Sysinternals

Sysinternals 网站由 Mark Russinovich 于 1996 年创建，用于托管该公司先进的系统实用程序和技术信息。 无论是 IT 专业人员还是开发人员，你都会发现 Sysinternals 实用程序可帮助你管理、排查 Windows 和 Linux 系统与应用程序的问题并进行诊断。

- 阅读 Sysinternals 工具的官方指南《使用 Windows Sysinternals 工具排除故障》
- 阅读 Sysinternals 博客，以了解工具更新的详细更新日志
- 观看 Mark 在 YouTube 上的 Sysinternals 更新视频
- 观看 Mark 最受好评的《无法解释的案例》故障排除演示和其他网络直播
- 阅读 Mark 的博客，其中重点介绍了如何使用工具解决实际问题
- 查看 Sysinternals“学习资源”页
- 在 Sysinternals 论坛中发布问题

Sysinternals Live

Sysinternals Live 是一项服务，支持你直接从 Web 运行 Sysinternals 工具，而无需手动下载它们。

在 Windows 资源管理器中将工具的 Sysinternals Live 路径输入为 `live.sysinternals.com/<toolname>` 或 `\\live.sysinternals.com\tools\<toolname>`。 在命令提示符处使用 `\\live.sysinternals.com\tools\<toolname>`。

可以访问 https://live.sysinternals.com/ 以在浏览器或 Windows 资源管理器中查看整个 Sysinternals Live 工具目录。

最近更新

新增功能 （2026 年 3 月 26 日）

- 适用于 macOS 的 listent 1.0
  listent 是一种 macOS 命令行工具，用于发现和列出可执行二进制文件的代码签名权利。 它支持静态扫描、实时进程监视和后台守护程序操作。

- ZoomIt v11.0
  此更新对 ZoomIt（屏幕放大和批注工具）添加了全景/滚动屏幕截图支持、截图期间的文

本提取、中断计时器改进，并为现有 .mp4 文件启用剪裁剪辑编辑器。

- Sysmon v15.2
  Sysmon 高级主机安全监视工具的此次更新改进了对内部事件队列的处理，使服务在高系统负载时更能抵御事件丢失。

- DebugView v5.0
  对 DebugView 的此更新是一种用于显示内核模式和 Win32 调试输出的工具，可改进 Windows 11 支持，并提供具有深色主题的新式 UI，并包括性能优化。

- NotMyFault v4.40
  更新了 NotMyFault 工具，这是一种可以在 Windows 系统上崩溃、挂起并导致内核内存泄漏的工具，此更新增加了安全内核和虚拟机监控程序崩溃触发器。

新增功能 （2026 年 2 月 4 日）

- ZoomIt v10.0
  此更新为 ZoomIt（屏幕放大和批注工具）添加了视频剪辑编辑器，用于在保存录制内容之前进行剪裁，并支持使用系统声音录制。

- 适用于 Linux 的 Sysmon 1.5
  Linux 的 Sysmon 更新是一个工具，用于监视和记录系统活动，包括进程生命周期、网络连接、文件系统写入等等。此次更新增加了用于监视 Linux eBPF 程序加载的 `EbpfEvent`。

新增功能 （2025 年 12 月 16 日）

- Coreinfo v4.0
  对 Coreinfo 的此更新，该工具报告系统的处理器、套接字、NUMA 内存和缓存拓扑，以及支持的处理器功能，现在包括 GUI 版本，并添加了对新式 CPU 中存在的功能的检查。

新增功能 （2025 年 11 月 11 日）

- ZoomIt v9.20
  对 ZoomIt 的此更新（屏幕放大和批注工具）现在可以将屏幕录制保存为 MP4 或 GIF。

新增功能 （2025 年 10 月 13 日）

- ZoomIt v9.10
  ZoomIt 是屏幕缩放、录制和批注实用工具，可为高质量视觉对象添加图像平滑效果。

新增功能 （2025 年 9 月 16 日）

- jcd v1.0
  jcd （跳转更改目录）是适用于 Linux 和 macOS 的 Sysinternals 命令行工具，它提供具有子字符串匹配和智能选择的快速目录导航。

Last updated on 2026/03/26

Sysinternals 实用工具索引

Sysinternals 套件
整个 Sysinternals 实用工具集汇总到单一下载中。

Sysinternals Suite for Nano Server
单一下载中的适用于 Nano Server 的 Sysinternals 套件。

适用于 ARM64 的 Sysinternals 套件
单个下载版的适用于 ARM64 的 Sysinternals 工具套件。

Microsoft Store中的Sysinternals Suite
通过 Microsoft Store 安装和更新 Sysinternals 实用工具。

AccessChk
v6.15 (2022 年 5 月 11 日)
AccessChk 是一款命令行工具，用于查看文件、注册表项、服务、进程、内核对象等有哪些有效权限。

AccessEnum
v1.35（2022 年 9 月 29 日）
此简单而强大的安全工具可以显示系统中哪些用户拥有对目录、文件和注册表项的访问权限。使用它来查找权限中的漏洞。

AdExplorer
v1.52（2022 年 11 月 28 日）
Active Directory 浏览器是一个高级的 Active Directory（AD）查看器和编辑器。

AdInsight
v1.2（2015 年 10 月 26 日）
LDAP（轻型目录访问协议）实时监视工具，旨在排查Active Directory客户端应用程序问题。

AdRestore
v1.2（2020 年 11 月 25 日）
取消删除 Server 2003 Active Directory对象。

Autologon
v3.10（2016 年 8 月 29 日）
在登录期间绕过密码屏幕。

自动运行

v14.11（2024 年 2 月 6 日）

查看在系统启动时和用户登录时配置为自动启动的程序。 Autoruns 还会显示应用程序可在其中配置自动启动设置的注册表和文件位置的完整列表。

BgInfo

v4.33（2025 年 2 月 13 日）

此完全可配置的程序会自动生成桌面背景，其中包含有关系统的重要信息，包括 IP 地址、计算机名称、网络适配器等。

BlueScreen

v3.2（2006 年 11 月 1 日）

此屏幕保护程序不仅准确模拟蓝屏，还模拟重启（使用 CHKDSK 完成），并适用于 WINDOWS NT 4、Windows 2000、Windows XP、Server 2003 和 Windows 95 和 98。

CacheSet

v1.02（2021 年 11 月 16 日）

CacheSet 是一个程序，可用于使用 NT 提供的函数控制缓存管理器的工作集大小。 它与 NT 的所有版本兼容。

ClockRes

v2.1（2016 年 7 月 4 日）

查看系统时钟的分辨率，这也是最大计时器分辨率。

Contig

v1.83（2023 年 3 月 9 日）

你是否希望快速对常用文件进行碎片整理？ 使用 Contig 优化单个文件，或创建连续的新文件。

Coreinfo*v4.0 （2025 年 12 月 16 日）*

Coreinfo 是新命令行实用程序，可显示逻辑处理器与物理处理器、NUMA 节点和它们所在套接字之间的映射，以及分配给每个逻辑处理器的缓存。

Ctrl2Cap

v3.0（2025 年 2 月 13 日）

Ctrl2Cap 是帮助将 Caps Lock 键重新映射到 Ctrl 的工具。

DebugView

v5.0 （2026 年 3 月 26 日）

Sysinternals 又一个开创性成果：此程序拦截设备驱动程序对 DbgPrint 的调用，以及 Win32 程

序对 OutputDebugString 的调用。 它允许在没有活动调试器的情况下查看和记录本地计算机或 Internet 上的调试会话输出。

台式机

v2.01（2021 年 10 月 12 日）

使用此新实用工具时，可以创建最多四个虚拟桌面，并使用托盘界面或热键预览每个桌面上的内容，并在它们之间轻松切换。

Disk2vhd

v2.02（2021 年 10 月 12 日）

Disk2vhd 简化了物理系统向虚拟机的迁移（p2v.md）。

DiskExt

v1.2（2016 年 7 月 4 日）

显示卷磁盘映射。

Diskmon

v2.02（2021 年 10 月 12 日）

此实用工具捕获所有硬盘活动，或充当系统托盘中的软件磁盘活动指示灯。

DiskView

v2.41（2020 年 10 月 15 日）

图形磁盘扇区实用工具。

磁盘使用情况（DU）

v1.62（2020 年 11 月 4 日）

按目录查看磁盘使用情况。

EFSDump

v1.03（2021 年 10 月 12 日）

查看加密文件的信息。

FindLinks

v1.1（2016 年 7 月 4 日）

FindLinks 会报告为指定文件存在的文件索引和任何硬链接（同一 volume.md 上的备用文件路径）。 只要文件至少具有一个引用它的文件名，文件的数据就会保持已分配状态。

处理

v5.0（2022 年 10 月 26 日）

这是一个方便的命令行实用程序，可显示哪些文件由哪些进程打开等。

Hex2dec

v1.1（2016 年 7 月 4 日）

将十六进制数转换为十进制数，反之亦然。

jcd*1.0.1 2025 年 10 月 13 日）*

使用子字符串匹配和智能选择功能增强的 Linux 和 macOS 目录浏览。Junction

v1.07（2016 年 7 月 4 日）

创建 Win2K NTFS 符号链接。

LDMDump

v1.02（2006 年 11 月 1 日）

转储逻辑磁盘管理器的磁盘数据库的内容，该数据库描述Windows 2000 动态磁盘的分区。

ListDLLs

v3.2（2016 年 7 月 4 日）

列出当前加载的所有 DLL，包括其加载位置和版本号。

listent

1.0 （2026 年 3 月 26 日）

一个命令行工具，用于发现和列出 macOS 可执行二进制文件的代码签名权利。 支持静态扫描、实时进程监视和后台守护程序操作。

LiveKd

v5.62（2017 年 5 月 16 日）

使用Microsoft内核调试器检查实时系统。

LoadOrder

v1.02（2021 年 10 月 12 日）

查看设备在 WinNT/2K 系统上的加载顺序。

LogonSessions

v1.41（2020 年 11 月 25 日）

列出系统上的活动登录会话。

MoveFile

v1.02（2020 年 9 月 17 日）

允许为下一次重新启动安排移动和删除命令。

NotMyFault*v4.40 （2026 年 3 月 26 日）*

Notmyfault 是一个工具，可以导致你的 Windows 系统崩溃、挂起，并引发内核内存泄漏。

NTFSInfo

v1.2（2016 年 7 月 4 日）

使用 NTFSInfo 查看有关 NTFS 卷的详细信息，包括主文件表 (MFT) 的大小和位置及 MFT 区域，以及 NTFS 元数据文件的大小。

PendMoves

v1.3（2020 年 9 月 17 日）

枚举将在下一次启动时执行的文件重命名和删除命令的列表。

PipeList

v1.02（2016 年 7 月 4 日）

显示系统上的命名管道，包括每个管道的最大实例数和活动实例数。

PortMon

v3.03（2012 年 1 月 12 日）

使用此高级监视工具监视串行和并行端口活动。 它了解所有标准串行和并行 IOCTL，甚至会显示发送和接收的部分数据。 版本 3.x 具有强大的新 UI 增强和高级筛选功能。

ProcDump

v11.1（2025 年 11 月 13 日）

此命令行实用工具旨在捕获其他难以隔离和重现 CPU 峰值的进程转储。 它还可作为一个通用的进程转储文件创建工具，并能在进程出现挂起窗口或未处理异常时进行监控和生成进程转储文件。

进程资源管理器*v17.11（2026 年 4 月 9 日）*

了解哪些文件、注册表项和其他对象进程已打开，它们已加载了哪些 DLL 等。 这个独特而强大的实用工具甚至会显示每个进程的所有者。

进程监视器

v4.01（2024 年 6 月 20 日）

实时监视文件系统、注册表、进程、线程和 DLL 活动。

PsExec

v2.43（2023 年 4 月 11 日）

在远程系统上执行进程。

PsFile

v1.04（2023 年 3 月 30 日）

查看远程打开的文件。

PsGetSid

v1.46（2023 年 3 月 30 日）

显示计算机或用户的 SID。

PsInfo

v1.79（2023 年 3 月 30 日）

获取有关系统的信息。

PsKill

v1.17（2023 年 3 月 30 日）

终止本地或远程进程。

PsPing

v2.12（2023 年 3 月 30 日）

测量网络性能。

PsList

v1.41（2023 年 3 月 30 日）

显示有关进程和线程的信息。

PsLoggedOn

v1.35（2016 年 6 月 29 日）

显示已登录到系统的用户。

PsLogList

v2.82（2023 年 3 月 30 日）

导出事件日志记录。

PsPasswd

v1.25（2023 年 3 月 30 日）

更改帐户密码。

PsService

v2.26（2023 年 3 月 30 日）

查看和控制服务。

PsShutdown

v2.6（2023 年 3 月 30 日）

关闭计算机，然后重启计算机（可选）。

PsSuspend

v1.08（2023 年 3 月 30 日）

暂停和继续进程。

PsTools

v2.51（2023 年 4 月 11 日）

PsTools 套件包含命令行实用工具，用于列出在本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志等。

RAMMap

v1.63 （2026 年 3 月 26 日）

高级物理内存使用情况分析实用程序，可在多个不同的选项卡上以不同方式显示使用情况信息。

RDCMan

v3.12 （2026 年 2 月 4 日）

管理多个远程桌面连接。

RegDelNull

v1.11（2016 年 7 月 4 日）

扫描并删除那些包含嵌入空字符、标准注册表编辑工具无法删除的注册表项。

注册表使用情况（RU）

v1.2（2016 年 7 月 4 日）

查看指定注册表项的注册表空间使用情况。

RegJump

v1.11（2021 年 10 月 12 日）

跳转到在 Regedit 中指定的注册表路径。

SDelete

v2.06 （2026 年 3 月 5 日）

使用此符合 DoD 标准的安全删除程序安全地覆盖敏感文件并清理以前删除的文件的可用空间。

ShareEnum

v1.61（2021 年 10 月 12 日）

扫描网络上的文件共享，并查看其安全设置以关闭安全漏洞。

ShellRunas

v1.02（2021 年 10 月 12 日）

通过一个方便的 shell 上下文菜单条目以不同的用户身份启动程序。

Sigcheck

v2.91 (2026 年 2 月 4 日)

转储文件版本信息，并验证计算机上的图像是否已进行数字签名。

数据流

v1.6 (2016 年 7 月 4 日)

显示 NTFS 备用流。

字符串

v2.54 (2021 年 6 月 22 日)

在二进制图像中搜索 ANSI 和 UNICODE 字符串。

Sync

v2.2 (2016 年 7 月 4 日)

将缓存的数据刷新到磁盘。

Sysmon

v15.2 (2026 年 3 月 26 日)

通过Windows事件日志监视和报告关键系统活动。

TCPView

v4.19 (2023 年 4 月 11 日)

活动套接字查看器。

VMMap

v3.4 (2023 年 10 月 18 日)

VMMap 是进程虚拟和物理内存分析实用程序。

VolumeId

v2.1 (2016 年 7 月 4 日)

设置 FAT 或 NTFS 驱动器的卷 ID。

Whois

v1.20 (2019 年 12 月 11 日)

查看谁拥有 Internet 地址。

WinObj

v3.14 (2022 年 1 月 27 日)

此处提供了最终对象管理器命名空间查看器。

ZoomItv11.0 *(2026 年 3 月 26 日)*

用于在屏幕上缩放和绘图的演示文稿实用工具。

Last updated on 2026/04/09

Sysinternals 文件和磁盘实用工具

AccessChk
此工具显示你指定的用户或组对文件、注册表项或 Windows 服务的访问权限。

AccessEnum
这个简单但功能强大的安全工具可显示谁有权访问系统上的目录、文件和注册表项。 使用它来查找权限中的漏洞。

CacheSet
CacheSet 是一个程序，可用于使用 NT 提供的函数控制缓存管理器的工作集大小。 它与 NT 的所有版本兼容。

Contig
希望你能够快速对常用文件进行碎片整理？ 使用 Contig 优化单个文件，或创建连续的新文件。

Disk2vhd
Disk2vhd 简化了物理系统到虚拟机（p2v）的迁移。

DiskExt
显示卷磁盘映射。

DiskMon
此实用工具捕获所有硬盘活动，或充当系统托盘中的软件磁盘活动指示灯。

DiskView
图形磁盘扇区实用工具。

磁盘使用情况（DU）
按目录查看磁盘使用情况。

EFSDump
查看加密文件的信息。

FindLinks
FindLinks 报告文件索引和指定文件存在的任何硬链接（同一卷上的备用文件路径）。 只要文件至少具有一个引用它的文件名，文件的数据就会保持已分配状态。

jcd
jcd 是一种命令行工具，它为 Linux 和 macOS 提供子字符串匹配和智能选择的快速目录导航。

交接点
创建 Win2K NTFS 符号链接。

LDMDump

转储逻辑磁盘管理器的磁盘数据库的内容，该数据库描述 Windows 2000 动态磁盘的分区。

listent

一个命令行工具，用于发现和列出 macOS 可执行二进制文件的代码签名权利。 支持静态扫描、实时进程监视和后台守护程序操作。

MoveFile

计划下一次重新启动时执行文件重命名和删除命令。 这对于清理固执或正在使用的恶意软件文件非常有用。

NTFSInfo

使用 NTFSInfo 查看有关 NTFS 卷的详细信息，包括主文件表 (MFT) 的大小和位置及 MFT 区域，以及 NTFS 元数据文件的大小。

PendMoves

查看在下次系统启动时计划删除或重命名哪些文件。

进程监视器

实时监视文件系统、注册表、进程、线程和 DLL 活动。

PsFile

查看远程打开的文件。

PsTools

PsTools 套件包括命令行实用工具，用于列出在本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志等。

SDelete

使用此符合 DoD 标准的安全删除程序安全地覆盖敏感文件并清理以前删除的文件的可用空间。

ShareEnum

扫描网络上的文件共享，并查看其安全设置以关闭安全漏洞。

Sigcheck

转储文件版本信息，并验证计算机上的图像是否已进行数字签名。

数据流

显示 NTFS 备用流。

Sync

将缓存的数据刷新到磁盘。

VolumeID

设置 FAT 或 NTFS 驱动器的卷 ID。

Last updated on 2026/03/26

AccessChk v6.15

项目 • 2024/07/25

作者： Mark Russinovich

发布日期：2022 年 5 月 11 日

 **下载 AccessChk** (1 MB)
立即从 Sysinternals Live 运行。

简介

为了确保其创建的环境是安全的，Windows 管理员通常需要了解特定用户或组对哪此类型的资源具有访问权限，资源包括文件、目录、注册表项、全局对象和 Windows 服务等。 AccessChk 能够以直观的界面和输出快速回答此类问题。

安装

AccessChk 是一个控制台程序。 将 AccessChk 复制到可执行路径上。 键入“accesschk”会显示其使用语法。

使用 AccessChk

用法：

Windows 命令提示符

```
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>
```

展开表

参数	说明
-a	名称是 Windows 帐户权限。 指定 `"*"` 为名称以显示分配给用户的所有权限。 请注意，指定特定权限时，仅显示直接分配给此权限的组和帐户。
-c	名称是 Windows 服务，例如 `ssdpsrv`。 指定 `"*"` 作为名称，以显示所有服务和 `scmanager`，检查服务控制管理器的安全性。

参数	说明
-d	仅进程目录或顶级键
-e	令显示明确设置的完整性级别（Windows Vista 以及更高级别）
-f	如果遵循 `-p`，则显示包括组和权限在内的进程令牌完整信息。 否则是由逗号分隔的帐户列表，用于从输出进行筛选。
-h	名称是文件或打印机共享。 将 `"*"` 指定为显示所有共享的名称。
-i	转储完整访问控制列表时，忽略仅具有继承的 ACE 的对象。
-k	名称是注册表项，例如 `hklm\software`
-l	显示完整的安全描述符。 添加 `-i` 以忽略继承的 ACE。
-n	仅显示没有访问权限的对象
-o	名称是对象管理器命名空间中的对象（默认为根）。 若要查看目录中的内容，请指定以斜杠为结尾的名称，或添加 `-s`。 添加 `-t` 和对象类型（如部分），以便仅查看特定类型的对象。
-p	名称是进程名称或 PID，例如 `cmd.exe`（将 `"*"` 指定为显示所有进程的名称）。 添加 `-f` 以显示包括组和权限在内的进程令牌完整信息。 添加 `-t` 以显示线程。
-nobanner	不显示启动横幅和版权消息。
-r	仅显示具有访问权限的对象
-s	Recurse
-t	对象类型筛选器，例如 `"section"`
-u	禁止显示错误
-v	详细（包括 Windows Vista 完整性级别）
-w	仅显示具有写入权限的对象

如果指定用户或组名称和路径，AccessChk 将报告该帐户的有效权限；否则，它将显示安全描述符中引用的帐户的有效访问权限。

默认情况下，路径名称被解释为文件系统路径（使用 `"\pipe\"` 前缀来指定已命名的管道路径）。 对于每个对象，如果帐户具有读取权限，`W` 具有写入权限，以及两项权限中任何一项都没有，则 AccessChk 打印“`R`”。 `-v` 开关让 AccessChk 转储授予帐户的特定访问权限。

示例

以下命令报告 Power 用户帐户对 `\Windows\System32` 中的文件和目录具有的访问权限：

Windows 命令提示符

```
accesschk "power users" c:\windows\system32
```

此命令显示用户组中哪些 Windows 服务成员具有写入访问权限：

Windows 命令提示符

```
accesschk users -cw *
```

查看 `HKLM\CurrentUser` 下特定帐户无权访问的注册表项：

Windows 命令提示符

```
accesschk -kns austin\mruss hklm\software
```

查看 HKLM\Software 密钥的安全性：

Windows 命令提示符

```
accesschk -k hklm\software
```

查看 Vista 上的 `\Users\Mark` 下具有显式完整性级别的所有文件：

Windows 命令提示符

```
accesschk -e -s c:\users\mark
```

查看每个人都可以修改的所有全局对象：

Windows 命令提示符

```
accesschk -wuo everyone \basednamedobjects
```

 **下载 AccessChk** (1 MB)

立即从 Sysinternals Live 运行。

AccessEnum v1.35

项目 • 2024/07/25

作者：Mark Russinovich

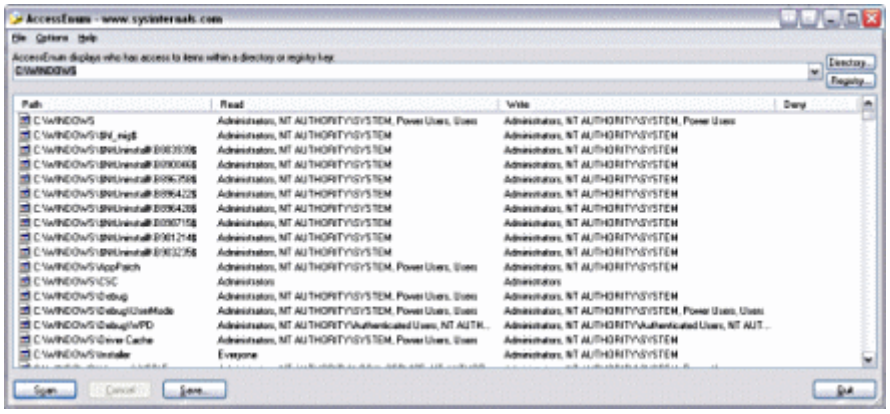
发布时间：2022 年 9 月 29 日

下载 AccessEnum (135 KB)

立即从 Sysinternals Live 运行。

简介

虽然基于 Windows NT 的系统采用的灵活安全模型允许完全控制安全性和文件权限，但管理权限以便用户对文件、目录和注册表项具有适当访问权限可能很困难。 没有内置的方法可以快速查看用户对目录树或键的访问。 *AccessEnum* 可在数秒内提供文件系统和注册表安全设置的完整视图，使其成为帮助查找安全漏洞和在必要时锁定权限的理想工具。



工作原理

AccessEnum 使用标准 Windows 安全 API，使用读取、写入和拒绝访问信息填充其 listview。

下载 AccessEnum (135 KB)

立即从 Sysinternals Live 运行。

CacheSet v1.02

项目 • 2024/07/25

作者：Mark Russinovich

发布时间：2021 年 12 月 16 日

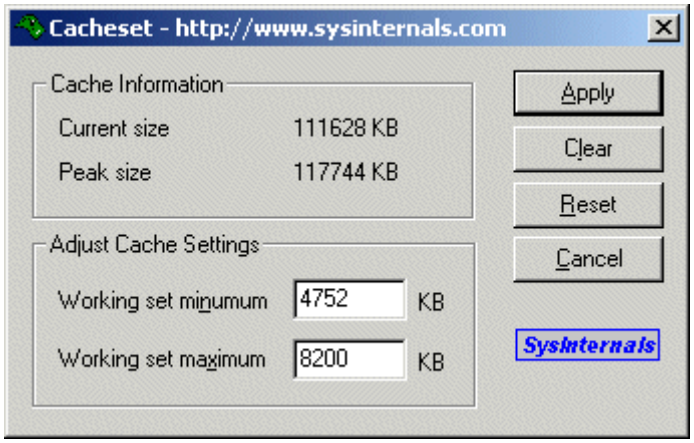
下载 CacheSet **(417 KB)**
立即从 Sysinternals Live 运行。

简介

CacheSet 是一个小应用程序，可用于操作系统文件缓存的工作集参数。 与 CacheMan 不同，*CacheSet* 在所有版本的 NT 上运行，无需修改即可在新的 Service Pack 版本上运行。 除了可以控制最小和最大工作集大小，它还允许重置缓存的工作集，强制它根据需要从最小起点增长。 此外，与 CacheMan 不同，使用 *CacheSet* 所做的更改会立即影响缓存的大小。

使用 *CacheSet* 优化系统缓存大小的性能，如果不按照 CacheMan 调整内部变量的方式是无法实现的。

注意：若要在 NT 4.0 Service Pack 4 及更高版本上使用 *CacheSet*，必须具有"增加配额"权限（管理员帐户默认拥有此权限）。 *CacheSet* 已更新为启用此权限，使其在 SP4 上运行。



安装和使用

启动后，它会显示系统文件缓存的当前大小（每秒更新两次）、其峰值大小（自上次重新启动以来的最大大小），并允许设置新的最小和最大工作集大小。

设置新大小只需输入新的最小和最大大小，然后点击“应用”按钮。 如果收到错误，则意味着存在以下情况之一：输入的最大值小于最小值、输入的最小值小于系统工作集的最小大小，或者输入的最大值大于系统工作集的最大大小。 调整输入的值，然后重试。

你可能会注意到，缓存的大小会立即更改，然后继续快速缩小或增长。 这是因为系统每秒自动剪裁一次工作集。 释放的缓存页面仍在内存中，但可以快速放弃以供需要更多内存的其他程序使用。 同样，当应用程序访问文件系统数据时，缓存可轻松重新获得页面。

重置以前的值随时可以通过点击“重置”按钮还原缓存的工作集值，这些值在上次启动 *CacheSet* 时处于活动状态。

清除缓存的工作集可以通过按“清除”按钮强制缓存释放所有页面。 请注意，缓存可以根据需要再次增长，这与刷新缓存不同 - 分配给缓存的页面只是可供其他程序使用，可以被缓存回收。

使用命令行接口可以在 *CacheSet* 的命令行上输入最小和最大工作集大小。 *CacheSet* 将应用这些新值，不予提示。 因此，可以将 *CacheSet* 添加到“开始”程序组，以在每次启动时自动设置缓存的大小。

用法： CacheSet [**最小工作集**] [**最大工作集**]

工作原理

CacheSet 使用 **NtQuerySystemInformation** 调用来获取有关缓存设置的信息，使用 **NtSetSystemInformation** 设置新的大小信息。 进程的工作集信息充当 NT 内存管理器关于应分配给应用程序的物理内存页数的指南。 因为它们是指南，所以条件可能会导致内存管理器将工作集增大到大于最大值，或缩小到小于最小值。 但是，这些设置是影响应用程序整体分配以及响应能力的因素。 对于 *CacheSet*，应用程序是文件系统缓存。

NtSetSystemInformation 在内部调用 **MmAdjustWorkingSetSize**，这会增大应用程序的工作集或对其进行剪裁。 如果传递给 **MmAdjustWorkingSetSize** 的第三个参数为 1，则会调整系统缓存的工作集，否则在当前进程上进行调整（系统信息调用仅影响系统缓存）。 传入的最小值和最大值为 -1 会导致 **MmAjustWorkingSetSize** 执行工作集清除操作，从而从应用程序的工作集中释放所有页面。

下载 CacheSet (417 KB)

立即从 Sysinternals Live 运行。

运行平台：

- 客户端：Windows Vista 及更高版本。

- 服务器：Windows Server 2008 及更高版本。

Contig v1.83

项目 • 2023/08/03

作者： Mark Russinovich

发布日期：2023 年 3 月 9 日

下载 Contig (366 KB)

简介

市场上有许多 NT 磁盘碎片整理程序，包括 Winternals *Defrag Manager*。 这些工具可用于执行磁盘的常规碎片整理，但尽管大多数文件都是在这些实用工具处理的驱动器上进行碎片整理的，但某些文件可能不是。 此外，很难确保对常用的特定文件进行碎片整理 - 由于所应用的碎片整理产品所使用的碎片整理算法的特定原因，这些文件可能仍然保持碎片化状态。 最后，即使所有文件都已进行碎片整理，但对关键文件的后续更改仍可能导致它们碎片化。 只有运行完整的碎片整理操作，用户才有希望再次对它们进行碎片整理。

Contig 是一个单文件碎片整理程序，它可尝试使文件在磁盘上保持连续。 它非常适合对持续碎片化的文件进行快速优化，或对你希望尽量减少碎片的文件进行快速优化。

使用 Contig

Contig 是一种对指定文件进行碎片整理的实用工具。 使用它来优化常用文件的执行。

用法：

Windows 命令提示符

```
Contig.exe [-a] [-s] [-q] [-v] [existing file]
Contig.exe [-f] [-q] [-v] [drive:]
Contig.exe [-v] [-l] -n [new file] [new file length]
```

参数	说明
-a	分析碎片
-f	分析可用空间碎片
-l	设置有效数据长度以便快速创建文件（需要管理员权限）

参数	说明
-q	安静模式
-s	递归子目录
-v	详细

Contig 还可以分析以下 NTFS 元数据文件并对其进行碎片整理：

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

工作方式

Contig 使用通过 NT 4.0 引入的本机 Windows NT 碎片整理支持（有关详细信息，请参阅我的碎片整理 API 文档）。 它将首先扫描磁盘，以收集可用区域的位置和大小。 然后确定问题文件所在的位置。 接下来，*Contig* 会根据可用区域和文件当前包含的碎片数来决定是否可以优化文件。 如果文件可以优化，则会将其移动到磁盘的可用空间中。

更多信息

Helen Custer 的《*Inside Windows NT*》很好地概述了对象管理器名称空间，Mark 的 1997 年 10 月 Windows NT 杂志专栏*"Inside the Object Manager"*（当然）也是出色的概述。

下载 Contig (366 KB)

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。
- Nano Server：2016 及更高版本。

Disk2vhd v2.02

项目 • 2023/08/09

作者：Mark Russinovich

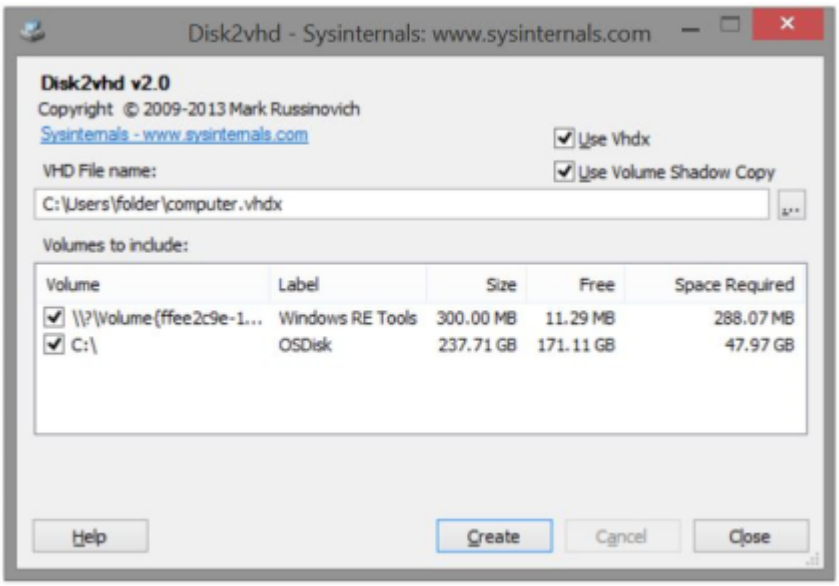
发布日期：2021 年 10 月 12 日

下载 Disk2vhd (564 KB)
立即从 Sysinternals Live 运行。

简介

Disk2vhd 是一个实用工具，用于创建 VHD（虚拟硬盘 - Microsoft 的虚拟机磁盘格式）版本的物理磁盘，以便在 Microsoft 虚拟电脑或 Microsoft Hyper-V 虚拟机 (VM) 中使用。 Disk2vhd 和其他物理转虚拟工具的区别在于，你可以在联机系统上运行 Disk2vhd。 Disk2vhd 使用 Windows XP 中引入的 Windows 卷快照功能，为要包含在转换中的卷创建一致的时间点快照。 甚至可以让 Disk2vhd 在本地卷上创建 VHD，即使 VHD 可以通过转换获得（但磁盘上的 VHD 不同于转换的 VHD，其性能更优）。

Disk2vhd 用户界面列出了系统上存在的卷：



它将为所选卷所在的每个磁盘创建一个 VHD。 它保留磁盘的分区信息，但仅复制所选磁盘上的卷的数据内容。 例如，这使你能够仅捕获系统卷并排除数据卷。

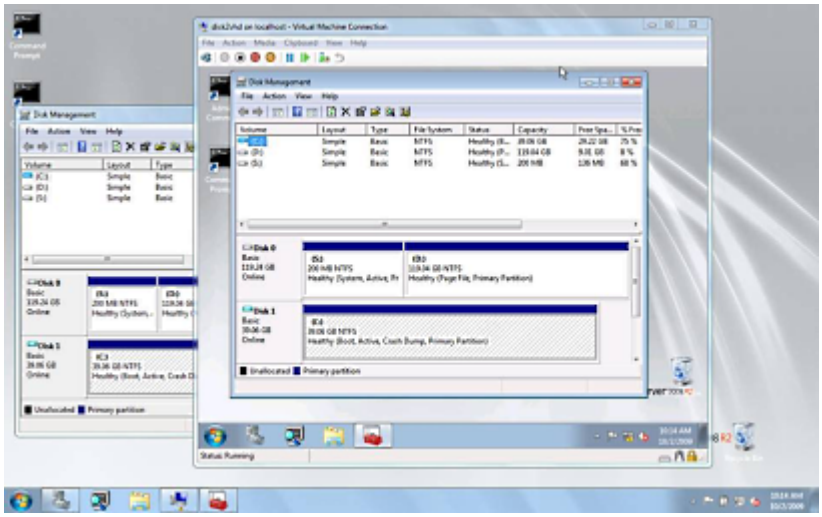
> 虚拟电脑支持的最大虚拟磁盘大小为 127GB。 如果基于更大的磁盘创建 VHD，则无法从虚拟电脑 VM 访问该 VHD。

若要使用 Disk2vhd 生成的 VHD，请创建具有所需特征的 VM，并将 VHD 作为 IDE 磁盘添加到 VM 的配置中。 首次启动时，启动所捕获 Windows 副本的 VM 将检测 VM 的硬件并自动安装驱动程序（如果映像中存在）。 如果所需的驱动程序不存在，请通过虚拟电脑或 Hyper-V 集成组件安装它们。 还可以使用 Windows 7 或 Windows Server 2008 R2 磁盘管理或 Diskpart 实用工具附加到 VHD。

> 如果计划从 VHD 启动，请不要附加到创建这些 VHD 时所在的同一系统上的 VHD。 如果这样做，Windows 将为 VHD 分配新的磁盘签名，以避免与 VHD 源磁盘的签名冲突。 Windows 通过磁盘签名引用启动配置数据库 (BCD) 中的磁盘，因此当发生这种情况时，在 VM 中启动的 Windows 将无法找到启动磁盘。
>
> Disk2vhd 不支持在启用 Bitlocker 的情况下转换卷。 如果要为此类卷创建 VHD，请先关闭 Bitlocker 并等待卷完全解密。

Disk2vhd 在 Windows Vista、Windows Server 2008 及更高版本（包括 x64 系统）上运行。

下面的屏幕截图显示在虚拟机中运行的 Windows Server 2008 R2 Hyper-V 系统副本（该虚拟机基于创建该虚拟机时所在的系统）：



（单击图像可放大）

命令行用法

Disk2vhd 包括命令行选项，支持你编写 VHD 的创建脚本。 通过驱动器号（如 c:）指定你要在快照中包含的卷，或者使用“*”包含所有卷。

用法：**disk2vhd <[drive: [drive:]...]|[*]><vhdfile>**
示例：**disk2vhd * c:\vhd\snapshot.vhd**

> Windows 安装的物理到虚拟硬盘驱动器迁移对于拥有软件保障和 Windows XP、Windows Vista 和 Windows 7 的完整零售副本的客户而言是一项有效的功能。 软件

> 保障为用户提供了宝贵的权益，请联系 Microsoft Corporation 以获取更多信息。 原始设备制造商 (OEM) 使用 OEM 版本的 Windows XP、Windows Vista 和 Windows 7 安装的这些产品根据 Microsoft 许可条款，可能不会转移到虚拟硬盘。

 **下载 Disk2vhd** **(564 KB)**

立即从 Sysinternals Live 运行。

DiskExt v1.2

项目 • 2024/11/21

作者：Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 DiskExt** **(498 KB)**

简介

DiskExt 演示了 IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS 命令的使用，其返回有关卷分区位于什么磁盘（多分区磁盘可以位于多个磁盘上）以及分区在磁盘上位置的信息。

 **下载 DiskExt** **(498 KB)**

DiskMon v2.02

项目 • 2024/07/25

作者：Mark Russinovich

发布时间：2021 年 10 月 12 日

 **下载 Diskmon** **(488 KB)**
立即从 Sysinternals Live 运行。

简介

DiskMon 是一个应用程序，用于记录并显示 Windows 系统上的所有硬盘活动。 还可以将 *DiskMon* 最小化到系统托盘中，在那里它充当磁盘指示灯，当有磁盘读取活动时显示绿色图标，而当有磁盘写入活动时显示红色图标。

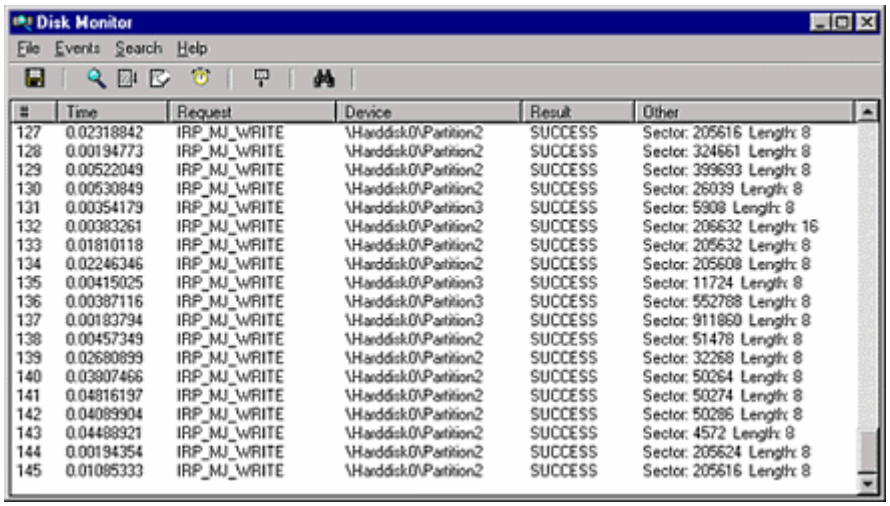
安装和使用

安装 *DiskMon* 就像解压缩并键入“diskmon”一样简单。菜单和工具栏按钮可用于禁用事件捕获、控制列表视图的滚动，以及将列表视图内容保存到 ASCII 文件。

若要让 *DiskMon* 在系统托盘中充当磁盘指示灯，请选择“选项|最小化到托盘”菜单项，或使用“/l”（小写 L）命令行开关启动 *DiskMon*（例如 diskmon /l）。 若要重新激活 *DiskMon* 窗口，请双击 *DiskMon* 托盘图标。 若要在托盘中创建 Diskmon 的快捷方式，请在 Program Files\Startup 文件夹中创建快捷方式，编辑快捷方式的属性，并将“目标”设置为指向可执行文件，路径以引号括起，开关放在引号外：

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

读取和写入偏移量以扇区（512 字节）表示。 事件可以按其持续时间（以微秒为单位）进行计时，也可以用它们启动的绝对时间进行标记。 “历史记录深度”对话框可用于指定将保留在 GUI 中的最大记录数（0 表示没有限制）。



实现

DiskMon 使用内核事件跟踪。 事件跟踪记录在 Microsoft 平台 SDK 中，SDK 包含 TraceDmp 的源代码，*DiskMon* 基于该源代码。

下载 Diskmon (488 KB)

立即从 Sysinternals Live 运行。

Disk Usage v1.62

项目 • 2024/07/25

作者： Mark Russinovich

发布日期：2020 年 11 月 4 日

] **下载 Du** **(1.62 MB)**

简介

Du（磁盘使用情况）会报告指定目录的磁盘空间使用情况。 默认情况下，它会递归目录以显示目录及其子目录的总大小。

使用 Disk Usage (DU)

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

展开表

参数	说明
-c	将输出打印为 CSV。 使用 -ct 实现制表符分隔。
-l	指定信息的子目录深度（默认为 0 级）。
-n	不要递归。
-v	显示中间目录的大小 (KB)。
-u	对硬链接文件的每个实例进行计数。
-q	安静。
-nobanner	不显示启动横幅和版权消息。

CSV 输出的格式为：

Path, CurrentFileCount, CurrentFileSize, FileCount, DirectoryCount, DirectorySize, DirectorySizeOnDisk

 **下载 Du** **(1.62 MB)**

DiskView v2.41

项目 • 2024/07/25

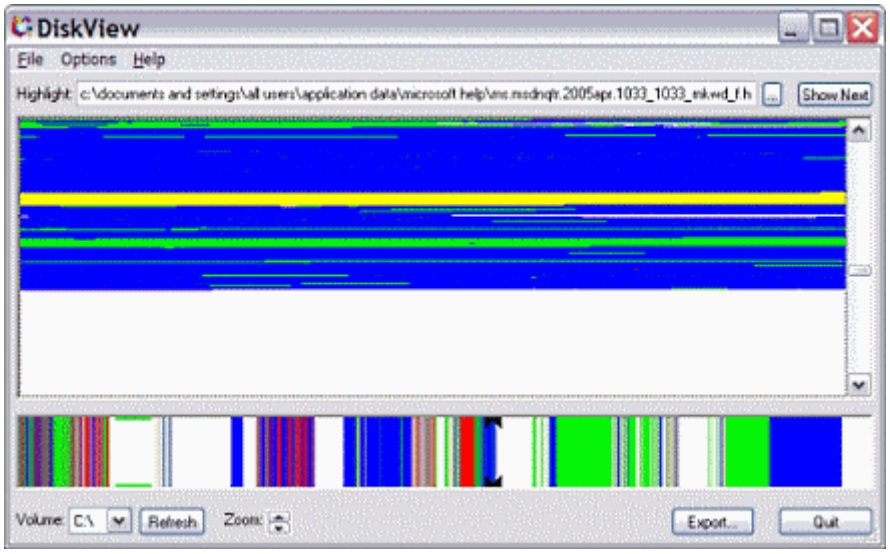
作者：Mark Russinovich

发布事件：2020 年 10 月 15 日

下载 DiskView (800 KB)
立即从 Sysinternals Live 运行。

简介

DiskView 可显示磁盘的图形地图，支持你确定文件所在的位置，或者通过单击簇查看哪个文件占用它。 双击可获取有关簇分配到的文件的详细信息。



下载 DiskView (800 KB)
立即从 Sysinternals Live 运行。

EFSDump v1.03

项目 • 2024/11/21

作者：Mark Russinovich

发布时间：2021 年 10 月 12 日

 **下载 EFSDump** **(161 KB)**

简介

Windows 2000 引入了加密文件系统 (EFS)，以便用户可以保护其敏感数据。 一些新 API 首次推出以支持此便利系统，其中就有 one-QueryUsersOnEncryptedFile，它让你能够查看谁有权访问加密文件。 此小程序使用 API 显示有权访问加密文件的帐户。

使用 EFSDump

展开表

参数	说明
-s	递归子目录。

EFSDump 采用通配符，例如“efsdump *.txt”。

 **下载 EFSDump** **(161 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

jcd 1.0.1

作者： Mark Russinovich

发布时间： 2025 年 10 月 13 日

下载适用于 Linux 和 macOS 的 jcd （GitHub）

介绍

`jcd` （跳转更改目录）是基于 Rust 的命令行工具，它通过子字符串匹配和智能选择提供增强的目录导航。 它就像`cd`命令，但具有更强的功能！

Features

- 选项卡导航：智能循环遍历所有匹配项，并提供视觉反馈和动画加载指示器
- 双向标签页循环：Tab键向前循环，Shift+Tab键向后循环匹配项
- 区分大小写控制：使用 `-i` 标志进行不区分大小写的匹配，默认值区分大小写。
- 目录忽略支持：使用 `.jcdignore` 具有正则表达式模式的文件跳过不需要的目录
- 灵活忽略配置：支持项目本地、用户和系统范围的忽略文件
- 首次匹配跳转：输入后按 Enter 可立即导航至最佳匹配项
- 优先级匹配顺序：

    1. 完全匹配优于部分匹配
    2. 向上树匹配（父目录）具有最高优先级
    3. 按邻近度排序的树下树匹配（子目录）
    4. 同一优先级内的字母排序

- 子字符串匹配：按部分名称匹配查找目录
- 双向搜索：既向上搜索目录树，也向下搜索子目录

Usage

text

```
Usage:
  jcd [-i] [-x] <directory_pattern>   - Changes directory according to the pattern

Flags:
  -i                    - Case-insensitive matching (default: case-sensitive)
  -x                    - Bypass ignore patterns (search all directories)

directory_pattern:
```

```
jcd <substring>        # Navigate to directory matching substring
jcd <absolute_path>    # Navigate to absolute path
jcd <path/pattern>     # Navigate using path-like patterns
```

安全性

如果你认为你发现了安全问题，请通过 项目的 GitHub 存储库 报告它，而不是打开公共问题。

下载适用于 Linux 和 macOS 的 jcd （GitHub）

运行于：

- Linux
- macOS

Last updated on 2026/03/26

LDMDump v1.02

项目 • 2024/07/25

作者：Mark Russinovich

发布日期：2006 年 11 月 1 日

 **下载 LDMDump** **(43 KB)**

简介

Windows 2000 引入了一种新型磁盘分区方案，该方案由名为逻辑磁盘管理器 (LDM) 的组件管理。 基本磁盘实现标准 DOS 样式的分区表，而动态磁盘使用 LDM 分区。 与 DOS 分区不同，LDM 分区具有多种优势，包括跨磁盘复制、高级卷配置的磁盘上存储（跨卷、镜像卷、条带卷和 RAID-5 卷）。 我在 *Windows 2000 Magazine* 上发表的关于 Windows NT/2000 存储管理的系列文章（3/4 月两期）介绍了每种分区方案的细节。

除了 Windows 2000 资源工具包中的磁盘管理 MMC-snapin 和一个名为 dmdiag 的工具外，没有用于调查描述系统分区布局的 LDM 磁盘数据库内部的工具。 *LDMDump* 是一个实用工具，可用于准确检查磁盘的系统 LDM 数据库副本中存储的内容。 *LDMDump* 显示 LDM 数据库专用标头、目录和对象数据库的内容（其中存储分区、组件和卷定义），然后使用分区表和卷列表汇总其查找结果。

安装和使用 LDMDump

若要使用 *LDMDump*，只需向其传递磁盘的标识符。

用法：ldmdump [-] [-d#]

展开表

参数	说明
-	显示支持的选项和用于输出值的度量单位。
-d#	指定要检查的 *LDMDump* 的磁盘数。 例如，“ldmdump /d0”具有 *LDMDump* 显示存储在磁盘 0 上的 LDM 数据库信息。

工作方式

没有已发布的 API 可用于获取有关磁盘 LDM 分区的详细信息，并且 LDM 数据库格式已完全取消记录。 *LDMDump* 是在各种不同系统上和不断变化的条件下对 LDM 数据库内容的研究基础上开发的。

更多信息

有关磁盘上的 LDM 结构的详细信息，请参阅：

- *走进存储管理，第 2 部分*，作者 Mark Russinovich，Windows 2000 Magazine，2000 年 4月。

 **下载 LDMDump** **(43 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

listent 1.0

作者：马里奥·赫沃特

发布时间： 2026 年 3 月 26 日

下载 listent for macOS（GitHub）

介绍

一个命令行工具，用于发现和列出 macOS 可执行二进制文件的代码签名权利。 支持静态扫描、实时进程监视和后台守护程序操作。

`listent` 以递归方式扫描目录以查找可执行二进制文件并提取其代码签名权利。 它专为需要审核或了解 macOS 应用程序请求的权限的安全研究人员、开发人员和系统管理员设计。

功能

核心功能

- **快速扫描**：使用智能筛选和进度指示器高效遍历目录树
- **权利提取**：使用 macOS `codesign` 从二进制文件中提取权利
- **灵活的筛选**：使用 glob 模式支持按路径和特定权利键进行筛选
- **多种输出格式**：人工可读和结构化 JSON 输出
- **多个路径**：在单个命令中扫描多个目录
- **优雅中断**：使用 Ctrl+C 优雅取消

操作模式

1. 静态扫描模式 （默认）

扫描文件和目录以获取权限：

Bash

```
# Scan default locations (/usr/bin and /usr/sbin)
listent

# Scan specific paths
listent /usr/bin /usr/sbin

# Filter by entitlement patterns
```

```
listent -e "com.apple.security.*"
listent -e "*network*" -e "*debug*"

# JSON output for automation
listent /usr/bin -e "*security*" --json
```

2. 实时监视模式

监视与权限相关的新流程：

Bash

```
# Monitor all new processes
listent monitor

# Monitor with custom polling interval
listent monitor --interval 0.5

# Monitor specific entitlements only
listent monitor -e "com.apple.security.network.*"
```

3. 守护程序模式

在前台持续运行监视（适用于测试或手动守护程序操作）：

Bash

```
# Run as daemon in foreground
listent daemon run

# Daemon with custom config file
listent daemon run --config /etc/listent/custom.toml
```

自定义配置文件模板（`daemon.toml`）：

toml

```
[daemon]
# How often to poll for new processes, in seconds (0.1 - 300.0)
polling_interval = 1.0
# Start automatically when loaded by launchd (RunAtLoad)
auto_start = true

[monitoring]
# Filesystem paths to scan for running process binaries.
# Empty list = monitor processes from all paths.
path_filters = ["/usr/bin", "/usr/sbin"]
# Entitlement patterns to match (glob syntax). Empty list = all entitlements.
```

```
# Examples: "com.apple.security.*", "*network*"
entitlement_filters = []
```

查询日志：

Bash

```
# View listent logs in real-time
log stream --predicate 'subsystem == "com.microsoft.sysinternals.listent"' --level
info

# View recent logs
log show --predicate 'subsystem == "com.microsoft.sysinternals.listent"' --last 1h

# Filter for errors only
log show --predicate 'subsystem == "com.microsoft.sysinternals.listent" AND
messageType == error' --last 24h
```

4. 后台守护程序服务

以通过 launchd 管理的持久系统服务方式运行监控功能：

Bash

```
# Install and start daemon
sudo listent daemon install

# Check daemon status
listent daemon status

# View daemon logs
listent daemon logs
listent daemon logs --since 1h
listent daemon logs --since 30m
listent daemon logs --since "2025-01-15 10:00"
listent daemon logs --format json
listent daemon logs -f                    # Follow logs in real-time

# Stop daemon process
listent daemon stop

# Uninstall service
sudo listent daemon uninstall
```

示例

静态扫描

Bash

```
# Basic scan with progress (uses default /usr/bin and /usr/sbin)
listent

# Multi-directory scan with filtering
listent /usr/bin /usr/sbin -e "*security*"

# Find all network-related entitlements
listent -e "*network*" --json | jq '.results[].entitlements'

# Scan quietly (suppress warnings)
listent /usr/bin --quiet
```

进程监视

Bash

```
# Monitor all processes with 2-second intervals
listent monitor --interval 2.0

# Monitor only security-related entitlements
listent monitor -e "com.apple.security.*"

# Run as daemon with custom config
listent daemon run --config /etc/listent/daemon.toml
```

守护程序管理

Bash

```
# Install daemon with default monitoring (requires sudo)
sudo listent daemon install

# Install with custom configuration file
sudo listent daemon install --config /path/to/config.toml

# View recent daemon activity
listent daemon logs --since 1h

# Check if daemon is running
listent daemon status

# Stop and remove daemon
listent daemon stop
sudo listent daemon uninstall
```

配置

命令行选项

- **路径**：可将多个路径指定为位置参数：`listent /path1 /path2`
- **权限筛选**：`-e "pattern"` 支持完全匹配和 glob（`*`、`?`、`[]`）
- **输出格式**：`--json` 或 `-j` 对于结构化输出，默认值为人可读
- **静默模式**：`--quiet` 或 `-q` 禁止显示有关不可读文件的警告
- **监视**：`listent monitor` 子命令支持实时进程监视
- **监视间隔**：`--interval SECONDS` 设置轮询频率（0.1-300.0，默认值：1.0）
- **守护程序模式**：`listent daemon run` 作为后台守护程序进程运行
- **守护程序管理**：`listent daemon install|uninstall|status|stop|logs`
- **配置文件**：`--config FILE` 或 `-c FILE` 指定守护程序配置路径

权利模式

Bash

```
# Exact match
-e "com.apple.security.network.client"

# Wildcard patterns
-e "com.apple.security.*"        # All Apple security entitlements
-e "*network*"                   # Any entitlement containing "network"
-e "*.debug.*"                   # Debug-related entitlements

# Multiple patterns (OR logic)
-e "com.apple.private.*" -e "*.debug.*"
```

守护程序配置

守护程序设置是通过 TOML 配置文件配置的：

- **默认位置**：`~/.config/listent/daemon.toml`
- **自定义路径**：使用 `--config` 和 `daemon install` 组合

若要更改配置，请编辑配置文件并重启守护程序：

Bash

```
# Edit config
nano ~/.config/listent/daemon.toml
```

```
# Restart daemon
listent daemon stop
sudo listent daemon install
```

示例守护程序配置：

toml

```toml
[daemon]
polling_interval = 1.0
auto_start = true

[monitoring]
path_filters = []
entitlement_filters = ["com.apple.security.*", "*network*"]

[logging]
level = "info"
subsystem = "com.microsoft.sysinternals.listent"
category = "daemon"
```

故障排除

Ctrl+C 在外部终端中不起作用

如果 Ctrl+C 不会在 Terminal.app 或 iTerm2 中中断扫描，这是因为 macOS 终端信号处理问题。

解决方法：在运行 `listent` 之前，请执行：

Bash

```bash
trap - INT
```

这会删除任何现有的中断陷阱并还原默认的 SIGINT 行为。 之后，Ctrl+C 应正常工作。

注意：此问题不会影响 VS Code 的集成终端。

输出格式

Human-Readable （默认）

```
```

```
Found 2 binaries with 5 total entitlements:

/usr/bin/security:
  com.apple.private.platformsso.security: true

/usr/bin/nc:
  com.apple.security.network.client: true
  com.apple.security.network.server: true

Scan Summary:
  Scanned: 156 files
  Matched: 2 files
  Duration: 2.34s
```

JSON 格式

JSON


```json
{
  "results": [
    {
      "path": "/usr/bin/security",
      "entitlements": {
        "com.apple.private.platformsso.security": true
      },
      "entitlement_count": 1
    }
  ],
  "summary": {
    "scanned": 156,
    "matched": 2,
    "duration_ms": 2340,
    "skipped_unreadable": 0
  }
}
```


安全性

如果你认为你发现了安全问题，请通过 项目的 GitHub 存储库 报告它，而不是打开公共问题。

下载适用于 Linux 和 macOS 的 jcd （GitHub）

运行于：

- macOS

Last updated on 2026/03/26

PendMoves v1.3 和 MoveFile v1.02

项目 • 2024/02/08

作者： Mark Russinovich 发布日期：2020 年 9 月 17 日

 **下载 PendMoves 和 MoveFile** (988 KB)

介绍

有几个应用程序（例如服务包和修补程序），它们必须替换正在使用的文件，但却无法替换。 因此，Windows 提供了 MoveFileEx API 来重命名或删除文件，并使调用方能够指定他们希望在下次系统启动时且在引用文件之前执行操作。 会话管理器通过从 HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations 值读取已注册的重命名和删除命令来执行此任务。

PendMoves 用法

这个小程序会转储挂起的重命名/删除值的内容，并在无法访问源文件时报告错误。

Usage: pendmoves
以下示例输出显示了计划在下次重启时删除临时安装文件：

```
Shell
```

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

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

MoveFile 用法

随附的 MoveFile 实用程序可为下一次重新启动安排 move 和 delete 命令：**usage: movefile [源] [目标]**
如果指定空目标 ("")，会在启动时删除源。 删除 test.exe 的示例如下：

```
Shell
```

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

 下载 PendMoves 和 MoveFile (988 KB)

NTFSInfo v1.2

项目 • 2023/08/04

作者：Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 NTFSInfo (143 KB)**

简介

NTFSInfo 是一个小应用，用于显示有关 NTFS 卷的信息。 其转储包括驱动器分配单元的大小、关键 NTFS 文件的位置以及卷上的 NTFS 元数据文件的大小。 此信息通常只是为了满足用户的好奇心，但 *NTFSInfo* 确实显示了一些有趣的内容。 例如，你可能听说过 FAT 文件系统的文件分配表的 NTFS 等效项。 它叫做主文件表 (MFT)，由描述驱动器上所有文件和目录位置的固定大小的记录组成。 MFT 令人惊讶的一点是，它就像任何其他文件一样被作为文件进行管理。 除了指定卷的群集和 MFT 记录的大小外，*NTFSInfo* 还会显示磁盘上（相对于群集）MFT 的位置及其大小。 为了防止 MFT 碎片化，NTFS 会在 MFT 周围保留一部分磁盘，除非磁盘空间不足，否则不会分配给其他文件。 此区域称为 MFT-Zone，*NTFSInfo* 会告诉你 MFT-Zone 在磁盘上的位置以及为其保留的驱动器百分比。

你可能还会惊讶地发现，与 MFT 一样，所有 NTFS 元数据都在文件中管理。 例如，有一个名为 $Boot 的文件映射到覆盖驱动器的启动扇区。 该卷的群集映射保存在名为 $Bitmap 的另一个文件中。 这些文件位于 NTFS 根目录中，但除非你知道它们存在，否则你看不到它们。 尝试在 NTFS 卷的根目录中键入“dir /ah $boot”，你会看到 $boot 文件。 *NTFSInfo* 会执行与“dir /ah”等效的操作，显示所有 NTFS（3.51 和 4.0）元数据文件的名称和大小。

NTFSInfo 是为了配合我 1998 年 1 月 *Windows NT Magazine*的“NT Internals”专栏，其中描述了 NTFS 内部数据结构。

安装和使用

NTFSInfo 适用于所有版本的 NTFS，但适用于 Windows NT 5.0 的 NTFS 具有 *NTFSInfo* 尚未对其进行编程的不同元数据文件。 要使 *NTFSInfo* 正常工作，你必须具有管理权限。

用法：NTFSInfo x

参数	说明
x	你想要检查的 NTFS 卷的驱动器号。

工作原理

NTFSInfo 使用未记录的文件系统控制 (FSCTL) 调用从 NTFS 获取有关卷的信息。 它会输出此信息以及 NTFS 元数据文件的目录转储。

 **下载 NTFSInfo** **(143 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

PendMoves v1.3 和 MoveFile v1.02

项目 • 2024/02/08

作者： Mark Russinovich 发布日期：2020 年 9 月 17 日

 **下载 PendMoves 和 MoveFile** (988 KB)

介绍

有几个应用程序（例如服务包和修补程序），它们必须替换正在使用的文件，但却无法替换。 因此，Windows 提供了 MoveFileEx API 来重命名或删除文件，并使调用方能够指定他们希望在下次系统启动时且在引用文件之前执行操作。 会话管理器通过从 HKLM\System\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations 值读取已注册的重命名和删除命令来执行此任务。

PendMoves 用法

这个小程序会转储挂起的重命名/删除值的内容，并在无法访问源文件时报告错误。

Usage: pendmoves
以下示例输出显示了计划在下次重启时删除临时安装文件：

```
Shell
```

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

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

MoveFile 用法

随附的 MoveFile 实用程序可为下一次重新启动安排 move 和 delete 命令：**usage: movefile [源] [目标]**
如果指定空目标 ("")，会在启动时删除源。 删除 test.exe 的示例如下：

```
Shell
```

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

 下载 PendMoves 和 MoveFile (988 KB)

RegMon for Windows v7.04

项目 • 2023/08/04

作者：Mark Russinovich

发布时间：2006 年 11 月 1 日

RegMon 和 FileMon 不再可供下载。 从 Windows 2000 SP4、Windows XP SP2、Windows Server 2003 SP1 和 Windows Vista 开始，这些 Windows 版本已被进程监视器取代。

相关实用工具

下面是 Sysinternals 中提供的一些其他监视工具：

- PortMon - 串行和并行端口监视器
- 进程监视器 - 进程和线程监视器
- DiskMon - 硬盘监视器
- DebugView - 调试输出监视器

SDelete v2.06

作者：Mark Russinovich

发布时间： 2026 年 3 月 5 日

下载下载 SDelete（328 KB）

简介

Windows NT/2000 (Win2K) C2 合规性的一个功能是实现对象重用保护。 这意味着，当应用程序分配文件空间或虚拟内存时，它无法查看以前存储在 Windows NT/2K 为其分配的资源中的数据。 Windows NT 在向应用程序提供任何类型的资源之前，都会先将内存清零，并将磁盘上放置文件的扇区清零。 但是，对象重用并不要求将文件在删除之前占用的空间清零。 这是因为 Windows NT/2K 的设计假设操作系统控制对系统资源的访问。 但是，当操作系统不处于活动状态时，可以使用原始磁盘编辑器和恢复工具来查看和恢复操作系统已解除分配的数据。 即使使用 Win2K 的加密文件系统 (EFS) 加密文件，在创建文件的新加密版本后，文件的原始未加密文件数据也会保留在磁盘上。

确保已删除的文件以及使用 EFS 加密的文件不被恢复的唯一方法是使用安全的删除应用程序。 安全删除应用程序使用证明可以使磁盘数据不可恢复的技术覆盖已删除文件的磁盘数据，甚至在使用能够读取磁性介质上暴露弱删除文件模式的恢复技术时也是如此。 SDelete（安全删除）就是这样的应用程序。 可以使用 SDelete 来安全地删除现有文件，也可以安全地擦除磁盘未分配部分中存在的任何文件数据（包括已删除或加密的文件）。 SDelete 实施国防部的清除和清理标准 DOD 5220.22-M，让你确信使用 SDelete 删除后，文件数据将永久消失。 请注意，SDelete 可安全地删除文件数据，但不会删除位于可用磁盘空间中的文件名。

使用 SDelete

SDelete 是一个命令行实用工具，它包含许多选项。 在任何给定的使用中，它都允许删除一个或多个文件和/或目录，或者清理逻辑磁盘上的可用空间。 SDelete 接受通配符作为目录或文件说明符的一部分。

用法：

Windows 命令提示符

```
sdelete [-p passes] [-r] [-s] [-q] [-f] <file or directory [...]>
sdelete [-p passes] [-q] [-z|-c] <drive letter [...]>
sdelete [-p passes] [-q] [-z|-c] <physical disk number [...]>
```

展开表

参数	说明
-c	清理可用空间。
-f	强制将仅包含字母的参数视为文件/目录，而不是磁盘。 如果参数包含其他字符（例如路径分隔符或文件扩展名），则不需要此参数。
-p	指定覆盖次数（默认值为 1）。
-q	静默模式。
-r	删除 Read-Only 属性。
-s	递归处理子目录。
-z	将可用空间清零（有利于虚拟磁盘优化）。
-nobanner	不显示启动横幅和版权消息。

- 为了进行清理，磁盘不得带有任何卷。
- 对于驱动器号，请包括 ，例如 。

SDelete 的工作方式

安全删除没有特殊属性的文件相对简单：安全删除程序只是使用安全删除模式覆盖文件。 更棘手的是安全地删除 Windows NT/2K 压缩、加密和稀疏文件，并安全地清理磁盘可用空间。

NTFS 以 16 个集群块为单位管理压缩、加密和稀疏文件。 如果程序写入此类文件的现有部分，则 NTFS 在磁盘上分配新空间来存储新数据，并在写入新数据后解除分配文件以前占用的群集。 NTFS 采取这种保守的方法的原因如下：与数据完整性相关，在压缩和稀疏文件的情况下，新分配大于现有分配（新的压缩数据大于旧的压缩数据）。 因此，企图覆盖此类文件也无法成功移除磁盘上的文件内容。

若要处理这些类型的文件，SDelete 依赖于碎片整理 API。 使用碎片整理 API，SDelete 可以准确确定磁盘上的哪些群集被属于压缩、稀疏和加密文件的数据占用。 *SDelete*知道哪些群集包含文件的数据后，它可以打开磁盘进行原始访问并覆盖这些群集。

清理可用空间带来了另一个挑战。 由于 FAT 和 NTFS 不提供应用程序直接寻址可用空间的方法，因此 SDelete 有两个选项之一。 第一个是，它可以像处理压缩、稀疏和加密文件一样，以原始访问的方式打开磁盘，并覆盖空闲空间。 此方法存在一个大问题：即使 SDelete 被编码为完全能够计算 NTFS 和 FAT 驱动器的可用空间部分（这不是小事），它也会存在与系统上发生的活动文件操作发生冲突的风险。 例如，假设 SDelete 确定群集是空闲的，而此时文件系统驱动程序（FAT、NTFS）决定为另一个应用程序正在修改的文件分配群集。 文件系统驱动程序将新数据写入群集，然后 SDelete 出现并覆盖新写入的数据：文件的新数据不见了。 如果为文件系统元数据分配群集，则问题更严重，因为 SDelete 会损坏文件系统的磁盘结构。

第二种方法（也是 SDelete 采用的方法）是间接覆盖可用空间。 首先，SDelete 会分配其能够处理的最大的文件。 SDelete 使用非缓存文件 I/O 执行此操作，以防止 NT 文件系统缓存的内容被丢弃，并被与 SDelete 的占用空间文件相关的无用数据所替换。 由于非缓存文件 I/O 必须与扇区（512 字节）对齐，即使 SDelete 无法再扩展文件，也可能未能为 SDelete 文件分配一些剩余空间。 为了获取任何剩余空间，SDelete 接下来会分配其所能分配的最大缓存文件。 对于这两个文件，SDelete 执行安全覆盖，确保以前可用的所有磁盘空间都已安全清理。

在 NTFS 驱动器上，SDelete 的作业在分配并覆盖这两个文件后不一定会完成。 SDelete 还必须使用适合 MFT 记录的文件填满 NTFS MFT（主文件表）中的任何现有可用部分。 MFT 记录的大小通常为 1KB，磁盘上的每个文件或目录至少需要一条 MFT 记录。 小文件完全存储在其 MFT 记录之内，而不适合记录的文件则在 MFT 之外分配到群集。 所有 *SDelete* 需要做的就是分配尽可能大的文件——当文件在 MFT 记录中占用了 NTFS 的所有可用空间时，NTFS 会阻止文件增长，因为磁盘上没有剩余可用的群集（它们正被之前分配的两个文件*SDelete*占据）。 然后，SDelete 将重复该过程。 当 SDelete 甚至无法再创建新文件时，它知道主文件表（MFT）中以前可用的所有记录都已完全填充有安全覆盖的文件。

若要覆盖您删除的文件的文件名，SDelete 会重命名该文件 26 次，每次将文件名的每个字符替换为连续的字母字符。 例如，对文件名“foo.txt”的第一次重命名是“AAA.AAA”。

清理磁盘可用空间时 SDelete 不安全地删除文件名的原因是删除文件名需要直接操作目录结构。 目录结构可以具有包含已删除文件名的可用空间，但可用目录空间不能分配给其他文件。 因此，SDelete 无法分配此可用空间，以便可以安全地覆盖它。

下载下载 SDelete（328 KB）

运行于：

- 客户端：Windows 10及更高版本。
- 服务器：Windows Server 2012及更高版本。
- Nano Server：2016 及更高版本。

Last updated on 2026/03/05

Sigcheck v2.91

作者： Mark Russinovich

发布时间： 2026 年 2 月 4 日

 **下载 Sigcheck** **(645 KB)**

简介

Sigcheck 是一种命令行实用工具，可显示文件版本号、时间戳信息和数字签名详细信息（例如证书链）。 它还提供一个用于在 VirusTotal 上检查文件状态的选项、一个针对 40 多个防病毒引擎执行自动文件扫描的站点，以及一个用于上传文件以供扫描的选项。

用法：

Windows 命令提示符

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

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

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

展开表

参数	说明
-a	显示扩展的版本信息。 报告的熵度量是文件内容信息的每字节位数。
-accepteula	以无提示的方式接受 Sigcheck EULA（无交互式提示）
-c	采用逗号分隔符的 CSV 输出
-ct	采用制表符分隔符的 CSV 输出
-d	转储目录文件的内容
-e	仅扫描可执行映像（不考虑其扩展）
-f	在指定的目录文件中查找签名
-h	显示文件哈希
-i	显示目录名和签名链

参数	说明
-l	遍历符号链接和目录联接
-m	转储清单
-n	仅显示文件版本号
-o	使用 -h 选项时，对以前由 Sigcheck 捕获的 CSV 文件中所捕获的哈希执行病毒总数查找。 此用法适用于扫描脱机系统。
-nobanner	不显示启动横幅和版权消息。
-r	禁止检查证书吊销情况
-p	根据指定的策略（由其 GUID 表示）验证签名。
-s	递归操作子目录
-t[u][v]	转储指定证书存储的内容（对于所有存储，使用“*”）。 指定 -tu 以查询用户存储（默认为计算机存储）。 追加“-v”，要求 Sigcheck 下载受信任的 Microsoft 根证书列表，并仅输出未根目录到该列表上的证书的有效证书。 如果站点不可访问，则改为使用当前目录中的 authrootstl.cab 或 authroot.stl（如果存在）。
-u	如果启用了 VirusTotal 检查，则显示 VirusTotal 未知或具有非零检测的文件，否则仅显示未签名的文件。
-v[rs]	在 VirusTotal (www.virustotal.com) 上基于文件哈希查询恶意软件。 添加“r”，打开具有非零检测的文件的报表。 如果指定了“s”选项，会将报告为“以前未扫描”的文件上传到 VirusTotal。 请注意，扫描结果可能在 5 分钟或更长时间内不可用。
-vt	在使用 VirusTotal 功能之前，必须接受 VirusTotal 服务条款。 请参阅：https://www.virustotal.com/en/about/terms-of-service/ 如果尚未接受条款，并且忽略了此选项，系统会以交互方式提示你。

使用此工具的一种方法是，使用以下命令在 `\Windows\System32` 目录中检查未签名的文件：

Windows 命令提示符

```
sigcheck -u -e c:\windows\system32
```

应对未签名的任何文件的用途进行调查。

 **下载 Sigcheck (645 KB)**

运行软件：

- 客户端：Windows 8.1 及更高版本

- 服务器：Windows Server 2012 及更高版本
- Nano Server：2016 及更高版本

了解更多

- Malware Hunting with the Sysinternals Tools （使用 Sysinternals 工具搜寻恶意软件）
  在本演示文稿中，Mark 展示了如何使用 Sysinternals 工具来识别、分析和清理恶意软件。

Last updated on 2026/02/05

Streams v1.6

项目 • 2024/07/25

作者： Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 Streams** (499 KB)

介绍

NTFS 文件系统为应用程序提供了创建备用信息数据流的能力。 默认情况下，所有数据都存储在文件的主要未命名数据流中，但通过使用语法“file:stream”，可以读取和写入备用项。 并非所有应用程序都是为了访问备用流而编写的，但可以非常简单地演示流。 首先，从命令提示符内更改为 NTFS 驱动器上的目录。 接下来，输入“echo hello > test:stream”。 刚刚创建了名为“stream”的流，其与文件“test”关联。 请注意，查看测试大小时，它报告为 0，在任何文本编辑器中打开该文件时，它看起来都是空的。 要查看流，请输入“more < test:stream”（type 命令不接受流语法，因此必须使用更多）。

NT 没有任何工具可以供查看哪些 NTFS 文件有与其相关的流，所以我自己编写了一个。 Streams 将检查指定的文件和目录（注意，目录也可以有备用数据流），并通知其在这些文件内遇到的任何命名流的名称和大小。 Streams 使用未记录的本机函数来检索文件流信息。

使用流

用法: streams [-s] [-d] <**文件或目录**>

展开表

参数	说明
-s	递归子目录。
-d	删除流。
Streams 采用通配符，例如“streams *.txt”。	

 **下载 Streams** (499 KB)

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

Sync v2.2

项目 • 2024/07/25

作者： Mark Russinovich

发布时间：2016 年 7 月 4 日

下载 Sync (500 KB)

介绍

UNIX 提供了一个名为 Sync 的标准实用工具，可用于指示操作系统将所有文件系统数据刷新到磁盘，以确保数据稳定且不会在系统发生故障时丢失。 否则，缓存中存在的任何已修改数据都将丢失。 下面是我编写的等效工具，称为 Sync，适用于所有版本的 Windows。 每当你想要知道已修改的文件数据是否安全地存储在硬盘驱动器上时，请使用它。 遗憾的是，Sync 需要管理权限才能运行。 此版本还允许刷新可移动驱动器，例如 ZIP 驱动器。

使用 Sync

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

展开表

参数	描述
-r	刷新可移动驱动器。
-e	弹出可移动驱动器。

指定特定驱动器（例如“c e”）将导致 Sync 仅刷新这些驱动器。

下载 Sync (500 KB)

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

VolumeID v2.1

项目 • 2024/07/25

作者：Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 VolumeID** **(194 KB)**

简介

虽然 Windows NT/2000 以及 Windows 95 和 98 的内置标签实用工具允许你更改磁盘卷的标签，但它不提供任何更改卷 ID 的方法。 此实用工具 VolumeID 允许更改 FAT 和 NTFS 磁盘的 ID（软盘或硬盘驱动器）。

用法：volumeid <driveletter:> xxxx-xxxx

这是一个命令行工具，必须从命令提示符窗口运行。

请注意，在下次重启之前，NTFS 卷上的更改将不可见。 此外，在更改卷 ID 之前，应关闭已运行的任何应用程序。NT 可能会变得混乱，并认为在 FAT 卷 ID 更改后，介质（磁盘）已更改，并弹出消息指出应重新插入原始磁盘 (!)。 然后，它可能会让使用这些驱动器的应用程序的磁盘请求失败。

 **下载 VolumeID** **(194 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

Sysinternals 网络实用工具

项目 • 2023/08/03

AD 资源管理器

Active Directory 资源管理器是高级的 Active Directory (AD) 查看器和编辑器。

AD Insight

AD Insight 是一种 LDAP（轻型目录访问协议）实时监视工具，旨在对 Active Directory 客户端应用程序进行故障排除。

AdRestore

取消删除 Server 2003 Active Directory 对象。

PipeList

显示系统上的命名管道，包括每个管道的最大实例数和活动实例数。

PsFile

查看远程打开的文件。

PsPing

测量网络性能。

PsTools

PsTools 套件包含命令行实用工具，用于列出在本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志等。

ShareEnum

扫描网络上的文件共享，并查看其安全设置以关闭安全漏洞。

TCPView

活动套接字命令行查看器。

Whois

查看谁拥有 Internet 地址。

Active Directory 资源管理器 v1.52

项目 • 2023/08/03

作者： Mark Russinovich

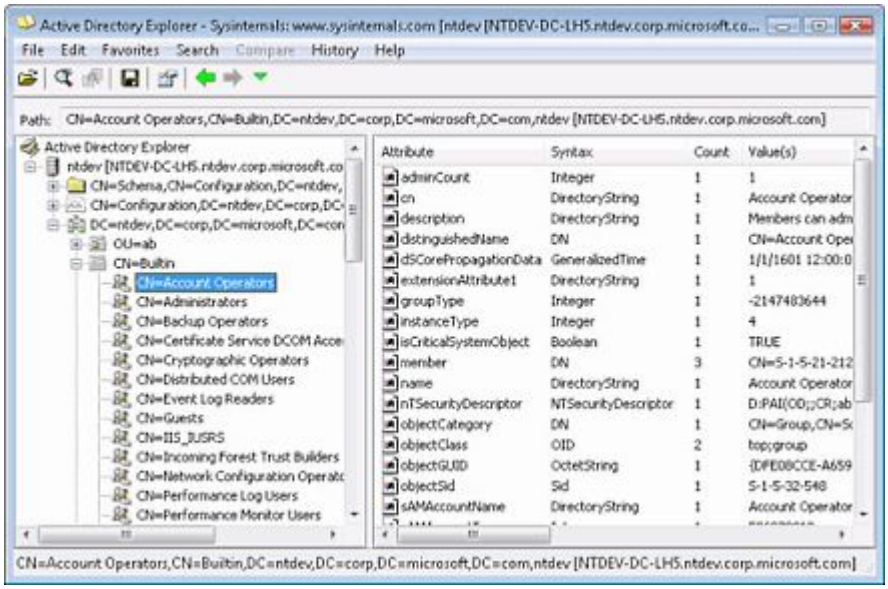
发布时间：2022 年 11 月 28 日

下载 AdExplorer (1.1 MB)
立即从 Sysinternals Live 运行。

简介

Active Directory 资源管理器（AD 资源管理器）是高级 Active Directory (AD) 查看器和编辑器。 可以使用 AD 资源管理器轻松导航 AD 数据库、定义收藏夹位置、查看对象属性和属性，而无需打开对话框、编辑权限、查看对象的架构，并执行可以保存和重新执行的复杂搜索。

AD 资源管理器还能够保存 AD 数据库的快照，以便进行离线查看和比较。 加载保存的快照时，可以像浏览实时数据库一样导航和探索它。 如果有一个 AD 数据库的两个快照，则可以使用 AD 资源管理器的比较功能来查看它们之间更改了哪些对象、属性和安全权限。



下载 AdExplorer (1.1 MB)

立即从 Sysinternals Live 运行。

Active Directory v1.2 见解

项目 • 2023/08/03

作者：Mark Russinovich

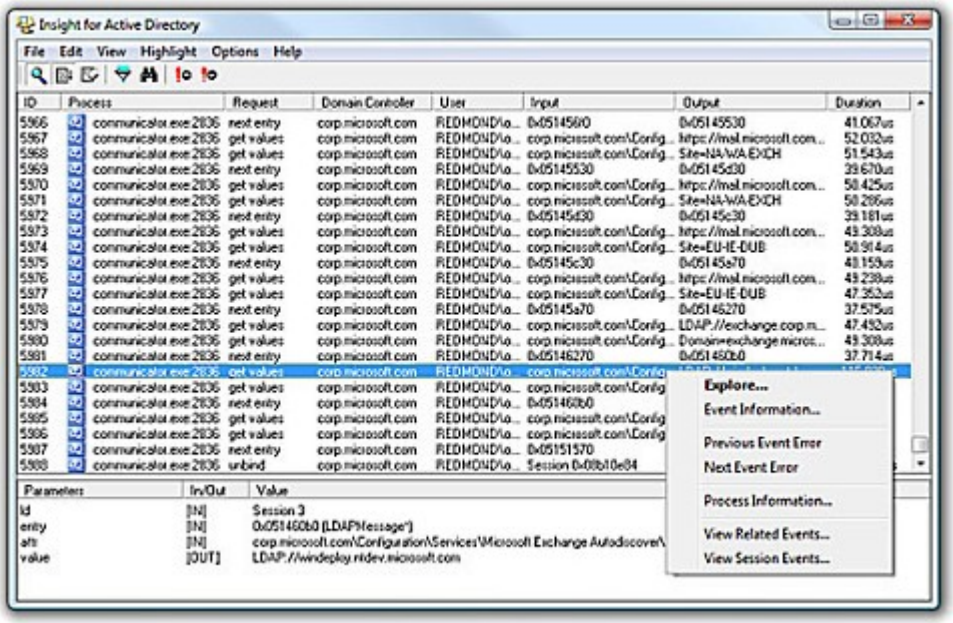
发布时间：2015 年 10 月 26 日

下载 AdInsight (3.3 MB)
立即从 Sysinternals Live 运行。

简介

ADInsight 是一种 LDAP（轻型目录访问协议）实时监视工具，旨在对 Active Directory 客户端应用程序进行故障排除。 使用 Active Directory 客户端与服务器通信的详细跟踪来解决 Windows 身份验证、Exchange、DNS 和其他问题。

ADInsight 使用 DLL 注入技术截获应用程序在 Wldap32.dll 库中发出的调用，该库是基础 Active Directory API（例如 ldap 和 ADSI）的标准库。 与网络监视工具不同，ADInsight 可截获并解释所有客户端 API，包括不会导致传输到服务器的 API。 ADInsight 会监视它可以将其跟踪 DLL 加载到其中的任何进程，这意味着它不需要管理权限，但如果使用管理权限运行，它还将监视系统进程，包括 Windows 服务。



下载 AdInsight (3.3 MB)

立即从 Sysinternals Live 运行。

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

相关链接

使用 Sysinternals AdRestore 实用工具，可以在 Windows Server 2003 域中还原已删除的对象。

AD 资源管理器是高级 Active Directory (AD) 查看器和编辑器。

AdRestore v1.2

项目 • 2023/10/07

作者：Mark Russinovich

发布时间：2020 年 11 月 25 日

 **下载 AdRestore (512 KB)**

介绍

Windows Server 2003 引入了还原已删除（“tombstoned”）对象的功能。 此简单的命令行实用工具可枚举域中已删除的对象，并提供还原每个对象的选项。 源代码基于 Microsoft 平台 SDK 中的示例代码。 此 MS 知识库文章介绍了 AdRestore 的用法：

840001：如何在 Active Directory 中还原已删除的用户帐户及其组成员身份

 **下载 AdRestore 512 KB)**

PipeList v1.02

项目 • 2024/07/25

发布时间：2016 年 7 月 4 日

 **下载 PipeList (496 KB)**

简介

是否知道实现命名管道的设备驱动程序实际上是文件系统驱动程序？ 事实上，驱动程序的名称是 NPFS.SYS，表示“命名管道文件系统”。 你可能还会发现令人惊讶的是，可以获得系统上定义的命名管道的目录列表。 未记录此事实，也无法使用 Win32 API 执行此操作。 直接使用 NtQueryDirectoryFile（Win32 FindFile API 所依赖的本机函数）可以列出管道。 列出 NPFS 返回的目录还会指示为每个管道设置的最大管道实例数和活动实例数。

 **下载 PipeList (496 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

PsFile v1.04

项目 • 2024/02/08

作者： Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools** (5 MB)

介绍

“net file”命令显示其他计算机在你执行命令的系统上打开的文件列表，但它会截断长路径名称，并且不让你查看远程系统的该信息。 *PsFile* 是一个命令行实用工具，用于显示系统上远程打开的文件列表，还允许按名称或文件标识符关闭打开的文件。

安装

只需将 *PsFile* 复制到可执行文件路径，然后键入“psfile”。

使用 PsFile

PsFile 的默认行为是列出本地系统上由远程系统打开的文件。 键入命令后跟“-”会显示有关命令语法的信息。

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

展开表

参数	说明
-u	指定登录远程计算机的可选用户名。
-p	指定用户名的密码。 如果省略此密码，系统将提示你输入密码，而不会将其回显到屏幕。
Id	要显示信息或关闭的文件的标识符（由 PsFile 指定）。
路径	要显示或关闭信息匹配的文件的完整或部分路径。
-c	关闭由 ID 或路径确定的文件。

工作原理

PsFile 使用平台 SDK 中记录的 NET API。

 **下载 PsTools** (5 MB)

PsTools

PsFile 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

PsPing v2.12

项目 • 2023/08/03

作者：Mark Russinovich

发布日期：2023 年 3 月 30 日

 **下载 PsTools (5 MB)**

简介

PsPing 实现了 Ping 功能、TCP ping、延迟和带宽测量。 使用以下命令行选项显示每个测试类型的使用情况：

安装

将 PsPing 复制到可执行文件路径。 键入“psping”会显示其使用情况语法。

使用 PsPing

PsPing 实现了 Ping 功能、TCP ping、延迟和带宽测量。 使用以下命令行选项显示每个测试类型的使用情况：

用法：

Windows 命令提示符

```
psping -? [i|t|l|b\]
```

参数	说明
-? I	ICMP ping 的使用情况。
-? T	TCP ping 的使用情况。
-? L	延迟测试的使用情况。
-? B	带宽测试的使用情况。

ICMP ping 使用情况：

Windows 命令提示符

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

参数	说明
-h	打印直方图（默认桶计数为 20）。
	如果指定一个参数，它会被解释为桶计数，直方图将包含覆盖值的整个时间范围的桶数。 指定以逗号分隔的时间列表来创建自定义直方图（例如“0.01,0.05,1,5,10”）。
-i	间隔(秒)。 对于快速 ping，指定 0。
-l	请求大小。 追加“k”表示千字节，追加“m”表示兆字节。
-n	ping 的数量，或者追加“s”来指定秒数，例如“10s”。
-q	不要在 ping 期间输出。
-t	执行 ping，直到按 Ctrl+C 停止，并键入 Ctrl+Break 查看统计信息。
-w	具有指定迭代次数的预热（默认值为 1）。
-4	强制使用 IPv4。
-6	强制使用 IPv6。

对于高速 ping 测试，请使用 -q 和 -i 0。

TCP ping 使用情况：

Windows 命令提示符

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

参数	说明
-h	打印直方图（默认桶计数为 20）。
	如果指定一个参数，它会被解释为桶计数，直方图将包含覆盖值的整个时间范围的桶数。 指定以逗号分隔的时间列表来创建自定义直方图（例如“0.01,0.05,1,5,10”）。
-i	间隔(秒)。 对于快速 ping，指定 0。
-l	请求大小。 追加“k”表示千字节，追加“m”表示兆字节。
-n	ping 的数量，或者追加“s”来指定秒数，例如“10s”。

参数	说明
-q	不要在 ping 期间输出。
-t	执行 ping，直到按 Ctrl+C 停止，并键入 Ctrl+Break 查看统计信息。
-w	具有指定迭代次数的预热（默认值为 1）。
-4	强制使用 IPv4。
-6	强制使用 IPv6。

对于高速 ping 测试，请使用 -q 和 -i 0。

TCP 和 UDP 延迟使用情况：

服务器：

Windows 命令提示符

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

客户端：

Windows 命令提示符

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

参数	说明
-f	运行期间的开源防火墙端口。
-u	UDP（默认为 TCP）。
-h	打印直方图（默认桶计数为 20）。
	如果指定一个参数，它会被解释为桶计数，直方图将包含覆盖值的整个时间范围的桶数。 指定以逗号分隔的时间列表来创建自定义直方图（例如“0.01,0.05,1,5,10”）。
-l	请求大小。 追加“k”表示千字节，追加“m”表示兆字节。
-n	发送/接收数。 追加“s”来指定秒数，例如“10s”
-r	从服务器接收而不是发送。
-w	具有指定迭代次数的预热（默认值为 5）。

参数	说明
-4	强制使用 IPv4。
-6	强制使用 IPv6。
-s	服务器侦听地址和端口。

服务器可以同时提供延迟和带宽测试，并在你使用 Control-C 终止它之前保持活动状态。

TCP 和 UDP 带宽使用情况：

服务器：

Windows 命令提示符

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

客户端：

Windows 命令提示符

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

参数	说明
-f	运行期间的开源防火墙端口。
-u	UDP（默认为 TCP）。
-b	带宽测试。
-h	打印直方图（默认桶计数为 20）。
	如果指定一个参数，它会被解释为桶计数，直方图将包含覆盖值的整个时间范围的桶数。 指定以逗号分隔的时间列表来创建自定义直方图（例如“0.01,0.05,1,5,10”）。
-i	未完成的 I/O 的数量（默认为最小 16 个，即 CPU 核心数的 2 倍）。
-l	请求大小。 追加“k”表示千字节，追加“m”表示兆字节。
-n	发送/接收数。 追加“s”来指定秒数，例如“10s”
-r	从服务器接收而不是发送。

参数	说明
-w	指定迭代的预热（默认为 CPU 核心数的 2 倍）。
-4	强制使用 IPv4。
-6	强制使用 IPv6。
-s	服务器侦听地址和端口。

服务器可以同时提供延迟和带宽测试，并在你使用 Control-C 终止它之前保持活动状态。

示例

以下命令对 10 次迭代执行 ICMP ping 测试，有 3 次预热迭代：

Windows 命令提示符

```
psping -n 10 -w 3 marklap
```

若要执行 TCP 连接测试，请指定端口号。 以下命令会尽快对目标执行连接尝试，仅在完成 100 次迭代和 1 次预热迭代后才打印摘要：

Windows 命令提示符

```
psping -n 100 -i 0 -q marklap:80
```

若要为服务器配置延迟和带宽测试，只需指定 `-s` 选项以及服务器将绑定到的源地址和端口：

Windows 命令提示符

```
psping -s 192.168.2.2:5000
```

执行 TCP 延迟测试需要缓冲区大小。 此示例测量将 8 KB 数据包发送到目标服务器的往返延迟，完成后打印一个包含 100 个桶的直方图）：

Windows 命令提示符

```
psping -l 8k -n 10000 -h 100 192.168.2.2:5000
```

以下命令会测试在目标 IP 地址上侦听 10 秒的 PsPing 服务器的带宽，并生成一个具有 100 个桶的直方图。 请注意，测试必须在预热后至少运行一秒钟，才能生成直方图。 只

需添加 `-u`，让 PsPing 执行 UDP 带宽测试即可。

Windows 命令提示符

```
psping -b -l 8k -n 10000 -h 100 192.168.2.2:5000
```

 **下载 PsTools** (5 MB)

PsTools

PsPing 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 PsTools 的本地和远程系统。

运行软件：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

ShareEnum v1.61

项目 • 2023/08/03

作者： Mark Russinovich

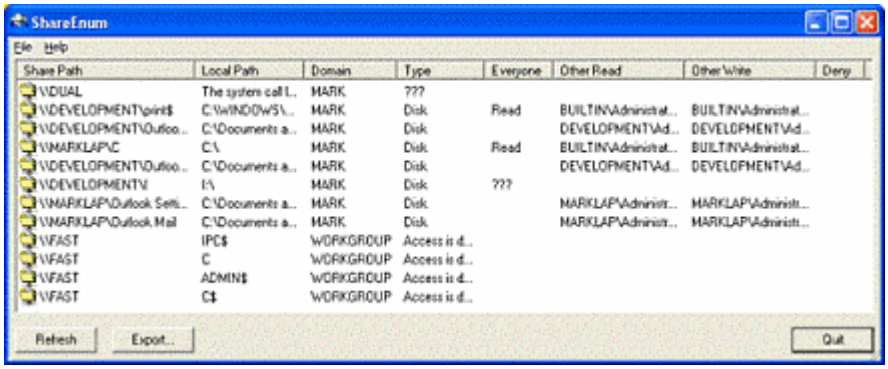
发布时间：2021 年 10 月 12 日

下载 ShareEnum (483 KB)
立即从 Sysinternals Live 运行。

简介

经常被忽视的 Windows NT/2000/XP 网络安全的一个方面是文件共享。 当用户定义安全性宽松的文件共享时，会出现常见的安全漏洞，允许未经授权的用户查看敏感文件。 没有内置工具来列出可在网络上查看的共享及其安全设置，但 *ShareEnum* 填补了这一空白，允许锁定网络中的文件共享。

运行 *ShareEnum* 时，它会使用 NetBIOS 枚举扫描可访问的域中的所有计算机，显示文件和打印共享及其安全设置。 因为只有域管理员才能查看所有网络资源，所以从域管理员帐户运行 *ShareEnum* 时最有效。



工作原理

ShareEnum 使用 **WNetEnumResource** 来枚举域及其中的计算机，并使用 **NetShareEnum** 枚举计算机上的共享。

下载 ShareEnum (483 KB)

立即从 Sysinternals Live 运行。

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

TCPView v4.19

项目 • 2024/07/25

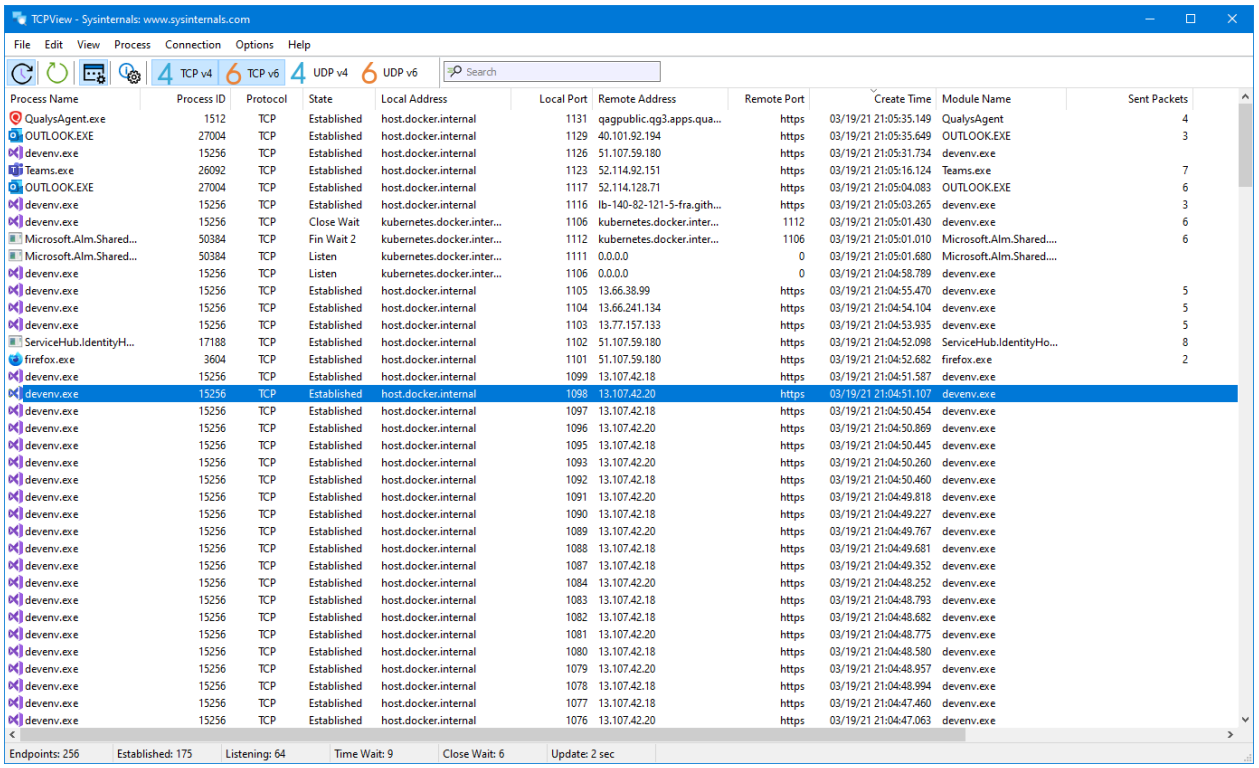
作者：Mark Russinovich

发布时间：2023 年 4 月 11 日

下载 TCPView (1.5 MB)
立即从 Sysinternals Live 运行。

简介

TCPView 是一个 Windows 程序，可向你显示系统上所有 TCP 和 UDP 终结点的详细列表，包括本地和远程地址以及 TCP 连接的状态。 TCPView 还会报告拥有该终结点的进程的名称。 TCPView 提供了 Windows 随附的一组信息更丰富且更便于展示的 Netstat 程序。 TCPView 下载包括 Tcpvcon，这是具有相同功能的命令行版本。



使用 TCPView

在启动 TCPView 时，它将枚举所有活动的 TCP 和 UDP 终结点，从而将所有 IP 地址解析为其域名版本。 可以使用工具栏按钮或菜单项切换已解析名称的显示。 TCPView 可显示拥有每个终结点的进程的名称，包括服务名称（如果有）。

默认情况下，TCPView 每秒更新一次，但你可以使用“**选项|刷新速率**”菜单项更改速率。将状态从一个更新更改为下一个更新的终结点以黄色突出显示；已删除的终结点以红色显示，新终结点则以绿色显示。

可以通过选择“**文件|关闭连接**”，或通过右键单击连接并选择所生成上下文菜单中的“**关闭连接**”来关闭已建立的 TCP/IP 连接（标记为“已建立”状态的连接）。

可以使用“**保存**”菜单项将 TCPView 的输出窗口保存到文件。

使用 Tcpvcon

Tcpvcon 用法类似于内置 Windows netstat 实用工具的用法：

用法：

```
Shell

tcpvcon [-a] [-c] [-n] [process name or PID]
```

展开表

参数	说明
-a	显示所有终结点（默认为显示已建立的 TCP 连接）。
-c	将输出打印为 CSV。
-n	不要解析地址。

 **下载 TCPView** (1.5 MB)

立即从 Sysinternals Live 运行。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

Whois v1.21

项目 • 2024/07/25

作者： Mark Russinovich

发布时间：2019 年 12 月 11 日

 **下载 Whois** **(585 KB)**

简介

Whois 执行你指定的域名或 IP 地址的注册记录。

使用情况

用法： **whois [-v] domainname [whois.server]**

展开表

参数	说明
-v	打印 whois 信息以供引荐

域名可以是 DNS 名称（例如 www.sysinternals.com）或 IP 地址（例如 66.193.254.46）。

 **下载 Whois** **(585 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

Sysinternals 进程实用工具

项目 • 2023/08/04

Autoruns

查看在系统启动时和用户登录时配置为自动启动的程序。 Autoruns 还会显示应用程序可在其中配置自动启动设置的注册表和文件位置的完整列表。

Handle

这是一个方便的命令行实用程序，可显示哪些文件由哪些进程打开等。

ListDLLs

列出当前加载的所有 DLL，包括其加载位置和版本号。 版本 2.0 会输出已加载模块的完整路径名称。

PortMon

使用此高级监视工具监视串行和并行端口活动。 它了解所有标准串行和并行 IOCTL，甚至会显示发送和接收的部分数据。 版本 3.x 具有强大的新 UI 增强和高级筛选功能。

ProcDump

此新的命令行实用工具旨在捕获其他难以隔离和重现 CPU 峰值的进程转储。 它还充当常规进程转储创建实用工具，还可以在进程具有挂起窗口或未经处理的异常时监视和生成进程转储。

进程资源管理器

了解哪些文件、注册表项和其他对象进程已打开，它们已加载了哪些 DLL 等。 这个独特而强大的实用工具甚至会显示每个进程的所有者。

进程监视器

实时监视文件系统、注册表、进程、线程和 DLL 活动。

PsExec

远程执行进程。

PsGetSid

显示计算机或用户的 SID。

PsKill

终止本地或远程进程。

PsList

显示有关进程和线程的信息。

PsService

查看和控制服务。

PsSuspend

暂停和继续进程。

PsTools

PsTools 套件包含命令行实用工具，用于列出在本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志等。

ShellRunas

通过一个方便的 shell 上下文菜单条目以不同的用户身份启动程序。

VMMap

查看进程的已提交虚拟内存类型明细，以及操作系统分配给这些类型的物理内存量（工作集）。 确定进程内存使用量的来源以及应用程序功能的内存成本。

适用于 Windows v14.11 的 Autoruns

项目 • 2024/02/06

作者：Mark Russinovich

发布日期：2024 年 2 月 6 日

下载 Autoruns 和 Autorunsc (2.8 MB)
立即从 Sysinternals Live 运行。

https://www.microsoft.com/zh-cn/videoplayer/embed/RW14GhU?autoplay=true&loop=true&controls=false&postJsllMsg=true&autoCaptions=zh-cn

使用 ZoomIt 创建

简介

此实用工具对任何启动监视器的自动启动位置都有最全面的了解，它显示在系统启动或登录期间，以及在启动各种内置 Windows 应用（如 Internet Explorer、Explorer 和媒体播放器）时，配置为运行哪些程序。 这些程序和驱动程序包含在启动文件夹、Run、RunOnce 和其他注册表项中。 *Autoruns* 报告 Explorer 外壳扩展、工具栏、浏览器帮助程序对象、Winlogon 通知、自动启动服务等等。 *Autoruns* 远超其他自动启动实用工具。

Autoruns 的“**隐藏已签名的 Microsoft 项**”选项可帮助放大已添加到系统中的第三方自动启动映像，并支持查看为系统上配置的其他帐户配置的自动启动映像。 下载包中还包含命令行等效项，可输出 CSV 格式 Autorunsc。

你可能会惊讶于有这么多可执行文件是自动启动的！

使用情况

只需运行 *Autoruns*，它就会向显示当前配置的自动启动应用程序，以及可用于自动启动配置的注册表和文件系统位置的完整列表。 Autoruns 显示的自动启动位置包括登录项、Explorer 加载项、Internet Explorer 加载项（包括浏览器帮助对象 (BHO)）、Appinit DLL、映像劫持、启动执行映像、Winlogon 通知 DLL、Windows 服务和 Winsock 分层服务提供商、媒体编解码器等。 切换选项卡以查看不同类别的自动启动。

要查看配置为自动运行的可执行文件的属性，请选择它，然后使用“**属性**”菜单项或工具栏按钮。 如果 Process Explorer 正在运行，并且有活动进程正在执行所选的可执行文件，则**条目**菜单中的 **Process Explorer** 菜单项将打开执行所选映像的进程的进程属性对话框。

导航到显示的注册表或文件系统位置或自动启动项目的配置，方法是选择该项目并使用“**跳转到项目**”菜单项或工具栏按钮，然后导航到自动启动映像的位置。

要禁用自动启动项，请取消选中其复选框。 要删除自动启动配置项，请使用“**删除**”菜单项或工具栏按钮。

“选项”菜单包括几个显示筛选选项，例如仅显示非 Windows 项，以及访问扫描选项对话框，从中可以启用签名验证、Virus Total 哈希和文件提交。

在“**用户**”菜单中选择项以查看不同用户帐户的自动启动映像。

有关显示选项的更多信息和其他信息，请参阅联机帮助。

Autorunsc 使用情况

Autorunsc 是 Autoruns 的命令行版本。 其使用情况语法为：

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

展开表

参数	说明
-a	自动启动项选择：
*	全部。
b	启动执行。
d	Appinit DLL。
e	Explorer 加载项。
g	边栏小工具（Vista 和更高）
h	映像劫持。
i	Internet Explorer 加载项。
k	已知 DLL。
l	登录启动（这是默认设置）。
m	WMI 项。
n	Winsock 协议和网络提供商。
o	编解码器。

参数	说明
p	打印机监视器 DLL。
r	LSA 安全提供程序。
s	自动启动服务和非禁用驱动程序。
t	计划的任务。
w	Winlogon 项。
-c	将输出打印为 CSV。
-ct	将输出打印为制表符分隔值。
-h	显示文件哈希。
-m	隐藏 Microsoft 项（如果与 -v 一起使用，则为已签名项）。
-s	验证数字签名。
-t	以标准化 UTC (YYYYMMDD-hhmmss) 显示时间戳。
-u	如果启用了 VirusTotal 检查，则显示 VirusTotal 未知或具有非零检测的文件，否则仅显示未签名的文件。
-x	将输出打印为 XML。
-v[rs]	基于文件哈希查询恶意软件的 VirusTotal。 添加“r”，打开具有非零检测的文件的报表。 如果指定了“s”选项，会将报告为“以前未扫描”的文件上传到 VirusTotal。 请注意，扫描结果可能在 5 分钟或更长时间内不可用。
-vt	在使用 VirusTotal 功能之前，必须接受 VirusTotal 服务条款。 如果尚未接受条款，并且忽略了此选项，系统会以交互方式提示你。
-z	指定要扫描的脱机 Windows 系统。
user	指定将显示其自动运行项目的用户帐户名称。 指定“*”以扫描所有用户配置文件。

相关链接

- **Windows 内部书籍**：关于 Windows 内部机制的权威性书籍的官方更新和勘误页，由 Mark Russinovich 和 David Solomon 编写。
- **Windows Sysinternals 管理员参考**：Mark Russinovich 和 Aaron Margosis 编写的 Sysinternals 实用工具官方指南，其中包含各项工具的说明、其功能、如何使用这些工具进行故障排除，以及它们的实际使用示例。

下载

 **下载 Autoruns 和 Autorunsc** (2.8 MB)

立即从 Sysinternals Live 运行。

Handle v5.0

项目 • 2023/08/03

作者： Mark Russinovich

发布时间：2022 年 10 月 26 日

 **下载 Handle** (729 KB)

简介

有没有想过哪个程序打开了特定的文件或目录？ 现在可以了解了。*Handle* 是一个实用工具，用于显示有关系统中任何进程的打开句柄的信息。 可以使用它查看打开了文件的程序，或查看程序的所有句柄的对象类型和名称。

还可以在 Sysinternals 中获取此程序基于 GUI 的版本，即*进程资源管理器*。

安装

通过键入“handle”运行 *Handle*。 必须具有管理权限才能运行 *Handle*。

使用情况

Handle 的目标是搜索打开的文件引用，因此，如果不指定任何命令行参数，它将列出系统中引用打开文件的所有句柄的值以及文件名。 它还需要多个参数来修改此行为。

用法： `handle [[-a [-l]] [-v|-vt] [-u] | [-c <handle> [-y]] | [-s]] [-p <process>|<pid>] [name]`

参数	说明
-a	转储有关所有类型的句柄的信息，而不仅仅是引用文件的句柄。 其他类型包括端口、注册表项、同步基元、线程和进程。
-l	仅显示页面文件支持的节句柄。
-c	关闭指定的句柄（解释为十六进制数）。 必须通过其 PID 指定进程。 **警告：** 关闭句柄可能会导致应用程序或系统不稳定。
-g	打印授予的访问权限。
-y	不要提示关闭句柄确认。

参数	说明
-s	打印每种类型的打开句柄的计数。
-u	搜索句柄时显示拥有用户名。
-v	使用逗号分隔符的 CSV 输出。
-vt	使用制表符分隔符的 CSV 输出。
-p	此参数不会检查系统中的所有句柄，而是将 Handle 的扫描范围缩小到以名称进程开头的进程。 因此： **handle -p exp** 将为以“exp”开头的所有进程转储打开的文件，其中包括 Explorer。
name	存在此参数，以便你可以指示 Handle 搜索对具有特定名称的对象的引用。 例如，如果想要知道哪个进程（如果有）打开了“c:\windows\system32”，则可以键入： **handle windows\system** 名称匹配不区分大小写，指定的片段可以是路径中你感兴趣的任意位置。

句柄输出

当未处于搜索模式（通过将名称片段指定为参数来启用）时，Handle 会将其输出划分为要为其打印句柄信息的每个进程的部分。 虚线用作分隔符，你将在其正下方看到进程名称及其进程 ID (PID)。 进程名称下面列出了句柄值（十六进制）、与句柄关联的对象类型以及对象名称（如果有）。

在搜索模式下，*Handle* 会打印进程名称，ID 列在左侧，具有匹配项的对象的名称位于右侧。

更多信息

可以在 *Windows Internals 第 4 版* 中找到有关对象管理器的详细信息，也可以使用 WinObj 浏览对象管理器名称空间来了解详细信息。

 **下载 Handle** (729 KB)

ListDLLs v3.2

项目 • 2024/11/21

作者：Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 ListDLLs** **(307 KB)**

简介

ListDL 是实用工具，用于报告加载到进程中的 DLL。 可以使用它列出加载到所有进程、特定进程中的所有 DLL，或者列出已加载特定 DLL 的进程。 ListDL 还可以显示 DLL 的完整版本信息（包括其数字签名），并可用于扫描未签名 DLL 的进程。

使用情况

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

展开表

参数	说明
processname	转储进程加载的 DLL（接受部分名称）。
pid	转储与指定进程 ID 关联的 DLL。
dllname	仅显示已加载指定 DLL 的进程。
-r	标记由于未在其基址加载而重定位的 DLL。
-u	仅列出未签名的 DLL。
-v	显示 DLL 版本信息。

示例

列出加载到 Outlook.exe 中的 DLL，包括其版本信息：

listdlls -v outlook

列出加载到任何进程中的任何未签名 DLL：

ListDLLs

显示已加载 MSO.DLL 的进程：

listdlls -d mso.dll

 **下载 ListDLLs** **(307 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

适用于 Windows v3.03 的 Portmon

项目 • 2023/08/03

作者：Mark Russinovich

发布日期：2012 年 1 月 12 日

 **下载 Portmon** **(226 KB)**
立即从 Sysinternals Live 运行。

简介

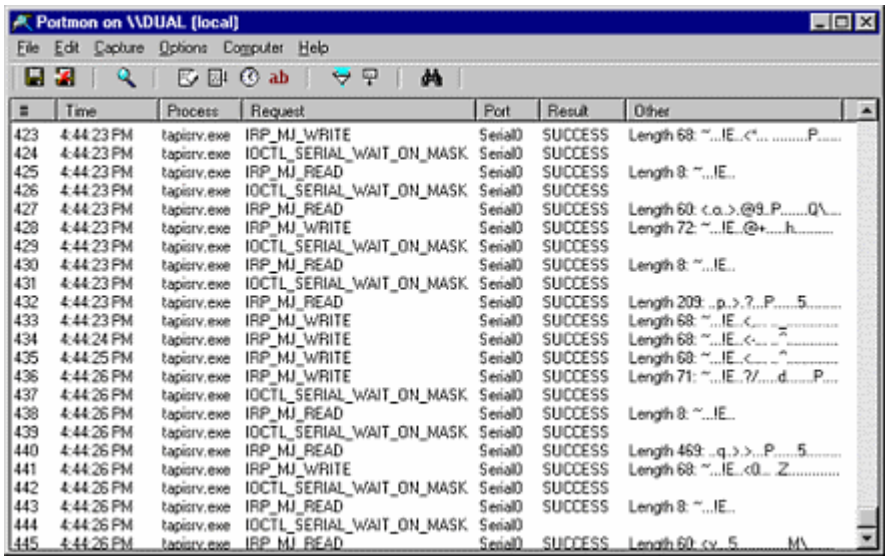
Portmon 是一个实用工具，用于监视和显示系统上的所有串行和并行端口活动。 它具有高级筛选和搜索功能，是探索 Windows 工作方式、查看应用程序如何使用端口或跟踪系统或应用程序配置中问题的强大工具。

Portmon 3.x

Portmon 版本 3.x 引入了许多强大功能。

- **远程监视**：从任何可通过 TCP/IP（甚至是通过 Internet）访问的计算机捕获内核模式和/或 Win32 调试输出。 可以同时监视多台远程计算机。 如果你在 Windows NT/2K 系统上运行 Portmon，并从同一网络邻居中的另一个 Windows NT/2K 系统进行捕获，则 *Portmon* 甚至会安装其客户端软件本身。
- **最近筛选列表**：*Portmon* 已扩展了强大的筛选功能，可记住最近的筛选选择，并提供一个便于重新做出这些选择的界面。
- **剪贴板复制**：在输出窗口中选择多行，并将其内容复制到剪贴板。
- **突出显示**：突出显示与突出显示筛选条件匹配的调试输出，甚至可自定义突出显示颜色。
- **日志到文件**： 捕获时将调试输出写入文件。
- **打印**：将捕获的全部或部分调试输出打印到打印机。
- **单文件有效负载**：*Portmon* 现在作为一个文件实施。

在线帮助文件详细介绍了所有这些功能以及其他功能。



安装和使用

只需执行 *Portmon* 程序文件 (portmon.exe)，*Portmon* 将立即开始捕获调试输出。 若要在 Windows 95 上运行 *Portmon*，必须从 Microsoft 获取 WinSock2 更新。 请注意，如果在 Windows NT/2K 上运行 *Portmon*，则 portmon.exe 必须位于非网络驱动器上，并且你必须具有管理权限。 菜单、热键或工具栏按钮可用于清除窗口、将受监视的数据保存到文件、搜索输出、更改窗口字体等。 在线帮助介绍了 *Portmon* 的所有功能。

Portmon 了解所有串行和并行端口 I/O 控制 (IOCTL) 命令，并将它们和与其关联参数相关的有趣信息一同显示。 对于读取和写入请求，*Portmon* 显示缓冲区的前几十个字节，使用“.”表示不可打印的字符。 使用“显示十六进制”菜单选项，可在 ASCII 和缓冲区数据的原始十六进制输出之间切换。

工作原理：WinNT

Portmon GUI 负责标识串行端口和并行端口。 它通过枚举在 HKEY_LOCAL_MACHINE\Hardware\DeviceMap\SerialComm 下配置的串行端口和在 HKEY_LOCAL_MACHINE\Hardware\DeviceMap\Parallel Ports 下定义的并行端口来执行此操作。 这些密钥包含串行和并行端口设备名称与 Win32 可访问名称之间的映射。

选择要监视的端口时，*Portmon* 会向其设备驱动程序发送请求，其中包含你感兴趣的 NT 名称（例如 \device\serial0）。 驱动程序使用标准筛选 API 将其自己的筛选设备对象附加到目标设备对象。 首先，它使用 **ZwCreateFile** 打开目标设备。 然后，它将从 **ZwCreateFile** 接收回的句柄转换为设备对象指针。 创建自己的与目标特征匹配的筛选设备对象后，驱动程序会调用 **IoAttachDeviceByPointer** 来建立筛选条件。 在此之后，*Portmon* 驱动程序将看到针对目标设备的所有请求。

Portmon 具有所有标准串行和并行端口 IOCTL 的内置知识，这是应用程序和驱动程序配置端口和从端口读取状态信息的主要方式。 IOCTL 在 DDK 文件

\ddk\src\comm\inc\ntddser.h 和 \ddk\src\src\comm\inc\ntddpar.h 中定义，有些记录在 DDK 中。

工作原理：Windows 95 和 98

在 Windows 95 和 98 上，*Portmon* GUI 依赖于动态加载的 VxD 来捕获串行和并行活动。 Windows VCOMM（虚拟通信）设备驱动程序充当并行和串行设备的接口，因此访问端口的应用程序间接使用其服务。 *Portmon* VxD 使用标准 VxD 服务挂钩来截获对 VCOMM 功能的所有访问。 与 NT 设备驱动程序一样，*Portmon* 的 VxD 会将请求以友好的格式显示出来。 在 Windows 95 和 98 上，*Portmon* 会监视所有端口，因此在 NT 上没有端口选择。

 **下载 Portmon** (226 KB)

立即从 Sysinternals Live 运行。

ProcDump v11.1

作者：Mark Russinovich 和 Andrew Richards

发布时间： 2025 年 11 月 13 日

 ProcDump (1.2 MB)

下载 ProcDump for Linux (GitHub)
下载 ProcDump for Mac (GitHub)

https://learn-video.azurefd.net/vod/player?id=a4624e00-b3ac-455c-a5a2-710ae862e42f&locale=zh-cn&embedUrl=%2Fsysinternals%2Fdownloads%2Fprocdump

使用 ZoomIt 创建

简介

ProcDump 是一个命令行实用工具，其主要用途是监视应用程序的 CPU 峰值，并在出现峰值期间生成故障转储，管理员或开发人员可以使用这些转储来确定出现峰值的原因。 ProcDump 还支持挂起窗口监视（使用与 Windows 和任务管理器使用的窗口挂起相同的定义）、未处理的异常监视，并且可以根据系统性能计数器的值生成转储。 它还可用作可嵌入到其他脚本中的常规进程转储实用工具。

使用 ProcDump

捕获使用情况：

Windows 命令提示符

```
procdump.exe [-mm] [-ma] [-mt] [-mp] [-mc <Mask>] [-md <Callback_DLL>] [-mk]
             [-n <Count>]
             [-s <Seconds>]
             [-c|-cl <CPU_Usage> [-u]]
             [-m|-ml <Commit_Usage>]
             [-p|-pl <Counter> <Threshold>]
             [-h]
             [-e [1] [-g] [-b] [-ld] [-ud] [-ct] [-et]]
             [-l]
             [-t]
             [-f  <Include_Filter>, ...]
             [-fx <Exclude_Filter>, ...]
             [-dc <Comment>]
             [-o]
             [-r [1..5] [-a]]
```

```
            [-at <Timeout>]
            [-wer]
            [-64]
            {
                {{[-w] <Process_Name> | <Service_Name> | <PID>} [<Dump_File> |
<Dump_Folder>]}
            |
                {-x <Dump_Folder> <Image_File> [Argument, ...]}
            }
```

安装使用情况：

Windows 命令提示符

```
procdump.exe -i [Dump_Folder]
            [-mm] [-ma] [-mt] [-mp] [-mc <Mask>] [-md <Callback_DLL>] [-mk]
            [-r]
            [-at <Timeout>]
            [-k]
            [-wer]
```

卸载使用情况：

Windows 命令提示符

```
procdump.exe -u
```

转储类型：

展开表

转储类型	说明
-mm	写入“小型”转储文件。 （默认值） - 包括直接和间接引用的内存（堆栈及其引用的内容）。 - 包括所有元数据（进程、线程、模块、句柄、地址空间等）。
-ma	写入“完整”转储文件。 - 包括所有内存（映像、映射和专用内存）。 - 包括所有元数据（进程、线程、模块、句柄、地址空间等）。
-mt	写入“分类”转储文件。 - 包括直接引用的内存（堆栈）。 - 包括有限的元数据（进程、线程、模块和句柄）。 - 尝试删除敏感信息，但不能保证删除。
-mp	写入“小型增强”转储文件。 - 包括所有专用内存和所有读/写映像或映射内存。 - 包括所有元数据（进程、线程、模块、句柄、地址空间等）。

转储类型	说明
	- 为了使大小最小化，将排除超过 512MB 的最大专用内存区域。 内存区域定义为相同大小的内存分配的总和。 转储与完整转储一样详细，但大小只有完整转储的 10%-75%。 - 注意：由于调试限制，CLR 进程将转储为完整转储 (-ma)。
-mc	写入“自定义”转储文件。 - 包括由指定的 `MINIDUMP_TYPE` 掩码（十六进制）定义的内存和元数据。
-md	写入“回调”转储文件。 - 包括由指定 DLL 的名为 `MiniDumpWriteDump` 的 `MiniDumpCallbackRoutine` 回调例程定义的内存。 - 包括所有元数据（进程、线程、模块、句柄、地址空间等）。
-mk	同样写入“内核”转储文件。 - 包括进程中线程的内核堆栈。 - 使用克隆 (`-mk`) 时，OS 不支持内核转储 (`-r`)。 - 使用多个转储大小时，将针对每个转储大小进行内核转储。

条件：

展开表

条件	说明
-a	避免中断。 需要 `-r`。 如果触发器会导致目标由于超出并发转储限制而长时间挂起，则将跳过该触发器。
-at	避免超时时中断。 在 `N` 秒取消触发器的收集。
-b	将调试断点视为异常（否则忽略它们）。
-c	CPU 阈值，高于该阈值则创建进程转储。
-cl	CPU 阈值，低于该阈值则创建进程转储。
-dc	将指定的字符串添加到生成的转储注释。
-e	当进程遇到未经处理的异常时写入转储。 包含 `1` 以在第一次出现异常时创建转储。 添加 `-ld` 以在加载 DLL（模块）时创建转储（应用筛选）。 添加 `-ud` 以在卸载 DLL（模块）时创建转储（应用筛选）。 添加 `-ct` 以在创建线程时创建转储。 添加 `-et` 以在线程退出时创建转储。
-f	筛选（包括）DLL 加载/卸载时的异常内容、调试日志记录和文件名。 支持通配符 (*)。

条件	说明
-fx	筛选（排除）DLL 加载/卸载时的异常内容、调试日志记录和文件名。 支持通配符 (*)。
-g	在托管进程中作为本机调试程序运行（无互操作）。
-h	如果进程有一个挂起的窗口（至少 5 秒不响应窗口消息），则写入转储。
-k	克隆 (`-r`) 后或在转储收集结束时终止进程。
-l	显示进程的调试日志记录。
-m	创建转储的内存提交阈值（以 MB 为单位）。
-ml	当内存提交低于指定的 MB 值时触发。
-n	退出前要写入的转储数。
-o	覆盖现有转储文件。
-p	当性能计数器达到或超过指定阈值时触发。 某些计数器和/或实例名称可能区分大小写。
-pl	当性能计数器低于指定阈值时触发。
-r	使用克隆进行转储。 并发限制是可选的（默认值 1，最大值 5）。 使用克隆 (`-mk`) 时，OS 不支持内核转储 (`-r`)。 警告：高并发值可能会影响系统性能。 - Windows 7：使用反射。 OS 不支持 `-e`。 - Windows 8.0：使用反射。 OS 不支持 `-e`。 - Windows 8.1 及更高版本：使用 PSS。 支持所有触发器类型。
-s	写入转储前的连续秒数（默认值为 10）。
-t	进程终止时写入转储。
-u	处理相对于单核的 CPU 使用率（与 `-c` 配合使用）。
-v	DEBUG ONLY：详细输出。
-w	如果指定的进程未运行，请等待启动。
-wer	将（最大的）转储排队到 Windows 错误报告。
-x	使用可选参数启动指定的映像。 如果它是商店应用程序或包，ProcDump 将（仅）在下次激活时启动。
-y	HIDDEN：商店应用程序激活。
-64	默认情况下，在 64 位 Windows 上运行时，ProcDump 将捕获 32 位进程的 32 位转储。 此选项会替代以创建 64 位转储。 仅用于 WOW64 子系统调试。

许可协议：

使用 `-accepteula` 命令行选项自动接受 Sysinternals 许可协议。

自动终止：

`-cancel <Target Process PID>`

使用此选项或设置名称为 `ProcDump-<PID>` 的事件与键入 Ctrl+C 正常终止 ProcDump 相同。 正常终止可确保在捕获处于活动状态时恢复进程。 取消适用于监视进程的所有 ProcDump 实例。

文件名：

默认转储文件名：`PROCESSNAME_YYMMDD_HHMMSS.dmp`

支持以下替换：

展开表

替换	说明
PROCESSNAME	进程名
PID	进程 ID
EXCEPTIONCODE	异常代码
YYMMDD	年/月/日
HHMMSS	小时/分钟/秒

示例

- 写入名为“notepad”的进程的小型转储（只能存在一个匹配项）：

  Windows 命令提示符

  ```
  C:\>procdump notepad
  ```

- 写入 PID 为“4572”的进程的完整转储：

  Windows 命令提示符

  ```
  C:\>procdump -ma 4572
  ```

- 首先写入小型转储，然后使用 PID“4572”写入进程的完整转储：

Windows 命令提示符

```
C:\>procdump -mm -ma 4572
```

- 在名为“notepad”的进程中每隔 5 秒写入 3 个小型转储：

Windows 命令提示符

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

- 当名为“consume”的进程超过 20% CPU 使用率 5 秒时，最多写入 3 个小型转储：

Windows 命令提示符

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

- 当其中一个窗口未响应超过 5 秒时，写入名为“hang.exe”的进程的小型转储：

Windows 命令提示符

```
C:\>procdump -h hang.exe
```

- 当其中一个窗口未响应超过 5 秒时，写入名为“hang.exe”的进程的完整或内核转储：

Windows 命令提示符

```
C:\>procdump -ma -mk -h hang.exe
```

- 当系统总 CPU 使用率超过 20% 持续 10 秒时，写入名为“outlook”的进程的小型转储：

Windows 命令提示符

```
C:\>procdump outlook -s 10 -p "\Processor(_Total)\% Processor Time" 20
```

- 当 Outlook 的句柄计数超过 10,000 时，写入名为“outlook”的进程的完整转储：

Windows 命令提示符

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

- 当句柄计数超过 10,000 时，写入“svchost”PID 1234、实例 #87 的完整转储：

Windows 命令提示符

```
C:\>procdump -ma 1234 -p "\Process(svchost#87)\Handle Count" 10000
```

注意：多实例计数器
如果计数器有多个实例，则需要包含名称和/或实例编号。

```txt
\Processor(NNN)\% Processor Time
\Thermal Zone Information(<name>)\Temperature
\Process(<name>[#NNN])\<counter>
```

旧版 OS 要求附加 `\Process` 计数器的 PID。

```txt
\Process(<name>[_PID])\<counter>
```

提示：使用性能监视器查看计数器（尤其是区分大小写）。
提示：对于基于 的计数器，使用 PowerShell 将 PID 映射到其 `\Process(*)`。

```pwsh
Get-Counter -Counter "\Process(*)\ID Process"
```

- 为第 2 次异常写入完整转储：

```Windows 命令提示符
C:\>procdump -ma -e w3wp.exe
```

- 为第 1 次和第 2 次异常写入完整转储：

```Windows 命令提示符
C:\>procdump -ma -e 1 w3wp.exe
```

- 为调试字符串消息写入完整转储：

```Windows 命令提示符
C:\>procdump -ma -l w3wp.exe
```

- 为 w3wp.exe 的每个第 1 次或第 2 次异常写入最多 10 个完整转储：

```Windows 命令提示符
C:\>procdump -ma -n 10 -e 1 w3wp.exe
```

- 如果异常的代码/名称/消息包含“`NotFound`”，则最多写入 10 个完整转储：

```
Windows 命令提示符
C:\>procdump -ma -n 10 -e 1 -f NotFound w3wp.exe
```

- 如果调试字符串消息包含“`NotFound`”，则最多写入 10 个完整转储：

```
Windows 命令提示符
C:\>procdump -ma -n 10 -l -f NotFound w3wp.exe
```

- 等待名为“记事本”的进程（并监视其是否有异常）：

```
Windows 命令提示符
C:\>procdump -e -w notepad
```

- 启动名为“记事本”的进程（并监视其是否有异常）：

```
Windows 命令提示符
C:\>procdump -e -x c:\dumps notepad
```

- 注册以启动并尝试激活商店“应用程序”。 激活后，新的 ProcDump 实例将启动：

```
Windows 命令提示符
C:\>procdump -e -x c:\dumps Microsoft.BingMaps_8wekyb3d8bbwe!AppexMaps
```

- 注册以启动应用商店“包”。 激活后，新的 ProcDump 实例将（手动）启动：

```
Windows 命令提示符
C:\>procdump -e -x c:\dumps Microsoft.BingMaps_1.2.0.136_x64__8wekyb3d8bbwe
```

- 当 Microsoft Exchange 信息存储具有未经处理的异常时，将写入小型增强转储：

```
Windows 命令提示符
C:\>procdump -mp -e store.exe
```

- 无需写入转储即可显示 w3wp.exe 的异常代码/名称：

```
Windows 命令提示符
```

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

- Windows 7/8.0；使用反射可减少 5 个连续触发器的中断：

  Windows 命令提示符

  ```
  C:\>procdump -r -ma -n 5 -s 15 wmplayer.exe
  ```

- Windows 8.1+；使用 PSS 减少 5 个并发触发器的中断：

  Windows 命令提示符

  ```
  C:\>procdump -r 5 -ma -n 5 -s 15 wmplayer.exe
  ```

- 将 ProcDump 作为 (AeDebug) 事后调试器安装：

  Windows 命令提示符

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

  ..或..

  Windows 命令提示符

  ```
  C:\Dumps>procdump -ma -i
  ```

- 将 ProcDump 作为 (AeDebug) 事后调试器卸载：

  Windows 命令提示符

  ```
  C:\>procdump -u
  ```

请参阅示例命令行列表（示例在上面列出）：

Windows 命令提示符

```
C:\>procdump -? -e
```

相关链接

- **Windows Internals 书籍**：关于 Windows Internals 的权威性书籍的官方更新和勘误页，由 Mark Russinovich 和 David Solomon 编写。
- **Windows Sysinternals 管理员参考**：Mark Russinovich 和 Aaron Margosis 编写的 Sysinternals 实用工具官方指南，其中包含各项工具的说明、其功能、如何使用这些工具进

行故障排除，以及它们的实际使用示例。

 ProcDump (1.2 MB)

下载 ProcDump for Linux (GitHub)
下载 ProcDump for Mac （GitHub）

运行平台：

- 客户端：Windows 11 及更高版本。
- 服务器：Windows Server 2016 及更高版本。

了解更多

- Defrag Tools：#9 - ProcDump 本集 Defrag Tools 介绍该工具捕获的内容和预期的中断持续时间
- 碎片整理工具：#10 - ProcDump - 触发器 本集涵盖了触发器选项，特别是第 1 几率和第 2 几率异常
- 碎片整理工具：#11 - ProcDump - Windows 8 与进程监视器 本集涵盖了新型应用程序支持和进程监视器日志记录支持

Last updated on 2025/11/13

进程资源管理器 v17.11

作者： Mark Russinovich

发布时间： 2026 年 4 月 9 日

 **下载进程资源管理器** **(3.4 MB)**
立即从 Sysinternals Live 运行。

https://learn-video.azurefd.net/vod/player?id=27421f3d-e796-4ecd-935d-ea78cd638757&locale=zh-cn&embedUrl=%2Fsysinternals%2Fdownloads%2Fprocess-explorer

使用 ZoomIt 创建

介绍

有没有想过哪个程序打开了特定的文件或目录？ 你现在可以搞清楚了。*进程资源管理器*可显示有关打开或加载了哪些句柄和 DLL 进程的信息。

*进程资源管理器*界面由两个子窗口组成。 顶部窗口始终显示当前活动进程的列表，包括其所属帐户的名称，而底部窗口中显示的信息取决于*进程资源管理器*所处的模式：如果它处于句柄模式，你将看到顶部窗口中选择的进程已打开的句柄；如果*进程资源管理器*处于 DLL 模式，则会看到进程已加载的 DLL 和内存映射文件。 *进程资源管理器*还具有强大的搜索功能，可快速显示哪些进程打开了特定的句柄或加载了 DLL。

*Process Explorer*的独特功能有助于跟踪 DLL 版本问题或处理泄漏，并深入了解Windows和应用程序的工作方式。

相关链接

- Windows Internals Book 这本由马克·鲁西诺维奇和大卫·所罗门撰写的权威书籍的官方更新和勘误页。
- Windows Sysinternals 管理员参考 Mark Russinovich 和 Aaron Margosis 提供的 Sysinternals 实用工具的官方指南，包括所有工具的说明、其功能、如何使用它们进行故障排除，以及示例实际使用案例。

下载

 **下载进程资源管理器** **(3.4 MB)**

立即从 Sysinternals Live 运行。

运行于：

- 客户端：Windows 11和更高。
- 服务器：Windows Server 2016及更高。

安装

只需运行*进程资源管理器* (procexp.exe)。

帮助文件描述了*进程资源管理器*的操作和用法。 如果有疑问或问题，请访问 Microsoft Q&A 上的 Process Explorer 部分。

符号使用注意事项

将路径配置为 DBGHELP.DLL 并且符号路径使用符号服务器时，DBGHELP.DLL 的位置还必须包含支持所用服务器路径的 SYMSRV.DLL。 请参阅 SymSrv 文档或有关如何使用符号服务器的详细信息。

了解详细信息

下面是 Sysinternals 中提供的一些其他句柄和 DLL 查看工具和信息：

- 未解之谜的案例... 在本视频中，Mark 描述了他如何解决Windows上看似棘手的系统和应用程序问题。
- Handle - 命令行句柄查看器
- ListDLLs - 命令行 DLL 查看器
- PsList - 本地/远程命令行进程列出工具
- PsKill - 本地/远程命令行进程终止程序
- Defrag Tools：#2 - 进程资源管理器 在 Defrag Tools 的这一集中，Andrew Richards 和 Larry Larsen 详细展示了如何使用进程资源管理器查看进程，无论是在某个时间点还是从历史角度。
- Windows Sysinternals Primer：Process Explorer、Process Monitor and More Process Explorer 在 TechEd 2010 上由 Aaron Margosis 和 Tim Reckmeyer 交付的第一个 Sysinternals Primer 中得到了很多关注。

Last updated on 2026/04/09

进程监视器 v4.01

2025/09/16

作者： Mark Russinovich

发布时间：2024 年 6 月 20 日

 **下载进程监视器** (2.9 MB)

下载 Procmon for Linux (GitHub)

立即从 Sysinternals Live 运行。

简介

进程监视器 是 Windows 的高级监视工具，可显示实时文件系统、注册表和进程/线程活动。 它结合了两个旧版 Sysinternals 实用工具（*Filemon* 和 *Regmon*）的功能，并添加了广泛的增强功能列表，包括丰富的非破坏性筛选、全面的事件属性（如会话 ID 和用户名）、可靠的进程信息、具有每个操作的集成符号支持的全线程堆栈、同时记录到文件等等。 其独特强大的功能将使进程监视器成为系统故障排除和恶意软件搜寻工具包中的核心实用工具。

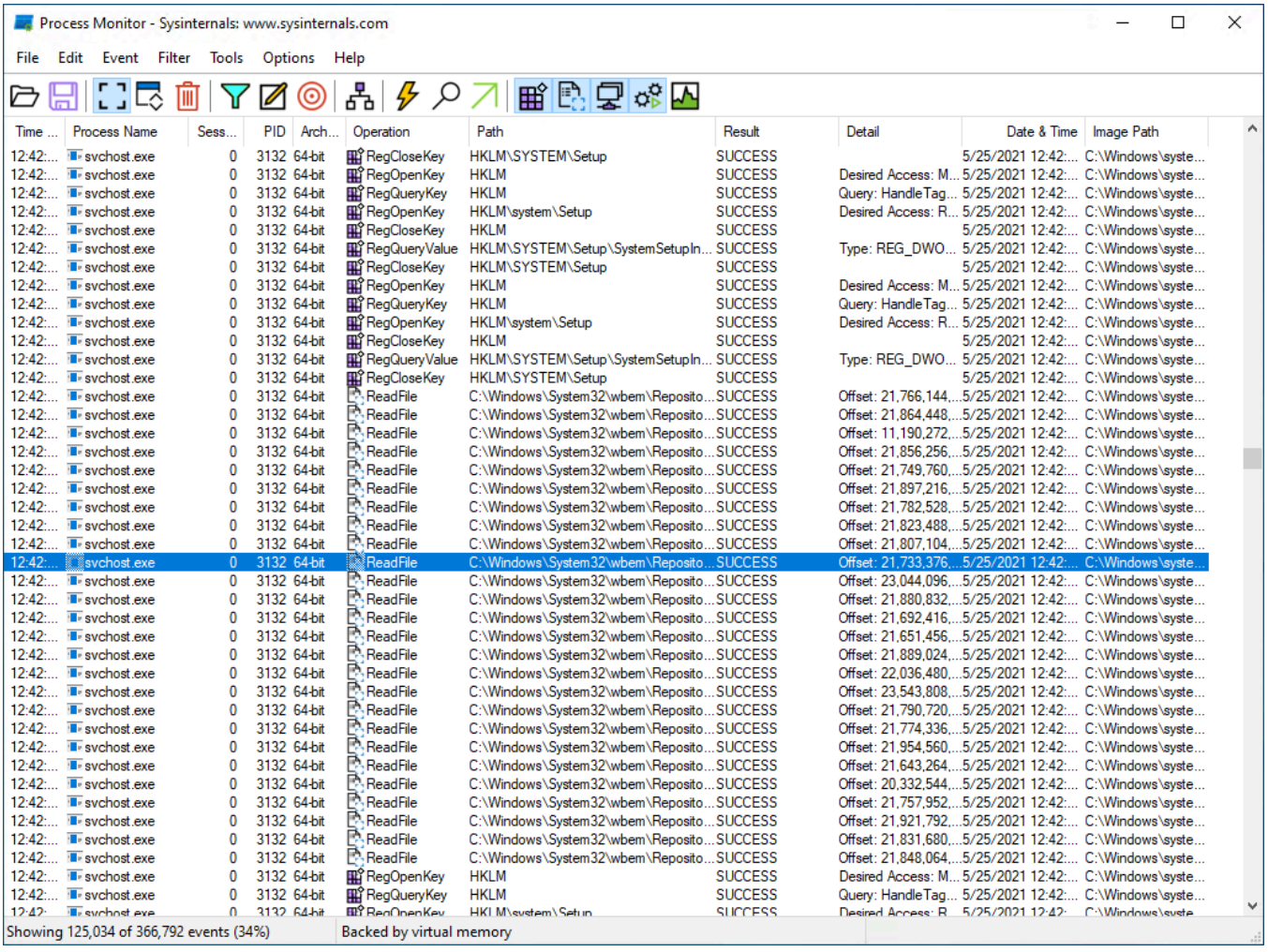
进程监视器功能概述

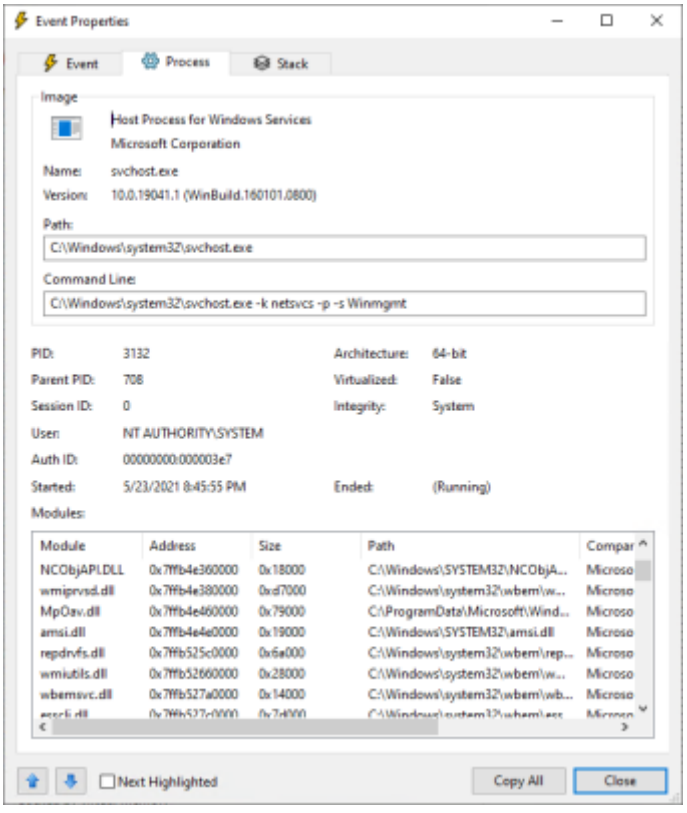
进程监视器具有强大的监视和筛选功能，包括：

- 为操作输入和输出参数捕获更多数据
- 使用非破坏性筛选器，可以在不丢失数据的情况下设置筛选器
- 在许多情况下可以捕获每个操作的线程堆栈，以识别操作的根本原因
- 可靠捕获进程详细信息，包括图像路径、命令行、用户和会话 ID
- 任何事件属性的可配置和可移动列
- 可以为任何数据字段设置筛选器，包括未配置为列的字段
- 高级日志记录体系结构可扩展到数千万个捕获的事件和千兆字节的日志数据
- 进程树工具显示跟踪中引用的所有进程的关系
- 本机日志格式保留所有数据，以便在不同的进程监视器实例中加载
- 进程工具提示可用于轻松查看进程图像信息
- 详细信息工具提示允许方便地访问不适合列的格式化数据
- 可取消搜索
- 所有操作的启动时间日志记录

熟悉进程监视器功能的最佳方式是通读帮助文件，然后在实时系统上访问其每个菜单项和选项。

屏幕截图


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name Sess... PID Arch... Operation Path Result Detail Date & Time Image Path
svchost.exe 0 3132 64-bit RegCloseKey HKLM\SYSTEM\Setup SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegOpenKey HKLM SUCCESS Desired Access: M... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegQueryKey HKLM SUCCESS Query: HandleTag... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegOpenKey HKLM\system\Setup SUCCESS Desired Access: R... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegCloseKey HKLM SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegQueryValue HKLM\SYSTEM\Setup\SystemSetupIn... SUCCESS Type: REG_DWO... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegCloseKey HKLM\SYSTEM\Setup SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegOpenKey HKLM SUCCESS Desired Access: M... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegQueryKey HKLM SUCCESS Query: HandleTag... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegOpenKey HKLM\system\Setup SUCCESS Desired Access: R... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegCloseKey HKLM SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegQueryValue HKLM\SYSTEM\Setup\SystemSetupIn... SUCCESS Type: REG_DWO... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegCloseKey HKLM\SYSTEM\Setup SUCCESS 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,766,144,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,864,448,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 11,190,272,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,856,256,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,749,760,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,897,216,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,782,528,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,823,488,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,807,104,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,733,376,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 23,044,096,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,880,832,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,692,416,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,651,456,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,889,024,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 22,036,480,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 23,543,808,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,790,720,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,774,336,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,954,560,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,643,264,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 20,332,544,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,757,952,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,921,792,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,831,680,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit ReadFile C:\Windows\System32\wbem\Reposito... SUCCESS Offset: 21,848,064,... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegOpenKey HKLM SUCCESS Desired Access: M... 5/25/2021 12:42:... C:\Windows\syste...
svchost.exe 0 3132 64-bit RegQueryKey HKLM SUCCESS Query: HandleTag... 5/25/2021 12:42:... C:\Windows\syste...
Showing 125,034 of 366,792 events (34%)
Backed by virtual memory


Event Properties
Event Process Stack
Image
Host Process for Windows Services
Microsoft Corporation
Name: svchost.exe
Version: 10.0.19041.1 (WinBuild.160101.0800)
Path:
C:\Windows\system32\svchost.exe
Command Line:
C:\Windows\system32\svchost.exe -k netsvcs -p -s Winmgmt
PID: 3132
Architecture: 64-bit
Parent PID: 708
Virtualized: False
Session ID: 0
Integrity: System
User: NT AUTHORITY\SYSTEM
Auth ID: 00000000:000003e7
Started: 5/23/2021 8:45:55 PM
Ended: (Running)
Modules:
Module Address Size Path Compar
NCObjAPI.DLL 0x7ffb4e360000 0x18000 C:\Windows\SYSTEM32\NCObjA... Microso
wmiprvsd.dll 0x7ffb4e380000 0xd7000 C:\Windows\system32\wbem\w... Microso
MpOav.dll 0x7ffb4e460000 0x79000 C:\ProgramData\Microsoft\Wind... Microso
amsi.dll 0x7ffb4e4e0000 0x19000 C:\Windows\SYSTEM32\amsi.dll Microso
repdrvfs.dll 0x7ffb525c0000 0x6a000 C:\Windows\system32\wbem\rep... Microso
wmiutils.dll 0x7ffb52660000 0x28000 C:\Windows\system32\wbem\w... Microso
wbemsvc.dll 0x7ffb527a0000 0x14000 C:\Windows\system32\wbem\wb... Microso
Next Highlighted
Copy All
Close

相关链接

- **Windows Internals 书籍**
  关于 Windows Internals 的权威性书籍的官方更新和勘误页，由 Mark Russinovich 和 David Solomon 编写。
- **Windows Sysinternals 管理员参考**
  由 Mark Russinovich 和 Aaron Margosis 编写的 Sysinternals 实用工具官方指南，其中包含各项工具的说明、其功能、如何使用这些工具进行故障排除，以及它们的实际使用示例。

下载

 **下载进程监视器** (2.9 MB)

立即从 Sysinternals Live 运行。

运行软件：

- 客户端：Windows 10 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

PsExec v2.43

项目 • 2023/10/20

作者：Mark Russinovich

发布时间：2023 年 4 月 11 日

 **下载 PsTools (5 MB)**

介绍

Telnet 等实用工具和远程控制程序（如 Symantec 的 PC Anywhere）可以让你在远程系统上执行程序，但它们的设置可能很麻烦，需要你在想要访问的远程系统上安装客户端软件。 PsExec 是一种轻量级 telnet 替代品，可让你在其他系统上执行进程，并为控制台应用程序提供完整交互性，而无需手动安装客户端软件。 PsExec 最强大的用途包括在远程系统上启动交互式命令提示符，以及 IpConfig 等远程启用工具，否则无法显示有关远程系统的信息。

注意：某些防病毒扫描程序报告一个或多个工具感染了“远程管理员”病毒。 PsTools 均不包含病毒，但它们已被病毒使用，这就是它们触发病毒通知的原因。

安装

只需将 PsExec 复制到可执行文件路径即可。 键入“psexec”会显示其使用语法。

使用 PsExec

请参阅 2004 年 7 月期 *Windows IT 专业人员杂志*中 Mark 的文章，其中介绍了 PsExec 的高级用法。

用法：

Windows 命令提示符

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

参数	说明
-a	使用逗号分隔应用程序可以在上面运行的处理器，其中 1 是编号最低的 CPU。 例如，若要在 CPU 2 和 CPU 4 上运行应用程序，请输入：“-a 2,4”
-c	将指定的可执行文件复制到远程系统以执行。 如果省略此选项，则应用程序必须位于远程系统上的系统路径中。
-d	不要等待进程终止（非交互式）。
-e	不要加载指定帐户的配置文件。
-f	复制指定的程序，即使文件已存在于远程系统上。
-i	运行程序，使其与远程系统上指定会话的桌面进行交互。 如果未指定会话，则进程在控制台会话中运行。 当尝试以交互方式运行控制台应用程序（使用重定向的标准 IO）时，**需要**此标志。
-h	如果目标系统为 Vista 或更高版本，则使用帐户的提升令牌（如果可用）运行进程。
-l	以受限用户身份运行进程（删除 Administrators 组，并仅允许分配给 Users 组的权限）。 在 Windows Vista 上，进程以低完整性运行。
-n	指定连接到远程计算机的超时时间（以秒为单位）。
-p	指定用户名的可选密码。 如果省略此内容，系统将提示你输入隐藏密码。
-r	指定要创建或与之交互的远程服务的名称。
-s	在系统帐户中运行远程进程。
-u	指定登录远程计算机的可选用户名。
-v	仅当指定文件的版本号较高或比远程系统上的版本号新时，才复制指定文件。
-w	设置进程的工作目录（相对于远程计算机）。
-x	在 Winlogon 安全桌面上显示 UI（仅限本地系统）。
-priority	指定 -low、-belownormal、-abovenormal、-high 或 -realtime，以便以不同的优先级运行进程。 使用 -background 在 Vista 上以低内存和 I/O 优先级运行。
computer	指示 PsExec 在指定的远程计算机上运行应用程序。 如果省略计算机名称，PsExec 将在本地系统上运行应用程序，如果指定通配符 (*)，PsExec 将在当前域中的所有计算机上运行命令。
@file	PsExec 将在文件中列出的每台计算机上执行命令。
cmd	要执行的应用程序的名称。
arguments	要传递的参数（请注意，文件路径必须是目标系统上的绝对路径）。

参数	说明
-accepteula	此标志禁止显示许可证对话框。
-nobanner	此标志会消除启动横幅和版权消息。

可以用引号将名称中有空格的应用程序括起来，例如

Windows 命令提示符

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

输入仅在你按 Enter 键时传递到远程系统。 键入 Ctrl-C 将终止远程进程。

如果省略用户名，该进程将在远程系统上的帐户上下文中运行，但无权访问网络资源(因为它正在模拟）。 如果远程进程需要访问网络资源或在不同的帐户中运行，请在 `Domain\User` 语法中指定有效的用户名。 请注意，密码和命令在传输到远程系统时会加密。

PsExec 返回的错误代码特定于所执行的应用程序，而不是 PsExec。

示例

我写的这篇文章介绍了 PsExec 的工作原理，并提供了有关如何使用它的提示：

以下命令在 `\\marklap` 上启动交互式命令提示符：

Windows 命令提示符

```
psexec -i \\marklap cmd
```

此命令使用 `/all` 开关在远程系统上执行 IpConfig，并在本地显示生成的输出：

Windows 命令提示符

```
psexec -i \\marklap ipconfig /all
```

此命令将程序 `test.exe` 复制到远程系统，以交互方式执行：

Windows 命令提示符

```
psexec -i \\marklap -c test.exe
```

指定已安装在远程系统上的程序的完整路径（如果它不在系统的路径上）：

Windows 命令提示符

```
psexec -i \\marklap c:\bin\test.exe
```

在系统帐户中以交互方式运行 Regedit，以查看 SAM 和安全密钥的内容：

Windows 命令提示符

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

若要以受限用户权限运行 Internet Explorer，请使用以下命令：

Windows 命令提示符

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

 **下载 PsTools (5 MB)**

PSTools

PsExec 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

PsGetSid v1.46

项目 • 2023/10/07

作者： Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools** (5 MB)

介绍

PsGetsid 允许将 SID 转换为其显示名称，反之亦然。 它适用于内置帐户、域帐户和本地帐户。

安装

只需将 *PsGetSid* 复制到你的可执行文件路径，然后键入“psgetsid”。

使用情况

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

参数	说明
-u	指定登录远程计算机的可选用户名。
-p	指定用户名的可选密码。 如果省略此内容，系统将提示你输入隐藏密码。
帐户	PsGetSid 将报告指定用户帐户的 SID，而不是计算机的。
SID	PsGetSid 将报告指定 SID 的帐户。
计算机	指示 PsGetSid 在指定的远程计算机上执行命令。 如果省略计算机名称，PsGetSid 将在本地系统上运行命令，如果指定通配符 (*)，PsGetSid 将在当前域中的所有计算机上运行命令。
@file	PsGetSid 将在文件中列出的每台计算机上执行命令。

如果想要查看计算机的 SID，只需将计算机的名称作为命令行参数传递即可。 如果要查看用户的 SID，请在命令行上为帐户命名（例如“administrator”）并命名一个可选的计算机名称。

如果运行的帐户对要查询的计算机没有管理权限，请指定用户名。 如果未将密码指定为选项，则 *PsGetSid* 将提示你输入密码，以便你可以在不显示出来的情况下键入它。

 **下载 PsTools (5 MB)**

PsTools

PsGetSid 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

PsKill v1.17

项目 • 2023/08/03

作者： Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools** (5 MB)

简介

Windows NT/2000 不附带命令行“kill”实用工具。 可以在 Windows NT 或 Win2K 资源工具包中获取一个，但工具包的实用工具只能终止本地计算机上的进程。 *PsKill* 是一种终止实用工具，它不仅可以执行资源工具包版本的功能，还可以终止远程系统上的进程。 你甚至无需在目标计算机上安装客户端，就可以使用 *PsKill* 终止远程进程。

安装

只需将 *PsKill* 复制到可执行文件路径，并使用下面定义的命令行选项键入 pskill。

使用 PsKill

请参阅《Windows IT Pro》杂志 2004 年 9 月期中 Mark 的文章，其中介绍了 *PsKill* 的高级用法。

使用进程 ID 运行 *PsKill* 会指示它在本地计算机上终止该 ID 的进程。 如果指定进程名称，则 *PsKill* 将终止具有该名称的所有进程。

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

参数	说明
-	显示支持的选项。
-t	终止进程及其后代。
\\computer	指定要终止的进程正在其上执行的计算机。 远程计算机必须可以通过 NT 网络邻居访问。
-u username	如果要终止远程系统上的进程，并且在其中执行的帐户对远程系统没有管理权限，则必须使用此命令行选项以管理员身份登录。 如果未将密码包含在 -p 选项中，则

参数	说明
	PsKill 将提示你输入密码，而不会将输入回显到显示器上。
-p password	此选项可以在命令行中指定登录密码，以便可以从批处理文件中使用 PsList。 如果指定帐户名并省略 -p 选项，PsList 会以交互方式提示输入密码。
process id	指定要终止的进程的进程 ID。
process name	指定要终止的一个或多个进程的进程名称。

PsKill Microsoft 知识库文章

此 Microsoft 知识库文章引用 *PsKill*：

810596：PSVR2002：尝试访问项目视图时，出现“此视图中没有要显示的信息”错误消息（https://support.microsoft.com/kb/810596)

 **下载 PsTools** (5 MB)

PsTools

PsKill 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

PsList v1.41

作者： Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools** (5 MB)

简介

只需运行 **pslist** 以获取有关每个进程的当前列表和统计信息，或筛选仅显示以特定名称开头的进程（例如 **pslist exp** ）将仅显示以“exp”开头的进程，其中包括 Explorer for instance。

展开表

参数	说明
-d	显示线程详细信息。
-m	显示内存详细信息。
-x	显示进程、内存信息和线程。
-t	显示进程树。
-s [n]	在任务管理器模式下运行，时长为指定的可选秒数。 按 Esc 键中止。
-r n	任务管理器模式刷新率（以秒为单位）（默认值为 1）。
\\computer	*PsList* 不会显示本地系统的进程信息，而是显示指定的系统的信息。 如果安全凭据不允许从远程系统获取性能计数器信息，请包括带有用户名和密码的 -u 切换以登录到远程系统。
-u	指定登录远程计算机的可选用户名。
-p	此选项可以在命令行中指定登录密码，以便可以从批处理文件中使用 *PsList*。 如果指定帐户名并省略 -p 选项，*PsList* 会以交互方式提示输入密码。
name	显示以指定名称开头的进程信息。
-e	与进程名称完全匹配。
pid	此参数没有列出系统中所有正在运行的进程，而是将 *PsList* 的扫描范围缩小到具有指定 PID 的进程。 因此： **pslist 53** 将转储具有 PID 53 的进程的统计信息。

工作方式

与 Windows 的内置 PerfMon 监视工具一样， *PsList* 使用 Windows 性能计数器来获取它显示的信息。 可以在 Win32 Docs 中找到有关 Windows 性能计数器的文档。

统计信息缩写图例

所有内存值都以 KB 为单位显示。

- **Pri**：优先级
- **Thd**：线程数
- **Hnd**：句柄数量
- **VM**：虚拟内存
- **WS**：工作集
- **Priv**：专用虚拟内存
- **Priv Pk**：专用虚拟内存峰值
- **Faults**：页面错误
- **NonP**：非分页池
- **Page**：分页池
- **Cswtch**：上下文切换总数

 **下载 PsTools (5 MB)**

PsTools

PsList 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

Last updated on 2026/02/06

PsService v2.26

项目 • 2024/11/21

作者：Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools (5 MB)**

简介

PsService 是适用于 Windows 的服务查看器和控制器。 与 Windows NT 和 Windows 2000 资源工具包中包含的 SC 实用工具相同，PsService 会显示服务的状态、配置和依赖项，并允许你执行启动、停止、暂停、恢复和重启操作。 与 SC 实用工具不同，PsService 允许使用其他帐户登录到远程系统，以防运行该工具的帐户在远程系统上没有所需的权限。 PsService 提供唯一的服务搜索功能，用于标识网络上服务的活动实例。 例如，如果要查找运行 DHCP 服务器的系统，可以使用搜索功能。

最后，PsService 同时适用于 NT 4、Windows 2000 和 Windows Vista，而 Windows 2000 资源工具包 SC 版本需要 Windows 2000，PsService 无需手动输入“resume index”即可获取服务信息的完整列表。 >

安装

只需将 PsService 复制到可执行文件路径，然后键入“PsService”。

使用 PsService

PsService 的默认行为是显示本地系统上已配置的服务（包括正在运行和已停止的服务）。 在命令行上输入命令会调用特定功能，某些命令接受选项。 键入命令后跟“-”会显示有关命令语法的信息。

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

展开表

参数	说明
查询	显示服务的状态。
config	显示服务的配置。

参数	说明
setconfig	设置服务的启动类型（禁用、自动、按需）。
start	启动服务。
stop	停止服务。
restart	停止服务，然后重新启动服务。
pause	暂停服务
cont	恢复暂停的服务。
depend	列出依赖于指定服务的服务。
security	转储服务的安全描述符。
find	在网络中搜索指定的服务。
\\computer	针对指定的 NT/Win2K 系统。 如果安全凭据不允许从远程系统获取性能计数器信息，请包括带有用户名和密码的 -u 切换以登录到远程系统。 如果指定 -u 选项，但未使用 -p 选项指定密码，PsService 将提示你输入密码，并且不会将其回显到屏幕。

工作方式

PsService 使用平台 SDK 中记录的服务控制管理器 API。

 **下载 PsTools** **(5 MB)**

PsTools

PsService 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 PsTools 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

PsSuspend v1.08

项目 • 2024/07/25

作者： Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools** **(5 MB)**

简介

使用 *PsSuspend*，可以暂停本地或远程系统上的进程，在进程消耗你希望由其他进程使用的资源时，这是需要采取的操作。 暂停不会终止消耗资源的进程，而是允许它在以后的某个时间点继续操作。

安装

将 *PsSuspend* 复制到可执行文件路径，并使用下面定义的命令行选项键入“pssuspend”。

使用 PsSuspend

使用进程 ID 运行 *PsSuspend* 会指示它在本地计算机上暂停或恢复该 ID 的进程。 如果指定进程名称，*PsSuspend* 将暂停或恢复具有该名称的所有进程。 指定 -r 开关以恢复挂起的进程。

用法： **pssuspend [-] [-r] [\\computer [-u username] [-p password]] <进程名称|进程id>**

展开表

参数	说明
-	显示支持的选项。
-r	如果暂停了指定的进程，则恢复指定的进程。
\\computer	指定要暂停或恢复的进程正在其上执行的计算机。 远程计算机必须可以通过 NT 网络邻居访问。
-u username	如果要暂停远程系统上的进程，并且在其中执行的帐户对远程系统没有管理权限，则必须使用此命令行选项以管理员身份登录。 如果未使用 -p 选项包含密码，则 *PsSuspend* 将提示你输入密码，而不会将输入回显到显示器上。

参数	说明
-p password	使用此选项，可以在命令行中指定登录密码，以便可以从批处理文件中使用 *PsSuspend*。 如果指定帐户名并省略 -p 选项，则 *PsSuspend* 会以交互方式提示输入密码。
进程 ID	指定要暂停或恢复的进程的进程 ID。
进程名称	指定要暂停或恢复的进程的进程名称。

PsSuspend 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

 **下载 PsTools** **(5 MB)**

PsTools

PsSuspend 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

PsTools

项目 • 2024/07/25

作者：Mark Russinovich

发布时间：2023 年 4 月 11 日

 **下载 PsTools Suite** (5 MB)

简介

Windows NT 和 Windows 2000 资源工具包附带许多命令行工具，可帮助你管理 Windows NT/2K 系统。 过去一段时间内，我开发了一系列类似的工具，包括一些未包含在资源工具包中的工具。 这些工具的区别在于，它们都可以用来管理远程系统以及本地系统。 套件中的第一个工具是 PsList，此工具可用于查看有关进程的详细信息，并且套件在持续开发中。 PsList 中的“Ps”前缀与标准 UNIX 进程列表命令行工具名为“ps”有关，因此我为所有工具采用此前缀，以便将它们绑定到名为 PsTools 的工具套件中。

> **备注**
>
> 某些防病毒扫描程序报告一个或多个工具感染了“远程管理员”病毒。 PsTools 均不包含病毒，但它们已被病毒使用，这就是它们触发病毒通知的原因。

PsTools 套件中包含的工具（可作为包下载）包括：

- PsExec - 远程执行进程
- PsFile - 显示远程打开的文件
- PsGetSid - 显示计算机或用户的 SID
- PsInfo - 列出有关系统的信息
- PsPing - 测量网络性能
- PsKill - 按名称或进程 ID 终止进程
- PsList - 列出有关进程的详细信息
- PsLoggedOn - 查看谁在本地并通过资源共享登录（包含完整源）
- PsLogList - 转储事件日志记录
- PsPasswd - 更改帐户密码
- PsService - 查看和控制服务
- PsShutdown - 关闭计算机，然后重启计算机（可选）
- PsSuspend - 挂起进程
- PsUptime - 显示系统自上次重新启动以来已运行多长时间（PsUptime 的功能已合并到 PsInfo 中）

PsTools 下载包包含一个 HTML 帮助文件，其中包括所有工具的完整使用情况信息。

 **下载 PsTools Suite** (5 MB)

运行软件：

- 客户端：Windows 8.1 及更高版本
- 服务器：Windows Server 2012 及更高版本
- Nano Server：2016 及更高版本

安装

这些工具无需专门安装。 甚至不需要在目标远程计算机上安装任何客户端软件。 通过键入名称以及所需的任何命令行选项即可运行它们。 若要显示完整的使用情况信息，请指定"-? "命令行选项。 如果有疑问或问题，请访问 Sysinternals PsTools 论坛。

相关链接

PsTools 简介：Wes Miller 在他的《TechNet 杂志》专栏的 3 月专栏中简要介绍了 Sysinternals PsTools。

ShellRunas v1.02

项目 • 2024/07/25

作者：Mark Russinovich 和 Jon Schwartz

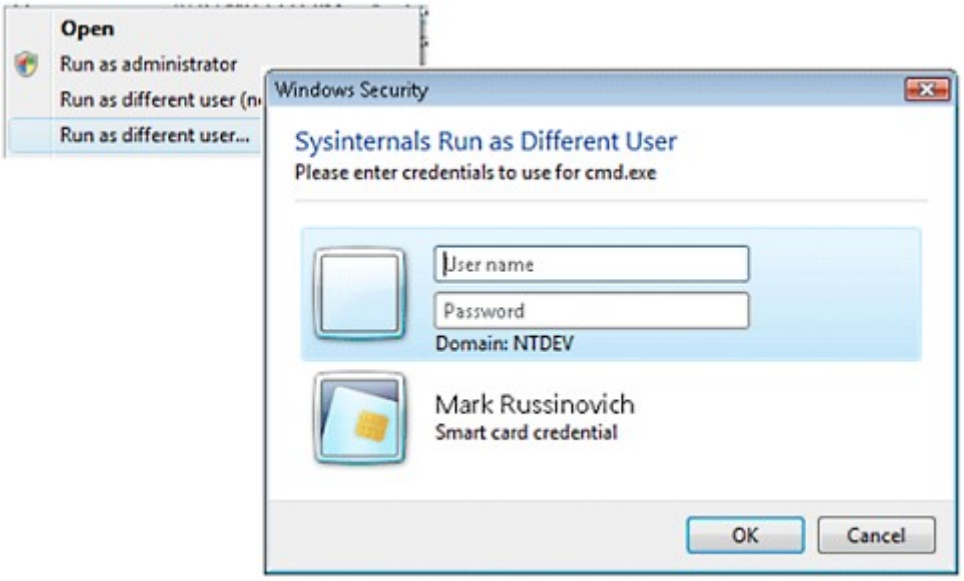
发布时间：2021 年 10 月 12 日

下载 ShellRunas (90 KB)

简介

命令行 Runas 实用工具可方便地在不同帐户下启动程序，但如果你是 Explorer 的重度用户，它就不方便了。 ShellRunas 提供与 Runas 类似的功能，通过方便的 shell 上下文菜单条目以其他用户身份启动程序。

屏幕快照



使用 ShellRunas

用法:

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

展开表

参数	说明
/reg	注册 ShellRunas shell 上下文菜单项
/regnetonly	注册 Shell /netonly 上下文菜单项 **注意：**程序启动时，命令提示符会闪烁
/unreg	注销 ShellRunas shell 上下文菜单项
/quiet	注册或注销 ShellRunas shell 上下文菜单项，不显示结果对话框
/netonly	如果指定的凭据仅用于远程访问，请使用
<program>	使用指定的凭据和参数运行程序

 **下载 ShellRunas** (90 KB)

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

获取帮助

如果遇到问题或疑问，请访问 Sysinternals 论坛。

VMMap v3.4

项目 • 2023/10/20

作者：Mark Russinovich

发布时间：2023 年 10 月 18 日

 **下载 VMMap** (7.6 MB)
立即从 Sysinternals Live 运行。

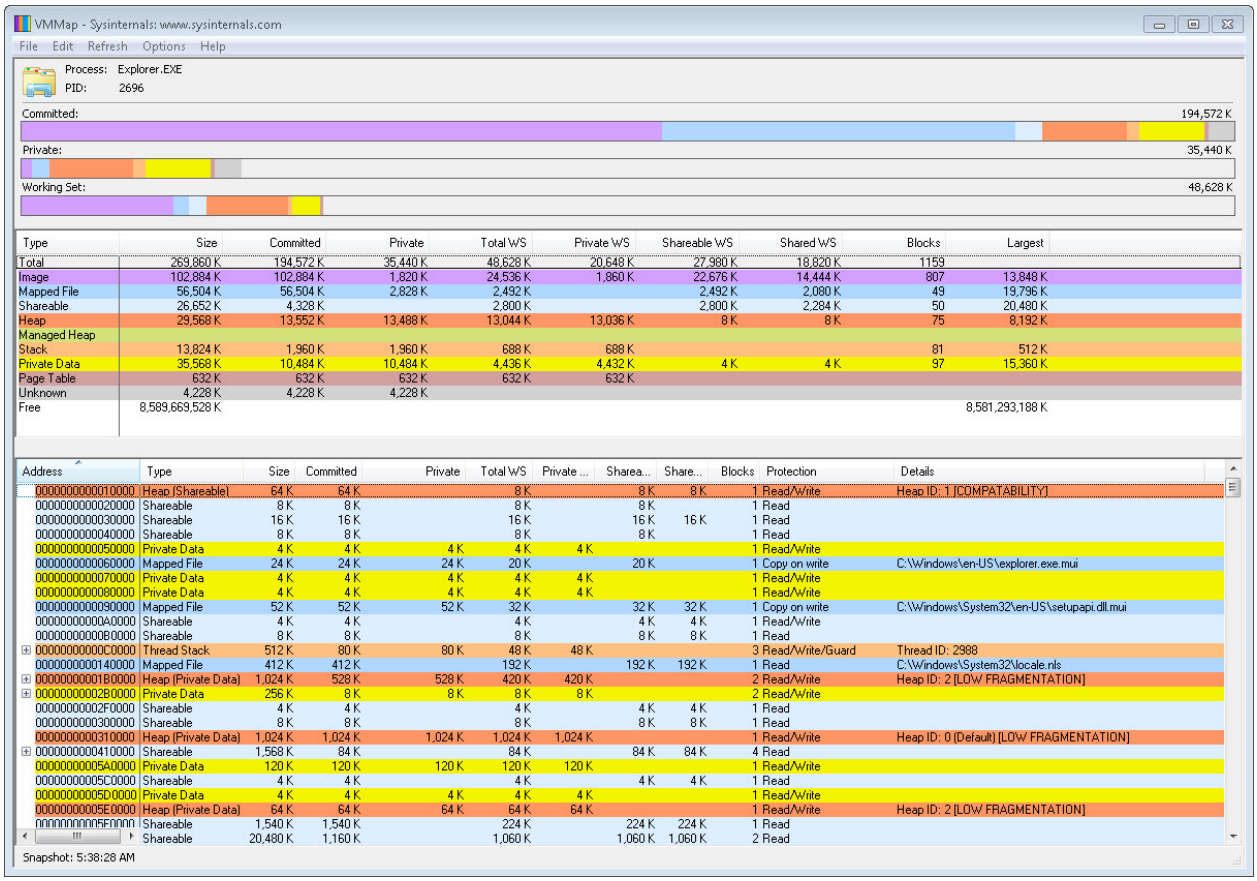
介绍

VMMap 是进程虚拟和物理内存分析实用程序。 它可显示进程的已提交虚拟内存类型明细，以及操作系统分配给这些类型的物理内存量（工作集）。 除了内存使用情况的图形表示形式外，VMMap 还可显示摘要信息和详细的进程内存映射。 借助强大的筛选和刷新功能，可以识别进程内存使用情况的来源以及应用程序功能的内存成本。

除了用于分析实时进程的灵活视图外，VMMap 还支持以多种形式导出数据，包括可保留所有信息以便可以重新加载的本机格式。 它还包括用于启用脚本方案的命令行选项。

对于希望了解和优化其应用程序内存资源使用情况的开发人员，VMMap 是一种理想的工具。

屏幕快照



相关链接

- **Windows Internals 书籍**
  关于 Windows Internals 的权威性书籍的官方更新和勘误页，由 Mark Russinovich 和 David Solomon 编写。
- **Windows Sysinternals 管理员参考**：Mark Russinovich 和 Aaron Margosis 编写的 Sysinternals 实用工具官方指南，其中包含各项工具的说明、其功能、如何使用这些工具进行故障排除，以及它们的实际使用示例。

下载 VMMap (7.6 MB)

立即从 Sysinternals Live 运行。

运行软件：

- 客户端：Windows 10 及更高版本。
- 服务器：Windows Server 2016 及更高版本。

了解详细信息

- Defrag Tools：7 - VMMap
  在本期《碎片整理工具》中，Andrew Richards 和 Larry Larsen 介绍了如何使用 VMMap 查看虚拟内存的使用方式以及是否存在任何内存泄漏。

Sysinternals 安全实用程序

项目 • 2023/08/03

AccessChk

此工具显示指定的用户或组对文件、注册表项或 Windows 服务的访问权限级别。

AccessEnum

这个简单但功能强大的安全工具可显示谁有权访问系统上的目录、文件和注册表项。 使用它来查找权限中的漏洞。

Autologon

在登录期间绕过密码屏幕。

Autoruns

查看在系统启动时和用户登录时配置为自动启动的程序。 Autoruns 还会显示应用程序可在其中配置自动启动设置的注册表和文件位置的完整列表。

LogonSessions

列出活动登录会话

进程资源管理器

了解哪些文件、注册表项和其他对象进程已打开，它们已加载了哪些 DLL 等。 这个独特而强大的实用工具甚至会显示每个进程的所有者。

PsExec

使用受限用户权限执行进程。

PsLoggedOn

显示已登录到系统的用户。

PsLogList

转储事件日志记录。

PsTools

PsTools 套件包含命令行实用工具，用于列出在本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志等。

Rootkit Revealer

RootkitRevealer 是一种高级 rootkit 检测实用程序。

SDelete

使用此符合 DoD 标准的安全删除程序安全地覆盖敏感文件并清理以前删除的文件的可用空间。

ShareEnum

扫描网络上的文件共享，并查看其安全设置以关闭安全漏洞。

ShellRunas

通过一个方便的 shell 上下文菜单条目以不同的用户身份启动程序。

Sigcheck

转储文件版本信息，并验证系统上的映像是否已进行数字签名。

Sysmon

通过 Windows 事件日志监视和报告关键系统活动。

Autologon v3.10

项目 • 2023/08/03

作者： Mark Russinovich

发布时间：2016 年 8 月 29 日

 **下载 Autologon** (495 KB)
立即从 Sysinternals Live 运行。

简介

Autologon 使你能够轻松配置 Windows 的内置自动登录机制。 Windows 使用通过 Autologon 输入的凭据（已在注册表中加密）自动登录指定的用户，而不用等待用户输入其名称和密码。

[!警告] 尽管密码在注册表中作为 *LSA 机密*加密，但具有管理权限的用户可以轻松检索和解密密码。 （有关详细信息，请参阅保护自动登录密码）

Autologon 使用起来很简单。 只需运行 autologon.exe，填写对话框，然后点击“启用”就可以了。 下次系统启动时，Windows 会尝试使用输入的凭据在控制台上登录用户。 请注意，Autologon 不会验证提交的凭据，也不会验证指定的用户帐户是否允许登录到计算机。

若要关闭自动登录，请点击“*禁用*”。 此外，如果在系统执行自动登录之前按住 Shift 键，则将为该登录禁用自动登录。 还可以将用户名、域和密码作为命令行参数传递：

自动登录用户域密码

注意： Exchange Activesync 密码限制到位后，Windows 不会处理自动登录配置。

 **下载 Autologon** (495 KB)
立即从 Sysinternals Live 运行。

LogonSessions v1.41

项目 • 2024/07/25

作者： Mark Russinovich

发布时间：2020 年 11 月 25 日

 **下载 LogonSessions** (667 KB)

简介

如果你认为登录系统时只有一个活动登录会话，此实用工具会让你大吃一惊。 它列出当前处于活动状态的登录会话，如果指定 -p 选项，则列出在每个会话中运行的进程。

用法： logonsessions [-c[t]] [-p]

展开表

参数	说明
-c	将输出打印为 CSV。
-ct	将输出打印为制表符分隔值。
-p	列出登录会话中运行的进程。

示例输出

Shell

```
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
```

 **下载 LogonSessions** **(667 KB)**

运行平台：

- 客户端：Windows Vista（32 位）及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

NewSID v4.10

项目 • 2023/08/11

作者：Mark Russinovich

发布时间：2006 年 11 月 1 日

注意：NewSID 已停用，不再可供下载。 请参阅 Mark Russinovich 的博客文章：NewSID 停用和机器 SID 复制谜题

重要事项

关于 SID，Microsoft 不支持使用 NewSID 准备的图像，我们只支持使用 SysPrep 准备的映像。 Microsoft 尚未对所有部署克隆选项测试 NewSID。

有关 Microsoft 官方政策的更多信息，请参阅以下知识库文章：

- **有关 Windows XP 安装的磁盘复制 Microsoft 策略**

简介

许多组织使用磁盘映像克隆来执行 Windows 的大规模推出。 此技术涉及将已完全安装和配置的 Windows 计算机的磁盘复制到其他计算机的磁盘驱动器上。 这些其他计算机立即显示已经过相同安装过程，可以马上使用。

相较于其他推出方法，虽然此方法可节省数小时的工作和麻烦，但其主要问题是每个克隆的系统都有相同的计算机安全 ID (SID)。 这一事实会损害工作组环境中的安全性，在具有多个相同计算机 SID 的网络中，可移动媒体的安全性也可能受损。

Windows 社区的需求已促使多家公司开发可在克隆系统后更改计算机 SID 的程序。 然而，赛门铁克的 SID Changer 及其 Ghost Walker 仅作为每家公司高端产品的一部分出售。 此外，它们都是在 DOS 命令提示符下运行的（Altiris 的转换器类似于 *NewSID*）。

NewSID 是我们开发的程序，用于更改计算机的 SID。 它是免费的 Win32 程序，这表示它可以很容易地在先前克隆过的系统上运行。

在使用此程序之前，请阅读整篇文章。

版本信息：

- 4.0 版引入了对 Windows XP 和 .NET Server 的支持，这是向导式界面，允许指定要应用的 SID、注册表压缩以及重命名计算机的选项（这会导致 NetBIOS 和 DNS 名称

的更改）。

- 3.02 版更正了 NewSid 在将项旧 SID 重命名为新 SID 时，无法正确复制具有无效值类型的默认值的 bug。 NT 实际上在 SAM 中的某些时间使用了这样的无效值。 此 bug 的症状是在授权用户更新帐户信息时报告访问遭拒绝的错误消息。
- 3.01 版为 Microsoft 事务服务器创建的无法访问的注册表项添加了解决方法。 如果没有解决方法，*NewSID* 将提前退出。
- 版本 3.0 引入了 SID 同步功能，其指示 *NewSID* 从另一台计算机获取要应用的 SID。
- 2.0 版有自动模式选项，可以更改计算机名称。
- 1.2 版修复了 1.1 版中引入的 bug：某些文件系统安全描述符没有更新。
- 1.1 版更正了相对较小的 bug，其只影响某些安装。 它还进行了更新，以更改与文件和打印机共享的权限设置相关联的 SID。

克隆和替代推出方法

在企业环境中执行大规模 Windows 推出（通常是数百台计算机）的最热门方法之一基于磁盘克隆技术。 系统管理员在模板计算机上安装公司使用的基本操作系统和加载项软件。 将机器配置为在公司网络中运行后，会使用自动磁盘或系统复制工具（如赛门铁克的 *Ghost*、PowerQuest 的 *Image Drive* 和 Altiris 的 *RapiDeploy*）将模板计算机的驱动器复制到数十台或数百台计算机上。 然后对这些克隆进行最后的调整，例如分配唯一名称，然后供公司员工使用。

另一种热门推出方式是使用 Microsoft *sysdiff* 实用程序（Windows Resource Kit 的一部分）。 此工具要求系统管理员在每台计算机上执行完全安装（通常是脚本化无人参与安装），然后 *sysdiff* 使加载项软件自动安装映像。

由于跳过了安装，而且磁盘扇区复制比文件复制更高效，因此与同等 sysdiff 安装相比，基于克隆的推出可以节省数十个小时。 此外，系统管理员不必学习如何使用无人参与安装或 *sysdiff*，或者创建和调试安装脚本。 仅此就可以节省数小时的工作。

SID 重复问题

克隆的问题在于，它只得到 Microsoft 非常有限的支持。 Microsoft 表示，只有在 Windows 安装程序的 GUI 部分之前完成的克隆系统才得到支持。 当安装到此阶段时，将为计算机分配名称和唯一计算机 SID。 如果在此步骤之后克隆了系统，则克隆的计算机都将具有相同的计算机 SID。 请注意，仅更改计算机名称或将计算机添加到其他域不会更改计算机 SID。 如果计算机先前与域关联，更改名称或域只会更改域 SID。

要了解克隆可能导致的问题，首先需要了解计算机上的各个本地帐户是如何获分配 SID 的。 本地帐户的 SID 由计算机 SID 和附加 RID（相对 ID）组成。 RID 从固定值开始，并

为每个创建的帐户增加一个值。 这表示，例如，一台计算机上的第二个帐户将被赋予与克隆上的第二个帐户相同的 RID。 结果是两个帐户都具有相同的 SID。

重复 SID 在基于域的环境中没问题，因为域帐户具有基于域 SID 的 SID。 但是，根据 Microsoft 知识库文章 Q162001“请勿磁盘复制 Windows NT 的已安装版本”，在工作组环境中，安全性基于本地帐户 SID。 因此，如果两台计算机的用户具有相同 SID，则工作组将无法区分用户。 一个用户可以访问的所有资源，包括文件和注册表项，另一个用户也可以访问。

重复 SID 可能导致问题的另一个例子是，具有 NTFS 格式的可移动媒体，以及本地帐户安全属性应用于文件和目录。 如果将这样的媒体移动到具有相同 SID 的另一台计算机，则如果无法访问文件的本地帐户的帐户 ID 恰好与安全属性中的帐户 ID 匹配，则可以访问这些文件。 如果计算机具有不同 SID，这就不可能发生。

Mark 写了一篇题为“*NT 推出选项*”的文章，发表于 6 月份的 *Windows NT 杂志*。 它更详细地讨论了重复 SID 问题，并介绍了 Microsoft 对克隆的官方立场。 要查看网络上是否存在重复 SID 问题，请使用 PsGetSid 以显示机器 SID。

NewSID

NewSID 是我们为更改计算机 SID 而开发的程序。 它首先为计算机生成随机 SID，然后更新其在注册表和文件安全描述符中找到的现有计算机 SID 实例，用新 SID 替换出现内容。 *NewSID* 需要管理权限才能运行。 它有两个功能：更改 SID 和更改计算机名称。

要使用 *NewSID* 的自动运行选项，请在命令行中指定“/a”。 还可以通过在“/a”切换后包含新名称来指示它自动更改计算机名称。 例如：

newsid /a [新名称]

将在没有提示的情况下运行 *NewSID*，将计算机名称更改为“新名称”，并在一切正常的情况下重新启动计算机。

注意：如果预期运行 *NewSID* 的系统正在运行 IISAdmin，则必须在运行 *NewSID* 之前停止 IISAdmin 服务。 使用此命令停止 IISAdmin 服务：net stop iisadmin /y

NewSID 的 SID 同步功能，允许指定从其他计算机获取新 SID，而不是随机生成。 此功能使备份域控制器 (BDC) 可以移动到新域，因为 BDC 与域的关系是由它与其他域控制器 (DC) 具有相同的计算机 SID 来标识的。 只需选择“同步 SID”按钮并输入目标计算机的名称。 必须具有更改目标计算机注册表项的安全设置权限，这通常表示必须以域管理员身份登录才能使用此功能。

请注意，运行 *NewSID* 时，注册表的大小将增长，因此请确保注册表的最大大小将适应增长。 我们发现，这种增长对系统性能没有明显的影响。 注册表增长的原因是，由于 *NewSID* 应用了临时安全设置，注册表变得零碎。 删除设置后，注册表不会压缩。

重要提示：请注意，虽然我们已经彻底测试了 *NewSID*，但必须自担使用它的风险。 与任何更改文件和注册表设置的软件一样，强烈建议在运行 *NewSID* 之前完全备份计算机。

移动 BDC

以下是要将 BDC 从一个域移动到另一个域时应遵循的步骤：

1. 启动要移动的 BDC 并登录。 使用 *NewSID* 将 BDC 的 SID 与 BDC 移动的目的地域的 PDC 同步。
2. 重新启动更改了 SID (BDC) 的系统。 由于 BDC 现在关联的域已经具有活动 PDC，因此它将在其新域中作为 BDC 启动。
3. BDC 将在服务器管理器中显示为工作站，因此请使用"添加到域"按钮将 BDC 添加到其新域。 添加时，请确保指定 BDC 单选按钮。

工作方式

NewSID 通过读取现有计算机 SID 开始。 计算机的 SID 存储在注册表的 **SECURITY** 配置单元，位于 **SECURITY\SAM\Domains\Account** 下。 此项具有名为 F 和 V 的值。V 值是二进制值，在其数据末尾嵌入了计算机 SID。 *NewSID* 确保此 SID 为标准格式（3 个 32 位的子颁发机构前面有三个 32 位颁发机构字段）。

接下来，*NewSID* 为计算机生成新的随机 SID。 *NewSID* 系列煞费苦心地创建了真正随机的 96 位值，它取代了构成计算机 SID 的 3 个子颁发机构值中的 96 位。

接下来是计算机 SID 替换的三个阶段。 在第一阶段，扫描 **SECURITY** 和 **SAM** 注册表配置单元，查找项值中出现的旧计算机 SID 以及项名称。 在一个值中找到 SID 时，它会被新计算机 SID 替换，当在某名称中找到该 SID 时，项及其子项会被复制到新的子项，其具有相同名称，除了使用新 SID 替换旧 SID。

最后两个阶段涉及更新安全描述符。 注册表项和 NTFS 文件具有与其关联的安全性。 安全描述符包括条目（其可识别哪个帐户拥有资源，哪个组是主要组所有者），指定用户或组允许操作的可选条目列表（称为自由访问控制列表 - DACL），以及可选的条目列表（指定特定用户或组执行的哪些操作将在系统事件日志（系统访问控制列表 - SACL）中生成条目）。 用户或组在这些安全描述符中用其 SID 进行标识，正如先前所述，本地用户帐户（除了内置帐户，如管理员、来宾等）的 SID 由计算机 SID 和 RID 组成。

安全描述符更新的第一部分发生在计算机上的所有 NTFS 文件系统文件上。 每个安全描述符都会扫描计算机 SID 的出现情况。 当 *NewSID* 找到 SID 时，它会用新计算机 SID 替换它。

安全描述符更新的第二部分在注册表上执行。 首先，*NewSID* 必须确保它扫描所有配置单元，而不仅仅是那些已加载的配置单元。 每个用户帐户都有注册表配置单元，其在用户

登录时加载为 **HKEY_CURRENT_USER**，但在用户未登录时保留在用户配置文件目录中的磁盘上。 *NewSID* 通过枚举 **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList** 项（指向存储这些位置的目录）来标识所有用户配置单元位置的位置。 然后，它使用 **HKEY_LOCAL_MACHINE** 下的 RegLoadKey 将它们加载到注册表中，并扫描整个注册表，检查每个安全描述符以搜索旧计算机 SID。 更新的执行方式与文件相同，完成后 *NewSID* 将卸载其加载的用户配置单元。 作为最后一步，*NewSID* 扫描 **HKEY_USERS** 项，其包含当前登录用户的配置单元以及 .Default 配置单元。 这是必要的，因为不能加载一个配置单元两次，所以当 *NewSID* 加载其他用户配置单元时，登录的用户配置单元不会加载到 **HKEY_LOCAL_MACHINE** 中。

最后，*NewSID* 必须更新 **ProfileList** 子项以引用新帐户 SID。 在更改帐户 SID 以反映新计算机 SID 后，此步骤对于使 Windows NT 将配置文件与用户帐户正确关联是必要的。

NewSID 通过赋予自身以下权限：System、Backup、Restore 和 Take Ownership 来确保其可以访问和修改系统中的每个文件和注册表项。

PsLoggedOn v1.35

项目 • 2024/11/21

作者： Mark Russinovich

发布时间：2016 年 6 月 29 日

 **下载 PsTools** **(2.7 MB)**

简介

可以使用“net”命令("net session")确定谁正在使用本地计算机上的资源，但是，没有内置方法来确定谁正在使用远程计算机的资源。 此外，NT 不提供任何工具来查看本地或远程登录到计算机的人员。 *PsLoggedOn*是小程序，它显示本地登录的用户以及通过本地计算机或远程计算机的资源登录的用户。 如果指定用户名而不是计算机，*PsLoggedOn*会搜索网络邻域中的计算机，并告知你用户当前是否已登录。

*PsLoggedOn*对本地登录用户的定义是将其配置文件加载到注册表中的用户，因此*PsLoggedOn*通过扫描 HKEY_USERS 密钥下的密钥来确定登录的用户。 对于名称为用户 SID（安全标识符）的每个密钥，*PsLoggedOn*会查找并显示相应的用户名。 为了确定谁通过资源共享登录到计算机，*PsLoggedOn*使用*NetSessionEnum* API。 请注意，*PsLoggedOn*会将你显示为通过资源共享登录到你查询的远程计算机，因为*PsLoggedOn*需要登录才能访问远程系统的注册表。

安装

只需将*PsLoggedOn*复制到可执行文件路径，然后键入 "psloggedon"。

使用 PsLoggedOn

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

展开表

参数	说明
-	显示支持的选项和用于输出值的度量单位。
-l	仅显示本地登录，而不是本地和网络资源登录。
-x	不显示登录时间。

参数	说明
\\computername	指定要列出其登录信息的计算机的名称。
username	如果指定用户名*PsLoggedOn*，请在网络中搜索该用户登录的计算机。 如果要确保特定用户未在即将更改其用户配置文件配置时登录，这非常有用。

 **下载 PsTools** (2.7 MB)

PsTools

*PsLoggedOn*是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为*PsTools*的本地和远程系统。

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

PsLogList v2.82

项目 • 2024/07/25

作者： Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools** **(5 MB)**

介绍

资源工具包附带实用工具 elogdump，允许在本地或远程计算机上转储事件日志的内容。 *PsLogList*是 elogdump 的克隆，但*PsLogList*允许在当前安全凭据集不允许访问事件日志的情况下登录到远程系统，*PsLogList*从你查看的事件日志所在的计算机上检索消息字符串。

安装

只需将*PsLogList*复制到可执行文件路径，然后键入 "psloglist"。

使用 PsLogList

*PsLogList*的默认行为是采用事件日志记录的直观友好格式，在本地计算机上显示系统事件日志的内容。 命令行选项允许查看不同计算机上的日志、使用不同的帐户查看日志，或者以字符串搜索友好方式设置输出格式。

用法： psloglist [-] [\\computer[,**计算机**[,...] | @file [-u **用户名** [-p **密码**]]] [-s [-t **分隔符**]] [-m #|-n #|-h #|-d #|-w][-c][-x][-r][-a mm/dd/yy][-b mm/dd/yy][-f **筛选器**] [-i ID[,ID[,...] | -e ID[,ID[,...]]] [-o **事件源**[,**事件源**][,..]]] [-q **事件源**[，**事件源**][,..]]] [-l **事件日志文件**] <eventlog>

展开表

参数	说明
@file	在文件中列出的每台计算机上执行命令。
-a	转储在指定日期之后标记的记录。
-b	转储在指定日期之前标记的记录。
-c	显示后清除事件日志。

参数	说明
-d	仅显示前 n 天的记录。
-c	显示后清除事件日志。
-e	排除具有指定 ID 或 ID 的事件（最多 10 个）。
-f	使用筛选器字符串筛选事件类型（例如，"-f w" 筛选警告）。
-h	仅显示前 n 个小时的记录。
-i	仅显示具有指定 ID 或 ID 的事件（最多 10 个）。
-l	从指定的事件日志文件转储记录。
-m	仅显示前 n 分钟的记录。
-n	仅显示指定的最新条目数。
-o	仅显示来自指定事件源的记录（例如 \"-o cdrom\"）。
-p	指定用户名的可选密码。 如果省略此内容，系统将提示你输入隐藏密码。
-q	省略指定事件源或源中的记录（例如 \"-q cdrom\"） 。
-r	从最远到最近转储日志。
-s	此开关每行都有*PsLogList*打印事件日志记录，字段用逗号分隔。 此格式便于文本搜索，例如 psloglist
-t	默认分隔符为逗号，但可以使用指定的字符替代。
-u	指定登录远程计算机的可选用户名。
-w	等待新事件，在生成时将其转储（仅本地系统）。
-x	转储扩展数据
eventlog	eventlog

工作方式

与 Win NT/2K 的内置事件查看器和资源工具包的 elogdump 一样，*PsLogList*使用事件日志 API，该 API 记录在 Windows 平台 SDK 中。 *PsLogList*在正在查看的事件日志所在的系统上加载消息源模块，以便正确显示事件日志消息。

 **下载 PsTools** **(5 MB)**

PsTools

*PsLogList*是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为*PsTools*的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

RootkitRevealer v1.71

项目 • 2023/08/03

作者：Mark Russinovich

发布时间：2006 年 11 月 1 日

下载 RootkitRevealer (231 KB)
立即从 Sysinternals Live 运行。

简介

RootkitRevealer 是一种高级 rootkit 检测实用工具。 它在 Windows XP (32 位) 和 Windows Server 2003 (32 位) 上运行，它的输出会列出可能表明存在用户模式或内核模式 rootkit 的注册表和文件系统 API 差异。 RootkitRevealer 可成功检测许多持久性 rootkit，包括 AFX、Vanquish 和 HackerDefender（注意：RootkitRevealer 不应用于检测不会尝试隐藏其文件或注册表项的 rootkit，如 Fu）。 如果你用它来识别 rootkit 的存在，请告诉我们!

不再存在命令行版本的原因是恶意软件创建者已开始使用 RootkitRevealer 的可执行名称来针对 RootkitRevealer 的扫描。 因此，我们更新了 RootkitRevealer，以从作为 Windows 服务运行的其自身随机命名副本执行扫描。 这种类型的执行不利于命令行接口。 请注意，你可以使用命令行选项对记录到文件的结果执行自动扫描，这相当于命令行版本的行为。

什么是 Rootkit?

术语 rootkit 用于描述恶意软件（包括病毒、间谍软件和木马病毒）尝试躲过间谍软件阻止程序、防病毒和系统管理实用程序的机制和技术。 有几种 rootkit 的分类，具体取决于恶意软件是否在重启后依然存在，以及它是在用户模式还是内核模式下执行。

持久性 Rootkit
持久性 rootkit 是在每次系统启动时激活的恶意软件。 由于此类恶意软件包含必须在每次系统启动时或用户登录时自动执行的代码，因此它们必须将代码存储在持久存储（如注册表或文件系统）中，并配置一种无需用户干预即可执行代码的方法。

基于内存的 Rootkit
基于内存的 rootkit 是没有持久性代码的恶意软件，因此在重启后无法生存。

用户模式 Rootkit
rootkit 会尝试通过多种方法逃避检测。 例如，用户模式 rootkit 可能会拦截对 Windows

FindFirstFile/FindNextFile API 的所有调用，这些调用由文件系统浏览实用工具（包括资源管理器和命令提示符）用来枚举文件系统目录的内容。 当应用程序执行目录列出时，本来会返回包含标识与 rootkit 相关的文件的结果条目，但 rootkit 会拦截并修改输出以删除这些条目。

Windows 本机 API 充当用户模式客户端和内核模式服务之间的接口，更复杂的用户模式 rootkit 会拦截本机 API 的文件系统、注册表和进程枚举函数。 这会防止扫描程序通过将 Windows API 枚举的结果与本机 API 枚举返回的结果进行比较来检测它们。

内核模式 Rootkit
内核模式 rootkit 可能更强大，因为它们不仅可以在内核模式下拦截本机 API，还可以直接操控内核模式数据结构。 隐藏恶意软件进程的常见方法是从内核的活动进程列表中删除进程。 由于进程管理 API 依赖于列表的内容，恶意软件进程将不会显示在任务管理器或进程资源管理器等进程管理工具中。

RootkitRevealer 的工作原理

由于持久性 rootkit 会通过更改 API 结果来工作，让使用 API 的系统视图与存储中的实际视图不同，因此 RootkitRevealer 会将最高级别的系统扫描结果与最低级别的系统扫描结果进行比较。 最高级别是 Windows API，最低级别是文件系统卷或注册表配置单元的原始内容（配置单元文件是注册表的磁盘存储格式）。 因此，RootkitRevealer 会将操控 Windows API 或本机 API 以从目录列表中删除其状态的 rootkit（无论是用户模式还是内核模式）视为 Windows API 返回的信息与在 FAT 或 NTFS 卷文件系统结构的原始扫描中看到的信息之间的差异。

Rootkit 是否可以躲过 RootkitRevealer
从理论上讲，rootkit 有可能会躲过 RootkitRevealer。 要做到这一点，需要拦截 RootkitRevealer 对注册表配置单元数据或文件系统数据的读取，并更改数据的内容，使 rootkit 的注册表数据或文件不存在。 但是，这需要迄今为止 rootkit 中未见的成熟程度。 要更改这些数据，需要深入了解 NTFS、FAT 和注册表配置单元格式，以及更改数据结构以隐藏 rootkit 的能力，但这并不会导致 RootkitRevealer 标记的结构或副作用差异不一致或无效。

是否有一种肯定的方法可以知道 rootkit 的存在
通常，无法从正在运行的系统内部做到。 内核模式 rootkit 可以控制系统行为的任何方面，因此任何 API 返回的信息（包括由 RootkitRevealer 执行的注册表配置单元的原始读取和文件系统数据）都可能遭到入侵。 虽然将系统的在线扫描和安全环境（例如启动到基于 CD 的操作系统安装）的脱机扫描进行比较更可靠，但 rootkit 可以针对此类工具来规避检测。

底线是，永远不会有通用的 rootkit 扫描程序，但最强大的扫描程序是与防病毒集成的线上/线下比较扫描程序。

使用 RootkitRevealer

RootkitRevealer 要求运行它的账户分配有备份文件和目录、加载驱动程序和执行卷维护任务（Windows XP 和更高）的权限。 默认情况下，管理员组会被分配这些权限。 为了尽量减少误报，请在空闲系统上运行 RootkitRevealer。

为了获得最佳结果，请退出所有应用程序，并在 RootkitRevealer 扫描过程中使系统保持空闲状态。

如果有疑问或问题，请访问 Sysinternals RootkitRevealer 论坛。

手动扫描

若要扫描系统，请在系统上启动它，然后按“扫描”按钮。 RootkitRevealer 会扫描系统，并在窗口底部的状态区域中报告其操作，在输出列表中指出差异。 可以配置的选项：

- **隐藏 NTFS 元数据文件：**此选项默认处于打开状态，并且使 RootkitRevealer 不显示标准 NTFS 元数据文件，这些文件在 Windows API 中隐藏。
- **扫描注册表：**此选项默认处于打开状态。 取消选择它后，RootkitRevealer 将不执行注册表扫描。

启动自动扫描

RootkitRevealer 支持多个自动扫描系统选项：

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

参数	说明
-a	完成后自动扫描并退出。
-c	将输出格式设置为 CSV。
-m	显示 NTFS 元数据文件。
-r	不扫描注册表。

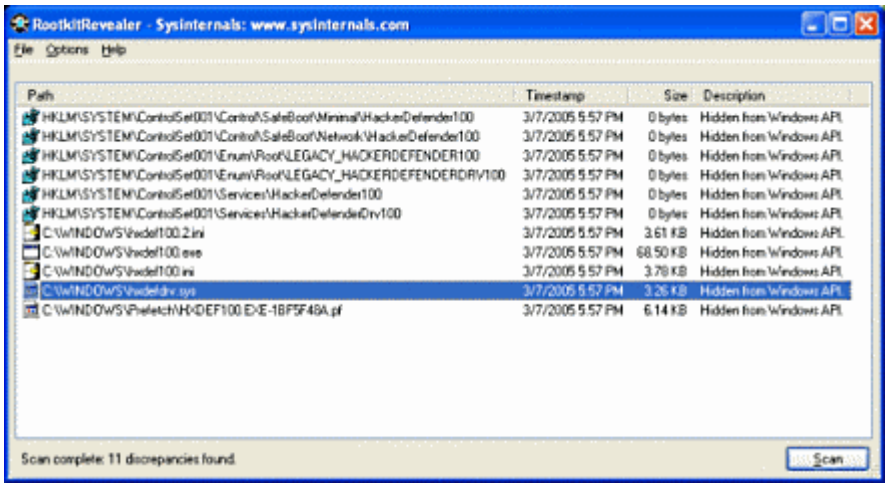
请注意，文件输出位置必须位于本地卷上。

如果指定了 -c 选项，则不会报告进度，并且会以 CSV 格式输出差异，以便轻松导入数据库。 可以使用如下所示的命令行通过 Sysinternals PsExec 实用工具执行远程系统的扫描：

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

解释输出

这是 RootkitRevealer 检测是否存在常用 HackerDefender rootkit 的屏幕截图。 注册表项差异表明，存储 HackerDefender 的设备驱动程序和服务设置的注册表项对 Windows API 不可见，但存在于注册表配置单元数据的原始扫描中。 同样，与 HackerDefender 关联的文件对 Windows API 目录扫描不可见，但存在于原始文件系统数据的扫描中。



应检查所有差异，并确定它们表明的存在 rootkit 的可能性。 遗憾的是，无法根据输出确定是否存在 rootkit，但应检查所有报告的差异，以确保它们可解释。 如果你确定已安装 rootkit，请在网上搜索删除说明。 如果不确定如何删除 rootkit，则应重新格式化系统硬盘并重新安装 Windows。

除了下面有关可能的 RootkitRevealer 差异的信息外，Sysinternals 的 RootkitRevealer 论坛还讨论了检测到的 rootkit 和特定的误报。

在 Windows API 中隐藏

这些差异是大多数 rootkit 所表现出的差异：但是，如果你尚未选中“隐藏 NTFS 元数据文件”，则你应该会在任何 NTFS 卷上看到许多此类条目，因为 NTFS 会向 Windows API 隐藏其元数据文件（如 $MFT 和 $Secure）。 NTFS 卷上存在的元数据文件因 NTFS 版本和卷上已启用的 NTFS 功能而异。 还有一些防病毒产品（如卡巴斯基防病毒）使用 rootkit 技术隐藏存储在 NTFS 备用数据流中的数据。 如果运行的是此类病毒扫描程序，则你会在每个 NTFS 文件上看到备用数据流的“在 Windows API 中隐藏”的差异。
RootkitRevealer 不支持输出筛选器，因为 rootkit 可以利用任何筛选。 最后，如果在扫描期间删除了文件，则也可能看到此差异。

这是在 Windows Server 2003 中定义的 NTFS 元数据文件的列表：

- $AttrDef
- $BadClus
- $BadClus:$Bad
- $BitMap

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

禁止访问。
RootkitRevealer 绝不应报告此差异，因为它使用允许其访问系统上的任何文件、目录或注册表项的机制。

在 Windows API、目录索引中可见，但在 MFT 中不可见。
在 Windows API 中可见，但在 MFT 或目录索引中不可见。
在 Windows API、MFT 中可见，但在目录索引中不可见。
在目录索引中可见，但在 Windows API 或 MFT 中不可见。

文件系统扫描由三个组件构成：Windows API、NTFS 主文件表 (MFT) 和 NTFS 磁盘目录索引结构。 这些差异表明一个文件只会出现在一个或两个扫描中。 一个常见原因是会在扫描期间创建或删除文件。 下面是 RootkitRevealer 针对扫描期间创建的文件的差异报告的示例：

C:\newfile.txt
2005/3/1 下午 5:26
8 字节
在 Windows API 中可见，但在 MFT 或目录索引中不可见。

Windows API 长度与原始配置单元数据不一致。
Rootkit 可以尝试通过歪曲注册表值的大小来隐藏自身，使其内容对 Windows API 不可见。 应检查任何此类差异，但它也可能显示为扫描期间注册表值更改的结果。

Windows API 与原始配置单元数据之间的类型不匹配。
注册表值具有类型，例如 DWORD 和 REG_SZ，此差异指出，通过 Windows API 报告的值的类型与原始配置单元数据的类型不同。 例如，rootkit 可以通过将其存储为 REG_BINARY 值并让 Windows API 认为它是 REG_SZ 值来屏蔽其数据。如果它在数据的开头存储了一个 0，则 Windows API 将无法访问后续数据。

键名称包含嵌入的 null。
Windows API 将键名称视为以 null 结尾的字符串，而内核将它们视为计数字符串。 因此，可以创建对操作系统可见的注册表项，但仅对 Regedit 等注册表工具部分可见。 Sysinternals 的 Reghide 示例代码演示了此方法，恶意软件和 rootkit 都会使用此方法来隐藏注册表数据。 使用 Sysinternals RegDelNull 实用工具删除包含嵌入 null 的键。

Windows API 与原始配置单元数据之间的数据不匹配。
如果在注册表扫描正在进行时更新注册表值，则会发生此差异。 经常更改的值包括时间戳，例如 Microsoft SQL Server 运行时间值（如下所示）和病毒扫描程序的"上次扫描时间"值。 应调查任何报告的值，以确保它是有效的应用程序或系统注册表值。

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

Rootkit 资源

以下网站和书籍是有关 rootkit 的详细信息的来源：

Sony, Rootkits and Digital Rights Management Gone Too Far
阅读 Mark 的博客文章，了解他在他的一台计算机上发现和分析索尼 rootkit 的故事。

Unearthing Rootkits
Mark 在 6 月的 *Windows IT Pro Magazine* 文章概述了 rootkit 技术以及 RootkitRevealer 的工作原理。

Rootkits: Subverting the Windows Kernel
Greg Hoglund 和 Jamie Butler 写的这本书是目前对 rootkit 最全面的论述。

www.phrack.org
这个网站存储了 *Phrack* 的存档，Phrack 是面向破解者的杂志，开发人员可在其中讨论安全相关产品的缺陷、rootkit 技术和其他恶意软件技巧。

The Art of Computer Virus Research and Defense，作者：Peter Szor

Malware: Fighting Malicious Code，作者：Ed Skoudis 和 Lenny Zeltser

Windows Internals，第 4 版，作者：Mark Russinovich 和 Dave Solomon（这本书没有讨论 rootkit，但了解 Windows 体系结构有助于了解 rootkit）。

下载 RootkitRevealer (231 KB)

立即从 Sysinternals Live 运行。

Sysmon v15.2

通过 Mark Russinovich 和 Thomas Garnier

发布时间： 2026 年 3 月 26 日

 **下载 Sysmon** (4.6 MB)

下载适用于 Linux 的 Sysmon (GitHub)

简介

系统监视器 (*Sysmon*) 是一项 Windows 系统服务，也是一个设备驱动程序，一旦安装在系统上，就会在系统重新启动后一直驻留，以监视系统活动并将其记录到 Windows 事件日志中。 它提供有关进程创建、网络连接和文件创建时间更改的详细信息。 通过使用 Windows 事件收集或 SIEM 代理收集生成的事件，然后对事件进行分析，你可识别恶意或异常活动，并了解入侵者和恶意软件如何在网络上运行。 该服务作为受保护的进程运行，从而禁止广泛的用户模式交互。

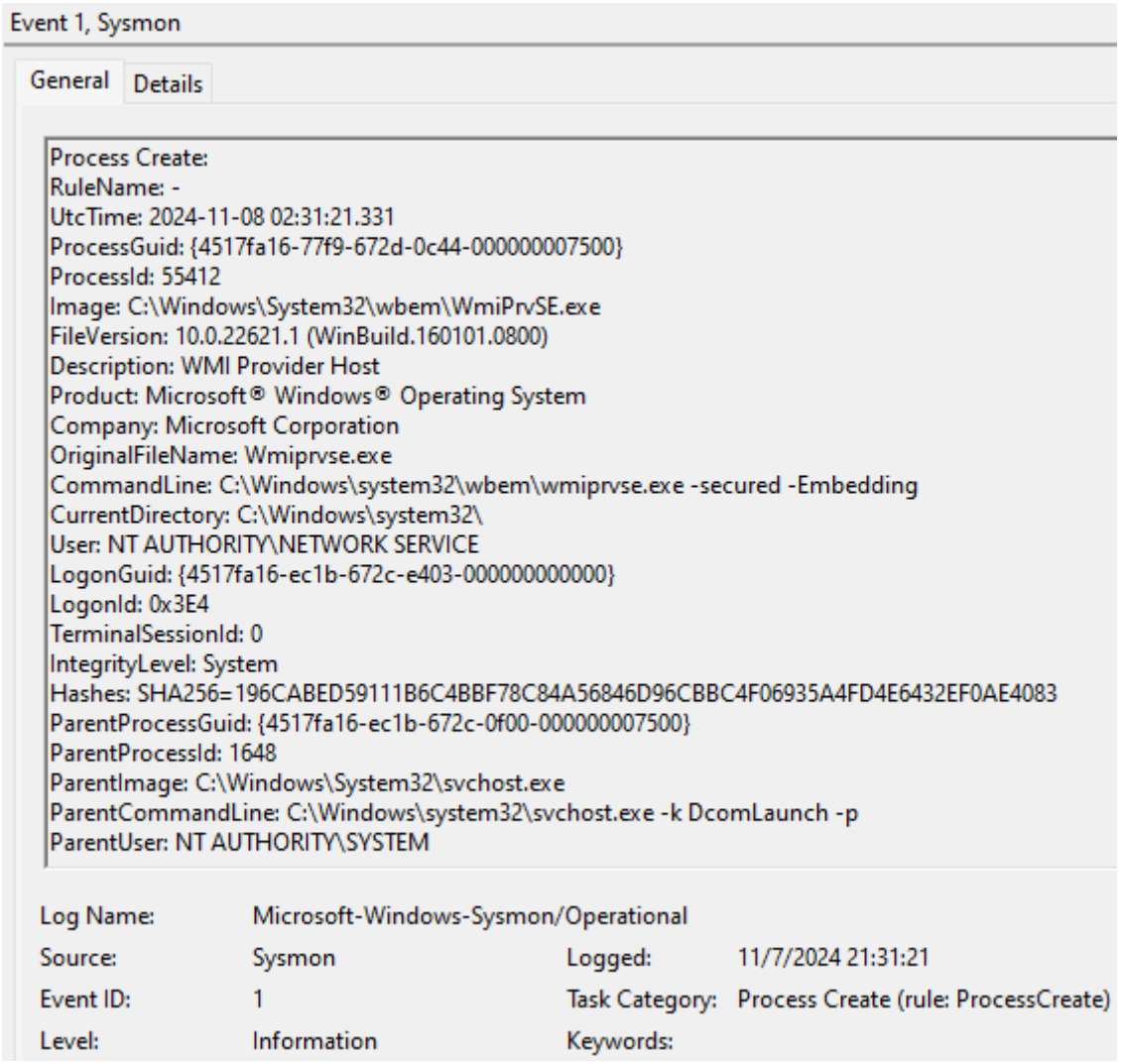
请注意，“Sysmon”不会提供对其生成的事件的分析，也不会尝试隐藏自己以免受攻击者的攻击。

Sysmon 功能概述

Sysmon 包括以下功能：

- 记录使用完整命令行的当前进程和父进程的进程创建。
- 记录使用 SHA1（默认）、MD5、SHA256 或 IMPHASH 的进程映像文件的哈希。
- 可以同时使用多个哈希。
- 在进程创建事件中包含一个进程GUID，以便在Windows重新使用进程ID时实现事件关联。
- 在每个事件中包含一个会话 GUID，以便在同一登录会话中关联事件。
- 记录驱动程序或 DLL 的加载及其签名与哈希。
- 记录对磁盘和卷的原始读取访问事件。
- （可选）记录网络连接，包括每个连接的源进程、IP 地址、端口数量、主机名和端口名称。
- 检测文件创建时间的更改，以了解文件真正创建的时间。 修改文件创建时间戳是恶意软件常用的技术，目的是掩盖其踪迹。
- 如果注册表中发生更改，则自动化重新加载配置。
- 进行规则筛选以动态包含或不包含某些事件。
- 在启动进程之初生成事件，以捕获相当复杂的内核模式恶意软件进行的活动。

屏幕截图



使用情况

使用简单命令行选项来安装和卸载 Sysmon，以及检查和修改其配置的常见用法：

安装：`sysmon64 -i [<configfile>]`
更新配置：`sysmon64 -c [<configfile>]`
安装事件清单：`sysmon64 -m`
打印架构：`sysmon64 -s`
卸载：`sysmon64 -u [force]`

展开表

参数	说明
-i	安装服务和驱动程序。 可以选择配置文件。

参数	说明
-c	如果未提供其他参数，则更新已安装的 Sysmon 驱动程序的配置或转储当前配置。 可选地接受配置文件。
-m	安装事件清单（在服务安装时也会自动安装）。
-s	打印配置架构定义。
-u	卸载服务和驱动程序。 使用“`-u force`”会导致卸载继续进行，即使未安装一些组件。

服务会立即记录事件，驱动程序将作为引导启动驱动程序进行安装，以便从启动的早期阶段捕获活动，并且服务启动时会将这些事件写入事件日志。

在 Vista 以及更新的系统上，事件存储在 `Applications and Services Logs/Microsoft/Windows/Sysmon/Operational` 中。 在较旧的系统中，事件写入到“`System`”事件日志。

如果需要与配置文件有关的更多信息，请使用“`-? config`”命令。

指定 `-accepteula` 在安装时自动接受 EULA，否则系统会以交互方式提示你接受。

安装或卸载都不需要重启。

示例

使用默认设置进行安装（进程映像已经过 SHA1 哈希处理，且没有网络监视）

Windows 命令提示符

```
sysmon -accepteula -i
```

使用配置文件安装 Sysmon（如下所述）

Windows 命令提示符

```
sysmon -accepteula -i c:\windows\config.xml
```

卸载

Windows 命令提示符

```
sysmon -u
```

转储当前配置

Windows 命令提示符

```
sysmon -c
```

使用配置文件重新配置正在运行的 Sysmon（具体说明如下）

Windows 命令提示符

```
sysmon -c c:\windows\config.xml
```

将配置更改为默认设置

Windows 命令提示符

```
sysmon -c --
```

显示配置架构

Windows 命令提示符

```
sysmon -s
```

事件

在 Vista 以及更新的系统上，事件存储在 `Applications and Services Logs/Microsoft/Windows/Sysmon/Operational` 中；在较旧的系统上，事件写入“`System`”事件日志。 事件时间戳采用 UTC 标准时间。

下面是 Sysmon 生成的每种事件类型的示例。

事件 ID 1：进程创建

进程创建事件提供有关新创建的进程的扩展信息。 完整命令行提供进程执行的相关上下文。 “`ProcessGUID`”字段是此进程在整个域中的唯一值，能够简化事件关联。 哈希是文件的完整哈希，其中包含“`HashType`”字段中的算法。

事件 ID 2：进程更改了文件创建时间

当进程明确修改了文件创建时间时，将注册更改文件创建时间事件。 此事件可帮助跟踪文件的实际创建时间。 攻击者可能会更改后门的文件创建时间，使其看起来像是随操作系统一起安装

的。 请注意，许多进程会合法地更改文件的创建时间，这种行为不一定表示恶意活动。

事件 ID 3：网络连接

网络连接事件记录计算机上的 TCP/UDP 连接。 此项默认禁用。 每个连接都通过 `ProcessId` 和 `ProcessGuid` 字段链接到一个进程。 该事件还包含源和目标主机名 IP 地址、端口号和 IPv6 状态。

事件 ID 4：Sysmon 服务状态已更改

服务状态更改事件报告 Sysmon 服务的状态（已启动或已停止）。

事件 ID 5：进程已终止

进程终止事件在进程终止时进行报告。 它提供进程的 `UtcTime`、 `ProcessGuid` 和 `ProcessId`。

事件 ID 6：驱动程序已加载

驱动程序加载事件提供有关系统上驱动程序加载的信息。 会提供已配置的哈希以及签名信息。 出于性能，签名以异步方式创建，指示加载后文件是否被删除。

事件 ID 7：映像已加载

映像加载事件在特定进程中记录模块加载时的日志。 此事件默认处于禁用状态，需要使用“`-l`”选项进行配置。 它表示模块被加载的过程、哈希值和签名信息。 出于性能，签名以异步方式创建，指示加载后文件是否被删除。 应小心配置此事件，因为监视所有映像加载事件会产生大量日志记录。

事件 ID 8：CreateRemoteThread

“`CreateRemoteThread`”事件检测一个进程在另一个进程中创建线程的时间。 恶意软件使用这种方法注入代码并隐藏在另一个进程中。 此事件指示源进程和目标进程。 它提供将会在新线程中运行的代码的相关信息： `StartAddress`、 `StartModule` 和 `StartFunction`。 请注意， `StartModule` 和 `StartFunction` 字段是推断出来的。如果起始地址在加载的模块或已知导出的函数之外，则这两个字段可能为空。

事件 ID 9：RawAccessRead

“`RawAccessRead`”事件检测进程在使用“`\\.\`”表示从驱动器进行读取操作时。 恶意软件通常使用这种方法让已锁定不许读取的文件发生数据泄露，以及避开文件访问审计工具。 此事件指示源进程和目标设备。

事件 ID 10：进程访问

进程访问事件报告进程打开另一个进程的操作，这一操作通常伴随信息查询，或读取或写入目标进程的地址空间。 这使得能够检测到黑客工具，这些工具通过读取本地安全机构 (Lsass.exe) 等进程的内存内容来窃取凭据，以便在哈希传递攻击中使用。 如果有诊断实用工具反复打开进程来查询其状态，则启用此事件会产生大量日志记录。因此，一般而言应该仅使用移除预计的访问的筛选器来完成此操作。

事件 ID 11：FileCreate

当文件被创建或覆盖时，文件创建操作会被记录下来。 此事件可用于监视自动启动位置，例如启动文件夹，以及临时和下载目录，这些是初始感染期间恶意软件会前往的常见位置。

Event ID 12：RegistryEvent（对象创建和删除）

注册表项和值创建和删除操作映射到此事件类型，此事件可用于监视对注册表自动启动位置的更改，或特定恶意软件注册表修改。

Sysmon 使用注册表根键名称的缩写版本，具体映射如下：

展开表

键名	缩写
`HKEY_LOCAL_MACHINE`	`HKLM`
`HKEY_USERS`	`HKU`
`HKEY_LOCAL_MACHINE\System\ControlSet00x`	`HKLM\System\CurrentControlSet`
`HKEY_LOCAL_MACHINE\Classes`	`HKCR`

事件 ID 13：RegistryEvent（值设置）

此注册表事件类型识别注册表值修改。 此事件记录为类型 `DWORD` 和 `QWORD` 的注册表值写入的值。

事件 ID 14：注册表事件（键和值重命名）

注册表项和值重命名操作映射到此事件类型，记录重命名后的项或值的新名称。

事件 ID 15：FileCreateStreamHash

此事件记录已命名文件流的创建，并生成事件来记录流被分配到的文件（未命名流）的内容哈希值，以及已命名流的内容。 有的恶意软件变体通过浏览器下载来放置其可执行文件或配置设置，此事件旨在根据浏览器附加 `Zone.Identifier` "Web 标记"流来捕获此类情况。

事件 ID 16：ServiceConfigurationChange（服务配置更改）

此事件记录 Sysmon 配置中的更改，例如，更新筛选规则的时间。

事件 ID 17：PipeEvent（管道已创建）

当创建已命名的管道时生成此事件。 恶意软件通常使用已命名管道进行进程间通信。

事件 ID 18：PipeEvent（管道已连接）

此事件记录客户端和服务器之间建立已命名管道连接的时间。

事件 ID 19：WmiEvent（检测到 WmiEventFilter 活动）

注册 WMI 事件筛选器时，恶意软件使用此方法来执行攻击，此事件记录 WMI 命名空间、筛选器名称和筛选器表达式。

事件 ID 20：WmiEvent（检测到 WmiEventConsumer 活动）

此事件记录 WMI 消费者的注册，记录消费者名称、日志和目的地。

事件 ID 21：WmiEvent（检测到 WmiEventConsumerToFilter 活动）

当使用者绑定到某个筛选器时，此事件记录下该使用者的姓名和筛选器路径。

事件 ID 22：DNSEvent（DNS 查询）

无论结果是成功还是失败、是否会缓存，当进程执行 DNS 查询时都会生成此事件。 已为 Windows 8.1 添加了此事件的遥测，因此它在 Windows 7 及更早版本上不可用。

事件 ID 23：文件删除（文件已被存档）

文件已删除。 除了记录此事件，被删除的文件还保存在 `ArchiveDirectory` 中（`C:\Sysmon` 是默认）。 正常运行的情况下，此目录可能会增长到不合理的大小，请参阅事件 ID 26：`FileDeleteDetected`，其行为虽然类似，但是不保存被删除的文件。

事件 ID 24：ClipboardChange——剪贴板中有新内容

系统剪贴板内容发生变化时会生成此事件。

事件 ID 25：进程篡改（进程映像更改）

当检测到像“hollow”或“herpaderp”这样的进程隐藏手段时，会生成此事件。

事件编号26：文件删除检测（文件删除已被记录）

文件已删除。

事件 ID 27：FileBlockExecutable

当 Sysmon 检测并阻止创建可执行文件（PE 格式）时生成此事件。

事件 ID 28：FileBlockShredding

当 Sysmon 检测并阻止 SDelete 等工具粉碎文件时生成此事件。

事件 ID 29：FileExecutableDetected

当 Sysmon 检测到新建可执行文件（PE 格式）时生成此事件。

事件 ID 255：错误

当 Sysmon 中发生错误时生成此事件。 如果系统负载过重且无法执行某些任务或 Sysmon 服务中存在 bug，或者即使不满足某些安全和完整性条件，也可能发生这些错误。 可以在 Sysinternals 论坛上报告任何 bug。

配置文件

可以在 **-i**（安装）或 **-c**（安装）配置开关之后指定配置文件。 它们更方便地部署预设配置并筛选捕获的事件。

简单的配置 xml 文件如下所示：

XML

```xml
<Sysmon schemaversion="4.82">
  <!-- Capture all hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condition="contains">microsoft</Signature>
      <Signature condition="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include" />
    <!-- Log network connection if the destination port equal 443 -->
    <!-- or 80, and process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
    </NetworkConnect>
  </EventFiltering>
</Sysmon>
```

配置文件中包含 Sysmon 标记上的架构版本属性。 此版本独立于 Sysmon 二进制版本，允许解析较旧的配置文件。 可以使用“`-? config`”命令行来获取当前的架构版本。 配置条目直接在“`Sysmon`”标记下，筛选器在“`EventFiltering`”标记下。

配置项

配置条目类似于命令行开关，包括以下内容

配置条目包括以下内容：

展开表

条目	值	说明
ArchiveDirectory	字符串	卷根上的目录的名称，删除时复制文件将移动到其中。 目录受系统 ACL 保护（可使用 Sysinternals 提供的 PsExec 来访问使用“`psexec -sid cmd`”的目录）。 默认：`Sysmon`
检查吊销状态	布尔	控制签名吊销检查。 默认：`True`

条目	值	说明
CopyOnDeletePE	布尔	保留已删除的可执行映像文件。 默认：`False`
CopyOnDeleteSIDs	字符串	将保留文件删除的帐户 SID 列表，以逗号分隔。
CopyOnDeleteExtensions	字符串	删除时保留的文件的扩展名。
删除后复制进程	字符串	将为其保留文件删除的进程名称。
DnsLookup	布尔	控制反向 DNS 查询。 默认：`True`
DriverName	字符串	使用驱动程序和服务映像的指定名称。
哈希算法	字符串	用于哈希处理的哈希算法。 支持的算法包括 MD5、SHA1、SHA256、IMPHASH 和 *（全部）。 默认：`None`

命令行开关拥有其在 Sysmon 使用输出中所述的配置条目。 参数是否可选取决于标记。 如果命令行开关还启用事件，则需要通过其过滤器标签对其进行配置。 可以指定 `-s` 开关，让 Sysmon 打印完整的配置架构，包括事件标记以及每个事件的字段名称和类型。 例如，以下是“`RawAccessRead`”事件类型的架构：

XML

```
<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>
```

事件筛选条目

事件筛选允许筛选生成的事件。 许多情况下，事件中的噪声太大，无法收集到所有信息。 例如，你可能只对某一个进程而非所有进程的网络连接感兴趣。 这种情况下，可以筛选主机上的

输出，减少要收集的数据。

每个事件在配置文件中的 EventFiltering 节点下都有自己的筛选器标记：

展开表

ID	标记	事件
1	ProcessCreate	进程创建
2	文件创建时间	文件创建时间
3	NetworkConnect	检测到网络连接
4	不适用	Sysmon 服务状态更改（无法筛选）
5	ProcessTerminate	进程已终止
6	DriverLoad	驱动程序已加载
7	ImageLoad	图像已加载
8	CreateRemoteThread	检测到 Remote Thread 创建
9	RawAccessRead	检测到 RawAccessRead 功能
10	ProcessAccess	进程被访问
11	FileCreate	文件已创建
12	RegistryEvent	已添加或删除注册表对象
13	注册事件	注册表值已设定
14	RegistryEvent	注册表对象已重命名
15	FileCreateStreamHash	文件流已创建
16	不适用	Sysmon 配置更改（无法筛选）
17	PipeEvent	已命名管道已创建
18	PipeEvent	已命名管道已连接
19	WmiEvent	WMI 筛选器
20	WmiEvent	WMI 使用者
21	WmiEvent	WMI 消费者筛选器
22	DnsQuery	DNS 查询
23	FileDelete（文件删除）	删除已存档文件

ID	标记	事件
24	剪贴板变更	剪贴板中的新内容
25	进程篡改	进程映像更改
26	文件删除检测到	文件删除操作已记录
27	FileBlockExecutable	文件阻止可执行
28	文件块粉碎 (FileBlockShredding)	文件块粉碎
29	检测到可执行文件	检测到可执行文件

还可以在任务名称上的事件查看器中找到这些标记。

如果有事件匹配，则应用“`onmatch`”筛选器。 可以使用筛选器标记的“`onmatch`”属性对其进行更改。 如果值为“`"include"`”，则表示仅包含匹配的事件。 如果设置为“`"exclude"`”，则将包含事件，但规则匹配时除外。 可以为每个事件 ID 同时指定一个包含筛选器集和一个排除筛选器集，其中排除匹配项具有优先处理权。

每个筛选器可包含零个或多个规则。 筛选标签下的每个标签都是事件的字段名。 对于指定相同字段名称条件的规则，其行为为 OR 条件；对于指定不同字段名称条件的规则，其行为为 AND 条件。 字段规则还可以使用条件来匹配值。 条件如下所示（所有条件均不区分大小写）：

展开表

条件	说明
is	所有值默认都相等
是任意	字段是`;`分隔值之一
不是	值不同
contains	字段包含此值
包含任意	字段包含`;`分隔的值中的任意一个
包含全部	字段包含所有以`;`分隔的值
不包含	字段不包含此值
不包含任意	字段不包含由`;`分隔的一个或多个值
排除全部	字段不包含任何由`;`分隔的值
以...开始	字段以此值开头

条件	说明
结尾为	字段以此值结尾
不以...开头	字段不以此值开头
不以...结尾	字段不以此值结尾
小于	按字典顺序比较的结果小于零
大于	字典顺序比较的结果大于零
图像	匹配图像路径（完整路径或仅图像名称）。 例如：`lsass.exe` 将与 `c:\windows\system32\lsass.exe` 匹配

可以通过将其指定为属性来使用不同的条件。 排除路径中包含 iexplore.exe 的进程网络活动：

XML

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

若要让 Sysmon 报告哪个规则匹配导致记录事件，请将名称添加到规则中：

XML

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

可以对同一标记同时使用包含和不包含规则，其中不包含规则优先级高于包含规则。 在规则中，筛选条件具有 OR 行为。

在前面介绍的示例配置中，网络筛选器使用包含规则和不包含规则来捕获除名称中包含 `iexplore.exe` 以外的所有进程到端口 80 和 443 的活动。

还可以通过使用规则组替代规则组合方式，该规则组允许将一个或多个事件的规则组合类型显式设置为 AND 或 OR。

下面的示例演示此用法。 在第一个规则组中，当仅使用 `timeout.exe` 的命令行属性执行 `100` 时将会生成进程创建事件，但 `ping.exe` 和 `timeout.exe` 的终止会生成进程终止事件。

XML

```
  <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>
```

 下载 Sysmon (4.6 MB)

运行于：

- 客户端：Windows 10 及更高版本。
- 服务器：Windows Server 2016 及更高版本。

Last updated on 2026/03/26

Sysinternals 系统信息实用程序

项目 • 2023/08/03

Autoruns

查看在系统启动时和用户登录时配置为自动启动的程序。 Autoruns 还会显示应用程序可在其中配置自动启动设置的注册表和文件位置的完整列表。

ClockRes

查看系统时钟的分辨率，这也是最大计时器分辨率。

Coreinfo

Coreinfo 是一个命令行实用程序，可显示逻辑处理器与物理处理器、NUMA 节点和它们所在套接字之间的映射，以及分配给每个逻辑处理器的缓存。

Handle

这是一个方便的命令行实用程序，可显示哪些文件由哪些进程打开等。

LiveKd

使用 Microsoft 内核调试程序检查实时系统。

LoadOrder

查看设备在 WinNT/2K 系统上的加载顺序。

LogonSessions

列出系统上的活动登录会话。

PendMoves

枚举将在下一次启动时执行的文件重命名和删除命令的列表。

进程资源管理器

了解哪些文件、注册表项和其他对象进程已打开，它们已加载了哪些 DLL 等。 这个独特而强大的实用工具甚至会显示每个进程的所有者。

进程监视器

实时监视文件系统、注册表、进程、线程和 DLL 活动。

ProcFeatures

此小程序可报告处理器和 Windows 对物理地址扩展和无执行缓冲区溢出保护的支持。

PsInfo

获取有关系统的信息。

PsLoggedOn

显示登录到系统的用户

PsTools

PsTools 套件包含命令行实用工具，用于列出在本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志等。

RAMMap

高级物理内存使用情况分析实用程序，可在多个不同的选项卡上以不同方式显示使用情况信息。

WinObj

此处提供了最终对象管理器命名空间查看器。

ClockRes v2.1

项目 • 2024/07/25

作者：Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 ClockRes** **(494 KB)**

简介

曾经想过系统时钟的分辨率是多少，或者应用程序能获得的最大计时器分辨率吗？ 答案位于名为 *GetSystemTimeAdjustment* 的简单函数中，*ClockRes* 小程序执行该函数并显示结果。

 **下载 ClockRes** **(494 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

Coreinfo v4.0

作者： Mark Russinovich

发布时间： 2025 年 12 月 16 日

 Coreinfo **(3 MB)**

简介

Coreinfo 是一个实用工具，显示逻辑处理器与物理处理器、NUMA 节点和它们所在的套接字之间的映射，以及分配给每个逻辑处理器的缓存。 它使用低级别 Windows API（用户模式和内核模式）直接从作系统检索详细的 CPU 拓扑信息。 命令行版本输出映射到逻辑处理器的表示形式，并用星号标示，例如“`*`”。 UI 提供了多个专用视图来探索系统 CPU 拓扑的不同方面，包括逻辑核心和物理核心、NUMA 节点、套接字、缓存层次结构和实时性能指标。 Coreinfo 可用于深入了解系统的处理器和缓存拓扑。

安装

将存档提取到一个目录中，然后根据体系结构通过在该目录中键入`Coreinfo` / `Coreinfo64`或`Coreinfo64a`来运行 Coreinfo。 启动 `CoreInfoEx` / `CoreInfoEx64` / `CoreInfoEx64a` 的 UI 版本。

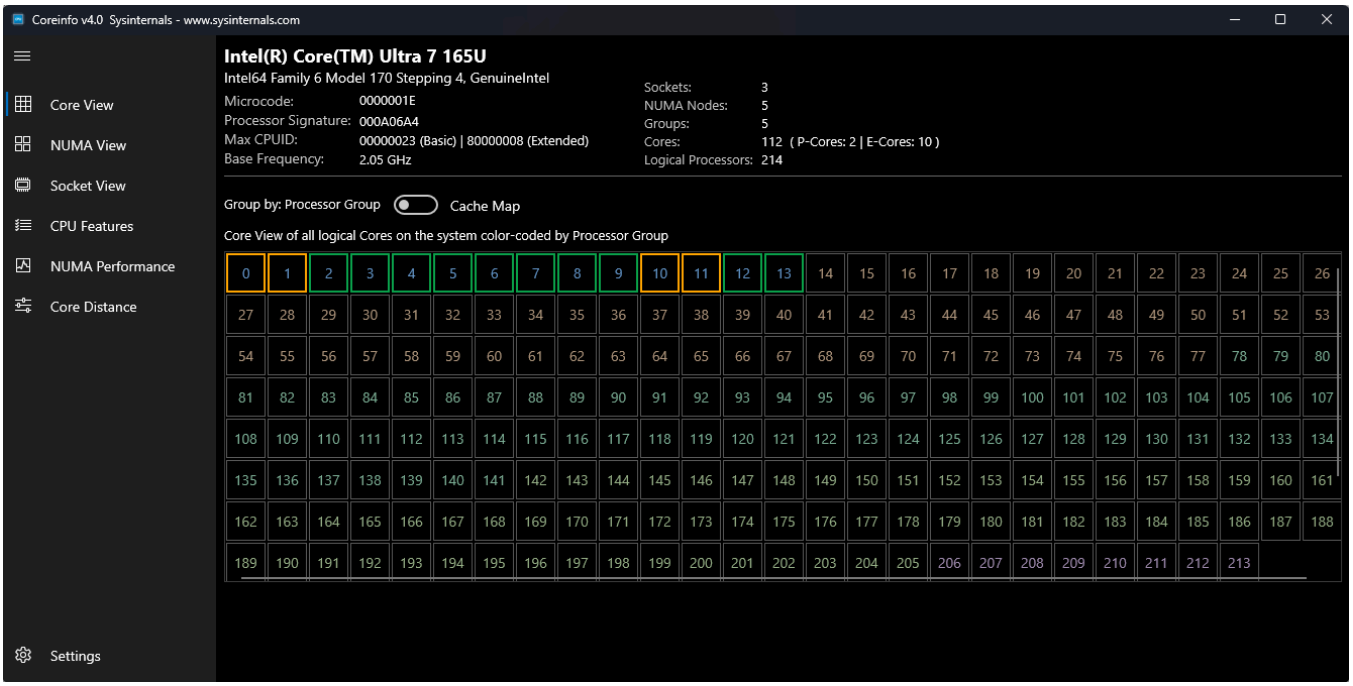
注意： 某些功能可能需要管理权限才能完成信息检索。

用户界面概述

Coreinfo UI 由多个关键组件组成：

主窗口布局

- **顶部面板**：显示系统信息，包括 CPU 名称、体系结构和核心计数
- **导航窗格** （左）： 提供对不同视图的快速访问
- **内容区域** （中心）： 显示所选视图的数据和可视化效果
- **详细信息窗格** （底部）： 选择核心或单元格时显示详细信息
- **设置**：访问外观选项和应用程序首选项



主窗口显示完整的 UI 布局， 深色模式

导航视图

左侧导航窗格提供对六个专用视图的访问权限：

1. 核心视图

核心视图在网格布局中显示系统中的所有逻辑处理器，显示逻辑核心与其物理资源之间的关系。

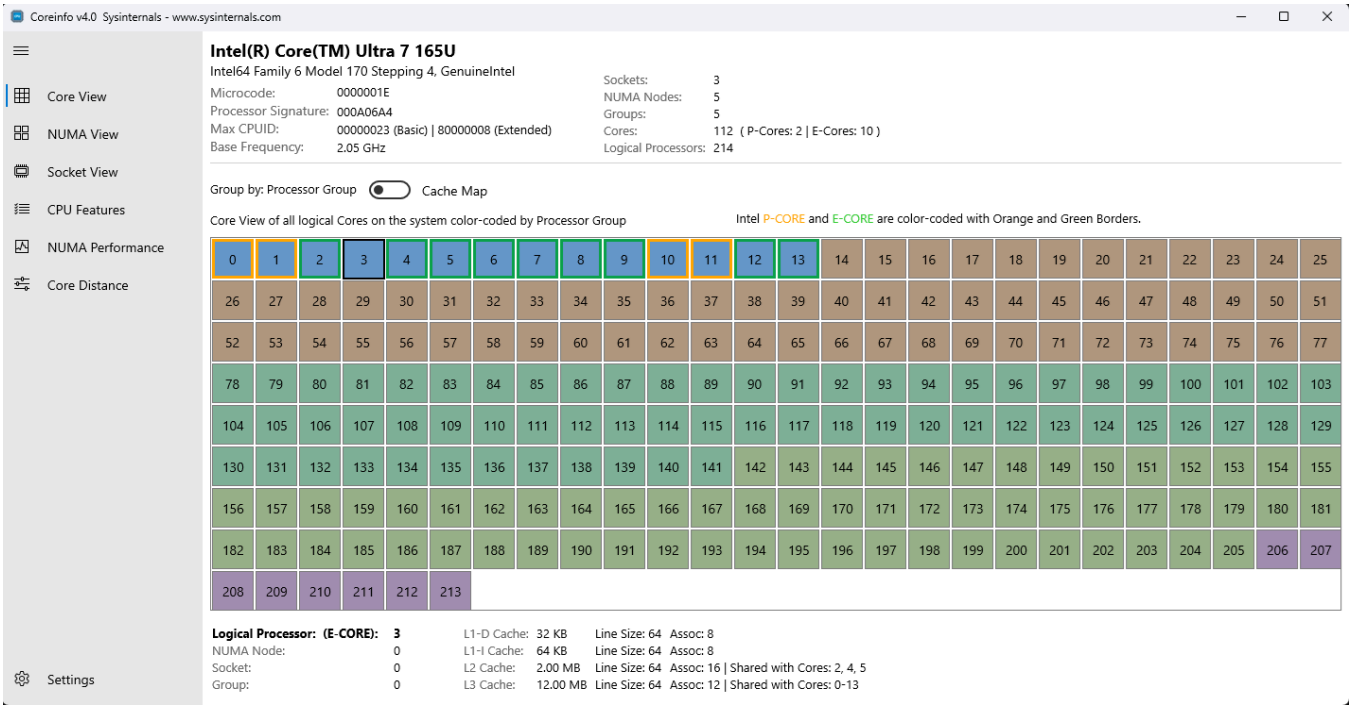
功能：

- **网格布局**：每个单元格表示逻辑处理器
- **核心类型指示器**：
  - P 核心（性能核心）- 颜色独特
  - E-Core （效率核心） - 颜色不同
  - 标准核心 - 默认着色
- **缓存映射切换**：在默认视图和缓存层次结构视图之间进行切换
- **交互式选择**：单击任意核心以查看底部窗格中的详细信息

显示的信息：

- 逻辑处理器编号
- 核心类型（如果适用为 P-Core/E-Core）
- 关联的缓存级别（L1、L2、L3）
- NUMA 节点分配
- 套接字分配

- 组分配



核心视图以网格布局显示逻辑处理器

详细信息窗格（选择核心组件时）：

- 处理器掩码和相关性
- 缓存层次结构（数据缓存、指令缓存、统一缓存）
- 缓存大小和关联性
- 缓存行大小

---

2. NUMA 视图

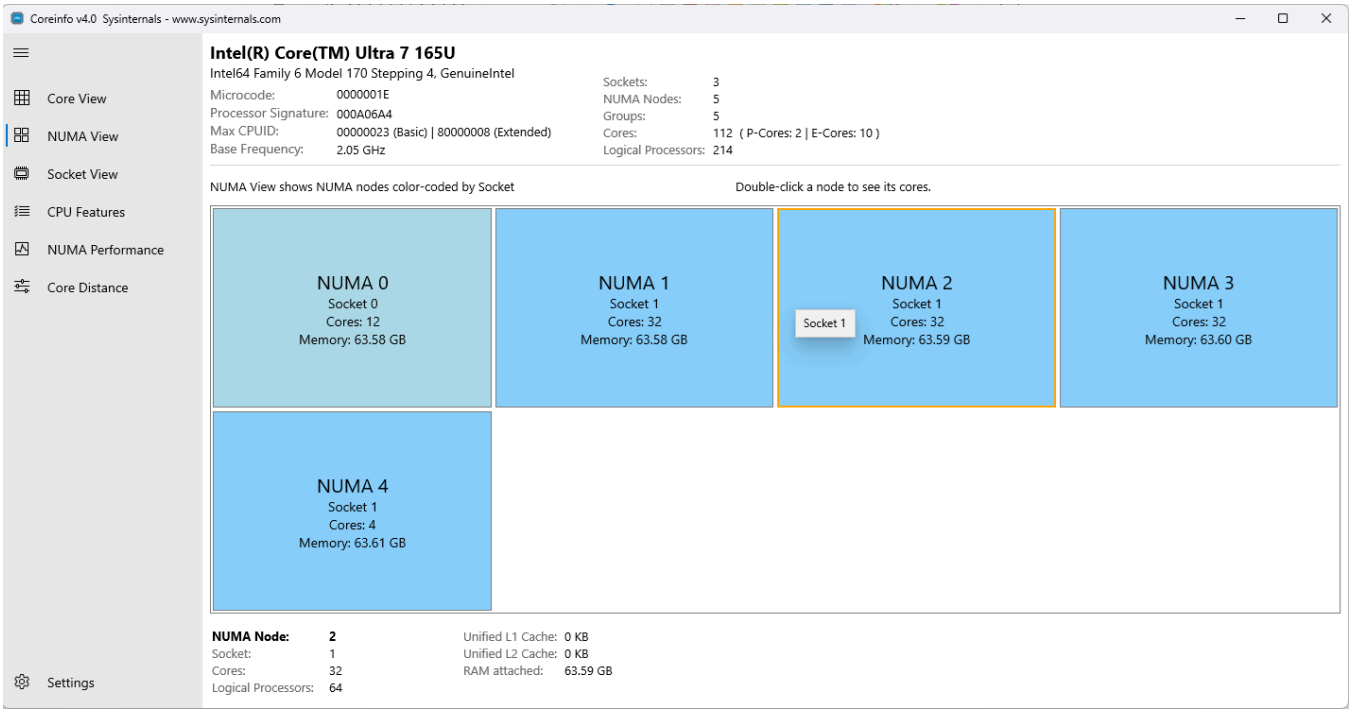
NUMA（非统一内存访问）视图按其 NUMA 节点分配组织核心，使得内存局部性和访问模式更易于理解。

功能：

- **基于节点的架构**：按 NUMA 节点分组的核心
- **物理与逻辑核心**：显示每个节点的两个计数
- **内存信息**：显示每个 NUMA 节点的可用内存
- **交互式导航**：
  - 单击 NUMA 节点，在底部详细信息窗格中显示其详细信息
  - 双击 NUMA 节点，导航到"核心视图"，显示所选 NUMA 节点中的所有核心
- **分层显示**：显示 NUMA 节点与核心之间的关系

显示的信息：

- NUMA 节点数
- 每个 NUMA 节点的核心数（物理核心和逻辑核心）
- 每个节点的内存容量
- 跨节点的核心分布
- 效率核心计数（如果适用）



NUMA 视图，显示了按照 NUMA 节点组织的核心

用例：

- 优化内存访问模式
- 理解 NUMA 识别应用程序的性能
- 规划线程/进程放置以实现最佳性能

---

3. 套接字视图

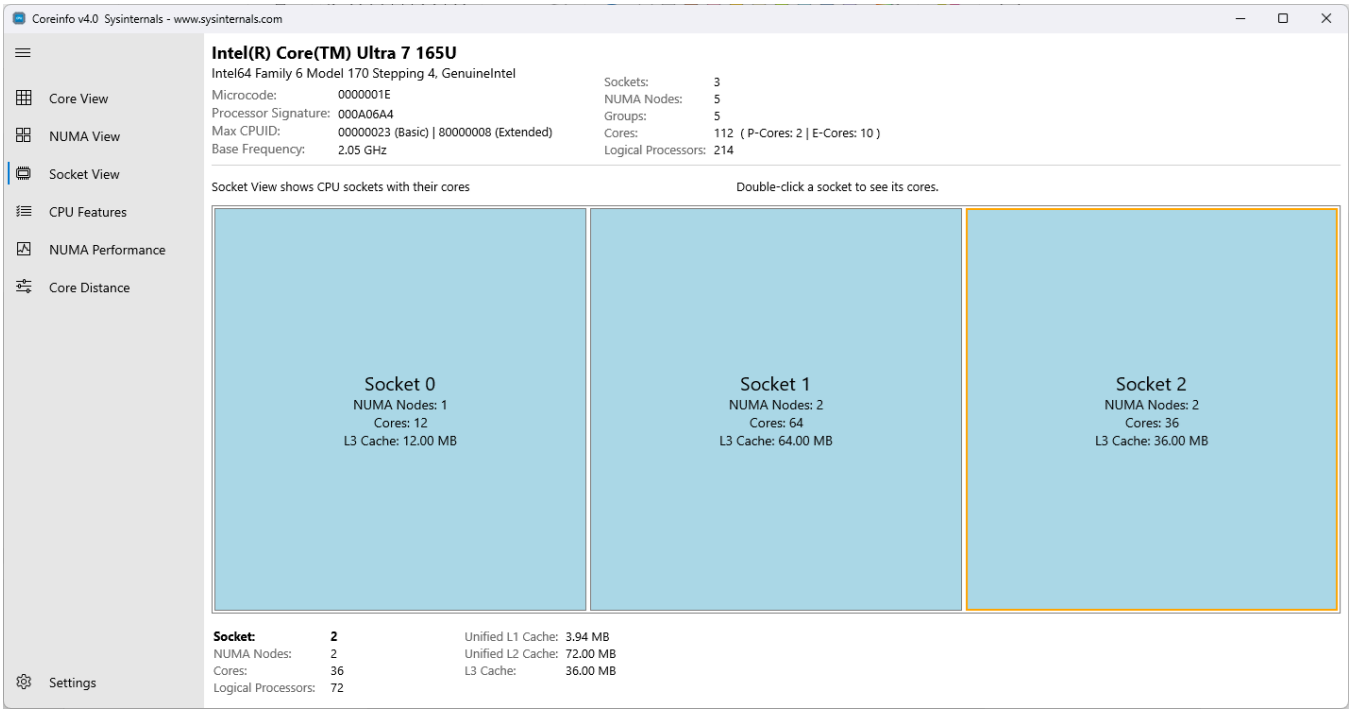
套接字视图显示按物理 CPU 插槽组织的处理器核心，有助于了解多插槽系统和插槽级资源分布。

功能：

- 基于物理插槽的分组：按物理插槽组织的内核
- **套接字信息**：套接字计数和核心分发
- **交互式导航**：
  - 单击套接字，在底部详细信息窗格中显示其详细信息
  - 双击套接字以导航到“核心视图”，显示所选套接字中的所有核心
- **缓存共享**：可视化哪些核心共享套接字级缓存

显示的信息：

- 物理连接器数量
- 套接字上的核心数（包括物理核心和逻辑核心）
- 套接字级缓存信息
- 每个套接字的 NUMA 节点数



套接字视图显示核心按 CPU 套接字进行组织

用例：

- 多路 CPU 插槽系统分析
- 了解跨套接字通信成本
- 在多个插槽服务器中规划工作负载分配

---

4. CPU 功能视图

CPU 功能视图显示 CPU 支持的处理器功能、指令集扩展和硬件功能的综合列表。

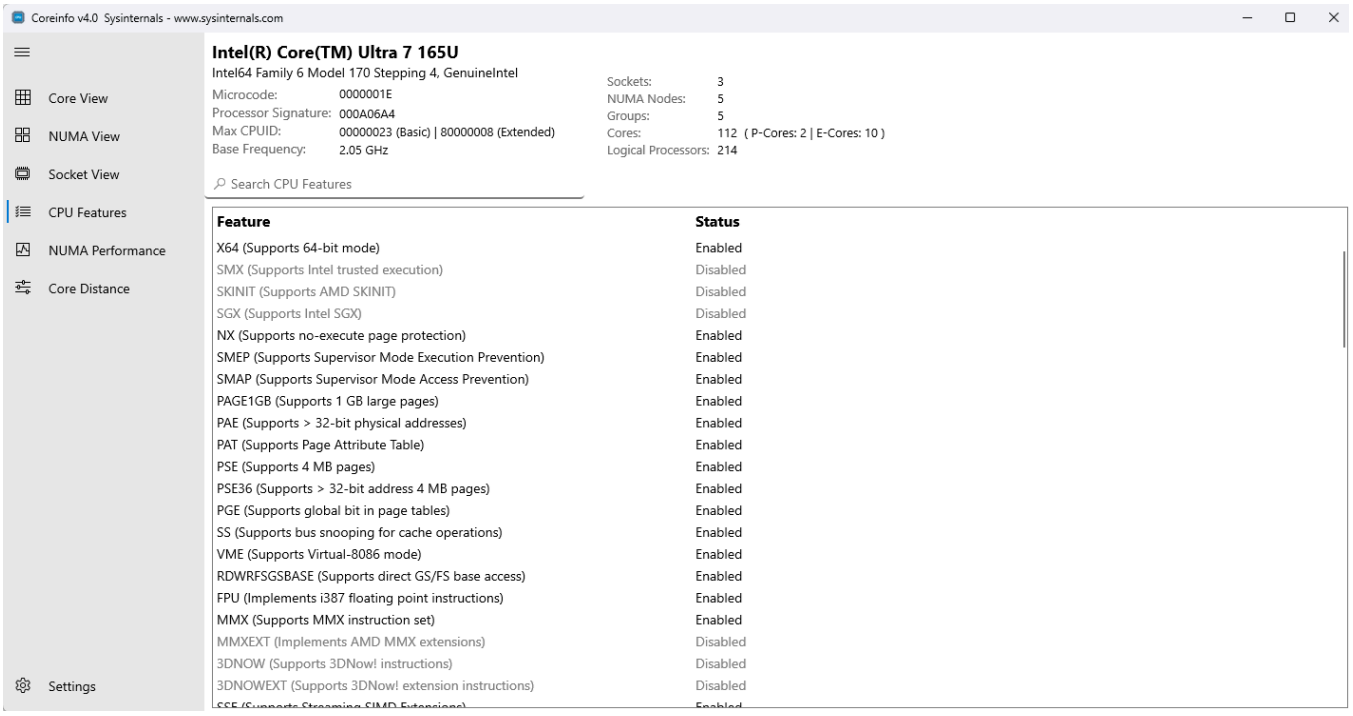
功能：

- **可搜索列表**：使用搜索栏快速查找特定 CPU 功能
- **状态指示器**：通过颜色标识清晰地指示受支持与不支持的功能
  - 支持的功能以普通颜色显示
  - 不支持或禁用的功能会灰色显示
- **功能类别**：
  - 虚拟化（VMX、SVM、虚拟机监控程序）
  - 64 位支持 （EM64T， NX）

- 指令集（SSE、AVX、AES 等）
- 电源管理（EIST、ACPI、热）
- 安全功能（SMX、SKINIT）
- 内存功能（PAE、PAT、PSE）
- 调试和监视功能

显示的信息：

- 功能缩写
- 功能状态（支持/不支持）
- 完整功能说明（详细信息窗格中）



CPU 特性视图，显示处理器功能列表

注意： 某些虚拟化功能（如 VMX、SVM）在运行虚拟机监控程序活动时或从虚拟机内部运行时，可能会错误地报告为不可用。 Coreinfo 必须在没有运行管理程序的系统上执行，才能获得准确的结果。

用例：

- 在部署应用程序之前验证指令集可用性
- 检查虚拟化支持
- 了解处理器生成和功能
- 调试由于缺少 CPU 功能而导致的性能问题

---

5. NUMA 性能视图

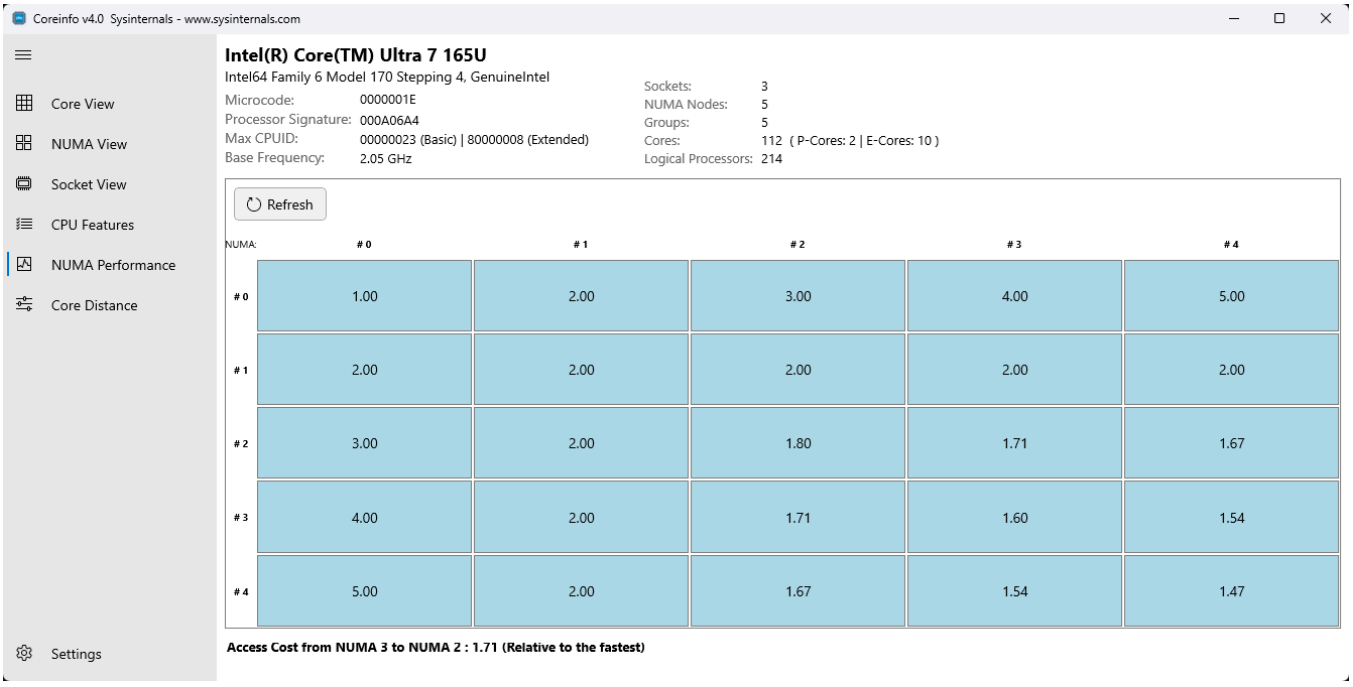
NUMA 性能视图提供网格可视化效果，显示 NUMA 节点之间的内存访问成本，帮助识别 NUMA 系统中的性能瓶颈。

功能：

- **网格可视化**：显示 NUMA 节点之间的相对内存访问成本的矩阵
- **交互式矩阵**：将鼠标悬停在单元格上以查看详细的性能信息
- **Real-Time 更新**：通过选择“刷新”按钮动态更新性能数据
- **相对成本显示**：显示从不同 NUMA 节点访问内存的相对成本

显示的信息：

- NxN 矩阵，其中 N = NUMA 节点数
- 从源 NUMA 节点（行）到目标 NUMA 节点（列）的内存访问成本
- 显示相对性能成本的数字值
- 对角单元格显示本地内存访问（通常成本最低）



NUMA 性能网格，显示内存访问成本

了解网格：

- **对角元素**：表示本地内存访问（节点访问自己的内存） - 通常是最低值
- **对角线元素**：表示具有较高相对成本的远程内存访问
- **对称性**：矩阵可能不是完全对称的，因为访问成本可能因方向而异

用例：

- 识别与 NUMA 相关的性能瓶颈
- 优化内存分配策略
- 为 NUMA 系统规划进程/线程固定

- 了解跨节点内存访问处罚

---

6. 核心距离视图

核心距离视图显示单个 CPU 核心之间的通信成本的详细热度图，提供有关核心到核心延迟和通信效率的见解。

功能：

- Core-Level **热度地图**：彩色编码矩阵，显示核心之间的相对距离
  - 绿色/蓝色 = 低延迟（同一核心群集，共享缓存）
  - 黄色/橙色 = 中等延迟（同一插槽，不同集群）
  - 红色 = 高延迟（不同的套接字或 NUMA 节点）
- **交互式浏览**：将鼠标悬停在网格画布上以查看详细的距离信息
- **精细分析**：以最佳粒度显示核心到核心关系
- **动态刷新**：使用"刷新"按钮动态获取更新的核心距离数据

显示的信息：

- NxN 矩阵，其中 N = 逻辑处理器数
- 从源核心（行）到目标核心的相对距离/延迟（列）
- 用于快速识别核心关系的颜色编码
- 详细信息窗格中的详细距离指标

核心距离热度地图，显示核心到核心通信成本

了解距离图：

- **对角元素**：始终为零（自身核心）

- **低距离（绿色）**：核心共享 L2 或 L3 缓存
- **中等距离（黄色）**：同一套接字上的核心，但在不同的缓存域
- **高距离（红色）**：位于不同套接字或 NUMA 节点上的核心

用例：

- 线程相关性优化
- 了解缓存一致性域
- 确定用于通信线程的最佳核心对
- 分析多线程应用程序性能
- 设计低延迟应用程序的 CPU 固定策略

交互式功能

核心选择和详细信息

在任意视图（核心视图、NUMA 视图或套接字视图）中单击一个核心会在底部的详细信息窗格中显示相关详细信息：

- **处理器信息**：逻辑处理器编号、掩码和相关性
- **缓存层次结构**：
  - L1 数据缓存（大小、关联性、行大小）
  - L1 指令缓存（大小、关联性、行大小）
  - L2 缓存（大小、关联性、行大小）
  - L3 缓存（大小、关联性、行大小）
- **拓扑信息**：NUMA 节点、套接字和组分配
- **核心类型**：P-Core、E-Core 或标准核心指定

搜索功能

CPU 功能视图包括一个搜索栏，可用于快速查找特定处理器功能：

1. 单击搜索图标
2. 键入功能名称或缩写
3. 列表自动筛选以显示匹配功能
4. 清除搜索以还原完整列表

缓存映射切换

在核心视图中，在两种可视化模式之间切换：

- **默认模式**：按逻辑排列显示核心
- **缓存映射模式**：重新组织核心以可视化缓存共享关系

视图之间的导航

- 使用左侧导航窗格在视图之间切换
- 查看特定 NUMA 节点或套接字时，再次单击同一视图将返回到整体视图
- 导航窗格中突出显示了当前视图

设置和自定义

通过导航菜单中的“设置”选项访问设置。

外观设置

主题选项：

- **浅**色：针对明亮环境优化的浅色方案
- **深**色：深色方案以减少眼睛紧张
- **系统默认值**：自动匹配 Windows 主题首选项

保存到文件

导出核心拓扑数据：

- 使用 “**保存到**” 选项将核心拓扑数据转储到文件
- 输出格式与命令行工具输出相同

了解系统拓扑

核心类型（混合体系结构）

新式 CPU 可能具有具有不同核心类型的混合体系结构：

- **P 核心（性能）**：针对单线程工作负载和要求苛刻的工作负荷优化的高性能核心
- **E-Cores （效率）**：针对后台任务和多线程工作负荷优化的节能核心

Coreinfo UI 可清楚地识别和区分所有适用视图中的这些核心类型。

NUMA 体系结构

什么是 NUMA? 非统一内存访问（NUMA）是一种内存设计，其中每个处理器都有可快速访问的本地内存，以及需要处理器间通信的远程内存。

为什么它很重要：

- 本地内存访问明显快于远程访问
- 应用程序性能可能会受到 NUMA 布局的影响
- 了解 NUMA 拓扑对于高性能计算至关重要

使用 Coreinfo UI 进行 NUMA 优化：

1. 使用 **NUMA 视图** 了解系统的 NUMA 拓扑
2. 查看 **NUMA 性能视图** 以查看内存访问成本
3. 根据 NUMA 节点分配优化线程/进程放置
4. 使用 **核心距离视图** 了解 NUMA 节点内部和跨 NUMA 节点之间的核心到核心通信

缓存层次结构

缓存级别：

- **L1 缓存**：最小和最快，拆分为数据和指令缓存
- **L2 缓存**：较大的统一缓存，通常专用于每个核心
- **L3 缓存**：最大的统一缓存，通常在多个核心之间共享

使用缓存信息：

- 了解哪些核心共享缓存资源
- 优化缓存共享核心的数据本地性
- 在核心视图中使用缓存映射模式可视化缓存域

从命令行使用 Coreinfo

对于每个资源，它显示对应于指定资源的 OS 可见处理器的映射，其中“*”表示适用的处理器。例如，在 4 核系统上，缓存输出中的一行包含核心 3 和 4 共享的映射。

用法：

Windows 命令提示符

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

展开表

参数	说明
-c	有关核心的转储信息。
-f	转储核心功能信息。
-g	有关组的转储信息。
-l	有关缓存的转储信息。
-n	有关 NUMA 节点的转储信息。
-s	有关套接字的转储信息。
-m	转储 NUMA 访问成本。
-v	仅转储与虚拟化相关的功能，包括对二级地址转换的支持。 （需要 Intel 系统的管理权限）。

默认情况下，除`-v`之外，其他选项均处于选中状态。

Coreinfo 输出：

txt

```
Coreinfo v4.0 - Dump information on system CPU and memory topology
Copyright © 2008-2025 Mark Russinovich
Sysinternals - www.sysinternals.com

Intel(R) Core(TM) Ultra 7 165U
Intel64 Family 6 Model 170 Stepping 4, GenuineIntel

Microcode signature: 0000001E
Processor signature: 000A06A4

Maximum implemented CPUID leaves: 00000023 (Basic), 80000008 (Extended).
Maximum implemented address width: 48 bits (virtual), 46 bits (physical).

HTT             *       Hyperthreading enabled
CET             *       Supports Control Flow Enforcement Technology
Kernel CET      -       Kernel-mode CET Enabled
User CET        *       User-mode CET Allowed

X64             *       Supports 64-bit mode
SMX             -       Supports Intel trusted execution
SKINIT          -       Supports AMD SKINIT
SGX             -       Supports Intel SGX
NX              *       Supports no-execute page protection
SMEP            *       Supports Supervisor Mode Execution Prevention
SMAP            *       Supports Supervisor Mode Access Prevention
PAGE1GB         *       Supports 1 GB large pages
PAE             *       Supports > 32-bit physical addresses
```

```
PAT             *       Supports Page Attribute Table
PSE             *       Supports 4 MB pages
PSE36           *       Supports > 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
RDWRFSGSBASE    *       Supports direct GS/FS base access
FPU             *       Implements i387 floating point 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
SSE4a           -       Supports Streaming SIMDR Extensions 4a
SSE4.1          *       Supports Streaming SIMD Extensions 4.1
SSE4.2          *       Supports Streaming SIMD Extensions 4.2
AES             *       Supports AES extensions
AVX             *       Supports AVX instruction extensions
AVX2            *       Supports AVX2 instruction extensions
AVX-512-F       -       Supports AVX-512 Foundation instructions
AVX-512-DQ      -       Supports AVX-512 double and quadword instructions
AVX-512-IFAMA   -       Supports AVX-512 integer Fused multiply-add instructions
AVX-512-PF      -       Supports AVX-512 prefetch instructions
AVX-512-ER      -       Supports AVX-512 exponential and reciprocal instructions
AVX-512-CD      -       Supports AVX-512 conflict detection instructions
AVX-512-BW      -       Supports AVX-512 byte and word instructions
AVX-512-VL      -       Supports AVX-512 vector length instructions
FMA             *       Supports FMA extensions using YMM state
MSR             *       Implements RDMSR/WRMSR instructions
MTRR            *       Supports Memory Type Range Registers
XSAVE           *       Supports XSAVE/XRSTOR instructions
OSXSAVE         *       Supports XSETBV/XGETBV instructions
RDRAND          *       Supports RDRAND instruction
RDSEED          *       Supports RDSEED instruction
CMOV            *       Supports CMOVcc instruction
CLFSH           *       Supports CLFLUSH instruction
CX8             *       Supports compare and exchange 8-byte instructions
CX16            *       Supports CMPXCHG16B instruction
BMI1            *       Supports bit manipulation extensions 1
BMI2            *       Supports bit manipulation extensions 2
ADX             *       Supports ADCX/ADOX instructions
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
ERMSB           *       Supports Enhanced REP MOVSB/STOSB
PCLMULDQ        *       Supports PCLMULDQ instruction
POPCNT          *       Supports POPCNT instruction
LZCNT           *       Supports LZCNT instruction
SEP             *       Supports fast system call instructions
```

```
LAHF-SAHF       *       Supports LAHF/SAHF instructions in 64-bit mode
HLE             -       Supports Hardware Lock Elision instructions
RTM             -       Supports Restricted Transactional Memory 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
INVPCID         *       Supports INVPCID instruction
PDCM            *       Supports Performance Capabilities MSR
RDTSCP          *       Supports RDTSCP instruction
TSC             *       Supports RDTSC instruction
TSC-DEADLINE    *       Local APIC supports one-shot deadline timer
TSC-INVARIANT   *       TSC runs at constant rate
xTPR            *       Supports disabling task priority messages
EIST            *       Supports Enhanced Intel Speedstep
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
HTT             *       Hyperthreading
PREFETCHW       *       PrefetchW instruction support
HYPERVISOR      *       Hypervisor is present
VMX             -       Supports Intel hardware-assisted virtualization
EPT             -       Supports Intel extended page tables (SLAT)
URG             -       Supports Intel unrestricted guest

Logical to Physical Processor Map:
**----------  Physical Processor 0 (Hyperthreaded)
--*----------  Physical Processor 1
---*----------  Physical Processor 2
----*---------  Physical Processor 3
-----*--------  Physical Processor 4
------*-------  Physical Processor 5
-------*------  Physical Processor 6
--------*-----  Physical Processor 7
---------*----  Physical Processor 8
----------**--  Physical Processor 9 (Hyperthreaded)
------------*-  Physical Processor 10
-------------*  Physical Processor 11

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

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

No NUMA nodes.
```

```
Logical Processor to Cache Map:
**------------  Data Cache          0, Level 1,   48 KB, Assoc  12, LineSize  64
**------------  Instruction Cache   0, Level 1,   64 KB, Assoc  16, LineSize  64
**------------  Unified Cache       0, Level 2,    2 MB, Assoc  16, LineSize  64
**********----  Unified Cache       1, Level 3,   12 MB, Assoc  12, LineSize  64
--*-----------  Data Cache          1, Level 1,   32 KB, Assoc   8, LineSize  64
--*-----------  Instruction Cache   1, Level 1,   64 KB, Assoc   8, LineSize  64
--****--------  Unified Cache       2, Level 2,    2 MB, Assoc  16, LineSize  64
---*----------  Data Cache          2, Level 1,   32 KB, Assoc   8, LineSize  64
---*----------  Instruction Cache   2, Level 1,   64 KB, Assoc   8, LineSize  64
----*---------  Data Cache          3, Level 1,   32 KB, Assoc   8, LineSize  64
----*---------  Instruction Cache   3, Level 1,   64 KB, Assoc   8, LineSize  64
-----*--------  Data Cache          4, Level 1,   32 KB, Assoc   8, LineSize  64
-----*--------  Instruction Cache   4, Level 1,   64 KB, Assoc   8, LineSize  64
------*-------  Data Cache          5, Level 1,   32 KB, Assoc   8, LineSize  64
------*-------  Instruction Cache   5, Level 1,   64 KB, Assoc   8, LineSize  64
------****----  Unified Cache       3, Level 2,    2 MB, Assoc  16, LineSize  64
-------*------  Data Cache          6, Level 1,   32 KB, Assoc   8, LineSize  64
-------*------  Instruction Cache   6, Level 1,   64 KB, Assoc   8, LineSize  64
--------*-----  Data Cache          7, Level 1,   32 KB, Assoc   8, LineSize  64
--------*-----  Instruction Cache   7, Level 1,   64 KB, Assoc   8, LineSize  64
---------*----  Data Cache          8, Level 1,   32 KB, Assoc   8, LineSize  64
---------*----  Instruction Cache   8, Level 1,   64 KB, Assoc   8, LineSize  64
----------**--  Data Cache          9, Level 1,   48 KB, Assoc  12, LineSize  64
----------**--  Instruction Cache   9, Level 1,   64 KB, Assoc  16, LineSize  64
----------**--  Unified Cache       4, Level 2,    2 MB, Assoc  16, LineSize  64
------------*-  Data Cache         10, Level 1,   32 KB, Assoc   8, LineSize  64
------------*-  Instruction Cache  10, Level 1,   64 KB, Assoc   8, LineSize  64
------------**  Unified Cache       5, Level 2,    2 MB, Assoc  16, LineSize  64
-------------*  Data Cache         11, Level 1,   32 KB, Assoc   8, LineSize  64
-------------*  Instruction Cache  11, Level 1,   64 KB, Assoc   8, LineSize  64

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

 Sysinternals Live下载下载 Coreinfo （3 MB）立即运行。

运行于：

- 客户端：Windows 11 及更高版本。
- 服务器：Windows Server 2016 及更高版本。

Last updated on 2025/12/17

LiveKd v5.63

项目 • 2023/08/03

作者：Mark Russinovich 和 Ken Johnson

发布日期：2020 年 4 月 28 日

 **下载 LiveKd (700 KB)**

简介

LiveKD 是我为《*Inside Windows 2000，第 3 版*》随附 CD 编写的实用工具，现已免费提供。 使用 *LiveKD*，可以在实时系统上本地运行 Kd 和 Windbg Microsoft 内核调试程序，它们是 Windows 调试工具包的一部分。 执行处理故障转储文件的所有调试程序命令，以深入查看系统内部情况。 有关如何使用内核调试程序浏览系统的信息，请参阅 Windows 调试工具文档和我们的书籍。

虽然最新版本的 Windbg 和 Kd 在 Windows Vista 和 Server 2008 上具有类似的功能，但与 Windbg 和 Kd 自有的实时内核调试功能相比，LiveKD 实现的功能更多，例如使用 !thread 命令查看线程堆栈。

安装

首先从 Microsoft 网站下载并安装 Windows 调试工具包：

https://msdn.microsoft.com/library/windows/hardware/ff551063(v=vs.85).aspx

如果将工具安装到其默认目录 \Program Files\Microsoft\Debugging Tools for Windows，则可以从任何目录运行 *LiveKD*；否则，应将 LiveKD 复制到安装工具的目录。

如果还没有为运行 *LiveKD* 的系统安装符号，*LiveKD* 将询问你是否希望它自动配置系统以使用 Microsoft 的符号服务器（有关符号文件和 Microsoft 符号服务器的信息，请参阅 Windows 调试工具文档）。

注意： Microsoft 调试程序会报错，标识找不到 LIVEKDD.SYS 的符号。 这是意料之中的，因为我没有为 LIVEKDD.SYS 提供符号，并且它不会影响调试程序的行为。

使用 LiveKd

用法：

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]

参数	说明
-hv	指定要调试的 Hyper-V VM 的名称或 GUID。
-hvd	包含虚拟机监控程序页（仅限 Windows 8.1 及更高版本）。
-hvl	列出正在运行的 Hyper-V VM 的名称和 GUID。
-k	指定要执行的调试程序映像的完整路径和文件名
-m	创建镜像转储，这是内核内存的一致视图。 只有内核模式内存可用，并且此选项可能需要大量的可用物理内存。 可以选择提供用于指定要包含哪个区域的标志掩码（提取自下表，默认为 0x18F8）： 0001 - 处理专用，0002 - 映射文件， 0004 - 共享部分，0008 - 页表页， 0010 - 分页池，0020 - 非分页池， 0040 - 系统 PTE，0080 - 会话页， 0100 - 元数据文件，0200 - AWE 用户页， 0400 - 驱动程序页，0800 - 内核堆栈， 1000 - WS 元数据，2000 - 大页面 默认值可捕获大多数内核内存内容，建议使用。 此选项可与 -o 一起使用，以更快地保存一致的转储。 镜像转储需要 Windows Vista 或 Windows Server 2008 或更高版本。 Sysinternals RamMap 提供了可选择以包含的可用内存区域分布的图形摘要。
-ml	使用本机支持生成实时转储（仅限 Windows 8.1 及更高版本）。
-mp	指定单个进程，其用户模式内存内容应包含在镜像转储中。 仅对 -m 选项有效。
-o	将 memory.dmp 保存到磁盘，而不是启动调试程序。
-p	在 LiveKd 处于活动状态时暂停目标 Hyper-V VM（议与 -o 一起使用）。 指定要调试的 Hyper-V VM 的名称或 GUID。
-hvl	列出正在运行的 Hyper-V VM 的名称和 GUID。
-vsym	显示有关符号加载操作的详细调试信息。
-w	运行 windbg 而不是 kd

所有其他选项将直通传递到调试程序。

注意：如果调试程序挂起，请使用 Ctrl-Break 终止并重启调试程序。

默认情况下，LiveKd 会运行 kd.exe。

 **下载 LiveKd** **(700 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

LoadOrder v1.02

项目 • 2023/08/03

作者：Mark Russinovich

发布时间：2021 年 10 月 12 日

 **下载 LoadOrder** (1.1 MB)
立即从 Sysinternals Live 运行。

简介

这个小程序显示了 Windows NT 或 Windows 2000 系统加载设备驱动程序的顺序。 请注意，在 Windows 2000 上，即插即用驱动程序的加载顺序实际上可能与计算的顺序不同，因为在设备检测和枚举期间，即插即用驱动程序是按需加载的。

 **下载 LoadOrder** (1.1 MB)

立即从 Sysinternals Live 运行。

运行软件：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

ProcFeatures v1.1

项目 • 2023/08/03

作者：Mark Russinovich

发布时间：2006 年 11 月 1 日
停用时间：2011 年 9 月 1 日

> **ⓘ 重要**
>
> ProcFeatures 已停用，因为对 **Coreinfo** 的最新添加使此实用工具过时。 Coreinfo v3 现在显示系统处理器支持的处理器功能。

PsInfo v1.79

项目 • 2024/02/08

作者：Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools (5 MB)**

介绍

PsInfo 是一个命令行工具，它可用于收集有关本地或远程 Windows NT/2000 系统的关键信息，包括安装类型、内核版本、已注册的组织和所有者、处理器数量及其类型、物理内存量、系统的安装日期以及到期日期（如果为试用版）。

安装

只需将 *PsInfo* 复制到你的可执行文件路径，然后键入“psinfo”。

使用 PsInfo

默认情况下，*PsInfo* 会显示本地系统的信息。 指定远程计算机名称以从远程系统获取信息。 由于 *PsInfo* 依赖于远程注册表访问来获取其数据，因此远程系统必须运行远程注册表服务，并且运行 *PsInfo* 的帐户必须有权访问远程注册表的 HKLM\System 部分。

为了帮助自动更新 Service Pack，*PsInfo* 会返回系统的 Service Pack 数的值（例如 0 表示无 Service Pack，1 表示 SP 1 等）。

用法: psinfo [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]

展开表

参数	说明
\\computer	在指定的远程计算机上执行命令。 如果省略计算机名称，则命令在本地系统上运行，如果指定通配符 (*)，则命令将在当前域中的所有计算机上运行。
@file	在指定的文本文件中列出的每台计算机上运行命令。
-u	指定登录远程计算机的可选用户名。

参数	说明
-p	指定用户名的可选密码。 如果省略此内容，系统将提示你输入隐藏密码。
-h	显示已安装的修补程序的列表。
-s	显示已安装的应用程序的列表。
-d	显示磁盘卷信息。
-c	以 CSV 格式打印。
-t	-c 选项的默认分隔符为逗号，但可以使用指定的字符替代。
filter	Psinfo 将仅显示与筛选器匹配的字段的数据。 例如，“psinfo service”仅列出 service pack 字段。

示例输出

Shell

```
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
```

工作方式

PsInfo 使用远程注册表 API 从系统的注册表读取系统信息，并使用 WMI 来确定是否已激活 Windows XP 安装。

 **下载 PsTools** (5 MB)

PsTools

PsInfo 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

RAMMap v1.63

作者：Mark Russinovich

发布时间： 2026 年 3 月 26 日

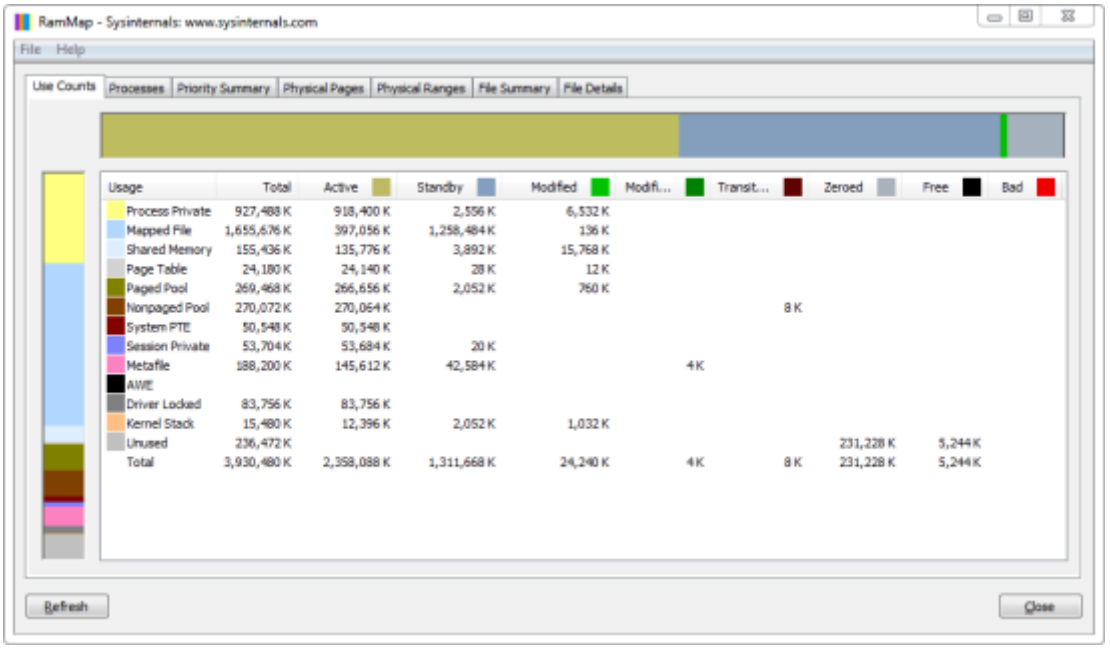
RAMMap **(719 KB)**
立即从 **Sysinternals Live** 运行。

你是否曾想知道 Windows 究竟是如何分配物理内存的，在 RAM 中缓存了多少文件数据，或者内核和设备驱动程序使用了多少 RAM？ RAMMap 让回答这些问题变得轻而易举。 RAMMap 是适用于 Windows Vista 及更高版本的高级物理内存使用情况分析实用工具。 它在几个不同的选项卡上以不同方式显示使用情况信息：

- 使用计数：按类型和分页列表列出的使用情况摘要
- 进程：进程工作集大小
- 优先级摘要：确定备用列表大小优先级
- 物理页：所有物理内存的每页使用量
- 物理范围：物理内存地址
- 文件摘要：RAM 中的文件数据（按文件显示）
- 文件详细信息：每个文件中的各个物理页

使用 RAMMap 了解 Windows 管理内存的方式、分析应用程序内存使用情况，或回答有关 RAM 分配方式的特定问题。 使用 RAMMap 的刷新功能可以更新显示，并且支持保存和加载内存快照。

有关 RAMMap 使用的标签的定义，以及了解 Windows 内存管理器使用的物理内存分配算法，请参阅 Windows 内部版，第 5 版。



相关链接

- **Windows 内部机制解析**：Mark Russinovich 和 David Solomon 所著 Windows 内部机制解析书籍的官方更新和勘误页面。
- **Windows Sysinternals 管理员参考**：Mark Russinovich 和 Aaron Margosis 提供的 Sysinternals 实用工具的官方指南，包括所有工具的说明、其功能的说明、如何使用它们进行故障排除，以及示例实际使用案例。

 RAMMap **(719 KB)**

立即从 **Sysinternals Live** 运行。

运行于：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

了解更多

- Defrag Tools：6 - RAMMap
  在本集 Defrag Tools 中，Andrew Richards 和 Larry Larsen 介绍了如何使用 RAMMap 来查看 RAM 的使用情况并判断是否存在任何内存压力。

Last updated on 2026/03/26

WinObj v3.14

项目 • 2024/07/25

作者： Mark Russinovich

发布日期：2022 年 1 月 27 日

 **下载 WinObj** **(1.8 MB)**
立即从 Sysinternals Live 运行。

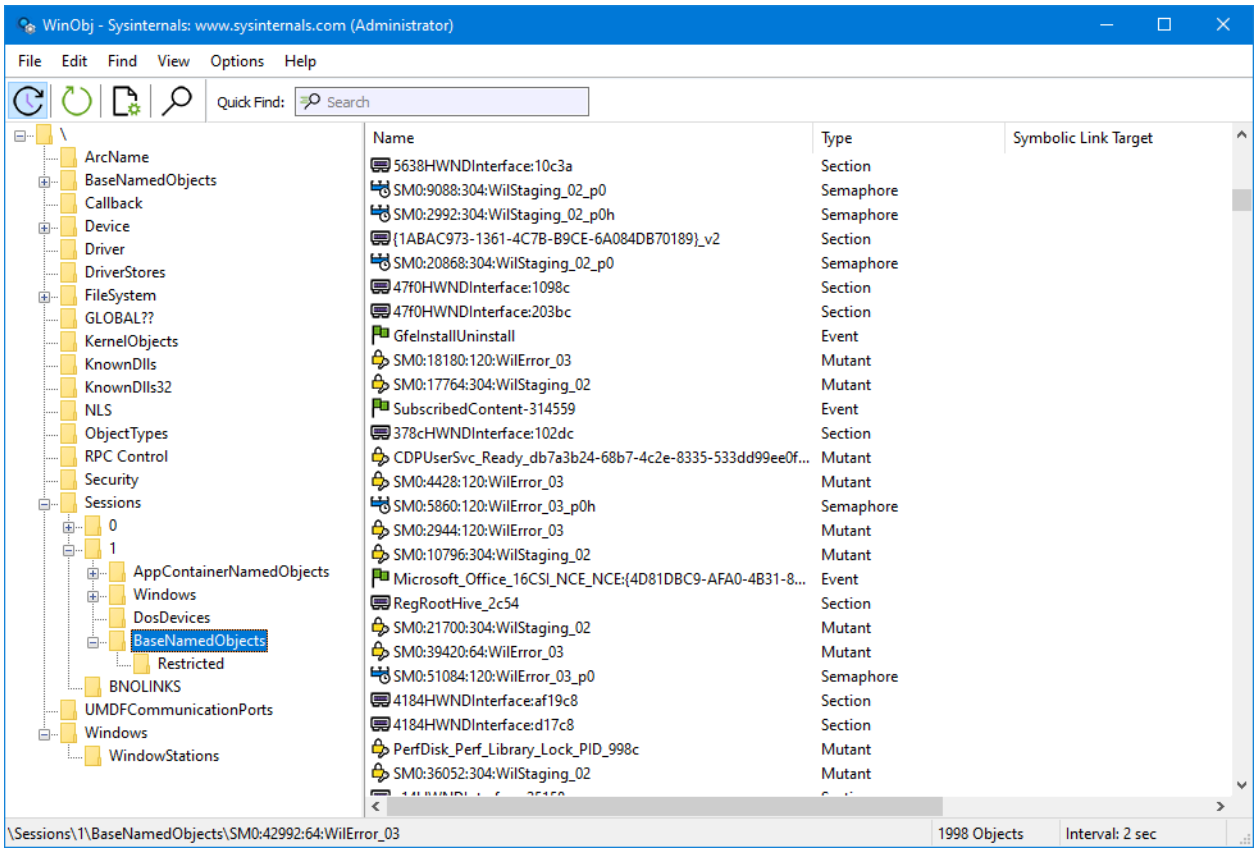
介绍

如果你是关注安全的系统管理员、跟踪对象相关问题的开发人员，或者只是对对象管理器命名空间感到好奇，那么 *WinObj* 是一个必备工具。

WinObj 是一个程序，它使用本机 Windows API（由 NTDLL.DLL 提供）来访问和显示 NT 对象管理器命名空间上的信息。 Winobj 看起来可能类似于同名的 Microsoft SDK 程序，但 SDK 版本存在许多重大 bug，导致无法显示准确信息（例如，其句柄和引用计数信息完全失效）。 此外，我们的 WinObj 还能理解很多其他对象类型。 最后，WinObj 版本 3.0 具有用户界面增强功能（包括深色主题），知道如何打开设备对象，在创建/销毁对象时提供动态更新，并允许搜索和筛选。

安装和使用

WinObj 没有设备驱动程序组件，因此你可以像运行任何 Win32 程序一样运行它。



工作原理

对象管理器负责管理 NT 对象。 作为此职责的一部分，它会维护一个内部命名空间，其中各种操作系统组件、设备驱动程序和 Win32 程序可以存储和查找对象。 本机 NT API 提供的例程允许用户模式程序浏览命名空间并查询位于该处的对象的状态，但这些接口没有提供文档。

更多信息

Helen Custer 的 *Inside Windows NT* 很好地概述了对象管理器命名空间，Mark 的 1997 年 10 月 WindowsITPro 杂志 专栏“Inside the Object Manager”也是（当然）很出色的概述。

下载 WinObj (1.8 MB)
立即从 Sysinternals Live 运行。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

Sysinternals 杂项实用工具

2025/09/18

AD 资源管理器

Active Directory 浏览器是专业的 Active Directory (AD) 查看工具和编辑工具。

AdRestore

在 Server 2003 域中还原被标记为墓碑的 Active Directory 对象。

Autologon

在登录期间绕过密码屏幕。

BgInfo

此完全可配置的程序自动生成桌面背景，其中包括有关系统的重要信息，包括 IP 地址、计算机名称、网络适配器等。

BlueScreen

此屏幕保存程序不仅准确模拟蓝屏，还模拟重启（使用 CHKDSK 完成），并且适用于 Windows Vista、Server 2008 及更高版本。

Ctrl2cap

这是一个内核模式驱动程序，它演示键盘输入筛选在键盘类驱动程序上方，以便将 caps-lock 转换为控制键。 在此级别进行筛选允许在 NT 识别到键之前就对其进行转换和隐藏。 Ctrl2cap 还演示如何使用 NtDisplayString（）将消息打印到初始化蓝屏。

DebugView

Sysinternals 的另一项创新：此程序截获设备驱动程序发出的 DbgPrint 调用以及 Win32 程序发出的 OutputDebugString。 它允许在没有活动调试器的情况下查看和记录本地计算机或 Internet 上的调试会话输出。

桌面

通过此新实用工具，可以创建多达四个虚拟桌面，并使用托盘界面或热键预览每个桌面上的内容，并在它们之间轻松切换。

Hex2dec

将十六进制数转换为十进制，反之亦然。

NotMyFault

Notmyfault 是一个工具，你可以用它使你的 Windows 系统崩溃、挂起，并导致内核内存泄漏。

PsLogList

转储事件日志记录。

PsTools

PsTools 套件包括命令行实用工具，用于列出在本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志等。

RegDelNull

扫描并删除包含由标准注册表编辑工具不可删除的嵌入 null 字符的注册表项。

注册表使用情况（RU）

查看指定注册表项的注册表空间使用情况。

RegJump

跳转到在 Regedit 中指定的注册表路径。

字符串

在二进制图像中搜索 ANSI 和 UNICODE 字符串。

ZoomIt

用于在屏幕上缩放和绘图的演示实用工具。

BgInfo v4.33

项目 • 2025/02/13

作者： Mark Russinovich

发布时间： 2025 年 2 月 13 日

下载 BgInfo (2.2 MB)
立即从 Sysinternals Live 运行。

介绍

你曾多少次进入办公室中的系统，需要单击多个诊断窗口来提醒自己系统配置的重要内容，例如系统的名称、IP 地址或操作系统版本？ 如果你管理多台计算机，可能需要 BGInfo。 它会自动在桌面背景上显示有关 Windows 计算机的相关信息，例如计算机名称、IP 地址、Service Pack 版本等。 你可以编辑任何字段以及字体和背景色，将其放在启动文件夹中，这样每次启动都会运行，甚至可以将其配置为显示在登录屏幕的背景中。

由于 BGInfo 编写新的桌面位图后即退出，因此无需担心它会消耗系统资源或干扰其他应用程序。

Sysinternals BgInfo

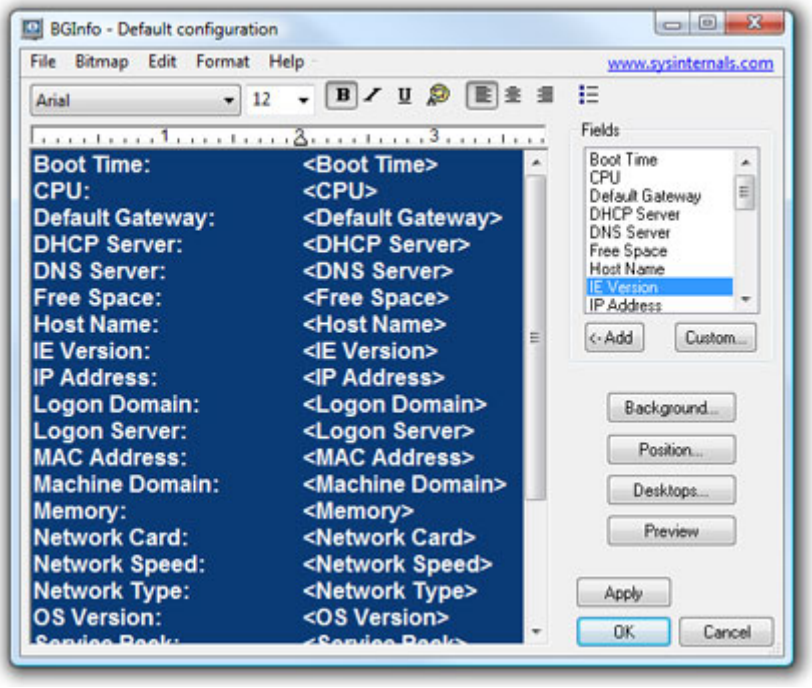
安装和使用

有关使用 BgInfo 的入门信息，请参阅 Mark 在《Windows IT 专业人员杂志》上发表的 *Power Tools* 一文。 如果有疑问或问题，请访问 Sysinternals BgInfo 论坛。

通过将 BGInfo 放入“Startup”文件夹中，可以确保每次启动时显示的系统信息都是最新的。 确定要显示的信息后，请使用命令行选项 /timer:0，在不显示对话框的情况下更新显示。

还可以使用 Windows 计划程序定期运行 BGInfo，以确保长时间运行的系统保持最新状态。

如果创建 BGInfo 配置文件（使用“文件 | 保存设置”菜单项），则可以通过添加 /Ipath 或 /iq<path> 命令行选项，在其他系统上自动导入和使用这些设置。 <>



使用 BgInfo

运行 BGInfo 时，会显示其默认桌面背景的外观和内容。 如果不执行任何操作，它将自动应用这些设置，并在 10 秒倒计时结束后退出。

选择任何按钮或菜单项将禁用计时器，你可以自定义背景信息的布局和内容。

如果你希望 BGInfo 编辑或使用存储在文件中的配置（而不是存储在注册表中的默认配置），请在命令行上指定文件名：

BGInfo MyConfig.bgi

外观按钮

字段：选择在桌面上显示的信息及其显示顺序。 对于网络字段（NIC、IP、MAC 等），系统会为系统上的每个网卡创建单独的条目。 使用“自定义”按钮可添加自己定义的特殊信息。

背景：选择要用于背景的颜色和/或壁纸。 如果选择“复制现有设置”选项，BGInfo 将使用登录用户当前选择的任何信息。 最终用户可以使用此选项个性化设置其桌面，同时仍显示 BGInfo 信息。

位置：选择要将文本放置在屏幕上的位置。 如果某些项很长（例如某些网卡名称），可以使用“行限制”项来换行。 “补偿任务栏位置”复选框用于调整文本的位置，以确保它不被任务栏遮挡。 使用“多监视器配置”按钮可以指定应如何处理附加到单个控制台的多个监视器。

桌面：选择应用配置时更新的桌面。 默认情况下，仅更改“用户桌面”壁纸。 启用“控制台用户登录桌面”选项，可指定在任何人登录系统之前，应在登录桌面上显示壁纸。 在 Windows 95/98/ME 系统上，用户和登录屏幕使用相同的桌面，因此此选项没有任何作用。 启用“终端服务用户登录桌面”选项，可指定应在“终端服务”登录屏幕上显示壁纸。 此选项仅在运行终端服务的服务器上有用。

预览：显示应用于系统时所显示的背景。

配置菜单项

以下选项控制位图的生成方式、位置以及如何导入/导出设置。

文件 | 打开：打开 BGInfo 配置文件。

文件 | 另存为：将当前 BGInfo 配置的副本保存到新文件中。 创建后，你可以让 BGInfo 稍后使用该文件，只需在命令行上指定该文件，或使用“文件 | 打开”菜单项即可。

文件 | 重置默认设置：删除所有配置信息，并将 BGInfo 重置为其默认（安装时）状态。 如果无法确定如何撤消更改，或者 BGInfo 不确定位图的当前状态，请使用此选项。

文件 | 数据库：指定一个 .XLS、.MDB 或 .TXT 文件或到 SQL 数据库的连接字符串，BGInfo 将使用它来存储生成的信息。 使用此文件收集网络上一个或多个系统的历史记录。 必须确保访问该文件的所有系统都安装了相同版本的 MDAC 和 JET 数据库支持。 建议至少使用 MDAC 2.5 和 JET 4.0。 如果指定 XLS 文件，则该文件必须已存在。

如果你希望 BGInfo 更新数据库而不修改用户的壁纸，可以在“桌面”对话框中取消选择所有桌面；BGInfo 仍会更新数据库。

位图 | 256 种颜色：将位图限制为 256 种颜色。 此选项将生成较小的位图。

位图 | 高彩色/真彩色：创建 16 位或 24 位颜色位图。

位图 | 匹配显示器：创建色彩深度与显示器色彩深度匹配的位图。 由于当用户更改显示器的色彩深度时，BGInfo 生成的位图不会更新，因此位图和显示器深度的某些组合可能会出现意外结果（尤其是文本和背景的抖色）。

位图 | 位置：指定要放置输出位图文件的位置。 在终端服务服务器上，位图应放置在每个用户的唯一位置。

编辑 | 插入图像：用于在输出中插入位图图像。 由于 BGInfo 的配置信息存储在注册表中，并且 Windows 会限制注册表值的大小，因此在插入较大的图像时可能会遇到错误。在 Windows 9x/Me 系统上，此限制为 16K，而在 NT/2000/XP 系统上，此限制为 64K。

命令行选项

展开表

参数	说明
<路径>	指定要用于当前会话的配置文件的名称。 按“确定”或“应用”时，会自动将配置更改保存回文件。 如果此参数不存在，BGInfo 将使用当前用户下存储在注册表中的默认配置信息(“HKEY_CURRENT_USER\Software\Winternals\BGInfo”)。
/timer	指定倒计时计时器的超时值（以秒为单位）。 指定零将更新显示，而不显示配置对话框。 指定 300 秒或更长时间将完全禁用计时器。
/popup	使 BGInfo 在不更新桌面的情况下创建一个包含配置信息的弹出窗口。 信息的格式与在桌面上显示时完全相同，但位于适合屏幕大小的窗口中。 使用此选项时，不会更新历史记录数据库。
/Silent	禁止显示错误消息。
/taskbar	使 BGInfo 在不更新桌面的情况下将图标放置在任务栏的状态区域中。 单击该图标会使配置的信息出现在弹出窗口中。 使用此选项时，不会更新历史记录数据库。
/all	指定 BGInfo 应更改当前登录系统的所有用户的壁纸。 此选项在终端服务环境中非常有用，或者计划定期在多人使用的系统上运行 BGInfo 时（请参阅下文的“使用计划”）非常有用。
/log	使 BGInfo 将错误写入指定的日志文件，而不生成警告对话框。 此选项对于跟踪 BGInfo 在计划程序下运行时发生的错误非常有用。
/rtf	使 BGInfo 将其输出文本写入 RTF 文件。 包括所有格式设置信息和颜色。

 **下载 BgInfo**] (2.2 MB)

立即从 Sysinternals Live 运行。

运行平台：

- 客户端：Windows 10 及更高版本。
- 服务器：Windows Server 2016 及更高版本。

BlueScreen 屏幕保护程序 v3.2

项目 • 2023/08/04

作者：Mark Russinovich

发布时间：2006 年 11 月 1 日

下载 Bluescreen (64 KB)

简介

NT 世界最可怕的颜色之一是蓝色。 在 NT 系统中，每当出现严重错误时，就会弹出令人厌恶的蓝屏死机 (BSOD)。 Bluescreen 是一种屏幕保护程序，它不仅可以真实地模拟 BSOD，还可以模拟在系统启动期间看到的启动屏幕。

- 在安装 NT 4.0 的系统中，它还可以模拟磁盘驱动器的 chkdsk 错误！
- 在 Windows 2000、Windows 95 和 Windows 98 上，它显示 Windows 2000 启动初始屏幕，并完成旋转进度条和进度控制更新！
- 在 Windows XP 和 Windows Server 2003 上，它显示 XP/Server 2003 启动初始屏幕及进度栏！

Bluescreen 每隔 15 秒左右在不同的蓝屏和模拟启动之间循环一次。 实际上，Bluescreen 的 BSOD 和系统启动屏幕上显示的所有信息都是从系统配置中获取的，其准确性甚至可以欺骗高级 NT 开发人员。 例如，NT 内部版本号、处理器版本、加载的驱动程序和地址、磁盘驱动器特性以及内存大小都取自运行 Bluescreen 的系统。

使用 Bluescreen 惊艳你的朋友，吓跑你的敌人！

安装和使用

注意：在 Windows 95 或 98 上运行 Bluescreen 之前，必须将 Windows 2000 系统上的 \winnt\system32\ntoskrnl.exe 复制到 \Windows 目录。 如果在 Windows NT/2K 上，只需将 Sysinternals BLUESCRN.SCR 复制到 \system32 目录，如果在 Windows 95 或 98 上，则需复制到 \Windows\System 目录。 右键单击桌面，将弹出“显示设置”对话框，然后选择“屏幕保护”选项卡。使用下拉列表找到“Sysinternals Bluescreen”并将其应用为新的屏幕保护程序。 选择“设置”按钮启用伪磁盘活动，可以更加逼真！

更多信息

如需了解真实蓝屏的产生原因，以及蓝屏上的信息的含义，请参阅我的 1997 年 12 月《Windows ITPro 杂志》 NT Internals 专栏的“Inside the Blue Screen”。

注意：某些病毒扫描程序会将 Bluescreen 屏幕保护程序标记为病毒。 如果你的病毒扫描程序存在这种情况，则可能无法使用此屏幕保护程序。

 下载 Bluescreen (64 KB)

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

CpuStres v2.0

项目 • 2023/08/04

作者：Pavel Yosifovich

发布时间：2018 年 7 月 18 日

 **下载 CpuStres** (2.2 MB)

简介

CpuStres
CpuStres 是实用工具，可以通过在紧密循环中运行多达 64 个线程来模拟 CPU 活动。

每个线程都可以独立启动、暂停或停止，并且可以使用以下参数进行配置：

- **活动级别**：可以是“低”、“中”、“忙”或“最大”，用于控制线程在两个周期之间的休眠时间。 将此值设置为“最大”将导致线程连续运行。
- **优先级**：控制线程优先级。 有关线程优先级的详细信息，请参考 Mark Russinovich 的《Windows 内部书籍》

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2003 及更高版本
- Nano Server：2016 及更高版本

相关链接

- **Windows Internals 书籍**：关于 Windows Internals 的权威性书籍的官方更新和勘误页，由 Mark Russinovich 和 David Solomon 编写。

下载

 **下载 CpuStres** (2.2 MB)
立即从 Sysinternals Live 运行。

Ctrl2Cap v3.0

项目 • 2025/02/22

作者：Mark Russinovich

发布时间： 2025 年 2 月 13 日

 **下载 Ctrl2Cap** **(132 KB)**

简介

Ctrl2Cap 是帮助将 Caps Lock 键重新映射到 Ctrl 的工具。 像我这样从 UNIX 迁移到 NT 的人习惯于将 control 键置于标准电脑键盘上 caps-lock 键的位置，因此这样的实用工具对于我们的编辑工作至关重要。

安装和使用

在解压 Ctrl2Cap 文件的目录中，通过运行命令 `ctrl2cap /install` 来安装 Ctrl2Cap。 要卸载，请输入 `ctrl2cap /uninstall`。

 **下载 Ctrl2Cap** **(132 KB)**

运行平台：

- 客户端：Windows 10 及更高版本。
- 服务器：Windows Server 2016 及更高版本。

DebugView v5.0

作者： Mark Russinovich

发布时间： 2026 年 3 月 26 日

 DebugView (1012 KB)
立即从 Sysinternals Live 运行。

简介

Debugview 是一个应用程序，支持你监视本地系统上或可通过 TCP/IP 访问的网络上任何计算机上的调试输出。 它可以同时显示内核模式和 Win32 调试输出，因此无需调试器来捕获应用程序或设备驱动程序生成的调试输出，也无需修改应用程序或驱动程序以使用非标准调试输出 API。

> ⓘ **注意**
>
> *DebugView* v5.0 需要 Windows 10 版本 1809（内部版本 17763）/Windows Server 2019 或更高版本。

DebugView 进行捕获

DebugView 将捕获：

- Win32 **OutputDebugString**
- 内核模式 **DbgPrint**
- **DbgPrint** 的所有内核模式变体

如果 *DebugView* 在崩溃时正在捕获数据，则还会从 Windows 故障转储文件中提取在崩溃之前生成的内核模式调试输出信息。

DebugView 功能

DebugView 具有一组可用于控制和管理调试输出的强大功能。

版本 5.0 的新增功能：

- **深色模式和新式 UI：** *DebugView* 现在使用 Windows XAML 岛技术提供完全重新设计的界面。 UI 会自动遵循系统范围的浅色或深色主题设置，深色模式一致地应用于标题栏、菜单、工具栏、对话框和输出列表视图。 现代化工具栏和菜单栏提供与其他 Sysinternals 工具（如进程监视器）一致的视觉样式。

- **自动崩溃恢复：** 当 *DebugView* 检测到上一个会话由于未正常关闭（例如系统崩溃）而结束时，它会自动扫描 Windows 故障转储文件，从上一个会话恢复挂起的内核调试跟踪，并在输出窗口中显示它们。 这样就可以对系统故障发生时捕获的内核模式调试输出进行事后分析，而无需任何手动干预。
- **大型捕获的 UI 虚拟化：** 输出列表视图现在使用所有者数据虚拟化，这意味着随时仅呈现可见行。 这样，*DebugView* 就可以有效地处理包含数十万或数百万条调试消息的捕获，而不会占用过多内存或 UI 速度变慢。
- **专用 PID 列：** 默认情况下会显示新的进程 ID 列，以便更轻松地识别生成每个调试输出消息的进程。 可以从“选项”菜单打开或关闭 PID 列。
- **按需 UAC 提升：** *DebugView* 在启动时不再需要管理权限。 仅当启用内核模式捕获或其他需要提升权限的操作时，它才会以标准用户身份启动，并通过 UAC 提示请求提升。
- **DPI 感知呈现：** 在高 DPI 显示器上，菜单图标、工具栏按钮、对话框和输出列表都正确缩放。

版本 4.6 新增功能：

- **支持 Windows Vista 32 位和 64 位**

4.5 版本新增功能：

- **支持日志文件滚动更新：**为了更好地支持长期运行的捕获，DebugView 现在可以每天创建新的日志文件，并且可以选择在执行此操作时清除显示。

版本 4.4 新增功能：

- **支持适用于 x64 的 Windows Server 2003 64 位版本和 Windows XP 64 位版本：** *DebugView* 现在可捕获 64 位版本 Windows 上的内核模式调试输出。
- **时钟时间切换：**现在，可以在时钟时间和已用时间模式之间切换。

版本 4.3 新增功能：

- **支持 Windows XP SP2：** *DebugView* 现在可捕获 Windows XP SP2 上的内核模式调试输出。
- **更多突出显示筛选器：**许多用户要求提供更多突出显示筛选器。
- **日志文件包装：**当达到指定大小限制时，使用新的日志文件选项可将 *DebugView* 包装到日志文件的开头。
- **更大的缓冲区：**更大的 Win32 和内核模式缓冲区会降低删除调试输出的可能性。
- **明文输出字符串：**当 *DebugView* 看到特殊的调试输出字符串“DBGVIEWCLEAR”时，它会清除输出。
- **客户端最小化到托盘：**现在，可以在托盘中运行最小化的客户端。

版本 4.2 新增功能：

- **已修复内核挂钩 bug**：*DebugView* 有时会错误地报告它无法在 Windows XP 和 Server 2003 上挂钩内核模式调试输出。
- **客户端全局捕获选项**：使用新选项，客户端可以在从非控制台会话运行时捕获终端服务器系统上的控制台 Win32 调试输出。
- **筛选功能改进**：现在可以设置更长的筛选器，并在输出中包含进程 ID 时，应用于 Win32 进程 ID。
- **改进的故障转储支持**：修复了与从故障转储中提取内核模式输出相关的几个 bug，并且 *DebugView* 现在会加载生成的日志文件。
- **更多突出显示筛选器**：*DebugView* 现在具有 10 个突出显示筛选器，而以前是 5 个。
- **插入注释**：使用新的菜单项可将注释插入到输出中。
- **新切换开关**：使用新的命令行开关，可以指定历史记录深度和加载日志文件。
- **更好的气球提示**：如果输出行比屏幕更宽，则鼠标悬停气球提示词会自动换行。

版本 4.1 新增功能：

- **保存和加载筛选器**：可以保存和加载筛选器，包括高亮颜色。
- **加载保存的日志**：现在，可以将日志文件加载回 *DebugView* 输出窗口。
- **捕获启动时内核模式调试输出**：在 Windows 2000 下，可以使用 *DebugView* 捕获驱动程序从启动过程最早时间点生成的调试输出。

下面是一个列表，其中突出显示了 *DebugView* 的一些其他功能：

- **远程监视**：从任何可通过 TCP/IP（甚至是通过 Internet）访问的计算机捕获内核模式和/或 Win32 调试输出。 可以同时监视多台远程计算机。 如果你在 Windows 2000 系统上运行 DebugView，并从同一网络邻居中的另一个 Windows 2000 系统进行捕获，则 *DebugView* 甚至会自行安装其客户端软件。
- **最近筛选列表**：*DebugView* 会记住你最近的筛选器选择，其界面可帮助你轻松地重新选择它们。
- **专用 PID 列**： 单独的进程 ID 列显示生成每个调试消息的进程，可从“选项”菜单切换。
- **剪贴板复制**：在输出窗口中选择多行，并将其内容复制到剪贴板。
- **日志到文件**：在捕获的同时将调试输出写入文件。
- **打印**：将捕获的全部或部分调试输出打印到打印机。
- **单文件有效负载**：*DebugView* 是作为一个文件实现的。
- **故障转储支持**：*DebugView* 可以从故障转储中恢复其缓冲区，并将输出保存到日志文件，以便用户可以将 Windows 驱动程序在故障发生前生成的输出发送给你。 在版本 5.0 中，检测到未正常关闭时，会在启动时自动执行此恢复过程。

在线帮助文件详细介绍了所有这些功能以及更多内容。

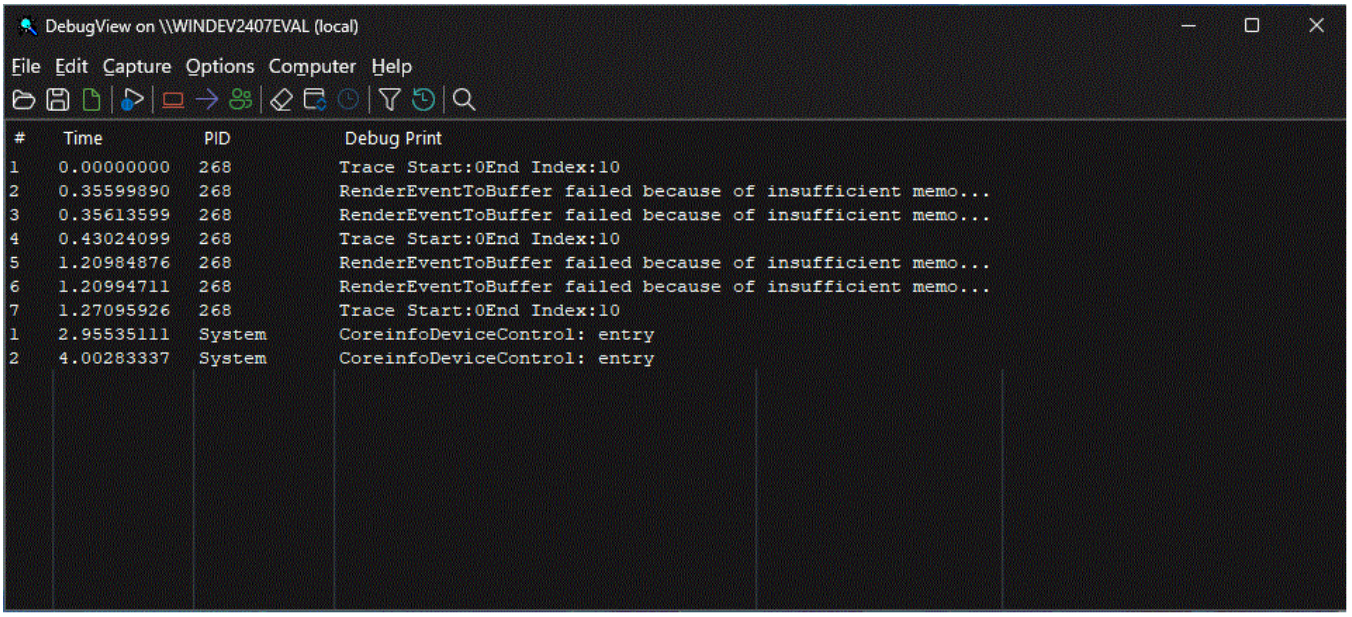
系统要求

DebugView v5.0 需要 Windows 10 版本 1809（内部版本 17763）或 Windows Server 2019 或更高版本。 现代 UI 基于 Windows XAML Islands 构建，因此需要此操作系统的最低版本。 较旧版本的 Windows 上的用户应使用 *DebugView* v4.90。

安装和使用

只需执行 *DebugView* 程序文件 (dbgview.exe)，*DebugView* 就会立即开始捕获调试输出。 *DebugView* 以标准用户身份启动;仅当启用内核模式捕获或其他需要管理权限的操作时，才会提示你通过 UAC 提升。 菜单、热键或工具栏按钮可用于清除窗口、将受监视的数据保存到文件、搜索输出、更改窗口字体等。 在线帮助介绍了 *DebugView* 的所有功能。

如果在系统崩溃期间以前的*DebugView*会话处于活动状态，*DebugView*将在下次启动时自动检测到异常关闭，扫描故障转储文件，并显示从上一会话中恢复的所有内核调试跟踪。



这是 *DebugView* 捕获调试输出的屏幕截图。 请注意具有专用 PID 列和突出显示筛选器的新式深色模式接口。

DebugView (1012 KB)

立即从 Sysinternals Live 运行。

Last updated on 2026/04/01

Desktops v2.01

项目 • 2024/07/25

作者：Mark Russinovich

发布时间：2021 年 10 月 12 日

 **下载 Desktops** **(199 KB)**
立即从 Sysinternals Live 运行。

简介

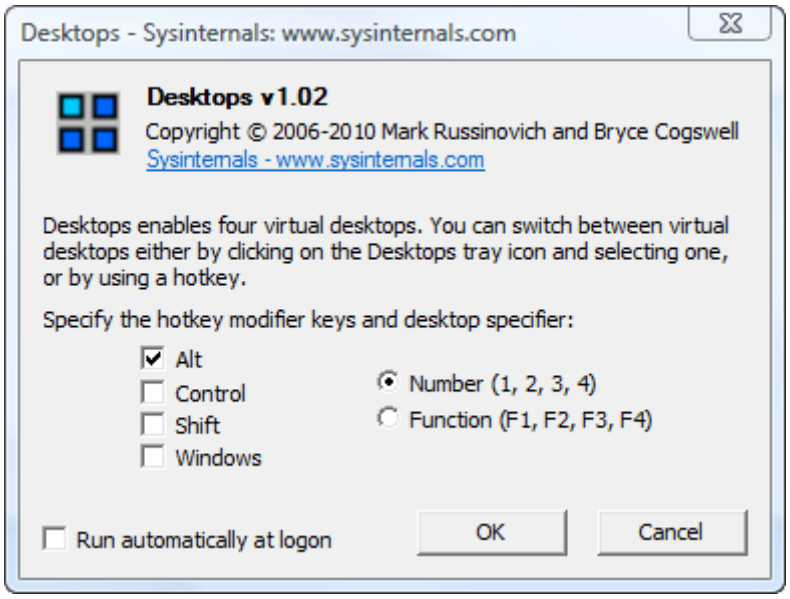
通过 Desktops，可将应用程序整理到最多 4 个虚拟桌面上。 在第一个桌面上阅读电子邮件，在第二个桌面上浏览网站，在第三个桌面上使用生产力软件进行工作，不会让未使用的窗口杂乱。 配置用于切换桌面的热键后，可以通过单击托盘图标打开桌面预览和切换窗口，或者通过使用热键来创建和切换桌面。

使用 Desktops

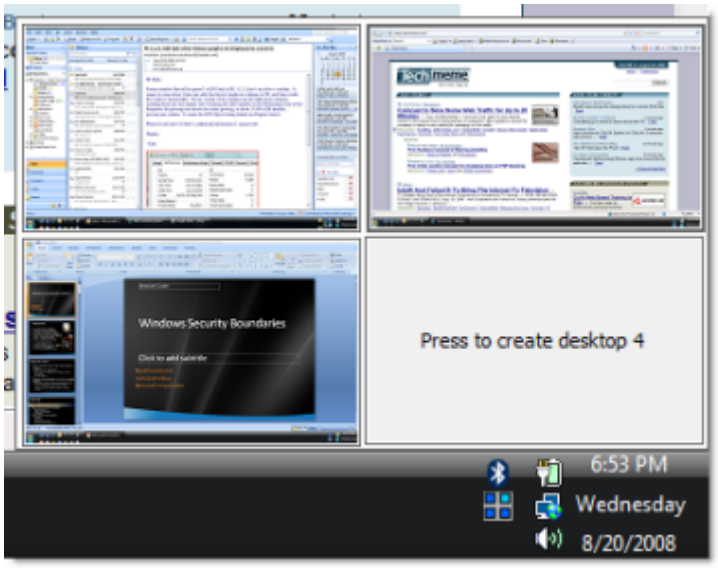
其他虚拟桌面实用工具会显示桌面上处于活动状态的窗口并隐藏其余窗口来实现其桌面，而与它们不同，Sysinternals Desktops 为每个桌面使用一个 Windows 桌面对象。 应用程序窗口在创建时绑定到桌面对象，因此 Windows 会维持窗口与桌面之间的连接，并知道在你切换桌面时要显示哪些窗口。 这使得 Sysinternals Desktops 非常轻型，并且没有 bug，而另一种方法容易导致活动窗口的视图与可见窗口不一致。

不过，Desktops 对 Windows 桌面对象的依赖意味着它无法提供其他虚拟桌面实用工具的某些功能。 例如，Windows 不提供将窗口从一个桌面对象移动到另一个桌面对象的方法，并且由于必须在每个桌面上运行单独的资源管理器进程来提供任务栏和开始菜单，因此大多数托盘应用程序仅在第一个桌面上可见。 此外，无法删除桌面对象，因此 Desktops 不提供关闭桌面的方法，因为这会导致出现孤立的窗口和进程。 因此，建议通过注销来退出 Desktops。

屏幕快照



配置对话框



Tray Desktop Switch Window

下载 Desktops (199 KB)

立即从 Sysinternals Live 运行。

运行软件：

- 客户端：Windows 7、Windows 8、Windows 8.1 和 Windows 10。
- 服务器：Windows Server 2008 - Windows Server 2022。

Hex2dec v1.1

项目 • 2024/11/21

作者：Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 Hex2dec** **(578 KB)**

简介

厌倦了运行 Calc 在十六进制和十进制之间转换？ 现在，你可以使用这个简单的命令行实用工具。

用法：hex2dec [hex|decimal]

包括 x 或 0x 作为数字的前缀，以指定十六进制值。
例如，将 1233 十进制转换为十六进制：hex2dec 1233
例如，将 0x1233 十六进制转换为十进制：hex2dec 0x1233

 **下载 Hex2dec** **(578 KB)**

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

NotMyFault v4.4

作者：Mark Russinovich

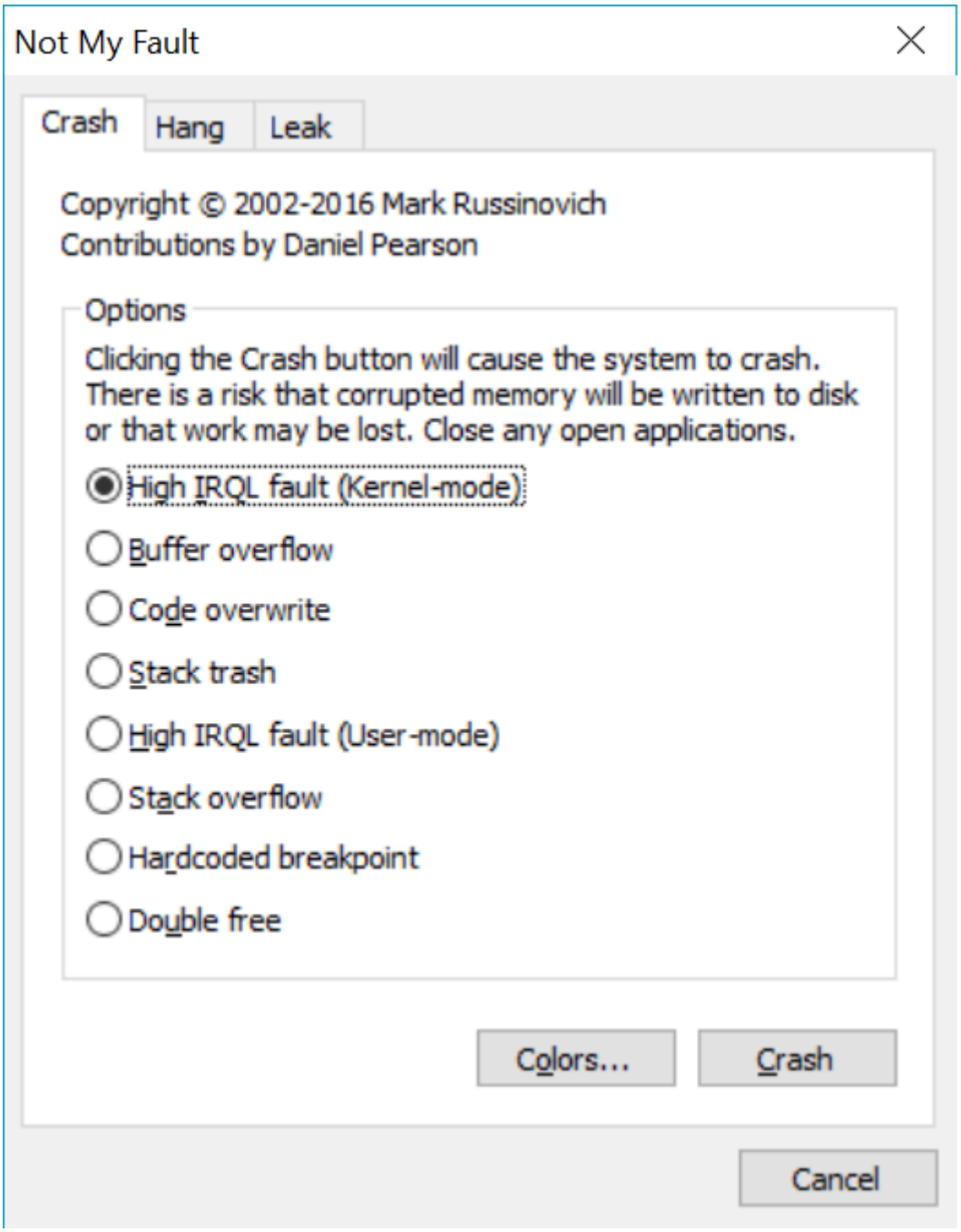
发布时间： 2026 年 3 月 26 日

 **下载 NotMyFault (1.4 MB)**

简介

Notmyfault 是一种工具，可用于在 Windows 系统上崩溃、挂起和导致内核内存泄漏。 它对学习识别和诊断设备驱动和硬件问题很有帮助，还可以用来在行为异常的系统上生成蓝屏转储文件。 下载文件包括 32 位和 64 位版本，以及适用于 Nano Server 的命令行版本。 Windows Internals 中的第 7 章使用 Notmyfault 演示池泄漏故障排除，第 14 章使用它进行故障分析示例。

屏幕截图



使用情况

可以使用 GUI 版本或命令行版本。 Notmyfault 需要管理权限。

用法：

notmyfaultc.exe 崩溃 crash_type_num

Shell

```
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
```

或者 **notmyfaultc.exe hang hang_type_num**

Shell

```
  hang type:
    0x01: Hang with IRP
    0x02: Hang with DPC
```

 下载 NotMyFault (1.4 MB)

Last updated on 2026/04/01

PsPasswd v1.25

项目 • 2023/08/03

作者： Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools** (5 MB)

简介

作为标准安全做法的一部分，在多台计算机上管理本地管理帐户的系统管理员需要定期更改帐户密码。 *PsPasswd* 是一种可用于更改本地或远程系统上的帐户密码的工具，使管理员能够创建批处理文件，在他们管理的计算机上运行 *PsPasswd*，以便对管理员密码进行大规模更改。

PsPasswd 使用 Windows 密码重置 API，因此不会明确通过网络发送密码。

安装

只需将 *PsPasswd* 复制到可执行路径，并使用如下所示的命令行语法键入“pspasswd”。

使用 PsPasswd

可以使用 *PsPasswd* 更改本地或远程计算机上的本地或域帐户的密码。

用法： pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] Username [NewPassword]

参数	说明
computer	在指定的远程计算机上执行命令。 如果省略计算机名称，则命令在本地系统上运行，如果指定通配符 (*)，则命令将在当前域中的所有计算机上运行。
@file	在指定的文本文件中列出的每台计算机上运行命令。
-u	指定登录远程计算机的可选用户名。
-p	指定用户名的可选密码。 如果省略此内容，系统将提示你输入隐藏密码。
用户名	指定要更改密码的帐户的名称。
NewPassword	新密码。 如果省略，则应用 NULL 密码。

 下载 PsTools (5 MB)

PsTools
PsPasswd 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 *PsTools* 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

PsShutdown v2.6

作者：Mark Russinovich

发布时间：2023 年 3 月 30 日

 **下载 PsTools (5 MB)**

简介

PsShutdown 是类似于 Windows 附带的关闭实用工具的命令行实用工具，但能够执行更多作。 除了支持用于关闭或重新启动本地或远程计算机的相同选项外，PsShutdown 还可以注销控制台用户或锁定控制台（锁定需要 Windows 2000 或更高版本）。 PsShutdown 无需手动安装客户端软件。

安装

只需将 PsShutdown 复制到可执行文件路径，并使用下面定义的命令行选项键入 psshutdown。

使用 PsShutdown

请参阅《Windows IT 专业杂志》2005年2月刊中的Mark的文章 https://www.itprotoday.com/microsoft-windows/psshutdown，其中介绍了*PsShutdown*的高级用法。

可以使用 PsShutdown 对本地或远程计算机执行关闭、注销用户、锁定系统或中止即将进行的关闭等操作。

用法：psshutdown [[\\computer[,computer[,..] | @file [-u 用户 [-p psswd]]]-s|-r|-h|-d|-k|-a|-l|-o|-x [-f] [-c] [-t nn|h:m] [-n s] [-v nn] [-e [u|p]:xx:yy] [-m "message"]

展开表

参数	说明
-	显示支持的选项。
computer	在指定的远程计算机上执行命令。 如果省略计算机名称，则命令在本地系统上运行，如果指定通配符 (*)，则命令将在当前域中的所有计算机上运行。
@file	在指定的文本文件中列出的每台计算机上运行命令。
-u	指定登录远程计算机的可选用户名。

参数	说明
-p	指定用户名的可选密码。 如果省略此内容，系统将提示你输入隐藏密码。
-a	中止关闭（仅在进行倒计时时才可能操作）。
-c	允许交互用户中止关闭。
-d	暂停计算机。
-e	关闭原因代码。
	为用户原因代码指定“u”，为计划关闭原因代码指定“p”。
	xx 是主要原因代码（必须小于 256）。
	yy 是次要原因代码（必须小于 65536）。
-f	强制所有正在运行的应用程序在关闭期间退出，不让它们有机会正常保存其数据。
-h	将计算机休眠。
-k	关闭计算机电源（如果不支持关闭电源，请重新启动）。
-l	锁定计算机。
-m	此选项用于指定在关闭倒计时开始时向登录用户显示的消息。
-n	指定连接到远程计算机的超时时间（以秒为单位）。
-o	注销控制台用户。
-r	关闭后重新启动。
-s	不断电关闭。
-t	指定关闭之前的倒计时秒数（默认值：20 秒）或关闭时间（以 24 小时表示法）。
-x	关闭显示器（如果支持，系统将启动新式待机）
-v	显示关闭前指定秒数的消息。 如果省略此参数，将显示关闭通知对话框，同时将值指定为 0 会导致不显示任何对话。

 **下载 PsTools (5 MB)**

PsTools

PsShutdown 是 Sysinternals 命令行工具日益增多的工具包的一部分，可帮助管理名为 PsTools 的本地和远程系统。

运行平台：

- 客户端：Windows 8.1 及更高版本。
- 服务器：Windows Server 2012 及更高版本。

Last updated on 2026/02/06

远程桌面连接管理器 v3.12

作者：Julian Burger

发布时间： 2026 年 2 月 4 日

 **远程桌面连接管理器** **(116.1 MB)**
立即从 Sysinternals Live 运行。

介绍

RDCMan 管理多个远程桌面连接。 这对于管理需要定期访问每台计算机（例如自动签到系统和数据中心）的服务器实验室非常有用。

服务器组织到命名组中。 可以使用单个命令连接到组中的所有服务器或断开其连接。 可以将组中的所有服务器作为一组缩略图查看，显示每个会话中的实时操作。 服务器可以从父组或凭据存储继承其登录设置。 因此，更改实验室帐户密码时，只需更改 RDCMan 在一个位置中存储的密码。 通过使用本地登录用户的机构的 CryptProtectData 或 X509 证书进行加密，从而安全存储密码。

操作系统版本早于 Win7/Vista 的用户需要获取终端服务客户端版本 6。 可以从 Microsoft 下载中心获取此内容：XP; Win2003

升级注意：具有此版本的 RDCMan 的 RDG 文件与较旧的程序版本不兼容。 使用此版本打开并保存的任何旧 RDG 文件都将备份为 filename.old

---

显示内容

远程桌面连接管理器显示内容包括菜单、包含服务器组的树、拆分条和工作区。

菜单

RDCMan 中有多个顶级菜单：

- **文件** - 加载、保存和关闭 RDCMan 文件组
- **编辑** - 添加、删除和编辑服务器和组的属性。
- **会话** - 连接、断开连接和注销会话
- **视图** - 用于控制服务器树、虚拟组和工作区大小的可见性的选项
- **远程桌面** - 允许以分层方式访问组和服务器，类似于服务器树；主要用于隐藏服务器树时
- **工具** - 更改应用程序属性
- **帮助** - 了解 RDCMan（你可能已找到此信息）

树

大多数工作（例如添加、删除和编辑服务器和组）都可以通过右击树节点来完成。 可以使用拖放移动服务器和组。

键盘快捷方式：

- **输入**：连接到所选服务器。
- **Shift+Enter**：使用“连接方式”功能连接到所选服务器。
- **删除**：删除所选服务器或组。
- **Shift+Delete**：毫无疑问，删除所选服务器或组。
- **Alt+Enter**：所选服务器或组的“打开属性”对话框。
- **Tab**：如果已选择连接的服务器，使其具有焦点。

使用**[View.Server tree location]**菜单选项在窗口的左边缘或右边缘找到树。

服务器树可以通过**[View.Server tree visibility]**菜单选项进行停靠、自动隐藏或始终隐藏。 如果未显示服务器树，仍可通过远程桌面菜单访问服务器。 树自动隐藏时，拆分条在窗口左侧保持可见。 将鼠标悬停在它上方会将服务器树重新置于视图中。

工作区

工作区显示内容取决于树中选择的节点。 如果选择了服务器，工作区会显示该服务器的远程桌面客户端。 如果选择了组，工作区会显示该组中服务器的缩略图。 可以通过“视图”菜单以及调整 RDCMan 窗口的大小来指定工作区的大小。 拖动框架，使用**[View.Lock window size]**阻止窗口调整大小。

注意：连接的服务器可以从缩略图视图的键盘导航中接收焦点。 哪个服务器具有焦点并不总是显而易见，因此请小心。 有设置可控制此内容：[Display Settings.Allow thumbnail session interaction]。

全屏模式

要在全屏模式下使用服务器，请选择服务器以使其具有焦点，然后按**Ctrl+Alt+Break**（此键可配置，请参阅快捷键。）要退出全屏模式，请再次按**Ctrl+Alt+Break**或者使用连接标题栏中的最小化/还原按钮。 可以跨多个监视器（如果通过监视器跨越选项启用）。

快捷键

可在此处找到终端服务快捷键的完整列表。 其中一些可以从“热键”选项卡进行配置。

文件存储

RDCMan 中的顶级组织单位是远程桌面文件组。 文件组是存储在单个物理文件中的组和/或服务器的集合。 服务器不能位于组外部，组不能位于文件外部。

文件具有服务器组的所有特征，但不能更改其父级。

群组

组包含服务器和配置信息的列表（例如登录凭据）。 配置设置可以从另一个组或应用程序默认值继承。 组可以嵌套，但是同质：组可以包含组或服务器，但不能同时包含两者。 组中的所有服务器可以同时连接或断开连接。

在树视图中选择组后，其下方的服务器会显示在缩略图视图中。 缩略图可以显示实际的服务器窗口，也可以仅显示连接状态。 全局缩略图视图属性可以通过**[Tools.Options.Client Area]**选项卡进行调整，而组/服务器特定的设置位于“显示设置”中。

智能组

智能组基于一组规则动态填充。 智能组的所有同级组的祖先都有资格加入。

连接的虚拟组

当服务器处于已连接状态时，会自动添加到连接的虚拟组。 无法显式添加或删除已连接组的服务器。

可以通过“视图”菜单打开/关闭“连接的组”。

重新连接虚拟组

有时，服务器会断开连接，并且会在未指定的时间内有意脱机，例如，在 OS 更新后重启时。 在这种情况下，请将有问题的服务器拖到“重新连接组”。 RDCMan 将持续尝试连接到服务器，直到成功。

可以通过“视图”菜单打开/关闭“重新连接组”。

收藏夹虚拟组

收藏夹虚拟组是常用服务器的平面文件。 可以从服务器树添加任何服务器。 当树中有许多服务器并且通常使用不同组中的少数服务器时，这非常有用。

可以通过“视图”菜单打开/关闭“收藏夹组”。

连接到虚拟组

“连接到虚拟组”包含非用户创建的组成员的服务器。 有关详细信息，请参阅“临时连接”。

当临时连接存在时，“连接到组”可见，当没有临时连接时，该组消失。

最近的虚拟组

“最近的虚拟组”包含最近访问的服务器。

可以通过“视图”菜单打开/关闭“最近的组”。

服务器

服务器具有服务器名称（计算机的网络名称或 IP 地址）、可选显示名称和登录信息。 登录信息可能继承自另一个组。

手动添加服务器

可以批量将遵循模式的服务器名称添加到组中。 有两个模式类：

- 迭代 - `{a,b,c}` 迭代以逗号分隔的内容。
- 范围 - `[1-5]` 迭代数值范围。 为下限添加前缀 `0`，指定最小宽度。

示例：

- `server1{a,b,c}`： 加载项 `server1a`, `server1b`, `server1c`
- `server[001-15]`： 加载项 `server001`, `server002`, ..., `server015`
- `{dca,dcb}rack[1-5]sql[1-2]`： 加载项 `dcarack1sql1`, `dcarack1sql2`, `dcarack2sql1`, ..., `dcarack5sql2`, `dcbrack1sql1`, ... `dcbrack5sql2`

从文本文件导入服务器

服务器可以从文本文件导入到组中。 文件格式只是每行一个服务器名称：

```txt
Server1
SecondServer
YANS
```

还可以在对话框中显式指定服务器名称。

所有服务器都导入到具有相同首选项的同一组中。 如果导入的服务器与现有服务器同名，现有服务器的首选项会更新为新首选项。

临时连接

可以通过 [Session.Connect to] 功能创建临时服务器连接。 这些服务器将添加到“连接到虚拟组”。 在这里，将其移动到用户创建的组，从而将它们转换为真实服务器。 RDCMan 退出时，不会保留“连接到组”中剩余的服务器。

Windows Azure

在 **[连接设置]** 选项卡中，*按此处所述*，在负载均衡配置中输入角色名称和角色实例名称，例如 `Cookie: mstshash=MyServiceWebRole#MyServiceWebRole_IN_0#Microsoft.WindowsAzure.Plugins.RemoteAccess.Rdp`

会话操作

在会话中，焦点可以释放到另一个会话或服务器树。

- 焦点向左释放（默认值为**Ctrl+Alt+Left**）：这会选择之前选择的会话。
- 焦点向右释放（默认值为**Ctrl+Alt+Right**）：此时会显示对话框，用于选择焦点位置。 将有按钮用于到达最近使用的会话，以及用于服务器树的按钮和用于最小化 RDCMan 的按钮。

某些键组合和 Windows 操作在远程会话上执行可能很棘手--尤其是在远程会话中启动 RDCMan 本身时--例如， **Ctrl+Alt+Del**。这些内容可从**[Session.Send keys]**和**[Session.Remote actions]**菜单项获取。

全局选项

[Tool.Options]菜单项显示“选项对话框”。 全局设置（例如，工作区大小）可从此处修改。 大多数与服务器相关的选项（例如，热键和体验页上的选项）在下次连接服务器之前不会生效。

常规

隐藏主菜单，直到按下 Alt
可以隐藏主菜单，直到按下 Alt 键或按鼠标左键点击窗口标题区域。

自动保存间隔
可以让 RDCMan 定期自动保存打开的文件。 选中“自动保存”复选框，并指定保存间隔（以分钟

为单位）。 间隔为 0 不会定期保存，但在退出 RDCMan 时会取消保存提示。

启动时重新连接连接的服务器的提示
RDCMan 会记住程序退出时连接的服务器。 在下一次运行时，会提示选择要重新连接的服务器。 禁用此选项会自动重新连接之前连接的所有服务器。 有关影响此行为的命令行开关，请参阅命令行。

默认组设置
点击此按钮会打开对话框，用于为继承层次结构的基级别配置设置。 例如，如果文件组设置为从其父级继承，则这就是设置的来源。

树

点击以选择使远程客户端具有焦点
使用鼠标点击选择服务器树控件中的节点时，默认行为是将焦点保持在树控件上。 有选项用于更改此项，以将焦点置于所选服务器上。

树控件处于非活动状态时将节点变暗
RDCMan 可以在树控件处于非活动状态时将其变暗。 这呈现出键盘焦点更明显的视觉区别。

工作区

工作区大小
此选项调整 RDCMan 窗口的工作区大小。 “**[View.Client size]**”菜单中也提供了这些选项。

缩略图单位大小
缩略图单位大小可以指定为绝对像素大小或客户端面板宽度的相对百分比。

热键

许多远程桌面热键都可配置。 但是，映射有限。 例如，如果默认键为 Alt-something，替换项也必须为 Alt-something。 要更改热键，请导航到热键的文本框，然后按新的 "something" 键。

体验

根据计算机的可用带宽，需要限制 Windows UI 功能以提高性能。 连接速度下拉列表可用于一起设置所有选项，也可以单独自定义。 这些功能包括：桌面背景、拖动时显示全屏内容、菜单和窗口动画以及窗口主题。

全屏显示

显示全屏连接栏
自动隐藏连接栏
当服务器以全屏模式显示时，远程桌面 activeX 控件会在窗口顶部提供 UI 连接栏。 此栏可以打开和关闭。 打开后，可以选择将其固定或自动隐藏。

全屏窗口始终位于顶部
当 RDCMan 在全屏模式下显示服务器时，可以选择始终将窗口显示为最顶部的窗口。

必要时使用多个监视器
默认情况下，全屏会话仅限于包含服务器窗口的监视器。 可以在全屏选项中启用多个监视器跨越。 如果远程桌面大于窗口的监视器，它将根据需要跨尽可能多的监视器以适应远程会话。 请注意，仅使用矩形区域，因此，如果有两个具有不同垂直分辨率的监视器，则使用两者中较短的一个。 此外，远程桌面控件的硬性限制为 4096x2048。

本地选项

组和服务器具有多个选项卡式属性页，其中包含各种自定义选项。 其中许多页面对于组和服务器通用。 选中“从父级继承”复选框时，以下设置会从父容器继承。 大多数与服务器相关的更改（例如，远程桌面大小）在下次连接服务器之前不会生效。

文件设置

此页仅针对文件属性显示。 它包含文件组名称的选项，显示文件的完整路径（无法编辑），并具有注释字段。

组设置

此页仅针对组属性显示。 它包含用于组名称、父嵌套和注释的选项。

服务器设置

此页仅针对服务器属性显示。 它包含用于服务器名称、其显示名称、父嵌套和注释的选项。 可以使用 VM 控制台连接选项通过 RDP 将 SCVMM 虚拟机连接到主机。 使用 PowerShell 命令：

```PowerShell
get-vm | ft ElementName,Name,Id
```

以确定与 VM 对应的 ID。

登录凭据

“登录凭据”属性页包含与远程登录相关的选项。 在此页设置用户名、密码和域。 可以使用 domain\user 格式一起指定域和用户名。 登录到计算机“域”而不是 Windows 域时，可以指定 [server] 或 [display]。 前者将在登录时替换为服务器名称，后者将替换为显示名称。 当有一组需要以管理员身份登录的计算机时，这非常有用。 默认情况下，在属性页中输入的“登录设置”用于新连接。 如果要为新连接临时自定义这些设置，请使用“连接方式”菜单项进行连接。

网关设置

“网关设置”属性页包含用于使用 TS 网关服务器的选项。 “网关名称”、“身份验证方法”和“本地地址绕过”选项位于此页。 从 Vista SP1 和 Longhorn 服务器开始的操作系统的用户将具有有关登录凭据的其他选项：

网关用户名和密码的显式输入 能够与远程服务器共享网关凭据

连接设置

“连接设置”选项卡包括用于自定义会话的连接方式以及登录时发生的情况的设置。

可以指定是否应连接到控制台会话以及远程桌面连接端口。

还有一些设置允许在连接时运行程序。 输入程序名称以及该程序的工作目录（可选）。 请注意，只有在首次连接到控制台会话时，这些操作才有效。 也就是说，重新连接到会话或连接到控制台会话以外的会话不会运行程序。 （至少，根据经验观察，终端服务就是这样运作的。）

远程桌面设置

此页指定了远程桌面的大小。 这是逻辑桌面大小，而不是其物理客户端视图。 例如，如果远程桌面大小为 1280 x 1024，客户端大小为 1024 x 768，会看到带有滚动条的远程桌面的 1024 x 768 视图。 如果客户端大小为 1600 x 1200，整个远程桌面会可见，并有灰色边框偏移。

指定“与工作区相同”将使远程桌面的大小与 RDCMan 客户端面板相同，即不包括服务器树的 RDCMan 窗口工作区。 指定“全屏”将使远程桌面的大小与查看服务器的屏幕大小相同。 请注意，远程桌面大小在连接到服务器时确定。 为连接的服务器更改此设置将不起作用。

远程桌面的最大大小由远程桌面 ActiveX 控件的版本决定。 版本 5（Vista 前）的最大大小为 1600 x 1200；版本 6 (Vista)的最大大小为 4096 x 2048。 此限制在连接时（而不是数据输入期间）强制执行。 这是在多台计算机共享同一 RDCMan 文件时的情况。

本地资源

远程服务器的各种资源可能会传送到客户端。 远程计算机声音可以本地播放、远程播放或完全禁用。 Windows 组合键（例如，涉及实际 Windows 键以及 Alt+Tab 等其他特殊项的组合键）

可以始终应用于客户端计算机，始终应用于远程计算机，或窗口化时应用于客户端，以及在全屏模式下应用于远程计算机。 客户端驱动器、端口、打印机、智能卡和剪贴板资源可以自动共享到远程计算机。

安全设置

可以指定在建立连接之前是否需要对远程计算机进行身份验证。

显示设置

可从此页自定义缩略图显示设置。

第一个选项是：缩略图比例。 这指定要分配给给定服务器显示内容的缩略图单位数。 所有服务器都默认为 1。 可以更改此设置以增加重要服务器的显示内容。 例如，服务器可以按 3 或 5 缩放，使远程会话在缩略图显示中非常可用，同时仍允许查看许多其他服务器。 这是服务器的唯一选项。

组有三个附加选项：预览缩略图中的会话、允许缩略图会话交互和显示断开连接的缩略图。 第一个是缩略图视图是否显示持续更新的实际实时连接。 第二个（依赖于第一个）指定缩略图会话是否可用。 最后一个选项控制断开连接的服务器是否显示在缩略图视图中。

加密设置

RDCMan 可以通过 CryptProtectData 或 X509 证书使用本地用户的凭据加密存储在文件中的密码。 “默认组设置”和“文件设置”对话框中提供了“加密设置”选项卡。

具有私钥的当前用户的个人证书可用于加密。 可以按以下方式创建此类证书：

PowerShell

```
New-SelfSignedCertificate -KeySpec KeyExchange -KeyExportPolicy Exportable -
HashAlgorithm SHA1 -KeyLength 2048 -CertStoreLocation "cert:\CurrentUser\My" -
Subject "CN=MyRDCManCert"
```

这会在当前用户的个人证书存储中创建名为 "`MyRDCManCert`" 的证书。 要在另一台计算机上安装此证书，必须使用私钥将其导出。

配置文件管理

可以从此选项卡中添加、编辑和删除凭据配置文件。

列出远程会话

RDCMan 对管理远程会话的支持有限，但从其连接的会话除外。 **[Session.List Sessions]**菜单项调用该功能。

请注意，运行 RDCMan 的帐户必须在远程服务器上具有查询信息权限才能列出会话。 此外，远程会话必须可直接访问，而不是通过网关服务器进行访问。 必须授予断开连接和注销权限才能执行这些操作。 有关远程桌面权限的详细信息，请参阅 msdn。

命令行

默认情况下，RDCMan 将打开上次程序关闭时加载的文件。 可以在 RDCMan 命令行上显式指定文件以替代此设置。 此外，还接受以下开关：

- `/reset` - 重置持久化的应用程序首选项，例如窗口位置和大小。
- `/noopen` - 从空环境开始，不要打开之前加载的文件。
- `/c server1[,server2...]` - 连接指定的服务器
- `/reconnect` - 在不提示的情况下连接关闭时连接的所有服务器
- `/noconnect` - 不提示连接关闭时连接的服务器

查找服务器

有对话框用于查找通过**Ctrl+F**或**Edit.Find**（服务器）命令访问的服务器。 与正则表达式模式匹配的所有服务器都显示在对话框中，并且可以通过上下文菜单执行操作。 该模式与全名（`group\server`）匹配。

凭据配置文件

凭据配置文件将登录凭据全局存储到 RDCMan 或文件中。 这允许跨无共同祖先的组使用相同的存储凭据。 一种使用方案是在单个位置中存储用于登录到服务器和网关的凭据。 密码更改时，可以编辑一次。 另一种方案是跨组共享 RDG 文件时。 不会将密码存储在文件中（由于 RDCMan 使用的加密的用户特定性质，这可能会出现问题），而是创建配置文件（例如，每个用户在其全局存储中定义的 "Me"）。

可以通过两种方式更新凭据配置文件的设置。 第一种是从凭据对话框中编辑，然后将完全相同的配置文件名称/域保存到同一存储中（文件或全局）。 这将询问你是否要更新。 另一种方式是再次转到凭据存储的组属性（文件或全局）并使用“配置文件管理”选项卡。

文件范围凭据配置文件密码根据包含文件的加密设置进行加密。 全局凭据配置文件使用默认组设置。

策略

RDCMan 从`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\RDCMan`注册表项中检索策略信息。

- `DisableLogOff` - 将此`DWORD`值创建为非零，以在整个 RDCMan 中禁用注销命令。

FAQ

- *如何使用智能卡凭据登录?*

  在"本地资源"选项卡中启用"重定向智能卡"。

- *通过网关连接时出现错误，例如错误 50331656。 为什么?*

  必须将网关指定为 FQDN。

- *如何使自动登录正常工作?*

  必须启用组策略控制它。 使用 MMC"组策略"管理单元并导航到"本地计算机策略/计算机配置/管理模板/Windows 组件/终端服务/加密和安全性"。 双击"连接时始终提示客户端输入密码"，然后点击"已禁用"框。

- *如何在连接服务器时调整远程桌面的大小?*

  你无法管理。 要调整大小，必须断开连接并重新连接（使用重新连接功能一步完成此操作）。 RDCMan 服务器可以在"显示设置"下选择自动重新连接到停靠服务器和未停靠服务器的新分辨率。

下载

远程桌面连接管理器 **(116.1 MB)**
立即从 Sysinternals Live 运行。

运行平台:

- 客户端：Windows 11 及更高版本。
- 服务器：Windows Server 2016 及更高版本。

Last updated on 2026/02/04

RegDelNull v1.11

项目 • 2024/07/25

作者： Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 RegDelNull** (511 KB)

简介

此命令行实用工具搜索并允许删除包含嵌入 null 字符的注册表项，否则使用标准注册表编辑工具无法删除这些注册表项。 注意：删除注册表项可能会导致与其关联的应用程序失败。

使用 RegDelNull

用法: regdelnull <**路径**> [-s]

展开表

参数	说明
-s	递归到子项。

以下是在 RegHide 示例程序创建了null 嵌入项的系统上使用 RegDelNull 的示例：

Shell

```
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.
```

 **下载 RegDelNull** (511 KB)

运行平台：

- 客户端：Windows Vista（32 位）及更高版本
- 服务器：Windows Server 2008（32 位）及更高版本
- Nano Server：2016 及更高版本

注册表使用情况 (RU) v1.2

项目 • 2024/07/25

作者： Mark Russinovich

发布时间：2016 年 7 月 4 日

 **下载 RU** **(507 KB)**

简介

Ru（注册表使用情况）报告指定注册表项的注册表空间使用情况。 默认情况下，它递归子项以显示项及其子项的总大小。

使用注册表使用情况 (RU)

使用情况: ru [-c[t]] [-l <**级别**> | -n | -v] [-q] <**绝对路径**>

使用情况: ru [-c[t]] [-l <**级别**> | -n | -v] [-q] -h <**配置单元文件**> [**相对路径**]

展开表

参数	说明
-c	将输出打印为 CSV。 指定 -ct 作为制表符分隔符。
-h	加载指定配置单元文件，执行大小计算，然后卸载并压缩它。
-l	指定信息的子项深度（默认为一级）。
-n	请勿递归。
-q	安静（没有横幅）。
-v	显示所有子项的大小。

CSV 输出的格式为：

Path,CurrentValueCount,CurrentValueSize,ValueCount,KeyCount,KeySize,WriteTime

 **下载 RU** **(507 KB)**

Reghide

项目 • 2024/11/21

发布日期：2006 年 11 月 1 日

 **下载 RegHide** **(38 KB)**通过 Sysinternals Live **立即运行。**

简介

Win32 API 和本机 API 之间的细微但显著差异（请参阅 Native API 内部，了解有关此基本未记录的接口的详细信息）是描述名称的方式。 在 Win32 API 中，字符串被解释为以 NULL 结尾的 ANSI（8 位）或宽字符（16 位）字符串。 在本机 API 中，按 Unicode（16 位）字符串计数。 虽然这种区别通常并不重要，但产生了一种有趣的情况：有一类名称可以使用本机 API 引用，但不能使用 Win32 API 描述。

 **下载 RegHide** **(38 KB)**

立即从 Sysinternals Live 运行。

运行平台：

- 客户端：Windows Vista 及更高版本。
- 服务器：Windows Server 2008 及更高版本。

RegJump v1.11

项目 • 2024/11/21

作者：Mark Russinovich

发布时间：2021 年 10 月 12 日

 **下载 RegJump** **(164 KB)**

简介

此小命令行小程序采用注册表路径，并使 Regedit 对该路径开放。 它接受标准形式（如 HKEY_LOCAL_MACHINE）和缩写形式（如 HKLM）的根密钥。

usage: regjump <<path>|-c>

展开表

参数	说明
-c	从剪贴板复制路径。

例如：regjump HKLM\Software\Microsoft\Windows

 **下载 RegJump** **(164 KB)**

Strings v2.54

项目 • 2024/07/25

作者：Mark Russinovich

发布时间：2021 年 6 月 22 日

 **下载 Strings (534 KB)**

简介

使用 NT 和 Win2K 意味着可执行文件和对象文件将多次嵌入 UNICODE 字符串，而使用标准 ASCII 字符串或 grep 程序无法轻松看到这些字符串。 因此，我们决定使用自己的字符串。 Strings 只会扫描你传递的文件，查找默认长度为 3 个 或更多 UNICODE（或 ASCII）字符的 UNICODE 或 ASCII 字符串。 请注意，它也适用于 Windows 95。

使用 Strings

用法：

Windows 命令提示符

```
strings [-a] [-f offset] [-b bytes] [-n length] [-o] [-q] [-s] [-u] <file or directory>
```

Strings 采用通配符表达式作为文件名，其他命令行参数定义如下：

展开表

参数	说明
-a	仅限 Ascii 搜索（默认为 Unicode 和 Ascii）
-b	要扫描的文件字节数
-f	开始扫描的文件偏移量。
-o	文件字符串中的打印偏移已找到
-n	最小字符串长度（默认值为 3）
-s	递归子目录

参数	说明
-u	仅限 Unicode 搜索（默认为 Unicode 和 Ascii）
-nobanner	不显示启动横幅和版权消息。

若要使用字符串搜索一个或多个文件是否存在特定字符串，请使用如下所示的命令：

Windows 命令提示符

```
strings * | findstr /i TextToSearchFor
```

 下载 Strings (534 KB)

运行平台：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2008 及更高版本
- Nano Server：2016 及更高版本

Testlimit v5.24

项目 • 2023/08/03

作者： Mark Russinovich

发布日期：2016 年 11 月 17 日

 **下载 Testlimit** (234 KB)

简介

Testlimit 是一种命令行实用工具，可用于通过模拟内存、句柄、进程、线程和其他系统对象的低资源条件来对电脑和/或应用程序进行压力测试。

用法： Testlimit [[-h [-u]] | [-p [-n]] | [-t [-n [KB]]] | [-u [-i]] | [-g [**对象大小**]] | [-a|-d|-l|-m|-r|-s|-v [MB]] | [-w]] [-c [**计数**]] [-e [**秒数**]]

参数	说明
-a	以指定的 MB 单位泄漏地址窗口扩展 (AWE) 内存（默认值为 1）
-c	要分配的对象计数（默认值是“尽可能多”）。 这必须是指定的最后一个选项
-d	以指定的 MB 单位泄漏和触摸内存（默认值为 1）
-e	两次分配之间经过的秒数（默认值为 0）
-g	创建指定大小的 GDI 句柄（默认为 1 字节）。 将大小指定为 0 将导致 GDI 对象耗尽
-h	创建句柄。 指定 -u 也会分配文件对象
-i	耗尽 USER 桌面堆
-l	分配指定数量的大页面（舍入到大大小的倍数）
-m	以指定的 MB 单位泄漏内存（默认值为 1）
-p	创建进程 - 添加 -n 以设置最小工作集。 添加 -n 以将进程的最小工作集设置为最小
-r	以指定的 MB 单位保留内存（默认值为 1）
-s	以指定的 MB 单位泄露共享内存（默认值为 1）
-t	创建线程 - 添加 -n 以指定最小堆栈保留（以 KB 为单位）
-u	创建菜单的 USER 句柄

参数	说明
-v	以指定的 MB 单位对内存执行 VirtualLock（默认值为 1）
-w	将工作集最小值重置为最高可能值

运行软件：

- 客户端：Windows Vista 及更高版本
- 服务器：Windows Server 2003 及更高版本
- Nano Server：2016 及更高版本

相关链接

- **Windows Internals 书籍**：关于 Windows Internals 的权威性书籍的官方更新和勘误页，由 Mark Russinovich 和 David Solomon 编写。
- **Windows Sysinternals 管理员参考**：Mark Russinovich 和 Aaron Margosis 编写的 Sysinternals 实用工具官方指南，其中包含各项工具的说明、其功能、如何使用这些工具进行故障排除，以及它们的实际使用示例。

下载

 **下载 Testlimit** (234 KB)
立即从 Sysinternals Live 运行。

ZoomIt v11.0

作者： Mark Russinovich

发布时间： 2026 年 3 月 26 日

 **ZoomIt** **(2.4 MB)**
立即 从 Sysinternals Live 运行。

从 Microsoft PowerToys 下载 （GitHub）

https://learn-video.azurefd.net/vod/player?id=31330ae9-ccc2-4001-a9ce-35dcbb8b5aa2&locale=zh-cn&embedUrl=%2Fsysinternals%2Fdownloads%2Fzoomit

通过 ZoomIt 创建

介绍

ZoomIt 是用于技术展示和演示的屏幕缩放、注释和录制工具。 还可以使用 ZoomIt 将屏幕截图截取到剪贴板或文件。 ZoomIt 在系统托盘中不显眼地运行，可使用可自定义的热键激活，它能够放大屏幕区域，在缩放时四处移动，并在缩放后的图像上进行绘制。 我编写了 ZoomIt 以满足我的具体需求，并在我的所有演示中使用它。

ZoomIt 适用于所有版本的 Windows，你可以在平板电脑上使用触控和笔输入进行 ZoomIt 绘图。

使用 ZoomIt

首次运行 ZoomIt 时，它会显示一个配置对话框，用于描述 ZoomIt 的行为，让我们指定用于缩放和在不缩放的情况下进入绘图模式的备用热键，并自定义绘图笔的颜色和大小。 我使用“无缩放绘图”选项，以本机分辨率在屏幕上进行注释。 ZoomIt 还包括一个中断计时器功能，即使在你离开计时器窗口时也保持活动状态，并使你能够通过单击 ZoomIt 托盘图标返回到计时器窗口。

快捷方式

ZoomIt 提供了许多快捷方式，可以极大地扩展它的使用。

展开表

函数	快捷键
缩放模式	Ctrl + 1
放大	鼠标向上滚动或向上箭头
缩小	鼠标向下滚动或向下箭头
开始绘制（在缩放模式下）	左键单击
停止绘制（在缩放模式下）	右键单击
开始绘制（不在缩放模式下）	Ctrl + 2
增加/减少线条和光标大小（绘图模式）	Ctrl + 鼠标向上/向下滚动或箭头键
将光标居中（绘图模式）	空格键
白板（绘图模式）	W
Blackboard（绘图模式）	K
键入文本（左对齐）	T
在文本框中键入文字（右对齐）	Shift + T
增加/减小字号（键入模式）	Ctrl + 鼠标向上/向下滚动或箭头键
红笔	R
红色荧光笔	Shift + R
绿笔	G
绿色荧光笔	Shift + G
蓝笔	B
蓝色突出显示笔	Shift + B
黄笔	Y
黄色荧光笔	Shift + Y
橙笔	O
橙色荧光笔	Shift + O
粉笔	P
粉红色荧光笔	Shift + P

函数	快捷键
模糊笔	X
绘制直线	长按 Shift
绘制矩形	长按 Ctrl
绘制椭圆	长按 Tab
绘制箭头	长按 Ctrl + Shift
擦除最后一个绘图	Ctrl+Z
擦除所有绘图	E
将屏幕截图复制到剪贴板	Ctrl + C
将屏幕截图裁剪到剪贴板	Ctrl+Shift+C
将屏幕截图另存为 PNG	Ctrl + S
将裁剪的屏幕截图保存到文件	Ctrl+Shift+S
将屏幕区域复制到剪贴板	Ctrl + 6
将屏幕区域保存到文件	Ctrl + Shift + 6
将文本（OCR）从屏幕区域复制到剪贴板	Ctrl + Alt + 6
启动/停止保存为 MP4 或 GIF 的全屏录制（Windows 10 2019 年 5 月更新及更高版本）	Ctrl + 5
裁剪屏幕录制并保存为 MP4 或 GIF（适用于 Windows 10 2019 年 5 月更新及更高版本）	Ctrl + Shift + 5
仅录制鼠标光标所在窗口的屏幕，保存为MP4或GIF（Windows 10 2019年5月更新及更高版本）	Ctrl + Alt + 5
显示倒计时计时器	Ctrl + 3
增加/减少时间	Ctrl + 鼠标向上/向下滚动或箭头键
最小化计时器（而不暂停）	Alt + Tab
最小化时显示计时器	左键单击 ZoomIt 图标
LiveZoom 模式	Ctrl + 4
LiveDraw 模式	Ctrl + Shift + 4
启动 DemoType	Ctrl + 7

函数	快捷键
移回至前一个代码片段 (DemoType)	Ctrl+Shift+7
开始/停止全景录制	Ctrl + 8
前进到下一代码片段（DemoType 用户驱动模式）	空格键
退出	Esc 或右键单击

 **ZoomIt** **(2.4 MB)**

立即 从 Sysinternals Live 运行。

从 Microsoft PowerToys 下载 (GitHub)

Last updated on 2026/03/26

Sysinternals 套件

By Mark Russinovich 更新时间：2026 年 4 月 9 日

下载 Sysinternals Suite（167.8 MB） **下载适用于 Nano Server 的 Sysinternals 套件**（9.6 MB）
下载适用于 ARM64 的 Sysinternals 套件（15.3 MB）
install Sysinternals Suite from the Microsoft Store

介绍

Sysinternals 故障排除实用工具已汇总到单个工具套件中。 此文件包含单独的故障排除工具和帮助文件。 其中不包含 BSOD 屏幕保护程序等非故障排除工具。

此套件是以下精选 Sysinternals 工具的集成包：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、PendMoves、PipeList、PortMon、ProcDump、Process Explorer、Process Monitor、PsExec、PsFile、PsGetSid、PsInfo、PsKill、PsList、PsLoggedOn、PsLogList、PsPasswd、PsPing、PsService、PsShutdown、PsSuspend、PsTools、RAMMap、RDCMan、RegDelNull、RegHide、RegJump、Registry Usage (RU)、SDelete、ShareEnum、ShellRunas、Sigcheck、Streams、Strings、Sync、Sysmon、TCPView、VMMap、VolumeID、WhoIs、WinObj、ZoomIt

---

Last updated on 2026/04/10

Microsoft Store

Sysinternals 套件

版本 2026.4
2026 年 4 月 9 日

Sysinternals Suite 作为 MSIX 捆绑包 从 微软商店 安装。

使用情况

与大多数其他 MSIX 包一样，Sysinternals Suite 按用户安装，但二进制文件存储在安全位置并由用户共享。 图形工具（如进程资源管理器）将添加到Windows“开始”菜单。 从Windows 11开始，它们分组到 Sysinternals Suite 文件夹中（VisualGroup 属性）。

> ⓘ **注意**
>
> Windows 10不支持 MSIX 包的“开始”菜单文件夹，因此工具不会分组到 Sysinternals Suite 文件夹中。

所有可执行文件都可以通过 Windows 应用程序执行别名从路径访问：

txt

```
Microsoft.SysinternalsSuite_8wekyb3d8bbwe

    accesschk.exe       AccessEnum.exe      ADExplorer.exe      ADInsight.exe
    adrestore.exe       Autologon.exe       Autoruns.exe        autorunsc.exe
    Bginfo.exe          Cacheset.exe        Clockres.exe        Contig.exe
    Coreinfo.exe        CPUSTRES.EXE        ctrl2cap.exe        Dbgview.exe
    Desktops.exe        disk2vhd.exe        diskext.exe         Diskmon.exe
    DiskView.exe        du.exe              efsdump.exe         FindLinks.exe
    handle.exe          hex2dec.exe         junction.exe        Listdlls.exe
    livekd.exe          LoadOrd.exe         LoadOrdC.exe        logonsessions.exe
    movefile.exe        notmyfault.exe      notmyfaultc.exe     ntfsinfo.exe
    pendmoves.exe       pipelist.exe        procdump.exe        procexp.exe
    Procmon.exe         PsExec.exe          psfile.exe          PsGetsid.exe
    PsInfo.exe          pskill.exe          pslist.exe          PsLoggedon.exe
    psloglist.exe       pspasswd.exe        psping.exe          PsService.exe
    psshutdown.exe      pssuspend.exe       RAMMap.exe          RDCMan.exe
    RegDelNull.exe      regjump.exe         ru.exe              sdelete.exe
    ShareEnum.exe       ShellRunas.exe      sigcheck.exe        streams.exe
    strings.exe         sync.exe            Sysmon.exe          tcpvcon.exe
```

```
tcpview.exe          Testlimit.exe       vmmap.exe           Volumeid.exe
whois.exe            Winobj.exe          ZoomIt.exe
```

应用执行别名

- 若要查看所有内容，请从Windows搜索或设置中搜索“管理应用执行别名”。
- 它们是 Windows 为 MSIX 包管理的一种特殊类型的重解析点。
- 它们存储在用户配置文件的目录中，该目录位于以下路径中：
  - **%LOCALAPPDATA%\Microsoft\WindowsApps**
- Sysinternals Suite 的完整列表位于以下目录中：
  - **%LOCALAPPDATA%\Microsoft\WindowsApps\Microsoft\SysinternalsSuite_8wekyb3d8bbwe**
  - 查看此处是列出包中所有应用执行别名的方法。
- 卸载 MSIX 包后，将会删除它们。

处理器体系结构

- MSIX 捆绑包包含了适用于 ARM64、x64 和 x86 的单独的包。
- 请仅下载并安装与 OS 匹配的包。
- 打包的可执行文件没有后缀（对于 x64 为“64”，对于 ARM 64 则为“64a”）。
  - 例如，x64 上的 procexp.exe 与未打包的 procexp64.exe 相同。

Last updated on 2026/04/09

Sysinternals 社区

项目 • 2024/01/15

在 Twitter 上关注

- Follow @Sysinternals
- Follow @MarkRussinovich

在 Microsoft Q&A 上搜索和发布问题

Q&A 上的 Windows Sysinternals 提供了越来越多的技术问答存档以供搜索。

Sysinternals 资源

项目 • 2023/08/03

书籍

Windows Internals 书籍
关于 Windows Internals 的权威性书籍的官方更新和勘误页，由 Mark Russinovich 和 David Solomon 编写。

使用 Windows Sysinternals 工具进行故障排除
Mark Russinovich 和 Aaron Margosis 编写的 Sysinternals 实用工具官方指南，其中包含各项工具的说明、其功能、如何使用这些工具进行故障排除，以及它们的实际使用示例。

文章

- 了解 Windows Vista 内核：第一部分
- 了解 Windows Vista 内核：第二部分
- 了解 Windows Vista 内核：第三部分
- 了解 Windows Vista 用户帐户控制
- 深入了解 Windows Server 2008 内核变化

视频与 Web 广播

Sysinternals@25
查找来自这场特别活动的所有视频：

- Fireside Chat with Mark Russinovich （与 Mark Russinovich 进行炉边谈话）
- Sysinternals Overview （Sysinternals 概述）
- Process Explorer Deep Dive （深入了解进程资源管理器）
- Process Monitor Deep Dive （深入了解进程监视器）
- Sysmon Deep Dive （深入了解 Sysmon）
- Autoruns Deep Dive （深入了解 Autoruns）
- ProcDump Deep Dive （深入了解 ProcDump）
- PsTools Deep Dive （深入了解 PsTools）
- Sysinternals for Linux Deep Dive （深入了解 Sysinternals for Linux）

Candid talk from the man behind your favorite Windows tools （来自你喜欢的 Windows 工具的开发人员的坦率演讲）
Mark 与 Larry Seltzer 讨论了 Sysinternals 的历史和未来。

Defrag Tools 节目

Defrag Tools 节目的第 1-12 集重点介绍 Sysinternals 工具。 每一集介绍了在技术支持节目 Defrag 中使用的特定工具，讲解了何时以及为何使用这些工具，并提供了有关任何充分利用这些工具的提示：

- Defrag Tools：1 - 生成 U 盘
- Defrag Tools：2 - 进程资源管理器
- Defrag Tools：3 - 进程监视器
- Defrag Tools：4 - 进程监视器 - 示例
- Defrag Tools：5 - Autoruns 和 MSConfig
- Defrag Tools：6 - RAMMap
- Defrag Tools：7 - VMMap
- Defrag Tools：8 - Mark Russinovich
- Defrag Tools：9 - ProcDump
- Defrag Tools：10 - ProcDump - 触发器
- Defrag Tools：11 - ProcDump - Windows 8 和进程监视器
- Defrag Tools：12 - TaskMgr 和 ResMon

Mark 的网络广播

可按需查看 Mark 关于 Sysinternals、Windows Internals 和 Windows Azure 的 20 几个热门演示。 直接从作者那里获得有关使用 Sysinternals 工具进行故障排除的提示和技巧。

TWC: Sysinternals Primer: TechEd 2014 Edition （TWC：Sysinternals Primer：TechEd 2014 Edition）

Aaron Margosis 讲解热门 Sysinternals Primer 系列的最新版本，他与 Mark Russinovich 合著了《Windows Sysinternals 管理员参考》。 Sysinternals 实用工具是 Windows 平台上所有计算机专业人员的重要工具。 Mark Russinovich 广受欢迎的“无法解释的案例”(Case Of The Unexplained) 介绍了这些工具在高级故障排除场景中的一些功能。 这个教程系列作为补充资料，着重介绍实用工具本身，在时间允许的情况下深入介绍尽可能多的功能。 期待看到一些高级分析（例如使用 Windows PowerShell 操作 Procmon 结果），以及有趣/实用的新功能。

Sysinternals Primer： Autoruns, Disk2Vhd, ProcDump, BgInfo and AccessChk （Sysinternals Primer：Autoruns、Disk2Vhd、ProcDump、BgInfo 和 AccessChk）

Sysinternals 实用工具是 Windows 平台上所有计算机专业人员的重要工具。 Mark Russinovich 广受欢迎的“无法解释的案例”(Case Of The Unexplained) 介绍了这些工具在高级故障排除场景中的一些功能。 这个教程课程作为补充材料，着重介绍使用工具本身，提供了提示和技巧，便于你使用他们的完整工具来进行故障排除和系统管理。 这个课程采用的格式与去年评价颇高的内容相同，课上讲解了一组最有用的 Sysinternals 工具。

Unintended Consequences of Security Lockdowns (uses Sysinternals utilities a lot) （安全锁定的意外结果（大量使用 Sysinternals 实用工具））
注重安全的组织常常会根据 Microsoft、美国联邦政府机构或其他安全组织的规范性指导锁定他们的系统。 有时，这些设置可能会导致令人不快的意外和意想不到的负面影响。 该课程介绍并演示了可能会出现的一些常见问题，以及这些设置实际上在哪些方面提供了帮助或造成了伤害。 不向管理员授予“调试”权限是否有好处？ “隐藏删除区域信息的机制”是否损坏了任何内容？ “需要通过受信任的路径输入凭据”设置所带来的不变是否值得？ 来看看吧！

Windows Sysinternals Primer: Process Explorer, Process Monitor and More （Windows Sysinternals Primer：进程资源管理器、进程监视器等精彩内容）
Sysinternals 实用工具是 Windows 平台上所有计算机专业人员的重要工具。 Mark Russinovich 广受欢迎的“无法解释的案例”(Case Of The Unexplained) 介绍了这些工具在高级故障排除场景中的一些功能。 这个教程课程由 Aaron Margosis 和 Tim Reckmeyer 提供，充当补充材料，它重点介绍这些实用工具，在时间允许的情况下深入介绍尽可能多的功能。 了解可让你更有效地使用 Sysinternals 实用工具的提示和技巧。

新闻稿

Sysinternals 新闻稿存档

Mark 的网络广播

项目 • 2023/08/10

观看来自 TechEd、BUILD 和其他有关 Azure、安全性、Windows 故障排除、恶意软件搜寻的会议中 Mark 广受好评的演讲的免费点播录像。 如果你对这些网络广播中的某个主题有疑问，请访问 Sysinternals 论坛 以获得其他用户和我们的管理员的解答和帮助。

Case of the Unexplained

- The Case of the Unexplained 2016
- 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 的“The Case of...” 博客文章 在他排名第一的 TechEd 活动的网络广播录像中焕发生机。 通过观看 Mark 使用 Sysinternals 和其他高级工具解决实际问题的示例，了解如何排查最棘手的 Windows 和应用程序问题。 请务必查看所有网络广播，因为它们包含完全不同的故障排除示例并演示了不同的技术。

Microsoft Azure

- 下一代 Azure 计算平台 了解与 Azure 资源管理器 (ARM) 集成以启用基于角色的访问控制 (RBAC) 的方法、标记和基于模板的部署，以及与 Docker 兼容的 Windows 容器如何使代码立即部署并在任何环境中统一工作。 另请了解 Service Fabric（Microsoft 的超大规模微服务 PaaS），它为从 Azure DB 到 Cortana 的所有功能提供支持，并为应用程序带来最先进的高密度、高可用性和有状态计算功能。
- Mark Russinovich 和 Mark Minasi 讨论云计算 观看 Mark Russinovich 和 Mark Minasi 进行热烈的讨论，分享他们如何看待云计算带来的颠覆以及它对 IT 专业人员和开发人员的意义。 Mark Russinovich 从领先的 Microsoft Azure 体系结构的角度出发，Mark Minasi 则带来了他的 IT 专业知识和外部观点。
- 公有云安全：在恶意多租户环境中生存 公有云计算的兴起带来了新的一套尚未被广泛理解的安全注意事项。 Mark 以处理公有云安全系统的独特视角描述了公有云服务提供商和云客户面临的威胁，包括恶意内部人员、共享技术、数据泄露和数据丢失。 对于每种情况，他都评估了相应的风险，并探讨了静态加密、传输中加密和其他安全最佳做法等缓解措施的价值，将热度与现实区分开来，以便在组织迁移到云时做出明智的决策。

- Mark Russinovich 和 Mark Minasi 讨论云计算 (https://channel9.msdn.com/events/teched/northamerica/2014/dcim-b386) 观看 Mark Russinovich 和 Mark Minasi 进行热烈的讨论，分享他们如何看待云计算带来的颠覆以及它对 IT 专业人员和开发人员的意义。 Mark Russinovich 从领先的 Microsoft Azure 体系结构的角度出发，Mark Minasi 则带来了他的 IT 专业知识和外部观点。 公有云的经济性、PaaS 和 IaaS 的未来、企业如何将本地环境与云连接起来、你应如何看待公有云中的安全性，以及哪些技能对 IT 专业人员和开发人员很重要，这些只是他们共同探索的一些领域。
- Microsoft Azure 上的基础结构服务：虚拟机和虚拟网络 (https://channel9.msdn.com/events/teched/northamerica/2013/mdc-b212) 此活动概述了新的 Windows Azure 基础结构服务 (IaaS)，包括对 Windows Server 和 Linux 持久性虚拟机的支持、适用于混合应用程序和本地/云连接的新网络功能，以及支持由 PaaS 和 IaaS 角色组成的应用程序。 Mark 介绍了 IaaS 如何融入到 Windows Azure 中以将现有服务器应用程序扩展到云，并演示 IaaS VM 部署和复杂的多 VM 应用程序。
- Microsoft Azure Internals Mark Russinovich 深入介绍了 Microsoft 数据中心操作系统。 面向已经具备 Windows Azure 实操经验并了解其基本概念的开发人员，此活动将深入探讨 Windows Azure 计算平台的体系结构设计。 了解 Microsoft 的数据中心体系结构、部署和更新 Windows Azure 应用时的幕后情况，以及它如何监视和响应计算机、它自己的组件及其托管的应用的运行状况。
- Microsoft Azure 简介：云操作系统 加入 Mark Russinovich，了解 Microsoft 的新云 OS 的总体情况。 此活动面向对 Windows Azure 没有先前知识的观众，它将首先介绍 Windows Azure 平台即服务 (PaaS) 应用理念，以及它与传统服务器应用的区别。 然后，它会通过构建并部署到云的真实 Windows Azure 服务演示关键概念，介绍 Windows Azure 服务模型，包括更新和容错域等概念。 最后，该活动将讨论不同的服务更新选项，并详细说明 Windows Azure 在检测到服务或硬件设备出现故障时遵循的恢复步骤。
- 走进 Microsoft Azure：云操作系统 Mark Russinovich 深入探讨了 Microsoft 的新云 OS。 面向已经具备 Windows Azure 实操经验并了解其基本概念的开发人员，此活动将深入探讨 Windows Azure 的计算平台的体系结构设计。 你将了解 Microsoft 的数据中心体系结构、部署和更新 Windows Azure 应用时的幕后情况，以及它如何监视和响应计算机、它自己的组件及其托管的应用的运行状况。
- Channel9：MarkRussinovich：Microsoft Azure、云操作系统和平台即服务 Mark 介绍了他在 Windows Azure 团队中的工作、为什么全球都要迁移到云、平台即服务 (PaaS) 的含义以及 Windows Azure 如何交付 PaaS。

Windows Internals

- Tech-Ed 北美 2011：Windows 内存管理的奥秘揭示，第 1 部分 (https://channel9.msdn.com/events/teched/northamerica/2011/wcl405) [Tech-Ed

北美 2011：Windows 内存管理的奥秘揭示，第 2 部分（https://channel9.msdn.com/events/teched/northamerica/2011/wcl406) 如果你想了解系统提交的内存和进程提交的内存之间的区别，想知道任务管理器显示的所有内存数字的真正含义，或者想要深入了解进程的内存相关的影响，那么这个讲座很适合你。 在这个北美 2011 点播网络广播中观看 Mark 的演讲。

- Pushing the Limits of Windows（https://channel9.msdn.com/events/teched/europe/2009/cli402) 观看 Mark 解释 Windows 在对象句柄、虚拟内存和物理内存方面的限制。 在此过程中，他解释了这些限制从何而来以及如何监视应用程序，以便在它们接近上限时收到警报，进而调整系统大小以满足其资源需求。
- 走进 Windows Server 2008R2 虚拟化和 VHD 改进（https://channel9.msdn.com/events/teched/northamerica/2009/vir401) Mark 帮助你深入了解新的 Windows 虚拟化和 VHD 功能，包括实时 VM 迁移、核心停放和计时器合并、虚拟机监控程序电源管理支持以及新的硬件辅助来宾内存管理。 他通过从 VHD 启动的 Windows 安装来完成整个演示，向你介绍 Windows 如何实现本机 VHD 堆栈，以及启动体系结构进行了怎样的更改来适应从 VHD 映像的启动。
- Channel9：Mark Russinovich 走进 Windows 7 Mark 谈论了 Windows 7 和 Windows Server 2008R2 中的内核更改，包括计划程序的调度程序锁的移除、支持多达 256 个 CPU、从 VHD 启动、MinWin、核心停放以节省电源等。
- Channel9：Mark Russinovich：走进 Windows 7 Redux 在对上一篇走进 Windows 7 相关讨论的后续补充中，Mark 深入系统内部探讨 Windows 7 的细节（其累积效应有助于使 Windows 7 Microsoft 成为迄今为止最可靠、最可缩放且最高效的通用操作系统）。
- Channel9：Mark 讨论了在 Microsoft 工作、Windows Server 2008 的内核、MinWin vs ServerCore 和 Hyper-V Channel 9 与技术研究员和 Sysinternals 创始人 Mark Russinovich 畅聊，深入探讨了 Windows Server 2008 内核中的新增功能。 当然，我们还讨论了许多内容，包括 HyperV、应用程序虚拟化、内核体系结构等。

安全

- TWC：传递哈希：攻击者如何扩散以及如何阻止他们 传递哈希可将一台计算机的漏洞转化为整个基础结构的破坏。 攻击的发布以及应对工具的缺乏迫使企业依赖于繁重和无效的技术。 在此活动中，我们将解构 PtH 威胁，展示攻击的执行方式，以及如何使用 Windows 中最近推出的新特性和功能来应对攻击。
- TWC：Mark Russinovich 和 Sysinternals 工具与恶意软件搜寻 Mark 概述了多个 Sysinternals 工具，包括进程监视器、进程资源管理器和 Autoruns，重点介绍可用于恶意软件分析和删除的功能。 这些实用工具支持对进程、文件系统和注册表活动以及自动启动执行点进行深入检查和控制。 他演示了它们的恶意软件搜寻功能，包括一些最新、真实的恶意软件示例，并使用这些工具来识别和清理恶意软件。

- License to Kill：使用 Sysinternals 工具进行恶意软件搜寻 此活动概述了多个 Sysinternals 工具，包括进程监视器、进程资源管理器和 Autoruns，重点介绍可用于恶意软件分析和删除的功能。 这些实用工具支持对进程、文件系统和注册表活动以及自动启动执行点进行深入检查和控制。 你将通过使用这些工具识别和清理恶意软件的多个真实案例来了解它们的恶意软件搜寻功能，最后的环节是对 Stuxnet 感染的系统影响的实时分析。
- Zero Day: A Non-Fiction View 在这个他备受欢迎的 RSA 会议演讲的 20 分钟简短版中，Mark 提到，他的畅销网络惊悚小说《ZeroDay》很可能以非虚构的形式实现。
- 使用 Sysinternals 工具清除零日恶意软件 来自 Mark 广受好评的 Blackhat US 2011 演示的幻灯片展示了如何使用 Sysinternals 工具来搜寻和消除恶意软件。
- Channel9：Mark 谈论 Windows 安全和核心体系结构 观看 Mark 的 Channel 9 采访，他在其中谈到了他如何创办 Windows Internals、Windows Vista 中新的安全功能、用户帐户控制，以及他在 Microsoft 所做的工作。

碎片整理工具

- Defrag Tools Shows *Defrag Tools* 节目的第 1 - 12 集重点介绍 Sysinternals 工具。每一集介绍了在技术支持节目 Defrag 中使用的特定工具，讲解了何时以及为何使用这些工具，并提供了有关任何充分利用这些工具的提示：
  - Defrag Tools：#1 - 生成 U 盘
  - Defrag Tools：#2 - 进程资源管理器
  - Defrag Tools：#3 - 进程监视器
  - Defrag Tools：#4 - 进程监视器 - 示例
  - Defrag Tools：#5 - Autoruns 和 MSConfig
  - Defrag Tools：#6 - RAMMap
  - Defrag Tools：#7 - VMMap
  - Defrag Tools：#8 - Mark Russinovich
  - Defrag Tools：#9 - ProcDump
  - Defrag Tools：#10 - ProcDump - 触发器
  - Defrag Tools：#11 - ProcDump - Windows 8 & 进程监视器
  - Defrag Tools：#12 - TaskMgr 和 ResMon

Windows 内部书籍

项目 • 2023/08/04

Windows 内部书籍第 7 版 (第 1 部分) 介绍了 Windows 10 和 Windows Server 2016 的体系结构和核心内部机制。 这本书有助于：

- 了解 Windows 系统体系结构及其常规组件
- 使用内核调试程序等工具浏览内部数据结构
- 了解 Windows 如何使用进程进行管理和隔离
- 了解和查看线程计划以及如何管理 CPU 资源
- 深入了解 Windows 安全模型，包括安全风险缓解的最新进展
- 了解 Windows 如何管理虚拟和物理内存
- 了解 I/O 系统如何管理物理设备和设备驱动程序

第 7 版由 Pavel Yosifovich、Alex Ionescu、Mark Russinovich 和 David Solomon 撰写。 自第 6 版（涵盖 Windows 7 和 Windows Server 2008 R2）以来，添加了新材料。

第 7 版第 2 部分（由 Andrea Allievi、Mark E. Russinovich、Alex Ionescu 和 David A. Solomon 撰写）现已出版，为第 7 版第一部分缺失的主题提供了宝贵资源。 其中包括启动流程、新存储技术以及 Windows 系统和管理机制。

第 7 版目录，第 1 部分：

- 第 1 章：概念和工具
- 第 2 章：系统体系结构
- 第 3 章：流程和作业
- 第 4 章：线程
- 第 5 章：内存管理
- 第 6 章：I/O 系统
- 第 7 章：安全性

本书可在 Microsoft Press 网站上购买（第 7 版第 1 部分；第 7 版，第 2 部分）。

书籍历史

这是由 Helen Custer 撰写、原名为《Inside Windows NT》（Microsoft Press，1992 年）书籍 （在 Microsoft Windows NT 3.1 首次发布之前）的第七版。 《Inside Windows NT》是有史以来出版的第一本关于 Windows NT 的书籍，提供了对系统体系结构和设计的关键见解。 《Inside Windows NT》第二版（Microsoft Press，1998 年）由 David Solomon 撰写。 它更新了原书，涵盖了 Windows NT 4.0，并大幅度提高了技术深度。

《Inside Windows 2000》，第三版（Microsoft Press，2000 年）由 David Solomon 和 Mark Russinovich 撰写。 其加入了许多新主题，如启动和关闭、服务内部机制、注册表内部机制、文件系统驱动程序和网络。 它还涵盖了 Windows 2000 中的内核更改，如 Windows 驱动模型 (WDM)、即插即用、电源管理、Windows Management Instrumentation (WMI)、加密、作业对象和终端服务。 《Windows 内部书籍》第四版是 Windows XP 和 Windows Server 2003 的更新，增加了更多内容，聚焦于帮助 IT 专业人员利用其对 Windows 内部机制的了解，例如使用 Windows Sysinternals 中的关键工具和分析故障转储。

《Windows 内部书籍》第五版是 Windows Vista 和 Windows Server 2008 的更新。 它见证了 Mark Russinovich 在 Microsoft（他现在是 Azure CTO）的职位转为全职工作，并增加了一位新的合著者 Alex Ionescu。 新内容包括映像加载器、用户模式调试设备、Advanced Local Procedure Call (ALPC) 和 Hyper-V。 下一版本，《Windows 内部书籍》第六版进行了全面更新，以解决 Windows 7 和 Windows Server 2008 R2 中的许多内核更改，并进行了许多新实践试验，以反映工具中的更改。

第七版更改

自本系列上次更新以来，Windows 已经发布了多个版本，即将发布 Windows 10 和 Windows Server 2016。 Windows 10 本身，作为 Windows 目前的未来名称，自最初发布到发布-生产 (RTM) 以来，已经发布了几个版本，每个版本都标有 4 位数版本号，表示发布的年份和月份，例如 2017 年 3 月完成的 Windows 10 1703 版。 以上内容表明，自 Windows7 以来，Windows 至少经历了 6 个版本。 从 Windows 8 开始，Microsoft 开始了操作系统融合的过程，这对开发和 Windows 工程团队本身都是有益的。 Windows 8 和 Windows Phone 8 已收敛内核，新式应用收敛出现在 Windows 8.1 和 Windows Phone 8.1 中。 Windows 10 的收敛已完成，它运行在桌面设备/笔记本电脑、服务器、XBOX One、手机 (Windows Mobile 10)、HoloLens 和各种物联网 (IoT) 设备上。 随着这一大统一的完成，就是时候推出该系列的新版本了，它现在终于可以赶上近五年的变化，在未来将是更加稳定的内核体系结构。 因此，这本最新的书籍涵盖了 Windows 的各个方面，从 Windows 8 到 Windows 10，版本 1703。 此外，本版加入了 Pavel Yosifovich 作为新的合著者。

书籍工具

有几个工具是专门为这本书编写的，它们在 WindowsInternalsGitHub 存储库 中提供了完整源代码。

Troubleshooting with the Windows Sysinternals Tools

项目 • 2023/08/09

《An update to Windows Sysinternals Administrator's Reference》
作者：Mark Russinovich 和 Aaron Margosis
《Troubleshooting with the Windows Sysinternals Tools》是介绍 Sysinternals 工具的官方书籍，由工具作者兼 Sysinternals 联合创始人 Mark Russinovich 和 Windows 专家 Aaron Margosis 撰写。 该书详细介绍了 65 种以上的工具，并用完整章节介绍进程资源管理器、进程监视器和自动运行等主要工具。 该书除了在工具章节中介绍提示和技巧外，它还针对用户使用的工具添加了 45 个"案例中无法解释的..."示例，以用于解决实际问题。 立即购买该书，将你的 Windows 故障排除和系统管理技能提升到一个新的水平。

订购书籍

可以从以下在线零售商那里购买该书：

- Microsoft Press Store
- Amazon
- Barnes & Noble
- 独立书商 – Shop local

还可以通过 O'REILLY Media 在线阅读。

书籍说明

IT 专业人员和高级用户认为免费的 Windows Sysinternals 工具对于诊断、故障排除和深入了解 Windows 平台不可或缺。 在此大幅更新的指南中，Sysinternals 创建者 Mark Russinovich 和 Windows 专家顾问 Aaron Margosis 会帮助你使用这些功能强大的工具来优化任何 Windows 系统的可靠性、效率、性能和安全性。 作者首先介绍了 Sysinternals 的功能，并帮助你快速入门。 接下来，他们深入介绍每个主要工具，从进程资源管理器和进程监视器到 Sysinternals 的安全和文件实用工具。 然后，基于这些知识，他们展示了用于解决实际案例的工具，这些案例涉及错误消息、挂起、迟缓和恶意软件感染等。

Windows Sysinternals 创建者 Mark Russinovich 和 Aaron Margosis 向你展示如何：

- 使用进程资源管理器显示详细的进程和系统信息
- 使用进程监视器捕获低级别的系统事件，并快速筛选输出以缩小根本原因范围
- 列出、分类和管理在启动或登录计算机时或者运行 Microsoft Office 或 Internet Explorer 时运行的软件

- 验证文件、正在运行的程序以及这些程序中加载的模块的数字签名
- 使用可识别和清理恶意软件侵袭的自动运行、进程资源管理器、Sigcheck 和进程监视器功能
- 检查对文件、密钥、服务、共享和其他对象的权限
- 使用 Sysmon 监视网络中与安全相关的事件
- 当进程满足指定条件时生成内存转储
- 远程执行进程，并关闭远程打开的文件
- 管理 Active Directory 对象和跟踪 LDAP API 调用
- 捕获有关处理器、内存和时钟的详细数据
- 排查设备无法启动、使用中的文件错误、无法解释的通信和许多其他问题
- 了解其他地方没有详细记载的 Windows 核心概念

示例章节

可以通过此 Amazon.com 链接 阅读书籍中的示例。

目录

- 第 20 章 恶意软件
- 第 21 章 了解系统行为
- 第 22 章 开发人员故障排除

错误

请参阅 Microsoft Press 网站 上的“勘误表和更新”选项卡&

内部本机应用程序

项目 • 2023/08/03

Mark Russinovich 发布时间：2006 年 11 月 1 日

简介

如果你对 NT 的体系结构有一些熟悉，你可能知道 Win32 应用程序使用的 API 不是“真正的”NT API。 NT 的操作环境（包括 POSIX、OS/2 和 Win32）通过自己的 API 与其客户端应用程序通信，但使用 NT“本机”API 与 NT 通信。 本机 API 大多是没有记录的，Windows NT 设备驱动程序工具包中只介绍了其 250 个函数中的约 25 个。

但大多数人不知道的是，NT 上的“本机”应用程序不是任何操作环境的客户端。 这些程序使用本机 NT API，不能使用 Win32 等操作环境 API。 为什么需要此类程序“在启动 Win32 子系统之前必须运行的任何程序（登录框出现时）必须是本机应用程序。 本机应用程序最明显的示例是在初始化蓝屏期间运行 chkdsk 的“autochk”程序， （即在屏幕上打“.”的程序）。 当然，Win32 操作环境服务器 CSRSS.EXE（客户端-服务器运行时子系统）也必须是本机应用程序。

在本文中，我将介绍本机应用程序的生成方式及其工作原理。

Autochk 如何得到执行

Autochk 在加载 NT 的启动和系统启动驱动程序之间以及打开分页时运行。 此时，启动序列会话管理器 (smss.exe) 正在将 NT 的用户模式环境关闭，并且没有其他程序处于活动状态。 **HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute** 值（MULTI_SZ）包含由会话管理器执行的程序的名称和参数，是指定 Autochk 的位置。 如果查看此值，通常会发现以下内容，其中“Autochk”作为参数传递“*”：

```
Shell

Autocheck Autochk *
```

会话管理器 在 <winnt>\system32 目录中查找此值中列出的可执行文件。 Autochk 运行时，不会打开任何文件，因此 *Autochk* 可以在原始模式下打开任何卷（包括启动驱动器），并操作其磁盘上的数据结构。 这在以后的任何时间点都不可能实现。

生成本机应用程序

Microsoft 不会记录它，但 NT DDK 生成实用工具知道如何使本机应用程序（且可能将其用于编译 *Autochk*）。 可以在定义应用程序的 SOURCES 文件中指定信息，这与对设备驱动程序执行的操作相同。 但是，在 SOURCES 文件中需要一个本机应用程序，而不是指示生成需要驱动程序，如下所示：

```
Shell

TARGETTYPE=PROGRAM
```

生成 实用工具使用标准生成文件来指导 \ddk\inc\makefile.def，它在编译本机应用程序时查找名为 nt.lib 的运行时库。 遗憾的是，Microsoft 不会将此文件与 DDK 一起交付（它包含在 Server 2003 DDK 中，但我怀疑，如果你链接到该版本，本机应用程序将无法在 XP 或 Windows 2000 上运行）。 但是，可以通过在 makefile.def 中包含一行来解决此问题，该行通过指定 Visual C++ 的运行时库 msvcrt.lib 替代 nt.lib 的选择

如果在 DDK 的“已检查生成”环境中运行 *生成* ，它将在 %BASEDIR%\lib%CPU%\Checked（例如c:\ddk\lib\i386\checked\native.exe）下生成具有完整调试信息的本机应用程序，如果在“免费生成”环境中调用它，则程序的发布版本最终将位于 %BASEDIR%\lib%CPU%\Free 中。 这些位置与设备驱动程序映像通过生成放置的位置相同。

本机应用程序具有“.exe”文件扩展名，但无法像运行 Win32 .exe 一样运行它们。 如果尝试，你将收到以下消息：

应用程序不能在 Windows NT 模式下运行。

在本机应用程序内

本机应用程序的入口点不是 **winmain** 或 **main**，而是 **NtProcessStartup**。 与其他 Win32 入口点不同，本机应用程序必须访问作为唯一参数传递的数据结构，才能找到命令行参数。

本机应用程序的大多数运行时环境都由 NT 的本机 API 导出库 NTDLL.DLL 提供。 本机应用程序必须使用 NTDLL 函数 **RtlCreateHeap** 创建自己的堆，以便从中分配存储。 内存通过 **RtlAllocateHeap** 从堆分配，并使用 **RtlFreeHeap** 释放。 如果本机应用程序希望在屏幕上打印某些内容，则必须使用函数 **NtDisplayString**，该函数将输出到初始化蓝屏。

本机应用程序不会像 Win32 程序一样简单地从其启动函数返回，因为没有要返回到的运行时代码。 相反，它们必须通过调用 **NtProcessTerminate** 来终止自身。

NTDLL 运行时由数百个函数组成，这些函数允许本机应用程序执行文件 I/O、与设备驱动程序交互以及执行进程间通信。 不幸的是，正如我前面所指出的，这些函数中的绝大多数都是没有记录的。

Sysinternals 新闻稿存档

项目 • 2023/08/03

- 第 1 卷
  - 第 1 期 - 1999 年 4 月 14 日
  - 第 2 期 - 1999 年 5 月 15 日
  - 第 3 期 - 1999 年 6 月 19 日
  - 第 4 期 - 1999 年 8 月 5 日
  - 第 5 期 - 1999 年 10 月 12 日
- 第 2 卷
  - 第 1 期 - 2000 年 1 月 6 日
  - 第 2 期 - 2000 年 3 月 27 日
  - 第 3 期 - 2000 年 6 月 14 日
  - 第 4 期 - 2000 年 8 月 30 日
  - 第 5 期 - 2000 年 11 月 30 日
- 第 3 卷
  - 第 1 期 - 2001 年 4 月 18 日
  - 第 2 期 - 2001 年 8 月 20 日
- 第 4 卷
  - 第 1 期 - 2002 年 1 月 7 日
  - 第 2 期 - 2002 年 8 月 12 日
  - 第 3 期 - 2002 年 10 月 16 日
- 第 5 卷
  - 第 1 期 - 2003 年 2 月 19 日
  - 第 2 期 - 2003 年 6 月 23 日
- 第 6 卷
  - 第 1 期 - 2004 年 4 月 27 日
  - 第 2 期- 2004 年 7 月 30 日
- 第 7 卷
  - 第 1 期 - 2005 年 1 月 5 日
  - 特殊公告 - 2005 年 4 月 11 日
  - 第 2 期 - 2005 年 8 月 24 日
- 第 8 卷
  - 第 1 期 - 2006 年 3 月 2 日
  - 第 2 期，Sysinternals 站点迁移 - 2006 年 10 月 30 日
  - 第 3 期，Sysinternals TechCenter - 2006 年 11 月 6 日
  - 第 4 期，网站更新 - 2006 年 11 月 8 日

Sysinternals 软件许可条款

项目 • 2023/08/04

这些许可条款是 Sysinternals（Microsoft Corporation 的全资子公司）和你之间的协议。 请阅读条款内容。 它们适用于从 technet.microsoft.com/sysinternals 下载的软件，其中包括接收该软件的媒介（如有）。 条款也适用于任何 Sysinternals

- 更新、
- 补充、
- 基于 Internet 的服务,
- 并支持服务

除非这些项目附带有其他条款。 如果确实附带有其他条款，则应遵守其他条款。

使用该软件即表示接受这些条款。 如果您不接受这些条款，请不要使用该软件。

如果你遵守这些许可条款，你将拥有以下权利。

安装和使用权利

您可以在您的设备上安装和使用该软件任意数量的副本。

许可范围

软件只授予使用许可，而非出售。 本协议只授予您使用该软件的某些权利。 Sysinternals 保留所有其他权利。 除非适用法律赋予您此项限制之外的权利，否则您只能在本协议明示规定的范围内使用该软件。 在按规定使用该软件时，您必须遵守软件中的所有技术限制，这些限制只允许您以特定方式使用该软件。 您不得

- 绕过该软件中的任何技术限制；
- 对该软件进行反向工程、反编译或反汇编；尽管有此项限制，但如果适用法律明示允许上述活动，则仅在适用法律明示允许的范围内从事上述活动不在此限；
- 制作超过本协议所规定或适用法律（尽管有此项限制）所允许数量的该软件的副本；
- 发布该软件供他人复制；
- 出租、租赁或出借该软件；
- 将该软件或本协议转让给任何第三方；或
- 使用该软件提供商业软件托管服务。

Sensitive Information

请注意，与捕获“进程状态”信息的其他调试工具类似，由 Sysinternals 工具保存的文件可能包括个人可识别或其他敏感信息（如用户名、密码、访问文件的路径和访问注册表的路径）。 使用本软件即表示你已了解到这一点，并对通过使用本软件向 Microsoft 或任何其他方提供的任何个人身份或其他敏感信息承担全部责任。

数据收集

Sysinternals 工具不收集任何数据。 请参考 Microsoft 隐私声明 。

文档

任何对您的计算机或内部网络拥有有效访问权的人都可以出于内部参考目的复制和使用文档。

出口限制

该软件受美国出口法律和法规的约束。 您必须遵守适用于该软件的所有国内和国际出口法律和法规。 这些法律包括对目的地、最终用户和最终用途的各种限制。 有关其他信息，请访问 www.microsoft.com/exporting 。

支持服务

因为此软件按“原样”提供，我们可能不会为它提供支持服务。

完整协议

本协议以及您使用的补充、更新、基于 Internet 的服务和支持服务的有关条款，共同构成了该软件和支持服务的完整协议。

适用的法律

美国 。 如果你在美国购买该软件，则对本协议的解释以及由于违反本协议而引起的索赔均以华盛顿州法律为准并受其管辖，而不考虑冲突法原则。 您所居住的州的法律管辖所有其他索赔项目，包括根据州消费者保护法、不正当竞争法、以及侵权法提出的相关索赔。

美国以外 。 如果您在任何其他国家/地区购买该软件，则您所在国家/地区的法律适用。

法律效力

本协议规定了某些合法权利。 根据您所在国家/地区的法律规定，您可能享有其他权利。 您还可能享有与您的软件卖方相关的权利。 如果您所在国家/地区的法律不允许本协议改变您所在国家/地区法律赋予您的权利，则本协议将不改变您按照所在国家/地区的法律应享有的权利。

免责声明

软件按"原样"授予许可。使用该软件的风险需要你自己承担。 Sysinternals 不提供任何明示担保、保障或条件。 根据您当地的法律，您可能享有本协议无法改变的其他消费者权利。 在你当地法律允许的范围内，sysinternals 排除有关适销性、针对特定目的的适用性和不侵权的默示担保。

损害和赔偿责任的限制和排除

只能因直接损害从 sysinternals 及其供应商处获得退款，退款金额上限为 $5.00。 您不能因其他任何损害获得退款，包括后果性损害、利润损失、特别的损害、间接损害或附带性损害。

该限制适用于

- 与第三方 Internet 站点上或第三方程序中的软件、服务、内容（包括代码）相关的任何情况；以及
- 在适用法律允许的范围内，因违约、违反担保、保证或条件、严格责任、过失或其他侵权行为引起的索赔。

即使 Sysinternals 知道或应该知道可能会出现损害，此项限制也同样适用。 由于您所在国家/地区可能不允许排除或限制附带的、后果性的或其他损害赔偿责任，上述限制和排除可能不适用于您。

发行说明：由于此软件在加拿大魁北克分发，因此本协议的某些条款同时以法语提供如下。

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 许可常见问题解答

常见问题解答

发布日期：2009 年 9 月 28 日

我可以在我公司拥有的计算机上自由加载或使用 Sysinternals 实用工具的多少个副本吗?

你可不限次数地在你的设备或你支持的设备上安装和使用该软件。

我可以在我的软件中、我的网站上或通过我的杂志分发 Sysinternals 实用工具?

不是。 我们不提供任何分发许可证，即使第三方免费分发它们也是如此。 我们鼓励用户从我们的下载中心下载实用工具，在这里他们可以获得最新版本的实用工具。

我是否可以许可或重复使用任何 Sysinternals 源代码?

不是。 我们将不再提供用于下载或许可的 Sysinternals 源代码。

Sysinternals 工具是否继续免费提供?

是，Microsoft 没有移除这些工具或对其收费的计划。

是否向 Sysinternals 工具提供了技术支持?

不是。 所有 Sysinternals 工具都“按原样”提供，没有 Microsoft 官方支持。 我们维护着一个 Sysinternals 专属社区支持论坛：https://forum.sysinternals.com/ 。