Group Policy od A do Z

Lukáš Brázda | MCT, MCSA, MCSE | lukas@brazda.org

OBSAH

- Úvod
- Správa GPO objektů
- Správa vnitřků GPO
- Troubleshooting
- Co když GPO nestačí?

1) Úvod

PROČ GPO?

- Workgroup – změny nastavení provádíte ručně na jednotlivých PC
  - Tvorba účtů uživatelů, resety hesel
  - Stejně tak, nastavování firewallů, kvality hesel, certifikátů, mapování jednotek nebo tiskáren…

- AD doména
  - Centrální správa uživatelských účtů
  - Možnost použití GPO jako centrálního nástroje pro nastavení počítačů i uživatelů

CO GPO UMÍ?

- Změna nastavení PC nebo OS
- Změna nastavení uživatele
- Spouštění skriptů
- Instalace SW
- Mapování disků / tiskáren
- Atp.

- Jednotlivostí, co umějí GPO nastavovat jsou řádově tisíce (jen Administrative Templates obsahují dohromady asi 3500 položek nastavení)

POLITIKY OBECNĚ

- Lokální
  - C:\Windows\System32\GroupPolicy
  - Od Windows Vista existuje více lokálních politik
  - GPEdit.msc
  - MMC.exe + Snap-in

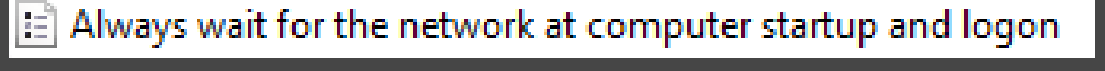
- Doménové
  - Uložené částečně v databázi AD a v adresáři SYSVOL
  - Group Policy Management Konzole (GPMC)
  - Group Policy Manahement Editor (GPME)

KDY SE POLITIKY APLIKUJÍ?

- Lokální
  - Okamžitě
- Doménové
  - Start počítače / přihlášení uživatele
  - Refresh intervaly 90 až 120 minut (DC mají refresh 5 minut)
  - Ruční vynucení (GPUpdate, Invoke-GPUpdate)
  - Security CSE aplikuje každých 16h (i když se nic nezměnilo)
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
    - MaxNoGPOListChangesInterval

ZPŮSOBY APLIKOVÁNÍ POLITIKY

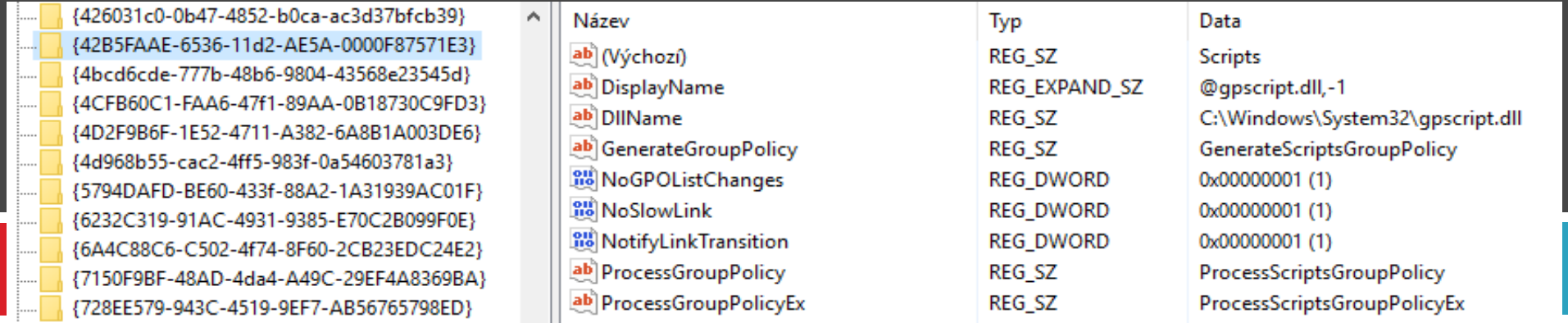
- Background vs. Foreground
  - Některá GPO nastavení se aplikují pouze při startu PC / přihlášení uživatele
  - Toto platí i pro některé Preferences (různé podle verze OS)

- Synchronous vs. Asynchronous
  - Podle toho, jestli Windows čekají na aplikování GPO než uživatele nechají přihlásit
  - Modifikace chování: 

  - Typicky instalace SW se aplikují pouze v režimu Foreground + Synchronous

KDO POLITIKY APLIKUJE?

- Nikdo nikam nic netlačí
- GPO si stahují klienti a servery samy z DC (z adresáře SYSVOL)
- Na klientech služba Group Policy Client
- Aplikování provádí CSE (Client Side Extensions)
- Seznam CSE v registrech:
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions



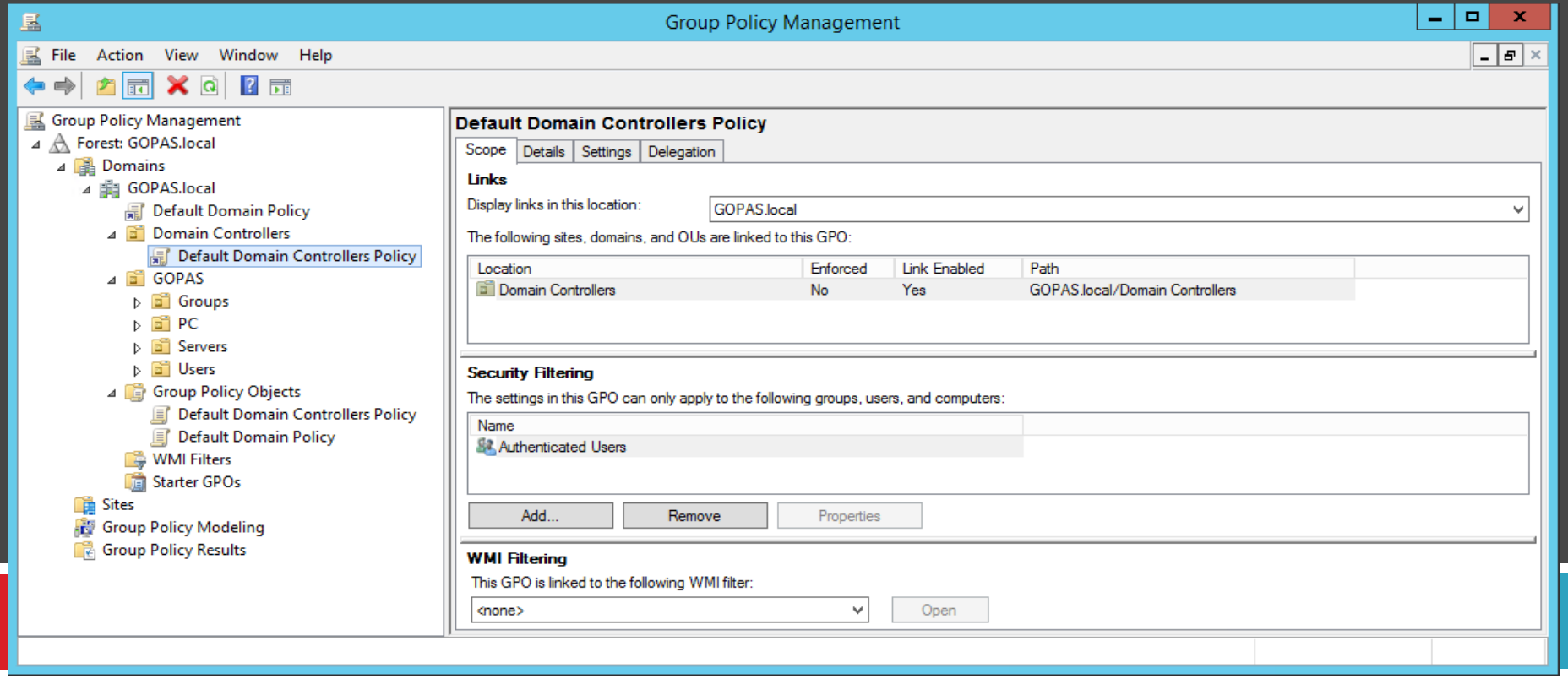
GPO MÁ DVĚ ČÁSTI

- Container (obecné info o GPO)
  - Objekt v AD
  - Atributy: versionNumber, gPCFileSysPath, gPCWQLFilter
  - Replikuje se spolu s databází AD
- Template (co GPO nastavuje a jak)
  - Adresář v SYSVOL
  - GPT.ini
  - Registry.pol
  - Replikuje FRS nebo DFS (WS2016 už nepodporuje FRS)
- Dvě různé replikační technologie mohou způsobovat inkonzistence v GPO

2) Správa GPO objektů

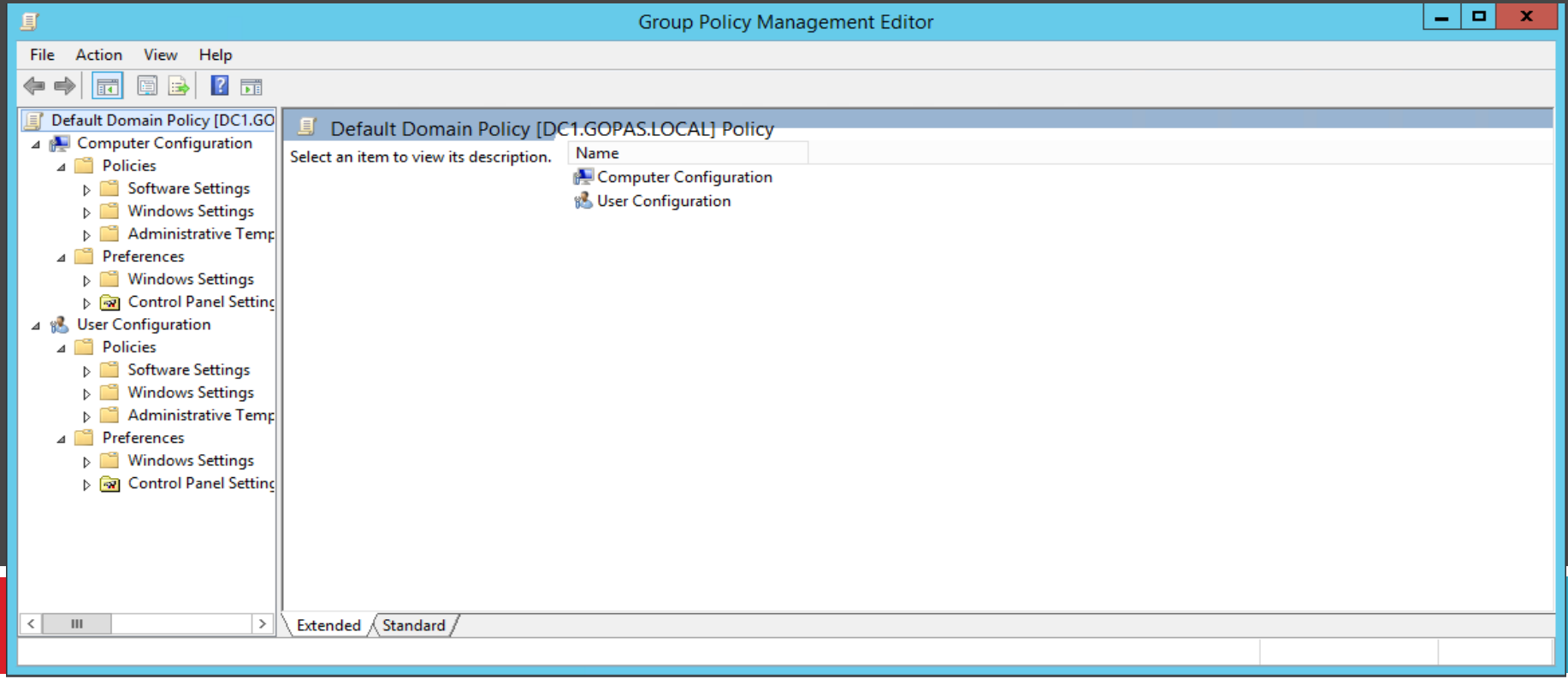
SPRÁVA OBJEKTŮ GPO

- Group Policy Management Console (GPMC)



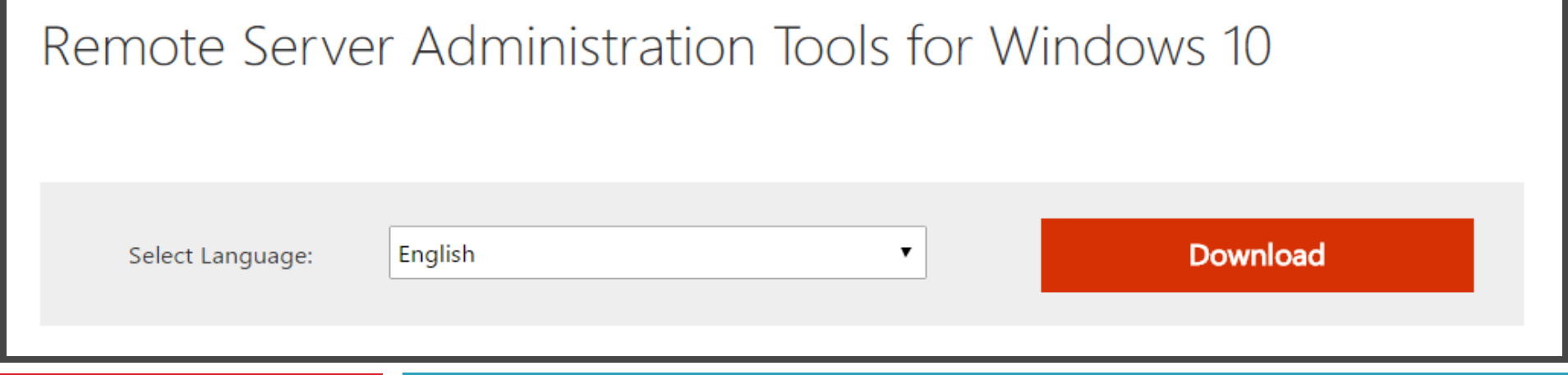
SPRÁVA „VNITŘKŮ“ GPO

- Group Policy Management Editor



SPRÁVA GPO Z KLIENTSKÉHO OS

- Remote Server Administration Tools (RSAT)
  - Windows 7 SP1: https://www.microsoft.com/en-US/download/details.aspx?id=7887
  - Windows 8.1: https://www.microsoft.com/en-US/download/details.aspx?id=39296
  - Windows 10: https://www.microsoft.com/en-us/download/details.aspx?id=45520



ADVANCED GPMC

- Separátní konzola od MS
- Součástí placeného produktu MDOP
- Rozšiřuje funkčnost vestavěné GPMC o:
  - Automatické verzování GPO
  - Snadné obnovy a porovnání různých verzí jedné GPO
  - Delegovací a schvalovací model
  - Ne-editování GPO „zaživa“

VÝCHOZÍ DOMÉNOVÉ GPO

- Default Domain Policy
  - Politiky na hesla
  - Vlastnosti Kerberos protokolu
  - Nastavení EFS Recovery Agenta
  - atd.
- Default Domain Controllers Policy
  - User Rights Assigments
  - Nastavení Auditování
  - atd.
- Restore pomocí DCGPOFix.exe
  - https://technet.microsoft.com/en-us/library/hh875588(v=ws.11).aspx

KAM LZE GPO APLIKOVAT?

- GPO lze navázat na:
  - AD Site (ve výchozím stavu se nezobrazují)
  - AD Domain
  - AD Organizational Unit

- GPO nelze navázat přímo na:
  - Uživatele
  - Počítač
  - Skupinu
  - Systémové kontejnery

KAM LZE GPO APLIKOVAT?

- V GPMC je vidět strom AD
- Nejsou zde ale vidět některé objekty, které v AD vidět jsou:
  - Built-in
  - Computers
  - Users
  - atd.

- Změna výchozího OU pro uživatele a počítače:
  - Redircmp.exe DN
  - Redirusr.exe DN

GPMC: DEMO

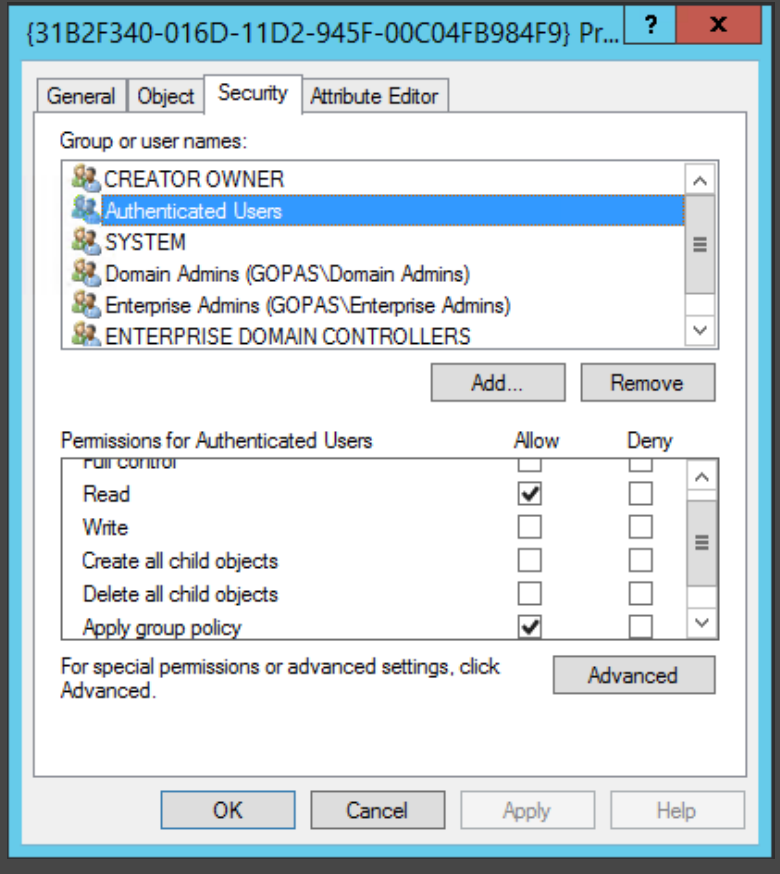
APLIKOVÁNÍ GPO

- Objekt GPO může v AD jen existovat a neaplikovat se
- Všechny GPO najdete v kontejneru Group Policy Objects
- Pro aplikaci je třeba vytvořit GPO Link
- GPO Link:
  - Vazba mezi objektem GPO a objektem v AD
  - Jedna GPO může mít více linků
  - Link enabled / disabled
  - Parametr enforced
  - Smazání linku nesmaže celý objekt GPO

SECURITY FILTERING

- GPO nelze navázat přímo na uživatele
- Filtrovat lze podle uživatele, počítače, skupiny
- Oprávnění Allow / Deny
- Pro aplikování GPO:
  - Read
  - Apply Group Policy

- GPMC – Delegation – Adanced
- ADUC, ADSIEdit



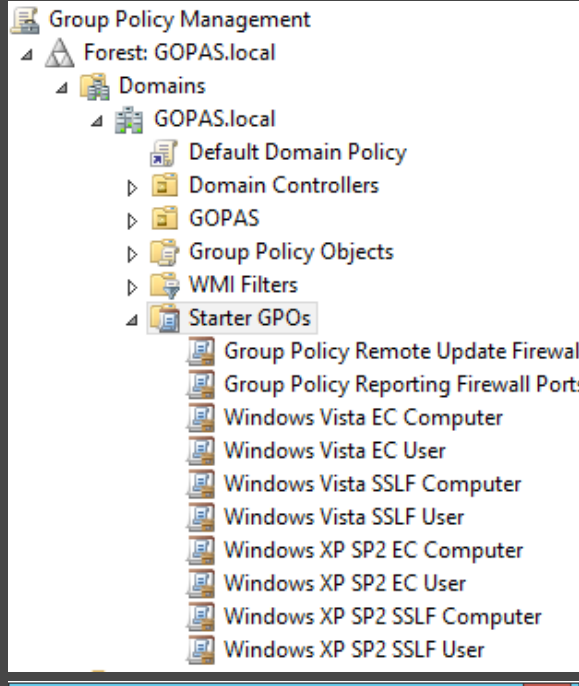
WMI FILTERING

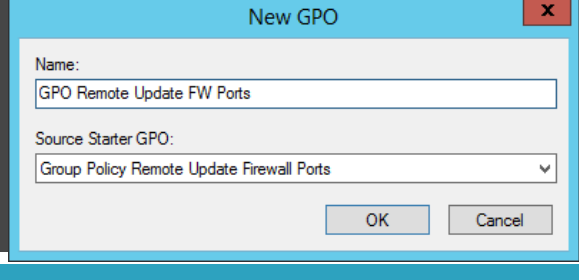
- Ne vždy vyhovuje filtrovat podle skupiny nebo uživatele
- Nástroje:
  - MSInfo32.exe
  - WMICodeCreator – https://www.microsoft.com/en-us/download/details.aspx?id=8572
  - Get-WMIObject Win32_OperatingSystem | FL *
  - Get-CIMInstance
- Příklady:

```
Select * from Win32_OperatingSystem where Caption = "Microsoft Windows 10 Pro"
Select * from Win32_ComputerSystem where Manufacturer = "Dell" and Model = "XPS 13" or Model = "XPS 12"
```

STARTER GPO

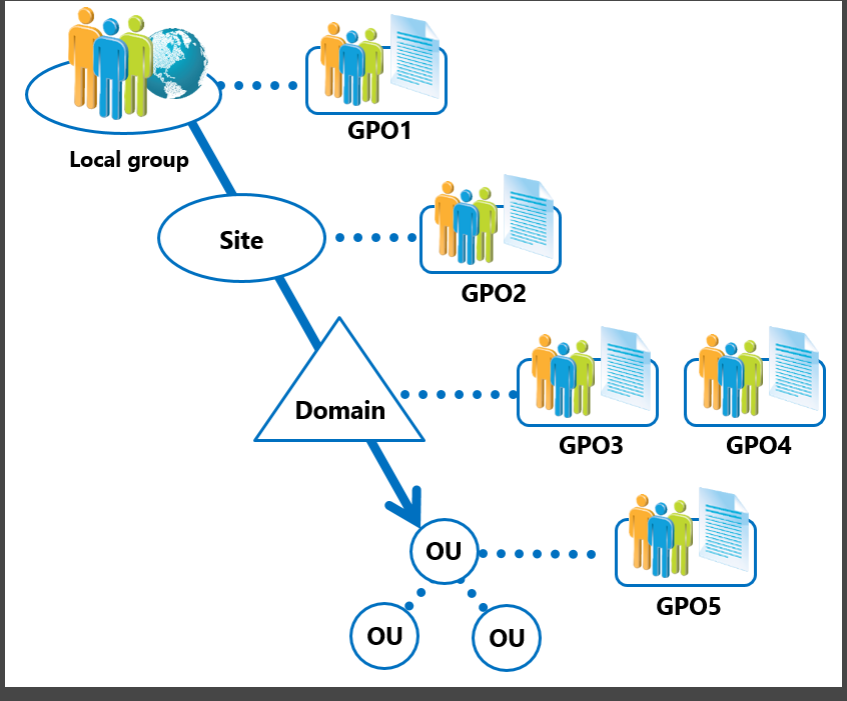
- Předkonfigurované GPO
- Export / import z *.cab souborů
- Na jejich základě lze tvořit nové GPO objekty





POŘADÍ APLIKOVÁNÍ POLITIK

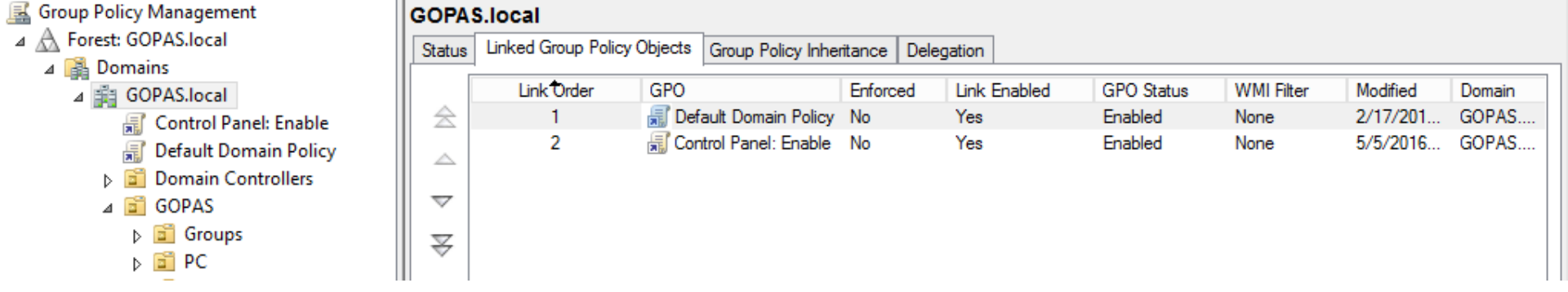
- Lokální politiky
  1. Local GPO
  2. Administrator / Non-Administrator GPO
  3. Local User Specific GPO
- Doménové GPO
  1. AD Site GPO
  2. AD Domain GPO
  3. AD Organizational Unit GPO



- V případě konfliktu má prioritu později aplikovaná politika

VÍCE GPO NA JEDNOM AD OBJEKTU?

- Jak určovat prioritu více GPO např. na OU?
- Záložka Linked GPO
- Posuvníky
- Link Order není pořadí, ale PRIORITA
- Nižší číslo = vyšší priorita = jakoby pozdější aplikování



DĚDIČNOST GPO + ENFORCED GPO

- Stejně jako na file systemu i v GPO funguje dědičnost
- Tzn. GPO aplikovaná na doménu se stejně prodědí na podřízené objekty
- Dědí se i do ne-OU kontejnerů (Built-in, Computers, Users)
- Dědičnost lze blokovat na úrovni OU

- Parametr Enforced na GPO Linku:
  - Ignoruje blokování dědičnosti
  - V případě konfliktu má prioritu „vynucená“ GPO

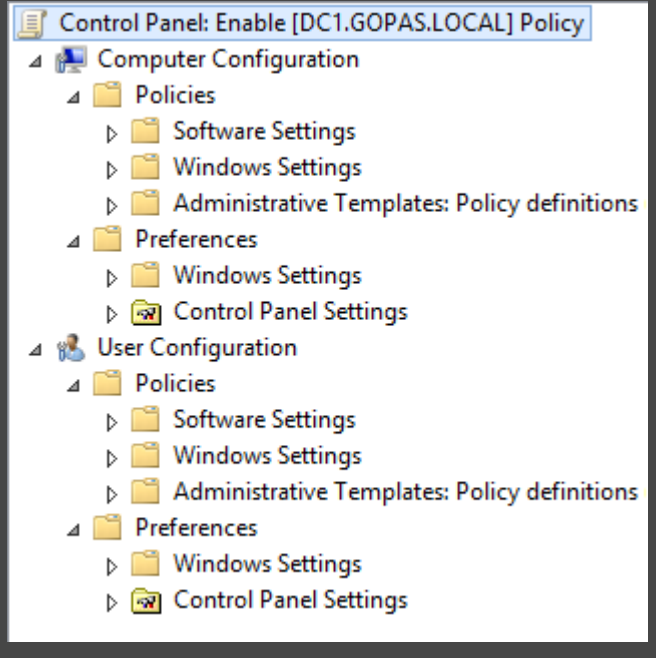
OPERACE S GPO OBJEKTY

- Záloha
- Obnova
- Kopírování
- Import
- Migrace mezi AD + Migration Table
- Automatizace:
  - Get-Command –Module GroupPolicy
  - GPMS Scripting Samples: https://msdn.microsoft.com/en-us/library/aa814151(v=vs.85).aspx
  - MS Scripting Center: https://gallery.technet.microsoft.com/scriptcenter

3) Správa vnitřků GPO

GROUP POLICY MANAGEMENT EDITOR

- Uvnitř GPO vždy dvě větve:
  - User Configuration
  - Computer Configuration
- Tyto se dále větví na:
  - Policies
  - Preferences
- Pozor na správné cílení GPO
- PC si neumí aplikovat User větev a obráceně!

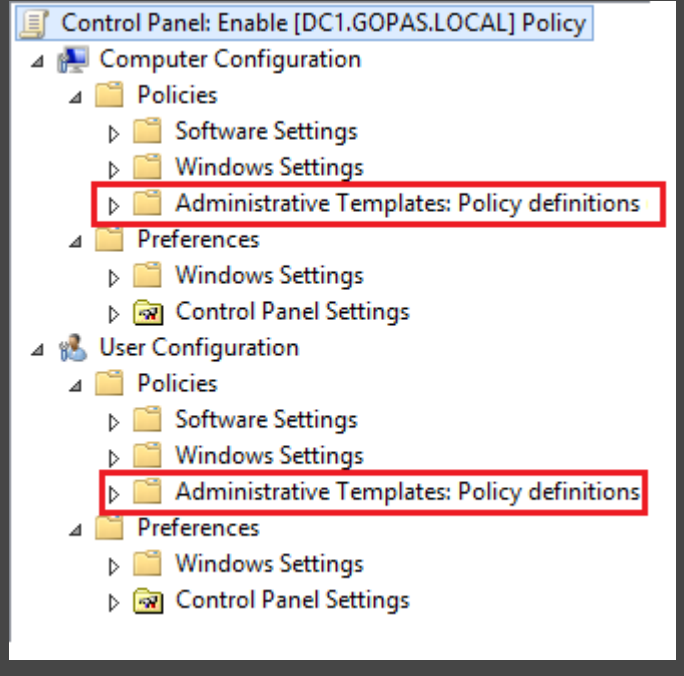


LOOPBACK PROCESSING

- Speciální režim aplikování GPO
- Typicky v situaci když:
  - Potřebujete ovlivnit nastavení uživatele pouze, když se přihlašuje na konkrétní PC / Server
  - Klasická situace s terminálovými (RDS) službami
- Vytváříte GPO cílenou na PC, ale editujete v ní User větev
- Loopback chování třeba explicitně zapnout
- Dva režimy:
  - Merge
  - Replace

ADMINISTRATIVE TEMPLATES

- Nastavení definována v ADMX souborech
- C:\Windows\PolicyDefinitions
- K nim existuje ADML jazyková definice
- V ADMX souboru je uvedeno:
  - Která část registrů se má editovat a jak
- Jsou rozšiřitelné o další ADMX soubory
  - Office 2013 / 2016 Templates
- Dá se v nich fulltextově filtrovat



CENTRAL STORE

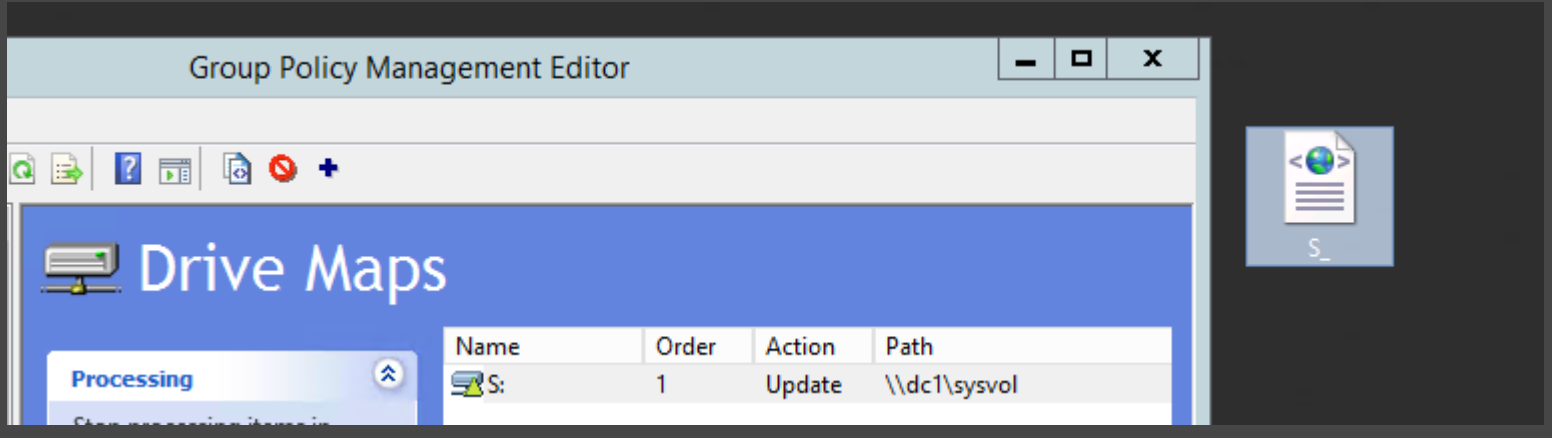
- Pokud si ADMX soubory nahrajete do jednoho DC, ostatní DC je „neuvidí“
- Využijeme toho, že se SYSVOL replikuje mezi DC
- Adresář PolicyDefinitions nakopírujeme do SYSVOLu:
  - C:\Windows\SYSVOL\sysvol\{Domain Name}\Policies

- GPME hledá ADMX soubory nejprve v Central Storu
- Nové ADMX soubory tedy kopírujte přímo do Central Storu

GROUP POLICY PREFERENCES

- Vytvářet jen ve WS2008+ a Vista+
- Jsou jen v doménových GPO
- Jde o nastavení, která se dříve nastavovat přes GPO nedala nebo se dělala blbě :-)
- Nabízejí akce Create, Delete, Replace, Update
- Volitelně se provádějí pod účtem SYSTÉM nebo v kontextu uživatele
- Volitelně se dají aplikovat pouze jedenkrát (tedy ne při refresh intervalech)
- Item-Level Targeting
- Klávesy F5 – F8 pro selektivní nastavení

GPP: DRAG AND DROP

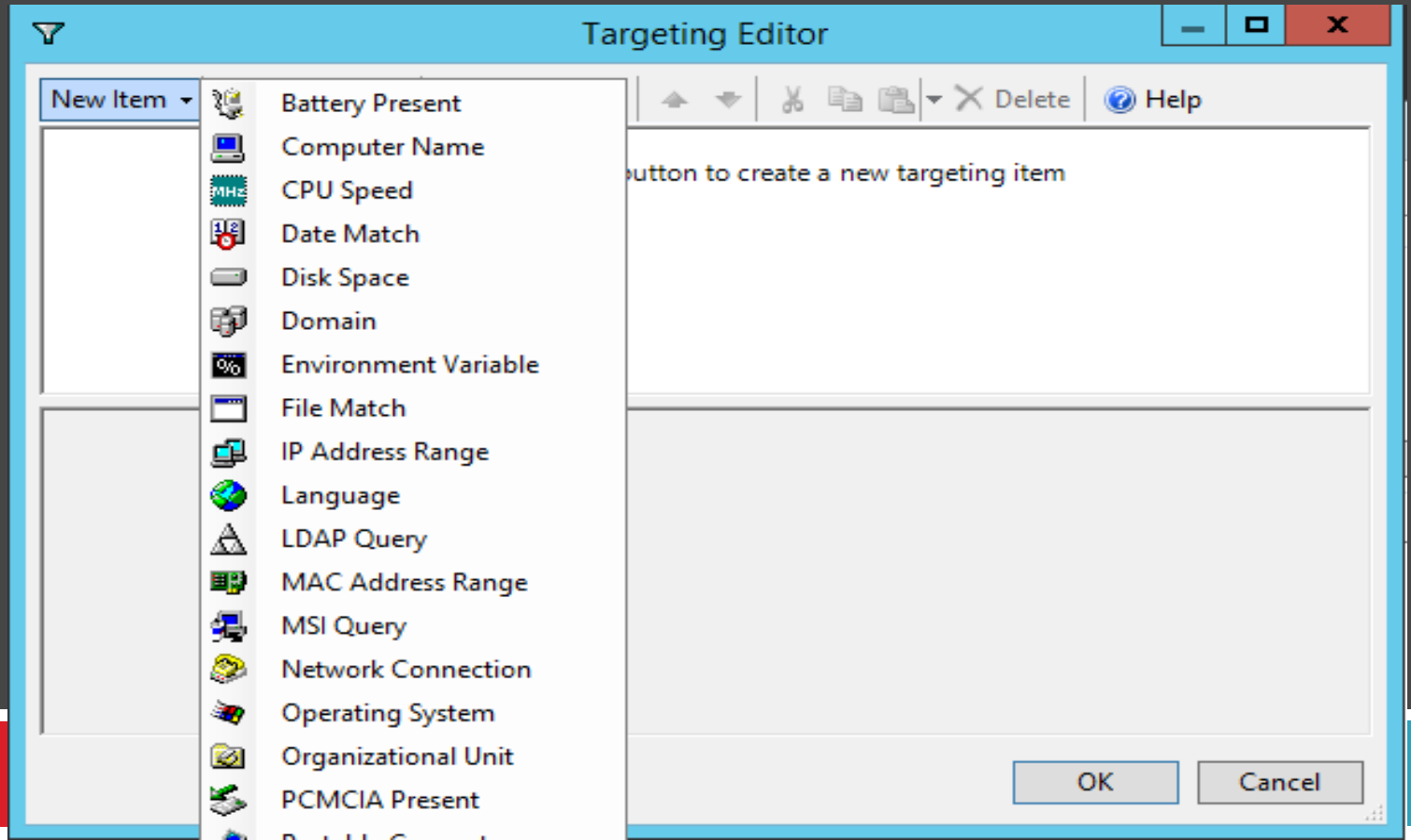


S_ - Notepad

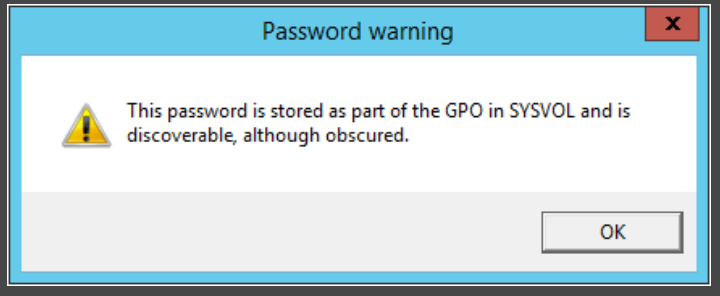
File Edit Format View Help

```
<?xml version="1.0" encoding="utf-8"?>
<Drive clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}" name="S:" status="S:" image="2" changed="2016-06-21 13:25:43"
uid="{AEF3EE60-BA13-4B77-8820-75DE737A5F0F}"><Properties action="U" thisDrive="NOCHANGE" allDrives="NOCHANGE" userName=""
path="\\dc1\sysvol" label="SHARE" persistent="1" useLetter="1" letter="S"/></Drive>
```

GPP: ITEM LEVEL TARGETING



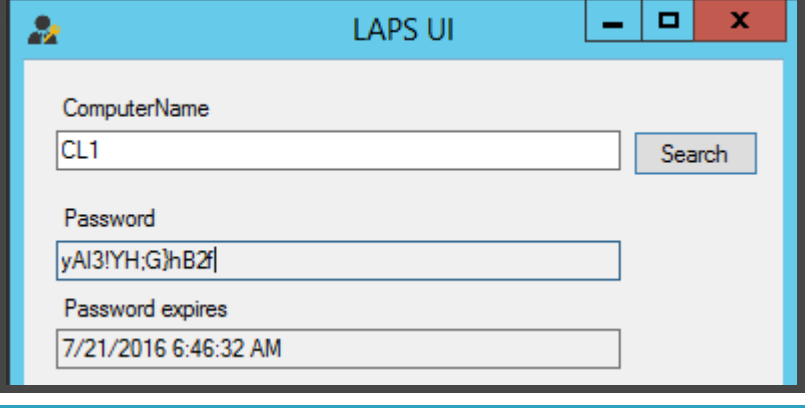
GPP: SPRÁVA LOKÁLNÍCH UŽIVATELŮ



- GPP umožnují mimo jiné:
  - Vytvořit lokálního uživatele + nastavit jeho heslo
  - Přenastavit hesla existujícím lokálním uživatelům
- To znamená, že někde v SYSVOLu to heslo musí být
- Heslo uloženo reverzibilně (atribut cPassword)
- Problém popisuje KB2962486 https://support.microsoft.com/en-us/kb/2962486
  - Je tam i vzorový skript na detekci cPassword hesel
  - Invoke-PasswordRoll.ps1
- Nestačilo by nastavení Security Filteringu?

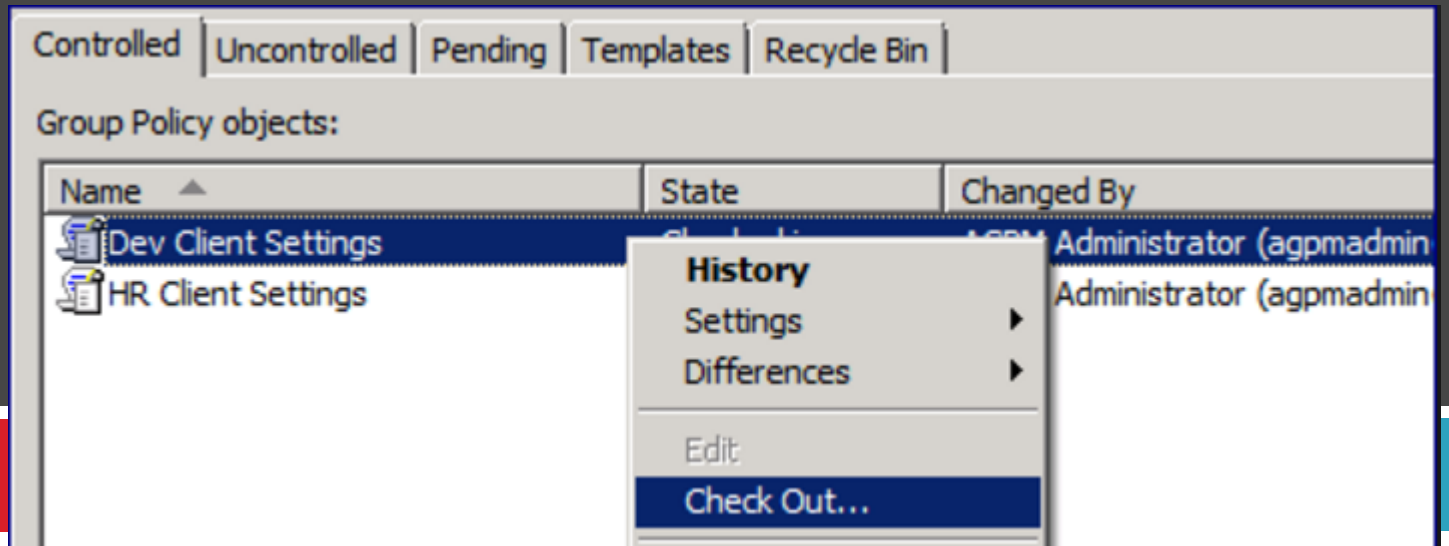
LOCAL ADMIN PASSWORD SOLUTION (LAPS)

- Jiří Formáček (MSFT)
- https://www.microsoft.com/en-us/download/details.aspx?id=46899
- Nástroj na generování unikátních hesel lokálních Administrátorů (SID *–500)
- Hesla ukládá do AD do computer účtu (nový atribut ms-Mcs-AdmPwd)



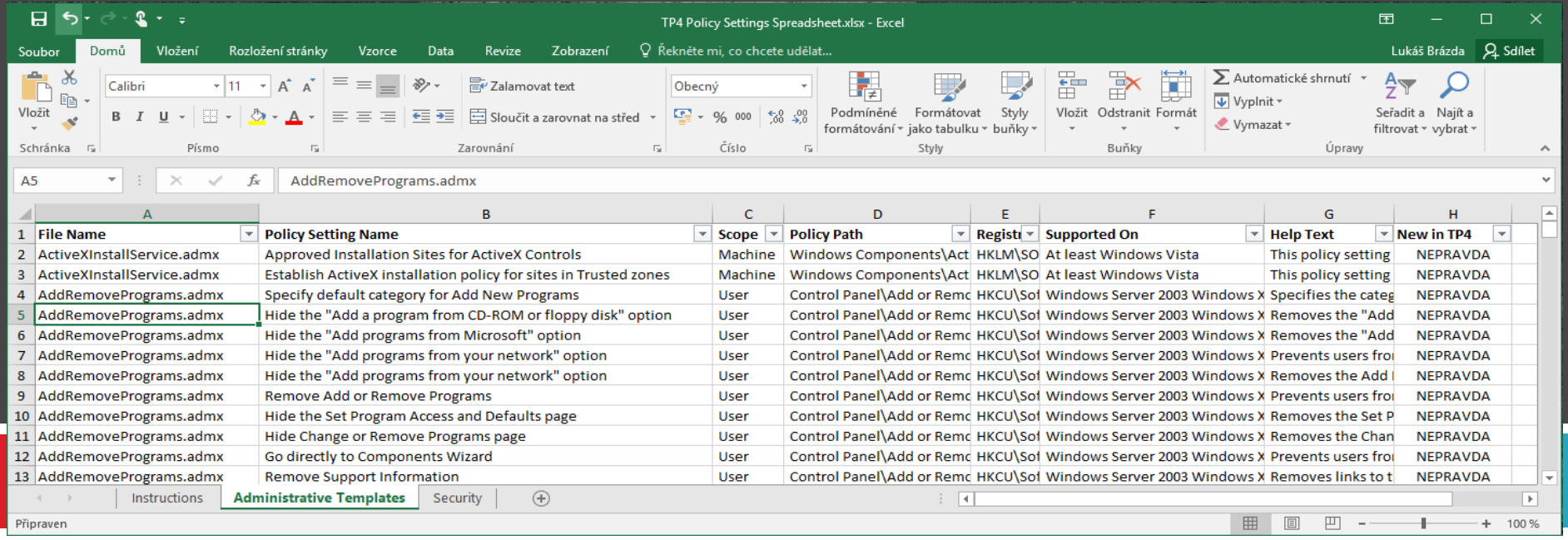
POZOR NA EDITOVÁNÍ ZAŽIVA

- GPME nemá v sobě tlačítko Save…
- Jinými slovy kdykoli nějakou GPO editujete, děláte tak v provozu
- Pokud něco změníte a někomu zrovna přijde refresh interval, nastavení si asi aplikuje
- AGPMC se chová lépe



GPO REFERENCE GUIDE

- Seznam všech vestavěných GPO nastavení
- XLSX soubory ke stažení:
  - https://www.microsoft.com/en-us/download/details.aspx?id=25250



	A	B	C	D	E	F	G	H
1	File Name	Policy Setting Name	Scope	Policy Path	Registi	Supported On	Help Text	New in TP4
2	ActiveXInstallService.admx	Approved Installation Sites for ActiveX Controls	Machine	Windows Components\Act	HKLM\SO	At least Windows Vista	This policy setting	NEPRAVDA
3	ActiveXInstallService.admx	Establish ActiveX installation policy for sites in Trusted zones	Machine	Windows Components\Act	HKLM\SO	At least Windows Vista	This policy setting	NEPRAVDA
4	AddRemovePrograms.admx	Specify default category for Add New Programs	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Specifies the categ	NEPRAVDA
5	AddRemovePrograms.admx	Hide the "Add a program from CD-ROM or floppy disk" option	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Removes the "Add	NEPRAVDA
6	AddRemovePrograms.admx	Hide the "Add programs from Microsoft" option	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Removes the "Add	NEPRAVDA
7	AddRemovePrograms.admx	Hide the "Add programs from your network" option	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Prevents users fro	NEPRAVDA
8	AddRemovePrograms.admx	Hide the "Add programs from your network" option	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Removes the Add	NEPRAVDA
9	AddRemovePrograms.admx	Remove Add or Remove Programs	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Prevents users fro	NEPRAVDA
10	AddRemovePrograms.admx	Hide the Set Program Access and Defaults page	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Removes the Set P	NEPRAVDA
11	AddRemovePrograms.admx	Hide Change or Remove Programs page	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Removes the Chan	NEPRAVDA
12	AddRemovePrograms.admx	Go directly to Components Wizard	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Prevents users fro	NEPRAVDA
13	AddRemovePrograms.admx	Remove Support Information	User	Control Panel\Add or Remc	HKCU\Sof	Windows Server 2003 Windows X	Removes links to t	NEPRAVDA

4) Troubleshooting

VYNUCENÍ GPO REFRESH VZDÁLENĚ

- Před WS2012 se dal použít nástroj psexec.exe od SysInternals
- Od WS2012 je na to v GPMC tlačítko (jen na OU)
- Nebo CMDLet: Invoke-GPUpdate -RandomDelayInMinutes

RYCHLOST APLIKOVÁNÍ GPO

- Faktory které NEMAJÍ vliv na rychlost aplikování politik:
  - Množství GPO objektů v AD (Group Policy Object Container)
  - Nepoužívání vlastnosti „GPO status“
  - Množství nastavení uvnitř GPO objektu
  - Počet GPO objektů nalinkovaných na uživatele nebo počítač
- Faktory které MAJÍ vliv na rychlost aplikování politik:
  - Divné, špatně otestované skripty (logon, startup, atp.)
  - Problémy s DNS, inkonzistence v GPO
  - Mapování neexistujících tiskáren nebo disků (+ velké ovladače)
  - Velké množství GPO objektů linkovaných na uživatele nebo počítač (přes pomalou linku)

PROČ SE NĚKDY GPO NEAPLIKUJÍ?

- Faktory ovlivňující (ne)aplikování GPO:
  - Slow-link Detection
  - Kešovaná hesla uživatelů
  - Asynchronní zpracování GPO

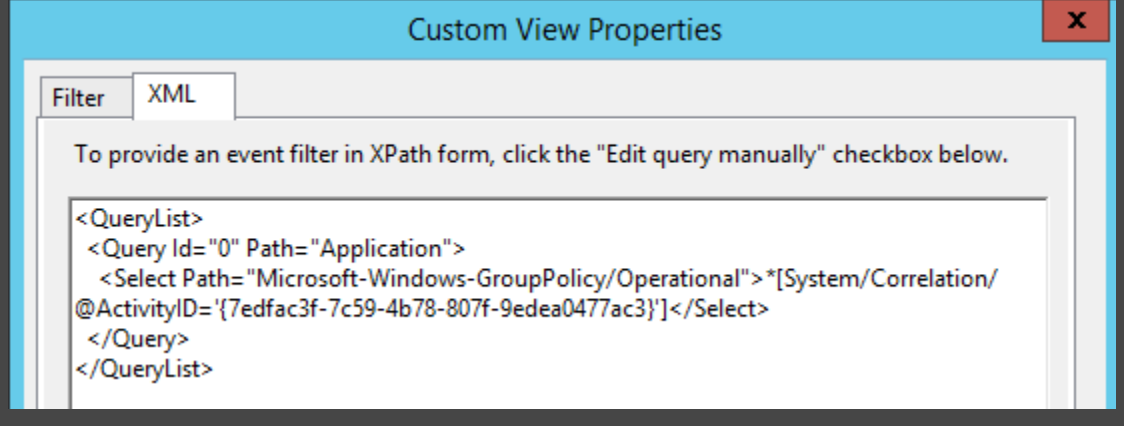
TROUBLESHOOTING

- Při každém aplikování politik vznikají tzv. RSoP data
- Prohlížet se dají:
  - GPResult.exe (lokálně / vzdáleně)
  - Group Policy Results (lokálně / vzdáleně z GPMC)
  - Group Policy Modeling (nejsou to ostrá data, jen simulace)
- RSOP.msc
- EventViewer:
  - System – obecné (krátké) informace o aplikování politik
  - GroupPolicy Operational – detailní info

FILTROVÁNÍ EVENTLOGU

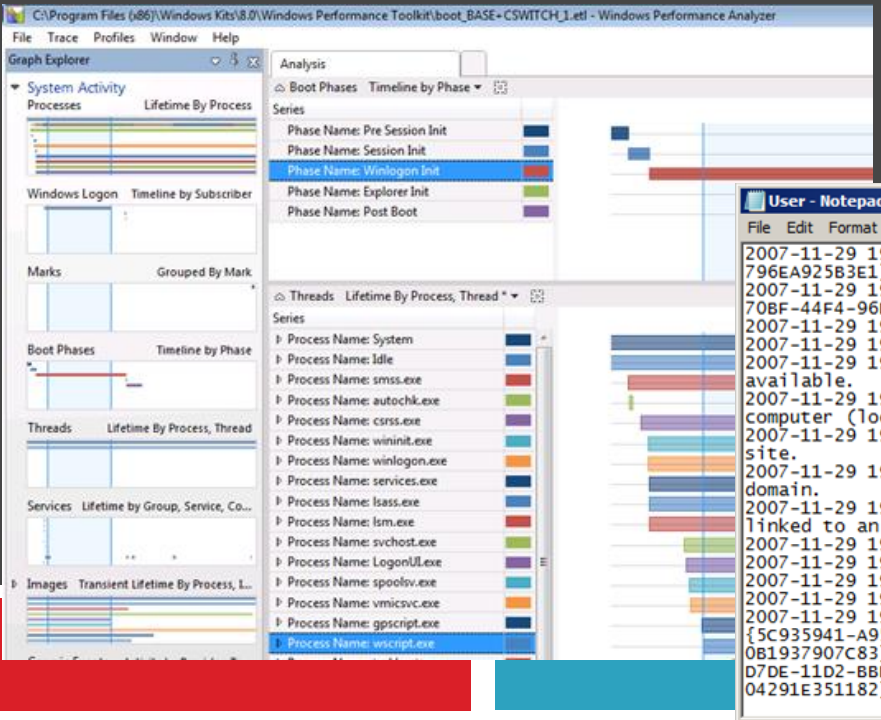
- Předdefinovaný filtr v XML

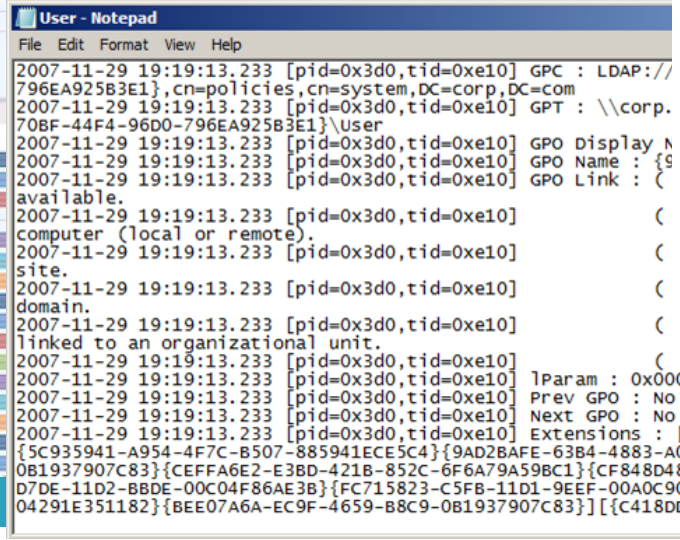
<QueryList><Query Id="0" Path="Application"><Select Path="Microsoft-Windows-GroupPolicy/Operational">[System/Correlation/@ActivityID='{INSERT ACTIVITY ID HERE}']</Select></Query></QueryList>*

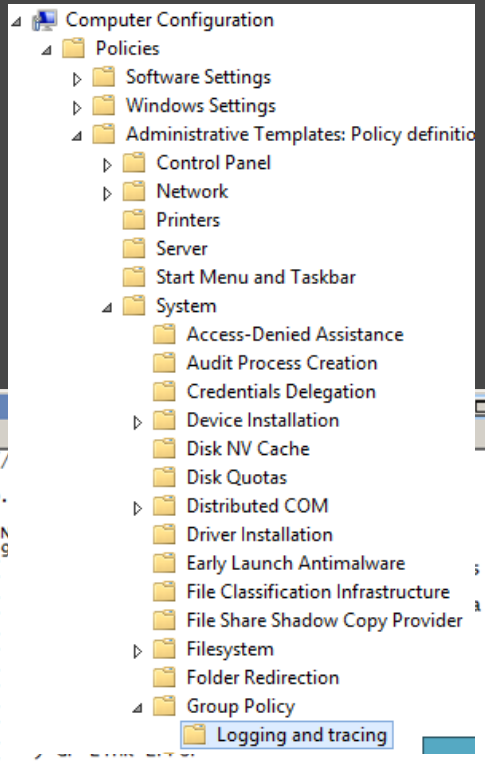


TROUBLESHOOTING: ADVANCED

- GPO Tracing
- Windows Performance Analyzer







TROUBLESHOOTING: EVENTY

Get Applicable GPOs Start	4126
Get Applicable GPOs End Success	5126
Get Applicable GPOs End Fail	7126
GPO process sync mode slowlink detected	6344
GPO Process sync mode NO DC	6345
GPO Process switch sync mode to async	6346
Gpsvc start	4115
Gpsvc stop	5115

Gpsvc stop	5115
Gp session start	4117
Gp session return winLogon call	5351
Gp session end	5117
Gp session end with error	7117
Gp save to cache start	4216
Gp save to cache end	5216
Gp save to cache end with error	7216
Gp load from cache start	4217
Gp load from cache end	5217
Gp load from cache end with error	7217
Gp cache first WMI query start	4218
Gp cache first WMI query end	5218
Gp service init start	4116
Gp service init end	5116
Gp policy download start	4257
Gp policy download end	5257

TIPY

- Network Emulator Client (simlace slow-link)
- Windows 8.1 GPO Cache

5) Co když GPO nestačí?

PS: DESIRED STATE CONFIGURATION

- S DSC se nestaráte o konfiguraci serveru, ale o definování konfigurace
- Používá PowerShell syntaxi a CMDLety
- Vytváří nebo definuje konfigurační soubory
- Tuto konfiguraci následně aplikuje na servery
- Cílem konfiguračních souborů je „ujišťovat se“, že server je nastavený jak chci
- Pokud konfiguraci definovanou pomocí DSC server nesplňuje, DSC zjedná nápravu
- DSC je založeno na standardech:
  - MOF: Management File Object
  - CIM: Common Information Model

DESIRED STATE CONFIGURATION

- Requirements:
  - Windows Management Framework 4.0
  - .NET Framework 4.5
  - WS2008 R2 nebo Windows 7
  - KB2883200 (pro WS2012 R2 a Windows 8.1)
  - PowerShell Remoting
- Dva základní režimy:
  - Push: konfigurační soubory jsou „tlačeny“ na vzdálené servery (Start-DSCConfiguration)
  - Pull: definujeme centrální server a ostatní servery z něj „tahají“ konfiguraci sami (30minut):
    - HTTP(S)
    - SMB

DSC: RESOURCE PROVIDERS

- Get-DSCResource
- Další zdroje lze získat:
  - Od MS (DSC Resource Waves)
  - Od komunity (např. na GitHubu)
  - Find-Package

```
PS C:\> Get-DscResource

ImplementedAs   Name
-------------   ----
Binary          File
PowerShell      Archive
PowerShell      Environment
PowerShell      Group
Composite       GroupSet
Binary          Log
PowerShell      Package
Composite       ProcessSet
PowerShell      Registry
PowerShell      Script
PowerShell      Service
Composite       ServiceSet
PowerShell      User
PowerShell      WaitForAll
PowerShell      WaitForAny
PowerShell      WaitForSome
PowerShell      WindowsFeature
Composite       WindowsFeatureSet
PowerShell      WindowsOptionalFeature
Composite       WindowsOptionalFeatureSet
PowerShell      WindowsProcess
```

- $env:ProgramFiles\WindowsPowerShell\Modules
- https://gallery.technet.microsoft.com/scriptcenter/DSC-Resource-Kit-All-c449312d
- https://github.com/PowerShellOrg/DSC

DSC PŘÍKLAD

```
Configuration MojeDSC {

param(
[Parameter(Position=0,Mandatory)]
[ValidateNotNullorEmpty()]
[string[]]$ComputerName
)
    Node $ComputerName
    {
        #povol feature
        WindowsFeature Backup {
            Name = "Windows-Server-Backup"
            Ensure = "Present"
        }
        #nastartuj sluzbu
        Service RemoteRegistry {
            Name = "RemoteRegistry"
            StartUpType = "Automatic"
        }
        #vytvor adresar
        File TestFolder {
            Type = "Directory"
            Ensure = "Present"
            DestinationPath = "C:\TestDirectory"
        }
    }#zaviram node
}#zaviram konfiguraci

```

JUST ENOUGH ADMINISTRATION (JEA)

- Možnost pomocí PowerShell DSC limitovat, jaké operace lze provádět přes PowerShell (i remote). Omezit lze na CMDLety, parametry, hodnoty parametrů atp.
- JEA Toolkit
- JEA Endpoint

- JEA Helper Tool 2.0

- Enter-PSSesion –ComputerName SRV1 –ConfigurationName RestartService