Ing. Lubomír Ošmera

MCT, MCSE: Cloud Platform and infrastructure

Tipy a triky pro administrátory Windows, nejen v PowerShellu

OSMERA@LUBOMIROSMERA.CZ

Osnova

- PowerShell - Syntaxe, stavební kameny, …
- Powershell vs. Cmd – staré příkazy novým a efektivnějším způsobem
- PowerShell v akci – běžné a méně běžné úlohy admina pomocí Powershell a cmd
- Kde se bez Powershellu neobejdeme a kde je lepší užít konzoli
- Remoting, Security, Scheduled Powershell tasks, jednoduché skripty

Cíle:

- naučit se alternativním způsobům administrace Windows, víc být kamarád s PS
- Objevit nové možnosti, sadu zajímavých příkazů
- K automatizaci a zjednodušení práce není zapotřebí skriptů o desítkách řádků, kouzla dokáží i párřádkové příkazy

Základy syntaxe, jak pracovat v PowerShellu

- Verb
  - Add
  - Set
  - Remove
  - New
  - Get
  - …

+

- Object:
  - Process
  - Service
  - ADUSER
  - ADGROUP
  - …

Základy syntaxe, jak pracovat v PowerShellu

- PREDNASKAWUG2019.ps1

Staré záležitosti moderními způsoby

- Systeminfo.ps1

Přidávání, odebírání rolí v Powershell

- Jak přidávat role rychleji bez klikání
- Jak dlouho trvá přidání role ve wizardu vs. v powershellu
- Activedirectory.ps1

Active Directory

- Adcommands.ps1
- DELETE_adusercomplet.ps1
- Přidaní userů z csv

Group Policy konzole

- Jsou Group Policies zdravé?
- Filtry administrative templates v grafické konzoli
- Permissions read for user

Wmi filtry

- ProductType="1" -> Client operating systems
- ProductType="2" -> Domain controllers
- ProductType="3" -> Servers that are not domain controllers

- 1703:
  select Version from Win32_OperatingSystem WHERE Version like "10.0.15063" AND ProductType="1" AND OSArchitecture = "64-bit"

- 8.1 – Version like "6.3%" 8.0 - Version like "6.2%" 7.0 - Version like "6.3%"

Performance countery

- Perfmon.ps1

Hyper-V

- Příklad, kde je PowerShell nezbytný?
- Hyper-V.ps1

Bezpečnost Windows Powershell

Spouštení skriptů – dá se vůbec omezit

- Powershell.exe -ExecutionPolicy ByPass
- SET-EXECUTIONPOLICY –Executionpolicy unrestrictred –scope process

- powershell jea
- Applocker

Bezpečnost PS - CREDENTIALS

- Security_credentials.ps1

Vzdálené ovládání - Remoting

- WSMAN – protokol, WINRM - služba
- 5985 (HTTP), 5986 (HTTPS)
- Kerberos autentizace
- DEFAULT HTTP, používá se AES256

Vzdálené ovládání - PSRemoting

Enter-pssession –computername <…>

Invoke-command –computername <…> -scriptblock {…;…;…}

Invoke-command –computername <…> -scriptblock {…;…;…} –asjob

Invoke-command –computername <…> -filepath .\script.ps1

Zapnutí remotingu

- Enable-psremoting
- Hromadně
  - Gpo
    - **Computer Configuration >Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service**
  - Winrm service automaticky
  - Firewall pravidla

Remoting a BPA

- Troubleshooting.ps1

Certifikační autorita

- Pkiview.msc
- Velmi zajímavé powershell commands spíše z externích zdrojů <*https://www.sysadmins.lv/projects/pspki/Set-CRLValidityPeriod.aspx*>

Konzole MMC

- https://www.dell.com/support/article/cz/cs/czdhs1/sln290582/common-microsoft-management-consoles-mmc-for-managing-windows-servers?lang=en

- Dsa.msc
- Mstsc.exe
- gpmc
- Ncpa.cpl