

深入解析Windows操作系统（第6版） 下册



[深入解析Windows操作系统（第6版） 下册_下载链接1](#)

著者:【美】 Mark Russinovich

出版者:电子工业出版社

出版时间:2018-4

装帧:

isbn:9787121336430

《深入解析Windows操作系统（第6版）下册》是关于Windows操作系统原理的最新著作，全面深入地阐述了Windows操作系统的整体结构及内部工作细节。《深入解析Windows操作系统（第6版）下册》针对Windows 7、Windows Server 2008 R2

做了全面更新，通过许多练习实验让你直接感受到Windows的内部行为。另外，《深入解析Windows操作系统（第6版）下册》还介绍了一些高级诊断技术，以便使系统运行得更加平稳和高效。无论你是开发人员还是系统管理员，都可以在本书中找到一些关键的、有关体系结构方面的知识，从而更好地做系统设计、调试和性能优化。

《深入解析Windows操作系统（第6版）下册》适合广大Windows平台开发人员、IT专业从业人员阅读。

作者介绍:

Mark Russinovich is a Technical Fellow in the Windows Azure™ group at Microsoft. He is coauthor of Windows SysInternals Administrator's Reference, co-creator of the Sysinternals tools available from Microsoft TechNet, and coauthor of the Windows Internals book series.

David A. Solomon is coauthor of the Windows Internals book series and has taught his Windows internals class to thousands of developers and IT professionals worldwide, including Microsoft staff. He is a regular speaker at Microsoft conferences, including TechNet and PDC.

Alex Ionescu is a chief software architect and consultant expert in low-level system software, kernel development, security training, and reverse engineering. He teaches Windows internals course with David Solomon, and is active in the security research community.

目录: 第8章 I/O系统 1

8.1 I/O系统组件 1

I/O管理器 3

典型的I/O处理过程 4

8.2 设备驱动程序 5

设备驱动程序的类型 5

WDM驱动程序 6

分层的驱动程序 7

实验：查看已加载的驱动程序列表 9

驱动程序的结构 11

驱动程序对象和设备对象 13

实验：看一看设备对象 15

实验：显示驱动程序和设备对象 17

打开设备 18

实验：查看设备句柄 21

实验：查看Windows设备名称之间的映射 23

8.3 I/O处理 24

I/O类型 24

同步I/O和异步I/O 24

快速I/O 25

实验：查看一个驱动程序登记的快速I/O例程 25

映射文件I/O和文件缓存 26

分散/聚集I/O 27

I/O请求包 27

IRP栈单元 28

实验：查看驱动程序的分发例程 29

实验：查看一个线程的未完成IRP 29
IRP缓冲区管理 30
针对单层驱动程序的I/O请求 32
为一个中断提供服务 33
完成一个I/O请求 34
同步 36
针对分层的驱动程序的I/O请求 38
实验：查看一个设备栈 39
实验：查看IRP 40
线程无关I/O 45
I/O取消 45
用户发起的I/O取消 46
线程终止时的I/O取消 47
实验：调试一个无法被杀死的进程 48
I/O完成端口 49
IoCompletion对象 50
使用完成端口 50
I/O完成端口操作 52
I/O优先级支持 54
I/O优先级 54
优先化策略 55
I/O优先级反转的避免（I/O优先级继承） 57
I/O优先级提升和撞升 57
实验：“非常低”和“正常” I/O吞吐量的对比 58
实验：I/O优先级提升/撞升的性能分析 59
带宽预留（计划的文件I/O） 60
容器通知 60
驱动程序检验器（Driver Verifier） 61
8.4 内核模式驱动程序框架（KMDF） 63
KMDF驱动程序的结构和操作 64
实验：显示KMDF驱动程序 65
KMDF数据模型 66
KMDF的I/O模型 69
8.5 用户模式驱动程序框架（UMDF） 72
8.6 即插即用（PnP）管理器 76
即插即用支持的级别 77
驱动程序对于即插即用的支持 77
驱动程序加载、初始化和安装 79
Start值 80
设备列举 81
实验：将设备树转储出来 84
设备栈 85
设备栈的驱动程序加载 86
实验：在设备管理器中查看详细的devnode信息 88
驱动程序安装 90
实验：检查一个驱动程序的INF文件 92
实验：查看目录（catalog）文件 93
8.7 电源管理器 94
电源管理器的操作 96
驱动程序的电源操作 97
实验：查看一个驱动程序的电源映射关系 97
实验：查看系统的电源能力和策略 98
驱动程序和应用程序对于设备电源的控制 100
电源可用性请求 100

实验：在调试器中查看一个电源可用性请求 101
实验：利用Powercfg查看电源可用性请求 103
处理器电源管理（PPM） 103
核心停运的策略 104
利用率函数 105
实验：查看利用率和频率的信息 106
实验：查看利用率和频率的历史 107
算法覆盖 108
增加/减少动作 108
各种阈值和策略的设置 109
实验：查看当前的核心停运策略 111
“性能检查”算法 112
实验：查看当前的PPM检查信息 116
8.8 本章总结 118
第9章 存储管理 119
9.1 有关存储的术语 119
9.2 磁盘设备 120
旋转磁盘 120
磁盘的扇区格式 120
固态硬盘 122
NAND型闪存 122
文件的删除和irim命令 124
9.3 磁盘驱动程序 125
Winload 125
磁盘类、端口和小端口驱动程序 126
iSCSI驱动程序 127
多路径I/O（MPIO）驱动程序 128
实验：观察物理磁盘I/O 130
磁盘设备对象 130
分区管理器 131
9.4 卷的管理 132
基本磁盘 133
MBR风格的分区 133
GPT（GUID分区表）分区方案 133
基本磁盘卷管理器 134
动态磁盘 135
LDM数据库 135
实验：使用LDMDump来查看LDM数据库 137
LDM和GPT或MBR风格的分区方案 139
动态磁盘的卷管理器 140
多分区卷的管理 140
跨距卷 141
条带卷 142
实验：观察镜像卷的I/O操作 143
RAID-5卷 145
卷名字空间 145
挂载管理器 146
挂载点 147
卷的挂载 148
实验：查看VPB 149
卷的I/O操作 152
虚拟磁盘服务 153
9.5 虚拟硬盘（VHD文件）支持 155
附载VHD的操作 156

- 嵌套的文件系统 156
- 9.6 BitLocker驱动器加密 157
 - 加密密钥 159
 - 可信平台模块 (TPM) 161
 - BitLocker引导过程 163
 - BitLocker密钥的恢复 165
 - 全卷加密驱动程序 166
 - BitLocker的管理 167
 - BitLocker To Go 168
- 9.7 卷影像 (shadow) 拷贝服务 170
 - 影像拷贝 170
 - “克隆”影像拷贝 170
 - “写时复制”影像拷贝 170
 - VSS的架构 170
 - VSS的操作 171
 - 影像拷贝提供者 172
 - 实验：查看Microsoft影像拷贝提供者的过滤型设备对象 173
 - Windows中的用途 174
 - 备份 174
 - 实验：查看影像卷的设备对象 174
 - “之前的版本”和系统还原 175
 - 实验：导航到“之前的版本” 176
 - 实验：映射卷影像设备对象 177
- 9.8 本章总结 178
- 第10章 内存管理 179
 - 10.1 内存管理器简介 179
 - 内存管理器组件 180
 - 内部同步 181
 - 检查内存的使用情况 182
 - 实验：查看系统内存信息 182
 - 10.2 内存管理器提供的服务 184
 - 大页面和小页面 185
 - 保留页面和提交页面 187
 - 实验：保留的页面对比提交的页面 188
 - 提交限额 190
 - 锁住内存 190
 - 分配粒度 191
 - 共享内存和映射文件 192
 - 实验：查看内存映射文件 193
 - 保护内存 194
 - “不可执行”页面保护 196
 - 实验：查看进程上的DEP保护 199
 - 软件的数据执行保护 200
 - 写时复制 201
 - 地址窗口扩展 203
 - 10.3 内核模式堆 (系统内存池) 204
 - 内存池的大小 205
 - 实验：确定最大的池大小值 206
 - 监视内存池的使用 208
 - 实验：诊断内存池泄漏 210
 - 快查表 (Look-Aside List) 211
 - 实验：查看系统的快查表 212
 - 10.4 堆管理器 212
 - 堆的类型 213

- 堆管理器结构 214
- 堆同步 215
- 低碎片堆 215
- 堆的安全特性 216
- 堆的调试特性 217
- pageheap 218
- 容错堆 218
- 10.5 虚拟地址空间的布局结构 219
- x86地址空间的布局结构 221
- 实验：检查一个应用程序能否感知大地址空间 222
- x86系统地址空间的布局结构 223
- x86会话空间 224
- 实验：查看会话 224
- 实验：查看会话空间的使用情况 225
- 系统页表项（PTE，Page Table Entry） 226
- 实验：查看会话空间的使用情况 226
- 64位地址空间布局结构 227
- x64虚拟寻址的限制 230
- Windows x64的16TB限制 231
- 动态的系统虚拟地址空间管理 233
- 实验：查询系统虚拟地址的用量 234
- 实验：设置系统虚拟地址的限制值 235
- 系统的虚拟地址空间配额 236
- 用户地址空间的布局结构 237
- 实验：对用户虚拟地址空间进行分析 238
- 映像随机化 239
- 栈的随机化 240
- 堆的随机化 240
- 内核地址空间中的ASLR 240
- 对安全性缓和措施的控制 240
- 实验：查看进程上的ASLR保护 241
- 10.6 地址转译 241
- x86虚拟地址转译 242
- 页目录 245
- 实验：检查页目录和PDE 245
- 页表和页表项 246
- 页表项中硬件和软件的“写”位 247
- 页面内的字节 248
- 地址转译快查缓冲区 248
- 物理地址扩展（PAE） 249
- 实验：转译地址 251
- x64虚拟地址转译 253
- IA64虚拟地址转译 254
- 10.7 页面错误处理 255
- 无效PTE 256
- 原型PTE 258
- 页面换入I/O 259
- 冲突的页面错误 260
- 聚簇的页面错误 260
- 页面文件 261
- 实验：查看系统页面文件 262
- 提交用量和系统提交限额 263
- 提交用量和页面文件的大小 266
- 实验：利用任务管理器来查看页面文件使用量 266

- 10.8 栈 268
 - 用户栈 268
 - 实验：创建最大数量的线程 268
 - 内核栈 269
 - 实验：观察内核栈的使用量 269
 - DPC栈 270
- 10.9 虚拟地址描述符 270
 - 进程的VAD 271
 - 实验：查看虚拟地址描述符 272
 - 旋转VAD 272
- 10.10 NUMA 273
- 10.11 内存区对象 274
 - 实验：查看内存区对象 275
 - 实验：查看控制区域 277
- 10.12 驱动程序检验器 280
- 10.13 页面帧编号数据库 284
 - 实验：查看PFN数据库 287
 - 页面列表的动态变化 288
 - 实验：空闲列表和零页面列表 289
 - 实验：已修改列表和备用列表 291
 - 页面优先级 296
 - 实验：观察区分优先级的备用列表 298
 - 已修改页面写出器 299
- PFN数据结构 301
 - 实验：查看PFN项 304
- 10.14 物理内存的限制 305
 - Windows客户版本的限制 306
 - 32位客户的有效内存限制 307
- 10.15 工作集 309
 - 按需换页 309
 - 逻辑预取器 310
 - 实验：窥探预取文件内部 312
 - 实验：观察预取文件的读和写 312
 - 放置策略 313
 - 工作集管理 314
 - 实验：查看进程工作集大小 316
 - 实验：工作集与虚拟大小 316
 - 实验：在调试器中查看工作集列表 317
 - 平衡集管理器和交换器 318
 - 系统工作集 319
 - 内存通知事件 320
 - 实验：查看内存资源通知事件 321
- 10.16 主动式内存管理（Superfetch） 322
 - 各个组件 322
 - 跟踪过程和日志记录 324
 - 场景 325
 - 页面优先级和重平衡 326
 - 鲁棒性能 328
 - RAM优化软件 329
 - ReadyBoost 330
 - ReadyDrive 331
 - 统一缓存 332
 - 进程反射 334
 - 实验：利用Prefetch来观察进程反射的行为 336

- 10.17 本章总结 337
- 第11章 缓存管理器 338
 - 11.1 缓存管理器的关键特性 338
 - 单个中心化的系统缓存 339
 - 内存管理器 339
 - 缓存一致性 339
 - 虚拟块缓存 341
 - 流式缓存机制 341
 - 对可恢复文件系统的支持 341
 - 11.2 缓存的虚拟内存管理 342
 - 11.3 缓存的大小 344
 - 缓存的虚拟大小 344
 - 缓存的工作集大小 344
 - 实验：查看系统缓存的工作集 345
 - 缓存的物理大小 345
 - 11.4 缓存的数据结构 347
 - 系统范围的缓存数据结构 347
 - 实验：查看系统缓存的工作集 349
 - 针对每个文件的缓存数据结构 350
 - 实验：查看共享的和私有的缓存表 353
 - 11.5 文件系统接口 355
 - 从缓存中来回拷贝数据 356
 - 通过映射和锁定接口进行缓存 356
 - 通过直接内存访问接口进行缓存 357
 - 11.6 快速I/O 357
 - 11.7 预读（Read Ahead）和滞后写（Write Behind） 359
 - 智能预读 359
 - 回写缓存（Write-Back Caching）和延迟写（Lazy Writing） 361
 - 实验：观察缓存管理器的活动情况 362
 - 禁止一个文件的延迟写出行为 367
 - 强迫缓存被直写（write-through）到磁盘上 367
 - 刷新映射文件 367
 - 实验：观察缓存的刷新 368
 - 写节流（Write Throttling） 369
 - 实验：查看写节流参数 370
 - 系统线程 370
 - 11.8 本章总结 371
- 第12章 文件系统 372
 - 12.1 Windows文件系统格式 373
 - CDFS 373
 - UDF 374
 - FAT12、FAT16和FAT32 374
 - exFAT 377
 - NTFS 377
 - 12.2 文件系统驱动程序总体结构 378
 - 本地FSD 379
 - 远程FSD 380
 - 锁定 381
 - 实验：查看已注册文件系统的列表 383
 - 文件系统操作 387
 - 显式文件I/O 388
 - 内存管理器的修改页面写出器和映射页面写出器 392
 - 缓存管理器的延迟写出器（Lazy Writer） 392
 - 缓存管理器的预读线程 392

- 内存管理器的页面错误处理器 393
- 文件系统过滤型驱动程序 393
- 进程监视器 393
- 实验：查看进程监视器的过滤型驱动程序 394
- 12.3 诊断文件系统的问题 395
- 进程监视器的基本和高级模式 395
- 实验：在一个空闲系统上查看文件系统的活动 395
- 进程监视器诊断技巧 396
- 12.4 公用日志文件系统 397
- 列集操作 397
- 日志的类型 398
- 日志的布局结构 400
- 日志序列号 401
- 日志块 401
- 所有者页面 402
- 虚拟LSN到物理LSN的转译 403
- 管理策略 404
- 12.5 NTFS设计目标和特性 404
- 高端（High-End）文件系统的需求 404
- 可恢复性 405
- 安全性 405
- 数据冗余和容错能力 405
- NTFS的高级特性 406
- 多数据流 406
- 实验：查看数据流 408
- 基于Unicode的名称 408
- 通用的索引设施 409
- 动态的坏簇重新映射 409
- 硬链接（link）和交接（junction） 409
- 实验：创建一个硬链接 410
- 符号（软）链接和交接（junction） 410
- 实验：创建一个符号链接 412
- 压缩文件和稀疏文件 412
- 变化日志 413
- 针对每个用户的卷配额 413
- 链接跟踪 414
- 加密 415
- POSIX支持 416
- 碎片整理 416
- 动态分区 417
- 12.6 NTFS文件系统驱动程序 419
- 12.7 NTFS在磁盘上的结构 421
- 卷（volume） 421
- 簇（cluster） 422
- 主文件表（MFT） 423
- 实验：查看NTFS信息 425
- 文件记录号 426
- 文件记录 426
- 文件名 429
- 隧道传输 431
- 驻留的和非驻留的属性 432
- 数据压缩和稀疏文件 435
- 压缩稀疏数据 435
- 压缩非稀疏数据 437

- 稀疏文件 439
- 变化日志文件 439
- 实验：读取变化日志 441
- 索引 442
- 对象ID 444
- 配额跟踪 444
- 统一的安全性 445
- 重解析点 447
- 事务支持 447
- 隔离性 448
- 实验：理解和管理事务 449
- 事务型API 450
- 资源管理器 451
- 实验：查询资源管理器的信息 452
- 磁盘上的实现 453
- 日志的实现 454
- 恢复的实现 455
- 12.8 NTFS的恢复支持 455
- 设计 456
- 元数据日志记录 457
- 日志文件服务（LFS） 457
- 日志记录类型 459
- 恢复 461
- 分析扫描（Analysis Pass） 462
- 重做扫描（Redo Pass） 463
- 撤销扫描（Undo Pass） 463
- NTFS的坏簇恢复 465
- 自我修复 468
- 12.9 加密文件系统（EFS）安全性 469
- 第一次加密一个文件 472
- 加密文件数据 473
- 解密过程 474
- 加密文件的备份 474
- 实验：查看EFS信息 475
- 加密文件的复制 475
- 12.10 本章总结 476
- 第13章 启动和停机 477
- 13.1 引导过程 477
- BIOS引导准备 477
- BIOS引导扇区和Bootmgr 481
- UEFI引导过程 495
- 从iSCSI引导 496
- 初始化内核和执行体子系统 497
- 实验：加载器参数块 497
- Smss、Csrss和Wininit 504
- 未完成的文件重命名操作 507
- ReadyBoot 509
- 自动启动的映像文件 510
- 实验：Autoruns 511
- 13.2 引导和启动问题的故障检查 511
- 最后已知的好配置 512
- 安全模式 512
- 安全模式下的驱动程序加载 513
- 能感知安全模式的用户程序 514

安全模式下的引导日志 515
Windows恢复环境 (WinRE) 516
引导状态文件 519
解决常见的引导问题 520
MBR损坏 520
引导扇区损坏 520
BCD的错误配置 520
系统文件损坏 521
Windows资源保护 522
System储巢损坏 523
启动屏幕之后的崩溃或者挂起 523
13.3 停机 525
实验：验证HungAppTimeout值 526
13.4 本章总结 528
第14章 崩溃转储分析 529
14.1 Windows为什么会崩溃 529
14.2 蓝屏 530
Windows崩溃的原因 531
14.3 诊断崩溃问题 533
14.4 崩溃转储文件 535
实验：查看转储文件的信息 539
崩溃转储的生成 540
14.5 Windows错误报告 542
14.6 在线崩溃分析 543
14.7 基本的崩溃转储分析 545
Notmyfault 545
基本的崩溃转储分析 546
详细的分析 547
14.8 使用崩溃诊断工具 549
缓冲区溢出、内存破坏和特殊内存池 550
实验：通过驱动程序检验器启用特殊内存池 552
代码改写和系统代码写保护 553
14.9 高级的崩溃转储分析 554
栈破坏 555
挂起的或无响应的系统 557
实验：利用LiveKd来生成Hyper-V客户的转储 559
当没有崩溃转储时 561
实验：附载一个内核调试器 562
14.10 对常见停止代码的分析 564
0xD1 - DRIVER_IRQL_NOT_LESS_OR_EQUAL 564
0x8E - KERNEL_MODE_EXCEPTION_NOT_HANDLED 566
0x7F - UNEXPECTED_KERNEL_MODE_TRAP 567
0xC5 - DRIVER_CORRUPTED_EXPOOL 569
硬件故障 571
实验：蓝屏屏幕保护程序 572
• • • • • ([收起](#))

[深入解析Windows操作系统（第6版）下册_下载链接1](#)

标签

操作系统

windows

计算机

深入解析Windows操作系统

Windows内核

计算机系统

計算機

编程

评论

[深入解析Windows操作系统（第6版） 下册_下载链接1](#)

书评

[深入解析Windows操作系统（第6版） 下册_下载链接1](#)