Microsoft

Windows Sysinternals实战指南

[美] Mark Russinovich　Aaron Margosis 著　刘晖 译

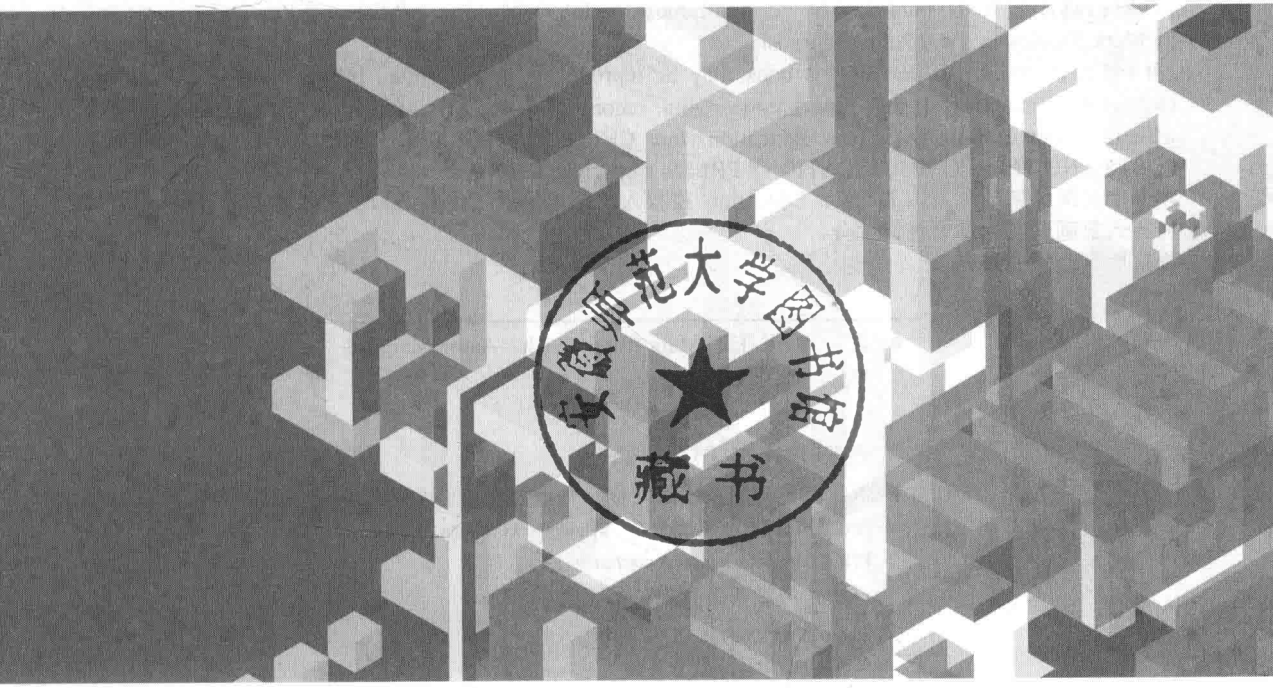
- 微软官方著作最新版
- 助你轻松提升Windows的可靠性和性能

Troubleshooting with the Windows Sysinternals Tools

中国工信出版集团　人民邮电出版社 POSTS & TELECOM PRESS

Windows Sysinternals实战指南

[美] Mark Russinovich Aaron Margosis 著 刘晖 译



Troubleshooting with the Windows Sysinternals Tools

人民邮电出版社
北京

图书在版编目（CIP）数据

Windows Sysinternals实战指南 / （美）马克·拉西诺维（Mark Russinovich），（美）艾伦·马格西斯（Aaron Margosis）著；刘晖译. — 北京：人民邮电出版社，2017.10
ISBN 978-7-115-46365-4

Ⅰ. ①W… Ⅱ. ①马… ②艾… ③刘… Ⅲ. ①Windows操作系统－指南 Ⅳ. ①TP316.7-62

中国版本图书馆CIP数据核字(2017)第218218号

版权声明

◆ 著　[美] Mark Russinovich　Aaron Margosis
译　刘　晖
责任编辑　王峰松
责任印制　焦志炜

◆ 人民邮电出版社出版发行　北京市丰台区成寿寺路 11 号
邮编　100164　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市海波印务有限公司印刷

◆ 开本：800×1000　1/16
印张：34.75
字数：710 千字　2017 年 10 月第 1 版
印数：1－2 000 册　2017 年 10 月河北第 1 次印刷

著作权合同登记号　图字：01-2017-0990 号

定价：118.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

内容提要

Windows Sysinternals 工具已被很多 IT 专家和高级用户用作在 Windows 平台上进行问题诊断和排错，以及深入理解 Windows 系统的全功能“瑞士军刀”。这本由 Sysinternals 创始人 Mark Russinovich 与 Windows 专家 Aaron Margosis 联手编著的实战指南图书详细介绍了 Sysinternals 每款工具的独到功能，并用较多篇幅深入介绍了如何通过几款重量级工具优化 Windows 系统的可靠性、执行效率、性能以及安全性。最后，还通过大量现实案例介绍了通过这些工具解决程序出错、停止响应、卡顿、恶意软件感染等问题的思路、方法以及完整过程。

序言

新版《Windows Sysinternals 实战指南》的到来让人惊喜，我在苏格兰乡村庄园收到这本书的同时正在筹划一次骑行活动，当时的激动之情无疑于首次体验飞行。现在我已经意识到，对于没有魔法的人（我们将其称之为 Sysintuggle[1]），无论领悟能力如何，作者正在试图解决“人们为什么不再读说明书了？”这样的问题，而结论实在让人无言，“因为那些小册子根本没什么用”（他们在解决问题的过程中也获得了更多经验和收获，足以应对哪怕最严重的问题）。但其实他们根本没有意识到这本书所蕴含的价值。

我静下心来开始阅读本书。轻抚书脊，平静地翻开，开始浏览。这是一本很有魅力的书，有着最高的质量，仿佛每一页都在彰显着实用的魔法。通过与《Windows Internals》中的理论遥相呼应，读者可以从中获得最全面的知识和神奇的魔力。通过充分利用本书中介绍的技术和思路，可以帮助读者顺利应对各种问题。本书可以帮助读者更好地领悟 Windows，预防恶意软件。本书可以告诉读者如何获得见解，更顺利地完成排错，甚至轻松解决蓝屏死机问题。我开始一边读一边做笔记，重点页面开始折角，留白处写满了心得体会，就这样给自己准备了一个不可或缺的参考工具。这本书会在我的书架上占据最醒目的位置。

对于希望将“不可能”变为“可能”的读者，本书提供了巨大的参考价值。如果你在公司中担任系统管理员，那么无论公司规模或大或小，都能从本书中有所收获。Russinovich 教授无疑是这个年龄段中最耀眼的天才，他和同事联手合作给我们带来了如此不可或缺的宝藏。

一个著名的人

2016 年 5 月

1 译注：此处的“Sysintuggle”是一个自造词。在《哈利·波特》系列电影中，使用麻瓜（Muggle）称呼没有魔法能力的普通人，其中的“M”是魔法（Magic）的首字母，因此这里使用“Sysintuggle”称呼没有“Sysint”能力，即 System Internal（系统原理）能力的人。

前言

Sysinternals Suite 工具套件包含超过 70 种适用于 Windows 平台的高级诊断和排错工具，这些工具由我——Mark Russinovich 和 Bryce Cogswell 开发而来。微软于 2006 年收购 Sysinternals 后，这些工具开始通过微软（TechNet 旗下）Windows Sysinternals 网站免费提供下载和使用。

本书目标在于帮助读者熟悉 Sysinternals 工具，了解如何更充分地利用这些工具。本书还将介绍一些我和他人使用这些工具解决 Windows 系统现实问题的范例。

虽然本书是我与 Aaron Margosis 合著的，但完全表达了我的观点。Aaron 也对本书做出了巨大的贡献，这本书的顺利出版离不开他的辛苦工作。

注意 有关本书出版过程中的内容改动，请参阅前言“后期改动”一节。

本书涉及的工具

本书介绍了 Windows Sysinternals 网站（http://technet.microsoft.com/en-us/sysinternals/default.aspx）提供的所有 Sysinternals 工具在撰写本文时（2016 年初夏）包含的全部功能。然而 Sysinternals 工具的开发进度非常快，现有工具会不断获得新增功能，此外时不时还会引入新的工具（为及时了解最新进展，请订阅“Sysinternals 网站讨论”博客的 RSS 信息源：http://blogs.technet.microsoft.com/sysinternals/）。在你阅读本书的时候，其中一些内容可能已经过时了，不过你依然应该尽量使用最新版 Sysinternals 工具，以便获得新增功能以及各种瑕疵修复。

本书并未涉及已弃用并不再通过 Sysinternals 网站提供的工具。如果你依然在使用 RegMon（注册表监视器）或 FileMon（文件监视器），可以考虑使用第 5 章介绍的 Process Monitor 取代这些工具。计算机行业首个 Rootkit 检测工具 Rootkit Revealer（正是这个工具发现了“Sony rootkit”）也已完成使命顺利退役。此外还有其他几个提供了独特价值的工具（例如 Newsid 和 EfsDump）也已经由于不再需要或 Windows 已包含类似的功能而退役。

Sysinternals 的历史

我开发的首个 Sysinternals 工具是 Ctrl2cap，它的诞生有一定的必然性。我从 1995 年开始使用 Windows NT，之前主要使用 UNIX，该系统的键位设置在标准 PC 键盘上 Caps Lock 键的位置是 Ctrl 键。我不想适应新的键位布局，于是开始研究 Windows NT 设备驱动的开发，并写了一个能将 Caps Lock 键的按压转换为 Ctrl 键的按压结果并传递至 Windows NT 输入系统的驱动。Ctrl2cap 目前依然放在 Sysinternals 网站上，我还在自己的所有系统中使用着。

Ctrl2cap 是我所开发的深入至 Windows NT 底层技术，同时提供了实用功能的众多工具中的第一个成员。在这之后我与 Bryce Cogswell 联手开发了 NTFSDOS。我和 Bryce 最初在卡内基梅隆大学（Carnegie Mellon University）研究生院相识，我们一起完成了多篇学术论文，并发起了一个为 Windows 3.1 开发软件的初创项目。当时我产生了一个念头，想要写一个能够让用户通过无处不在的 DOS 软盘访问 NTFS 分区的工具。Bryce 觉得这个工具在编程方面会遇到一些有趣的挑战，大概一个月后我们完成了该工具的开发并发布了第一个版本。

随后我还与 Bryce 合作开发了另外两个工具：Filemon 和 Regmon。NTFSDOS、Filemon 以及 Regmon 这 3 个工具奠定了 Sysinternals 的基础。当时我们发布的 Filemon 和 Regmon 可运行于 Windows 95 和 Windows NT 系统上，可用来查看文件系统和注册表活动，这样的功能在当时是独一无二的，很快成为我们排错过程中必不可少的帮手。

随后 Bryce 和我决定将这些工具共享给其他人，但当时我们并没有自己的网站，所以最初我们将这些工具放在了另一位友人——Andrew Schulman 的网站上。我最初认识他时，他也在研究 DOS 和 Windows 95 的内部运作。由于当时需要通过中间人来发布这些工具，因此我们无法根据进度及时更新这些工具并修复瑕疵，因此 Bryce 和我在 1996 年 9 月创建了 NTInternals.com 网站，通过这个网站发布我们的工具，以及我们撰写的有关 Windows 95 和 Windows NT 内部运作的文章。后来我们觉得可以通过销售自己开发的工具赚点零花钱，所以在网站上线的同一个月，我们成立了商用软件公司 Winternals Software，并通过 NTInternals.com 上放置的一个横幅广告为新公司吸引流量。我们以 Winternals Software 公司身份发布的第一个工具是 NTRecover，这个工具可以帮助用户将无法启动的 Windows NT 系统的磁盘挂载到其他可以使用的计算机上，然后像访问本地磁盘一样访问故障计算机中的文件。

NTInternals.com 的使命是分发免费的工具软件，我们利用对 Windows 操作系统的深入理解开发了一系列功能强大的诊断、监视和管理工具。经过几个月的发展，该网站终于在 1996 年 12 月发展成图 0-1 的样子（这还要感谢 Internet Archive 的 Wayback Machine 功能可以让我们随时回顾历史），当时该网站的每天访客数已经达到 1500 人，逐渐成为互联网革命开始前的“上古时代”最受欢迎的 Windows 工具网站。1998 年，在微软公司律师的

“启发”下，我们将网站改名为 Sysinternals.com。

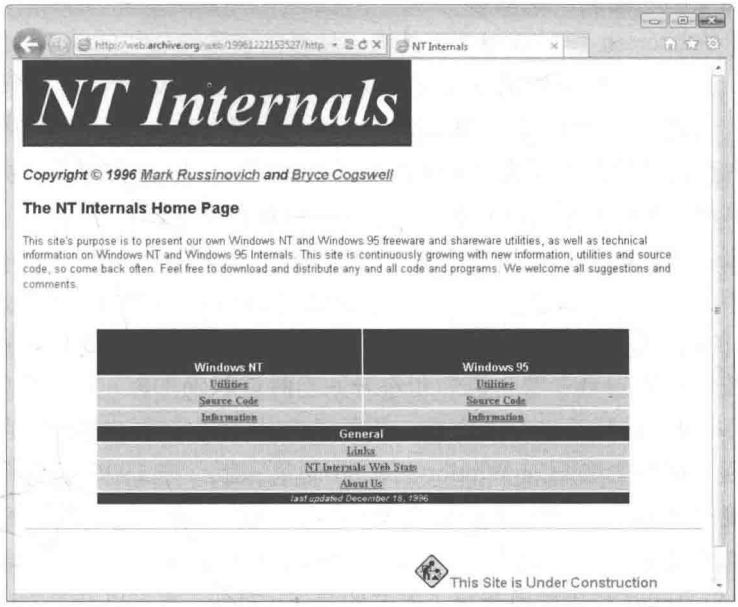


图 0-1　NTInternals.com 网站

过去多年来，我们开发的工具一直在不断完善。我们根据自己的实际需要，根据大量早期用户的反馈和建议，并根据我们所设想的有关 Windows 内部各类信息的呈现方式开发了更多工具。

Sysinternals 工具主要可分为 3 个基本类别：针对程序开发工作的，针对系统排错工作的，以及针对系统管理工作的。可以获取并显示程序调试语句的 DebugView 工具是我所开发的第一个面向开发者的工具，该工具主要用来帮我开发设备驱动。显示进程所加载 DLL 信息的 DLLView，以及可以显示进程所打开句柄的进程列表 GUI 工具 HandleEx，这两个工具是最早开发出来的排错工具（我在 2001 年将 DLLView 和 HandleEx 的工具合并在一起开发了 Process Explorer）。本书第 7 章将要介绍的 PsTools 则是最受欢迎的管理工具，为了方便大家下载，我把它们捆绑成了一个工具套件。PSTools 系列首个工具 PsList 最初的灵感来源于 UNIX 中用于查看进程列表的 PS 命令。这些工具的数量和功能不断增加，很快形成了一个工具套件，可以帮助用户更轻松地针对远程系统执行各种任务，而无须事先在远程系统上安装任何特殊软件。

到了 1996 年，我开始为《Windows IT Pro》杂志撰文，我的文章主要介绍 Windows 内部原理和 Sysinternals 工具，此外我还写了介绍其他功能的文章，例如 1996 年撰写的一篇引起广泛争议的文章让我在微软内部正式扬名，尽管大部分意见并非正面的。当时我在“Inside the Difference Between Windows NT Workstation and Windows NT Server”这篇文章

中指出，Windows NT Workstation 和 Windows NT Server 操作系统之间的差异仅仅是微软出于产品营销角度的考虑而产生的。

随后我发布的 Ntcrash 和 Ntcrash2 工具进一步恶化了微软与我的关系，这两个现在被称之为“Fuzzer”[1]的工具会使用随机生成的垃圾数据阻塞 Windows NT 系统调用接口。这些工具可检测出大量使用弱参数验证（Weak parameter validation），进而可能由于非特权用户模式进程造成内存出错和蓝屏崩溃的系统调用（在 20 世纪 90 年代的系统安全大环境下，这种问题被简单地视作可靠性方面的小瑕疵，不像现在会被视作“重要”的安全瑕疵）。

随着这些工具的继续完善和增加，我开始考虑专门撰写一本有关 Windows 内部原理的图书。当时市面上已经有了类似的图书：《Inside Windows NT》（Microsoft Press，1992 年出版），本书的第一版由 Helen Custer 撰写，并伴随 Windows NT 3.1 一起出版。本书第二版由操作系统领域的知名专家、讲师和作者，当时就职于 DEC 公司的 David Solomon 围绕 Windows NT 4.1 重写并进行了完善。我并没有从头开始写一本类似的书，而是联系他并建议与他联手撰写主要面向 Windows 2000 的第三版。在 1996 年那篇文章余波渐平后，随着我直接向 Windows 开发人员提交 Windows 瑕疵报告，我与微软的关系正在逐渐回温，但 David 依然需要获得微软的允许，好在微软也同意了。

随后 David Solomon 和我联手撰写了本书的第三、第四、第五以及第六版。从第四版开始，本书改名为《Windows Internals》。从第五版开始，我们选择了 Alex Ionescu 作为合著者。到第六版，书中包含的内容实在太多，于是我们决定将该书分为上下两部。就在我们完成《Inside Windows 2000》（Microsoft Press，2000 年出版）后不久，我开始与 David 合作讲授他的 Windows 内部原理研讨会课程，并加入了我所撰写的内容。这一由微软向全球 Windows 开发者提供的课程大量借助 Sysinternals 工具向学生介绍有关 Windows 内部运作的深入信息，当这些学生返回自己的开发者和 IT 专业人员工作岗位后，也陆续开始使用我们开发的这些工具。

到了 2006 年，我与微软的关系已经好转并维持了多年，Winternals 也逐渐开发出一整套企业管理软件，经过多年的发展已经有了 100 多名员工，同时 Sysinternals 工具的每月下载量达到了 2 百万次。2006 年 7 月 18 日，微软收购了 Winternals 和 Sysinternals。不久之后 Bryce 和我（图 0-2 是我们在 2006 年的合影）加入了 Windows 团队并搬家到

图 0-2　Mark Russinovich 和 Bryce Cogswell 的合影

1　译注：此处的 Fuzzer 是指用于 Fuzz testing（模糊测试）的工具，这是现在比较常见的一种测试方法，其核心思想是以自动或半自动方式生成随机数据输入到一个程序中，并监视程序异常，如崩溃，断言（Assertion）失败，以发现可能的程序错误，如内存泄漏。这种模糊测试常用于检测软件或计算机系统的安全漏洞，详见：https://en.wikipedia.org/wiki/Fuzz_testing。

雷德蒙。目前我担任 Microsoft Azure 首席技术官的职务，主要负责领导 Azure 云计算平台的技术战略和架构。

当时的收购，主要目标在于确保 Bryce 和我开发的工具能继续免费提供，并且我们构建的社区能够继续发展，这两个目标都实现了。目前，托管在 technet.microsoft.com 上的 Windows Sysinternals 网站已成为整个 TechNet 访问量最大的网站之一，平均每月下载量高达 450 万次。Sysinternals 的高级用户会时不时访问该网站获取最新版工具以及新发布的工具，例如最近我们发布的 Sysmon 和 PsPing，与此同时他们也会积极参与 Sysinternals 社区，在撰写本文时，这个飞速成长的社区已经有超过 42000 名注册用户。我还会继续对现有工具进行完善，并增加新的工具。

很多人曾建议如果能针对这些工具写一本书就太好了，但直到 David Solomon 也提出类似的建议，这个项目才开始提上日程。我在微软承担的工作使得我没有足够的时间另外写一本书，但 David 觉得可以找人来帮忙。最终 Aaron Margosis 同意与我合作，为此我感到很高兴。Aaron 是 Microsoft Cybersecurity Services 部门的首席顾问，他对 Windows 安全性和应用程序兼容性有着极为深入的理解。我与 Aaron 相识多年，他卓越的写作技能，对 Windows 内部原理的熟悉程度，以及对 Sysinternals 工具的娴熟掌握使得他成为理想的合著者。

本书的目标读者

本书适合 Windows IT 专家、高级用户，以及希望更充分利用 Sysinternals 工具的开发者阅读。无论你对这些工具有怎样的了解，无论你管理着大企业或小公司的系统，或者只是维护着家人或朋友的计算机，本书中涉及的工具、技巧，以及经验都可以帮助你更高效地对 Windows 故障进行排错，让系统管理运维和监控工作变得更简单。

前提假设

本书会假设你已经熟悉并了解 Windows 操作系统。如果能对进程、线程、虚拟内存，以及 Windows 命令行等概念有基本了解，则将对阅读本书起到更大的帮助，本书第 2 章“Windows 核心概念”对上述部分概念也有所涉及。

本书的组织方式

本书分为 3 部分。第 1 部分“入门”概括介绍了 Sysinternals 工具和 Sysinternals 网站，并介绍了所有工具中通用的功能，会告诉你如何获得帮助，同时还介绍了可以帮你更好地

理解整个平台及这些工具所呈现信息应了解的一些 Windows 核心概念。

第 2 部分“使用指导”详细介绍了所有 Sysinternals 工具的功能、命令行选项、系统要求，以及注意事项。在大量屏幕截图和用例的帮助下，这部分内容可以回答你关于这些工具可能产生的各种问题。对于一些重要的工具，例如 Process Explorer 和 Process Monitor，会用专门的章节进行介绍，后续章节则会按照类别介绍不同的工具，例如安全工具、Active Directory 工具，以及文件工具。

第 3 部分“排错——‘难解之谜’”通过真实案例介绍了 Aaron 和我，以及全球各地管理员和高级用户使用 Sysinternals 工具解决实际问题的过程。

本书中的约定和特色

为了让相关信息更易读，更益于参照，本书中内容的呈现使用了下列约定。

- 标有“注意”字样的方框提供了为成功完成某些步骤需要注意的事项或其他备选的实现方法。
- 需要用户输入的文字（代码块除外）将加粗显示。
- 两个按键名称之间的加号（+）意味着必须同时按下这些按键。例如“按下 Alt+Tab”意味着需要按下 Alt 键，并在不松手的情况下按 Tab 键。
- 两个或多个菜单项之间的竖线（例如 文件 | 关闭）意味着需要先选择第一个菜单或菜单项，随后选择下一个项目，以此类推。
- 在命令行语法规范中，竖线意味着“OR（或）”，方括号意味着“可选”，斜体字意味着需要用户输入的信息对应的占位符，花括号意味着分组，省略号代表重复模式。例如：

```
procdump
    [-ma | -mp | -d callback_DLL] [-64] [-r [1..5] [-a] [-o]
    [-n count] [-s secs]
    [-c|-cl percent [-u]] [-m|-ml commit] [-p|-pl counter_threshold]
    [-e [1 [-g] [-b]]] [-h] [-l] [-t] [-f filter,...]
    {
      {{[-w] process_name}|service_name|PID } [dump_file | dump_folder] } |
      {-x dump_folder image_file [arguments]}
    }
```

上述代码意味着**-ma**、**-mp** 或**-d** 是可选使用的；如果使用**-d**，必须为 *callback_DLL* 赋值。此外还可选择使用**-f** 选项，如果使用，则必须提供一个或多个 *filter* 值。最后四行的分组意味着必须指定一个 *process_name*、*service_name* 或 *PID*，或使用**-x** 选项并提供 *dump_folder* 和 *image_file*。

系统要求

除非特别注明，Sysinternals 工具可在下列受支持的 Windows 版本，包括 64 位版中运行：

- Windows Vista；
- Windows 7；
- Windows 8.1；
- Windows 10（桌面）[1]；
- Windows Server 2008；
- Windows Server 2008 R2；
- Windows Server 2012；
- Windows Server 2012 R2；
- Windows Server 2016，包括 Nano Server。

一些工具运行时需要管理权利，其他工具中部分功能可能需要管理权利。

后期改动

在本书即将完工的过程中，为了对 Windows Server 2016 新增的 Nano Server 模式提供支持，本书涉及的很多工具均发布了新版本。Nano Server 是一种小痕迹、无头式（Headless）Windows Server 2016 安装选项，仅包含最少量的功能和服务。对 Sysinternals 用户来说，最值得关注的地方在于 Nano Server 不包含 32 位子系统和 GUI 组件。正如在本书“第 1 章：Sysinternals 工具入门”中所述，每款 Sysinternals 工具均会和其他必要的文件，例如 64 位库文件一起打包成一个 32 位可执行文件，这些嵌入的资源可按需提取并执行。当然，所有这些 32 位映像均无法在 Nano Server 上运行，于是我为控制台模式的工具创建了原生的 64 位版本，并在文件名末尾附加了“64.exe”字样。例如 64 位版 SigCheck.exe 变成 SigCheck64.exe。此外我还创建了控制台版本的 LoadOrd（加载顺序）工具：LoadOrdC.exe，以及一个原生的 64 位版 LoadOrdC64.exe。

Nano Server 的管理严重依赖 PowerShell Remoting。PowerShell 会将标准错误（stderr）流的所有输出视作对错误的陈述。控制台模式的 Sysinternals 工具会始终将 Banner 和语法信息写入 Stderr。为改善这些工具对 PowerShell，尤其是 Nano Server 的支持，现在这些工具已可将 Banner 和语法信息写入标准输出（stdout）流，并会使用新增的**-nobanner** 命令行选项忽略 Banner 输出。然而要注意，该选项取代了以往很多工具用来实现类似功能的**-q** 选项。

1 所有 Sysinternals 工具均为 Win32 应用，仅支持 x86 和 x64 架构系统，不兼容 Windows 10 Mobile、IoT、Xbox 等。

致谢

首先 Aaron 和我要感谢 Sysinternals 的共同创始人 Bryce Cogswell，他对 Sysinternals 工具的开发做出了卓越贡献。借助我们之间的良好合作，Bryce 和我才有机会联手发布各种实用的 Sysinternals 工具。Bryce 已于 2010 年 10 月从微软退休，无论他今后的目标是什么，我们希望他好运。

此外也要感谢 David Solomon 鼓励 Mark 撰写这本书，负责对本书很多章节的审阅，并为第一版作序。多年来，Dave 都是最热心的 Sysinternals“布道师”之一，针对不同新功能提供了宝贵的建议。

感谢 Luke Kim 在本项目升级到最新版 Microsoft Visual Studio，为开发工作提供 Visual Studio Team Services（VSTS）源代码控制系统，优化构建和发布流程，管理 Sysinternals.com 网站和 live.sysinternals.com 基础架构服务器（现已运行在 Azure 之上）过程中提供的大量帮助。同时还要感谢 Kent Sharkey 发布的 Sysinternals.com 网站更新。

几年前，只有 Bryce 和我负责这些工具的开发，但我也开始逐渐接受其他开发者的贡献。Ken Johnson、Andrew Richards、Thomas Garnier、David Magnotti、Dmitry Davydok、Daniel Pearson、Justin Jiang 和 Nano Server 团队的其他成员、Giulia Biagini、Pavel Yosifovich，以及 Aaron Margosis 均对一些功能的开发做出了自己的贡献。

此外还要感谢 John Sheehan 对以往未曾公开过的 AppContainers 工作原理进行的深入介绍；Alex Ionescu 提供了有关受保护进程的技术细节；感谢 Ned Pyle、Marty Lichtel 和 Carl Harrison 允许将他们以前发布的案例纳入本书。

本书的技术审阅和修订过程中，得到了来自下列人员提供的宝贵见解和建议，我们也要向他们表示感谢：Andrew Richards、Bhaskar Rastogi、Bruno Aleixo、Burt Harris、Chris Jackson、Crispin Cowan、Greg Cottingham、Ken Johnson（即 Skywing）、Luke Kim、Mario Raccagni、Steve Thomas，以及 Yong Rhee。

Aaron 和我对于邀请那个著名的人为这本书作序本来并没有抱太大希望，他竟然同意了，至今我们依然难以置信。万分感谢 N.P.（Noted Person）[1]。

我们还要感谢 Microsoft Press 的 Devon Musgrave（策划编辑兼开发编辑）和 Carol Dillingham（项目编辑）在本书出版过程中付出的辛苦工作，尤其要感谢他们在本来规定好的交稿日期“无限”延后的过程中表现出的耐心。感谢 Waypoint Press 的 Steve Sagman 在项目管理和排版方面提供的支持。同时要感谢负责技术加工的 Christophe Nasarre 和负责文案编辑的 Roger LeBlanc。Aaron 还想向自己的妻子 Elise 和孩子 Elana、Jonah 和 Gabriel 表示感谢，谢谢他们的爱和支持。另外 Aaron 还要感谢 Brenda Schrier 拍摄的作者照片，并要感谢华盛顿国家棒球俱乐部和西汉姆联队。

1 那个“著名的人”，他的秘密身份其实是 Chris Jackson，即 The App Compat Guy，亦即 Captain Inappropriate。

Mark 也希望对他的妻子 Daryl 和女儿 Maria 表示感谢，感谢她们对自己工作的支持。

勘误、更新和图书支持

我们已经尽了最大努力确保本书内容精确无误。你可以访问 http://aka.ms/TroubleshootSysint/errata 查看本书的最新勘误列表和相应的修订。

如果发现勘误中未列出的错误，也可通过上述页面提交给我们。

如果需要进一步支持，可向 Microsoft Press 图书支持部门发送电子邮件：mspinput@microsoft.com。

然而请注意，上述邮件地址并不提供有关微软软件的产品支持。若要获得有关微软软件或硬件产品的支持，请访问 http://support.microsoft.com。

Microsoft Press 提供的免费电子书

从技术概述到针对特定话题的深入信息，Microsoft Press 针对种类丰富的不同话题提供了免费电子书。这些电子书分为 PDF、EPUB，以及适用于 Kindle 的 Mobi 格式，可随时通过下列地址下载：

http://aka.ms/mspressfree

你也可以经常访问上述地址下载最新发布的电子书！

读者反馈

对于 Microsoft Press 来说，读者的满意是我们的头等要务，读者的反馈是我们最珍视的资产。请通过下列地址告诉我们你对这本书的想法：

http://aka.ms/tellpress

这个调查非常简短，我们会仔细阅读每位读者的意见和建议。提前感谢大家的反馈！

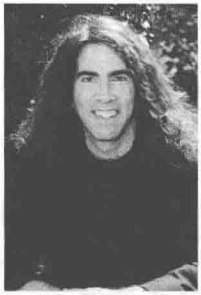
保持联系

书读完了联系也不能中断，你可以关注 Microsoft Press 的 Twitter 账号：http://twitter.com/MicrosoftPress。

关于作者

Mark Russinovich 是 Microsoft Azure 首席技术官，主要负责微软云计算平台的技术战略和架构。他是分布式系统、操作系统内部原理以及网络安全方面公认的专家。他撰写了 Jeff Aiken 系列网络惊险小说《Zero Day》《Trojan Horse》以及《Rogue Code》，同时也是 Microsoft Press 出版的《Windows Internals》多版图书的合著者。Russinovich 在 1996 年创立了 Winternals Software 公司，该公司 2006 年被微软收购，同时 Russinovich 也加入了微软。此外 Russinovich 还建立了 Sysinternals 网站，并通过该网站创作和发布了数十款广受欢迎的 Windows 管理和诊断工具。他还是业内各大技术会议，包括 Microsoft Ignite、Microsoft//build、RSA Conference 等活动的特邀演讲嘉宾。

你可以通过 markruss@microsoft.com 联系 Mark，或关注他的 Twitter 账号：https://www.twitter.com/markrussinovich。



Aaron Margosis 是微软 Global Cybersecurity Practice 部门首席顾问，从 1999 年起开始与安全意识极强的客户打交道。Aaron 专精于 Windows 安全、最小特权、应用程序兼容性，以及锁定环境的配置。他是微软各大会议的主要发言人，开发了很多帮助组织实现高安全环境的常用工具，包括 LUA Buglight、Policy Analyzer、IE Zone Analyzer、LGPO.exe（本地组策略对象工具）以及 MakeMe Admin，这些工具均可从他的个人博客（https://blogs.msdn. microsoft.com/aaron_margosis），以及他作为主要作者的两个团队博客（https://blogs.technet.microsoft.com/fdcc 和 https://blogs.technet.microsoft.com/SecGuide）下载。

你可以通过 aaronmar@microsoft.com 联系 Aaron，或关注他的 Twitter 账号：https://www.twitter.com/AaronMargosis。

关于译者

刘晖，IT 技术和 Windows 操作系统爱好者，热衷于研究 Windows 客户端和服务器技术，多次当选微软最有价值专家（MVP）称号，曾出版过多本有关微软技术的原创和翻译图书。

目录

第 1 部分　入门