Služby, Registry, Procesy, BCD, Události

Richard Biječek

Microsoft CERTIFIED IT Professional

Služby

- Služba (angl. service) je program běžící na pozadí
- Typicky není interaktivní
- Může být spuštěna OS při bootování, nezávisle na přihlášení uživatele
- V Unix OS je ekvivalentem „daemon“

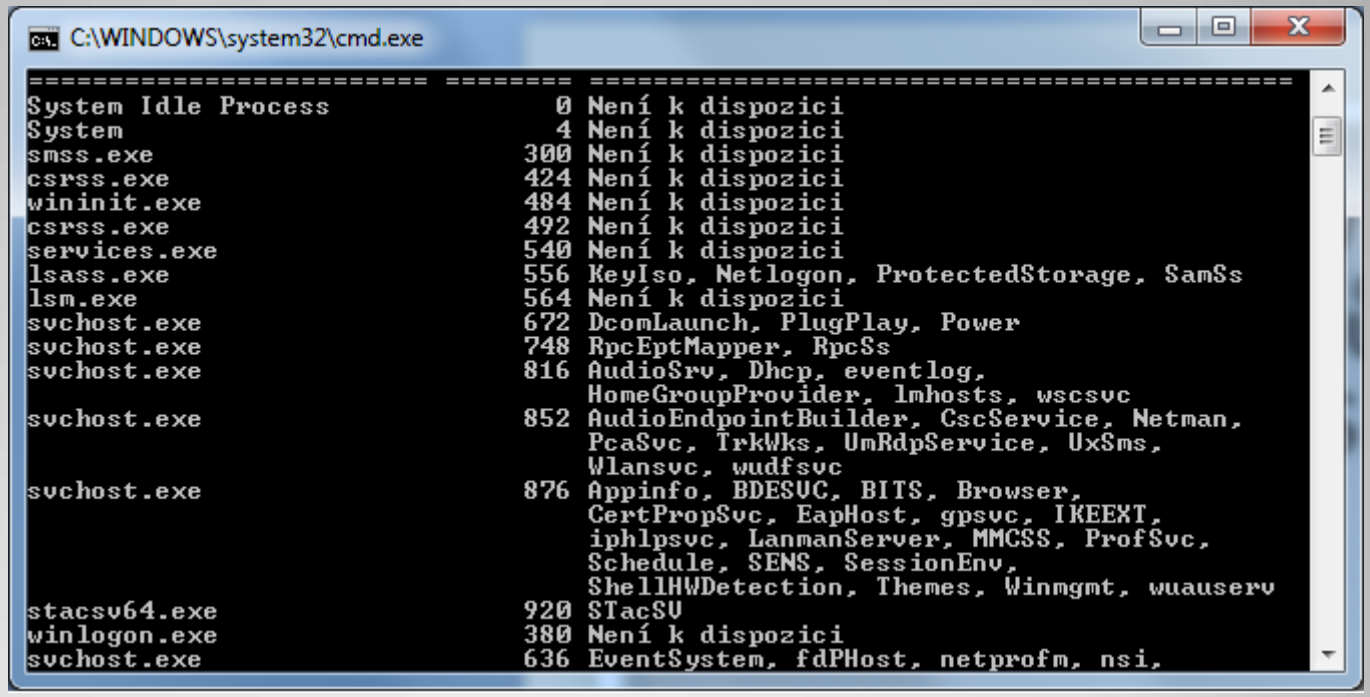
Příklady služeb

- Služby jsou zejména:
  - Serverové role (AD, DNS, IIS, DHCP, …)
  - Komponenty OS (Windows Update, Motivy, Windows Defender, Systémový čas …)
  - Klienti síťové komunikace (DHCP klient, DNS klient…)
  - Obsluha HW (Plug and Play, …)
  - Serverové aplikace (SQL server, Apache …)
  - Další SW 3. stran (např. Update Antiviru)

Služby

- Zejména každá serverová aplikace by měla být nainstalována jako služba
- Běh poté není závislý na přihlášeném uživateli
- „Aplikace“ nemůže běžet bez přihlášení uživatele
- Pozor na některé starší SW „aplikace“ třetích stran

- Každá služba v OS má svůj host proces
- Host proces může být sdílen, typicky u komponent OS



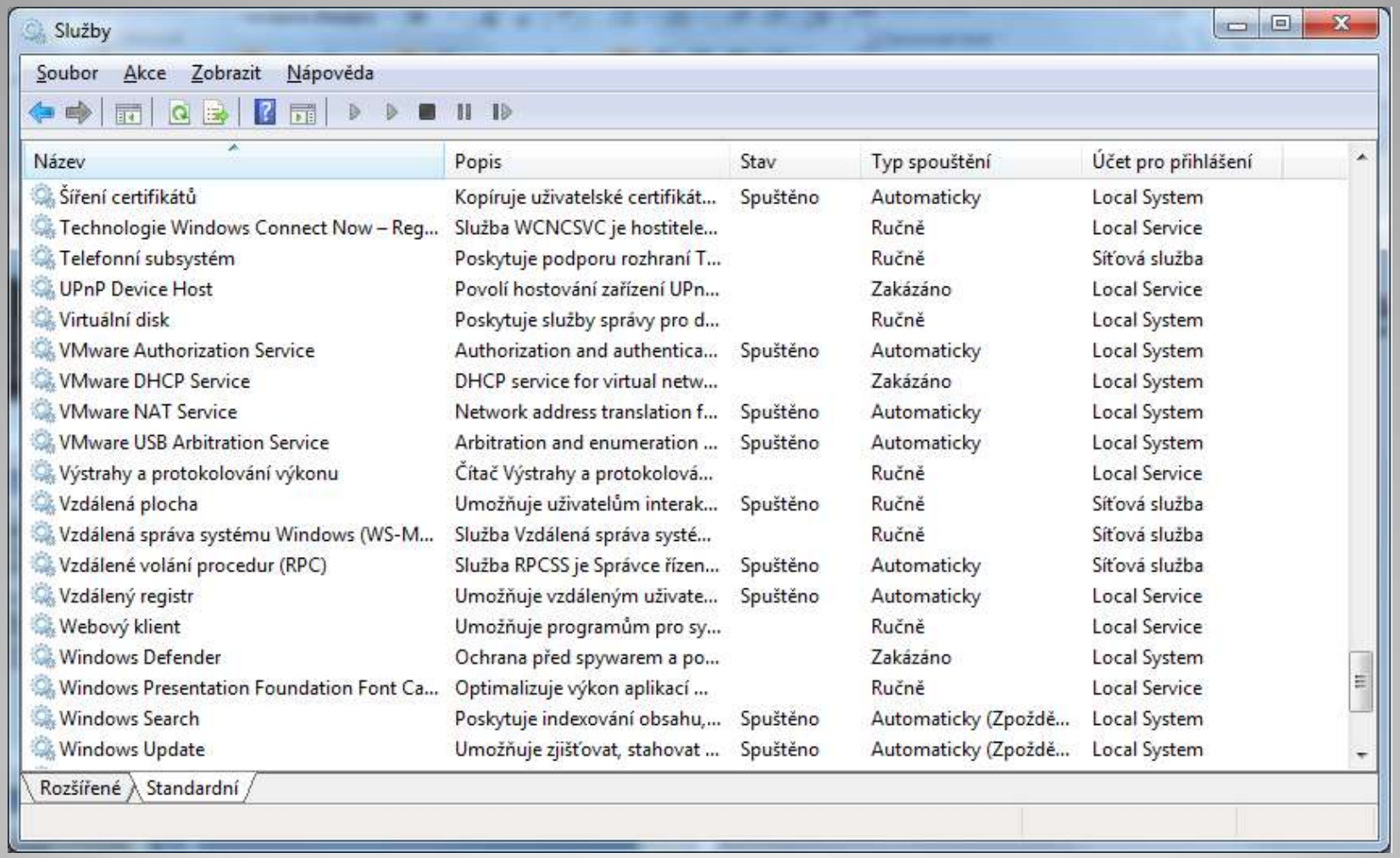
Vlastnosti služeb

Spouštění služeb

- Každá služba má Typ spouštění:
  - Automaticky - je spouštěna při bootu OS
  - Ručně - není spouštěna OS, může být spuštěna správcem, aplikací
  - Zakázáno - Službu nelze spustit
  - Automaticky (Zpožděné spuštění) – Nový typ od Vista / 2008 – Totéž co „Automaticky“ ale s prodlevou oproti ostatním; Použito pro doplňkové komponenty jako Windows Update

Identifikace služeb

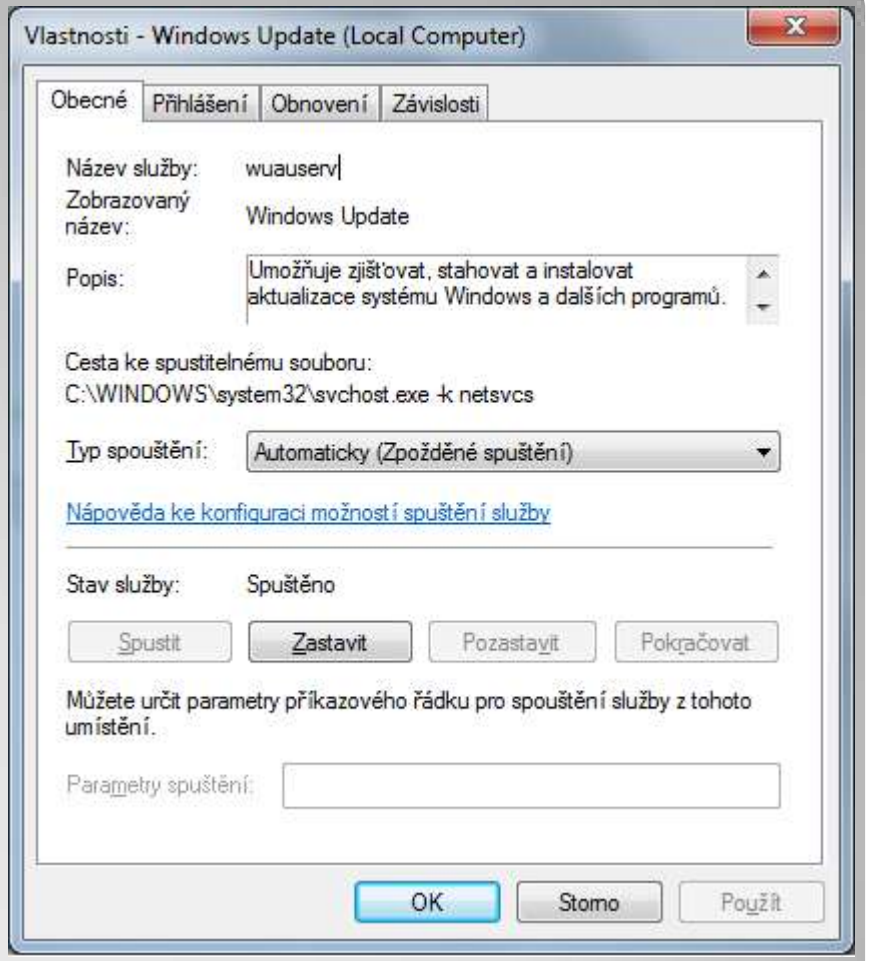
- Služba je identifikována názvem
- Existuje tzv. „dlouhý název“
  - **Display Name**
- A „krátký název“
  - **Service Name**
- Dlouhý název je lokalizován (český, anglický, finský) zatímco krátký název je vždy stejný.
- Názvy mohou být značně odlišné!



Konfigurace služeb - GUI

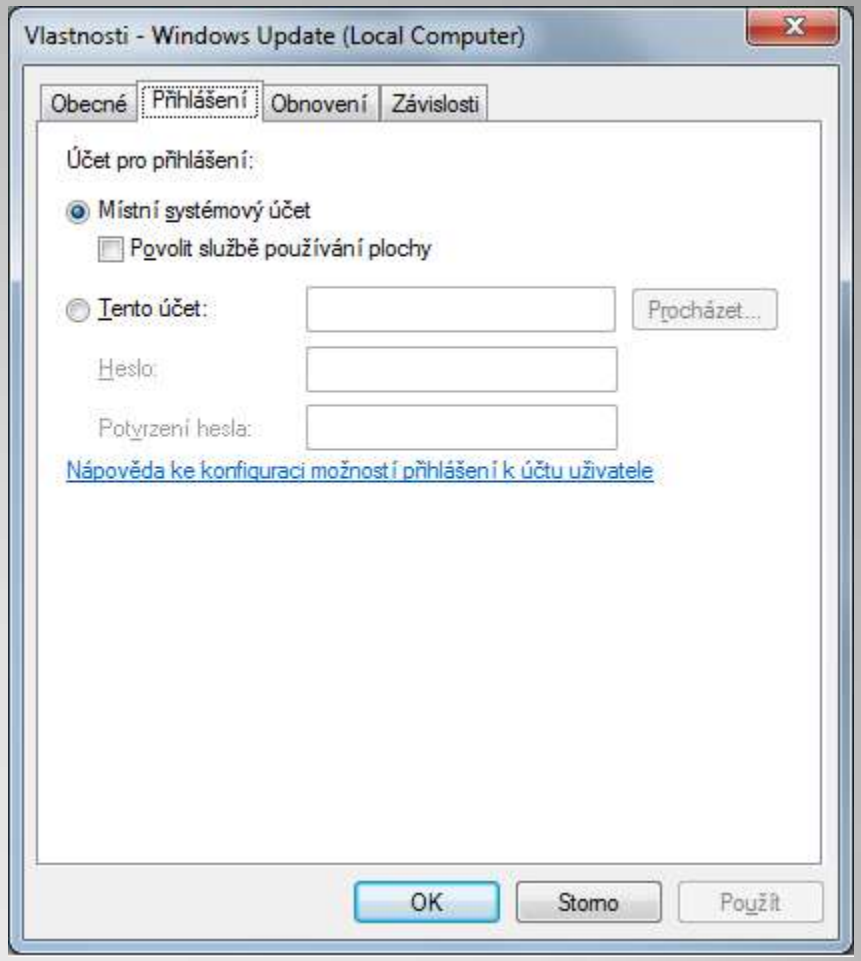
Vlastnosti služby

- Vlastnosti v GUI
  - Obecné ➔
  - Přihlášení
  - Obnovení
  - Závislosti



Vlastnosti služby

- Přihlášení
- =Účet pod kterým služba běží
  - Účet „Systém“
  - Libovolný uživatel
- Přidělujeme pouze nutná práva
- U systémových služeb NEMĚNIT



Vlastnosti služby

- Je možno definovat činnosti při selhání
- Restart služby (která selhala)
- Restart OS
- Jiné činnosti (spuštění skriptu, příkazu)

- Také je možno definovat závislosti
- Definují seznam služeb, které musí běžet aby se mohla spustit jiná služba

Stav služby

- Možné stavy služby
  - Zastavena (stopped) … Lze spustit
  - Spuštěna (Started) … Lze zastavit / pozastavit
  - Spouštění (Starting) … Nelze ovládat
  - Zastavování (Stopping) … Nelze ovládat
  - Pozastavena (Paused)
    - Jen pro vybrané služby

Ovládání služeb - CMD

- Užitečné příkazy:
- NET START <název>
- NET STOP <název>

- Komplexní příkaz SC
- SC <příkaz> <název>

- SC Start <název>
- SC Stop <název>
- SC GetDisplayName <název>
- SC GetKeyName <název>
- SC QC <název>

- SC SdShow <název>
- SC SdSet <název>

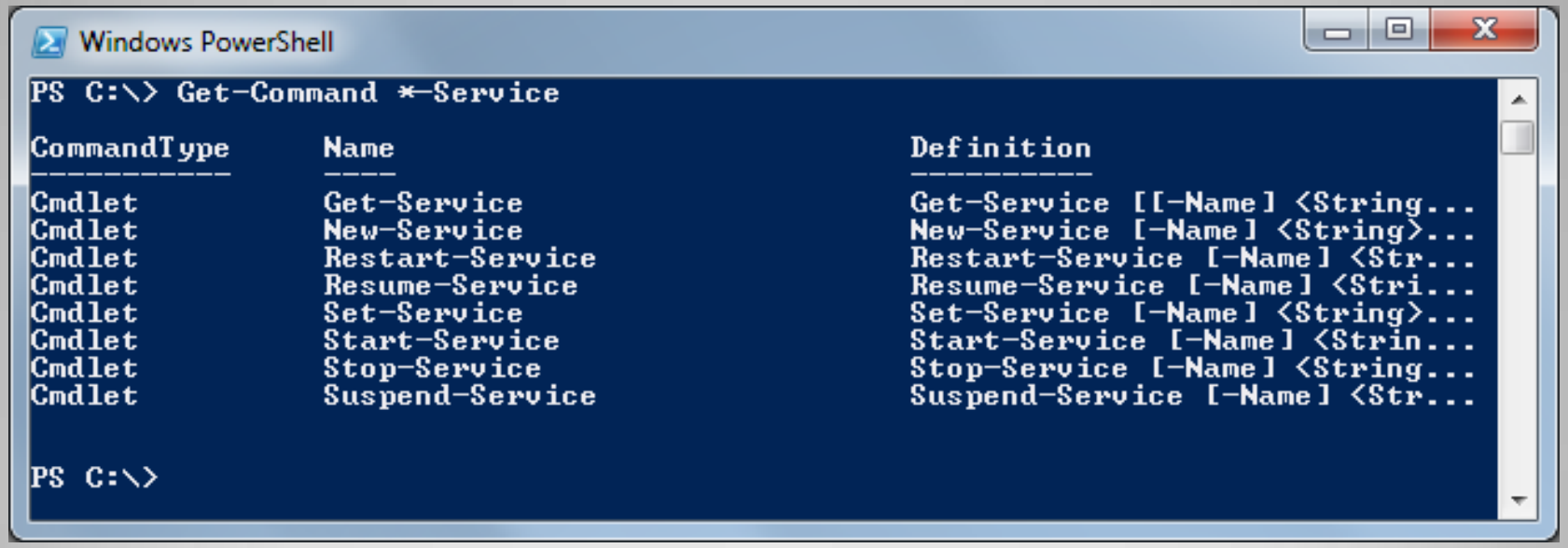
Ovládání služeb - CMD

- Každá služba má definován ACL
- Windows neobsahují GUI pro tento ACL
- Lze vypsat / nastavit jen pomocí SC
- Používá syntaxi SDDL
  - (Security Descriptor Definition Language)

Zabezpečení služeb

Ovládání služeb - PowerShell

- PowerShell – objekt Service
- Omezené použití
  - Nelze: Oprávnění, Zjistit typ spouštění



Windows Registry

- Co jsou registry?
- Teoreticky:
- Hierarchická databáze obsahující nastavení pro Windows OS a aplikace
- Prakticky:
- Místo, kde nalezneme nastavení systému a aplikací, která nejsou jinak dostupná

Dělení registru

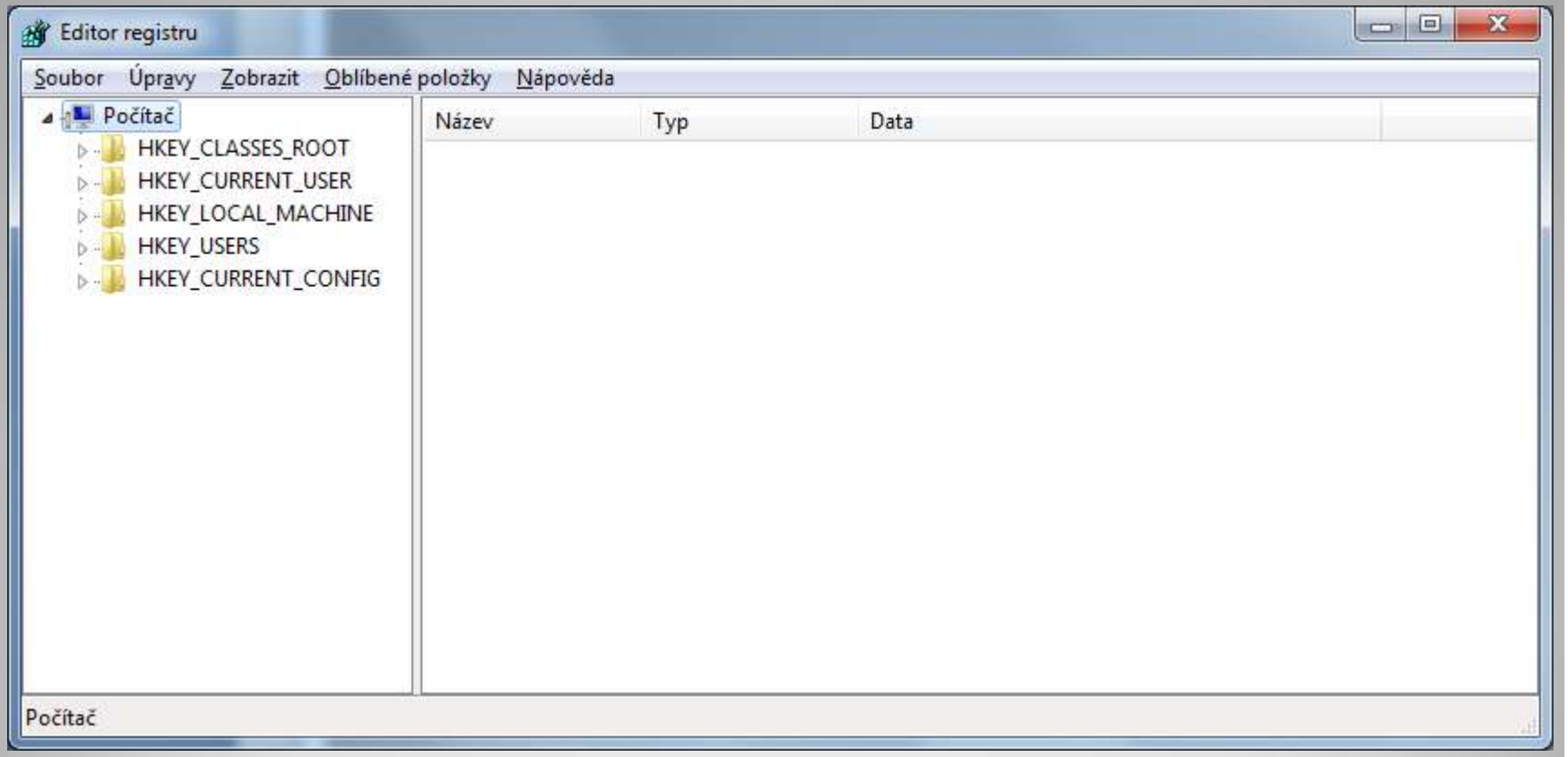
- HKEY_LOCAL_MACHINE (HKLM)
  - Obsahuje nastavení počítače
- HKEY_USERS (HKU)
  - Obsahuje podklíče nastavení uživatelů
- HKEY_CURRENT_USER (HKCU)
  - Obsahuje nastavení aktuálního uživatele
- HKEY_CURRENT_CONFIG (HKCC)
  - Podklíč HKLM, nastavení HW profilu
- HKEY_CLASSES_ROOT (HKCR)
  - Podklíč HKLM, registrace aplikačních komp.

- V registrech pracujeme se dvěma základními typy objektů:
- Klíč (registry key)
  - Ekvivalent složky / adresáře
  - Rozděluje nastavení do přehledná hierarchie
- Hodnota (registry value)
  - Obsahuje data (vlastní nastavení)

Registry – datové typy

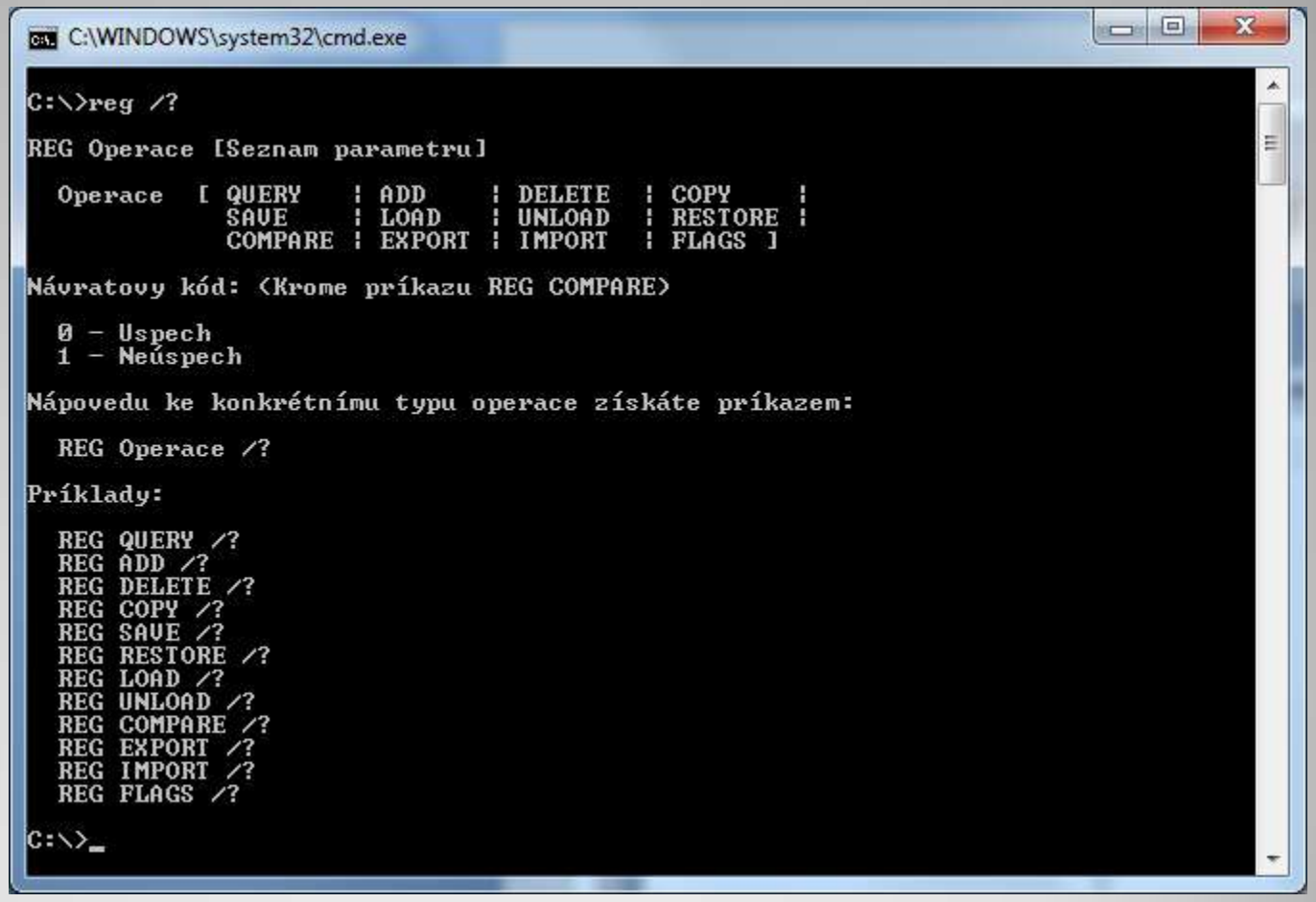
- Registry mají binární strukturu
- Každá hodnota má definován datový typ
- Nejčastěji používané:
- REG_SZ (řetězec UTF-16)
- REG_MULTI_SZ (pole řetězců UTF-16)
- REG_DWORD (číselná hodnota 32bit)
- REG_QWORD (číselná hodnota 64bit)
- REG_BINARY (libovolná data)

- REGEDIT – Editor Registru



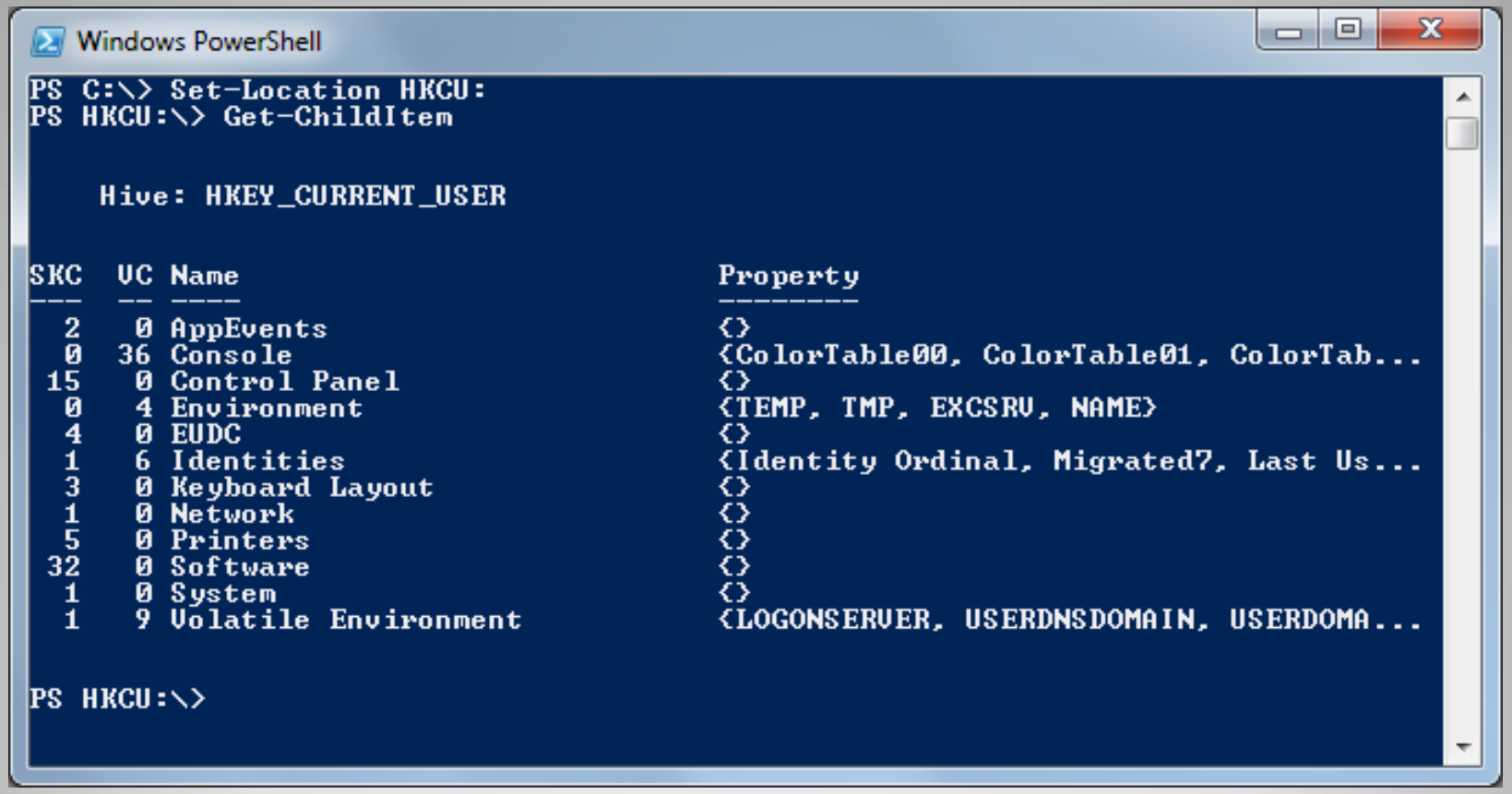
Práce s registry

- Příkaz REG



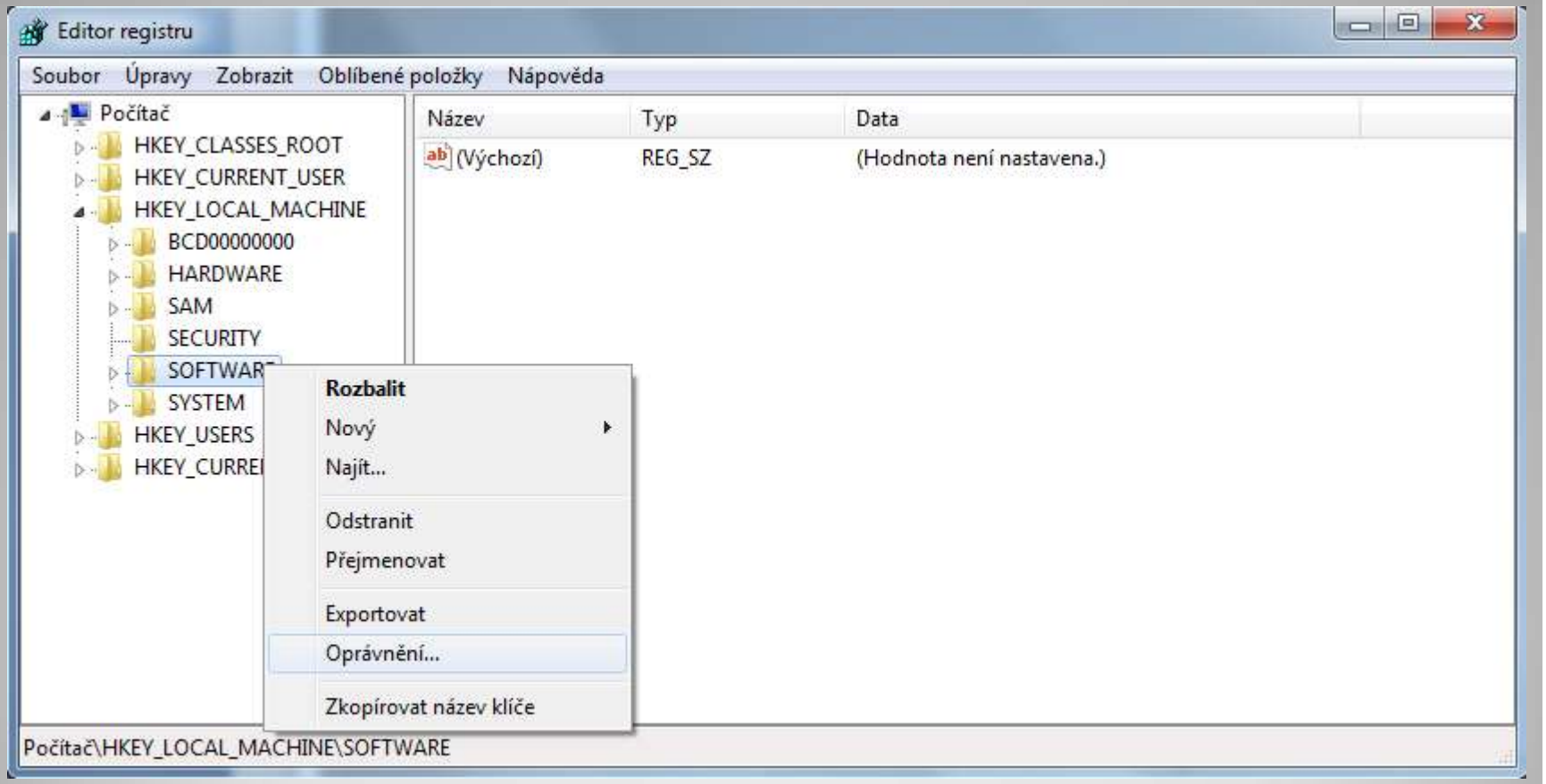
Práce s registry - CMD

- PowerShell provider pro registry



Práce s registry - PowerShell

- Každý klíč registru má ACL



Oprávnění v registrech

Registry - vybrané nastavení

- HKLM\System\CurrentControlSet\Services
  - Nastavení ovladačů a služeb
- HKLM\Software
  - Kořenová lokace nastavení aplikací (machine)
- HKCU\Software
  - Kořenová lokace nastavení aplikací (user)
- HKU\.DEFAULT\ControlPanel\Keyboard
  - Nastavení „NUM Lock“ pro přihlašovací dialog

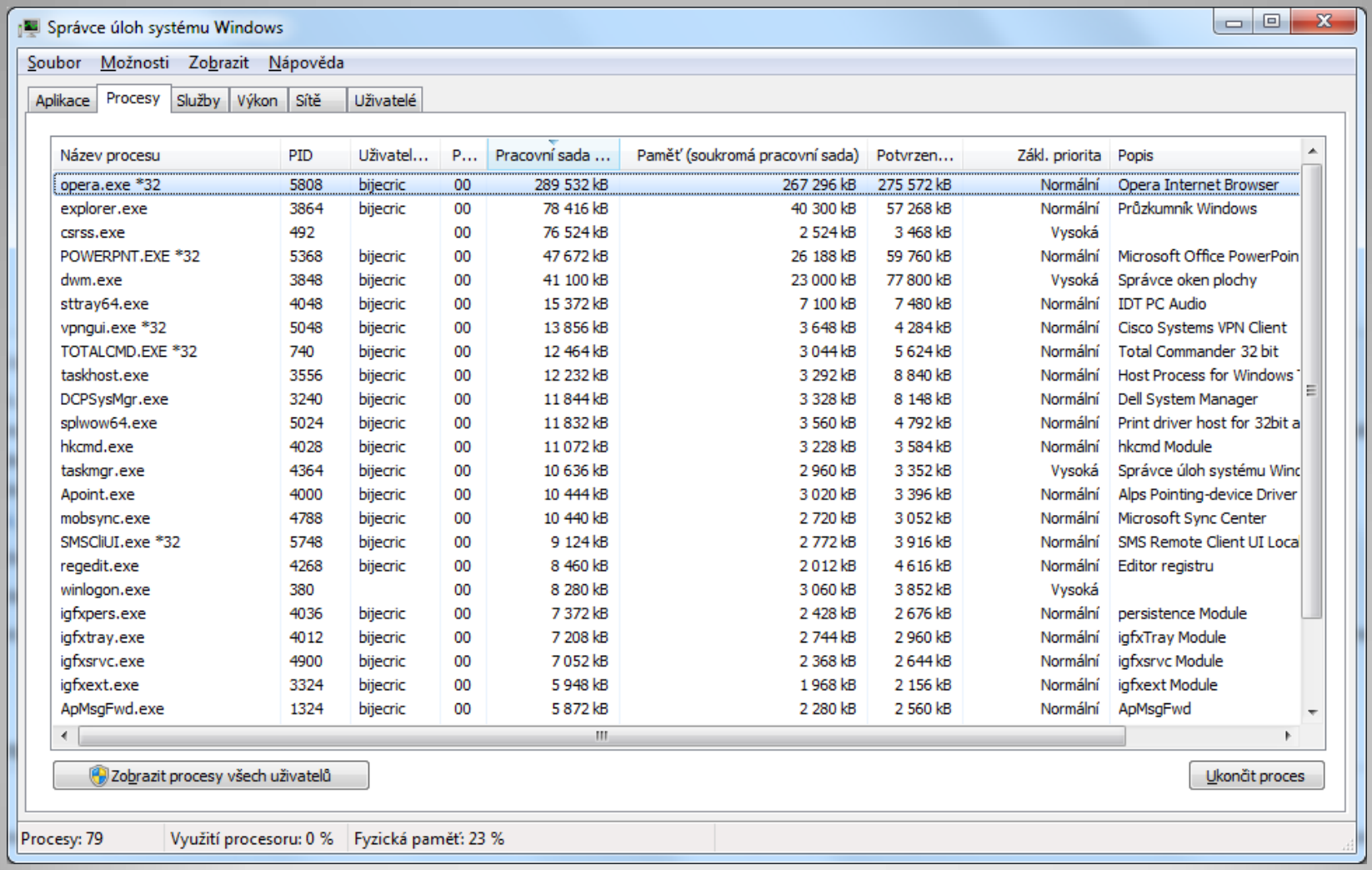
Registry - vybrané nastavení

- HKLM\Software\Policies
  - Nastavení aplikované z GPO (adm. templates)
- HKCU\Software\Policies
  - Nastavení aplikované z GPO (adm. templates)
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  - Aplikace pro spuštění po přihlášní uživatele
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - Aplikace pro spuštění po přihlášní uživatele

Procesy ve Windows

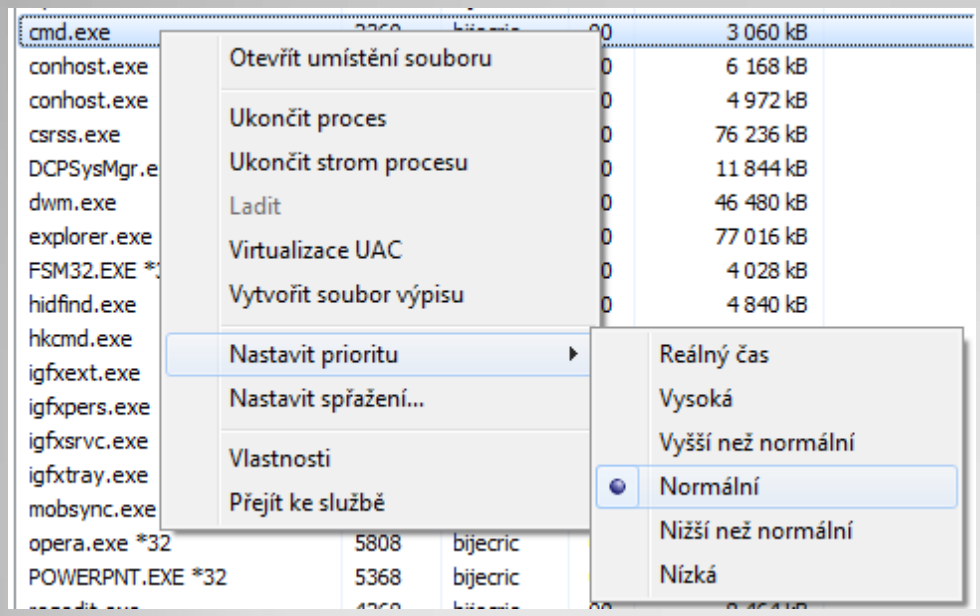
- Každá běžící aplikace v sytému (a také služba / služby) jsou reprezentovány procesem
- Proces obecně reprezentuje programový kód, jeho aktivitu, stav a alokovanou paměť

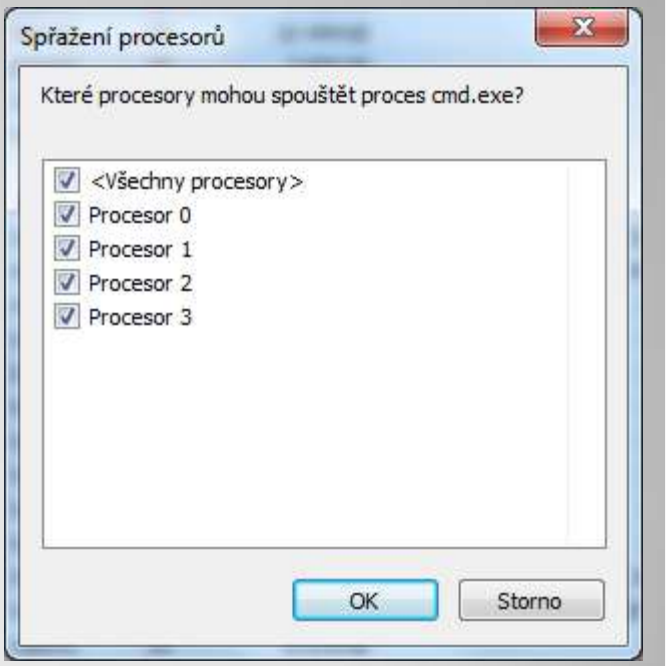
- Technická poznámka:
  Procesy neběží, vlákna ano ☺



Správa procesů

- Možnosti nastavení činnosti procesů
- Priorita = přístup k CPU
- Spřažení = vazba na konkrétní jádro CPU





Správa procesů

Správa procesů

- Kromě Správce úloh (Task Manager) také:
- Příkazy TASKLIST / TASKKILL
- PowerShell cmd-lets *-Process

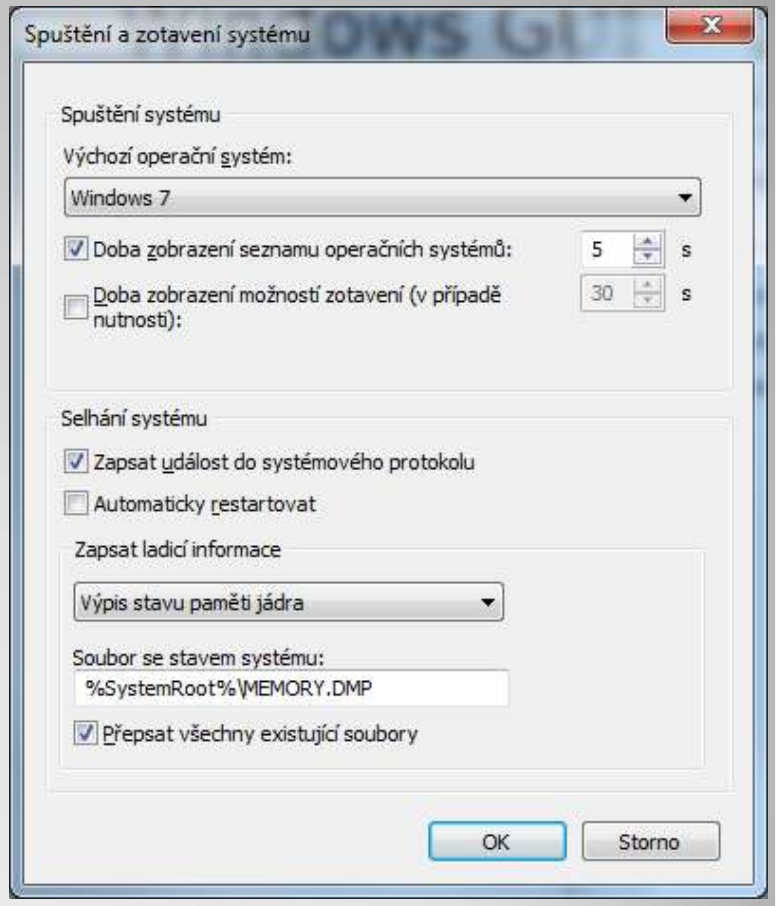
Spuštění systému, BCD

- Boot sektor disku předá řízení →
- Windows Boot Manager (BOOTMGR)
  - Zjistí aktivní oddíl
  - načte Boot Configuration Data (BCD)
- BCD je firmware-nezávislá databáze
  - Uložena na EFI oddílu
  - Nebo v \boot\bcd souboru systémového oddílu

BCD

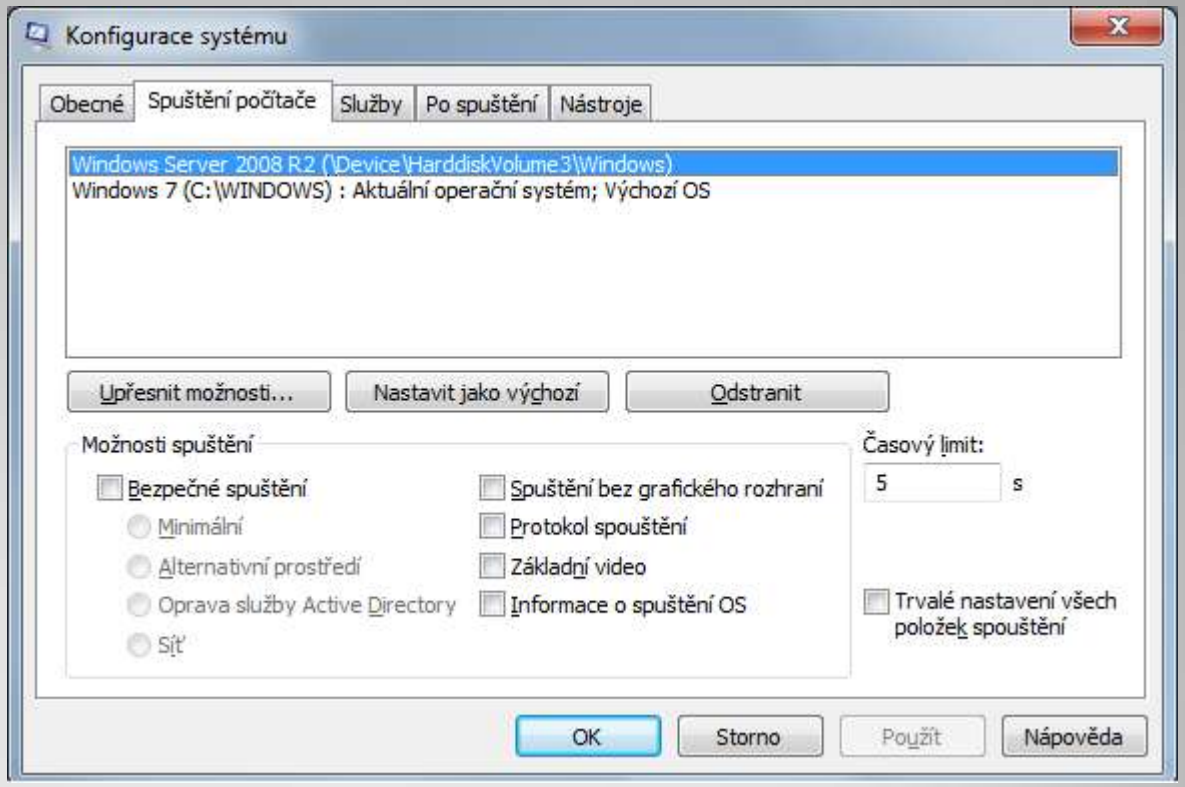
- BCD může obsahovat záznamy
  - Pro načtení NT6.x systémů
  - Načtení NT5.x systémů (NTLDR)
  - Odkaz na partition boot record
    - Slouží ke spuštění ostatních systémů

- Windows GUI – základní konfigurace
- „Spuštění Systému“ ➔



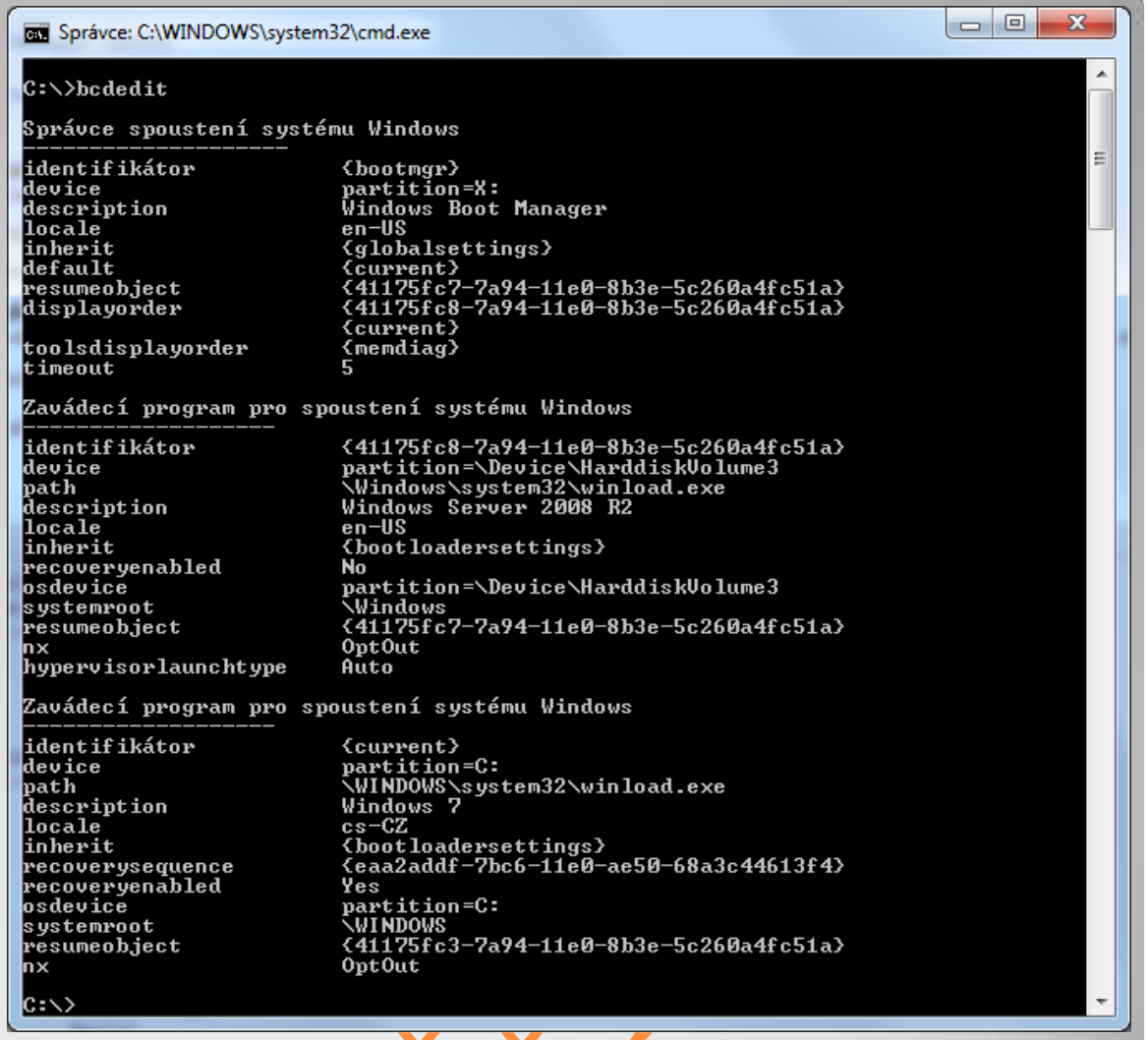
Konfigurace spouštění OS

- msconfig.exe



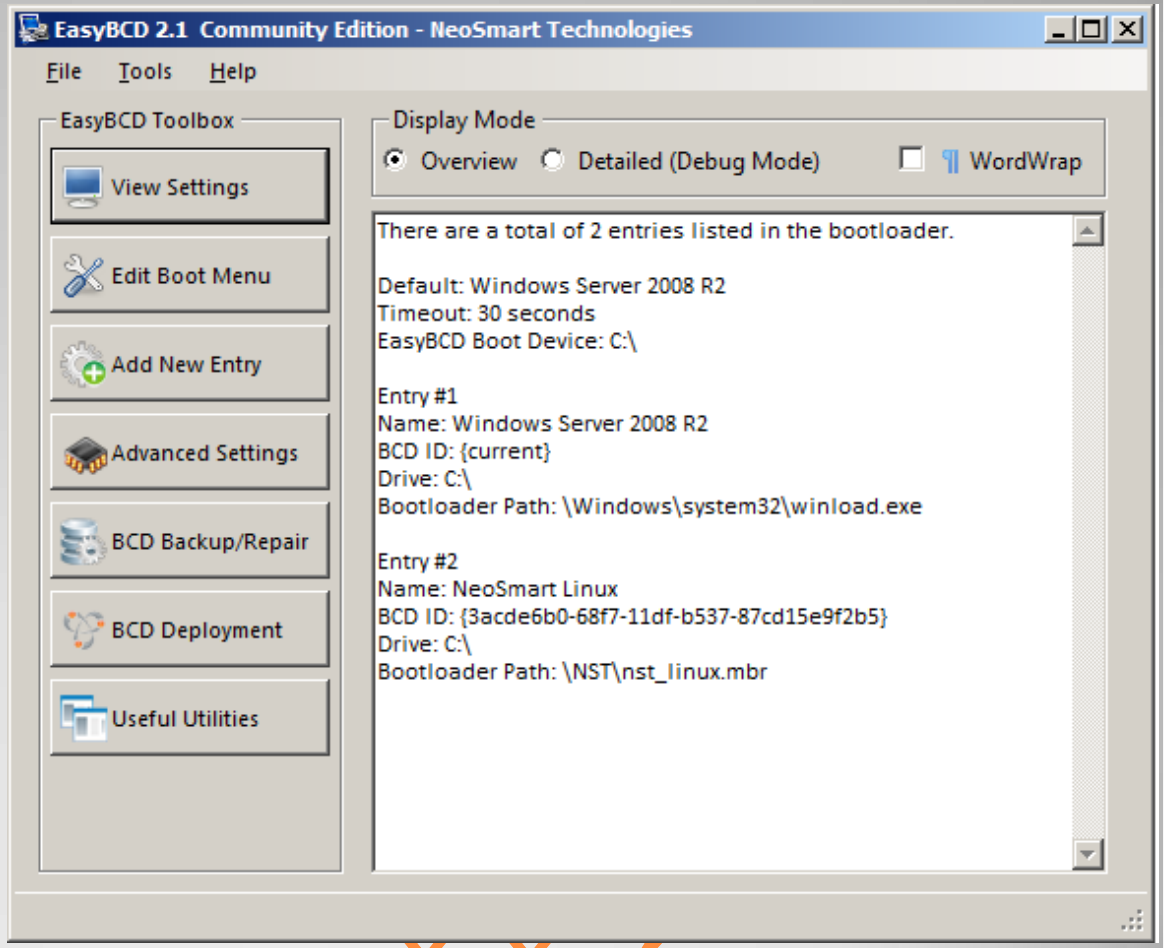
Konfigurace spouštění OS

- bcdedit.exe
- Úplná správa BCD databáze



Konfigurace spouštění OS

- Nástroje třetích stran
- „Grafický BCDedit“
- Například ➔
- EasyBCD



Konfigurace spouštění OS

Události, Prohlížeč událostí

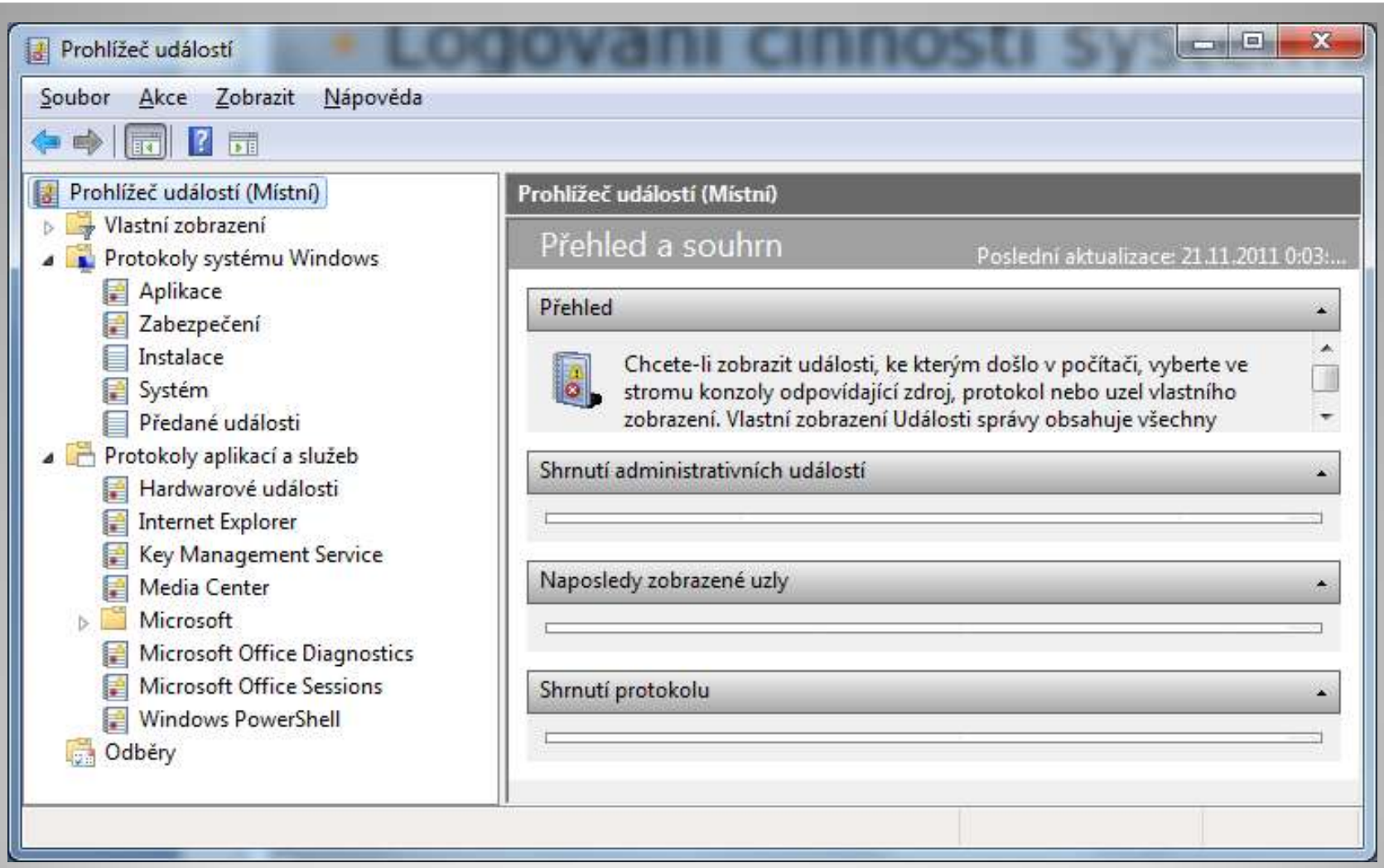
- Logování činností systému a aplikací
- Jednotný formát souborů (*.EVTX)
- Prohlížení přes konzolu
  - „Prohlížeč událostí“ / „Event Viewer“

Logy

- Základní systémové:
  - Application, System, Security
- Aplikační (pro některé služby)
  - DNS Server, Active Directory, DFS Replication
- Ostatní logy
  - Detailní logy jednotlivých činností / aplikací / služeb

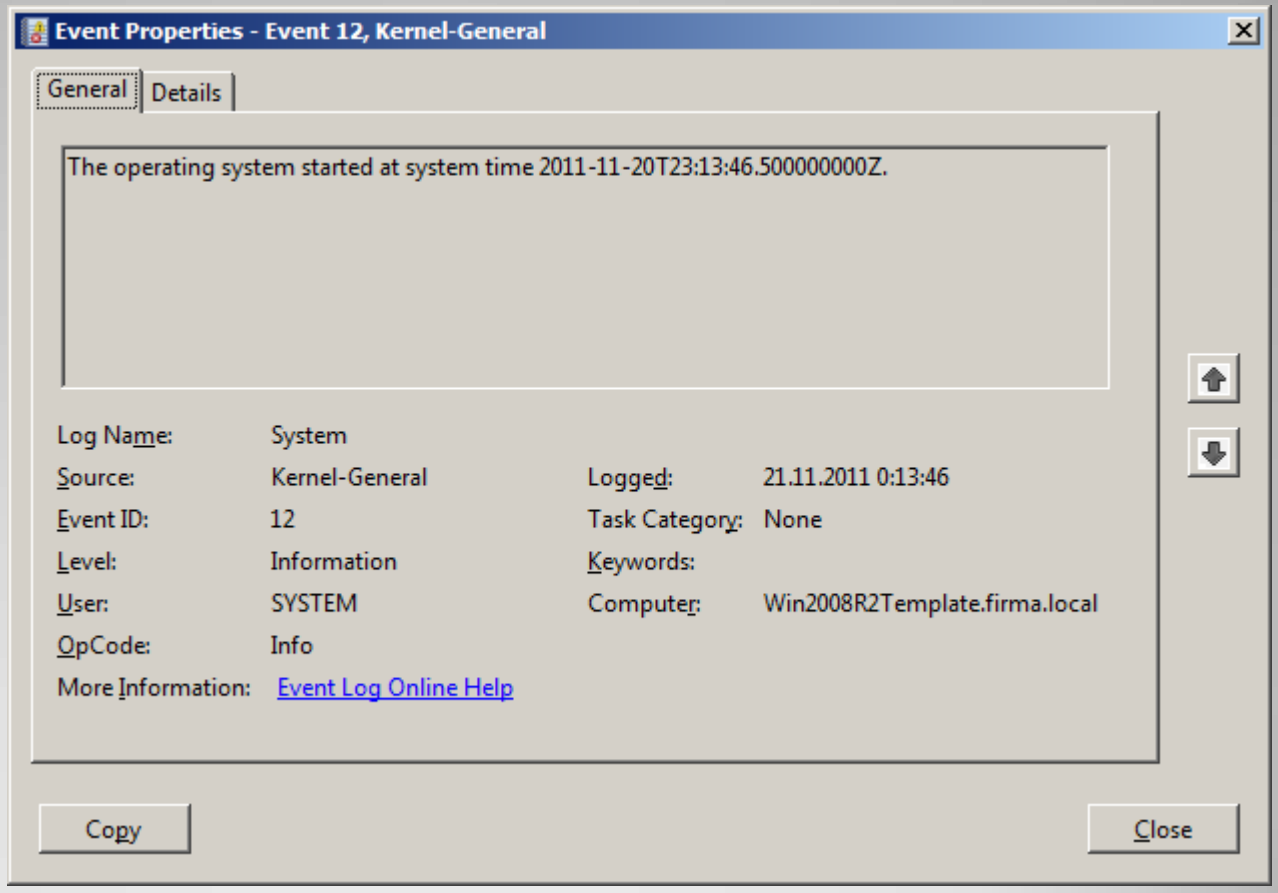
Události

- Záznam v logu = Událost
- Každá událost má:
  - Zdroj
  - ID (Dohromady se Zdrojem jendoznačné)
  - Datum a čas
  - Počítač
  - Úroveň (Informace, Varování, Chyba)



Prohlížeč událostí

- Příklad události



Událost

- Další činnosti
  - Filtrování
  - Exportování
  - Nastavení vlastnostú logování
- Viz praktické ukázky

Práce s prohlížečem událostí