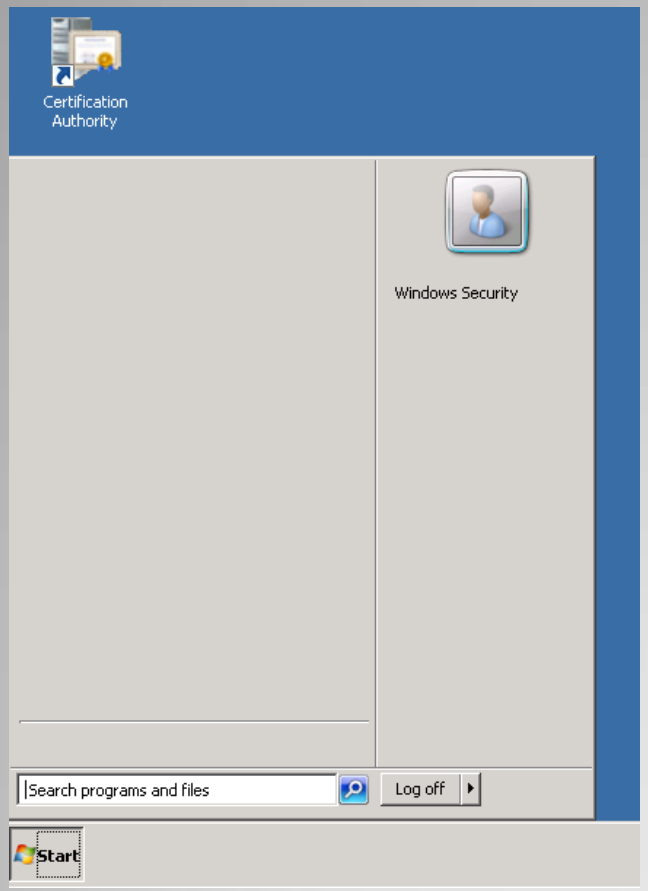
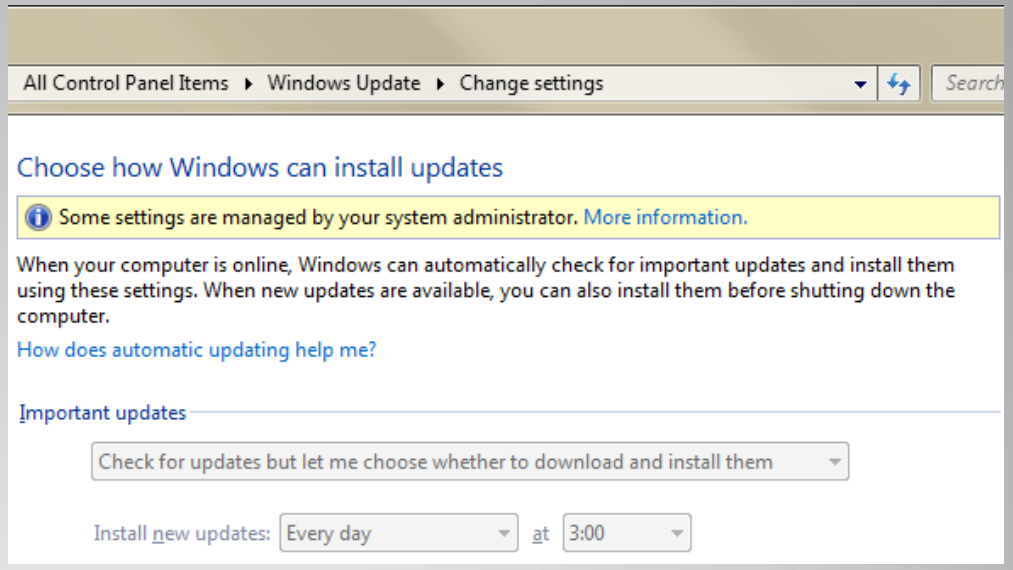
Group policy

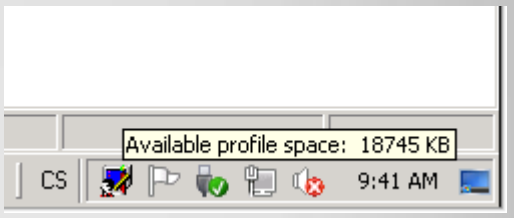
Jan Žák

Microsoft CERTIFIED Trainer

Systems Administration
Systems Engineering





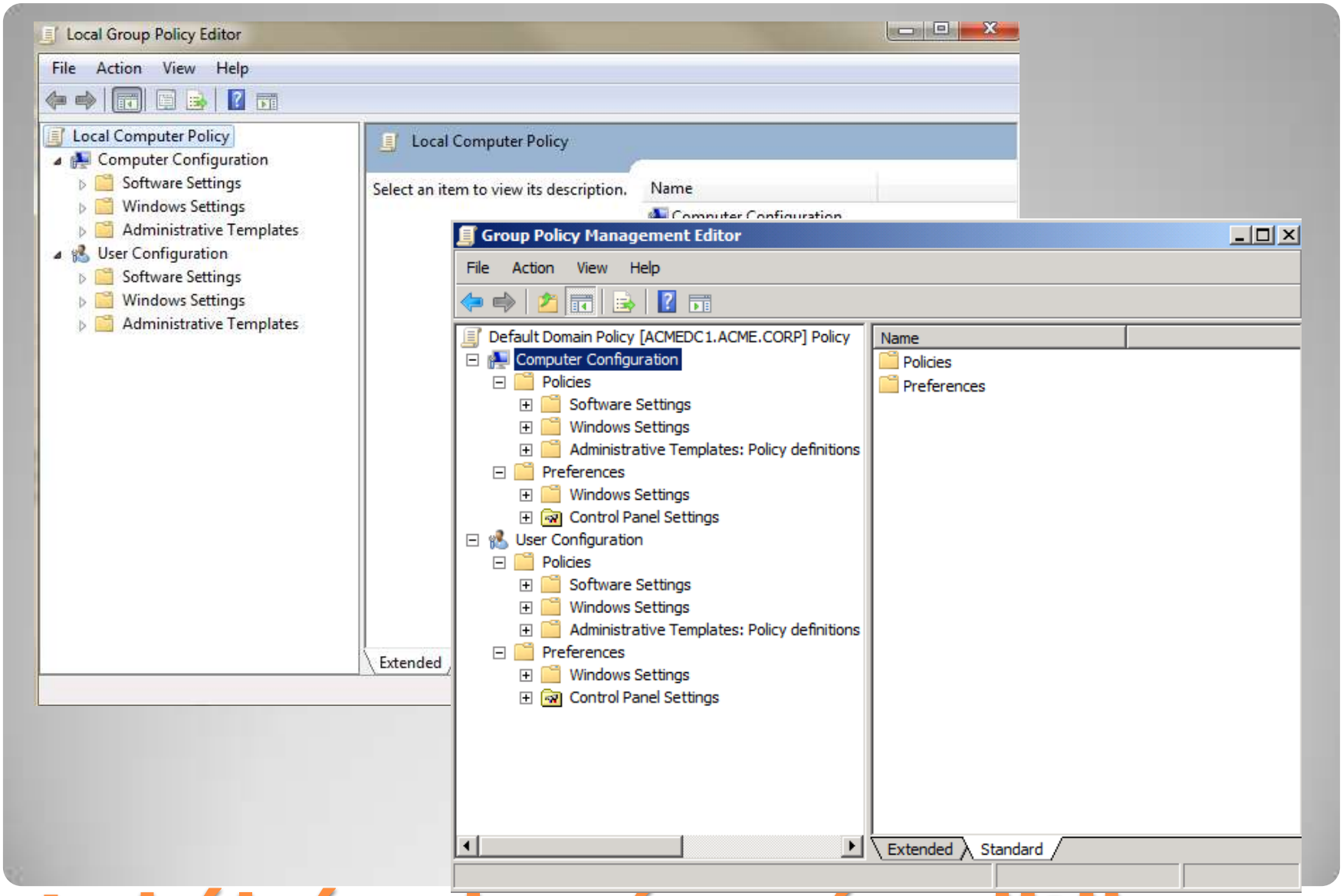


K čemu Group Policy?

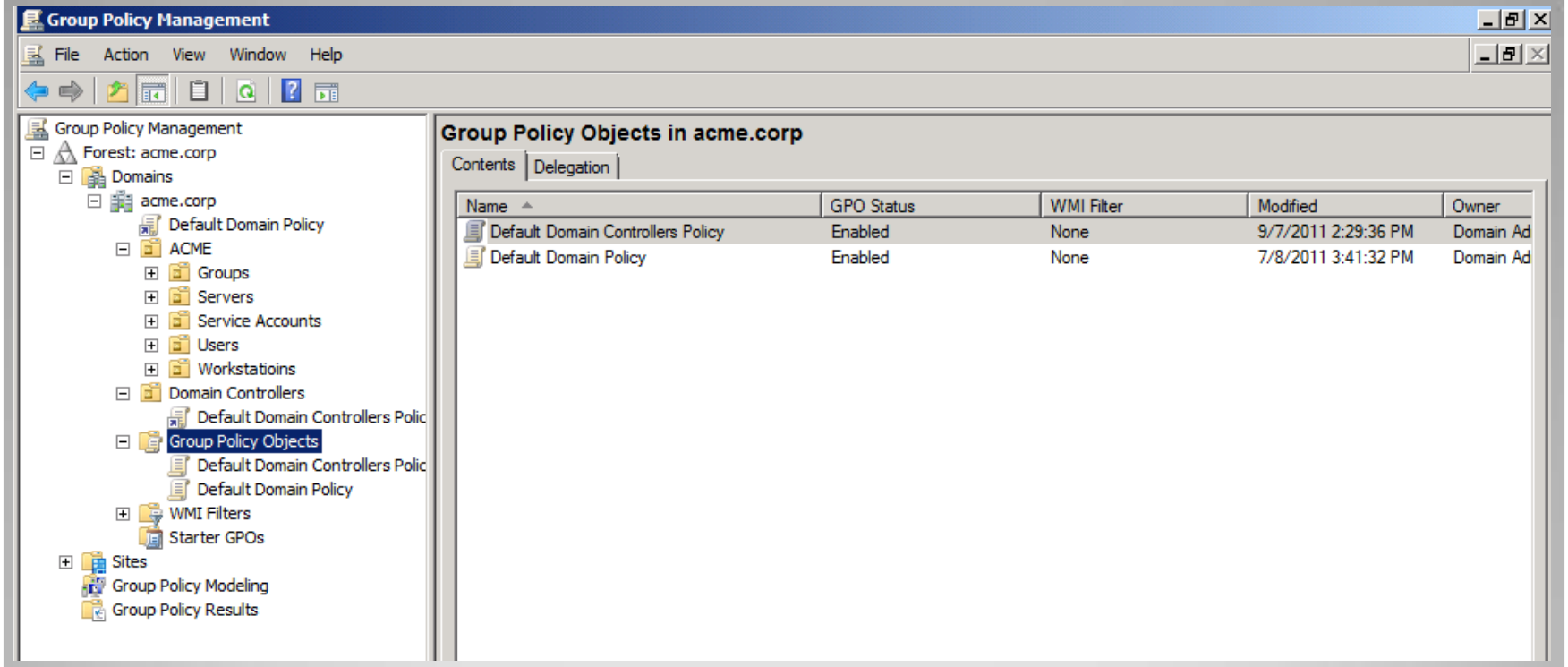
Zpracování GP

Pořadí zpracování GP

- Group Policy lokálního počítače
- Group Policy objekty pro sídlo (site)
- Group Policy objekty pro doménu
- Group Policy objekty pro organizační jednotky

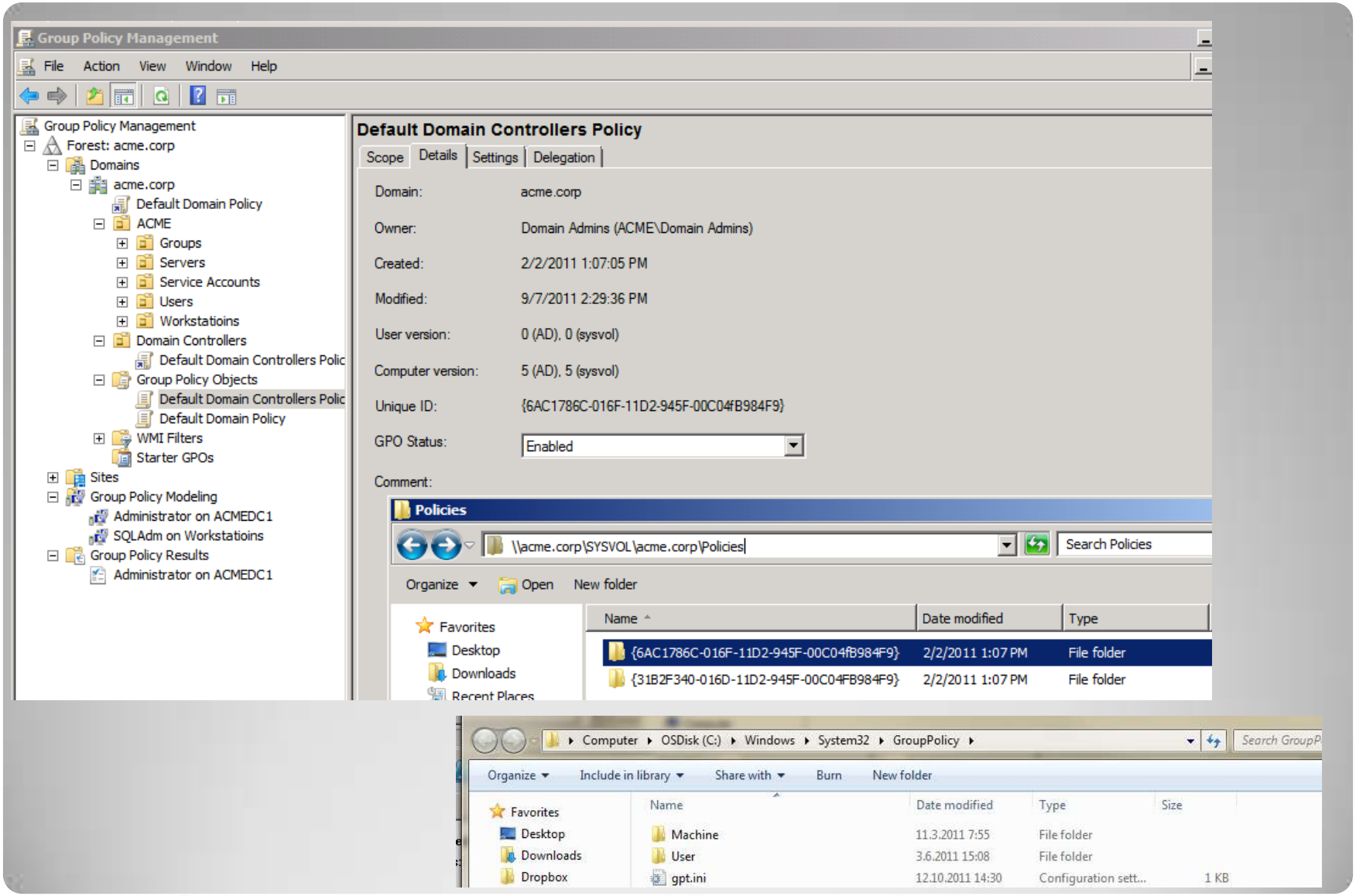


Lokální a doménové politiky



- Administrative Tools → Group Policy Management (gpmc.msc)
- Pro editaci politik lokálního počítače: gpedit.msc

Group Policy Management Console

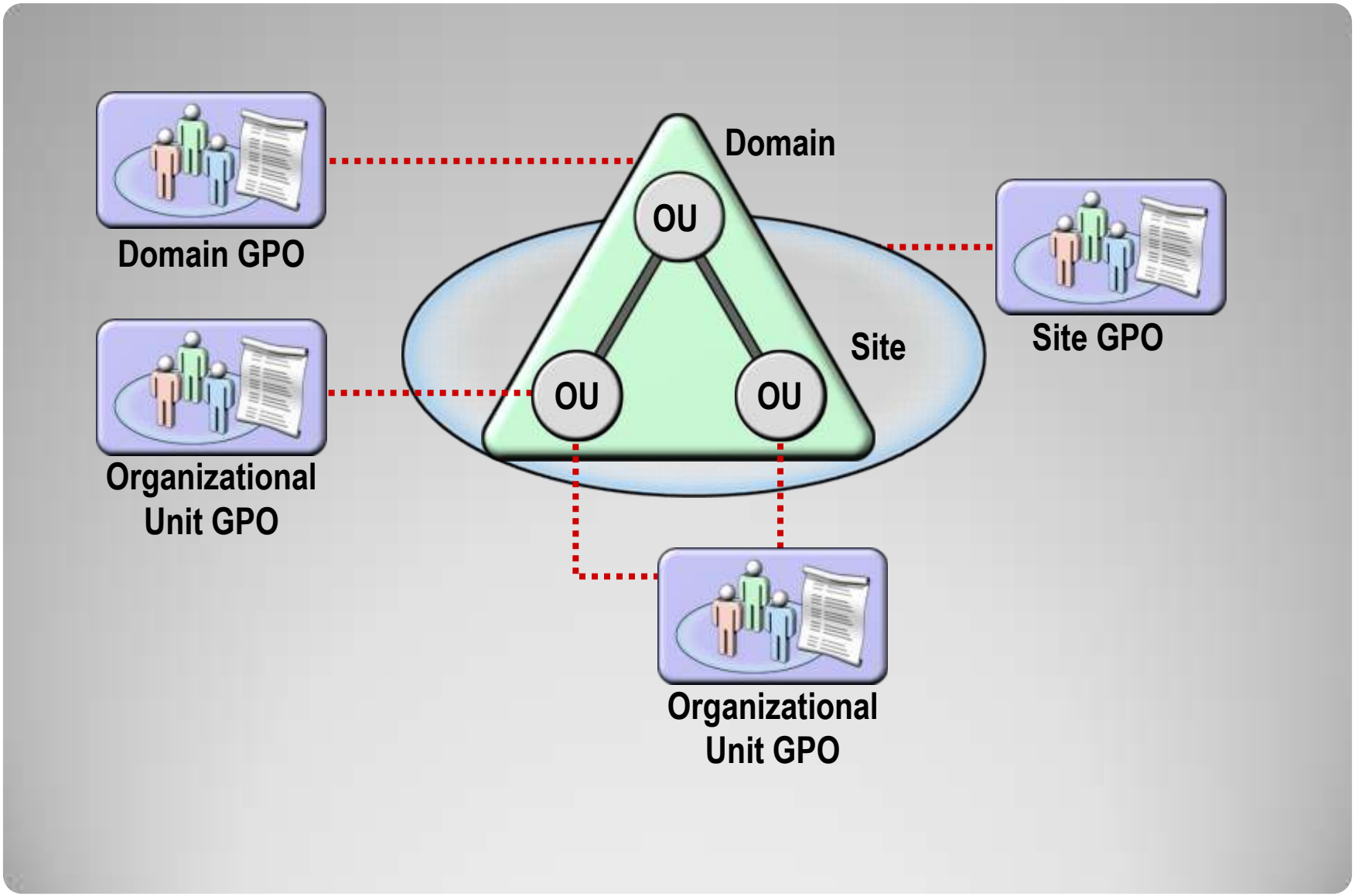


Co je Group Policy Object?

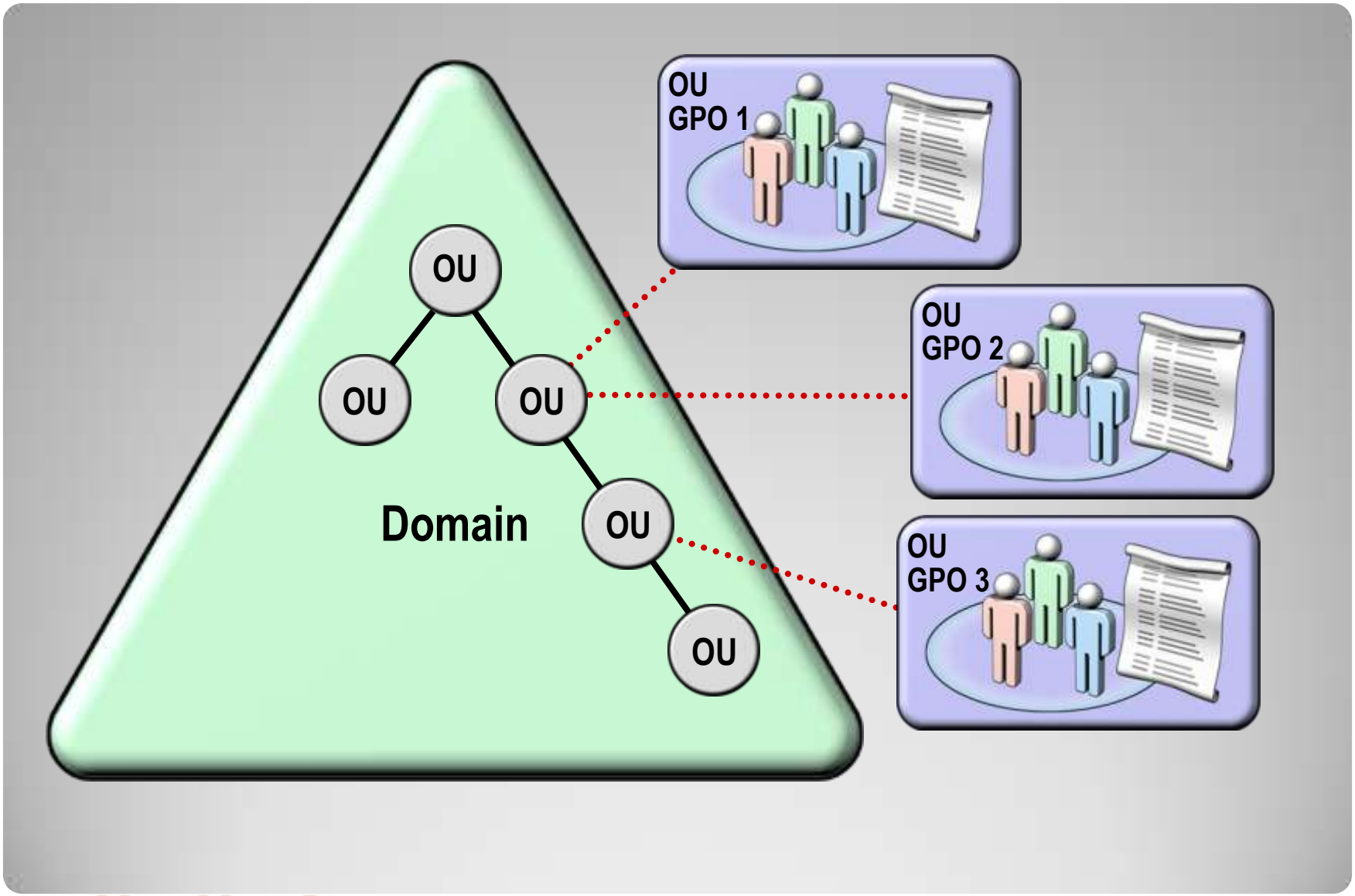
- GP pro uživatele:
  - Software settings
  - Windows settings
    - Folder Redirection
    - IE settings
  - Administrative templates
    - Windows Components
    - Desktop settings

- GP pro počítače:
  - Software settings
  - Windows settings
    - Security settings
    - Startup/Shutdown scritps
  - Administrative templates
    - Control Panel
    - Network
    - System

User /Computer Configuration Settings


Domain
OU
Site
OU
OU
Domain GPO
Site GPO
Organizational
Unit GPO
Organizational
Unit GPO

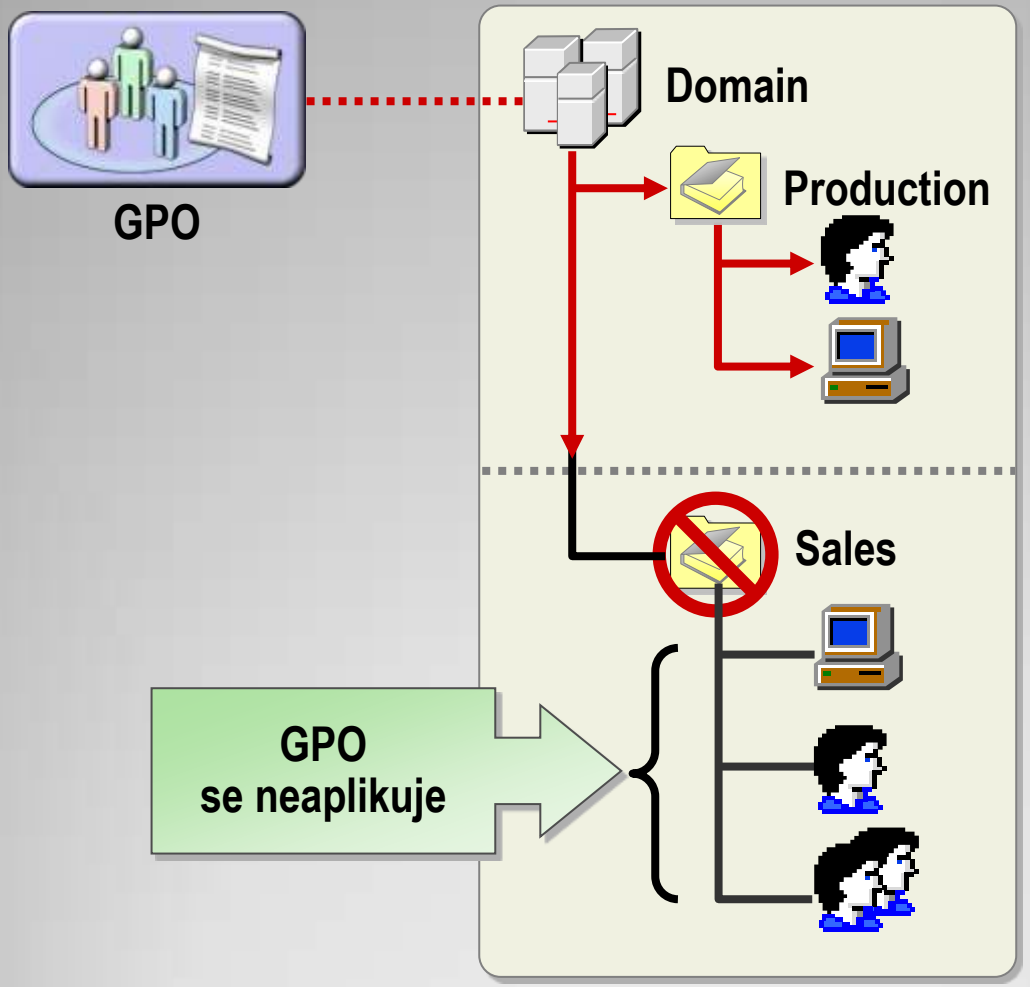
GPO Link



Dědění politik

Atributy GPO linků

- Enforced
  - Má přednost před ostatními politikami - „vždy vyhraje“
- Link Enabled / Disabled
  - Link lze dočasně deaktivovat, např. při řešení problémů
- Deleted
  - Links lze smazat, GPO zůstane zachován
- Multiple Links
  - Při aplikaci více GPO na jeden kontejner, opět je důležité stanovit pořadí aplikování politik.



Blokování dědění GPO

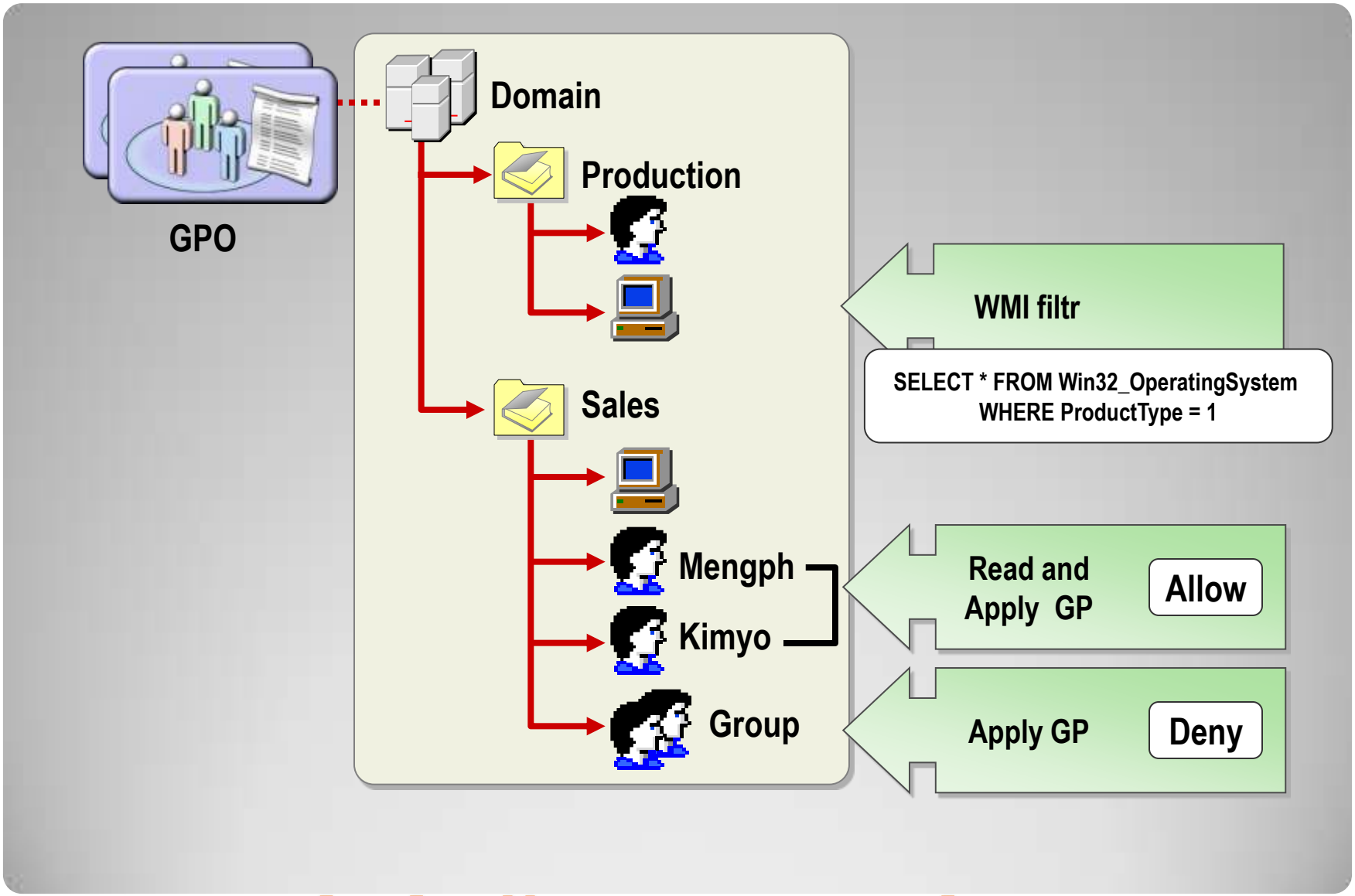
Konflikty GPO

Pokud nastane konflikt při nasazení GPO, vyhrává GPO podřízeného kontejneru.

Konfliktní jsou jednotlivá nastavení, nikoliv celé GPO.

Také „enforced“ GPO vyhrává.

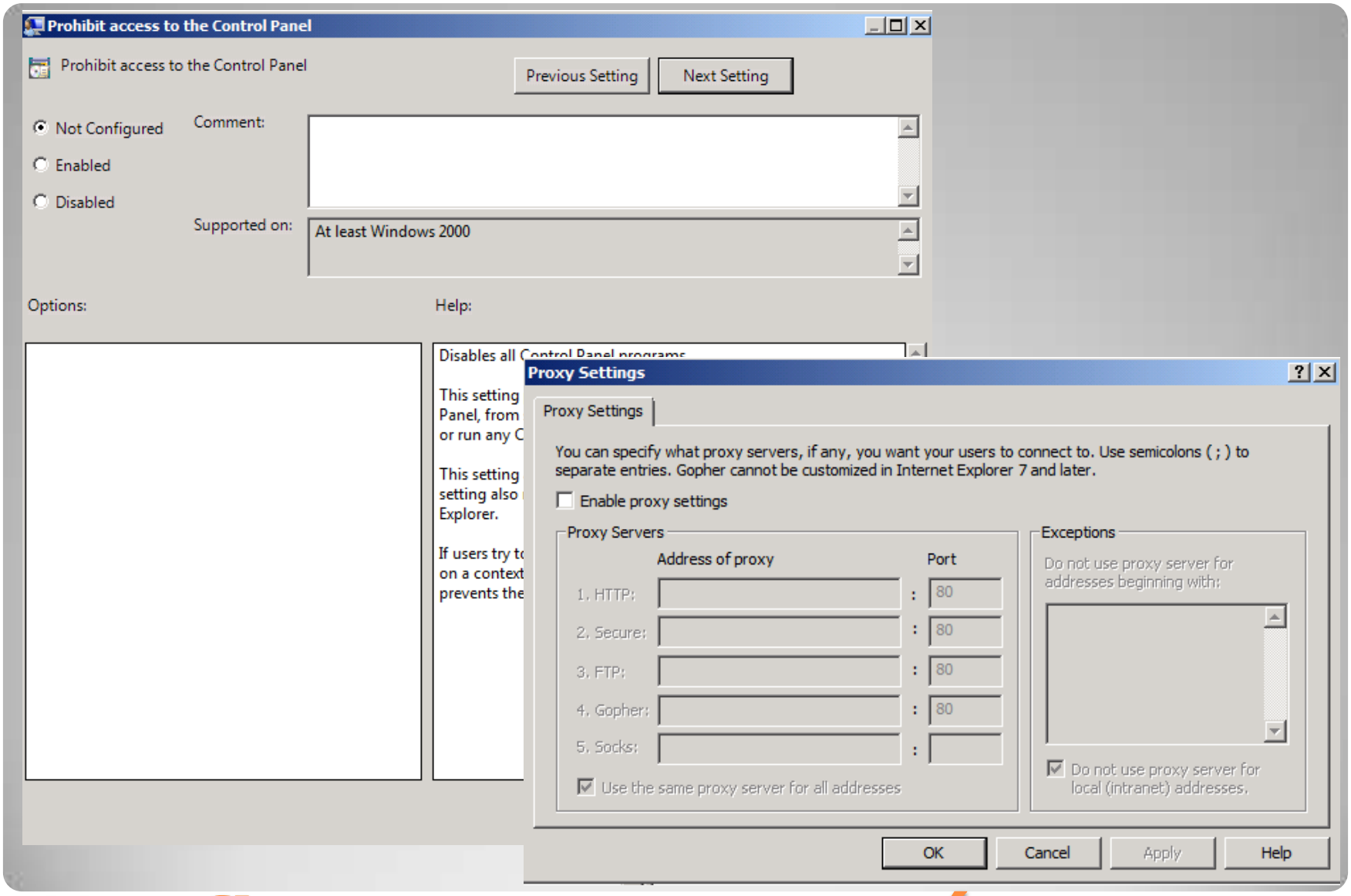
...



Filtrování při nasazení GP

Typické využití GP

- Správa uživatelů a počítačů
- Nasazení softwaru
- Vynucení zabezpečení
- Vynucení konfigurace pracovního prostředí
- Vynutit a spravovat členství ve skupinách
- Použití „loopback processingu“



Konfigurace nastavení

Skripty v GP

- Pro počítače
  - Startup scripty
  - Shutdown scripty
- Pro uživatele
  - Logon scripty
  - Logoff scripty

Skripty mohou být umístěny ve složce SYSVOL a replikovány na všechny DC

Proč skripty?

Skripty v politikách mohou:

- Provádět úkoly, které nelze nakonfigurovat v GP (nebo by bylo nutné zkompilovat vlastní GP)
- Vyčistit prostředí a vrátit počítač do původního stavu
- Zajistit bezpečné prostředí např. smazáním temp složek atd.

Od Windows 2008 lze často místo skriptů využít „preferences“

Software a GP

Omezení spouštění aplikací
Instalace aplikací

Software Restriction Policy

- SRP identifikuje a řídí spouštění softwaru na klientských počítačích
- Omezuje instalaci softwaru a pomáhá chránit před nákazou
- Základní komponenty jsou skupiny softwaru
  - Unrestricted
  - Disallowed
  - Výjimky z výchozích pravidel

Pravidla pro SRP

Hash Rule

- Pro identifikaci softwaru se používají MD5 nebo SHA1 hashe
- Používá se pro povolení nebo omezení konkrétních verzí programu/souboru

Certificate Rule

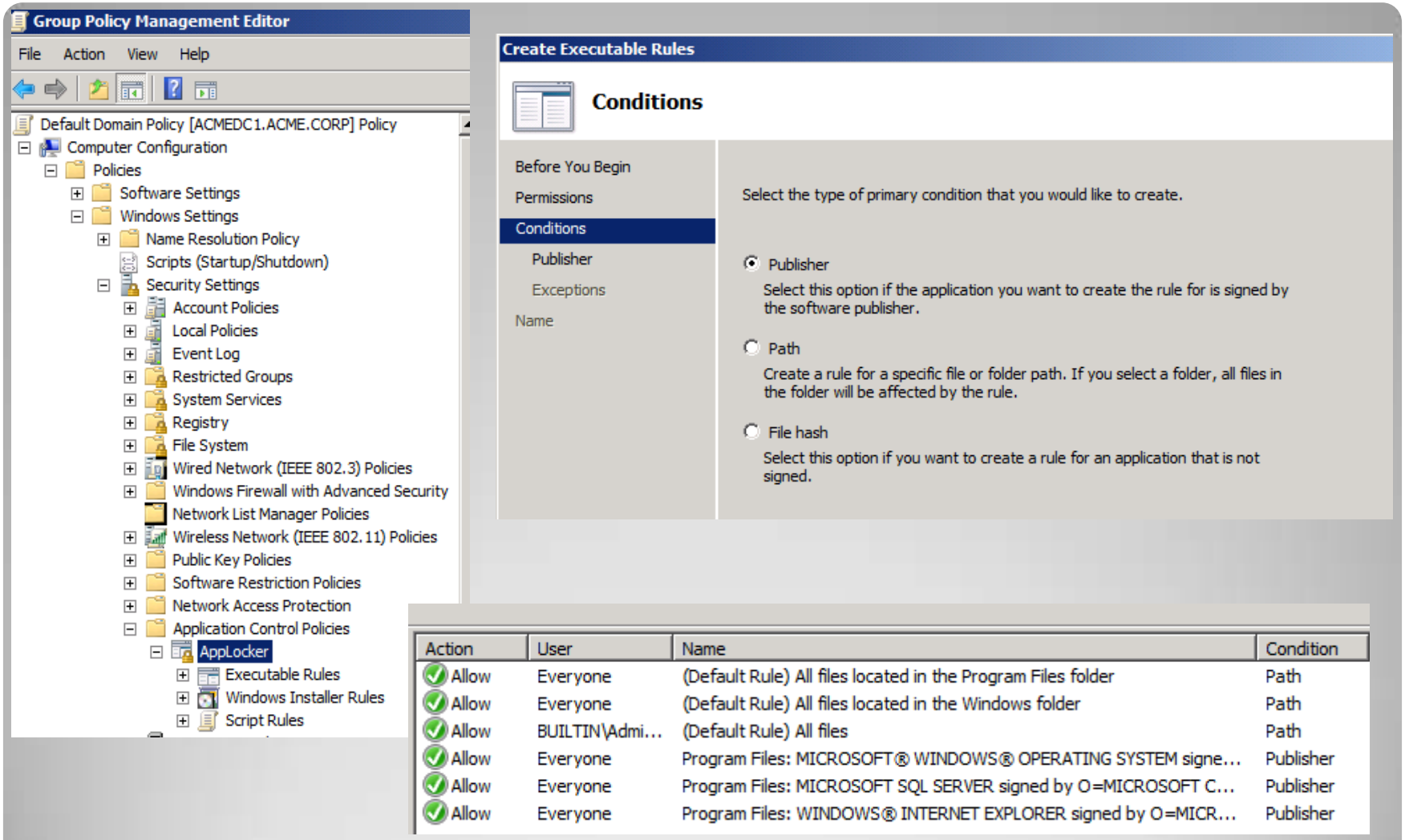
- Kontroluje přítomnost digitálních podpisů aplikace
- Lze využít např. pro omezení spouštění Win32 aplikací nebo ActiveX komponent

Path Rule

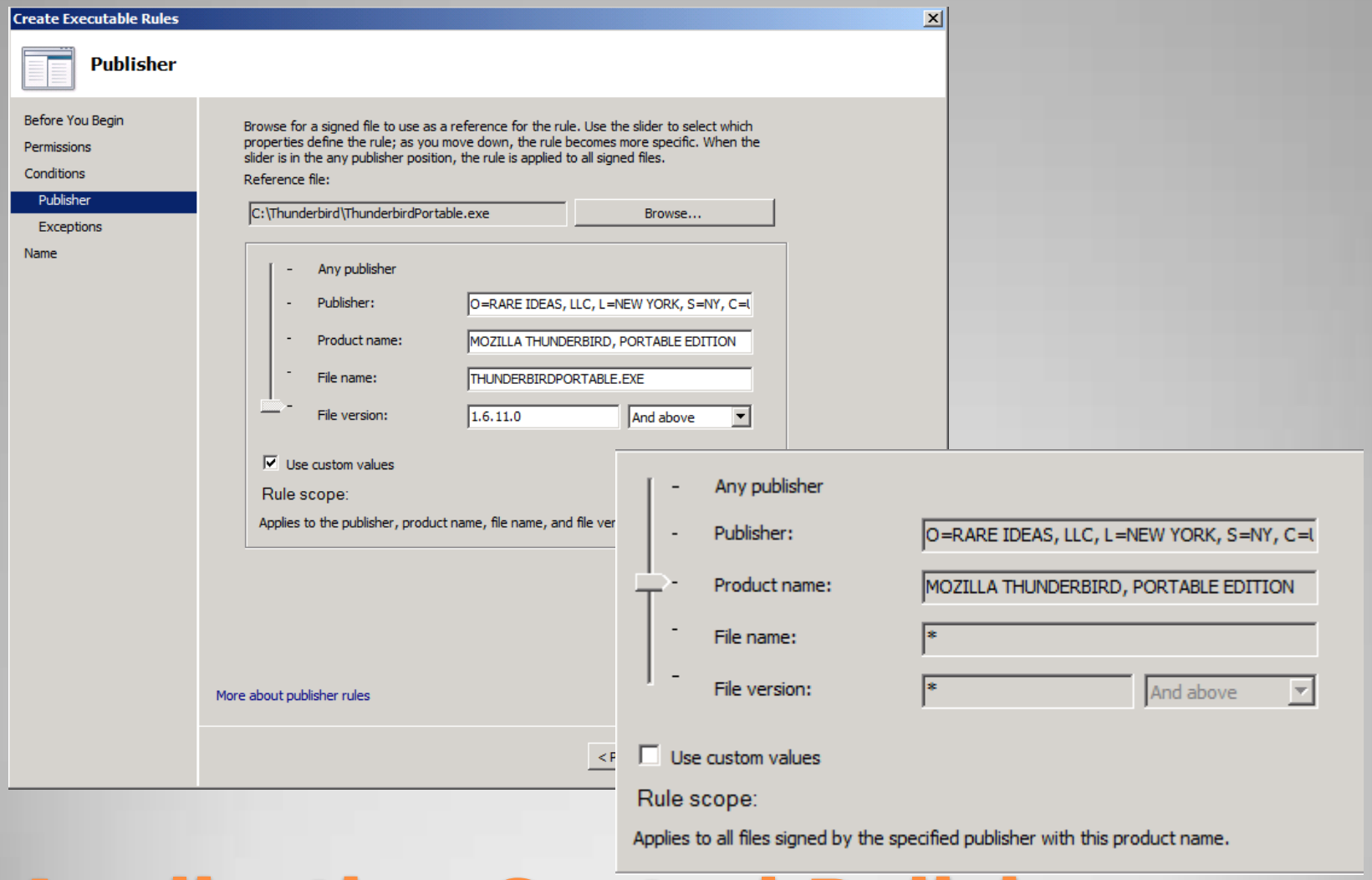
- Umožní definovat cestu k souboru
- Vhodné pro více souborů v programové složce
- Klíčové při zpřísněném režimu

Internet Zone Rule

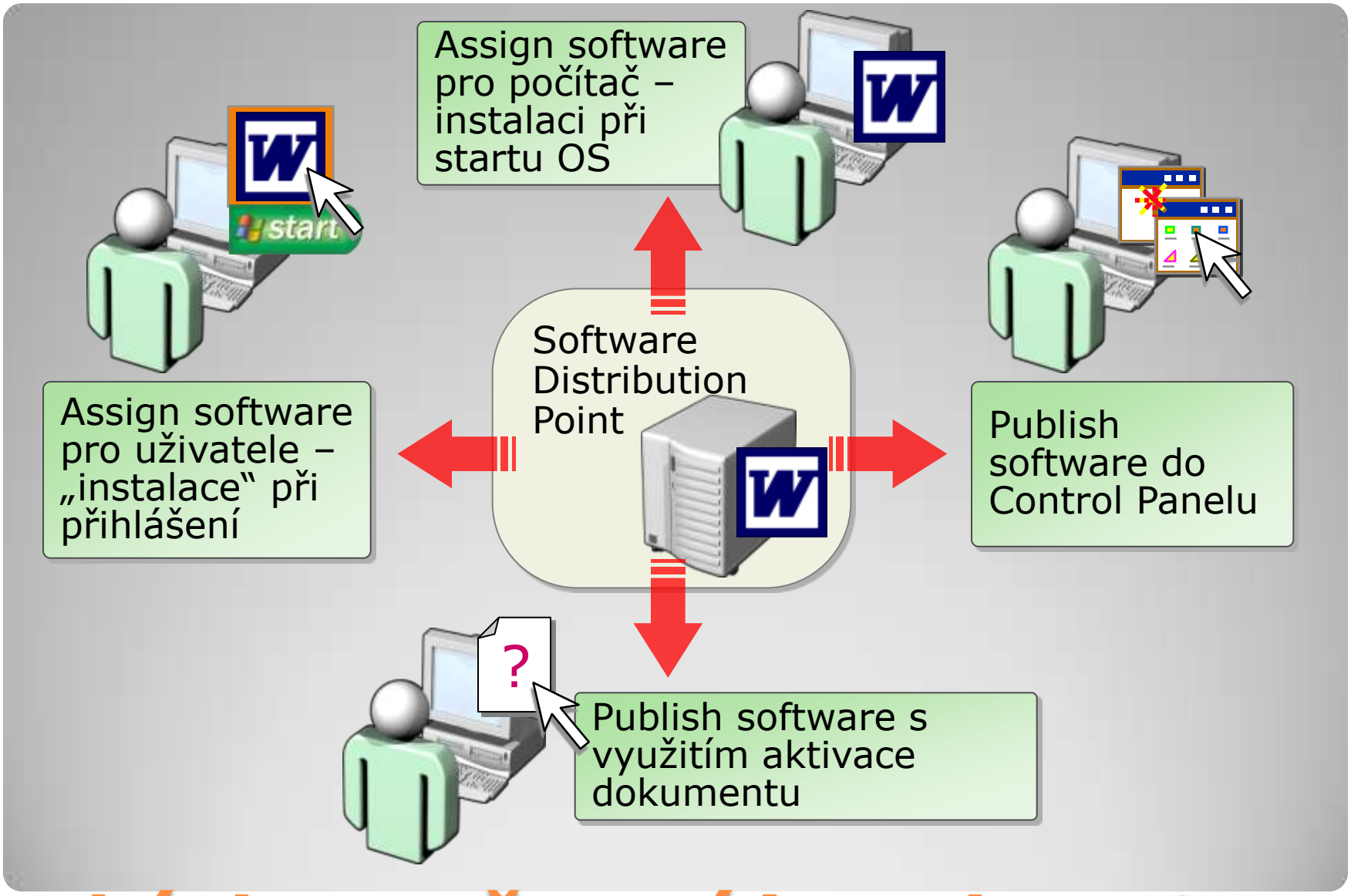
- Řídí přístupy pro jednotlivé zóny
- Pro maximální možnosti zabezpečení přístupů k webovým aplikacím



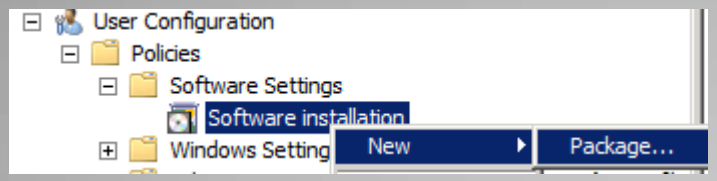
Application Control Policies (AppLocker, jen pro W7 Ult+Ent)

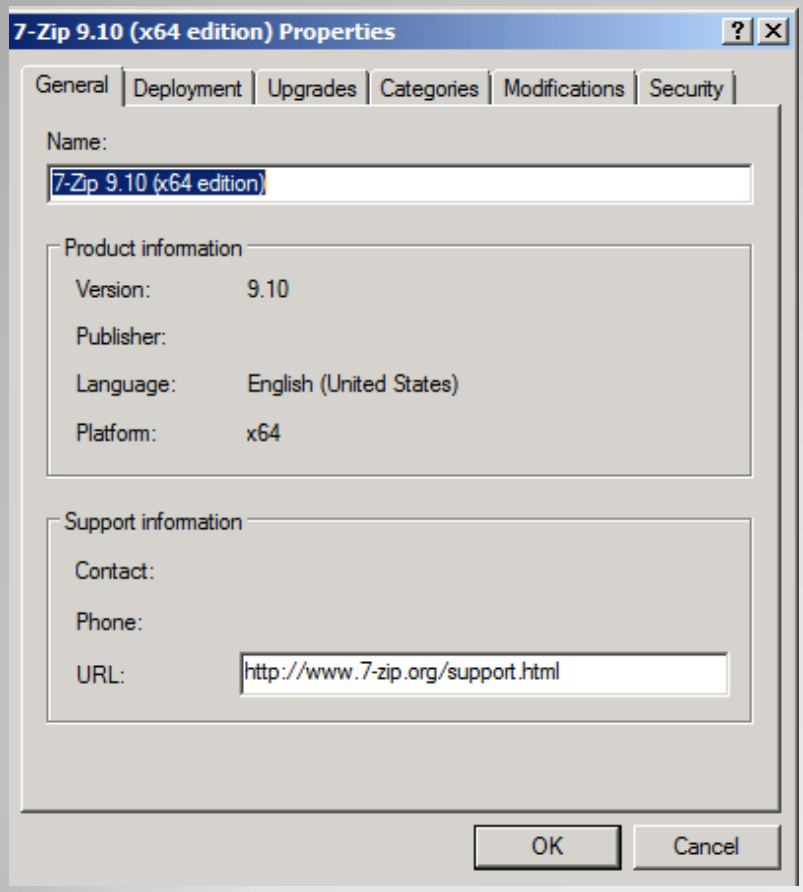


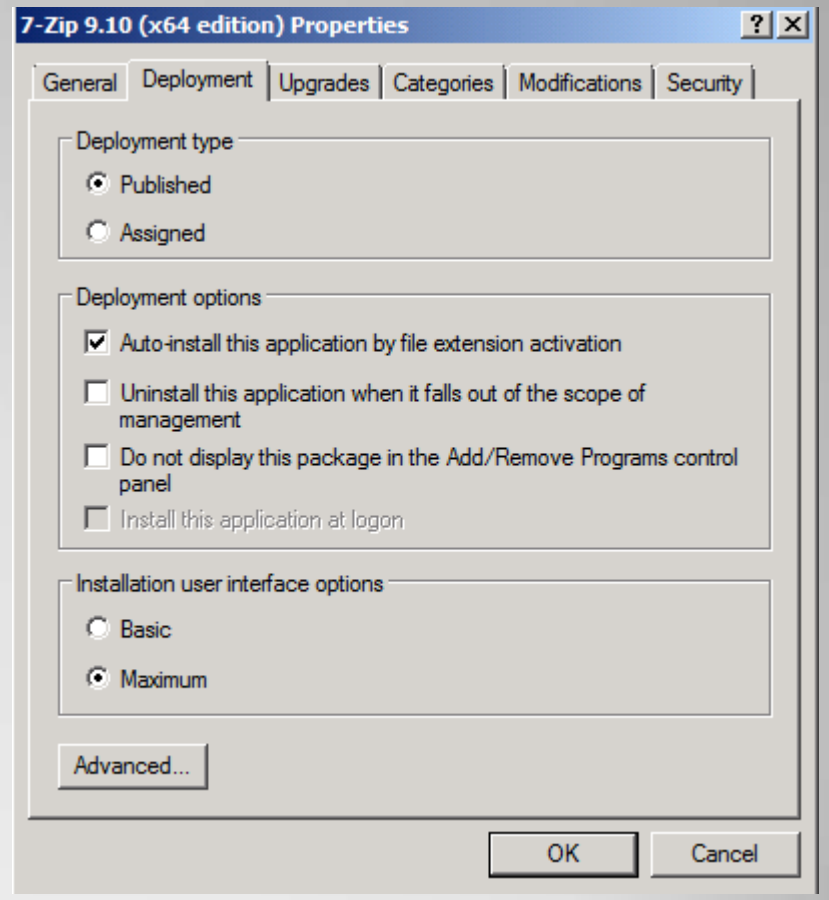
Application Control Policies (AppLocker)



Ukázky možností instalace SW







Nasazení nového balíčku

Pracovní prostředí

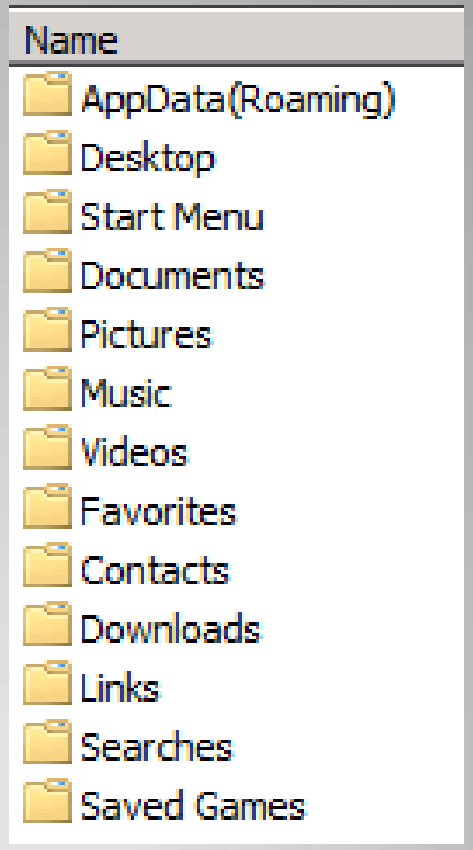
Přesměrování složek (Folder Redirection)

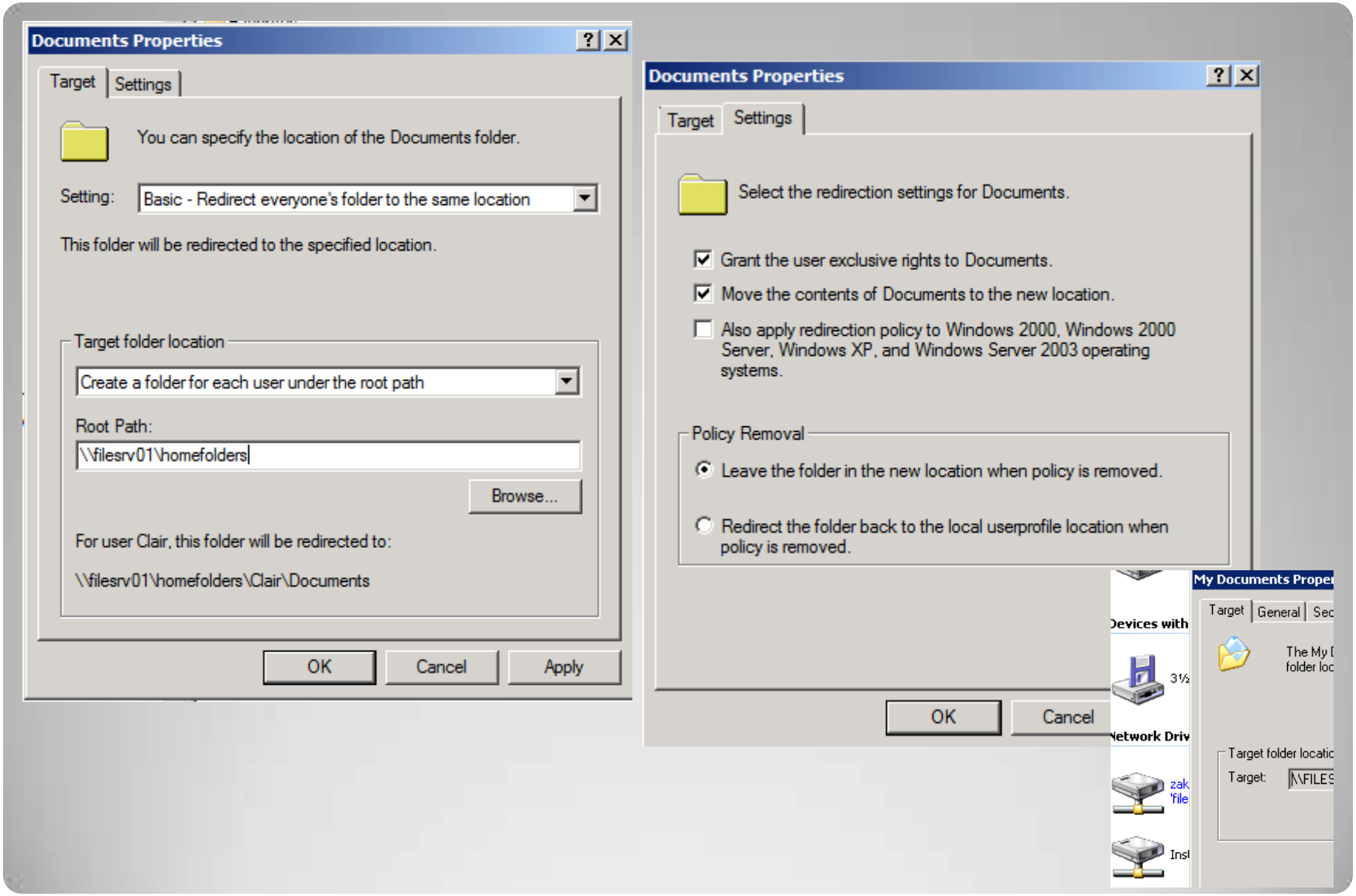
Folder Redirection umožňuje:

- Přesměrování složek v rámci lokálního počítače nebo na síťový disk
- Transparentnost vůči uživatelům – uživatel nevidí rozdíl
- Usnadní použití cestovních profilů (roaming profiles)
- Uživatel neřeší U:\ , X:\

Konfigurace Folder Redirection

- **Basic**
  stejné nastavení pro všechny
- **Advanced**
  rozdílné nastavení pro různé skupiny uživatelů
- **Follow the Documents folder**
  vytvoří podsložku ve složce Documents
- **Not configured**





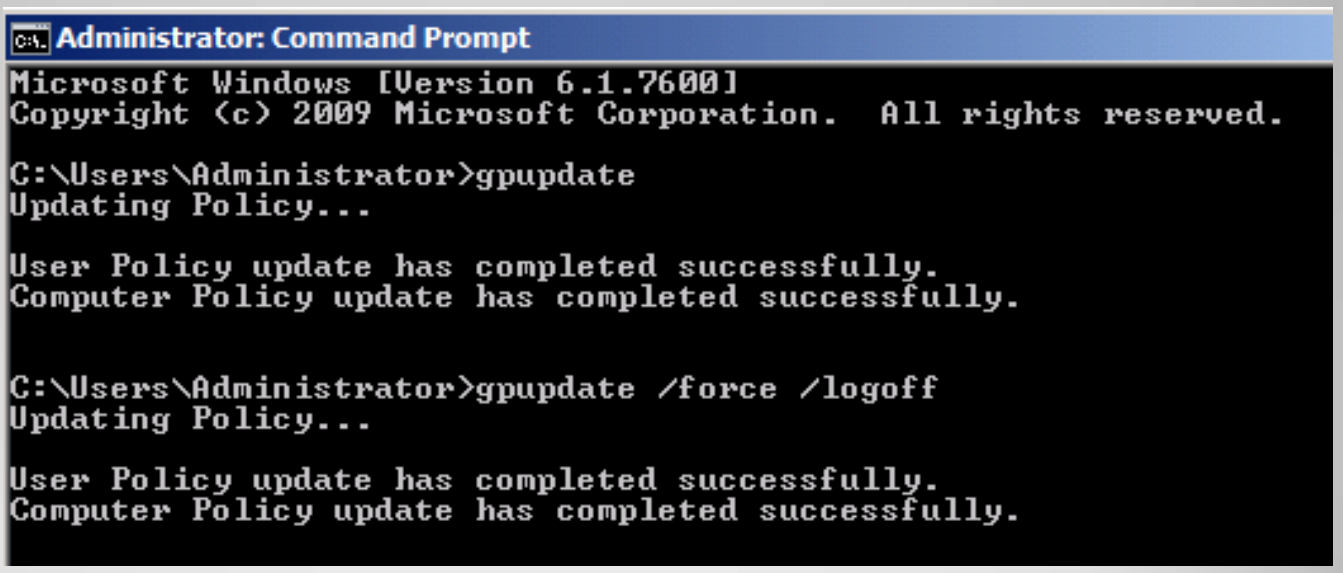
Přesměrování složky Documents

Zabezpečení přesměrovaných složek

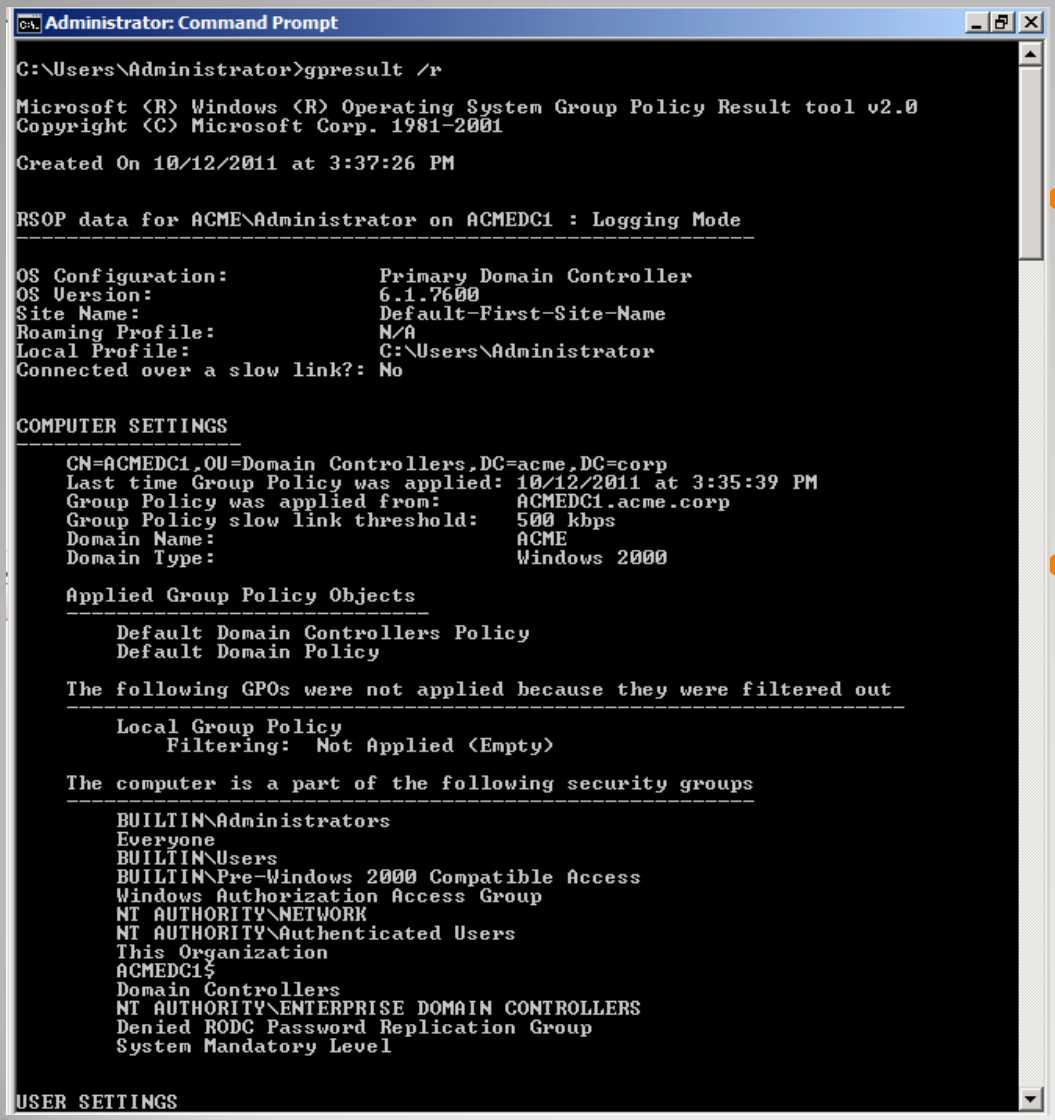
- NTFS práva pro root složku
- Shared folder práva pro root složku
- NTFS práva pro každou uživatelskou složku
- IPSec
- Dostatečný výkon serveru a sítě
- Zálohování
- Nastavení diskových kvót
- …

Další nástroje pro diagnostiku GP

- Manuální obnovení aktualizovaných politik
- Vynucení aplikování nastavení
- Další možnosti jako restart nebo odhlášení v případě potřeby

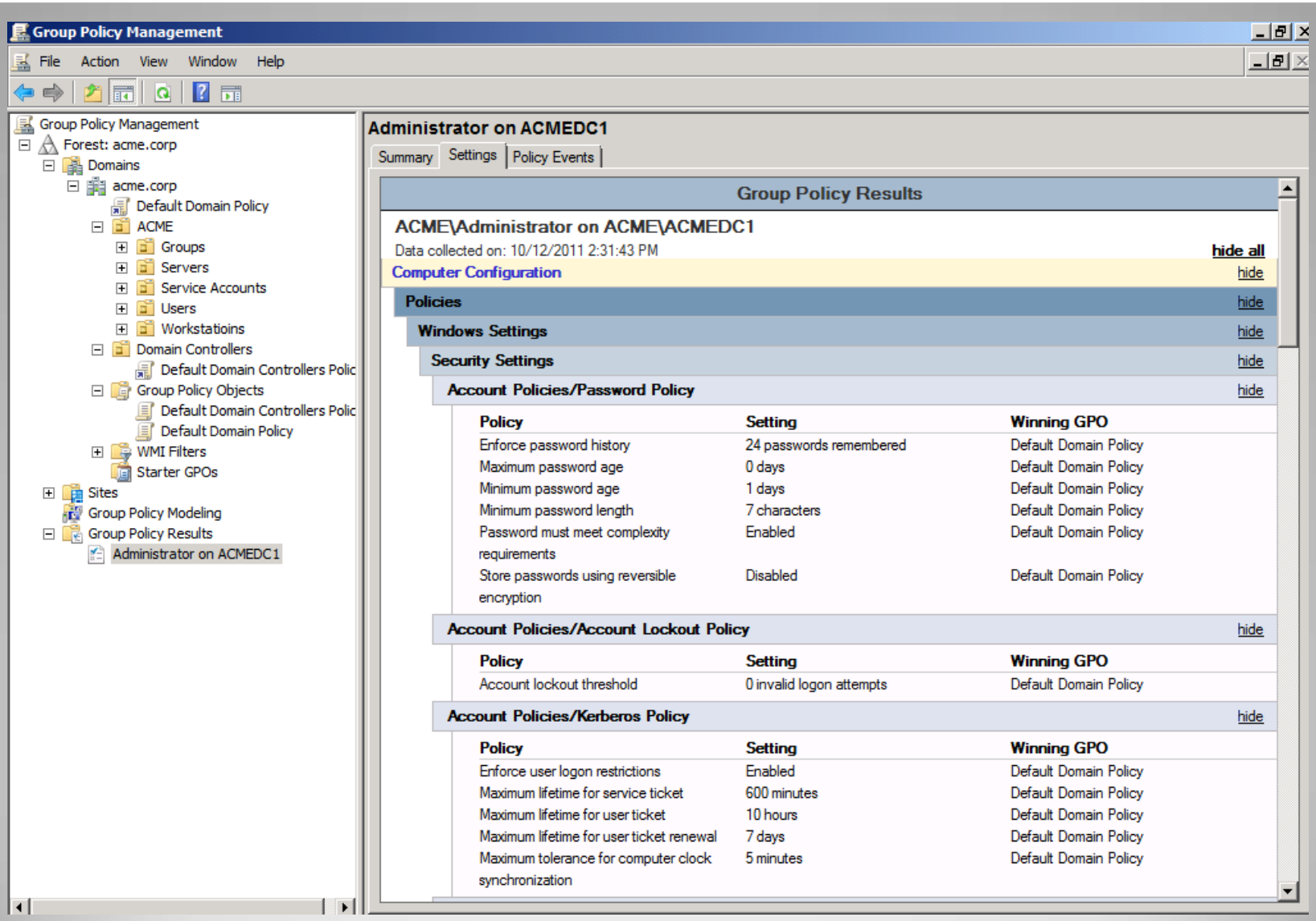


Gpupdate.exe

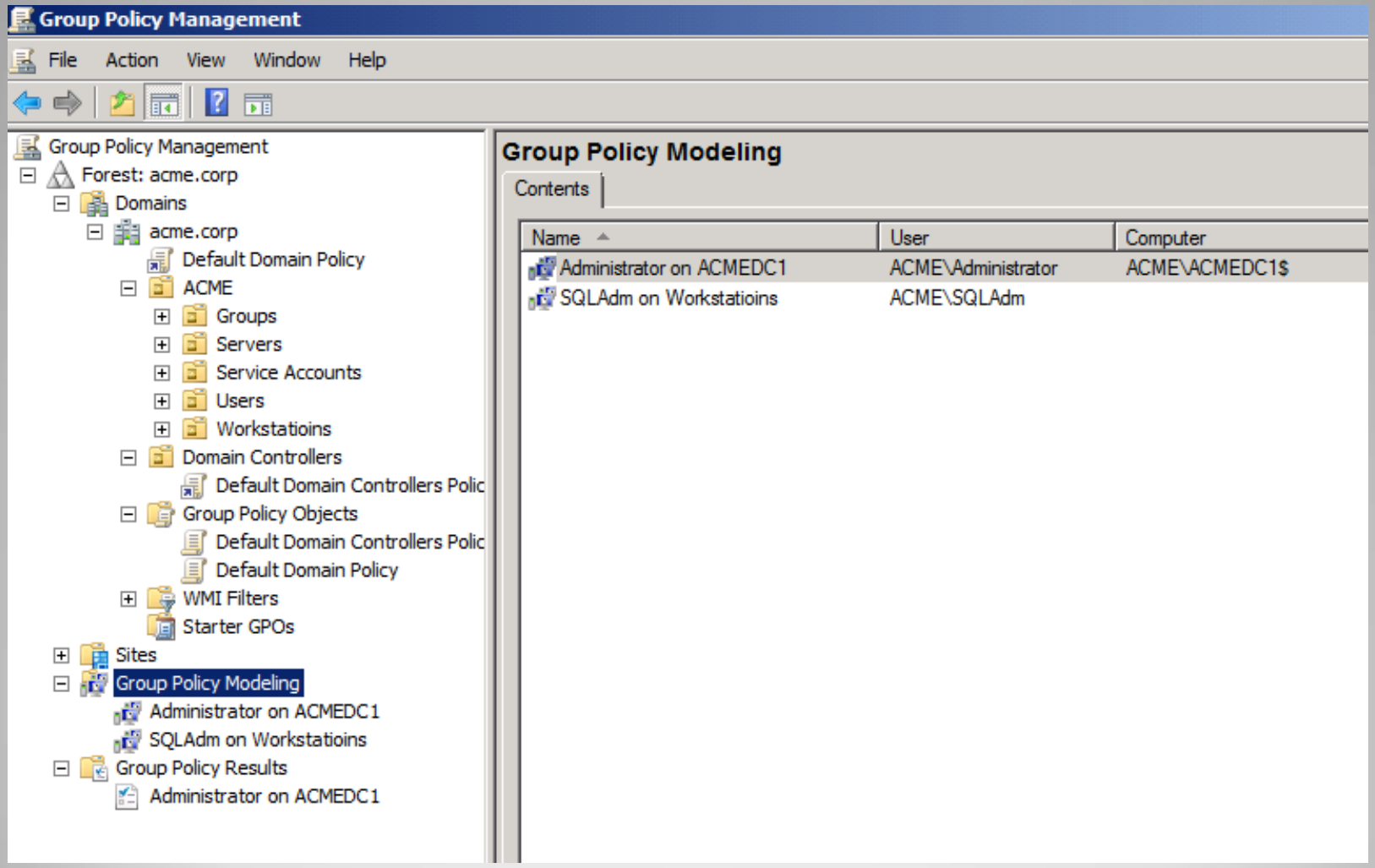


- Zobrazení výsledné sady zásad pro uživatele a počítač
- Vygenerování souboru v výslednými zásadami (htm)

Gpresult.exe

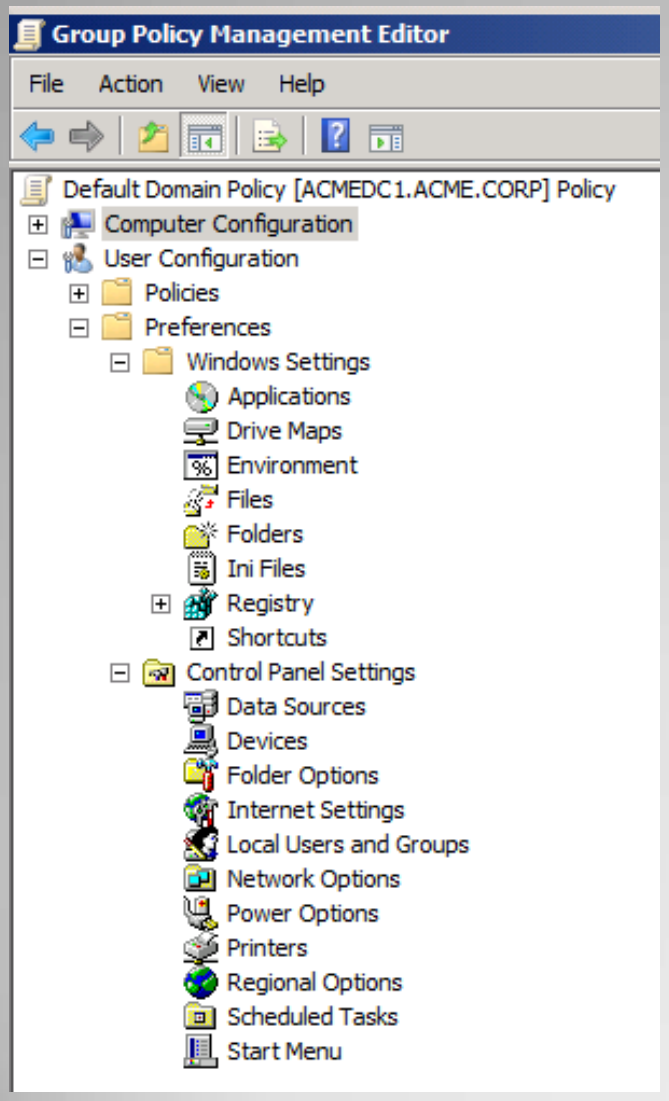


Reporty – výsledné zásady



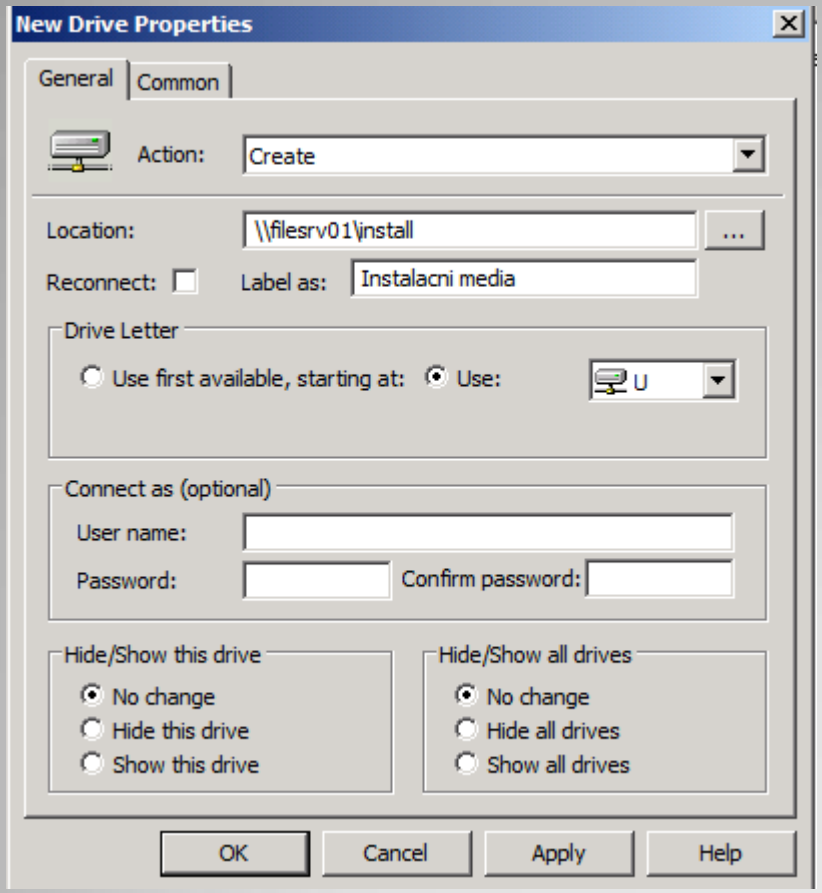
Group Policy Modeling

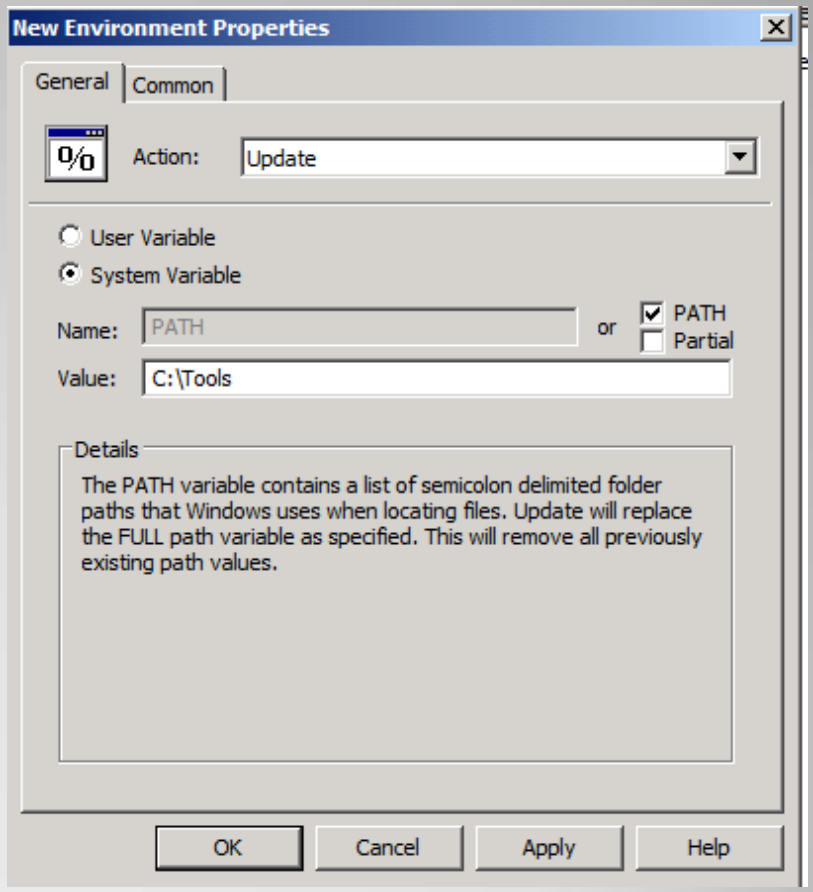
Preferences



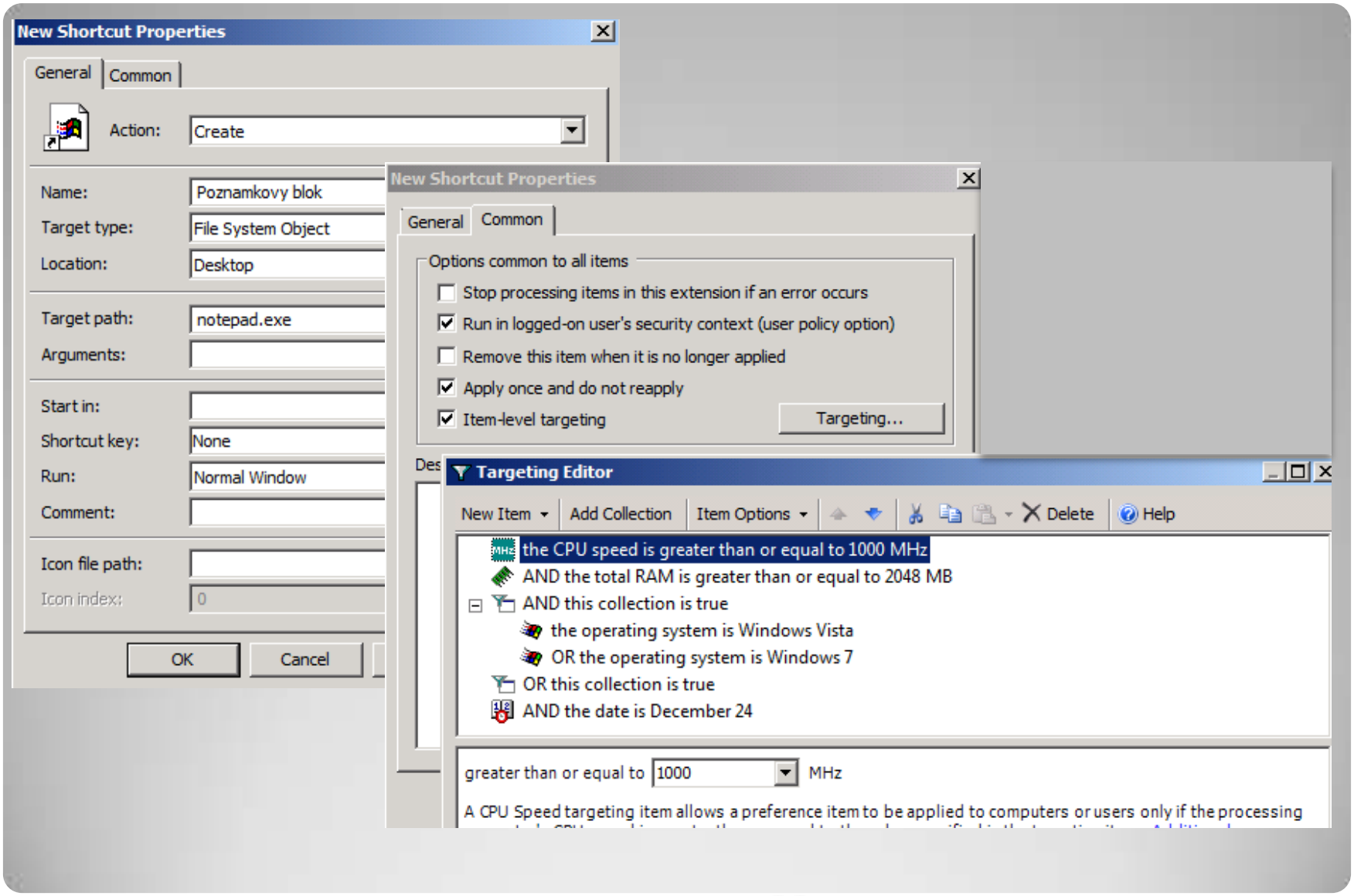
- **Policies** neumožňují uživateli změnit nastavení.
- **Preferences** přidávají další možnosti. Mohou se aplikovat jednorázově nebo opakovaně. Uživatel má možnost provádět změny nastavení.

Preferences

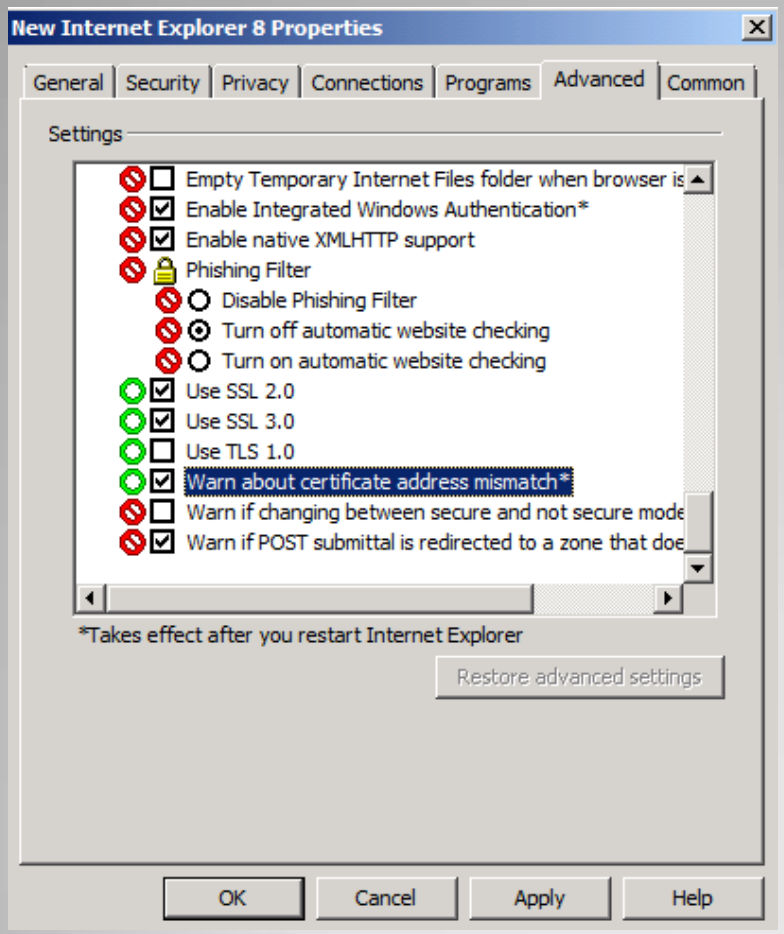




Preferences - příklady



Preferences – možnosti



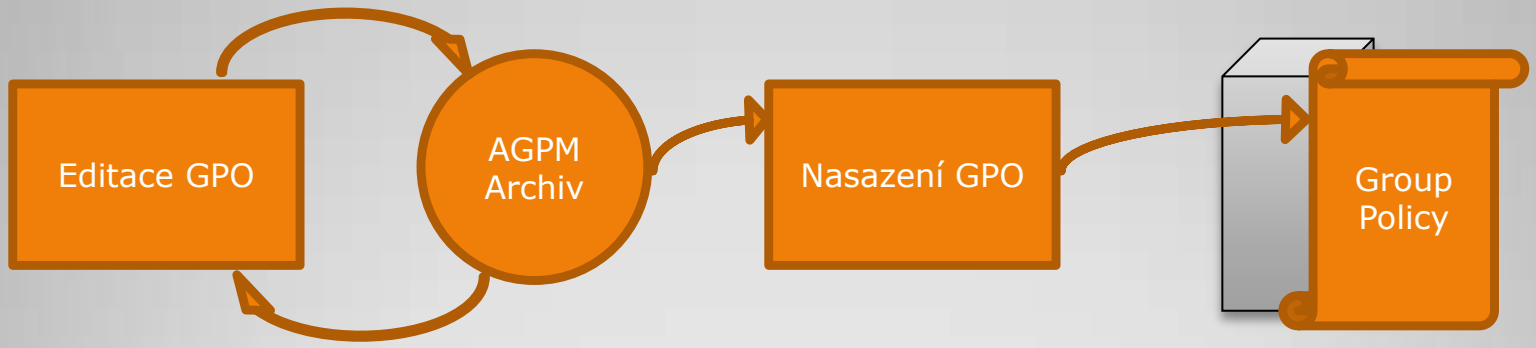
- **F5** – Konfigurace všech nastavení
- **F6** – Konfigurace vybraného nastavení
- **F7** – Ignorování vybraného nastavení
- **F8** – Ignorování všech nastavení

Preferences – F5 F6 F7 F8

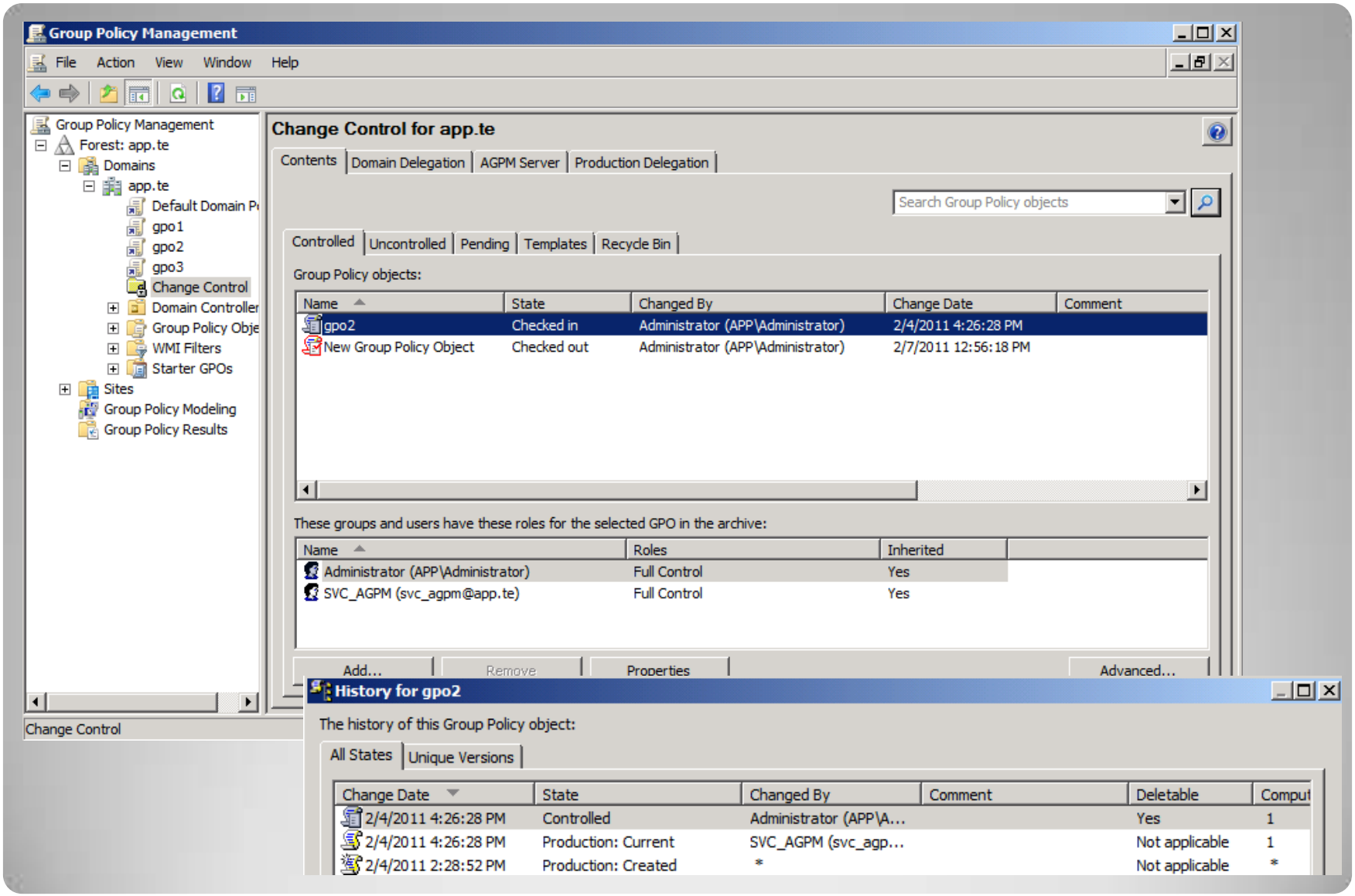
Advanced Group Policy Management

AGPM

- Archiv AGPM poskytuje offline úložiště pro GPO
- Změny v GPO jsou ukládány do archivu a neovlivňují produkční prostředí dokud nejsou schváleny a nasazeny do produkce.

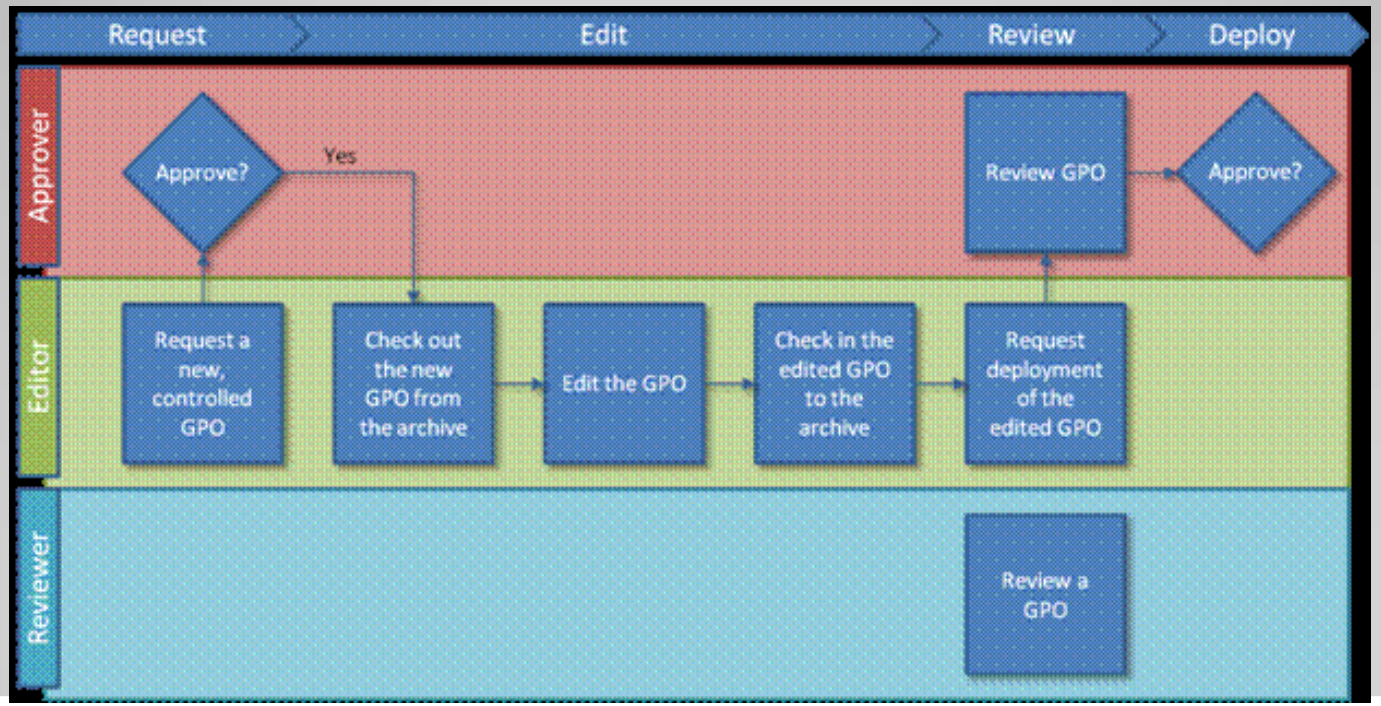


Offline editace



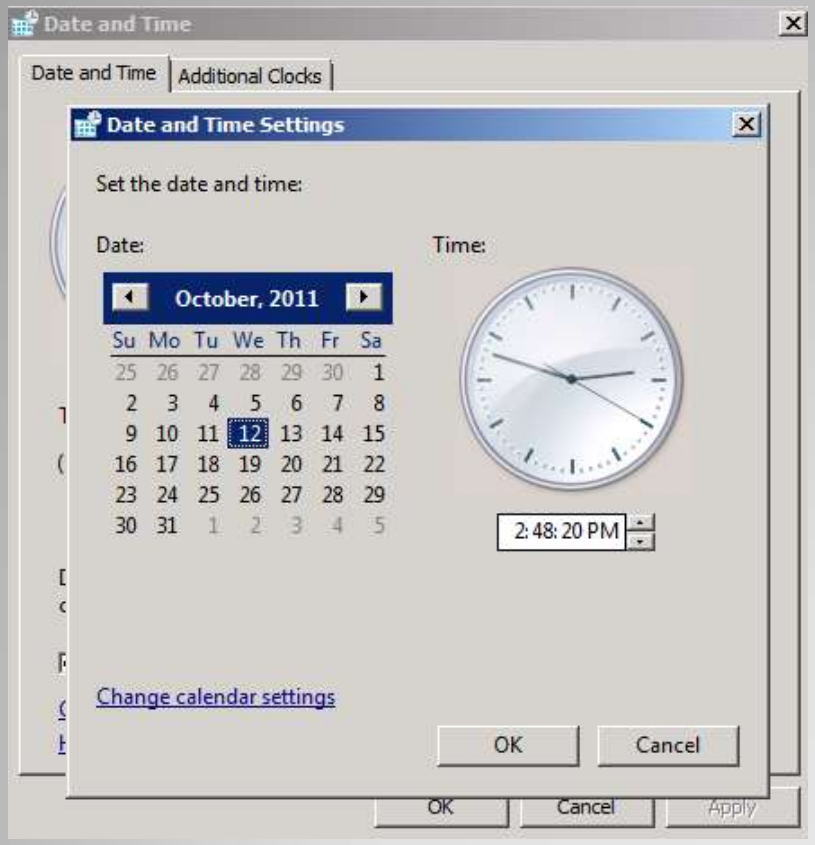
Integrace do GPMC

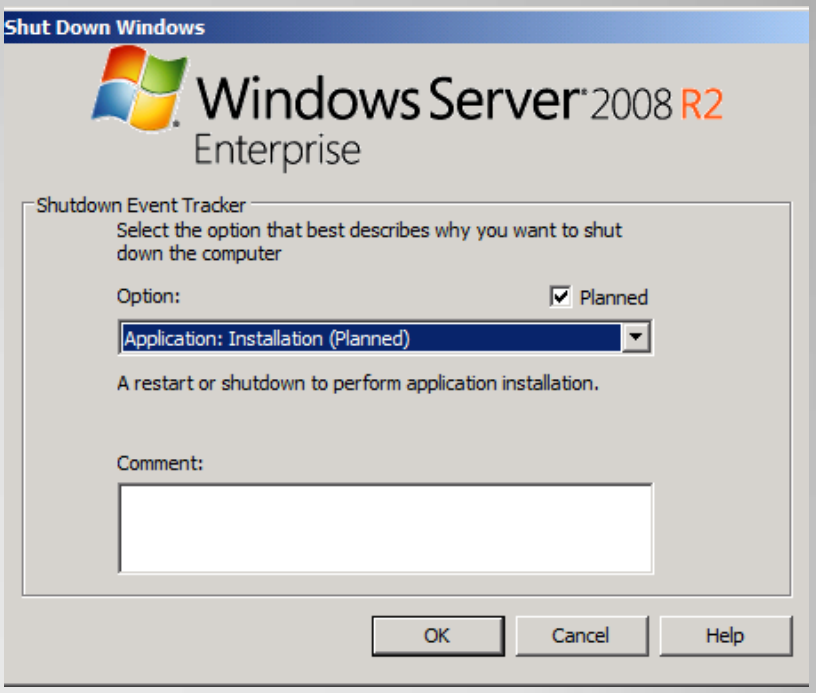
- **Reviewer** může číst a porovnávat GPO. Nemůže GPO editovat ani nasazovat do produkce (deploy).
- **Editor** může číst a porovnávat GPO. Může vyjmout GPO z archivu (check out), editovat GPO a vkládat je zpět (check in). Může požádat a o nasazení.
- **Approver** může schválit či zamítnout vytvoření nebo nasazení GPO.



AGPM – delegování rolí

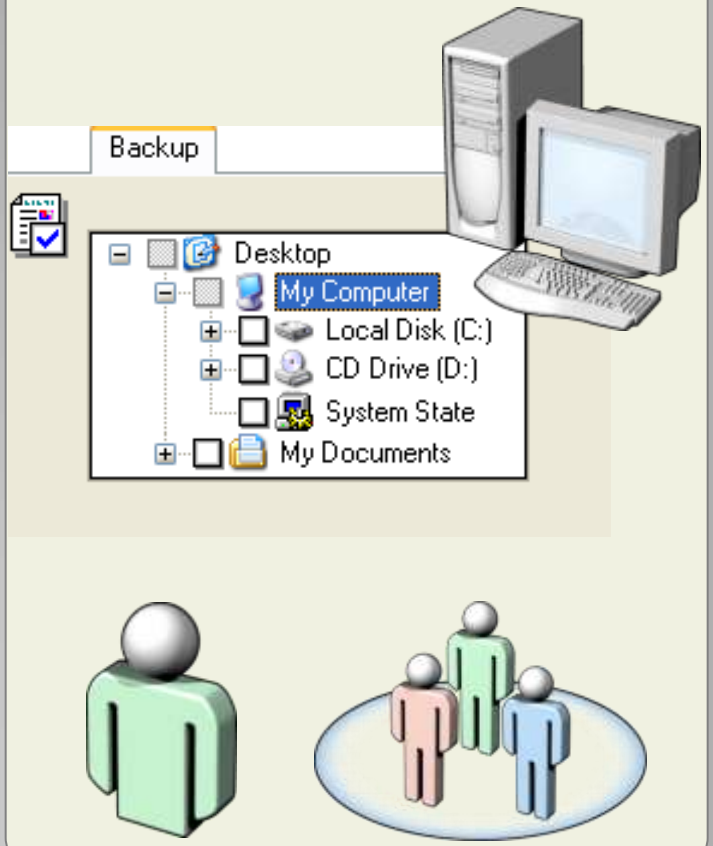
Rights vs. Permissions



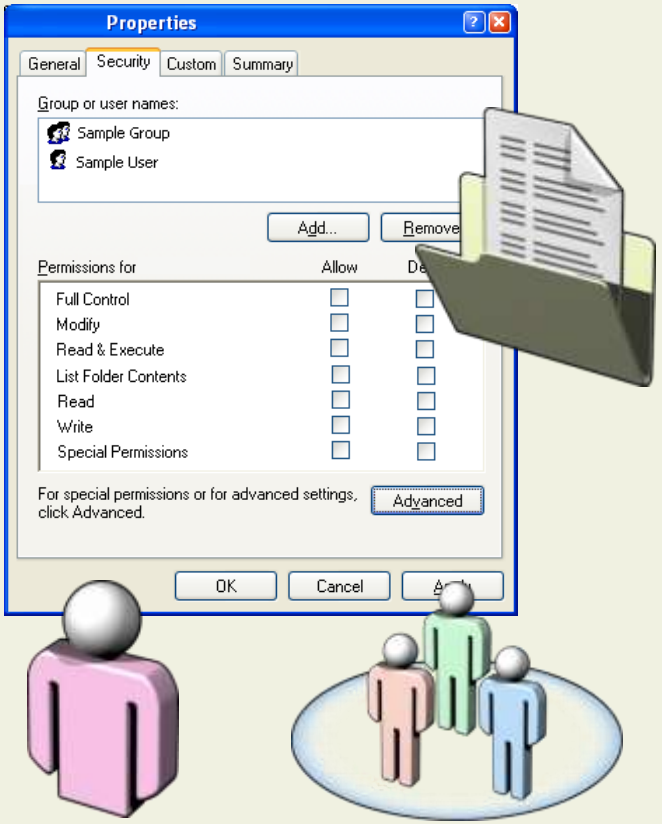


Příklady „User Rights“

User Rights:
Akce v systému



Permissions:
Operace s objekty



Rights vs. Permissions