Skupinové politiky

Co je skupinová politika?

- Skupinová politika (Group Policy, GPO)
  - Sada předvoleb, která nastavuje chování počítačů 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
  - Správa pomocí nástroje Group Policy Management Console

Struktura GPO

- GPO jsou uloženy na dvou místech
  - V kontejneru skupinové politiky (Group Policy Container, GPC)
  - V šabloně skupinové politiky (Group Policy Template, GPT)

- Kontejner skupinové politiky
  - Objekt Active Directory
  - Active Directory Users and Computers -> System -> Policies
  - Obsahuje stav GPO, informaci o verzi, informaci o WMI filtrech, seznam komponent, které mají nastavení v GPO

Struktura GPO

- Šablona skupinové politiky (Group Policy Template, GPT)
  - Adresářová struktura v adresáři SYSVOL na doménovém řadiči (%systemroot%\SYSVOL\sysvol)
  - Obsahuje kompletní nastavení a informace o GPO včetně nastavení administrativních šablon, zabezpečení, instalace softwaru, skriptů a přesměrování adresářů
  - Administrativní šablony (soubory .adm) obsahují změny v nastavení registrů počítače a/nebo uživatele; pro Windows Vista se používají nové šablony v XML formátu (soubory .admx)
  - Název GPT adresáře je GUID (Globally Unique Identifier) GPO, které jsme vytvořili; to je identické s GUIDem, který používá AD k identifikaci GPC tohoto objektu

Struktura GPO

- 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

Použití GPO

- GPO je možné přilinkovat na úrovni
  - Organizační jednotky
  - Domény
  - Site
- Nastavení GPO je dědičné
  - Na objekt uložený v kontejneru/organizační jednotce se aplikují
    - Všechny GPO přilinkované přímo na tento kontejner
    - Všechny GPO přilinkované na všechny nadřazené kontejnery
    - Všechny GPO přilinkované na doménu, ve které se objekt nachází
    - Všechny GPO přilinkované na site, do které spadá IP adresa stroje

Použití GPO

- Na každé úrovni je možné přilinkovat libovolné množství GPO
- V případě 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

- Block inheritance
  - Nastavuje se na úrovni OU
  - Blokuje dědičnost všech politik uvedených hierarchicky výš od vybrané OU, kromě vynucených politik
- Enforce inheritance
  - Aplikuje se na GPO
  - Vynutí dědičnost vybrané GPO hierarchicky níž do všech OU, i kdyby byly cestou nějaká blokování

Best practices – nasazení GPO

- Aplikovat GPO pokud možno na co nejvyšší úrovni
  - maximálně využívat dědičnost
- Omezit množství skupinových politik
  - Každá konfigurační změna by měla být ideálně v nejvýše jedné GPO
- Vytvářet specifické skupinové politiky
- Dodržovat jmenné konvence názvů GPO
- Skupinové politiky aplikujte na Sity pouze v případě, že se vztahují opravdu k Sitám a ne k doménám
- Vyvarovat se použití Block inheritance a Enforce inheritance

Aplikace GPO

- Kdy jsou nastavení GPO aplikovány
  - Start počítače – aplikují se nastavení počítače a startup skripty
  - Přihlášení uživatele – aplikují se nastavení uživatele a logon skripty
  - Doběhnutí časovače – aplikují se nastavení uživatele a některá nastavení počítače; žádné skripty
    - Nastavitelné, obvykle 90 +- 30 minut
  - Ruční aktualizace – aplikují se nastavení uživatele a některá nastavení počítače; žádné skripty
    - gpupdate (/force)

Aplikace GPO

- Loopback processing
  - Použití nastavení z části User configuration na počítač
  - Computer Configuration -> Administrative Templates -> System -> Group Policy -> User Group Policy loopback processing mode
  - 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

Úkoly

1. Přidat do domény stanici s Windows 7
2. Najít a prohlédnout si obě úložiště GPO (SYSVOL a AD)
3. Vytvořit novou GPO a přilinkovat ji na OU
4. Projít User configuration a Computer configuration
5. Povolení/zakázání GPO
6. Aplikování GPO
    1. Restart
    2. Logon
    3. Gpupdate
    4. Aplikování User/computer conf na účty osob/počítačů/skupin
7. Vyzkoušet dědičnost GPO
8. Block inheritance/enforce