Desktop systémy Microsoft Windows

IW1/XMW1 2017/2018

Peter Solár

solar@pocitacoveskoleni.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 6. 12. 2017

Monitorování a výkon

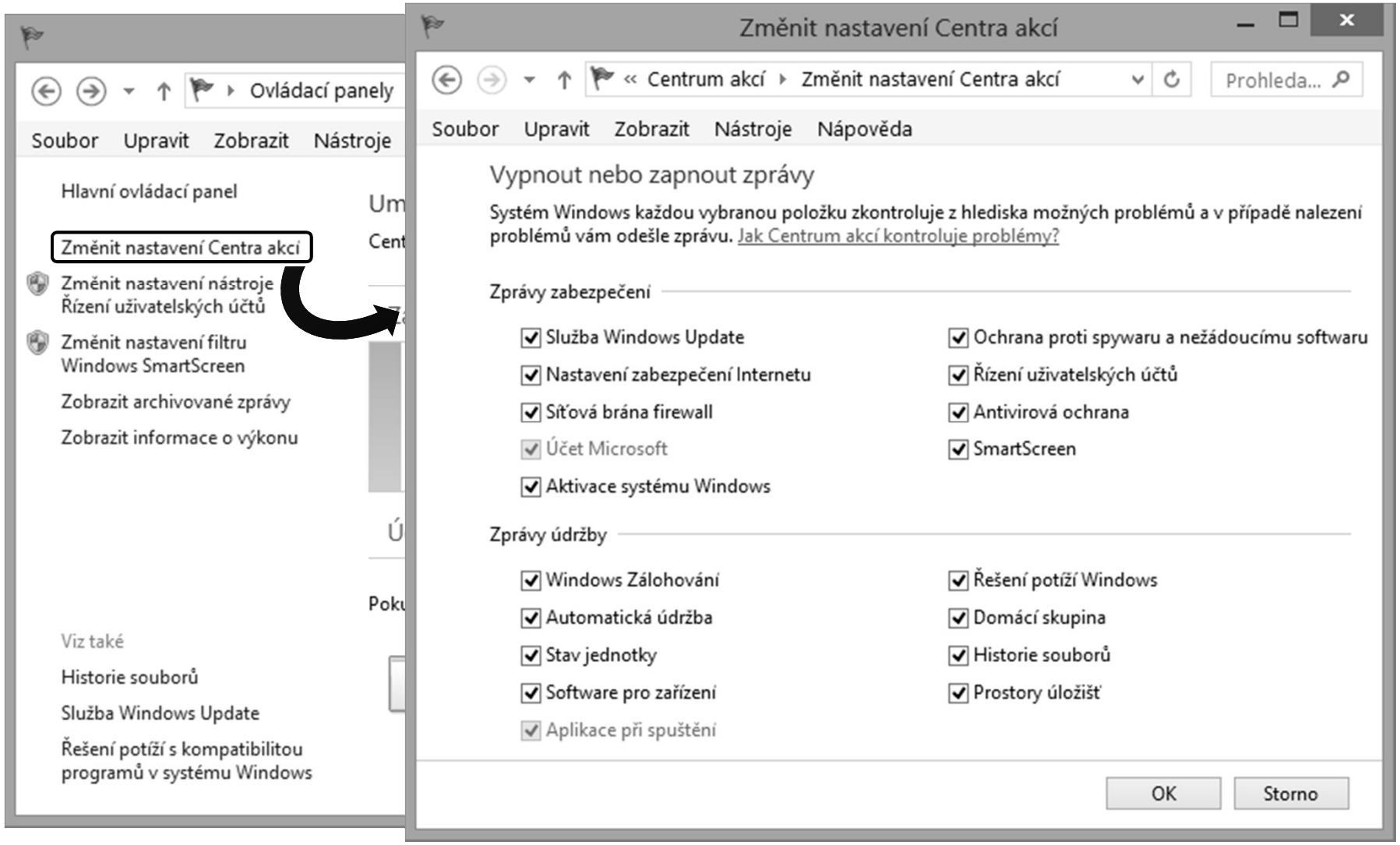
Nástroje pro monitorování počítače

- Monitorování stavu počítače
  - Základní informace o stavu počítače
    - Zabezpečení a údržba (dříve 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

Zabezpečení a údržba (Security and Maintenance)

- Monitoruje stav počítače z pohledu bezpečnosti a údržby a oznamuje problémy týkají 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, …)
  - Stavu (diskových) jednotek a Prostorů úložišť
  - …
- Spuštění přes Ovládací panely

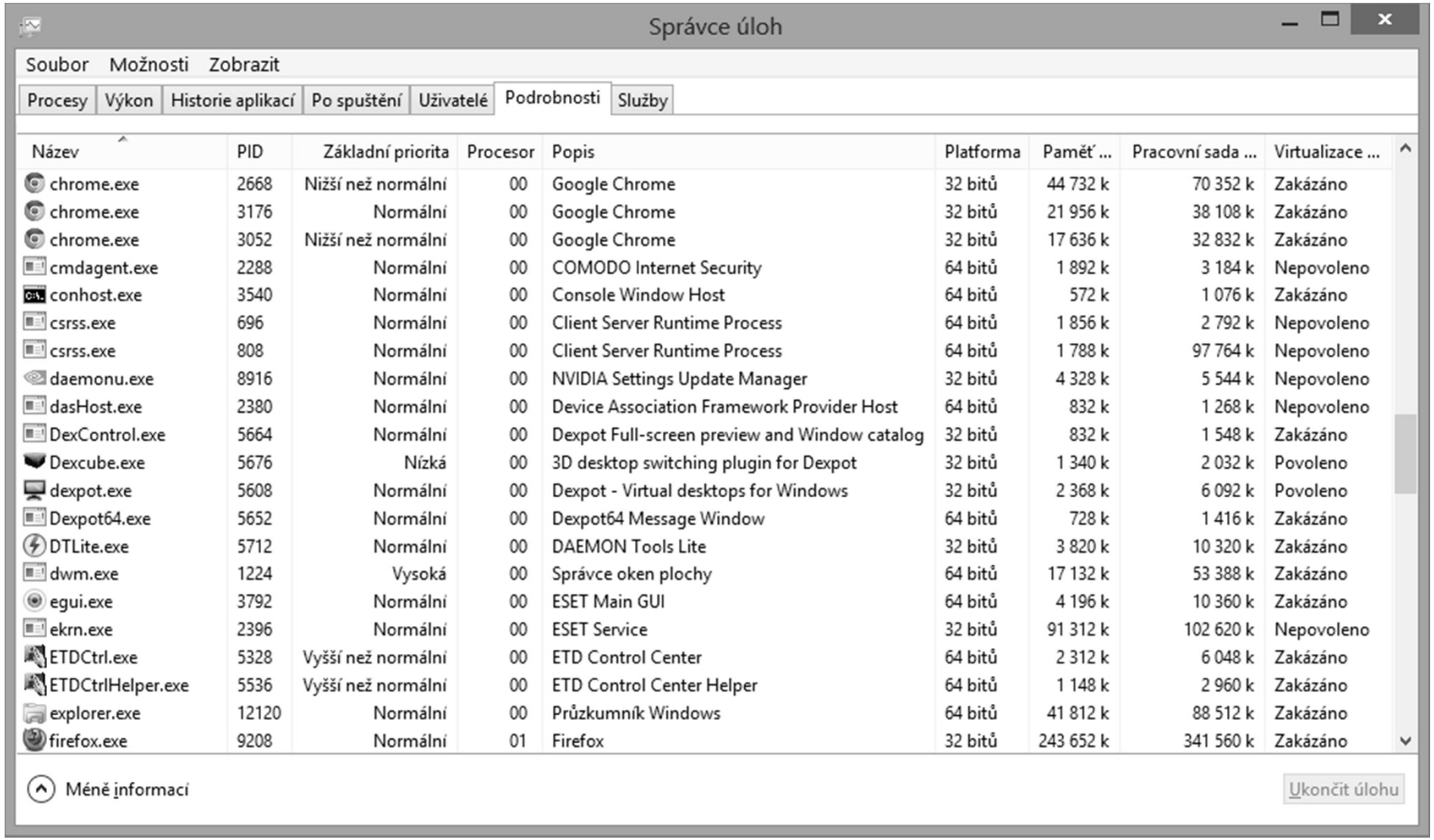
Nastavení oznamování problémů



Správce úloh (Task Manager)

- Poskytuje základní informace o výkonu počítače
- Umožňuje správu procesů, služeb a sezení
  - Informace o procesech (využití CPU, paměti, …)
  - 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

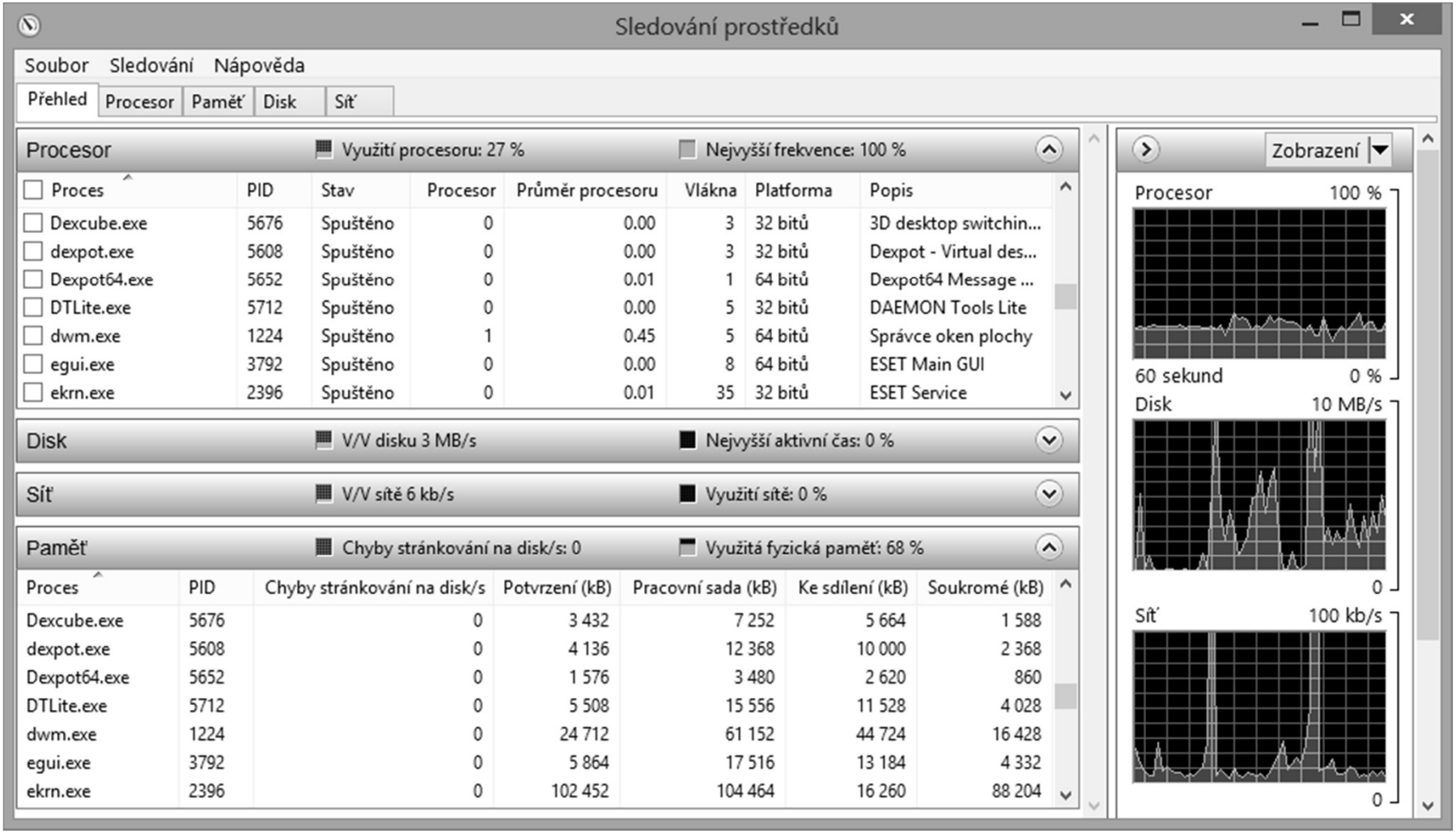


Název	PID	Základní priorita	Procesor	Popis	Platforma	Paměť ...	Pracovní sada ...	Virtualizace ...
chrome.exe	2668	Nižší než normální	00	Google Chrome	32 bitů	44 732 k	70 352 k	Zakázáno
chrome.exe	3176	Normální	00	Google Chrome	32 bitů	21 956 k	38 108 k	Zakázáno
chrome.exe	3052	Nižší než normální	00	Google 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

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

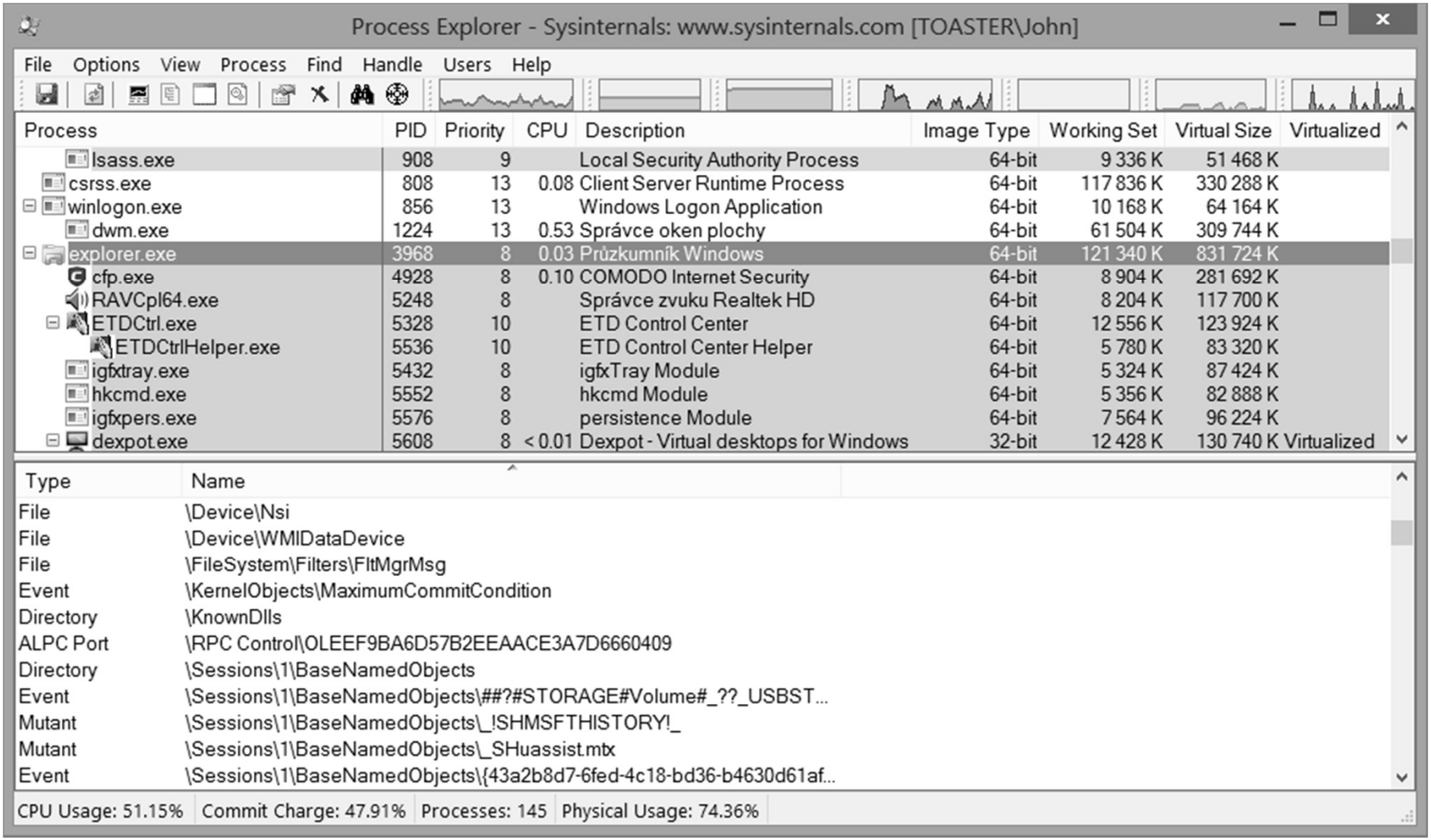
Nástroj Sledování prostředků



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, …

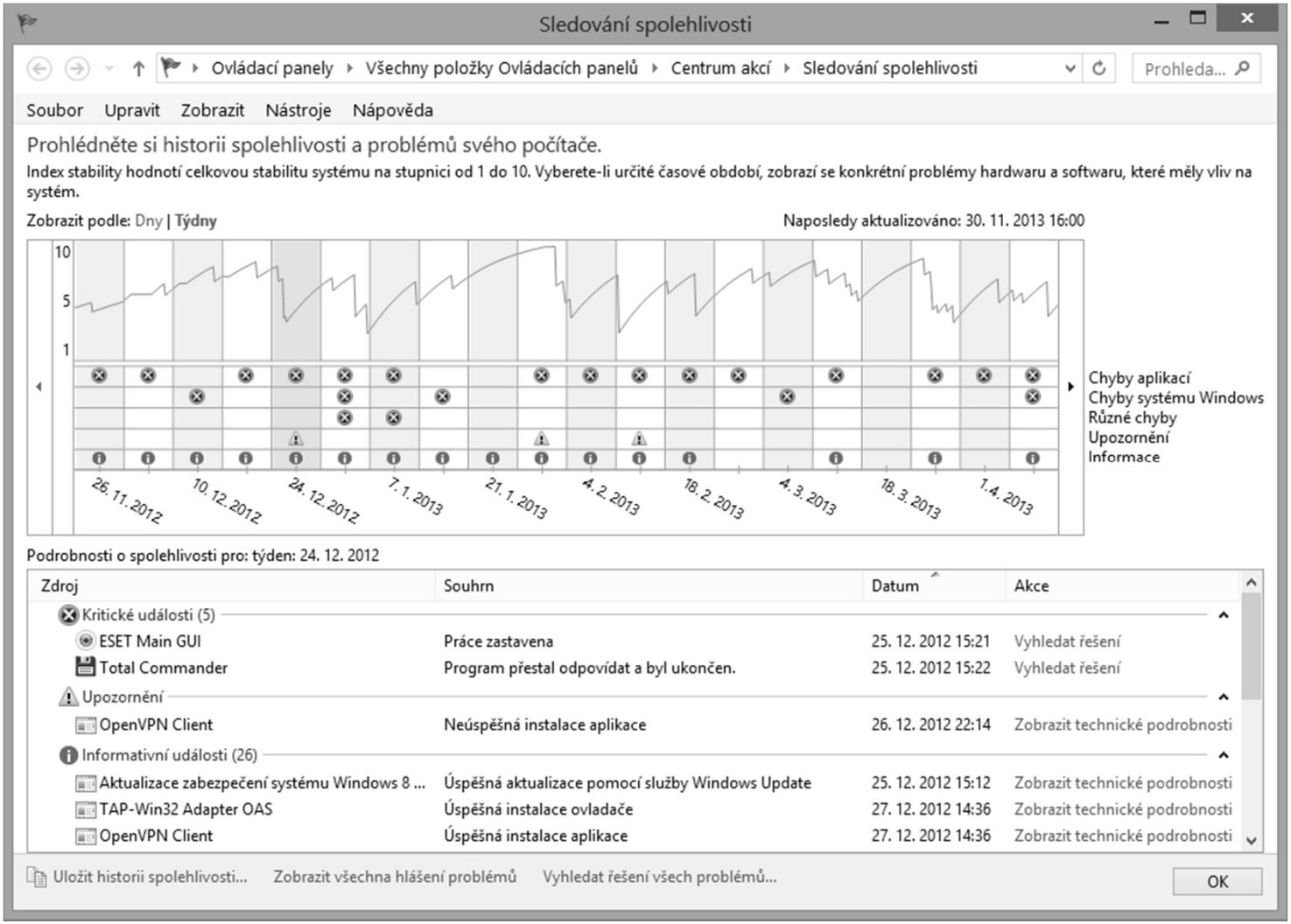
Nástroj Process Explorer



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

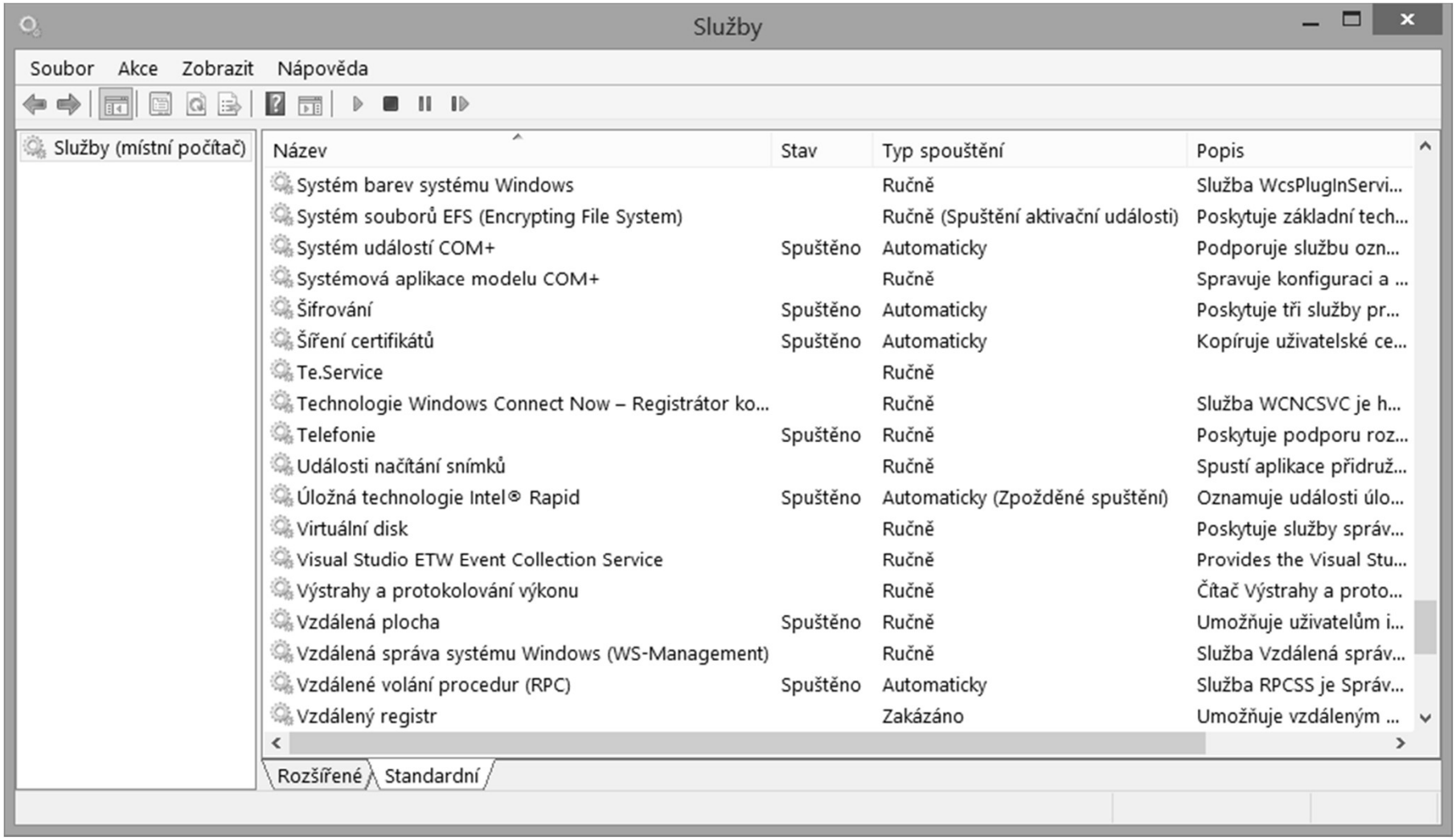
Nástroj Sledování spolehlivosti



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



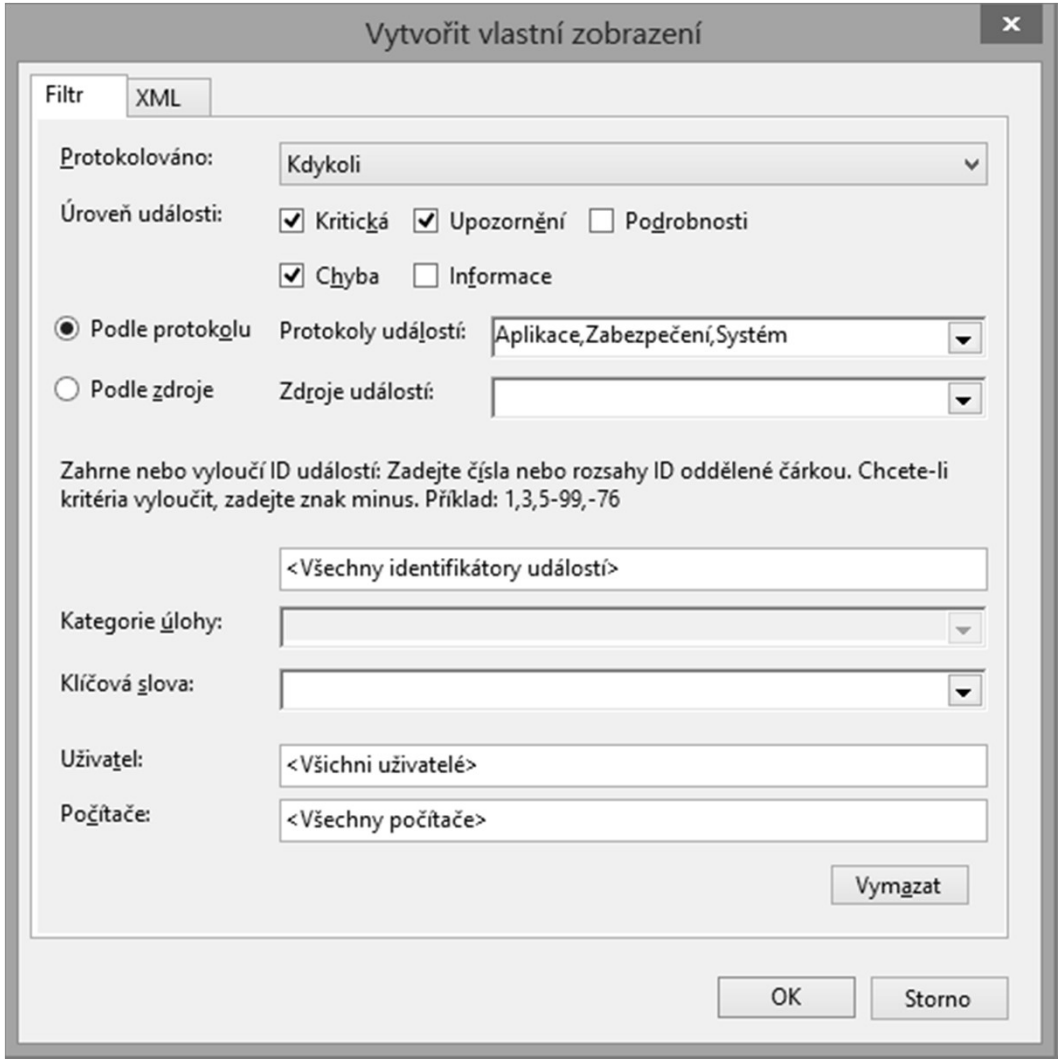
Prohlížeč událostí (Event Viewer)

- 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 funkcionalita

- 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)



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

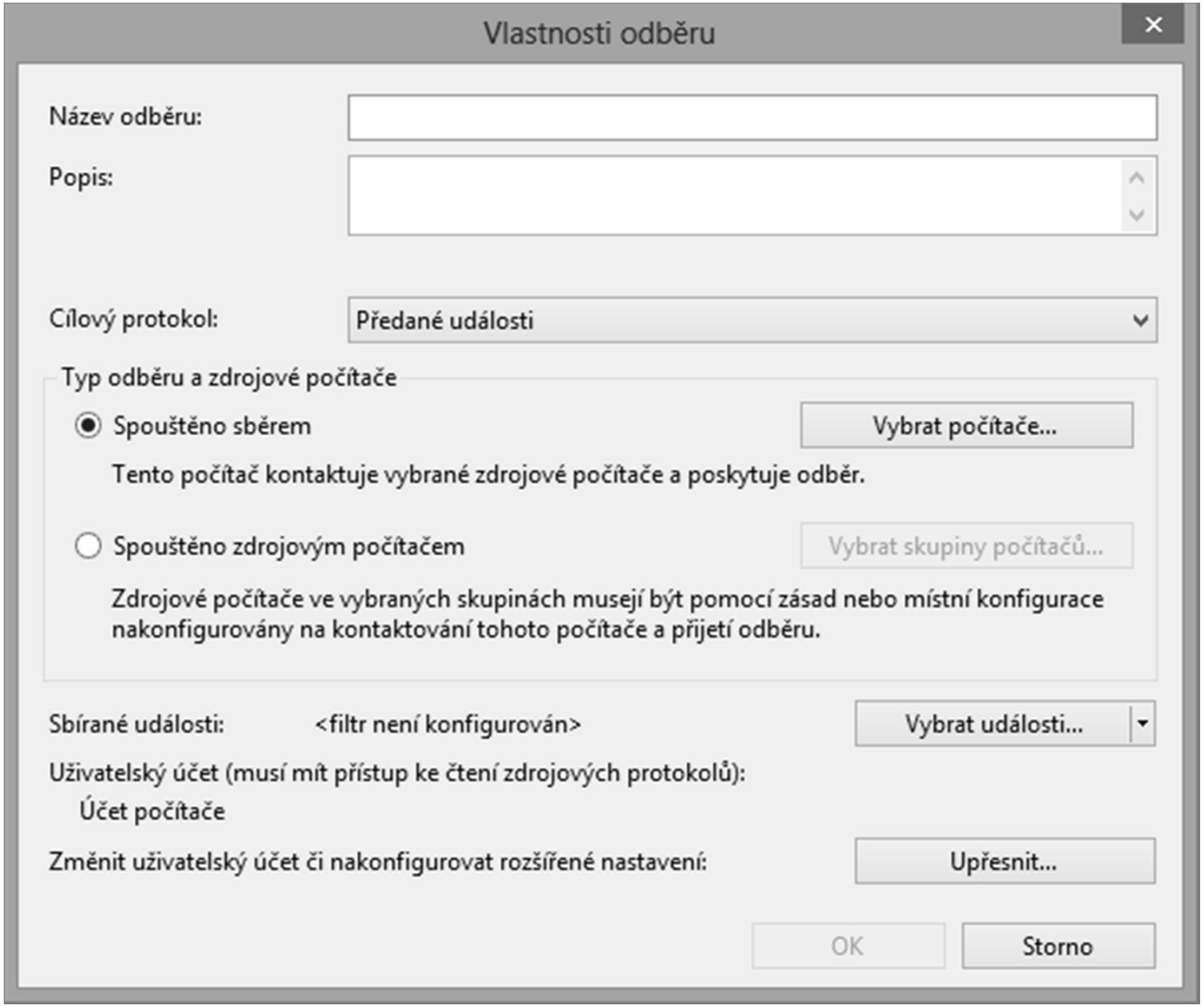
Předávání událostí (Event Forwarding)

- 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

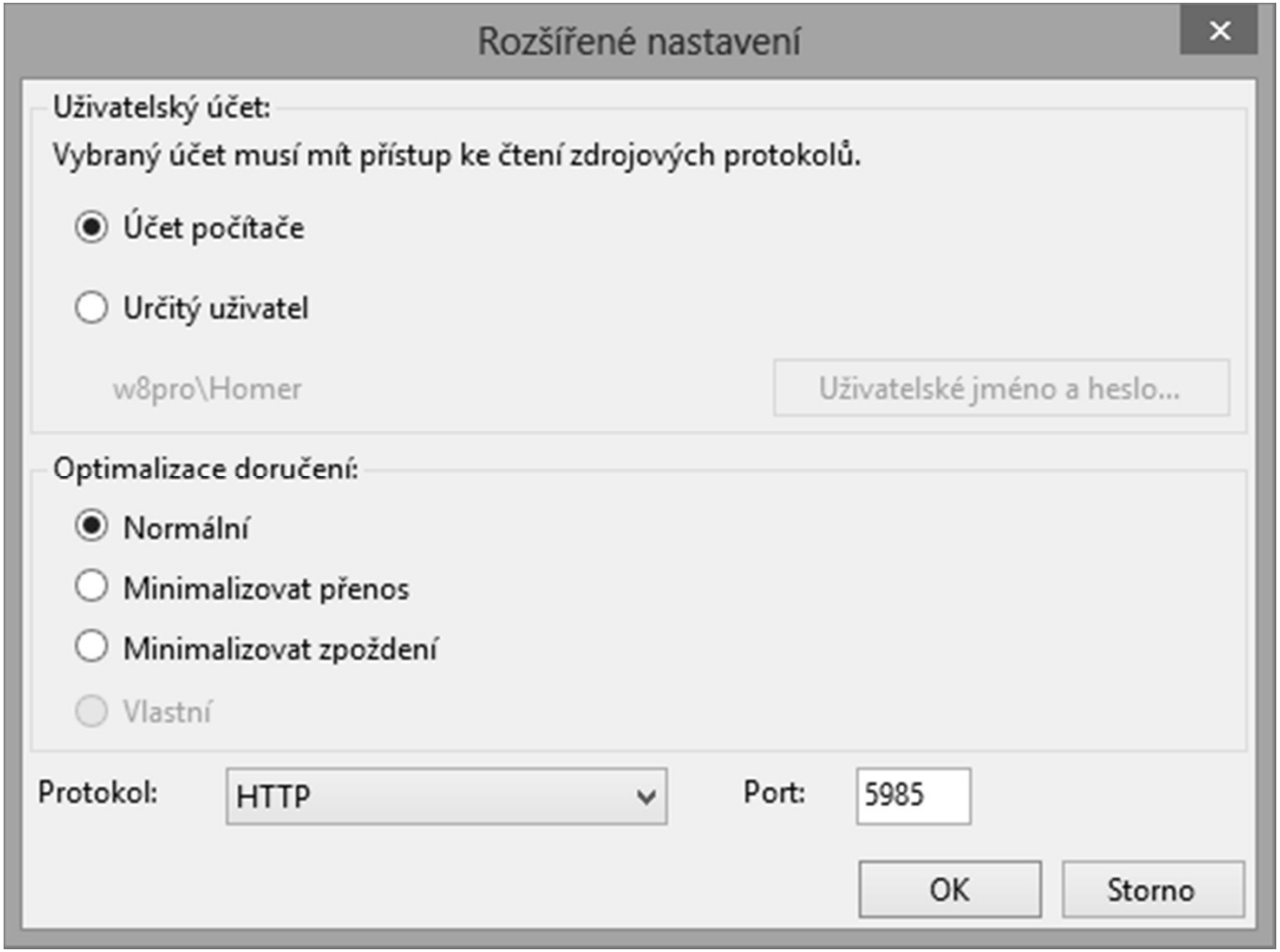
Režimy odběrů (subscription) událostí

- 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



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

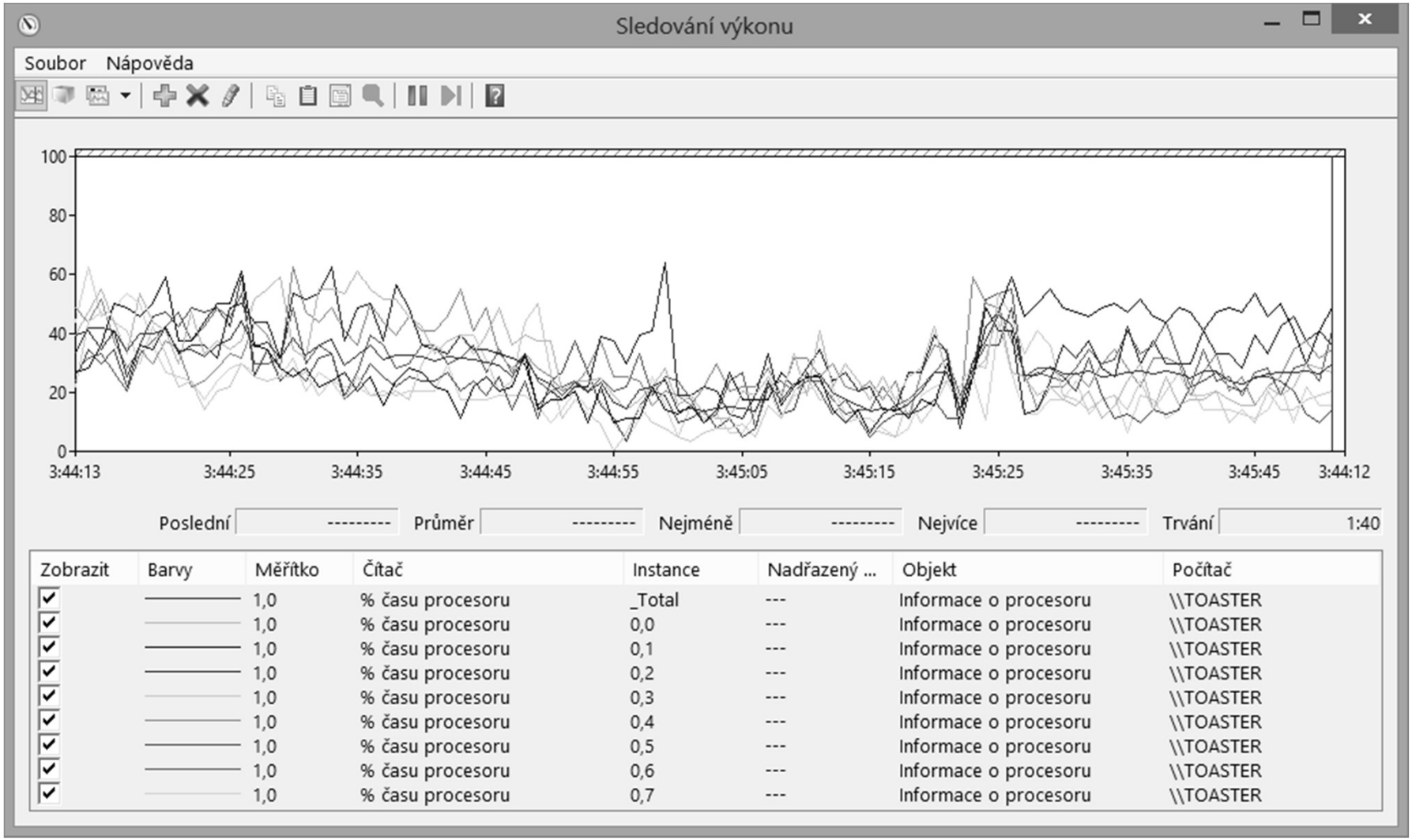
Typy čítačů

- Čítače hardwaru (zařízení)
  - 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 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

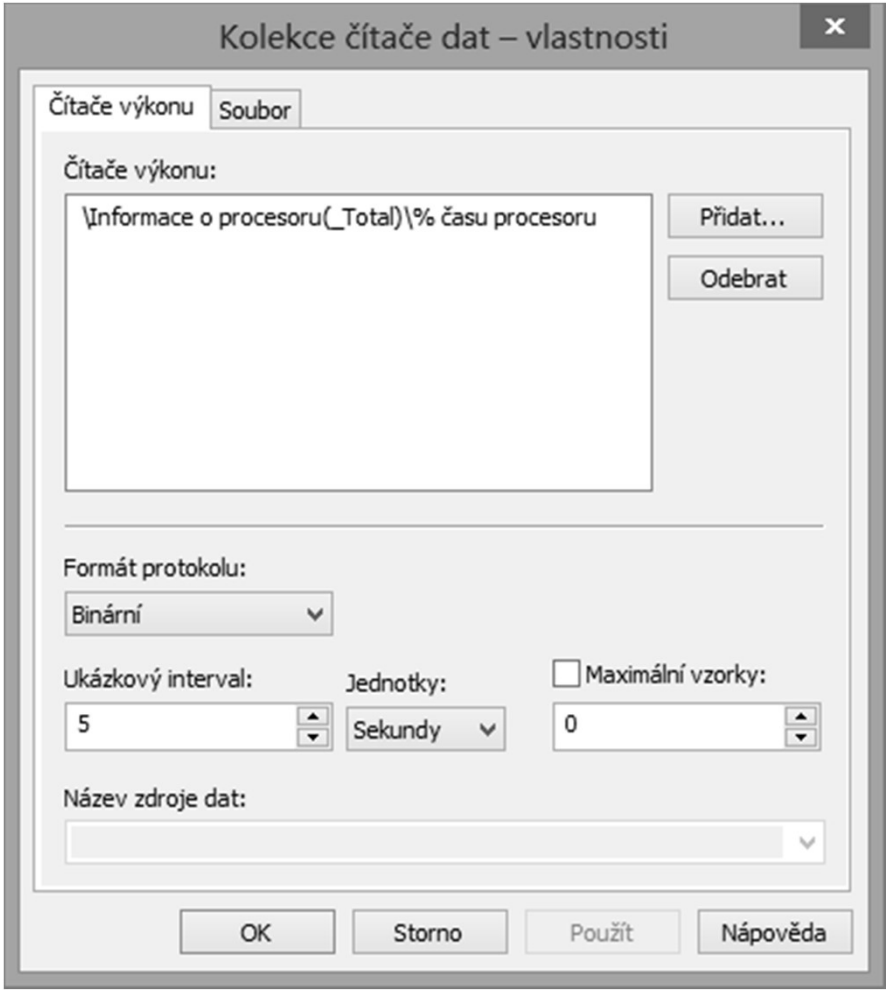
Systémové sady kolekcí dat

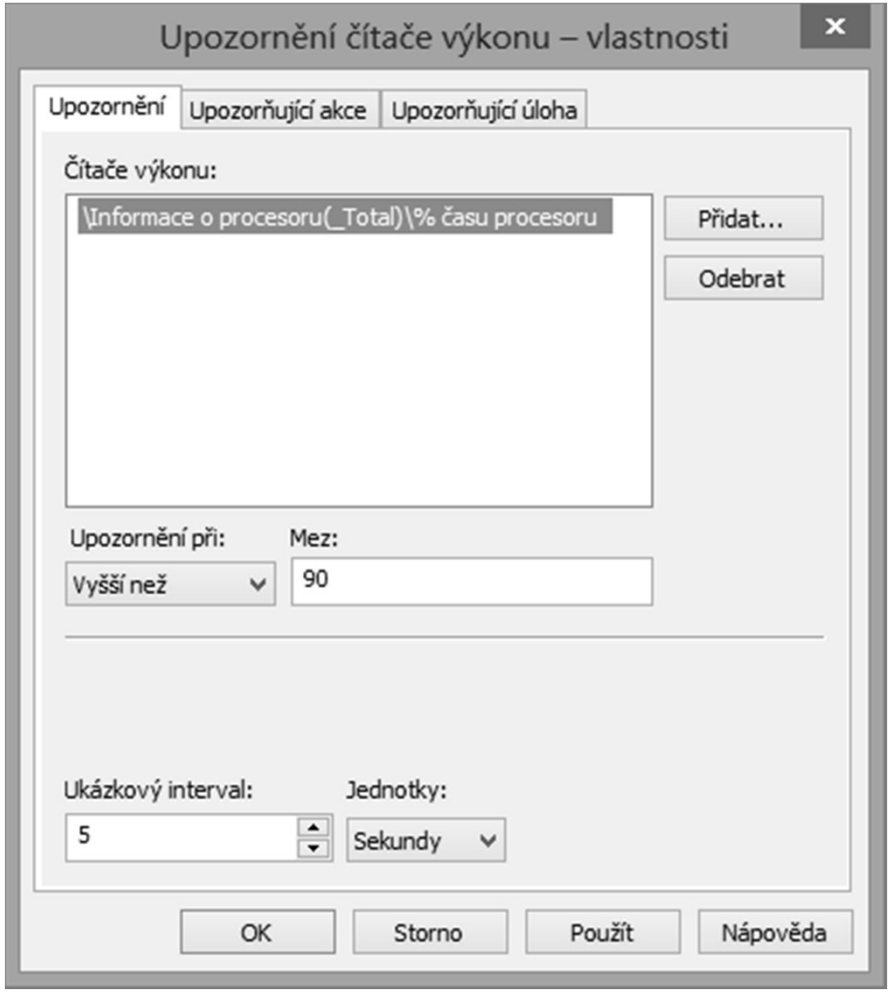
- Výkon systému (*System Performance*)
  - Zaznamenává hodnoty čítačů procesor, fyzický disk, paměť, IPv4, IPv6, …
  - Zaznamenává data trasování jádra
  - Vhodné při náhlém zpomalení počítače
- Diagnostika systému (*System Diagnostics*)
  - Zaznamenává stejné informace jako Výkon systému
  - Zaznamenává 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





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
  - 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