

Služby, Registry, Procesy, BCD, Události

Richard Biječek

Microsoft
CERTIFIED
IT Professional

- 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“

Služby

- 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)

Příklady služeb

- 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

Služby

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

```

=====
System Idle Process      0  Není k dispozici
System                   4  Není k dispozici
smss.exe                 300 Není k dispozici
csrss.exe                424 Není k dispozici
wininit.exe              484 Není k dispozici
csrss.exe                492 Není k dispozici
services.exe            540 Není k dispozici
lsass.exe                556 KeyIso, Netlogon, ProtectedStorage, SamSs
lsm.exe                  564 Není k dispozici
svchost.exe              672 DcomLaunch, PlugPlay, Power
svchost.exe              748 RpcEptMapper, RpcSs
svchost.exe              816 AudioSrv, Dhcp, eventlog,
                        HomeGroupProvider, lmhosts, wscsv
svchost.exe              852 AudioEndpointBuilder, CscService, Netman,
                        PcaSvc, TrkWks, UmRdpService, UxSms,
                        Wlansvc, wudfsvc
svchost.exe              876 Appinfo, BDESVC, BITS, Browser,
                        CertPropSvc, EapHost, gpsvc, IKEEXT,
                        iphlpsvc, LanmanServer, MMCSS, ProfSvc,
                        Schedule, SEMS, SessionEnv,
                        ShellHWDetection, Themes, Winmgmt, wuauerv
stacsv64.exe             920 STacSV
winlogon.exe             380 Není k dispozici
svchost.exe              636 EventSystem, fdPHost, netprofm, nsi,
  
```

Vlastnosti 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

Spouštění služeb

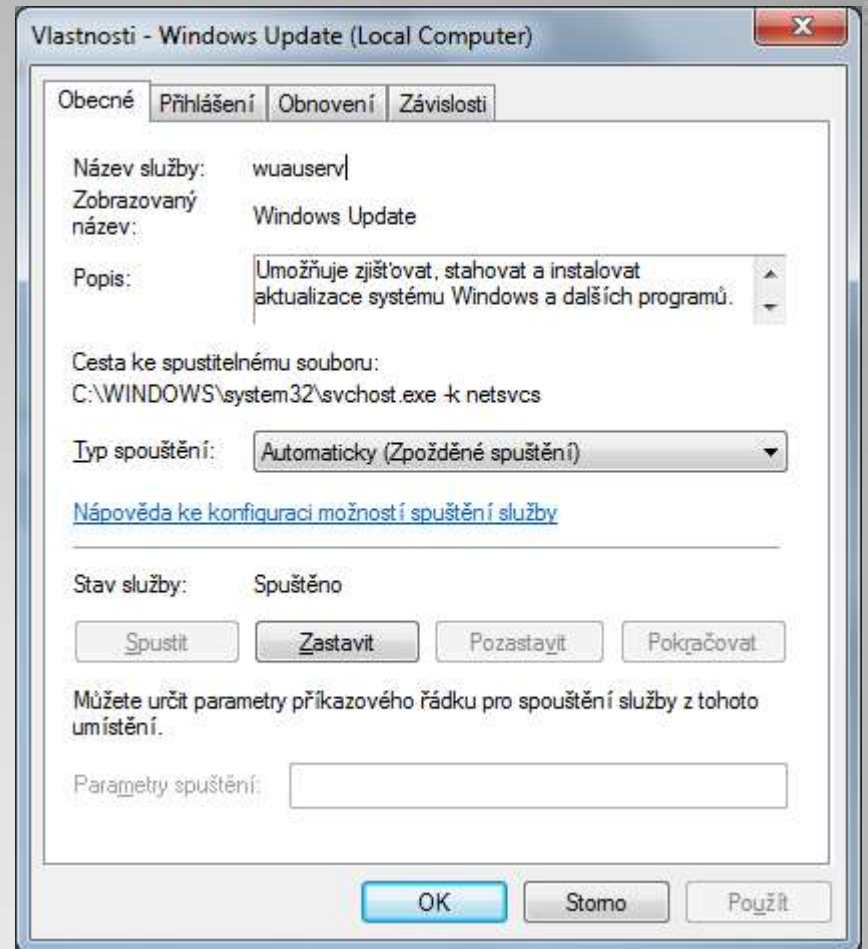
- Služba je identifikována názvem
- Existuje tzv. „dlouhý název“
 - **Display Name**
- A „krátký název“
 - **Service Name**
- Dlouhý název je lokalizován (český, anglický, finský) zatímco krátký název je vždy stejný.
- Názvy mohou být značně odlišné!

Identifikace služeb

Název	Popis	Stav	Typ spouštění	Účet pro přihlášení
Šíření certifikátů	Kopíruje uživatelské certifikát...	Spuštěno	Automaticky	Local System
Technologie Windows Connect Now – Reg...	Služba WCNCSVC je hostitele...		Ručně	Local Service
Telefonní subsystém	Poskytuje podporu rozhraní T...		Ručně	Síťová služba
UPnP Device Host	Povolí hostování zařízení UPn...		Zakázáno	Local Service
Virtuální disk	Poskytuje služby správy pro d...		Ručně	Local System
VMware Authorization Service	Authorization and authentica...	Spuštěno	Automaticky	Local System
VMware DHCP Service	DHCP service for virtual netw...		Zakázáno	Local System
VMware NAT Service	Network address translation f...	Spuštěno	Automaticky	Local System
VMware USB Arbitration Service	Arbitration and enumeration ...	Spuštěno	Automaticky	Local System
Výstrahy a protokolování výkonu	Čítač Výstrahy a protokolová...		Ručně	Local Service
Vzdálená plocha	Umožňuje uživatelům interak...	Spuštěno	Ručně	Síťová služba
Vzdálená správa systému Windows (WS-M...	Služba Vzdálená správa systé...		Ručně	Síťová služba
Vzdálené volání procedur (RPC)	Služba RPCSS je Správce řízen...	Spuštěno	Automaticky	Síťová služba
Vzdálený registr	Umožňuje vzdáleným uživate...	Spuštěno	Automaticky	Local Service
Webový klient	Umožňuje programům pro sy...		Ručně	Local Service
Windows Defender	Ochrana před spywarem a po...		Zakázáno	Local System
Windows Presentation Foundation Font Ca...	Optimalizuje výkon aplikací ...		Ručně	Local Service
Windows Search	Poskytuje indexování obsahu,...	Spuštěno	Automaticky (Zpoždě...	Local System
Windows Update	Umožňuje zjišťovat, stahovat ...	Spuštěno	Automaticky (Zpoždě...	Local System

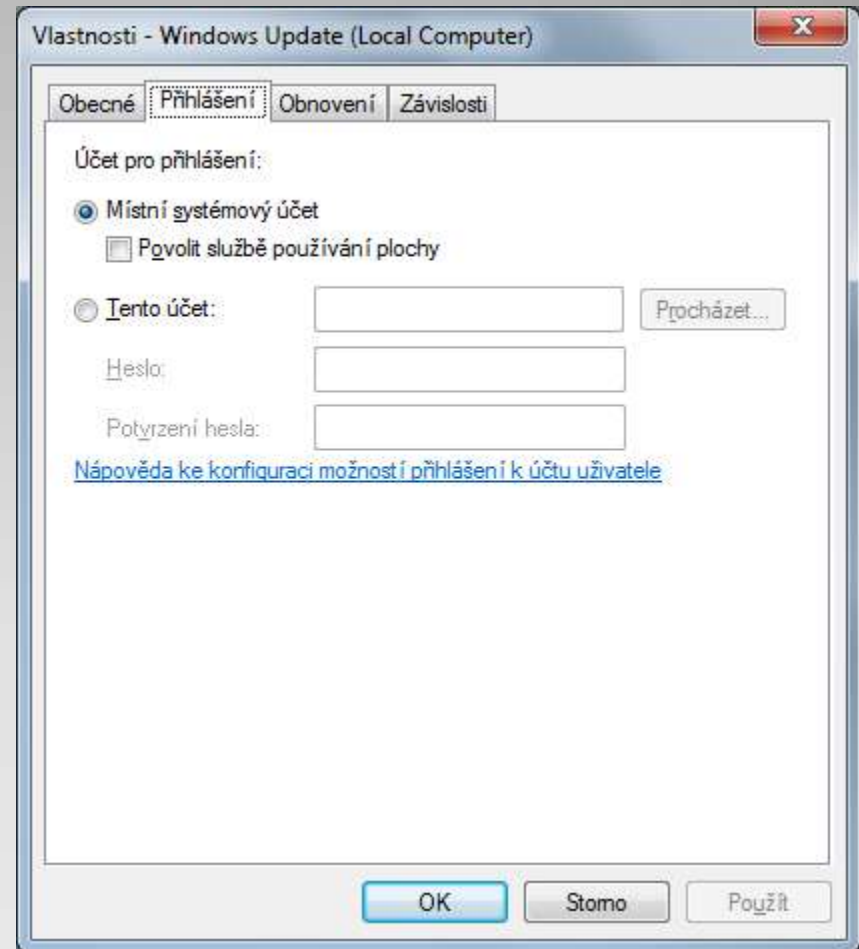
Konfigurace služeb - GUI

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



Vlastnosti služby

- Přihlášení
- = Účet pod kterým služba běží
 - Účet „System“
 - 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

Vlastnosti 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

Stav služby

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

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

Ovládání služeb - CMD

- 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 vypsát / nastavit jen pomocí SC
- Používá syntaxi SDDL
 - (Security Descriptor Definition Language)



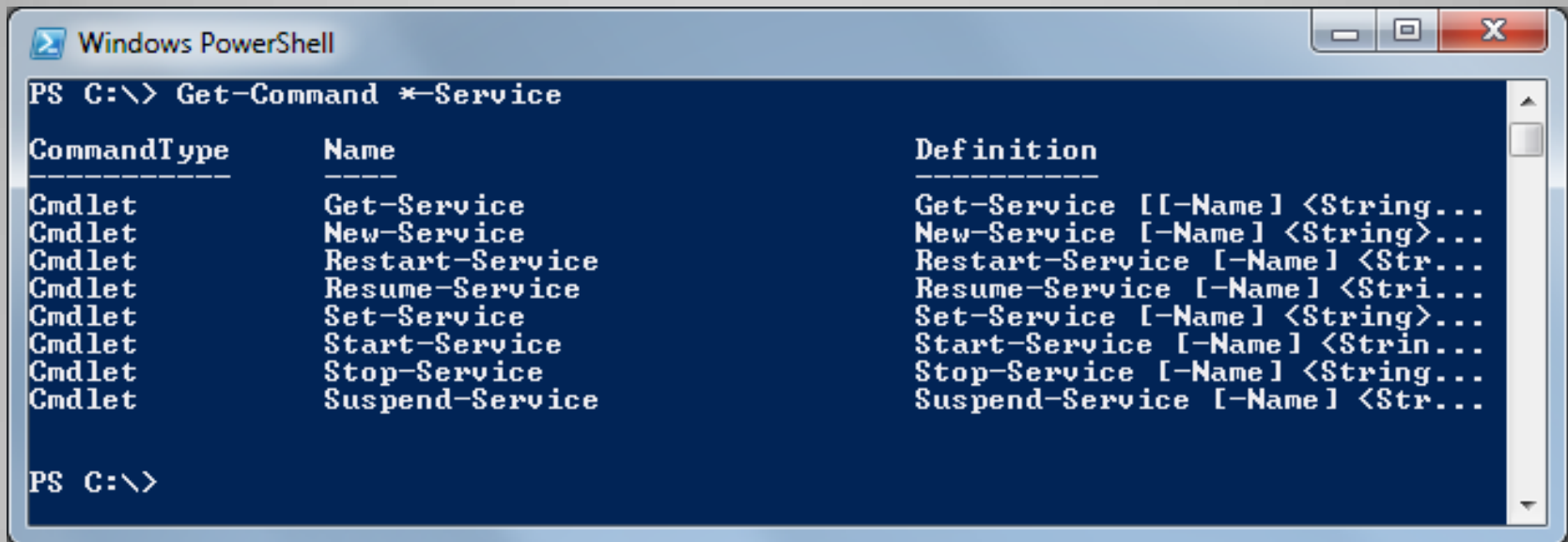
```
C:\WINDOWS\system32\cmd.exe

C:\>sc sdshow wuauerv
D:(A;;;CCLCSWRPLOGR;;;AU)(A;;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;;CCDCLCSWRPWPDTLO
CRSDRCWDWO;;;SY)

C:\>
```

Zabezpečení služeb

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



```
Windows PowerShell
PS C:\> Get-Command *-Service

CommandType      Name                Definition
-----
Cmdlet            Get-Service         Get-Service [[-Name] <String>...
Cmdlet            New-Service         New-Service [-Name] <String>...
Cmdlet            Restart-Service     Restart-Service [-Name] <Str...
Cmdlet            Resume-Service      Resume-Service [-Name] <Stri...
Cmdlet            Set-Service         Set-Service [-Name] <String>...
Cmdlet            Start-Service       Start-Service [-Name] <Strin...
Cmdlet            Stop-Service        Stop-Service [-Name] <String...
Cmdlet            Suspend-Service     Suspend-Service [-Name] <Str...
```

Ovládání služeb - PowerShell

- 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

Windows Registry

- 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.

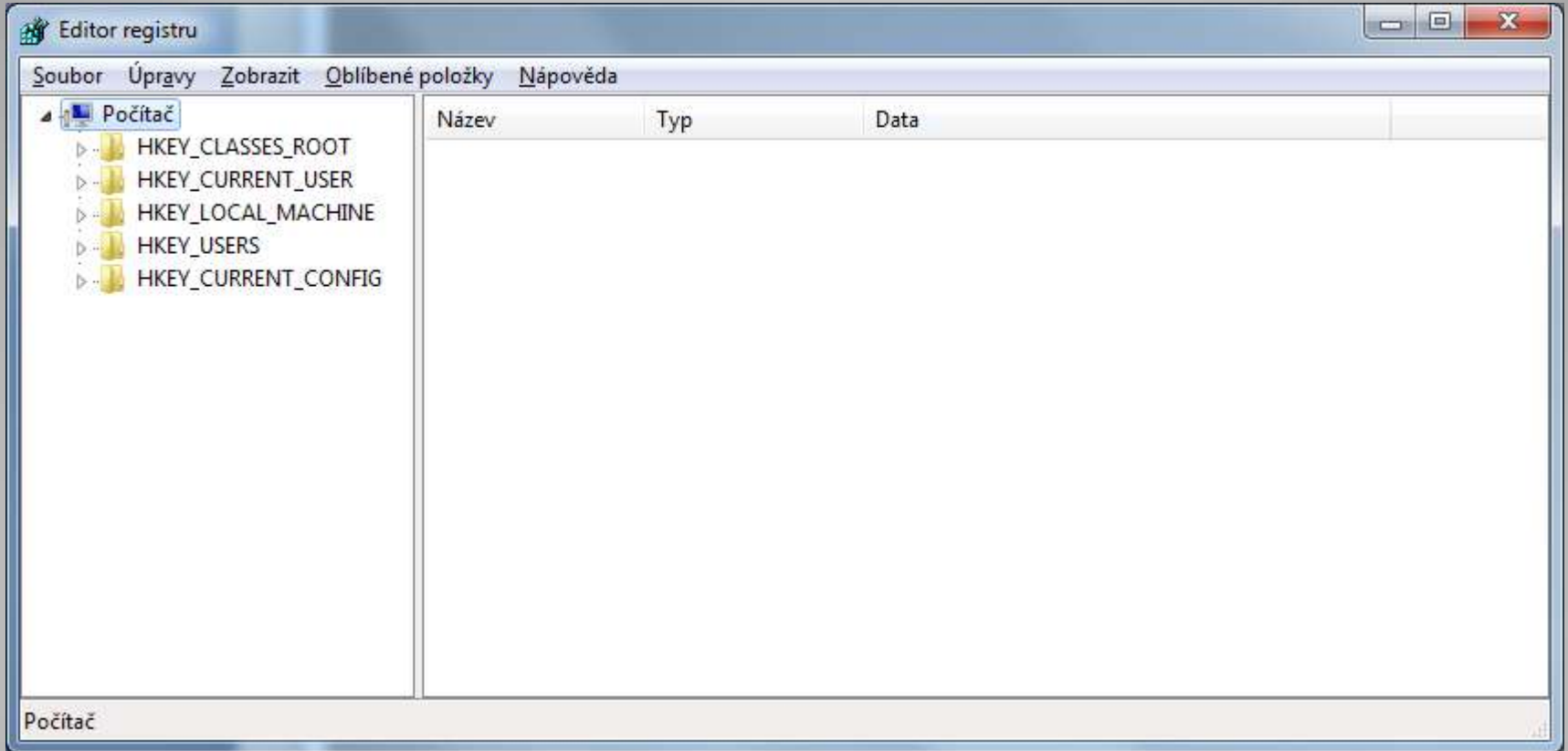
Dělení registru

- 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 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)

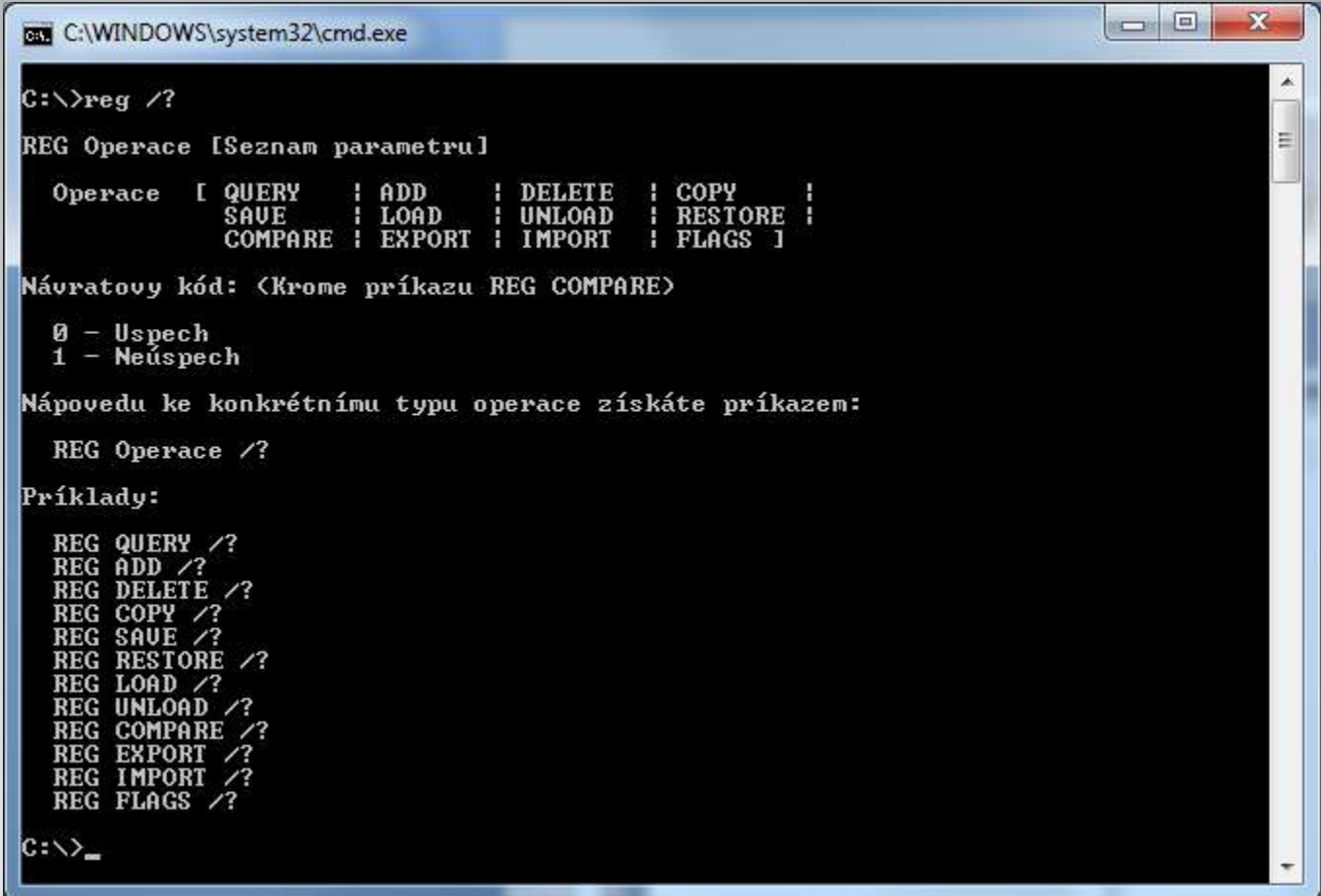
Registry – datové typy

- REGEDIT – Editor Registru



Práce s registry

- Příkaz REG



```
C:\WINDOWS\system32\cmd.exe

C:\>reg /?

REG Operace [Seznam parametru]

Operace [ QUERY      | ADD      | DELETE  | COPY     |
          SAVE       | LOAD     | UNLOAD  | RESTORE  |
          COMPARE    | EXPORT   | IMPORT  | FLAGS   ]

Návratový kód: <Krome příkazu REG COMPARE>

0 - Úspěch
1 - Neúspěch

Nápovedu ke konkrétnímu typu operace získáte příkazem:

REG Operace /?

Příklady:

REG QUERY /?
REG ADD /?
REG DELETE /?
REG COPY /?
REG SAVE /?
REG RESTORE /?
REG LOAD /?
REG UNLOAD /?
REG COMPARE /?
REG EXPORT /?
REG IMPORT /?
REG FLAGS /?

C:\>_
```

Práce s registry - CMD

- PowerShell provider pro registry

```
Windows PowerShell
PS C:\> Set-Location HKCU:
PS HKCU:\> Get-ChildItem

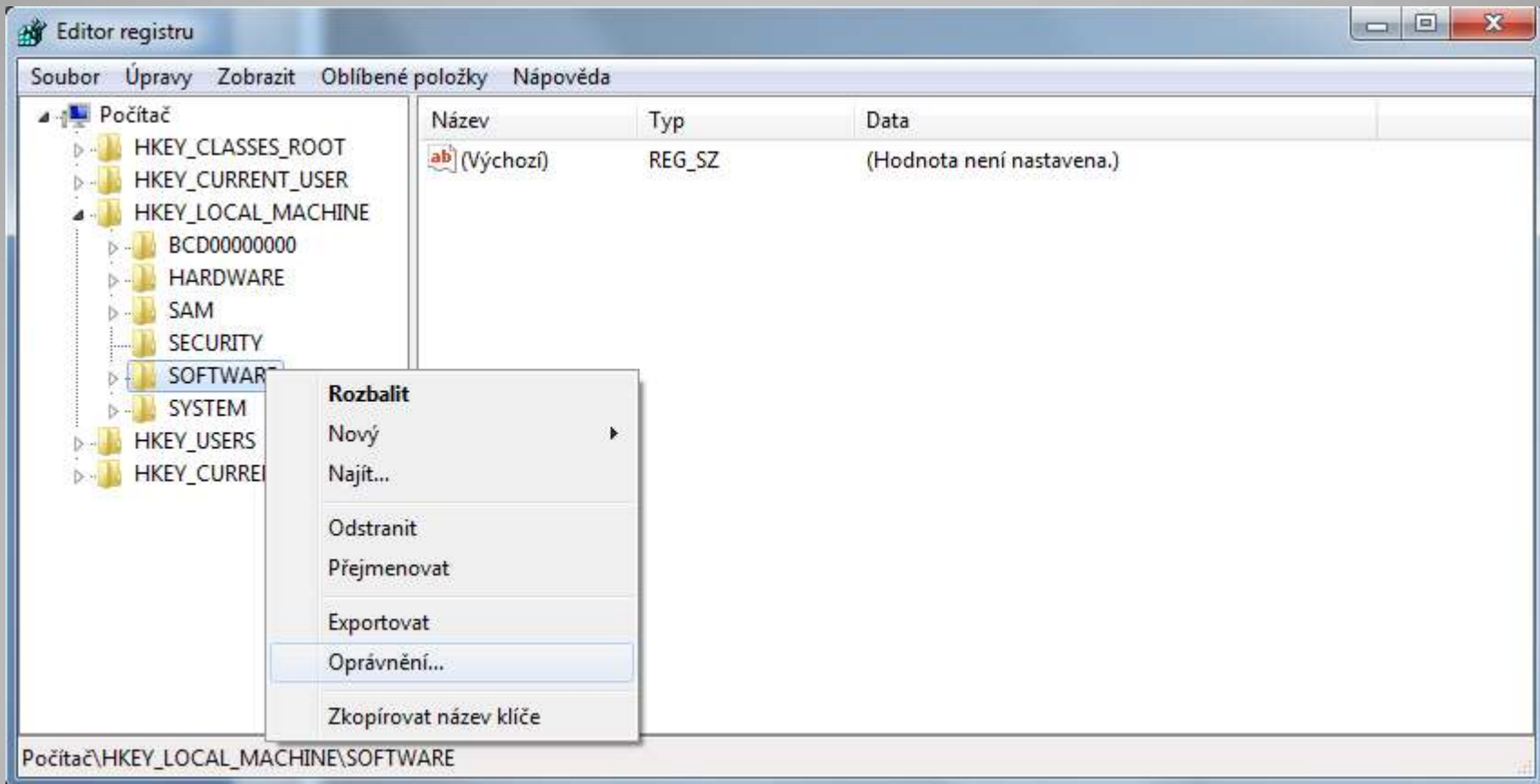
Hive: HKEY_CURRENT_USER

SKC UC Name Property
--- --
2 0 AppEvents {}
0 36 Console {ColorTable00, ColorTable01, ColorTab...
15 0 Control Panel {}
0 4 Environment {TEMP, TMP, EXCSRU, NAME}
4 0 EUDC {}
1 6 Identities {Identity Ordinal, Migrated?, Last Us...
3 0 Keyboard Layout {}
1 0 Network {}
5 0 Printers {}
32 0 Software {}
1 0 System {}
1 9 Volatile Environment {LOGONSERVER, USERDNSDOMAIN, USERDOMA...

PS HKCU:\>
```

Práce s registry - PowerShell

- Každý klíč registru má ACL



Oprávnění v registrech

- 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 přihlášení uživatele
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 - Aplikace pro spuštění po přihlášení uživatele

Registry - vybrané nastavení

- Každá běžící aplikace v systému (a také služba / služby) jsou reprezentovány procesem
- Proces obecně reprezentuje programový kód, jeho aktivitu, stav a alokovanou paměť
- Technická poznámka:
Procesy neběží, vlákna ano 😊

Procesy ve Windows

Správce úloh systému Windows

Šoubor Možnosti Zobrazit Nápověda

Aplikace **Procesy** Služby Výkon Síť Uživatelé

Název procesu	PID	Uživatel...	P...	Pracovní sada ...	Paměť (soukromá pracovní sada)	Potvrzen...	Zákl. priorita	Popis
opera.exe *32	5808	bijecric	00	289 532 kB	267 296 kB	275 572 kB	Normální	Opera Internet Browser
explorer.exe	3864	bijecric	00	78 416 kB	40 300 kB	57 268 kB	Normální	Průzkumník Windows
csrss.exe	492		00	76 524 kB	2 524 kB	3 468 kB	Vysoká	
POWERPNT.EXE *32	5368	bijecric	00	47 672 kB	26 188 kB	59 760 kB	Normální	Microsoft Office PowerPoin
dwm.exe	3848	bijecric	00	41 100 kB	23 000 kB	77 800 kB	Vysoká	Správce oken plochy
stray64.exe	4048	bijecric	00	15 372 kB	7 100 kB	7 480 kB	Normální	IDT PC Audio
vpngui.exe *32	5048	bijecric	00	13 856 kB	3 648 kB	4 284 kB	Normální	Cisco Systems VPN Client
TOTALCMD.EXE *32	740	bijecric	00	12 464 kB	3 044 kB	5 624 kB	Normální	Total Commander 32 bit
taskhost.exe	3556	bijecric	00	12 232 kB	3 292 kB	8 840 kB	Normální	Host Process for Windows
DCPSysMgr.exe	3240	bijecric	00	11 844 kB	3 328 kB	8 148 kB	Normální	Dell System Manager
splwow64.exe	5024	bijecric	00	11 832 kB	3 560 kB	4 792 kB	Normální	Print driver host for 32bit a
hkcmd.exe	4028	bijecric	00	11 072 kB	3 228 kB	3 584 kB	Normální	hkcmd Module
taskmgr.exe	4364	bijecric	00	10 636 kB	2 960 kB	3 352 kB	Vysoká	Správce úloh systému Winc
Apoint.exe	4000	bijecric	00	10 444 kB	3 020 kB	3 396 kB	Normální	Alps Pointing-device Driver
mobsync.exe	4788	bijecric	00	10 440 kB	2 720 kB	3 052 kB	Normální	Microsoft Sync Center
SMSCLIUI.exe *32	5748	bijecric	00	9 124 kB	2 772 kB	3 916 kB	Normální	SMS Remote Client UI Loca
regedit.exe	4268	bijecric	00	8 460 kB	2 012 kB	4 616 kB	Normální	Editor registru
winlogon.exe	380		00	8 280 kB	3 060 kB	3 852 kB	Vysoká	
igfxpers.exe	4036	bijecric	00	7 372 kB	2 428 kB	2 676 kB	Normální	persistence Module
igfxtray.exe	4012	bijecric	00	7 208 kB	2 744 kB	2 960 kB	Normální	igfxTray Module
igfxsrv.exe	4900	bijecric	00	7 052 kB	2 368 kB	2 644 kB	Normální	igfxsrv Module
igfxext.exe	3324	bijecric	00	5 948 kB	1 968 kB	2 156 kB	Normální	igfxext Module
ApMsgFwd.exe	1324	bijecric	00	5 872 kB	2 280 kB	2 560 kB	Normální	ApMsgFwd

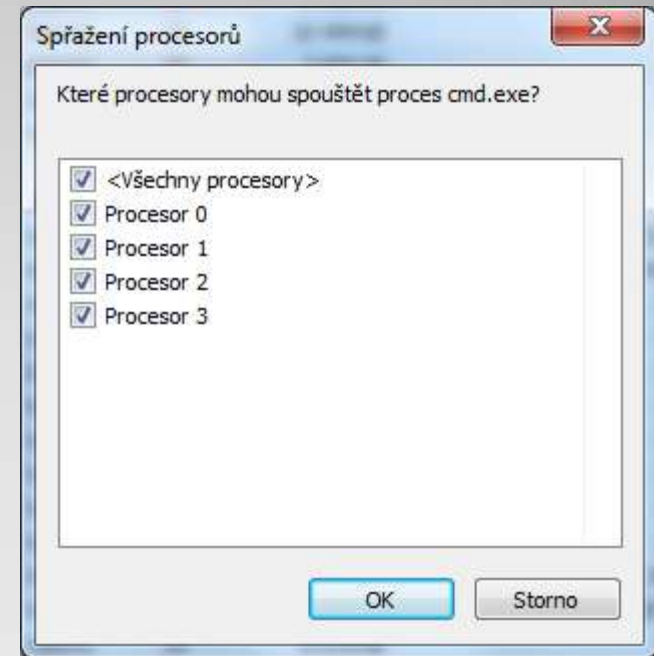
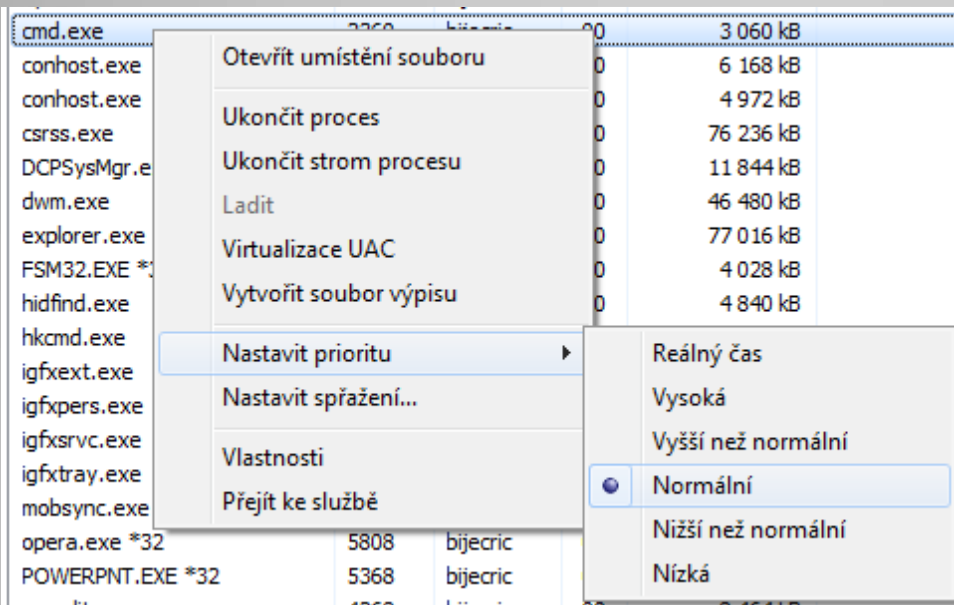
Zobrazit procesy všech uživatelů

Ukončit proces

Procesy: 79 Využití procesoru: 0 % Fyzická paměť: 23 %

Správa procesů

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



Správa procesů

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

Správa procesů

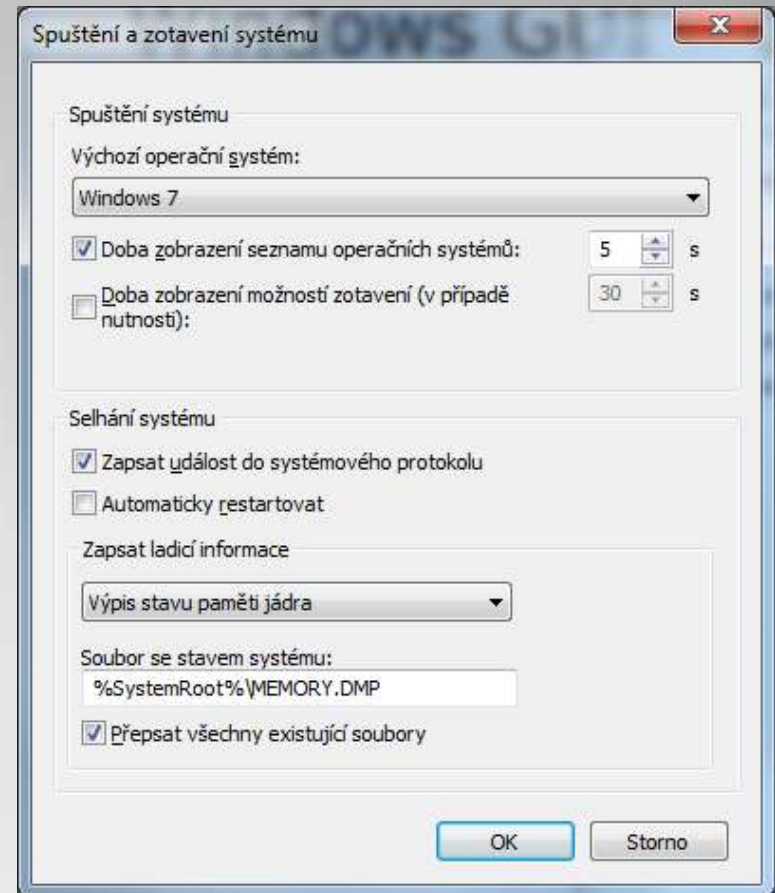
- Boot sektor disku předá řízení →
- Windows Boot Manager (BOOTMGR)
 - Zjistí aktivní oddíl
 - načte Boot Configuration Data (BCD)
- BCD je firmware-nezávislá databáze
 - Uložena na EFI oddílu
 - Nebo v \boot\bcd souboru systémového oddílu

Spuštění systému, 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

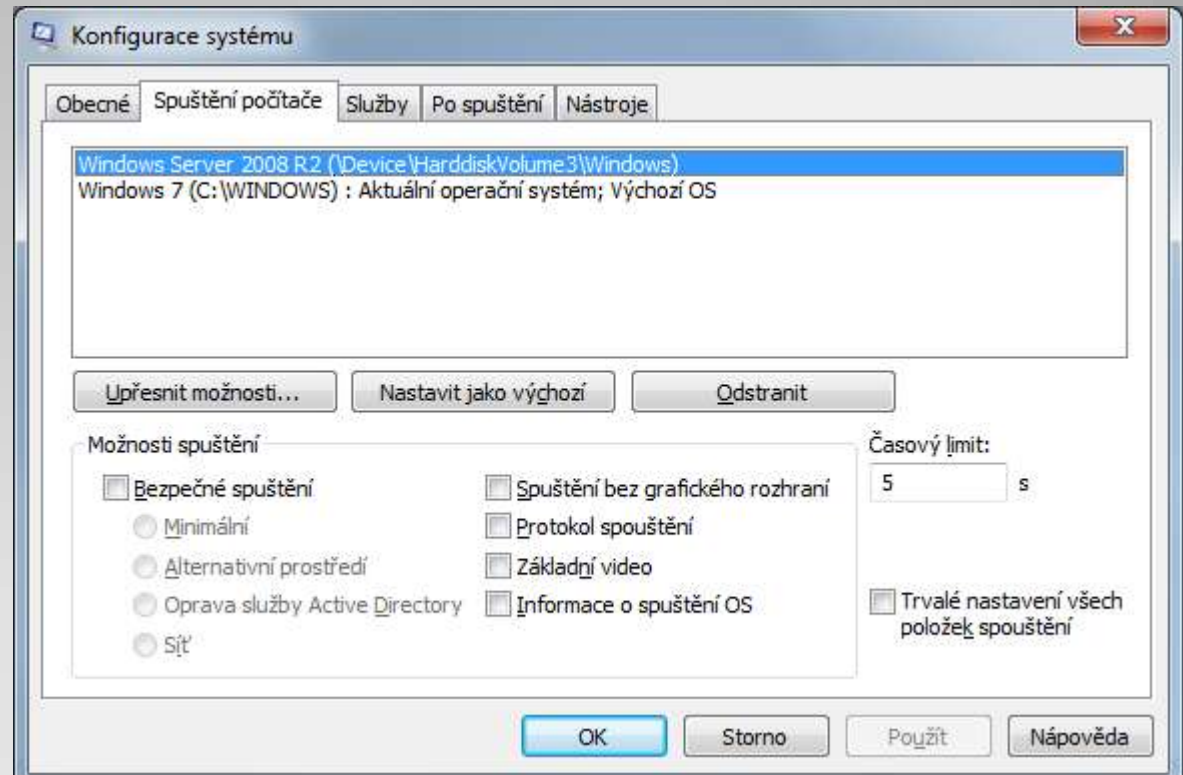
BCD

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



Konfigurace spouštění OS

- msconfig.exe



Konfigurace spuštění OS

- bcdedit.exe
- Úplná správa BCD databáze

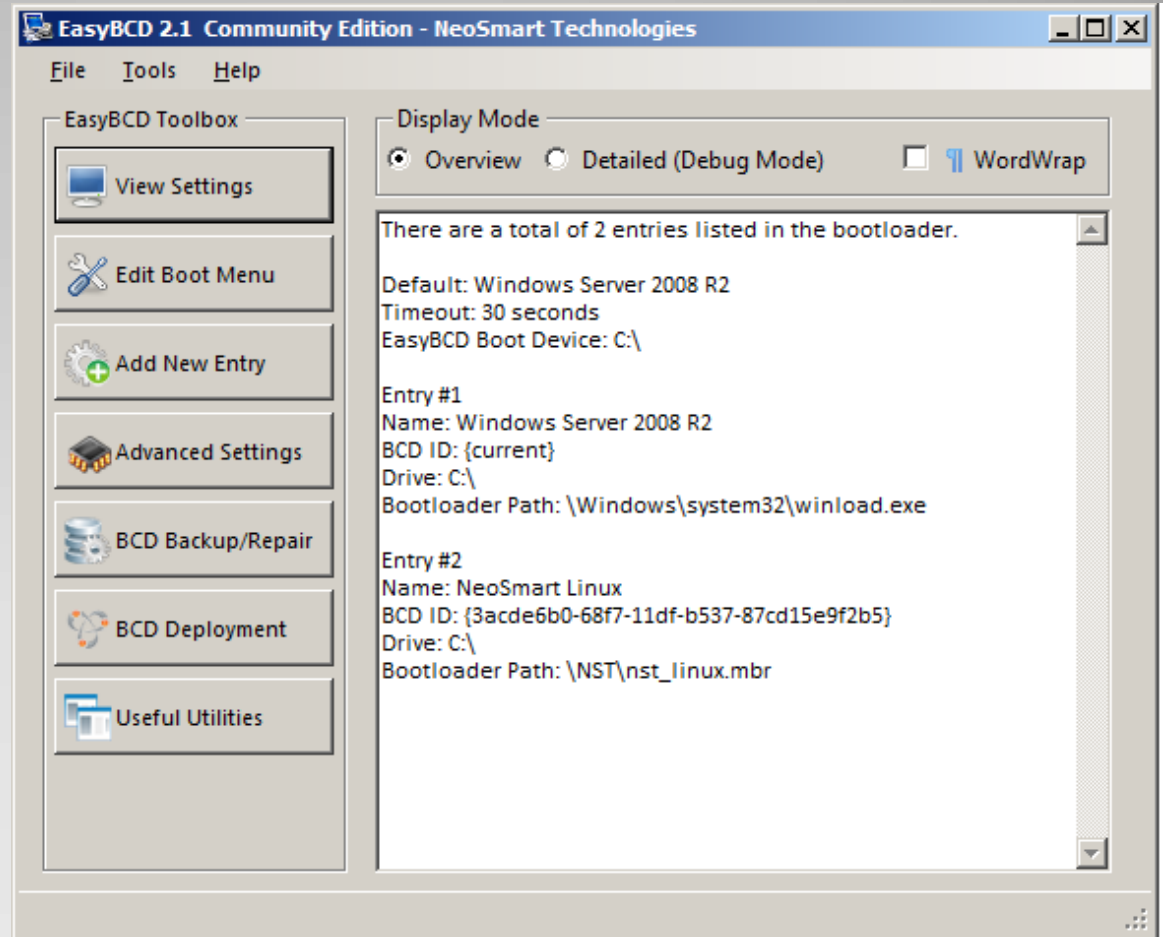
```
cmd. Správce: C:\WINDOWS\system32\cmd.exe
C:\>bcdedit
Správce spouštění systému Windows
-----
identifikátor          {bootmgr}
device                 partition=X:
description            Windows Boot Manager
locale                 en-US
inherit                {globalsettings}
default                {current}
resumeobject           {41175fc7-7a94-11e0-8b3e-5c260a4fc51a}
displayorder           {41175fc8-7a94-11e0-8b3e-5c260a4fc51a}
toolsdisplayorder     {memdiag}
timeout                5

Zavádecí program pro spouštění systému Windows
-----
identifikátor          {41175fc8-7a94-11e0-8b3e-5c260a4fc51a}
device                 partition=\Device\HarddiskVolume3
path                   \Windows\system32\winload.exe
description            Windows Server 2008 R2
locale                 en-US
inherit                {bootloadersettings}
recoveryenabled       No
osdevice               partition=\Device\HarddiskVolume3
systemroot             \Windows
resumeobject           {41175fc7-7a94-11e0-8b3e-5c260a4fc51a}
nx                     OptOut
hypervisorlaunchtype  Auto

Zavádecí program pro spouštění systému Windows
-----
identifikátor          {current}
device                 partition=C:
path                   \WINDOWS\system32\winload.exe
description            Windows 7
locale                 cs-CZ
inherit                {bootloadersettings}
recoverysequence       {eaa2addf-7bc6-11e0-ae50-68a3c44613f4}
recoveryenabled       Yes
osdevice               partition=C:
systemroot             \WINDOWS
resumeobject           {41175fc3-7a94-11e0-8b3e-5c260a4fc51a}
nx                     OptOut
C:\>
```

Konfigurace spouštění OS

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



Konfigurace spouštění OS

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

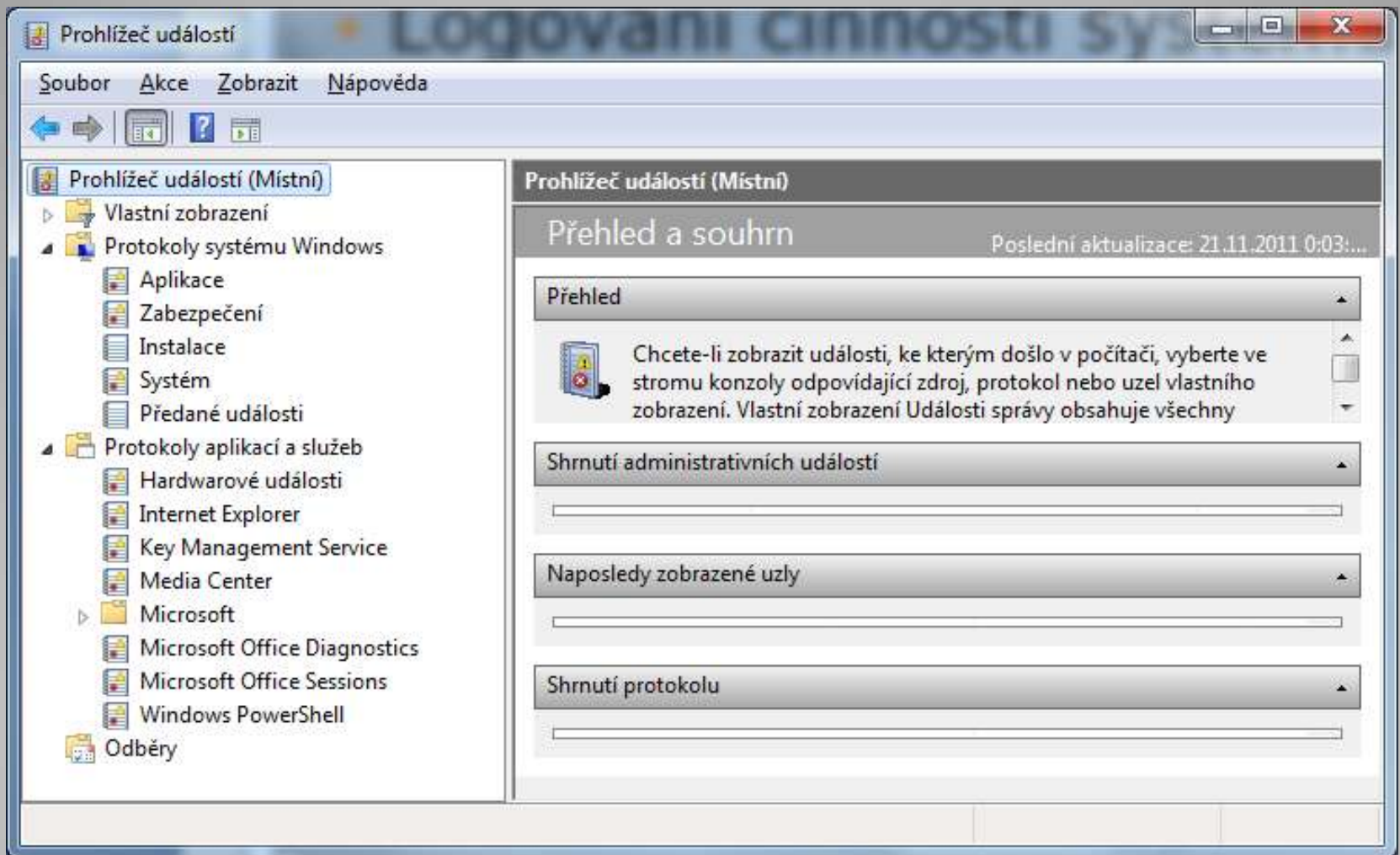
Události, Prohlížeč událostí

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

Logy

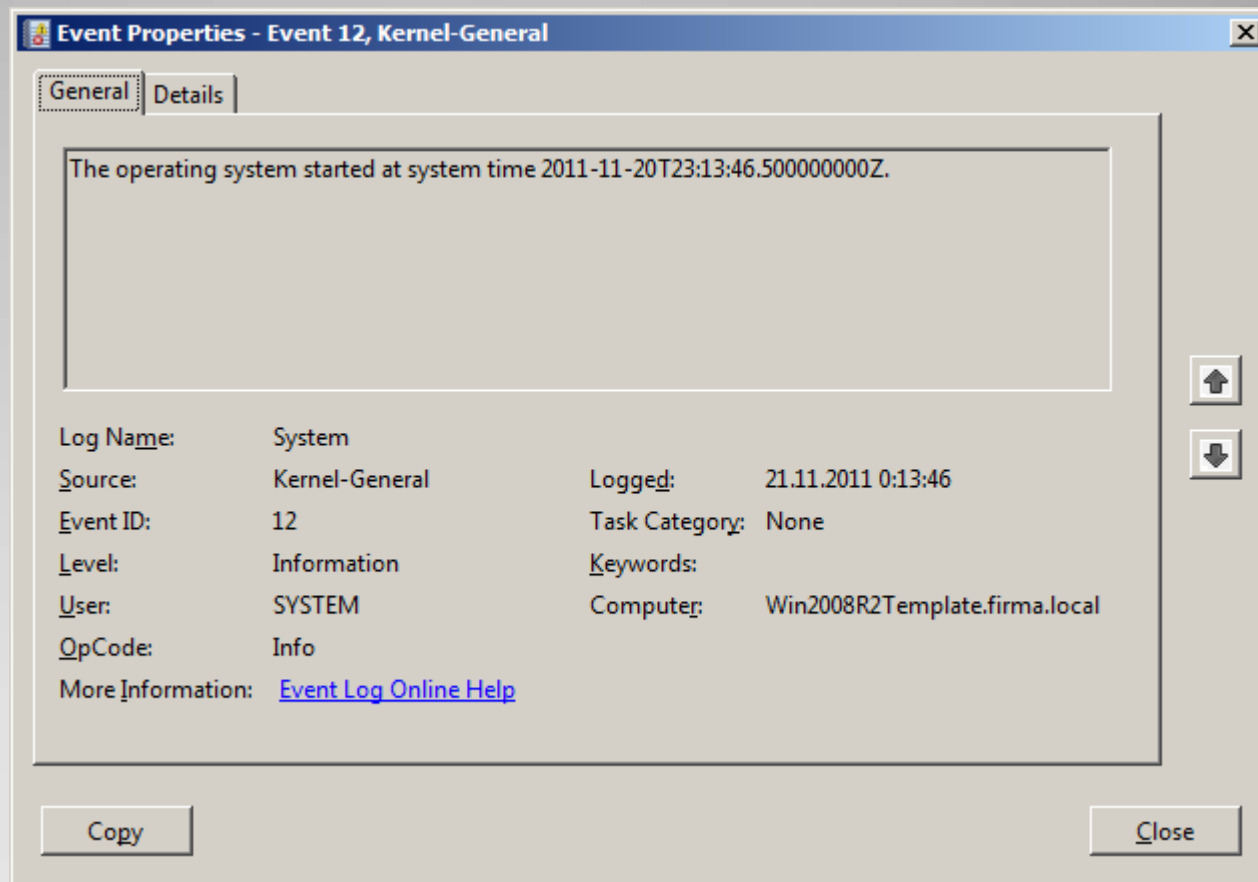
- Záznam v logu = Událost
- Každá událost má:
 - Zdroj
 - ID (Dohromady se Zdrojem jednoznačné)
 - Datum a čas
 - Počítač
 - Úroveň (Informace, Varování, Chyba)

Události



Prohlížeč událostí

- Příklad události



Událost

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

Práce s prohlížečem událostí