

22 Procesy v OS MS Windows

Obsah hodiny



Obsahem hodiny je popis procesů z pohledu jednotlivých OS.

Cíl hodiny



Po této hodině budete schopni:

- zjistit informace o procesech
- orientovat se v možnostech použití Správce procesů
- orientovat se v příkazech pro práci s procesy
- popsat možnosti komunikace mezi procesy
- popsat možnosti zrušení procesu

Klíčová slova



Správce úloh, Tasklist, Taskkill, Zabíjení proces, PID, Priorita procesů

22.1 Procesy v OS MS Windows

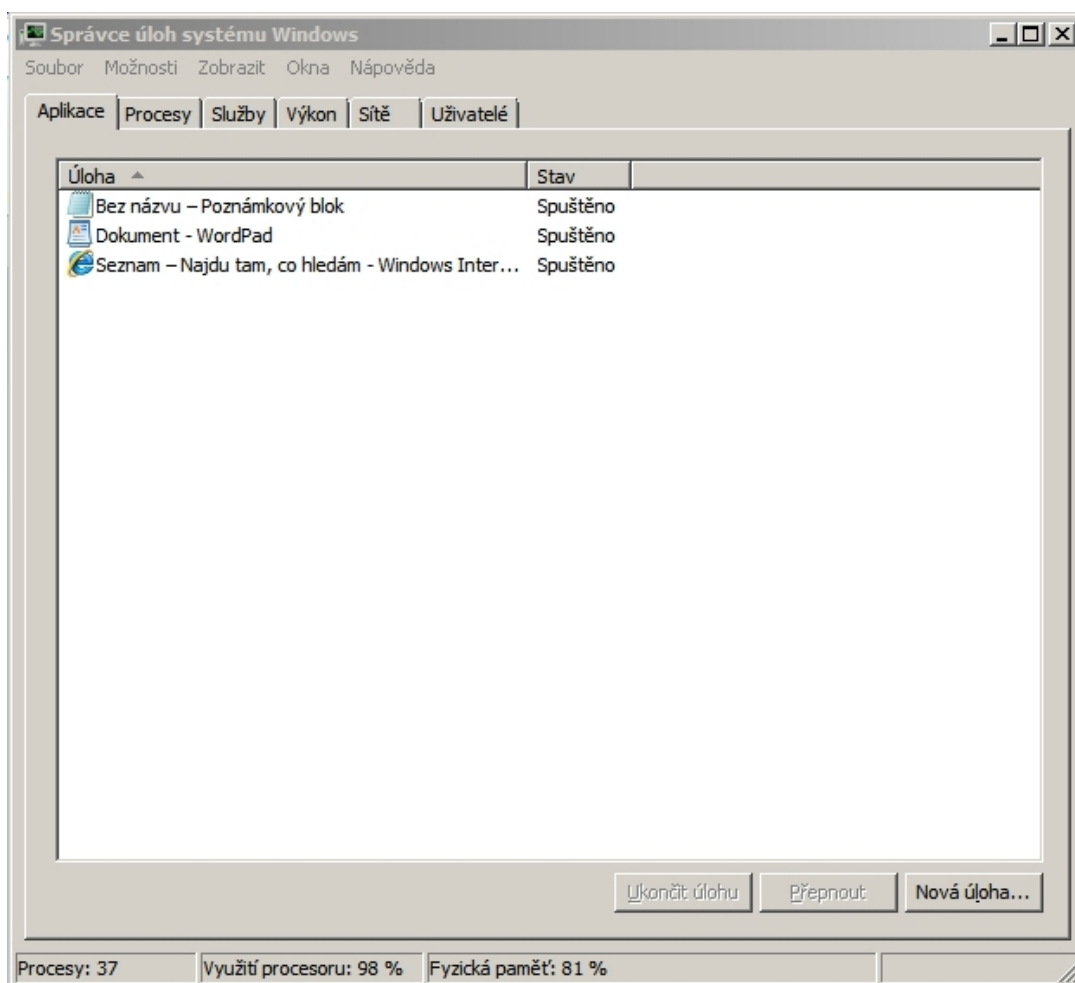
Informace o procesech lze zjistit pomocí Správce úloh: tj. trojhmatem Ctrl+Alt+Delete a kliknutím na Správce úloh, nebo Ctrl+Shift+Escape.



Obrázek 22-1 Ctrl-Alt-Delete

Správce úloh zobrazuje programy, procesy a služby, které jsou aktuálně spuštěny na počítači. Je možné jej využít ke sledování výkonu počítače, k ukončení programu, který neodpovídá, nebo sledovat stav sítě a zjišťovat, kteří uživatelé jsou aktuálně k počítači připojeni.

Je normální, že ve Windows na počítači běží spousta nejrůznějších aplikací - jejich počet je v podstatě omezen pouze velikostí dostupné paměti a výkonem procesoru, ve Správci úloh je vidět pouze zlomkem toho, co se děje uvnitř operačního systému.



Obrázek 22-2 Správce procesů - Windows 7

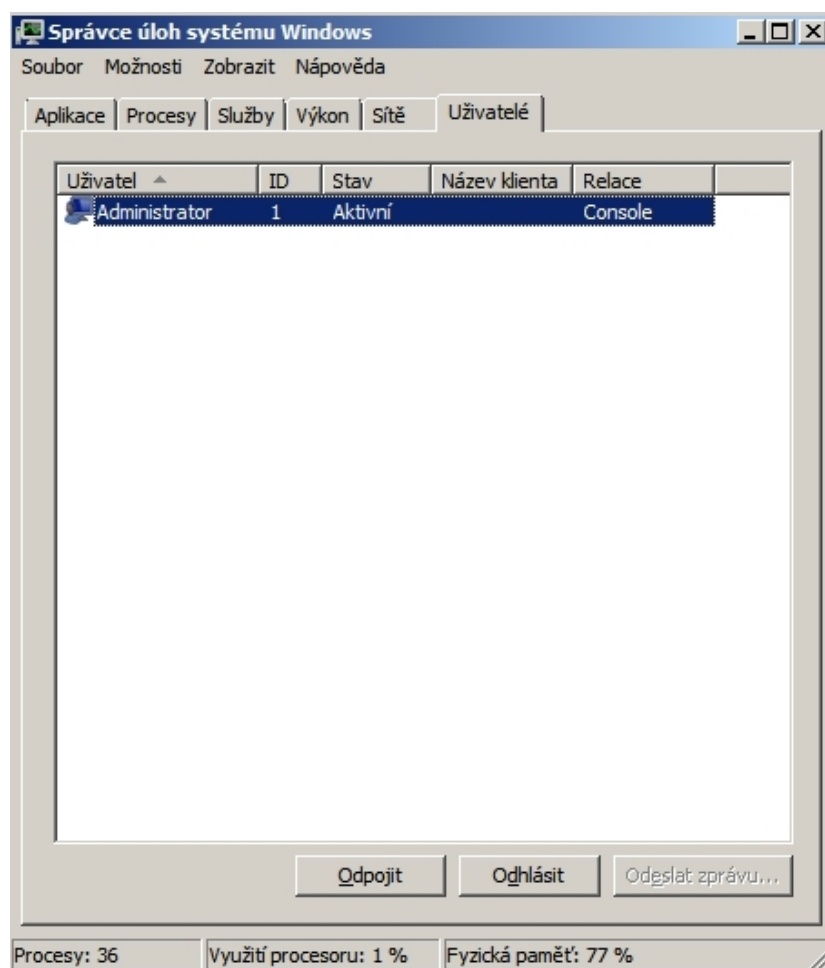
Aplikace. Na kartě Správce úloh se zobrazuje seznam aktuálně spuštěných programů. Je možno vybranou aplikaci ukončit, zobrazit procesy spojené s aplikací.

Procesy. Záložka obsahuje seznam všech běžících procesů v systému. Je možno ukončit proces (včetně procesů, které proces spustil), měnit prioritu procesu, nastavit spřažení procesorů s procesem (nastavení, které CPU proces realizuje).

Výkon. Na kartě Výkon se zobrazí souhrnné statistiky o výkonu systému, především celková výše vytížení CPU a paměti. Je možno mimo jiné zobrazit, co běží v režimu jádra (červeně) a co v uživatelském režimu (zeleně).

Sítě. Pod touto záložkou se v reálném čase zobrazuje zatížení aktivních síťových připojení. Ve spodní části okna konzoly je k vidění seznam všech dostupných síťových připojení, využití síťových připojení v procentech, maximální možná přenosová rychlost a aktuální stav síťových připojení.

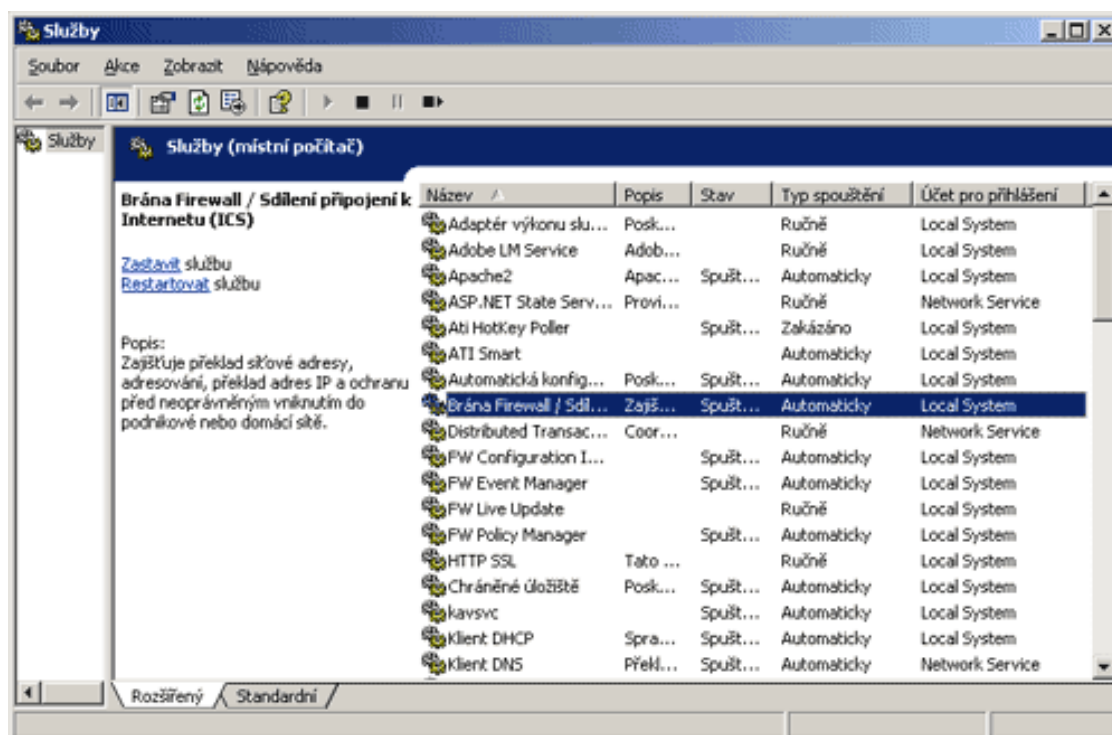
Uživatelé. U většiny desktopových počítačů se na záložce Uživatelé zobrazuje pouze aktuálně přihlášený uživatel. U počítače, který sdílí některé ze svých systémových prostředků, se zde však zobrazují i aktuálně přihlášení uživatelé. Tlačítka, která se nacházejí ve spodní části, se používají k jejich násilnému odpojení nebo odhlášení, popřípadě zaslání zprávy.



Obrázek 22-3 Přehled služeb: msconfig.exe

Služby. Záložka Služby poskytuje informace o spuštěných službách (každá služba je vlastně proces, který je spuštěn OS)

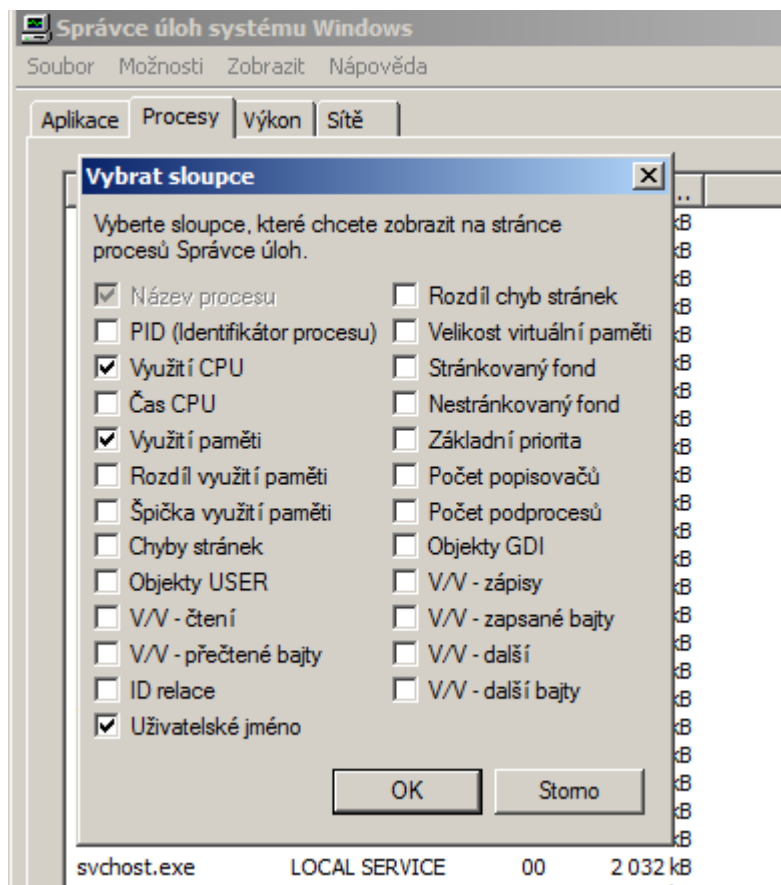
Přehled všech služeb a podrobnější informace o službách poskytuje nástroj Služby. (příkaz services.msc, Start-Nástroje systému-Služby nebo přes kontextovou nabídku na ikoně Tento počítač, volba Spravovat - menu Služby). Nástroj umožňuje zastavení, spuštění nebo zakázání služby (automaticky – při startu OS nebo ručně). Výhoda nástroje Služby je v tom, že zobrazuje i stručný popis každé služby.



Obrázek 22-4 Nástroj Služby

22.2 Priorita procesů: Záložka Procesy

Priority je možno zobrazit přes Správce úloh: Zobrazit-Vybrat sloupce (slovní vyjádření), nebo pomocí specializovaných nástrojů. Nastavovat je lze jen velmi omezeně.



Obrázek 22-5: Rozšíření výpisu o další informace o procesech

Hodnoty priority procesů se pohybují od 0-31:

- 0: Nulový proces
- 1: Nečinný proces
- 4: Nízká priorita
- 6: Podprůměrná priorita
- 8: Normální priorita
- 10: Nadprůměrná priorita
- 13: Vysoká priorita
- 15: Maximální priorita pro běžné procesy
- 24: Priorita procesů reálného času
- 31: maximální hodnota

22.3 Některé procesy v MS Windows

csrss.exe

Původní anglický nezkrácený název tohoto procesu je Client Server Runtime Subsystem a má na starosti základní běh součástí Windows. Zároveň se ale jedná o častý terč virů a červů, Jestliže je procesorová zátěž dlouhodobě vysoká, doporučuje se aktualizovat antivir a spustit kontrolu systému.

explorer.exe

Řada uživatelů si vinou podobného pojmenování tento proces plete s procesem pro Internet Explorer. Jedná se přitom o proces, který má na starosti zobrazení a práci s plochou, hlavním panelem nebo například nabídkou Start.

lsass.exe

Proces, který má na starosti podstatnou část bezpečnosti, a sice autentizaci uživatelů.

services.exe

Proces sloužící pro spuštění služeb, které jsou ve skutečnosti samostatnými procesy. Spouštění a správa služeb však z větší části spadá pod proces svchost.exe.

smss.exe

Tento proces se zaměřuje na aktuální běh Windows v uživatelském profilu, kromě jiného má na starosti například spuštění některých programů definovaných v registru.

spoolsv.exe

Proces, který si bere na starosti tiskárny a jednotlivé tiskové úlohy.

winlogon.exe

Hlavním posláním tohoto procesu je zprostředkování funkcí pro přihlášení jednotlivých uživatelů, zamykání počítače, změnu přihlašovacích údajů a dalších bezpečnostních možností.

svchost.exe

Je proces v počítači hostící nebo obsahující další samostatné služby, které systém Windows používá při vykonávání různých funkcí.

V počítači může být spuštěno několik výskytů procesu svchost.exe a každý z těchto výskytů obsahuje jiné služby. Jeden výskyt procesu svchost.exe může hostit jedinou službu pro určitý program, zatímco další výskyt může hostit několik služeb vztahujících se k systému Windows.

Pro zjištění, které služby jsou spuštěny v rámci určité instance procesu svchost.exe, lze použít opět program Správce úloh: Procesy/Zobrazit procesy všech uživatelů. V kontextovém menu (pravé tlačítko) položka instance procesu svchost.exe /Přejít na službu: na kartě Služby se zvýrazní služby přidružené k vybranému procesu.

22.4 Procesy v příkazové řádce

Zobrazení informací o procesech - tasklist

Zobrazuje jednoduchý seznam běžících procesů, jejich název, identifikátor PID, název a číslo relace a informaci o tom, kolik paměti daný proces momentálně zabírá.

tasklist /V

Zobrazí na obrazovce trochu více informací. K těm základním přidává aktuální stav procesu, uživatele, pod kterým proces běží, čas a pojmenování procesu určené k zobrazení v titulku okna aplikace.

tasklist /Svc

Přidá informace o tom, jaký je vztah mezi spuštěnými procesy a spuštěnými službami. Výstup ve formě tabulky zobrazuje název procesu, jeho identifikátor PID a veškeré služby, které s tímto procesem souvisejí (jsou-li takové).

tasklist /M

Zobrazí seznam procesů s návazností na použité DLL. Pokud nějaká knihovna DLL způsobuje počítači problémy, lze do seznamu vypsat jen ty spuštěné procesy, které tuto knihovnu používají, takto:

tasklist /M knihovna.dll.

Zabíjení a ukončení procesů ve Windows

Informace získané pomocí příkazu tasklist je možné použít k ukončování a zabíjení procesů pomocí příkazového řádku. Slouží k tomu příkaz **taskkill** s řadou přepínačů.

Označení procesu, který má být pomocí příkazu taskkill ukončen, lze provést několika způsoby: pomocí identifikátoru PID, nebo označením názvu procesu:

taskkill /pid 5560 - ukončí proces s PID 5560

taskkill /im chrome.exe - ukončí všechny procesy s názvem chrome.exe

V uvedené ukázce prohlížeč Google Chrome otevírá pro každé okno samostatný proces. To zabraňuje kompletnímu pádu celé aplikace, zároveň však nelze celý Google Chrome zavřít na základě uvedení jediného PID. Použitím přepínače /im, se zavřou všechna okna prohlížeče najednou.

Příkaz taskkill dále umožňuje ukončovat všechny podprocesy související se zavíraným procesem. Například:

```
taskkill /t /pid 5560
```

Ukončí proces s PID 5560 a všechny jeho podprocesy, tedy třeba programy, které spustil.

Pokud nějaká aplikace přestane reagovat a odmítá se normálně ukončit, lze ukončení procesu vynutit a tzv. jej zabít pomocí přepínače /F:

```
taskkill /F /pid 5560.
```

22.5 Komunikace mezi procesy

Komunikace mezi procesy v MS Windows je založená na zprávách mezi okny: skoro každý proces vytvořený ve Windows má někde okno, byť třeba neviditelné, aby mohl občas zkontrolovat zprávy zaslané tomuto oknu, zprávy pravidelně vyzvedává a zpracovává

Pokud proces nemá okna, je bez milosti sestřelen, aniž by na to mohl nějak reagovat.

I ukončení sezení a zavření všech aplikací je řešeno přes okna, kdy Windows posílají oknům postupně dvě zprávy, na které může proces reagovat a připravit se na ukončení.

Signály z konzole.

Jedná se o signály obsluhy kláves Ctrl+C, Ctrl+Break a zavření konzolového okna křížkem.

V okamžiku vzniku tohoto signálu se založí v postižené aplikaci vlákno, které zavolá obsluhu tohoto signálu.

Signalizace služeb (services)

Všechny procesy, které se spouští jako služba jsou zaregistrovány na SCM interface (Service Control Manager). Toto interface pomocí zvláštního vlákna v procesu volá zaregistrované funkce na zapnutí či vypnutí služby. Sama služba si pak musí zajistit spouštění či zastavování svých vláken a vyřešit komunikaci mezi nimi. To je důvod, proč někdy službu nelze ukončit (zvláště, pokud služba zamrzla) a také, proč například Apache ve Windows se spouští dvakrát (první instance se registruje na SCM a na požadavky SCM spouští vlastní webserver jako druhou instanci. Apache je původem napsaný pro Linux a tak se tímto způsobem emuluje funkce init.d scriptu)

22.6 Náměty pro cvičení

- Vypište seznam procesů a převedte do Excelu *tasklist /Fo Csv*

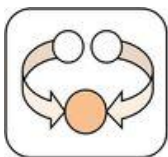
Pro uložení tohoto výstupu do souboru CSV, zpracujete v Excelu nebo jiném tabulkovém programu, použijte příkaz v tomto tvaru:

tasklist /Fo Csv >> procesy.csv.

Soubor vznikne v aktuální složce, kde se v příkazovém řádku nacházíte.

- Vyzkoušejte příkazy uvedené v textu.

Shrnutí kapitoly



Informace o procesech ve Windows lze zjistit pomocí Správce úloh (Ctrl+Alt+Delete - Správce úloh).

Správce úloh zobrazuje programy, procesy a služby, které jsou aktuálně spuštěny na počítači. Je možné jej využít ke sledování výkonu počítače, k ukončení programu, který neodpovídá, nebo sledovat stav sítě a zjišťovat, kteří uživatelé jsou aktuálně k počítači připojeni.

MS Windows používá prioritní plánování. Hodnoty priority procesů se pohybují od 0-31. Omezení lze upravit.

Seznam běžících procesů (jejich název, identifikátor PID, název a číslo relace a informaci o tom, kolik paměti daný proces momentálně zabírá) lze zjistit také řádkovým příkazem *tasklist*.

Informace získané pomocí příkazu *tasklist* je možné použít k ukončování a zabíjení procesů pomocí příkazu *taskkill*.

Komunikace mezi procesy v MS Windows je založena zejména na zprávách mezi okny: Pokud proces nemá okna, je zrušen, aniž by na to mohl nějak reagovat.

Přehled všech služeb a podrobnější informace o službách poskytuje nástroj Služby. (příkaz *services.msc*).

Kontrolní otázky a úkoly



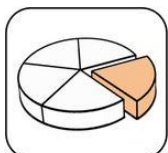
- 1) Jakými způsoby lze zjistit v MS Windows informace o procesech?
- 2) Jak lze ukončit procesy v MS Windows?
- 3) Na čem je založena komunikace mezi procesy v MS Windows?
- 4) Co umožňuje správce úloh v MS Windows?

Otázky k zamyšlení



- 1) Vyzkoušejte příkazy uvedené v kapitole *Náměty pro cvičení*.

Použitá literatura a jiné zdroje:



- [1] Windows.microsoft.com/ [online]. [cit. 2011-12-07]. Co je svchost.exe?. Dostupné z WWW: <<http://windows.microsoft.com/cs-CZ/windows-vista/What-is-svchost-exe#>>>.
- [2] BITTO, Ondřej . Průvodce: Procesy Windows, kterých se nemusíte bát. živě.cz [online]. 31. 1. 2009, [cit. 2011-12-07]. Dostupný z WWW: <<http://jnp.zive.cz/pruvodce-procesy-windows-kterych-se-nemusite-bat>>>.
- [3] BRADLEY, Tony ; ČEPIČKA, David . Správce úloh jako nástroj pro řešení problémů. PCWorld [online]. 29.05.2011, [cit. 2011-12-07]. Dostupný z WWW: <<http://pcworld.cz/software/spravce-uloh-jako-nastroj-pro-reseni-problemu-1-dil-20356>>>.
- [4] POLZER, Jan. extrawindows.cnews.cz [online]. 31. 3. 2009 [cit. 2011-12-07]. Procesy a příkazový řádek Windows. Dostupné z WWW: <<http://extrawindows.cnews.cz/procesy-prikazovy-radek-windows>>>.
- [5] BITTO, Ondřej. *Windows 8: Konečně vychytaný Správce úloh?* [online]. 25. 11. 2011 [cit. 2011-12-07]. Dostupné z: <<http://jnp.zive.cz/windows-8-konecne-vychytany-spravce-uloh>>>.