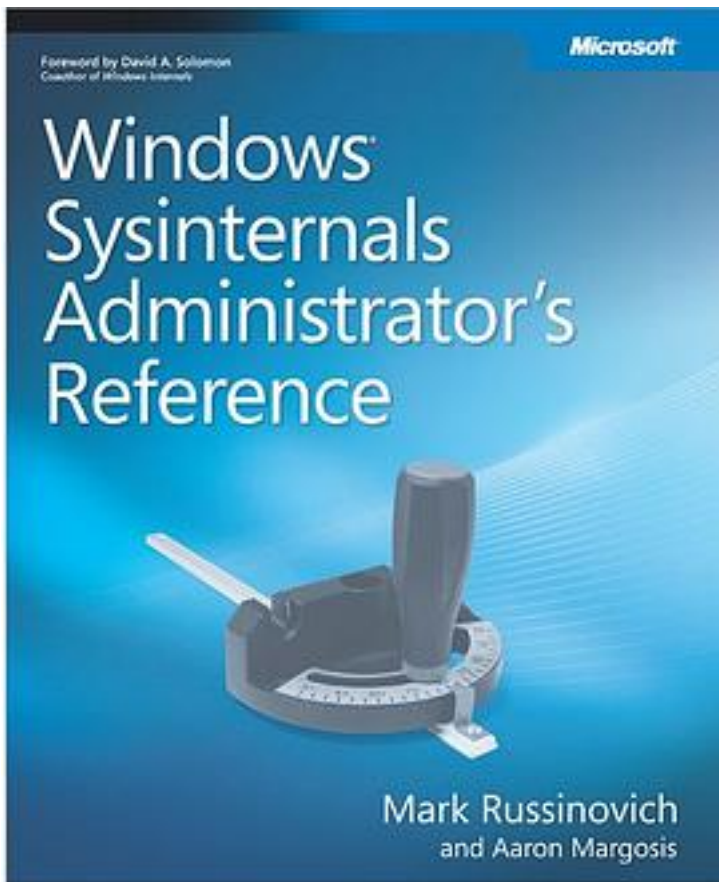


Windows Sysinternals Administrator's Reference



[Windows Sysinternals Administrator's Reference_下载链接1](#)

著者:Mark E. Russinovich

出版者:Microsoft Press

出版时间:2011-6-1

装帧:

isbn:9780735656727

Description

Get in-depth guidance—and inside insights—for using the Windows Sysinternals tools, direct from Sysinternals creator Mark Russinovich and Windows expert Aaron Margosis.

Full Description

Get in-depth guidance—and inside insights—for using the Windows Sysinternals tools available from Microsoft TechNet. Guided by Sysinternals creator Mark Russinovich and Windows expert Aaron Margosis, you'll drill into the features and functions of dozens of free file, disk, process, security, and Windows management tools. And you'll learn how to apply the book's best practices to help resolve your own technical issues the way the experts do.

Diagnose. Troubleshoot. Optimize.

Analyze CPU spikes, memory leaks, and other system problems

Get a comprehensive view of file, disk, registry, process/thread, and network activity

Diagnose and troubleshoot issues with Active Directory®

Easily scan, disable, and remove autostart applications and components

Monitor application debug output

Generate trigger-based memory dumps for application troubleshooting

Audit and analyze file digital signatures, permissions, and other security information

Execute Sysinternals management tools on one or more remote computers

Master Process Explorer, Process Monitor, and Autoruns

作者介绍:

Mark Russinovich

Mark Russinovich is a Technical Fellow in the Windows Azure group at Microsoft working on Microsoft's datacenter operating system. He is a widely recognized expert in Windows operating system internals as well as operating system security and design. Russinovich is the author of the recently published cyberthriller Zero Day, co-author of the Microsoft Press Windows Internals books, and co-author of the Sysinternals Administrator's Reference. 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's Tech • Ed, WinHEC, and Professional Developers Conference.

=====

Aaron Margosis

Aaron Margosis is a Windows nerd, focusing a lot on security, running with least privilege, and the application compatibility impacts of doing so. He has published a number of useful tools over the years, including MakeMeAdmin, LUA Buglight, IE Zone Analyzer, and the Local Group Policy utilities on the Microsoft FDCC/USGCB blog. He

delivers training around application compatibility to customers and at conferences with an emphasis on government-mandated locked-down environments. Aaron joined Microsoft Services in 1999, where he works primarily with US government customers.

目录: Table of Contents

Getting Started

Chapter 1 Getting Started with the Sysinternals Utilities

Overview of the Utilities

The Windows Sysinternals Web Site

Sysinternals License Information

Chapter 2 Windows Core Concepts

Administrative Rights

Processes, Threads, and Jobs

User Mode and Kernel Mode

Handles

Call Stacks and Symbols

Sessions, Window Stations, Desktops, and Window Messages

Usage Guide

Chapter 3 Process Explorer

Procexp Overview

Main Window

DLLs and Handles

Process Details

Thread Details

Verifying Image Signatures

System Information

Display Options

Procexp as a Task Manager Replacement

Miscellaneous Features

Keyboard Shortcut Reference

Chapter 4 Process Monitor

Getting Started with Procmon

Events

Filtering and Highlighting

Process Tree

Saving and Opening Procmon Traces

Logging Boot, Post-Logoff, and Shutdown Activity

Long-Running Traces and Controlling Log Sizes

Importing and Exporting Configuration Settings

Automating Procmon: Command-Line Options

Analysis Tools

Injecting Debug Output into Procmon Traces

Toolbar Reference

Chapter 5 Autoruns

Autoruns Fundamentals

Autostart Categories

Saving and Comparing Results

AutorunsC

Autoruns and Malware

Chapter 6 PsTools

Common Features

Psexec

PsFile

PsGetSid
PsInfo
PsKill
PsList
PsLoggedOn
PsLogList
PsPasswd
PsService
PsShutdown
PsSuspend
PsTools Command-Line Syntax
PsTools System Requirements
Chapter 7 Process and Diagnostic Utilities
VMMap
ProcDump
DebugView
LiveKd
ListDLLs
Handle
Chapter 8 Security Utilities
SigCheck
AccessChk
AccessEnum
ShareEnum
ShellRunAs
Autologon
LogonSessions
SDelete
Chapter 9 Active Directory Utilities
AdExplorer
AdInsight
AdRestore
Chapter 10 Desktop Utilities
BgInfo
Desktops
ZoomIt
Chapter 11 File Utilities
Strings
Streams
NTFS Link Utilities
DU (Disk Usage)
Post-Reboot File Operation Utilities
Chapter 12 Disk Utilities
Disk2Vhd
Diskmon
Sync
DiskView
Contig
PageDefrag
DiskExt
LDMDump
VolumeID
Chapter 13 Network and Communication Utilities
TCPView

Whois
Portmon
Chapter 14 System Information Utilities
RAMMap
CoreInfo
ProcFeatures
WinObj
LoadOrder
PipeList
ClockRes
Chapter 15 Miscellaneous Utilities
RegJump
Hex2Dec
RegDelNull
Bluescreen Screen Saver
Ctrl2Cap
Troubleshooting— “The Case of the Unexplained...”
Chapter 16 Error Messages
The Case of the Locked Folder
The Case of the Failed AV Update
The Case of the Failed Lotus Notes Backups
The Case of the Failed Play-To
The Case of the Crashing Proksi Utility
The Case of the Installation Failure
The Case of the Missing Folder Association
The Case of the Temporary Registry Profiles
Chapter 17 Hangs and Sluggish Performance
The Case of the IExplore-Pegged CPU
The Case of the Excessive ReadyBoost
The Case of the Slow Keynote Demo
The Case of the Slow Project File Opens
The Compound Case of the Outlook Hangs
Chapter 18 Malware
The Case of the Sysinternals-Blocking Malware
The Case of the Process-Killing Malware
The Case of the Fake System Component
The Case of the Mysterious ASEP
Appendix About the Authors
• • • • • ([收起](#))

[Windows Sysinternals Administrator's Reference 下载链接1](#)

标签

计算机

工具

软件

DEV

Windows

评论

[Windows Sysinternals Administrator's Reference 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.

[Windows Sysinternals Administrator's Reference 下载链接1](#)