KAPITOLA 3

Správa zásad skupiny

V této kapitole:

Při práci se zásadami skupiny je základním nástrojem konzola Správa zásad skupiny (Group Policy Management Console, GPMC). V kapitole 1 „Úvod do zásad skupiny" a podrobněji v příloze A se uvádí, že konzolu Správa zásad skupiny musíte nejprve nainstalovat a že postup instalace závisí na operačním systému, který běží na vašem počítači. Příloha A také popisuje krok za krokem, jak systém zásad skupiny různými způsoby rozšířit. Pokud váš počítač neobsahuje klientská rozšíření zásad skupiny, můžete je nainstalovat, abyste mohli začít používat jak předvolby zásad, tak nastavení zásad.

K některým aplikacím, například k součástem systému Microsoft Office, existují šablony a doplňky pro zásady skupiny, takže tyto aplikace lze také ovládat přes systém zásad skupiny. Hlubší kontrola používání zásad skupiny je k dispozici prostřednictvím klientských a serverových komponent pro pokročilou správu zásad skupiny (Advanced Group Policy Management, AGPM). Jedná se o sadu rozšíření pro konzolu Správa zásad skupiny, která obsahuje řízení změn a další funkce.

V této kapitole se dozvíte o technikách práce s konzolou GPMC. V kapitole 4 „Pokročilá správa zásad skupiny" se naučíte využívat dodatečné funkce poskytované sadou AGPM.

Porozumění výsledné sadě zásad

Zásady skupiny se týkají pouze uživatelů a počítačů. Konfigurační volby zásad skupiny mají dvě kategorie: Konfigurace počítače (Computer Configuration), která obsahuje sady nastavení pro počítače, a Konfigurace uživatele (User Configuration) obsahující

nastavení pro uživatele. V každé z obou kategorií se rozlišují nastavení zásad a předvolby zásad.

Oba tyto typy zásad se dále dělí na několik hlavních tříd voleb, v nichž jsou další podtřídy. V případě nastavení zásad rozeznáváme tři hlavní třídy:

- **Nastavení softwaru (Software Settings)** – automatická instalace nového softwaru a softwarových upgradů. Používá se i pro odinstalování softwaru.
- **Nastavení systému Windows (Windows Settings)** – ovládání klíčových nastavení systému Windows pro počítače i uživatele, včetně skriptování a zabezpečení. Pro uživatele jsou k dispozici také služby vzdálené instalace, přesměrování složky a údržby aplikace Internet Explorer.
- **Šablony pro správu (Administrative Templates)** – správa nastavení registru, slouží ke změnám konfigurace operačního systému, komponent Windows a aplikací. Šablony pro správu jsou určeny pro specifickou verzi operačního systému.

Předvolby zásad mají dvě hlavní třídy voleb:

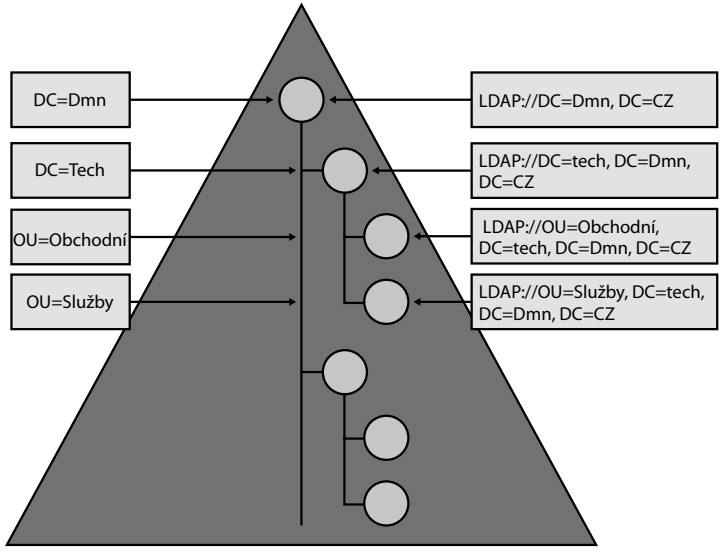
- **Nastavení systému Windows (Windows Settings)** – konfigurace klíčových nastavení systému Windows pro počítače i uživatele, včetně proměnných prostředí, souborů, složek, hodnot v registru a zástupců. Pro počítače jsou k dispozici navíc sdílené síťové složky, pro uživatele aplikace a mapování jednotek.
- **Nastavení ovládacích panelů (Control Panel Settings)** – konfigurace rozličných voleb a utilit v ovládacích panelech, mezi nimi zdrojů dat, zařízení, možností složky, možností sítě, napájení a tiskárny.

Jestliže klient zásad skupiny běžící na počítači aplikuje objekty GPO na uživatele a počítač, jejich efekt (tedy konečný výsledek dědičnosti a dalšího zpracování) je kumulativní. Souhrnný efekt zásad skupiny na konkrétní uživatele nebo počítače se nazývá Výsledky zásad skupiny (Resultant Set of Policy, RSoP). Zjištění exaktních výsledků zásad skupiny slouží k ověření, jak přesně se zásady v určitém případě aplikují.

Výsledky zásad skupiny pro uživatele nebo počítač jsou k dispozici v konzole Správa zásad skupiny (GPMC) prostřednictvím Průvodce výsledky zásad skupiny (Group Policy Results Wizard). K modelování změn, které byste chtěli učinit, slouží Průvodce modelováním zásad skupiny (Group Policy Modeling Wizard). Oba tito průvodci se probírají v sekci „Plánování změn zásad skupiny“ v kapitole 7, „Zpracování zásad skupiny“.

V Active Directory jsou objekty seřazeny do hierarchické stromové struktury zvané *adresářový strom*. Ve struktuře tohoto stromu se odráží schéma domény a používá se k určení vztahu rodič-potomek mezi objekty uloženými v adresáři. Obrázek 3.1 ilustruje adresářový strom domény. Doména samotná je rodičovským objektem všech objektů v doméně a jako taková představuje kořen stromu. Samotný objekt domény má mezi potomky další objekty s obsahem (kontejnery), například poddomény a organizační jednotky (OU), stejně jako standardní objekty, mezi které patří uživatelé, počítače

a tiskárny. Na obrázku je tech.dmn.cz poddoménou dmn.cz a tato poddoména má dvě hlavní organizační jednotky: obchodní oddělení a oddělení služeb.



Obrázek 3.1: Doména dmn.cz a její adresářový strom

Active Directory používá pro přístup k objektům v adresáři protokol LDAP (Lightweight Directory Access Protocol). Na každý adresářový objekt se dá odkázat prostřednictvím cesty LDAP. Pro obchodní oddělení v doméně tech.dmn.cz je odpovídající cesta LDAP://OU=Obchodní, DC=tech, DC=Dmn, DC=CZ. Zde *LDAP://* určuje, že se jedná o protokol LDAP, a *LDAP://OU=Obchodní, DC=tech, DC=Dmn, DC=CZ* reprezentuje přesné umístění oddělení v Active Directory. V cestě jsou uvedeny všechny komponenty jména příslušného objektu. (OU je zkratka pro organizační jednotku – Organizational Unit, DC pro komponentu domény – Domain Component.) Přesná cesta k objektu bez určení protokolu představuje rozpoznané jméno objektu (Distinguished Name, DN).

Objekty v adresáři mají i svá relativní jména, známá také jako relativní rozpoznané jméno objektu (Relative Distinguished Name, RDN). To obsahuje jen poslední část jména objektu, například pro obchodní oddělení v tech.dmn.cz je to OU=Obchodní. V tomto oddělení nechť je definován uživatel Josef a počítač JosefovoPC. Jejich relativní jména budou CN=Josef, respektive CN=JosefovoPC; zkratka CN zde znamená obvyklé jméno (Common Name). Celá jména DN obou těchto objektů pak budou CN=Josef, OU=Obchodní, DC=tech, DC=Dmn, DC=CZ a CN=JosefovoPC, OU=Obchodní, DC=tech, DC=Dmn, DC=CZ.

Jméno DN identifikuje umístění objektu v adresáři. Dozvíte se z něho, ve kterých kontejnerech je který objekt umístěn, ale také jaké jsou mezi těmito kontejnery vztahy. Tyto

vztahy jsou velmi podstatné při aplikaci zásad skupiny. Když víte, kde má objekt v adresářovém stromě své místo a ve kterém kontejneru se nachází, máte klíč k tomu, který objekt GPO se typicky bude na tento objekt aplikovat. Je však důležité mít na paměti, že zásady skupiny se nedědí z rodičovské domény na doménu potomka a že jméno DN objektu nic neříká o tom, kde je fyzicky umístěn.

Z praxe: Dědičnost funguje jinak uvnitř domén a jinak mezi doménami navzájem. Uvnitř domény se objekt GPO na nejvyšší úrovni přenáší do objektů GPO na nižších úrovních. To znamená, že objekt GPO pro doménu se automaticky zdědí v jejích organizačních jednotkách. Objekt GPO pro doménu a pro organizační jednotku na nejvyšší úrovni se dědí v organizačních jednotkách nižších úrovní a tak dále. Mezi rodičovskou doménou a doménou potomka však dědičnost není automatická. Doména potomka totiž automaticky nezdědí objekt GPO od rodičovské domény. Microsoft doporučuje nepřenášet objekty GPO mezi doménami, protože když je objekt GPO získán z jiné domény, zpracování zásad skupiny může významně zpomalit proces přihlášení a odhlášení. Z tohoto důvodu je jen velmi zřídka v doménách potomka dědičnost vynucena.

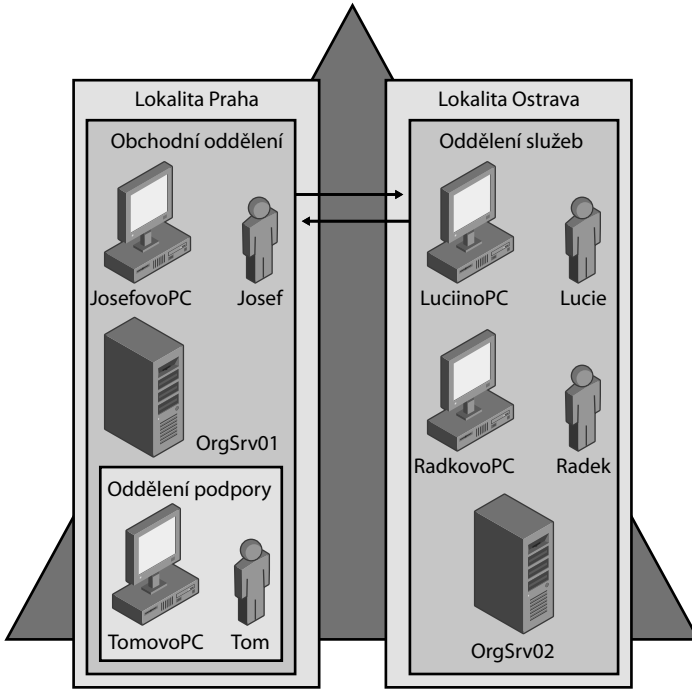
Ačkoli adresářová cesta informuje o většině kontejnerů obsahujících objekty GPO, které mají vliv na nějakého uživatele nebo počítač, není tato informace úplná. Některé objekty GPO jsou zde zcela vynechány, a ty mají co do činění s lokalitami.

Lokality slouží k projekci skutečné fyzické struktury sítě. Jelikož lokality jsou zcela oddělené a nezávislé na logických prvcích v adresáři, nemusí nutně existovat žádný vztah mezi vašimi síťovými lokalitami a doménami v adresářové struktuře. Doména může pokrývat jednu nebo více lokalit, ale také lokalita může obsahovat jednu nebo více domén.

Na obrázku 3.2 je znázorněn bližší pohled na doménu tech.dmn.cz a její objekty. Jak je patrné, s touto doménou jsou spjaty dvě lokality:

- **Lokalita Praha** – tato lokalita má dvě organizační jednotky: oddělení obchodu a podpory. Obchodní oddělení, které je na nejvyšší úrovni, obsahuje dva počítačové a jeden uživatelský objekt. Oddělení podpory, jehož je obchodní oddělení rodičovskou organizační jednotkou, obsahuje jeden objekt typu počítač a jeden typu uživatel. OrgSrv01 je řadič domény, zatímco JosefovoPC a TomovoPC jsou pracovní stanice.
- **Lokalita Ostrava** – v této lokalitě máme jedinou organizační jednotku, oddělení služeb, jejíž součástí je několik výpočetních zdrojů. Oddělení služeb je organizační jednotkou nejvyšší úrovně, bez podřízených organizačních jednotek. Obsahuje tři objekty typu počítač a dva typu uživatel. OrgSrv02 je doménový řadič, RadkovoPC a LuciinoPC jsou pracovní stanice.

Podle tohoto diagramu přesně poznáte, které objekty jsou umístěny v Active Directory ve kterých kontejnerech. Víte také, ve kterých lokalitách jsou umístěny jaké objekty. To všechno vám dává kompletní přehled o tom, které objekty GPO se aplikují na které adresářové objekty. Protože, jak víme, počítače a uživatelé jsou ovlivněni také místními



Obrázek 3.2: Rozvrstvení objektů v doméně tech.dnm.cz

objekty LGPO, na objekt JosefovoPC se budou vztahovat následující objekty GPO, a to v tomto pořadí:

1. Místní objekt GPO pro JosefovoPC
2. Objekt GPO pro lokalitu Praha
3. Objekt GPO svázaný s poddoménou tech.dmn.cz
4. Objekt GPO propojený s organizační jednotkou Obchodní oddělení

Na uživatele Josefa by se uplatnily úplně stejné objekty GPO, jež by se aplikovaly ve stejném pořadí, aby nastavily povolené akce a omezení svázané s jeho účtem.

Když pokročíme v našem příkladu a vynecháme přitom místní objekty GPO, zjistíme, že zásady skupiny se na počítače a uživatele uplatňují takto:

- Na úrovni lokality Praha se všechny objekty svázané s touto lokalitou aplikují na JosefovoPC, Josefa, OrgSrv01, TomovoPC a Toma. Naproti tomu objekty GPO propojené s lokalitou Ostrava mají vliv na LuciinoPC, Lucii, RadkovoPC, Radka a OrgSrv02.

- Na úrovni domény máme objekty GPO propojené s doménou tech.dmn.cz, a ty se aplikují na JosefovoPC, Josefa, OrgSrv01, TomovoPC, Toma, LuciinoPC, Lucii, RadkovoPC, Radka a OrgSrv02.
- Dále je zde úroveň organizační jednotky, kde objekty GPO svázané s obchodním oddělením se týkají objektů JosefovoPC, Josef a OrgSrv01. Objekty GPO propojené s oddělením podpory mění nastavení pro TomovoPC a Toma. Nakonec objekty GPO z oddělení služeb mají vliv na LuciinoPC, Lucii, RadkovoPC, Radka a OrgSrv02.

Výsledné sady zásad našich objektů, po vynechání místních objektů GPO, by tedy vypadaly takto:

- **Josef –** výsledné zásady skupiny pro Josefa jdou od lokality Praha přes tech.dnm.cz po obchodní oddělení.
- **JosefovoPC –** výsledná sada zásad pro JosefovoPC jde od lokality Praha přes tech.dnm.cz po obchodní oddělení.
- **OrgSrv01 –** výsledné zásady pro OrgSrv01 jdou od lokality Praha přes tech.dnm.cz po obchodní oddělení.
- **Lucie –** výsledné zásady skupiny Lucie jdou v pořadí lokalita Ostrava, doména tech.dmn.cz, a pak oddělení služeb.
- **LuciinoPC –** výsledné zásady pro LuciinoPC mají pořadí lokalita Ostrava, doména tech.dmn.cz, a nakonec oddělení služeb.
- **Radek –** Radkovy výsledné zásady skupiny se uplatňují od lokality Ostrava přes doménu tech.dmn.cz po oddělení služeb.
- **RadkovoPC –** výsledné zásady pro RadkovoPC jdou od lokality Ostrava přes doménu tech.dmn.cz po oddělení služeb.
- **OrgSrv02 –** na OrgSrv02 se výsledné zásady projeví v pořadí od lokality Ostrava přes doménu tech.dmn.cz po oddělení služeb.
- **Tom –** výsledné zásady skupiny pro Toma jdou od lokality Praha přes tech.dnm.cz po obchodní oddělení, a pak dále na oddělení podpory.
- **TomovoPC –** výsledné zásady skupiny objektu TomovoPC začínají u lokality Praha, pokračují přes doménu tech.dnm.cz a obchodní oddělení až k oddělení podpory.

Při pohledu na výsledné zásady skupiny je třeba uvážit jeden důležitý aspekt, a to následky provedených změn. Tedy co se stane, když například Lucie odcestuje do Prahy a v kanceláři se připojí na počítač Josefa, nebo když Tom z oddělení podpory zajede do Ostravy a připojí se na RadkovoPC. Následky v systému zásad skupiny jsou tyto:

- **Lucie se v Praze připojuje na JosefovoPC –** JosefovoPC je předmětem Konfigurace počítače (Computer Configuration) v objektech GPO pro lokalitu Praha, doménu tech.dmn.cz a obchodní oddělení. Lucie (připojující se na JosefovoPC v Praze) obdrží nastavení Konfigurace uživatele (User Configuration), jež jsou součástí objektů GPO pro lokalitu Ostrava, doménu tech.dmn.cz a oddělení služeb. Stan-

dardní chování způsobí, že Konfigurace uživatele (User Configuration) v objektech GPO pro Lucii mají v případě konfliktu přednost.

- **Tom se v Ostravě připojuje na RadkovoPC –** RadkovoPC je předmětem Konfigurace počítače (Computer Configuration) v objektech GPO pro lokalitu Ostrava, doménu tech.dmn.cz a oddělení služeb. Tom (přihlašující se na RadkovoPC v Ostravě) obdrží nastavení Konfigurace uživatele (User Configuration), jež jsou součástí objektů GPO pro lokalitu Praha, doménu tech.dmn.cz, obchodní oddělení a oddělení podpory. Ve standardním nastavení má Konfigurace uživatele (User Configuration) v objektech GPO pro Toma přednost.
- **Přesunutí serveru OrgSrv01 do oddělení podpory –** OrgSrv01 (po přesunu do oddělení podpory) je předmětem objektů GPO pro lokalitu Praha, doménu tech.dmn.cz, obchodní oddělení a oddělení podpory. Nastavení zásad pro oddělení podpory pak mají přednost.

Tip: V této sekci jsme se soustředili na zpracování zásad napříč lokalitami a doménami. Tímto způsobem probíhá sice zpracování zásad skupiny uvnitř doménové struktury, ale nefunguje tak napříč různými doménovými strukturami. Máte-li zájem o toto téma, najděte si sekci „Zpracování zásad napříč doménovými strukturami" v kapitole 8 „Údržba a obnovení zásad skupiny".

Správa místních zásad skupiny

V sekci „Typy objektů GPO" v kapitole 2 „Nasazení zásad skupiny" jsme již zmínili, že ve Windows Vista, Windows Serveru 2008 a novějších verzích Windows je možné používat na jediném počítači více místních objektů GPO (LGPO) – pokud ovšem tento počítač není řadičem domény. Dříve mohly mít počítače pouze jediný objekt LGPO.

U počítačů náležících pracovní skupině (narozdíl od strojů v doméně) můžete zjistit, že vám používání více objektů LGPO vyhovuje, protože již nemusíte explicitně povolovat a zakazovat nastavení, která nějak souvisí s vykonáváním administrativních úkonů. Místo toho zavedete jeden objekt LGPO pro administrátory a druhý pro ostatní uživatele.

V případě zapojení počítače do domény se však budete chtít pravděpodobně více objektům LGPO vyhnout. V doménách má totiž většina uživatelů i počítačů již s sebou svázané vícenásobné objekty GPO. Přidání více objektů LGPO k této již tak pestré skladbě může způsobit zbytečné komplikace. Proto zvažte, zda zpracování objektů LGPO zcela nezakázat. Ze sekce „Typy objektů GPO" v kapitole 2 vyplývá, že k tomu stačí použít nastavení Vypnout zpracování místních objektů Zásad skupiny (Turn Off Local Group Policy Objects Processing) v Konfigurace počítače\Zásady\Šablony pro správu\Systém\Zásady skupiny (Computer Configuration\Policies\Administrative Templates\System\Group Policy).

K práci s objekty LGPO je nutné použít účet administrátora. V doméně lze použít účet, který je členem skupiny Enterprise Admins, Domain Admins nebo místní skupiny

Administrators na počítači. V pracovní skupině je třeba účet, který je členem místní skupiny Administrators.

Objekty LGPO na nejvyšší úrovni

S výjimkou řadičů domény mají všechny počítače vybavené Windows 2000 a novějšími editovatelný objekt LGPO. Nejrychlejší cestou, jak se k tomuto objektu na místním počítači dostat, je následující příkaz na příkazovém řádku:

```
gpedit.msc /gpcomputer: "%ComputerName%"
```

Tento příkaz spustí konzolu Správa zásad skupiny v prostředí Microsoft Management Console (MMC), s nastaveným místním počítačem jako cílovým. V příkazu se vyskytuje %ComputerName%, což je proměnná prostředí obsahující jméno místního počítače. Musí být obalena dvojitými uvozovkami, jak je z příkladu patrné. Objekt LGPO nejvyšší úrovně na vzdáleném počítači můžete editovat následujícím příkazem vloženým na příkazový řádek:

```
gpedit.msc /gpcomputer: "VzdálenýPočítač"
```

Zde *VzdálenýPočítač* je hostitelské jméno nebo plně kvalifikované doménové jméno (FQDN) vzdáleného počítače. I v tomto případě jsou uvozovky vyžadovány, jako v následujícím příkladě:

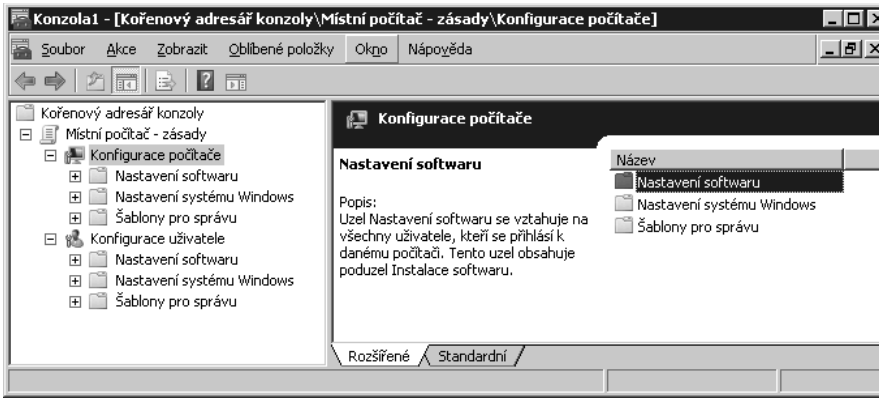
```
gpedit.msc /gpcomputer: "OrgSrv01"
```

Přístup k objektu LGPO nejvyšší úrovně na počítači můžete získat také následujícím postupem:

1. Klepněte na Start, napište do okna pro hledání **mmc** a stiskněte Enter.
2. V konzole Microsoft Management Console klepněte na Soubor (File) a dále na Přidat nebo odebrat modul snap-in (Add/Remove Snap-In).
3. V dialogu Přidat nebo odebrat moduly snap-in (Add Or Remove Snap-Ins) klepněte na Editor objektů zásad skupiny (Group Policy Object Editor) a pak klepněte na Přidat (Add).
4. V dialogu Vyberte objekt zásad skupiny (Select Group Policy Object) klepněte na Dokončit – výchozím objektem je místní počítač.

Nyní můžete ovládat nastavení místních zásad skupiny prostřednictvím nabízených voleb. Protože místní zásady nemají předvolby zásad, neuvidíte v sekcích Computer Configuration (Konfigurace počítač) ani User Configuration (Konfigurace uživatele) zvláštní uzly Zásady (Policies) a Předvolby (Preferences) – viz obrázek 3.3.

Tip: V konzole MMC je možné mít otevřeno více objektů LGPO. V dialogu Přidat nebo odebrat moduly snap-in (Add Or Remove Snap-Ins) jednoduše přidejte jednu instanci Editoru místních zásad skupiny (Local Group Policy Object Editor) pro každý objekt, se kterým chcete pracovat.



Obrázek 3.3: Nastavení místních zásad skupiny

Protože objekty LGPO obsahují jen nastavení zásad, nemůžete v rámci místních zásad konfigurovat předvolby zásad. Nastavení zásad, která jsou k dispozici lokálně, závisí na tom, zda je počítač členem domény nebo pracovní skupiny, a obsahují následující položky:

- Zásady účtů pro hesla, uzamčení účtů a modul Kerberos
- Místní zásady auditu, přiřazení uživatelských práv a možností zabezpečení
- Volby pro záznam událostí, včetně konfigurace velikosti protokolu, přístupu k němu a jeho úschovy, a to vše pro protokoly aplikací, systému i zabezpečení
- Nastavení bezpečnostních omezení pro skupiny, systémové služby, klíče registru a souborový systém
- Možnosti zabezpečení pro bezdrátové sítě, veřejné klíče a zabezpečení protokolu IP (IPSec)
- Vymezení aplikací, jejichž spouštění není v počítači povoleno

Standardní objekty LGPO jsou na počítačích Windows Vista a Windows 2008 Server uloženy ve složce %SystemRoot%\System32\GroupPolicy. Zde najdete následující podsložky:

- **Machine** – uchovává ve složce Script počítačové skripty a v souboru Registry.pol informace o zásadách založených na části registru HKEY_LOCAL_MACHINE (HKLM).
- **User** – obsahuje uživatelské skripty ve složce Script a informace o zásadách založených na registru pro HKEY_CURRENT_USER (HKCU) v souboru Registry.pol.

Tyto složky a soubory byste neměli přímo editovat, ale místo toho byste měli použít odpovídající funkce v nástrojích pro správu zásad skupiny. V Editoru správy zásad skupiny (Group Policy Object Editor) můžete konfigurovat místní zásady skupiny, stejně jako doménové zásady skupiny. Zásadu aplikujete jejím povolením a konfigurací pří-

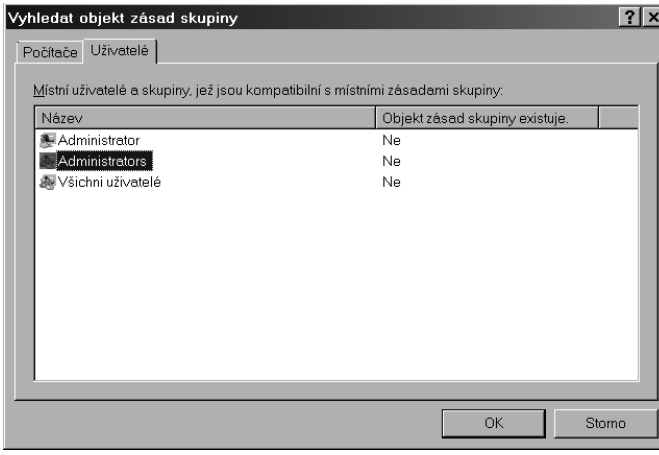
padných dalších voleb dle potřeby. Povolená zásada je zapnuté a aktivní nastavení. Když nechcete, aby se zásada aplikovala, musíte ji zakázat. Zakázaná zásada je vypnuté a neaktivní nastavení. Vynucení nebo blokování dědičnosti může toto chování změnit, jak je popsáno v sekci „Dědičnost zásad skupiny" v kapitole 7.

Tip: Standardně jsou soubory a složky se zásadami skryté. Když chcete v Průzkumníku Windows (Windows Explorer) skryté soubory vidět, zvolte v nabídce Nástroje (Tools) položku Možnosti složky (Folder Options), klepněte na panel Zobrazení (View), vyberte Zobrazovat skryté soubory a složky (Show Hidden Files And Folders) a zrušte Skrýt chráněné soubory operačního systému (doporučeno) (Hide Protected Operating System Files (Recommended)), klepněte na Ano (Yes) v okně s upozorněním a pak klepněte na OK.

Ostatní objekty LGPO

Standardně existuje na počítači jediný místní objekt zásad skupiny. Je však možné vytvořit a upravovat další objekty podle potřeby. Vytvořit nebo získat přístup k administrátorskému nebo neadministrátorskému místnímu objektu zásad skupiny můžete s pomocí následujícího postupu:

1. Klepněte na Start, v okně pro hledání zapište **mmc** a stiskněte Enter. V konzole Microsoft Management Console klepněte na Soubor (File) a dále na Přidat nebo odebrat modul snap-in (Add/Remove Snap-In).
2. V dialogu Přidat nebo odebrat moduly snap-in (Add Or Remove Snap-Ins) klepněte na Editor objektů zásad skupiny (Group Policy Object Editor) a pak klepněte na Přidat (Add).
3. V dialogu Vyberte objekt zásad skupiny (Select Group Policy Object) klepněte na Procházet (Browse). Objeví se dialog Vyhledat objekt zásad skupiny (Browse For A Group Policy Object), klepněte na panel Uživatelé (Users).
4. Na panelu Uživatelé (Users), který ukazuje obrázek 3.4, jsou položky ve sloupci Objekt zásad skupiny existuje (Group Policy Exists). Říkají, zda byl vytvořen odpovídající místní objekt zásad skupiny. Můžete provést některou z těchto akcí:
   - Zvolte Administrators a vytvořte nebo získejte přístup k administrátorskému místnímu objektu zásad skupiny.
   - Zvolte Všichni uživatelé (Non-Administrators) a vytvořte nebo získejte přístup k neadministrátorskému místnímu objektu zásad skupiny.
   - Vyberte některého místního uživatele, jehož specifický místní objekt zásad skupiny chcete vytvořit nebo k němu získat přístup.
5. Klepněte na OK. Jestliže zvolený objekt ještě neexistuje, bude pro vás vytvořen. V opačném případě bude otevřen již existující objekt pro prohlížení a editaci.



Obrázek 3.4: Zvolte typ místního objektu zásad skupiny, který chcete vytvořit nebo s kterým chcete pracovat

Nastavení zásad pro administrátory, neadministrátory a jednotlivé uživatele je uloženo na počítači s Windows Vista nebo Windows 2008 Serveru ve složce %SystemRoot%\System32\GroupPolicyUsers. Protože tyto objekty LGPO se aplikují na nastavení konfigurace uživatele, uživatelská nastavení ve složce %SystemRoot%\System32\GroupPolicyUsers obsahují jen podsložku User, a tato podsložka obsahuje uživatelské skripty ve složce Script a informace o zásadách založených na části registru HKEY_CURRENT_USER (HKCU) v souboru Registry.pol.

Správa doménových zásad skupiny

Doménové zásady skupiny jsou k dispozici, pokud je nainstalovaná služba AD DS (Active Directory Domain Services). Od té chvíle každá lokalita, doména a organizační jednotka může mít své vlastní zásady skupiny. Zásady uvedené v seznamu pro daný kontejner výše mají vyšší přednost než zásady nacházející se v seznamu na nižší pozici. S tímto na paměti můžete zajistit, že zásady skupiny jsou adekvátně uplatněny na odpovídající lokality, domény a organizační jednotky.

Práce s objekty GPO v lokalitách, doménách a organizačních jednotkách

Když začínáte pracovat s doménovými zásadami skupiny, zjistíte, že každá doména ve vaší organizaci má dva výchozí objekty GPO: Default Domain Controllers Policy GPO a Default Domain Policy GPO. Oba tyto výchozí objekty jsou nepostradatelné pro správné fungování a zpracování systému zásad skupiny. Standardně má objekt Default Domain Controllers Policy GPO nejvyšší přednost mezi všemi objekty GPO propojenými s orga-

nizační jednotkou Domain Controllers, zatímco objekt Default Domain Policy GPO má nejvyšší přednost mezi všemi objekty GPO propojenými s celou doménou.

Zásady skupiny pro lokality, domény a organizační jednotky jsou uloženy na doménovém řadiči ve složce %SystemRoot%\Sysvol\Domain\Policies. Pro každou zásadu definovanou na řadiči domény zde najdete její podsložku. Jméno odpovídající podsložky je globální jednoznačný identifikátor (GUID) této zásady. Jedinečný identifikátor GUID pro danou zásadu skupiny najdete na stránce Vlastnosti (Properties), v panelu Obecné (General), v rámečku Souhrn (Summary). V každé z těchto složek pro zásady skupiny jsou pak další podsložky:

- **Machine** – uchovává ve složce Script počítačové skripty a v souboru Registry.pol informace o zásadách založených na části registru HKEY_LOCAL_MACHINE (HKLM).
- **User** – obsahuje uživatelské skripty ve složce Script a informace o zásadách založených na větvi registru HKEY_CURRENT_USER (HKCU) v souboru Registry.pol.

Stejně jako v případě místních zásad skupiny, ani tyto složky a soubory neupravujte přímo. Místo toho použijte odpovídající funkce některého z nástrojů pro správu zásad skupiny. Nejlepším nástrojem pro správu doménových zásad skupiny je konzola Správa zásad skupiny (Group Policy Management Console, GPMC). S konzolou GPMC můžete ovládat všechny aspekty zásad skupiny, pokud máte příslušná administrátorská oprávnění. Účet, který k tomu používáte, musí být členem jedné ze skupin Enterprise Admins nebo Domain Admins, nebo musí mít delegovaná oprávnění pro práci s jistými rysy zásad skupiny.

Členové skupiny Enterprise Admins mohou měnit nastavení zásad pro doménovou strukturu, jejíž jsou součástí. Pokud je například uživatel VáclavS členem skupiny Enterprise Admins v doménové struktuře dmn.cz, může řídit nastavení zásad skupiny pro jakoukoli doménu, jež je potomkem dmn.cz, a samozřejmě také pro samotnou rodičovskou doménu dmn.cz. To znamená, že má přístup k zásadám skupiny pro domény tech.dmn.cz, cs.dmn.cz a dmn.cz.

Členové skupiny Domain Admins mohou dělat správu zásad skupiny pro doménu, v níž se nacházejí. Kdyby byl například uživatel VáclavS členem skupiny Domain Admins v doméně tech.dmn.cz, mohl by ovládat konfiguraci zásad skupiny pro doménu tech.dmn.cz, ale už by tak nemohl činit pro domény cs.dmn.cz ani dmn.cz. V jiných doménách by musel také mít oprávnění člena skupiny Domain Admins, aby mohl ovládat jejich zásady skupiny (nebo člena skupiny Enterprise Admins pro celou doménovou strukturu, jak bylo již zmíněno).

Při delegování administrátorských oprávnění mějte na paměti, že daný účet má jen specifická oprávnění, která delegujete. Mezi aktivity, které se mohou v systému zásad skupiny delegovat, patří:

- Oprávnění spravovat propojení zásad skupiny
- Oprávnění generovat výsledky zásad skupiny pro účely protokolování
- Oprávnění generovat výsledky zásad skupiny pro účely plánování

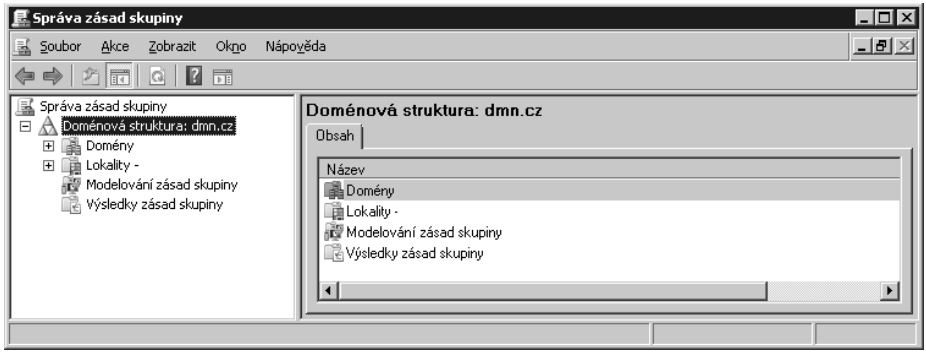
Tato delegovaná oprávnění jsou odlišná od rolí AGPM, které budou popsány v sekci „Delegování oprávnění pro řízení změn" v kapitole 4. Role AGPM umožňují delegovat oprávnění jen v rámci systému pro řízení změn.

Doménové zásady skupiny se ovládají v konzole Správa zásad skupiny (Group Policy Management Console, GPMC). Jakmile ji nainstalujete, můžete ji spouštět z nabídky Nástroje pro správu (Administrative Tools). Klepněte na Start, dále na Všechny programy (All Programs), Nástroje pro správu (Administrative Tools) a nakonec na Group Policy Management.

Jak znázorňuje obrázek 3.5, levý panel konzoly GPMC obsahuje standardně dva uzly nejvyšší úrovně: Správa zásad skupiny (Group Policy Management), který je kořenovým adresářem konzoly, a Doménová struktura (Forest), který reprezentuje doménovou strukturu, k níž jste právě připojeni, pojmenovanou podle kořenové domény této doménové struktury. Když rozbalíte uzel doménové struktury, uvidíte následující poduzly:

- **Domény (Domains)** – poskytuje přístup k nastavení zásad pro domény v doménové struktuře, kterou spravujete. Standardně jste připojeni k vaší přihlašovací doméně, ale můžete přidat připojení k dalším doménám. Když se podíváte dovnitř uzlu domény, uvidíte objekt Default Domain Policy GPO, organizační jednotku Domain Controllers (a odpovídající objekt Default Domain Controllers Policy GPO) a další objekty GPO definované v doméně.
- **Lokality (Sites)** – umožňuje prohlížet a řídit nastavení zásad skupiny pro lokality v odpovídající doménové struktuře. Lokality jsou standardně skryty.
- **Modelování zásad skupiny (Group Policy Modeling)** – dává možnost spouštět Průvodce modelováním zásad skupiny (Group Policy Modeling Wizard), který pomáhá plánovat nasazení zásad skupiny do produkčního prostředí a simulovat nastavení pouze pro testovací účely. K dispozici jsou zde také všechny uložené modely zásad.
- **Výsledky zásad skupiny (Group Policy Results)** – poskytuje přístup k Průvodci výsledky zásad skupiny (Group Policy Results Wizard). Pro každou doménu, k níž jste připojeni, máte z jednoho místa k dispozici všechny odpovídající objekty GPO a organizační jednotky.

Objekty GPO, které naleznete v konzole GPMC jako součásti kontejnerů domény, lokality nebo organizační jednotky, ve skutečnosti nejsou skutečné objekty GPO, ale jejich propojení. Skutečné objekty GPO jsou k nalezení pod uzlem Objekty zásad skupiny (Group Policy Objects) pro vybranou doménu. Je také užitečné vědět, že ikony pro propojení objektů GPO se poznají podle malé šipky v levém dolním rohu, podobně jako je tomu u ikon zástupců.



Obrázek 3.5: Přístup k objektům GPO pro domény, lokality a organizační jednotky

Přístup k dalším doménovým strukturám

Konzola GPMC byla navržena pro práci s více doménovými strukturami, doménami a lokalitami. Když ji poprvé spustíte, jste automaticky připojeni k vaší přihlašovací doméně a doménové struktuře. K dalším doménovým strukturám se připojíte takto:

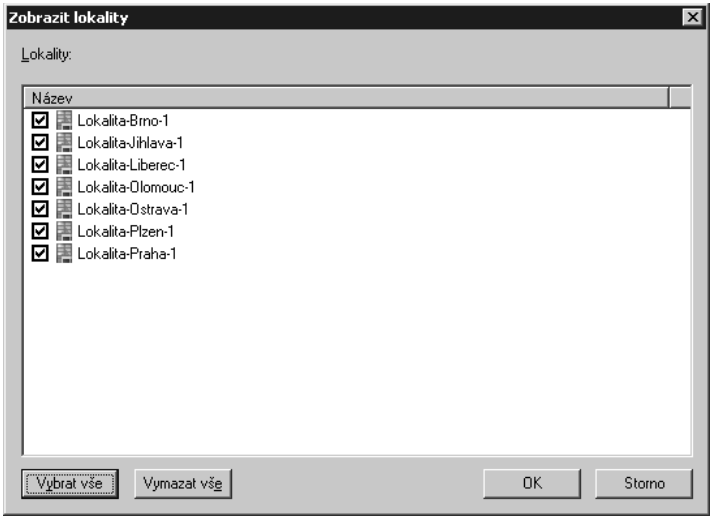
1. Spusťte konzolu Správa zásad skupiny (GPMC) klepnutím na Start, Všechny programy (All Programs), Nástroje pro správu (Administrative Tools) a Group Policy Management. Nebo na příkazovém řádku napište **gpmc.msc**.
2. Klepněte pravým tlačítkem na uzel Správa zásad skupiny (Group Policy Management) ve stromu konzoly a zvolte Přidat doménovou strukturu (Add Forest).
3. V dialogu Přidat doménovou strukturu (Add Forest) zapište název domény v doménové struktuře, ke které se chcete připojit. Nakonec klepněte na OK.

Pokud je nastaven vztah důvěryhodnosti k této doméně, bude připojení realizováno a obdržíte informace o doménové struktuře, i když nemáte nastavenu důvěryhodnost na úrovni celé doménové struktury. Od této chvíle bude při každém dalším spuštění konzoly GPMC uvedena v seznamu i nová doménová struktura.

Zobrazení lokalit v připojených doménových strukturách

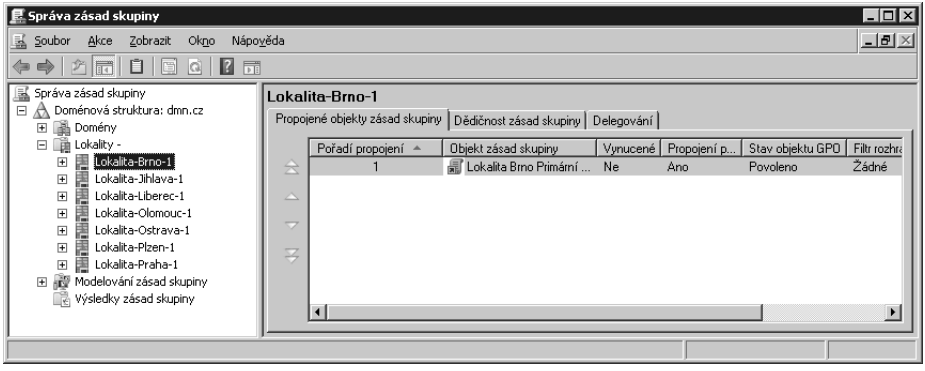
Konzola GPMC standardně neukazuje lokality. Pokud chcete v jisté doménové struktuře pracovat s lokalitami, řiďte se následujícími kroky:

1. Spusťte konzolu Správa zásad skupiny (GPMC) klepnutím na Start, Všechny programy (All Programs), Nástroje pro správu (Administrative Tools) a Group Policy Management. Nebo na příkazovém řádku napište **gpmc.msc**.
2. Rozbalte doménovou strukturu, se kterou chcete pracovat, klepnutím na odpovídající uzel. Klepněte pravým tlačítkem na uzel Lokality (Sites) a pak klepněte na Zobrazit lokality (Show Sites). V dialogu Zobrazit lokality (Show Sites), který ilustruje obrázek 3.6, zaškrtněte lokality, se kterými chcete pracovat, a zrušte volbu u lokalit, se kterými pracovat nechcete. Klepněte na OK.



Obrázek 3.6: Volba lokalit, které chcete vidět v konzole Správa zásad skupiny

Kdykoli od této chvíle nastartujete konzolu Správa zásad skupiny (GPMC), budou zvolené lokality dostupné pod uzlem Lokality (Sites), jak je patrné na obrázku 3.7.



Obrázek 3.7: Přístup k lokalitám v konzole Správa zásad skupiny

Přístup k dalším doménám

V konzole Správa zásad skupiny (GPMC) si můžete procházet domény, ke kterým jste připojeni, seřazené podle doménových struktur. Standardně jste připojeni k vaší přihlašovací doméně a odpovídající doménové struktuře. Když chcete pracovat s dalšími doménami v jisté doménové struktuře, následujte tento postup:

1. Spusťte konzolu Správa zásad skupiny (GPMC) klepnutím na Start, Všechny programy (All Programs), Nástroje pro správu (Administrative Tools) a Group Policy Management. Nebo na příkazovém řádku napište **gpmc.msc**.
2. Expandujte položku pro doménovou strukturu, ve které chcete pracovat, a pak ji rozbalte poklepáním uzel Domény (Domains).
3. Jestliže doména, se kterou chcete pracovat, v seznamu chybí, klepněte pravým tlačítkem na uzel Domény (Domains) v příslušné doménové struktuře a zvolte Zobrazit domény (Show Domains).
4. V dialogu Zobrazit domény (Show Domains) zaškrtněte políčko pro domény, se kterými chcete pracovat, a zrušte volbu u domén, se kterými pracovat nechcete. Pak klepněte na OK.

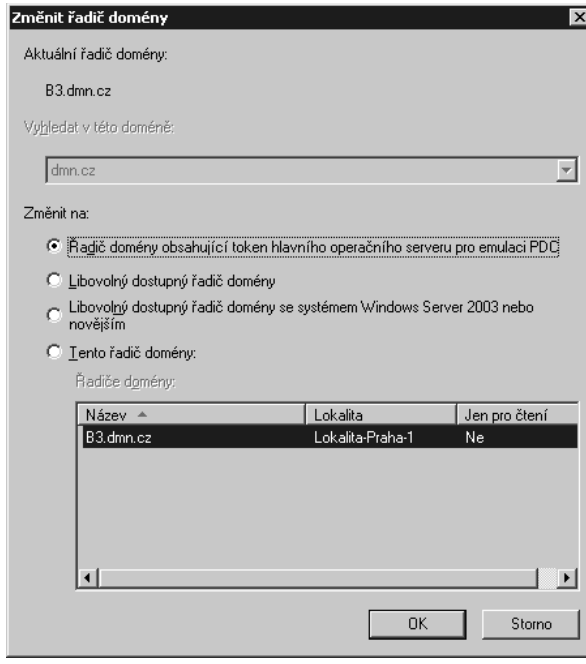
Od této chvíle se po startu konzoly Správa zásad skupiny (GPMC) objeví v seznamu Domény (Domains) právě vámi zvolené domény v dané doménové struktuře.

Změna zaměření doménového řadiče

Kdykoli spustíte konzolu Správa zásad skupiny (GPMC), je provedeno spojení se systémem Active Directory na tom doménovém řadiči, který hraje roli emulátoru PDC pro vaši přihlašovací doménu. Konzola GPMC si od něho vyžádá seznam všech objektů GPO a organizačních jednotek v doméně. Děje se tak prostřednictvím LDAP přístupu do adresářové databáze a protokolem SMB (Server Message Block), s jehož pomocí si konzola čte obsah svazku SYSVOL. Pokud z nějakého důvodu není emulátor PDC dostupný, například když server neběží nebo je odpojen od sítě, konzola GPMC zobrazí výzvu k výběru z těchto možností: pracovat se zásadami skupiny na doménovém řadiči, ke kterému jste právě připojeni, nebo na libovolném doménovém řadiči. Je také možné ručně změnit chování konzoly GPMC a přinutit ji pracovat s jiným řadičem, než je emulátor PDC. Tento krok se nazývá *změna zaměření doménového řadiče*.

Výběr doménového řadiče pro práci v konzole GPMC se děje podle domén:

1. Spusťte konzolu Správa zásad skupiny (GPMC) klepnutím na Start, Všechny programy (All Programs), Nástroje pro správu (Administrative Tools) a Group Policy Management. Nebo na příkazovém řádku napište **gpmc.msc**.
2. Expandujte položku pro doménovou strukturu, ve které chcete pracovat, a pak rozbalte poklepáním uzel Domény (Domains).
3. Klepněte pravým tlačítkem na doménu, pro kterou chcete změnit zaměření doménového řadiče. Vyberte Změnit řadič domény (Change Domain Controller), a otevře se dialog Změnit řadič domény (Change Domain Controller), který vidíte na obrázku 3.8.
4. Doménový řadič, ke kterému jste právě připojeni, je uveden v horní části okna jako Aktuální řadič domény (Current Domain Controller). Máte k dispozici následující možnosti pod Změnit na (Change To) – po jejich výběru vždy klepněte na OK:



Obrázek 3.8: Změna zaměření doménového řadiče

- **Řadič domény obsahující token hlavního operačního serveru pro emulaci PDC (The Domain Controller With The Operations Master Token For The PDC Emulator)** – tuto možnost zvolte, když z nějakého důvodu nejste připojeni k emulátoru PDC a chcete zkusit v tuto chvíli znovu takové spojení zavést. Pokud byl například emulátor PDC odpojen od sítě kvůli údržbě a nyní již je opět připojen, můžete se pokusit o opětovné připojení.
- **Libovolný dostupný řadič domény (Any Available Domain Controller)** – tato volba slouží k připojení k libovolnému řadiči domény. Použijte ji, když nemáte požadavky na verzi operačního systému Windows doménového řadiče, ke kterému se připojujete.
- **Libovolný dostupný řadič domény se systémem Windows 2003 nebo novějším (Any Available Domain Controller Running Windows Server 2003 Or Later)** – pokud potřebujete doménový řadič s operačním systémem Windows 2003 nebo novějším, je to volba pro vás.
- **Tento řadič domény (This Domain Controller)** – zde si můžete vybrat v oblasti Řadiče domény (Domain Controllers) libovolný doménový řadič ze seznamu. U každého řadiče je patrná také lokalita, ve které se nachází, což vám může pomoci vybrat si řadič v požadované lokalitě.

Delegace oprávnění pro správu zásad skupiny

V systému Active Directory získají administrátoři automaticky oprávnění provádět různé úkony správy zásad skupiny. Další jedinci mohou taková oprávnění získat prostřednictvím jejich delegování. Delegace oprávnění pro správu zásad skupiny má v Active Directory vždy určité důvody. Uživatelům, kteří nejsou členy skupin Enterprise Admins ani Domain Admins, lze udělit oprávnění provádět některé nebo všechny z následujících operací:

- Prohlížet nastavení, měnit nastavení, odstraňovat objekty GPO a měnit zabezpečení
- Administrovat propojení existujících objektů GPO nebo generovat výsledky zásad skupiny
- Vytvářet objekty GPO (a tím také spravovat ty objekty GPO, které již vytvořili)

Oprávnění, která jste tímto způsobem delegovali, se odehrávají mimo řízení změn poskytované funkcionalitou AGPM a diskutované v sekci „Používání řízení změn" v kapitole 4. Pokud plánujete AGPM pro řízení změn nasadit, budete nuceni oprávnění delegovaná pro správu zásad skupiny omezit a pečlivě sledovat.

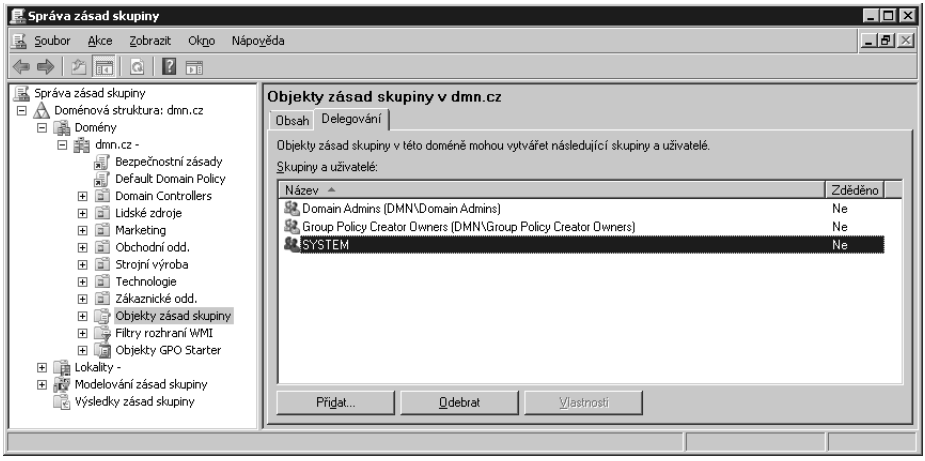
Zjištění a přiřazení práv pro vytváření objektů GPO

V systému Active Directory mají administrátoři možnost vytvářet v doménách objekty GPO. Kdokoli v doméně vytvořil objekt GPO, má oprávnění měnit jeho konfiguraci. Chcete-li zjistit, kdo má v doméně právo vytvářet objekty GPO, sledujte následující kroky:

1. V konzole Správa zásad skupiny (GPMC) expandujte položku pro doménovou strukturu, ve které chcete pracovat, a pak rozbalte uzel Domény (Domains).
2. Expandujte uzel požadované domény. Jestliže tuto doménu nevidíte v seznamu, klepněte pravým tlačítkem na uzel Domény (Domains) a pak klepněte na Zobrazit domény (Show Domains). Nyní si můžete vybrat domény, které se mají zobrazovat.
3. Zvolte uzel Objekty zásad skupiny (Group Policy Objects). Jak demonstruje obrázek 3.9, v panelu Delegování (Delegation) se objeví seznam uživatelů a skupin, které mohou vytvářet objekty GPO.

Uživateli, který není administrátorem, nebo celé skupině (včetně uživatelů a skupin z jiných domén) můžete povolit vytváření objektů GPO (a tak jim implicitně dát i právo měnit objekty GPO, které sami vytvořili). Oprávnění vytvářet objekty GPO udělíte uživateli nebo skupině takto:

1. V konzole Správa zásad skupiny (GPMC) expandujte položku pro doménovou strukturu, ve které chcete pracovat, a pak rozbalte uzel Domény (Domains).
2. Expandujte uzel požadované domény. Jestliže tuto doménu nevidíte v seznamu, klepněte pravým tlačítkem na uzel Domény (Domains) a pak klepněte na Zob-



Obrázek 3.9: Kontrola oprávnění pro vytváření objektů GPO

razit domény (Show Domains). Nyní si můžete vybrat domény, které se mají zobrazovat.

3. Zvolte uzel Objekty zásad skupiny (Group Policy Objects). V pravé části okna zvolte panel Delegování (Delegation). Uvidíte aktuální seznam oprávnění přidělených jednotlivým uživatelům a skupinám pro tvorbu objektů GPO. Klepnutím na Přidat (Add) pokračujete v přidání tohoto práva dalšímu uživateli nebo skupině.
4. Do okna Vyberte objekt typu: uživatel, počítač nebo skupinu (Select User, Computer, Or Group) zapište uživatele nebo skupinu, jíž chcete udělit oprávnění, a klepněte na OK.

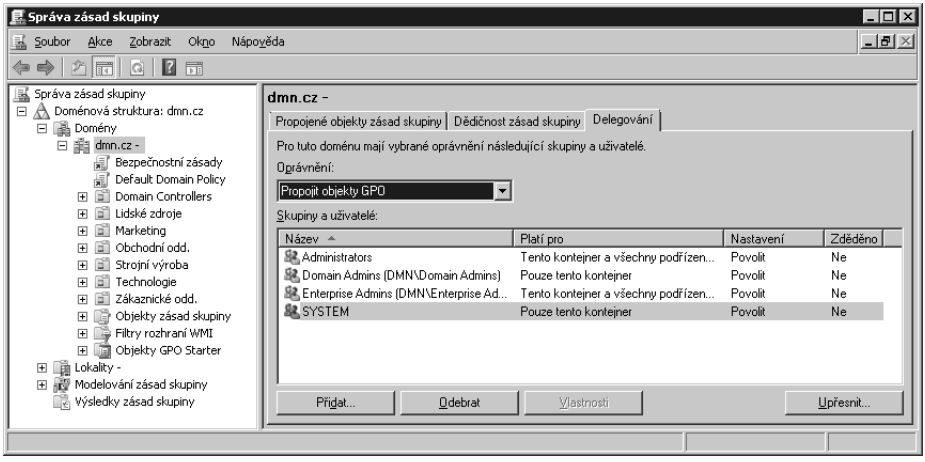
Seznam uživatelů a skupin v panelu Delegování (Delegation) se adekvátně upraví. Budete-li chtít později právo vytvářet objekty GPO vzít zpět, zvolte v panelu Delegování (Delegation) příslušného uživatele nebo skupinu a klepněte na Odebrat (Remove).

Zjištění oprávnění pro správu zásad skupiny

Konzola Správa zásad skupiny (GPMC) poskytuje několik způsobů, jak zjistit přístupová oprávnění pro správu zásad. Informace o oprávněních k systému zásad skupiny pro jistou lokalitu, doménu nebo organizační jednotku získáte takto:

1. V konzole Správa zásad skupiny (GPMC) expandujte položku pro doménovou strukturu, ve které chcete pracovat, a pak rozbalte uzel Domény (Domains) nebo Lokality (Sites) podle potřeby.
2. Když vyberete libovolnou doménu, lokalitu nebo organizační jednotku, na pravé straně okna se aktualizuje několik panelů. Zvolte panel Delegování (Delegation), který ukazuje obrázek 3.10.

3. V seznamu Oprávnění (Permission) zvolte oprávnění, které si chcete ověřit. Uživatelé a skupiny se zvoleným oprávněním jsou pak uvedeni v seznamu Skupiny a uživatelé (Groups And Users). Volby pro typ oprávnění jsou následující:
   - **Propojit objekty GPO (Link GPOs)** – uživatel či skupina mohou zakládat a měnit propojení objektů GPO ve zvolené lokalitě, doméně nebo organizační jednotce.
   - **Provést analýzu vytváření modelů zásad skupiny (Perform Group Policy Modeling Analysis)** – uživatel nebo skupina mají právo zjišťovat výslednou sadu zásad skupiny pro účely plánování.
   - **Číst data výsledků zásad skupiny (Read Group Policy Results Data)** – uživatel či skupina jsou oprávněni zjišťovat aktuální výsledky zásad skupiny tak, jak jsou právě uplatňovány, pro účely ověření a protokolování.



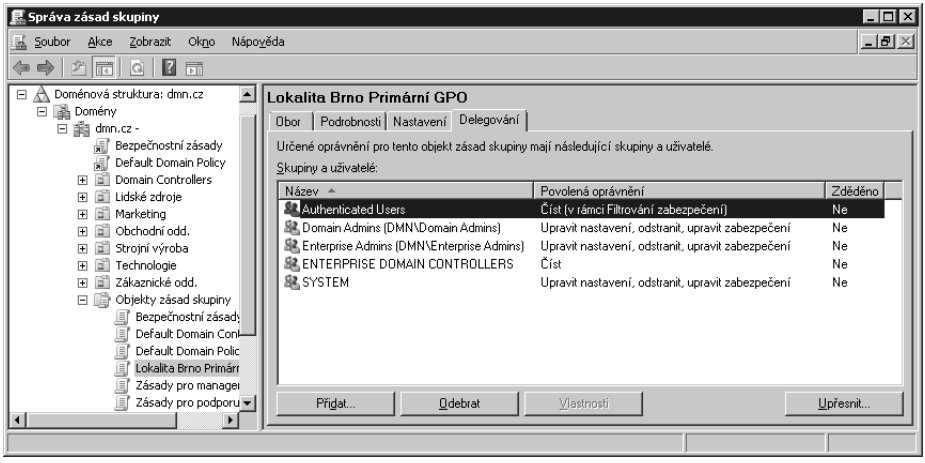
Obrázek 3.10: Kontrola oprávnění pro lokalitu, doménu nebo organizační jednotku

Můžete chtít také stanovit, kteří uživatelé a skupiny mají přístup k jistému objektu GPO a jaká oprávnění jim byla udělena. Učiníte tak tímto postupem:

1. V konzole Správa zásad skupiny (GPMC) expandujte položku pro doménovou strukturu, ve které chcete pracovat, a pak rozbalte uzel Domény (Domains).
2. Expandujte uzel požadované domény. Jestliže tuto doménu nevidíte v seznamu, klepněte pravým tlačítkem na uzel Domény (Domains) a pak klepněte na Zobrazit domény (Show Domains). Nyní si můžete vybrat domény, které se mají zobrazovat.
3. Rozbalte uzel Objekty zásad skupiny (Group Policy Objects). Když pak označíte objekt GPO, jehož oprávnění chcete ověřit, v pravé části okna dojde k aktualizaci a objeví se několik panelů. Z nich vyberte panel Delegování (Delegation), který

ilustruje obrázek 3.11. Objeví se práva pro jednotlivé uživatele a skupiny. Existují tři obecné typy oprávnění:

- **Číst (Read)** – uživatel nebo skupina si může prohlížet objekt GPO a jeho nastavení.
- **Upravit nastavení (Edit Settings)** – uživatel nebo skupina má povoleno prohlížet si objekt GPO a jeho nastavení a také měnit toto nastavení. Nemá však možnost smazat tento objekt GPO nebo zasahovat do jeho zabezpečení.
- **Upravit nastavení, odstranit, upravit zabezpečení (Edit Settings, Delete, Modify Security)** – uživateli nebo skupině je umožněno prohlížet objekt GPO a jeho nastavení, měnit tato nastavení, odstranit objekt GPO nebo upravit jeho zabezpečení.



Obrázek 3.11: Kontrola oprávnění pro konkrétní objekt GPO

Když na panelu Delegování (Delegation) vyberete skupinu, máte možnost zvolit tlačítko Vlastnosti (Properties). Po jeho stisknutí se objeví okno Vlastnosti (Properties) a v něm se dozvíte další detaily o zvolené skupině. Panely v tomto okně poskytují následující informace:

- **Obecné (General)** – zobrazuje název skupiny, popis a e-mailovou adresu (pokud je použita). Je také vidět typ a rozsah skupiny.
- **Členové (Members)** – podává přehled o uživatelích a skupinách, kteří jsou členy vybrané skupiny. Můžete zde i přidávat a odebírat členy skupiny (za předpokladu, že k tomu máte dostatečná oprávnění v rámci domény).
- **Je členem (Member Of)** – představuje skupiny, jichž je zvolená skupina členem. I zde je možné přidávat a odebírat členství, pokud k tomu máte v doméně příslušná práva.

- **Správce objektu (Managed By)** – podává informaci o uživateli, který byl určen jako správce této skupiny. Po klepnutí na Změnit (Change) můžete přiřadit skupině jiného správce. Existuje-li nějaký správce pro skupinu, je k dispozici tlačítko Vlastnosti (Properties), které vede k informacím o účtu tohoto správce. Tlačítko Vymazat (Clear) slouží k odstranění správce skupiny.

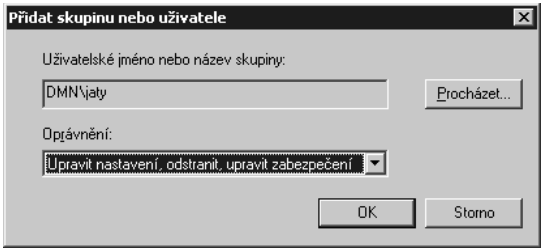
Delegace řídicích funkcí pro práci s objekty GPO

Uživateli, který není administrátorem, nebo celé skupině (včetně uživatelů a skupin z jiných domén) lze umožnit práci s objektem GPO určeným pro doménu, lokalitu či organizační jednotku. Rozsah přidělených oprávnění nabývá následujících možností:

- **Číst (Read)** – uživatel nebo skupina si může prohlížet objekt GPO a jeho nastavení.
- **Upravit nastavení (Edit Settings)** – uživatel nebo skupina má povoleno prohlížet si objekt GPO a jeho nastavení, a také měnit toto nastavení. Nemá však možnost smazat tento objekt GPO nebo zasahovat do jeho zabezpečení.
- **Upravit nastavení, odstranit, upravit zabezpečení (Edit Settings, Delete, Modify Security)** – uživateli nebo skupině je umožněno prohlížet objekt GPO a jeho nastavení, měnit tato nastavení, odstranit objekt GPO nebo upravit jeho zabezpečení.

Příslušná oprávnění pro uživatele nebo skupinu udělíte takto:

1. V konzole Správa zásad skupiny (GPMC) expandujte položku pro doménovou strukturu, ve které chcete pracovat, a pak rozbalte uzel Domény (Domains).
2. Expandujte uzel požadované domény. Jestliže tuto doménu nevidíte v seznamu, klepněte pravým tlačítkem na uzel Domény (Domains) a pak klepněte na Zobrazit domény (Show Domains). Nyní si můžete vybrat domény, které se mají zobrazovat.
3. Rozbalte uzel Objekty zásad skupiny (Group Policy Objects) a pak zvolte v levé části okna objekt GPO, se kterým chcete pracovat. V pravé části okna klepněte na panel Delegování (Delegation).
4. Objeví se aktuální seznam oprávnění pro jednotlivé uživatele a skupiny. Pro udělení oprávnění dalšímu uživateli nebo skupině klepněte na Přidat (Add).
5. Do okna Vyberte objekt typu: uživatel, počítač nebo skupinu (Select User, Computer, Or Group) zapište uživatele nebo skupinu, jíž chcete udělit oprávnění, a klepněte na OK.
6. V dialogu Přidat skupinu nebo uživatele (Add Group Or User), který si můžete prohlédnout na obrázku 3.12, zvolte udělená oprávnění, a to: Číst (Read); Upravit nastavení (Edit Settings); nebo Upravit nastavení, odstranit, upravit zabezpečení (Edit Settings, Delete, Modify Security). Klepněte na OK.



Obrázek 3.12: Udělení oprávnění uživateli nebo skupině

Seznam uživatelů a skupin v panelu Delegování (Delegation) je nyní upraven adekvátně nově uděleným oprávněním. Pokud budete někdy v budoucnosti potřebovat oprávnění vzít zpět, běžte na panel Delegování (Delegation), zvýrazněte uživatele nebo skupinu a klepněte na Odebrat (Remove).

Poznámka: Nejlepší způsob, jak delegovat oprávnění, představují tlačítka Přidat (Add) a Odebrat (Remove) na panelu Delegování (Delegation). Přesto je možné klepnout také na tlačítko Upřesnit (Advanced) a budete moci prohlížet a měnit přímo jemná nastavení zabezpečení objektu. Po klepnutí na tlačítko Upřesnit (Advanced) se zobrazí dialog Nastavení zabezpečení (Security Settings) pro daný objekt GPO. V tomto dialogu je možné volit uživatele nebo skupiny, kteří již mají udělena oprávnění, a tato oprávnění si prohlížet nebo měnit. Také přidávání a odebírání oprávnění uživatelům a skupinám lze provádět přímo v tomto okně.

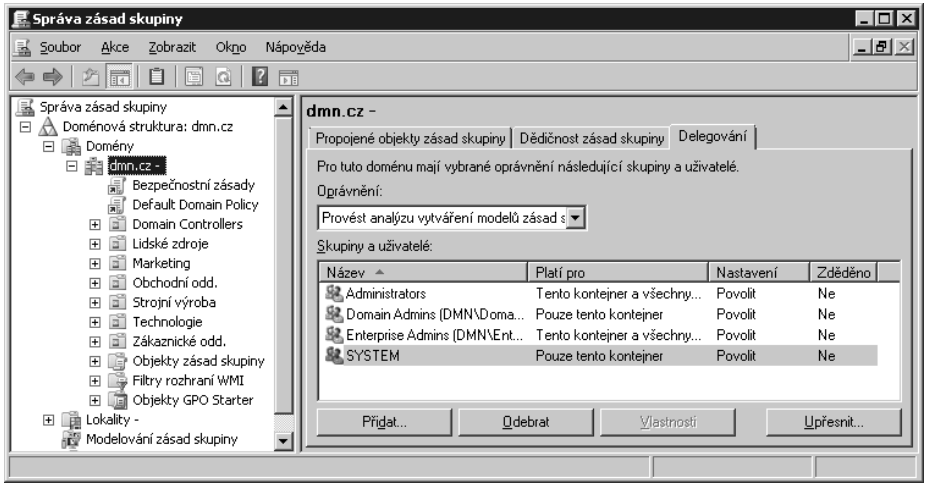
Delegace autority pro správu propojení a výsledků zásad skupiny

Uživateli, který není administrátorem, nebo celé skupině (včetně uživatelů a skupin z jiných domén) máte možnost povolit správu propojení objektů GPO a výsledků zásad skupiny. Odpovídající oprávnění lze udělit v libovolné kombinaci a definují se takto:

- **Propojit objekty GPO (Link GPOs)** – uživatel či skupina mohou zakládat a měnit propojení objektů GPO ve zvolené lokalitě, doméně nebo organizační jednotce.
- **Provést analýzu vytváření modelů zásad skupiny (Perform Group Policy Modeling Analysis)** – uživatel nebo skupina mají právo zjišťovat výslednou sadu zásad skupiny pro účely plánování.
- **Číst data výsledků zásad skupiny (Read Group Policy Results Data)** – uživatel či skupina jsou oprávněni zjišťovat aktuální výsledky zásad skupiny tak, jak jsou právě uplatňovány, pro účely ověření a protokolování.

Tato oprávnění udělíte uživateli nebo skupině, když se budete držet následujících kroků:

1. V konzole Správa zásad skupiny (GPMC) expandujte položku pro doménovou strukturu, ve které chcete pracovat, a pak rozbalte uzel Domény (Domains) nebo Lokality (Sites) podle potřeby.
2. Když vyberete libovolnou doménu, lokalitu nebo organizační jednotku, na pravé straně okna se aktualizuje několik panelů. Zvolte panel Delegování (Delegation).
3. V seznamu Oprávnění (Permission) vyberte druh oprávnění, který chcete udělit (viz obrázek 3.13). Možnosti jsou: Propojit objekty GPO (Link GPOs), Provést analýzu vytváření modelů zásad skupiny (Perform Group Policy Modeling Analysis) nebo Číst data výsledků zásad skupiny (Read Group Policy Results Data).
4. Objeví se aktuální stav oprávnění pro jednotlivé uživatele a skupiny. Pro přidělení zvoleného typu oprávnění klepněte na Přidat (Add).
5. Do okna Vyberte objekt typu: uživatel, počítač nebo skupinu (Select User, Computer, Or Group) zapište uživatele nebo skupinu, jíž chcete udělit oprávnění, a klepněte na OK.
6. V dialogu Přidat skupinu nebo uživatele (Add Group Or User), který ilustruje obrázek 3.14, specifikujte, jak by se měla oprávnění uplatnit. Volba Tento kontejner a všechny podřízené kontejnery (This Container And All Child Containers) znamená, že oprávnění se udělí pro všechny kontejnery (objekty v hierarchii Active Directory) podřízené aktuálnímu kontejneru (a v něm pochopitelně také). Volbou Pouze tento kontejner (This Container Only) způsobíte aplikaci oprávnění jen na aktuální kontejner. Klepněte na OK.



Obrázek 3.13: Volba oprávnění, jež budou prohlížena nebo udělena