Desktop systémy Microsoft Windows

IW1/XMW1 2011/2012

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

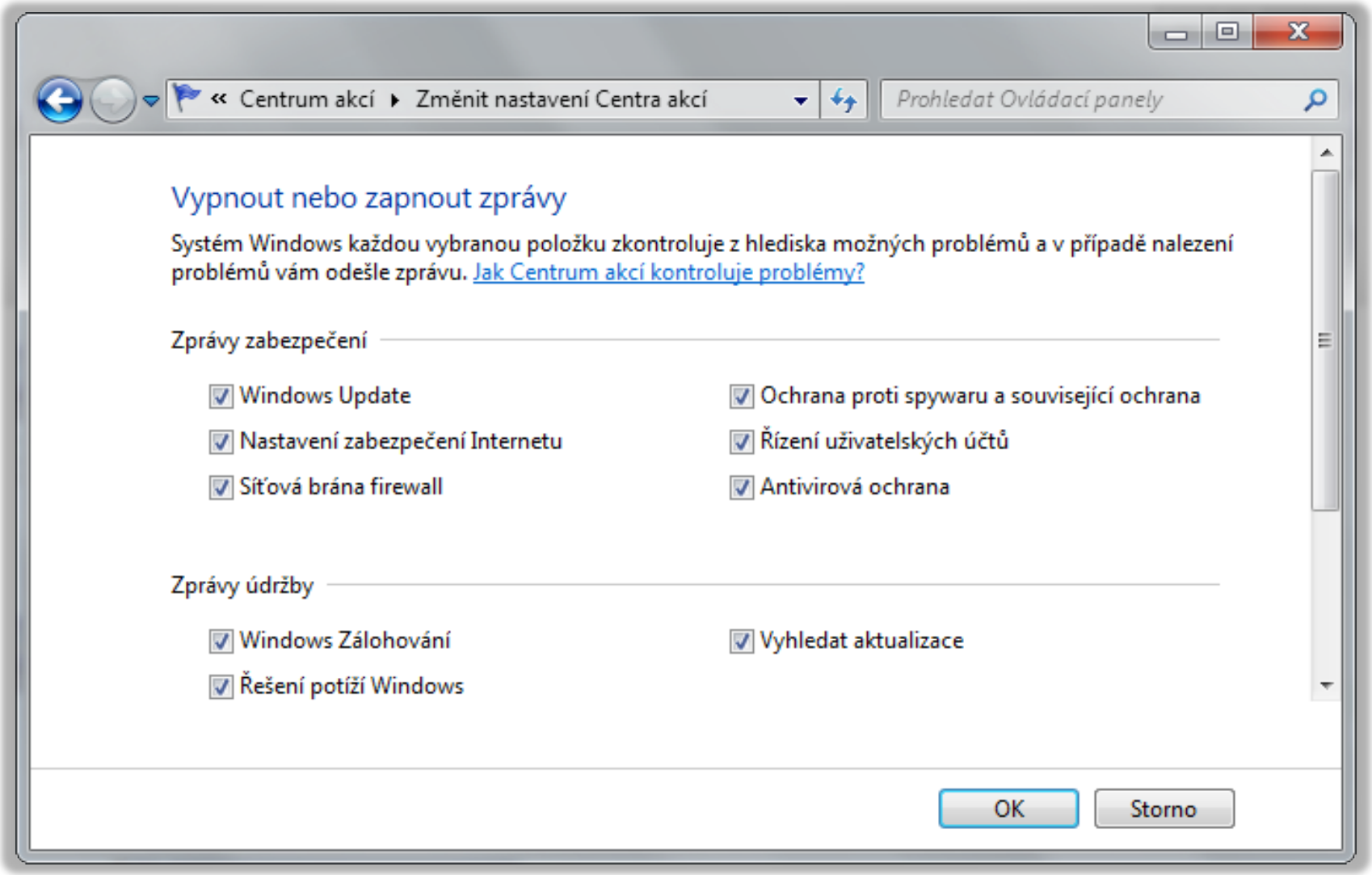
Revize 28.11.2011

Monitorování a výkon

Centrum akcí (Action Center)

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

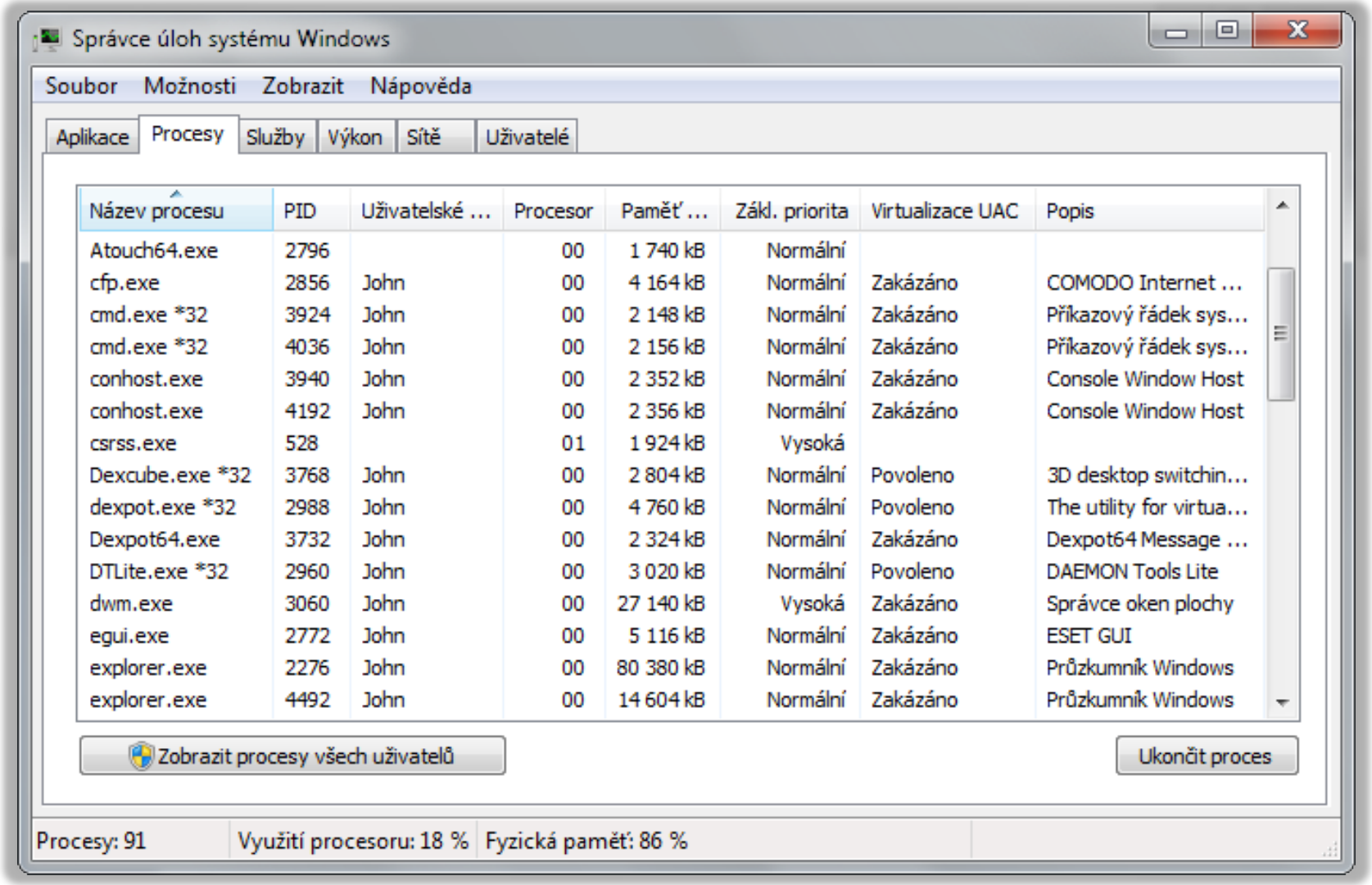
Nastavení oznamování problémů



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**

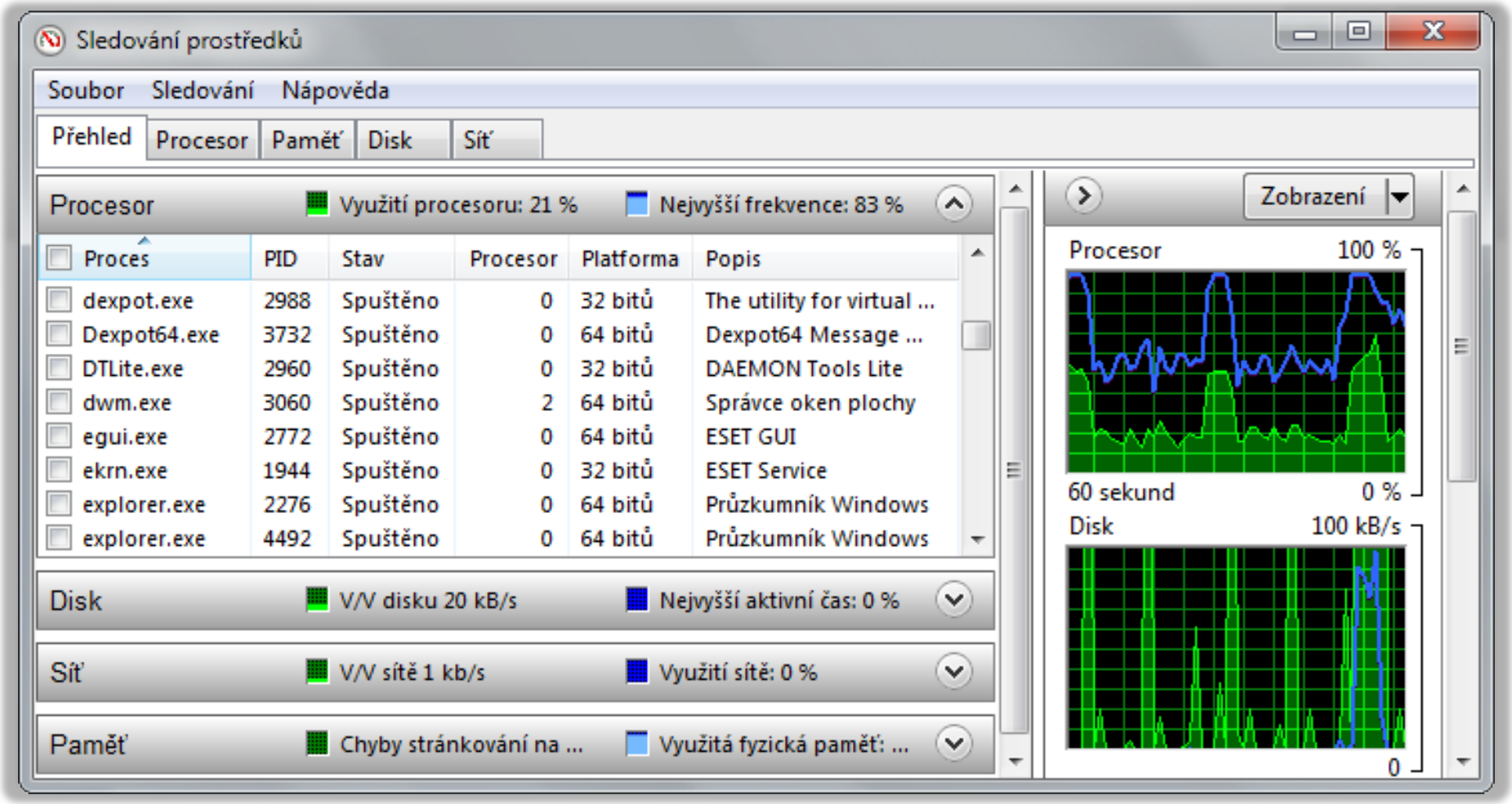
Správa procesů pomocí Správce úloh



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

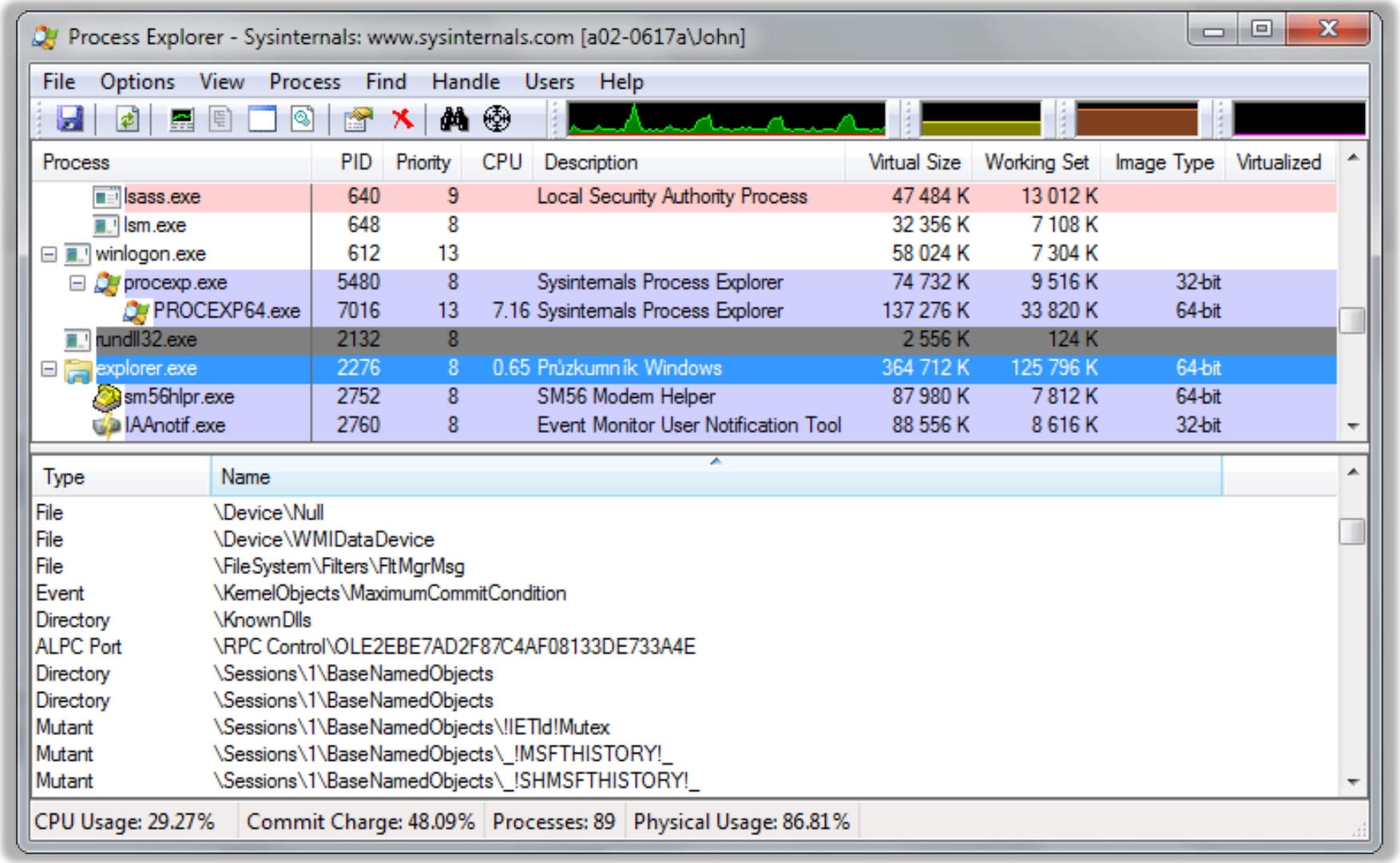
Nástroj Sledování prostředků



Process Explorer

- Rozšíření Správce úloh (a Sledování prostředků)
  - Poskytuje detailní informace o procesech, zdrojích, …
- 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

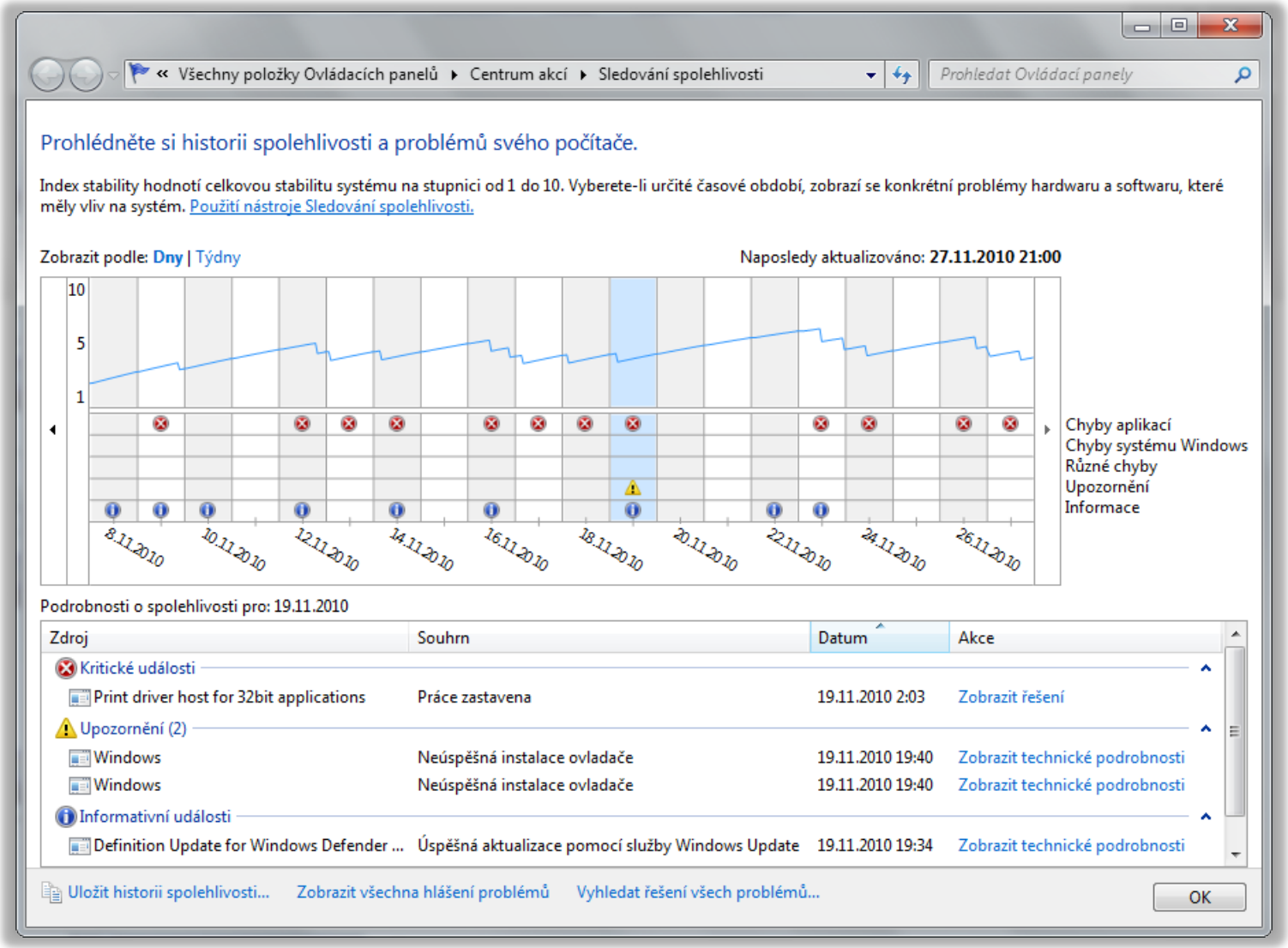
Nástroj Process Explorer



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

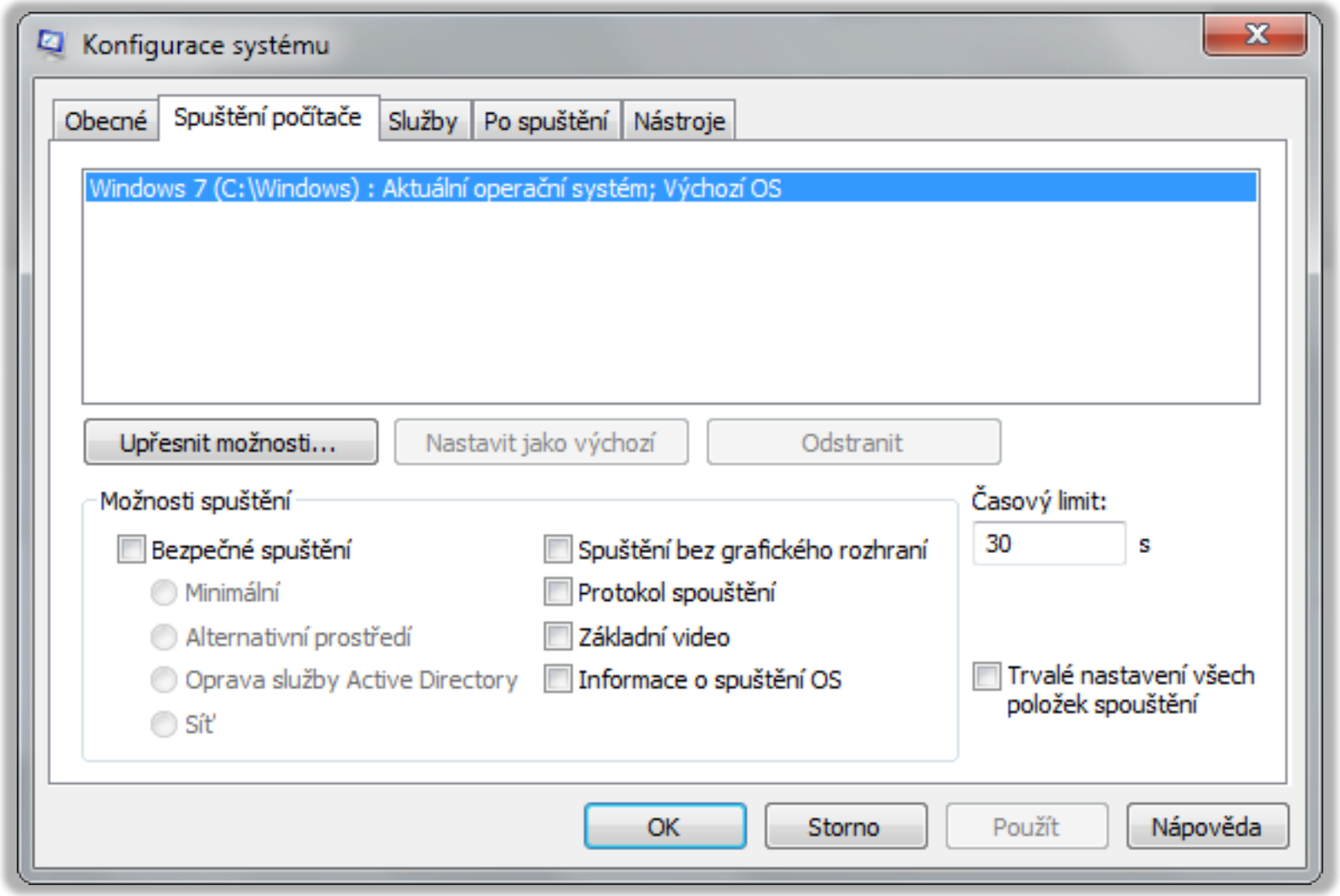
Nástroj Sledování spolehlivosti



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**

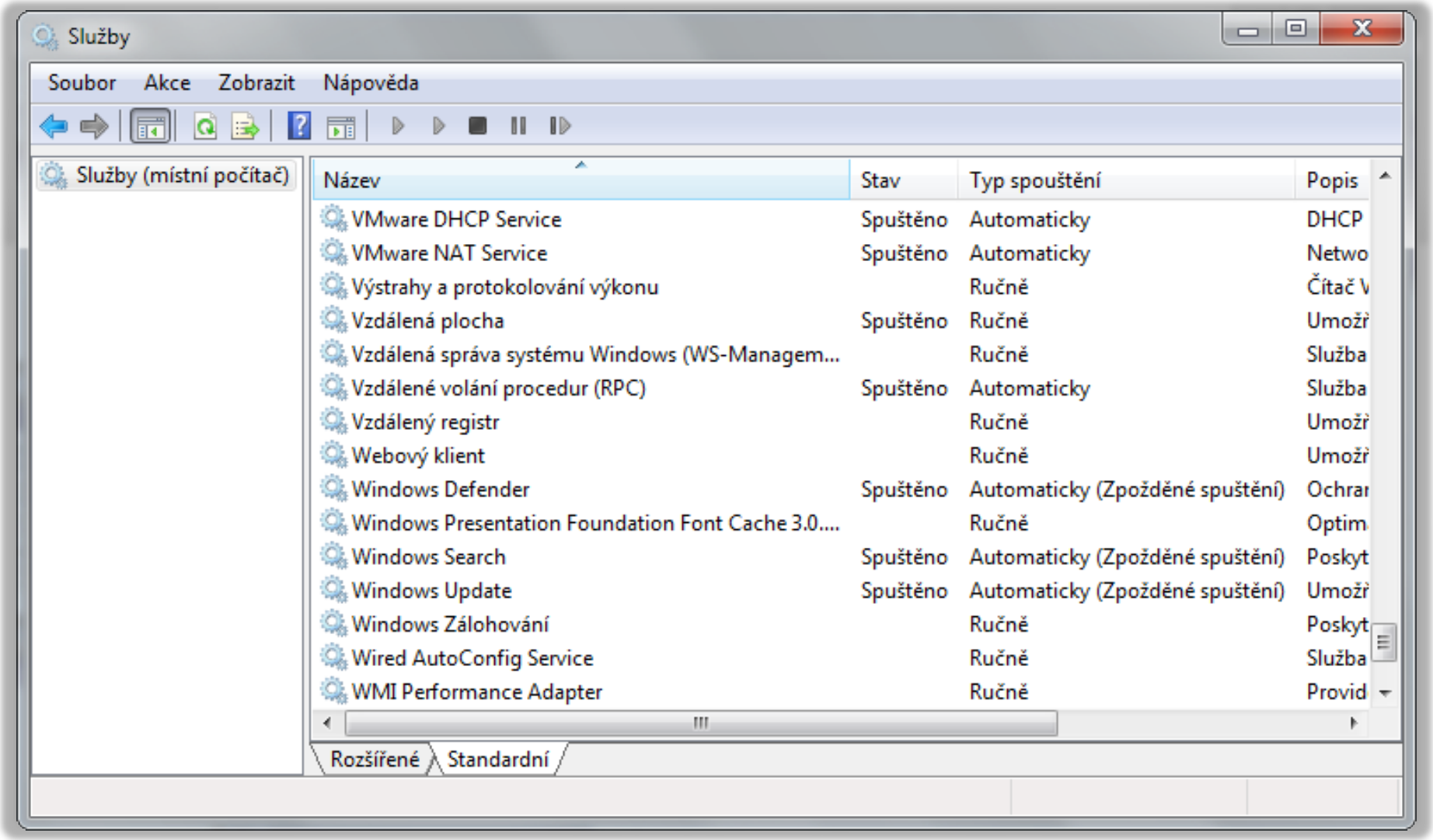
Nástroj konfigurace systému



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 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)

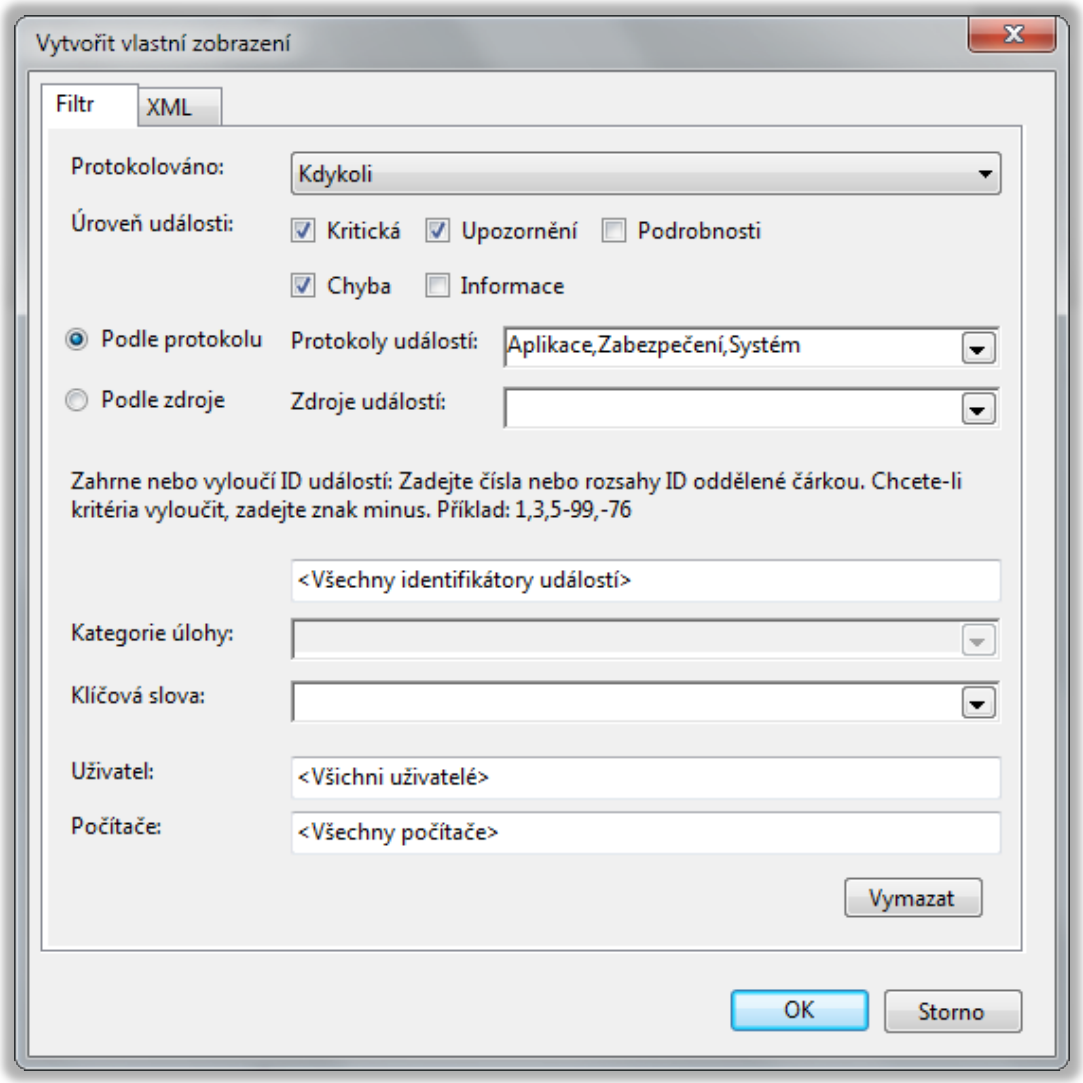
Další možnosti a funkcionalita

- 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
- 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)



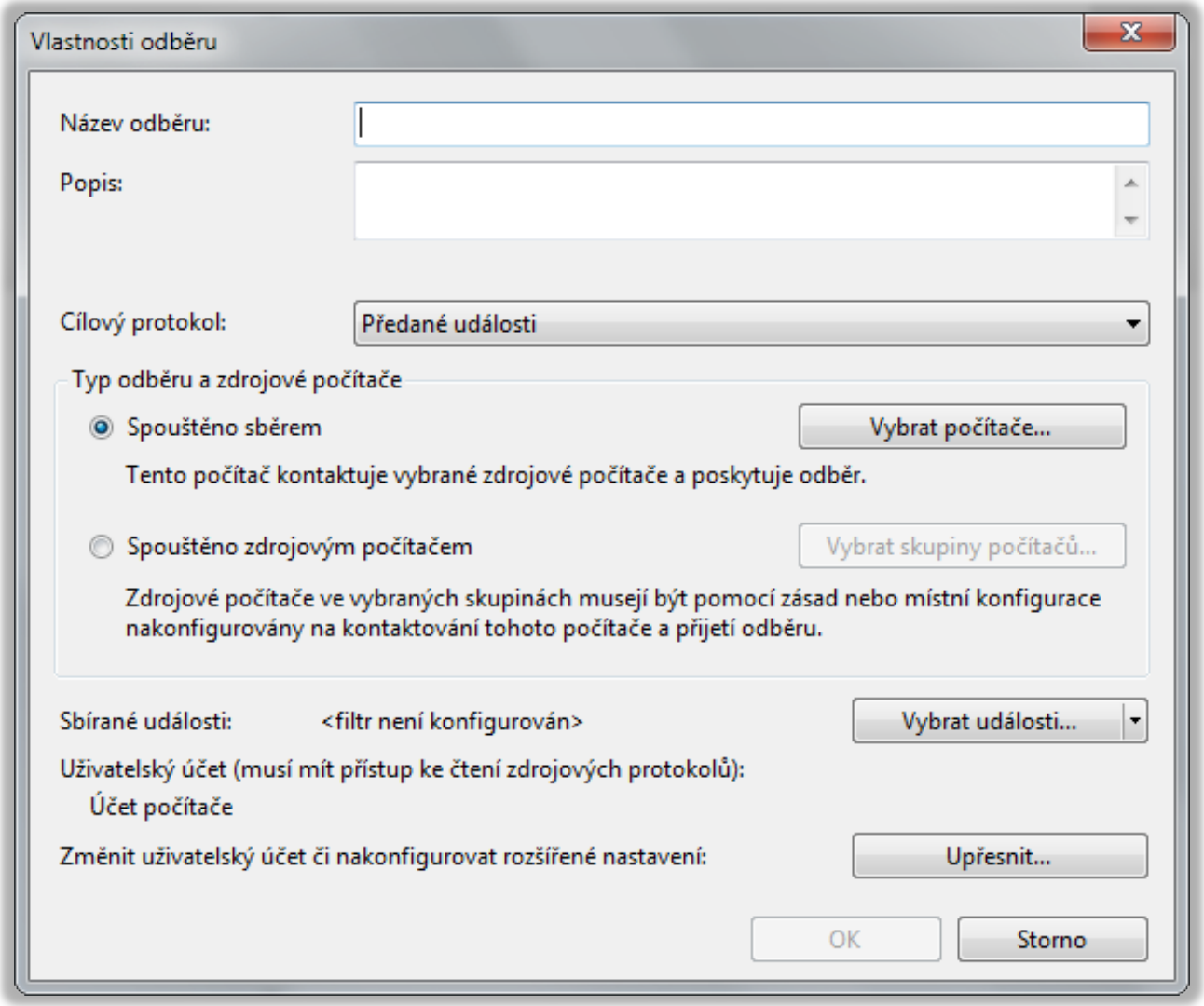
Předávání událostí (Event Forwarding)

- 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

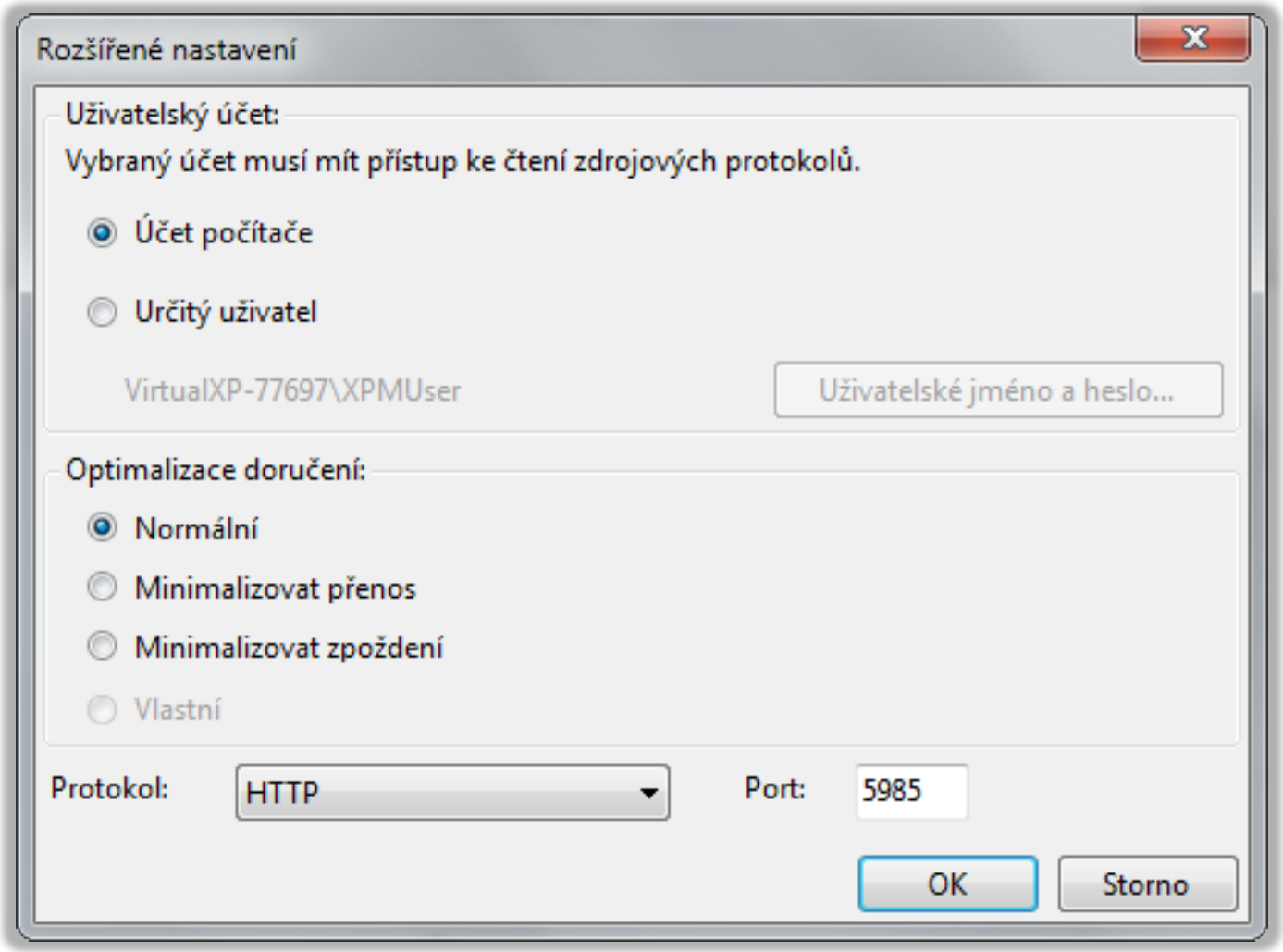
Režimy odběrů (subscription) událostí

- 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

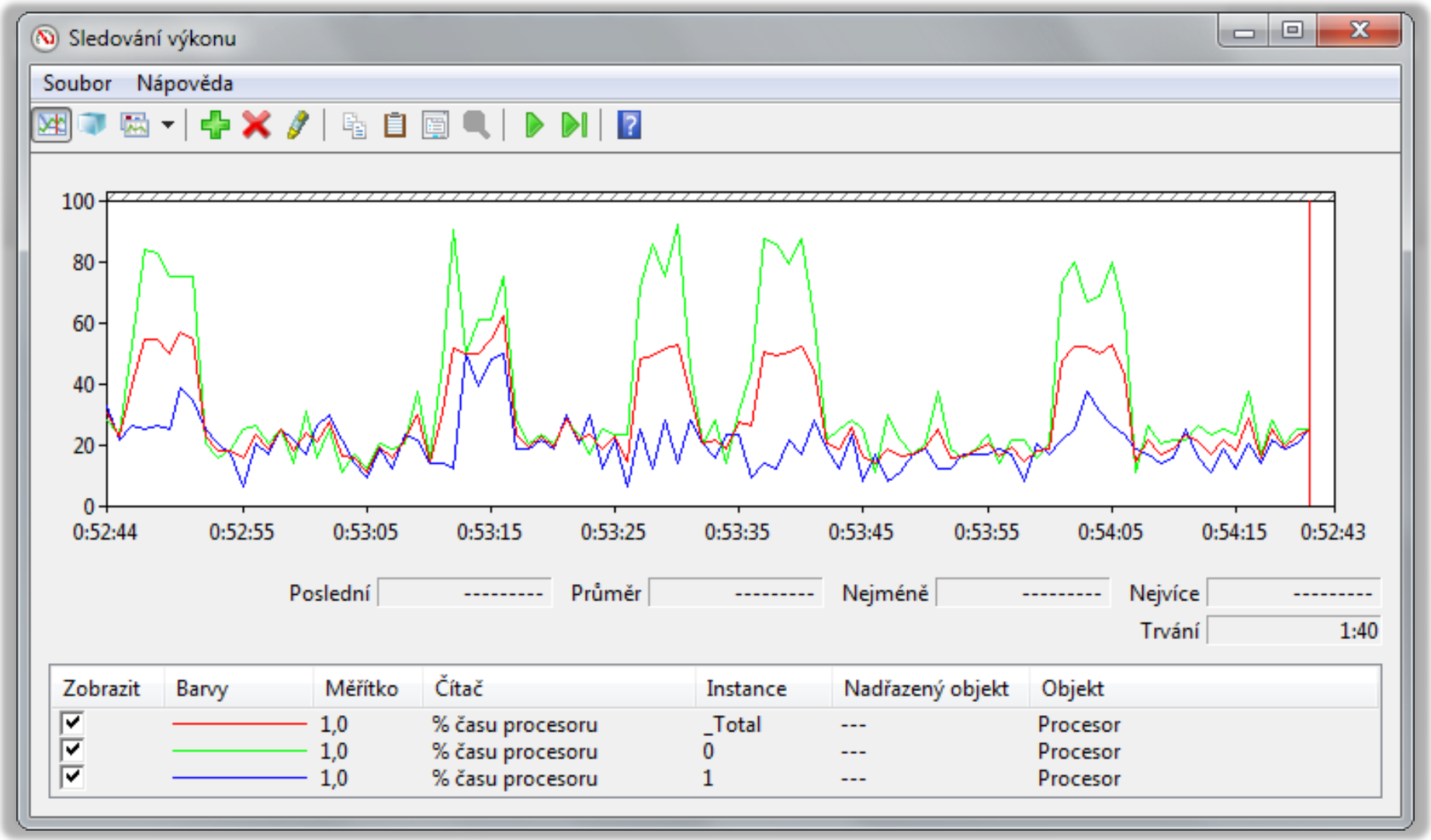
Typy čítačů

- 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 (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

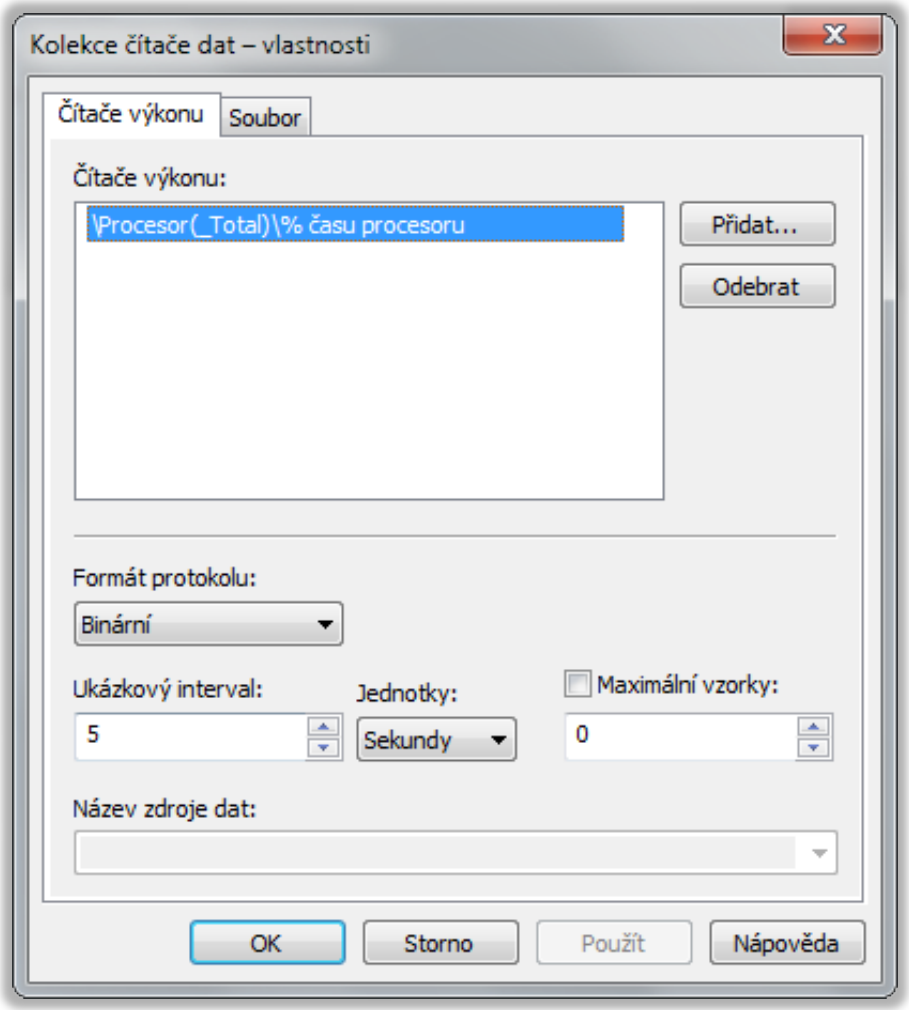
Systémové sady kolekcí dat

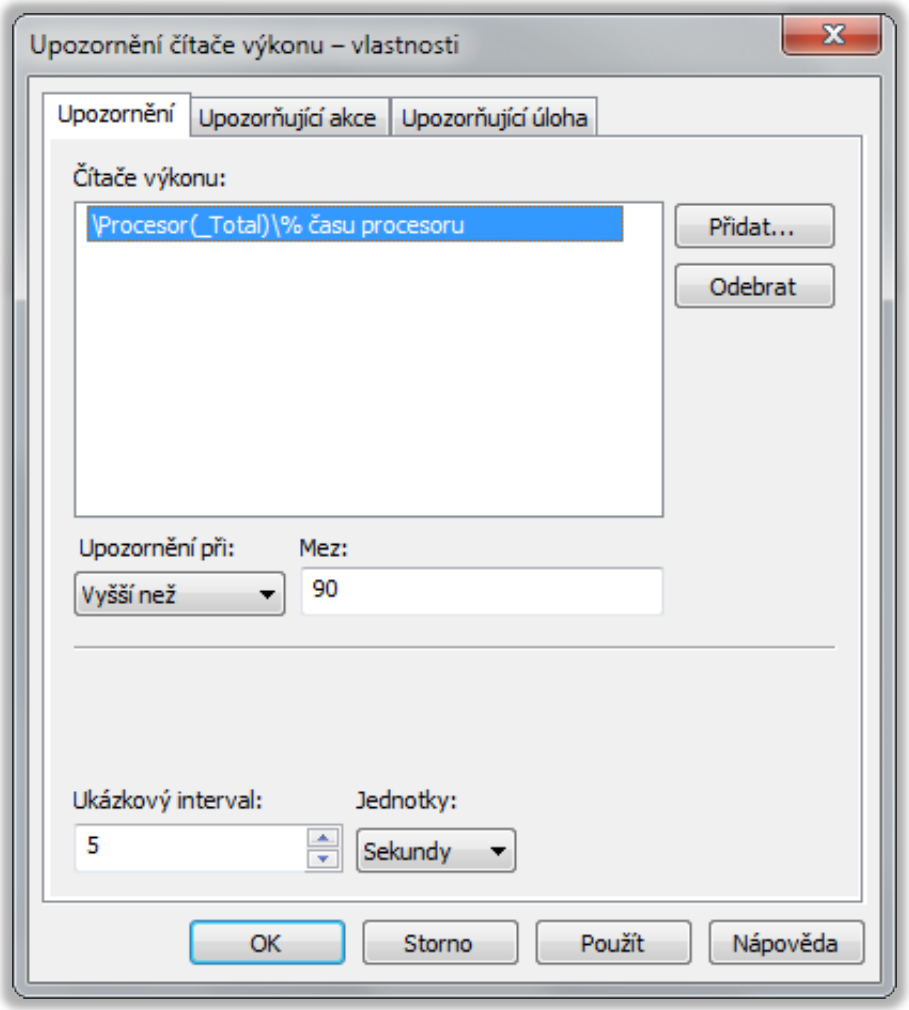
- Výkon systému (*System Performance*)
  - Zaznamenává hodnoty čítačů procesor, fyzický disk, paměť, IPv4, IPv6, …
  - Zaznamenává data trasování jádra
  - Vhodné při náhlém zpomalení počítače
- Diagnostika systému (*System Diagnostics*)
  - Zaznamenává stejné informace jako Výkon systému
  - Zaznamenává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

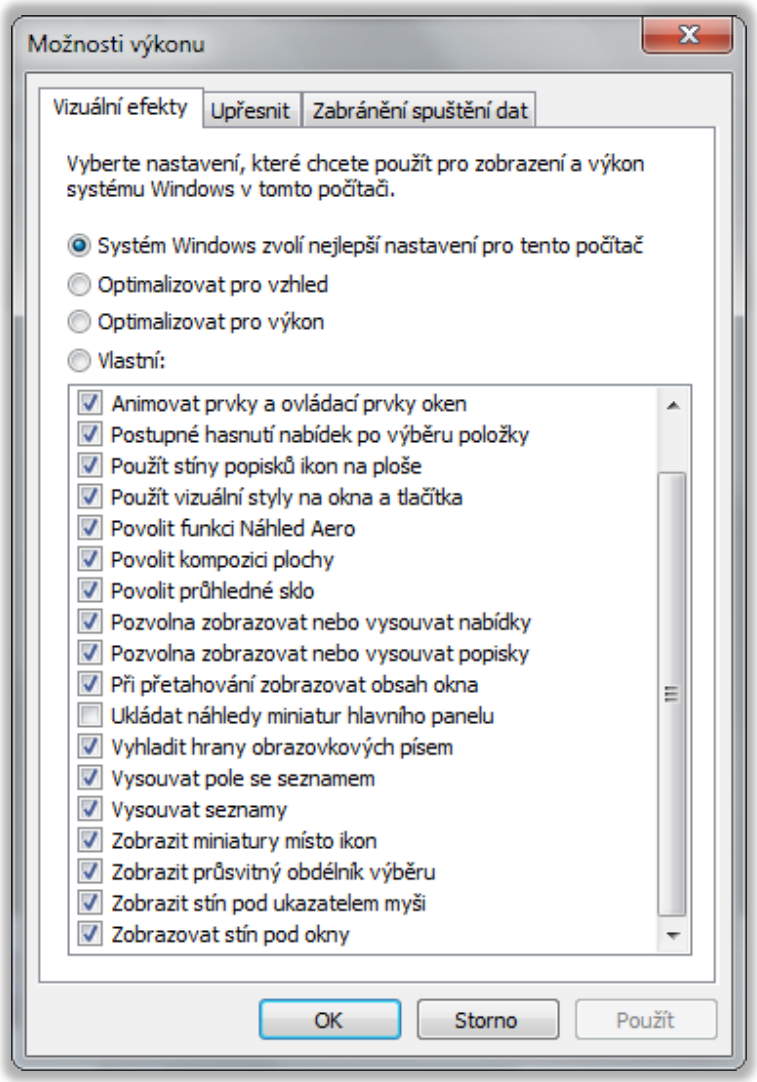
Správa pomocí příkazové řádky (2)

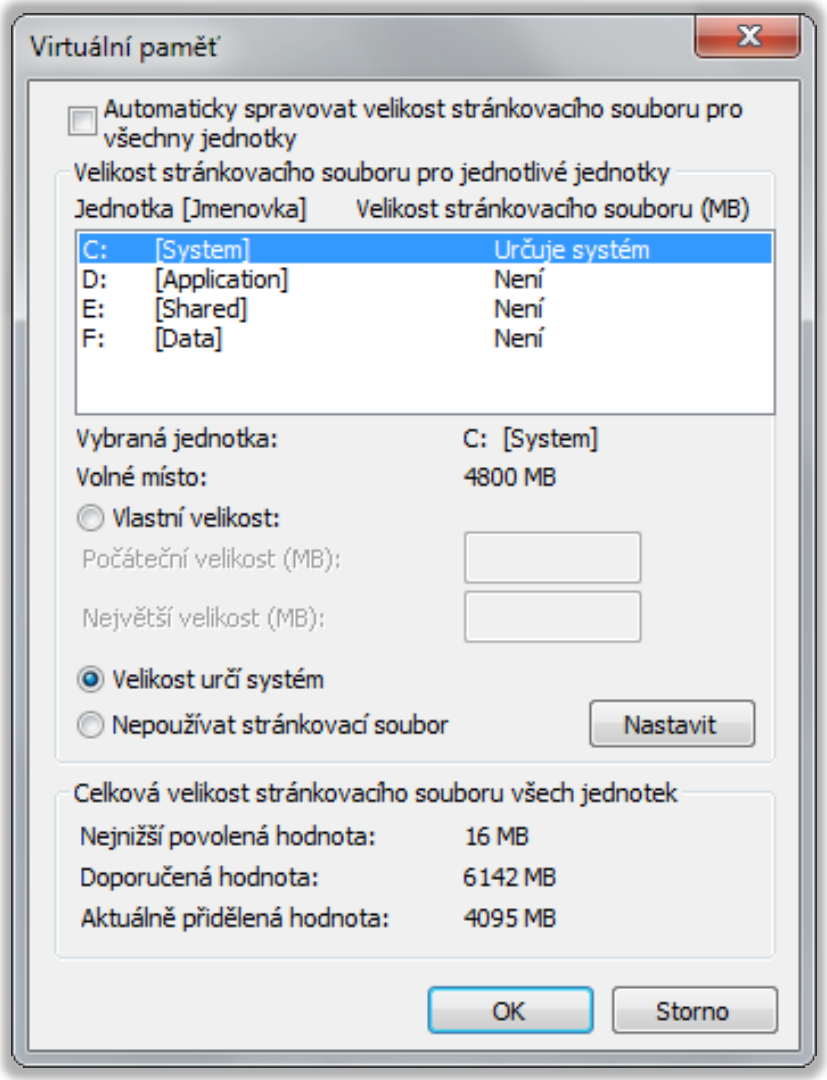
- Import / export (šablon) sad kolekcí dat
  - **logman { import | export } -xml *<soubor-šablony>***
- Informace o kolekcích dat v sadě kolekcí dat
  - **logman query *<sada>***
- Spouštění / zastavování sad kolekcí dat
  - **logman { start | stop } *<sada>***
- Generování sestavy diagnostiky systému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

Možnosti výkonu

- Umožňuje nastavit různé optimalizace ovlivňující výkon systému (a počítače)
- Konfigurace
  - 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





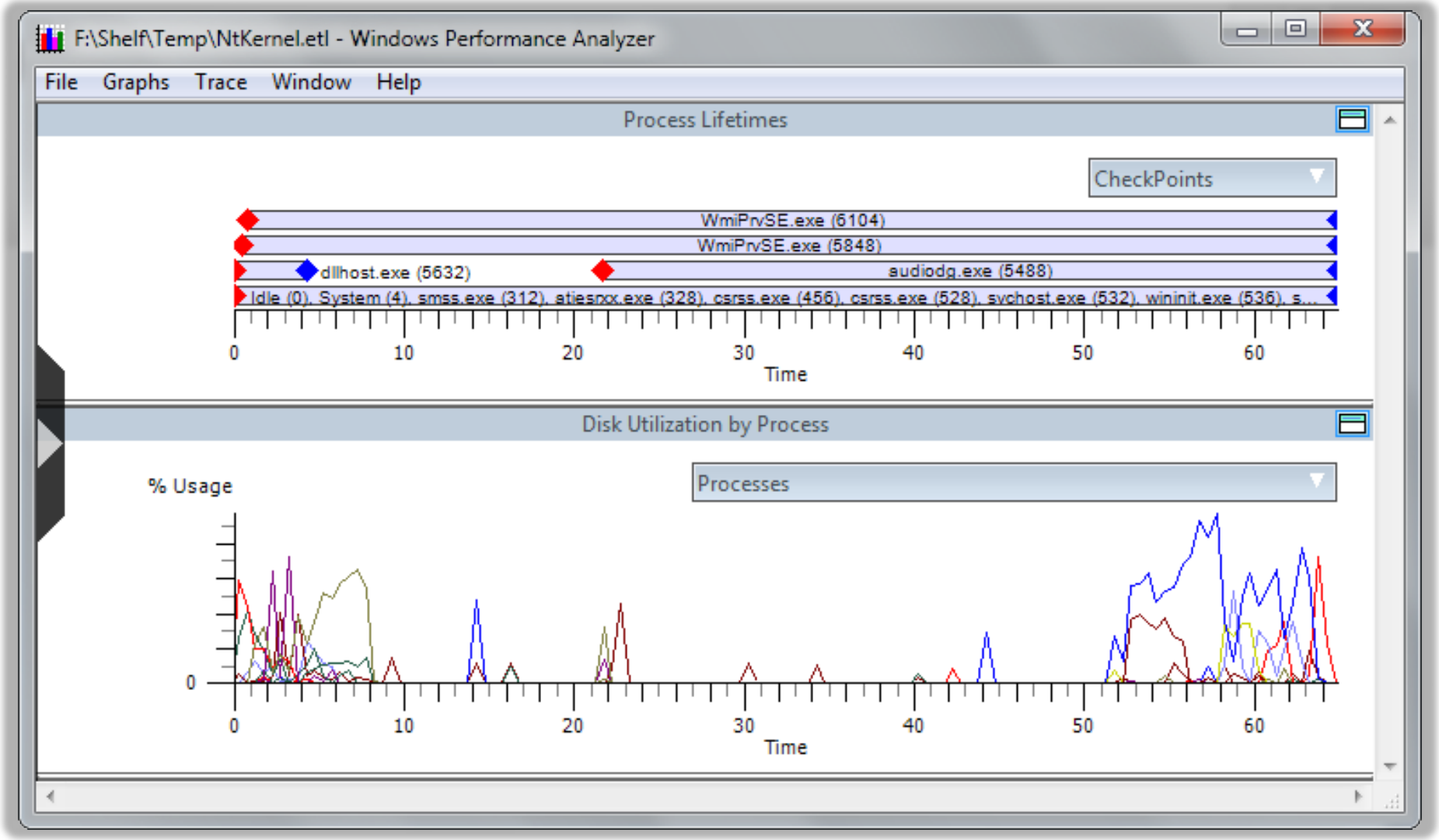
Windows Performance Toolkit (WPT)

- Sada nástrojů pro profilování (měření a analýzu výkonu) systému a aplikací
  - Trasování událostí generovaných systémem (jádrem) nebo jednotlivými aplikacemi
  - Monitorování hodnot čítačů
- Součást Microsoft Windows SDK
- Zachytávaní (a zaznamenávaní) 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 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

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

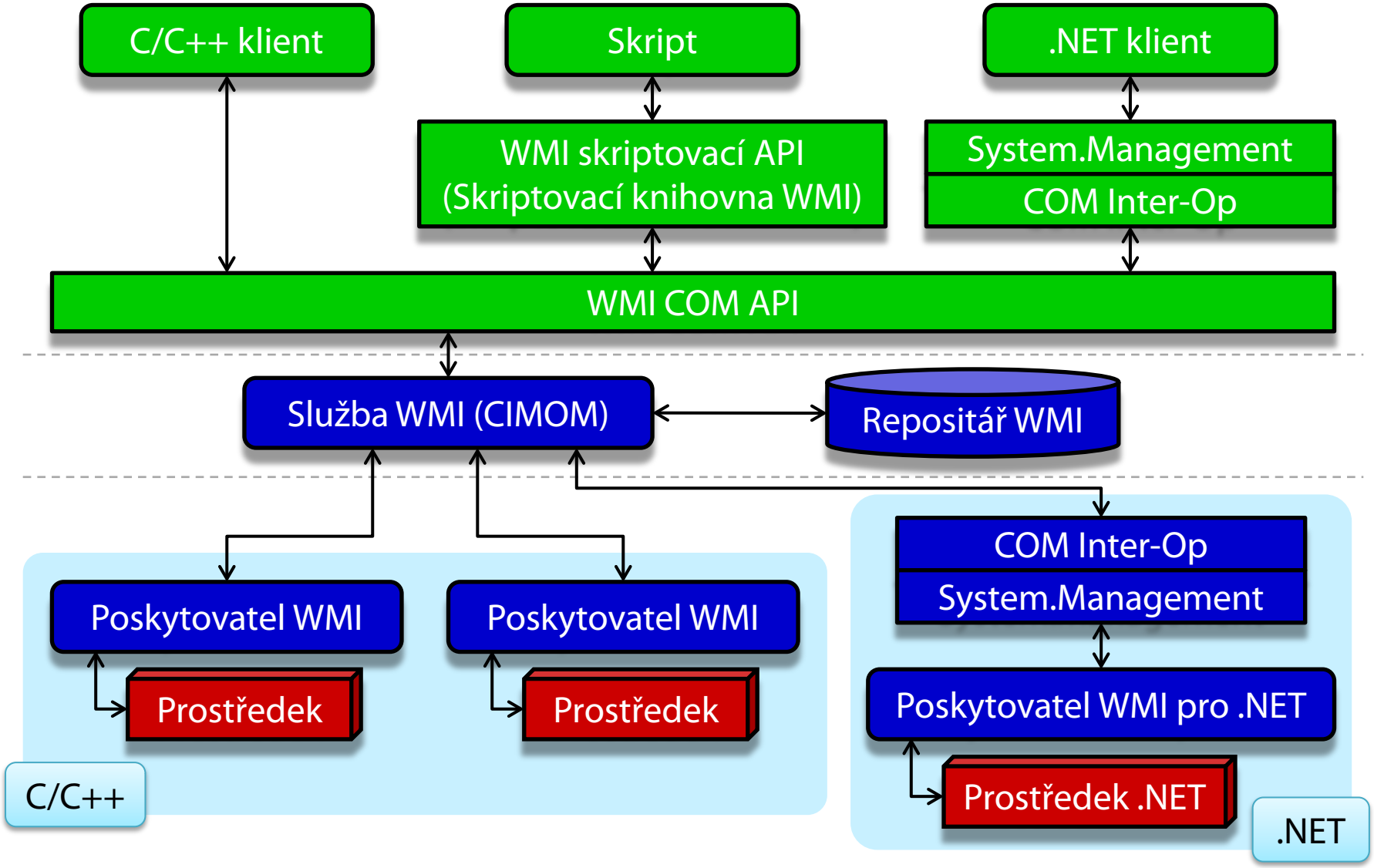
Poskytovatelé WMI (WMI Providers)

- 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

Infrastruktura 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
```

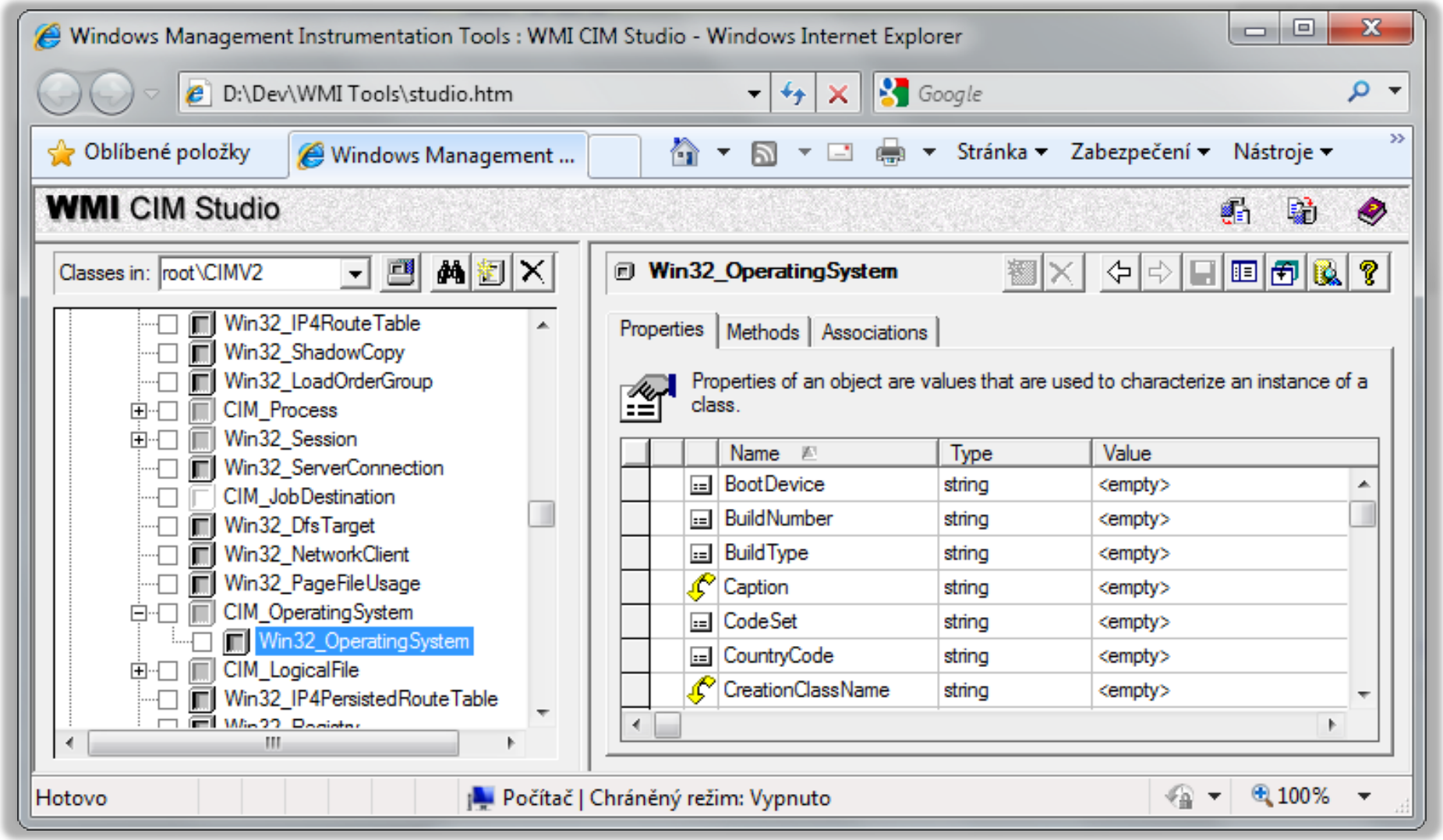
- PowerShell

```
$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



WMI Object Browser