Windows 2008 R2 PowerShell

Lumír Návrat

Shelly v MS systémech

- COMMAND.COM (DOS, Win 9x)
- CMD.EXE (NT)
  - Základní příkazy, spouštění programů, primitivní skriptování (*.BAT, *.CMD)
- Windows Script Host (*.VBS)
  - Nemožnost interaktivního vykonávání
- PowerShell

Historie PowerShellu

- 2003 – první zmínka
- 2006 v 1.0
  - Volitelně pro XP, 2003, Vista, 2008
- 2009 v 2.0
  - Integrována ve Win7, 2008 R2
  - Dnes volitelně i pro starší verze (XP+)
- 2012 v 3.0 součást Windows Management Framework
  - W7, W2008, W2008R2 a novější
- 2013 v 4.0
  - Spíš aktualizace, podpora Remote debugging
- 2008 Pash
  - Začátek portace pod *NIX systémy v rámci projektu MONO
- 2016 Převedeno pod Open Source

Příkazy PowerShellu

- Cmd-lets [Commandlets]
  - Nativní příkazy, jedná se o .NET třídy
- PowerShell skripty
  - Soubory *.PS1
- PowerShell funkce
- Spustitelné soubory
  - Kompatibilita s „CMD.EXE“ příkazy

- PowerShell není case sensitive

Provideři PowerShellu

- Stromové struktury jsou přístupné přes providery.
  - Není omezení jen na disky, složky, soubory
- Souborový systém
  - Stejně jako jiná příkazová prostředí
  - C: D: E:
- Registry Windows
  - HKLM: HKCU:
- Systémové proměnné
  - Env:
- Proměnné
  - [scope]:jméno

Cmd-lets

- Nativní příkazy (.NET třídy)
- Pevně daná struktura <verb>-<noun>
- Například:
  - Get-Help
  - Get-ChildItem
  - Start-Service
  - Format-Table
  - New-ADUser
  - …
- Doplňování názvů pomocí TAB

Aliasy

- Zástupné názvy pro příkazy
- například: „DIR“ nebo „LS“
  - Jsou aliasy pro Get-ChildItem
- Je možno vytvářet vlastní
  - New-Alias

```
PS C:\> Get-Alias | `
>> Where-Object {$_.Definition -like '*-Object'} | `
>> Format-Table Definition, Name -AutoSize
>>

Definition      Name
----------      ----
Compare-Object  diff
ForEach-Object  foreach
ForEach-Object  %
Group-Object    group
Select-Object   select
Sort-Object     sort
Tee-Object      tee
Where-Object    where
Where-Object    ?
```

```
PS C:\> gal|?{$_.Definition-like'*-ob*'}|ft n*,def* -a
```

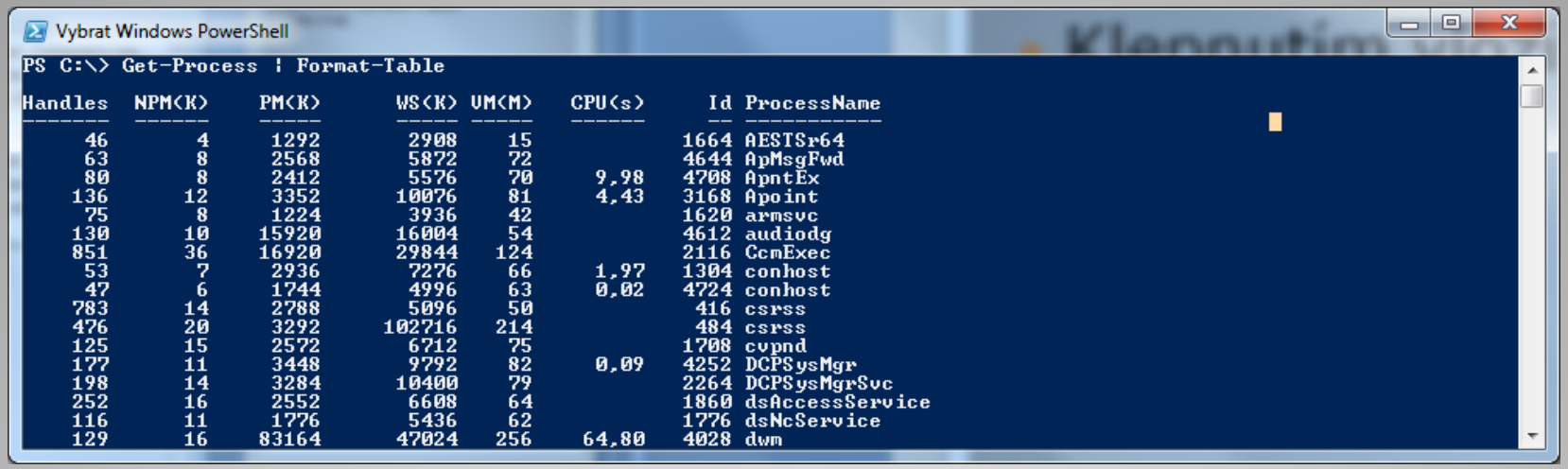
Aliasy (about_aliases)

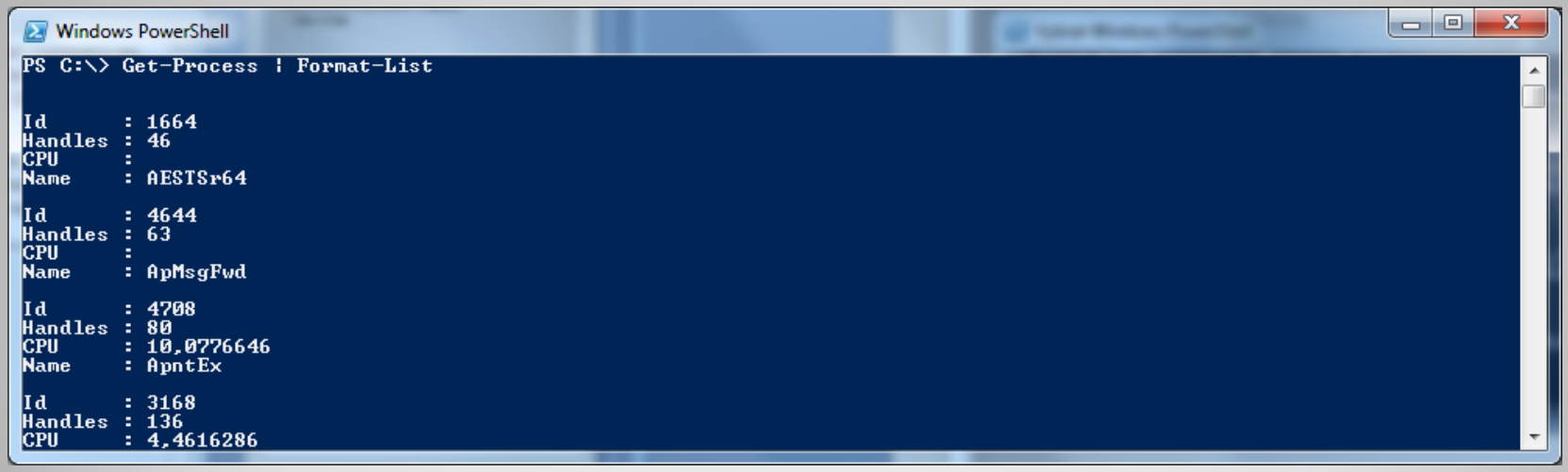
Nápověda

- Jednotná nápověda
- Get-Help
- Příklad použití: Get-Help Get-ChildItem
- Nápověda k nápovědě: Get-Help Get-Help
- 4 úrovně:
  - Základní
  - Detailní (-detailed)
  - Kompletní (-full)
  - Příklady (-examples)

Objektová pipeline

- Předávání dat mezi příkazy pomocí „|“
- Nepředává se text, ale objekty
  - Formátování výstupu je nezávislé
- Get-Process | Sort-Object

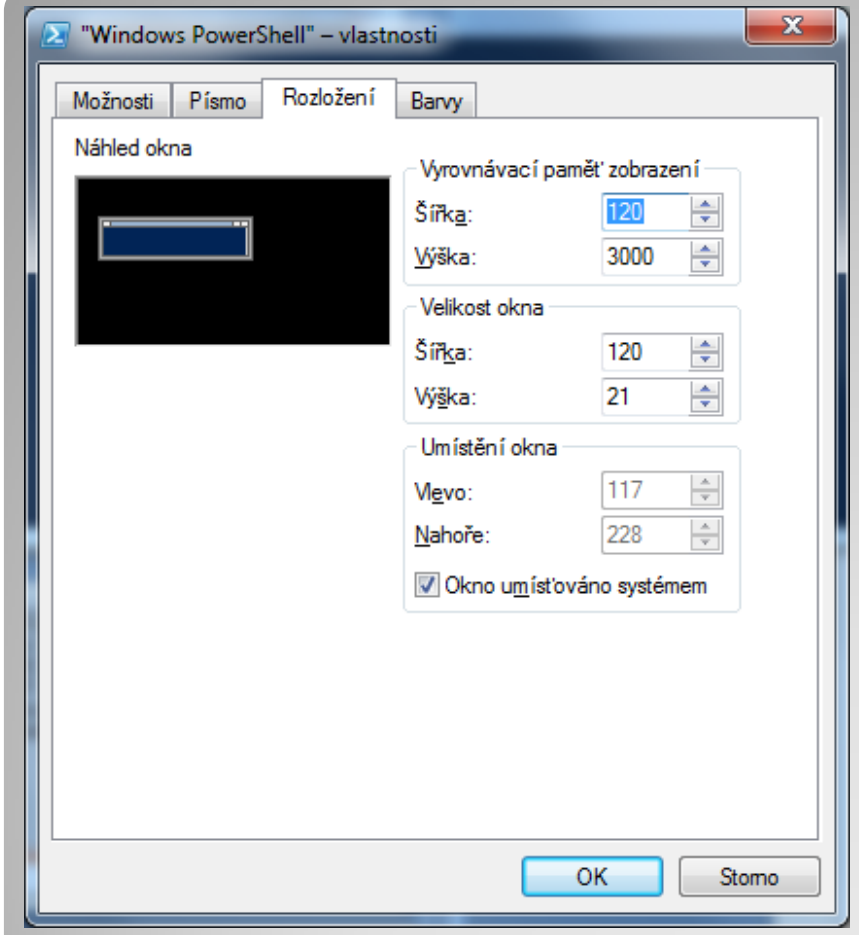




Formátování výstupu

Práce s prostředím

- ↑ ↓ Listování mezi použitými příkazy
- → Naposledy použitý příkaz po zn.
- F3 Naposledy použitý příkaz
- F7 Seznam použitých příkazů
- Esc Vymázání zadaného příkazu
- Tab Doplnění názvu (příkaz, objekt)



- Nastavení paměti zobrazení, může limitovat výstup příkazu
- Další možnosti
  - Režim rychlých úprav
  - Příme označování
  - Copy = Enter
  - Paste = pr.tl. myší

Práce s prostředím

Proměnné (about_variables)

- Syntaxe: $název
- Nedeklarují se
- Bez typové kontroly
- Příklad použití:
  - $cislo = 2

- $_
  - Reprezentuje aktuální objekt v rouře
- $args
  - Parametry příkazu

Filtrování objektů

- Filtrování dle podmínky
  - Where-Object {<podmínka>}
- Operátory (about_Comparison_Operators)
  - -eq … = -gt … > -lt … <
  - -ne … <> -ge … >= -le … <=
  - -and -or -not
  - -like (maska) -match (reg. Výrazy)

Výběr a třídění objektů

- Výběr objektů dle pořadí
  - Select-Object
  - -First, -Last
- Třídění objektů
  - Sort-Object
  - Sort-Object -descending

- Následují příklady

Příklady

Příklady

- Get-Process
  - Vypíše běžící procesy
- Get-Process | Sort-Object WS –Descending
  - Vypíše běžící procesy seřazeny dle využití paměti
- Get-Process | Where-Object { $_.WS -gt 20MB }
  - Vypíše běžící procesy s využitím pamětí větším než 20MB
- Get-Process | Sort-Object Handles -Descending | Select-Object -first 3 | Export-Csv C:\procesy.csv
  - Zapíše do CSV souboru 3 procesy s nejvyšším počtem handles v systému

Příklady

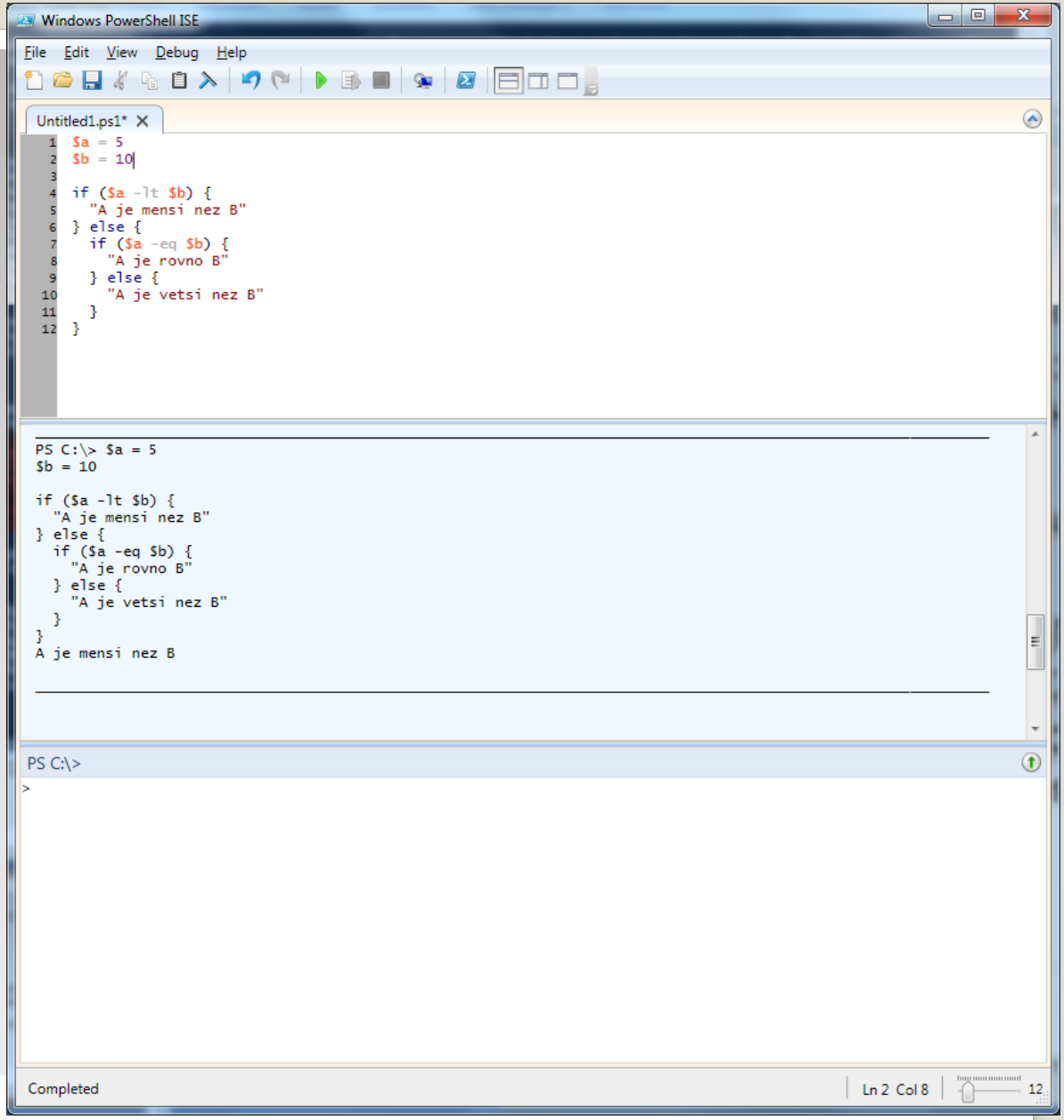
- Get-Service
  - Vypíše služby v systému
- Get-Service | Get-Member
  - Vypíše všechny vlastnosti objektu Service
- Get-Service | Where-Object { $_.displayname -like "*Firewall"} | Stop-Service
  - Zastaví službu, jejíž název končí na „Firewall“

Příklady

- MkDir C:\Tmp
  - Vytvoří složku „Tmp“ na oddíle C:
- Set-Location C:\Tmp
  - Přejde do složky „C:\Tmp“
- CD C:\Tmp
  - Totéž, s využitím aliasu „CD“
- Get-ChildItem C:\Windows -Recurse -Force | Sort-Object length -Descending | Select-Object -first 1
  - Vypíše největší soubor ze složky Windows

Příklady

- Set-Location hklm:
  - Nastaví registr počítače (HKLM) jako providera
- Get-Childitem hklm:
  - Vypíše klíče registru HKLM
- LS hklm:
  - Totéž s využitím aliasu „LS“
- New-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run -name "Kalkulacka" –PropertyType "String" -value "calc.exe„
  - Vytvoří v uvedené cestě novou hodnotu typu String



PowerShell ISE

```
$a = 5
$b = 10

if ($a -lt $b) {
  "A je mensi nez B"
} else {
  if ($a -eq $b) {
    "A je rovno B"
  } else {
    "A je vetsi nez B"
  }
}
```

Příklad základního skriptu

```
PS D:\pracovni\sws\2016-2017> .\skript.ps1
.\skript.ps1 : File D:\pracovni\sws\2016-2017\skript.ps1 cannot be loaded because running scripts is disabled on this s
ystem. For more information, see about_Execution_Policies at http://go.microsoft.com/fwlink/?LinkID=135170.
At line:1 char:1
+ .\skript.ps1
+ ~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
PS D:\pracovni\sws\2016-2017>
```

- **Set-ExecutionPolicy**
  - Restricted, AllSigned, RemoteSigned, Unrestricted

Spouštění skriptu (about_signing)

Zdroje se syntaxí

- http://technet.microsoft.com/en-us/library/ee221100.aspx
- http://technet.microsoft.com/library/dn425048.aspx
- http://blogs.technet.com/b/technetczsk/archive/2009/07/22/serial-windows-powershell-uvod-cast-1.aspx
- http://pechanec.cz/Default.aspx?pageid=7