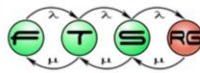


Hibakeresés Windowson

dr. Micskei Zoltán

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



Utolsó módosítás: 2014. 02. 24.

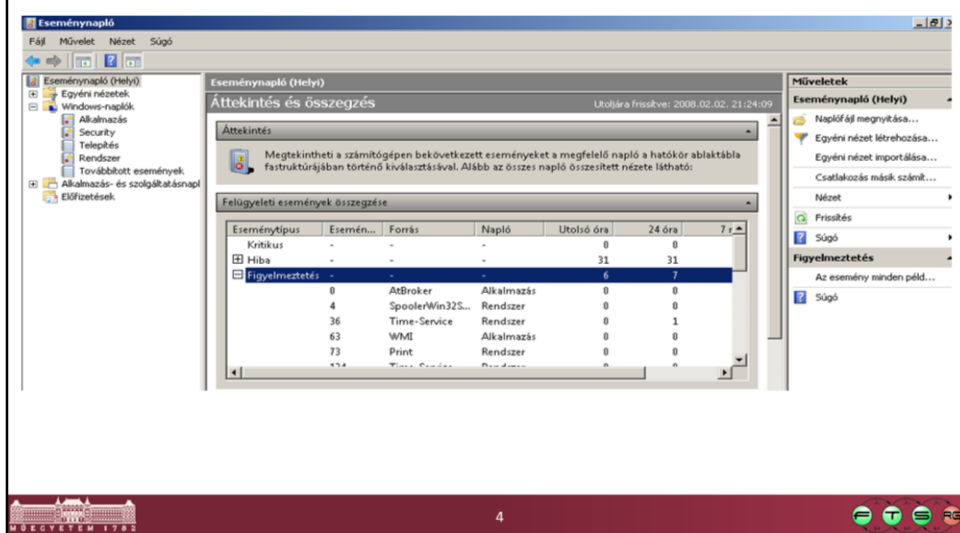
Hiba esetén

- **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

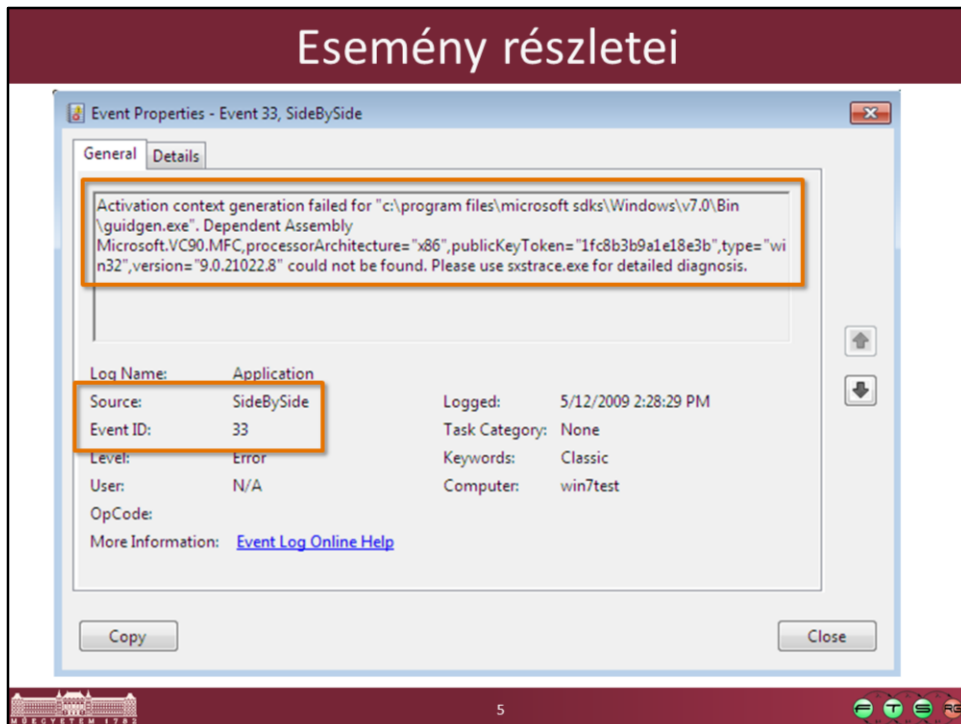


Az Eseménynapló a Windows platform központi naplózó komponense, amibe mind az operációs rendszer, mind a külső alkalmazások írhatnak.

Jól kereshető és szűrhető, sokféle programozási nyelvből elérhető (C++, .NET nyelvek, szkriptek...)

Hibakeresési, diagnosztikai feladatok esetén ez az egyik elsődleges információforrásunk.

Esemény részletei



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/6d349385\(ws.10\).aspx](http://technet.microsoft.com/en-us/library/6d349385(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.

6


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



The screenshot shows a browser window displaying a Microsoft Knowledge Base article. The address bar shows the URL: <http://support.microsoft.com/kb/830092/>. The article title is "In Windows Server 2003 and in Windows XP, W32Time frequently logs Event ID 50, and poor time synchronization occurs". Below the title, there is a "Hotfix Download Available" section with a link to "View and request hotfix downloads". The article content includes a "SYMPTOMS" section with the following text: "When the Windows Time service (W32Time) synchronizes with an external clock, the following event may frequently appear in the System log: Event ID: 50, Source: W32time, Type: Warning. The time service detected a time difference of greater than 5000 milliseconds for 900 seconds. The time difference might be caused by synchronization with low-accuracy time sources or by suboptimal network conditions. The time service is no longer synchronized and cannot provide the time to other clients or update the system clock. When a valid time stamp is received from a time service provider, the time service will correct itself."

■ 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 analízátor, 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**

Esettanulmány 1

IISEXPRESS: „The data is invalid”

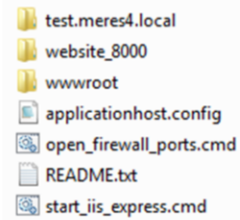
UNIVERSITÄT
MÜNCHEN 1793

Three circular icons: a green circle with a white 'T', a green circle with a white 'E', and a red circle with a white 'R'.

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.

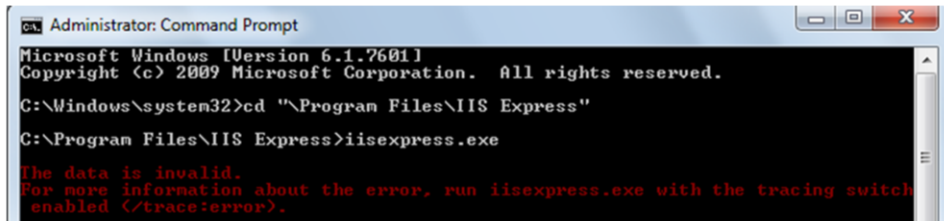
Környezet: IIS Express

- 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



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd "%Program Files%\IIS Express"
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).
```

„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 fájljal
 - 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

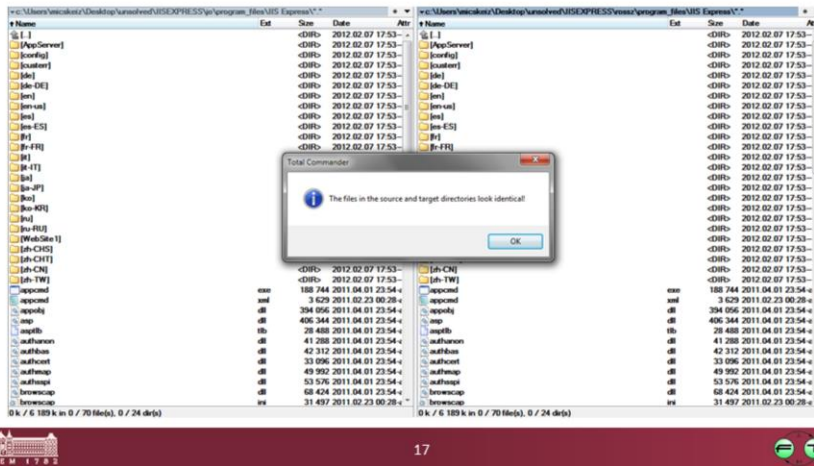
IIS újratelepítés (cheat:)

- 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)

Process Monitor - isexpress_jo.PML

Time	Process Name	PID	Operation	Path
12:30...	isexpress.exe	3900	CreateFile	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:30...	isexpress.exe	3900	QueryStandardInfor...	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:30...	isexpress.exe	3900	ReadFile	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:30...	isexpress.exe	3900	CreateFile	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:30...	isexpress.exe	3900	CreateFile	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:30...	isexpress.exe	3900	QueryInformationVol...	C:\
12:30...	isexpress.exe	3900	FileSystemControl	C:\
12:30...	isexpress.exe	3900	CreateFile	C:\Program Files
12:30...	isexpress.exe	3900	SetBasicInformation...	C:\Program Files
12:30...	isexpress.exe	3900	QueryFileInternalInfo...	C:\Program Files
12:30...	isexpress.exe	3900	FileSystemControl	C:\Program Files
12:30...	isexpress.exe	3900	CreateFile	C:\Program Files
12:30...	isexpress.exe	3900	CreateFile	C:\Program Files\IIS Express
12:30...	isexpress.exe	3900	SetBasicInformation...	C:\Program Files\IIS Express
12:30...	isexpress.exe	3900	QueryFileInternalInfo...	C:\Program Files\IIS Express
12:30...	isexpress.exe	3900	FileSystemControl	C:\Program Files\IIS Express
12:30...	isexpress.exe	3900	CreateFile	C:\Program Files\IIS Express
12:30...	isexpress.exe	3900	QueryFileInternalInfo...	C:\Program Files\IIS Express\App Server
12:30...	isexpress.exe	3900	SetBasicInformation...	C:\Program Files\IIS Express\App Server
12:30...	isexpress.exe	3900	QueryFileInternalInfo...	C:\Program Files\IIS Express\App Server
12:30...	isexpress.exe	3900	FileSystemControl	C:\Program Files\IIS Express
12:30...	isexpress.exe	3900	CreateFile	C:\Program Files\IIS Express\App Server
12:30...	isexpress.exe	3900	CreateFile	C:\Program Files\IIS Express\App Server
17:18...	isexpress.exe	3900	CreateFile	C:\Program Files\IIS Express\App Server

Showing 3 090 of 6 426 events (48%) Backed by c:\Users\mickeis\Desktop\unsolved\B...

Process Monitor - is_express_wrong.PML

Time	Process Name	PID	Operation	Path
12:34...	isexpress.exe	3276	CreateFile	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:34...	isexpress.exe	3276	QueryStandardInfor...	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:34...	isexpress.exe	3276	ReadFile	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:34...	isexpress.exe	3276	CreateFile	C:\Windows\Prefetch\IISExpress.EXE-0FD...
12:34...	isexpress.exe	3276	CreateFile	C:\
12:34...	isexpress.exe	3276	QueryInformationVol...	C:\
12:34...	isexpress.exe	3276	FileSystemControl	C:\
12:34...	isexpress.exe	3276	CreateFile	C:\Program Files
12:34...	isexpress.exe	3276	SetBasicInformation...	C:\Program Files
12:34...	isexpress.exe	3276	QueryFileInternalInfo...	C:\Program Files
12:34...	isexpress.exe	3276	FileSystemControl	C:\Program Files
12:34...	isexpress.exe	3276	CreateFile	C:\Program Files
12:34...	isexpress.exe	3276	CloseFile	C:\Program Files\IIS Express
12:34...	isexpress.exe	3276	SetBasicInformation...	C:\Program Files\IIS Express
12:34...	isexpress.exe	3276	QueryFileInternalInfo...	C:\Program Files\IIS Express
12:34...	isexpress.exe	3276	FileSystemControl	C:\Program Files\IIS Express
12:34...	isexpress.exe	3276	CloseFile	C:\Program Files\IIS Express
12:34...	isexpress.exe	3276	CreateFile	C:\Program Files\IIS Express\config

Showing 1 818 of 2 434 events (74%) Backed by c:\Users\mickeis\Desktop\unsolved\B...

- Nehéz meglátni a különbséget

Futások összehasonlítása (2)

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

```
1.Process Name:Operation:Path:Result
2.Llsexpress.exe:Process Start.:SUCCESS
3.Llsexpress.exe:Thread Create.:SUCCESS
4.Llsexpress.exe:Load Image:C:\Program Files\IIS Express\Llsexpress.exe:SUCCESS
5.Llsexpress.exe:Load Image:C:\Windows\System32\url.dll:SUCCESS
6.Llsexpress.exe>CreateFile:C:\Windows\Fetch\IISEXPRESS.EXE-SPD746F.pf:SUCCESS
7.Llsexpress.exe:QueryStandardInformationFile:C:\Windows\Fetch\IISEXPRESS.EXE-SPD746F.pf:SUCCESS
8.Llsexpress.exe:ReadFile:C:\Windows\Fetch\IISEXPRESS.EXE-SPD746F.pf:SUCCESS
9.Llsexpress.exe:CloseFile:C:\Windows\Fetch\IISEXPRESS.EXE-SPD746F.pf:SUCCESS
10.Llsexpress.exe>CreateFile:C:\SUCCESS
11.Llsexpress.exe:QueryInformationVolume:C:\SUCCESS
12.Llsexpress.exe:FileOpenControl:C:\SUCCESS
13.Llsexpress.exe>CreateFile:C:\Program Files:SUCCESS
14.Llsexpress.exe:SetBasicInformationFile:C:\Program Files:SUCCESS
15.Llsexpress.exe:QueryFileInternalInformationFile:C:\Program Files:SUCCESS
16.Llsexpress.exe:FileOpenControl:C:\Program Files:END OF FILE
17.Llsexpress.exe:CloseFile:C:\Program Files:SUCCESS
18.Llsexpress.exe>CreateFile:C:\Program Files\IIS Express:SUCCESS
19.Llsexpress.exe:SetBasicInformationFile:C:\Program Files\IIS Express:SUCCESS
20.Llsexpress.exe:QueryFileInternalInformationFile:C:\Program Files\IIS Express:SUCCESS
21.Llsexpress.exe:FileOpenControl:C:\Program Files\IIS Express:END OF FILE
22.Llsexpress.exe:CloseFile:C:\Program Files\IIS Express:SUCCESS
23.Llsexpress.exe>CreateFile:C:\Program Files\IIS Express\AppDev:SUCCESS
24.Llsexpress.exe:SetBasicInformationFile:C:\Program Files\IIS Express\AppDev:SUCCESS
25.Llsexpress.exe:QueryFileInternalInformationFile:C:\Program Files\IIS Express\AppDev:SUCCESS
26.Llsexpress.exe:FileOpenControl:C:\Program Files\IIS Express\AppDev:SUCCESS
27.Llsexpress.exe:CloseFile:C:\Program Files\IIS Express\AppDev:SUCCESS
28.Llsexpress.exe>CreateFile:C:\Program Files\IIS Express\conf:SUCCESS
29.Llsexpress.exe:SetBasicInformationFile:C:\Program Files\IIS Express\conf:SUCCESS
30.Llsexpress.exe:QueryFileInternalInformationFile:C:\Program Files\IIS Express\conf:SUCCESS
31.Llsexpress.exe:FileOpenControl:C:\Program Files\IIS Express\conf:SUCCESS

1.Process Name:Operation:Path:Result
2.Llsexpress.exe:Process Start.:SUCCESS
3.Llsexpress.exe:Thread Create.:SUCCESS
4.Llsexpress.exe:Load Image:C:\Program Files\IIS Express\Llsexpress.exe:SUCCESS
5.Llsexpress.exe:Load Image:C:\Windows\System32\url.dll:SUCCESS
6.Llsexpress.exe>CreateFile:C:\Windows\Fetch\IISEXPRESS.EXE-SPD746F.pf:SUCCESS
7.Llsexpress.exe:QueryStandardInformationFile:C:\Windows\Fetch\IISEXPRESS.EXE-SPD746F.pf:SUCCESS
8.Llsexpress.exe:ReadFile:C:\Windows\Fetch\IISEXPRESS.EXE-SPD746F.pf:SUCCESS
9.Llsexpress.exe:CloseFile:C:\Windows\Fetch\IISEXPRESS.EXE-SPD746F.pf:SUCCESS
10.Llsexpress.exe>CreateFile:C:\SUCCESS
11.Llsexpress.exe:QueryInformationVolume:C:\SUCCESS
12.Llsexpress.exe:FileOpenControl:C:\SUCCESS
13.Llsexpress.exe>CreateFile:C:\Program Files:SUCCESS
14.Llsexpress.exe:SetBasicInformationFile:C:\Program Files:SUCCESS
15.Llsexpress.exe:QueryFileInternalInformationFile:C:\Program Files:SUCCESS
16.Llsexpress.exe:FileOpenControl:C:\Program Files:END OF FILE
17.Llsexpress.exe:CloseFile:C:\Program Files:SUCCESS
18.Llsexpress.exe>CreateFile:C:\Program Files\IIS Express:SUCCESS
19.Llsexpress.exe:SetBasicInformationFile:C:\Program Files\IIS Express:SUCCESS
20.Llsexpress.exe:QueryFileInternalInformationFile:C:\Program Files\IIS Express:SUCCESS
21.Llsexpress.exe:FileOpenControl:C:\Program Files\IIS Express:END OF FILE
22.Llsexpress.exe:CloseFile:C:\Program Files\IIS Express:SUCCESS
23.Llsexpress.exe>CreateFile:C:\Program Files\IIS Express\conf:SUCCESS
24.Llsexpress.exe:SetBasicInformationFile:C:\Program Files\IIS Express\conf:SUCCESS
25.Llsexpress.exe:QueryFileInternalInformationFile:C:\Program Files\IIS Express\conf:SUCCESS
26.Llsexpress.exe:FileOpenControl:C:\Program Files\IIS Express\conf:SUCCESS
```

- 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

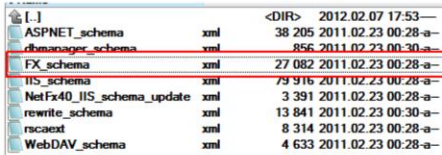
```
C:\Program Files\IIS Express>appcmd.exe list module
```

```
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. )
```

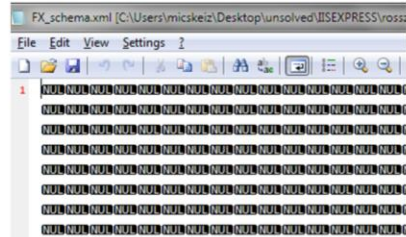


Nyertünk: FX_schema.xml

- Mi van az FX_schema.xml-ben?



File Name	Extension	Size	Modified
<DIR>		2012.02.07 17:53	
ASPNET_schema	xml	38 205	2011.02.23 00:28-a-
dbmanager_schema	xml	856	2011.02.23 00:30-a-
FX_schema	xml	27 082	2011.02.23 00:28-a-
IIS_schema	xml	79 916	2011.02.23 00:28-a-
NetFx40_IIS_schema_update	xml	3 391	2011.02.23 00:28-a-
rewrite_schema	xml	13 841	2011.02.23 00:30-a-
rscact	xml	8 314	2011.02.23 00:28-a-
WebDAV_schema	xml	4 633	2011.02.23 00:28-a-



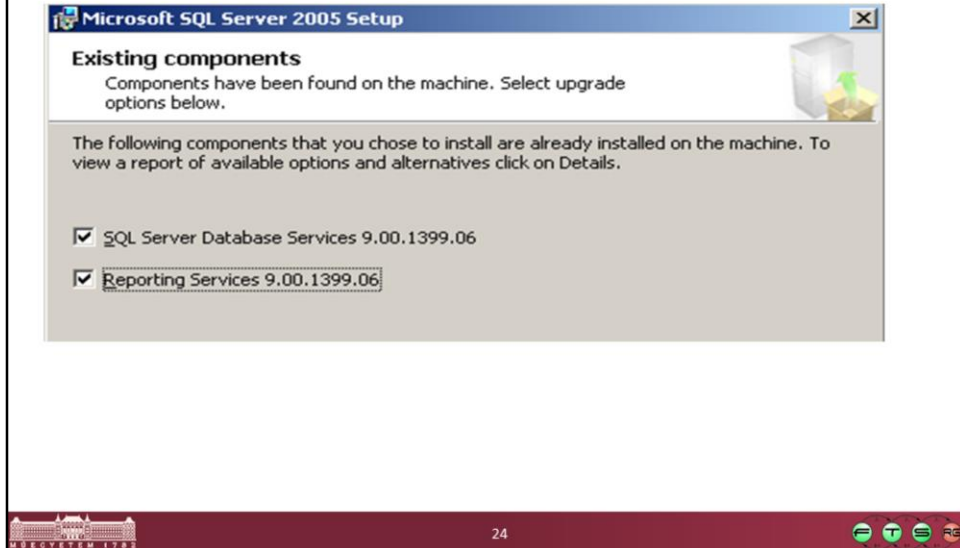
- A fájl látszólag megvan, de csupa NUL a tartalma
- (Snapshot eldobása közben sérült meg?)

Esettanulmány 2

SQL Server Upgrade hiba

SQL Server upgrade

- D:\>setup.exe SKUUPGRADE=1



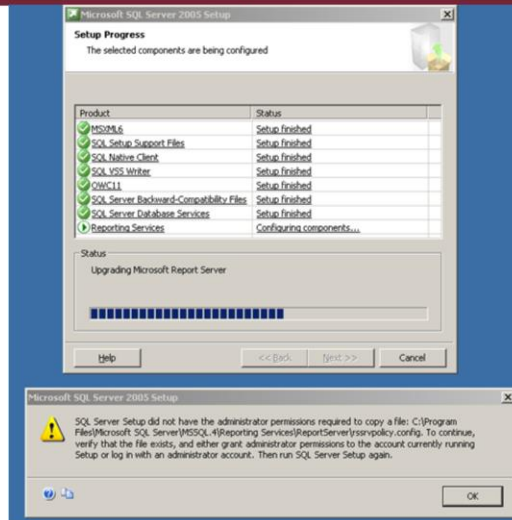
Leírás: **SKUUPGRADE of Reporting Services fails with could not write rssrvpolicy.config,**

<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/>

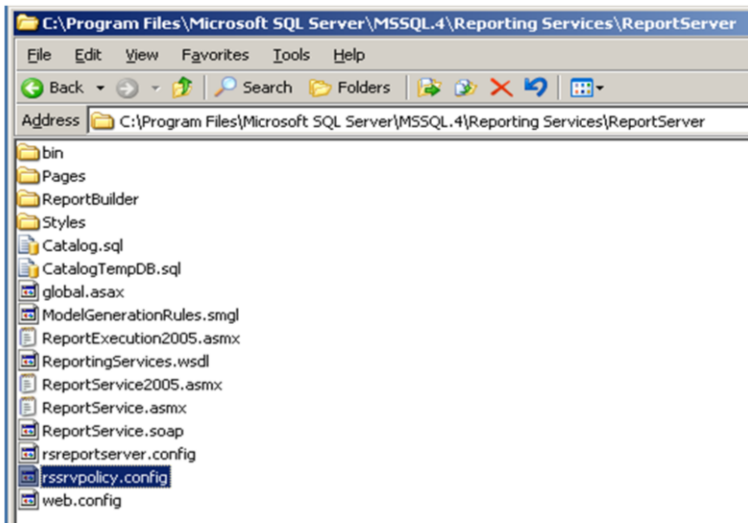
Hiba a telepítés során



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

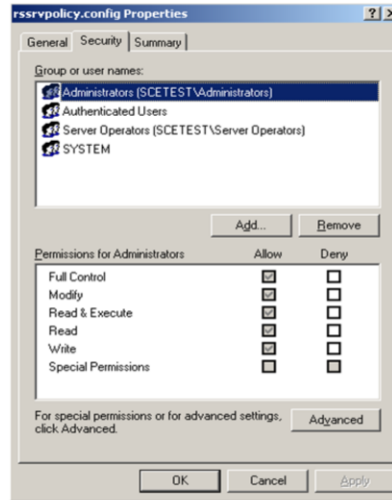


A fájl pedig létezik...



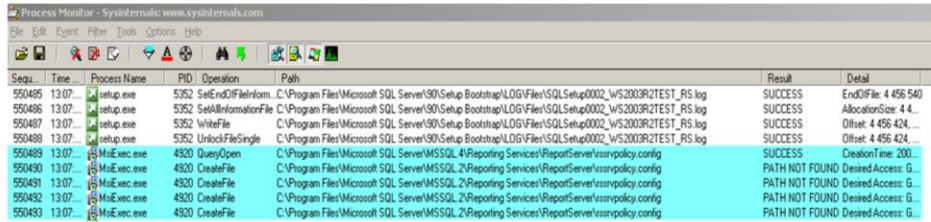
És van hozzá jogosultságunk is... ??

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



Process Monitor

- Pár százezer esemény közül kikeressük a relevánsakat:



Sequ...	Time	Process Name	PID	Operation	Path	Result	Detail
550495	13.07...	setup.exe	5352	SetEndOfFileInform...	C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0002_WS2003R2TEST_RS_log	SUCCESS	EndOfFile: 4 456 540
550496	13.07...	setup.exe	5352	SetInformationFile	C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0002_WS2003R2TEST_RS_log	SUCCESS	AllocationSize: 4 4...
550487	13.07...	setup.exe	5352	WriteFile	C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0002_WS2003R2TEST_RS_log	SUCCESS	Offset: 4 456 424, ...
550489	13.07...	setup.exe	5352	UnlockFileSingle	C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG\Files\SQLSetup0002_WS2003R2TEST_RS_log	SUCCESS	Offset: 4 456 424, ...
550489	13.07...	MsiExec.exe	4920	QueryOpen	C:\Program Files\Microsoft SQL Server\MSSQL.4\Reporting Services\ReportServer\ssrs\policy.config	SUCCESS	CreationTime: 200...
550490	13.07...	MsiExec.exe	4920	CreateFile	C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer\ssrs\policy.config	PATH NOT FOUND	Desired Access: G...
550491	13.07...	MsiExec.exe	4920	CreateFile	C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer\ssrs\policy.config	PATH NOT FOUND	Desired Access: G...
550492	13.07...	MsiExec.exe	4920	CreateFile	C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer\ssrs\policy.config	PATH NOT FOUND	Desired Access: G...
550493	13.07...	MsiExec.exe	4920	CreateFile	C:\Program Files\Microsoft SQL Server\MSSQL.2\Reporting Services\ReportServer\ssrs\policy.config	PATH NOT FOUND	Desired Access: G...

- 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

The screenshot shows the Image Distributor application interface. At the top, a table lists machines (itec1 to itec12) with columns for Machine Name, Turned On, Free Space (GB), and Lftp Service. Machine itec1 is selected. Below the table is an Event log window showing the following entries:

```
[13.26.55] Starting multicast copy: IBMLaborok\teszt-image\Windows XP Professional-000001-s001.vmdk (13 MB)
[13.27.02] UFTP status: Host itec1 finished in 5.046 seconds with 0 NAKs
[13.27.02] Copied: IBMLaborok\teszt-image\Windows XP Professional-000001-s001.vmdk (0.07, 2 MB/s)
[13.27.02] Unicast copied IBMLaborok\teszt-image\vmware-2.log (72 kB) to itec1
[13.27.02] Source file "\\itec1\c$\temp\ufpt\Windows XP Professional-000001-s001.vmdk" not found, multicast copy was unsuccessful on host itec1.
[13.27.02] Unicast copied IBMLaborok\teszt-image\Windows XP Professional.nvram (8 kB) to itec1
[13.27.02] Unicast copied IBMLaborok\teszt-image\Windows XP Professional.vmdk (905 b) to itec1
[13.27.02] Copy finished. Check target machines.
```

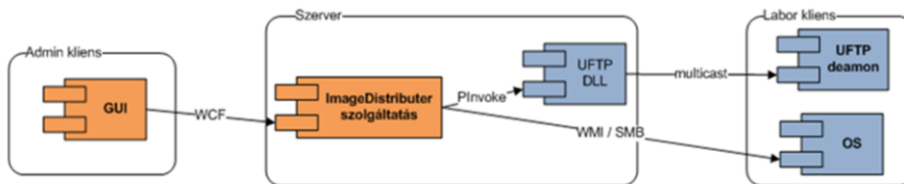
The error message is highlighted in red. The application also shows a tree view of images on the server and a taskbar at the bottom with the number 31.

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

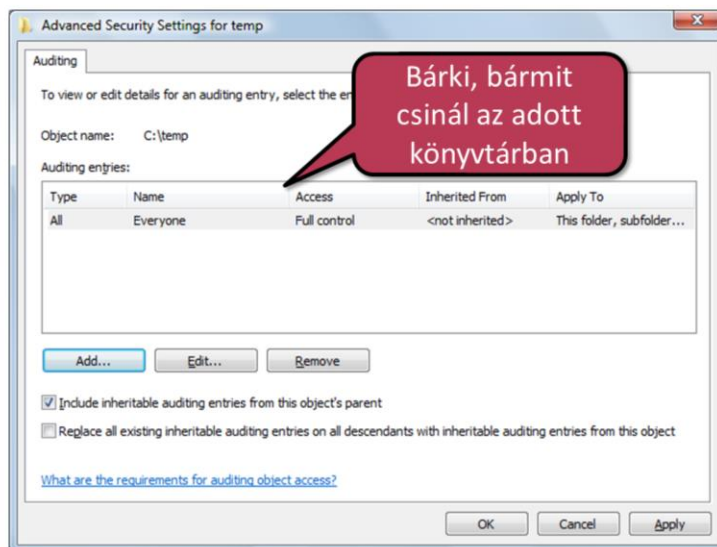
A fájl hozzáférés Process Monitorban

Event	Process	Stack
Date:	2009.09.22. 13:27:02	
Thread:	3852	
Class:	File System	
Operation:	CreateFile	
Result:	NAME NOT FOUND	
Path:	\\itc1\c\$\temp\ufp\Windows XP Professional-000001-s001.vmdk	
Duration:	0.0005817	

Desired Access:	Read Attributes
Disposition:	Open
Options:	Open Reparse Point
Attributes:	n/a
ShareMode:	Read, Write, Delete
AllocationSize:	n/a

A fájlt Explorerben megnézve pedig ott van, akkor miért ez az eredmény?

NTFS szintű naplózás beállítása (SACL)



Bejegyzés a biztonsági naplóban

A handle to an object was requested.

Subject:
Security ID:
Account Name: ImageDistributer
Account Domain: FTSLAB
Logon ID: 0x3d0227

Object:
Object Server: Security
Object Type: File
Object Name: C:\temp\ufstp*.vmdk
Handle ID: 0x1220

Process Information:
Process ID: 0x4
Process Name:

Access Request Information:
Transaction ID: {00000000-0000-0000-0000-0000-0000-0000-0000-0000}
Accesses: DELETE
ReadAttributes

Melyik folyamat

Milyen típusú hozzáférés

Fájl hozzáférések sorrendje

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

Megoldás:

- Az uftp.exe még írni akarta és fogta a fájlt az ImageDistributor hozzáférése előtt

Tanulság

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

Ha nagy baj van



A problem has been detected and windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

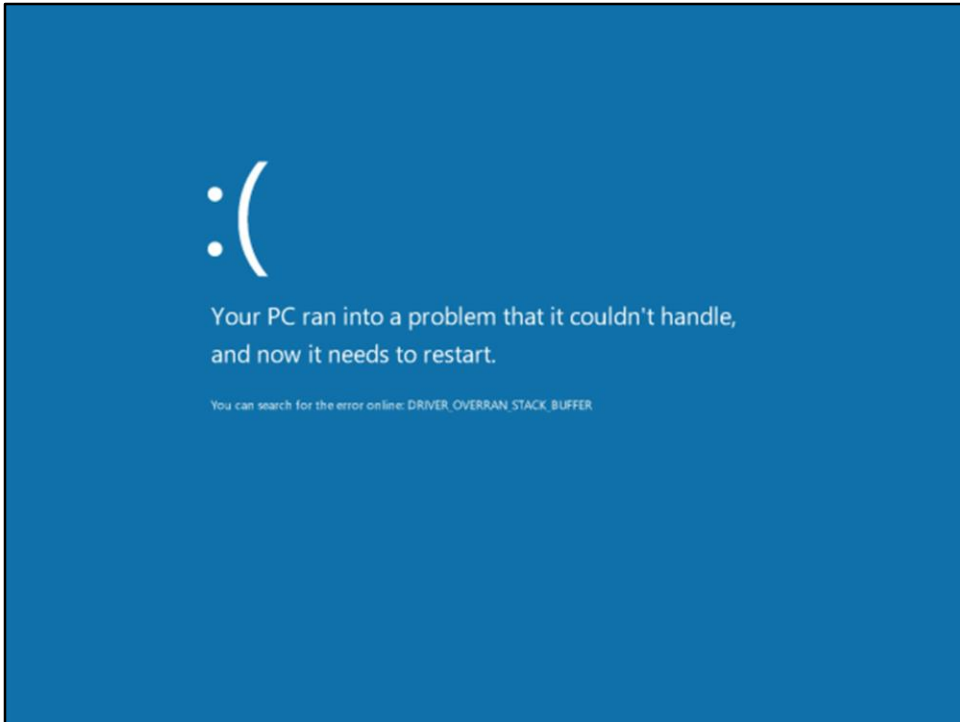
Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c

41

Ez a klasszikus BSOD képernyő



Ez a Windows 8-ban bevezetett új BSOD képernyő

Blue Screen of Death (BSOD)

- Becsületes neve: **STOP error**, bug check
 - Azonosítás: STOP error code
- Ha nem lát már más kiutat a rendszer
 - Nagyobb baj elkerülése
- Nem rossz dolog, ne a hírnököt gyűlöljük 😊
- KeBugCheckEx függvény (Bugcheck.h)



43



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

Példa bug check (MSDN)

Bug Check 0xA: IRQL_NOT_LESS_OR_EQUAL



The IRQL is a value of DISPATCH_LEVEL or above. Windows or a kernel-mode driver accessed paged memory at DISPATCH_LEVEL or above.

Importance This bug check is a STOP error. If you have experienced a STOP error, you should contact your computer manufacturer for assistance. If you have a copy of Windows, you can attempt to recover from this error. A hardware device, its driver, or related software might have caused this error. If your copy of Windows came with a recovery partition, you can use it to restore your computer. If you have a backup of your computer, you can restore it. Microsoft provides support. To find contact information for Microsoft or your computer manufacturer, contact support.

Kód

Név

If you have experience with computers and want to try to recover from this error, follow the steps provided in the Microsoft article [How to Fix BlueScreen \(STOP\) Errors that Cause Windows to Shut Down or Restart Unexpectedly](#).

The following actions might prevent an error like this from happening again:

1. Download and install updates and device drivers for your computer from Windows Update.
2. Scan your computer for computer viruses.
3. Check your hard disk for errors.

IRQL_NOT_LESS_OR_EQUAL Parameters

The following parameters are displayed on the blue screen.

Parameter	Description
1	Memory referenced
2	IRQL at time of reference
3	0: Read 1: Write
4	Address which referenced memory

Paraméterek listája (segít a hibát értelmezni)

Javasolt megoldások

Cause
This bug check is issued if paged memory (or invalid memory) is accessed when the IRQL is too high. The error that generates this bug check usually occurs after the installation of a faulty device driver, system service, or BIOS.



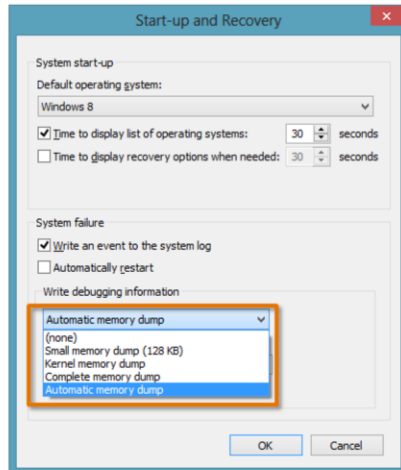
Forrás: [http://msdn.microsoft.com/en-us/library/ff560129\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ff560129(v=VS.85).aspx)

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

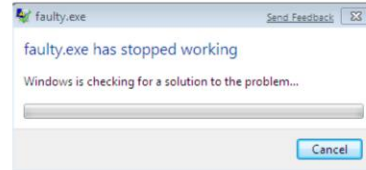


MSDN. **Crash Dump Files**, <http://msdn.microsoft.com/en-us/library/ff539316.aspx>

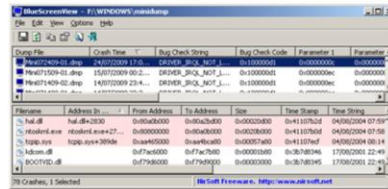
Ask the Core Team. „**Windows 8 and Windows Server 2012: Automatic Memory Dump**”,
<http://blogs.technet.com/b/askcore/archive/2012/09/12/windows-8-and-windows-server-2012-automatic-memory-dump.aspx>

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

```
Command
-----
C:\>!analyze -v
*****
*                                     *
*                               Bugcheck Analysis                               *
*                                     *
*****

KMODE_EXCEPTION_FATAL [0x000021a]
The Windows process terminated unexpectedly.
!analyze -v
Arg1: e2b5c1b8 String that identifies the problem.
Arg2: c0000005 Error Code.
Arg3: 7c9104c3
Arg4: 010ca214

Debugging Details:
-----
Unable to get nt!KiCurrentExeBufferOffset
Unable to get nt!KiCurrentExeBufferBase
EXCEPTION_CODE: (NTSTATUS) 0xc0000021a - (Fatal System Error) The \hs system process
EXCEPTION_PARAMETER1: e2b5c1b8
EXCEPTION_PARAMETER2: c0000005
EXCEPTION_PARAMETER3: 7c9104c3
EXCEPTION_PARAMETER4: 010ca214
ADDITIONAL_DEBUG_TEXT: Windows Subsystem
BUGCHECK_STR: 0xc0000021a_corrupt_exe_c0000005
CUSTOMER_CRASH_COUNT: 3
DEFAULT_BUCKET_ID: DRIVER_FAULT
PROCESS_NAME: csrss.exe
LAST_CONTROL_TRANSFER: from 805c5ee6 to 804f9104
```



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

```
Windows Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable UGA Mode
Last Known Good Configuration (your most recent settings that worked)
Directory Services Restore Mode (Windows domain controllers only)
Debugging Mode
Disable automatic restart on system failure

Start Windows Normally
Reboot
Return to OS Choices Menu

Use the up and down arrow keys to move the highlight to your choice.
```



A description of the Safe Mode Boot options in Windows XP

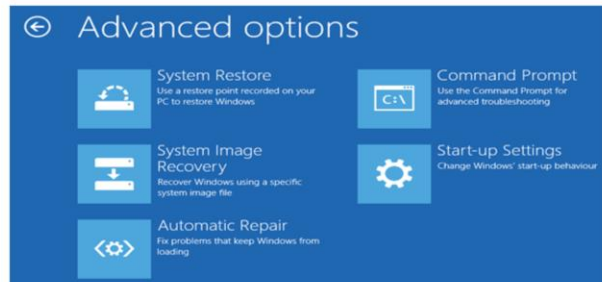
<http://support.microsoft.com/default.aspx?scid=kb;en-us;315222>

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:)



51



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>

Boot Configuration Database

```
Administrator: Command Prompt
C:\Windows\system32>bcdedit

Windows Boot Manager
-----
identifier          (bootmgr)
device              partition=C:
description         Windows Boot Manager
locale              en-US
inherit             (globalsettings)
default             (current)
resumeobject        {4eeb6a3e-7e74-11db-a8d2-ea49727b933a}
displayorder        (current)
toolsdisplayorder   (memdiag)
timeout             30

Windows Boot Loader
-----
identifier          (current)
device              partition=C:
path                \Windows\system32\winload.exe
description         Microsoft Windows Uista
locale              en-US
inherit             (bootloadersettings)
osdevice            partition=C:
systemroot           \Windows
resumeobject        {4eeb6a3e-7e74-11db-a8d2-ea49727b933a}
nx                  OptIn
```

■ GUI eszköz: *msconfig.exe*

DEMO



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

Esettanulmány: csrss BSOD

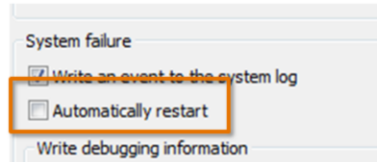
- Megtörtént eseményeken alapul
- Hibajelenség:
 - Laborgép folyamatosan újraindul
 - Néha a bejelentkezésig még eljut



Részletes leírás: [0xc000021A: csrss kék halál a laborban](http://micskeiz.wordpress.com/2009/05/21/0xc000021a-csrss-kek-halal-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

Crash dump megnézése

- Minidump készült automatikusan

- C:\Windows\Minidump

```
ERROR_CODE: (NTSTATUS) 0xc000021a - (Fatal System Error) The %hs system proces
EXCEPTION_CODE: (NTSTATUS) 0xc000021a - (Fatal System Error) The %hs system pr
EXCEPTION_PARAMETER1: e2b5cfb8
EXCEPTION_PARAMETER2: c0000005
EXCEPTION_PARAMETER3: 7c9106c3
EXCEPTION_PARAMETER4: c8ec24
ADDITIONAL_DEBUG_TEXT: Windows SubSystem
BUGCHECK_STR: 0xc000021a_csrss.exe_c0000005
CUSTOMER_CRASH_COUNT: 3
DEFAULT_BUCKET_ID: DRIVER_FAULT
PROCESS_NAME: csrss.exe
LAST_CONTROL_TRANSFER: from 805c5eee to 804f9f0d

STACK_TEXT:
ba217934 805c5eee 0000004c c000021a ba2179b0 nt!KeBugCheckEx+0x1b
ba217970 80555401 00000001 0000004c c000021a nt!PcShutdownBugCheck+0x5c
ba217b28 80612d8a c000021a 00000004 00000001 nt!ExpSystemErrorHandler+0x511
ba217cd4 8061330b c000021a 00000004 00000001 nt!ExpRaiseHardError+0x9a
ba217d44 805413fc c000021a 00000004 00000001 nt!NtRaiseHardError+0x16b
ba217d44 7c90eb94 c000021a 00000004 00000001 nt!KiFastCallEntry+0x1c
WARNING: Frame IP not in any known module. Following frames may be wrong.
00c8ea94 7c90e273 75b432b7 c000021a 00000004 0x7c90eb94
00c8e9ec 75b44aea 00c8eb14 75b468b1 00c8eb1c 0x7c90e273
00c8eaf0 00c8eb14 75b468b1 00c8eb1c 00000001 0x75b44aea
00c8eaf4 75b468b1 00c8eb1c 00000001 00c8eb1c 0xc8eb14
00c8eb14 00c8ec24 00c8eb40 7c9037bf 00c8ec08 0x75b468b1
00c8ec08 00000000 00000000 7c9106c3 00000002 0xc8ec24
```

csrss.exe
halt meg

Nem látjuk, hogy
mi vezetett a
hibához. Miért?



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.

```
STACK_TEXT:
b202f934 805f5e00 00000000 00000031 1202f000 ntUserCheck+50x1b
b202f934 805f5e00 00000000 00000031 1202f000 ntUserCheck+0x5c
b202f934 805f5e00 00000000 00000031 1202f000 ntUserHandler+0x511
b202f934 805f5e00 00000000 00000031 1202f000 ntUserHandler+0x9a
b202f934 805f5e00 00000000 00000031 1202f000 ntUserHandler+0x16b
b202f934 805f5e00 00000000 00000031 1202f000 ntUserHandler+0xfc
0069eb40 0069f3d2 00000000 00000000 00000000 CallRet
0069eb40 0069f3d2 00000000 00000000 00000000 Error+0xc
0069eb40 0069f3d2 00000000 00000000 00000000 AddExceptionHandler+0xb3
0069eb40 0069f3d2 00000000 00000000 00000000 TestThread+0x4d4
0069eb40 0069f3d2 00000000 00000000 00000000 CSXSP!ExceptionHandler3+0x61
0069eb40 7c900000 0069ffe4 0069ec24 ntdll!ExecuteHandler2+0x26
0069ebf0 7c900000 0069ec24 0069ec08 ntdll!ExecuteHandler+0x24
0069ebf0 7c900000 0069ec24 0069ec08 ntdll!KiUserExceptionDispatcher+0xe
0069f110 7c900000 00160000 00000000 0000009c ntdll!RtlAllocateHeap+0x1da
0069f110 75e92f21 75e92f38 0000005b 75e9c578
sxs!CSxsPointerBase<CXMLNamespaceManager::CNamespacePrefix,CSxsPointer<CXMLNamespaceManager::CNamespacePrefix
,CXMLNamespaceManager::CNamespacePrefix> >::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
0069fdb0 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
-.-:@
```

Ez akar hibás memóriát foglalni
Ki az az sxs modul?



SxS – Side by Side assemblies

- Rendszer DLL-ekből különböző verziók tárolása
 - [About Isolated Applications and Side-by-side Assemblies](#)

- [Activation Context Creation flow](#)
 - CreateProcess/CreateActCtx is called.
 - CreateProcess/CreateActCtx sends the message to CSRSS
 - CSRSS receives the message, creates the activation context
 - Once the activation context is created, CSRSS returns
 - CreateProcess/CreateActCtx proceeds.
 - The getaway from the flow above is: **most work is done in CSRSS.exe.**



60



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☺

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>