 Windows Server 2008 开始，已经有了 server core，不难看出，微软已经认识到自身服务器上的不足，包括 Exchange 2007，都有了 PowerShell 接口，console 的连接所占用的资源远比 GUI 方式的连接要小，全命令行方式的服务器环境也更加稳定，PowerShell 综合了 VBScript 和 Linux Shell 的语法，可以说也是吸引一部分 Linux 管理员的一个表态，将来 Windows Server 家族中一定会有更多的产品能够以命令行方式运行)。从管理员角度讲，对比一下这样的两个场景：泡上一杯咖啡，坐在电脑桌前，或是座位都没坐暖就被一个电话拉到某地。不言而喻，在自己的电脑上敲击键盘、点点鼠标，远比跑到机房或者用户的计算机上敲击命令舒适得多。使用 PowerShell 管理 Windows 服务器，对于很多管理任务来说，就是执行几个脚本、敲击几行命令的事情。

在翻译本书时，正值上海炎炎的夏日，只有到了晚上，心境稍稍平静后才能开始着手翻译。开始时，对一些专业术语的拿捏以及上下文、前后章节的用语一致十分头疼。由于中文的丰富，往往前文的一个词到了后文就用其他词替代，而忽略了一致性。经过对译文的再三校对，已经将这种差异尽可能降到最低。

从来没有如此认真、反复地阅读一本全英文计算机图书，从中了解了自己平时很少接触的一些技术特性和用法，这次的翻译对我个人来说是一笔不小的财富。

最后，我要谢谢我的父母和我的妻子，他们为我创造了一个良好的环境，并且给了我极大的鼓励和支持。

译 者



前　言

本书对 Windows 管理员、开发人员、程序员和任何想使用 Windows PowerShell V2 来控制和配置计算机的人来说是十分简洁和有用的资源。这是一本简单易读的指南，目的就是方便读者随时参考。本书讨论所有使用 Windows PowerShell 执行的核心管理任务。因为本书通过精简的篇幅提供最大的价值，所以读者不必在数百页无关的信息里费力查找自己真正需要的内容，而是迅速、准确地找到完成工作所需的内容。

简而言之，本书旨在充当读者的随身指南，只要在使用 Windows PowerShell 管理计算机时遇到问题，就可以参考本书。本书重点介绍日常的管理程序、经常性的任务、归档的示例和典型但不经常遇到的选项。本书的写作目标之一是在保证内容精简的同时，尽可能涵盖更多的信息，使它成为有价值的资源。然而，不同于动辄上千页的大部头或者只有 100 页的快速参考，本书是一本有价值的资源指南，它能帮助你快速而方便地处理日常任务、解决问题和实现高级管理(如自动监视、性能跟踪、网络故障排查、安全管理和远程配置)。

本书的目标读者

本书介绍 Windows PowerShell V2。目标读者包括以下几类：

- Windows 管理员
- Windows 系统维护人员
- 有管理员职责的高级用户
- 从较早版本升级到 Windows PowerShell 2.0 的管理员

为了包含尽可能多的知识，我不得不假设读者具备基本的网络技能并对 Windows 有基本了解，并且已经在系统中安装 Windows PowerShell。记住，我不会花整章的篇幅来介绍 Windows 构架或 Windows PowerShell 的安装。尽管如此，本书会涵盖使用 PowerShell 来修改安全描述符、管理域成员、创建还原检查点、配置事务日志等内容。

我也假设读者相当熟悉 Windows 命令、程序和 Windows 命令行。如果需要学习 Windows 基础知识，建议阅读 Windows 文档。

本书的结构

本书针对 Windows 计算机的日常管理，因此是按工作任务而非 Windows 功能来编排组织的。能够方便、快速地查阅是这类实际操作指南的重要特点。本书有详细的目录可用于快速找到问题的答案。本书还有很多其他便于快速查阅的特性，例如快速按步骤操作的说明、

列表、汇总表和交叉引用。

第 1 章提供 PowerShell 管理工具、技术和概念的综述。可以了解 PowerShell 的图形界面和命令行界面。第 2 章介绍 PowerShell 的概述，详细描述了使用参数启动 PowerShell 控制台的技术、运行脚本的方式、可用的格式化选项和如何使用系列命令。

Windows 提供了许多 PowerShell 命令来帮助管理日常操作。第 3 章介绍个人配置文件和工作环境的装载方式，用于扩展 PowerShell 的技术，包括添加提供程序到工作环境的管理单元和模块扩展(它们必须被事先导入才能使用)。第 4 章讨论命令的远程执行、远程会话和远程后台任务。远程工作时，是在自己计算机上的 Windows PowerShell 中输入命令，而在一台或多台远程计算机上执行这些命令。第 5 章介绍 PowerShell 操作的核心结构，其中包括如何设置变量、使用表达式及管理字符串、数组和集合。第 6 章主要讨论别名、函数和对象。在操作 PowerShell 时，使用别名、函数和对象能事半功倍，并有助于执行任何能想到的管理任务。

第 7 章深入介绍脚本、个人配置文件和命令，内容包括如何创建脚本和事务，以及控制循环和条件语句。第 8 章讨论如何使用 PowerShell 管理服务器角色、角色服务和 Windows 功能。第 9 章介绍盘点计算机和评估硬件配置的技术，以及如何确定是否有需要注意的问题。第 10 章讨论用于管理文件系统、安全和审核的技术。在使用 PowerShell 时，操作多个目录和文件和操作单个目录和文件一样容易。

第 11 章介绍如何控制和配置网络共享、打印机和 TCP/IP 网络。第 12 章讨论管理和防护注册表，内容包括如何读写注册表值，如何查看并设置访问控制列表和如何配置注册表审核。第 13 章介绍用于监视计算机和优化性能的工具和技术。最后，第 14 章详细介绍如何进行系统调优，以及帮助识别和纠正系统问题的技术。

本书的约定

本书采用多种方法来保证内容清晰易懂。要求读者实际输入的命令采用粗体显示，代码采用等宽字体，新术语也以粗体显示。本书还有以下特色段落。

- **最佳实践** 在涉及高级配置和管理概念时所使用的最好的技巧。
- **警告** 当有潜在问题时给出警告，提醒留意。
- **注意** 提供某一需要强调的内容的详细信息。
- **更多信息** 提供与主题相关的更多信息。
- **实践提示** 在讨论某些高级应用的主题时提供真实环境下的建议。
- **安全警告** 指出重要的安全问题。
- **提示** 提供有用的提示或额外的信息。

我真诚地希望读者能发现本书提供了快速而有效地执行重要管理任务所需的一切信息。如有任何意见，欢迎发送电子邮件至 williamstanek@aol.com。

查找额外的在线内容

与本书相关的补充材料会放到 Microsoft Press 的 Windows Server and Client 网站上。补充材料包括本书的更新、文章、配套内容的链接、勘误表、样章等。该网站位于 http://microsoftpresssrv.libredigital.com/serverclient/，它会定期更新。在我的网站上能找到关于本书的讨论，网址为 www.williamstanek.com，也可以在 Twitter 上 follow WilliamStanek。

支　持

我们已尽全力确保本书的准确性。Microsoft Press 通过万维网提供本书勘误，网址为 http://www.microsoft.com/mspress/support。

如果您对本书有任何看法、问题或者想法，请通过以下任何一种方式告知我们。

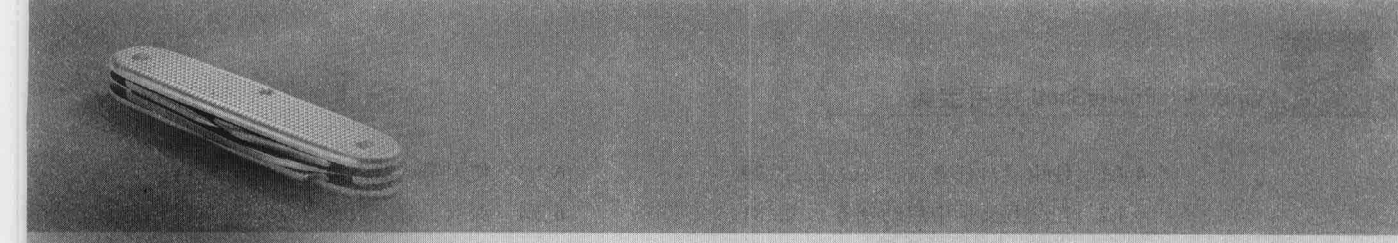
- 传统信件：

Microsoft Press
Attn: Editor, Windows PowerShell 2.0 Administrator's Pocket Consultant
One Microsoft Way
Redmond, WA 98052-6399

- 电子邮件：

mspinput@microsoft.com

请注意，以上的地址不提供产品支持。关于产品技术支持信息，请访问微软网站 http://support.microsoft.com/。



目　录

第 1 章　介绍 Windows PowerShell 1

1.1　Windows PowerShell 入门.....1
1.2　运行 Windows PowerShell.....2
1.2.1　使用 Windows PowerShell 控制台.....2
1.2.2　使用 Windows PowerShell 集成脚本环境.....4
1.2.3　配置 Windows PowerShell 控制台属性.....6
1.2.4　使用命令记录.....7
1.3　使用 cmdlet 和脚本.....8
1.3.1　使用 cmdlet.....8
1.3.2　使用 cmdlet 参数.....11
1.3.3　使用外部命令.....12
1.3.4　使用脚本.....13

第 2 章　充分利用 Windows PowerShell.....19

2.1　初始化环境.....20
2.1.1　传递启动参数.....20
2.1.2　调用 Windows PowerShell.....21
2.1.3　使用-Command 运行命令.....21
2.1.4　使用-File 运行脚本.....23
2.1.5　使用嵌套的控制台.....23
2.2　理解命令输入、解析和输出.....23
2.2.1　基本行编辑.....24
2.2.2　语法解析的工作机制.....25
2.2.3　解析被赋予的值.....26
2.2.4　解析异常.....27
2.2.5　解析的输出.....28
2.3　输出的写操作和格式化.....29
2.3.1　使用格式化的 cmdlet.....29
2.3.2　写到输出流.....35
2.3.3　渲染并完成输出.....39
2.3.4　重定向输入、输出和错误的更多信息.....40

第 3 章　管理 Windows PowerShell 环境.....43

3.1　使用配置文件.....43
3.1.1　创建配置文件.....44
3.1.2　理解执行次序.....45
3.1.3　使用命令路径.....46
3.2　Windows PowerShell 扩展.....48
3.2.1　使用 Windows PowerShell 扩展.....48
3.2.2　使用管理单元.....49
3.2.3　使用提供程序.....52
3.2.4　浏览和使用提供程序驱动器.....58
3.2.5　使用模块.....62
3.2.6　用于 Exchange Server 和 SQL Server 的 PowerShell 扩展.....66

第 4 章　使用会话、任务和远程处理.....69

4.1　启用远程命令.....69
4.2　执行远程命令.....71
4.2.1　理解远程执行.....71
4.2.2　远程命令.....71
4.2.3　调用远程命令.....74
4.3　建立远程会话.....76
4.3.1　调用会话.....76
4.3.2　理解远程执行和对象序列化.....78
4.4　建立远程后台任务.....79

4.4.1 使用后台任务 79
4.4.2 在交互会话中启动任务 81
4.4.3 非交互地运行任务 84
4.5 不使用 WinRM 的远程工作 86

第 5 章 Windows PowerShell 核心结构 89

5.1 使用表达式和运算符 89
5.1.1 算术运算符、组合运算符和赋值运算符 89
5.1.2 比较运算符 92
5.1.3 其他运算符 97
5.2 使用变量和变量值 98
5.2.1 变量要素 99
5.2.2 赋值并转换数据类型 103
5.2.3 管理变量作用域 107
5.2.4 自动变量、偏好变量和环境变量 110
5.3 使用字符串 116
5.3.1 单引号字符串和双引号字符串 117
5.3.2 转义符和通配符 118
5.3.3 多行字符串 120
5.3.4 字符串运算符 122
5.4 使用数组和集合 125
5.4.1 创建和使用一维数组 126
5.4.2 使用强制转换数组结构 127
5.4.3 赋值和删除值 128
5.4.4 在数组中使用严格类型 129
5.4.5 使用多维数组 129

第 6 章 管理别名、函数和对象 133

6.1 创建和使用别名 133
6.1.1 使用内置的别名 133
6.1.2 创建别名 136
6.1.3 导入和导出别名 138
6.2 创建和使用函数 139
6.2.1 创建函数 139
6.2.2 使用扩展的函数 140
6.2.3 使用筛选器函数 141
6.2.4 深入了解函数 142
6.2.5 测试函数定义 143
6.2.6 使用内置函数 144
6.3 使用对象 147
6.3.1 对象要素 147
6.3.2 对象的方法和属性 149
6.3.3 对象的类型 151
6.3.4 深入了解对象 154
6.4 使用 COM 对象和.NET Framework 对象 156
6.4.1 创建和使用 COM 对象 156
6.4.2 使用.NET Framework 类和对象 160
6.5 使用 WMI 对象和查询 163

第 7 章 使用命令和脚本管理计算机 167

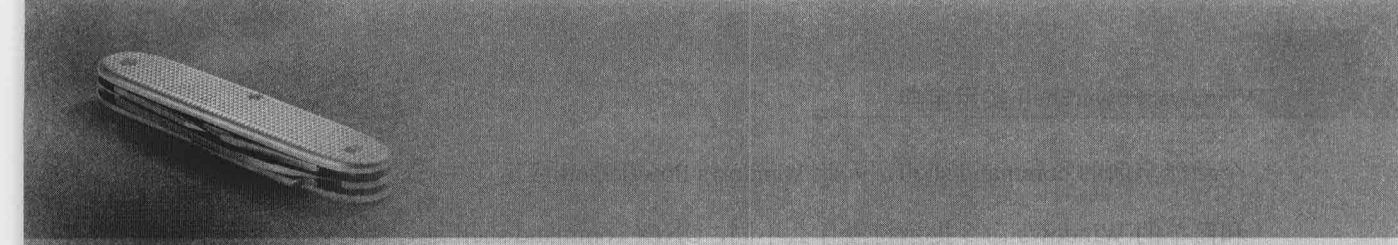
7.1 深入了解脚本和个人配置文件 167
7.2 创建记录 169
7.3 创建事务 171
7.3.1 理解事务 171
7.3.2 使用事务 173
7.4 脚本中的常用元素 174
7.4.1 使用注释和初始化语句 174
7.4.2 使用条件语句 177
7.4.3 使用控制循环 182

第 8 章 管理角色、角色服务和功能 187

8.1 服务器管理器要素 187
8.1.1 服务器管理器命令 188
8.1.2 可用的角色和角色服务 189
8.1.3 可用的功能 192
8.2 检查已安装的角色、角色服务和功能 195
8.3 安装角色、角色服务和功能 196
8.3.1 添加角色、角色服务和功能 197
8.3.2 处理配置错误和其他问题 198
8.4 卸载角色、角色服务和功能 199

8.4.1 移除角色、角色服务和功能.....199
8.4.2 处理移除错误和其他问题.....200
第 9 章 盘点并评估 Windows 系统.....201
9.1 获取基本的系统信息.....201
9.1.1 确定当前用户、域和计算机名.....202
9.1.2 确定并设置日期和时间.....203
9.1.3 指定认证凭据.....204
9.2 检查系统配置和工作环境.....204
9.2.1 确定 Windows Updates 和 service pack.....205
9.2.2 获取详细系统信息.....207
9.2.3 确定可用的用户和组.....211
9.3 评估系统硬件.....212
9.3.1 检查固件版本和状态.....212
9.3.2 检查物理内存和处理器.....213
9.3.3 检查磁盘和分区.....215
9.3.4 检查并管理设备驱动.....219
9.3.5 深入挖掘.....221
第 10 章 管理文件系统、安全和审核.....225
10.1 管理 PowerShell 驱动器、目录和文件.....225
10.1.1 添加和移除 PowerShell 驱动器.....225
10.1.2 创建并管理目录和文件.....227
10.2 操作文件内容.....229
10.2.1 管理文件内容的命令.....229
10.2.2 读写文件内容.....230
10.3 获取安全描述符.....231
10.3.1 用于处理安全描述符的命令.....231
10.3.2 获取并设置安全描述符.....232
10.3.3 使用访问规则.....234
10.4 配置文件和目录权限.....236
10.4.1 设置基本权限.....237
10.4.2 设置特定权限.....239
10.4.3 获得所有者权限.....242
10.5 配置文件和目录审核.....243
第 11 章 管理共享、打印机和 TCP/IP 网络.....247
11.1 管理网络共享.....247
11.1.1 获取关于共享的信息.....247
11.1.2 修改共享设置.....249
11.1.3 创建共享.....250
11.1.4 删除共享.....251
11.2 管理打印机.....251
11.2.1 获取关于打印机的信息.....252
11.2.2 检查打印机驱动.....254
11.2.3 管理打印机连接.....254
11.3 管理 TCP/IP 网络.....255
11.3.1 获取关于网络适配器的信息.....255
11.3.2 配置静态 IP 地址.....258
11.3.3 配置动态 IP 地址.....261
11.4 配置 Windows 防火墙.....263
11.4.1 查看和管理 Windows 防火墙设置.....263
11.4.2 添加和移除防火墙端口.....266
第 12 章 管理并保护注册表.....269
12.1 理解注册表键和键值.....269
12.2 注册表导航.....270
12.3 管理注册表键和键值.....273
12.3.1 创建注册表键和键值.....274
12.3.2 复制注册表键和键值.....275
12.3.3 移动注册表键和键值.....275
12.3.4 重命名注册表键和键值.....276
12.3.5 删除注册表键和键值.....276
12.4 比较注册表键.....277
12.5 查看和管理注册表安全设置.....278
12.5.1 获取并设置注册表安全描述符.....279
12.5.2 使用注册表访问规则.....280

12.5.3 配置注册表权限.....281
12.5.4 获取注册表键的所有者权限.....285
12.6 审核注册表.....286
第 13 章 监视和优化 Windows 系统.....289
13.1 管理 Windows 事件和日志.....289
13.1.1 操作事件日志.....289
13.1.2 查看并筛选事件日志.....293
13.1.3 设置日志选项.....295
13.1.4 归档并清理事件日志.....296
13.1.5 将自定义事件写入事件日志.....297
13.1.6 创建并使用保存的查询.....299
13.2 管理系统服务.....300
13.2.1 查看配置的服务.....302
13.2.2 启动、停止和暂停服务.....304
13.2.3 配置服务启动.....306
13.2.4 管理服务的登录和恢复模式.....307
13.2.5 深入了解服务管理.....310
13.3 管理计算机.....316
13.3.1 用于管理计算机的命令.....316
13.3.2 重命名计算机帐号.....318
13.3.3 将计算机加入域.....319
13.3.4 将计算机添加到工作组.....320
13.3.5 从域和工作组中移除计算机.....321
13.3.6 管理计算机的重启和关闭.....322
13.4 创建并使用系统还原检查点.....323
13.4.1 用于配置系统还原的命令.....324
13.4.2 启用和禁用系统还原.....325
13.4.3 创建和使用检查点.....325
13.4.4 从还原点中恢复.....326
第 14 章 系统性能调优.....329
14.1 管理应用程序、进程和性能.....329
14.1.1 理解系统和用户进程.....330
14.1.2 检查正在运行的进程.....331
14.1.3 筛选进程输出.....335
14.1.4 查看正在运行的进程和服务之间的关系.....337
14.1.5 查看进程使用的 DLL 列表.....338
14.1.6 停止进程.....339
14.1.7 深入挖掘进程.....341
14.2 性能监视.....344
14.2.1 理解性能监视命令.....344
14.2.2 追踪性能数据.....345
14.3 通过监视探测并解决性能问题.....349
14.3.1 监视系统资源使用情况和进程.....349
14.3.2 监视内存分页和分页到磁盘.....351
14.3.3 为单独进程监视内存使用情况和工作内存集合.....352



第 1 章　介绍 Windows PowerShell

- Windows PowerShell 入门
- 运行 Windows PowerShell
- 使用 cmdlet 和脚本

如果你是一位 IT 专业人员，那么有可能听说过 Windows PowerShell，甚至可能已经阅读过其他关于 PowerShell 的图书且已经在工作中运用 PowerShell。不过，对于 PowerShell，你可能仍然有许多问题，或者很好奇 Windows PowerShell Version 2.0(PowerShell V2)提供的而其前身 Windows PowerShell Version 1.0 (PowerShell V1)没有提供的功能。毕竟，本书的主题是 Windows PowerShell 2.0。

每一个版本的 Windows 拥有内置的命令行来运行内嵌的命令、工具和脚本。Windows PowerShell 以新的和令人激动的方式扩展了命令行，过去只能通过扩展的命令才可能打开操作系统。无论是管理员、开发人员、程序员还是 IT 专业人员，都能使用 Windows PowerShell 来控制和配置运行基于 Windows 的操作系统的计算机，这就是本书的主要内容。

本章将着重介绍 Windows PowerShell 的基本知识。学习如何使用 PowerShell，如何运行命令，如何使用相关功能。对精通 Windows 的管理员、高水平的技术支持人员和熟练用户来说，Windows PowerShell 将变得越来越不可或缺。了解如何正确使用 Windows PowerShell，可以节约时间和精力，也更能显示平稳运行的系统和经常性出现问题的区别。另外，如果管理众多计算机，在日复一日的操作中，掌握 PowerShell 提供的节约时间的策略不仅仅是重要的，也是必要的。

实践提示　一般来说，可以在任何 Windows 版本中安装 Windows PowerShell V2，来学习本书中提及的技能。然而，一些功能(如远程和后台工作)，不是所有平台都能运行。因此，跨平台工作时，在把命令、选项和脚本使用到真实生产环境中之前，应该经常在那些孤立于生产网络环境中的计算机上，在开发环境和测试环境下测试它们。

1.1　Windows PowerShell 入门

任何一个有 UNIX 背景的人都可能熟悉 command shell(命令外壳)。大部分基于 UNIX 的操作系统都有几个功能全面的 command shell 可供使用，包括 Korn Shell(KSH)、C Shell(CSH)和 Bourne Shell(SH)。尽管所有 Windows 操作系统都有一个命令行环境，但是它们缺乏一

个功能全面的 command shell，因此 Windows PowerShell 应运而生。

和简单的 Windows 命令提示符没什么不同，UNIX command shell 通过执行内置命令、外部命令和命令行工具来操作，以文本方式输出到输出流来返回结果。输出流可以用多种方式来处理，包括重定向来作为另一个命令的输入。重定向一个命令的输出以作为另一个命令的输入的过程称为管道(piping)，这是一个被广泛使用的 shell 脚本技术。

C Shell 是更加复杂的 UNIX shell 家族中的一个。在很多方面，C Shell 是 C 程序语言和功能全面的 UNIX shell 环境的一个结合体。Windows PowerShell 将上述的功能完善的 command shell 与程序语言结合的理念进一步扩展。它是基于 C#的脚本语言和基于微软.NET Framework 对象模型的产物。

Windows PowerShell 基于 C#脚本语言，确保它的脚本可以轻松地被 C#开发人员和刚入门 C#的开发人员所理解。使用基于.NET Framework 的对象模型允许 Windows PowerShell 从一个命令到另一个命令传递完整的对象及其所有属性作为输出。重定向对象的能力十分强大，并且允许一系列的动态结果集合的处理。例如，不仅可以获得某个用户的名字，而且也能获得整个相关的用户对象。然后可以根据名字属性来处理这个用户对象的其他属性。

1.2 运行 Windows PowerShell

Windows PowerShell V2 在 V1 基础上做了扩展和增强。这些变更是显著的，而且它们同时改进了 PowerShell 的性能和功能。使用 PowerShell V2，能做到之前 PowerShell V1 做不到的事情，还能以更高效的方式执行标准任务(相较于以前)。下面将讨论 PowerShell 的选项和配置，同时涉及一些使用“命令记录”功能的技巧。

1.2.1 使用 Windows PowerShell 控制台

Windows PowerShell V2 预装在 Windows 7、Windows Server 2008 R2 和更高版本的 Windows 操作系统中。当然，也可以安装到 Windows XP、Windows Server 2003、Windows Vista 以及 Windows Server 2008 版本中。可以到微软下载中心(http://download.microsoft.com)下载适合于 32 位或 64 位的 Windows 各版本的 Windows PowerShell。

Windows PowerShell V2 同时拥有命令行环境和图形界面环境，用于运行命令或脚本。PowerShell 控制台(PowerShell.exe)是 32 位或 64 位环境下的命令行程序。在 32 位版本的 Windows 系统中，可以在%SystemRoot%\System32\WindowsPowerShell\v1.0 目录下找到这个可执行文件。在 64 位 Windows 系统中，可以在%SystemRoot%\SysWow64\WindowsPowerShell\v1.0 目录下找到 32 位版本的可执行文件，在%SystemRoot%\System32\WindowsPowerShell\v1.0 目录下找到 64 位版本的可执行文件。

注意　%SystemRoot%指系统根环境变量(即 Windows 操作系统目录)。Windows 操作系统有许多环境变量，用于指定用户特指或者系统特指的值。在本书中，将经常使用标准的 Windows 语法规则 %变量名% 来指定环境变量。

实践提示　Windows PowerShell V2 依赖于.NET Framework。计算机需要运行.NET Framework 2.0 及以上版本才能使用 PowerShell 的核心功能。只有运行 Windows Vista 或更高 Windows 版本，并且运行.NET Framework 3.51 及之后新版本的计算机才能支持 Windows PowerShell V2 中的高级功能。

可以使用“开始”菜单中的“搜索”文本框来启动 PowerShell 控制台。单击“开始”按钮，在“搜索”文本框中输入 **powershell**，然后按 Enter 键。或者，可以单击“开始”|“所有程序”|“附件”|Windows PowerShell，选择 Windows PowerShell V2。在 64 位系统中，默认启动 64 位的 PowerShell，如果需要在 64 位系统中启动 32 位的 PowerShell，必须选择 Windows PowerShell x86 V2 项。

也可以在 Windows 命令行 shell(cmd.exe)中输入 **powershell** 来启动 Windows PowerShell，如下所示：

```
powershell
```

图 1.1 显示了一个 PowerShell 的窗口。默认情况下，窗体最多可显示宽为 120 个字符、长为 50 行的文本。当窗口中有更多文本需要显示，或者输入了一些命令，而 PowerShell 控制台的窗口已满，那么之前的文本会向上滚动。如果想在一个命令输出时暂时停止在当前窗口中的显示，可以按下 Ctrl+S 组合键。然后再次按下 Ctrl+S 组合键继续或者 Ctrl+C 组合键来终止当前命令的运行。

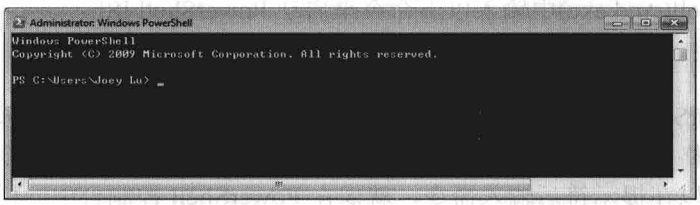


图 1.1　在使用 PowerShell 时，将经常使用命令行环境

在 Windows 7 中，显示文本如下：

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Joey Lu>
```

在这里，PowerShell 的命令提示符显示当前工作目录，用 PS 表示，默认情况下是 %UserProfile%，表示当前用户的用户配置文件目录。在命令提示符之后有一个光标在闪烁，

表示 PowerShell 正处于交互处理模式。在交互处理模式中，可以在提示符之后直接输入命令并按下 Enter 键执行。例如，输入 **get-childitem** 并按 Enter 键获得当前目录列表。

Windows PowerShell 也有非交互处理模式，用于执行一系列命令。在非交互处理模式下时，PowerShell 逐一读取并且执行命令，但不会输出提示给当前用户。典型的例子是从一个脚本文件中读取一串命令，但可以在非交互处理模式下启动 PowerShell 控制台。

要退出 PowerShell，输入 **exit**。如果之前从一个命令提示符下启动了 PowerShell，输入 **exit** 后将返回命令提示符。如果想在 PowerShell 中运行一个分离的 PowerShell 实例，可以在 PowerShell 提示符下输入 **powershell**。这样的调用方式允许使用特定参数初始化 PowerShell 同时使用分离的会话。

1.2.2 使用 Windows PowerShell 集成脚本环境

Windows PowerShell 图形环境的官方名称是 Windows PowerShell 集成脚本化境(ISE)。使用这一应用程序(powershell_ise.exe)，可以在一个单独的集成界面下运行命令以及编写、运行、调试脚本。有 32 位和 63 位图形环境可供 Windows PowerShell 使用，可以在 PowerShell 控制台目录下找到相应的可执行文件。

可以通过使用“开始”菜单中的“搜索”文本框启动 PowerShell。单击“开始”，在“搜索”文本框中输入 **powershell**，然后选择要运行的 PowerShell 版本。或者，可以单击“开始”|“所有程序”|“附件”| Windows PowerShell，然后选择 PowerShell V2 ISE。在 64 位系统中，默认启动 64 位的 Windows PowerShell V2 ISE。如果需要在 64 位系统中使用 32 位的 Windows PowerShell V2 ISE，必须选择 Windows PowerShell V2 ISE(x86)项。

可以在命令行 shell(cmd.exe)中输入以下命令来启动 PowerShell ISE：

```
powershell_ise
```

图 1.2 显示 PowerShell ISE 的主窗口。默认情况下，主窗口显示“脚本”窗格、“命令”窗格和“输出”窗格。在“脚本”窗格中，可以为 PowerShell 脚本输入命令和文本。在“命令”窗格中，可以在提示符后输入命令，就像在 PowerShell 控制台中一样。“输出”窗格显示执行脚本或命令的结果。

在“脚本”或“命令”窗格中输入文本后，文本的颜色将依据输入的文本是命令、函数、变量还是其他类型的文本而改变。“视图”菜单选项允许控制显示的窗格。如果之前“脚本”窗格是隐藏的，可以选择“显示脚本窗格”来显示。如果需要，再次选取来隐藏它。当“脚本”窗格显示后，可以选择“在右侧显示脚本窗格”让它在右侧显示，而不是在顶端停靠。再次选择这一选项可以还原到先前位置。如果倾向于让“命令”窗格在“输出”窗格上端显示，选择“在顶部显示命令窗格”选项。我个人倾向的布局是“命令”窗格在上方，“脚本”窗格靠右(如图 1.3 所示)。这样的排列确保工作时窗口的简洁。也可以使用点击、拖动来定义每个窗格的大小。