

# Desktop systémy Microsoft Windows

IW1/XMW1 2016/2017

**Jan Fiedor**

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 29. 11. 2016

# Monitorování a výkon

# Nástroje pro monitorování počítače

- Monitorování **stavu** počítače
  - Základní informace o stavu počítače
    - Centrum akcí
  - Monitorování stavu počítače v reálném čase
    - Správce úloh, Sledování prostředků a Process Explorer
  - Zjišťování dalších informací o stavu počítače
    - Sledování spolehlivosti, Služby a Prohlížeč událostí
- Monitorování **výkonu** počítače
  - Sledování výkonu a Sady kolekcí dat
  - Možnosti výkonu

# Centrum akcí (Action Center)

- **Monitoruje** stav počítače z pohledu **bezpečnosti** a **údržby** a **oznamuje** problémy týkající se
  - Služby **Windows Update** (systém je aktuální, ...)
  - Antivirové ochrany (je přítomná a aktuální, ...)
  - **Řízení uživatelských účtů** a **Brány Firewall** (povoleny)
  - Zálohování a **Historie souborů** (zálohy vytvářeny, ...)
  - Stav (diskových) jednotek a **Prostorů úložišť**
  - ...
- Spuštění přes **Ovládací panely**

# Nastavení oznamování problémů

The image shows two overlapping windows from the Windows operating system. The background window is the 'Ovládací panely' (Control Panel) window, with the 'Změnit nastavení Centra akcí' (Change Action Center settings) link highlighted in blue. A blue arrow points from this link to the foreground window.

The foreground window is titled 'Změnit nastavení Centra akcí' (Change Action Center settings). It has a breadcrumb path: 'Centrum akcí > Změnit nastavení Centra akcí'. The window contains the following content:

- Vypnout nebo zapnout zprávy** (Turn off or on notifications)  
System Windows každou vybranou položku zkontroluje z hlediska možných problémů a v případě nalezení problémů vám odešle zprávu. [Jak Centrum akcí kontroluje problémy?](#)
- Zprávy zabezpečení** (Security messages)
  - Služba Windows Update
  - Ochrana proti spywaru a nežádoucímu softwaru
  - Nastavení zabezpečení Internetu
  - Řízení uživatelských účtů
  - Síťová brána firewall
  - Antivirová ochrana
  - Účet Microsoft
  - SmartScreen
  - Aktivace systému Windows
- Zprávy údržby** (Maintenance messages)
  - Windows Zálohování
  - Řešení potíží Windows
  - Automatická údržba
  - Domácí skupina
  - Stav jednotky
  - Historie souborů
  - Software pro zařízení
  - Prostory úložišť
  - Aplikace při spuštění

At the bottom right of the window are 'OK' and 'Storno' (Cancel) buttons.

# Správce úloh (Task Manager)

- Poskytuje základní informace o **výkonu** počítače
- Umožňuje správu **procesů**, **služeb** a **sezení**
  - **Informace** o procesech (využití CPU, paměti, ...)
  - Nastavení **spřažení** (*affinity*) a **priority** procesů
  - Povolení / zakázání **virtualizace** procesů
  - Možnost **ukončování** běhu procesů a výběru **aplikací**, jenž mají být spuštěny při **startu** systému **Windows**
- Spuštění příkazem **taskmgr**, klávesovou zkratkou **CTRL+SHIFT+ESC** nebo přes **CTRL+ALT+DEL**

# Správa procesů pomocí Správce úloh

Správce úloh

Soubor Možnosti Zobrazit

Procesy Výkon Historie aplikací Po spuštění Uživatelé Podrobnosti Služby

Název	PID	Základní priorita	Procesor	Popis	Platforma	Paměť ...	Pracovní sada ...	Virtualizace ...
chrome.exe	2668	Nižší než normální	00	Google Chrome	32 bitů	44 732 k	70 352 k	Zakázáno
chrome.exe	3176	Normální	00	Google Chrome	32 bitů	21 956 k	38 108 k	Zakázáno
chrome.exe	3052	Nižší než normální	00	Google Chrome	32 bitů	17 636 k	32 832 k	Zakázáno
cmdagent.exe	2288	Normální	00	COMODO Internet Security	64 bitů	1 892 k	3 184 k	Nepovoleno
conhost.exe	3540	Normální	00	Console Window Host	64 bitů	572 k	1 076 k	Zakázáno
csrss.exe	696	Normální	00	Client Server Runtime Process	64 bitů	1 856 k	2 792 k	Nepovoleno
csrss.exe	808	Normální	00	Client Server Runtime Process	64 bitů	1 788 k	97 764 k	Nepovoleno
daemonu.exe	8916	Normální	00	NVIDIA Settings Update Manager	32 bitů	4 328 k	5 544 k	Nepovoleno
dasHost.exe	2380	Normální	00	Device Association Framework Provider Host	64 bitů	832 k	1 268 k	Nepovoleno
DexControl.exe	5664	Normální	00	Dexpot Full-screen preview and Window catalog	32 bitů	832 k	1 548 k	Zakázáno
Dexcube.exe	5676	Nízká	00	3D desktop switching plugin for Dexpot	32 bitů	1 340 k	2 032 k	Povoleno
dexpot.exe	5608	Normální	00	Dexpot - Virtual desktops for Windows	32 bitů	2 368 k	6 092 k	Povoleno
Dexpot64.exe	5652	Normální	00	Dexpot64 Message Window	64 bitů	728 k	1 416 k	Zakázáno
DTLite.exe	5712	Normální	00	DAEMON Tools Lite	32 bitů	3 820 k	10 320 k	Zakázáno
dwm.exe	1224	Vysoká	00	Správce oken plochy	64 bitů	17 132 k	53 388 k	Zakázáno
egui.exe	3792	Normální	00	ESET Main GUI	64 bitů	4 196 k	10 360 k	Zakázáno
ekrn.exe	2396	Normální	00	ESET Service	32 bitů	91 312 k	102 620 k	Nepovoleno
ETDCtrl.exe	5328	Vyšší než normální	00	ETD Control Center	64 bitů	2 312 k	6 048 k	Zakázáno
ETDCtrlHelper.exe	5536	Vyšší než normální	00	ETD Control Center Helper	64 bitů	1 148 k	2 960 k	Zakázáno
explorer.exe	12120	Normální	00	Průzkumník Windows	64 bitů	41 812 k	88 512 k	Zakázáno
firefox.exe	9208	Normální	01	Firefox	32 bitů	243 652 k	341 560 k	Zakázáno

Méně informací Ukončit úlohu

# 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: 27 % ■ Nejvyšší frekvence: 100 %

Proces	PID	Stav	Procesor	Průměr procesoru	Vláčna	Platforma	Popis
<input type="checkbox"/> Dexcube.exe	5676	Spuštěno	0	0.00	3	32 bitů	3D desktop switchin...
<input type="checkbox"/> dexpot.exe	5608	Spuštěno	0	0.00	3	32 bitů	Dexpot - Virtual des...
<input type="checkbox"/> Dexpot64.exe	5652	Spuštěno	0	0.01	1	64 bitů	Dexpot64 Message ...
<input type="checkbox"/> DTLite.exe	5712	Spuštěno	0	0.00	5	32 bitů	DAEMON Tools Lite
<input type="checkbox"/> dwm.exe	1224	Spuštěno	1	0.45	5	64 bitů	Správce oken plochy
<input type="checkbox"/> egui.exe	3792	Spuštěno	0	0.00	8	64 bitů	ESET Main GUI
<input type="checkbox"/> ekrn.exe	2396	Spuštěno	0	0.01	35	32 bitů	ESET Service

**Disk** ■ V/V disku 3 MB/s ■ Nejvyšší aktivní čas: 0 %

**Síť** ■ V/V síť 6 kb/s ■ Využití síť: 0 %

**Paměť** ■ Chyby stránkování na disk/s: 0 ■ Využitá fyzická paměť: 68 %

Proces	PID	Chyby stránkování na disk/s	Potvrzení (kB)	Pracovní sada (kB)	Ke sdílení (kB)	Soukromé (kB)
Dexcube.exe	5676	0	3 432	7 252	5 664	1 588
dexpot.exe	5608	0	4 136	12 368	10 000	2 368
Dexpot64.exe	5652	0	1 576	3 480	2 620	860
DTLite.exe	5712	0	5 508	15 556	11 528	4 028
dwm.exe	1224	0	24 712	61 152	44 724	16 428
egui.exe	3792	0	5 864	17 516	13 184	4 332
ekrn.exe	2396	0	102 452	104 464	16 260	88 204

Zobrazení

Procesor 100 %

60 sekund 0 %

Disk 10 MB/s

0

Síť 100 kb/s

0

# Process Explorer

- Rozšíření **Správce úloh** (a **Sledování prostředků**)
  - Poskytuje **detailní** informace o běžících **procesech**
  - **Zdarma** ke stažení na webu **Windows Sysinternals**
- 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, ...

# Nástroj Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [TOASTER\John]

File Options View Process Find Handle Users Help

Process	PID	Priority	CPU	Description	Image Type	Working Set	Virtual Size	Virtualized
lsass.exe	908	9		Local Security Authority Process	64-bit	9 336 K	51 468 K	
csrss.exe	808	13	0.08	Client Server Runtime Process	64-bit	117 836 K	330 288 K	
winlogon.exe	856	13		Windows Logon Application	64-bit	10 168 K	64 164 K	
dwm.exe	1224	13	0.53	Správce oken plochy	64-bit	61 504 K	309 744 K	
explorer.exe	3968	8	0.03	Průzkumník Windows	64-bit	121 340 K	831 724 K	
cfp.exe	4928	8	0.10	COMODO Internet Security	64-bit	8 904 K	281 692 K	
RAVCpl64.exe	5248	8		Správce zvuku Realtek HD	64-bit	8 204 K	117 700 K	
ETDCtrl.exe	5328	10		ETD Control Center	64-bit	12 556 K	123 924 K	
ETDCtrlHelper.exe	5536	10		ETD Control Center Helper	64-bit	5 780 K	83 320 K	
igfxtray.exe	5432	8		igfxTray Module	64-bit	5 324 K	87 424 K	
hkcmd.exe	5552	8		hkcmd Module	64-bit	5 356 K	82 888 K	
igfxpers.exe	5576	8		persistence Module	64-bit	7 564 K	96 224 K	
dexpot.exe	5608	8	< 0.01	Dexpot - Virtual desktops for Windows	32-bit	12 428 K	130 740 K	Virtualized

Type	Name
File	\Device\Nsi
File	\Device\WMIDataDevice
File	\FileSystem\Filters\FitMgrMsg
Event	\KernelObjects\MaximumCommitCondition
Directory	\KnownDlls
ALPC Port	\RPC Control\OLEEF9BA6D57B2EEEAACE3A7D6660409
Directory	\Sessions\1\BaseNamedObjects
Event	\Sessions\1\BaseNamedObjects\##?#STORAGE#Volume#_??_USBST...
Mutant	\Sessions\1\BaseNamedObjects\_!SHMSFTHISTORY!_
Mutant	\Sessions\1\BaseNamedObjects\_SHuassist.mtx
Event	\Sessions\1\BaseNamedObjects\{43a2b8d7-6fed-4c18-bd36-b4630d61af...

CPU Usage: 51.15% Commit Charge: 47.91% Processes: 145 Physical Usage: 74.36%

# 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

Sledování spolehlivosti

Ovládací panely > Všechny položky Ovládacích panelů > Centrum akcí > Sledování spolehlivosti

Soubor Upravit Zobrazit Nástroje Nápověda

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.

Zobrazit podle: Dny | **Týdny** Naposledy aktualizováno: 30. 11. 2013 16:00

Chyby aplikací  
Chyby systému Windows  
Různé chyby  
Upozornění  
Informace

Podrobnosti o spolehlivosti pro: týden: 24. 12. 2012

Zdroj	Souhrn	Datum	Akce
<b>✘ Kritické události (5)</b>			
ESET Main GUI	Práce zastavena	25. 12. 2012 15:21	<a href="#">Vyhledat řešení</a>
Total Commander	Program přestal odpovídat a byl ukončen.	25. 12. 2012 15:22	<a href="#">Vyhledat řešení</a>
<b>⚠ Upozornění</b>			
OpenVPN Client	Neúspěšná instalace aplikace	26. 12. 2012 22:14	<a href="#">Zobrazit technické podrobnosti</a>
<b>i Informativní události (26)</b>			
Aktualizace zabezpečení systému Windows 8 ...	Úspěšná aktualizace pomocí služby Windows Update	25. 12. 2012 15:12	<a href="#">Zobrazit technické podrobnosti</a>
TAP-Win32 Adapter OAS	Úspěšná instalace ovladače	27. 12. 2012 14:36	<a href="#">Zobrazit technické podrobnosti</a>
OpenVPN Client	Úspěšná instalace aplikace	27. 12. 2012 14:36	<a href="#">Zobrazit technické podrobnosti</a>

Uložit historii spolehlivosti... Zobrazit všechna hlášení problémů Vyhledat řešení všech problémů... OK

# 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 **nabootování** celého systému

# MMC konzole Služby

The screenshot shows the Windows Services console window titled "Služby". The interface includes a menu bar (Soubor, Akce, Zobrazit, Nápověda), a toolbar with navigation and control icons, and a left-hand tree view showing "Služby (místní počítač)". The main area displays a table of services.

Název	Stav	Typ spouštění	Popis
Systém barev systému Windows		Ručně	Služba WcsPlugInServi...
Systém souborů EFS (Encrypting File System)		Ručně (Spuštění aktivační události)	Poskytuje základní tech...
Systém událostí COM+	Spuštěno	Automaticky	Podporuje službu ozn...
Systémová aplikace modelu COM+		Ručně	Spravuje konfiguraci a ...
Šifrování	Spuštěno	Automaticky	Poskytuje tři služby pr...
Šíření certifikátů	Spuštěno	Automaticky	Kopíruje uživatelské ce...
Te.Service		Ručně	
Technologie Windows Connect Now – Registrátor ko...		Ručně	Služba WCNCsvc je h...
Telefonie	Spuštěno	Ručně	Poskytuje podporu roz...
Události načítání snímků		Ručně	Spustí aplikace přidruž...
Úložná technologie Intel® Rapid	Spuštěno	Automaticky (Zpožděné spuštění)	Oznamuje události úlo...
Virtuální disk		Ručně	Poskytuje služby správ...
Visual Studio ETW Event Collection Service		Ručně	Provides the Visual Stu...
Výstrahy a protokolování výkonu		Ručně	Čítač Výstrahy a proto...
Vzdálená plocha	Spuštěno	Ručně	Umožňuje uživatelům i...
Vzdálená správa systému Windows (WS-Management)		Ručně	Služba Vzdálená správ...
Vzdálené volání procedur (RPC)	Spuštěno	Automaticky	Služba RPCSS je Správ...
Vzdálený registr		Zakázáno	Umožňuje vzdáleným ...

At the bottom of the window, there are tabs for "Rozšířené" and "Standardní".

# 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 **systemu**)
  - **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
- **Export** událostí do XML, CSV nebo TXT souboru
- **Zasílání** událostí na **vzdálené** počítače

# Definice vlastního zobrazení (filtru)

Vytvořit vlastní zobrazení

Filtr XML

Protokolováno: Kdykoli

Úroveň události:  Kritická  Upozornění  Podrobnosti  
 Chyba  Informace

Podle protokolu Protokoly události: Aplikace,Zabezpečení,System

Podle zdroje Zdroje události:

Zahrne nebo vyloučí ID události: 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

# Protokoly systému Windows

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

# 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: Předané události ▾

Typ odběru a zdrojové počítače

Spouštěno sběrem Vybrat počítače...  
Tento počítač kontaktuje vybrané zdrojové počítače a poskytuje odběr.

Spouštěno zdrojovým počítačem Vybrat skupiny počítačů...  
Zdrojové počítače ve vybraných skupinách musejí být pomocí zásad nebo místní konfigurace nakonfigurovány na kontaktování tohoto počítače a přijetí odběru.

Sbírané události: <filtr není konfigurován> Vybrat události... ▾

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

Změnit uživatelský účet či nakonfigurovat rozšířené nastavení: Upřesnit...

OK Storno

# Pokročilá nastavení odběru

**Rozšířené nastavení**

**Uživatelský účet:**  
Vybraný účet musí mít přístup ke čtení zdrojových protokolů.

Účet počítače

Určitý uživatel

w8pro\Homer

Uživatelské jméno a heslo...

**Optimalizace doručení:**

Normální

Minimalizovat přenos

Minimalizovat zpoždění

Vlastní

Protokol: HTTP

Port: 5985

OK Storno

# 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



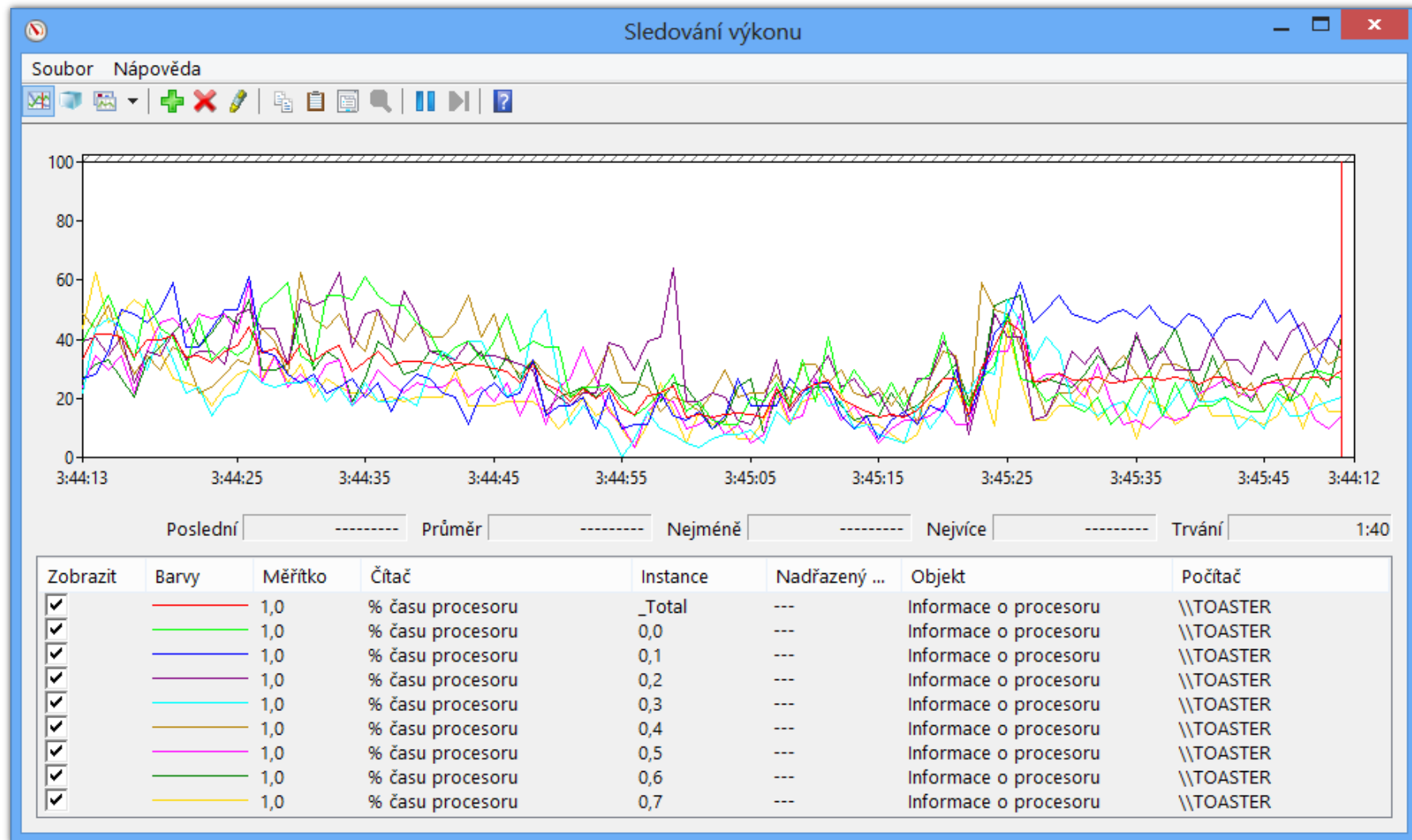
# Typy čítačů

- 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 **systemu**
- Mohou zaznamenávat
  - **Hodnoty** nebo **překročení** mezí **čítačů** (výstrahy)
  - 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, uživatelích, ...)
  - 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**
    - Zobrazit **zprávu** (zastaralé), lze nahradit voláním **msg.exe**
    - Odeslat **e-mail** (zastaralé), lze nahradit voláním **Windows PowerShell** příkazu (*cmdletu*) **Send-MailMessage**

# Nastavení čítačů a upozornění čítačů

Kolekce čítače dat – vlastnosti

Čítače výkonu Soubor

Čítače výkonu:

\Informace o procesoru(\_Total)\% času procesoru

Přidat...

Odebrat

Formát protokolu:

Binární

Ukázkový interval: 5

Jednotky: Sekundy

Maximální vzorky: 0

Název zdroje dat:

OK Storno Použít Nápověda

Upozornění čítače výkonu – vlastnosti

Upozornění Upozorňující akce Upozorňující úloha

Čítače výkonu:

\Informace o procesoru(\_Total)\% času procesoru

Přidat...

Odebrat

Upozornění při: Vyšší než

Mez: 90

Ukázkový interval: 5

Jednotky: Sekundy

OK Storno Použít Nápověda

# 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 (šablona)** 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
  - **Vizuálních efektů** grafického rozhraní systému
  - **Přidělování** času procesoru **službám** a **programům**
  - Stránkovacích souborů
  - **Prevence** spouštění kódu z **nespustitelných** oblastí
- Přístup přes **Vlastnosti systému** (záložka **Upřesnit**) nebo příkazem **SystemPropertiesPerformance**

# Vizuální efekty a virtuální paměť

