

Skupinové politiky 2

Práce s 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.
- Blokování dědičnosti (Block inheritance)
 - Nastavuje se na úrovni OU.
 - Blokuje dědičnost všech politik uvedených hierarchicky výš od vybrané OU, kromě vynucených politik.
 - Používat velmi opatrně.

Práce s GPO

- Vynucení dědičnosti (Enforced inheritance)
 - Nastavuje se na GPO.
 - Vynutí dědičnost vybrané GPO hierarchicky níž do všech OU, i kdyby byly cestou nějaká blokování.
 - Používat s rozmyslem, podobně jako blokování.
- Pozor na změny ve zpracování politik při použití vynucení a blokování politik!

Práce s GPO

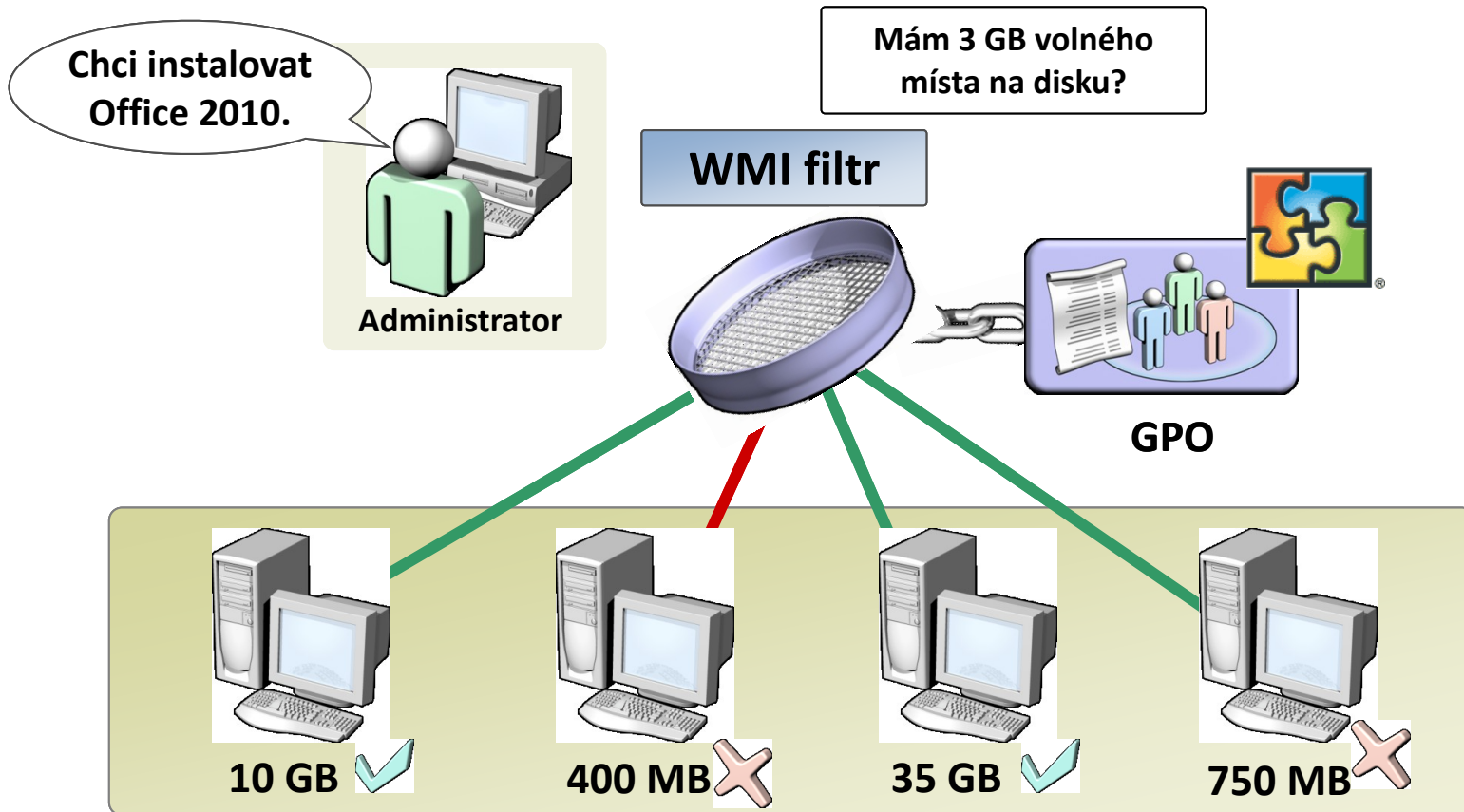
- Filtrování zabezpečení (Security Filtering)
 - Možnost, jak zjemnit aplikaci GPO na konkrétní uživatele a/nebo skupiny.
 - Ve výchozím nastavení má každý GPO povolené čtení a aplikaci skupinové politiky pro skupinu Authenticated Users, což zahrnuje všechny autentizované uživatele i počítače.
 - Může 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.

Práce s GPO

- Filtrování pomocí WMI (WMI Filtering)
 - 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"`

Práce s GPO

- Filtrování pomocí WMI (WMI Filtering)



Práce s GPO

- 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.

Práce s 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 objekt uživatele, následně se stáhne seznam politik pro objekt počítače a zařadí se za seznam politik pro objekt uživatele; postupně se vše aplikuje; pokud dojde ke konfliktu některých nastavení, tak "vítězí" nastavení pro objekt počítače, protože jsou později na seznamu;
 - Replace – stáhne se pouze seznam politik pro objekt počítače a použijí se jako nastavení pro objekt uživatele; politiky, které jsou standardně nalinkovány na objekt uživatele jsou zcela ignorovány;

Správa GPO

- Kontejner Group Policy Objects vs. OU
 - Vytvoření GPO
 - Back Up...
 - Restore from Backup...
 - Import Settings...
 - Save Report...

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.
 - Resultant Set of Policy (RSoP)
- 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.