

Ing. Lubomír Ošmera
MCT, MCSE, CCNA, CEH

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, wmi, 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
- FIREWALL.PS1

Přidávání, odebírání rolí v Powershell

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

Active Directory

- Adcommands.ps1
- Přidání userů z csv: Aduserfull.ps1

Group Policy konzole

- adcommands.ps1
- Backup: <https://social.technet.microsoft.com/Forums/en-US/3919f85e-7ba1-4e4b-9e82-66b42ad508c4/group-policy-link-backup?forum=winserverDS>

Hyper-V

- Příklad, kde je PowerShell nezbytný – configuration version
- Hyper-V.ps1

Scheduled tasks

- Scheduledtasks.ps1

Bezpečnost Windows Powershell

Spouštění skriptů – dá se vůbec omezit?

- Powershell.exe -ExecutionPolicy unrestricted
- SET-EXECUTIONPOLICY –Executionpolicy unrestricted –scope process

Příklad řešení ochrany před spouštěním skriptů

- powershell jea
- Applocker

Bezpečnost PS - CREDENTIALS

- Security_credentials.ps1

Vzdálené ovládání - Remoting

- Remoting je název specifické funkce která užívá speciické služby a protokol
- Nejedná se o každý příkaz, který má parametr –computername (get-process – remote registry service, wmi – rpc)
- WSMAN – protokol, WINRM - služba
- 5985 (HTTP), 5986 (HTTPS)
- Kerberos autentizace
- DEFAULT HTTP, používá se AES256

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.ps1

Vzdálené ovládání - PSRemoting

`Enter-pssession -computername <...>`

`Invoke-command -computername <...> -scriptblock {...;...;...}`

`Invoke-command -computername <...> -scriptblock {...;...;...} -asjob`

`Invoke-command -computername <...> -filepath .\script.ps1`

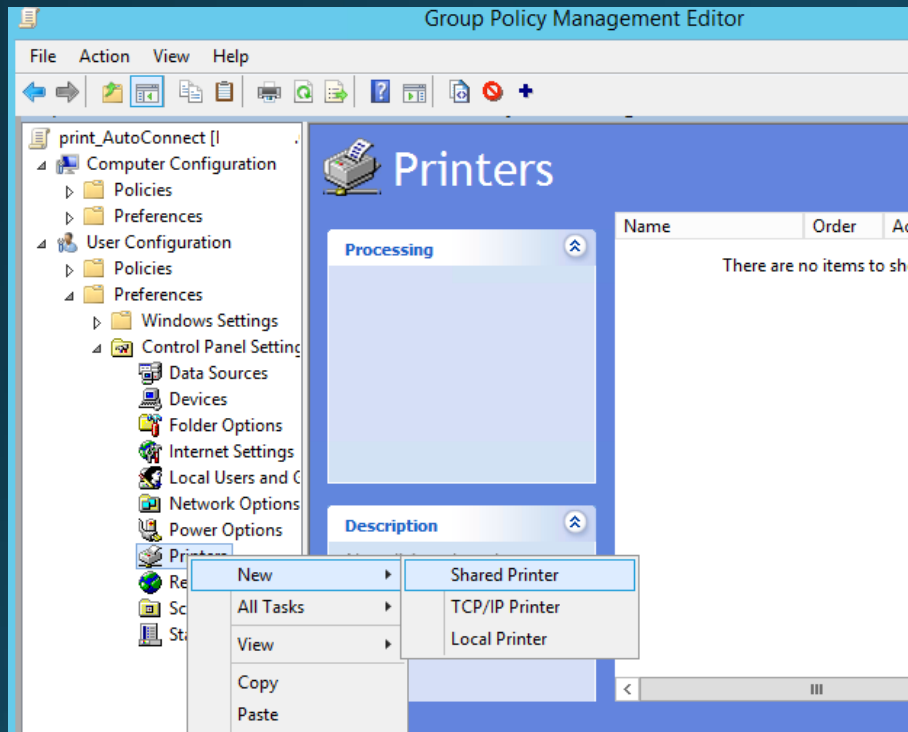
WMI

- Lokální admin na remote pc
- Windows management instrumentation (wmi) firewall pravidlo

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%"

Remoting a tiskárny – problém s ovladači



User Configuration - Policy - Administrative Templates - Control Panel - Printers - Printer - Point and Print Restriction

User Configuration - Policies - Administrative Templates - Control Panel - Printers

Azure Ad connect troubleshooting

- Azurerepair.ps1

Kontakt

- https://lubomirosmerna.cz/?page_id=985
- <https://cz.linkedin.com/in/lubomirosmerna>
- osmerna@lubomirosmerna.cz