

# 《深入解析Windows操作系统：第6版》

## 图书基本信息

书名：《深入解析Windows操作系统：第6版（上册）》

13位ISBN编号：9787121219566

10位ISBN编号：7121219565

出版时间：2014-4-1

出版社：电子工业出版社

作者：拉希诺维奇 (Mark Russinovich), David A. Solomon, Alex Ionescu

页数：685

译者：潘爱民, 范德成

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu111.com](http://www.tushu111.com)

# 《深入解析Windows操作系统：第6》

## 内容概要

《深入解析Windows操作系统：第6版（上册）》是著名的操作系统内核专家Mark Russinovich和David Solomon、Allen Ionescu撰写的关于Windows操作系统原理的最新版著作，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。本书针对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，本书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校。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，以及性能优化。

《深入解析Windows操作系统：第6版（上册）》适合广大Windows平台开发人员、IT专业从业人员等参考阅读。

## 书籍目录

译者序

III

引言

V

本书的结构

V

本书的历史

V

第6版的变化

VI

练习实验

VI

本书没有覆盖的话题

VI

提醒和告诫

VII

致谢

VII

勘误和本书支持

IX

倾听您的声音

IX

保持联系

IX

第1章概念和工具

1

1.1 WINDOWS操作系统的版本

1

1.2 基础概念和术语

2

WINDOWS API

2

服务、函数和例程

4

进程、线程和作业

5

虚拟内存

13

内核模式和用户模式

15

终端服务及多个会话

19

对象和句柄

20

安全性

21

注册表

22	
UNICODE	
23	
1.3 挖掘WINDOWS内部机理	
23	
性能监视器	
24	
内核调试	
25	
WINDOWS软件开发工具 (WINDOWS SDK)	
30	
WINDOWS驱动程序开发工具	
30	
SYSINTERNALS工具	
31	
1.4 本章总结	
31	
第2章系统架构	
33	
2.1 需求和设计目标	
33	
2.2 操作系统模型	
34	
2.3 总体架构	
35	
可移植性	
37	
对称多处理	
38	
可伸缩性	
40	
客户机和服务器版本之间的差异	
41	
检查版本	
44	
2.4 关键的系统组件	
46	
环境子系统和子系统DLL	
47	
NTDLL.DLL	
53	
执行体	
54	
内核	
56	
硬件抽象层 (HAL)	
60	
设备驱动程序	
62	

系统进程	
67	
2.5 本章总结	
77	
第3章系统机制	
79	
3.1 陷阱分发	
79	
中断分发	
81	
定时器处理	
110	
异常分发	
120	
系统服务分发	
130	
3.2 对象管理器	
137	
执行体对象	
139	
对象结构	
142	
3.3 同步	
174	
高IRQL的同步	
175	
低IRQL的同步	
180	
3.4 系统辅助线程	
202	
3.5 WINDOWS全局标志	
205	
3.6 高级本地过程调用（ALPC）	
206	
连接模型	
207	
消息模型	
208	
异步操作	
211	
视图、区域和内存区	
211	
属性	
212	
BLOB、句柄和资源	
213	
安全性	
214	
性能	

214	
调试和跟踪	
215	
3.7 内核事件跟踪	
217	
3.8 WOW64	
220	
WOW64进程地址空间布局结构	
221	
系统调用	
221	
异常分发	
222	
用户APC分发	
222	
控制台支持	
222	
用户回调	
222	
文件系统重定向	
222	
注册表的重定向	
223	
I/O控制请求	
224	
16位安装器应用程序	
225	
打印	
225	
一些限制	
225	
3.9 用户模式调试	
226	
内核支持	
226	
原生支持	
227	
WINDOWS子系统支持	
229	
3.10 映像加载器	
229	
进程初始化早期工作	
231	
DLL名称解析	
232	
DLL名称重定向	
233	
已加载模块数据库	
235	

导入信息解析	239
导入过程初始化的后期处理	241
SWITCHBACK	242
API集	243
3.11 超级监督者(HYPER-V)	245
分区	246
父分区	247
子分区	249
硬件仿真和支持	251
3.12 内核事务管理器	265
3.13 热补丁支持	267
3.14 内核补丁保护	269
3.15 代码完整性	271
3.16 本章总结	272
第4章管理机制	273
4.1 注册表	273
查看和修改注册表	273
注册表用法	274
注册表数据类型	275
注册表逻辑结构	276
事务型注册表 (TXR)	284
监视注册表活动	285
注册表的内部机理	289
4.2 服务	301
服务应用	

301	
服务账户	
307	
服务控制管理器	
318	
服务启动	
320	
启动错误	
324	
接受当前引导和“最后已知的好控制集”	
325	
服务失败	
327	
服务停机	
328	
共享的服务进程	
329	
服务标记	
333	
4.3 统一的后台进程管理器	
333	
初始化	
334	
UBPM API	
335	
提供者注册	
335	
消费者注册	
337	
TASKHOST	
338	
服务控制程序	
339	
4.4 WINDOWS管理设施	
340	
提供者	
341	
公共信息模型（CIM）和可管理对象的格式语言	
343	
类关联	
347	
WMI实现	
348	
WMI安全性	
350	
4.5 WINDOWS诊断基础设施	
351	
WDI设施	
351	

诊断策略服务

351

诊断功能

353

4.6 本章总结

354

第5章进程、线程和作业

355

5.1 进程的内部机理

355

数据结构

355

5.2 受保护进程

362

5.3 CREATEPROCESS的流程

364

阶段1：转换并验证参数和标志

365

阶段2：打开将要被执行的映像

368

阶段3：创建WINDOWS执行体进程对象（PSPALLOCATEPROCESS）

371

阶段4：创建初始线程，以及它的栈和执行环境

376

阶段5：执行特定于WINDOWS子系统的初始化后处理

378

阶段6：启动初始线程的执行

380

阶段7：在新进程环境下执行进程初始化

380

5.4 线程的内部机理

386

数据结构

386

一个线程的诞生

391

5.5 检查线程活动

392

受保护进程的线程上的访问限制

394

5.6 工作者工厂（线程池）

396

5.7 线程调度

400

WINDOWS调度概述

400

优先级别

402

线程状态

408	
分发器数据库	
412	
时限	
414	
优先级提升	
420	
环境切换	
438	
调度情形	
438	
空闲（IDLE）线程	
442	
线程选择	
445	
多处理器系统	
447	
多处理器系统上的线程选择	
456	
处理器的选择	
457	
5.8 基于处理器份额的调度	
459	
分布式公平份额调度	
459	
CPU比率的限制	
466	
5.9 动态的处理器添加与更换	
467	
5.10 作业对象	
468	
作业的限制	
469	
作业集	
470	
5.11 本章总结	
472	
第6章安全性	
473	
6.1 安全等级	
473	
可信计算机系统评估标准（TCSEC）	
473	
6.2 安全系统组件	
476	
6.3 保护对象	
480	
访问检查	
481	

安全标识符 (SID)	483
虚拟服务账户	503
安全描述符和访问控制	507
6.4 AUTHZ API	522
6.5 账户权限和特权	524
账户权限	524
特权	526
超级特权	533
6.6 进程和线程的访问令牌	535
6.7 安全审计	535
对象访问的审计	537
全局审计策略	540
高级审计策略设置	541
6.8 登录 (LOGON)	542
WINLOGON初始化	543
用户登录步骤	545
可保证的认证	549
用户认证的生物识别框架	550
6.9 用户账户控制和虚拟化	552
文件系统和注册表虚拟化	553
权限提升	560
6.10 应用程序标识 (APPID)	568
6.11 APPLOCKER	569
6.12 软件限制策略	575
6.13 本章总结	

577	
第7章网络	
579	
7.1 WINDOWS的网络总体结构	
579	
OSI参考模型	
580	
WINDOWS网络组件	
582	
7.2 网络API	
585	
WINDOWS套接字 ( WINDOWS SOCKETS )	
585	
WINSOCK内核	
591	
远过程调用	
593	
WEB访问API	
597	
命名管道和邮件槽	
600	
NETBIOS	
605	
其他的网络API	
607	
7.3 多重定向器支持	
614	
多提供者转发器	
614	
多UNC提供者	
617	
代理提供者	
618	
重定向器	
619	
小重定向器	
621	
服务器消息块与子重定向器	
622	
7.4 分布式文件系统名字空间	
623	
7.5 分布式文件系统复制	
624	
7.6 脱机文件	
625	
缓存模式	
627	
幻影 ( GHOSTS )	
629	

数据安全性

629

缓存的结构

630

7.7 BRANCHCACHE

631

缓存模式

633

BRANCHCACHE优化下的应用程序数据获取：SMB序列

638

BRANCHCACHE优化下的应用程序数据获取：HTTP序列

640

7.8 名称解析

642

域名系统

642

对等体名称解析协议

642

7.9 位置和拓扑结构

645

网络位置感知

645

网络连接状态指示器

646

链路层拓扑发现

649

7.10 协议驱动程序

649

WINDOWS过滤平台

652

7.11 NDIS驱动程序

658

NDIS小端口的变化形式

662

面向连接的NDIS

662

外接NDIS ( REMOTE NDIS )

665

QOS

667

7.12 绑定

669

7.13 分层的网络服务

670

术语对照表

681

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu111.com](http://www.tushu111.com)