

Áttekintés

Windows Internals, 6. kiadás, 1. kötet

1. fejezet	Fogalmak és eszközök
2. fejezet	A rendszer architektúrája
3. fejezet	Rendszermechanizmusok
4. fejezet	Felügyeleti eszközök
5. fejezet	Folyamatok, szálak, munkaegységek
6. fejezet	Biztonság
7. fejezet	Hálózatkezelés

Windows Internals, 6. kiadás, 2. kötet (elérhető 2013. ősztől)

8. fejezet	I/O rendszer
9. fejezet	Tárolókezelés
10. fejezet	Memóriakezelés
11. fejezet	Gyorsítótár-kezelő
12. fejezet	Fájlrendszerek
13. fejezet	Indítás és leállítás
14. fejezet	Az összeomlási memóriakép elemzése

Tartalomjegyzék

Bevezetés	xv
A könyv felépítése.....	xv
A könyv előzményei	xv
A 6. kiadás újdonságai	xvi
Gyakorlatok	xvi
Kihagyott témakörök.....	xvi
Figyelmeztetés	xvii
Köszönetnyilvánítás.....	xvii
Hibajegyzék és segítség kérése a könyvhöz	xix
Kíváncsiak vagyunk az olvasók véleményére	xix
Maradjunk kapcsolatban!	xix
1. fejezet – Fogalmak és eszközök.....	1
A Windows operációs rendszer változatai	1
Alapvető fogalmak és szakkifejezések	2
Windows API	2
Szolgáltatások, függvények és rutinok.....	4
Folyamatok, szálak, munkaegységek.....	5
Virtuális memória	16
Kernelmód és felhasználói mód.....	18
Terminálszolgáltatás és több munkamenet.....	23
Objektumok és objektumazonosítók.....	24
Biztonság.....	25
Beállításjegyzék.....	26
Unicode	27
Részletesen a Windows működéséről	28
Performance Monitor	28
Kernel-hibakeresés	30
Windows SDK	36
Windows Driver Kit.....	36
Sysinternals-eszközök.....	37
Összefoglalás	37
2. fejezet – A rendszer architektúrája.....	39
Követelmények és tervezési célok.....	39
Az operációs rendszer modellje.....	40
Az architektúra áttekintése	41
Hordozhatóság.....	44
Szimmetrikus többprocesszoros működés	45

Skálázhatóság.....	47
Az ügyfél és a kiszolgálóoldali változatok közti különbségek.....	48
Hibakeresési fordítás	53
A rendszer fő összetevői.....	55
Környezeti alrendszerek és alrendszer-DLL-ek.....	57
Ntdll.dll.....	63
Futtatórendszer	64
Kernel.....	68
A hardverabsztrakciós réteg.....	71
Device drivers.....	74
Rendszerfolyamatok.....	80
Összefoglalás	92
3. fejezet – Rendszermechanizmusok.....	93
Cspadakisztás	93
Megszakításkiosztás.....	95
Időzítő feldolgozása	132
Kivételkiosztás.....	145
Rendszerszolgáltatás-kiosztás	156
Objektumkezelő.....	166
Futtatórendszer-objektumok	169
Objektumstruktúra	172
Szinkronizáció	212
Magas szintű IRQL-szinkronizáció.....	214
Alacsony megszakításszintű szinkronizálás	219
Rendszermunkaszálak	247
Windowsbeli globális jelzők	249
Fejlett helyi eljárás hívás.....	251
Kapcsolatmodell	252
Üzenetmodell	254
Aszinkron működés.....	257
Nézetek, területek és szakaszok	258
Attributes	258
Blobok, azonosítók és erőforrások	259
Biztonság.....	260
Teljesítmény	261
Hibakeresés és nyomonkövetés	262
Kernelesemény-követés	264
Wow64.....	269
Wow64-folyamat címterületének felosztása.....	270
Rendszerhívások	270
Kivételkiosztás.....	270

Felhasználói APC-szétosztás.....	270
Parancssori támogatás.....	271
Felhasználói visszahívások.....	271
Fájlrendszer-átírányítás.....	271
Beállításjegyzék-átírányítás.....	272
I/O-vezérlés kérése.....	273
16 bites telepítőalkalmazások.....	274
Nyomtatás.....	274
Korlátozások.....	274
Hibakeresés felhasználói módban.....	275
Kernel-támogatás.....	275
Natív támogatás.....	277
A Windows-alrendszer-támogatás.....	278
A memóriakép-betöltő.....	279
Korai folyamatinitializálás.....	281
DLL-névfeloldás és -átírányítás.....	283
Betöltött moduladatbázis.....	286
Importelemzés.....	291
Importálás utáni folyamatinitializálás.....	292
SwitchBack.....	294
API-készletek.....	295
Hipervizor (Hyper-V).....	298
Partíciók.....	299
Szülőpartíció.....	300
Gyermekpartíciók.....	302
Hardveremuláció és támogatás.....	305
Kernelbeli tranzakciókezelő.....	321
Működés alatti foltozás támogatása.....	324
Kernelfoltozási védelem.....	326
Kódintegritás.....	330
Összefoglalás.....	331
4. fejezet – Felügyeleti eszközök.....	333
A beállításjegyzék.....	333
A beállításjegyzék megjelenítése és módosítása.....	333
A beállításjegyzék használata.....	334
A beállításjegyzék adattípusai.....	335
A beállításjegyzék logikai struktúrája.....	336
Tranzakcióalapú beállításjegyzék (TxR).....	345
A beállításjegyzék-műveletek megfigyelése.....	347
A Process Monitor belseje.....	348
A beállításjegyzék működése.....	352

Szolgáltatások	367
Szolgáltatásalkalmazások	367
A szolgáltatáskezelő	388
Szolgáltatások indulása	391
Indítási hibák	396
A rendszerbetöltés és az utolsó helyes beállítás	397
Szolgáltatások hibái	399
Szolgáltatások leállítása	401
Közös szolgáltatásfolyamatok	402
Szolgáltatáscímkék	406
Unified Background Process Manager	407
Inicializálás	408
UBPM API	409
Szolgáltató regisztrálása	409
Fogyasztó regisztrálása	411
Feladatfuttató	413
Szolgáltatásvezérlő programok	413
Windows-felügyeleti műszerezés	414
Szolgáltatók	416
A közös információmodell és a felügyeltobjektum- formátumú nyelv	418
Osztálytársítás	422
WMI-megvalósítás	424
WMI-biztonság	426
A Windows diagnosztikai infrastruktúrája	427
WDI-műszerezés	427
Diagnosztikai házirend-szolgáltatás	428
Diagnosztikai funkció	430
Összefoglalás	431
5. fejezet – Folyamatok, szálak, munkaegységek	433
A folyamat belseje	433
Adatszerkezetek	433
Védett folyamatok	442
A CreateProcess folyamat	444
1. fázis: Paraméterek és jelzők konvertálása és ellenőrzése	446
2. fázis: A végrehajtandó memóriakép megnyitása	450
3. fázis: A Windows végrehajtó rendszerbeli folyamatobjektum létrehozása (<i>PspAllocateProcess</i>)	453
4. fázis: A kezdeti szál, a verem és a környezet létrehozása	460
5. fázis: Windows-alrendszer-specifikus utóinicializálás végrehajtása	462
6. fázis: A kezdeti szál végrehajtásának indítása	465

7. fázis: Folyamatinitializálás végrehajtása az új folyamat környezetében	465
A szálak belsejében	471
Adatszerkezetek	471
Egy szál születése.....	478
A száltevékenység vizsgálata.....	479
A védett folyamatszálak korlátozásai	482
Dolgozó-metódusgenerátorok (szálkészletek)	484
Szálütemezés	488
A Windows ütemezésének áttekintése.....	489
Prioritásszintek.....	491
Szálállapotok.....	498
Kiosztó-adatbázis.....	503
Kvantum.....	505
Prioritásemelés	513
Környezetváltás.....	534
Ütemezési helyzetek	535
Üresjárati szálak.....	539
Szálkiválasztás.....	544
Többprocesszoros rendszerek.....	545
Szálkiválasztás többprocesszoros rendszereken.....	557
Processzorkiválasztás	558
Processzormegosztás-alapú ütemezés	561
Distributed Fair Share Scheduling.....	561
Processzoridő-korlátozások	569
Dinamikusprocesszor-hozzáadás és -csere	570
Munkaegység-objektumok.....	572
Munkaegység-korlátozások	573
Munkaegységkészletek	574
Összefoglalás	578
6. fejezet – Biztonság.....	579
Biztonsági minősítések.....	579
Kéértékelési szempontok megbízható számítógép-rendszerekhez.....	579
Közös szempontrendszer	582
A biztonsági rendszer összetevői.....	582
Objektumok védelme	587
Hozzáférés-ellenőrzés	589
Biztonsági azonosítók (SID-ek).....	592
Virtuális szolgáltatásfókok.....	616
Biztonsági leírók és hozzáférés-szabályozás	620
Az AuthZ API.....	639
Fiókjogosultságok és -privilegiumok	642

Fiókjogosultságok.....	643
Privilegiumok.....	644
Szuperprivilegiumok.....	652
Folyamatok és szálak hozzáférési jogkivonatai.....	654
Biztonsági naplózás	655
Objektumok hozzáféréseinek naplózása.....	656
Globális naplózási házirend	659
Speciális naplózási házirend-beállítások	662
Bejelentkezés.....	663
Winlogon-inicializálás	664
Felhasználó bejelentkezésének a lépései.....	666
Biztosított hitelesítés	672
Felhasználóhitelesítési biometrikus keretrendszer	673
A felhasználói fiókok felügyelete és a virtualizáció	676
Fájlrendszer- és beállításjegyzék-virtualizáció	677
Jogosultságemelés	685
Alkalmazásazonosítás (AppID)	696
AppLocker	697
Szoftverkorlátozó házirendek	705
Összefoglalás	707
7. fejezet – Hálózatkezelés.....	709
A Windows hálózati architektúrája.....	709
Az OSI-referenciamodell.....	709
Windows hálózatkezelési összetevők.....	713
Hálózati API-k	717
Windows Sockets	717
Winsock-kernel	724
RPC (Remote Procedure Call – távoli eljáráshívás).....	727
Webhozzáférési API-k	732
Nevesített csövek és mailslotok	735
NetBIOS	742
Más hálózati API-k.....	745
Több átirányító használata.....	752
Több szolgáltatót kezelő útválasztó.....	753
Multiple UNC Provider	756
Helyettesítő szolgáltatók.....	759
Átirányító	759
Míniatírányítók	761
A kiszolgáló üzenetblokk (Server Message Block) és az alátírányítók.....	762
Elosztottfájlrendszer-névtér.....	764

Elosztottfájlrendszer-replikáció.....	766
Kapcsolat nélküli fájlok.....	767
Gyorsítótárazási módok.....	769
Szellemképek.....	771
Adatbiztonság.....	772
Gyorsítótár-szerkezet.....	772
BranchCache.....	774
Gyorsítótárazási módok.....	777
BranchCache-optimalizált alkalmazásbetöltés: SMB-szekvencia.....	782
BranchCache-optimalizált alkalmazásbetöltés: HTTP-szekvencia.....	785
Névfeloldás.....	787
Domain Name System.....	787
Peer Name Resolution Protocol.....	788
Hely és topológia.....	791
Hálózati hely-figyelés.....	791
Hálózati kapcsolat állapotának a jelzője.....	792
Kapcsolati rétegbeli topológiafelderítés.....	795
Protokollillesztő programok.....	796
Windows Filtering Platform.....	800
NDIS-illesztőprogramok.....	807
Az NDIS-miniport változatai.....	812
Kapcsolatorientált NDIS.....	813
Távoli NDIS.....	816
QoS.....	818
Kötés.....	821
Rétegzett hálózati szolgáltatások.....	822
Távoli hozzáférés.....	822
Active Directory.....	823
Network Load Balancing.....	825
Network Access Protection.....	827
Közvetlen hozzáférés.....	834
Összefoglalás.....	835
Tárgymutató.....	837

Bevezetés

A Windows Internals 6. kiadása olyan gyakorlott számítástechnikai szakemberek (mind a fejlesztők, mind a rendszergazdák) számára készült, akik szeretnék megérteni a Microsoft Windows 7 és a Windows Server 2008 R2-es operációs rendszerek alapvető összetevőinek belső működését. Ezeknek az ismereteknek a birtokában a fejlesztők jobban megérthetik a tervezési döntések mögött rejlő logikai alapokat, amikor kimondottan Windows platformra szánt alkalmazásokat fejlesztenek. Ez a tudás többek között az összetett problémák hibakeresésekor segítheti a fejlesztőket. A rendszergazdák is előnyt kovácsolhatnak mindezekből, hiszen a „felszín alatti” rendszerműködés megismerése segít abban, hogy a rendszer teljesítménybeli viselkedését megértsük, valamint megkönnyíti a rendszerproblémák hibakeresését, ha valami nem úgy működik, ahogyan elvárnánk. A könyv elolvasása után jobban megérthetjük a Windows működésének mikéntjét és viselkedésének okait.

A könyv felépítése

Története során első ízben a *Windows Internals* két részben jelenik meg. A könyv anyagának frissítése az egyes Windows-kiadások megjelenését követően jelentős időt vesz igénybe, így a tartalom két részre bontásával az első rész hamarabb kiadható.

Ebben a könyvben az 1. rész első két fejezete az alapvető fogalmak meghatározásával, a könyvben használt eszközök bemutatásával, valamint a rendszer architektúrájának és összetevőinek általános leírásával indul. A következő két fejezet ismerteti a kulcsfontosságú mögöttes mechanizmusokat a rendszerben. Az 1. rész az operációs rendszer három alapösszetevőjének részletezésével zárul: a folyamatokat, a szálakat, a munkaegységeket; a biztonságot; valamint a hálózatkezelést ismerteti.

A 2. rész, amely angolul 2012 őszén jelent meg* a többi alapvető fontosságú alrendszert mutatja be: az I/O rendszert, a tárolókezelést, a memóriakezelést, a gyorsítótár-kezelőt és a fájlrendszereket. A 2. rész a rendszerindítás és -leállítás folyamatának, valamint az összeomlási memória elemzésének vizsgálatával zárul.

A könyv előzményei

Ez kötet az eredetileg *Inside Windows NT* (Microsoft Press, 1992) című könyvnek a hatodik kiadása, amelyet Helen Custer írt (a Microsoft Windows NT 3.1 kezdeti kiadása előtt). Az *Inside Windows NT* volt az olyan első könyv, amelynek témája a Windows NT volt, és bepillantást nyújtott a rendszer architektúrájába, valamint tervezési részleteibe. Az *Inside Windows NT 2. kiadása* (Microsoft Press, 1998) szerzője David Solomon. Az eredeti könyv frissítéseként témája a Windows NT 4.0 volt, és már sokkal elmélyültebb technikai tartalommal rendelkezett.

Az Inside Windows 2000 3. kiadását (Microsoft Press, 2000) David Solomon és Mark Russinovich írta. Ez a kiadás nagyon sok új témát tárgyalt, például a rendszerindítást

* Magyarul 2013 nyarán várható. (A kiadó)

és -leállítás, a szolgáltatások belső működését, a beállításjegyzék belső funkcióját, a fájlrendszerillesztő programokat, valamint a hálózatkezelést. Foglalkozott a Windows 2000 kernelváltozásaival, például a WDM-mel (Windows Driver Model – windowsos illesztőprogram-modell), a Plug and Play-jel, az energiagazdálkodással, a WMI-vel (Windows Management Instrumentation – Windows-felügyeleti műszerezés), a titkosítással, a munkaegység-objektummal és a terminálszolgáltatással. *A Windows Internals 4. kiadása* a Windows XP és a Windows Server 2003 frissítése lett, és további témaköröket tartalmazott, amelyek arra összpontosítottak, hogy segítsék az üzemeltetőket abban, hogy kihasználhassák a Windows belső működésével kapcsolatos ismereteiket, például a Windows Sysinternals (www.microsoft.com/technet/sysinternals) kulcsfontosságú eszközeinek a használatával és az összeomlási memóriakép elemzésével. *A Windows Internals 5. kiadása* a Windows Vista és a Windows Server 2008-as frissítése volt. Az új témakörök közé tartozott a memóriakép-betöltő, a felhasználói módú hibakeresés lehetősége, valamint a Hyper-V.

A 6. kiadás újdonságai

A legújabb kiadás a Windows 7 és a Windows Server 2008 R2-es kernelváltozásainak bemutatásához készült. A gyakorlatok tükrözik az eszközök módosításait.

Gyakorlatok

Még a Windows forráskódjához való közvetlen hozzáférés nélkül is rengeteg információ összegyűjthető a Windows belső működéséről az olyan eszközök, mint a kernel-hibakereső, valamint a Sysinternals és a Winsider Seminars & Solutions eszközeinek a segítségével. Amikor egy adott eszközzel leleplezhető vagy bemutatható a Windows belső viselkedésének néhány szempontja, az eszköz kipróbálásának lépéseit a „KÍSÉRLET” dobozok listázzák. A kísérletekkel a könyv valamennyi fejezetében találkozhatunk, és érdemes a gyakorlatokat a könyv olvasásakor végrehajtani – a Windows belső működésének látható bizonyítékai sokkal mélyebb benyomást tesznek, mint a pusztá olvasás.

Kihagyott témakörök

A Windows hatalmas és összetett operációs rendszer. A könyv nem foglalkozik a Windows belső működését érintő valamennyi idevágó témakörrel, inkább az alapszintű rendszerösszetevőkre összpontosít. Nem ismerteti például a COM+-technológiát, a Windows elosztott objektumorientált programozási infrastruktúráját vagy a Microsoft .NET keretrendszert, a felügyelt kódú alkalmazások alapját.

Mivel a könyv a belső működést tanulmányozza, és nem felhasználói, programozási vagy rendszerfelügyeleti kézikönyv, nem ecseteli a Windows használatának, programozásának vagy beállításának a részleteit.

Figyelmeztetés

Mivel a könyv a Windows operációs rendszer belső architektúrájának és működésének nem dokumentált viselkedését írja le (például a belső kernelstruktúrákat és függvényeket), ez a tartalom a különböző Windows-kiadások között változhat. (Ellenben a nyilvánosan elérhető interfészekon, például a Windows API-n, nem hajtanak végre inkompatibilitást okozó módosításokat.)

A „módosítás” nem feltétlenül jelenti azt, hogy a könyvben ismertetett részletek biztosan változnak az egyes kiadások között, de nem biztos, hogy változatlanok maradnak. Bármelyik szoftver, amely a nem dokumentált interfészeket használja, működésképtelenné válhat a Windows jövőbeli kiadásában. Még rosszabb, hogy a kernelmódban futó szoftverek (például az eszközüillesztő programok), amelyek a nem dokumentált interfészeket alkalmazzák, rendszerösszeomlás áldozataivá válhatnak, amikor azokat a Windows egy újabb kiadásán futtatjuk.

Köszönetnyilvánítás

Először is köszönet illeti Jamie Hanrahant és Brian Catlint az Azius, LLC-től, amiért csatlakoztak hozzánk a projektben – segítségük nélkül a könyvet nem fejeztük volna be. A biztonsági és hálózatkezelési fejezetek frissítéseinek nagy része tőlük származik, és hozzájárultak a felügyeleti eszközökkel, valamint a folyamatokkal és szálakkal kapcsolatos fejezetek aktualizálásához. Az Azius a Windows belső működését és az eszközüillesztő programok rejtelmét oktatja. Bővebb információ a www.azius.com webhelyen található.

Szeretnénk elismerni Alex Ionescu érdemeit, aki ezen kiadás teljes jogú társszerzője. Alex átfogó tevékenységet nyújtott az 5. kiadásban, és méltányolandó további munkája is ebben a kiadásban.

Köszönetet érdemel Eric Traut és Jon DeVaan, mert biztosították David Solomon hozzáféréseit a Windows forráskódjához, amely a könyvön végzett munkájához, illetve a Windows belső működésével kapcsolatos tananyagok továbbfejlesztéséhez elengedhetetlen volt.

Az 5. kiadással kapcsolatban nem tettünk említést három bíráló munkájáról és hozzájárulásáról: Arun Kishan, Landy Wang, és Aaron Margosis – ismét köszönet illeti őket. És újfent köszönet kell mondani Arunnak és Landynek, hogy részletes kritikával és építő észrevételekkel járultak hozzá ehhez a kiadáshoz.

A Microsoft Windows fejlesztői csoportjának véleménye, ismeretei és támogatása nélkül a könyv nem ereszkedhetett volna a technikai részletek ilyen mélységeibe, illetve az információk nem lehetnének ilyen pontosak. Tehát köszönet illeti a következő szakembereket, akik javaslataikkal és ismereteikkel hozzájárultak a könyvhöz:

- Greg Cottingham
- Joe Hamburg
- Jeff Lambert

- Pavel Lebedynskiy
- Joseph East
- Adi Oltean
- Alexey Pakhunov
- Valerie See

A hálózatkezelési fejezet kapcsán külön köszönet illeti Gianluigi Nuscát és Tom Jollyt, akik jóval túlteljesítették kötelességüket: Gianluigi rendkívüli segítséget nyújtott a BranchCache szolgáltatással kapcsolatos tartalom összeállításában (az anyag több bekezdése is tőle származik), és Tom Jolly saját ismeretei és javaslatai mellett (amelyek mindig kiválóak voltak) több fejlesztőt is bevont a munkába. Következzék azok névsora, akik hozzájárultak a hálózatkezeléssel kapcsolatos fejezethez:

- Roopesh Battepati
- Molly Brown
- Greg Cottingham
- Dotan Elharrar
- Eric Hanson
- Tom Jolly
- Manoj Kadam
- Greg Kramer
- David Kruse
- Jeff Lambert
- Darene Lewis
- Dan Lovinger
- Gianluigi Nusca
- Amos Ortal
- Ivan Pashov
- Ganesh Prasad
- Paul Swan
- Shiva Kumar Thangapandi

Amos Ortal és Dotan Elharrar a NAP, Shiva Kumar Thangapandi pedig az EAP témakörében nyújtott rendkívüli segítséget.

Christophe Nasarre, a szakmai lektor részletes ellenőrzése nagymértékben hozzájárult a könyv szakmai pontosságához és konzisztenciájához.

Ismét szeretnénk köszönetet mondani Ilfak Guilfanovnak, a Hex-Rays (www.hex-rays.com) munkatársának az IDA Pro Advanced és a Hex-Rays licenckért, amelyeket Alex Ionescu rendelkezésére bocsátottak, hogy meggyorsíthassa a Windows-kernel fordított tervezését.

Végül a szerzők szeretnék megköszönni a Microsoft Press nagyszerű munkatársainak segítségét, akik nélkül a könyv nem készülhetett volna el. Dave Musgrave ket-tős feladatkört töltött be beszerzési szerkesztőként és fejlesztési szerkesztőként, míg Carol Dillingham projektszerkesztőként felügyelte a munkát. A könyv minőségének szintjét Steve Sagman szerkesztői és termelési vezető, Roger LeBlanc segédszerkesztő, Audrey Marr korrektor és Christina Yeager indexelő munkája biztosította.

Végül, de nem utolsósorban köszönet illeti Ben Ryant, a Microsoft Press kiadó-vezetőjét, aki rendületlenül hisz annak jelentőségében, hogy a Windows belső részleteinek el kell jutnia az olvasókhöz.

Hibajegyzék és segítség kérése a könyvhöz

Mindent elkövettünk, hogy biztosítsuk a könyv tartalmának pontosságát. A könyv megjelenése óta felfedezett hibák listája és kiigazítása a Microsoft Press webhelyén található: <http://go.microsoft.com/fwlink/?Linkid=245675>

Ha az olvasó újabb hibát talál, ezt ugyanezen a webhelyen jelezheti.

Ha további segísre lenne szükség, a megjegyzéseket vagy a kérdéseket a Microsoft Press technikai tanácsadási részlegének a mspinput@microsoft.com e-mail címére lehet elküldeni.

A Microsoft-szoftver terméktámogatása a fenti címeken keresztül nem érhető el.

Kíváncsiak vagyunk az olvasók véleményére

A Microsoft Press számára fontos és értékes az olvasói elégedettség, az olvasó visszajelzése. Véleményeket a könyvről az alábbi kérdőív kitöltésével lehet eljuttatni hozzánk: <http://www.microsoft.com/learning/booksurvey>

A kérdőív rövid, és minden megjegyzés fontos. Köszönjük a segítséget!

Maradjunk kapcsolatban!

Folytassuk az értekezést akár a Twitteren is: <http://twitter.com/MicrosoftPress>.

