GPO

Co jsou GPO

- Skupinová politika (Group Policy, GPO)
  - Sada předvoleb, která nastavuje chování počítače a možnosti uživatelů
  - S její pomocí lze nastavovat registry, NTFS oprávnění, politiky bezpečnosti a auditu, instalace softwaru, přihlašovací a odhlašovací skripty, přesměrování adresářů, nastavení IE a další
  - V doménovém prostředí umožňují centralizovanou správu
  - Správa pomocí nástroje Group Policy Management Console

Local vs Domain GPO

- Domain GPO
  - Vytvářeny a ukládány na DC (SYSVOL)
  - Aplikují se na vybrané doménové uživatele a počítače
  - Automaticky se vytvoří Default Domain Policy a Default Domain Controllers Policy
  - 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)
    - Account Policy se mohou definovat jen v GPO linkované na doménu
  - Default Domain Controllers Policy
    - Aplikuje se jen na DC
    - Definuje základní pravidla zabezpečení, auditování a práv uživatelů (User Rights)

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, gPCMachineExtensionsNames,.. ale neobsahuje žádná GPO nastavení!
- GPT je kolekce souborů uložená v %SystemRoot%\SYSVOL\MojeDoména\Policies\{GUID}, která obsahuje nastavení dané politiky včetně nastavení administrativních šablon, zabezpečení, instalace software, skriptů,..

GPO settings

- Nastavení v GPO je rozděleno do 2 částí
  - Computer configuration
    - Vztahuje se pouze na účty počítačů
    - Nastavení počítače bez ohledu na to, který uživatel s ním pracuje
  - User configuration
    - Vztahuje se pouze na účty uživatelů
    - Uživatelská nastavení bez ohledu na to, ke kterému počítači se uživatel přihlašuje
  - .. Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates
    - Preferences

Administrative Templates

- Šablony obsahující nastavení systému/uživatele
- Provádějí změny v chráněné části registrů (standard. uživ. nemohou změnit)
- Do Windows XP/Server 2003
  - Textový soubor s koncovkou ADM
  - Obsahoval jak nastavení, tak UI pro GPMC
  - ADM šablony jsou uloženy v C:\Windows\inf
  - ADM šablony se kopírují do každé GPO kde jsou použity (bobtnající SYSVOL)
  - Pro každý jazyk další ADM soubor
- Od Windows Vista/Server 2008
  - Xml formát kde se jedna šablona skládá ze dvou částí (adml,admx)
  - Neukládají se v GPO
  - Adml soubor obsahuje jen UI pro GPMC konzoli (jeden soubor pro každý jazyk)
  - Admx soubor pak obsahuje nastavení (klíče registru včetně hodnot)
  - ADMX šablony jsou uloženy v %SystemRoot%\PolicyDefinitions nebo v Central Store
- Zadefinované změny se ukládají v souboru registry.pol (v GPT), který slouží pro nastavení cílových objekt.

Administrative Templates

- Central store je adresář v SYSVOL, který slouží jako centrální úložiště pro všechny admx šablony používané v dané doméně
  - Vytvořím jej zkopírováním adresáře C:\Windows\PolicyDefinitions do \\FQDN\SYSVOL\FQDN\policies\
- Tyto šablony se dají vytvořit ručně či nástroji jako admxmigrator
- Někteří výrobci poskytují tyto správcovské šablony pro snadnou centrální správu svých aplikací (MS Office, Google, Adobe,..)
- Managed vs Unmanaged policy settings
  - Managed
    - Při vypadnutí uživatele | stroje ze scope politiky se změny ztratí
    - HKLM\Software\Policies (to samé pro HKCU)
    - HKLM\Software\Microsoft\Windows\Current Version\Policies (-||-)
    - Tyto klíče jsou chráněny, tedy ne-administrátoři nemohou tyto nastavení změnit
  - Unmanaged
    - Změny jsou trvalé (i při vypadnutí ze scope politiky nastavení zůstanou)
    - Standardně jsou v GPMC skryty (filter options – managed – no)

Kontrolní otázky

1. Pokud mám v doméně Central store pro ukládání AT, použije se při aplikování politiky AT z lokálního úložiště AT daného stroje nebo z Central store?
   - Ani jedno, protože při aplikování GPO už nejsou samotné AT potřeba. Vezmou se nastavení registru z vytvořeného registry.pol souboru (uložen v GPT) a ty se (díky CSE) aplikují na stroj/uživatele.
2. Jaké jsou výhody Central store?
   - Snadný update pokud dojde k vydání nových AT. Snadná distribuce ručně vytvořených AT.
3. Pokud používáme systém s ADMX šablonami, můžeme přidat i staré ADM?
   - Můžeme skrze GPMC konzoli. Zobrazí se poté v Administrative templates - Classic Administrative Templates (ADM).
4. Pokud vytvořím politiku v OS Server 2003 a poté provedu povýšení domény na Server 2008 zůstanou v GPT části GPO i adm soubory?
   - Ano. Řešením je buď vytvořit politiky znovu (import nastavení nepomůže protože se importují i adm soubory). Nebo v GPO pravým na AT a Add/Remove Templates...a odebrat staré templates.
5. Jak se zbavit bugu u filtrování AT (nic to nenajde)?
   - Přepnutím klávesnice na anglickou ☺
6. V jakém souboru v GPT se ukládají změny nadefinované v AT?
   - V adresáři dané politiky v souboru Registry.pol.

Preferences

- Preferences
  - Od Windows Vista
  - Obsahují nepovinná nastavení (uživatelé mohou změnit)
  - Mapování disků, systémové proměnné, registry, power options, start menu options, printers, scheduled tasks, .. (př. Zakázání možnosti připojit usb hdd)
  - Změny jsou trvalé (i po vypadnutí ze scope politiky) až na výjimky (remove this item when it is no longer applied)
  - Na rozdíl od AT po odebrání smažou daný klíč (nevrátí se na původní hodnotu)
  - Item-level targeting

GPO replication

- GPC a GPT se replikují zvlášť a proto může nastat problém, kdy stanice vidí v AD novou GPO (GPC), ale GPT ještě není v SYSVOL (Policy processing error)
- 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
- Gpotool pro kontrolu verze GPT a GPC nějaké GPO

Linkování GPO

- Linkování = přiřazení GPO na nějakou strukturu v AD
- GPO je možné přilinkovat na úrovni
  - Site
    - na všechny objekty v rámci lesa spadající do dané Site
    - GPO je uložena na DC kde byla vytvořena (proto musí být stále dostupný!)
    - Neukazují se v „Linked Group Policy Objects“
  - Domain
    - Pozor nezdědí se na child domény
  - OU
- Na každé úrovni je možné přilinkovat libovolné množství GPO (aplikuje se však jen 999)

Dědičnost

- Nastavení GPO je dědičné
  - Na objekt uložený v OU se aplikují:
    - Všechny GPO přilinkované na site, do které spadá IP adresa stroje
    - Všechny GPO přilinkované na doménu, ve které se objekt nachází
    - Všechny GPO přilinkované na všechny nadřazené OU
    - Všechny GPO přilinkované přímo na OU ve které je uložen
- Block inheritance
  - Nastavuje se na úrovni OU
  - Blokuje dědičnost všech politik uvedených hierarchicky výš od vybrané OU, krom enforced politik
- Enforce inheritance
  - Aplikuje se na GPO
  - Vynutí dědičnost vybrané GPO hierarchicky níž do všech OU, i kdyby byly cestou nějaká blokování
  - Enforce GPO se aplikují jako poslední (v případě více enforced GPO platí, čím výš tím silnější = domain gpo > ou gpo)

Pořadí zpracování GPO

- GPO se zpracovávají v tomto pořadí:
  - (Lokální politiky jsou-li nějaké a nejsou-li zakázány)
  - Všechny GPO přilinkované na Site, do které spadá IP adresa stroje
  - Všechny GPO přilinkované na doménu, ve které se objekt nachází
  - Všechny GPO přilinkované na všechny nadřazené OU
  - Všechny GPO přilinkované přímo na OU s objektem
- V případ konfliktních nastavení mezi více GPO se uplatní nastavení z GPO, která je blíže samotnému objektu (například v případě kolize nastavení na úrovni domény a OU se uplatní nastavení GPO přilinkované na OU)
- Pokud jsou konfliktní GPO na stejné úrovni, rozhoduje pořadí zpracování (hodnota Link Order – GPO s nejnižším číslem se aplikuje jako poslední)

Kontrolní otázky

V Default Domain Policy která je **enforced**, je zapnuto (enable) zakázání spouštění regeditu.

Na OU ve které je umístěn PC1 je nalinkovaná GPO, která je taktéž **enforced** a ta zakazuje zákázaní spouštění regeditu (disable na danou politiku) ☺

1. Když se uživatel přihlásí k stroji PC1 bude moct spustit regedit nebo ne?
   - Nebude moct, protože u více enforced politik platí, že čím „výš" politika je tím je „silnější". Default Domain Policy je v hierarchii GPO výše než GPO linkovaná na OU, tedy přebije její konfliktní nastavení.

GPO Scope

- Filtrování zabezpečení (Security Filtering)
  - Možnost, jak zjemnit aplikaci GPO na konkrétní uživatele a/nebo skupiny
  - Může být v některých případech velkým usnadněním práce se skupinovými politikami, ale naproti tomu může vést k nesmírným problémům při ladění politik a při jejich správě
  - Ve výchozím nastavení mají členové skupiny Authenticated Users (všichni autentizovaní uživatelé i počítače) právo READ a APPLY GROUP POLICY na každou GPO.
  - Exclude skrze záložku Delegation (deny – apply group policy)
  - Deny oprávnění se nijak nezobrazují v Security filtering u GPO

GPO Scope 2

- Filtrování pomocí WMI
- WMI = Windows Management Instrumentation
  - Dynamická aplikace skupinových politik = když se má na počítač nebo uživatele aplikovat GPO obsahující WMI filtr, tak si AD nejdříve ověří zda počítač či uživatel splňují podmínku WMI filtru a teprve v případě úspěchu je tato politika aplikována.
  - WMI dotazovací jazyk (WQL) má podobnou syntaxi jako SQL.
  - Příklady:
    - test zda se jedná o 64b OS

    SELECT * FROM Win32_Processor WHERE AddressWidth = '64'

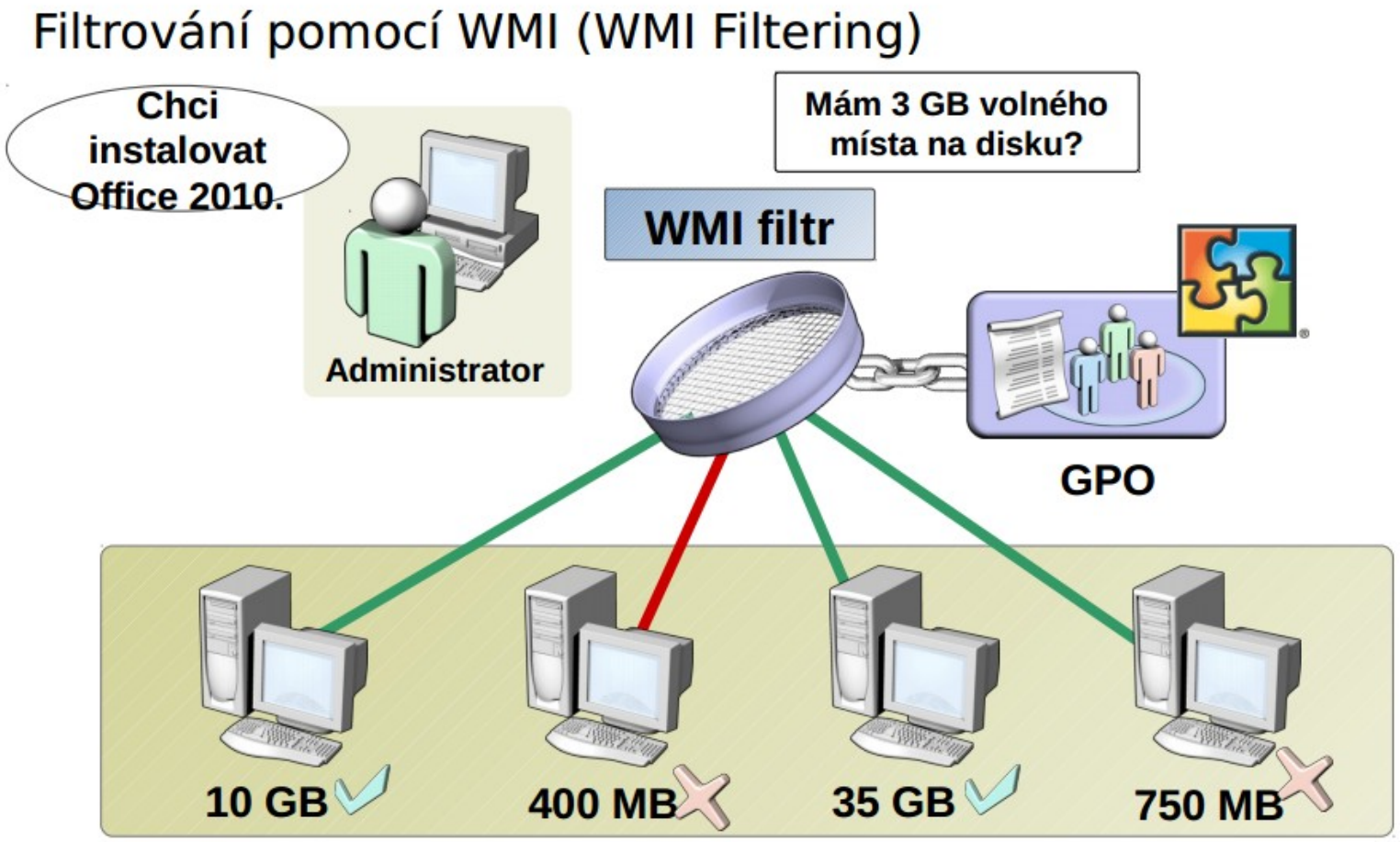
    - test zda se jedná alespoň o OS Windows Vista či Server 2008

    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"

WMI Filtering



Loopback Processing

- Loopback processing
  - Pro stroje kde chceme konzistentní prostředí bez ohledu na to, kdo se přihlásí
  - Na stroj je aplikována i User Configuration část GPO (ne jen Computer Configuration)
  - Jak stroj, na který je gpo aplikována, tak uživatel, který se přihlašuje musí mít právo GPO aplikovat (security filtering)
  - Jakmile povolím tak se aplikuje User Configuration část z **každé** politiky aplikované na daný stroj (ne jen z té, ve které jsem loopback povolil)
  - Computer Configuration -> Policies -> Administrative Templates -> System -> Group Policy -> User Group Policy loopback processing mode
  - rsop může ukazovat, že se politiky neaplikovaly (pokud obsahují jen user conf.)
- Merge – stáhne se seznam politik pro uživatele, následně znovu seznam pro počítač, zařadí se za seznam politik pro uživatele a postupně se vše aplikuje. Pokud dojde ke konfliktu některých nastavení, tak "vítězí" nastavení počítače
- Replace – stáhnou se pouze politiky pro počítač a použijí se jako nastavení pro uživatele

Kontrolní otázky

- V Default Domain Policy která je enforced je zapnut Loopback processing mode a nastaveno (enabled) skrytí ikony koše v user configuration části GPO
- Na OU kde je pc1 je nastaveno Block Inheritance a je v ní přilinkována politika, která v User Configuration části zakazuje (disabled) politiku skrytí ikony koše

1. Pokud se přihlásí doménový administrátor na stroj pc1 bude mít na ploše ikonu koše či nikoli?
   - Nebude. Je zapnut loopback processing (díky enforce projde doménová politika i přes block inheritance a stejně tak díky enforce má větší váhu než na OU nalinkovaná politika)
2. Pokud se přihlásí lokální uživatel pepik na stroj pc1 uvidí ikonu koše?
   - Uvidí. Na **lokální uživatelské** účty se nedají aplikovat doménové politiky (mohu ale nakonfigurovat lokální politiky a pak je rozkopírovat do C:\Windows\System32\GroupPolicy)

Kontrolní otázky

1. Je potřeba mít v Security Filtering politiky nalinkované na OU s pc1, která zapíná Loopback Processing a definuje nějaká nastavení v User Configuration části i účet uživatele/skupiny nebo stačí účet pc1?
   - Je potřeba jak účet stroje(pc1) tak účet uživatele/skupiny na které se má politika aplikovat
2. Jak pomocí Security Filtering docílit toho, že když se k pc1 přihlásí xadmin tak na ploše bude mít ikonu koše, ale kdokoli jiný ji bude mít skrytou?
   - Pro stroj pc1 zapnu loopback processing a v security filtering politiky, která zakazuje zobrazení koše přidám uživatele xadmin a dám mu deny na apply group policy
3. Jak docílit toho, že pouze když se k pc1 přihlásí někdo ze skupiny GG_homeless, tak se na ploše skryje ikona koše?
   - Pro stroj pc1 zapnu loopback processing a v security filtering politiky, která zakazuje zobrazení koše vyhodím authenticated users a přidám jen účet stroje a skupiny GG_homeless
4. Když nechci aby se vůbec stahovala user configuration část GPO uživatele hlásícího se na stroj ps1, použiji merge či replace mód Loopback Processingu?
   - Replace

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 vše má vliv na výsledný průnik nastavení

- GPO linkované na sajtu, doménu, či OU a jestli jsou povolené
- Zdali je GPO enforced
- Zdali je někde block inheritance
- Security filtering
- WMI filtering
- Enable | Disable | Not configured
- Preferences targeting
- Loopback policy processing
- Slowlink detection

Aplikace GPO

- Foreground GP processing
  - Computer politiky se aplikují při startu pc
  - User politiky se aplikují při přihlášení uživatele
- Background refresh probíhá každých 90min +- 30 (nastavitelné)
  - Defaultně se aplikují pouze změněné GPO (VersionNumber)
  - Security politiky se aplikují každých 16hodin ať se změnily či ne (každých 5minut na DC)
- Ruční refresh
  - pomocí gpupdate /force
- VersionNumber se ukládá jako atribut GPC a v GTP v souboru GTP.ini
- Ne každá politika může být aplikována na pozadí (některé kolem auditování, intalace software, přesměrování adresáře, mapování disků, skripty,..)

CSE (Client Side Extension

- CSE jsou knihovny dll, které aplikují stažená „surová data“ (GPT) doménové politiky na daný stroj
- O různé části GPO se starají různé CSE (Security CSE, Group Policy Drive Maps CSE,…)
- Každé CSE má vlastní GUID pro jednoznačnou identifikaci (tento GUID je uložen jak v GPT = GPE.ini tak v GPC = gPCMachineExtensionNames, gPCUserExtentionNames)
- Seznam CSE včetně GUID a dll je uložen v HKLM\ Software\ Microsoft\ Windows NT\ CurrentVersion\ Winlogon\ GPExtensions
- Pokud by chyběla nějaká knihovna, tak politiky které zpracovává se nemohou aplikovat!

Zpracování GPO

- Jak se GPO zpracovává při spuštění počítače:
- Počítač najde DC a přihlásí se k němu, stejně jako uživatel. Pro úspěšné přihlášení musí být povolené následující porty. UDP 53 (DNS), UDP a TCP 389 (LDAP), TCP 135 (RPC Portmapper), UDP 88 (Kerberos)
- Počítač pomocí NLA (network location awareness)(dříve ICMP paketů) zjistí zda je na pomalé lince (Slow Link Detection)
- 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 filtrů na všechny GPO, které našel + si požádá o atributy jako je cesta ke GPT, číslo verze GPC, gpCMachineExtensionNames a gpCUserExtensionnames attribut.
- Počítač pomocí SMB (port TCP 445) se připojí k SYSVOLu a přečte si GPT.INI pro každé GPO které se na něj aplikuje.

Zpracování GPO 2.

- Group Policy process začne porovnávat verzi GPO 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
- Po přihlášení uživatele, se celý proces opakuje s nastaveními aplikovanými na uživatele

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 vliv nemá)

Operace s GPO 2.

- Povolení/zakázání Computer/User části GPO
  - Motivace – větší rychlost zpracování politik => spokojenější uživatelé.
- 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

Starter GPOs

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

Search

- Pro hledání politik je možné použít zabudovaný search v GPMC
- Mohu tak najít politiky které mají např. zadefinovaný nějaký startup script
- Online vyhledávání dostupných nastavení GPO

Ladění GPO

- Group Policy Results
  - Group Policy Results je obdobou příkazu gpresult.exe. Tedy pro vybraný počítač a uživatele zobrazí, jak se aplikovaly politiky. GPO Results je možné provádět pouze na lokálním počítači, nebo počítači, který je dostupný pomocí RPC (remote procedure call) na portu 135 a uživateli, který byl minimálně jednou přihlášen, tedy již se na něj jednou politiky aplikovaly. (AT \ Network \ Network Connections \ Windows Firewall \ Domain Profile - Windows Firewall: Allow Inbound Remote Administration Exception)
  - Resultant Set of Policy (RSoP.msc)
- 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 GPO 2

- Event Viewer
  - System – zdroj Group Policy
  - Applications and Services Logs\Microsoft\Windows\GroupPolicy\Operational
  - Sledování konkrétního zpracování GPO (pomocí ActivityID)
    - V systém logu najit záznam GPO který nás zajímá a v XML – friendly view zkopírovat hodnotu ActivityID
    - 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 3

- Zapnutí debug logů - Computer Configuration \ Policies \ Administrative Templates \ System \ Group 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)

Ladění GPO 4

Gplogview.exe

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

Dcgpofix

- Utilita pro obnovení Default domain policy a Default domain controllers policy

GPMonitor.exe

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

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..)
- Ve jméně zbytečně nepoužívat slova jako politika a GPO

Best Practices

- Aplikovat GPO pokud možno na co nejvyšší úrovni
  - maximálně využívat dědičnost
- Neupravovat defaultní politiky, ale raději přidat 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 2

- 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 ☺

Úkoly

1. Přidat do domény stanici s Windows 7
2. Najít a prohlédnout si úložiště GPO (SYSVOL a AD)
3. Projít User configuration a Computer configuration

Úkoly 2

- Vytvořte strukturu OU
  - Pocitac (sem přemístěte server3)
    - Ucebna (sem přemístěte klientský stroj)
- Vytvořte GPO Pocitac a Pocitac_Ucebna a nalinkujte je na příslušné OU

1. Nastavte GPO tak, aby uživatelé, kteří se přihlásí na server3 nemohli spustit regedit. Na klientovi jim však spustit půjde.
2. V GPO Pocitac přidejte v Allow log on through Remote Desktop Services (User rights assignment) skupinu Domain Users
3. V GPO Pocitac přidejte domain users do restricted groups – remote desktop users.
4. V GPO Pocitac nastavte aby se na strojích do systémové proměnné PATH přidalo C:\temp, ale po vypadnutí stroje ze scope této politiky se hodnota zase odstranila! (Preferences)
5. Každý uživatel, který se přihlásí na jakýkoli ze strojů v OU Pocitace bude mít zamčený taskbar a nebude moct ani měnit jeho properties (UC\AT\..)
6. Vynuťte aplikování skriptů i při detekci pomalé linky a i když nedošlo k modifikaci gpo (CC\AT\System\..)

Úkoly 3

- Vytvořte strukturu OU
  - Uzivatele
    - Studenti
    - Ucitele
- Vytvořte GPO Uzivatele, Uzivatele_Studenti a Uzivatele_Ucitele a nalinkujte je na příslušné OU
- Nastavte aby všichni uživatelé v OU Uzivatele měli v IE homepage „lamer.cz“, učitelé však budou mít jako homepage „is.muni.cz“
- Studentům odeberte RUN dialog ze start menu (budou stále moci použít zkratku win +r?)
- Pro všechny změňte interval background refresh zpracování user configuration části GPO na 15min (UC\AT\System\Group Policy)
- V GPO Uzivatele nastavte zakázání spouštění regeditu. Učitelé však musí být schopni jej spustit!
- Nastavení zkontrolujte přihlášením skrze studentský a učitelský účet na server3 a win7 klienta

Úkoly 4

- Vyzkoušejte chování v případě použití Block inheritance a Enforce (na víc GPO které nastavují stejnou věc)
- Vyzkoušejte chování při zakázání GPO a následném gpupdate na stanici na kterou se měla aplikovat (kontrola přes rsop)

Úkoly 5

1. Vytvořit Central store pro admx (vytvořit adresář %SystemRoot%\SYSVOL\domain\Policies\PolicyDefinitions a do něj nakopírovat obsah adresáře %SystemRoot%\PolicyDefinitions (zkontrolovat v nějaké gpo kliknutím na administrative templates)
2. Stáhnout AT pro Google Chrome a nahrát je do Central store. Ověřit, že se ukazují při editování GPO
3. Na klientovi vyzkoušet rsop.msc a gpupdate /force
4. Zazálohovat GPO a poté zkusit obnovu a import settings
5. Vyzkoušet powershell cmdlety pro práci s GPO
    1. import-module grouppolicy
    2. get-command –module grouppolicy