Serverové systémy Microsoft Windows

IW2/XMW2 2013/2014

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 19. 3. 2014

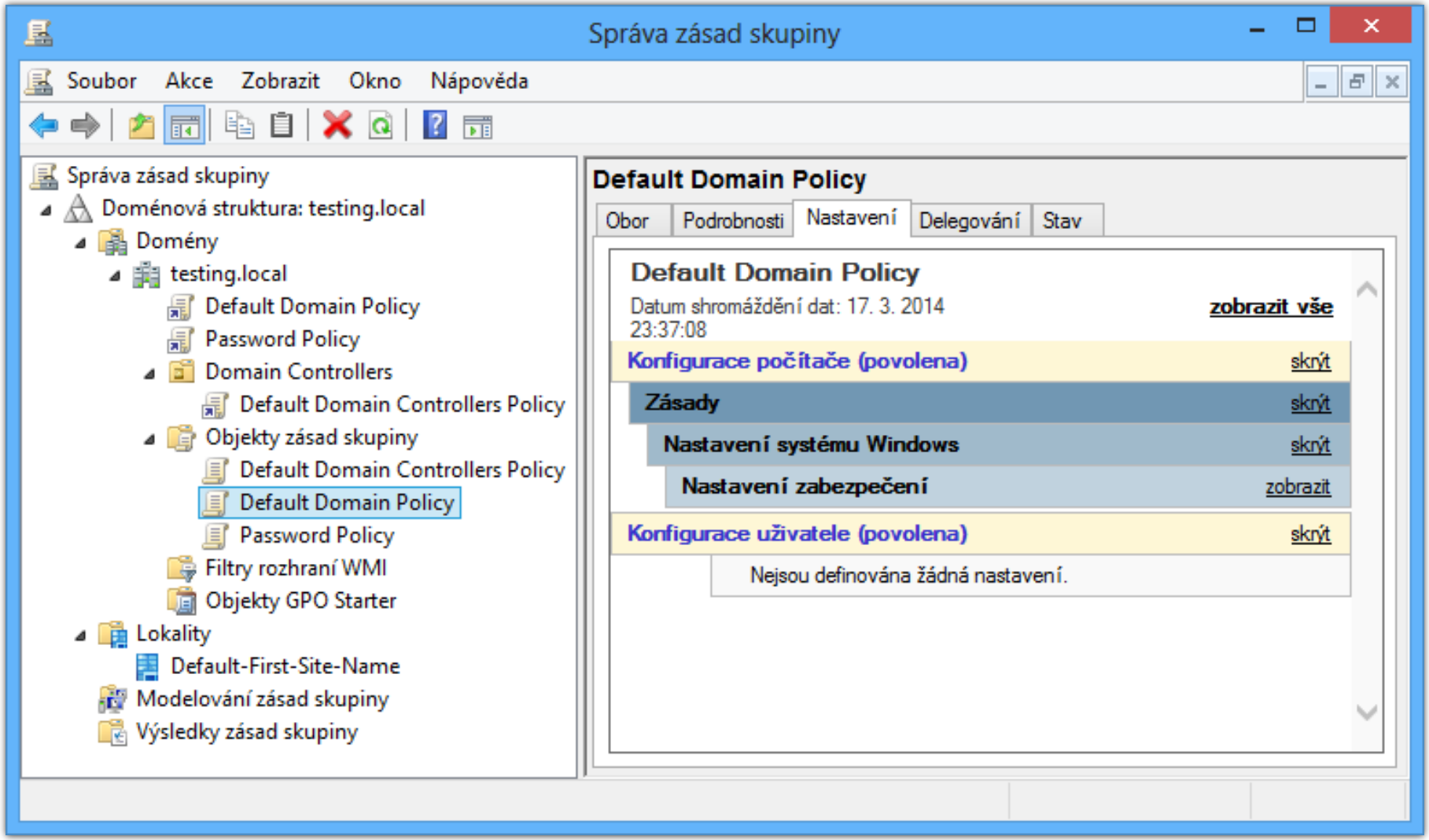
Active Directory

Zásady skupiny (objekty, zpracování)

Zásady skupiny (Group Policies)

- Umožňují centrální správu a konfiguraci systémů Windows, aplikací a uživatelů v Active Directory
  - Určují co (ne)může dělat uživatel na daném počítači
- Sada nastavení popisujících konfiguraci počítačů a/nebo uživatelů v prostředí Active Directory
  - Nastavení definována a uložena na řadičích domény
- Správa pomocí konzole Správa zásad skupiny (GPMC, *Group Policy Management Console*)
  - K dispozici po přidání funkce Správa zásad skupiny

Správa zásad skupiny



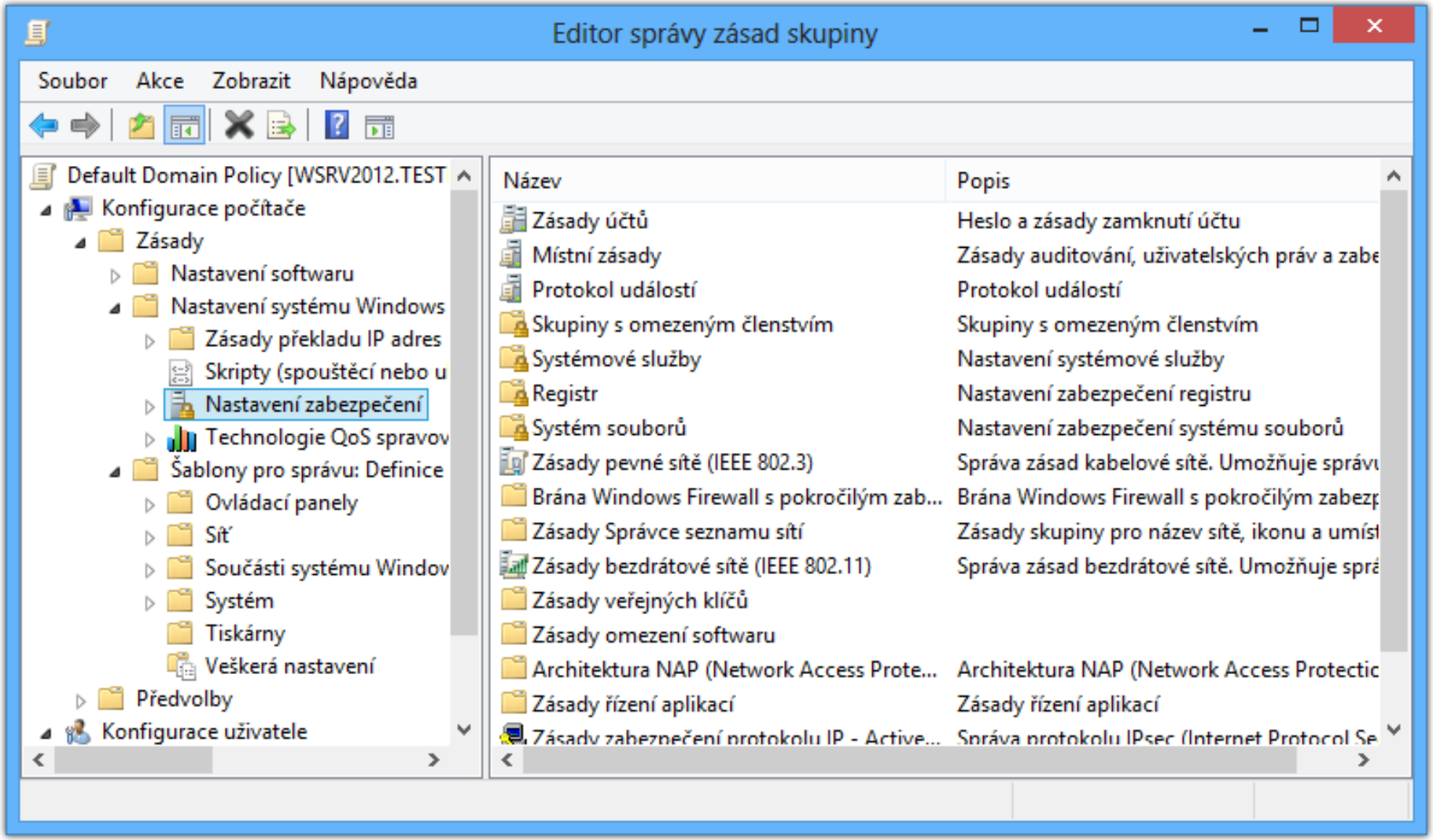
Nastavení zásady (policy setting)

- Zásada (*policy*)
  - Specifické nastavení systému Windows (registru, …)
  - Windows 8 a Server 2012 obsahuje přes 3500 zásad
- Definuje změnu v konfiguraci systému Windows
  - Většina nastavení se týká jen povolení resp. zakázání nějaké služby, vlastnosti nebo funkcionality systému
  - Některá nastavení vyžadují dodatečné informace
- Zásady mohou být nedefinovány (*not defined*)
  - Uplatní se dříve aplikované nebo výchozí nastavení

Aplikace nastavení zásad

- Nastavení aplikovaná na celý počítač
  - Obsažena pod uzlem konfigurace počítače (*computer configuration settings*)
  - Má přednost v případě, že je stejná zásada nastavena i v sekci aplikující nastavení na přihlášené uživatele
  - Nastavení zabezpečení (hesla, práva, …), systému, …
- Nastavení aplikovaná na přihlášeného uživatele
  - Obsažena pod uzlem konfigurace uživatele (*user configuration settings*)
  - Nastavení plochy, nabídky Start, součástí systému, …

Konfigurace počítače a uživatele



Objekty zásad skupiny (GPO objekty)

- Objekty Active Directory, jenž obsahují jednotlivá nastavení zásad
  - Fyzická reprezentace zásad skupiny v Active Directory
- Aplikace nastavení na základě rozsahu (*scope*)
  - Určuje uživatele a počítače, na které se mají aplikovat nastavení obsažená v daném GPO objektu
  - Lze definovat pomocí
    - GPO odkazu (*GPO link*)
    - WMI filtru (*Windows Management Instrumentation filter*)
    - Bezpečnostního filtru (*Security filter*)

GPO odkazy (GPO links)

- Propojují GPO objekty s doménami, místy (*sites*) a organizačními jednotkami (OUs)
  - Každý GPO objekt může být propojen s jedním i více kontejnery (doménami, místy, OU jednotkami)
  - Nastavení aplikováno na uživatele a počítače v těchto kontejnerech (a ostatních obsažených kontejnerech)
- Určují maximální rozsah GPO objektu
  - Filtry mohou z tohoto rozsahu vyřadit uživatele nebo počítače, ale nemohou žádné další přidat

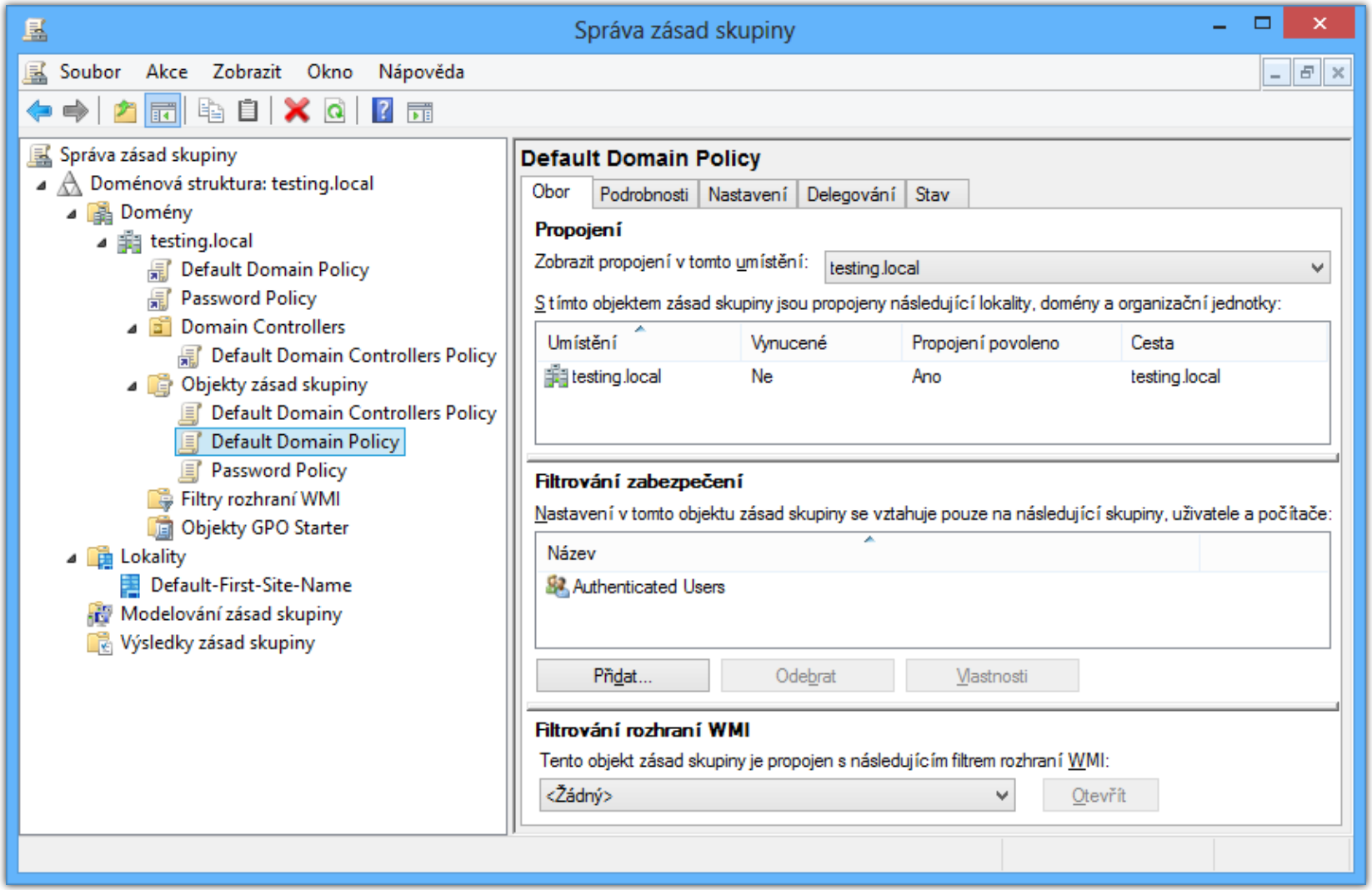
Filtry

- WMI filtry
  - Omezují rozsah GPO objektů na uživatele a počítače, kteří splňují zadaný WMI dotaz (*query*)
  - Např. omezení aplikace na konkrétní operační systém

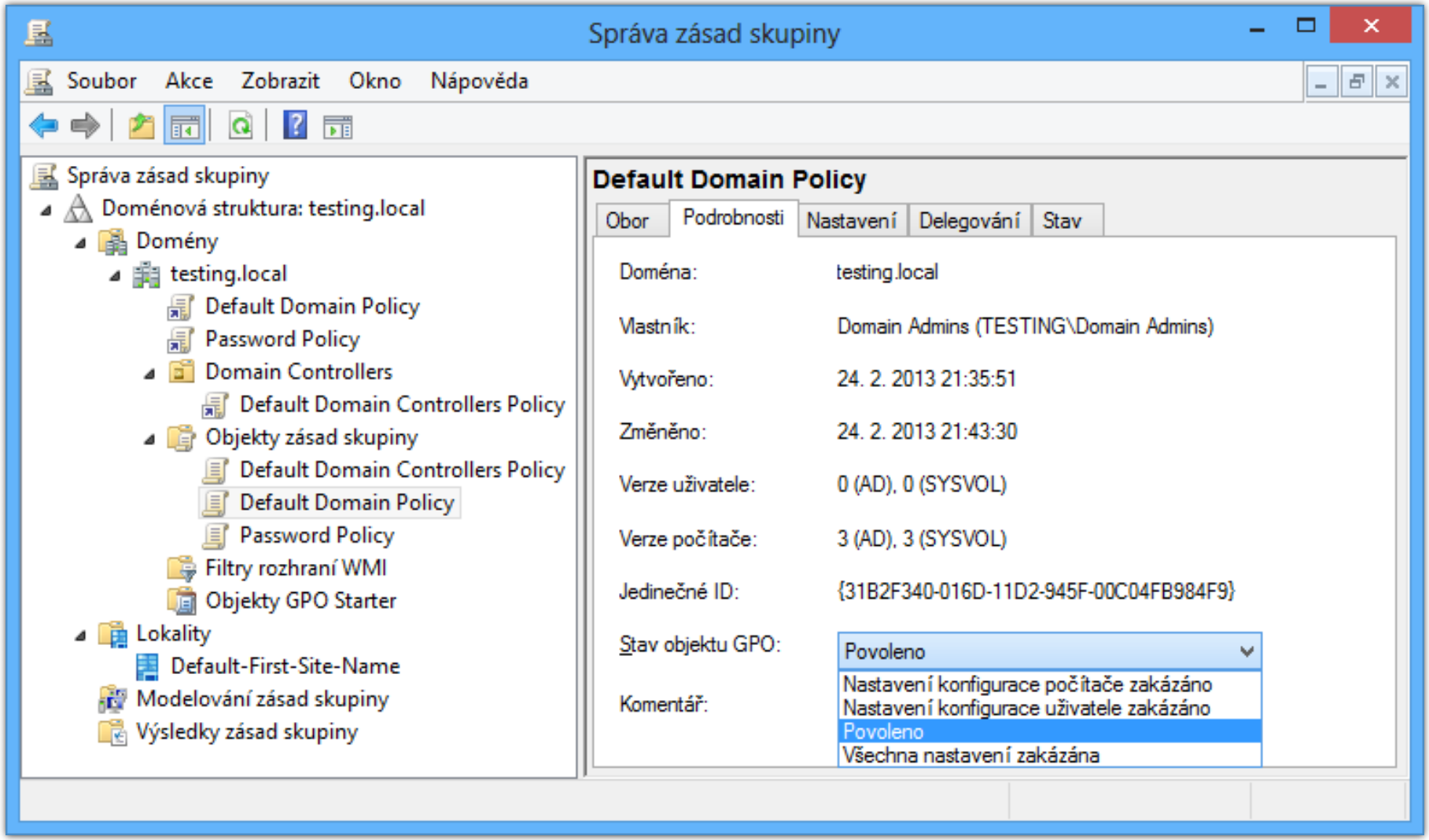
```
Select * from Win32_OperatingSystem
where Caption = "Microsoft Windows 7 Professional"
```

- Bezpečnostní filtry
  - Omezují rozsah GPO objektů na uživatele a počítače, jenž (ne)náleží do zadané (bezpečnostní) skupiny
  - Nastavují oprávnění pro čtení a použití zásad skupiny

Nastavení rozsahu GPO objektu



Nastavení stavu GPO objektu



Typy GPO objektů

- Lokální GPO objekty (*Local GPOs*)
  - Ovlivňují pouze počítač, na kterém jsou definovány
  - Uloženy v adresáři ***<systém>*\System32\GroupPolicy**
  - Od Windows Vista a Server 2008 možnost vytváření více než jednoho GPO objektu (*multiple local GPOs*)
- Doménové GPO objekty (*Domain GPOs*)
  - Aplikovány na různé počítače a uživatele v doméně
  - Uloženy v Active Directory (na řadičích domény)

Lokální (multiple local) GPO objekty

- GPO místního počítače (*Local Computer GPO*)
  - Jediný lokální GPO objekt, kde lze definovat nastavení aplikované na počítač (konfigurace počítače)
  - Uživatelská nastavení aplikována na všechny uživatele
- GPO speciálních skupin
  - Obsahuje uživatelská nastavení aplikované na správce nebo ostatní uživatele (nelze použít jiné skupiny)
- GPO místních uživatelů (*User-Specific Local GPO*)
  - Zahrnuje uživatelská nastavení pro jednoho uživatele

Pořadí aplikace lokálních GPO objektů

- Podle specifičnosti (menší rozsah, vyšší priorita)
- Konfigurace počítače
  1) GPO místního počítače
- Konfigurace uživatele
  1) GPO místního počítače
  2) GPO správců / ostatních uživatelů
  3) GPO přihlášeného uživatele

Doménové GPO objekty (odkazy)

- GPO objekty připojené k místu (*Site GPOs*)
  - Aplikovány na všechny počítače v konkrétním místě a na uživatele přihlášené na těchto počítačích
- GPO objekty připojené k doméně (*Domain GPOs*)
  - Aplikovány na všechny počítače a uživatele v doméně
- GPO objekty připojené k organizační jednotce (*OU GPOs*)
  - Aplikovány na všechny počítače a uživatele obsažené v organizační jednotce a vnořených org. jednotkách

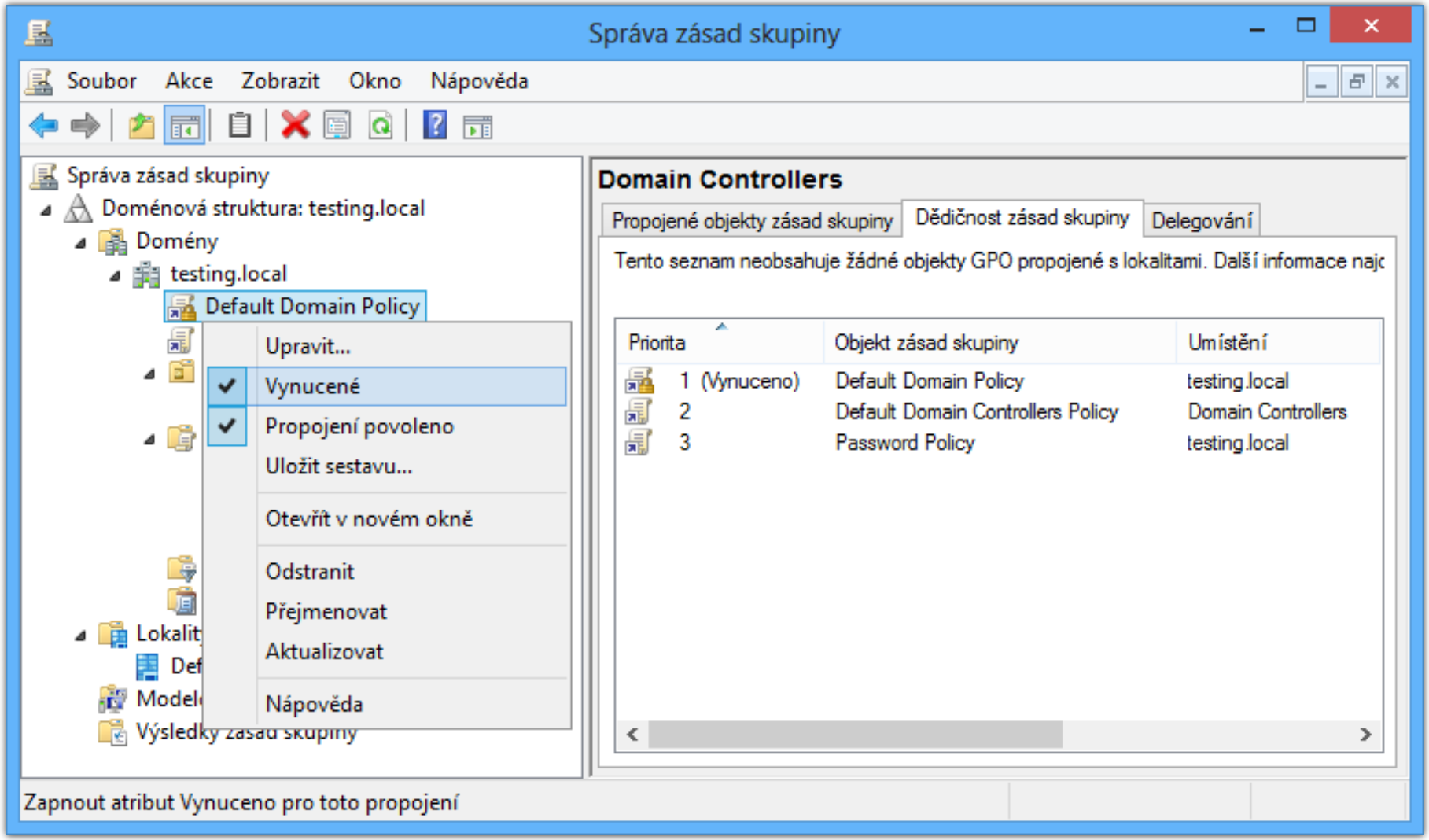
Základní doménové GPO objekty

- Výchozí zásady domény (*Default Domain Policy*)
  - Připojen k doméně
    - Aplikace na veškeré uživatele a počítače v dané doméně
  - Definuje nastavení týkající se hesel, uzamykání účtů a služby Kerberos
- Výchozí zásady řadičů domény (*Default Domain Controllers Policy*)
  - Připojen k organizační jednotce Řadiče domény
    - Aplikace na všechny (obsažené) řadiče domény
  - Definuje nastavení ohledně zásad auditu a práv

Vynucené (enforced) GPO objekty

- Mají vyšší prioritu než standardní GPO objekty
  - Aplikovány jako poslední (přepisují dřívější nastavení)
- Vytvářejí se vynucením konkrétního GPO odkazu
  - Stejný GPO objekt může být zároveň standardní GPO objekt i vynucený GPO objekt (záleží jak je připojen)
- Ignorují (neplatí pro ně) blokování dědičnosti
  - Vždy aplikovány na uživatele a počítače ve vnořených kontejnerech (organizačních jednotkách)

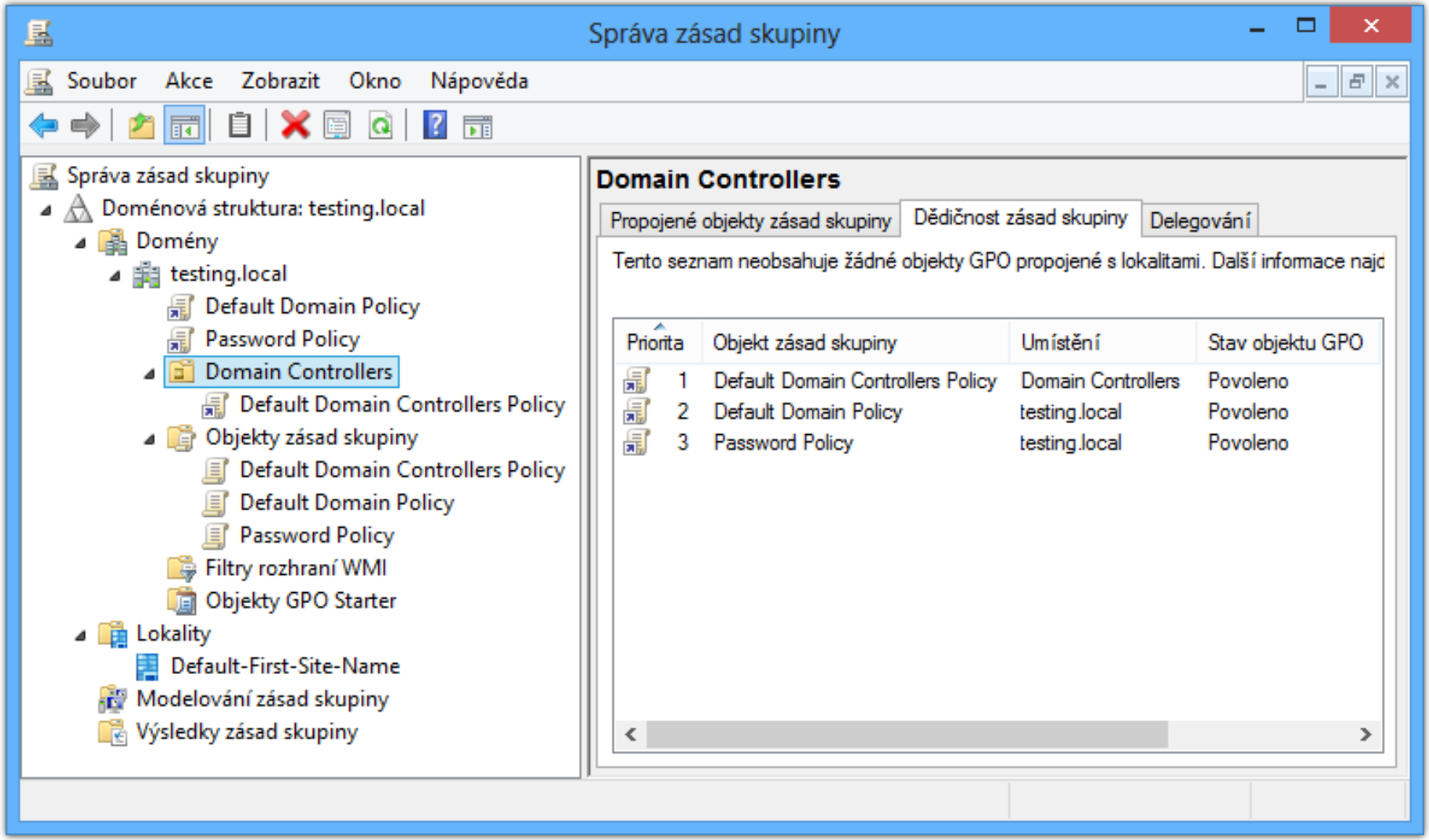
Vynucení aplikace GPO objektu



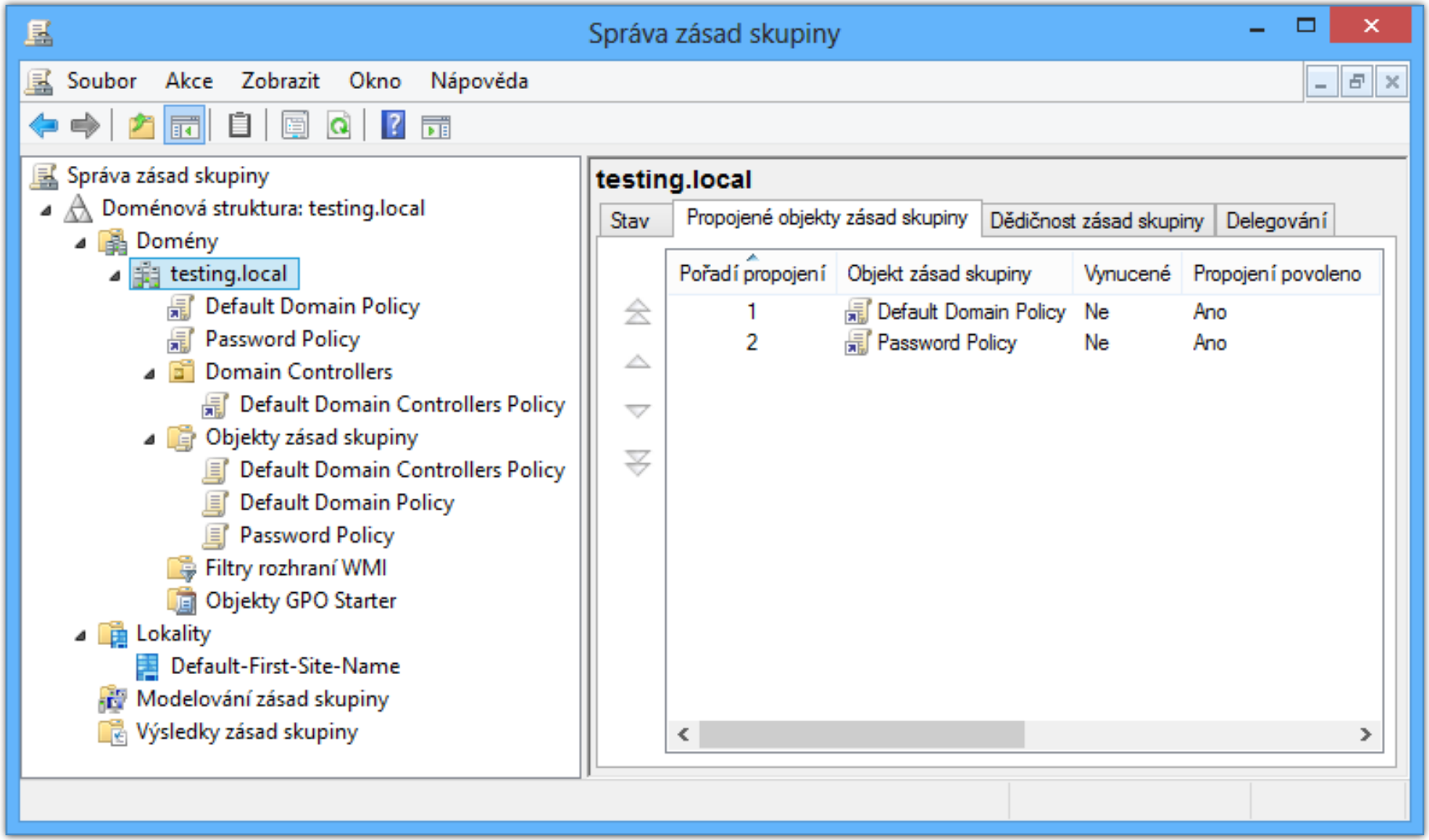
Pořadí aplikace GPO objektů

1) Lokální GPO objekty
2) Doménové GPO objekty
   a) Připojené k místu
   b) Připojené k doméně
   c) Připojené k organizačním jednotkám
3) Vynucené doménové GPO objekty
   a) Připojené k organizačním jednotkám
   b) Připojené k doméně
   c) Připojené k místu

Zjištění pořadí aplikace GPO objektů



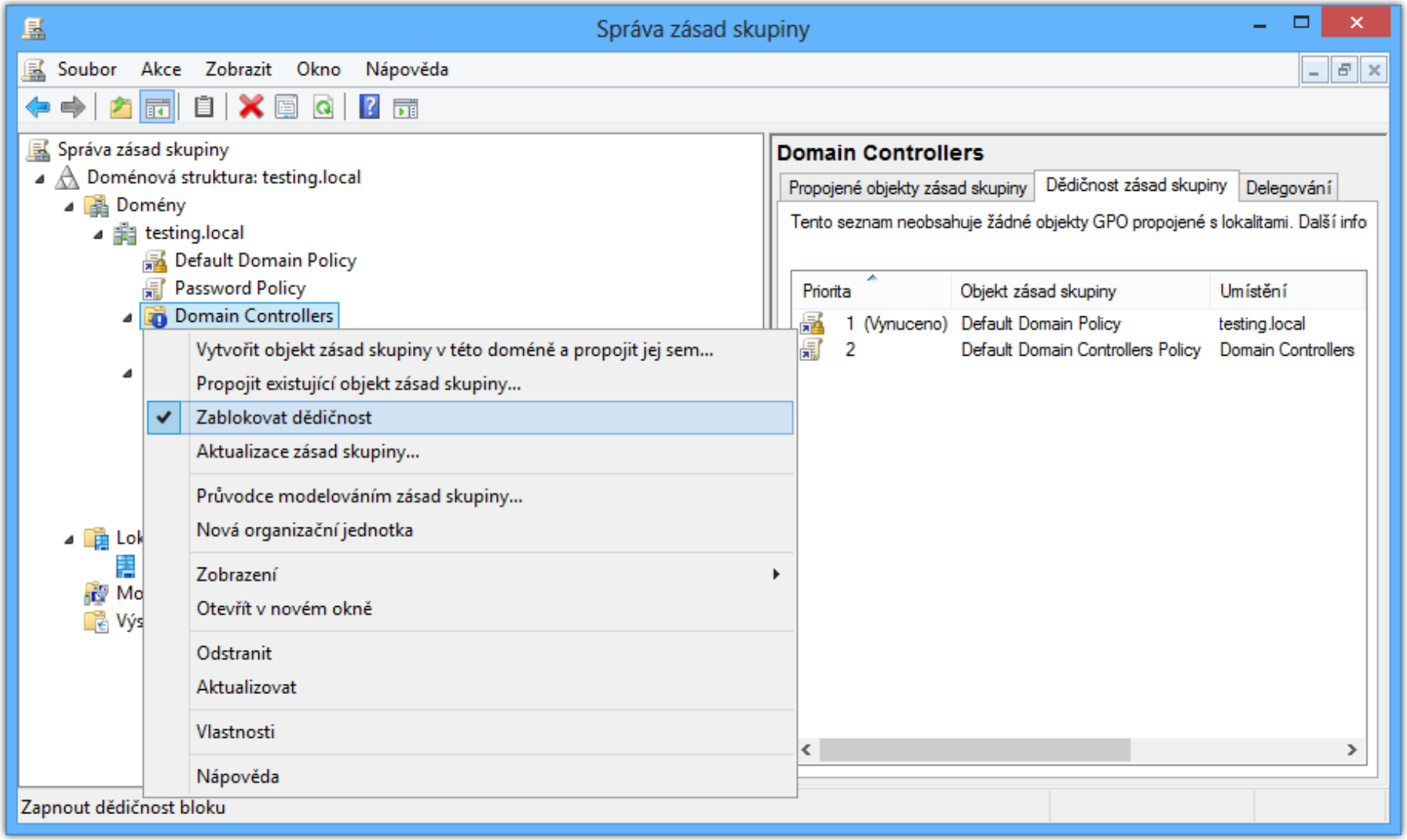
Pořadí aplikace v rámci kontejneru



Blokování dědičnosti (GPO objektů)

- Zabraňuje aplikaci nadřazených GPO objektů na uživatele a počítače v konkrétním kontejneru
  - Blokuje dědění GPO objektů z otcovských kontejnerů
  - Nelze použít pro blokování vynucených GPO objektů
- Nastavuje se na organizačních jednotkách nebo na celé doméně

Zablokování dědičnosti (GPO objektů)



Klient zásad skupiny

- Služba zajišťující aplikaci nastavení zásad na daný počítač nebo uživatele
  - Využívá *pull* metodu (klient sám stahuje GPO objekty z řadiče domény, řadič domény jen ověřuje přístup)
- Změny provádějí tzv. klientská (CSE) rozšíření
  - Zajišťují zpracování konkrétní kategorie zásad skupiny
- Rozdílové zpracování GPO objektů
  - Aplikace jen těch nastavení zásad, jenž byly změněny (jsou odlišné od nastavení aplikovaných předtím)
  - Lze vypnout (vynutit aplikaci všech nastavení zásad)

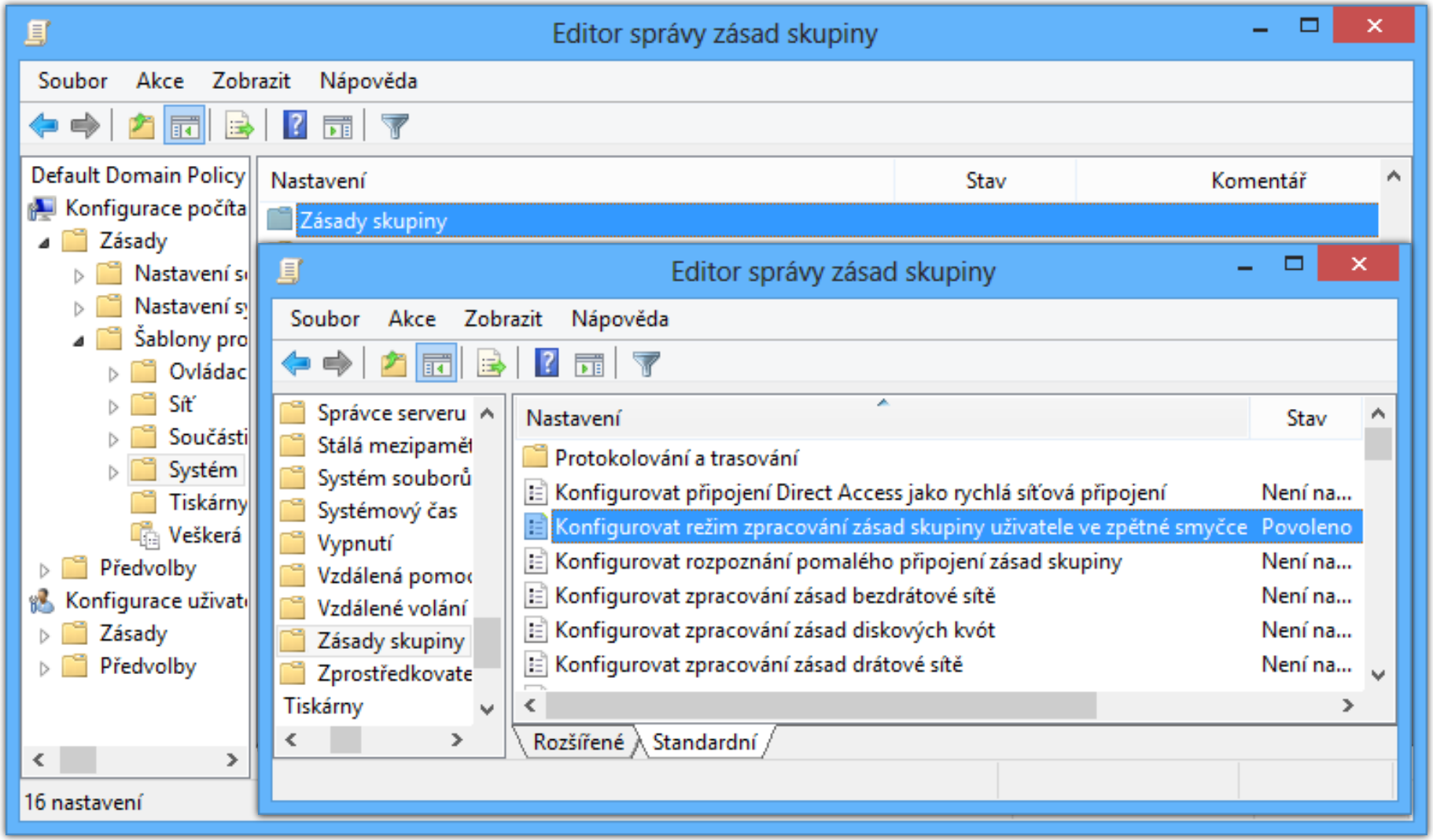
Postup zpracování zásad skupiny

1) Stažení seznamu GPO objektů
2) Zpracování obsažených GPO objektů
   a) Kontrola stavu GPO objektu (povolen / nepovolen)
   b) Kontrola oprávnění (číst a používat zásady skupiny)
   c) Vykonání a vyhodnocení WMI dotazu ve WMI filtru
3) Aplikace nastavení obsažených v GPO objektech
   a) Zpracování nastavení (definováno / nedefinováno)
   b) Zavolání odpovídajícího CSE rozšíření
4) Zopakování bodů 1) až 3) za 90 – 120 minut

Loopback zpracování zásad skupiny

- Umožňuje aplikovat nastavení zásad na uživatele na základě počítače, na který je přihlášen
  - Povoluje aplikaci uživatelských nastavení obsažených v GPO objektech, jenž mají ve svém rozsahu počítač, na který je uživatel přihlášen, a ne daného uživatele
- Povoluje se v zásadách skupiny
  - Projeví se teprve při druhé aplikaci zásad skupiny
    - Při první aplikaci dochází k přepnutí klienta zásad skupiny do loopback režimu zpracování
  - Nastavení počítače (nelze povolit pro určité uživatele)

Povolení loopback zpracování



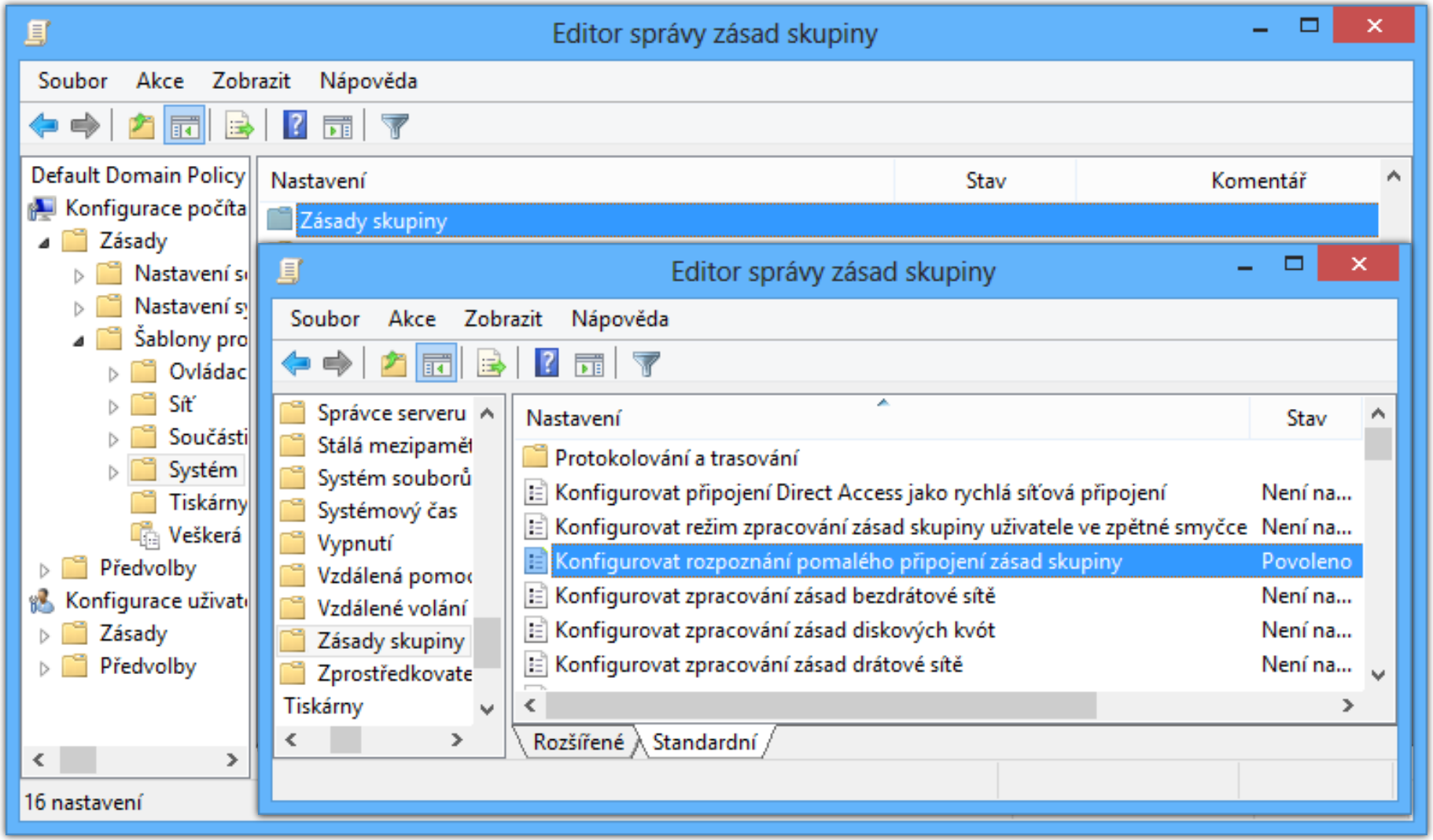
Režimy loopback zpracování

- Nahradit (*replace*)
  - Použije uživatelská nastavení z GPO objektů počítače, na kterém je daný uživatel přihlášen
  - Nastavení z GPO objektů uživatele jsou ignorovány
- Sloučit (*merge*)
  - Použije uživatelská nastavení z GPO objektů uživatele i počítače, na kterém je daný uživatel přihlášen
  - Nastavení z GPO objektů počítače aplikovány později (přepisují nastavení z GPO objektů uživatele)
    - Dodatečná úprava uživatelských nastavení pro daný počítač

Režim pomalého připojení (slow-link)

- Zabraňuje aplikaci nastavení některých zásad při detekci pomalého spojení s řadičem domény
  - Týká se hlavně nastavení zásad, jejichž aplikace vede k objemnějším přenosům dat (např. instalace SW)
- Aktivován pokud přenosová rychlost klesne pod definovaných práh (*threshold*)
  - Ve výchozím nastavení je práh 500 Kbit/s
  - Lze změnit v zásadách skupiny

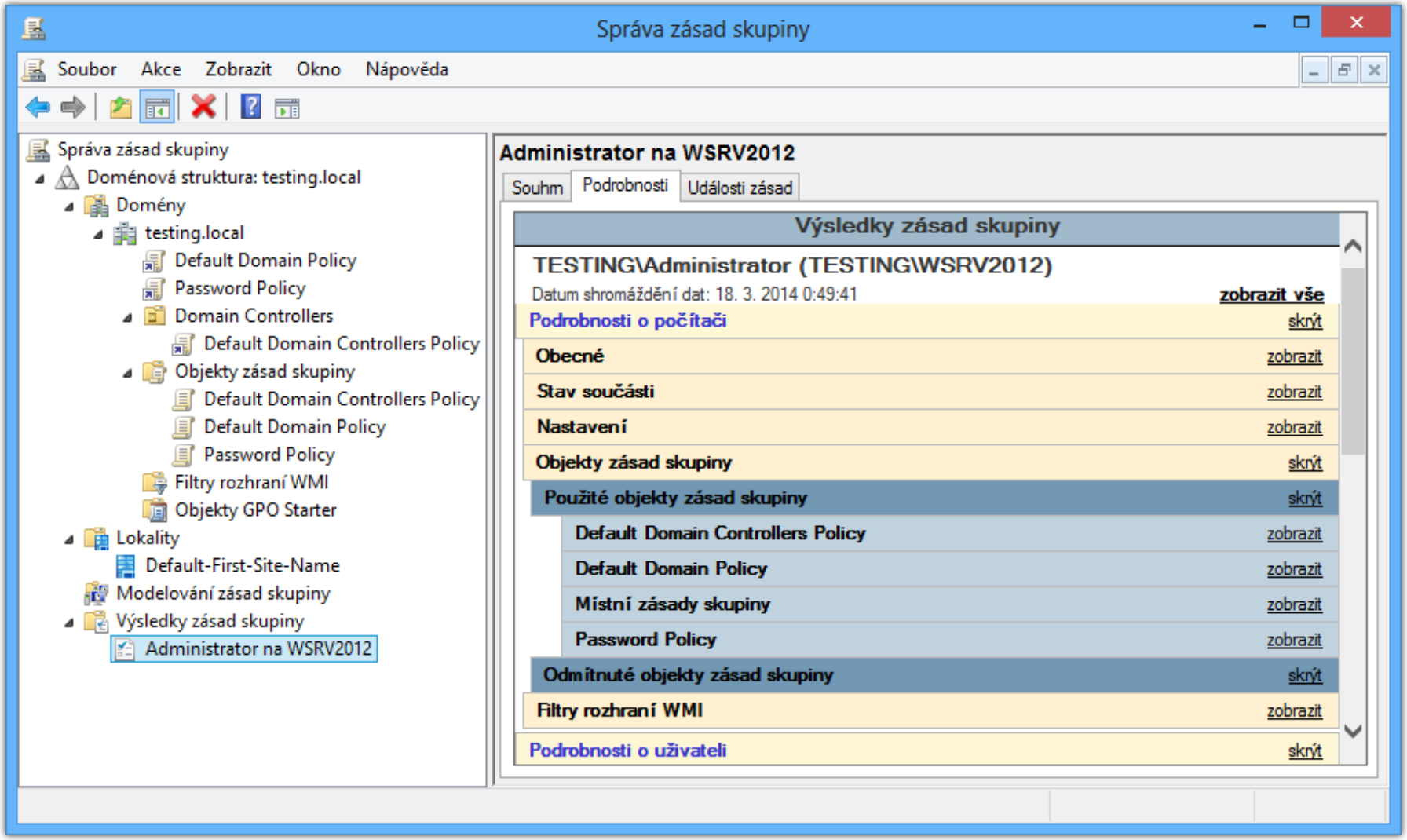
Nastavení prahu pro pomalé připojení



Výsledné sady zásad (RSoP)

- Vyhodnocují výslednou sadu nastavení zásad pro konkrétního uživatele nebo počítač
- Výsledky zásad skupiny (*results*)
  - Zjišťuje aktuální nastavení zásad
  - Možnost vyhodnocení pomocí nástroje **gpresult**
- Modelování zásad skupiny (*modeling*)
  - Simuluje výsledné nastavení zásad (např. po přesunu uživatele nebo počítače)
  - Realizují řadiče domény (musí být k dispozici)

Informace o použitých GPO objektech



Výsledná nastavení