Command line tools
Scripting

http://www.cs.vsb.cz/navrat

Jan Žák

Agenda

- Useful commands
- WMIC (Windows Management Instrumentation Command-line)
- Windows PowerShell
- Windows Script Host

Skripty ve Windows

.bat (MS-DOS batch file) MS-DOS operating system batch file

.cmd (CMD batch file) > Win 2000

.js (JScript file) Windows script

.vbs (VBScript file) Windows script

.wsf (Windows Script Host file) Container or project file for a Windows script; supported by WSH 2.0 and later.

.wsh (Windows Script Host files) Property file for a script file; supported by WSH 1.0 and later.

Command line tools

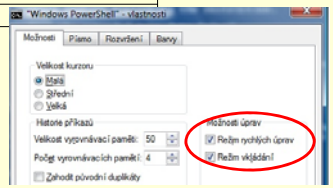
CMD vs. COMMAND

CMD je 32bit interpret, spouští dávky s příponou *.CMD

COMMAND je 16bit interpret (eumulace pomocí ntvdm.exe). Spouští dávky s příponou *.BAT

Command line and PowerShell

Šipka nahoru Šipka dolů	Vyvolání předchozího odeslaného příkazu
F7	Seznam předchozích předchozích příkazů
TAB	Kontextové doplňování příkazů, cest k souborům. Např. „CD PRO <TAB>“ automaticky doplní na „CD Program Files“
ESC	Vymazání celého aktuálního řádku
Ctrl-C	Přerušení běžícího programu



Základní příkazy

- Mkdir (md)
- Rmdir (rd)
- Copy
- Xcopy
- Move
- Rename (ren)
- Del (erase)
- Tree
- Dir
- Cd (+ „:“)
- Subst (subst t: c:\slozka)

Další příkazy

- Attrib (práce s atributy souborů a složek)
- Cacls (práce s příst. právy na NTFS)
- Pushd + popd (zapamatování si složek)
- More (stránkování výpisu
- Sort (třídění)
- Echo (výpis zpráv)
- Color + Title
- Path
- CHCP (!!! změna kódové stránky – důležité např. při importu do AD)
- Find (hledání řetězce)

Další příkazy (pokrač.)

- Start (spouštění programů)
- At (plánované provedení příkazu)
- Print (tisk souboru)
- Net (komplexní nástroj pro práci s uživateli, skupinami, sdílenými složkami...)
- Netsh (konfigurace sítě)
- Systeminfo
- Help ;-)
- ...

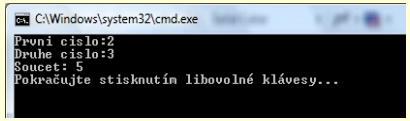
Proměnné

```
@echo off
Set promenna=Ahoj
Echo %promenna%
```

- %CD%
- %DATE%, %TIME%
- %RANDOM (0-32767)
- %ERRORLEVEL%
- %USERNAME%
- %TEMP%, %TMP%
- %PATH% ..

Vstup uživatele do dávky

```
@echo off
Set /p X=Prvni cislo:
Set /p Y=Druhe cislo:
Set /a "V=X+Y"
Echo Soucet: %V%
pause
```



Příkazy používané v dávkách

- Pause (pozastavení běhu)
- Goto (přechod na návěští)
- Call (volání jiné dávky)
- If (podmínečné zpracování)
- Else (rozšíření příkazu IF)
- Rem (komentář)
- For (práce s množinami) (dále For /L, For/F)

Správa objektů v AD

- Dsadd.exe (přidá uživatele, počítač, kontakt, skupinu nebo OU or user to a directory.
- Dsget.exe (zobrazí vybrané atributy)
- Dsmod.exe (modifikuje objekty)
- Dsmove.exe (přesun objektu v rámci domény)
- Dsquery.exe (vyhledá objekty podle kritérií)
- Dsrm.exe (odstraní objekt)
- Ntdsutil.exe (velice mocný nástroj pro práci s databází AD)

Příklady využití DSADD

- dsadd ou OrganizationalUnitDN [-desc Description] [{-s Server | -d Domain}][-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]
- dsadd group GroupDN [-secgrp {yes | no}] [-scope {l | g | u}] [-samid SAMName] [-desc Description] [-memberof Group ...] [-members Member ...] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}]

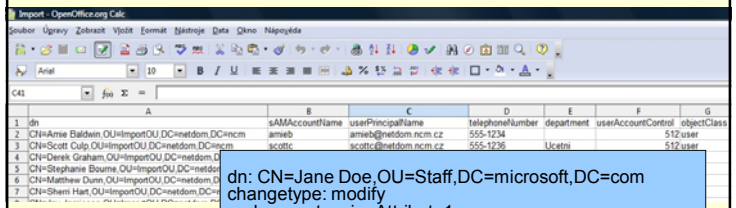
Příklady využití DSADD

- dsadd user UserDN [-samid SAMName] [-upn UPN] [-fn FirstName] [-mi Initial] [-ln LastName] [-display DisplayName] [-empid EmployeeID] [-pwd {Password | *}] [-desc Description] [-memberof Group ...] [-office Office] [-tel PhoneNumber] [-email Email] [-hometel HomePhoneNumber] [-pager PagerNumber] [-mobile CellPhoneNumber] [-fax FaxNumber] [-iptel IPPhoneNumber] [-webpg WebPage] [-title Title] [-dept Department] [-company Company] [-mgr Manager] [-hmdir HomeDirectory] [-hmdrv DriveLetter:][-profile ProfilePath] [-loscr ScriptPath] [-mustchpwd {yes | no}] [-canchpwd {yes | no}] [-reversiblepwd {yes | no}] [-pwdneverexpires {yes | no}] [-acctexpires NumberOfDays] [-disabled {yes | no}] [{-s Server | -d Domain}] [-u UserName] [-p {Password | *}] [-q] [{-uc | -uco | -uci}

Hromadný import uživatelů

- Dávky obsahujících DSADD, NET USER
- Skriptovací jazyky (WSH, JS, VB...)
- Csvde.exe (import/export objektů z/do AD)
- Ldifde.exe (import/export objektů z/do AD, modifikace objektů, rozšiřování schématu AD

Příklady využití CSVDE, LDIFDE




```
dn: CN=Jane Doe,OU=Staff,DC=microsoft,DC=com
changetype: modify
replace: extensionAttribute1
extensionAttribute1: Staff
-

dn: CN=John Doe,OU=Staff,DC=microsoft,DC=com
changetype: modify
replace: extensionAttribute1
extensionAttribute1: Staff
```

```
ldifde -f exportOu.ldf -s Server1 -d "dc=Export,dc=com" -p subtree
  -r "(objectCategory=organizationalUnit)" -l "cn,objectclass,ou"
```


Windows PowerShell

PS

Windows PowerShell (dříve známý jako Microsoft Shell, MSH či pod kódovým označením Monad) je rozšiřitelný shell se skriptovacím jazykem od společnosti Microsoft. Produkt je založen na objektově orientovaném programování a .NET Frameworku.

Shell je k dispozici volně ke stažení ve verzi 1.0 pro operační systémy Windows XP a vyšší. Pro svuj chod potřebuje .NET Framework 2.0.

Verze 2.0 momentálně v beta verzi.

PS

Windows PowerShell obsahuje cca 130 nástrojů pro správu systému.

Jeho možnosti je možné využít např. Pro správu Exchange Server 2007, System Center Operations Manager 2007, System Center Data Protection Manager V2, and System Center Virtual Machine Manager...

PS - po instalaci

%SYSTEMROOT%\System32\WindowsPowerShell
Nástroj je tedy možné spustit jednoduše pomocí příkazu
powershell.exe

(Skripty mohou být zakázány – viz
get-help about_signing)

PS

PowerShell můžete používat místo CMD (příkazy CD, IPCONFIG...), pozor ale na nový způsob práce se systémovými proměnnými:

%username% --> $env:username
%systemroot% --> $env:systemroot

PS - přesměrování výstupu

C:\Users\User\Desktop>ipconfig >ip.txt
vypíše konfiguraci do souboru ip.txt
C:\Users\User\Desktop>netstat >ip.txt
přepíše soubor ip.txt výstupem
C:\Users\User\Desktop>netstat >>ip.txt
doplní informace na konec souboru

Tip: sort < c:\soubor.txt > c:\soubor2.txt

PS - roury (PIPES)

Roury umožní přesměrovat výstup jednoho programu na vstup programu druhého:

TASKLIST | more (výpis se „zastaví“ po zaplnění obrazovky)
TASKLIST | sort (výpis bude seřazen abecedně)
NETSTAT -ano | findstr ":80" (zobrazí pouze řádky obsahující „:80“)

PS - typy příkazů

- běžné *.EXE programy (například IPCONFIG)
- příkazy **CMDLET** uloženy v *.DLL (například GET-PROCESS, GET-CHILDITEM)
- Aliasy - zkrácená jména nahrazující nějaké komplikovanější jméno příkazu (například DIR). Později se naučíme nějaký vytvořit
- Funkce - pojmenované skupiny příkazů.

PS - typy příkazů - pokračování

get-command ipconfig | fl
get-command get-process | fl
get-command get-children | fl
get-command dir | fl
get-command help | fl

(příkazy zjistí zda se jedná o cmdlet, exe...
fl mění formátování vystupu)

PS - další parametry

"" - Uvozovky
" - Apostrof
`` - Opačný apostrof
`n - Konec řádku (new line)
`t - Tab
`$ - Znak dolaru

ECHO "Hracka`tCena `nMic`t`20" > test.txt
type test.txt
Hracka Cena
Mic 20

PS - profil uživatele

•Profile.ps1 pro konkrétního uživatele nebo pro všechny uživatele:

function ffrun { & "$Env:ProgramFiles\\Mozilla Firefox\\firefox.exe" }

• další možností je vytvoření PSDrive (chová se jako disk):

New-PSDrive desktop FileSystem $([Environment]::GetFolderPath('Desktop'))

ii desktop (Invoke-Item – otevře plochu v Průzkumníkovi)

Další příkazy PowerShellu

Get-Location, pwd - zjistí aktuální adresář.

Invoke-Item xxx, ii xxx -spustí soubor, popř spustí průzkumníka v případě adresáře.

Set-ExecutionPolicy RemoteSigned - důležitý příkaz, který vám umožní spouštět vámi vytvořené skripty.

Get-Process xxx, gps, ps - bez parametru vypíše všechny procesy. S parametrem vypíše číslo procesu a další informace.

Get-Service xxx, gsv -stejné jako Get-Process, akorát pro services.

Get-History, ghy, h, history -vypíše historii příkazů a skriptů

Get-Time - vypíše datum a čas

Get-Locale - vypíše locale

Get-Command - vypíše přehled všech cmdletů

Invoke-Expression xxx, iex, & - spouštění ps skriptů

WMIC
(Windows Management Instrumentation Command-line)

WMIC

Nástroj WMIC poskytuje jednoduché rozhraní příkazového řádku pro službu WMI (Windows Management Instrumentation), které umožňuje využívat službu WMI ke správě počítačů se systémy řady Windows.

Nástroj WMIC spolupracuje se stávajícími příkazy nástrojů a prostředí a lze jej snadno rozšířit pomocí skriptů a dalších aplikací zaměřených na správu.

Příklady WMIC

Wmic process list brief (výpis seznamu procesů)

Wmic process get name (výpis pouze se jmény)

Wmic process where „name='explorer.exe'“ call terminate (ukončení procesu explorer.exe)

Wmic process where „name like ‚e%'“ get name (procesy začínající na „e“)

Wmic process call create „calc.exe“ (spuštění procesu)

Wmic service list brief (seznam běžících služeb)

Wmic service get Name, DisplayName (seznam služeb – dlouhé názvy)

Příklady WMIC

Wmic service list brief /format:hform > c:\sluzby.htm (výpis služeb do souboru html)

Wmic service Alerter Call StartService (spuštění služby alerter

Wmic os call reboot (restart PC)

Wmic /node:PC01 os call shutdown (vypnutí PC01)

Wmic baseboard get Product (id zákl. Desky)

Wmic Product get name (výpis nainst. SW)

wmic logicaldisk where drivetype=3 get name, freespace, systemname, filesystem, size, volumeserialnumber (výpis log. disků)

WSH

WSH

WSH vytváří prostředí pro spouštění skriptů – vytváří objekty a služby použitelné pro skripty, zároveň zajišťuje zabezpečení a spustí potřebny engine pro vykonání skritpu.

WSH objekty a služby

- Tisk hlášení na obrazovku
- Spouštění základních funkcí jako např. **CreateObject** a **GetObject**
- Připojování síťových disků
- Připojování tiskáren
- Čtení a vytváření proměnných
- Správa registrů

WSH - Hello World

WScript.Echo("Hello World!");

Soubor uložte jako „Hello.js“

WSH - vytvoření uživatele v AD

```
strContainer = ""
strName = "EzAdUser"
'*        Connect to a container              *
Set objRootDSE = GetObject("LDAP://rootDSE")
If strContainer = "" Then
  Set objContainer = GetObject("LDAP://" & _
    objRootDSE.Get("defaultNamingContext"))
Else
  Set objContainer = GetObject("LDAP://" & strContainer & "," & _
    objRootDSE.Get("defaultNamingContext"))
End If
'*      End connect to a container           *
Set objUser = objContainer.Create("user", "cn=" & strName)
objUser.Put "sAMAccountName", strName
objUser.SetInfo
```


Zdroje informací

http://www.microsoft.com/cze/windowsserver2008/features/powershell.aspx
http://cs.wikipedia.org/wiki/Windows_PowerShell
http://jakubgarfield.wordpress.com/2007/07/01/powershell-mocny-nastupce-prikazove-radky/
http://www.sevecek.com/index.php?id=23

http://technet2.microsoft.com/WindowsServer/cs/Library/68d1ebd3-a65a-46eb-9c44-e9bd836d253c1029.mspx?mfr=true
http://blogs.technet.com/jhoward/archive/2005/02/23/378726.aspx
http://hps.mallat.cz/view.php?cisloclanku=2004121601

http://msdn2.microsoft.com/en-us/library/9bbdkx3k.aspx
http://msdn2.microsoft.com/en-us/library/ms950396.aspx
http://en.wikipedia.org/wiki/Windows_Script_Host

http://technet2.microsoft.com/WindowsServer/cs/Library/68d1ebd3-a65a-46eb-9c44-e9bd836d253c1029.mspx?mfr=true
http://hps.mallat.cz/view.php?cisloclanku=2004121601
http://blogs.technet.com/jhoward/archive/2005/02/23/378726.aspx