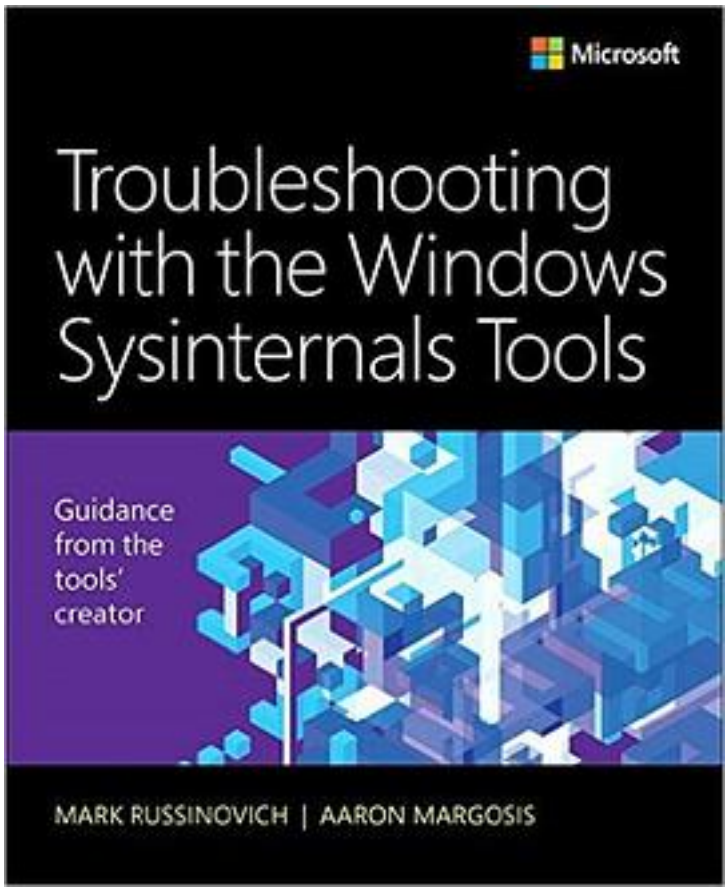
Troubleshooting with the Windows Sysinternals Tools (2nd Edition)



Troubleshooting with the Windows Sysinternals Tools (2nd Edition)_下载链接1_

著者:Mark E. Russinovich

出版者:Microsoft Press

出版时间:2016-10-27

装帧:Paperback

isbn:9780735684447

IT pros and power users consider the free Windows Sysinternals tools indispensable for diagnosing, troubleshooting, and deeply understanding the Windows platform. In this extensively updated guide, Sysinternals creator Mark Russinovich and Windows

expert Aaron Margosis help you use these powerful tools to optimize any Windows system’s reliability, efficiency, performance, and security. The authors first explain Sysinternals’ capabilities and help you get started fast. Next, they offer in-depth coverage of each major tool, from Process Explorer and Process Monitor to Sysinternals’ security and file utilities. Then, building on this knowledge, they show the tools being used to solve real-world cases involving error messages, hangs, sluggishness, malware infections, and much more.

Windows Sysinternals creator Mark Russinovich and Aaron Margosis show you how to:

Use Process Explorer to display detailed process and system information Use Process Monitor to capture low-level system events, and quickly filter the output to narrow down root causes List, categorize, and manage software that starts when you start or sign in to your computer, or when you run Microsoft Office or Internet Explorer Verify digital signatures of files, of running programs, and of the modules loaded in those programs Use Autoruns, Process Explorer, Sigcheck, and Process Monitor features that can identify and clean malware infestations Inspect permissions on files, keys, services, shares, and other objects Use Sysmon to monitor security-relevant events across your network Generate memory dumps when a process meets specified criteria Execute processes remotely, and close files that were opened remotely Manage Active Directory objects and trace LDAP API calls Capture detailed data about processors, memory, and clocks Troubleshoot unbootable devices, file-in-use errors, unexplained communication, and many other problems Understand Windows core concepts that aren’t well-documented elsewhere

作者介绍:

About the Author

Mark Russinovichis Chief Technology Officer of Microsoft Azure, where he oversees the technical strategy and architecture of Microsoft’s cloud computing platform. He is a widely recognized expert in distributed systems, operating system internals, and cybersecurity. He is the author of the Jeff Aiken cyberthriller novels, Zero Day, Trojan Horse, and Rogue Code, and co-author of the Microsoft Press Windows Internals books. Russinovich joined Microsoft in 2006 when Microsoft acquired Winternals Software, the company he cofounded in 1996, as well as Sysinternals, where he authors and publishes dozens of popular Windows administration and diagnostic utilities. He is a featured speaker at major industry conferences, including Microsoft Ignite, Microsoft //build, RSA Conference, and more. Aaron Margosisis a Principal Consultant with Microsoft’s Global Cybersecurity Practice, where he has worked with security-conscious customers since 1999. Aaron specializes in Windows security, least-privilege, application compatibility, and the configuration of locked-down environments. He is a top speaker at Microsoft conferences, and created many of the tools commonly used by organizations implementing high-security environments, including LUA Buglight, Policy Analyzer, IE Zone Analyzer, LGPO.exe (Local Group Policy Object utility), and MakeMeAdmin, which can be downloaded through his blog (https://blogs.msdn.microsoft.com/aaron_margosis)or through two team blogs for which he is a primary author (https://blogs.technet.microsoft.com/fdccandhttps://blogs.technet.microsoft.com/SecGuide).

Read more

目录:

标签

Windows

软件开发

程序设计

专业技术

Sysinternals

Troubleshooting

Profile

#FDP

#

评论

Troubleshooting with the Windows Sysinternals Tools (2nd Edition)_下载链接1_

书评

A great book, definitely worth having on anyone's book shelf, who uses Windows daily. The Mark's concerning blogs and videos about the topic of sysinternals tools could be referenced when reading this book.

Troubleshooting with the Windows Sysinternals Tools (2nd Edition)_下载链接1_