

# Desktop systémy Microsoft Windows

IW1/XMW1 2012/2013

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

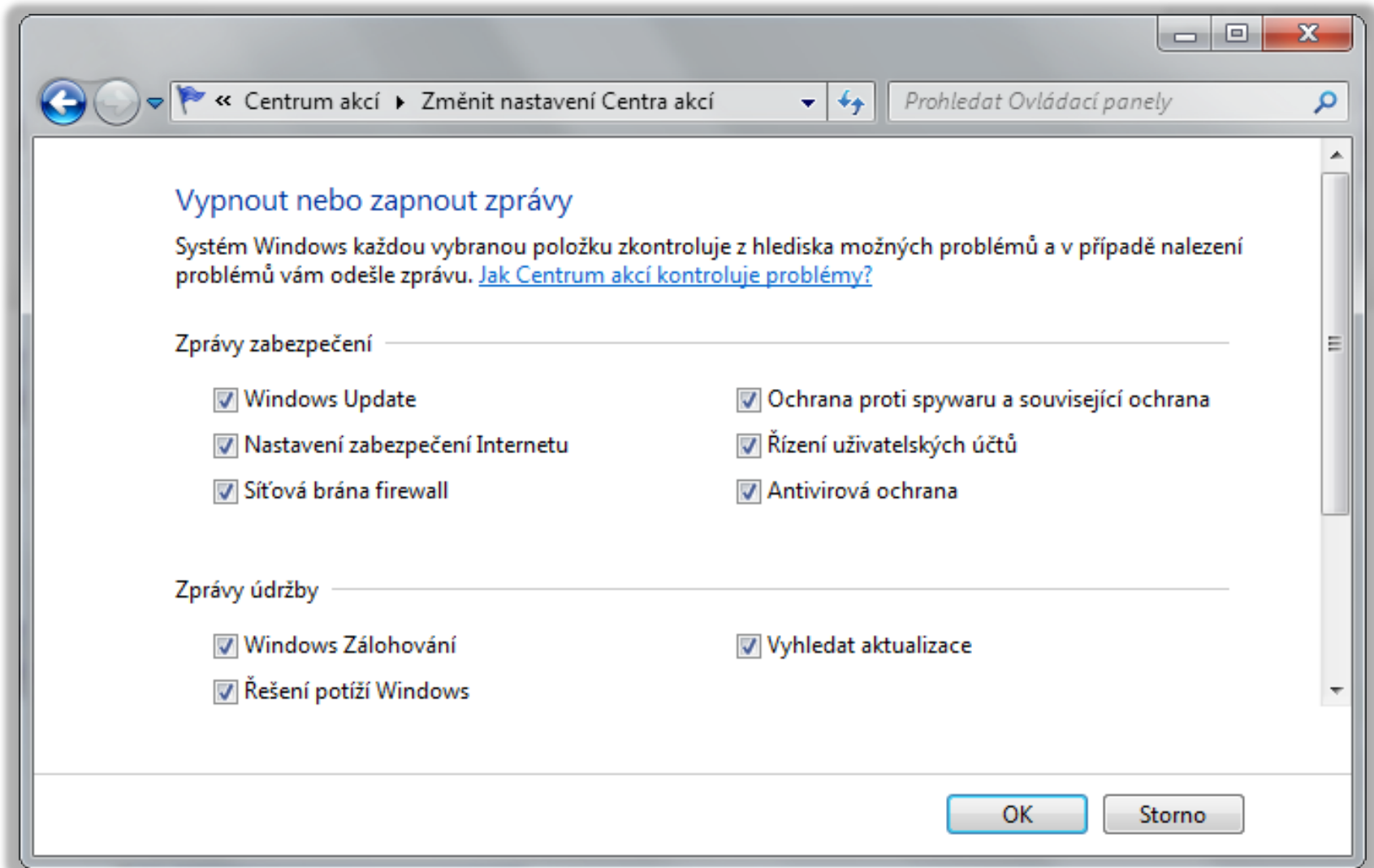
Revize 26.11.2012

# Monitorování a výkon

# Centrum akcí (Action Center)

- Monitoruje počítač a oznamuje problémy s
  - Bezpečností (bránou firewall, antivirem, ...)
  - Údržbou (zálohováním, aktualizacemi, ...)
- Spuštění přes Ovládací panely

# Nastavení oznamování problémů



# Správce úloh (Task Manager)

- Poskytuje základní informace o výkonu počítače
- Umožňuje správu procesů, služeb a sezení
  - Informace o procesech (využití CPU, paměti, ...)
  - Ukončování běhu procesů
  - Nastavení spřažení (*affinity*) a priority procesů
  - Povolení / zakázání virtualizace procesů
- Spuštění příkazem **taskmgr**, klávesovou zkratkou **CTRL+SHIFT+ESC** nebo přes **CTRL+ALT+DEL**

# Správa procesů pomocí Správce úloh

Správce úloh systému Windows

Soubor Možnosti Zobrazit Nápověda

Aplikace **Procesy** Služby Výkon Síť Uživatelé

Název procesu	PID	Uživatelské ...	Procesor	Paměť ...	Zákl. prioritá	Virtualizace UAC	Popis
Atouch64.exe	2796		00	1 740 kB	Normální		
cfp.exe	2856	John	00	4 164 kB	Normální	Zakázáno	COMODO Internet ...
cmd.exe *32	3924	John	00	2 148 kB	Normální	Zakázáno	Příkazový řádek sys...
cmd.exe *32	4036	John	00	2 156 kB	Normální	Zakázáno	Příkazový řádek sys...
conhost.exe	3940	John	00	2 352 kB	Normální	Zakázáno	Console Window Host
conhost.exe	4192	John	00	2 356 kB	Normální	Zakázáno	Console Window Host
csrss.exe	528		01	1 924 kB	Vysoká		
Dexcube.exe *32	3768	John	00	2 804 kB	Normální	Povoleno	3D desktop switchin...
dexpot.exe *32	2988	John	00	4 760 kB	Normální	Povoleno	The utility for virtua...
Dexpot64.exe	3732	John	00	2 324 kB	Normální	Zakázáno	Dexpot64 Message ...
DTLite.exe *32	2960	John	00	3 020 kB	Normální	Povoleno	DAEMON Tools Lite
dwm.exe	3060	John	00	27 140 kB	Vysoká	Zakázáno	Správce oken plochy
egui.exe	2772	John	00	5 116 kB	Normální	Zakázáno	ESET GUI
explorer.exe	2276	John	00	80 380 kB	Normální	Zakázáno	Průzkumník Windows
explorer.exe	4492	John	00	14 604 kB	Normální	Zakázáno	Průzkumník Windows

Zobrazit procesy všech uživatelů Ukončit proces

Procesy: 91 Využití procesoru: 18 % Fyzická paměť: 86 %

# Sledování prostředků

- Monitorování využití prostředků v reálném čase
  - Filtrování na základě procesů nebo služeb
  - Zjišťování závislostí mezi procesy (zda proces nečeká na prostředky aktuálně používané jinými procesy)
  - Informace o používaných souborech, klíčích registru, synchronizačních objektech, událostech, ...
  - Zavedené moduly (DLL knihovny, ovladače, ...)
  - Ustanovená TCP spojení a otevřené porty
- Spuštění příkazem **perfmon /res** či **resmon** nebo přes Správce úloh

# Nástroj Sledování prostředků

Sledování prostředků

Soubor Sledování nápověda

Přehled Procesor Paměť Disk Síť

Procesor ■ Využití procesoru: 21 % ■ Nejvyšší frekvence: 83 %

<input type="checkbox"/> Proces	PID	Stav	Procesor	Platforma	Popis
<input type="checkbox"/> dexpot.exe	2988	Spuštěno	0	32 bitů	The utility for virtual ...
<input type="checkbox"/> Dexpot64.exe	3732	Spuštěno	0	64 bitů	Dexpot64 Message ...
<input type="checkbox"/> DTLite.exe	2960	Spuštěno	0	32 bitů	DAEMON Tools Lite
<input type="checkbox"/> dwm.exe	3060	Spuštěno	2	64 bitů	Správce oken plochy
<input type="checkbox"/> egui.exe	2772	Spuštěno	0	64 bitů	ESET GUI
<input type="checkbox"/> ekrn.exe	1944	Spuštěno	0	32 bitů	ESET Service
<input type="checkbox"/> explorer.exe	2276	Spuštěno	0	64 bitů	Průzkumník Windows
<input type="checkbox"/> explorer.exe	4492	Spuštěno	0	64 bitů	Průzkumník Windows

Disk ■ V/V disku 20 kB/s ■ Nejvyšší aktivní čas: 0 %

Síť ■ V/V sítě 1 kb/s ■ Využití sítě: 0 %

Paměť ■ Chyby stránkování na ... ■ Využitá fyzická paměť: ...

Zobrazení

Procesor 100 %

60 sekund 0 %

Disk 100 kB/s

0



# Process Explorer

- Rozšíření Správce úloh (a Sledování prostředků)
  - Poskytuje detailní informace o běžících procesech
- Umožňuje (kromě řady dalších věcí)
  - Zobrazovat procesy ve stromové hierarchii na základě toho, jak byly vytvářeny (hierarchie otec/syn)
  - Vyhledávat procesy využívající zadané DLL knihovny nebo popisovače (soubory, klíče registru, ...)
  - Získávat podrobné informace o všech popisovačích, DLL knihovnách, vláknech, proměnných prostředí, ...
- Zdarma ke stažení na stránkách Microsoftu

# Nástroj Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [a02-0617a\John]

File Options View Process Find Handle Users Help

Process	PID	Priority	CPU	Description	Virtual Size	Working Set	Image Type	Virtualized
lsass.exe	640	9		Local Security Authority Process	47 484 K	13 012 K		
lsm.exe	648	8			32 356 K	7 108 K		
winlogon.exe	612	13			58 024 K	7 304 K		
procexp.exe	5480	8		Sysinternals Process Explorer	74 732 K	9 516 K	32-bit	
PROCEXP64.exe	7016	13	7.16	Sysinternals Process Explorer	137 276 K	33 820 K	64-bit	
rundll32.exe	2132	8			2 556 K	124 K		
explorer.exe	2276	8	0.65	Průzkumník Windows	364 712 K	125 796 K	64-bit	
sm56hlp.exe	2752	8		SM56 Modem Helper	87 980 K	7 812 K	64-bit	
IAAnotif.exe	2760	8		Event Monitor User Notification Tool	88 556 K	8 616 K	32-bit	

Type	Name
File	\Device\Null
File	\Device\WMIDataDevice
File	\FileSystem\Filters\FltMgrMsg
Event	\KernelObjects\MaximumCommitCondition
Directory	\KnownDlls
ALPC Port	\RPC Control\OLE2EBE7AD2F87C4AF08133DE733A4E
Directory	\Sessions\1\BaseNamedObjects
Directory	\Sessions\1\BaseNamedObjects
Mutant	\Sessions\1\BaseNamedObjects\!IETId!Mutex
Mutant	\Sessions\1\BaseNamedObjects\!MSFTHISTORY!_
Mutant	\Sessions\1\BaseNamedObjects\!SHMSFTHISTORY!_

CPU Usage: 29.27% Commit Charge: 48.09% Processes: 89 Physical Usage: 86.81%

# Sledování spolehlivosti

- Monitoruje stabilitu systému
  - Chyby aplikací a systému Windows
  - Úspěšné a neúspěšné instalace ovladačů, aktualizací, aplikací apod.
- Spuštění příkazem **perfmon /rel**
- Stabilita vyjádřena tzv. indexem stability
  - Vypočítán na základě počtu chyb za posledních 28 dní (starší chyby mají nižší váhu)
- Data jsou uchovávána po dobu 1 roku

# Nástroj Sledování spolehlivosti

Prohlédněte si historii spolehlivosti a problémů svého počítače.

Index stability hodnotí celkovou stabilitu systému na stupnici od 1 do 10. Vyberete-li určité časové období, zobrazí se konkrétní problémy hardwaru a softwaru, které měly vliv na systém. [Použití nástroje Sledování spolehlivosti.](#)

Zobrazit podle: **Dny** | Týdny Naposledy aktualizováno: 27.11.2010 21:00

Podrobnosti o spolehlivosti pro: 19.11.2010

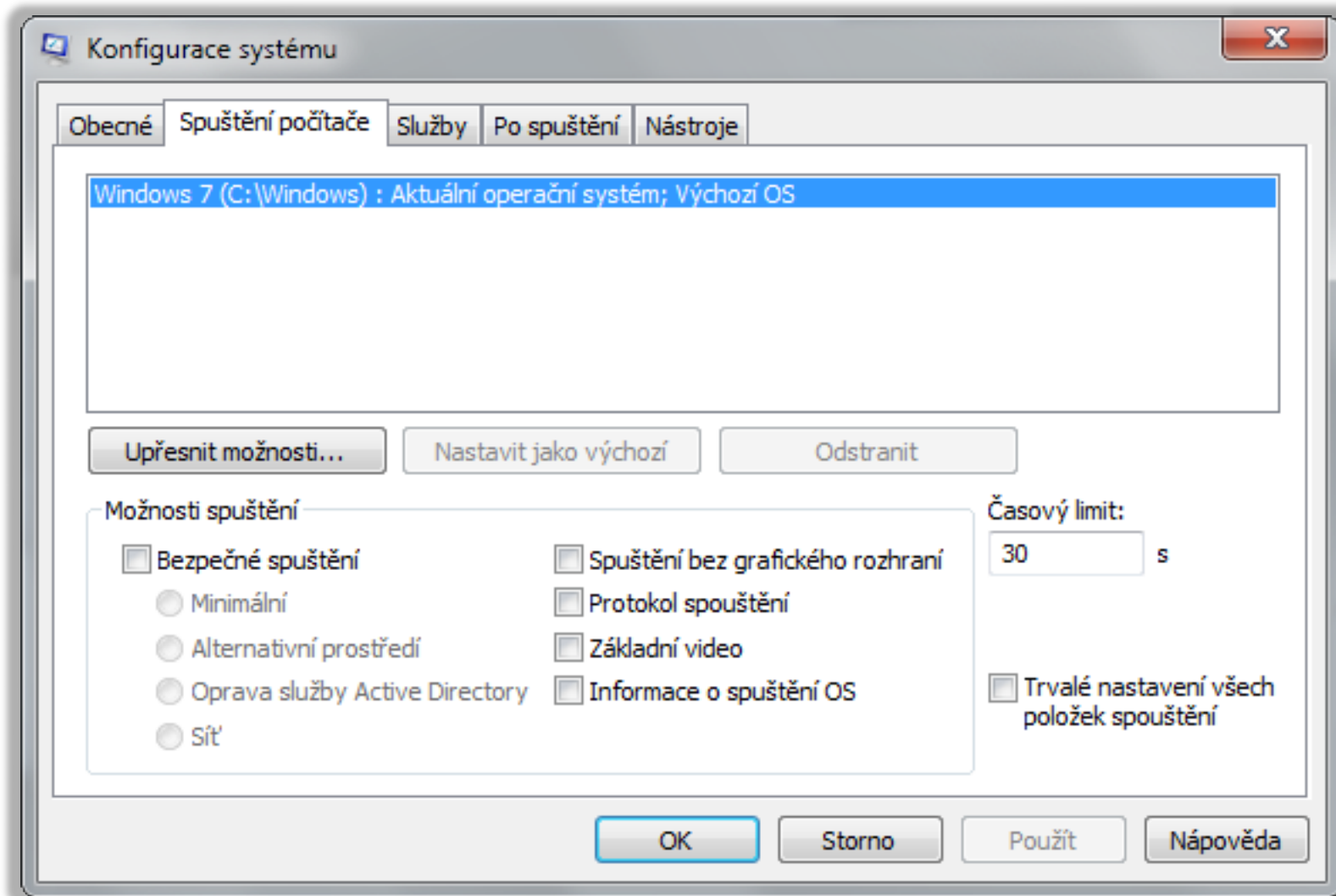
Zdroj	Souhrn	Datum	Akce
<b>⊗ Kritické události</b>			
Print driver host for 32bit applications	Práce zastavena	19.11.2010 2:03	<a href="#">Zobrazit řešení</a>
<b>⚠ Upozornění (2)</b>			
Windows	Neúspěšná instalace ovladače	19.11.2010 19:40	<a href="#">Zobrazit technické podrobnosti</a>
Windows	Neúspěšná instalace ovladače	19.11.2010 19:40	<a href="#">Zobrazit technické podrobnosti</a>
<b>i Informativní události</b>			
Definition Update for Windows Defender ...	Úspěšná aktualizace pomocí služby Windows Update	19.11.2010 19:34	<a href="#">Zobrazit technické podrobnosti</a>

Uložit historii spolehlivosti... [Zobrazit všechna hlášení problémů](#) [Vyhledat řešení všech problémů...](#) OK

# Konfigurace systému

- Řešení problémů se startem systému Windows
  - Určování služeb a aplikací, jenž mají být spuštěny při startu systému Windows
  - Konfigurace bootovací nabídky a možností spuštění systému Windows (protokolování, diagnostika, ...)
  - Povolení externího ladění
- Obsahuje odkazy na různé nástroje vhodné pro řešení problémů (nejen) s výkonem
- Spuštění příkazem **msconfig**

# Nástroj konfigurace systému



# Služby

- Poskytuje detailní informace o službách systému a pokročilé možnosti jejich správy
  - Informace o závislostech mezi službami
  - Specifikace účtu, pod kterým služba běží
  - Definice reakcí při selhání služby (restartovat službu, restartovat počítač nebo spustit program)
- Spuštění příkazem **services.msc**
- Služby se zpožděným spuštěním jsou spuštěny až po nabotování celého systému

# MMC konzole Služby

The screenshot shows the Windows Services console window titled "Služby". The window has a menu bar with "Soubor", "Akce", "Zobrazit", and "Nápověda". Below the menu bar is a toolbar with various icons for navigation and actions. The main area displays a list of services in a table format. The table has four columns: "Název", "Stav", "Typ spouštění", and "Popis". The services listed include VMware DHCP Service, VMware NAT Service, Výstrahy a protokolování výkonu, Vzdálená plocha, Vzdálená správa systému Windows (WS-Management...), Vzdálené volání procedur (RPC), Vzdálený registr, Webový klient, Windows Defender, Windows Presentation Foundation Font Cache 3.0..., Windows Search, Windows Update, Windows Zálohování, Wired AutoConfig Service, and WMI Performance Adapter. The status of each service is indicated in the "Stav" column, and the start type is in the "Typ spouštění" column. The description is in the "Popis" column. At the bottom of the window, there are tabs for "Rozšířené" and "Standardní".

Název	Stav	Typ spouštění	Popis
VMware DHCP Service	Spuštěno	Automaticky	DHCP
VMware NAT Service	Spuštěno	Automaticky	Netwo
Výstrahy a protokolování výkonu		Ručně	Čítač v
Vzdálená plocha	Spuštěno	Ručně	Umožň
Vzdálená správa systému Windows (WS-Management...)		Ručně	Služba
Vzdálené volání procedur (RPC)	Spuštěno	Automaticky	Služba
Vzdálený registr		Ručně	Umožň
Webový klient		Ručně	Umožň
Windows Defender	Spuštěno	Automaticky (Zpožděné spuštění)	Ochra
Windows Presentation Foundation Font Cache 3.0...		Ručně	Optim
Windows Search	Spuštěno	Automaticky (Zpožděné spuštění)	Poskyt
Windows Update	Spuštěno	Automaticky (Zpožděné spuštění)	Umožň
Windows Zálohování		Ručně	Poskyt
Wired AutoConfig Service		Ručně	Služba
WMI Performance Adapter		Ručně	Provid



# Prohlížeč událostí (Event Viewer)

- Umožňuje zobrazit obsah protokolů událostí
- Spuštění příkazem **eventvwr** nebo přes Ovládací panely (sekce Nástroje pro správu)
- Události jsou řazeny do 4 kategorií
  - Kritické (chyby, ze kterých se nebylo možné zotavit)
  - Chyby (chyby, jenž mohou ovlivnit běh systému)
  - Výstrahy (chyby, které mohou ovlivnit běh aplikace)
  - Informace (významnější informace o běhu systému)

# Další možnosti a funkcionality

- Filtrování událostí
  - Dočasně pomocí filtru
  - Trvale pomocí vlastního zobrazení (*custom view*)
    - Možnost importu a exportu (uložení jako XML soubor)
- Vykonávání úloh při výskytu konkrétních událostí
  - Možnost přiřadit úlohu (spuštění programu / skriptu, zaslání e-mailu nebo zobrazení zprávy) dané události
- Zasílání událostí na vzdálené počítače
- Export událostí do XML, CSV nebo TXT souboru

# Protokoly systému Windows

- Aplikace (*Application*)
  - Zahrnuje události nastalé činností běžících aplikací
- Zabezpečení (*Security*)
  - Zahrnuje události spojené s auditováním přístupu
- Systém (*System*)
  - Zahrnuje události systému Windows a jeho služeb
- Předané události (*Forwarded Events*)
  - Zahrnuje události zaslané z jiných počítačů

# Definice vlastního zobrazení (filtru)

Vytvořit vlastní zobrazení

Filtr XML

Protokolováno: Kdykoli

Úroveň události:  Kritická  Upozornění  Podrobnosti  
 Chyba  Informace

Podle protokolu Protokoly událostí: Aplikace,Zabezpečení,System

Podle zdroje Zdroje událostí:

Zahrne nebo vyloučí ID událostí: Zadejte čísla nebo rozsahy ID oddělené čárkou. Chcete-li kritéria vyloučit, zadejte znak minus. Příklad: 1,3,5-99,-76

<Všechny identifikátory událostí>

Kategorie úlohy:

Klíčová slova:

Uživatel: <Všichni uživatelé>

Počítače: <Všechny počítače>

Vymazat

OK Storno

# Předávání událostí (Event Forwarding)

- Zasílání specifických událostí na vzdálený počítač
  - Na cílovém počítači (jenž přijímá události) musí běžet alespoň Windows Vista nebo Server 2003 R2
  - Na zdrojovém počítači (jenž zasílá události) musí být alespoň Windows XP SP2 nebo Server 2003 SP1
  - Musí běžet pod účtem uživatele ze skupiny Event Log Readers (Administrators pro události ze Zabezpečení)
- Na obou počítačích musí běžet služby
  - Vzdálená správa systému Windows (WinRM)
  - Sběr událostí systému Windows

# Režimy odběrů (subscription) událostí

- Iniciované cílovým (*collector*) počítačem
  - Cílový počítač stahuje události ze zdrojových počítačů
  - Manuální konfigurace zdrojových počítačů
  - Vhodný pouze pro malé sítě
- Iniciované zdrojovým (*source*) počítačem
  - Zdrojové počítače zasílají události cílovému počítači
  - Konfigurace zdrojových počítačů přes zásady skupiny
  - Lze přidávat další počítače i po nastavení odběru
  - Vhodný v rozsáhlých sítích

# Vytvoření a nastavení odběru

Vlastnosti odběru

Název odběru:

Popis:

Cílový protokol:

Typ odběru a zdrojové počítače

Spouštěno sběrem

Tento počítač kontaktuje vybrané zdrojové počítače a poskytuje odběr.

Spouštěno zdrojovým počítačem

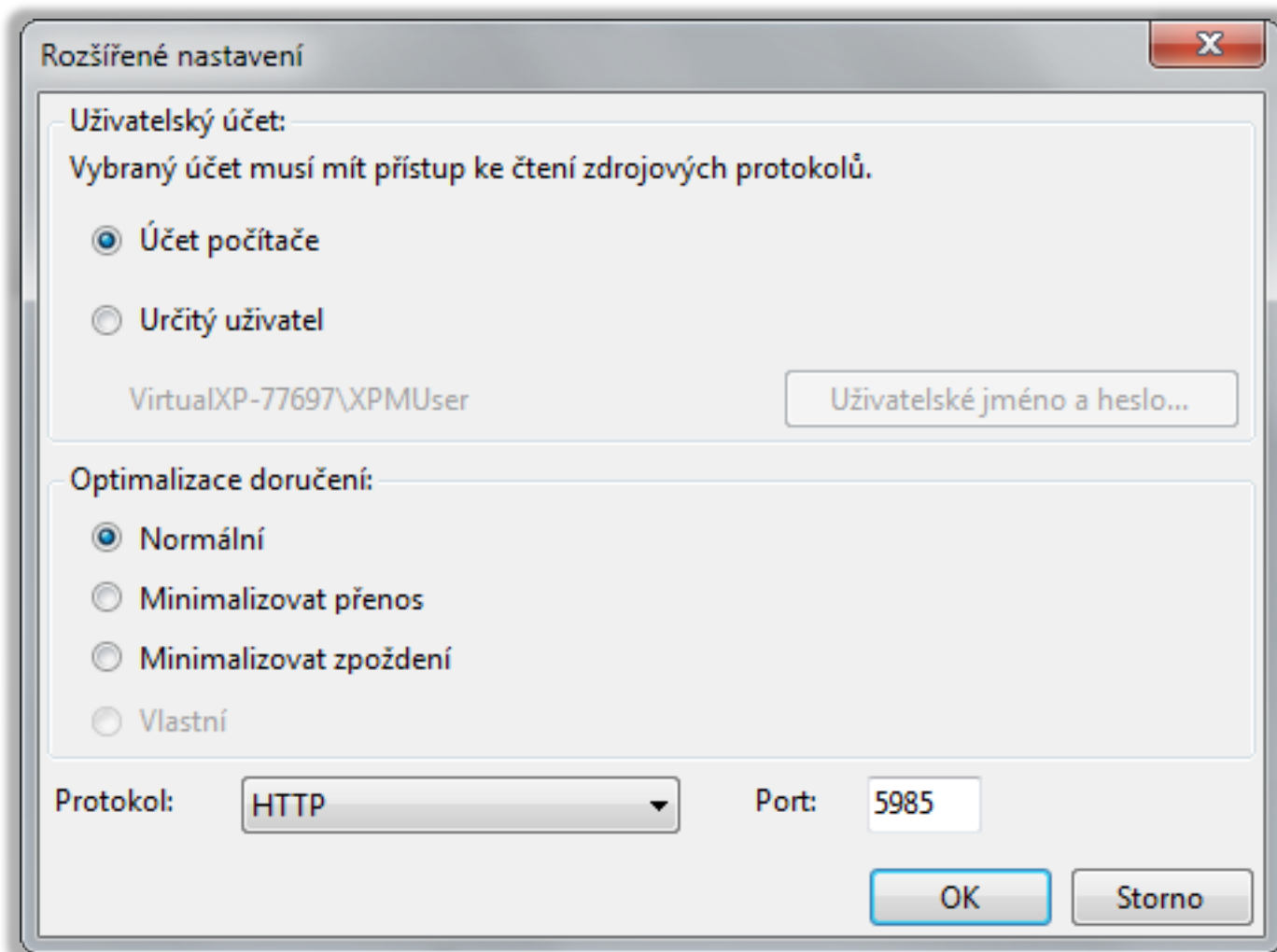
Zdrojové počítače ve vybraných skupinách musejí být pomocí zásad nebo místní konfigurace nakonfigurovány na kontaktování tohoto počítače a přijetí odběru.

Sbírané události:

Uživatelský účet (musí mít přístup ke čtení zdrojových protokolů):  
Účet počítače

Změnit uživatelský účet či nakonfigurovat rozšířené nastavení:

# Pokročilá nastavení odběru





# Monitorování výkonu počítače

- Monitorování hodnot čítačů (*counters*)
  - Každý čítač je vázán ke konkrétní instanci objektu
  - Speciální instance **\_Total** obsahující součet (průměr u procentuálních) hodnot všech instancí daného čítače
- Zatěžuje počítač
  - Vhodné monitorovat jen potřebné informace

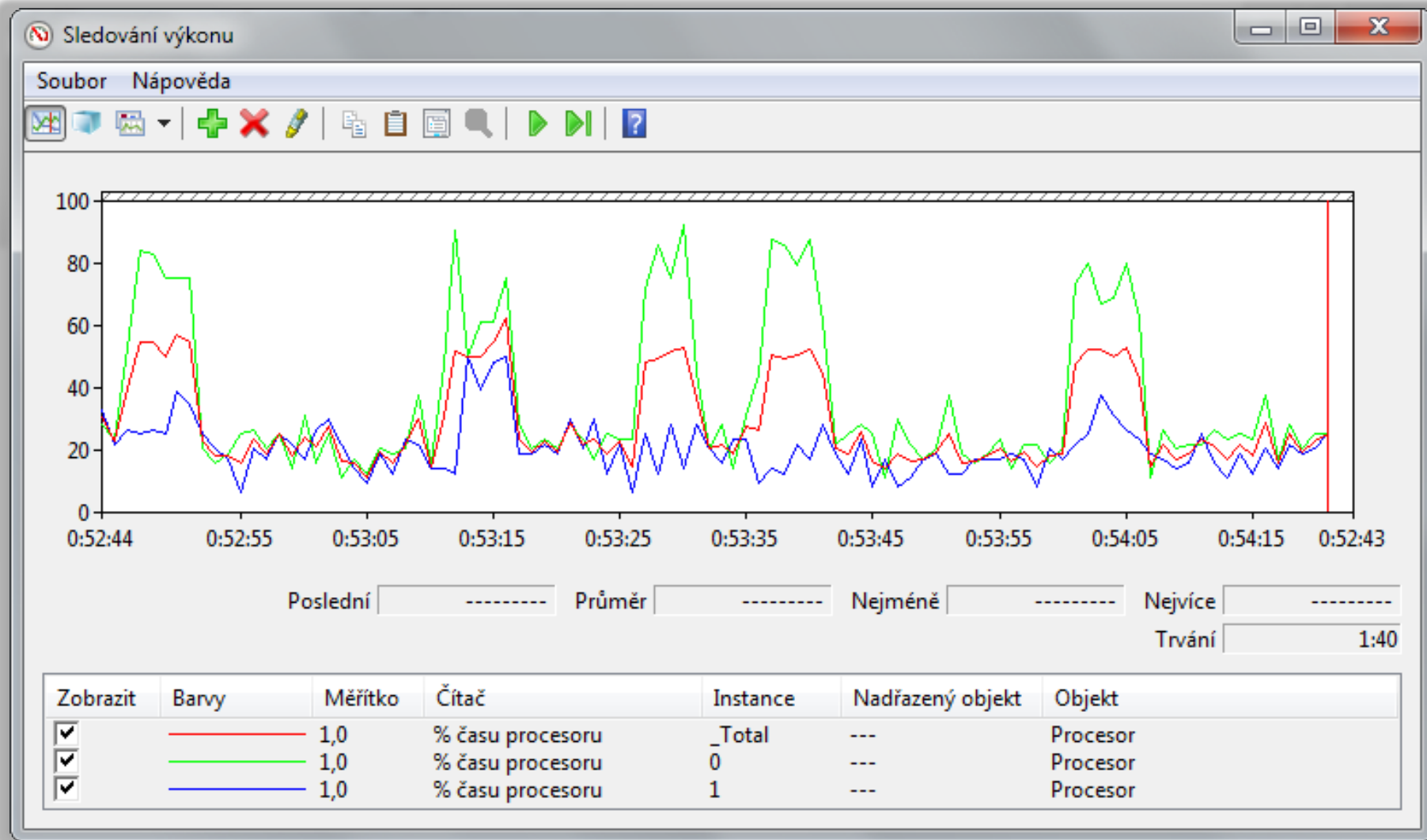
# Typy čítačů

- Čítače hardwaru (zařizení)
  - Procesor (vytížení procesoru, obsluha přerušení, ...)
  - Paměť (volná paměť, stránkování, mezipaměť, ...)
  - Logický disk (vytížení disku a fronty, volné místo, ...)
  - ...
- Čítače softwaru (aplikací)
  - TCP/IP stack (přijaté a odeslané datagramy, chyby, ...)
  - .NET platforma (procesy, třídy, výjimky, kompilátor, ...)
  - ...

# Sledování výkonu

- Sledování hodnot čítačů v reálném čase
  - Vizuální zobrazení ve formě grafu, histogramu nebo sestavy (hodnoty zobrazeny jako prostý text)
- Vizuální zobrazení hodnot čítačů zaznamenaných dříve pomocí sad kolekcí dat
- Lze spustit
  - Jako součást Sledování výkonu (**perfmon**)
  - Jako samostatný nástroj (**perfmon /sys**)
  - V režimu pro porovnávání grafů (**perfmon /comp**)

# Nástroj Sledování výkonu



# Sady kolekcí dat (Data Collector Sets)

- Monitorují činnost celého systému
- Mohou zaznamenávat
  - Hodnoty nebo překročení mezí (výstrahy) čítačů
  - Data trasování událostí (např. událostí jádra, služeb systému, platformy .NET, NTFS či **Active Directory**)
  - Informace o konfiguraci systému (hodnoty registrů nebo informace získané pomocí WMI dotazů)
- Výsledky zobrazeny pod uzlem Sestavy

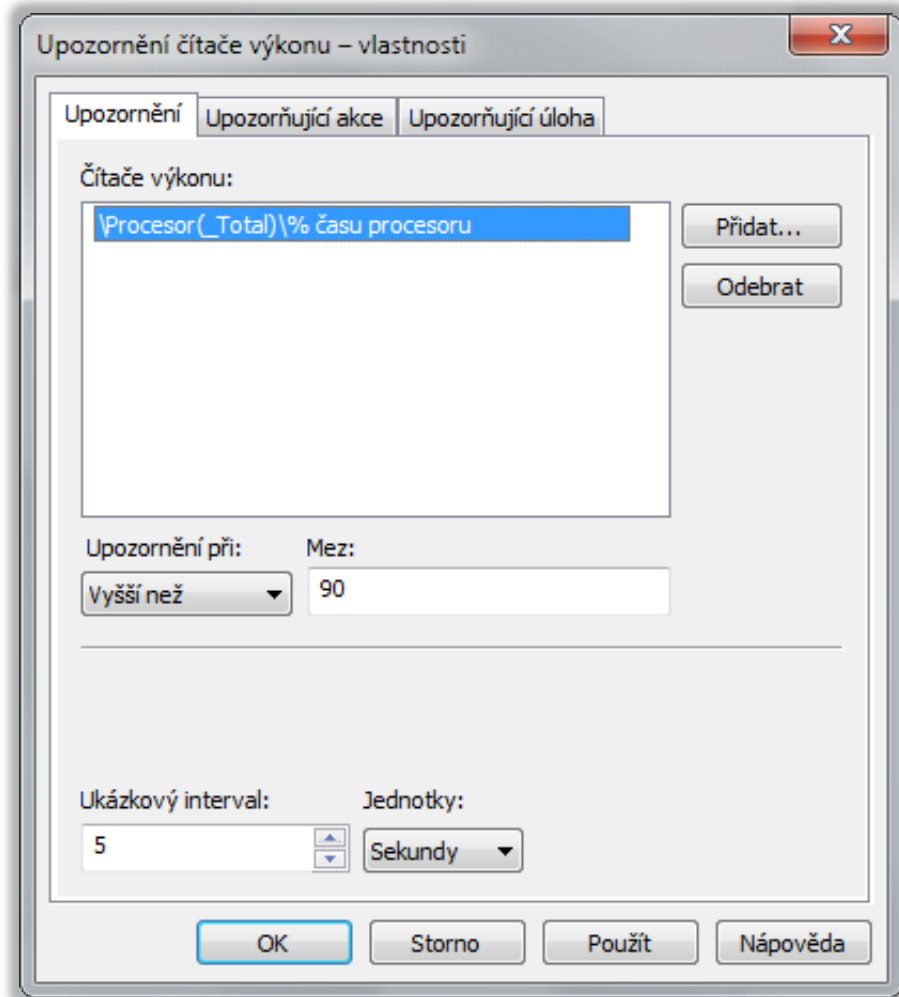
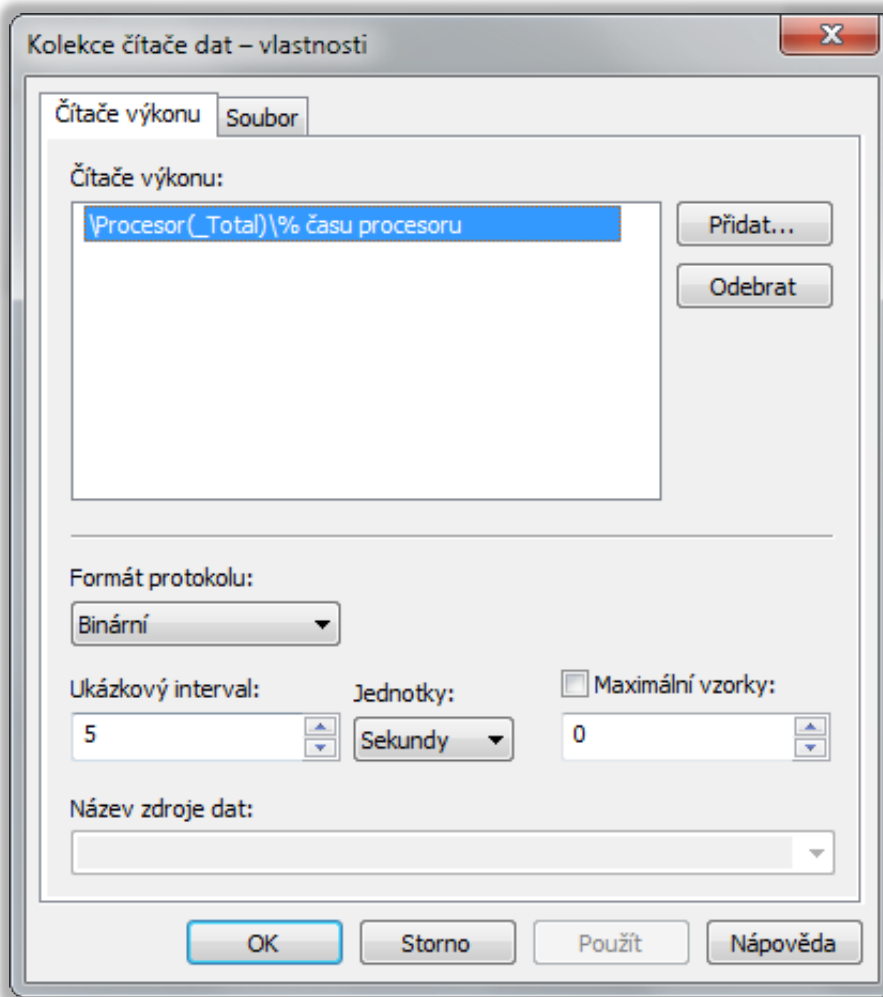
# Systemové sady kolekcí dat

- Výkon systému (*System Performance*)
  - Zaznamenává hodnoty čítačů procesor, fyzický disk, paměť, IPv4, IPv6, ...
  - Zaznamenává data trasování jádra
  - Vhodné při náhlém zpomalení počítače
- Diagnostika systému (*System Diagnostics*)
  - Zaznamenává stejné informace jako Výkon systému
  - Zaznamenává navíc detailní informace o systému (procesech, službách, zařízeních, uživateli, ...)
  - Vhodný při potížích s hardwarem nebo ovladači

# Upozornění čítačů výkonu

- Umožňuje detekovat překročení mezních hodnot vybraných čítačů
- Při detekci lze
  - Zaznamenat tuto událost do protokolu událostí
  - Spustit sadu kolekcí dat
  - Spustit naplánovanou úlohu
    - Spustit program / skript
    - Odeslat e-mail
    - Zobrazit zprávu

# Nastavení čítačů a upozornění čítačů





# Správa pomocí příkazové řádky (1)

- Vyžaduje oprávnění správce
- Vytváření / úprava (sad) kolekcí dat
  - **logman { create | update } { counter | trace | cfg | alert | api } <sada>\<kolekce> ...**
  - Možnost vytváření kolekce dat pro trasování rozhraní API (zaznamenávání volání API funkcí v programu)
- Vytvoření (sady) kolekce dat monitorující čítač(e)
  - **logman create counter <sada>\<kolekce> -c <čítač> [<čítač> ...] -si <interval> -sc <max-počet-vzorků>**

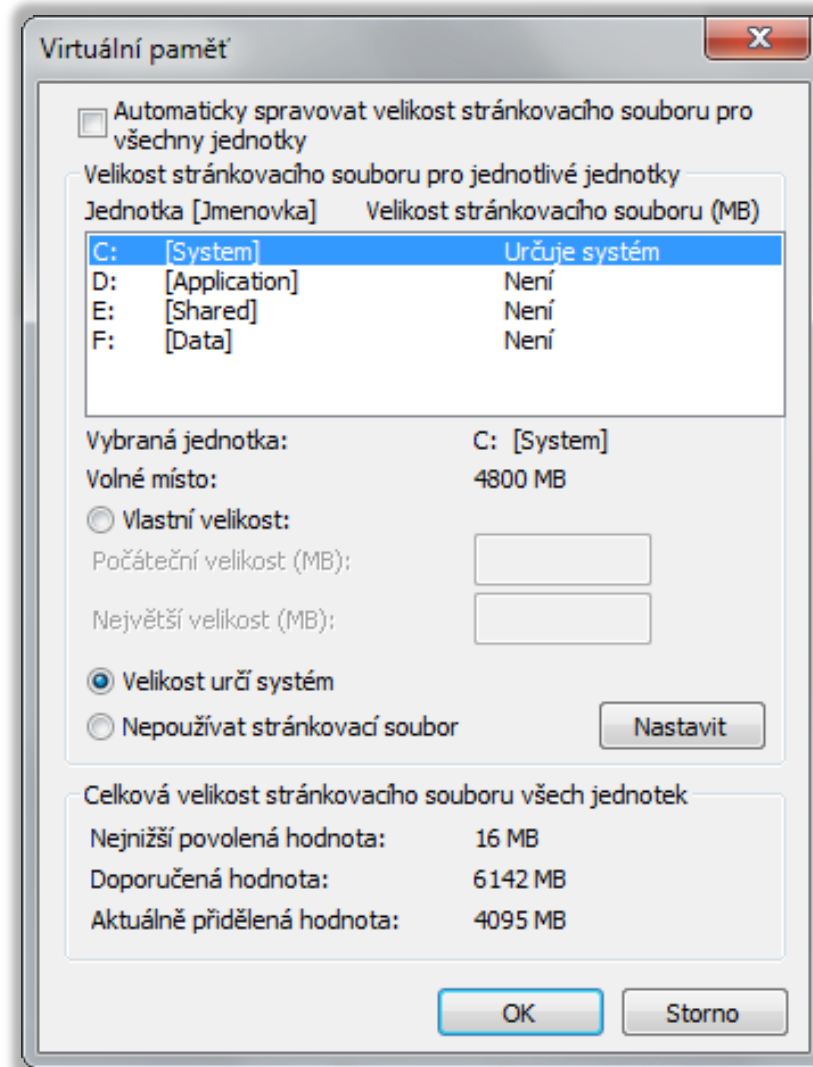
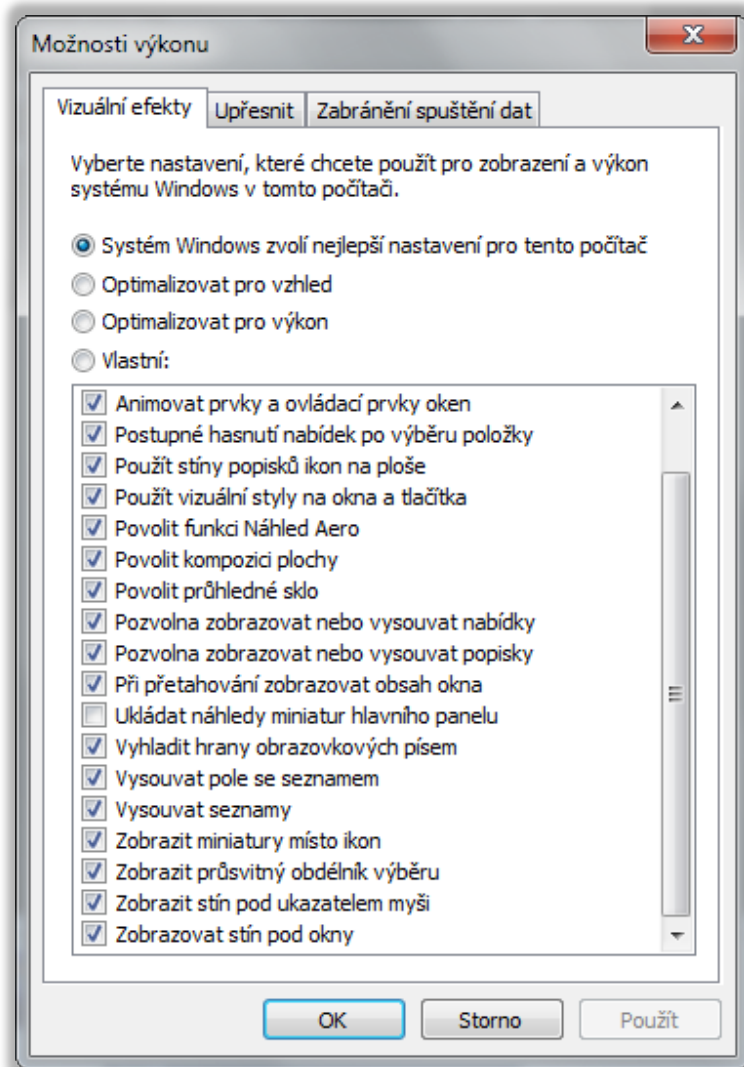
# Správa pomocí příkazové řádky (2)

- Import / export (šablon) sad kolekcí dat
  - **logman { import | export } -xml <*soubor-šablony*>**
- Informace o kolekcích dat v sadě kolekcí dat
  - **logman query <*sada*>**
- Spouštění / zastavování sad kolekcí dat
  - **logman { start | stop } <*sada*>**
- Generování sestavy diagnostiky systému
  - **perfmon /report**
  - Spouští sadu kolekcí dat Diagnostika systému

# Možnosti výkonu

- Umožňuje nastavit různé optimalizace ovlivňující výkon systému (a počítače)
- Konfigurace
  - Vizualních efektů grafického rozhraní systému
  - Přidělování času procesoru službám a programům
  - Stránkovacích souborů
  - Prevence spuštění kódu z nespustitelných oblastí
- Přístup přes Vlastnosti systému (záložka Upřesnit) nebo příkazem **SystemPropertiesPerformance**

# Vizuální efekty a virtuální paměť



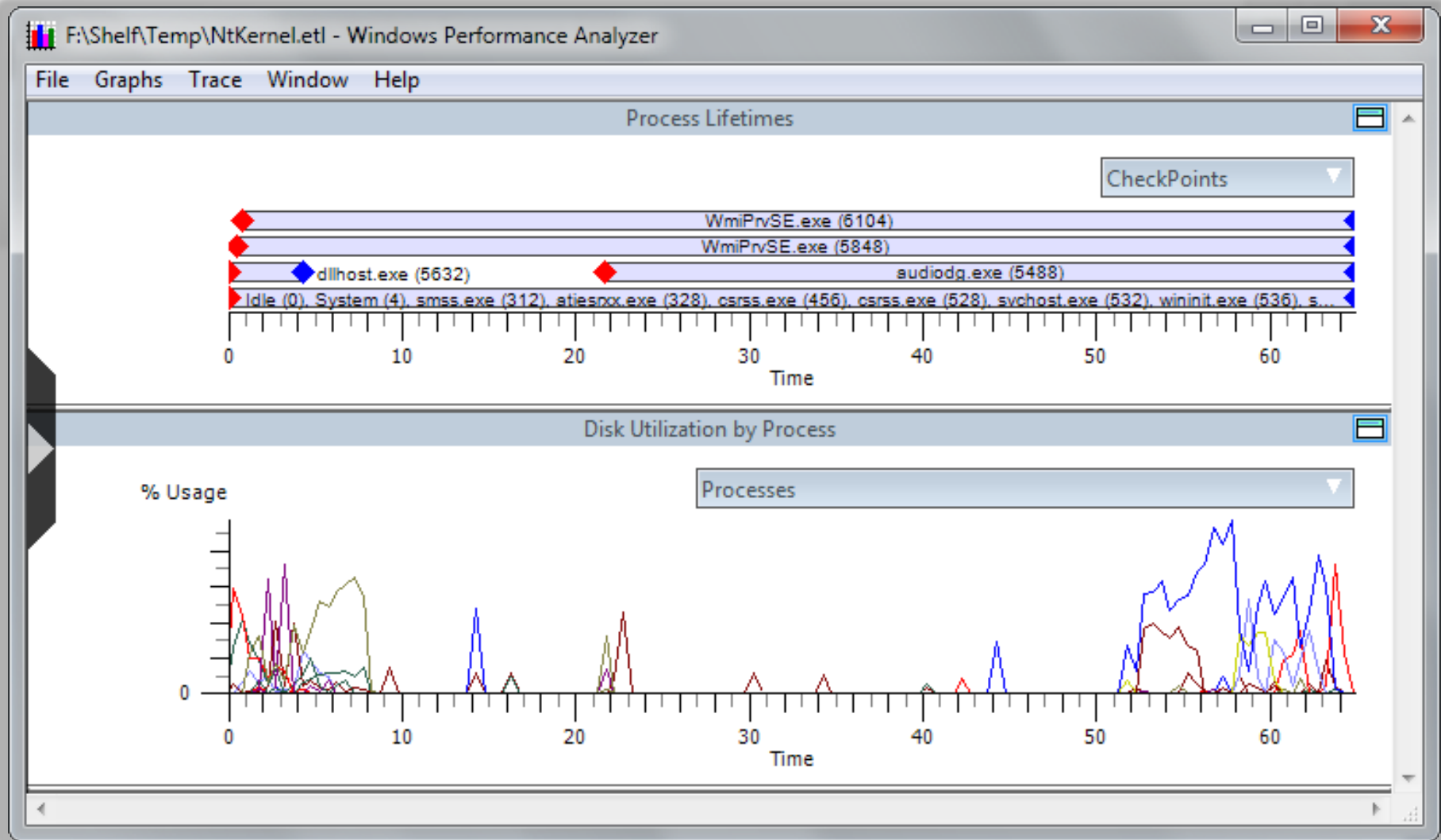
# Windows Performance Toolkit (WPT)

- Sada nástrojů pro profilování (měření a analýzu výkonu) systému a aplikací
  - Trasování událostí generovaných systémem (jádreem) nebo jednotlivými aplikacemi
  - Monitorování hodnot čítačů
- Součást Windows SDK a Windows ADK
- Zachytávání (a zaznamenávání) události ohledně
  - Přepnutí kontextu, přerušení, vyváření a ukončování procesů a vláken, odložených volání procedur, V/V operací s diskem, operací s registry, ...

# Nástroje

- Trace Capture, Processing, and Command-Line Analysis tool (**Xperf**)
  - Konfigurace poskytovatelů generujících události
  - Trasování událostí, vytváření tzv. *trace* (soubor ETL)
- Visual Trace Analysis tool (**Xperfview**)
  - Zobrazení *trace* (dříve zachycených událostí)
- On/Off Transition Trace Capture tool (**Xbootmgr**)
  - Trasování událostí během startu, vypínání, přechodu do režimu hibernace a spánku nebo obnově činnosti

# Ukázka vizualizace některých událostí



# WMI



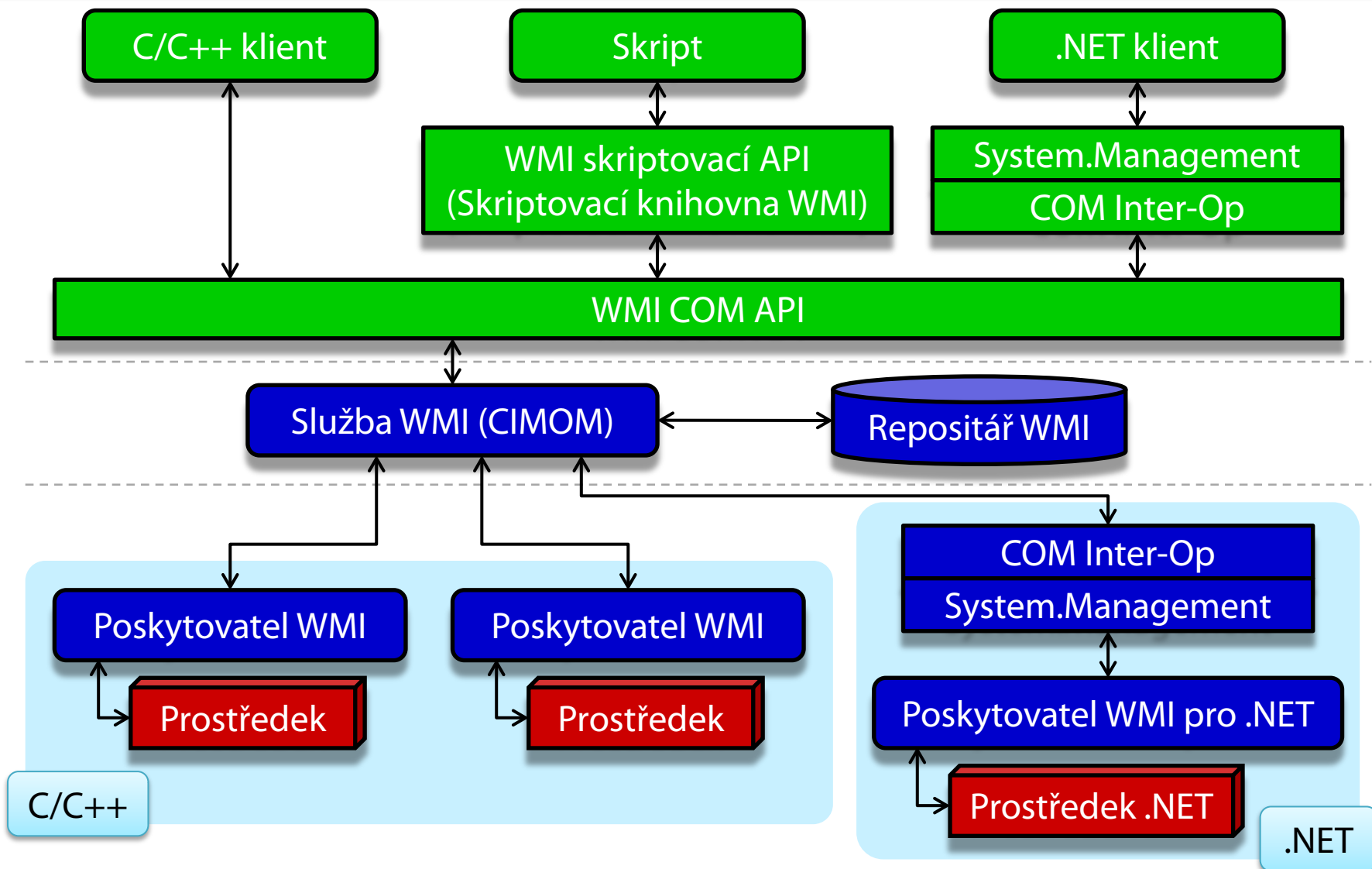
# WMI

- **Windows Management Instrumentation**
- Umožňuje přístup k informacím potřebným pro správu (prostředků) celého systému Windows
  - Implementace Web-based Enterprise Management
- Každý prostředek, jenž může být spravován přes WMI, je reprezentován vlastní WMI třídou
- Každá WMI třída popisuje
  - Vlastnosti prostředku
  - Akce, jenž lze použít pro správu prostředku

# Klienti WMI (WMI consumers)

- C/C++ programy
  - Přímá interakce s WMI pomocí COM API funkcí
- .NET programy
  - Interakce s WMI pomocí .NET objektů, které zajišťují interoperabilitu s COM (*Component Object Model*)
- Skripty
  - Interakce s WMI pomocí skriptovací knihovny WMI
    - Poskytuje sadu tzv. automatizačních objektů (*automation objects*), které umožňují autentizaci a připojení k WMI
    - Definuje objektový model spravovaných prostředků

# Infrastruktura WMI



# Služba WMI (WMI Service)

- Implementace CIMOM (*Common Information Model Object Manager*) v systému Windows
- Zajišťuje interakci mezi klienty WMI (označované *WMI consumers*) a poskytovateli WMI
  - Klienti WMI komunikují vždy jen se službou WMI
- Nevyřizuje požadavky klientů WMI, jen přeposílá tyto požadavky vhodným poskytovatelům WMI
  - Vhodní poskytovatele WMI (jenž jsou schopni daný požadavek vyřídit) jsou vyhledáni v repositáři WMI

# Poskytovatelé WMI (WMI Providers)

- Zprostředkovávají komunikaci mezi spravovaným prostředkem a CIMOM
  - Komunikují se spravovaným prostředkem pomocí API tohoto prostředku (odlišné pro každý prostředek)
  - Komunikují s CIMOM pomocí programového rozhraní WMI (standardizovaný model komunikace)
- Překládají WMI požadavky na volání specifických API funkcí konkrétního prostředku

# Repositář WMI (WMI Repository)

- Obsahuje definice veškerých dat zpřístupněných pomocí WMI (tzv. schéma)
  - Definice tříd reprezentujících spravované prostředky
  - Definice přítomných poskytovatelů WMI
- Třídy jsou organizovány hierarchicky
  - Rozděleny do jmenných prostorů (*namespaces*)
  - Seskupeny do skupin reprezentujících oblasti správy
- Instance prostředků nejsou uloženy v repositáři
  - Získány dynamicky pomocí poskytovatelů WMI

# Zjištění nainstalovaného systému

- VBScript

```
set objSWbemServices = _
    GetObject("winmgmts:\\localhost\root\cimv2")
set colSWbemObjectSet = _
    objSWbemServices.InstancesOf("Win32_OperatingSystem")
for each objSWbemObject in colSWbemObjectSet
    wscript.echo objSWbemObject.Caption
next
```

- PowerShell

```
$wmiObject = Get-WMIObject "Win32_OperatingSystem" `
    -ComputerName "localhost" -Namespace "root\cimv2"
$wmiObject.Caption
```

# WMI Administrative Tools

- WMI CIM Studio
  - Správa WMI tříd v repositáři WMI (úprava schématu)
- WMI Object Browser
  - Správa WMI objektů (zobrazení a modifikace hodnot vlastností, vykonávání metod apod.)
- WMI Event Registration Tool
  - Registrace a konfigurace odběratelů WMI událostí
- WMI Event Viewer
  - Prohlížení vygenerovaných WMI událostí

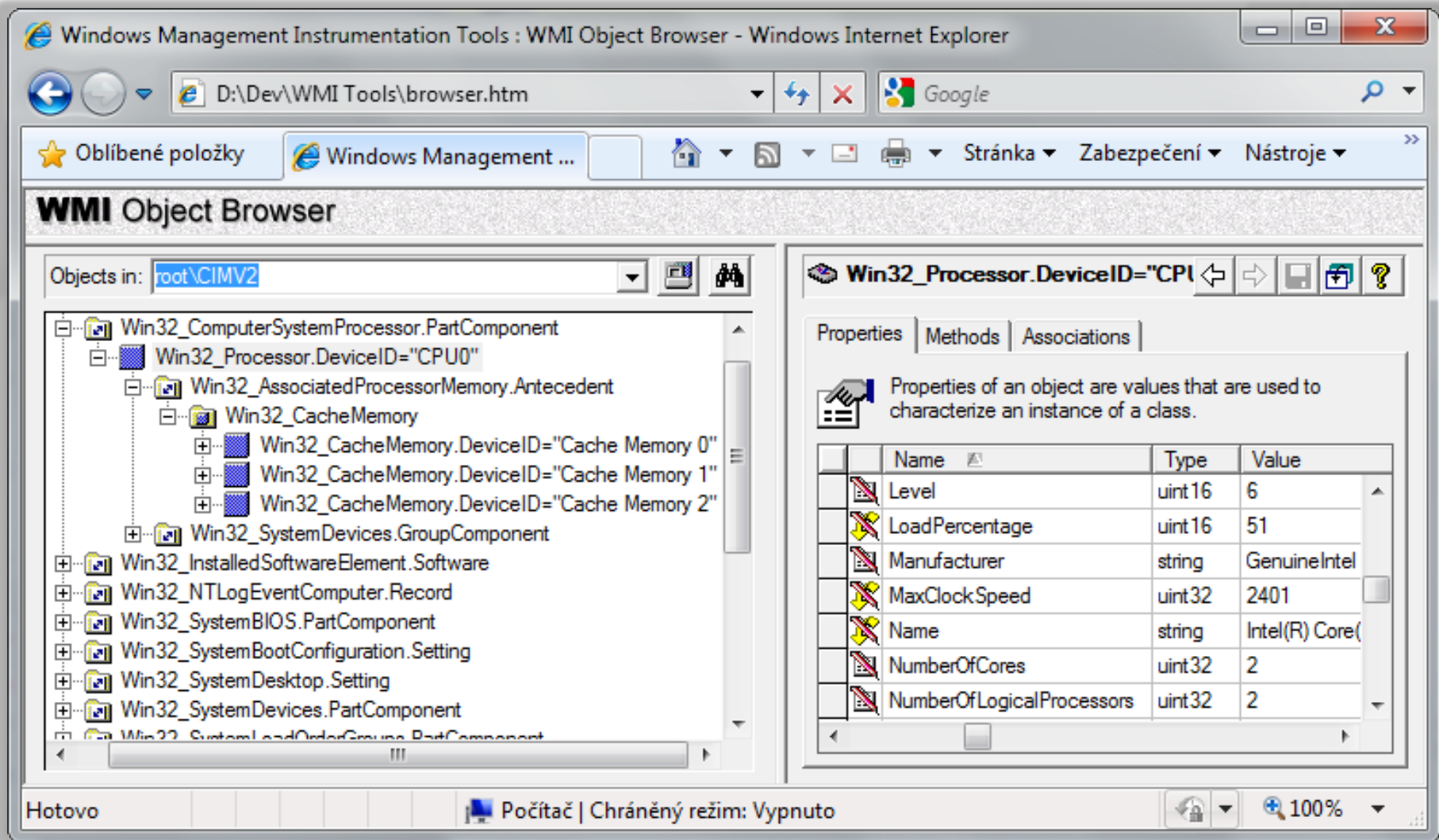


# WMI CIM Studio

The screenshot shows the WMI CIM Studio application window. The title bar reads "Windows Management Instrumentation Tools : WMI CIM Studio - Windows Internet Explorer". The address bar shows the file path "D:\Dev\WMI Tools\studio.htm". The main content area is divided into two panes. The left pane, titled "Classes in: root\CIMV2", displays a tree view of WMI classes, with "Win32\_OperatingSystem" selected and highlighted in blue. The right pane, titled "Win32\_OperatingSystem", shows the "Properties" tab. It contains a table of properties for the selected class. The table has columns for Name, Type, and Value. The properties listed are: BootDevice (string, <empty>), BuildNumber (string, <empty>), BuildType (string, <empty>), Caption (string, <empty>), CodeSet (string, <empty>), CountryCode (string, <empty>), and CreationClassName (string, <empty>). The status bar at the bottom shows "Hotovo", "Počítač | Chráněný režim: Vypnuto", and a zoom level of "100%".

Name	Type	Value
BootDevice	string	<empty>
BuildNumber	string	<empty>
BuildType	string	<empty>
Caption	string	<empty>
CodeSet	string	<empty>
CountryCode	string	<empty>
CreationClassName	string	<empty>

# WMI Object Browser



Windows Management Instrumentation Tools : WMI Object Browser - Windows Internet Explorer

D:\Dev\WMI Tools\browser.htm

Oblíbené položky Windows Management ...

## WMI Object Browser

Objects in: `root\CIMV2`

- Win32\_ComputerSystemProcessor.PartComponent
  - Win32\_Processor.DeviceID="CPU0"
    - Win32\_AssociatedProcessorMemory.Antecedent
      - Win32\_CacheMemory
        - Win32\_CacheMemory.DeviceID="Cache Memory 0"
        - Win32\_CacheMemory.DeviceID="Cache Memory 1"
        - Win32\_CacheMemory.DeviceID="Cache Memory 2"
      - Win32\_SystemDevices.GroupComponent
    - Win32\_InstalledSoftwareElement.Software
    - Win32\_NTLogEventComputer.Record
    - Win32\_SystemBIOS.PartComponent
    - Win32\_SystemBootConfiguration.Setting
    - Win32\_SystemDesktop.Setting
    - Win32\_SystemDevices.PartComponent
    - Win32\_SystemLoadOrderGroup.PartComponent

**Win32\_Processor.DeviceID="CPU0"**

Properties | Methods | Associations

Properties of an object are values that are used to characterize an instance of a class.

Name	Type	Value
Level	uint16	6
LoadPercentage	uint16	51
Manufacturer	string	GenuineIntel
MaxClockSpeed	uint32	2401
Name	string	Intel(R) Core(
NumberOfCores	uint32	2
NumberOfLogicalProcessors	uint32	2

Hotovo Počítač | Chráněný režim: Vypnuto 100%