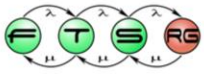
Operációs rendszerek (vimia219)

Hibakeresés Windowson

dr. Micskei Zoltán

http://mit.bme.hu/~micskeiz

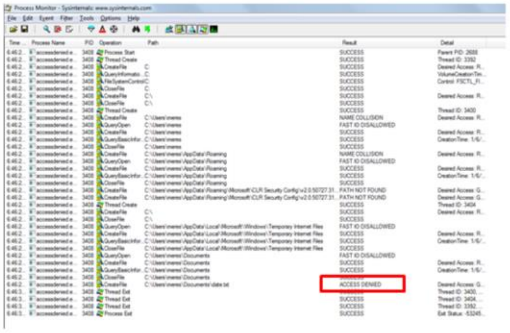


Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Utolsó módosítás: 2014. 02. 24.

DEMO Hozzáférési hiba megtalálása

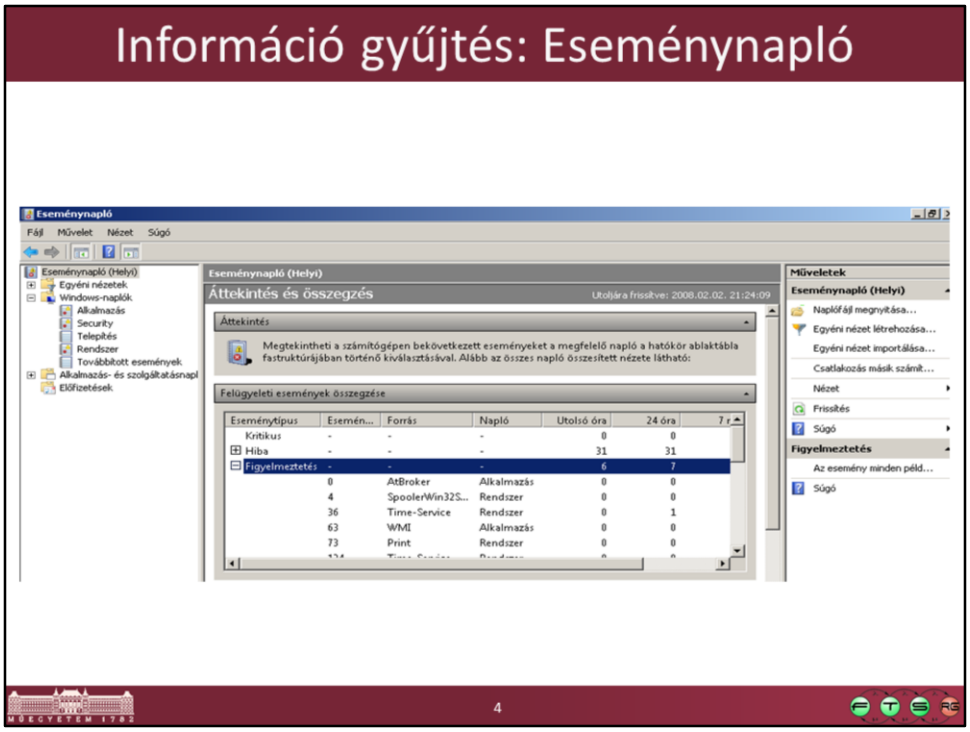
- Process Monitor használata:
  - Tools / Count occurrences: Result
  - Tools / File Summary



Hiba esetén

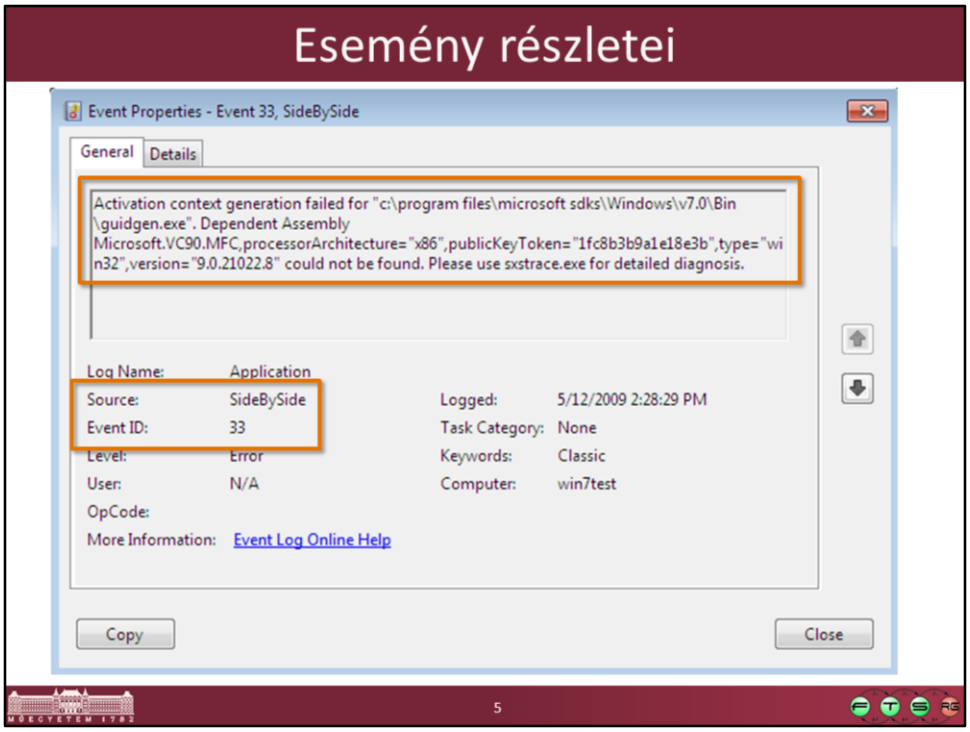
- Mi történt pontosan?
  - Ki okozta? Mikor? Miért?
  - Feljegyzések készítése (képernyőkép, lépések…)
  - Tudjuk reprodukálni?
- Információ begyűjtése
  - Hibanaplók (alkalmazás sajátja, rendszer)
  - Hibakereső eszközök (sysinternals, support tools…)
- Próbáljuk megérteni, mi történik

Információ gyűjtés: Eseménynapló



Az Eseménynapló a Windows platform központi naplózó komponense, amibe mind az operációs rendszer, mind a külső alkalmazások írhatnak.
Jól kereshető és szűrhető, sok féle programozási nyelvből elérhető (C++, .NET nyelvek, szkriptek…)

Hibakeresési, diagnosztikai feladatok esetén ez az egyik elsődleges információforrásunk.

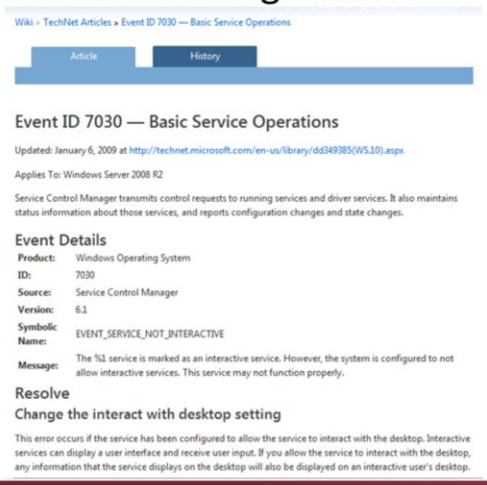


Az esemény azonosítása a forrás és az esemény azonosítója alapján történhet.

Egy adott eseményazonosító – eseményforrás pár egy bizonyos eseményt azonosít, de ennek a szövegében lehetne változó részek (pl. a fenti példában az elérési út mindig az adott szituációnak megfelelően generálódik).

Eventlog Online help

- Keresés a forrás + azonosító párosra
- Gyakori hibák esetén megoldás is:



Wiki > TechNet Articles > Event ID 7030 — Basic Service Operations

Article | History

Event ID 7030 — Basic Service Operations

Updated: January 6, 2009 at http://technet.microsoft.com/en-us/library/dd349385(WS.10).aspx

Applies To: Windows Server 2008 R2

Service Control Manager transmits control requests to running services and driver services. It also maintains status information about those services, and reports configuration changes and state changes.

Event Details

Product:	Windows Operating System
ID:	7030
Source:	Service Control Manager
Version:	6.1
Symbolic Name:	EVENT_SERVICE_NOT_INTERACTIVE
Message:	The %1 service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

Resolve

Change the interact with desktop setting

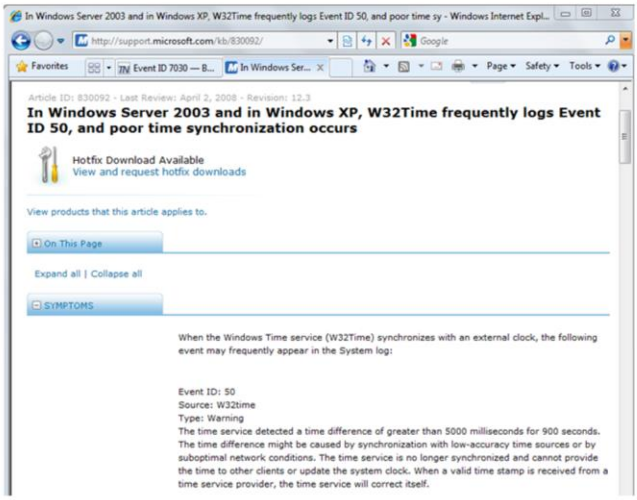
This error occurs if the service has been configured to allow the service to interact with the desktop. Interactive services can display a user interface and receive user input. If you allow the service to interact with the desktop, any information that the service displays on the desktop will also be displayed on an interactive user's desktop.

Forrás: http://social.technet.microsoft.com/wiki/contents/articles/event-id-7030-basic-service-operations.aspx

Információ gyűjtés folytatása

- További naplófájlok:
  - C:\Windows\System32\LogFiles
  - Alkalmazás-specifikus könyvtárak
- Keresés hibakód alapján
  - http://support.microsoft.com (KB cikkek)
  - http://www.eventid.net/

MS Knowledge Base cikkek



- Hibajelenség
- Megoldások:
  - Hotfix
  - Workaround
  - Ismert hiba
  - ...

Hibakeresés eszközei

Ha a hibajelzésből/naplóból nem egyértelmű, hogy mi a gond:

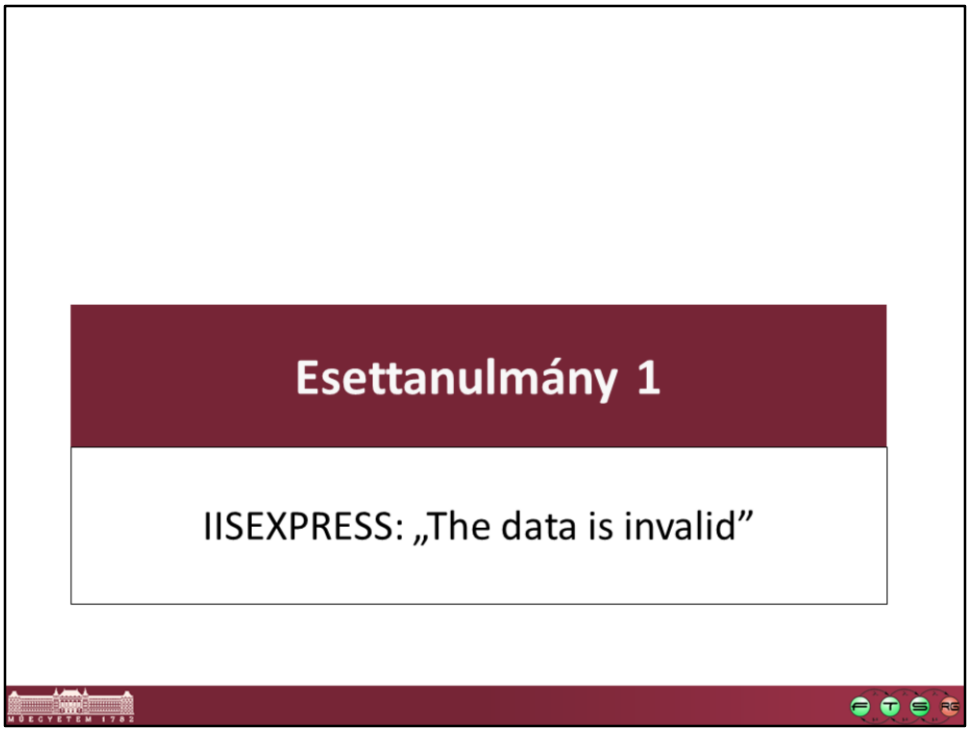
- Mi fut pontosan, mit használ?
  - Process Explorer
- Mit csinál pontosan?
  - Process Monitor
- Mit kommunikál a hálózaton?
  - Protokoll analizátor, pl. Wireshark
- Mennyi erőforrást használ?
  - Performance Monitor, Resource Monitor

Hibakeresés eszközei (2)

- Előbbiek passzív eszközök
  - Néha csak ezt lehet (pl. éles szerver)

Ha be is lehet avatkozni („intrusive”):

- Memória dump elmentése
  - Pl. sysinternals procdump
- Debugger csatlakoztatása
  - Pl. WinDbg

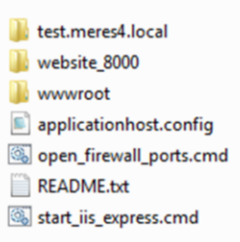


A következőkben néhány megtörtént eseten keresztül szemléltetjük, hogy a korábban felsorolt hibakereső eszközökkel, némi OS-ismerettel, valamint kitartással és szerencsével meg lehet találni elsőre rejtélyesnek tűnő hibák okát is.

Környezet: IIS Express

- IIS Express: web szerver fejlesztői változata

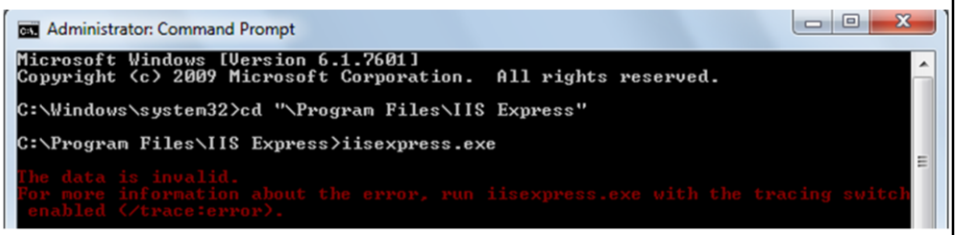
- Mérés labor 4:
  - Példa webszerver HTTP kérésekhez
  - Windows 7 virtuális gépben



- Félévkezdés előtt: minden megy a
  - saját gépemen,
  - végleges környezetben is

„Az előbb még ment minden…”

- Utolsó utáni ellenőrzés:
  - Virtuális gép állapotmentésének eldobása után



„The data is invalid.”

C:\Program Files\IIS Express>iisexpress.exe
The data is invalid. For more information about the error, run iisexpress.exe with the tracing switch enabled (/trace:error).

Hiba részletei

- `/trace:error` kapcsoló esetén is ugyanez
- Láthatóan konfigurációs hiba
  - Még a trace beállításokat sem tudja feldolgozni
  - Próbáljuk a beépített fájllal
    - `C:\Program Files\IIS Express>iisexpress.exe /config:"c:\Program Files\IIS Express\config\templates\PersonalWebServer\applicationhost.config" /trace:error`
  - Eredmény ugyanez, semmi részlet

Hiba részletei (2)

- Kimerítő keresés az indítási módok között
  - `iisexpress.exe`-nek nem maradt több kapcsolója
- `appcmd.exe`: parancssori felület

```
C:\Program Files\IIS Express>appcmd.exe list config
ERROR ( hresult:8007000d, message:Command execution failed.
The data is invalid.
 )

C:\Program Files\IIS Express>
```

- Végre van egy hibakódunk!
  - gg: 8007000d → főleg Windows Update hibák
  - gg: 8007000d iis → web.config hiba, nem telepített modulok | nálunk ez nem lehet, hisz ez a config eddig ment

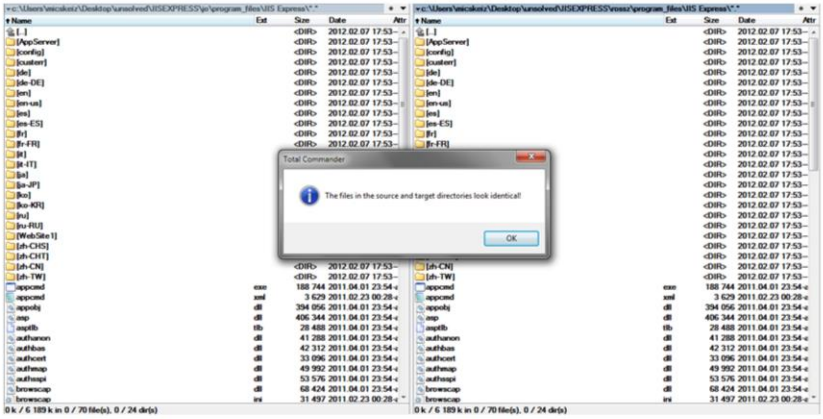
IIS újratelepítés (cheat:)

- Quick & dirty megoldás: IIS újratelepítés
  - Így működik ugyanazon a VM-en, ugyanaz a webhely
- Közvetlen probléma megoldva,
  - de nem tudjuk mi volt a gond…
  - jó lenne tudni :-)
- Hasonlítsuk össze a jó és a rossz állapotot!

Fájlok összehasonlítása

Fájlok megegyeznek:

- C:\program files\iis express; Documents\IISExpress; C:\inetpub; .NET FW\config

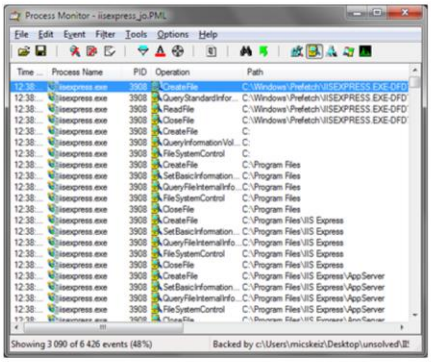


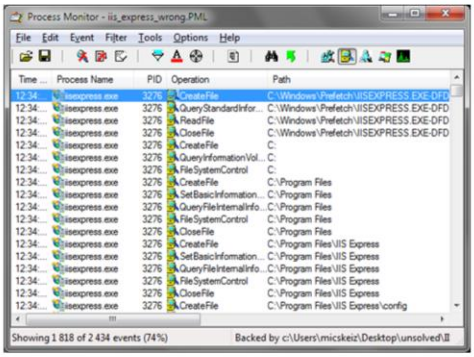
Registry összehasonlítása

- HKEY_LOCAL_MACHINE\Software alatt megegyezik
- IIS szövegre keresve látszólag megegyezik a jó és a rossz VM registry tartalma
- → Nézzük akkor mit csinál az iisexpress.exe

Futások összehasonlítása

- Fájl, registry kérések elkapása (Process Monitor)
- Események: 3090 (jó) vs. 1818 (rossz)

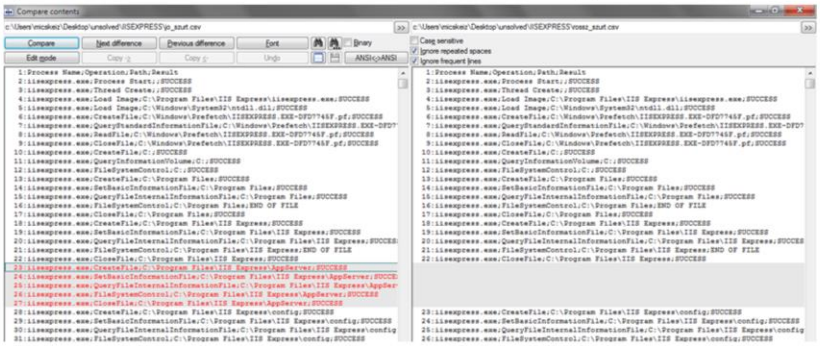




- Nehéz meglátni a különbséget

Futások összehasonlítása (2)

- Futás exportálása CSV-be
- Operation, Path, Result mezők megtartása



- 59 helyen különbözik, látszólag ugyanolyan visszatérési érték után tér el

Kifogytunk az ötletekből…

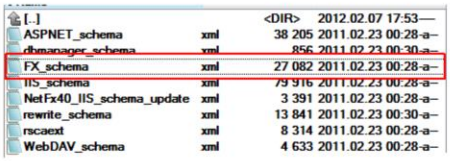
- Vissza az elejére
  - Hátha ki lehet listázni a konfigurációt
  - Nézzük meg az appcmd.exe-t még egyszer

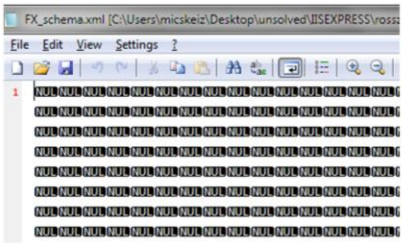
```
C:\Program Files\IIS Express>appcmd.exe list module

ERROR ( message:Configuration error MODULE
Filename: C:\Program Files\IIS
Express\config\schema\FX_schema.xml
Line Number: 0
Description: Configuration file is not well-formed
XML. )
```

Nyertünk: FX_schema.xml

- Mi van az FX_schema.xml-ben?





- A fájl látszólag megvan, de csupa NUL a tartalma
- (Snapshot eldobása közben sérült meg?)

Esettanulmány 2

SQL Server Upgrade hiba

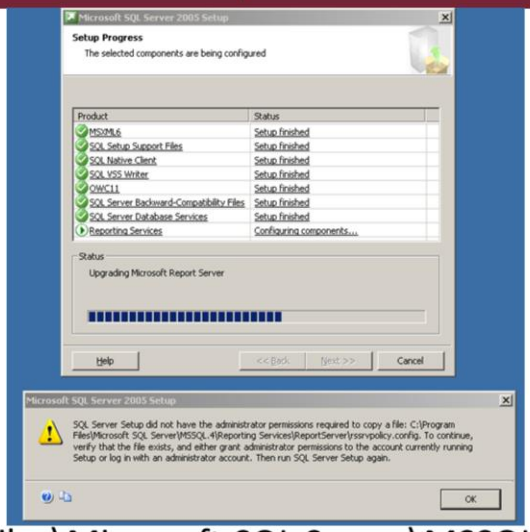
SQL Server upgrade

- D:\>setup.exe SKUUPGRADE=1

Leírás: **SKUUPGRADE of Reporting Services fails with could not write rssrvpolicy.config,**
http://social.technet.microsoft.com/Forums/en/sqlsetupandupgrade/thread/c75f35c7-f00d-45df-bdba-464ca5bd011a

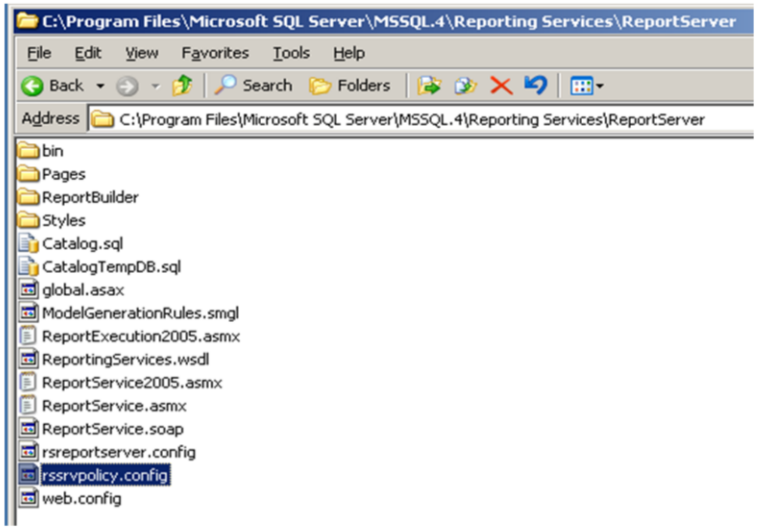
Vagy magyarul: **SCE 2007 vs. SQL 2005 Express**
http://micskeiz.wordpress.com/2007/08/27/sce-2007-vs-sql-2005-express/

Hiba a telepítés során



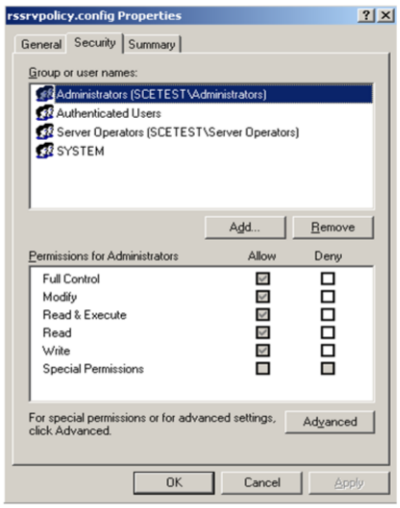
C:\Program Files\Microsoft SQL Server\MSSQL.4
\Reporting Services\ReportServer\rssrvpolicy.config

A fájl pedig létezik…



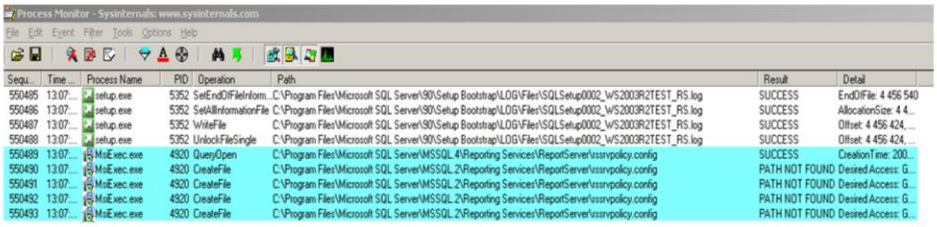
És van hozzá jogosultságunk is… ??

- A Rendszergazda felhasználó nevében ment a telepítő
- De a hibaüzenet szerint jogosultsági gond lehet



Process Monitor

- Pár százezer esemény közül kikeressük a relevánsakat:



- Ki látja mi a hiba?☺

Nem az a gondja, hogy MSSQL.4-ben lévő cél fájlt nem tudja írni, hanem az MSSQL.2-ben lévő forrásfájlt nem találja (persze, mert nem is abban a könyvtárban kéne keresnie!)

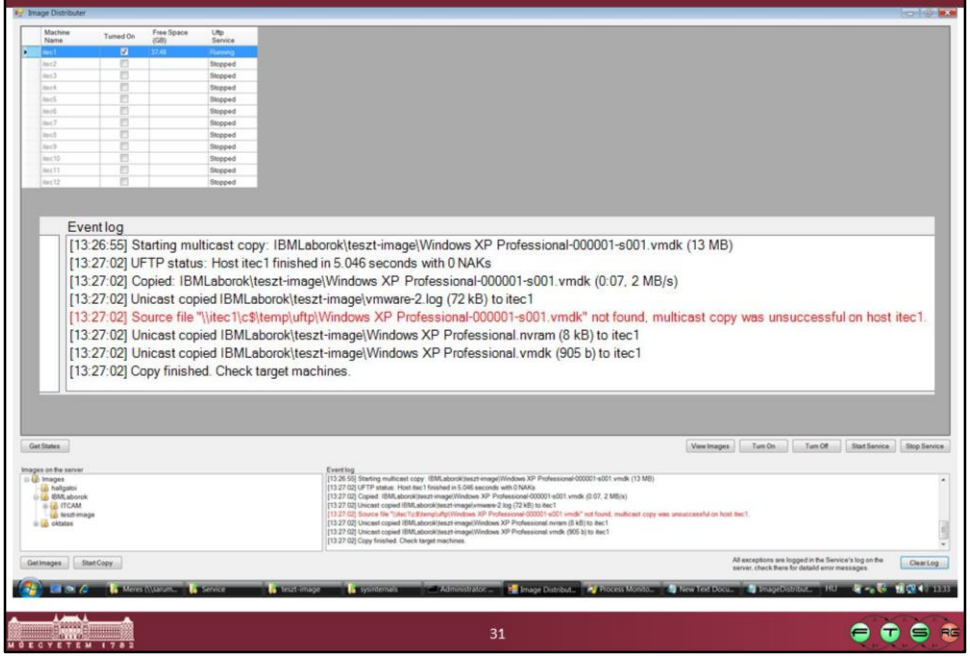
Tanulság

- Aljas hiba volt, mert megtévesztő az eredeti hibaüzenet…
- Ne higgyünk a hibaüzeneteknek☺
- Vannak eszközök, amivel meg lehet nézni, hogy mi történik a háttérben!

Esettanulmány 3

NAME NOT FOUND

„File not found” hiba

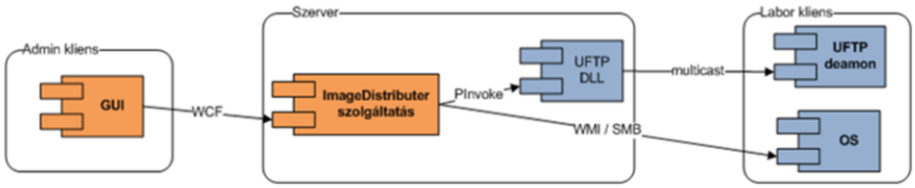


Részletes leírás: http://micskeiz.wordpress.com/2009/09/24/name-not-found-%E2%80%93-egy-furcsa-fajl-hozzaferesi-hiba/

Az alkalmazás működése

- Cél: adott könyvtár szétmásolása sok kliensre
  - Tipikusan virtuális gépek (5-10 GB)
- Nagyobb fájlokat multicast copy másolja (UFTP) egy ideiglenes könyvtárba
- Végén SMB megosztáson keresztül áthelyezi a végleges helyére

Az alkalmazás



Alkalmazás saját naplója

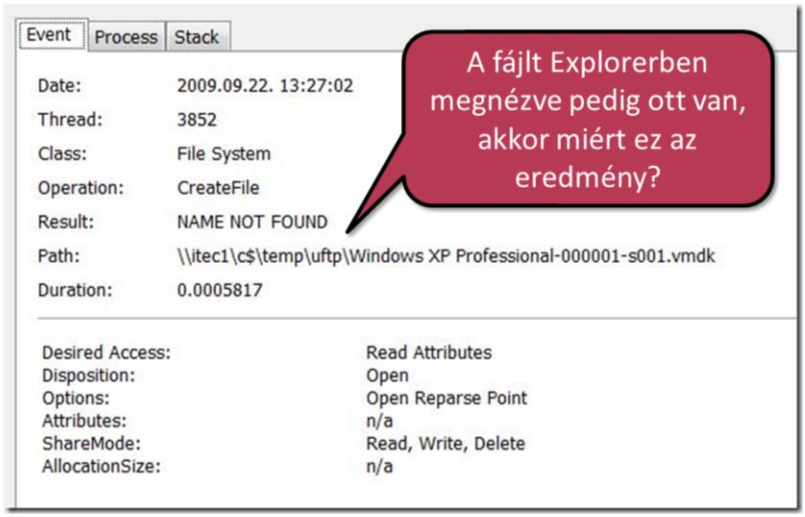
2009.09.22. 11:21:14:
Category: Info, RecursiveCopyFolders, CopyImage
Title: Info
Message: Unicast copied IBMLaborok\teszt-image\vmw
Severity: Information

2009.09.22. 11:21:14:
Category: Info, RecursiveCopyFolders, CopyImage
Title: Info
Message: Source file "\\itec1\c$\temp\uftp\Windows XP Professional-000001-s001.vmdk" not found, multicast copy was unsuccessful on host itec1.
Severity: Information

2009.09.22. 11:21:14:
Category: RecursiveCopyFolders, CopyImage
Title: TracerExit
Message: End Trace: Activity '814d6f3a-4604-475f-8ab3-7ff6154b386b' in method 'ImageDistributer.Service.ImageDistributerService.RecursiveCopyFolders' at 17877593865 ticks (elapsed time: 6,018 seconds)
Severity: Stop

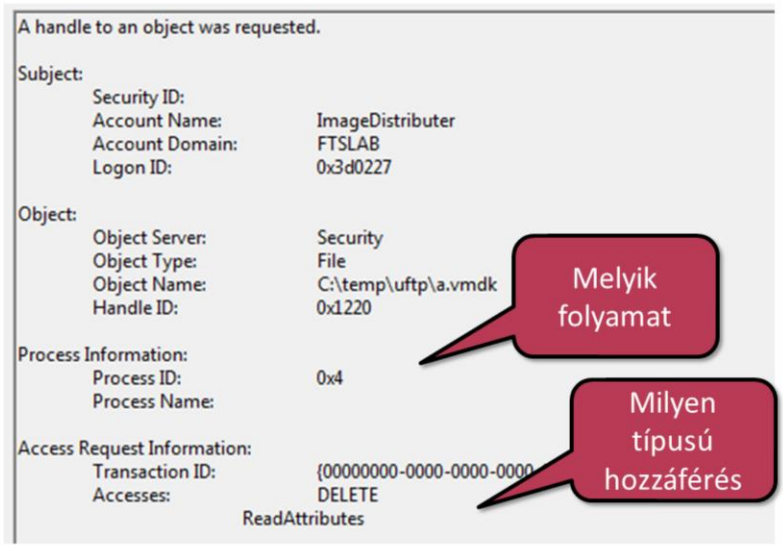
A saját részletes naplóban is csak ugyanaz a hiba volt

A fájl hozzáférés Process Monitorban



NTFS szintű naplózás beállítása (SACL)

Bejegyzés a biztonsági naplóban



Fájl hozzáférések sorrendje

Folyamat (PID)	Felhasználó	Leíró	Hozzáférési maszk	Szöveg
System (4)	ImageDistributer	0x1220	DELETE, ReadAttributes	A handle to an object was requested.
System (4)	ImageDistributer	0x1220	ReadAttributes	An attempt was made to access an object.
System (4)	ImageDistributer	0x1220	DELETE	An attempt was made to access an object.
System (4)	ImageDistributer	0x1220		An object was deleted.
System (4)	ImageDistributer	0x1220		The handle to an object was closed.
uftpd.exe (0xbf0)	SYSTEM	0x10c	WriteData, AppendData...	A handle to an object was requested.
uftpd.exe (0xbf0)	SYSTEM	0x10c	WriteData, AppendData	An attempt was made to access an object.
uftpd.exe (0xbf0)	SYSTEM	0x10c		The handle to an object was closed.

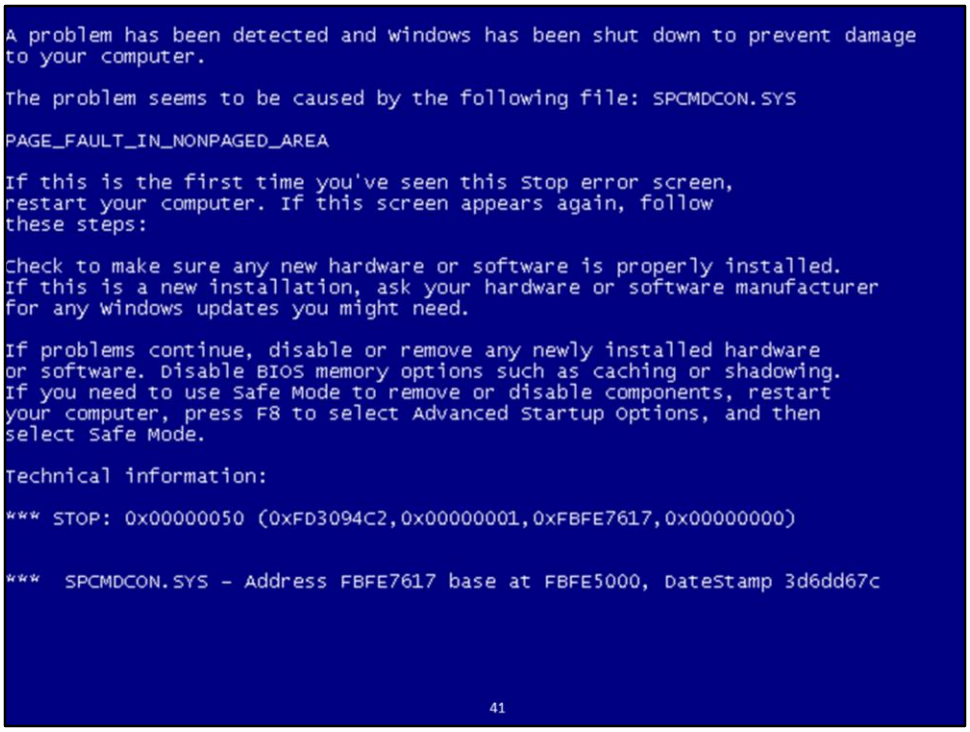
Megoldás:

- Az uftd.exe még írni akarta és fogta a fájlt az ImageDistributer hozzáférése előtt

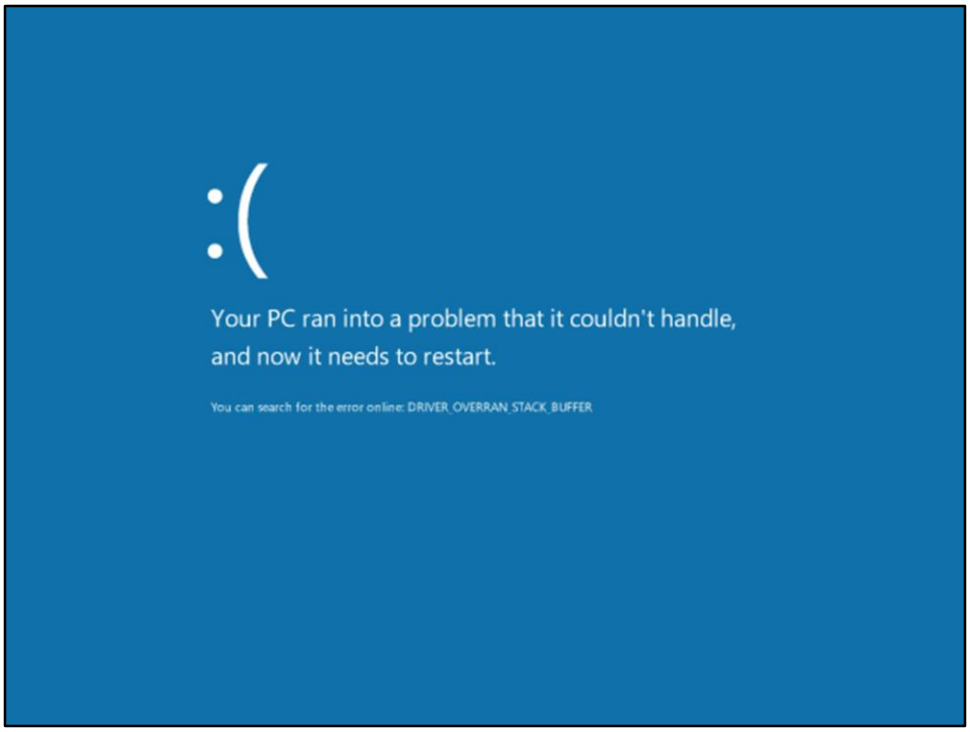
Tanulság

- Tudni kell, hogy intézi az OS az I/O kéréseket
- Ismerni kell az OS részletes naplózási lehetőségeit

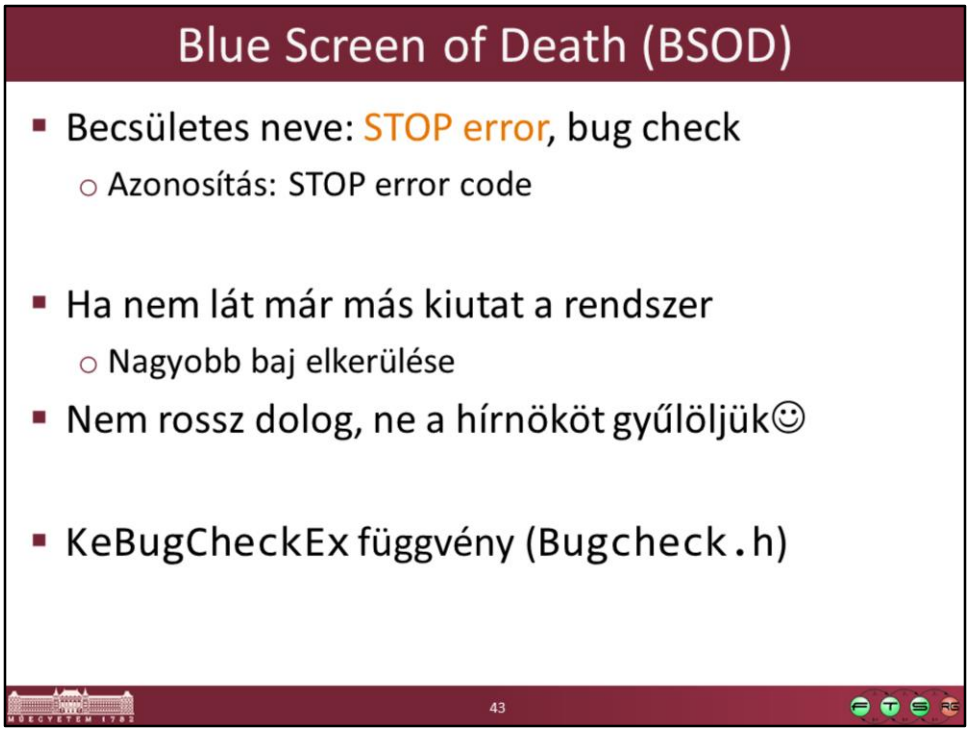
Ha nagy baj van



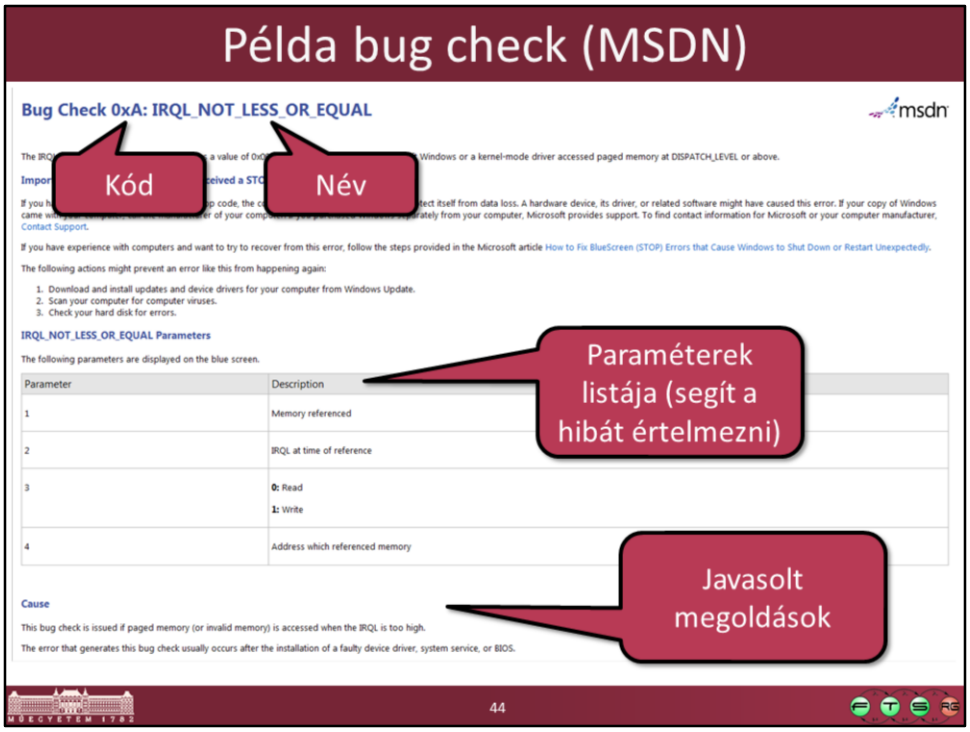
Ez a klasszikus BSOD képernyő



Ez a Windows 8-ban bevezetett új BSOD képernyő



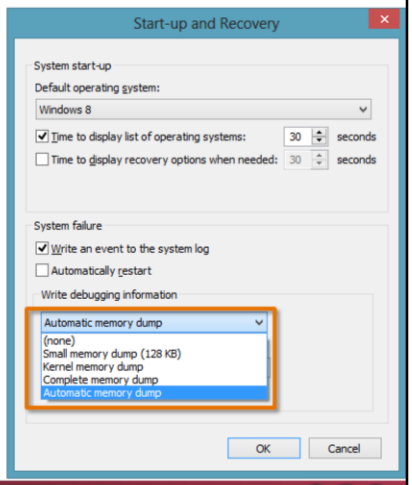
Bug Check Codes, http://msdn.microsoft.com/en-us/library/hh994433.aspx



Forrás: http://msdn.microsoft.com/en-us/library/ff560129(v=VS.85).aspx

Crash dump

- Memória részlet és CPU állapot elmentése
- Lapozófájlba írja ki ideiglenesen
- Fajtái:
  - Small memory dump
  - Kernel memory dump
  - Complete memory dump
  - Automatic memory dump

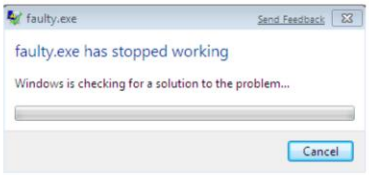


MSDN. **Crash Dump Files,** http://msdn.microsoft.com/en-us/library/ff539316.aspx

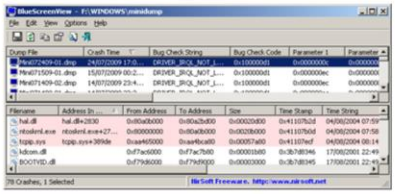
Ask the Core Team. „**Windows 8 and Windows Server 2012: Automatic Memory Dump**”, http://blogs.technet.com/b/askcore/archive/2012/09/12/windows-8-and-windows-server-2012-automatic-memory-dump.aspx

Crash dump elemzése

- Microsoft Error Reporting
  - MS szerverének elküldi
  - Elemzés, összehasonlítás
  - Visszajelzés, esetleg megoldás



- NirSoft (Nir Sofer): BlueScreenView
  - http://www.nirsoft.net
  - Meghajtók, hibakódok



Crash dump elemzése (haladó)

- Saját magunk:
  - WinDbg
  - `!analyze -v` parancs
  - Hibázó modul azonosítása

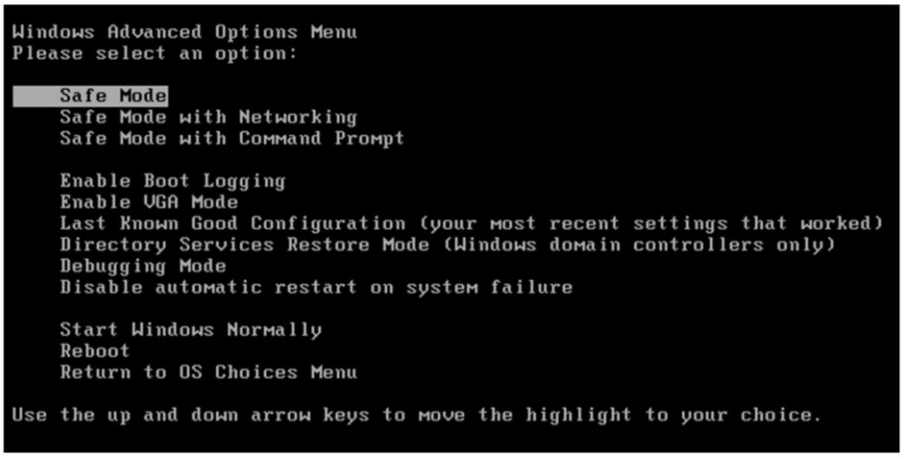
How to read the small memory dump files that Windows creates for debugging, http://support.microsoft.com/kb/315263/en-us

DEMO Blue Screen of Death (BSOD)

- Hibajelentés küldése (Error reporting)
- Memory dump készítése
- Minidump elemzése WinDgb-ben

Speciális módú indítás (pre Windows 8)

- F8 a Windows logó előtt



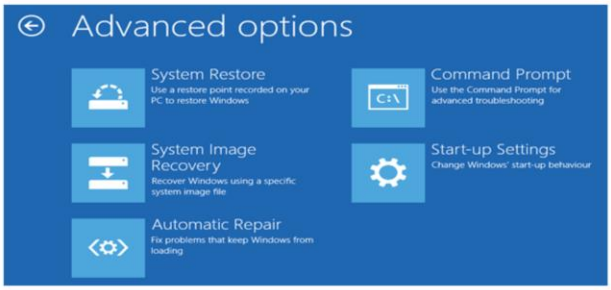
A description of the Safe Mode Boot options in Windows XP
http://support.microsoft.com/default.aspx?scid=kb;en-us;315222

Speciális módú indítási opciók

- Safe mode (Csökkentett mód)
  - csak a beépített meghajtók indulnak el
  - csak a legszükségesebb szolgáltatások
- Safe mode with Networking
  - hálózat is van
- Last Known Good Configuration

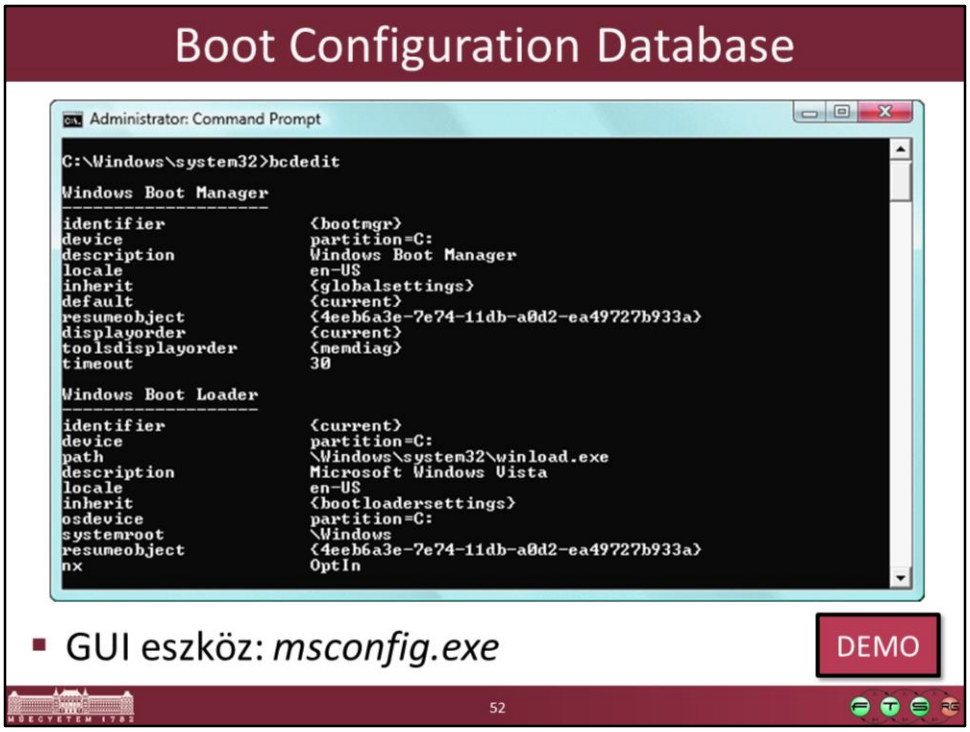
Speciális módú indítás (post Windows 8)

- Áttervezték a felületet és az indítás menetét
- (Túl gyorsan indulnak a modern gépek:)



Bővebben lásd:

- Building Windows 8 blog, Reengineering the Windows boot experience, URL: http://blogs.msdn.com/b/b8/archive/2011/09/20/reengineering-the-windows-boot-experience.aspx
- Bővebben lásd: Building Windows 8 blog, Designing for PCs that boot faster than ever before, URL: http://blogs.msdn.com/b/b8/archive/2012/05/22/designing-for-pcs-that-boot-faster-than-ever-before.aspx



Forrás: Mark Russinovich: Inside the Windows Vista kernel: Part 2, Technet Magazine

„Windows Vista has enhanced several aspects of startup and shutdown. Startup has improved with the introduction of the Boot Configuration Database (BCD) for storing system and OS startup configuration, a new flow and organization of system startup processes, new logon architecture, and support for delayed-autostart services. Windows Vista shutdown changes include pre-shutdown notification for Windows services, Windows services shutdown ordering, and a significant change to the way the OS manages power state transitions.

One of the most visible changes to the startup process is the absence of Boot.ini from the root of the system volume. That's because the boot configuration, which on previous versions of Windows was stored in the Boot.ini text file, is now stored in the BCD. One of the reasons Windows Vista uses the BCD is that it unifies the two current boot architectures supported by Windows: Master Boot Record (MBR) and Extensible Firmware Interface (EFI). MBR is generally used by x86 and x64 desktop systems, while EFI is used by Itanium-based systems (though desktop PCs are likely to ship with EFI support in the near future). The BCD abstracts the firmware and has other advantages over Boot.ini, like its support for Unicode strings and alternate pre-boot executables.

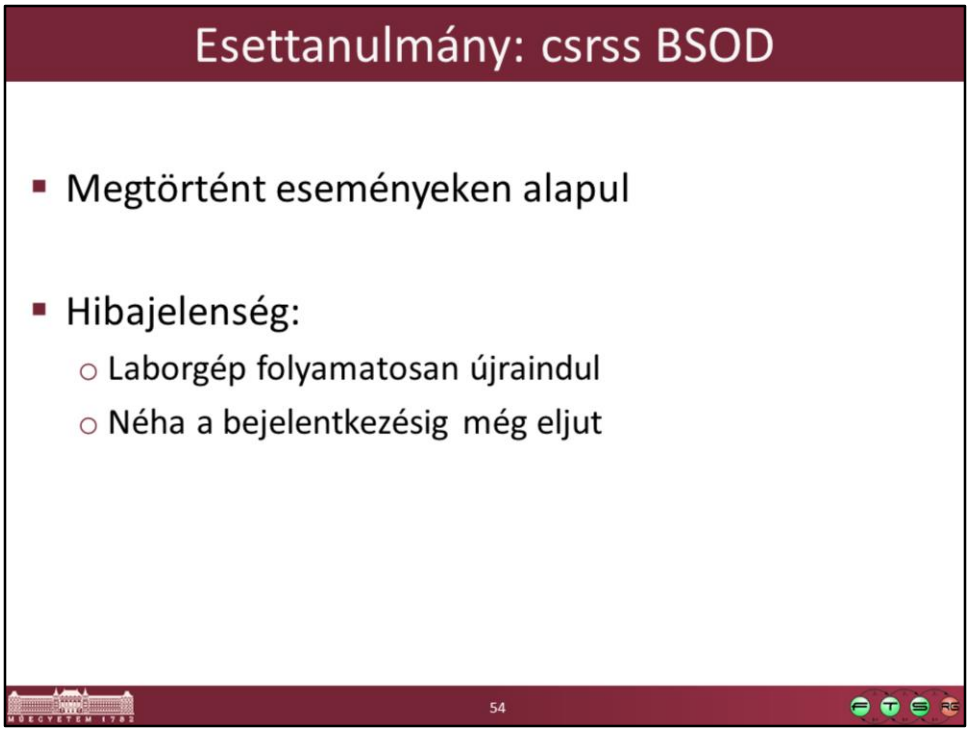
The BCD is actually stored on disk in a registry hive that loads into the Windows registry for access via registry APIs. On PCs, Windows stores it in \Boot\Bcd on the system volume. On EFI systems, it's on the EFI system partition. When the hive is loaded, it appears under HKLM\Bcd00000000, but its internal format is undocumented so editing it requires the use of a tool like %SystemRoot%\System32\Bcdedit.exe. Interfaces for manipulating the BCD are also made available for scripts and custom editors through Windows Management Instrumentation (WMI) and you can use the Windows System Configuration Utility (%SystemRoot%\System32\Msconfig.exe) to edit or add basic parameters, like kernel debugging options.

The BCD divides platform-wide boot settings, like the default OS selection and the boot menu timeout, from OS-specific settings such as OS boot options and the path to the OS boot loader. For example, Figure 3 shows that when you run Bcdedit with no command-line options, it displays platform settings in the Windows Boot Manager section at the top of the output, followed by OS-specific settings in the Windows Boot Loader section.

When you boot a Windows Vista installation, this new scheme divides the tasks that were handled by the operating system loader (Ntldr) on previous versions of Windows into two different executables: \BootMgr and %SystemRoot%\System32\Winload.exe. Bootmgr reads the BCD and displays the OS boot menu, while Winload.exe handles operating-system loading. If you're performing a clean boot, Winload.exe loads boot-start device drivers and core operating system files, including Ntoskrnl.exe, and transfers control to the operating system; if the system is resuming from hibernation, then it executes %SystemRoot%\System32\Winresume.exe to load the hibernation data into memory and resume the OS. Bootmgr also includes support for additional pre-boot executables. Windows Vista comes with the Windows Memory Diagnostic (\Boot\Memtest.exe) pre-configured as an option for checking the health of RAM, but third parties can add their own pre-boot executables as options that will display in Bootmgr's boot menu.”

Esettanulmány 4

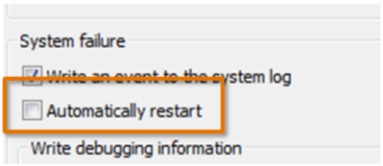
csrss BSOD



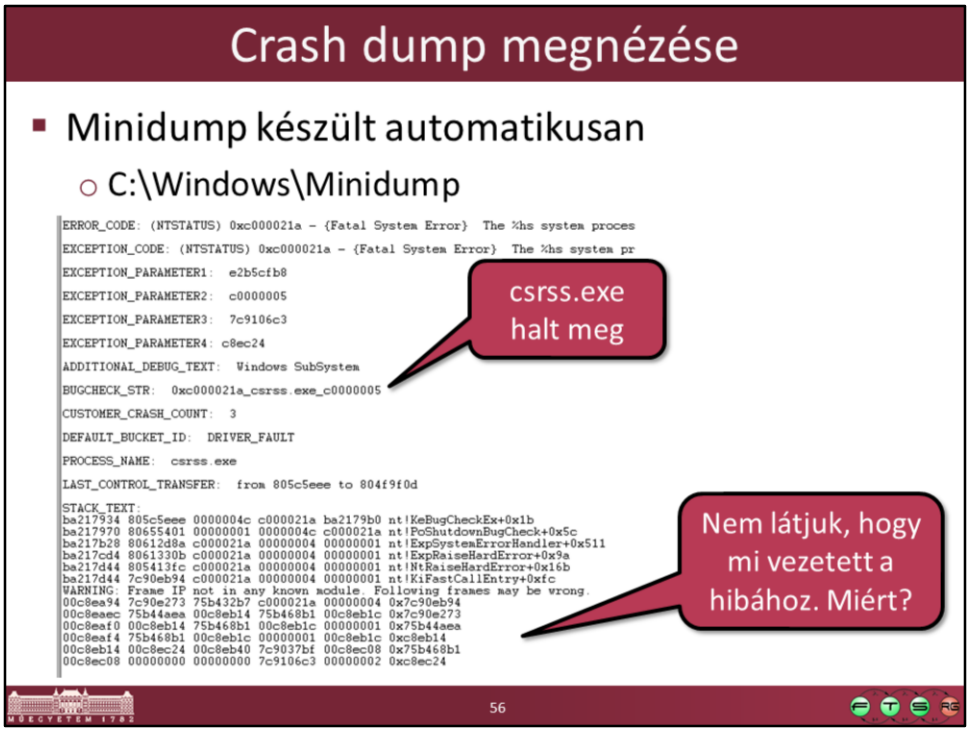
Részletes leírás: **0xC000021A: csrss kék halál a laborban**,
http://micskeiz.wordpress.com/2009/05/21/0xc000021a-csrss-kek-halal-a-laborban/

Első lépések

- Automatikus újraindítás kikapcsolása



- STOP hibakód így kiderül:
  - C000021A, {e2a5ee98, c0000005, 7c9106c3, 69ec24}
  - MSDN dokumentáció: Bug Checks
    - 0xC000021A: STATUS_SYSTEM_PROCESS_TERMINATED



Mert ez minidump, csak a kernel legfontosabb adatstruktúrái vannak benne. De nincs benne felhasználói módú memóriaterület, így a felhasználói módú veremtartalom sem.

Complete memory dump kiválasztása

- Az adott gépen nem lehetett teljes memória dumpot választani
- ???
- Windows XP SP2, 32 bit, 4GB RAM
  - KB274598 Complete memory dumps are not available on computers that have 2 or more gigabytes of RAM
- Boot.ini: /MaxMem=2000 segítségével a memória korlátozása

Complete memory dump analízise 1.

```
EXCEPTION_RECORD:  0069ec08 -- (.exr 0x69ec08)
ExceptionAddress: 7c9106c3
  (ntdll!RtlAllocateHeap+0x000001da)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 00000001
   Parameter[1]: 75e9193e
Attempt to write to address 75e9193e
```

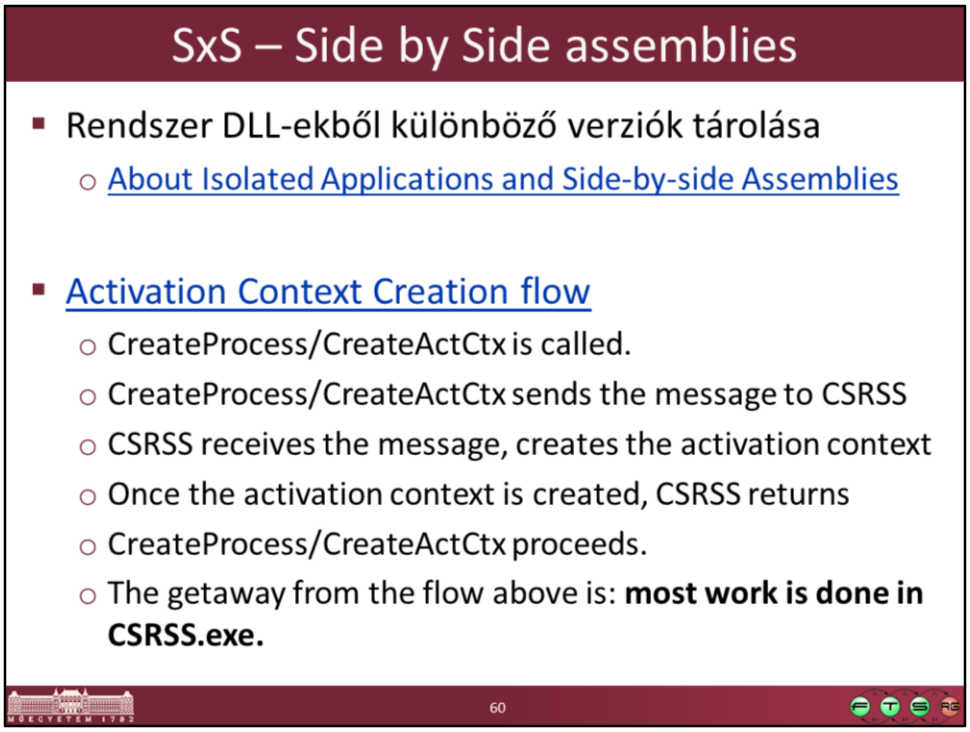
Problémát okozó utasítás

Complete memory dump analízise 1.

Ez akar hibás memóriát foglalni

Ki az az **sxs** modul?

```
STACK_TEXT:
b202f834 805e5eaa 0000004c c000021a b20269b0 ntdllKeBugCheckEx+0x1b
b207                                                    eck+0x5c
b20                                                     andler+0x511
b20                                                     or+0x9a
b20                                                     r+0x16b
b20                                                     +0xfc
006                                                     CallRet
006                                                     rror+0xc
006                                                     dExceptionFilter+0xb3
0069                                                    estThread+0x4d4
0069eb1c 7c9                                            _except_handler3+0x61
0069eb40 7c9                 e08 0069ffe4 0069ec24 ntdll!ExecuteHandler2+0x26
0069ebf0 7                   000000 0069ec24 0069ec08 ntdll!ExecuteHandler+0x24
0069ebf0                     00000000 0069ec24 0069ec08 ntdll!KiUserExceptionDispatcher+0xe
0069f110                     00160000 00000000 0000009c ntdll!RtlAllocateHeap+0x1da
0069f15                      0000005b 75e9c578
     sxs!CSxsPointerBase<CXMLNamespaceManager::CNamespacePrefix,CSxsPointer<CXMLNamespaceManager::CNamespacePrefix
     ,CXMLNamespaceManager::CNamespacePrefix::ms_szTypeName> >::HrAllocateBase+0x59
0069f3dc 75e938d2 00188e10 00000000 00000005 sxs!CXMLNamespaceManager::OnCreateNode+0x12e
0069f440 75e9435f 00176fd8 00188e10 00000000 sxs!CNodeFactory::CreateNode+0xa3
0069f4c8 75e98baa 00188e10 00000005 001884e8 sxs!XMLParser::Run+0x2fc
0069f834 75e99a0f 001884e8 0016af78 001884e8 sxs!SxspIncorporateAssembly+0x8b8
0069f880 75e998cd 001884e8 00000000 0069fde0 sxs!SxspCloseManifestGraph+0x98
0069fd1c 75b5a5ed 0069fd7c 0069fe38 0069ff94 sxs!SxsGenerateActivationContext+0x54c
0069fdbc 75b5a90d 0000005e 000006e8 0169fde0 basesrv!BaseSrvSxsCreateActivationContextFromStruct+0x194
0069fe80 75b54e96 00000110 000006e8 0069feec basesrv!BaseSrvSxsCreateProcess+0x160
0069fed0 75b44a47 000006e8 0069ffd8 00000005 basesrv!BaseSrvCreateProcess+0xeb
0069fff4 00000000 00000000 00000000 00000000 CSRSRV!CsrApiRequestThread+0x431
-,-'-@
```



MSDN. „**About Isolated Applications and Side-by-side Assemblies**”, URL: http://msdn.microsoft.com/en-us/library/aa374029%28v=vs.85%29.aspx

Junfeng Zhang's Windows Programming Notes. „**Activation Context Creation flow**”, 12 Jun 2007. URL: http://blogs.msdn.com/b/junfeng/archive/2007/06/12/activation-context-creation-flow.aspx

Nyomon vagyunk

- Nem okozhat az SxS újraindulást?
- support.microsoft.com oldalon keresés:
- The computer may restart when you add a manifest that has the Windows Vista extension to an .exe file or to a .dll file in Windows XP Service Pack 2 (SP2) (KB 921337)
  - sxs.dll verzió a gépeken: 5.1.2600.2180 (SP2-es)

Megoldás

- KB 921337 hotfix telepítése csökkentett módban
  - Ez frissíti az sxs.dll-t
- Újraindítás…
- Reménykedés…
- Nincs BSOD…
- Örülünk☺

Összefoglalás

Meg lehet oldani az összetett hibákat is

- Mi kell hozzá:
  - Operációs rendszer ismerete
  - Debugger
  - Google, KB cikkek, dokumentáció
  - Kitartás & gyakorlás
- Virtuális labor: *Windows hibakeresés*

További esettanulmányok

- Mark Russinovich: **Case of the Unexplained Presentations**, webcasts
  http://technet.microsoft.com/en-us/sysinternals/bb963887.aspx

http://technet.microsoft.com/en-us/sysinternals/bb963887.aspx