Contents

- Home
  - Learn
    - Mark's Webcasts
    - Windows Internals Book
    - Troubleshooting with the Windows Sysinternals Tools
    - Inside Native Applications
  - Downloads
    - File and Disk Utilities
      - AccessChk
      - AccessEnum
      - CacheSet
      - Contig
      - Disk2vhd
      - DiskExt
      - DiskMon
      - Disk Usage
      - DiskView
      - EFSDump
      - LDMDump
      - MoveFile
      - NTFSInfo
      - PageDefrag
      - PendMoves
      - RegMon
      - SDelete
      - Sigcheck
      - Streams
      - Sync
      - VolumeID

- Networking Utilities
  - Active Directory Explorer
  - Insight for Active Directory
  - AdRestore
  - PipeList
  - PsFile
  - PsPing
  - ShareEnum
  - TCPView
  - Whois
- Process Utilities
  - AutoRuns
  - Handle
  - ListDLLs
  - Portmon
  - ProcDump
  - Process Explorer
  - Process Monitor
  - PsExec
  - PsGetSid
  - PsKill
  - PsList
  - PsService
  - PsSuspend
  - PsTools
  - ShellRunas
  - VMMap
- Security Utilities
  - Autologon
  - LogonSessions
  - NewSID
  - PsLoggedOn

- PsLogList
- RootkitRevealer
- Sysmon
- System Information
  - ClockRes
  - Coreinfo
  - LiveKd
  - LoadOrder
  - ProcFeatures
  - PsInfo
  - RAMMap
  - WinObj
- Miscellaneous
  - BgInfo
  - BlueScreen Screen Saver
  - CpuStres
  - Ctrl2Cap
  - DebugView
  - Desktops
  - Hex2dec
  - NotMyFault
  - PsPasswd
  - PsShutdown
  - RegDelNull
  - Registry Usage
  - Reghide
  - RegJump
  - Strings
  - Testlimit
  - ZoomIt
- Sysinternals Suite

Community

Software License Terms

Licensing FAQ

Windows Sysinternals

5 minutes to read • Edit Online

The Sysinternals web site was created in 1996 by Mark Russinovich to host his advanced system utilities and technical information. Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications.

- Read the official guide to the Sysinternals tools, Troubleshooting with the Windows Sysinternals Tools
- Read the Sysinternals Blog for a detailed change feed of tool updates
- Watch Mark's top-rated Case-of-the-Unexplained troubleshooting presentations and other webcasts
- Read Mark's Blog which highlight use of the tools to solve real problems
- Check out the Sysinternals Learning Resources page
- Post your questions in the Sysinternals Forum

Sysinternals Live

Sysinternals Live is a service that enables you to execute Sysinternals tools directly from the Web without hunting for and manually downloading them. Simply enter a tool's Sysinternals Live path into Windows Explorer or a command prompt as live.sysinternals.com/<toolname> or \\live.sysinternals.com\tools\<toolname>.

You can view the entire Sysinternals Live tools directory in a browser at https://live.sysinternals.com/.

What's New

What's New (December 20, 2019)

- Scheduled livesite maintenance

What's New (December 11, 2019)

- Sysmon v10.42
  This update to Sysmon addresses a number of memory leaks, introduces the "Excludes Any" and "Excludes All" filtering conditions and resolves a number of bugs.
- Zoomit v4.52
  This update to Zoomit resolves a number of dual-monitor related issues.
- Whois v1.21
  This refresh of Whois contains various bug fixes.

What's New (September 16, 2019)

- Sysmon v10.41
  Resolves a config parsing issue with 10.4.

What's New (September 05, 2019)

- Sysmon v10.4
  This major update to Sysmon, a security event monitoring service, adds nested rule support to rule groups and "contains any" and "contains all" rule conditions for more flexible filtering, as well as several bug fixes.
- Process Explorer v16.30
  This update to Process Explorer adds a Shared Commit column to the process view, fixes a bug that caused

it to terminate when it is configured to run at logon and the system went to battery, and fixes bugs that prevented the system CPU graph from correctly showing multiple sockets.

What's New (June 20, 2019)

- SHA1 deprecation

What's New (June 11, 2019)

- Sysmon v10.0
  This release of Sysmon adds DNS query logging, reports OriginalFileName in process create and load image events, adds ImageName to named pipe events, logs pico process creates and terminates, and fixes several bugs.
- Autoruns v13.95
  This Autoruns updates adds support for redirected user Shell folders.

What's New (February 18, 2019)

- Sysmon v9.0
  Sysmon v9.0 introduces rule groups that enable the specification of AND or OR matching logic across a set of rules. It also fixes a memory leak in signature verification.

What's New (December 18, 2018)

- Sysmon v8.04
  This release reverted the filtering change made in 8.02 as this broke a number of configuration files. We are planning to revisit and enhance the filtering in the new year. It also fixed a BSOD in legacy named pipe filter used on Windows 7 and earlier, and a kernel memory leak that occurred when the configuration is reloaded.

What's New (October 17, 2018)

- Sigcheck v2.7
  Windows WinVerifyTrust function reports signed MSI files that have malware appended to them as signed, so Sigcheck now indicates when appended conent is present.

What's New (September 17, 2018)

- TLS 1.1 deprecation

What's New (July 5, 2018)

- Sysmon v8.0
  Sysmon now includes the ability to tag rules so that event log entries include the rule tag that generated them, as well as several bug fixes.
- Autoruns v13.90
  Autoruns now includes Runonce*\Depend entries, adds GPO logon and logoff locations, and fixes a bug in WMI path parsing.

What's New (February 13, 2018)

- Autoruns v13.82
  This Autoruns release shows Onenote addins and fixes several bugs.
- Process Monitor v3.50
  Process Monitor now includes a /runtime switch to control headless capture duration, correctly shows picoprocesses, displays details for file system APIs introduced in Windows 10, and includes numerous minor improvements and bug fixes.

What's New (January 2, 2018)

- Sysmon v7.0
  Sysmon now logs file version information, and the option to dump the configuration schema adds the ability to dump an older schema or dump all historical schemas.

What's New (November 19, 2017)

- Sysmon v6.20
  This Sysmon release adds the ability to change the Sysmon service and driver names to foil malware that use them to detect its presence.

- Whois v1.20
  Whois, a command-line utility that reports domain registration information for the specified domain, works with new whois registry server redirects.

What's New (September 11, 2017)

- Sysmon v6.10
  This update to Sysmon, a background monitor that records activity to the event log for use in security incident detection and forensics, adds monitoring of WMI filters and consumers, an autostart mechanism commonly used by malware, and fixes a bug in image load filtering.

- Process Monitor v3.40
  Process Monitor, a file system registry, process and network real-time monitor, now includes a /runtime switch for terminating monitoring after a specified amount of time, when in hexadecimal mode shows process tree process IDs in hexadecimal, and fixes a bug in automated boot log conversion.

- Autoruns v13.80
  This release of Autoruns, a utility for viewing and managing autostart execution points (ASEPs), adds additional autostart entry points, has asynchronous file saving, fixes a bug parsing 32-bit paths on 64-bit Windows, shows the display name for drivers and services, and fixes a bug in offline Virus Total scanning.

What's New (May 16, 2017)

- ProcDump v9.0
  This major update to ProcDump, a utility that enables process dump capture based on a variety of triggers, introduces the ability to take capture multiple dumps sizes. This is particularly useful when capturing crash dumps of applications susceptible to termination due to unresponsiveness (e.g. IIS Ping killing w3wp.exe). This release also adds support for an associated Kernel Dump of the process that includes the kernel stacks of the process.

What's New (February 17, 2017)

- Sysmon v6
  This release of Sysmon, a background monitor that records activity to the event log for use in security incident detection and forensics, introduces an option that displays event schema, adds an event for Sysmon configuration changes, interprets and displays registry paths in their common format, and adds named pipe create and connection events (thanks to Giulia Biagini for the contribution). Check out the related presentation from Mark's RSA Conference, "How to Go From Responding to Hunting with Sysinternals Sysmon."
- Autoruns v13.7
  Autoruns, an autostart entry point management utility, now reports print providers, registrations in the WMI\Default namespace, fixes a KnownDLLs enumeration bug, and has improved toolbar usability on high-DPI displays.
- AccessChk v6.1
  This update to AccessChk, a command-line utility that shows effective and actual permissions for file, registry, service, process object manager, and event logs, now reports Windows 10 process trust access control entries and token security attributes.

Sysinternals Learning Resources

3 minutes to read • Edit Online

Books

Windows Internals Book

The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.

Troubleshooting with the Windows Sysinternals Tools

The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Articles

- Inside the Windows Vista Kernel: Part 1
- Inside the Windows Vista Kernel: Part 2
- Inside the Windows Vista Kernel: Part 3
- Inside Windows Vista User Account Control
- Inside Windows Server 2008 Kernel Changes

Videos and Webcasts

Defrag Tools Shows

Episodes 1 – 12 of the *Defrag Tools* shows focus on Sysinternals tools. Each episode covers a specific tool used on the tech support show Defrag, covering when and why to use the tools, and providing tips on how to get the most out of them:

- Defrag Tools: #1 - Building your USB thumbdrive
- Defrag Tools: #2 - Process Explorer
- Defrag Tools: #3 - Process Monitor
- Defrag Tools: #4 - Process Monitor - Examples
- Defrag Tools: #5 - Autoruns and MSConfig
- Defrag Tools: #6 - RAMMap
- Defrag Tools: #7 - VMMap
- Defrag Tools: #8 - Mark Russinovich
- Defrag Tools: #9 - ProcDump
- Defrag Tools: #10 - ProcDump - Triggers
- Defrag Tools: #11 - ProcDump - Windows 8 & Process Monitor
- Defrag Tools: #12 - TaskMgr and ResMon

Mark's Webcasts

Two dozen of Mark's top-rated presentations on Sysinternals, Windows internals, and Windows Azure are available for on-demand viewing. Get tips and techniques on using the Sysinternals tools to troubleshoot directly from their author.

TWC: Sysinternals Primer: TechEd 2014 Edition

The latest edition of the popular Sysinternals Primer series with Aaron Margosis, Mark Russinovich's co-author of The Windows Sysinternals Administrator's Reference. The Sysinternals utilities are vital tools for any computer

professional on the Windows platform. Mark Russinovich's popular “Case Of The Unexplained” demonstrates some of their capabilities in advanced troubleshooting scenarios. This complementary tutorial series focuses primarily on the utilities themselves, deep-diving into as many features as time allows. Expect to see some advanced analysis, such as manipulating Procmon results with Windows PowerShell, and interesting/useful new features.

Sysinternals Primer: Autoruns, Disk2Vhd, ProcDump, BgInfo and AccessChk

The Sysinternals utilities are vital tools for any computer professional on the Windows platform. Mark Russinovich's popular "Case Of The Unexplained" demonstrates some of their capabilities in advanced troubleshooting scenarios. This complementary tutorial session focuses primarily on the utilities themselves, giving you tips and techniques for using their full functionality for troubleshooting and systems management. This session follows the same format as last year’s highly-rated delivery, and covers a different set of the most useful Sysinternals tools.

Unintended Consequences of Security Lockdowns (uses Sysinternals utilities a lot)

Security-conscious organizations often lock down their systems based on prescriptive guidance from Microsoft, US Federal government agencies or other security organizations. Sometimes these settings can lead to unpleasant surprises and unexpected side effects. This session describes and demonstrates some of the common issues that can arise, and whether and how those settings actually help or hurt. Is there benefit to not granting Administrators the “Debug” privilege? Does “Hide mechanisms to remove zone information” break anything? Is the “Require trusted path for credential entry” setting worth the inconvenience? Come see!

Windows Sysinternals Primer: Process Explorer, Process Monitor and More

The Sysinternals utilities are vital tools for any computer professional on the Windows platform. Mark Russinovich's popular "Case Of The Unexplained" demonstrates some of their capabilities in advanced troubleshooting scenarios. This complementary tutorial session by Aaron Margosis and Tim Reckmeyer focuses primarily on the utilities, deep-diving into as many features as time will allow. Learn tips and tricks that will make you more effective with the Sysinternals utilities.

Mark's Webcasts

8 minutes to read • Edit Online

Watch free on-demand recordings of Mark's top-rated presentations from TechEd, BUILD and other conferences on Azure, security, Windows troubleshooting, malware hunting. If you have a question about a topic in any of these webcasts, please visit the Sysinternals Forum for answers and help from other users and our moderators.

Case of the Unexplained

- The Case of the Unexplained 2015
- The Case of the Unexplained 2014
- The Case of the Unexplained 2013
- The Case of the Unexplained 2012
- The Case of the Unexplained 2011
- The Case of the Unexplained 2010
- Mark's "The Case of..." blog posts come alive in these recorded webcasts of his #1-rated TechEd sessions. Learn how to troubleshoot the toughest Windows and application problems by watching Mark use Sysinternals and other advanced tools to solve real-world examples. Be sure to check out all webcasts since they include totally different troubleshooting examples and demonstrate different techniques.

Microsoft Azure

- The Next Generation of Azure Compute Platform
  Learn about ways to integrate with Azure Resource Manager (ARM) to enable role-based access control (RBAC), tagging,and template-based deployments,and how Windows containers with Docker compatibility make your code deploy instantly and work consistently in any environment. Also learn how Service Fabric, Microsoft's hyper-scale micro-service PaaS that powers everything from Azure DB to Cortana, brings applications state-of-the art high-density, high availability and stateful computing capabilities.
- Mark Russinovich and Mark Minasi on Cloud Computing
  Join Mark Russinovich and Mark Minasi for a lively discussion as they share their views on the cloud computing disruption and what it means for IT pros and developers. Mark Russinovich brings his perspective from leading Microsoft Azure architecture and Mark Minasi brings his IT expertise and view from outside.
- Public Cloud Security: Surviving in a Hostile Multi-Tenant Environment
  The rise of public cloud computing has brought with it a new set of security considerations that are not widely understood. With a unique perspective from working on the security systems of a public cloud, Mark describes public cloud service provider and cloud customer threats, including malicious insiders, shared technology, data breaches, and data loss. For each, he assesses the risks and explores the value of mitigations like encryption-at-rest, encryption-in-flight, and other security best practices, separating hype from reality so that you can make educated decisions as your organization moves to the cloud.
- Mark Russinovich and Mark Minasi on Cloud Computing
  Join Mark Russinovich and Mark Minasi for a lively discussion as they share their views on the cloud computing disruption and what it means for IT pros and developers. Mark Russinovich brings his perspective from leading Microsoft Azure architecture and Mark Minasi brings his IT expertise and view from outside. The economics of public cloud, future of PaaS and IaaS, how enterprises will bridge their on-premises environments with the cloud, how you should look at security in the public cloud, and what skills are important for IT pros and developers are just some of the areas they explore together.
- Infrastructure Services on Microsoft Azure: Virtual Machines and Virtual Networks
  This session gives an overview of the new Windows Azure infrastructure services (IaaS), including support for

Windows Server and Linux persistent virtual machines, new networking capabilities for hybrid applications and on-premises/cloud connectivity, and support for applications that consist of PaaS and IaaS roles. Mark explains how IaaS fits into Windows Azure to extend existing server applications to cloud and shows demonstrations of IaaS VM deployment and complex multi-VM applications.

- Microsoft Azure Internals
  Mark Russinovich goes under the hood of the Microsoft datacenter operating system. Intended for developers who have already gotten their hands dirty with Windows Azure and understand its basic concepts, this session gives an inside look at the architectural design of the Windows Azure compute platform. Learn about Microsoft's datacenter architecture, what goes on behind the scenes when you deploy and update a Windows Azure app and how it monitors and responds to the health of machines, its own components, and the apps it hosts.
- Introduction to Microsoft Azure: The Cloud Operating System
  Join Mark Russinovich for an overview of Microsoft's new cloud OS. Assuming no prior knowledge of Windows Azure, this session will start by explaining the Windows Azure Platform-as-a-Service (PaaS) app philosophy and how it differs from that of traditional server apps. Then, demonstrating key concepts with a real Windows Azure service built and deployed to the cloud, we'll describe the Windows Azure service model, including concepts like update and fault domains. The session will then conclude by discussing the different service update options and detail the recovery steps Windows Azure follows when it detects that a service or a hardware device has failed.
- Inside Microsoft Azure: The Cloud Operating System
  Mark Russinovich goes under the hood of Microsoft's new cloud OS. Intended for developers who have already gotten their hands dirty with Windows Azure and understand its basic concepts, this session gives an inside look at the architectural design of Windows Azure's compute platform. You'll learn about Microsoft's datacenter architecture, what goes on behind the scenes when you deploy and update a Windows Azure app and how it monitors and responds to the health of machines, its own components and the apps it hosts.
- Channel9: MarkRussinovich: Microsoft Azure, Cloud Operating Systems and Platformas a Service
  Mark talks about what he's working on in the Windows Azure team, why the world is moving to the cloud, and what Platform-as-a-Service (PaaS) means and how Windows Azure delivers PaaS.

Windows Internals

- Tech-Ed North America 2011: Mysteries of Windows Memory Management Revealed, Part1
  Tech-Ed North America 2011: Mysteries of Windows Memory Management Revealed, Part2
  If you want to know the difference between System Committed memory and Process Committed memory, wondered what all those memory numbers shown by Task Manager really mean, or want to gain insight into the memory-related impact of a process, then this talk is for you. Watch Mark in this on-demand webcast from North America 2011.
- Pushing the Limits of Windows
  Watch as Mark explains Windows limits related to object handles, virtual memory and physical memory. Along the way he explains where the limits come from and how to monitor your applications so that you're warned when they approach the limits and so that you can size your systems to accommodate their resource requirements.
- Inside Windows Server 2008R2 Virtualization and VHD Improvements
  Mark takes you inside new Windows virtualization and VHD features, including live VM migration, core parking and timer coalescing, hypervisor power management support,and new hardware-assisted guest memory management. He delivers the entire presentation from a Windows installation that was booted from VHD to show you how Windows implements a native VHD stack and how the boot architecture has changed to accommodate booting from VHD images.
- Channel9: Mark Russinovich goes Inside Windows 7
  Mark talks about kernel changes in Windows 7 and Windows Server 2008R2, including the removal of the scheduler's dispatcher lock, support for up to 256 CPUs, boot from VHD, MinWin, core parking for power

savings and more.

- Channel9: Mark Russinovich: Inside Windows 7 Redux
  In a follow-on to the previous Inside Windows 7 discussion, Mark digs into the insides of Windows 7, way deep down in the system (the cumulative effects of which help to make Windows 7 Microsoft's most reliable, scalable and efficient general purpose operating system to date).
- Channel9: Mark talks about working at Microsoft, Windows Server 2008's kernel, MinWin vs ServerCore and Hyper-V
  Channel 9 chats with Technical Fellow and Sysinternals founder Mark Russinovich to dig a bit into what's new in the Windows Server 2008 kernel. Of course, we talk about many things including HyperV, application virtualization, kernel architecture, and more....

Security

- TWC: Pass-the-Hash: How Attackers Spread and How to Stop Them
  Pass-the-hash transforms the breach of one machine into total compromise of infrastructure. The publication of attacks, and lack of tools to respond, have forced enterprises to rely on onerous and ineffective techniques. In this session, we deconstruct the PtH threat, show how the attack is performed, and how it can be addressed using new features and functionality recently introduced in Windows.
- TWC: Malware Hunting with Mark Russinovich and the Sysinternals Tools
  Mark provides an overview of several Sysinternals tools, including Process Monitor, Process Explorer, and Autoruns, focusing on the features useful for malware analysis and removal. These utilities enable deep inspection and control of processes, file system and registry activity, and autostart execution points. He demonstrates their malware-hunting capabilities by presenting several current, real-world malware samples and using the tools to identify and clean malware.
- License to Kill: Malware Hunting with the Sysinternals tools
  This session provides an overview of several Sysinternals tools, including Process Monitor, Process Explorer, and Autoruns, focusing on the features useful for malware analysis and removal. These utilities enable deep inspection and control of processes, file system and registry activity, and autostart execution points. You will see demos for their malware-hunting capabilities through several real-world cases that used the tools to identify and clean malware,and conclude by performing a live analysis of a Stuxnet infection's system impact.
- Zero Day: A Non-Fiction View
  Mark makes the case for how his hit cyberthriller, ZeroDay, is likely to be realized in non-fiction form in this 20-minute short version of his well-popular RSA Conference session.
- Zero Day Malware Cleaning with the Sysinternals tools
  Slides from Mark's highly-rated Blackhat US 2011 presentation how to use the Sysinternals tools to hunt down and eliminate malware.
- Channel9: Mark Talks about Windows Security and Core Architecture
  Check out Mark's Channel 9 interview where he talks about how he got started with Windows internals, new security features in Windows Vista, User Account Control,and what he's doing at Microsoft.

Defrag Tools

- Defrag Tools Shows
  Episodes 1 – 12 of the *Defrag Tools* shows focus on Sysinternals tools. Each episode covers a specific tool used on the tech support show Defrag, covering when and why to use the tools, and providing tips on how to get the most out of them:
  - Defrag Tools: #1 - Building your USB thumbdrive
  - Defrag Tools: #2 - Process Explorer
  - Defrag Tools: #3 - Process Monitor
  - Defrag Tools: #4 - Process Monitor - Examples
  - Defrag Tools: #5 - Autoruns and MSConfig

- Defrag Tools: #6 - RAMMap
- Defrag Tools: #7 - VMMap
- Defrag Tools: #8 - Mark Russinovich
- Defrag Tools: #9 - ProcDump
- Defrag Tools: #10 - ProcDump - Triggers
- Defrag Tools: #11 - ProcDump - Windows 8 & Process Monitor
- Defrag Tools: #12 - TaskMgr and ResMon

Windows Internals Book

3 minutes to read • Edit Online

Windows Internals 7th edition (Part 1) covers the architecture and core internals of Windows 10 and Windows Server 2016. This book helps you:

- Understand the Windows system architecture and its general components
- Explore internal data structures using tools like the kernel debugger
- Understand how Windows uses processes for management and isolation
- Understand and view thread scheduling and how CPU resources are managed
- Dig into the Windows security model including recent advances in security mitigations
- Understand how Windows manages virtual and physical memory
- Understand how the I/O system manages physical devices and device drivers

The 7th edition was written by Pavel Yosifovich, Alex Ionescu, Mark Russinovich and David Solomon. New material has been added since the 6th edition (which covered Windows 7 and Windows Server 2008 R2). Since the 7th edition's part 2 is not yet available, the Windows Internals 6th edition (written by Mark Russinovich, David Solomon and Alex Ionescu) is an invaluable resource on missing topics from the first part of the 7th edition. These include system mechanisms, management mechanisms, networking, file systems, cache management and troubleshooting system crashes.

Table of contents of the 7th edition, part 1:

- Chapter 1: Concepts and Tools
- Chapter 2: System Architecture
- Chapter 3: Processes and Jobs
- Chapter 4: Threads
- Chapter 5: Memory Management
- Chapter 6: I/O System
- Chapter 7: Security

The book is available for purchase on the Microsoft Press site (7th edition Part 1; 6th Edition Part 1; 6th Edition Part 2).

History of the Book

This is the seventh edition of a book that was originally called Inside Windows NT (Microsoft Press, 1992), written by Helen Custer (prior to the initial release of Microsoft Windows NT 3.1). Inside Windows NT was the first book ever published about Windows NT and provided key insights into the architecture and design of the system. Inside Windows NT, Second Edition (Microsoft Press, 1998) was written by David Solomon. It updated the original book to cover Windows NT 4.0 and had a greatly increased level of technical depth. Inside Windows 2000, Third Edition (Microsoft Press, 2000) was authored by David Solomon and Mark Russinovich. It added many new topics, such as startup and shutdown, service internals, registry internals, file-system drivers, and networking. It also covered kernel changes in Windows 2000, such as the Windows Driver Model (WDM), Plug and Play, power management, Windows Management Instrumentation (WMI), encryption, the job object, and Terminal Services. Windows Internals, Fourth Edition was the Windows XP and Windows Server 2003 update and added more content focused on helping IT professionals make use of their knowledge of Windows internals, such as using key tools from Windows Sysinternals and analyzing crash dumps.

Windows Internals, Fifth Edition was the update for Windows Vista and Windows Server 2008. It saw Mark Russinovich move on to a full-time job at Microsoft (where he is now the Azure CTO) and the addition of a new

co-author, Alex Ionescu. New content included the image loader, user-mode debugging facility, Advanced Local Procedure Call (ALPC), and Hyper-V. The next release, Windows Internals, Sixth Edition, was fully updated to address the many kernel changes in Windows 7 and Windows Server 2008 R2, with many new hands-on experiments to reflect changes in the tools as well.

Seventh Edition Changes

Since this series' last update, Windows has gone through several releases, coming up to Windows 10 and Windows Server 2016. Windows 10 itself, being the current going-forward name for Windows, has had several releases since its initial Release-to-Manufacturing, or RTM, each labeled with a 4-digit version number indicating year and month of release, such as Windows 10, version 1703 that was completed in March 2017. The above implies that Windows has gone through at least 6 versions since Windows 7. Starting with Windows 8, Microsoft began a process of OS convergence, which is beneficial from a development perspective as well as for the Windows engineering team itself. Windows 8 and Windows Phone 8 had converged kernels, with modern app convergence arriving in Windows 8.1 and Windows Phone 8.1. The convergence story was complete with Windows 10, which runs on desktops/laptops, servers, XBOX One, phones (Windows Mobile 10), HoloLens, and various Internet of Things (IoT) devices. With this grand unification completed, the time was right for a new edition of the series, which could now finally catch up with almost half a decade of changes, in what will now be a more stabilized kernel architecture going forward. As such, this latest book covers aspects of Windows from Windows 8 to Windows 10, version 1703. Additionally, this edition welcomes Pavel Yosifovich as its new co-author.

Book tools

Several tools have been specifically written for the book, and they are available with full source code at https://github.com/zodiacon/WindowsInternals.

Troubleshooting with the Windows Sysinternals Tools

2 minutes to read • Edit Online

An update to Windows Sysinternals Administrator's Reference
By Mark Russinovich and Aaron Margosis
Troubleshooting with the Windows Sysinternals Tools is the official book on the Sysinternals tools, written by tool author and Sysinternals cofounder Mark Russinovich, and Windows expert Aaron Margosis. The book covers all 65+ tools in detail, with full chapters on the major tools like Process Explorer, Process Monitor, and Autoruns. In addition to tips and tricks in the tool chapters, it includes 45 "Case of the Unexplained..." examples of the tools used by users to solve real-world problems. Buy the book today and take your Windows troubleshooting and systems management skills to the next level.

Ordering the Book

You can purchase the book from these online retailers:

- Microsoft Press Store
- Amazon
- Barnes & Noble
- Independent booksellers – Shop local

You can also read it online through Safari.

Description of the Book

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 expert Windows consultant 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 runs 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

Sample Chapter

You can read samples from the book at this link on Amazon.com.

Table of Contents

- Part I: Getting started
  - Chapter 1 Getting started with the Sysinternals utilities
  - Chapter 2 Windows core concepts
- Part II: Usage guide
  - Chapter 3 Process Explorer
  - Chapter 4 Autoruns
  - Chapter 5 Process Monitor
  - Chapter 6 ProcDump
  - Chapter 7 PsTools
  - Chapter 8 Process and diagnostic utilities
  - Chapter 9 Security utilities
  - Chapter 10 Active Directory utilities
  - Chapter 11 Desktop utilities
  - Chapter 12 File utilities
  - Chapter 13 Disk utilities
  - Chapter 14 Network and communication utilities
  - Chapter 15 System information utilities
  - Chapter 16 Miscellaneous utilities
- Part III: Troubleshooting — "The Case of the Unexplained..."
  - Chapter 17 Error messages
  - Chapter 18 Crashes
  - Chapter 19 Hangs and sluggish performance
  - Chapter 20 Malware
  - Chapter 21 Understanding system behavior
  - Chapter 22 Developer troubleshooting

Errata

See the Errata & Updates tab on the Microsoft Press web site

Inside Native Applications

3 minutes to read • Edit Online

Mark Russinovich Published: November 1, 2006

Introduction

If you have some familiarity with NT's architecture you are probably aware that the API that Win32 applications use isn't the "real" NT API. NT's operating environments, which include POSIX, OS/2 and Win32, talk to their client applications via their own APIs, but talk to NT using the NT "native" API. The native API is mostly undocumented, with only about 25 of its 250 functions described in the Windows NT Device Driver Kit.

What most people don't know, however, is that "native" applications exist on NT that are not clients of any of the operating environments. These programs speak the native NT API and can't use operating environment APIs like Win32. Why would such programs be needed" Any program that must run before the Win32 subsystem is started (around the time the logon box appears) must be a native application. The most visible example of a native application is the "autochk" program that runs chkdsk during the initialization Blue Screen (its the program that prints the "."'s on the screen). Naturally, the Win32 operating environment server, CSRSS.EXE (Client-Server Runtime Subsystem), must also be a native application.

In this article I'm going to describe how native applications are built and how they work.

How Does Autochk Get Executed

Autochk runs in between the time that NT's boot and system start drivers are loaded, and when paging is turned on. At this point in the boot sequence Session Manager (smss.exe) is getting NT's user-mode environment off-the-ground and no other programs are active. The **HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute** value, a MULTI_SZ, contains the names and arguments of programs that are executed by Session Manager, and is where Autochk is specified. Here is what you'll typically find if you look at this value, where "Autochk" is passed "*" as an argument:

```
Autocheck Autochk *
```

Session Manager looks in the <winnt>\system32 directory for the executables listed in this value. When Autochk runs there are no files open so *Autochk* can open any volume in raw-mode, including the boot drive, and manipulate its on-disk data structures. This wouldn't be possible at any later point.

Building Native Applications

Microsoft doesn't document it, but the NT DDK Build utility knows how to make native applications (and its probably used to compile *Autochk*). You specify information in a SOURCES file that defines the application, the same as would be done for device drivers. However, instead of indicating to Build that you want a driver, you tell it you want a native applicationin the SOURCES file like this:

```
TARGETTYPE=PROGRAM
```

The *Build* utility uses a standard makefile to guide it, \ddk\inc\makefile.def, which looks for a run-time library named nt.lib when compiling native applications. Unfortunately, Microsoft doesn't ship this file with the DDK (its included in the Server 2003 DDK, but I suspect that if you link with that version your native application won't run

on XP or Windows 2000). However, you can work around this problem by including a line in makefile.def that overrides the selection of nt.lib by specifying Visual C++'s runtime library, msvcrt.lib

If you run *Build* under the DDK's "Checked Build" environment it will produce a native application with full debug information under %BASEDIR%\lib%CPU%\Checked (e.g. c:\ddk\lib\i386\checked\native.exe), and if you invoke it in the "Free Build" environment a release version of the program will end up in %BASEDIR%\lib%CPU%\Free. These are the same places device driver images are placed by Build.

Native applications have ".exe" file extensions but you cannot run them like Win32 .exe's. If you try you'll get the message:

The application cannot be run in Windows NT mode.

Inside a Native Application

Instead of **winmain** or **main**, the entry point for native applications is **NtProcessStartup**. Also unlike the other Win32 entry points, native applications must reach into a data structure passed as its sole parameter to locate command-line arguments.

The majority of a native application's runtime environment is provided by NTDLL.DLL, NT's native API export library. Native applications must create their own heap from which to allocate storage by using **RtlCreateHeap**, a NTDLL function. Memory is allocated from a heap with **RtlAllocateHeap** and freed with **RtlFreeHeap**. If a native application wishes to print something to the screen it must use the function **NtDisplayString**, which will output to the initialization Blue Screen.

Native applications don't simply return from their startup function like Win32 programs, since there is no runtime code to return to. Instead, they must terminate themselves by calling **NtProcessTerminate**.

The NTDLL runtime consists of hundreds of functions that allow native applications to perform file I/O, interact with device drivers, and perform interprocess communications. Unfortunately, as I stated earlier, the vast majority of these functions are undocumented.

Sysinternals Utilities Index

7 minutes to read • Edit Online

Sysinternals Suite

The entire set of Sysinternals Utilities rolled up into a single download.

Sysinternals Suite for Nano Server

Sysinternals Utilities for Nano Server in a single download.

AccessChk

v6.20 (November 19, 2017)

AccessChk is a command-line tool for viewing the effective permissions on files, registry keys, services, processes, kernel objects, and more.

AccessEnum

v1.32 (November 1, 2006)

This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

AdExplorer

v1.44 (November 15, 2012)

Active Directory Explorer is an advanced Active Directory (AD) viewer and editor.

AdInsight

v1.2 (October 26, 2015)

An LDAP (Light-weight Directory Access Protocol) real-time monitoring tool aimed at troubleshooting Active Directory client applications.

AdRestore

v1.1 (November 1, 2006)

Undelete Server 2003 Active Directory objects.

Autologon

v3.10 (August 29, 2016)

Bypass password screen during logon.

Autoruns

v13.95 (June 11, 2019)

See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

BgInfo

v4.26 (October 19, 2018)

This fully-configurable program automatically generates desktop backgrounds that include important information about the system including IP addresses, computer name, network adapters, and more.

BlueScreen

v3.2 (November 1, 2006)

This screen saver not only accurately simulates Blue Screens, but simulated reboots as well (complete with CHKDSK), and works on Windows NT 4, Windows 2000, Windows XP, Server 2003 and Windows 95 and 98.

CacheSet

v1.0 (November 1, 2006)

CacheSet is a program that allows you to control the Cache Manager's working set size using functions provided by NT. It's compatible with all versions of NT.

ClockRes

v2.1 (July 4, 2016)

View the resolution of the system clock, which is also the maximum timer resolution.

Contig

v1.8 (July 4, 2016)

Wish you could quickly defragment your frequently used files? Use Contig to optimize individual files, or to create new files that are contiguous.

Coreinfo

v3.31 (August 18, 2014)

Coreinfo is a new command-line utility that shows you the mapping between logical processors and the physical processor, NUMA node, and socket on which they reside, as well as the cache's assigned to each logical processor.

Ctrl2cap

v2.0 (November 1, 2006)

This is a kernel-mode driver that demonstrates keyboard input filtering just above the keyboard class driver in order to turn caps-locks into control keys. Filtering at this level allows conversion and hiding of keys before NT even "sees" them. Ctrl2cap also shows how to use NtDisplayString() to print messages to the initialization blue-screen.

DebugView

v4.81 (December 4, 2012)

Another first from Sysinternals: This program intercepts calls made to DbgPrint by device drivers and OutputDebugString made by Win32 programs. It allows for viewing and recording of debug session output on your local machine or across the Internet without an active debugger.

Desktops

v2.0 (October 17, 2012)

This new utility enables you to create up to four virtual desktops and to use a tray interface or hotkeys to preview what's on each desktop and easily switch between them.

Disk2vhd

v2.01 (January 21, 2014)

Disk2vhd simplifies the migration of physical systems into virtual machines (p2v.md).

DiskExt

v1.2 (July 4, 2016)

Display volume disk-mappings.

Diskmon

v2.01 (November 1, 2006)

This utility captures all hard disk activity or acts like a software disk activity light in your system tray.

DiskView

v2.4 (March 25, 2010.md)

Graphical disk sector utility.

Disk Usage (DU.md)

v1.61 (February 13, 2018)

View disk usage by directory.

EFSDump

v1.02 (November 1, 2006)

View information for encrypted files.

FindLinks
v1.1 (July 4, 2016)
FindLinks reports the file index and any hard links (alternate file paths on the same volume.md) that exist for the specified file. A file's data remains allocated so long as at it has at least one file name referencing it.

Handle
v4.11 (December 12, 2017)
This handy command-line utility will show you what files are open by which processes, and much more.

Hex2dec
v1.1 (July 4, 2016)
Convert hex numbers to decimal and vice versa.

Junction
v1.07 (July 4, 2016)
Create Win2K NTFS symbolic links.

LDMDump
v1.02 (November 1, 2006)
Dump the contents of the Logical Disk Manager's on-disk database, which describes the partitioning of Windows 2000 Dynamic disks.

ListDLLs
v3.2 (July 4, 2016)
List all the DLLs that are currently loaded, including where they are loaded and their version numbers.

LiveKd
v5.62 (May 16, 2017)
Use Microsoft kernel debuggers to examine a live system.

LoadOrder
v1.01 (July 4, 2016)
See the order in which devices are loaded on your WinNT/2K system.

LogonSessions
v1.4 (July 4, 2016)
List the active logon sessions on a system.

MoveFile
v1.01 (January 24, 2013)
Allows you to schedule move and delete commands for the next reboot.

NotMyFault
v4.01 (November 18, 2016)
Notmyfault is a tool that you can use to crash, hang, and cause kernel memory leaks on your Windows system.

NTFSInfo
v1.2 (July 4, 2016)
Use NTFSInfo to see detailed information about NTFS volumes, including the size and location of the Master File Table (MFT) and MFT-zone, as well as the sizes of the NTFS meta-data files.

PendMoves
v1.2 (February 5, 2013)
Enumerate the list of file rename and delete commands that will be executed the next boot.

PipeList

v1.02 (July 4, 2016)
Displays the named pipes on your system, including the number of maximum instances and active instances for each pipe.

PortMon
v3.03 (January 12, 2012)
Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLs and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.

ProcDump
v9.0 (May 16, 2017)
This command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.

Process Explorer
v16.21 (May 16, 2017)
Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process Monitor
v3.50 (February 13, 2018)
Monitor file system, Registry, process, thread and DLL activity in real-time.

PsExec
v2.2 (June 29, 2016)
Execute processes on remote systems.

PsFile
v1.03 (June 29, 2016)
See what files are opened remotely.

PsGetSid
v1.45 (June 29, 2016)
Displays the SID of a computer or a user.

PsInfo
v1.78 (June 29, 2016)
Obtain information about a system.

PsKill
v1.16 (June 29, 2016)
Terminate local or remote processes.

PsPing
v2.01 (January 29, 2014)
Measure network performance.

PsList
v1.4 (June 29, 2016)
Show information about processes and threads.

PsLoggedOn
v1.35 (June 29, 2016)
Show users logged on to a system.

PsLogList

v2.8 (June 29, 2016)
Dump event log records.

PsPasswd
v1.24 (June 29, 2016)
Changes account passwords.

PsService
v2.25 (June 29, 2016)
View and control services.

PsShutdown
v2.52 (December 4, 2006)
Shuts down and optionally reboots a computer.

PsSuspend
v1.07 (June 29, 2016)
Suspend and resume processes.

PsTools
v2.45 (July 4, 2016)
The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

RAMMap
v1.51 (May 31, 2018)
An advanced physical memory usage analysis utility that presents usage information in different ways on its several different tabs.

RegDelNull
v1.11 (July 4, 2016)
Scan for and delete Registry keys that contain embedded null-characters that are otherwise undeleteable by standard Registry-editing tools.

Registry Usage (RU.md)
v1.2 (July 4, 2016)
View the registry space usage for the specified registry key.

RegJump
v1.1 (April 20, 2015)
Jump to the registry path you specify in Regedit.

SDelete
v2.01 (February 13, 2018)
Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

ShareEnum
v1.6 (November 1, 2006)
Scan file shares on your network and view their security settings to close security holes.

ShellRunas
v1.01 (February 28, 2008)
Launch programs as a different user via a convenient shell context-menu entry.

Sigcheck
v2.70 (October 19, 2018)
Dump file version information and verify that images on your system are digitally signed.

Streams
v1.6 (July 4, 2016)
Reveal NTFS alternate streams.

Strings
v2.52 (June 20, 2013)
Search for ANSI and UNICODE strings in binary images.

Sync
v2.2 (July 4, 2016)
Flush cached data to disk.

Sysmon
v10.0 (June 11, 2019)
Monitors and reports key system activity via the Windows event log.

TCPView
v3.05 (July 25, 2011)
Active socket command-line viewer.

VMMap
v3.26 (June 11, 2019)
VMMap is a process virtual and physical memory analysis utility.

VolumeId
v2.1 (July 4, 2016)
Set Volume ID of FAT or NTFS drives.

Whois
v1.20 (November 19, 2017)
See who owns an Internet address.

WinObj
v2.22 (February 14, 2011)
The ultimate Object Manager namespace viewer is here.

ZoomIt
v4.5 (June 20, 2013)
Presentation utility for zooming and drawing on the screen.

Sysinternals File and Disk Utilities

2 minutes to read • Edit Online

AccessChk

This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services.

AccessEnum

This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

CacheSet

CacheSet is a program that allows you to control the Cache Manager's working set size using functions provided by NT. It's compatible with all versions of NT.

Contig

Wish you could quickly defragment your frequently used files? Use Contig to optimize individual files, or to create new files that are contiguous.

Disk2vhd

Disk2vhd simplifies the migration of physical systems into virtual machines (p2v).

DiskExt

Display volume disk-mappings.

DiskMon

This utility captures all hard disk activity or acts like a software disk activity light in your system tray.

DiskView

Graphical disk sector utility.

Disk Usage (DU)

View disk usage by directory.

EFSDump

View information for encrypted files.

FindLinks

FindLinks reports the file index and any hard links (alternate file paths on the same volume) that exist for the specified file. A file's data remains allocated so long as at it has at least one file name referencing it.

Junction

Create Win2K NTFS symbolic links.

LDMDump

Dump the contents of the Logical Disk Manager"s on-disk database, which describes the partitioning of Windows 2000 Dynamic disks.

MoveFile

Schedule file rename and delete commands for the next reboot. This can be useful for cleaning stubborn or in-use malware files.

NTFSInfo

Use NTFSInfo to see detailed information about NTFS volumes, including the size and location of the Master File Table (MFT) and MFT-zone, as well as the sizes of the NTFS meta-data files.

PageDefrag

Defragment the Windows paging file and Registry hives.

PendMoves

See what files are scheduled for delete or rename the next time the system boots.

Process Monitor

Monitor file system, Registry, process, thread and DLL activity in real-time.

PsFile

See what files are opened remotely.

PsTools

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

SDelete

Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

ShareEnum

Scan file shares on your network and view their security settings to close security holes.

Sigcheck

Dump file version information and verify that images on your system are digitally signed.

Streams

Reveal NTFS alternate streams.

Sync

Flush cached data to disk.

VolumeID

Set Volume ID of FAT or NTFS drives.

AccessChk v6.12

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 19, 2017

Download AccessChk (369 KB)
Run now from Sysinternals Live.

Introduction

As a part of ensuring that they've created a secure environment Windows administrators often need to know what kind of accesses specific users or groups have to resources including files, directories, Registry keys, global objects and Windows services. AccessChk quickly answers these questions with an intuitive interface and output.

Installation

AccessChk is a console program. Copy AccessChk onto your executable path. Typing "accesschk" displays its usage syntax.

Using AccessChk

Usage: accesschk [-s][-e][-u][-r][-w][-n][-v]-[f <account>,...][[-a]|[-k]|[-p [-f] [-t]]|[-h][-o [-t <object type>]][-c]|[-d]] [[-l [-i]]|[username]] <file, directory, registry key, process, service, object>

PARAMETER	DESCRIPTION
-a	Name is a Windows account right. Specify "*" as the name to show all rights assigned to a user. Note that when you specify a specific right, only groups and accounts directly assigned to the right are displayed.
-c	Name is a Windows Service, e.g. ssdpsrv. Specify "*" as the name to show all services and "scmanager" to check the security of the Service Control Manager.
-d	Only process directories or top-level keys
-e	Only show explicitly set-Integrity Levels (Windows Vista and higher only)
-f	If following -p, shows full process token information including groups and privileges. Otherwise is a list of comma-separated accounts to filter from the output.
-h	Name is a file or printer share. Specify '*' as the name to show all shares.
-i	Ignore objects with only inherited ACEs when dumping full access control lists.

PARAMETER	DESCRIPTION
-k	Name is a Registry key, e.g. hklm\software
-l	Show full security descriptor. Add -i to ignore inherited ACEs.
-n	Show only objects that have no access
-o	Name is an object in the Object Manager namespace (default is root). To view the contents of a directory, specify the name with a trailing backslash or add -s. Add -t and an object type (e.g. section) to see only objects of a specific type.
-p	Name is a process name or PID, e.g. cmd.exe (specify "*" as the name to show all processes). Add -f to show full process token information, including groups and privileges. Add -t to show threads.
-q	Omit Banner
-r	Show only objects that have read access
-s	Recurse
-t	Object type filter, e.g. "section"
-u	Suppress errors
-v	Verbose (includes Windows Vista Integrity Level)
-w	Show only objects that have write access

If you specify a user or group name and path, AccessChk will report the effective permissions for that account; otherwise it will show the effective access for accounts referenced in the security descriptor.

By default, the path name is interpreted as a file system path (use the "\pipe\" prefix to specify a named pipe path). For each object, AccessChk prints R if the account has read access, W for write access, and nothing if it has neither. The -v switch has AccessChk dump the specific accesses granted to an account.

Examples

The following command reports the accesses that the Power Users account has to files and directories in \Windows\System32:

accesschk "power users" c:\windows\system32

This command shows which Windows services members of the Users group have write access to:

accesschk users -cw *

To see what Registry keys under HKLM\CurrentUser a specific account has no access to:

accesschk -kns austin\mruss hklm\software

To see the security on the HKLM\Software key:

accesschk -k hklm\software

To see all files under \Users\Mark on Vista that have an explicit integrity level:

accesschk -e -s c:\users\mark

To see all global objects that Everyone can modify:

accesschk -wuo everyone \basednamedobjects

Download AccessChk (369 KB)
Run now from Sysinternals Live.

AccessEnum v1.32

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download AccessEnum (51 KB)
Run now from Sysinternals Live.

Introduction

While the flexible security model employed by Windows NT-based systems allows full control over security and file permissions, managing permissions so that users have appropriate access to files, directories and Registry keys can be difficult. There's no built-in way to quickly view user accesses to a tree of directories or keys. *AccessEnum* gives you a full view of your file system and Registry security settings in seconds, making it the ideal tool for helping you for security holes and lock down permissions where necessary.

How It Works

AccessEnum uses standard Windows security APIs to populate its listview with read, write and deny access information.

Download AccessEnum (51 KB)

Run now from Sysinternals Live.

CacheSet v1.0

3 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download CacheSet (44 KB)
Run now from Sysinternals Live.

Introduction

CacheSet is an applet that allows you to manipulate the working-set parameters of the system file cache. Unlike CacheMan, *CacheSet* runs on all versions of NT and will work without modifications on new Service Pack releases. In addition to providing you the ability to control the minimum and maximum working set sizes, it also allows you to reset the Cache's working set, forcing it to grow as necessary from a minimal starting point. Also unlike CacheMan, changes made with *CacheSet* have an immediate effect on the size of the Cache.

Use *CacheSet* to performance tune the system Cache size in a way not possible without tweaking internal variables the way CacheMan does.

Note: To use *CacheSet* on NT 4.0 Service Pack 4 and later you must have the "Increase Quota" privilege (administrator accounts have this privilege by default). *CacheSet* has been updated to enable this privilege so that it works on SP4.

Installation and Use

After it starts it presents the system file cache's current size (updated twice a second), it's peak size (the largest it's been since the last reboot), and lets you set new minimum and maximum working set sizes.

Setting New Sizes
Simply enter the new minimum and maximum sizes and hit the Apply button. If you get an error, then one of the following conditions holds: you've entered a maximum that is smaller than the minimum, the minimum you've entered is smaller than the minimum system working-set size, or the maximum you've entered is larger than the maximum system working-set sizes. Adjust the values you've entered and try again.

You may notice that the Cache's size changes immediately and then proceeds to shrink or grow quickly. This is because the system automatically trims working sets once a second. The Cache pages that are released are still in memory, but can be relinquished quickly for use by other programs that need more memory. Similarly, the Cache can eaily regain pages as applications access file system data.

Resetting Previous Values
At any time you can restore the Cache's working set values that were active when you last started *CacheSet* by hitting the Reset button.

Clearing the Cache's Working Set
You can force the Cache to release all of it's pages by pressing the Clear button. Note that the Cache can grow again as necessary, and that this is not the same as flushing the Cache - pages that were assigned to it are simply made available to other programs and can be reclaimed by the Cache.

Using the Command-Line Interface

You can enter the minimum and maximum working set sizes on *CacheSet*'s command line. *CacheSet* will apply these new values silently. Thus, you can add *CacheSet* to your Start program group to automatically set the Cache's sizes every time you boot.

Usage: CacheSet [minimum working set] [maximum working set]

How It Works

CacheSet uses a **NtQuerySystemInformation** call to obtain information about the Cache's settings and **NtSetSystemInformation** to set new sizing information. The working-set information for a process serves as guidelines for NT's Memory Manager regarding how many pages of physical memory should be assigned to the application. Because they are guidelines, conditions can result such that the Memory Manager grows a working-set to a size greater than the maximum, or shrinks it to less than the minimum. However, the settings are factors that will affect the overall allocation, and hence responsiveness, of an application. In the case of *CacheSet* the application is the file system Cache.

Internally **NtSetSystemInformation** calls **MmAdjustWorkingSetSize**, which either grows an application's working set or trims it. If the third parameter passed to **MmAdjustWorkingSetSize** is 1, the system Cache's working set is adjusted, otherwise the adjustment occurs on the current process (the system information calls affect only the system cache). Passing in a minimum and maximum of -1 causes **MmAjustWorkingSetSize** to perform a working-set clear operation, releasing all pages from the application's working set.

Download CacheSet (44 KB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Contig v1.8

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download Contig (241 KB)

Introduction

There are a number of NT disk defraggers on the market, including Winternals *Defrag Manager*. These tools are useful for performing a general defragmentation of disks, but while most files are defragmented on drives processed by these utilities, some files may not be. In addition, it is difficult to ensure that particular files that are frequently used are defragmented - they may remain fragmented for reasons that are specific to the defragmentation algorithms used by the defragging product that has been applied. Finally, even if all files have been defragmented, subsequent changes to critical files could cause them to become fragmented. Only by running an entire defrag operation can one hope that they might be defragmented again.

Contig is a single-file defragmenter that attempts to make files contiguous on disk. Its perfect for quickly optimizing files that are continuously becoming fragmented, or that you want to ensure are in as few fragments as possible.

Using Contig

Contig is a utility that defragments a specified file or files. Use it to optimize execution of your frequently used files.

Usage:

\src\Contig\Release\Contig.exe [-a] [-s] [-q] [-v] [existing file]

or \src\Contig\Release\Contig.exe [-f] [-q] [-v] [drive:]

or \src\Contig\Release\Contig.exe [-v] [-l] -n [new file] [new file length]

PARAMETER	DESCRIPTION
-a	Analyze fragmentation
-f	Analyze free space fragmentation
-l	Set valid data length for quick file creation (requires administrator rights)
-q	Quiet mode
-s	Recurse subdirectories
-v	Verbose

Contig can also analyze and defragment the following NTFS metadata files:

- $Mft
- $LogFile
- $Volume
- $AttrDef
- $Bitmap
- $Boot
- $BadClus
- $Secure
- $UpCase
- $Extend

How it Works

Contig uses the native Windows NT defragmentation support that was introduced with NT 4.0 (see my documentation of the defrag APIs for more information). It first scans the disk collecting the locations and sizes of free areas. Then it determines where the file in question is located. Next, *Contig* decides whether the file can be optimized, based on free areas and the number of fragments the file currently consists of. If the file can be optimized, it is moved into the free spaces of the disk.

More Information

Helen Custer's *Inside Windows NT* provides a good overview of the Object Manager name space, and Mark's October 1997 Windows NT Magazine column,"*Inside the Object Manager*", is (of course) an excellent overview.

Download Contig (241 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Disk2vhd v2.01

2 minutes to read • Edit Online

By Mark Russinovich

Published: January 21, 2014

Download Disk2vhd (879 KB)
Run now from Sysinternals Live.

Introduction

Disk2vhd is a utility that creates VHD (Virtual Hard Disk - Microsoft's Virtual Machine disk format) versions of physical disks for use in Microsoft Virtual PC or Microsoft Hyper-V virtual machines (VMs). The difference between Disk2vhd and other physical-to-virtual tools is that you can run Disk2vhd on a system that's online. Disk2vhd uses Windows' Volume Snapshot capability, introduced in Windows XP, to create consistent point-in-time snapshots of the volumes you want to include in a conversion. You can even have Disk2vhd create the VHDs on local volumes, even ones being converted (though performance is better when the VHD is on a disk different than ones being converted).

The Disk2vhd user interface lists the volumes present on the system:

It will create one VHD for each disk on which selected volumes reside. It preserves the partitioning information of the disk, but only copies the data contents for volumes on the disk that are selected. This enables you to capture just system volumes and exclude data volumes, for example.

> Virtual PC supports a maximum virtual disk size of 127GB. If you create a VHD from a larger disk it will not be accessible from a Virtual PC VM.

To use VHDs produced by Disk2vhd, create a VM with the desired characteristics and add the VHDs to the VM's configuration as IDE disks. On first boot, a VM booting a captured copy of Windows will detect the VM's hardware and automatically install drivers, if present in the image. If the required drivers are not present, install them via the Virtual PC or Hyper-V integration components. You can also attach to VHDs using the Windows 7 or Windows Server 2008 R2 Disk Management or Diskpart utilities.

> Do not attach to VHDs on the same system on which you created them if you plan on booting from them. If you do so, Windows will assign the VHD a new disk signature to avoid a collision with the signature of the VHD's source disk. Windows references disks in the boot configuration database (BCD) by disk signature, so when that happens Windows booted in a VM will fail to locate the boot disk.
>
> Disk2vhd does not support the conversion of volumes with Bitlocker enabled. If you wish to create a VHD for such a volume, turn off Bitlocker and wait for the volume to be fully decrypted first.

Disk2vhd runs on Windows Vista, Windows Server 2008, and higher, including x64 systems.

Here's a screenshot of a copy of a Windows Server 2008 R2 Hyper-V system running in a virtual machine on top of the system it was made from:

(click image to zoom)

Command Line Usage

Disk2vhd includes command-line options that enable you to script the creation of VHDs. Specify the volumes you want included in a snapshot by drive letter (e.g. c:) or use "*" to include all volumes.

Usage: **disk2vhd <[drive: [drive:]...]|[*]> <vhdfile>**
Example: **disk2vhd * c:\vhd\snapshot.vhd**

> Physical-to-virtual hard drive migration of a Windows installation is a valid function for customers with Software Assurance and full retail copies of Windows XP, Windows Vista, and Windows 7. Software Assurance provides users valuable benefits—please contact Microsoft Corporation for further information. Windows XP, Windows Vista and Windows 7 installed by Original Equipment Manufacturers (OEM) using OEM versions of these products may not be transferred to a virtual hard drive in accordance with Microsoft licensing terms.

Download Disk2vhd (879 KB)

Run now from Sysinternals Live.

DiskExt v1.2

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download DiskExt (146 KB)

Introduction

DiskExt demonstrates the use of the IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS command that returns information about what disks the partitions of a volume are located on (multipartition disks can reside on multiple disks) and where on the disk the partitions are located.

Download DiskExt (146 KB)

DiskMon for Windows v2.01

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download Diskmon (80 KB)
Run now from Sysinternals Live.

Introduction

DiskMon is an application that logs and displays all hard disk activity on a Windows system. You can also minimize *DiskMon* to your system tray where it acts as a disk light, presenting a green icon when there is disk-read activity and a red icon when there is disk-write activity.

Installation and Use

Installing *DiskMon* is as easy as unzipping it and typing, "diskmon." The menus and toolbar buttons can be used to disable event capturing, control the scrolling of the listview, and to save the listview contents to an ASCII file.

To have *DiskMon* function as a disk light in your system tray, select the Options|Minimize to Tray menu item, or start *DiskMon* with a "/l" (lower-case L) command-line switch e.g. diskmon /l. To reactivate the *DiskMon* window double-click on the *DiskMon* tray icon. To create a shortcut to Diskmon in the tray create a shortcut in your Program Files\Startup folder, edit the properties of the shortcut and set the Target to point at the executable with the path in quotations and the switch outside the quotes:

"C:\Sysinternals Tools\Diskmon.exe" /l

Read and write offsets are presented in terms of sectors (512 bytes). Events can be either timed for their duration (in microseconds), or stamped with the absolute time that they were initiated. The History Depth dialog can be used to specify the maximum number of records that will be kept in the GUI (0 signifies no limit).

Implementation

DiskMon uses kernel event tracing. Event tracing is documented in the Microsoft Platform SDK and the SDK contains source code to TraceDmp, on which *DiskMon* is based.

Download Diskmon (80 KB)

Run now from Sysinternals Live.

Disk Usage v1.61

2 minutes to read • Edit Online

By Mark Russinovich

Published: February 13, 2017

] **Download Du (174 KB)**

Introduction

Du (disk usage) reports the disk space usage for the directory you specify. By default it recurses directories to show the total size of a directory and its subdirectories.

Using Disk Usage (DU)

Usage: du [-c[t]] [-l <levels> | -n | -v] [-u] [-q] <directory>

PARAMETER	DESCRIPTION
-c	Print output as CSV. Use -ct for tab delimiting.
-l	Specify subdirectory depth of information (default is all levels).
-n	Do not recurse.
-v	Show size (in KB) of intermediate directories.
-u	Count each instance of a hardlinked file.
-q	Quiet (no banner).

CSV output is formatted as:

Path, CurrentFileCount, CurrentFileSize, FileCount, DirectoryCount, DirectorySize

] **Download Du (174 KB)**

DiskView v2.4

2 minutes to read • Edit Online

By Mark Russinovich

Published: March 25, 2010

Download DiskView (288 KB)
Run now from Sysinternals Live.

Introduction

DiskView shows you a graphical map of your disk, allowing you to determine where a file is located or, by clicking on a cluster, seeing which file occupies it. Double-click to get more information about a file to which a cluster is allocated.

Download DiskView (288 KB)

Run now from Sysinternals Live.

EFSDump v1.02

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download EFSDump (39 KB)

Introduction

Windows 2000 introduces the Encrypting File System (EFS) so that users can protect their sensitive data. Several new APIs make their debut to support this facility, including one-QueryUsersOnEncryptedFile-that lets you see who has access to encrypted files. This applet uses the API to show you what accounts are authorized to access encrypted files.

Using EFSDump

PARAMETER	DESCRIPTION
-s	Recurse subdirectories.

EFSDump takes wildcards e.g. 'efsdump *.txt'.

Download EFSDump (39 KB)

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

LDMDump v1.02

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download LDMDump (43 KB)

Introduction

Windows 2000 introduces a new type of disk partitioning scheme that is managed by a component called the Logical Disk Manager (LDM). Basic disks implement standard DOS-style partition tables, whereas Dynamic disks use LDM partitioning. LDM partitioning offers several advantages over DOS partitioning including replication across disks, on-disk storage of advanced volume configuration (spanned volume, mirrored volumes, striped volumes and RAID-5 volumes). My March/April two-part series on Windows NT/2000 storage management in *Windows 2000 Magazine* describes the details of each partitioning scheme.

Other than the Disk Management MMC-snapin and a tool called dmdiag in the Windows 2000 Resource Kit, there are no tools for investigating the internals of the LDM on-disk database that describes a system's partitioning layout. *LDMDump* is a utility that lets you examine exactly what is stored in a disk's copy of the system LDM database. *LDMDump* shows you the contents of the LDM database private header, table-of-contents, and object database (where partition, component and volume definitions are stored), and then summarizes its finding with partition table and volume listings.

Installing and Using LDMDump

To use *LDMDump* simply pass it the identifier of a disk.

Usage: ldmdump [-] [-d#]

PARAMETER	DESCRIPTION
-	Displays the supported options and the units of measurement used for output values.
-d#	Specifies the number of the disk for *LDMDump* to examine. For example, "ldmdump /d0" has *LDMDump* show the LDM database information stored on disk 0.

How it Works

There are no published APIs available for obtaining detailed information about a disk's LDM partitioning, and the LDM database format is completely undocumented. *LDMDump* was developed based on study of LDM database contents on a variety of different systems and under changing conditions.

More Information

For more information on the LDM on-disk structure, see:

- *Inside Storage Management, Part 2*, by Mark Russinovich, Windows 2000 Magazine, April 2000.

Download LDMDump (43 KB)

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PendMoves v1.02 and MoveFile v1.01

2 minutes to read • Edit Online

By Mark Russinovich Published: July 4, 2016

 **Download PendMovesand MoveFile (284 KB)**

Introduction

There are several applications, such as service packs and hotfixes, that must replace a file that's in use and is unable to. Windows therefore provides the MoveFileEx API to rename or delete a file and allows the caller to specify that they want the operation to take place the next time the system boots, before the files are referenced. Session Manager performs this task by reading the registered rename and delete commands from the HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations value.

PendMoves Usage

This applet dumps the contents of the pending rename/delete value and also reports an error when the source file is not accessible.

Usage: pendmoves
Here is example output that shows a temporary installation file is scheduled for deletion at the next reboot:

```
C:\\>pendmoves
PendMove v1.2
Copyright (C) 2013 Mark Russinovich
Sysinternals - www.sysinternals.com

Source: C:\\Config.Msi\\3ec7bbbf.rbf
Target: DELETE
```

MoveFile usage

The included MoveFile utililty allows you to schedule move and delete commands for the next reboot: **usage: movefile [source] [dest]**
Specifying an empty destination ("") deletes the source at boot. An example that deletes test.exe is:

```
movefile test.exe ""
```

 **Download PendMovesand MoveFile (284 KB)**

NTFSInfo v1.2

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download NTFSInfo (143 KB)

Introduction

NTFSInfo is a little applet that shows you information about NTFS volumes. Its dump includes the size of a drive's allocation units, where key NTFS files are located, and the sizes of the NTFS metadata files on the volume. This information is typically of little more than curiosity value, but *NTFSInfo* does show some interesting things. For example, you've probably heard about the NTFS equivalent of the FAT file system's File Allocation Table. Its called the Master File Table (MFT), and it is made up of constant sized records that describe the location of all the files and directories on the drive. What's surprising about the MFT is that it is managed as a file, just like any other. *NTFSInfo* will show you where on the disk (in terms of clusters) the MFT is located and how large it is, in addition to specifying how large the volume's clusters and MFT records are. In order to protect the MFT from fragmentation, NTFS reserves a portion of the disk around the MFT that it will not allocate to other files unless disk space runs low. This area is known as the MFT-Zone and *NTFSInfo* will tell you where on the disk the MFT-Zone is located and what percentage of the drive is reserved for it.

You might also be surprised to know that like the MFT, all NTFS meta-data are managed in files. For instance, there is a file called $Boot that is mapped to cover the drive's boot sector. The volume's cluster map is maintained in another file named $Bitmap. These files reside right in the NTFS root directory, but you can't see them unless you know they are there. Try typing "dir /ah $boot" at the root directory of an NTFS volume and you'll actually see the $boot file. *NTFSInfo* performs the equivalent of the "dir /ah" to show you the names and sizes of all of NTFS (3.51 and 4.0) meta-data files.

NTFSInfo is intended to accompany my January 1998 *Windows NT Magazine* "NT Internals" column, which describes NTFS internal data structures.

Installation and Usage

NTFSInfo works on all versions of NTFS, but NTFS for Windows NT 5.0 has different meta-data files that *NTFSInfo* has not been programmed for yet. In order for *NTFSInfo* to work you must have administrative privilege.

Usage: NTFSInfo x

PARAMETER	DESCRIPTION
x	The drive letter of the NTFS volume that you want to examine.

How It Works

NTFSInfo uses an undocumented File System Control (FSCTL) call to obtain information from NTFS about a volume. It prints this information along with a directory dump of NTFS meta-data files.

Download NTFSInfo (143 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

PageDefrag v2.32

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download PageDefrag (70 KB)
Run now from Sysinternals Live.

Introduction

One of the limitations of the Windows NT/2000 defragmentation interface is that it is not possible to defragment files that are open for exclusive access. Thus, standard defragmentation programs can neither show you how fragmented your paging files or Registry hives are, nor defragment them. Paging and Registry file fragmentation can be one of the leading causes of performance degradation related to file fragmentation in a system.

PageDefrag uses advanced techniques to provide you what commercial defragmenters cannot: the ability for you to see how fragmented your paging files and Registry hives are, and to defragment them. In addition, it defragments event log files and Windows 2000/XP hibernation files (where system memory is saved when you hibernate a laptop).

Installing and Using PageDefrag

When you run *PageDefrag* (pagedfrg.exe) you will be presented a listbox that tells you how many clusters make up your paging files, event log files, and Registry hives (SAM, SYSTEM, SYSTEM.ALT, SECURITY, SOFTWARE, .DEFAULT), as well as how many fragments those files are in. If you feel that these files are fragmented enough to warrant a shot at defragmenting them, or if you want to defragment them at every boot, select the appropriate radio button choice and click OK.

When you direct *PageDefrag* to defragment, the next time the system boots it will attempt to do so. Immediately after CHKDSK examines your hard drives *PageDefrag* uses the standard file defragmentation APIs (see my Inside Windows NT Disk Defragmenting page for documentation of these APIs) to defragment the files. As it processes each file *PageDefrag* will print on the boot-time startup screen the file name and its success at defragmenting it. If it is successful at reducing the fragmentation it will tell you the number of clusters the file started with and the number it consists of after the defragmentation.

In some cases *PageDefrag* may be unable to reduce fragmentation on one or more of the files, and it will indicate so on the boot-time Blue Screen. This can happen either because there is not enough space on the drive for defragmentation, or the free space itself is highly fragmented. For the best results you should use *PageDefrag* in conjunction with a commercial defragmentation utility or my free Contig defragmenter.

Command-Line Options

You can run *PageDefrag* non-interactively by specifying a command-line option for the setting you want:

Usage: pagedfrg [-e | -o | -n] [-t <seconds>]

PARAMETER	DESCRIPTION
-e	Defrag every boot.
-o	Defrag once.
-n	Never defrag.
-t	Set countdown to specified number of seconds.

Download PageDefrag (70 KB)

Run now from Sysinternals Live.

PendMoves v1.02 and MoveFile v1.01

2 minutes to read • Edit Online

By Mark Russinovich Published: July 4, 2016

 Download PendMovesand MoveFile (284 KB)

Introduction

There are several applications, such as service packs and hotfixes, that must replace a file that's in use and is unable to. Windows therefore provides the MoveFileEx API to rename or delete a file and allows the caller to specify that they want the operation to take place the next time the system boots,before the files are referenced. Session Manager performs this task by reading the registered rename and delete commands from the HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations value.

PendMoves Usage

This applet dumps the contents of the pending rename/delete value and also reports an error when the source file is notaccessible.

Usage: pendmoves
Here is example output that shows a temporary installation file is scheduled for deletion at the next reboot:

```
C:\\>pendmoves
PendMove v1.2
Copyright (C) 2013 Mark Russinovich
Sysinternals - www.sysinternals.com

Source: C:\\Config.Msi\\3ec7bbbf.rbf
Target: DELETE
```

MoveFile usage

The included MoveFile utililty allows you to schedule move and delete commands for the next reboot: **usage: movefile [source] [dest]**
Specifying an empty destination ("") deletes the source at boot. An example that deletes test.exe is:

```
movefile test.exe ""
```

 Download PendMovesand MoveFile (284 KB)

RegMon for Windows v7.04

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

RegMon and FileMon are no longer available for download. They have been replaced by Process Monitor on versions of Windows starting with Windows 2000 SP4, Windows XP SP2, Windows Server 2003 SP1, and Windows Vista.

Related Utilities

Here are some other monitoring tools available at Sysinternals:

- PortMon - a serial and parallel port monitor
- Process Monitor - a process and thread monitor
- DiskMon - a hard disk monitor
- DebugView - a debug output monitor

SDelete v2.02

6 minutes to read • Edit Online

By Mark Russinovich

Published: December 11, 2018

Download SDelete (221 KB)

Introduction

One feature of Windows NT/2000's (Win2K) C2-compliance is that it implements object reuse protection. This means that when an application allocates file space or virtual memory it is unable to view data that was previously stored in the resources Windows NT/2K allocates for it. Windows NT zero-fills memory and zeroes the sectors on disk where a file is placed before it presents either type of resource to an application. However, object reuse does not dictate that the space that a file occupies before it is deleted be zeroed. This is because Windows NT/2K is designed with the assumption that the operating system controls access to system resources. However, when the operating system is not active it is possible to use raw disk editors and recovery tools to view and recover data that the operating system has deallocated. Even when you encrypt files with Win2K's Encrypting File System (EFS), a file's original unencrypted file data is left on the disk after a new encrypted version of the file is created.

The only way to ensure that deleted files, as well as files that you encrypt with EFS, are safe from recovery is to use a secure delete application. Secure delete applications overwrite a deleted file's on-disk data using techiques that are shown to make disk data unrecoverable, even using recovery technology that can read patterns in magnetic media that reveal weakly deleted files. *SDelete* (Secure Delete) is such an application. You can use *SDelete* both to securely delete existing files, as well as to securely erase any file data that exists in the unallocated portions of a disk (including files that you have already deleted or encrypted). *SDelete* implements the Department of Defense clearing and sanitizing standard DOD 5220.22-M, to give you confidence that once deleted with *SDelete*, your file data is gone forever. Note that *SDelete* securely deletes file data, but not file names located in free disk space.

Using SDelete

SDelete is a command line utility that takes a number of options. In any given use, it allows you to delete one or more files and/or directories, or to cleanse the free space on a logical disk. *SDelete* accepts wild card characters as part of the directory or file specifier.

Usage: sdelete [-p passes] [-s] [-q] <file or directory> ...
sdelete [-p passes] [-z|-c] [drive letter] ...

PARAMETER	DESCRIPTION
-a	Remove Read-Only attribute.
-c	Clean free space.
-p passes	Specifies number of overwrite passes (default is 1).
-q	Don't print errors (Quiet).

PARAMETER	DESCRIPTION
-s or **-r**	Recurse subdirectories.
-z	Zero free space (good for virtual disk optimization).

How SDelete Works

Securely deleting a file that has no special attributes is relatively straight-forward: the secure delete program simply overwrites the file with the secure delete pattern. What is more tricky is securely deleting Windows NT/2K compressed, encrypted and sparse files, and securely cleansing disk free spaces.

Compressed, encrypted and sparse are managed by NTFS in 16-cluster blocks. If a program writes to an existing portion of such a file NTFS allocates new space on the disk to store the new data and after the new data has been written, deallocates the clusters previously occupied by the file. NTFS takes this conservative approach for reasons related to data integrity, and in the case of compressed and sparse files, in case a new allocation is larger than what exists (the new compressed data is bigger than the old compressed data). Thus, overwriting such a file will not succeed in deleting the file's contents from the disk.

To handle these types of files *SDelete* relies on the defragmentation API. Using the defragmentation API, *SDelete* can determine precisely which clusters on a disk are occupied by data belonging to compressed, sparse and encrypted files. Once *SDelete* knows which clusters contain the file's data, it can open the disk for raw access and overwrite those clusters.

Cleaning free space presents another challenge. Since FAT and NTFS provide no means for an application to directly address free space, *SDelete* has one of two options. The first is that it can, like it does for compressed, sparse and encrypted files, open the disk for raw access and overwrite the free space. This approach suffers from a big problem: even if *SDelete* were coded to be fully capable of calculating the free space portions of NTFS and FAT drives (something that's not trivial), it would run the risk of collision with active file operations taking place on the system. For example, say *SDelete* determines that a cluster is free, and just at that moment the file system driver (FAT, NTFS) decides to allocate the cluster for a file that another application is modifying. The file system driver writes the new data to the cluster, and then *SDelete* comes along and overwrites the freshly written data: the file's new data is gone. The problem is even worse if the cluster is allocated for file system metadata since *SDelete* will corrupt the file system's on-disk structures.

The second approach, and the one *SDelete* takes, is to indirectly overwrite free space. First, *SDelete* allocates the largest file it can. *SDelete* does this using non-cached file I/O so that the contents of the NT file system cache will not be thrown out and replaced with useless data associated with *SDelete*'s space-hogging file. Because non-cached file I/O must be sector (512-byte) aligned, there might be some left over space that isn't allocated for the *SDelete* file even when *SDelete* cannot further grow the file. To grab any remaining space *SDelete* next allocates the largest cached file it can. For both of these files *SDelete* performs a secure overwrite, ensuring that all the disk space that was previously free becomes securely cleansed.

On NTFS drives *SDelete*'s job isn't necessarily through after it allocates and overwrites the two files. *SDelete* must also fill any existing free portions of the NTFS MFT (Master File Table) with files that fit within an MFT record. An MFT record is typically 1KB in size, and every file or directory on a disk requires at least one MFT record. Small files are stored entirely within their MFT record, while files that don't fit within a record are allocated clusters outside the MFT. All *SDelete* has to do to take care of the free MFT space is allocate the largest file it can - when the file occupies all the available space in an MFT Record NTFS will prevent the file from getting larger, since there are no free clusters left on the disk (they are being held by the two files *SDelete* previously allocated). *SDelete* then repeats the process. When *SDelete* can no longer even create a new file, it knows that all the previously free records in the MFT have been completely filled with securely overwritten files.

To overwrite file names of a file that you delete, *SDelete* renames the file 26 times, each time replacing each

character of the file's name with a successive alphabetic character. For instance, the first rename of "foo.txt" would be to "AAA.AAA".

The reason that *SDelete* does not securely delete file names when cleaning disk free space is that deleting them would require direct manipulation of directory structures. Directory structures can have free space containing deleted file names, but the free directory space is not available for allocation to other files. Hence, *SDelete* has no way of allocating this free space so that it can securely overwrite it.

Download SDelete (151 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Sigcheck v2.73

2 minutes to read • Edit Online

By Mark Russinovich

Published: September 05, 2019

Download Sigcheck (799 KB)

Introduction

Sigcheck is a command-line utility that shows file version number, timestamp information, and digital signature details, including certificate chains. It also includes an option to check a file's status on VirusTotal, a site that performs automated file scanning against over 40 antivirus engines, and an option to upload a file for scanning.

usage: sigcheck [-a][-h][-i][-e][-l][-n][[-s]|[-c|-ct]|[-m]][-q][-r][-u][-vt][-v[r][s]][-f catalog file] <file or directory>

usage: sigcheck -d [-c|-ct] <file or directory>

usage: sigcheck -o [-vt][-v[r]] <sigcheck csv file>

usage: sigcheck -t[u][v] [-i] [-c|-ct] <certificate store name|*>

PARAMETER	DESCRIPTION
-a	Show extended version information. The entropy measure reported is the bits per byte of information of the file's contents.
-c	CSV output with comma delimiter
-ct	CSV output with tab delimiter
-d	Dump contents of a catalog file
-e	Scan executable images only (regardless of their extension)
-f	Look for signature in the specified catalog file
-h	Show file hashes
-i	Show catalog name and signing chain
-l	Traverse symbolic links and directory junctions
-m	Dump manifest
-n	Only show file version number

PARAMETER	DESCRIPTION
-o	Performs Virus Total lookups of hashes captured in a CSV file previously captured by Sigcheck when using the -h option. This usage is intended for scans of offline systems.
-nobanner	Quiet (no banner)
-r	Disable check for certificate revocation
-s	Recurse subdirectories
-t[u][v]	Dump contents of specified certificate store ('*' for all stores). Specify -tu to query the user store (machine store is the default). Append '-v' to have Sigcheck download the trusted Microsoft root certificate list and only output valid certificates not rooted to a certificate on that list. If the site is not accessible, authrootstl.cab or authroot.stl in the current directory are used instead, if present.
-u	If VirusTotal check is enabled, show files that are unknown by VirusTotal or have non-zero detection, otherwise show only unsigned files.
-v[rs]	Query VirusTotal (www.virustotal.com) for malware based on file hash. Add 'r' to open reports for files with non-zero detection. Files reported as not previously scanned will be uploaded to VirusTotal if the 's' option is specified. Note scan results may not be available for five or more minutes.
-vt	Before using VirusTotal features, you must accept VirusTotal terms of service. See: https://www.virustotal.com/en/about/terms-of-service/ If you haven't accepted the terms and you omit this option, you will be interactively prompted.

One way to use the tool is to check for unsigned files in your \Windows\System32 directories with this command:

sigcheck -u -e c:\windows\system32

You should investigate the purpose of any files that are not signed.

Download Sigcheck (799 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Learn More

- Malware Hunting with the Sysinternals Tools
  In this presentation, Mark shows how to use the Sysinternals tools to identify, analyze and clean malware.

Streams v1.6

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download Streams (140 KB)

Introduction

The NTFS file system provides applications the ability to create alternate data streams of information. By default, all data is stored in a file's main unnamed data stream, but by using the syntax 'file:stream', you are able to read and write to alternates. Not all applications are written to access alternate streams, but you can demonstrate streams very simply. First, change to a directory on a NTFS drive from within a command prompt. Next, type 'echo hello > test:stream'. You've just created a stream named 'stream' that is associated with the file 'test'. Note that when you look at the size of test it is reported as 0, and the file looks empty when opened in any text editor. To see your stream enter 'more < test:stream' (the type command doesn't accept stream syntax so you have to use more).

NT does not come with any tools that let you see which NTFS files have streams associated with them, so I've written one myself. Streams will examine the files and directories (note that directories can also have alternate data streams) you specify and inform you of the name and sizes of any named streams it encounters within those files. Streams makes use of an undocumented native function for retrieving file stream information.

Using Streams

Usage: streams [-s] [-d] <file or directory>

PARAMETER	DESCRIPTION
-s	Recurse subdirectories.
-d	Delete streams.
Streams takes wildcards e.g. 'streams *.txt'.	

Download Streams (140 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Sync v2.2

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

 **Download Sync (145 KB)**

Introduction

UNIX provides a standard utility called Sync, which can be used to direct the operating system to flush all file system data to disk in order to insure that it is stable and won't be lost in case of a system failure. Otherwise, any modified data present in the cache would be lost. Here is an equivalent that I wrote, called Sync, that works on all versions of Windows. Use it whenever you want to know that modified file data is safely stored on your hard drives. Unfortunately, Sync requires administrative privileges to run. This version also lets you flush removable drives such as ZIP drives.

Using Sync

Usage: sync [-r] [-e] [drive letter list]

PARAMETER	DESCRIPTION
-r	Flush removable drives.
-e	Ejects removable drives.

Specifying specific drives (e.g. "c e") will result in Sync only flushing those drives.

 **Download Sync (145 KB)**

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

VolumeID v2.1

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download VolumeID (194 KB)

Introduction

While Windows NT/2000 and Windows 95 and 98's built-in Label utility lets you change the labels of disk volumes, it does not provide any means for changing volume ids. This utiltity, VolumeID, allows you to change the ids of FAT and NTFS disks (floppies or hard drives).

Usage: volumeid <driveletter:> xxxx-xxxx

This is a command-line program that you must run from a command-prompt window.

Note that changes on NTFS volumes won't be visible until the next reboot. In addition, you should shut down any applications you have running before changing a volume id. NT may become confused and think that the media (disk) has changed after a FAT volume id has changed and pop up messages indicating that you should reinsert the original disk (!). It may then fail the disk requests of applications using those drives.

Download VolumeID (194 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Sysinternals Networking Utilities

2 minutes to read • Edit Online

AD Explorer

Active Directory Explorer is an advanced Active Directory (AD) viewer and editor.

AD Insight

AD Insight is an LDAP (Light-weight Directory Access Protocol) real-time monitoring tool aimed at troubleshooting Active Directory client applications.

AdRestore

Undelete Server 2003 Active Directory objects.

PipeList

Displays the named pipes on your system, including the number of maximum instances and active instances for each pipe.

PsFile

See what files are opened remotely.

PsPing

Measures network performance.

PsTools

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

ShareEnum

Scan file shares on your network and view their security settings to close security holes.

TCPView

Active socket command-line viewer.

Whois

See who owns an Internet address.

Active Directory Explorer v1.44

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 15, 2012

Download AdExplorer (244 KB)
Run now from Sysinternals Live.

Introduction

Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. You can use AD Explorer to easily navigate an AD database, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that you can save and re-execute.

AD Explorer also includes the ability to save snapshots of an AD database for off-line viewing and comparisons. When you load a saved snapshot, you can navigate and explore it as you would a live database. If you have two snapshots of an AD database you can use AD Explorer's comparison functionality to see what objects, attributes and security permissions changed between them.

Download AdExplorer (244 KB)

Run now from Sysinternals Live.

Insight for Active Directory v1.2

2 minutes to read • Edit Online

By Mark Russinovich

Published: October 26, 2015

Download AdInsight (113 KB)
Run now from Sysinternals Live.

Introduction

ADInsight is an LDAP (Light-weight Directory Access Protocol) real-time monitoring tool aimed at troubleshooting Active Directory client applications. Use its detailed tracing of Active Directory client-server communications to solve Windows authentication, Exchange, DNS, and other problems.

ADInsight uses DLL injection techniques to intercept calls that applications make in the Wldap32.dll library, which is the standard library underlying Active Directory APIs such ldap and ADSI. Unlike network monitoring tools, ADInsight intercepts and interprets all client-side APIs, including those that do not result in transmission to a server. ADInsight monitors any process into which it can load it's tracing DLL, which means that it does not require administrative permissions, however, if run with administrative rights, it will also monitor system processes, including windows services.

Download AdInsight (113 KB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Related Links

The Sysinternals AdRestore utility enables you to restore deleted objects on Windows Server 2003 domains.

AD Explorer is an advanced Active Directory (AD) viewer and editor.

AdRestore v1.1

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download AdRestore (42 KB)

Introduction

Windows Server 2003 introduces the ability to restore deleted ("tombstoned") objects. This simple command-line utility enumerates the deleted objects in a domain and gives you the option of restoring each one. Source code is based on sample code in the Microsoft Platform SDK. This MS KB article describes the use of AdRestore:

840001: How to restore deleted user accounts and their group memberships in Active Directory

Download AdRestore (42 KB)

PipeList v1.02

2 minutes to read • Edit Online

Published: July 4, 2016

Download PipeList (211 KB)

Introduction

Did you know that the device driver that implements named pipes is actually a file system driver? In fact, the driver's name is NPFS.SYS, for "Named Pipe File System". What you might also find surprising is that its possible to obtain a directory listing of the named pipes defined on a system. This fact is not documented, nor is it possible to do this using the Win32 API. Directly using NtQueryDirectoryFile, the native function that the Win32 FindFile APIs rely on, makes it possible to list the pipes. The directory listing NPFS returns also indicates the maximum number of pipe instances set for each pipe and the number of active instances.

Download PipeList (211 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

PsFile v1.03

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (1.6 MB)

Introduction

The "net file" command shows you a list of the files that other computers have opened on the system upon which you execute the command, however it truncates long path names and doesn't let you see that information for remote systems. *PsFile* is a command-line utility that shows a list of files on a system that are opened remotely, and it also allows you to close opened files either by name or by a file identifier.

Installation

Just copy *PsFile* onto your executable path, and type "psfile".

Using PsFile

The default behavior of *PsFile* is to list the files on the local system that are open by remote systems. Typing a command followed by "- " displays information on the syntax for the command.

Usage: psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]

PARAMETER	DESCRIPTION
-u	Specifies optional user name for login to remote computer.
-p	Specifies password for user name. If this is omitted, you will be prompted to enter the password without it being echoed to the screen.
Id	Identifier (as assigned by PsFile) of the file for which to display information or to close.
Path	Full or partial path of files to match for information display or close.
-c	Closes the files identifed by ID or path.

How it Works

PsFile uses the NET API, which is documented in the Platform SDK.

Download PsTools (1.6 MB)

PsPing v2.1

4 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

PsPing implements Ping functionality, TCP ping, latency and bandwidth measurement. Use the following command-line options to show the usage for each test type:

Installation

Copy *PsPing* onto your executable path. Typing "psping" displays its usage syntax.

Using PsPing

PsPing implements Ping functionality, TCP ping, latency and bandwidth measurement. Use the following command-line options to show the usage for each test type:

Usage: psping -? [i|t|l|b]

PARAMETER	DESCRIPTION	
-? I	Usage for ICMP ping.	
-? T	Usage for TCP ping.	
-? L	Usage for latency test.	
-? B	Usage for bandwidth test.	

ICMP ping usage:
psping [[-6]|[-4]] [-h [buckets | <val1>,<val2>,...]] [-i <interval>] [-l <requestsize>[k|m] [-q] [-t|-n <count>] [-w <count>] <destination>

PARAMETER	DESCRIPTION
-h	Print histogram (default bucket count is 20).
	If you specify a single argument, it's interpreted as a bucket count and the histogram will contain that number of buckets covering the entire time range of values. Specify a comma-separated list of times to create a custom histogram (e.g. "0.01,0.05,1,5,10").
-i	Interval in seconds. Specify 0 for fast ping.

PARAMETER	DESCRIPTION
-l	Request size. Append 'k' for kilobytes and 'm' for megabytes.
-n	Number of pings or append 's' to specify seconds e.g. '10s'.
-q	Don't output during pings.
-t	Ping until stopped with Ctrl+C and type Ctrl+Break for statistics.
-w	Warmup with the specified number of iterations (default is 1).
-4	Force using IPv4.
-6	Force using IPv6.

For high-speed ping tests use -q and -i 0.

TCP ping usage:
** psping [[-6]|[-4]] [-h [buckets | <val1>,<val2>,...]] [-i <interval>] [-l <requestsize>[k|m] [-q] [-t|-n <count>] [-w <count>] <destination:destport>**

PARAMETER	DESCRIPTION
-h	Print histogram (default bucket count is 20).
	If you specify a single argument, it's interpreted as a bucket count and the histogram will contain that number of buckets covering the entire time range of values. Specify a comma-separated list of times to create a custom histogram (e.g. "0.01,0.05,1,5,10").
-i	Interval in seconds. Specify 0 for fast ping.
-l	Request size. Append 'k' for kilobytes and 'm' for megabytes.
-n	Number of pings or append 's' to specify seconds e.g. '10s'.
-q	Don't output during pings.
-t	Ping until stopped with Ctrl+C and type Ctrl+Break for statistics.
-w	Warmup with the specified number of iterations (default is 1).
-4	Force using IPv4.
-6	Force using IPv6.

For high-speed ping tests use -q and -i 0.

TCP and UDP latency usage:

server: psping [[-6]|[-4]] [-f] <-s source:sourceport>

client: psping [[-6]|[-4]] [-f] [-u] [-h [buckets | <val1>,<val2>,...]] [-r] <-l requestsize>[k|m]] <-n count> [-w <count>] <destination:destport>

PARAMETER	DESCRIPTION
-f	Open source firewall port during the run.
-u	UDP (default is TCP).
-h	Print histogram (default bucket count is 20).
	If you specify a single argument, it's interpreted as a bucket count and the histogram will contain that number of buckets covering the entire time range of values. Specify a comma-separated list of times to create a custom histogram (e.g. "0.01,0.05,1,5,10").
-l	Request size. Append 'k' for kilobytes and 'm' for megabytes.
-n	Number of sends/receives. Append 's' to specify seconds e.g. '10s'
-r	Receive from the server instead of sending.
-w	Warmup with the specified number of iterations (default is 5).
-4	Force using IPv4.
-6	Force using IPv6.
-s	Server listening address and port.

The server can serve both latency and bandwidth tests and remains active until you terminate it with Control-C.

TCP and UDP bandwidth usage:

server: psping [[-6]|[-4]] [-f] <-s source:sourceport>

client: psping [[-6]|[-4]] [-f] [-u] [-h [buckets | <val1>,<val2>,...]] [-r] <-l requestsize>[k|m]] <-n count> [-i <outstanding>] [-w <count>] <destination:destport>

PARAMETER	DESCRIPTION
-f	Open source firewall port during the run.
-u	UDP (default is TCP).
-b	Bandwidth test.
-h	Print histogram (default bucket count is 20).

PARAMETER	DESCRIPTION
	If you specify a single argument, it's interpreted as a bucket count and the histogram will contain that number of buckets covering the entire time range of values. Specify a comma-separated list of times to create a custom histogram (e.g. "0.01,0.05,1,5,10").
-i	Number of outstanding I/Os (default is min of 16 and 2x CPU cores).
-l	Request size. Append 'k' for kilobytes and 'm' for megabytes.
-n	Number of sends/receives. Append 's' to specify seconds e.g. '10s'
-r	Receive from the server instead of sending.
-w	Warmup for the specified iterations (default is 2x CPU cores).
-4	Force using IPv4.
-6	Force using IPv6.
-s	Server listening address and port.

The server can serve both latency and bandwidth tests and remains active until you terminate it with Control-C.

Examples

This command executes an ICMP ping test for 10 iterations with 3 warmup iterations:
psping -n 10 -w 3 marklap

To execute a TCP connect test, specify the port number. The following command executes connect attempts against the target as quickly as possible, only printing a summary when finished with the 100 iterations and 1 warmup iteration:
psping -n 100 -i 0 -q marklap:80

To configure a server for latency and bandwidth tests, simply specify the -s option and the source address and port the server will bind to:
psping -s 192.168.2.2:5000

A buffer size is required to perform a TCP latency test. This example measures the round trip latency of sending an 8KB packet to the target server, printing a histogram with 100 buckets when completed:
psping -l 8k -n 10000 -h 100 192.168.2.2:5000

This command tests bandwidth to a PsPing server listening at the target IP address for 10 seconds and produces a histogram with 100 buckets. Note that the test must run for at least one second after warmup for a histogram to generate. Simply add -u to have PsPing perform a UDP bandwidth test.
psping -b -l 8k -n 10000 -h 100 192.168.2.2:5000

 Download PsTools (2.7 MB)

ShareEnum v1.6

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download ShareEnum (94 KB)
Run now from Sysinternals Live.

Introduction

An aspect of Windows NT/2000/XP network security that's often overlooked is file shares. A common security flaw occurs when users define file shares with lax security, allowing unauthorized users to see sensitive files. There are no built-in tools to list shares viewable on a network and their security settings, but *ShareEnum* fills the void and allows you to lock down file shares in your network.

When you run *ShareEnum* it uses NetBIOS enumeration to scan all the computers within the domains accessible to it, showing file and print shares and their security settings. Because only a domain administrator has the ability to view all network resources, *ShareEnum* is most effective when you run it from a domain administrator account.

How It Works

ShareEnum uses **WNetEnumResource** to enumerate domains and the computers within them and **NetShareEnum** to enumerate shares on computers.

Download ShareEnum (94 KB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

TCPView v3.05

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 25, 2011

Download TCPView (285 KB)
Run now from Sysinternals Live.

Introduction

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.

Using TCPView

When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. You can use a toolbar button or menu item to toggle the display of resolved names. On Windows XP systems, TCPView shows the name of the process that owns each endpoint.

By default, TCPView updates every second, but you can use the **Options|Refresh Rate** menu item to change the rate. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green.

You can close established TCP/IP connections (those labeled with a state of ESTABLISHED) by selecting **File|Close Connections**, or by right-clicking on a connection and choosing **Close Connections** from the resulting context menu.

You can save TCPView's output window to a file using the **Save** menu item.

Using Tcpvcon

Tcpvcon usage is similar to that of the built-in Windows netstat utility:

Usage: tcpvcon [-a] [-c] [-n] [process name or PID]

PARAMETER	DESCRIPTION
-a	Show all endpoints (default is to show established TCP connections).
-c	Print output as CSV.
-n	Don't resolve addresses.

Microsoft TCPView KB Article

This Microsoft KB article references TCPView:

816944: "Unexpected Error 0x8ffe2740 Occurred" Error Message When You Try to Start a Web Site

Download TCPView (285 KB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Whois v1.21

2 minutes to read • Edit Online

By Mark Russinovich

Published: December 11, 2019

 **Download Whois (387 KB)**

Introduction

Whois performs the registration record for the domain name or IP address that you specify.

Usage

Usage: whois [-v] domainname [whois.server]

PARAMETER	DESCRIPTION
-v	Print whois information for referrals

Domainname can be either a DNS name (e.g. www.sysinternals.com) or IP address (e.g. 66.193.254.46).

 **Download Whois (387 KB)**

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Sysinternals Process Utilities

2 minutes to read • Edit Online

Autoruns

See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

Handle

This handy command-line utility will show you what files are open by which processes, and much more.

ListDLLs

List all the DLLs that are currently loaded, including where they are loaded and their version numbers. Version 2.0 prints the full path names of loaded modules.

PortMon

Monitor serial and parallel port activity with this advanced monitoring tool. It knows about all standard serial and parallel IOCTLs and even shows you a portion of the data being sent and received. Version 3.x has powerful new UI enhancements and advanced filtering capabilities.

ProcDump

This new command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes. It also serves as a general process dump creation utility and can also monitor and generate process dumps when a process has a hung window or unhandled exception.

Process Explorer

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process Monitor

Monitor file system, Registry, process, thread and DLL activity in real-time.

PsExec

Execute processes remotely.

PsGetSid

Displays the SID of a computer or a user.

PsKill

Terminate local or remote processes.

PsList

Show information about processes and threads.

PsService

View and control services.

PsSuspend

Suspend and resume processes.

PsTools

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

ShellRunas

Launch programs as a different user via a convenient shell context-menu entry.

VMMap

See a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types. Identify the sources of process memory usage and the memory cost of application features.

Autoruns for Windows v13.96

By Mark Russinovich

Published: June 28, 2019

Download Autoruns and Autorunsc (1.6 MB)
Run now from Sysinternals Live.

Introduction

This utility, which has the most comprehensive knowledge of auto-starting locations of any startup monitor, shows you what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer and media players. These programs and drivers include ones in your startup folder, Run, RunOnce, and other Registry keys. *Autoruns* reports Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, auto-start services, and much more. *Autoruns* goes way beyond other autostart utilities.

Autoruns' **Hide Signed Microsoft Entries** option helps you to zoom in on third-party auto-starting images that have been added to your system and it has support for looking at the auto-starting images configured for other accounts configured on a system. Also included in the download package is a command-line equivalent that can output in CSV format, Autorunsc.

You'll probably be surprised at how many executables are launched automatically!

Screenshot

Usage

Simply run *Autoruns* and it shows you the currently configured auto-start applications as well as the full list of Registry and file system locations available for auto-start configuration. Autostart locations displayed by Autoruns include logon entries, Explorer add-ons, Internet Explorer add-ons including Browser Helper Objects (BHOs), Appinit DLLs, image hijacks, boot execute images, Winlogon notification DLLs, Windows Services and Winsock Layered Service Providers, media codecs, and more. Switch tabs to view autostarts from different categories.

To view the properties of an executable configured to run automatically, select it and use the **Properties** menu item or toolbar button. If Process Explorer is running and there is an active process executing the selected executable then the **Process Explorer** menu item in the **Entry** menu will open the process properties dialog box for the process executing the selected image.

Navigate to the Registry or file system location displayed or the configuration of an auto-start item by selecting the item and using the **Jump to Entry** menu item or toolbar button, and navigate to the location of an autostart image.

To disable an auto-start entry uncheck its check box. To delete an auto-start configuration entry use the **Delete** menu item or toolbar button.

The Options menu includes several display filtering options, such as only showing non-Windows entries, as well

as access to a scan options dialog from where you can enable signature verification and Virus Total hash and file submission.

Select entries in the **User** menu to view auto-starting images for different user accounts.

More information on display options and additional information is available in the on-line help.

Autorunsc Usage

Autorunsc is the command-line version of Autoruns. Its usage syntax is:

Usage: autorunsc [-a <*|bdeghiklmoprsw>] [-c|-ct] [-h] [-m] [-s] [-u] [-vt] [[-z] | [user]]]

PARAMETER	DESCRIPTION
-a	Autostart entry selection:
*****	All.
b	Boot execute.
d	Appinit DLLs.
e	Explorer addons.
g	Sidebar gadgets (Vista and higher)
h	Image hijacks.
i	Internet Explorer addons.
k	Known DLLs.
l	Logon startups (this is the default).
m	WMI entries.
n	Winsock protocol and network providers.
o	Codecs.
p	Printer monitor DLLs.
r	LSA security providers.
s	Autostart services and non-disabled drivers.
t	Scheduled tasks.
w	Winlogon entries.
-c	Print output as CSV.
-ct	Print output as tab-delimited values.

PARAMETER	DESCRIPTION
-h	Show file hashes.
-m	Hide Microsoft entries (signed entries if used with -v).
-s	Verify digital signatures.
-t	Show timestamps in normalized UTC (YYYYMMDD-hhmmss).
-u	If VirusTotal check is enabled, show files that are unknown by VirusTotal or have non-zero detection, otherwise show only unsigned files.
-x	Print output as XML.
-v[rs]	Query VirusTotal for malware based on file hash. Add 'r' to open reports for files with non-zero detection. Files reported as not previously scanned will be uploaded to VirusTotal if the 's' option is specified. Note scan results may not be available for five or more minutes.
-vt	Before using VirusTotal features, you must accept the VirusTotal terms of service. If you haven't accepted the terms and you omit this option, you will be interactively prompted.
-z	Specifies the offline Windows system to scan.
user	Specifies the name of the user account for which autorun items will be shown. Specify '*' to scan all user profiles.

Related Links

- **Windows Internals Book** The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- **Windows Sysinternals Administrator's Reference** The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download

Download Autoruns and Autorunsc (1.6 MB)

Run now from Sysinternals Live.

Handle v4.22

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 14, 2019

Download Handle (701 KB)

Introduction

Ever wondered which program has a particular file or directory open? Now you can find out. *Handle* is a utility that displays information about open handles for any process in the system. You can use it to see the programs that have a file open, or to see the object types and names of all the handles of a program.

You can also get a GUI-based version of this program, *Process Explorer*, here at Sysinternals.

Installation

You run *Handle* by typing "handle". You must have administrative privilege to run *Handle*.

Usage

Handle is targeted at searching for open file references, so if you do not specify any command-line parameters it will list the values of all the handles in the system that refer to open files and the names of the files. It also takes several parameters that modify this behavior.

usage: handle [[-a] [-u] | [-c <handle> [-l] [-y]] | [-s]] [-p <processname>|<pid>> [name]

PARAMETER	DESCRIPTION
-a	Dump information about all types of handles, not just those that refer to files. Other types include ports, Registry keys, synchronization primitives, threads, and processes.
-c	Closes the specified handle (interpreted as a hexadecimal number). You must specify the process by its PID. **WARNING:** Closing handles can cause application or system instability.
-l	Dump the sizes of pagefile-backed sections.
-y	Don't prompt for close handle confirmation.
-s	Print count of each type of handle open.
-u	Show the owning user name when searching for handles.

PARAMETER	DESCRIPTION
-p	Instead of examining all the handles in the system, this parameter narrows Handle's scan to those processes that begin with the name process. Thus: **handle -p exp** would dump the open files for all processes that start with "exp", which would include Explorer.
name	This parameter is present so that you can direct Handle to search for references to an object with a particular name. For example, if you wanted to know which process (if any) has "c:\windows\system32" open you could type: **handle windows\system** The name match is case-insensitive and the fragment specified can be anywhere in the paths you are interested in.

Handle Output

When not in search mode (enabled by specifying a name fragment as a parameter), Handle divides its output into sections for each process it is printing handle information for. Dashed lines are used as a separator, immediately below which you will see the process name and its process id (PID). Beneath the process name are listed handle values (in hexadecimal), the type of object the handle is associated with, and the name of the object if it has one.

When in search mode, *Handle* prints the process names and id's are listed on the left side and the names of the objects that had a match are on the right.

More Information

You can find more information on the Object Manager in *Windows Internals, 4th Edition* or by browsing the Object Manager name-space with WinObj.

Microsoft Handle KB Articles

The following Microsoft KB articles reference Handle for diagnosing or troubleshooting various problems:

- 245068: Err Msg: Access is Denied. You Don't Have Permissions or the File is in Use
- 276525: Your Computer May Stop Responding When You Monitor Open Handles

Download Handle (701 KB)

ListDLLs v3.2

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download ListDLLs (307 KB)

Introduction

ListDLLs is a utility that reports the DLLs loaded into processes. You can use it to list all DLLs loaded into all processes, into a specific process, or to list the processes that have a particular DLL loaded. ListDLLs can also display full version information for DLLs, including their digital signature, and can be used to scan processes for unsigned DLLs.

Usage

listdlls [-r] [-v | -u] [processname|pid]
listdlls [-r] [-v] [-d dllname]

PARAMETER	DESCRIPTION
processname	Dump DLLs loaded by process (partial name accepted).
pid	Dump DLLs associated with the specified process id.
dllname	Show only processes that have loaded the specified DLL.
-r	Flag DLLs that relocated because they are not loaded at their base address.
-u	Only list unsigned DLLs.
-v	Show DLL version information.

Examples

List the DLLs loaded into Outlook.exe, including their version information:

listdlls -v outlook

List any unsigned DLLs loaded into any process:

listdlls -u

Show processes that have loaded MSO.DLL:

listdlls -d mso.dll

Download ListDLLs (307 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Portmon for Windows v3.03

3 minutes to read • Edit Online

By Mark Russinovich

Published: January 12, 2012

Download Portmon (226 KB)
Run now from Sysinternals Live.

Introduction

Portmon is a utility that monitors and displays all serial and parallel port activity on a system. It has advanced filtering and search capabilities that make it a powerful tool for exploring the way Windows works, seeing how applications use ports, or tracking down problems in system or application configurations.

Portmon 3.x

Version 3.x of *Portmon* marks the introduction of a number of powerful features.

- **Remote monitoring:** Capture kernel-mode and/or Win32 debug output from any computer accessible via TCP/IP - even across the Internet. You can monitor multiple remote computers simultaneously. *Portmon* will even install its client software itself if you are running it on a Windows NT/2K system and are capturing from another Windows NT/2K system in the same Network Neighborhood.
- **Most-recent-filter lists:***Portmon* has been extended with powerful filtering capabilities and it remembers your most recent filter selections, with an interface that makes it easy to reselect them.
- **Clipboard copy:** Select multiple lines in the output window and copy their contents to the clipboard.
- **Highlighting:** Highlight debug output that matches your highlighting filter, and even customize the highlighting colors.
- **Log-to-file:** Write debug output to a file as its being captured.
- **Printing:** Print all or part of captured debug output to a printer.
- **One-file payload:***Portmon* is now implemented as one file.

The on-line help-file describes all these features, and more, in detail.

Installation and Use

Simply execute the *Portmon* program file (portmon.exe) and *Portmon* will immediately start capturing debug output. To run *Portmon* on Windows 95 you must get the WinSock2 update from Microsoft. Note that if you run *Portmon* on Windows NT/2K portmon.exe must be located on a non-network drive and you must have administrative privilege. Menus, hot-keys, or toolbar buttons can be used to clear the window, save the monitored data to a file, search output, change the window font, and more. The on-line help describes all of *Portmon's* features.

Portmon understands all serial and parallel port I/O control (IOCTLs) commands and will display them along with interesting information regarding their associated parameters. For read and write requests *Portmon* displays the first several dozen bytes of the buffer, using '.' to represent non-printable characters. The Show Hex menu option lets you toggle between ASCII and raw hex output of buffer data.

How it Works: WinNT

The *Portmon* GUI is responsible for identifying serial and parallel ports. It does so by enumerating the serial ports that are configured under HKEY_LOCAL_MACHINE\Hardware\DeviceMap\SerialComm and the parallel ports defined under HKEY_LOCAL_MACHINE\Hardware\DeviceMap\Parallel Ports. These keys contain the mappings between serial and parallel port device names and the Win32-accessible names.

When you select a port to monitor, *Portmon* sends a request to its device driver that includes the NT name (e.g. \device\serial0) that you are interested in. The driver uses standard filtering APIs to attach its own filter device object to the target device object. First, it uses **ZwCreateFile** to open the target device. Then it translates the handle it receives back from **ZwCreateFile** to a device object pointer. After creating its own filter device object that matches the characteristics of the target, the driver calls **IoAttachDeviceByPointer** to establish the filter. From that point on the *Portmon* driver will see all requests aimed at the target device.

Portmon has built-in knowledge of all standard serial and parallel port IOCTLs, which are the primary way that applications and drivers configure and read status information from ports. The IOCTLs are defined in the DDK file \ddk\src\comm\inc\ntddser.h and \ddk\src\comm\inc\ntddpar.h, and some are documented in the DDK.

How it Works: Windows 95 and 98

On Windows 95 and 98, the *Portmon* GUI relies on a dynamically loaded VxD to capture serial and parallel activity. The Windows VCOMM (Virtual Communications) device driver serves as the interface to parallel and serial devices, so applications that access ports indirectly use its services. The *Portmon* VxD uses standard VxD service hooking to intercept all accesses to VCOMM's functions. Like its NT device driver, *Portmon*'s VxD interprets requests to display them in a friendly format. On Windows 95 and 98 *Portmon* monitors all ports so there is no port selection like on NT.

 **Download Portmon (226 KB)**

Run now from Sysinternals Live.

ProcDump v9.0

6 minutes to read • Edit Online

By Mark Russinovich and Andrew Richards

Published: May 16, 2017

Download ProcDump (439 KB)

Download ProcDump for Linux (GitHub)

Introduction

ProcDump is a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that an administrator or developer can use to determine the cause of the spike. ProcDump also includes hung window monitoring (using the same definition of a window hang that Windows and Task Manager use), unhandled exception monitoring and can generate dumps based on the values of system performance counters. It also can serve as a general process dump utility that you can embed in other scripts.

Using ProcDump

usage: procdump [-a] [[-c|-cl CPU usage] [-u] [-s seconds]] [-n exceeds] [-e [1 [-b]] [-f <filter,...>] [-g] [-h] [-l] [-m|-ml commit usage] [-ma | -mp] [-o] [-p|-pl counter threshold] [-r] [-t] [-d <callback DLL>] [-64] <[-w] <process name or service name or PID> [dump file] | -i <dump file> | -u | -x <dump file> <image file> [arguments] >] [-? [-e]

PARAMETER	DESCRIPTION
-a	Avoid outage. Requires -r. If the trigger will cause the target to suspend for a prolonged time due to an exceeded concurrent dump limit, the trigger will be skipped.
-at	Avoid outage at Timeout. Cancel the trigger's collection at N seconds.
-b	Treat debug breakpoints as exceptions (otherwise ignore them).
-c	CPU threshold at which to create a dump of the process.
-cl	CPU threshold below which to create a dump of the process.
-d	Invoke the minidump callback routine named MiniDumpCallbackRoutine of the specified DLL.
-e	Write a dump when the process encounters an unhandled exception. Include the 1 to create dump on first chance exceptions.

PARAMETER	DESCRIPTION
-f	Filter the first chance exceptions. Wildcards (*) are supported. To just display the names without dumping, use a blank ("") filter.
-fx	Filter (exclude) on the content of exceptions and debug logging. Wildcards are supported.
-g	Run as a native debugger in a managed process (no interop).
-h	Write dump if process has a hung window (does not respond to window messages for at least 5 seconds).
-i	Install ProcDump as the AeDebug postmortem debugger. Only -ma, -mp, -d and -r are supported as additional options.
-k	Kill the process after cloning (-r), or at the end of dump collection
-l	Display the debug logging of the process.
-m	Memory commit threshold in MB at which to create a dump.
-ma	Write a dump file with all process memory. The default dump format only includes thread and handle information.
-mc	Write a custom dump file. Include memory defined by the specified MINIDUMP_TYPE mask (Hex).
-md	Write a Callback dump file. Include memory defined by the MiniDumpWriteDump callback routine named MiniDumpCallbackRoutine of the specified DLL.
-mk	Also write a Kernel dump file. Includes the kernel stacks of the threads in the process. OS doesn't support a kernel dump (-mk) when using a clone (-r). When using multiple dump sizes, a kernel dump is taken for each dump size.
-ml	Trigger when memory commit drops below specified MB value.
-mm	Write a mini dump file (default).
-mp	Write a dump file with thread and handle information, and all read/write process memory. To minimize dump size, memory areas larger than 512MB are searched for, and if found, the largest area is excluded. A memory area is the collection of same sized memory allocation areas. The removal of this (cache) memory reduces Exchange and SQL Server dumps by over 90%.
-n	Number of dumps to write before exiting.
-o	Overwrite an existing dump file.

PARAMETER	DESCRIPTION
-p	Trigger on the specified performance counter when the threshold is exceeded. Note: to specify a process counter when there are multiple instances of the process running, use the process ID with the following syntax: "\Process(<name>_<pid>)\counter"
-pl	Trigger when performance counter falls below the specified value.
-r	Dump using a clone. Concurrent limit is optional (default 1, max 5). CAUTION: a high concurrency value may impact system performance. - Windows 7 : Uses Reflection. OS doesn't support -e. - Windows 8.0 : Uses Reflection. OS doesn't support -e. - Windows 8.1+: Uses PSS. All trigger types are supported.
-s	Consecutive seconds before dump is written (default is 10).
-t	Write a dump when the process terminates.
-u	Treat CPU usage relative to a single core (used with -c). As the only option, Uninstalls ProcDump as the postmortem debugger.
-w	Wait for the specified process to launch if it's not running.
-wer	Queue the (largest) dump to Windows Error Reporting.
-x	Launch the specified image with optional arguments. If it is a Store Application or Package, ProcDump will start on the next activation (only).
-64	By default ProcDump will capture a 32-bit dump of a 32-bit process when running on 64-bit Windows. This option overrides to create a 64-bit dump. Only use for WOW64 subsystem debugging.
-?	Use -? -e to see example command lines.

If you omit the dump file name, it defaults to <processname>_<datetime>.dmp.

Use the -accepteula command line option to automatically accept the Sysinternals license agreement.

Automated Termination:
Setting an event with name "procdump-<PID>" is the same as typing Ctrl+C to gracefully terminate ProcDump

Filename:
Default dump filename: PROCESSNAME_YYMMDD_HHMMSS.dmp
The following substitutions are supported:

```
PROCESSNAME     Process Name
Process ID          PID
EXCEPTIONCODE   Exception Code
YYMMDD          Year/Month/Day
HHMMSS          Hour/Minute/Second
```

Examples

Write a mini dump of a process named 'notepad' (only one match can exist):

C:\>procdump notepad

Write a full dump of a process with PID '4572':

C:\>procdump -ma 4572

Write 3 mini dumps 5 seconds apart of a process named 'notepad':

C:\>procdump -s 5 -n 3 notepad

Write up to 3 mini dumps of a process named 'consume' when it exceeds 20% CPU usage for five seconds:

C:\>procdump -c 20 -s 5 -n 3 consume

Write a mini dump for a process named 'hang.exe' when one of it's Windows is unresponsive for more than 5 seconds:

C:\>procdump -h hang.exe hungwindow.dmp

Write a mini dump of a process named 'outlook' when total system CPU usage exceeds 20% for 10 seconds:

C:\>procdump outlook -p "\Processor(_Total)\% Processor Time" 20

Write a full dump of a process named 'outlook' when Outlook's handle count exceeds 10,000:

C:\>procdump -ma outlook -p "\Process(Outlook)\Handle Count" 10000

Write a MiniPlus dump of the Microsoft Exchange Information Store when it has an unhandled exception:

C:\>procdump -mp -e store.exe

Display without writing a dump, the exception codes/names of w3wp.exe:

C:\>procdump -e 1 -f "" w3wp.exe

Write a mini dump of w3wp.exe if an exception's code/name contains 'NotFound':

C:\>procdump -e 1 -f NotFound w3wp.exe

Launch a process and then monitor it for exceptions:

C:\>procdump -e 1 -f "" -x c:\dumps consume.exe

Register for launch, and attempt to activate, a modern 'application'. A new ProcDump instance will start when it activated to monitor for exceptions:

C:\>procdump -e 1 -f "" -x c:\dumpsMicrosoft.BingMaps_8wekyb3d8bbwe!AppexMaps

Register for launch of a modern 'package'. A new ProcDump instance will start when it is (manually) activated to monitor for exceptions:

C:\>procdump -e 1 -f "" -x c:\dumps Microsoft.BingMaps_1.2.0.136_x64__8wekyb3d8bbwe

Register as the Just-in-Time (AeDebug) debugger. Makes full dumps in c:\dumps.

C:\>procdump -ma -i c:\dumps

See a list of example command lines (the examples are listed above):

C:\>procdump -? -e

Related Links

- **Windows Internals Book**
  The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- **Windows Sysinternals Administrator's Reference**
  The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download ProcDump (439 KB)

Download ProcDump for Linux (GitHub)

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Learn More

- Defrag Tools: #9 - ProcDump
  This episode of Defrag Tools covers what the tool captures and expected outage durations
- Defrag Tools: #10 - ProcDump - Triggers
  This episode covers trigger options in particular 1st & 2nd chance exceptions
- Defrag Tools: #11 - ProcDump - Windows 8 & Process Monitor
  This episode covers modern application support and Process Monitor logging support

Process Explorer v16.31

2 minutes to read • Edit Online

By Mark Russinovich

Published: December 18, 2019

Download Process Explorer (1.9 MB)
Run now from Sysinternals Live.

Introduction

Ever wondered which program has a particular file or directory open? Now you can find out. *Process Explorer* shows you information about which handles and DLLs processes have opened or loaded.

The *Process Explorer* display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that *Process Explorer* is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if *Process Explorer* is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. *Process Explorer* also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded.

The unique capabilities of *Process Explorer* make it useful for tracking down DLL-version problems or handle leaks, and provide insight into the way Windows and applications work.

Related Links

- Windows Internals Book
  The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- Windows Sysinternals Administrator's Reference
  The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download

Download Process Explorer (1.9 MB)
Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher (Including IA64).
- Server: Windows Server 2008 and higher (Including IA64).

Installation

Simply run *Process Explorer* (procexp.exe).

The help file describes *Process Explorer* operation and usage. If you have problems or questions please visit the

Process Explorer forum on Technet.

Learn More

Here are some other handle and DLL viewing tools and information available at Sysinternals:

- The case of the Unexplained...
  In this video, Mark describes how he has solved seemingly unsolvable system and application problems on Windows.
- Handle - a command-line handle viewer
- ListDLLs - a command-line DLL viewer
- PsList - local/remote command-line process lister
- PsKill - local/remote command-line process killer
- Defrag Tools: #2 - Process Explorer
  In this episode of Defrag Tools, Andrew Richards and Larry Larsen show how to use Process Explorer to view the details of processes, both at a point in time and historically.
- Windows Sysinternals Primer: Process Explorer, Process Monitor and More
  Process Explorer gets a lot of attention in the first Sysinternals Primer delivered by Aaron Margosis and Tim Reckmeyer at TechEd 2010.

Process Monitor v3.53

2 minutes to read • Edit Online

By Mark Russinovich

Published: December 18, 2019

Download Process Monitor (1.5 MB)
Run now from Sysinternals Live.

Introduction

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Overview of Process Monitor Capabilities

Process Monitor includes powerful monitoring and filtering capabilities, including:

- More data captured for operation input and output parameters
- Non-destructive filters allow you to set filters without losing data
- Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation
- Reliable capture of process details, including image path, command line, user and session ID
- Configurable and moveable columns for any event property
- Filters can be set for any data field, including fields not configured as columns
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data
- Process tree tool shows relationship of all processes referenced in a trace
- Native log format preserves all data for loading in a different Process Monitor instance
- Process tooltip for easy viewing of process image information
- Detail tooltip allows convenient access to formatted data that doesn't fit in the column
- Cancellable search
- Boot time logging of all operations

The best way to become familiar with Process Monitor's features is to read through the help file and then visit each of its menu items and options on a live system.

Screenshots

Related Links

- **Windows Internals Book**

The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.

- **Windows Sysinternals Administrator's Reference**
  The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download

Download Process Monitor (1.5 MB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsExec v2.2

4 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

Utilities like Telnet and remote control programs like Symantec's PC Anywhere let you execute programs on remote systems, but they can be a pain to set up and require that you install client software on the remote systems that you wish to access. PsExec is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. PsExec's most powerful uses include launching interactive command-prompts on remote systems and remote-enabling tools like IpConfig that otherwise do not have the ability to show information about remote systems.

Note: some anti-virus scanners report that one or more of the tools are infected with a "remote admin" virus. None of the PsTools contain viruses, but they have been used by viruses, which is why they trigger virus notifications.

Installation

Just copy PsExec onto your executable path. Typing "psexec" displays its usage syntax.

Using PsExec

See the July 2004 issue of *Windows IT Pro Magazine* for Mark's article that covers advanced usage of PsExec.

Usage: psexec [\\computer[,computer2[,...] | @file\]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-i [session]][-c executable [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]

PARAMETER	DESCRIPTION
-a	Separate processors on which the application can run with commas where 1 is the lowest numbered CPU. For example, to run the application on CPU 2 and CPU 4, enter: "-a 2,4"
-c	Copy the specified executable to the remote system for execution. If you omit this option the application must be in the system path on the remote system.
-d	Don't wait for process to terminate (non-interactive).
-e	Does not load the specified account's profile.
-f	Copy the specified program even if the file already exists on the remote system.

PARAMETER	DESCRIPTION
-i	Run the program so that it interacts with the desktop of the specified session on the remote system. If no session is specified the process runs in the console session.
-h	If the target system is Vista or higher, has the process run with the account's elevated token, if available.
-l	Run process as limited user (strips the Administrators group and allows only privileges assigned to the Users group). On Windows Vista the process runs with Low Integrity.
-n	Specifies timeout in seconds connecting to remote computers.
-p	Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
-r	Specifies the name of the remote service to create or interact with.
-s	Run the remote process in the System account.
-u	Specifies optional user name for login to remote computer.
-v	Copy the specified file only if it has a higher version number or is newer on than the one on the remote system.
-w	Set the working directory of the process (relative to remote computer).
-x	Display the UI on the Winlogon secure desktop (local system only).
-priority	Specifies -low, -belownormal, -abovenormal, -high or -realtime to run the process at a different priority. Use -background to run at low memory and I/O priority on Vista.
computer	Direct PsExec to run the application on the remote computer or computers specified. If you omit the computer name, PsExec runs the application on the local system, and if you specify a wildcard (*), PsExec runs the command on all computers in the current domain.
@file	PsExec will execute the command on each of the computers listed in the file.
cmd	Name of application to execute.
arguments	Arguments to pass (note that file paths must be absolute paths on the target system).
-accepteula	This flag suppresses the display of the license dialog.

You can enclose applications that have spaces in their name with quotation marks e.g.

psexec \\marklap"c:\long name app.exe"

Input is only passed to the remote system when you press the Enter key. Typing Ctrl-C terminates the remote process.

If you omit a user name, the process will run in the context of your account on the remote system, but will not have access to network resources (because it is impersonating). Specify a valid user name in the Domain\User syntax if the remote process requires access to network resources or to run in a different account. Note that the password and command are encrypted in transit to the remote system.

Error codes returned by PsExec are specific to the applications you execute, not PsExec.

Examples

This article I wrote describes how PsExec works and gives tips on how to use it:

The following command launches an interactive command prompt on \\marklap:

psexec \\marklap cmd

This command executes IpConfig on the remote system with the /all switch, and displays the resulting output locally:

psexec \\marklap ipconfig /all

This command copies the program test.exe to the remote system and executes it interactively:

psexec \\marklap -c test.exe

Specify the full path to a program that is already installed on a remote system if its not on the system's path:

psexec \\marklap c:\bin\test.exe

Run Regedit interactively in the System account to view the contents of the SAM and SECURITY keys::

psexec -i -d -s c:\windows\regedit.exe

To run Internet Explorer as with limited-user privileges use this command:

psexec -l -d "c:\program files\internet explorer\iexplore.exe"

 **Download PsTools (2.7 MB)**

PSTools

PsExec is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsGetSid v1.45

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

 **Download PsTools (2.7 MB)**

Introduction

PsGetsid allows you to translate SIDs to their display name and vice versa. It works on builtin accounts, domain accounts, and local accounts.

Installation

Just copy *PsGetSid* onto your executable path, and type "psgetsid".

Usage

Usage: psgetsid [\\computer[,computer[,...] | @file\] [-u username [-p password]]] [account|SID]

PARAMETER	DESCRIPTION
-u	Specifies optional user name for login to remote computer.
-p	Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
Account	PsGetSid will report the SID for the specified user account rather than the computer.
SID	PsGetSid will report the account for the specified SID.
Computer	Direct PsGetSid to perform the command on the remote computer or computers specified. If you omit the computer name PsGetSid runs the command on the local system, and if you specify a wildcard (*), PsGetSid runs the command on all computers in the current domain.
@file	PsGetSid will execute the command on each of the computers listed in the file.

If you want to see a computer's SID just pass the computer's name as a command-line argument. If you want to see a user's SID, name the account (e.g. "administrator") on the command-line and an optional computer name.

Specify a user name if the account you are running from doesn't have administrative privileges on the computer you want to query. If you don't specify a password as an option, *PsGetSid* will prompt you for one so that you can type it in without having it echoed to the display.

 **Download PsTools (2.7 MB)**

PsTools

PsGetSid is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsKill v1.16

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

Windows NT/2000 does not come with a command-line 'kill' utility. You can get one in the Windows NT or Win2K Resource Kit, but the kit's utility can only terminate processes on the local computer. *PsKill* is a kill utility that not only does what the Resource Kit's version does, but can also kill processes on remote systems. You don't even have to install a client on the target computer to use *PsKill* to terminate a remote process.

Installation

Just copy *PsKill* onto your executable path, and type pskill with command-line options defined below.

Using PsKill

See the September 2004 issue of Windows IT Pro Magazine for Mark's article that covers advanced usage of *PsKill*.

Running *PsKill* with a process ID directs it to kill the process of that ID on the local computer. If you specify a process name *PsKill* will kill all processes that have that name.

Usage: pskill [-] [-t] [\\computer [-u username] [-p password]] <process name | process id>

PARAMETER	DESCRIPTION
-	Displays the supported options.
-t	Kill the process and its descendants.
\\computer	Specifies the computer on which the process you want to terminate is executing. The remote computer must be accessible via the NT network neighborhood.
-u username	If you want to kill a process on a remote system and the account you are executing in does not have administrative privileges on the remote system then you must login as an administrator using this command-line option. If you do not include the password with the -p option then *PsKill* will prompt you for the password without echoing your input to the display.
-p password	This option lets you specify the login password on the command line so that you can use PsList from batch files. If you specify an account name and omit the -p option PsList prompts you interactively for a password.

PARAMETER	DESCRIPTION
process id	Specifies the process ID of the process you want to kill.
process name	Specifies the process name of the process or processes you want to kill.

PsKill Microsoft KB Article

This Microsoft KB article references *PsKill*:

810596: PSVR2002: "There Is No Information to Display in This View" Error Message When You Try to Access a Project View

Download PsTools (2.7 MB)

PsTools

PsKill is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsList v1.4

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

PARAMETER	DESCRIPTION
pslist exp	would show statistics for all the processes that start with "exp", which would include Explorer.
-d	Show thread detail.
-m	Show memory detail.
-x	Show processes, memory information and threads.
-t	Show process tree.
-s [n]	Run in task-manager mode, for optional seconds specified. Press Escape to abort.
-r n	Task-manager mode refresh rate in seconds (default is 1).
\\computer	Instead of showing process information for the local system, *PsList* will show information for the NT/Win2K system specified. Include the -u switch with a username and password to login to the remote system if your security credentials do not permit you to obtain performance counter information from the remote system.
-u	username If you want to kill a process on a remote system and the account you are executing in does not have administrative privileges on the remote system then you must login as an administrator using this command-line option. If you do not include the password with the -p option then *PsList* will prompt you for the password without echoing your input to the display.
-p	password This option lets you specify the login password on the command line so that you can use *PsList* from batch files. If you specify an account name and omit the -p option *PsList* prompts you interactively for a password.
name	Show information about processes that begin with the name specified.

PARAMETER	DESCRIPTION
-e	Exact match the process name.
pid	Instead of listing all the running processes in the system, this parameter narrows *PsList's* scan to the process that has the specified PID. Thus: **pslist 53** would dump statistics for the process with the PID 53.

How it Works

Like Windows NT/2K's built-in PerfMon monitoring tool, *PsList* uses the Windows NT/2K performance counters to obtain the information it displays. You can find documentation for Windows NT/2K performance counters, including the source code to Windows NT's built-in performance monitor, PerfMon, in MSDN.

Memory Abbreviation Key

All memory values are displayed in KB.

- **Pri**: Priority
- **Thd**: Number of Threads
- **Hnd**: Number of Handles
- **VM**: Virtual Memory
- **WS**: Working Set
- **Priv**: Private Virtual Memory
- **Priv Pk**: Private Virtual Memory Peak
- **Faults**: Page Faults
- **NonP**: Non-Paged Pool
- **Page**: Paged Pool
- **Cswtch**: Context Switches

Download PsTools (2.7 MB)

PsTools

PsList is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsService v2.25

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

PsService is a service viewer and controller for Windows. Like the SC utility that's included in the Windows NT and Windows 2000 Resource Kits, *PsService* displays the status, configuration, and dependencies of a service, and allows you to start, stop, pause, resume and restart them. Unlike the SC utility, *PsService* enables you to logon to a remote system using a different account, for cases when the account from which you run it doesn't have required permissions on the remote system. *PsService* includes a unique service-search capability, which identifies active instances of a service on your network. You would use the search feature if you wanted to locate systems running DHCP servers, for instance.

Finally, *PsService* works on both NT 4, Windows 2000 and Windows Vista, whereas the Windows 2000 Resource Kit version of SC requires Windows 2000, and *PsService* doesn't require you to manually enter a "resume index" in order to obtain a complete listing of service information.>

Installation

Just copy *PsService* onto your executable path, and type "psservice".

Using PsService

The default behavior of *PsService* is to display the configured services (both running and stopped) on the local system. Entering a command on the command-line invokes a particular feature, and some commands accept options. Typing a command followed by "- " displays information on the syntax for the command.

Usage: psservice [\\computer [-u username] [-p password]] <command> <options>

PARAMETER	DESCRIPTION
query	Displays the status of a service.
config	Displays the configuration of a service.
setconfig	Sets the start type (disabled, auto, demand) of a service.
start	Starts a service.
stop	Stops a service.
restart	Stops and then restarts a service.
pause	Pauses a service

PARAMETER	DESCRIPTION
cont	Resumes a paused service.
depend	Lists the services dependent on the one specified.
security	Dumps the service's security descriptor.
find	Searches the network for the specified service.
\\computer	Targets the NT/Win2K system specified. Include the -u switch with a username and password to login to the remote system if your security credentials do not permit you to obtain performance counter information from the remote system. If you specify the -u option, but not a password with the -p option, *PsService* will prompt you to enter the password and will not echo it to the screen.

How it Works

PsService uses the Service Control Manager APIs that are documented in the Platform SDK.

 Download PsTools (2.7 MB)

PsTools

PsService is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsSuspend v1.07

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

PsSuspend lets you suspend processes on the local or a remote system, which is desirable in cases where a process is consuming a resource (e.g. network, CPU or disk) that you want to allow different processes to use. Rather than kill the process that's consuming the resource, suspending permits you to let it continue operation at some later point in time.

Installation

Copy *PsSuspend* onto your executable path and type "pssuspend" with command-line options defined below.

Using PsSuspend

Running *PsSuspend* with a process ID directs it to suspend or resume the process of that ID on the local computer. If you specify a process name *PsSuspend* will suspend or resume all processes that have that name. Specify the -r switch to resume suspended processes.

Usage: pssuspend [-] [-r] [\\computer [-u username] [-p password]] <process name | process id>

PARAMETER	DESCRIPTION
-	Displays the supported options.
-r	Resumes the specified processes specified if they are suspended.
\\computer	Specifies the computer on which the process you want to suspend or resume is executing. The remote computer must be accessible via the NT network neighborhood.
-u username	If you want to suspend a process on a remote system and the account you are executing in does not have administrative privileges on the remote system then you must login as an administrator using this command-line option. If you do not include the password with the -p option then *PsSuspend* will prompt you for the password without echoing your input to the display.
-p password	This option lets you specify the login password on the command line so that you can use *PsSuspend* from batch files. If you specify an account name and omit the -p option *PsSuspend* prompts you interactively for a password.

PARAMETER	DESCRIPTION
process id	Specifies the process ID of the process you want to suspend or resume.
process name	Specifies the process name of the process or processes you want to suspend or resume.

PsSuspend is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

 Download PsTools (2.7 MB)

PsTools

PsSuspend is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsTools

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download PsTools Suite (2.7 MB)

Introduction

The Windows NT and Windows 2000 Resource Kits come with a number of command-line tools that help you administer your Windows NT/2K systems. Over time, I've grown a collection of similar tools, including some not included in the Resource Kits. What sets these tools apart is that they all allow you to manage remote systems as well as the local one. The first tool in the suite was PsList, a tool that lets you view detailed information about processes, and the suite is continually growing. The "Ps" prefix in PsList relates to the fact that the standard UNIX process listing command-line tool is named "ps", so I've adopted this prefix for all the tools in order to tie them together into a suite of tools named *PsTools*.

> Some anti-virus scanners report that one or more of the tools are infected with a "remote admin" virus. None of the PsTools contain viruses, but they have been used by viruses, which is why they trigger virus notifications.*

The tools included in the *PsTools* suite, which are downloadable as a package, are:

- *PsExec* - execute processes remotely
- *PsFile* - shows files opened remotely
- *PsGetSid* - display the SID of a computer or a user
- *PsInfo* - list information about a system
- *PsPing* - measure network performance
- *PsKill* - kill processes by name or process ID
- *PsList* - list detailed information about processes
- *PsLoggedOn* - see who's logged on locally and via resource sharing (full source is included)
- *PsLogList* - dump event log records
- *PsPasswd* - changes account passwords
- *PsService* - view and control services
- *PsShutdown* - shuts down and optionally reboots a computer
- *PsSuspend* - suspends processes
- *PsUptime* - shows you how long a system has been running since its last reboot (PsUptime's functionality has been incorporated into *PsInfo*

The *PsTools* download package includes an HTML help file with complete usage information for all the tools.

Download PsTools Suite (2.7 MB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Installation

None of the tools requires any special installation. You don't even need to install any client software on the remote computers at which you target them. Run them by typing their name and any command-line options you want. To show complete usage information, specify the "-? " command-line option. If you have questions or problems, please visit the Sysinternals PsTools Forum.

Related Links

Introduction to the PsTools: Wes Miller gives a high-level overview of the Sysinternals PsTools in the March column of his TechNet Magazine column.

ShellRunas v1.01

2 minutes to read • Edit Online

By Mark Russinovich and Jon Schwartz

Published: February 28, 2008

Download ShellRunas (50 KB)

Introduction

The command-line Runas utility is handy for launching programs under different accounts, but it's not convenient if you're a heavy Explorer user. ShellRunas provides functionality similar to that of Runas to launch programs as a different user via a convenient shell context-menu entry.

Screenshot

Using ShellRunas

Usage:

shellrunas /reg [/quiet]
shellrunas /regnetonly [/quiet]
shellrunas /unreg [/quiet]
shellrunas [/netonly] <*program*> [*arguments*]

PARAMETER	DESCRIPTION
/reg	Registers ShellRunas shell context-menu entry
/regnetonly	Registers Shell /netonly context-menu entry **Note:** a command prompt will flash when the program starts
/unreg	Unregisters ShellRunas shell context-menu entry
/quiet	Register or unregisters ShellRunas shell context-menu entry without result dialog
/netonly	Use if specified credentials are for remote access only
<program>	Runs program with specified credentials and parameters

Download ShellRunas (50 KB)

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Getting Help

If you have problems or questions, please visit the Sysinternals Forum.

VMMap v3.26

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 11, 2018

Download VMMap (626 KB)
Run now from Sysinternals Live.

Introduction

VMMap is a process virtual and physical memory analysis utility. It shows a breakdown of a process's committed virtual memory types as well as the amount of physical memory (working set) assigned by the operating system to those types. Besides graphical representations of memory usage, VMMap also shows summary information and a detailed process memory map. Powerful filtering and refresh capabilities allow you to identify the sources of process memory usage and the memory cost of application features.

Besides flexible views for analyzing live processes, VMMap supports the export of data in multiple forms, including a native format that preserves all the information so that you can load back in. It also includes command-line options that enable scripting scenarios.

VMMap is the ideal tool for developers wanting to understand and optimize their application's memory resource usage.

Screenshot

Related Links

- **Windows Internals Book**
  The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- **Windows Sysinternals Administrator's Reference** The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download VMMap (586 KB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Getting Help

If you have problems or questions, please visit the Sysinternals Forum.

Learn More

- Defrag Tools: #7 - VMMap
  In this episode of Defrag Tools, Andrew Richards and Larry Larsen cover how to use VMMap to see how Virtual Memory is being used and if there have been any memory leaks.

Sysinternals Security Utilities

2 minutes to read • Edit Online

AccessChk

This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services.

AccessEnum

This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

Autologon

Bypass password screen during logon.

Autoruns

See what programs are configured to startup automatically when your system boots and you log in. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

LogonSessions

List active logon sessions

Process Explorer

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

PsExec

Execute processes with limited-user rights.

PsLoggedOn

Show users logged on to a system.

PsLogList

Dump event log records.

PsTools

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

Rootkit Revealer

RootkitRevealer is an advanced rootkit detection utility.

SDelete

Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

ShareEnum

Scan file shares on your network and view their security settings to close security holes.

ShellRunas

Launch programs as a different user via a convenient shell context-menu entry.

Sigcheck

Dump file version information and verify that images on your system are digitally signed.

Sysmon

Monitors and reports key system activity via the Windows event log.

Autologon v3.10

2 minutes to read • Edit Online

By Mark Russinovich

Published: August 29, 2016

Download Autologon (70 KB)
Run now from Sysinternals Live.

Introduction

Autologon enables you to easily configure Windows' built-in autologon mechanism. Instead of waiting for a user to enter their name and password, Windows uses the credentials you enter with Autologon, which are encrypted in the Registry, to log on the specified user automatically.

Autologon is easy enough to use. Just run autologon.exe, fill in the dialog, and hit Enable. To turn off auto-logon, hit *Disable*. Also, if the shift key is held down before the system performs an autologon, the autologon will be disabled for that logon. You can also pass the username, domain and password as command-line arguments:

autologon user domain password

Note: When Exchange Activesync password restrictions are in place, Windows will not process the autologon configuration.

Download Autologon (70 KB)
Run now from Sysinternals Live.

LogonSessions v1.4

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download LogonSessions (237 KB)

Introduction

If you think that when you logon to a system there's only one active logon session, this utility will surprise you. It lists the currently active logon sessions and, if you specify the -p option, the processes running in each session.

Usage: logonsessions [-c[t]] [-p]

PARAMETER	DESCRIPTION
-c	Print output as CSV.
-ct	Print output as tab-delimited values.
-p	List processes running in logon session.

Example output

```
C:\>logonsessions -p

[13] Logon session 00000000:6a6d6160:
    User name:    NTDEV\markruss
    Auth package: Kerberos
    Logon type:   RemoteInteractive
    Session:      1
    Sid:          S-1-5-21-397955417-626881126-188441444-3615555
    Logon time:   7/2/2015 6:05:31 PM
    Logon server: NTDEV-99
    DNS Domain:   NTDEV.CORP.MICROSOFT.COM
    UPN:          markruss@ntdev.microsoft.com
    15368: ProcExp.exe
    17528: ProcExp64.exe
    13116: cmd.exe
    17100: conhost.exe
     6716: logonsessions.exe
```

Download LogonSessions (237 KB)

Runs on:

- Client: Windows Vista (32-bit)and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

NewSID v4.10

By Mark Russinovich

Published: November 1, 2006

Note: NewSID has been retired and is no longer available for download. Please see Mark Russinovich's blog post: NewSID Retirement and the Machine SID Duplication Myth

IMPORTANT:

Regarding SIDs, Microsoft does not support images that are prepared using NewSID, we only support images that are prepared using SysPrep. Microsoft has not tested NewSID for all deployment cloning options.

For more information on Microsoft's official policy, please see the following Knowledge Base article:

- **The Microsoft policy concerning disk duplication of Windows XP installations**

Introduction

Many organizations use disk image cloning to perform mass rollouts of Windows. This technique involves copying the disks of a fully installed and configured Windows computer onto the disk drives of other computers. These other computers effectively appear to have been through the same install process, and are immediately available for use.

While this method saves hours of work and hassle over other rollout approaches, it has the major problem that every cloned system has an identical Computer Security Identifier (SID). This fact compromises security in Workgroup environments, and removable media security can also be compromised in networks with multiple identical computer SIDs.

Demand from the Windows community has lead several companies to develop programs that can change a computer's SID after a system has been cloned. However, Symantec's SID Changer andSymantec's Ghost Walker are only sold as part of each company's high-end product. Further, they both run from a DOS command prompt (Altiris' changer is similar to *NewSID*).

NewSID is a program we developed that changes a computer's SID. It is free and is a Win32 program, meaning that it can easily be run on systems that have been previously cloned.

Please read this entire article before you use this program.

Version Information:

- Version 4.0 introduces support for Windows XP and .NET Server, a wizard-style interface, allows you to specify the SID that you want applied, Registry compaction and also the option to rename a computer (which results in a change of both NetBIOS and DNS names).
- Version 3.02 corrects a bug where NewSid would not correctly copy default values with invalid value types when renaming a key with an old SID to a new SID. NT actually makes use of such invalid values at certain times in the SAM. The symptom of this bug was error messages reporting access denied when account information was updated by an authorized user.
- Version 3.01 adds a work-around for an inaccessible Registry key that is created by Microsoft Transaction Server. Without the work-around *NewSID* would quit prematurely.
- Version 3.0 introduces a SID-sync feature that directs *NewSID* to obtain a SID to apply from another computer.

- Version 2.0 has an automated-mode option, and let's you change the computer name as well.
- Version 1.2 fixes a bug in that was introduced in 1.1 where some file system security descriptors were not updated.
- Version 1.1 corrects a relatively minor bug that affected only certain installations. It also has been updated to change SIDs associated with the permission settings of file and printer shares.

Cloning and Alternate Rollout Methods

One of the most popular ways of performing mass Windows rollouts (typically hundreds of computers) in corporate environments is based on the technique of disk cloning. A system administrator installs the base operating system and add-on software used in the company on a template computer. After configuring the machine for operation in the company network, automated disk or system duplication tools (such as Symantec's*Ghost*, PowerQuest's*Image Drive*, and Altiris'*RapiDeploy*) are used to copy the template computer's drives onto tens or hundreds of computers. These clones are then given final tweaks, such as the assignment of unique names, and then used by company employees.

Another popular way of rolling out is by using the Microsoft *sysdiff* utility (part of the Windows Resource Kit). This tool requires that the system administrator perform a full install (usually a scripted unattended installation) on each computer, and then *sysdiff* automates the application of add-on software install images.

Because the installation is skipped, and because disk sector copying is more efficient than file copying, a cloned-based rollout can save dozens of hours over a comparable sysdiff install. In addition, the system administrator does not have to learn how to use unattended install or *sysdiff*, or create and debug install scripts. This alone saves hours of work.

The SID Duplication Problem

The problem with cloning is that it is only supported by Microsoft in a very limited sense. Microsoft has stated that cloning systems is only supported if it is done before the GUI portion of Windows Setup has been reached. When the install reaches this point the computer is assigned a name and a unique computer SID. If a system is cloned after this step the cloned machines will all have identical computer SIDs. Note that just changing the computer name or adding the computer to a different domain does not change the computer SID. Changing the name or domain only changes the domain SID if the computer was previously associated with a domain.

To understand the problem that cloning can cause, it is first necessary to understand how individual local accounts on a computer are assigned SIDs. The SIDs of local accounts consist of the computer's SID and an appended RID (Relative Identifier). The RID starts at a fixed value, and is increased by one for each account created. This means that the second account on one computer, for example, will be given the same RID as the second account on a clone. The result is that both accounts have the same SID.

Duplicate SIDs aren't an issue in a Domain-based environment since domain accounts have SID's based on the Domain SID. But, according to Microsoft Knowledge Base article Q162001, "Do Not Disk Duplicate Installed Versions of Windows NT", in a Workgroup environment security is based on local account SIDs. Thus, if two computers have users with the same SID, the Workgroup will not be able to distinguish between the users. All resources, including files and Registry keys, that one user has access to, the other will as well.

Another instance where duplicate SIDs can cause problems is where there is removable media formatted with NTFS, and local account security attributes are applied to files and directories. If such a media is moved to a different computer that has the same SID, then local accounts that otherwise would not be able to access the files might be able to if their account IDs happened to match those in the security attributes. This is not be possible if computers have different SIDs.

An article Mark has written, entitled "*NT Rollout Options,*" was published in the June issue of *Windows NT Magazine*. It discusses the duplicate SID issue in more detail, and presents Microsoft's official stance on cloning. To see if you have a duplicate SID issue on your network, use PsGetSid to display machine SIDs.

NewSID

NewSID is a program we developed to change a computer's SID. It first generates a random SID for the computer, and proceeds to update instances of the existing computer SID it finds in the Registry and in file security descriptors, replacing occurrences with the new SID. *NewSID* requires administrative privileges to run. It has two functions: changing the SID, and changing the computer name.

To use *NewSID's* auto-run option, specify "/a" on the command line. You can also direct it to automatically change the computer's name by including the new name after the "/a" switch. For example:

newsid /a [newname]

Would have *NewSID* run without prompting, change the computer name to "newname" and have it reboot the computer if everything goes okay.

Note: If the system on which you wish to run *NewSID* is running IISAdmin you must stop the IISAdmin service before running *NewSID*. Use this command to stop the IISAdmin service: net stop iisadmin /y

NewSID's SID-synchronizing feature that allows you to specify that, instead of randomly generating one, the new SID should be obtained from a different computer. This functionality makes it possible to move a Backup Domain Controller (BDC) to a new Domain, since a BDC's relationship to a Domain is identified by it having the same computer SID as the other Domain Controllers (DCs). Simply choose the "Synchronize SID" button and enter the target computer's name. You must have permissions to change the security settings of the target computer's Registry keys, which typically means that you must be logged in as a domain administrator to use this feature.

Note that when you run *NewSID* that the size of the Registry will grow, so make sure that the maximum Registry size will accommodate growth. We have found that this growth has no perceptible impact on system performance. The reason the Registry grows is that it becomes fragmented as temporary security settings are applied by *NewSID*. When the settings are removed the Registry is not compacted.

Important: Note that while we have thoroughly tested *NewSID*, you must use it at your own risk. As with any software that changes file and Registry settings, it is highly recommended that you completely back-up your computer before running *NewSID*.

Moving a BDC

Here are the steps you should follow when you want to move a BDC from one domain to another:

1. Boot up the BDC you want to move and log in. Use *NewSID* to synchronize the SID of the BDC with the PDC of the domain to which you wish to move the BDC.
2. Reboot the system for which you changed the SID (the BDC). Since the domain the BDC is now associated with already has an active PDC, it will boot as a BDC in its new domain.
3. The BDC will show up as a workstation in Server Manager, so use the "Add to Domain" button to add the BDC to its new domain. Be sure to specify the BDC radio button when adding.

How it Works

NewSID starts by reading the existing computer SID. A computer's SID is stored in the Registry's **SECURITY** hive under **SECURITY\SAM\Domains\Account**. This key has a value named F and a value named V. The V value is a binary value that has the computer SID embedded within it at the end of its data. *NewSID* ensures that this SID is in a standard format (3 32-bit subauthorities preceded by three 32-bit authority fields).

Next, *NewSID* generates a new random SID for the computer. *NewSID*'s generation takes great pains to create a truly random 96-bit value, which replaces the 96-bits of the 3 subauthority values that make up a computer SID.

Three phases to the computer SID replacement follow. In the first phase, the **SECURITY** and **SAM** Registry hives are scanned for occurrences of the old computer SID in key values, as well as the names of the keys. When the SID

is found in a value it is replaced with the new computer SID, and when the SID is found in a name, the key and its subkeys are copied to a new subkey that has the same name except with the new SID replacing the old.

The final two phases involve updating security descriptors. Registry keys and NTFS files have security associated with them. Security descriptors consist of an entry that identifies which account owns the resource, which group is the primary group owner, an optional list of entries that specify actions permitted by users or groups (known as the Discretionary Access Control List - DACL), and an optional list of entries that specify which actions performed by certain users or groups will generate entries in the system Event Log (System Access Control List - SACL). A user or a group is identified in these security descriptors with their SIDs, and as I stated earlier, local user accounts (other than the built-in accounts such as Administrator, Guest, and so on) have their SIDs made up of the computer SID plus a RID.

The first part of security descriptor updates occurs on all NTFS file system files on the computer. Every security descriptor is scanned for occurrences of the computer SID. When *NewSID* finds one, it replaces it with the new computer SID.

The second part of security descriptor updates is performed on the Registry. First, *NewSID* must make sure that it scans all hives, not just those that are loaded. Every user account has a Registry hive that is loaded as **HKEY_CURRENT_USER** when the user is logged in, but remains on disk in the user's profile directory when they are not. *NewSID* identifies the locations of all user hive locations by enumerating the **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList** key, which points at the directories in which they are stored. It then loads them into the Registry using RegLoadKey under **HKEY_LOCAL_MACHINE** and scans the entire Registry, examining each security descriptor in search of the old computer SID. Updates are performed the same as for files, and when its done *NewSID* unloads the user hives it loaded. As a final step *NewSID* scans the **HKEY_USERS** key, which contains the hive of the currently logged-in user as well as the .Default hive. This is necessary because a hive can't be loaded twice, so the logged-in user hive won't be loaded into **HKEY_LOCAL_MACHINE** when *NewSID* is loading other user hives.

Finally, *NewSID* must update the **ProfileList** subkeys to refer to the new account SIDs. This step is necessary to have Windows NT correctly associate profiles with the user accounts after the account SIDs are changed to reflect the new computer SID.

NewSID ensures that it can access and modify every file and Registry key in the system by giving itself the following privileges: System, Backup, Restore and Take Ownership.

PsLoggedOn v1.35

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

You can determine who is using resources on your local computer with the "net" command ("net session"), however, there is no built-in way to determine who is using the resources of a remote computer. In addition, NT comes with no tools to see who is logged onto a computer, either locally or remotely. *PsLoggedOn* is an applet that displays both the locally logged on users and users logged on via resources for either the local computer, or a remote one. If you specify a user name instead of a computer, *PsLoggedOn* searches the computers in the network neighborhood and tells you if the user is currently logged on.

PsLoggedOn's definition of a locally logged on user is one that has their profile loaded into the Registry, so *PsLoggedOn* determines who is logged on by scanning the keys under the HKEY_USERS key. For each key that has a name that is a user SID (security Identifier), *PsLoggedOn* looks up the corresponding user name and displays it. To determine who is logged onto a computer via resource shares, *PsLoggedOn* uses the *NetSessionEnum* API. Note that *PsLoggedOn* will show you as logged on via resource share to remote computers that you query because a logon is required for *PsLoggedOn* to access the Registry of a remote system.

Installation

Just copy *PsLoggedOn* onto your executable path, and type "psloggedon".

Using PsLoggedOn

Usage: psloggedon [-] [-l] [-x] [\\computername | username]

PARAMETER	DESCRIPTION
-	Displays the supported options and the units of measurement used for output values.
-l	Shows only local logons instead of both local and network resource logons.
-x	Don't show logon times.
\\computername	Specifies the name of the computer for which to list logon information.
username	If you specify a user name *PsLoggedOn* searches the network for computers to which that user is logged on. This is useful if you want to ensure that a particular user is not logged on when you are about to change their user profile configuration.

Download PsTools (2.7 MB)

PsTools

PsLoggedOn is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsLogList v2.81

2 minutes to read • Edit Online

By Mark Russinovich

Published: March 05, 2019

Download PsTools (2.7 MB)

Introduction

The Resource Kit comes with a utility, elogdump, that lets you dump the contents of an Event Log on the local or a remote computer. *PsLogList* is a clone of elogdump except that *PsLogList* lets you login to remote systems in situations your current set of security credentials would not permit access to the Event Log, and *PsLogList* retrieves message strings from the computer on which the event log you view resides.

Installation

Just copy *PsLogList* onto your executable path, and type "psloglist".

Using PsLogList

The default behavior of *PsLogList* is to show the contents of the System Event Log on the local computer, with visually-friendly formatting of Event Log records. Command line options let you view logs on different computers, use a different account to view a log, or to have the output formatted in a string-search friendly way.

usage: psloglist [-] [\\computer[,computer[,...] | @file [-u username [-p password]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w][-c][-x][-r][-a mm/dd/yy][-b mm/dd/yy][-f filter] [-i ID[,ID[,...] | -e ID[,ID[,...]]] [-o event source[,event source][,..]]] [-q event source[,event source][,..]]] [-l event log file] <eventlog>

PARAMETER	DESCRIPTION
@file	Execute the command on each of the computers listed in the file.
-a	Dump records timestamped after specified date.
-b	Dump records timestamped before specified date.
-c	Clear the event log after displaying.
-d	Only display records from previous n days.
-c	Clear the event log after displaying.
-e	Exclude events with the specified ID or IDs (up to 10).
-f	Filter event types with filter string (e.g. "-f w" to filter warnings).
-h	Only display records from previous n hours.

PARAMETER	DESCRIPTION
-i	Show only events with the specified ID or IDs (up to 10).
-l	Dump records from the specified event log file.
-m	Only display records from previous n minutes.
-n	Only display the number of most recent entries specified.
-o	Show only records from the specified event source (e.g. \"-o cdrom\").
-p	Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
-q	Omit records from the specified event source or sources (e.g. \"-q cdrom\").
-r	SDump log from least recent to most recent.
-s	This switch has *PsLogList* print Event Log records one-per-line, with comma delimited fields. This format is convenient for text searches, e.g. psloglist
-t	The default delimeter is a comma, but can be overriden with the specified character.
-u	Specifies optional user name for login to remote computer.
-w	Wait for new events, dumping them as they generate (local system only).
-x	Dump extended data
eventlog	eventlog

How it Works

Like Win NT/2K's built-in Event Viewer and the Resource Kit's elogdump, *PsLogList* uses the Event Log API, which is documented in Windows Platform SDK. *PsLogList* loads message source modules on the system where the event log being viewed resides so that it correctly displays event log messages.

Download PsTools (2.7 MB)

PsTools
PsLogList is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

RootkitRevealer v1.71

10 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download RootkitRevealer (231 KB)
Run now from Sysinternals Live.

Introduction

RootkitRevealer is an advanced rootkit detection utility. It runs on Windows XP (32-bit) and Windows Server 2003 (32-bit), and its output lists Registry and file system API discrepancies that may indicate the presence of a user-mode or kernel-mode rootkit. RootkitRevealer successfully detects many persistent rootkits including AFX, Vanquish and HackerDefender (note: RootkitRevealer is not intended to detect rootkits like Fu that don't attempt to hide their files or registry keys). If you use it to identify the presence of a rootkit please let us know!

The reason that there is no longer a command-line version is that malware authors have started targetting RootkitRevealer's scan by using its executable name. We've therefore updated RootkitRevealer to execute its scan from a randomly named copy of itself that runs as a Windows service. This type of execution is not conducive to a command-line interface. Note that you can use command-line options to execute an automatic scan with results logged to a file, which is the equivalent of the command-line version's behavior.

What is a Rootkit?

The term rootkit is used to describe the mechanisms and techniques whereby malware, including viruses, spyware, and trojans, attempt to hide their presence from spyware blockers, antivirus, and system management utilities. There are several rootkit classifications depending on whether the malware survives reboot and whether it executes in user mode or kernel mode.

Persistent Rootkits
A persistent rootkit is one associated with malware that activates each time the system boots. Because such malware contain code that must be executed automatically each system start or when a user logs in, they must store code in a persistent store, such as the Registry or file system, and configure a method by which the code executes without user intervention.

Memory-Based Rootkits
Memory-based rootkits are malware that has no persistent code and therefore does not survive a reboot.

User-mode Rootkits
There are many methods by which rootkits attempt to evade detection. For example, a user-mode rootkit might intercept all calls to the Windows FindFirstFile/FindNextFile APIs, which are used by file system exploration utilities, including Explorer and the command prompt, to enumerate the contents of file system directories. When an application performs a directory listing that would otherwise return results that contain entries identifying the files associated with the rootkit, the rootkit intercepts and modifies the output to remove the entries.

The Windows native API serves as the interface between user-mode clients and kernel-mode services and more sophisticated user-mode rootkits intercept file system, Registry, and process enumeration functions of the Native API. This prevents their detection by scanners that compare the results of a Windows API enumeration with that returned by a native API enumeration.

Kernel-mode Rootkits
Kernel-mode rootkits can be even more powerful since, not only can they intercept the native API in kernel-mode, but they can also directly manipulate kernel-mode data structures. A common technique for hiding the presence of a malware process is to remove the process from the kernel's list of active processes. Since process management APIs rely on the contents of the list, the malware process will not display in process management tools like Task Manager or Process Explorer.

How RootkitRevealer Works

Since persistent rootkits work by changing API results so that a system view using APIs differs from the actual view in storage, RootkitRevealer compares the results of a system scan at the highest level with that at the lowest level. The highest level is the Windows API and the lowest level is the raw contents of a file system volume or Registry hive (a hive file is the Registry's on-disk storage format). Thus, rootkits, whether user mode or kernel mode, that manipulate the Windows API or native API to remove their presence from a directory listing, for example, will be seen by RootkitRevealer as a discrepancy between the information returned by the Windows API and that seen in the raw scan of a FAT or NTFS volume's file system structures.

Can a Rootkit hide from RootkitRevealer
It is theoretically possible for a rootkit to hide from RootkitRevealer. Doing so would require intercepting RootkitRevealer's reads of Registry hive data or file system data and changing the contents of the data such that the rootkit's Registry data or files are not present. However, this would require a level of sophistication not seen in rootkits to date. Changes to the data would require both an intimate knowledge of the NTFS, FAT and Registry hive formats, plus the ability to change data structures such that they hide the rootkit, but do not cause inconsistent or invalid structures or side-effect discrepancies that would be flagged by RootkitRevealer.

Is there a sure-fire way to know of a rootkit's presence
In general, not from within a running system. A kernel-mode rootkit can control any aspect of a system's behavior so information returned by any API, including the raw reads of Registry hive and file system data performed by RootkitRevealer, can be compromised. While comparing an on-line scan of a system and an off-line scan from a secure environment such as a boot into an CD-based operating system installation is more reliable, rootkits can target such tools to evade detection by even them.

The bottom line is that there will never be a universal rootkit scanner, but the most powerful scanners will be on-line/off-line comparison scanners that integrate with antivirus.

Using RootkitRevealer

RootkitRevealer requires that the account from which its run has assigned to it the Backup files and directories, Load drivers and Perform volume maintenance tasks (on Windows XP and higher) privileges. The Administrators group is assigned these privileges by default. In order to minimize false positives run RootkitRevealer on an idle system.

For best results exit all applications and keep the system otherwise idle during the RootkitRevealer scanning process.

If you have questions or problems please visit the Sysinternals RootkitRevealer Forum.

Manual Scanning

To scan a system launch it on the system and press the Scan button. RootkitRevealer scans the system reporting its actions in a status area at the bottom of its window and noting discrepancies in the output list. The options you can configure:

- **Hide NTFS Metadata Files:** this option is on by default and has RootkitRevealer not show standard NTFS metadata files, which are hidden from the Windows API.

- **Scan Registry:** this option is on by default. Deselecting it has RootkitRevealer not perform a Registry scan.

Launching an Automatic Scan

RootkitRevealer supports several options for auto-scanning systems:

Usage: rootkitrevealer [-a [-c] [-m] [-r] outputfile]

PARAMETER	DESCRIPTION
-a	Automatically scan and exit when done.
-c	Format output as CSV.
-m	Show NTFS metadata files.
-r	Don't scan the Registry.

Note that the file output location must be on a local volume.

If you specify the -c option it does not report progress and discrepancies are printed in CSV format for easy import into a database. You can perform scans of remote systems by executing it with the Sysinternals PsExec utility using a command-line like the following:

psexec \\remote -c rootkitrevealer.exe -a c:\windows\system32\rootkit.log

Interpreting the Output

This is a screenshot of RootkitRevealer detecting the presence of the popular HackerDefender rootkit. The Registry key discrepancies show that the Registry keys storing HackerDefender's device driver and service settings are not visible to the Windows API, but are present in the raw scan of the Registry hive data. Similarly, the HackerDefender-associated files are not visible to Windows API directory scans, but are present in the scan of the raw file system data.

You should examine all discrepancies and determine the likelihood that they indicate the presence of a rootkit. Unfortunately, there is no definitive way to determine, based on the output, if a rootkit is present, but you should examine all reported discrepancies to ensure that they are explainable. If you determine that you have a rootkit installed, search the web for removal instructions. If you are unsure as to how to remove a rootkit you should reformat the system's hard disk and reinstall Windows.

In addition to the information below on possible RootkitRevealer discrepancies, the RootkitRevealer Forum at Sysinternals discusses detected rootkits and specific false-positives.

Hidden from Windows API

These discrepancies are the ones exhibited by most rootkits; however, if you haven't checked the Hide NTFS metadata files you should expect to see a number of such entries on any NTFS volume, since NTFS hides its metada files, such as $MFT and $Secure, from the Windows API. The metadata files present on NTFS volumes vary by version of NTFS and the NTFS features that have been enabled on the volume. There are also antivirus products, such as Kaspersky Antivirus, that use rootkit techniques to hide data they store in NTFS alternate data streams. If you are running such a virus scanner you'll see a Hidden from Windows API discrepancy for an alternate data stream on every NTFS file. RootkitRevealer does not support output filters because rootkits can take advantage of any filtering. Finally, if a file is deleted during a scan you may also see this discrepancy.

This is a list of NTFS metadata files defined as of Windows Server 2003:

- $AttrDef
- $BadClus
- $BadClus:$Bad
- $BitMap
- $Boot
- $LogFile
- $Mft
- $MftMirr
- $Secure
- $UpCase
- $Volume
- $Extend
- $Extend\$Reparse
- $Extend\$ObjId
- $Extend\$UsnJrnl
- $Extend\$UsnJrnl:$Max
- $Extend\$Quota

Access is Denied.
RootkitRevealer should never report this discrepancy since it uses mechanisms that allow it to access any file, directory, or registry key on a system.

Visible in Windows API, directory index, but not in MFT.
Visible in Windows API, but not in MFT or directory index.
Visible in Windows API, MFT, but not in directory index.
Visible in directory index, but not Windows API or MFT.

A file system scan consists of three components: the Windows API, the NTFS Master File Table (MFT), and the NTFS on-disk directory index structures. These discrepancies indicate that a file appears in only one or two of the scans. A common reason is that a file is either created or deleted during the scans. This is an example of RootkitRevealer's discrepancy report for a file created during the scanning:

C:\newfile.txt
3/1/2005 5:26 PM
8 bytes
Visible in Windows API, but not in MFT or directory index.

Windows API length not consistent with raw hive data.
Rootkits can attempt to hide themselves by misrepresenting the size of a Registry value so that its contents aren't visible to the Windows API. You should examine any such discrepancy, though it may also appear as a result of Registry values that change during a scan.

Type mismatch between Windows API and raw hive data.
Registry values have a type, such as DWORD and REG_SZ, and this discrepancy notes that the type of a value as reported through the Windows API differs from that of the raw hive data. A rootkit can mask its data by storing it as a REG_BINARY value, for example, and making the Windows API believe it to be a REG_SZ value; if it stores a 0 at the start of the data the Windows API will not be able to access subsequent data.

Key name contains embedded nulls.
The Windows API treats key names as null-terminated strings, whereas the kernel treats them as counted strings. Thus, it is possible to create Registry keys that are visible to the operating system, yet only partially visible to Registry tools like Regedit. The Reghide sample code at Sysinternals demonstrates this technique, which is used by

both malware and rootkits to hide Registry data. Use the Sysinternals RegDelNull utility to delete keys with embedded nulls.

Data mismatch between Windows API and raw hive data.
This discrepancy will occur if a Registry value is updated while the Registry scan is in progress. Values that change frequently include timestamps such as the Microsoft SQL Server uptime value, shown below, and virus scanner "last scan" values. You should investigate any reported value to ensure that its a valid application or system Registry value.

HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\RECOVERYMANAGER\MSSQLServer\uptime_time_utc
3/1/2005 4:33 PM
8 bytes

Rootkit Resources

The following Web sites and books are sources of more information on rootkits:

Sony, Rootkits and Digital Rights Management Gone Too Far
Read Mark's blog entry on his discovery and analysis of a Sony rootkit on one of his computers.

Unearthing Rootkits
Mark's June *Windows IT Pro Magazine* article provides an overview of rootkit technologies and how RootkitRevealer works.

Rootkits: Subverting the Windows Kernel
This book by Greg Hoglund and Jamie Butler is the most comprehensive treatment of rootkits available.

www.phrack.org
This site stores the archive of *Phrack*, a cracker-oriented magazine where developers discuss flaws in security-related products, rootkit techniques, and other malware tricks.

The Art of Computer Virus Research and Defense, by Peter Szor

Malware: Fighting Malicious Code, by Ed Skoudis and Lenny Zeltser

Windows Internals, 4th Edition, by Mark Russinovich and Dave Solomon (the book doesn't talk about rootkits, but understanding the Windows architecture is helpful to understanding rootkits).

Download RootkitRevealer (231 KB)

Run now from Sysinternals Live.

Sysmon v10.42

13 minutes to read • Edit Online

By Mark Russinovich and Thomas Garnier

Published: December 11, 2019

Download Sysmon (1.7 MB)

Introduction

System Monitor (*Sysmon*) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Note that *Sysmon* does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

Overview of Sysmon Capabilities

Sysmon includes the following capabilities:

- Logs process creation with full command line for both current and parent processes.
- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- Multiple hashes can be used at the same time.
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process IDs.
- Include a session GUID in each events to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Logs opens for raw read access of disks and volumes
- Optionally logs network connections, including each connection's source process, IP addresses, port numbers, hostnames and port names.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.
- Automatically reload configuration if changed in the registry.
- Rule filtering to include or exclude certain events dynamically.
- Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.

Screenshots

Usage

Uses Sysmon simple command-line options to install and uninstall it, as well as to check and modify Sysmon's

configuration:

Sysinternals Sysmon v10.0 - System activity monitor
Copyright (C) 2014-2019 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Usage:

Install: Sysmon.exe -i <configfile>
[-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]
[-l (<process,...>)]

Configure: Sysmon.exe -c <configfile>
[--|[-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]
[-l [<process,...>]]]

Uninstall: Sysmon.exe -u [force]

PARAMETER	DESCRIPTION
-c	Update configuration of an installed Sysmon driver or dump the current configuration if no other argument is provided. Optionally take a configuration file.
-d	Specify the name of the installed device driver image. Configuration entry: DriverName. The service image and service name will be the same.
-h	Specify the hash algorithms used for image identification (default is SHA1). It supports multiple algorithms at the same time. Configuration entry: HashAlgorithms.
-i	Install service and driver. Optionally take a configuration file.
-l	Log loading of modules. Optionally take a list of processes to track.
-m	Install the event manifest (done on service install as well).
-n	Log network connections. Optionally take a list of processes to track.
-r	Check for signature certificate revocation. Configuration entry: CheckRevocation.
-s	Print configuration schema definition.
-u	Uninstall service and driver. Adding force causes uninstall to proceed even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational"
On older systems, events are written to the System event log.

If you need more information on configuration files, use the '-? config' command. More examples are available

on the Sysinternals website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to accept it.

Neither install nor uninstall requires a reboot.

Examples

Install with default settings (process images hashed with sha1 and no network monitoring)
sysmon -accepteula –i

Install with md5 and sha256 hashing of process created and monitoring network connections
sysmon -accepteula –i –h md5,sha256 –n

Install Sysmon with a configuration file (as described below)

sysmon –accepteula –i c:\windows\config.xml

Uninstall
sysmon –u

Dump the current configuration
sysmon –c

Change the configuration to use all hashes, no network monitoring and monitoring of DLLs in Lsass
sysmon –c –h * –l lsass.exe

Change the configuration of sysmon with a configuration file (as described below)

sysmon –c c:\windows\config.xml

Change the configuration to default settings
sysmon –c --

Show the configuration schema:
sysmon -s

Events

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational", and on older systems events are written to the System event log. Event timestamps are in UTC standard time.

The following are examples of each event type that Sysmon generates.

Event ID 1: Process creation

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.

Event ID 2: A process changed a file creation time

The change file creation time event is registered when a file creation time is explicitly modified by a process. This event helps tracking the real creation time of a file. Attackers may change the file creation time of a backdoor to make it look like it was installed with the operating system. Note that many processes legitimately change the creation time of a file; it does not necessarily indicate malicious activity.

Event ID 3: Network connection

The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGUID fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.

Event ID 4: Sysmon service state changed

The service state change event reports the state of the Sysmon service (started or stopped).

Event ID 5: Process terminated

The process terminate event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.

Event ID 6: Driver loaded

The driver loaded events provides information about a driver being loaded on the system. The configured hashes are provided as well as signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading.

Event ID 7: Image loaded

The image loaded event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the –l option. It indicates the process in which the module is loaded, hashes and signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading. This event should be configured carefully, as monitoring all image load events will generate a large number of events.

Event ID 8: CreateRemoteThread

The CreateRemoteThread event detects when a process creates a thread in another process. This technique is used by malware to inject code and hide in other processes. The event indicates the source and target process. It gives information on the code that will be run in the new thread: StartAddress, StartModule and StartFunction. Note that StartModule and StartFunction fields are inferred, they might be empty if the starting address is outside loaded modules or known exported functions.

Event ID 9: RawAccessRead

The RawAccessRead event detects when a process conducts reading operations from the drive using the \\.\ denotation. This technique is often used by malware for data exfiltration of files that are locked for reading, as well as to avoid file access auditing tools. The event indicates the source process and target device.

Event ID 10: ProcessAccess

The process accessed event reports when a process opens another process, an operation that's often followed by information queries or reading and writing the address space of the target process. This enables detection of hacking tools that read the memory contents of processes like Local Security Authority (Lsass.exe) in order to steal credentials for use in Pass-the-Hash attacks. Enabling it can generate significant amounts of logging if there are diagnostic utilities active that repeatedly open processes to query their state, so it generally should only be done so with filters that remove expected accesses.

Event ID 11: FileCreate

File create operations are logged when a file is created or overwritten. This event is useful for monitoring autostart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.

Event ID 12: RegistryEvent (Object create and delete)

Registry key and value create and delete operations map to this event type, which can be useful for monitoring for changes to Registry autostart locations, or specific malware registry modifications.

Sysmon uses abbreviated versions of Registry root key names, with the following mappings:

KEY NAME	ABBREVIATION
HKEY_LOCAL_MACHINE	HKLM
HKEY_USERS	HKU
HKEY_LOCAL_MACHINE\System\ControlSet00x	HKLM\System\CurrentControlSet
HKEY_LOCAL_MACHINE\Classes	HKCR

Event ID 13: RegistryEvent (Value Set)

This Registry event type identifies Registry value modifications. The event records the value written for Registry values of type DWORD and QWORD.

Event ID 14: RegistryEvent (Key and Value Rename)

Registry key and value rename operations map to this event type, recording the new name of the key or value that was renamed.

Event ID 15: FileCreateStreamHash

This event logs when a named file stream is created, and it generates events that log the hash of the contents of the file to which the stream is assigned (the unnamed stream), as well as the contents of the named stream. There are malware variants that drop their executables or configuration settings via browser downloads, and this event is aimed at capturing that based on the browser attaching a Zone.Identifier "mark of the web" stream.

Event ID 17: PipeEvent (Pipe Created)

This event generates when a named pipe is created. Malware often uses named pipes for interprocess communication.

Event ID 18: PipeEvent (Pipe Connected)

This event logs when a named pipe connection is made between a client and a server.

Event ID 19: WmiEvent (WmiEventFilter activity detected)

When a WMI event filter is registered, which is a method used by malware to execute, this event logs the WMI namespace, filter name and filter expression.

Event ID 20: WmiEvent (WmiEventConsumer activity detected)

This event logs the registration of WMI consumers, recording the consumer name, log, and destination.

Event ID 21: WmiEvent (WmiEventConsumerToFilter activity detected)

When a consumer binds to a filter, this event logs the consumer name and filter path.

Event ID 22: DNSEvent (DNS query)

This event generates when a process executes a DNS query, whether the result is successful or fails, cached or not. The telemetry for this event was added for Windows 8.1 so it is not available on Windows 7 and earlier.

Event ID 255: Error

This event is generated when an error occurred within Sysmon. They can happen if the system is under heavy load and certain tasked could not be performed or a bug exists in the Sysmon service. You can report any bugs on the Sysinternals forum or over Twitter (@markrussinovich).

Configuration files

Configuration files can be specified after the **-i** (installation) or **-c** (installation) configuration switches. They make it easier to deploy a preset configuration and to filter captured events.

A simple configuration xml file looks like this:

The configuration file contains a schemaversion attribute on the Sysmon tag. This version is independent from the Sysmon binary version and allows the parsing of older configuration files. You can get the current schema version by using the "-? config" command line. Configuration entries are directly under the Sysmon tag and filters are under the EventFiltering tag.

Configuration Entries

Configuration entries are similar to command line switches. Command line switches have their configuration entry described in the Sysmon usage output. Parameters are optional based on the tag. If a command line switch also enables an event, it needs to be configured though its filter tag. You can specify the -s switch to have Sysmon print the full configuration schema, including event tags as well as the field names and types for each event. For example, here's the schema for the RawAccessRead event type:

```
<event name="SYSMON\_RAWACCESS\_READ" value="9" level="Informational"
template="RawAccessRead detected" rulename="RawAccessRead"
version="2">
  <data name="UtcTime" inType="win:UnicodeString" outType="xs:string"/>
  <data name="ProcessGuid" inType="win:GUID"/>
  <data name="ProcessId" inType="win:UInt32" outType="win:PID"/>
  <data name="Image" inType="win:UnicodeString" outType="xs:string"/>
  <data name="Device" inType="win:UnicodeString" outType="xs:string"/>
</event>
```

Event filtering entries

Event filtering allows you to filter generated events. In many cases events can be noisy and gathering everything is not possible. For example, you might be interested in network connections only for a certain process, but not all of them. You can filter the output on the host reducing the data to collect.

Each event has its own filter tag under the EventFiltering node in a configuration file:

ID	TAG	EVENT
1 ProcessCreate	Process Create	
2 FileCreateTime	File creation time	
3 NetworkConnect	Network connection detected	
4 n/a	Sysmon service state change (cannot be filtered)	
5 ProcessTerminate	Process terminated	
6 DriverLoad	Driver Loaded	
7 ImageLoad	Image loaded	
8 CreateRemoteThread	CreateRemoteThread detected	

ID	TAG	EVENT
9 RawAccessRead	RawAccessRead detected	
10 ProcessAccess	Process accessed	
11 FileCreate	File created	
12 RegistryEvent	Registry object added or deleted	
13 RegistryEvent	Registry value set	
14 RegistryEvent	Registry object renamed	
15 FileCreateStreamHash	File stream created	
16 n/a	Sysmon configuration change (cannot be filtered)	
17 PipeEvent	Named pipe created	
18 PipeEvent	Named pipe connected	
19 WmiEvent	WMI filter	
20 WmiEvent	WMI consumer	
21 WmiEvent	WMI consumer filter	
22 DNSQuery	DNS query	

You can also find these tags in the event viewer on the task name.

The onmatch filter is applied if events are matched. It can be changed with the "onmatch" attribute for the filter tag. If the value is 'include', it means only matched events are included. If it is set to 'exclude', the event will be included except if a rule match. You can specify both an include filter set and an exclude filter set for each event ID, where exclude matches take precedence.

Each filter can include zero or more rules. Each tag under the filter tag is a field name from the event. Rules that specify a condition for the same field name behave as OR conditions, and ones that specify different field name behave as AND conditions. Field rules can also use conditions to match a value. The conditions are as follows (all are case insensitive):

CONDITION	DESCRIPTION
is	Default, values are equals
is not	Values are different
contains	The field contains this value
contains any	The field contains any of the ; delimited values

CONDITION	DESCRIPTION
contains all	The field contains any of the ; delimited values
excludes	The field does not contain this value
excludes any	The field does not contain one or more of the ; delimited values
excludes all	The field does not contain any of the ; delimited values
begin with	The field begins with this value
end with	The field ends with this value
less than	Lexicographical comparison is less than zero
more than	Lexicographical comparison is more than zero
image	Match an image path (full path or only image name). For example: lsass.exe will match c:\windows\system32\lsass.exe

You can use a different condition by specifying it as an attribute. This excludes network activity from processes with iexplore.exe in their path:

<NetworkConnect onmatch="exclude"> <Image condition="contains">iexplore.exe</Image> </NetworkConnect>

To have Sysmon report which rule match resulted in an event being logged, add names to rules:

<NetworkConnect onmatch="exclude"> <Image name="network iexplore" condition="contains">iexplore.exe</Image> </NetworkConnect>

You can use both include and exclude rules for the same tag, where exclude rules override include rules. Within a rule, filter conditions have OR behavior, In the sample configuration shown earlier, the networking filter uses both an include and exclude rule to capture activity to port 80 and 443 by all processes except those that have iexplore.exe in their name.

It is also possible to override the way that rules are combined by using a rule group which allows the rule combine type for one or more events to be set explicity to AND or OR.

The following example demonstrates this usage. In the first rule group, a process create event will generate when timeout.exe is executed only with a command - line argument of "100", but a process terminate event will generate for termination of ping.exe and timeout.exe.

```
<EventFiltering>
  <RuleGroup name="group 1" groupRelation="and">
    <ProcessCreate onmatch="include">
      <Image condition="contains">timeout.exe</Image>
      <CommandLine condition="contains">100</CommandLine>
    </ProcessCreate>
  </RuleGroup>
  <RuleGroup groupRelation="or">
    <ProcessTerminate onmatch="include">
      <Image condition="contains">timeout.exe</Image>
      <Image condition="contains">ping.exe</Image>
    </ProcessTerminate>
  </RuleGroup>
  <ImageLoad onmatch="include"/>
</EventFiltering>
```

Download Sysmon (1.7 MB)

Runs on:

- Client: Windows 7 and higher.
- Server: Windows Server 2008 R2 and higher.

Sysinternals System Information Utilities

2 minutes to read • Edit Online

Autoruns

See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

ClockRes

View the resolution of the system clock, which is also the maximum timer resolution.

Coreinfo

Coreinfo is a command-line utility that shows you the mapping between logical processors and the physical processor, NUMA node, and socket on which they reside, as well as the cache's assigned to each logical processor.

Handle

This handy command-line utility will show you what files are open by which processes, and much more.

LiveKd

Use Microsoft kernel debuggers to examine a live system.

LoadOrder

See the order in which devices are loaded on your WinNT/2K system.

LogonSessions

List the active logon sessions on a system.

PendMoves

Enumerate the list of file rename and delete commands that will be executed the next boot.

Process Explorer

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process Monitor

Monitor file system, Registry, process, thread and DLL activity in real-time.

ProcFeatures

This applet reports processor and Windows support for Physical Address Extensions and No Execute buffer overflow protection.

PsInfo

Obtain information about a system.

PsLoggedOn

Show users logged on to a system

PsTools

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

RAMMap

An advanced physical memory usage analysis utility that presents usage information in different ways on its several different tabs.

WinObj

The ultimate Object Manager namespace viewer is here.

ClockRes v2.1

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download ClockRes (142 KB)

Introduction

Ever wondered what the resolution of the system clock was, or perhaps the maximum timer resolution that your application could obtain? The answer lies in a simple function named *GetSystemTimeAdjustment*, and the *ClockRes* applet performs the function and shows you the result.

Download ClockRes (142 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

Coreinfo v3.31

4 minutes to read • Edit Online

By Mark Russinovich

Published: August 18, 2014

Download Coreinfo (192 KB)

Introduction

Coreinfo is a command-line utility that shows you the mapping between logical processors and the physical processor, NUMA node, and socket on which they reside, as well as the cache's assigned to each logical processor. It uses the Windows' GetLogicalProcessorInformation function to obtain this information and prints it to the screen, representing a mapping to a logical processor with an asterisk e.g. '*'. Coreinfo is useful for gaining insight into the processor and cache topology of your system.

Installation

You run Coreinfo by typing "coreinfo".

Using CoreInfo

For each resource it shows a map of the OS-visible processors that correspond to the specified resources, with '*' representing the applicable processors. For example, on a 4-core system, a line in the cache output with a map of shared by cores 3 and 4.

Usage: coreinfo [-c][-f][-g][-l][-n][-s][-m][-v]

PARAMETER	DESCRIPTION
-c	Dump information on cores.
-f	Dump core feature information.
-g	Dump information on groups.
-l	Dump information on caches.
-n	Dump information on NUMA nodes.
-s	Dump information on sockets.
-m	Dump NUMA access cost.
-v	Dump only virtualization-related features including support for second level address translation.
(requires administrative rights on Intel systems).	

All options except -v are selected by default.

Coreinfo Output:

```
Coreinfo v3.03 - Dump information on system CPU and memory topology
Copyright (C) 2008-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

Intel(R) Xeon(R) CPU           W3520  @ 2.67GHz
Intel64 Family 6 Model 26 Stepping 5, GenuineIntel
EM64T           *       Supports 64-bit mode
VMX             -       Supports Intel hardware-assisted virtualization
SVM             -       Supports AMD hardware-assisted virtualization
HYPERVISOR      *       Hypervisor is present
HTT             *       Supports hyper-threading

SMX             -       Supports Intel trusted execution
SKINIT          -       Supports AMD SKINIT
EIST            *       Supports Enhanced Intel Speedstep

NX              *       Supports no-execute page protection
PAGE1GB         -       Supports 1GB large pages
PAE             *       Supports &gt; 32-bit physical addresses
PAT             *       Supports Page Attribute Table
PSE             *       Supports 4-MB pages
PSE36           *       Supports &gt; 32-bit address 4-MB pages
PGE             *       Supports global bit in page tables
SS              *       Supports bus snooping for cache operations
VME             *       Supports Virtual-8086 mode

FPU             *       Implements i387 FP instructions
MMX             *       Supports MMX instruction set
MMXEXT          -       Implements AMD MMX extensions
3DNOW           -       Supports 3DNow! instructions
3DNOWEXT        -       Supports 3DNow! extension instructions
SSE             *       Supports Streaming SIMD Extensions
SSE2            *       Supports Streaming SIMD Extensions 2
SSE3            *       Supports Streaming SIMD Extensions 3
SSSE3           *       Supports Supplemental SIMD Extensions 3
SSE4.1          *       Supports Streaming SIMD Extensions 4.1
SSE4.2          *       Supports Streaming SIMD Extensions 4.2

AES             -       Supports AES extensions
AVX             -       Supports AVX intruction extensions
FMA             -       Supports FMA extensions using YMM state
MSR             *       Implements RDMSR/WRMSR instructions
MTTR            *       Supports Mmeory Type Range Registers
XSAVE           -       Supports XSAVE/XRSTOR instructions
OSXSAVE         -       Supports XSETBV/XGETBV instructions

CMOV            *       Supports CMOVcc instruction
CLFSH           *       Supports CLFLUSH instruction
CX8             *       Supports compare and exchange 8-byte instructions
CX16            *       Supports CMPXCHG16B instruction
DCA             -       Supports prefetch from memory-mapped device
F16C            -       Supports half-precision instruction
FXSR            *       Supports FXSAVE/FXSTOR instructions
FFXSR           -       Supports optimized FXSAVE/FSRSTOR instruction
MONITOR         -       Supports MONITOR and MWAIT instructions
MOVBE           -       Supports MOVBE instruction
PCLULDQ         -       Supports PCLMULDQ instruction
POPCNT          *       Supports POPCNT instruction
SEP             *       Supports fast system call instructions

DE              *       Supports I/O breakpoints including CR4.DE
DTES64          -       Can write history of 64-bit branch addresses
DS              -       Implements memory-resident debug buffer
DS-CPL          -       Supports Debug Store feature with CPL
PCID            -       Supports PCIDs and settable CR4.PCIDE
PDCM            -       Supports Performance Capabilities MSR
```

```
RDTSCP          *       Supports RDTSCP instruction
TSC             *       Supports RDTSC instruction
TSC-DEADLINE    -       Local APIC supports one-shot deadline timer
xTPR            *       Supports disabling task priority messages

ACPI            *       Implements MSR for power management
TM              *       Implements thermal monitor circuitry
TM2             *       Implements Thermal Monitor 2 control
APIC            *       Implements software-accessible local APIC
x2APIC          -       Supports x2APIC

CNXT-ID         -       L1 data cache mode adaptive or BIOS

MCE             *       Supports Machine Check, INT18 and CR4.MCE
MCA             *       Implements Machine Check Architecture
PBE             *       Supports use of FERR#/PBE# pin

PSN             -       Implements 96-bit processor serial number

Logical to Physical Processor Map:
*---  Physical Processor 0
-*--  Physical Processor 1
--*-  Physical Processor 2
---*  Physical Processor 3

Logical Processor to Socket Map:
****  Socket 0

Logical Processor to NUMA Node Map:
****  NUMA Node 0

Logical Processor to Cache Map:
*---  Data Cache          0, Level 1,   32 KB, Assoc   8, LineSize  64
*---  Instruction Cache   0, Level 1,   32 KB, Assoc   4, LineSize  64
*---  Unified Cache       0, Level 2,  256 KB, Assoc   8, LineSize  64
-*--  Data Cache          1, Level 1,   32 KB, Assoc   8, LineSize  64
-*--  Instruction Cache   1, Level 1,   32 KB, Assoc   4, LineSize  64
-*--  Unified Cache       1, Level 2,  256 KB, Assoc   8, LineSize  64
--*-  Data Cache          2, Level 1,   32 KB, Assoc   8, LineSize  64
--*-  Instruction Cache   2, Level 1,   32 KB, Assoc   4, LineSize  64
--*-  Unified Cache       2, Level 2,  256 KB, Assoc   8, LineSize  64
---*  Data Cache          3, Level 1,   32 KB, Assoc   8, LineSize  64
---*  Instruction Cache   3, Level 1,   32 KB, Assoc   4, LineSize  64
---*  Unified Cache       3, Level 2,  256 KB, Assoc   8, LineSize  64
****  Unified Cache       4, Level 3,    8 MB, Assoc  16, LineSize  64

Logical Processor to Group Map:
****  Group 0
```

Download Coreinfo (192 KB)

LiveKd v5.62

3 minutes to read • Edit Online

By Mark Russinovich and Ken Johnson

Published: May 16, 2017

Download LiveKd (494 KB)

Introduction

LiveKD, a utility I wrote for the CD included with *Inside Windows 2000, 3rd Edition*, is now freely available. *LiveKD* allows you to run the Kd and Windbg Microsoft kernel debuggers, which are part of the Debugging Tools for Windows package, locally on a live system. Execute all the debugger commands that work on crash dump files to look deep inside the system. See the Debugging Tools for Windows documentation and our book for information on how to explore a system with the kernel debuggers.

While the latest versions of Windbg and Kd have a similar capability on Windows Vista and Server 2008, LiveKD enables more functionality, such as viewing thread stacks with the !thread command, than Windbg and Kd's own live kernel debugging facility.

Installation

First download and install the Debugging Tools for Windows package from Microsoft's web site:

https://msdn.microsoft.com/library/windows/hardware/ff551063(v=vs.85).aspx

If you install the tools to their default directory of \Program Files\Microsoft\Debugging Tools for Windows, you can run *LiveKD* from any directory; otherwise you should copy LiveKD to the directory in which the tools are installed.

If you haven't installed symbols for the system on which you run *LiveKD*, *LiveKD* will ask if you want it to automatically configure the system to use Microsoft's symbol server (see the Debugging Tools for Windows documentation for information on symbol files and the Microsoft symbol server).

NOTE: The Microsoft debugger will complain that it can't find symbols for LIVEKDD.SYS. This is expected, since I have not made symbols for LIVEKDD.SYS available, and does not affect the behavior of the debugger.

Using LiveKd

usage:

** liveKd [[-w]|[-k <debugger>]|[-o filename]] [-vsym] [-m[flags] [[-mp process]|[pid]]][debugger options]
liveKd [[-w]|[-k <debugger>]|[-o filename]] -ml [debugger options]
liveKd [[-w]|[-k <debugger>]|[-o filename]] [[-hl]|[-hv <VM name> [[-p]|[-hvd]]]] [debugger options]**

PARAMETER	DESCRIPTION
-hv	Specifies the name or GUID of the Hyper-V VM to debug.
-hvd	Includes hypervisor pages (Windows 8.1 and above only).

PARAMETER	DESCRIPTION
-hvl	Lists the names and GUIDs of running Hyper-V VMs.
-k	Specifies complete path and filename of debugger image to execute
-m	Creates a mirror dump, which is a consistent view of kernel memory. Only kernel mode memory will be available, and this option may need significant amounts of available physical memory. A flags mask that specifies which regions to include may optionally be provided (drawn from the following table, default 0x18F8): 0001 - process private, 0002 - mapped file, 0004 - shared section, 0008 - page table pages, 0010 - paged pool, 0020 - non-paged pool, 0040 - system PTEs, 0080 - session pages, 0100 - metadata files, 0200 - AWE user pages, 0400 - driver pages, 0800 - kernel stacks, 1000 - WS metadata, 2000 - large pages The default captures most kernel memory contents and is recommended. This option may be used with -o to save faster, consistent dumps. Mirror dumps require Windows Vista or Windows Server 2008 or above. Sysinternals RamMap provides a graphical summary of the distribution of the available memory regions that can be selected for inclusion.
-ml	Generate live dump using native support (Windows 8.1 and above only).
-mp	Specifies a single process whose user mode memory contents should be included in a mirror dump. Only effective with the -m option.
-o	Saves a memory.dmp to disk instead of launching the debugger.
-p	Pauses the target Hyper-V VM while LiveKd is active (recommended for use with -o). Specifies the name or GUID of the Hyper-V VM to debug.
-hvl	Lists the names and GUIDs of running Hyper-V VMs.
-vsym	Displays verbose debugging information about symbol load operations.
-w	Runs windbg instead of kd

All other options are passed through to the debugger.

Note: Use Ctrl-Break to terminate and restart the debugger if it hangs.

By default LiveKd runs kd.exe.

Download LiveKd (494 KB)

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

LoadOrder v1.01

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download LoadOrder (318 KB)
Run now from Sysinternals Live.

Introduction

This applet shows you the order that a Windows NT or Windows 2000 system loads device drivers. Note that on Windows 2000 plug-and-play drivers may actually load in a different order than the one calculated, because plug-and-play drivers are loaded on demand during device detection and enumeration.

Download LoadOrder (318 KB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

ProcFeatures v1.1

By Mark Russinovich

Published: November 1, 2006
Retired: September 1, 2011

NOTE: ProcFeatures has been retired, as the latest additions to **Coreinfo** make this utility obsolete. Coreinfo v3 now shows the processor features supported by the system's processors.

PsInfo v1.78

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

PsInfo is a command-line tool that gathers key information about the local or remote Windows NT/2000 system, including the type of installation, kernel build, registered organization and owner, number of processors and their type, amount of physical memory, the install date of the system, and if its a trial version, the expiration date.

Installation

Just copy *PsInfo* onto your executable path, and type "psinfo".

Using PsInfo

By default *PsInfo* shows information for the local system. Specify a remote computer name to obtain information from the remote system. Since *PsInfo* relies on remote Registry access to obtain its data, the remote system must be running the Remote Registry service and the account from which you run *PsInfo* must have access to the HKLM\System portion of the remote Registry.

In order to aid in automated Service Pack updates, *PsInfo* returns as a value the Service Pack number of system (e.g. 0 for no service pack, 1 for SP 1, etc).

Usage: psinfo [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]

PARAMETER	DESCRIPTION
\\computer	Perform the command on the remote computer or computers specified. If you omit the computer name the command runs on the local system, and if you specify a wildcard (*), the command runs on all computers in the current domain.
@file	Run the command on each computer listed in the text file specified.
-u	Specifies optional user name for login to remote computer.
-p	Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
-h	Show list of installed hotfixes.
-s	Show list of installed applications.
-d	Show disk volume information.

PARAMETER	DESCRIPTION
-c	Print in CSV format.
-t	The default delimiter for the -c option is a comma, but can be overriden with the specified character.
filter	Psinfo will only show data for the field matching the filter. e.g. "psinfo service" lists only the service pack field.

Example Output

```
C:\> psinfo \\development -h -d

PsInfo v1.6 - local and remote system information viewer
Copyright (C) 2001-2004 Mark Russinovich
Sysinternals - www.sysinternals.com

    System information for \\DEVELOPMENT:
    Uptime: 28 days, 0 hours, 15 minutes, 12 seconds
    Kernel version: Microsoft Windows XP, Multiprocessor Free
    Product type Professional
    Product version: 5.1
    Service pack: 0
    Kernel build number: 2600
    Registered organization: Sysinternals
    Registered owner: Mark Russinovich
    Install date: 1/2/2002, 5:29:21 PM
    Activation status: Activated
    IE version: 6.0000
    System root: C:\WINDOWS
    Processors: 2
    Processor speed: 1.0 GHz
    Processor type: Intel Pentium III
    Physical memory: 1024 MB
    Volume Type Format Label Size Free Free
    A: Removable 0%
    C: Fixed NTFS WINXP 7.8 GB 1.3 GB 16%
    D: Fixed NTFS DEV 10.7 GB 809.7 MB 7%
    E: Fixed NTFS SRC 4.5 GB 1.8 GB 41%
    F: Fixed NTFS MSDN 2.4 GB 587.5 MB 24%
    G: Fixed NTFS GAMES 8.0 GB 1.0 GB 13%
    H: CD-ROM CDFS JEDIOUTCAST 633.6 MB 0%
    I: CD-ROM 0%
    Q: Remote 0%
    T: Fixed NTFS Test 502.0 MB 496.7 MB 99%
    OS Hot Fix Installed
    Q147222 1/2/2002
    Q309521 1/4/2002
    Q311889 1/4/2002
    Q313484 1/4/2002
    Q314147 3/6/2002
    Q314862 3/13/2002
    Q315000 1/8/2002
    Q315403 3/13/2002
    Q317277 3/20/2002
```

How it Works

PsInfo uses the Remote Registry API to read system information from a system's Registry, and WMI to determine whether Windows XP installations have been activated.

Download PsTools (2.7 MB)

RAMMap v1.52

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 28, 2019

Download RAMMap (479 KB)
Run now from Sysinternals Live.

Have you ever wondered exactly how Windows is assigning physical memory, how much file data is cached in RAM, or how much RAM is used by the kernel and device drivers? RAMMap makes answering those questions easy. RAMMap is an advanced physical memory usage analysis utility for Windows Vista and higher. It presents usage information in different ways on its several different tabs:

- *Use Counts:* usage summary by type and paging list
- *Processes:* process working set sizes
- *Priority Summary:* prioritized standby list sizes
- *Physical Pages:* per-page use for all physical memory
- *Physical Ranges:* physical memory addresses
- *File Summary:* file data in RAM by file
- *File Details:* individual physical pages by file

Use RAMMap to gain understanding of the way Windows manages memory, to analyze application memory usage, or to answer specific questions about how RAM is being allocated. RAMMap's refresh feature enables you to update the display and it includes support for saving and loading memory snapshots.

For definitions of the labels RAMMap uses as well as to learn about the physical-memory allocation algorithms used by the Windows memory manager, please see Windows Internals, 5^th^ Edition.

Related Links

- **Windows Internals Book**
  **The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- **Windows Sysinternals Administrator's Reference**The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download RAMMap (479 KB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Learn More

- Defrag Tools: #6 - RAMMap
  In this episode of Defrag Tools, Andrew Richards and Larry Larsen cover using RAMMap to see how RAM is being used and tell if there has been any memory pressure.

WinObj v2.22

2 minutes to read • Edit Online

By Mark Russinovich

Published: February 14, 2011

Download WinObj (447 KB)
Run now from Sysinternals Live.

Introduction

WinObj is a must-have tool if you are a system administrator concerned about security, a developer tracking down object-related problems, or just curious about the Object Manager namespace.

WinObj is a 32-bit Windows NT program that uses the native Windows NT API (provided by NTDLL.DLL) to access and display information on the NT Object Manager's name space. Winobj may seem similar to the Microsoft SDK's program of the same name, but the SDK version suffers from numerous significant bugs that prevent it from displaying accurate information (e.g. its handle and reference counting information are totally broken). In addition, our WinObj understands many more object types. Finally, Version 2.0 of our WinObj has user-interface enhancements, knows how to open device objects, and will let you view and change object security information using native NT security editors.

Installation and Use

There is no device driver component to WinObj, so you can run it like any Win32 program.

How it Works

The Object Manager is in charge of managing NT objects. As part of this responsibility, it maintains an internal namespace where various operating system components, device drivers and Win32 programs can store and lookup objects. The native NT API provides routines that allow user-mode programs to browse the namespace and query the status of objects located there, but the interfaces are undocumented.

More Information

Helen Custer's *Inside Windows NT* provides a good overview of the Object Manager name space, and Mark's October 1997 WindowsITPro Magazine column, "Inside the Object Manager", is (of course) an excellent overview.

Download WinObj (447 KB)
Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Sysinternals Miscellaneous Utilities

2 minutes to read • Edit Online

AD Explorer

Active Directory Explorer is an advanced Active Directory (AD) viewer and editor.

AdRestore

Restore tombstoned Active Directory objects in Server 2003 domains.

Autologon

Bypass password screen during logon.

BgInfo

This fully-configurable program automatically generates desktop backgrounds that include important information about the system including IP addresses, computer name, network adapters, and more.

BlueScreen

This screen saver not only accurately simulates Blue Screens, but simulated reboots as well (complete with CHKDSK), and works on Windows Vista, Server 2008 and higher.

Ctrl2cap

This is a kernel-mode driver that demonstrates keyboard input filtering just above the keyboard class driver in order to turn caps-locks into control keys. Filtering at this level allows conversion and hiding of keys before NT even "sees" them. Ctrl2cap also shows how to use NtDisplayString() to print messages to the initialization blue-screen.

DebugView

Another first from Sysinternals: This program intercepts calls made to DbgPrint by device drivers and OutputDebugString made by Win32 programs. It allows for viewing and recording of debug session output on your local machine or across the Internet without an active debugger.

Desktops

This new utility enables you to create up to four virtual desktops and to use a tray interface or hotkeys to preview what's on each desktop and easily switch between them.

Hex2dec

Convert hex numbers to decimal and vice versa.

NotMyFault

Notmyfault is a tool that you can use to crash, hang, and cause kernel memory leaks on your Windows system.

PsLogList

Dump event log records.

PsTools

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

RegDelNull

Scan for and delete Registry keys that contain embedded null-characters that are otherwise undeleteable by standard Registry-editing tools.

Registry Usage (RU)

View the registry space usage for the specified registry key.

RegJump

Jump to the registry path you specify in Regedit.

Strings

Search for ANSI and UNICODE strings in binary images.

ZoomIt

Presentation utility for zooming and drawing on the screen.

BgInfo v4.28

6 minutes to read • Edit Online

By Mark Russinovich

Published: September 20, 2019

Download BgInfo (3.4 MB)
Run now from Sysinternals Live.

Introduction

How many times have you walked up to a system in your office and needed to click through several diagnostic windows to remind yourself of important aspects of its configuration, such as its name, IP address, or operating system version? If you manage multiple computers you probably need *BGInfo*. It automatically displays relevant information about a Windows computer on the desktop's background, such as the computer name, IP address, service pack version, and more. You can edit any field as well as the font and background colors, and can place it in your startup folder so that it runs every boot, or even configure it to display as the background for the logon screen.

Because *BGInfo* simply writes a new desktop bitmap and exits, you don't have to worry about it consuming system resources or interfering with other applications.

Sysinternals BgInfo

Installation and Use

See Mark's *Windows IT Pro Magazine* Power Tools article for a primer on using *BgInfo*. If you have questions or problems, please visit the Sysinternals BgInfo Forum.

By placing *BGInfo* in your **Startup** folder, you can ensure that the system information being displayed is up to date each time you boot. Once you've settled on the information to be displayed, use the command-line option /timer:0 to update the display without showing the dialog box.

You can also use the Windows Scheduler to run *BGInfo* on a regular basis to ensure long-running systems are kept up to date.

If you create a *BGInfo* configuration file (using the **File|Save Settings** menu item) you can automatically import and use those settings on other systems by adding the **/I<path>** or **/iq<path>** command line option.

Using BgInfo

When you run *BGInfo* it shows you the appearance and content of its default desktop background. If left untouched it will automatically apply these settings and exit after its 10 second count-down timer expires.

Selecting any button or menu item will disable the timer, allowing you to customize the layout and content of the background information.

If you want *BGInfo* to edit or use a configuration stored in a file (instead of the default configuration which is stored in the registry) specify the name of the file on the command line:

Appearance Buttons

Fields: Selects what information appears on the desktop, and the order in which it is displayed. For networking fields (NIC, IP, MAC, etc.) a separate entry is created for each network card on the system. Use the Custom button to add special information you define yourself.

Background: Selects the color and/or wallpaper to use for the background. If you select the **Copy existing settings** option then *BGInfo* will use whatever information is currently selected by the logged on user. This option allows end users to personalize their desktop while still displaying the *BGInfo* information.

Position: Selects the location on the screen at which to place the text. If some items are very long (for example some network card names) you can use the **Limit Lines to** item to wrap them. The **Compensate for Taskbar position** checkbox adjusts the position of the text to ensure that it is not covered by the Taskbar. The **Multiple Monitor Configuration** button allows you to specify how multiple monitors attached to a single console should be handled.

Desktops: Selects which desktops are updated when the configuration is applied. By default only the **User Desktop** wallpaper is changed. **Enabling the Logon Desktop for Console users** option specifies that the wallpaper should be displayed on the logon desktop that is presented before anyone has logged onto the system. On Windows 95/98/ME systems the same desktop is used for users and the login screen, so this option has no effect. Enabling the **Logon Desktop for Terminal Services users** option specifies that the wallpaper should be displayed on the Terminal Services login screen. This option is useful only on servers running Terminal Services.

Preview: Displays the background as it will appear when applied to your system.

Configuration Menu Items

These are options that control how the bitmap is produced, where it is located and how to import/export settings.

File | Open: Opens a *BGInfo* configuration file.

File | Save As: Saves a copy of the current *BGInfo* configuration to a new file. Once created, you can have *BGInfo* use the file later by simply specifying it on the command line, or by using **File|Open** menu option.

File|Reset Default Settings: Removes all configuration information and resets *BGInfo* to its default (install-time) state. Use this if you can't determine how to undo a change, or if *BGInfo* becomes confused about the current state of the bitmap.

File|Database: Specifies a .XLS, .MDB or .TXT file or a connection string to an SQL database that *BGInfo* should use to store the information it generates. Use this to collect a history of one or more systems on your network. You must ensure that all systems that access the file have the same version of MDAC and JET database support installed. It is recommended you use at least MDAC 2.5 and JET 4.0. If specifying an XLS file the file must already exist.

If you prefer to have *BGInfo* update the database without modifying the user's wallpaper you can unselect all desktops in the **Desktops** dialog; *BGInfo* will still update the database.

Bitmap|256 Colors: Limits the bitmap to 256 colors. This option produces a smaller bitmap.

Bitmap|High Color/True Color: Creates a 16-bit or 24-bit color bitmap.

Bitmap|Match Display: Creates a bitmap with color depth matching that of the display. Because the bitmap generated by *BGInfo* is not updated when a user changes the display's color depth you may see unexpected results (especially dithering of the text and background) with some combinations of bitmap and display depth.

Bitmap|Location: Specifies the location to place the output bitmap file. On Terminal Services servers the bitmap

should be placed in a location that is unique to each user.

Edit|Insert Image: Allows you to insert a bitmap image into the output. Because *BGInfo*'s configuration information is stored in the registry and Windows limits the size of registry values you may encounter errors when inserting larger images. On Windows 9x/Me systems the limit is 16K, while on NT/2000/XP systems the limit is 64K.

Command Line Options

PARAMETER	DESCRIPTION
<path>	Specifies the name of a configuration file to use for the current session. Changes to the configuration are automatically saved back to the file when OK or Apply is pressed. If this parameter is not present *BGInfo* uses the default configuration information which is stored in the registry under the current user ("HKEY_CURRENT_USER\Software\Winternals*BGInfo*").
/timer	Specifies the timeout value for the countdown timer, in seconds. Specifying zero will update the display without displaying the configuration dialog. Specifying 300 seconds or longer disables the timer altogether.
/popup	Causes *BGInfo* to create a popup window containing the configured information without updating the desktop. The information is formatted exactly as it would if displayed on the desktop, but resides in a fitted window instead. When using this option the history database is not updated.
/silent	Suppresses error messages.
/taskbar	Causes *BGInfo* to place an icon in the taskbar's status area without updating the desktop. Clicking the icon causes the configured information to appear in a popup window. When using this option the history database is not updated.
/all	Specifies that *BGInfo* should change the wallpaper for any and all users currently logged in to the system. This option is useful within a Terminal Services environment, or when *BGInfo* is scheduled to run periodically on a system used by more than one person (see Using a Schedule below).
/log	Causes *BGInfo* to write errors to the specified log file instead of generating a warning dialog box. This is useful for tracking down errors that occur when *BGInfo* is run under the scheduler.
/rtf	Causes *BGInfo* to write its output text to an RTF file. All formatting information and colors are included.

 **Download BgInfo**] **(3.4 MB)**

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

BlueScreen Screen Saver v3.2

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download BlueScreen (64 KB)

Introduction

One of the most feared colors in the NT world is blue. The infamous Blue Screen of Death (BSOD) will pop up on an NT system whenever something has gone terribly wrong. Bluescreen is a screen saver that not only authentically mimics a BSOD, but will simulate startup screens seen during a system boot.

- On NT 4.0 installations it simulates chkdsk of disk drives with errors!
- On Windows 2000, Windows 95, and Windows 98 it presents the Windows 2000 startup splash screen, complete with rotating progress band and progress control updates!
- On Windows XP and Windows Server 2003 it presents the XP/Server 2003 startup splash screen with progress bar!

Bluescreen cycles between different Blue Screens and simulated boots every 15 seconds or so. Virtually all the information shown on Bluescreen's BSOD and system start screen is obtained from your system configuration - its accuracy will fool even advanced NT developers. For example, the NT build number, processor revision, loaded drivers and addresses, disk drive characteristics, and memory size are all taken from the system Bluescreen is running on.

Use Bluescreen to amaze your friends and scare your enemies!

Installation and Use

Note: before you can run Bluescreen on Windows 95 or 98, you must copy \winnt\system32\ntoskrnl.exe from a Windows 2000 system to your \Windows directory. Simply copy Sysinternals BLUESCRN.SCR to your \system32 directory if on Windows NT/2K, or \Windows\System directory if on Windows 95 or 98. Right click on the desktop to bring up the Display settings dialog and then select the "Screen Saver" tab. Use the pull down list to find "Sysinternals Bluescreen" and apply it as your new screen saver. Select the "Settings" button to enable fake disk activity, which adds an extra touch of realism!

More Information

You can find out how real Blue Screens are generated, and what the information on the Blue Screen means in my December 1997 *Windows ITPro Magazine* NT Internals column, "*Inside the Blue Screen.*"

Note: Some virus scanners flag the Bluescreen screen saver as a virus. If this is the case with your virus scanner, you may not be able to use this screen saver.

Download BlueScreen (64 KB)

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

CpuStres v2.0

2 minutes to read • Edit Online

By Pavel Yosifovich

Published: July 18, 2018

Download Cpustres (2.2 MB)

Introduction

Cpustres
Cpustres is a utility that can be used to simulate CPU activity by running up to 64 threads in a tight loop.

Each thread can be started, paused or stopped independently and can be configured with the following parameters:

- **Activity Level** This can be Low, Medium, Busy or Maximum which controls how long the thread sleepss between cycles. Setting this value to Maximum causes the thread to run continuously.
- **Priority** This controls the thread priority. Refer to Windows Internals by Mark Russinovich for details on thread priorities

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2003 and higher
- Nano Server: 2016 and higher

Related Links

- **Windows Internals Book** The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- **Pavel's Blog** Pavel Yosifovich's blog describing the tool

Download

Download Cpustres (2.2 MB)
Run now from Sysinternals Live.

Ctrl2Cap v2.0

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 1, 2006

Download Ctrl2Cap (48 KB)

Introduction

Ctrl2cap is a kernel-mode device driver that filters the system's keyboard class driver in order to convert caps-lock characters into control characters. People like myself that migrated to NT from UNIX are used to having the control key located where the caps-lock key is on the standard PC keyboard, so a utility like this is essential for our editing well-being.

Installation and Use

Install Ctrl2cap running the command "ctrl2cap /install" from the directory into which you've unzipped the Ctrl2cap files. To uninstall type "ctrl2cap /uninstall".

How Ctrl2cap Works

On NT 4 Ctrlcap is actually quite trivial. It simply attaches itself to the keyboard class driver so that it will catch keyboard read requests. For each request, it posts an I/O completion callback, at which point it takes a peek at the scancode that is being returned. If it happens to be a caps-lock, ctrl2cap changes it into a left-control.

On Win2K Ctrl2cap is a WDM filter driver that layers in the keyboard class device's stack above the keyboard class device. This is in contrast to the Win2K DDK's kbfiltr example that layers itself between the i8042 port device and the keyboard class device. I chose to layer on top of the keyboard class device for several reasons:

- It means that the Ctrl2cap IRP_MJ_READ interception and manipulation code is shared between the NT 4 and Win2K versions.
- I don't need to supply an INF file and have the user go through the Device Manager to install Ctrl2cap - I simply modify the appropriate Registry value (the keyboard class devices's HKLM\System\CurrentControlSet\Control\Class UpperFilters value).

The disadvantage of my approach is (and this an advantage or disadvantage depending on your point of view):

- Because I don't install with an INF file via the Device Manager, the user is not warned that the Ctrl2cap driver file is not digitally signed by Microsoft.

In this particular case, I felt that the advantages outweigh the disadvantages. However, before you model a Win2K keyboard filter on Ctrl2cap I strongly suggest that you study the kbfiltr example from the Win2K DDK. Kbfiltr's interception point in the key input sequence makes it very easy for kbfiltr to inject keystrokes into the input stream.

More Information

For more information on writing filter drivers (drivers that attach themselves to other drivers so that they can see their input and/or output), here are sources to check out:

- The Windows NT and Windows 2000 DDK sample \src\storage\filter\diskperf
- The Windows 2000 DDK sample \src\input\kbfiltr
- "*Examining the Windows NT File System*," By Mark Russinovich, *Dr. Dobb's Journal*, February 1997
- The accompanying file system filter driver, Filemon

Download Ctrl2Cap (48 KB)

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

DebugView v4.90

4 minutes to read • Edit Online

By Mark Russinovich

Published: April 23, 2019

Download DebugView (464 KB)
Run now from Sysinternals Live.

Introduction

DebugView is an application that lets you monitor debug output on your local system, or any computer on the network that you can reach via TCP/IP. It is capable of displaying both kernel-mode and Win32 debug output, so you don't need a debugger to catch the debug output your applications or device drivers generate, nor do you need to modify your applications or drivers to use non-standard debug output APIs.

DebugView Capture

Under Windows 2000, XP, Server 2003 and Vista *DebugView* will capture:

- Win32 **OutputDebugString**
- Kernel-mode **DbgPrint**
- All kernel-mode variants of **DbgPrint** implemented in Windows XP and Server 2003

DebugView also extracts kernel-mode debug output generated before a crash from Window's 2000/XP crash dump files if *DebugView* was capturing at the time of the crash.

DebugView Capabilities

DebugView has a powerful array of features for controlling and managing debug output.

Features new to version 4.6:

- **Support for Windows Vista 32-bit and 64-bit**

Features new to version 4.5:

- **Support for log-file rollover:** To better support long-running captures, DebugView can now create a new log file each day, optionally clearing the display when doing so.

Features new to version 4.4:

- **Support for Windows Server 2003 64-bit Edition and Windows XP 64-bit Edition for x64:***DebugView* now captures kernel-mode debug output on 64-bit versions of Windows.
- **Clock-time toggle:** you can now toggle between clock time and elapsed time modes.

Features new to version 4.3:

- **Support for Windows XP SP2:***DebugView* now captures kernel-mode debug output on Windows XP SP2.
- **More highlighting filters:** Many people have asked for more highlighting filters.
- **Log file wrapping:** A new log file option has *DebugView* wrap around to the start of the log file when the specified size limit is reached.

- **Larger buffers:** Larger Win32 and kernel-mode buffers lessen the chance of dropped debug output.
- **Clear-output string:** When *DebugView* sees the special debug output string "DBGVIEWCLEAR" it clears the output.
- **Client minimize-to-tray:** You can now run the client minimized in the tray.

Features new to version 4.2:

- **Kernel-hook bug fixed:***DebugView* sometimes mistakenly report that it couldn't hook kernel-mode debug output on Windows XP and Server 2003.
- **Client global-capture option:** A new option allows the client to capture console Win32 debug output on Terminal Server systems when run from a non-console session.
- **Filtering improved:** Filters can be much longer and now apply to Win32 process IDs when process IDs are included in the output.
- **Crash-dump support improved:** Several bugs related to extracting kernel-mode output from crash dumps are fixed and *DebugView* now loads resulting log files.
- **More highlight filters:***DebugView* now has 10 highlight filters, up from 5.
- **Insert comments:** A new menu item lets you insert comments into output.
- **New switches:** New command-line switches allow you to specify history depth and load log files.
- **Better balloon tips:** If an output line is wider than the screen its mouse hover balloon tip word wraps.

Features new to version 4.1:

- **Save and load filters:** You can save and load filters, including the highlighting colors.
- **Load saved logs:** You can now load a log file back into the *DebugView* output window.
- **Capture boot-time kernel-mode debug output:** Under Windows 2000, you can use *DebugView* to capture debug output generated by drivers from the earliest point in the boot process.

Here is a list highlighting some of *DebugView*'s other features:

- **Remote monitoring:** Capture kernel-mode and/or Win32 debug output from any computer accessible via TCP/IP - even across the Internet. You can monitor multiple remote computers simultaneously. *DebugView* will even install its client software itself if you are running it on a Windows 2000 system and are capturing from another Windows 2000 system in the same Network Neighborhood.
- **Most-recent-filter lists:***DebugView* remembers your most recent filter selections, with an interface that makes it easy to reselect them.
- **Process ID option:** Toggle the display of process IDs for Win32 debug output.
- **Clipboard copy:** Select multiple lines in the output window and copy their contents to the clipboard.
- **Log-to-file:** Write debug output to a file as its being captured.
- **Printing:** Print all or part of captured debug output to a printer.
- **One-file payload:***DebugView* is implemented as one file.
- **Crash-Dump Support:***DebugView* can recover its buffers from a crash dump and save the output to a log file so that users can send you the output your Windows driver generated right up to the time of a crash.

The on-line help file describes all these features, and more, in detail.

Installation and Use

Simply execute the *DebugView* program file (dbgview.exe) and *DebugView* will immediately start capturing debug output. Note that if you run *DebugView* on Windows 2000/XP you must have administrative privilege to view kernel-mode debug output. Menus, hot-keys, or toolbar buttons can be used to clear the window, save the monitored data to a file, search output, change the window font, and more. The on-line help describes all of *DebugView*'s features.

This is a screenshot of *DebugView* capturing Win32 debug output from a remote system. Note the presence of a highlighting filter.

Download DebugView (464 KB)

Run now from Sysinternals Live.

Desktops v2.0

2 minutes to read • Edit Online

By Mark Russinovich

Published: October 17, 2012

Download Desktops (61 KB)
Run now from Sysinternals Live.

Introduction

Desktops allows you to organize your applications on up to four virtual desktops. Read email on one, browse the web on the second, and do work in your productivity software on the third, without the clutter of the windows you're not using. After you configure hotkeys for switching desktops, you can create and switch desktops either by clicking on the tray icon to open a desktop preview and switching window, or by using the hotkeys.

Using Desktops

Unlike other virtual desktop utilities that implement their desktops by showing the windows that are active on a desktop and hiding the rest, Sysinternals Desktops uses a Windows desktop object for each desktop. Application windows are bound to a desktop object when they are created, so Windows maintains the connection between windows and desktops and knows which ones to show when you switch a desktop. That making Sysinternals Desktops very lightweight and free from bugs that the other approach is prone to where their view of active windows becomes inconsistent with the visible windows.

Desktops reliance on Windows desktop objects means that it cannot provide some of the functionality of other virtual desktop utilities, however. For example, Windows doesn't provide a way to move a window from one desktop object to another, and because a separate Explorer process must run on each desktop to provide a taskbar and start menu, most tray applications are only visible on the first desktop. Further, there is no way to delete a desktop object, so Desktops does not provide a way to close a desktop, because that would result in orphaned windows and processes. The recommended way to exit Desktops is therefore to logoff.

Screenshot

Configuration Dialog

Tray Desktop Switch Window

Download Desktops (61 KB)

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

Hex2dec v1.1

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download Hex2dec (152 KB)

Introduction

Tired of running Calc every time you want to convert a hexadecimal number to decimal Now you can convert hex to decimal and vice versa with this simple command-line utility.

Usage: hex2dec [hex|decimal]

Include x or 0x as the prefix of the number to specify a hexadecimal value.
e.g. To translate 1233 decimal to hexadecimal: hex2dec 1233
e.g. To translate 0x1233 hexadecimal to decimal: hex2dec 0x1233

Download Hex2dec (152 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher
- Nano Server: 2016 and higher

NotMyFault v4.20

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 14, 2019

Download NotMyFault (1 MB)

Introduction

Notmyfault is a tool that you can use to crash, hang, and cause kernel memory leaks on your Windows system. It's useful for learning how to identify and diagnose device driver and hardware problems, and you can also use it to generate blue screen dump files on misbehaving systems. The download file includes 32-bit and 64-bit versions, as well as a command-line version that works on Nano Server. Chapter 7 in Windows Internals uses Notmyfault to demonstrate pool leak troubleshooting and Chapter 14 uses it for crash analysis examples.

Screenshots

Usage

You can use the GUI versions or the command-line version. Notmyfault requires administrative privileges.

Usage:

notmyfaultc.exe crash crash_type_num

```
crash type:
  0x01: High IRQL fault (Kernel-mode)
  0x02: Buffer overflow
  0x03: Code overwrite
  0x04: Stack trash
  0x05: High IRQL fault (User-mode)
  0x06: Stack overflow
  0x07: Hardcoded breakpoint
  0x08: Double Free
```

Or **notmyfaultc.exe hang hang_type_num**

```
hang type:
  0x01: Hang with IRP
  0x02: Hang with DPC
```

Download NotMyFault (1 MB)

PsPasswd v1.24

2 minutes to read • Edit Online

By Mark Russinovich

Published: June 29, 2016

Download PsTools (2.7 MB)

Introduction

Systems administrators that manage local administrative accounts on multiple computers regularly need to change the account password as part of standard security practices. *PsPasswd* is a tool that lets you change an account password on the local or remote systems, enabling administrators to create batch files that run *PsPasswd* against the computers they manage in order to perform a mass change of the administrator password.

PsPasswd uses Windows password reset APIs, so does not send passwords over the network in the clear.

Installation

Just copy *PsPasswd* onto your executable path, and type "pspasswd" with the command-line syntax shown below..

Using PsPasswd

You can use *PsPasswd* to change the password of a local or domain account on the local or a remote computer.

usage: pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] Username [NewPassword]

PARAMETER	DESCRIPTION
computer	Perform the command on the remote computer or computers specified. If you omit the computer name the command runs on the local system, and if you specify a wildcard (*), the command runs on all computers in the current domain.
@file	Run the command on each computer listed in the text file specified.
-u	Specifies optional user name for login to remote computer.
-p	Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
Username	Specifies name of account for password change.
NewPassword	New password. If ommitted a NULL password is applied.

Download PsTools (2.7 MB)

PsTools

PsPasswd is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

PsShutdown v2.52

2 minutes to read • Edit Online

By Mark Russinovich

Published: December 4, 2006

Download PsTools (2.7 MB)

Introduction

PsShutdown is a command-line utility similar to the shutdown utility from the Windows 2000 Resource Kit, but with the ability to do much more. In addition to supporting the same options for shutting down or rebooting the local or a remote computer, *PsShutdown* can logoff the console user or lock the console (locking requires Windows 2000 or higher). *PsShutdown* requires no manual installation of client software.

Installation

Just copy *PsShutdown* onto your executable path, and type psshutdown with command-line options defined below.

Using PsShutdown

See the February 2005 issue of Windows IT Pro Magazine for Mark's article that covers advanced usage of *PsKill*.

You can use *PsShutdown* to initiate a shutdown of the local or a remote computer, logoff a user, lock a system, or to abort an imminent shutdown.

Usage: psshutdown [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v nn] [-e [u|p]:xx:yy] [-m "message"]

PARAMETER	DESCRIPTION
-	Displays the supported options.
computer	Perform the command on the remote computer or computers specified. If you omit the computer name the command runs on the local system, and if you specify a wildcard (*), the command runs on all computers in the current domain.
@file	Run the command on each computer listed in the text file specified.
-u	Specifies optional user name for login to remote computer.
-p	Specifies optional password for user name. If you omit this you will be prompted to enter a hidden password.
-a	Aborts a shutdown (only possible while a countdown is in progress).
-c	Allows the shutdown to be aborted by the interactive user.

PARAMETER	DESCRIPTION
-d	Suspend the computer.
-e	Shutdown reason code.
	Specify 'u' for user reason codes and 'p' for planned shutdown reason codes.
	xx is the major reason code (must be less than 256).
	yy is the minor reason code (must be less than 65536).
-f	Forces all running applications to exit during the shutdown instead of giving them a chance to gracefully save their data.
-h	Hibernate the computer.
-k	Poweroff the computer (reboot if poweroff is not supported).
-l	Lock the computer.
-m	This option lets you specify a message to display to logged-on users when a shutdown countdown commences.
-n	Specifies timeout in seconds connecting to remote computers.
-o	Logoff the console user.
-r	Reboot after shutdown.
-s	Shutdown without power off.
-t	Specifies the countdown in seconds until the shutdown (default: 20 seconds) or the time of shutdown (in 24 hour notation).
-v	Display message for the specified number of seconds before the shutdown. If you omit this parameter the shutdown notification dialog displays and specifying a value of 0 results in no dialog.

Download PsTools (2.7 MB)

PsTools

PsShutdown is part of a growing kit of Sysinternals command-line tools that aid in the administration of local and remote systems named *PsTools*.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

RegDelNull v1.11

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download RegDelNull (152 KB)

Introduction

This command-line utility searches for and allows you to delete Registry keys that contain embedded-null characters and that are otherwise undeleteable using standard Registry-editing tools. Note: deleting Registry keys may cause the applications they are associated with to fail.

Using RegDelNull

Usage: regdelnull <path> [-s]

PARAMETER	DESCRIPTION
-s	Recurse into subkeys.

Here's an example of RegDelNull when used on a system on which the RegHide sample program has created a null-embedded key:

```
C:\>regdelnull hklm -sRegDelNull v1.10 - Delete Registry keys with embedded Nulls

Copyright (C) 2005-2006 Mark Russinovich
Sysinternals - www.sysinternals.com
Null-embedded key (Nulls are replaced by '*'):
HKLM\SOFTWARE\Systems Internals\Can't touch me!*
Delete (y/n) y
Scan complete.
```

Download RegDelNull (152 KB)

Runs on:

- Client: Windows Vista (32-bit) and higher
- Server: Windows Server 2008 (32-bit) and higher
- Nano Server: 2016 and higher

Registry Usage (RU) v1.2

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download RU (156 KB)

Introduction

Ru (registry usage) reports the registry space usage for the registry key you specify. By default it recurses subkeys to show the total size of a key and its subkeys.

Using Registry Usage (RU)

usage: ru [-c[t]] [-l <levels> | -n | -v] [-q] <absolute path>

usage: ru [-c[t]] [-l <levels> | -n | -v] [-q] -h <hive file> [relative path]

PARAMETER	DESCRIPTION
-c	Print output as CSV. Specify -ct for tab delimiting.
-h	Load the specified hive file, perform the size calculation, then unload it and compress it.
-l	Specify subkey depth of information (default is one level).
-n	Do not recurse.
-q	Quiet (no banner).
-v	Show size of all subkeys.

CSV output is formatted as:

Path,CurrentValueCount,CurrentValueSize,ValueCount,KeyCount,KeySize,WriteTime

Download RU (156 KB)

Reghide

2 minutes to read • Edit Online

Published: November 1, 2006

 **Download RegHide (38 KB) Run now** from Sysinternals Live.

Introduction

A subtle but significant difference between the Win32 API and the Native API (see Inside the Native API for more information on this largely undocumented interface) is the way that names are described. In the Win32 API strings are interpreted as NULL-terminated ANSI (8-bit) or wide character (16-bit) strings. In the Native API names are counted Unicode (16-bit) strings. While this distinction is usually not important, it leaves open an interesting situation: there is a class of names that can be referenced using the Native API, but that cannot be described using the Win32 API.

 **Download RegHide (38 KB)**

Run now from Sysinternals Live.

Runs on:

- Client: Windows Vista and higher.
- Server: Windows Server 2008 and higher.

RegJump v1.1

2 minutes to read • Edit Online

By Mark Russinovich

Published: April 20, 2015

 **Download RegJump (53 KB)**

Introduction

This little command-line applet takes a registry path and makes Regedit open to that path. It accepts root keys in standard (e.g. HKEY_LOCAL_MACHINE) and abbreviated form (e.g. HKLM).

usage: regjump <<path>|-c>

PARAMETER	DESCRIPTION
-c	Copy path from clipboard.

e.g.: regjump HKLM\Software\Microsoft\Windows

 **Download RegJump (53 KB)**

Strings v2.53

2 minutes to read • Edit Online

By Mark Russinovich

Published: July 4, 2016

Download Strings (150 KB)

Introduction

Working on NT and Win2K means that executables and object files will many times have embedded UNICODE strings that you cannot easily see with a standard ASCII strings or grep programs. So we decided to roll our own. Strings just scans the file you pass it for UNICODE (or ASCII) strings of a default length of 3 or more UNICODE (or ASCII) characters. Note that it works under Windows 95 as well.

Using Strings

usage: strings [-a] [-f offset] [-b bytes] [-n length] [-o] [-q] [-s] [-u] <file or directory>

Strings takes wild-card expressions for file names, and additional command line parameters are defined as follows:

PARAMETER	DESCRIPTION	
-a	Ascii-only search (Unicode and Ascii is default)	
-b	Bytes of file to scan	
-f	File offset at which to start scanning.	
-o	Print offset in file string was located	
-n	Minimum string length (default is 3)	
-q	Quiet (no banner)	
-s	Recurse subdirectories	
-u	Unicode-only search (Unicode and Ascii is default)	

To search one or more files for the presence of a particular string using strings use a command like this:

strings * | findstr /i TextToSearchFor

Download Strings (150 KB)

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2008 and higher

- Nano Server: 2016 and higher

Testlimit v5.24

2 minutes to read • Edit Online

By Mark Russinovich

Published: November 17, 2016

Download Testlimit (234 KB)

Introduction

Testlimit is a command-line utility that can be used to stress-test your PC and/or applications by simulating low resource conditions for memory, handles, processes, threads and other system objects.

usage: Testlimit [[-h [-u]] | [-p [-n]] | [-t [-n [KB]]] | [-u [-i]] | [-g [object size]] | [-a|-d|-l|-m|-r|-s|-v [MB]] | [-w]] [-c [count]] [-e [seconds]]

PARAMETER	DESCRIPTION
-a	Leak Address Windowing Extensions (AWE) memory in specified MBs (default is 1)
-c	Count of number of objects to allocate (default is as many as possible). This must be the last option specified
-d	Leak and touch memory in specified MBs (default is 1)
-e	Seconds elapsed between allocations (default is 0)
-g	Create GDI handles of specified size (default 1 byte). Specify a size of 0 to cause GDI object exhaustion
-h	Create handles. Specify -u to also allocate file objects
-i	Exhaust USER desktop heap
-l	Allocate the specified amount of large pages (rounded to large size multiple)
-m	Leak memory in specified MBs (default is 1)
-p	Create processes - add -n to set min working set. Add -n to set min working set of processes to smallest
-r	Reserve memory in specified MBs (default is 1)
-s	Leak shared memory in specified MBs (default is 1)
-t	Create threads - add -n to specify minimum stack reserve (in KB)

PARAMETER	DESCRIPTION
-u	Create USER handles to menus
-v	VirtualLock memory in specified MBs (default is 1)
-w	Reset working set minimum to highest possible value

Runs on:

- Client: Windows Vista and higher
- Server: Windows Server 2003 and higher
- Nano Server: 2016 and higher

Related Links

- **Windows Internals Book** The official updates and errata page for the definitive book on Windows internals, by Mark Russinovich and David Solomon.
- **Windows Sysinternals Administrator's Reference** The official guide to the Sysinternals utilities by Mark Russinovich and Aaron Margosis, including descriptions of all the tools, their features, how to use them for troubleshooting, and example real-world cases of their use.

Download

Download Testlimit (234 KB)

Run now from Sysinternals Live.

ZoomIt v4.52

2 minutes to read • Edit Online

By Mark Russinovich

Published: December 11, 2019

Download ZoomIt (448 KB)
Run now from Sysinternals Live.

Introduction

ZoomIt is a screen zoom and annotation tool for technical presentations that include application demonstrations. ZoomIt runs unobtrusively in the tray and activates with customizable hotkeys to zoom in on an area of the screen, move around while zoomed, and draw on the zoomed image. I wrote ZoomIt to fit my specific needs and use it in all my presentations.

ZoomIt works on all versions of Windows and you can use pen input for ZoomIt drawing on tablet PCs.

Using ZoomIt

The first time you run ZoomIt it presents a configuration dialog that describes ZoomIt's behavior, let's you specify alternate hotkeys for zooming and for entering drawing mode without zooming, and customize the drawing pen color and size. I use the draw-without-zoom option to annotate the screen at its native resolution, for example. ZoomIt also includes a break timer feature that remains active even when you tab away from the timer window and allows you to return to the timer window by clicking on the ZoomIt tray icon.

Shortcuts

ZoomIt offers a number of shortcuts which can extend its usage greatly.

FUNCTION	SHORTCUT
Begin Zoom In Mode	Ctrl+1
Zoom In	Up Key
Zoom Out	Down Key
Begin Drawing (While zoomed)	Left-Click
Begin Drawing (While not zoomed)	Ctrl+2
Red Pen Color	R
Blue Pen Color	B
Yellow Pen Color	Y
Green Pen Color	G

FUNCTION	SHORTCUT
Show Meeting Timer	Ctrl + 3
Live Zoom Mode	Ctrl + 4
Zoom In (Live mode)	Ctrl + Up
Zoom Out (Live mode)	Ctrl + Down

Download ZoomIt (448 KB)

Run now from Sysinternals Live.

Sysinternals Suite

2 minutes to read • Edit Online

By Mark Russinovich
Updated: December 18, 2019

Download Sysinternals Suite (29 MB) **Download Sysinternals Suite for Nano Server** (5.1 MB) **Download Sysinternals Suite for ARM64** (164 KB)

Introduction

The Sysinternals Troubleshooting Utilities have been rolled up into a single Suite of tools. This file contains the individual troubleshooting tools and help files. It does not contain non-troubleshooting tools like the BSOD Screen Saver.

The Suite is a bundling of the following selected Sysinternals Utilities: AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PageDefrag, PendMoves, PipeList, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RegDelNull, RegHide, RegJump, Registry Usage (RU), SDelete, ShareEnum, ShellRunas, Sigcheck, Streams, Strings, Sync, Sysmon, TCPView, VMMap, VolumeID, WhoIs, WinObj, ZoomIt

Sysinternals Community

2 minutes to read • Edit Online

Follow on Twitter

Follow @Sysinternals Follow @MarkRussinovich

Search and Post Questions in the Forums

The Sysinternals Forums allow you to search a growing archive of technical questions and answers.

Browse the Forums

Sysinternals Software License Terms

5 minutes to read • Edit Online

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from technet.microsoft.com/sysinternals, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services,
- and support services

for this software, unless other terms accompany those items. If so, those terms apply.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

If you comply with these license terms, you have the rights below.

Installation and User Rights

You may install and use any number of copies of the software on your devices.

Scope of License

The software is licensed, not sold. This agreement only gives you some rights to use the software. Sysinternals reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. You may not

- work around any technical limitations in the software;
- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- rent, lease or lend the software;
- transfer the software or this agreement to any third party; or
- use the software for commercial software hosting services.

Sensitive Information

Please be aware that, similar to other debug tools that capture “process state” information, files saved by Sysinternals tools may include personally identifiable or other sensitive information (such as usernames, passwords, paths to files accessed, and paths to registry accessed). By using this software, you acknowledge that you are aware of this and take sole responsibility for any personally identifiable or other sensitive information provided to Microsoft or any other party through your use of the software.

Documentation

Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

Export Restrictions

The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting .

Support Services

Because this software is "as is," we may not provide support services for it.

Entire Agreement

This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

Applicable Law

United States . If you acquired the software in the United States , Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

Outside the United States . If you acquired the software in any other country, the laws of that country apply.

Legal Effect

This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

Disclaimer of Warranty

The software is licensed "as-is." You bear the risk of using it. Sysinternals gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this agreement cannot change. To the extent permitted under your local laws, sysinternals excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

Limitation on and Exclusion of Remedies and Damages

You can recover from sysinternals and its suppliers only direct damages up to U.S. $5.00. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.

This limitation applies to

- anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Sysinternals knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this software is distributed in Quebec , Canada , some of the clauses in this agreement are provided below in French.

Remarque : Ce logiciel étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le logiciel visé par une licence est offert « tel quel ». Toute utilisation de ce logiciel est à votre seule risque et péril. Sysinternals n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Sysinternals et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne :

- tout ce qui est relié au logiciel, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Sysinternals connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

Sysinternals Licensing FAQ

2 minutes to read • Edit Online

Published: September 28, 2009

Q: How many copies of Sysinternals utilities may I freely load or use on computers owned by my company?

A: There is no limit to the number of times you may install and use the software on your devices or those you support.

Q: May I distribute Sysinternals utilities in my software, on my website, or with my magazine?

A: No. We are not offering any distribution licenses, even if the 3rd party is distributing them for free. We encourage people to download the utilities from our download center where they can be assured to get the most recent version of the utility.

Q: Can I license or re-use any Sysinternals source code?

A: No. We will no longer offer the Sysinternals source code for download or license.

Q: Will the Sysinternals tools continue to be freely available?

A: Yes, Microsoft has no plans to remove or charge for these tools..

Q: Is there technical support available for the Sysinternals tools?

A: No. All Sysinternals tools are offered 'as is' with no official Microsoft support. We do maintain a Sysinternals dedicated community support forum: https://forum.sysinternals.com/