# GPO

Ondřej Šebela

# Motivace

- Představte si, že máte ve firmě 5000 počítačů a uživatelů.
- Jaké máte možnosti, pokud budete chtít:
  - instalovat aplikace jako Google Chrome, Java a pravidelně je aktualizovat
  - zakázat ne-adminům spouštět CMD kromě úzké skupiny uživatelů
  - do skupiny administrators na každém stroji přidat účet pepa
  - povolit vybraná pravidla ve firewallu
  - …
- Jaké vás napadají výhody/nevýhody navrhovaných řešení?

# Co jsou Group Policy

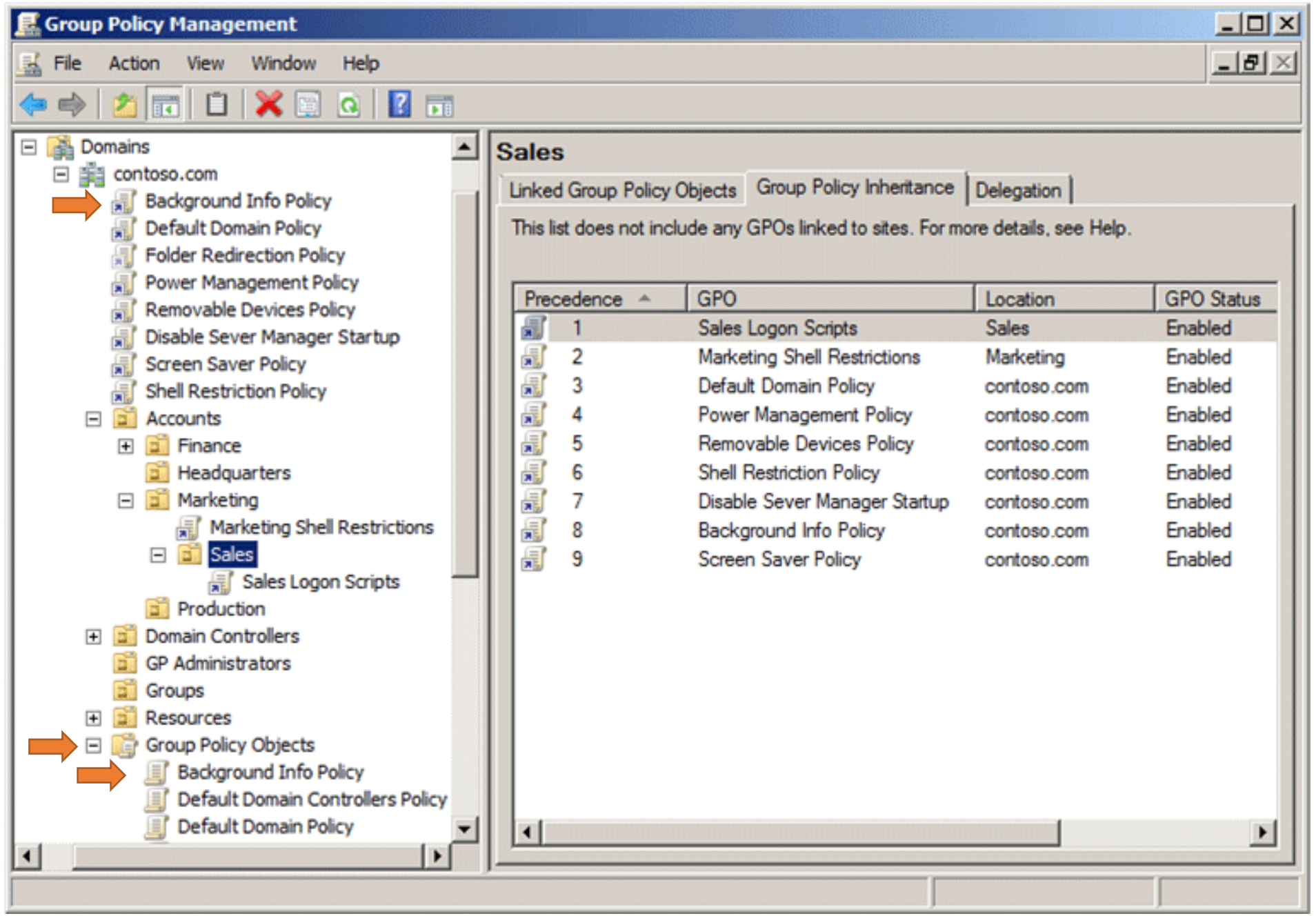
- Systémové politiky
- “GUI nadstavba registrů“
- Obsahují tisíce nastavení, kterými můžeme měnit například:
  - Konfiguraci služeb, úpravu nastavení systému, registrů, NTFS oprávnění, politik bezpečnosti a auditu, instalaci software, přihlašovací a odhlašovací skripty, přesměrování adresářů, nastavení IE, členství ve skupinách a mnoho dalších
- Dají se použít jak pro konfiguraci lokálního stroje/uživatelů (viz PV175), tak v doménovém prostředí, kde slouží pro **centralizovanou** správu všech strojů a uživatelů

# Princip fungování

- Vytvořím v Group Policy Management konzoli GP objekty (GPO) s různými nastaveními pro uživatele a počítače
- Uživatele a počítače roztřídím do OU
- Na danou strukturu OU nalinkuji vytvořená GPO
- Stroje/uživatelé na sebe aplikují nastavení z GPO a tím nakonfiguruji prostředí dle mých představ

# Domain GPO

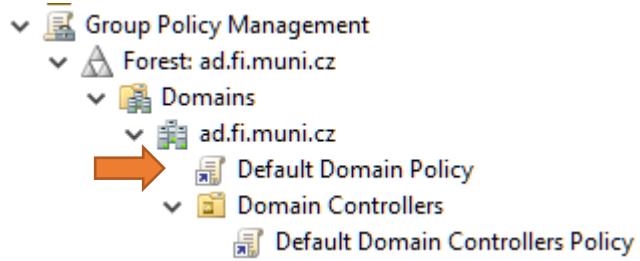
- Vytvářeny a ukládány na doménových řadičích (SYSVOL adresář)
- GPO je objekt (soubory) reprezentující námi vybranou sadu nastavení
- Linkují se na AD strukturu = aplikují se na všechny uživatele/počítače v daném umístění
- **Computer část GPO se aplikuje na stroje, user část potom na uživatele** v dané AD struktuře
- Správa pomocí nástroje Group Policy Management Console (GPMC)


Group Policy Management
File
Action
View
Window
Help
Domains
contoso.com
Background Info Policy
Default Domain Policy
Folder Redirection Policy
Power Management Policy
Removable Devices Policy
Disable Sever Manager Startup
Screen Saver Policy
Shell Restriction Policy
Accounts
Finance
Headquarters
Marketing
Marketing Shell Restrictions
Sales
Sales Logon Scripts
Production
Domain Controllers
GP Administrators
Groups
Resources
Group Policy Objects
Background Info Policy
Default Domain Controllers Policy
Default Domain Policy
Sales
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This list does not include any GPOs linked to sites. For more details, see Help.
Precedence
GPO
Location
GPO Status
1 Sales Logon Scripts Sales Enabled
2 Marketing Shell Restrictions Marketing Enabled
3 Default Domain Policy contoso.com Enabled
4 Power Management Policy contoso.com Enabled
5 Removable Devices Policy contoso.com Enabled
6 Shell Restriction Policy contoso.com Enabled
7 Disable Sever Manager Startup contoso.com Enabled
8 Background Info Policy contoso.com Enabled
9 Screen Saver Policy contoso.com Enabled

# GPO settings

- Nastavení v GPO je rozděleno do 2 částí podle toho, jaký typ objektů nastavuje:
  - Computer configuration
    - Nastavení počítače (bez ohledu na to, který uživatel s ním pracuje)
    - Nastavení se aplikují **pouze na účty počítačů**
  - User configuration
    - Uživatelská nastavení (bez ohledu na to, ke kterému počítači se uživatel přihlašuje)
    - Nastavení se aplikují **pouze na účty uživatelů**
- Je tedy velice důležité, ze které sekce nastavení pochází a na jaký typ objektů se GPO aplikuje! Tedy pokud nalinkuji GPO s nastaveními v User configuration části na OU s počítači, tak na nich k žádným změnám nedojde

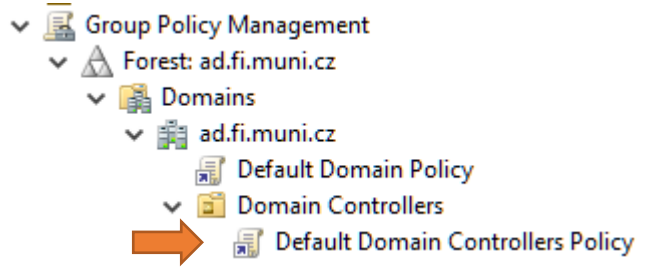
# Výchozí doménové politiky




- Default Domain Policy
  - Aplikuje se na všechny uživatele i počítače v doméně (včetně DC)
  - Definuje bezpečnostní nastavení (Account Policy - kerberos, password a account lockout policy)

  - Nastavení v sekci Account Policy se dají definovat jen v GPO linkovaných na doménu!
  - Nastavení hesla + lockout se však od Server 2008 dají definovat separátně pro uživatele i skupiny. Viz Fine-Grained Password Policies

# Výchozí doménové politiky




- Default Domain Controllers Policy
  - Aplikuje se jen na DC
  - Definuje základní pravidla zabezpečení, auditování a práv uživatelů (User Rights)

(Best practice: neupravovat je, raději nalinkovat novou GPO)

# Linkování GPO

- Všechny GPO jsou uloženy v **Group Policy Objects** kontejneru a na AD strukturu se pouze linkují
- Jednu GPO tedy mohu mít nalinkovanou na víc míst v AD
- GPO je možné přilinkovat na úrovni
  - Site
    - Na všechny objekty v rámci lesa spadající do dané Site
    - Neukazují se v „Linked Group Policy Objects“
    - GPO je uložena na DC kde byla vytvořena (proto musí být stále dostupný!)
  - Domain
    - Pozor, nezdědí se na child domény
  - OU
- GPO nemohu linkovat na některé výchozí kontejnery jako Users, Computers
- Na každé úrovni je možné přilinkovat libovolné množství GPO (aplikuje se však jen 999)

# Nakonfigurování prostředí

- Stáhněte si ze studijních materiálů tyto slajdy a 05_tools.zip
- Vytvořte hierarchii organizačních jednotek (OU)
  - Pocitace
    - Klienti + přemístěte do ní computer účet klientského virtuálu
  - Uzivatele
    - Zamestnanci + v ní vytvořte uživatele xpepik a xbubla
- PS
  - *New-ADOrganizationalUnit -Name Pocitace -Path "DC=ad,DC=local“*
  - *New-ADUser -AccountPassword (ConvertTo-SecureString -AsPlainText 'Pass123.' -Force) -ChangePasswordAtLogon $false -Name xpepik -Enabled $true -PasswordNeverExpires $true -Path ‘ou=Zamestnanci,ou=Uzivatele,dc=ad,dc=local'*

# Nakonfigurování prostředí

- Povolení funkce “Remote GPO Update”
  - Pomocí GPMC konzole
    - Otevřete sekci Starter GPOs (nechte je vygenerovat)
    - Z GPO „Group Policy Remote Update Firewall Ports“ vytvořte novou GPO „Group Policy Remote Update“ a tu nalinkujte na celou doménu
  - Pomocí PS
    - V GPMC otevřete sekci Starter GPO a nechte je vygenerovat
    - *New-GPO -Name "Group Policy Remote Update" -StarterGpoName "Group Policy Remote Update Firewall Ports" | New-GPLink -target "dc=ad,dc=local" -LinkEnabled yes*
- Vynuťte na klientovi aplikování nové GPO skrze gpupdate /force (v CMD)
- Otestujte remote update PS příkazem „*Invoke-GPUpdate ipklienta -RandomDelayInMinutes 0*“ (skrze GPMC má spoždění až 10 minut)

# Nakonfigurování prostředí

- Abychom se mohli na stroje přihlašovat přes RDP i ne-admin účty je potřeba přidat „Domain Users“ do „Remote Desktop Users“ skupiny
  - Vytvořte GPO „RDP access for domain users“ a nalinkujte ji na vaši doménu
  - V *CC – Policies - Windows Settings – Security Settings – Restricted Groups – Add Group – Browse – Domain users – OK – This group is a member of – ADD – remote desktop users*
- Aby to fungovalo i u serverů, je potřeba ještě
  - V *CC – Policies - Windows Settings – Security Settings – Local Policies – User Rights Assignment – Allow log on through remote desktop services – přidat users,domain users*
- Vynuťte okamžité aplikování politiky pomocí (*Invoke-GPUpdate ipklienta -RandomDelayInMinutes 0*)

# Úkol

- Na **OU Pocitace** nalinkujte GPO „**Modify permissions for temp**“, která nastaví skupině users modify práva na C:\temp
  - *CC -> Policies -> Windows Settings -> Security Settings -> File System*
- Na **OU Uzivatele** nalinkujte GPO „**IE homepage is.muni.cz**“ a nastavte v ní homepage IE na is.muni.cz
  - *UC -> Policies -> Administrative Templates -> Windows Components -> Internet Explorer -> Disable changing home page settings*
- Otestujte funkčnost GPO přihlášením jako xpepik na klientský stroj
  - Vytvořte adresář C:\temp + updatujte politiky

- V PS
  - *New-GPLink -Name „Modify permissions for temp“ -Target „ou=Pocitace,dc=ad, dc=local"*

# Dědičnost

- Nastavení z GPO se aplikují na objekty v AD struktuře, na kterou byla GPO nalinkována včetně všech podúrovní tzn. dědí se podobně jako NTFS oprávnění
- Zkontrolujte v GPMC na záložce **Group Policy Inheritance** u OU Pocitace, že je tam i Default Domain Policy, která je ale nalinkovaná o úroveň výš

# Aplikace GPO

- Foreground GP processing
  - **Computer** části GPO se aplikují při každém **startu počítače zapojeného do domény**
    - **Aplikuje se pod účtem daného stroje**
  - **User** části GPO se aplikují při **přihlášení doménového uživatele**
    - **Aplikuje se pod účtem uživatele, který se právě přihlašuje**
    - Z DC se ale od června 2016 stahují pod účtem stroje! Viz MS16-072
- Background refresh probíhá každých 90min +- 30 (nastavitelné)
  - Defaultně se aplikují pouze změněné GPO (VersionNumber)
  - Security politiky se aplikují každých 16 hodin ať se změnily či ne (každých 5minut na DC)
- Ruční refresh
  - Lokálně *gpupdate /force* (CMD) nebo vzdáleně *Invoke-GPUpdate* (Powershell)

Pozn.: ne všechna nastavení z GPO mohou být aplikována na pozadí (auditování, intalace software, přesměrování adresáře, mapování disků, skripty,..)

# Pořadí zpracování GPO

- Počítač/uživatel si vždy při zapnutí/přihlášení vytvoří seznam všech politik z OU, ve které se nachází jeho AD účet + GPO umístěných výše, seřadí je a začne na sebe aplikovat (Computer/User část dle jeho typu)
- Pokud existují konfliktní nastavení v GPO na různých úrovních, tak vyhraje nastavení z GPO, která se aplikovala později
- Pokud jsou konfliktní GPO na stejné úrovni, rozhoduje pořadí zpracování (hodnota Link Order – GPO s nejnižším číslem se aplikuje jako poslední == vyhrává)
  - V GPMC záložka **Linked Group Policy Objects**

# Pořadí zpracování GPO

- GPO se aplikují v tomto pořadí přičemž platí, že **poslední vyhrává**:
  1. (Lokální politiky jsou-li nějaké a nejsou-li zakázány)
  2. Všechny GPO přilinkované na site, do které spadá IP adresa stroje
  3. Všechny GPO přilinkované na doménu, ve které se objekt nachází
  4. Všechny GPO přilinkované na všechny nadřazené OU
  5. Všechny GPO přilinkované přímo na OU ve které je uložen
  6. Enforce GPO jsou-li nějaké (ale o tom později)

- Pořadí zpracování GPO ověřím v GPMC záložka **Group Policy inheritance**

# Úkol

- Vytvořte GPO „Read permission for temp“, která skupině Users nastaví u adresáře C:\temp read práva
- Nalinkujte tuto GPO na OU Pocitace a updatujte na klientovi politiky
- Zkontrolujte NTFS práva na C:\temp, změňte pořadí zpracování GPO, opět update a opět zkontrolujte
- Na klientovi v CMD puštěné pod adminem vygenerujte příkazem *gpresult /h report.html* a otevřete jej (bude tam vidět, která GPO „vyhrála“)

- V PS
  - *Set-GPLink -Name „Read permissions for temp“ -Target „ou=Pocitace,dc=ad, dc=local" -Order 1*

# Úkol pokračování

- GPO „Read permission for temp“ nalinkovanou na OU Pocitace disablujte a nalinkujte ji na OU Klienti
- Updatujte politiky na klientovi
- Zkontrolujte NTFS práva na C:\temp

- Disablujte „Read permission for temp“ na OU Klienti a opět updatujte politiky

- PS
  - Set-GPLink -name 'Read permission for temp' -LinkEnabled no -target 'ou=Pocitace,dc=ad, dc=local '

# Pořadí zpracování GPO 2.

- Block inheritance
  - Nastavuje se na OU
  - Blokuje dědičnost všech politik uvedených hierarchicky výš od vybrané OU
- Enforce inheritance
  - Nastavuje se na GPO
  - Vynutí aplikování vybrané GPO hierarchicky níž do všech OU, i kdyby byly cestou nějaká block inheritance
  - Enforce GPO se navíc aplikují jako poslední! (v případě více enforced GPO platí, čím „výš“ tím silnější)

Ideálně nepoužívat

- Blokování dědění zakáže totiž i aplikování Default Domain Policy což je nutné řešit (enforce či nalinkování na danou OU)

# Úkol

- Povolte všechny disablované GPO
- Zakažte dědění na OU Klienti
- Updatujte politiky na klientovi a zkontrolujte NTFS práva na C:\temp

- U GPO „Modify permissions for temp“ nastavte enforce a opět zkontrolujte

- Nalinkujte GPO „Read permissions for temp“ na vaši doménu, nastavte enforce a opět zkontrolujte

- V PS
  - *Set-GPinheritance -Target "ou=Klienti,ou=Pocitace,dc=ad,dc=local" -IsBlocked Yes*

Tip: po každé úpravě kontrolujte záložku **Group Policy Inheritance** (nezapomeňte na refresh - F5)

# GPO Scope – Security Filtering

- Potom co klient získá seřazený seznam GPO, je začne postupně aplikovat **pokud na to má právo**
- Ve výchozím nastavení mají členové skupiny Authenticated Users (všichni autentizovaní uživatelé **i počítače**) právo READ a APPLY GROUP POLICY na každou GPO
- Security Filtering ideálně **vůbec nepoužívat**
- Z DC se od června 2016 computer i **user** politiky stahují pod účtem stroje! Viz MS16-072

- Princip: Objekt má/nemá právo na sebe GPO aplikovat
- Pro: možnost granulárního aplikování GPO na konkrétní objekty
- Proti: horší správa, debugging, právo se nevztahuje na konkrétní GPO link, ale na samotnou GPO tzn. projeví se na všech lincích!
  - Deny oprávnění se nezobrazují v Security filtering u GPO
- Druhy použití:
  A. Dám právo jen vybrané skupině účtů (odebráním práv Authenticated Users a přidáním vlastní skupině účtů)
  B. Zakázání přístupu vybrané skupině účtů (přidáním deny práva skrze záložku Delegation)

# Úkol

- Zrušte všechny enforce a zákazy dědění
- Na OU Zamestnanci nalinkujte GPO „IE homepage seznam.cz“ a nastavte v ní homepage IE na seznam.cz
  - *UC -> Policies -> Administrative Templates -> Windows Components -> Internet Explorer -> Disable changing home page settings*
- Ověřte pod xpepik, že se homepage změnil
- Nastavte GPO „IE homepage seznam.cz“ tak, že xpepik jako jediný zaměstnanec v OU Zamestnanci bude mít jako homepage výchozí URL ve firmě, tedy is.muni.cz.
- Ověřte pod uživateli xpepik i xbubla, že se aplikuje správně

# Úkol

- Co když se na klientský stroj přihlásí doménový administrátor?
  - Na jakýkoli účet mimo scope politiky se politika neaplikuje = nebude mít nastaven žádný homepage. Ale nesouvisí to s tím, že je administrátor.
- Jak docílit toho, že se GPO aplikuje pouze pokud se přihlásí někdo ze skupiny Domain Admins?
  - V security filtering GPO vyhodím Authenticated Users a přidám jen skupinu Domain Admins (+ Domain Computers).
- Co když se přihlásí lokální uživatel?
  - Lokální účty nemají právo na sebe doménové politiky aplikovat.

# GPO Scope – WMI filtering

- Princip: než se GPO aplikuje, tak se nejdříve ověří, že WMI dotaz získal odpověď
- Pro: mohu vytvořit filtr prakticky na cokoli
- Proti: může dost zpomalit zpracování GPO, filtr se nevztahuje na konkrétní GPO link, ale na samotnou GPO tzn. projeví se na všech lincích!
- WMI filtry se ukládají v kontejneru WMI Filters a poté se linkují na GPO

# GPO Scope – WMI filtering

- WMI dotazovací jazyk (WQL) má podobnou syntaxi jako SQL.
  - Test na jméno stroje

  *SELECT * FROM Win32_ComputerSystem WHERE Name LIKE “%SIRENE%”*
  - Test na aktuální den v týdnu (projde jen o víkendu)

  *SELECT * FROM Win32_LocalTime WHERE DayOfWeek > 5*
  - Test zda se jedná o 64b OS

  *SELECT * FROM Win32_Processor WHERE AddressWidth = '64'*
  - Test zda se jedná alespoň o OS Windows Vista či Server 2008

  *SELECT Version FROM Win32_OperatingSystem WHERE Version >= ‘6’*
  - Test na volné místo (10MB) a NTFS file systém

  *SELECT * FROM Win32_LogicalDisk WHERE Name = "C:" AND DriveType = 3 AND FreeSpace > 10485760 AND FileSystem = " NTFS"*
- V PS otestuji
  - *Get-WmiObject -Query 'SELECT * FROM Win32_ComputerSystem WHERE Name LIKE "%SIRENE%"'*

# Administrative Templates

- Provádějí změny v chráněné části registrů (ne-admin uživ. nemohou měnit)
  - HKEY_LOCAL_MACHINE\Software\Policies
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
  - HKEY_CURRENT_USER\Software\Policies
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
- GPO aware aplikace + systém se dívají do těchto cest a dle případných nastavení upravují své nastavení
- Do Windows XP/Server 2003
  - Definice v textovém souboru s koncovkou ADM (pro každý jazyk jeden)
  - ADM šablony se kopírují do každé GPO kde jsou použity (bobtnající SYSVOL)
- Od Windows Vista/Server 2008
  - Definice šablon pomocí univerzálního XML formátu
  - ADMX šablony jsou uloženy v %SystemRoot%\PolicyDefinitions
  - Zadefinované změny se ukládají v souboru registry.pol, který se poté aplikuje na klientech

# Administrative Templates

- Šablony se dají vytvořit ručně či nástroji jako admxmigrator
- Někteří výrobci poskytují tyto šablony pro snadnou správu svých aplikací (MS Office, Google, Adobe,..)
- Managed vs Unmanaged nastavení
  - Managed
    - Při vypadnutí uživatele | stroje ze scope politiky se změny ztratí
    - 4 registry cesty viz předchozí slajd
  - Unmanaged
    - Změny jsou trvalé (i při vypadnutí ze scope politiky nastavení zůstanou)
    - Standardně jsou v GPMC skryty (filter options – managed – no)

# ADMX Central Store

- Standardně když konfigurujete GPO, tak v Administrator Templates sekci vidíte jen šablony, které jsou uloženy na vašem stroji. Tzn. složitá aktualizace, distribuce a konzistence šablon v doménovém prostředí
- Central store je adresář v SYSVOL, který slouží jako centrální úložiště pro všechny admx šablony používané v dané doméně. Tzn. výše zmíněné problémy odpadají
- Vytvoříme jej prostým zkopírováním adresáře C:\Windows\PolicyDefinitions do C:\Windows\SYSVOL\sysvol\jmenodomeny\Policies\
- Jakmile je vytvořen, GPMC automaticky zobrazí šablony z něj namísto lokálního umístění

# Úkol

- Dejte Edit u jakékoli GPO a podívejte se na část Administrative Templates (retrieved from local machine)
- Stáhněte ADMX templates pro Google Chrome z ISu či zde
- Na serveru1 vytvořte ADMX Central Store zkopírováním adresáře C:\Windows\PolicyDefinitions do C:\Windows\SYSVOL\sysvol\FQDN\Policies
- Zkopírujte do Central Store nové ADMX šablony pro Chrome
  - Obsah en-US (chrome.adml) do en-US a chrome.admx přímo do PolicyDefinitions
- Opět si otevřete nastavení nějaké GPO a zkontrolujte část Administrative Templates (retrieved from central store) a ověřte, že je dostupný nový template

# Preferences

- Rozšiřují možnosti doménových GPO
- Dostupné od Windows Vista
- Obsahují nepovinná nastavení (uživatelé mohou změnit)
- Mapování disků, systémové proměnné, úprava registrů, power options, start menu options, printers, scheduled tasks, kopírování souborů, ..

- Item-level targeting
- Remove this item when it is no longer applied
- Rozdíly mezi Create, Delete, Replace, Update akcemi

- Pozn. nepoužívat pro vytváření user účtů!

# Úkol

- Vytvořte GPO „Share Temp“ a nalinkujte ji na OU Klienti
- V Preferences v ní nastavte nasdílení adresáře C:\temp
- Otestujte na klientovi

- Povolte v „Apply Once and do not reapply“, zrušte ručně nasdílení adresáře a znovu GPO aplikujte

- Podívejte se na možnosti „Item-level targeting“

# Rozdíly mezi Preferences a Policy

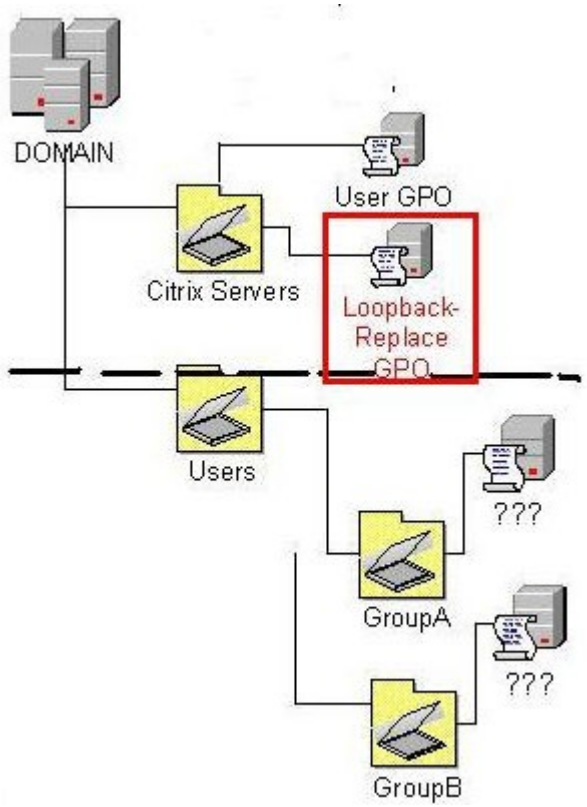
- Nastavení definovaná v Policy části zakáží i odpovídající interface v konfigurované app (je-li GPO aware)
- Pokud objekt vypadne ze scope GPO:
  - Klíče v registrech měněné nastaveními v Policy se vrátí na původní hodnoty
  - Klíče měněné nastaveními v Preferences zůstanou tak jak jsou (pokud nepoužiji „remove this item when it is no longer applied“)
- Pokud provedu nastavení v Policy, ve skutečnosti se nezmění odpovídající klíče v registrech, systém pouze použije nastavení z GPO více zde
- Policy se dají definovat v lokálních i doménových GPO, Preferences pouze v doménových

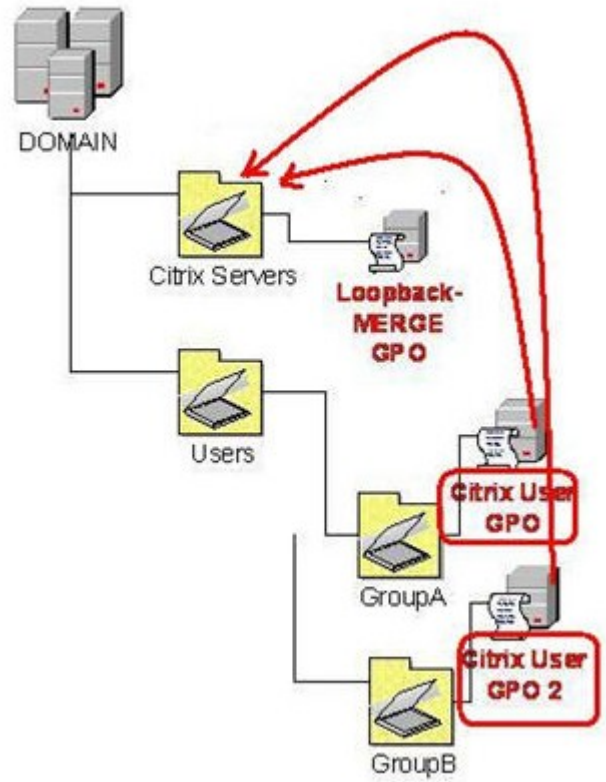
# Úkol

- Jak byste docílili toho, že na klientovi bude pokaždé jako homepage v IE stránka is.muni.cz? Tzn. ať už se přihlásí jakýkoli doménový uživatel.

# Loopback Processing

- Pro stroje kde chceme konzistentní prostředí bez ohledu na to, kdo se přihlásí
- **Z GPO aplikovaných na stroj se kromě Computer Configuration části začne aplikovat i User Configuration**
- Při přihlášení uživatele na stroj s loopbackem se u:
  - Merge – stáhne seznam uživatelových GPO, následně znovu seznam pro počítač, zařadí se za seznam GPO pro uživatele a postupně se vše aplikuje. Pokud dojde ke konfliktu některých nastavení, tak "vítězí" nastavení z GPO linkované na počítač
  - Replace – uživatelovy GPO vůbec nestahují. Seznam uživatelových GPO je nahrazen seznamem GPO linkovaných na daný stroj, přičemž User Conf. část politik se aplikuje **pod účtem uživatele**




Převzato z http://ibrahim.wikia.com/wiki/Article_of_the_Week:_Active_Directory_Integration_With_Citrix_-_GPO_Loopback_Processing

# Loopback Processing

- Computer Configuration -> Policies -> Administrative Templates -> System -> Group Policy -> Configure User Group Policy loopback processing mode
- Stroj, na který je GPO s user. conf. nastaveními aplikována musí mít na GPO alespoň READ (od Server 2008) a uživatel, který se přihlašuje musí mít na této GPO právo APPLY, jinak GPO nebude aplikována!
- Jakmile povolím, tak se začne aplikovat User Configuration část z **každé** politiky aplikované na daný stroj

# Úkol

- Zajistěte, aby jakýkoli uživatel, který se přihlásí na klienta, měl jako homepage v IE is.muni.cz
  1. Vytvořte GPO „Enable LoopBack - merge“, která povolí loopback v merge módu a nalinkujte na OU Klienti
  2. Vytvořte novou GPO „Loopback_IE homepage is.muni.cz“ se shodným nastavením jako má „IE homepage is.muni.cz“ a nalinkujte ji na OU Klienti
- Jak zajistíte výjimku z tohoto pravidla pro uživatele xbubla?
  - Dám mu **deny** právo na aplikování GPO „Loopback_IE homepage is.muni.cz“ linkované na OU Klienti (pozor projeví se i v GPO linkované na OU Uzivatele)
- Proč jsem nemohl nalinkovat rovnou GPO „IE homepage is.muni.cz“ a v ní jen upravit oprávnění?
  - Modifikuje se vždy daná GPO ne jen link tzn. xpepik by měl jako homepage seznam.cz
- Otestujte na klientovi oba úkoly pod účtem xpepik

# Úkol

- Zajistěte, aby jakýkoli uživatel, který se přihlásí na klienta, měl jako homepage v IE is.muni.cz
  1. Vytvořte GPO „Enable LoopBack - merge“, která povolí loopback v merge módu a nalinkujte na OU Klienti
  2. GPO „IE homepage is.muni.cz“ nalinkujte na OU Klienti
- Jak zajistíte výjimku z tohoto pravidla pro uživatele xbubla?
  - Dám mu **deny** právo na aplikování GPO „IE homepage is.muni.cz“ linkované na OU Klienti (pozor projeví se i v GPO linkované na OU Uzivatele, což ale nevadí)
- Jak zajistíte, že pouze členové skupiny Ucetni budou mit na klientovi vždy is.muni.cz jako homepage
  - Proč nemohu nalinkovat GPO „IE homepage is.muni.cz“ a v ní jen upravit oprávnění?
    - Modifikuje se vždy daná GPO ne jen link tzn. bych ovlivnil chování GPO na OU Uzivatele
- Otestujte na klientovi oba úkoly pod účtem xbubla

# Kontrolní otázky

- Když chci naprosto konzistentní prostředí ať už se přihlásí kdokoli, použiji merge či replace mód Loopback Processingu?
  - Replace
- Projeví se nějak zapnutý loopback i na lokálních uživatelích?
  - Ne. Nastavení lokálních uživatelů mohu měnit pouze lokálními politikami. Mohu ale udělat požadovaná nastavení no vybraném stroji (pro vybraného lok. uživatele), poté je vykopírovat na sdílenou složku a udělat logon skript, který je skopíruje do C:\Windows\System32\GroupPolicyUsers\SID_lok.uzivatele
- Na OU obsahující počítač PC1 jsou nalinkovány dvě GPO. První je enforce a nastavuje bílou plochu. Druhá zapíná loopback processing a zároveň nastavuje zelenou plochu. Jakou plochu bude uživatel mít po přihlášení na PC1? (Nastavení plochy je v user. conf. části.)
  - Bílou. Jelikož je zapnut loopback, vytvoří se seznam politik s user. conf. částí kde enforce politiky budou na konci = přebijí ostatní.

# Hledání konkrétního nastavení v GPO

- Pro hledání politik je možné použít zabudovaný search v GPMC
  - Mohu tak najít politiky které mají např. zadefinovaný nějaký startup script
- Mohu použít filter v Administrative Templates
- Online vyhledávání dostupných nastavení GPO
- Mohu si stáhnou xls se všemi dostupnými GPO a prohledávat ten

# Rekapitulace

- GPO mají nastavení zvlášť pro stroje a uživatele
- GPO se dají linkovat na sajtu, doménu, OU
- GPO se dědí shora dolů
  - Mohu ovlivnit pomocí block inheritance a enforce
- Na koho se bude GPO aplikovat mohu ovlivnit pomocí security a WMI filtrování
- Chci-li vytvořit konzistentní prostředí či prostě na stroj aplikovat nastavení z User Conf. části GPO použiji loopback processing

# Struktura GPO

- GPO se skládají ze dvou částí GP Container (GPC) a GP Template (GPT)
- **GPC** je **objekt** v AD uložený v ADUC\System\Policies\{GUID} obsahující atributy jako GUID, versionNumber, status, ... S touto částí GPO manipuluji v GPMC konzoli
- **GPT** je **kolekce souborů** uložená v %SystemRoot%\SYSVOL\FQDN\Policies\{GUID}, která obsahuje výsledné konfigurační soubory, které si klienti stahují a poté aplikují

# Úkol

- Prohlédněte si GPT i GPC politiky „IE homepage is.muni.cz“
  - Pro rychlé dohledání GUIDu můžete použít PS příkaz Get-Gpo –name „IE homepage is.muni.cz“
- Zejména soubor GPT.ini a Registry.pol

# Obsah GPT části

- Adm (pokud byla politika vytvořena v Server 2003)
- Group Policy
  - Obsahuje GPE.ini, který obsahuje seznam GUIDů pro každé CSE odkazované v GPO
- Machine
  - Applications
  - Microsoft
  - Preferences
  - Scripts
  - Registry.pol (nastavení z AT sekce)
- User (to samé jako Machine)
- GPT.ini (soubor obsahující číslo verze politiky,+1)
- Každé CSE vytváří jiný soubor pro svá nastavení

# GPO replication

- GPC a GPT se replikují zvlášť (proto může nastat problém, kdy stanice vidí v AD novou GPO (GPC), ale GPT ještě není v SYSVOL (Policy processing error)) nebo víc adminů modifikuje stejnou GPO ale na různých DC
- Replikace GPC v rámci Site probíhá v řádech sekund a mezi více Site dle aktuálního nastavení inter-site replikace
- GPT je replikováno v rámci replikace SYSVOLu
- Od Server 2008 replikace skrze DFS dříve FRS
- Editace GPO se standardně dělá na DC s PDC Emulator rolí

# Slow link detection

| Procesy | Aplikování při zjištění pomalé linky | Dá se změnit? |
|---|---|---|
| Zpracování zásad registru | Ano | Ne |
| Nastavení Internet Explorer | Ne | Ano |
| Politiky instalování SW | Ne | Ano |
| Politiky přesměrování adresy | Ne | Ano |
| Skripty | Ne | Ano |
| Politiky zabezpečení | Ano | Ne |
| Internet Protocol Security (IPSec) | Ne | Ano |
| Politiky bezdrátových sítí | Ne | Ano |
| EFS Recovery | Ano | Ano |
| Politiky diskových kvót | Ne | Ano |

# Co je potřeba brát v potaz při aplikování GPO

- GPO linkované na sajtu, doménu, či OU a jestli jsou povolené
- Zdali je GPO enforced
- Zdali je někde block inheritance
- Security & WMI filtering
- Samotná hodnota nastavení (Enable | Disable | Not configured)
- (Preferences targeting)
- Loopback policy processing
- Slowlink detection
- User politiky se aplikují pod účtem uživatele Computer pak pod účtem stroje

# CSE (Client Side Extension)

- CSE jsou knihovny dll (System 32), které aplikují stažená „surová data“ (GPT část) doménových politik na daný stroj
- O různé části GPO se starají různé CSE (Security CSE, Group Policy Drive Maps CSE,…)
- Seznam CSE je uložen v HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions
- Pokud by chyběla nějaká knihovna či byl poškozen registr, tak politiky které zpracovává se nemohou aplikovat!

# Zpracování GPO (stroj)

- Počítač najde DC a přihlásí se k němu. Pro úspěšné přihlášení musí být povolené následující porty. UDP 53 (DNS), UDP a TCP 389 (LDAP), TCP 135 (RPC Portmapper), UDP 88 (Kerberos)
- Počítač zjistí zda je na pomalé lince (Slow Link Detection). Pomocí NLA (network location awareness )(dříve ICMP paketů)
- Pomocí LDAPu zjistí jaké GPO jsou nalinkovány na OU, doménu, sajtu. Z těchto odpovědí si vytvoří seznam všech GPO které jsou na něj aplikovány
- Pomocí LDAPu pošle počítač otázku na seznam WMI filtrů na všechny GPO, které našel + si požádá o atributy jako je cesta ke GPT, číslo verze GPC, gpCMachineExtensionNames a gpCUserExtensionnames attribut.
- Počítač se pomocí SMB (port TCP 445) připojí k SYSVOLu a přečte si GPT.INI pro každou GPO která se na něj aplikuje

# Zpracování GPO (stroj)

- Group Policy process začne porovnávat verzi GPO v SYSVOLu s verzí GPO kterou má lokálně uloženou (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History)
- (Pokud se verze GPO nezměnila je přeskočena. V GPO se dá nastavit aby se toto nedělo a politiky se aplikovali pokaždé i když nenastala změna. Toto se dá vynutit i přes CMD pomocí příkazu gpupdate /force)
- CSE (Client Side Extension) zjistí zda má dostatečná práva na všechny GPO, které se mají aplikovat. Pokud ne dané GPO je vyhozeno ze seznamu. Pokud je na GPO nastaveno Enforced (vynucené) je v tomto kroku přeneseno na konec seznamu. Tzn. že nastavení z tohoto GPO vždycky vyhrají pokud nastane nějaký konflikt.
- CSE začne zpracovávat jednotlivá GPO (přesněji stažené GPT soubory)
- Po každém zpracovaní GPO, CSE zaloguje RSoP (Result of Policy) přes WMI do CIMOM databáze

# Starter GPOs

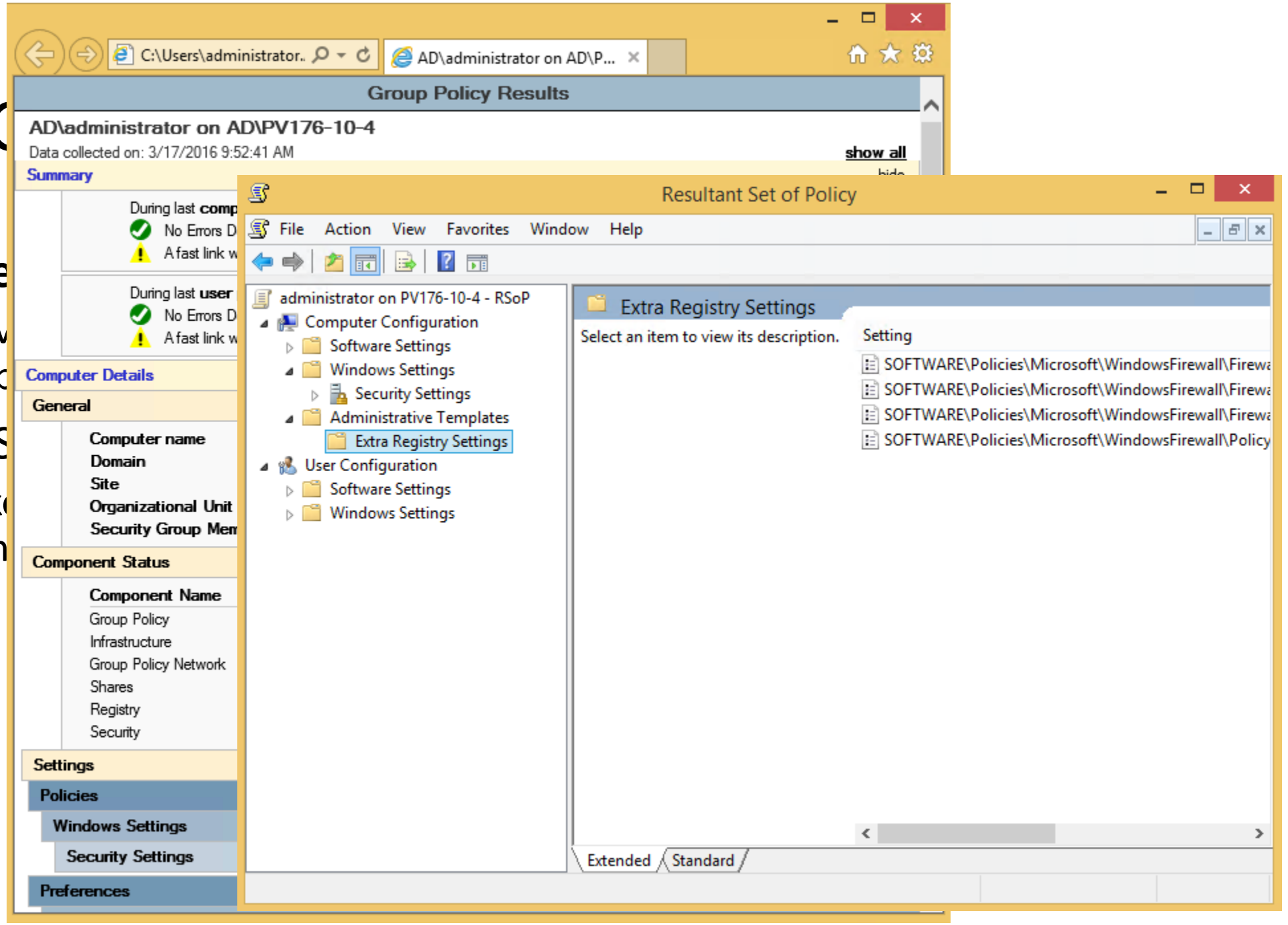
- Od Windows Server 2008
- Sada read-only politik s nadefinovanou sadou nastavení
- Mohou sloužit jako základ pro nové politiky
- Nové Starter GPO mohou obsahovat pouze nastavení z Administrative Templates
- Změny provedené v Starter GPO se neprojeví v politikách už vygenerovaných
- Popis EC a SSLF zde

# Ladění GPO GPMC

- Group Policy Results
  - Pro vybraný počítač a uživatele zobrazí, výsledek aplikování GPO. Chci-li výsledky i pro uživatel, je nutné, aby se na vybraném stroji alespoň jednou přihlásil (jinak není co zobrazovat).
- Group Policy Modeling
  - Group Policy Modeling, na rozdíl od předchozího aplikaci politik pouze simuluje a jedná se především o nástroj pro prověření nového nastavení před jeho nasazením do ostrého prostředí.

# Ladění G

- Příkaz **gpre**
  - Slouží k v
    Umí i exp
- Resultant S
  - V mmc k
    nastaven



# Úkol

- Vytvořte GPO s FW výjimkami potřebnými pro správnou funkčnost **Group Policy Results** na **všech** klientech v doméně (**použijte Starter GPO „Group Policy Reporting Firewall Ports“**)
- Otestujte zobrazením výsledků GP Results z klienta

- Na klientovi, kde jste přihlášení pomocí doménového účtu
  - Spusťte v CMD gpresult /F /H result.html a ten pak otevřete
  - Spusťte RSOP.msc

# Ladění GPO

- Event Viewer
  - System – zdroj Group Policy
  - Applications and Services Logs\Microsoft\Windows\GroupPolicy\Operational
  - Sledování konkrétního zpracování GPO User/Computer (pomocí ActivityID)
    - V logu najít záznam GPO který nás zajímá a v XML – friendly view zkopírovat hodnotu ActivityID

    a) Použít dané ID v PS skriptu Get-GPEventByCorrelationID.ps1

    b) Vytvořit Custom view. Jako xml query použít <QueryList><Query Id="0" Path="Application"><Select Path="Microsoft-Windows-GroupPolicy/Operational">*[System/Correlation/@ActivityID='{sem vlozit ACTIVITYID}']</Select> </Query></QueryList>

# Ladění GPO

PolicyReporter

- Po zapnutí debug logování zpracování GPO umožňuje snadné procházení vygenerovaného logu
  - Zapnutí logování se provede vytvořením registry záznamu HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Diagnostics - GPSvcDebugLevel (DWORD 0x30002)
  - Jak pracovat s GPSVC.log

Gplogview.exe

- Umožňuje realtime monitorování zpracování GPO (-m)
- Umožňuje vyexportovat event logy do souboru
  - I dle ActivityID (gplogview.exe –a ActivityID –o log.txt)

GPMonitor.exe

- Dostupný v  Windows Server 2003 Resource Kit Tools
- Logy ze strojů zasílá na centrální úložiště kde mohou být dále spravovány

# Úkol

- Z 05_tools.zip extrahujte GPLogView a PolicyReporter

- Zapněte na klientovi skrze GPO nebo importem ‘zapnuti debug logovani gpo.reg’ debug logování GPO
- Restartujte klienta, nainstalujte PolicyReporter a prohlédněte si log

- Spusťte GPLogView na klientovi v admin CMD s parametrem –m
  - V jiném CMD okně spusťte gpupdate /force a sledujte výstup
- Spusťte s parametrem –h –o report.html a prohlédněte výsledek

# Ladění GPO

- Zapnutí debug logů - CC\AT\System\Group Policy
- Dcgpofix (utilita pro obnovení Default domain policy a Default domain controllers policy)
- HKLM\software\microsoft\windows\currentversion\group policy
- Gpotool.exe (nástroj pro kontrolu konzistence verze GPT a GPC)
- Má klient správný DNS, IP, existují SRV záznamy pro DC,..?
- Politika, která používala nějaký WMI filtr se po jeho smazání přestane aplikovat (je potřeba zrušit WMI filtrování na dané GPO)
- Je na klientovi správný čas? Pokud nesedí o víc jak 5min tak se klient neautentizuje (Kerberos) = nestáhne politiky

# Operace s GPO

- Copy (ACL, Group Policy Objects)
- Back Up (links, permissions,files)
- Restore From Backup
- Import Settings
  - neimportuje linky ani oprávnění
  - Používá se u non-trusted domén kde se nedá použít copy-paste
- Save Report
- Delete (smaže GPO a všechny linky)
- Rename (linky jsou zachovány protože používají GUID)
- Link Enabled (mohu zakázat tento link – na výkon to ale vliv nemá)

# Operace s GPO

- Povolení/zakázání Computer/User části GPO
  - Motivace – větší rychlost zpracování politik => spokojenější uživatelé.
- Povolení/zakázání GPO
- Delegace oprávnění na GPO
  - Kteří uživatelé nebo skupiny mají oprávnění s politikou nakládat.
  - Využije se především ve větších prostředích, kde se uplatňuje více úrovní správců

# Naming conventions

- OU pojmenovávat krátkými stručnými, ale výstižnými názvy
- Rozmyslet se jestli OU budou rozděleny dle geografické či organizační struktury
- Používat konzistentní pojmenování (desktop==workstation)
- GPO pojmenovávat dle struktury OU na kterou jsou linkovány př. Pocitace_Zamestnanci_Ucetni) z vrchu – dolů (kvůli přehlednosti i v rsop..) nebo dle užití dané GPO
- Ve jméně zbytečně nepoužívat slova jako politika, GPO

# Best Practices

- Aplikovat GPO pokud možno na co nejvyšší úrovni
  - maximálně využívat dědičnost
- Neupravovat defaultní politiky, ale vytvořit nové
- Omezit množství skupinových politik
  - Každá konfigurační změna by měla být ideálně v nejvýše jedné GPO
  - Vhodné spíše kvůli přehlednosti než rychlosti zpracování
- Pomalost zpracování je než počtem gpo způsobena: spouštěním skriptů, mapování tiskáren, disků případně používáním wmi filtrů (raději používat item level targeting pokud je to možné)
- Dodržovat jmenné konvence názvů GPO
- Skupinové politiky aplikujte na Site pouze v případě , že se vztahují opravdu k rozsahu Site a ne k doménám

# Best Practices

- Vyvarovat se použití Block inheritance a Enforce inheritance
- Typicky 80% politik bude obsahovat většinu nastavení a bude statických a 20% bude obsahovat specifická nastavení, která se budou měnit častěji (monolitic vs functional approach)
- Pokud mám nějaká nastavení, která se často mění, je lepší pro ně vyhradit samostatnou GPO (aby se nemusely při každé změně aplikovat i nastavení která se v rámci té GPO nezměnily)
- Zakázat user/computer část GPO pokud se nepoužívá
- Pokud máte Software Assurance používejte Advanced Group Policy Management (verzování GPO,..)
- U používání security filtrování používat raději skupiny než samotné uživatelské účty (neodstraňovat úplně authenticated users, ale jen odebrat právo apply group policy, jinak bude politika Inaccesible)
- Stroje administrátorů mít v samostatné OU
- Mít testovací OU s testovacími GPO
- Zálohovat ☺

# Užitečné odkazy

- Group Policy Planning and Deployment Guide
- Administrative templates
- Troubleshooting (2)
- Jak použít WPA pro vyřešení pomalého zpracování GPO (supr)
- Podrobné info k GPO Preferences
- http://channel9.msdn.com/Events/TechEd/NorthAmerica/2014/WIN-B328#fbid=?hashlink=fbid zajímavé video
- https://technet.microsoft.com/cs-cz/library/dn581922.aspx souhrn

# GPO novinky v Win8 & Server 2012

- Gpupdate přímo v GPMC konzoli
- Vylepšené Group Policy Results v GPMC konzoli
- Nové Starter GPOs
- Pro Win8.1 je automaticky posunuto zpracování logon skriptů o 5 minut
- Nové podrobnější záznamy v Event Logu
  - ID 4257 GP policy download start
  - ID 5257 GP policy download end
  - …
- Nové možnosti logování zpracování GPO dostupné v GPO ☺
- Group Policy Caching odkaz
- Fine Grained Policy odkaz
- Další zde