Windows Server 2008

Group Policy

Kapesní rádce administrátora

Zásady skupiny ve Windows

William R. Stanek

- Aplikace a propojování objektů GPO
- Správa, nastavení a předvolby zásad skupiny
- Údržba a migrace složky SYSVOL
- Prohledávání a filtrování zásad skupiny
- Instalace doplňkových rozšíření a nástrojů

CPRESS

Microsoft

William R. Stanek

Group Policy
Zásady skupiny ve Windows
Kapesní rádce administrátora

Computer Press, a. s.
Brno
2010

Group Policy
Zásady skupiny ve Windows
Kapesní rádce administrátora

William R. Stanek

Computer Press, a.s., 2010. Vydání první.

Překlad: Josef Pojsl
Odborná korektura: Jiří Brejcha
Jazyková korektura: Petra Láníčková
Vnitřní úprava: Petr Klíma
Sazba: Petr Klíma
Rejstřík: Daniel Štreit
Obálka: Martin Sodomka

Komentář na zadní straně obálky: Libor Pácl
Technická spolupráce: Jiří Matoušek, Zuzana Šindlerová, Dagmar Hajdajová
Odpovědný redaktor: Libor Pácl
Technický redaktor: Jiří Matoušek
Produkce: Petr Baláš

Computer Press, a.s.,
Holandská 8, 639 00 Brno

Objednávky knih:
http://knihy.cpress.cz
distribuce@cpress.cz
tel.: 800 555 513

ISBN 978-80-251-2920-3
Prodejní kód: K1719
Vydalo nakladatelství Computer Press, a.s., jako svou 3460. publikaci.

Obsah

Obsah

Kapitola 4

Pokročilá správa zásad skupiny 123

Kapitola 5

Prohledávání a filtrování zásad skupiny 167

ČÁST III

Údržba a zotavení zásad skupiny

Kapitola 6

Kapitola 7

O autorovi

William R. Stanek se narodil v Burlingtonu v americkém státě Wisconsin, kde navštěvoval státní školy, mezi nimi i Janes Elementary School v Racine ve Wisconsinu. Je druhým nejmladším z pěti sourozenců. Po ukončení zaměstnání v armádě přesídlil do státu Washington, kde byl uchvácen drsnou krásou severozápadního pobřeží Pacifiku.

V roce 1985 narukoval do U. S. Air Force a vstoupil do programu dvouletého výcviku výzvědné služby a lingvistiky na Defense Language Institute. Po absolvování kurzu sloužil v poli v několika operacích v Asii a Evropě. V roce 1990 byl přijat na Air Combat School a krátce po absolvování se zúčastnil první války v Zálivu jako člen letecké bojové jednotky zaměřené na elektroniku. Během svých dvou výprav do války v Zálivu se William zúčastnil několika bojových a podpůrných leteckých akcí a zaznamenal přes 200 letových hodin v boji. Za vynikající nasazení ve válce získal devět válečných vyznamenání, včetně nejvyššího leteckého vyznamenání Spojených států amerických, kříže Air Force Distinguished Flying Cross, dále medaile Air Medal, Air Force Commendation Medal a Humanitarian Service Medal. Celkem byl za svou vojenskou kariéru 29krát dekorován.

V roce 1994 získal William titul bakaláře magna cum laude na Hawaii Pacific University. V roce 1995 pak získal na téže univerzitě magisterský titul s vyznamenáním. V roce 1996 odešel po jedenácti letech strávených v letectví z armády. Při práci v armádě pobýval v Texasu, Japonsku, Německu a na Havaji. Sloužil při podpoře operací Pouštní bouře (Desert Storm), Pouštní štít (Desert Shield) a operace Provide Comfort. Jeho poslední zastávkou u Air Force byla 324. výzvědná skvadrona na letecké základně Wheeler Army na Havaji.

V jeho rodině bylo vždy plno čtenářů a William vždy rád četl a vyprávěl příběhy. Ještě před začátkem školní docházky četl klasickou literaturu jako *Ostrov pokladů, Švýcarský Robinson, Robinson Crusoe* a *Tři mušketýři*. Později v dětství začal číst díla autorů jako Jules Verne, Sir Arthur Conan Doyle, Edgar Rice Boroughs, Ray Bradbury, Herman Melvile, Jack London, Charles Dickens a Edgar Allan Poe. O něm říká: „Edgar Allan Poe může být pěkně ponurý a temný, zvláště když máte 10 let. Ale já si vzpomínám, jak jsem byl jeho příběhy fascinován. Dodnes si pamatuji části jeho Krkavce, Zrádného srdce a Vražd v ulici Morgue."

William dokončil svůj první román v roce 1986 při pobytu v Japonsku, ale trvalo to skoro dalších deset let, než bylo jeho první dílo publikováno. Od té doby napsal a vydal téměř 100 knih, mezi nimi *Active Directory Kapesní rádce administrátora (Computer Press, 2009)*, *Microsoft Windows Server 2008 Kapesní rádce administrátora (Computer Press, 2008) a Mistrovství v Microsoft Windows Server 2008 (Computer Press, 2009)*.

V roce 1997 v článku o jeho dosavadním životě *Olympan* (The (Wash.) Olympian) Williama nazvali „Tváří za minulostí" („A Face Behind the Future"). V té době tvořil nové základy budoucnosti obchodování na Internetu. Dodnes William pokračuje ve formování budoucnosti internetového obchodování a technologií obecně a píše zásadní knihy o těchto tématech pro mnoho nakladatelů. William získal od svých kolegů v oboru knižního vydavatelství mnoho ocenění.

Ve svém volném čase tráví hodně času jízdou na horském kole a turistikou, avšak v současnosti jsou jeho dobrodružství v přírodě většinou omezena na krátké výlety po severozápadním tichomořském pobřeží USA. V roce 2009 vydá Microsoft stou Williamovu knihu. Williamův celoživotní příspěvek tištěnému slovu je takového rozsahu, že se stal jedním z vedoucích technologických autorů v dnešním světě.

Poděkování

Když se mě lidé ptají, kolik knih jsem už vlastně napsal, vím jen, že už píšu hodně dlouho, ale počet napsaných knih opravdu neznám. Dlouhá léta jsem měl ve svém životopise údaj, že jsem autorem více než 25 knih. Několikrát mě mí nakladatelé nabádali, abych v životopise uváděl přesnější číslo, takže někde kolem 61. knihy jsem začal počítat, abych je uspokojil. To bylo před pěti, šesti nebo sedmi lety, takže nyní se blížím počtu 100 nebo tak nějak.

Pro mě bylo vždy důležitější umění psát. Píšu rád, a ze všeho nejraději mám projekty, které jsou něčím podnětné. Podnětem pro psaní správcovy příručky k zásadám skupiny pro každý den bylo to, že jsem toho chtěl zahrnout tolik, že by to přesáhlo rámec kapesního rádce, který má být referenční příručkou obsahující vše potřebné. Kapesní rádce má mít příruční formát a musí být snadno čitelný, čili ten typ knihy, který vám pomůže vyřešit problém a udělat vaši práci, ať už jste kdekoli. Proto jsem musel mít neustále na mysli, že je nutné se soustředit na jádro správy zásad skupiny. Výsledkem je kniha, kterou držíte v ruce a která, jak doufám, je jednou z nejpraktičtějších příručních knih o zásadách skupiny.

V každém příručním rádci, který jsem napsal, a je jich přes tři tucty, jsem musel zmínit, že tým Microsoft Press je bezvadný. Maria Gargiulio byla nápomocna při psaní, pomáhala mi získat vše potřebné k napsání knihy a byla mým hlavním kontaktem u Microsoftu. Martin DelRe jako odpovědný redaktor věřil této knize od samého počátku a spolupráce s ním byla skvělá. Zhotovení a publikace celého textu by bez obou nebyly nikdy možné.

Naneštěstí pro autora (a naštěstí pro čtenáře), psaní je jen jednou z mnoha činností při publikaci nové knihy. Po něm přichází tisková příprava a přezkoumání textu. Musím uznat, že Microsoft Press má nejdůkladnější proces redakční a technické přípravy, jaký jsem viděl – a to jsem napsal mnoho knih pro mnoho různých nakladatelství. Řízením redakčních úprav byl pověřen John Pierce, a zejména jemu velmi děkuji, že mi pomohl zůstat u tématu a dodržet termín.

Technickým redaktorem knihy byl Mitch Tulloch, se kterým jsem vždy rád pracoval a který provedl solidní posouzení technického obsahu. Za pomoc v průběhu celého projektu chci poděkovat také Chrisi Nelsonovi, s nímž je fantastické pracovat, protože je vždy ochoten pomoci ze všech svých sil. Děkuji všem ostatním v Microsoft Press, kteří mi pomohli v celé mé spisovatelské kariéře a byli na svém místě, když jsem je nejvíce potřeboval.

Děkuji také Studiu B, Salkind Agency a mému agentovi, Neilu Salkindovi.

Snad jsem na nikoho nezapomněl, ale pokud ano, nebyl to záměr. *Na mou čest.*

Úvod

Tato kniha je jedinou na trhu, která byla od začátku do konce napsána s ohledem na předvolby i nastavení zásad skupiny. Stejně tak se jedná o jedinou knihu na trhu, která bere v úvahu konzolu Správa zásad skupiny i Pokročilou správu zásad skupiny. Díky tomu poskytuje tato kniha správcům jedinečný přístup. Výsledkem je, jak doufám, výstižný a poutavý zdroj informací pro správce Windows.

Protože cílem knihy je nabídnout co největší hodnotu v kapesním formátu, nemusíte se prodírat stovkami stran nadbytečných informací, než najdete to, co hledáte. Naopak, kniha obsahuje přesně to, co potřebujete, abyste udělali svou práci. Krátce, text je koncipován tak, aby byl hlavním zdrojem informací o správě zásad skupiny. Proto se kniha zaměřuje na denní administrativní úkony, často opakovaná zadání, komentované příklady a volby, které jsou názorné, ale ne nutně všeobecné.

Jedním z cílů bylo udržet obsah tak hutný, aby kniha zůstala kompaktní a dalo se v ní snadno orientovat, při zachování co nejvíce tak cenných informací. Takže místo objemného tisícistránkového svazku nebo lehoučké stostránkové referenční příručky dostáváte do ruky hodnotnou příručku, která pomůže rychle a snadno splnit běžné úkoly, vyřešit problémy a uplatnit funkce, jako je filtrování zásad skupiny, migrace svazku SYSVOL, implementace řízení změn, obnova objektů zásad skupiny (Group Policy Objects, GPO) a odstraňování problémů.

Komu je kniha určena

Tato publikace pokrývá správu zásad skupiny pro malé, střední a velké organizace. Kniha je zamýšlena pro:

- Současné správce Windows a sítí
- Zaměstnance technické podpory, kteří mají na starosti sítě Windows
- Zkušené uživatele s odpovědností správce
- Správce, kteří přecházejí z jiné platformy

Abychom do textu zabalili co nejvíce informací, předpokládáme, že čtenář má základní znalosti o sítích a orientuje se jak ve Windows, tak v Active Directory. Proto nevěnujeme celé kapitoly architektuře Windows, sítím Windows nebo Active Directory. Naproti tomu poskytujeme kompletní detaily všeho, co se týká zásad skupiny a čeho všeho s nimi lze docílit. Prozkoumáváme spletitosti zásad skupiny, popisujeme, jak držet krok se změnami v zásadách skupiny, jak instalovat rozšíření zásad skupiny, jak se zásady skupiny aplikují, a mnoho dalších informací.

Předpokládáme také, že čtenář je obeznámen s příkazy a procedurami ve Windows i v Active Directory. Pokud potřebujete vhled do základů Active Directory, dobrým zdrojem je *Active Directory Kapesní rádce administrátora* (Active Directory Administrator's Pocket Consultant, Microsoft Press, 2009).

Uspořádání knihy

Kniha byla navržena tak, aby ji bylo možné požívat při běžné dennodenní správě zásad skupiny, proto je uspořádána podle úkonů spíše než podle vlastností. Rychlost a snadnost vyřešení problémů jsou pro tento druh příručky neodmyslitelné. Kniha má podrobný obsah a rozsáhlý rejstřík určený pro rychlé vyhledávání odpovědí. Kromě toho jsou tu další pomůcky pro rychlé řešení situací, jako instrukce krok za krokem, seznamy, tabulky s přehlednými hlavními fakty a mnoho křížových odkazů. Kniha má několik částí a kapitol.

Zásady skupiny jsou sadou předvoleb a nastavení, aplikovatelných na konfigurace uživatelů a počítačů. Část I, „Implementace zásad skupiny", reviduje zásadní úkoly potřebné pro správu zásad skupiny. Kapitola 1 poskytuje přehled nástrojů, technik a konceptů svázaných se zásadami skupiny. Kapitola 2 zkoumá podstatné změny v zásadách skupiny a to, jak tyto změny ovlivňují způsob používání zásad skupiny. Tato kapitola se navíc zabývá podrobným přehledem používání předvoleb i nastavení zásad, včetně tipů, jakou z těchto technologií kdy použít.

Část II, „Ovládání zásad skupiny", hovoří o základních nástrojích a technikách, které se při řízení zásad skupiny používají. Kapitola 3 zkoumá konfiguraci lokálních objektů zásad skupiny (LGPO) a objektů zásad skupiny založených na Active Directory. Čtenář zjistí, jaké zásadní věci brát v úvahu při implementaci, nalezne tipy a techniky pro práci napříč doménami, lokalitami a doménovými strukturami. V kapitole 4 se diskutují funkce dostupné pro řízení změn při nasazení pokročilé správy zásad skupiny (Advanced Group Policy Management, AGPM). Dozvíte se, jak pracovat s časovou ?posloupností? v rámci systému řízení změn a konfigurovat samotné AGPM. Kapitola 5 se zabývá vyhledáváním a filtrováním zásad skupiny. Postupy zde popsané lze využít nejen k vyhledání nastavení zásad a objektů GPO, ale i ke správě bezpečnostních skupin a počítačů, na které se zásady aplikují.

Kniha pokračuje částí III, „Údržba a obnova zásad skupiny". Objekty GPO mají dvě složky: kontejnery zásad skupiny (Group Policy Container, GPC) uložené v Active Directory, a šablony zásad skupiny (Group Policy Template, GPT) uložené v SYSVOL. Kapitola 6 demonstruje, jak převést SYSVOL na replikovaný distribuovaný souborový systém (Distributed File System, DFS) a jak udržovat ukládání do SYSVOL. Najdete zde také tipy a techniky pro odstraňování problémů s replikací. Kapitola 7 se zabývá základními koncepty zásad skupiny a poskytuje návody a techniky potřebné pro ovládání způsobu, jak zásady skupiny fungují. Kapitola 8 zkoumá údržbu, obnovu a odstraňování problémů se zásadami skupiny. A nakonec příloha A poskytuje doporučení pro instalaci rozšíření a nástrojů zásad skupiny.

Konvence používané v knize

Pro přehlednost a snadnost čtení používáme pestrou kolekci prvků. Najdete zde přesná znění příkazů a jejich výstupů v písmu s konstantní roztečí. Pokud však je úkolem čtenáře, aby příkaz napsal, je zvýrazněn tučně. Při uvedení a definici nového termínu se používá kurziva.

Mezi další konvence patří:

Obvyklá praxe – jedná se o obvyklé postupy a techniky, které se běžně používají při práci s pokročilou konfigurací, a o koncepční záležitosti při administraci.

Upozornění – varování před potenciálními problémy, o kterých byste měli vědět.

Poznámka – rozvádí podrobnosti nějaké záležitosti, na kterou je kladen důraz.

Z praxe – rady ze života při probírání pokročilých témat.

Bezpečnostní výstraha – poukázání na záležitosti dotýkající se bezpečnosti.

Tip – cenné rady nebo dodatečné informace.

Pevně věříme, že v této knize najdete rychle a efektivně vše, co potřebujete při nejdůležitějších úkonech spojených s administrací. Své nápady neváhejte posílat na adresu *williamstanek@aol.com*. Děkujeme.

Další užitečné informace na síti

Jakmile se objeví jakýkoli nový nebo aktualizovaný materiál, který se nějak týká této knihy, bude vystaven na Microsoft Press Online Windows Server a Client Web Site. Můžete se těšit na aktualizace obsahu knihy, články, odkazy na doplňující informace, opravy chyb, vzorové kapitoly a další. Tyto stránky jsou na adrese *http://www.microsoft.com/learning/books/online/serverclient* a pravidelně se aktualizují.

Zpětná vazba

Pro přesnost informací obsažených v této knize jsme udělali všechno. Microsoft Press poskytuje korekce obsahu knih na následující webové adrese:

http://www.microsoft.com/mspress/support

Pokud máte k této knize komentáře, dotazy nebo nápady, posílejte je prosím na Microsoft Press jednou z následujících metod:

Poštovní adresa:

Microsoft Press
Attn: Editor, Windows Group Policy Administrator's Pocket Consultant
One Microsoft Way
Redmond, WA 98052-6399
E-mail: *mspinput@microsoft.com*

Na těchto adresách se však nedovoláte podpory k jednotlivým produktům. Produktová podpora je dostupná na následující webové adrese Microsoftu: *http://support.microsoft.com*.

Poznámka redakce českého vydání

I nakladatelství Computer Press, které pro vás tuto knihu přeložilo, stojí o zpětnou vazbu a bude na vaše podněty a dotazy reagovat. Můžete se obrátit na následující adresy:

Computer Press
redakce počítačové literatury
Holandská 8
639 00 Brno
nebo
knihy@cpress.cz.

Další informace a případné opravy českého vydání knihy najdete na internetové adrese *http://knihy.cpress.cz/K1719*. Prostřednictvím uvedené adresy můžete též naší redakci zaslat komentář nebo dotaz týkající se knihy. Na vaše reakce se srdečně těšíme.

ČÁST I

Implementace zásad skupiny

KAPITOLA 1

Úvod do zásad skupiny

V této kapitole:

Ať už jste zkušenými správci s letitými zkušenostmi se sítěmi Windows nebo nováčky se základním porozuměním problematice, váš dlouhodobý úspěch ve světě neustále se měnících technologií závisí stále více na tom, jak dobře rozumíte zásadám skupiny (Group Policy). *Zásady skupiny* jsou sadou předvoleb a nastavení, které jsou aplikovány na konfigurace uživatelů a počítačů. Zjednodušují administraci běžných a opakovaných úkonů, které se obtížně provádějí ručně, ale mohou být automatizovány (jako je nasazení nového softwaru nebo řízení toho, jaké programy mohou být nainstalovány). Zásady skupiny umožňují vytknout požadované konfigurační předvolby a nastavení do oddělených skupin. Důsledkem je možnost konfigurace pracovní plochy uživatelů podle specifických požadavků organizace a ovládání těchto konfigurací na každém počítači v celé síti.

Předvolby a nastavení zásad skupiny

Zásady skupiny si lze představovat také tak, že se jedná o sadu pravidel aplikovatelnou v prostředí celého podniku. Přestože zásady skupiny lze používat na servery a stanice vybavené Windows 2000 a novějšími, jejich implementace se od první verze ve Windows 2000 změnila. V případě Windows Vista Service Pack 1 a novějších a u Windows Serveru 2008, zásady skupiny obsahují jak ovládaná nastavení, známá jako *nastavení zásad (policy settings)*, tak neovládaná nastavení, kterým se říká *předvolby zásad (policy preferences)*. Když na Windows XP Service Pack 2 (SP2) a novější, Windows Vista nebo Windows Server 2003 Service Pack 1 (SP1) a novější zavedete klientská rozšíření zásad skupiny, můžete začít používat předvolby zásad skupiny i zde.

Nastavení zásad skupiny umožňuje řídit konfiguraci operačního systému a jeho komponent. Slouží také ke konfiguraci počítače, uživatelských skriptů, přesměrování adresářů, bezpečnosti počítače, instalaci softwaru a dalším účelům.

Předvolby zásad skupiny se uplatní při konfiguraci, nasazení a správě nastavení operačního systému a aplikací tam, kde to nebylo možné s pomocí dřívějších verzí zásad skupiny. Patří sem zdroje dat, mapované disky, proměnné prostředí, síťové disky, možnosti složky, zástupci a další. V mnoha případech zjistíte, že předvolby zásad skupiny jsou lepší cestou k cíli než konfigurace těchto nastavení v bitových obrazech Windows nebo s pomocí přihlašovacích skriptů.

Klíčovým rozdílem mezi předvolbami a nastaveními zásad je vynutitelnost. Zásady skupiny přísně vynucují nastavení zásad. Ty se používají k ovládání konfigurace operačního systému a jeho komponent. S jejich pomocí je také znemožněno v uživatelském rozhraní měnit nastavení, která jsou v kompetenci zásad skupiny. Většina nastavení zásad je uložena ve větvích registru, které jsou věnovány zásadám. Operační systém a způsobilé aplikace pak kontrolují tyto větve a rozhodují, zda a jak jsou zásadami ovlivněny různé aspekty operačního systému. Systém zásad skupiny aktualizuje nastavení zásad v pravidelném intervalu, který je standardně nastaven na 90 až 120 minut.

Poznámka: Když dojde na aplikace a jejich podporu zásad skupiny, používají se často termíny jako vyhovující nebo pro zásady skupiny způsobilé aplikace. Zásadám skupiny vyhovující nebo způsobilá aplikace je taková aplikace, která byla zvlášť uzpůsobena pro podporu zásad skupiny. To, zda je aplikace způsobilá pro zásady skupiny, je velmi podstatné. Tyto aplikace jsou naprogramovány tak, že nahlížejí do větví registru věnovaných zásadám a kontrolují, zda a jak jsou zásadami určovány jejich funkce a různé vlastnosti operačního systému. Nevyhovující, neuzpůsobené aplikace neobsahují kód, který by dělal tyto kontroly.

Naopak předvolby zásad nejsou systémem zásad skupiny přísně vynucovány. Předvolby nejsou ukládány ve větvích registru příslušných zásadám, ale na stejných místech registru, kam zapisují a odkud čtou svoje nastavení samotné aplikace a operační systém. Díky tomu jsou předvolby zásad použitelné i pro aplikace a funkce operačního systému, které nejsou pro zásady skupin zvlášť uzpůsobené. Zároveň ale není vyloučeno měnit tyto hodnoty z uživatelského rozhraní. Proto mohou uživatelé bez překážky měnit nastavení ovlivněná předvolbami zásad skupiny. A nakonec, ačkoli systém aktualizuje předvolby zásad se stejnou frekvencí jako nastavení zásad, je možné aktualizace předvoleb de facto vyřadit tak, že se použijí jen jednou.

Při práci s nastavením zásad mějte na paměti toto:

- Většina nastavení zásad se ukládá v části registru věnované zásadám.
- Nastavení jsou vynucena.
- Ovlivnění voleb z uživatelského rozhraní může být znemožněno.
- Nastavení se automaticky aktualizují.
- Nastavení zásad vyžadují uzpůsobené aplikace.
- Původní nastavení se nemění.
- Odstranění nastavení zásad obnovuje původní nastavení.

Zapamatujte si také základní parametry předvoleb zásad:

- Předvolby zásad jsou uloženy na stejných místech registru, kam zapisují a odkud je čtou aplikace a operační systém.
- Předvolby nejsou vynuceny.
- Ovlivnění předvoleb z uživatelského rozhraní není zakázáno.
- Předvolby mohou být automaticky aktualizovány nebo aplikovány jen jednou.
- Předvolby fungují i pro aplikace bez speciální podpory pro zásady skupin.
- Původní nastavení jsou přepsána.
- Odstranění předvoleb zásad neobnoví původní nastavení.

Z praxe: Rozhodnutí, zda použít nastavení zásad nebo předvolby zásad, se obvykle řídí podle toho, zda má být položka vynucena. Pokud má být volba nastavena bez vynucení, použijte předvolby zásad a zrušte automatické aktualizování. Při požadavku vynutit specifickou konfiguraci volte nastavení zásad nebo použijte předvolby zásad a povolte automatické aktualizování.

Objekty zásad skupiny (GPO)

Zásady skupiny jsou pro úspěšné nasazení Active Directory tak důležité, že je mnoho správců považuje přímo za komponentu Active Directory. Je to téměř pravda a je dobře, pokud tak smýšlíte, ale pro zásady skupiny ve skutečnosti Active Directory nutně nepotřebujete. Zásady skupiny lze používat v podnikovém prostředí (s doménami) stejně jako v místním prostředí (s pracovními skupinami).

Globální zásady skupiny

V podnikovém prostředí, kde je nasazeno Active Directory, je k dispozici úplná sada nastavení a předvoleb zásad. Tato sada zásad se nazývá *Doménové zásady skupiny, Zásady skupiny pro Active Directory* nebo jednoduše *Zásady skupiny*. Na doménových řadičích jsou zásady skupiny uchovávány v oblasti SYSVOL, kterou Active Directory používá pro replikaci zásad.

Zásady skupiny jsou logicky reprezentovány jako Objekty zásad skupiny (Group Policy objects, GPO). GPO je kolekcí nastavení zásad a předvoleb zásad skupiny. Jak detailně probírá sekce „Ukládání GPO“ v kapitole 8 „Údržba a rekonstrukce zásad skupiny“, každý objekt GPO má odpovídající kontejner (Group Policy Container, GPC) nebo šablonu (Group Policy Template, GPT).

Kontejner pro GPO je uložen v databázi Active Directory a je replikován normální procedurou replikace Active Directory. Kontejner se používá pro uchovávání vlastností vztahujících se k objektu GPO a je identifikován globálně jedinečným identifikátorem (GUID).

Šablona pro GPO je uložena v SYSVOL a je replikována prostřednictvím replikace SYSVOL. Šablona slouží k ukládání souborů souvisejících s GPO na disk a je určena stejným identifikátorem GUID jako kontejner.

Aplikace zásad skupiny spočívá ve vazbě GPO na komponenty struktury Active Directory. GPO je možné propojit s následujícími komponentami ve struktuře Active Directory:

- **Lokality** – *lokalita* (Site) je jedna nebo více podsítí spojených spolehlivým spojením. Lokality se používají k vytvoření adresářové struktury, která napodobuje fyzickou strukturu organizace. Lokalita má typicky stejné hranice jako lokální počítačová síť (LAN). Mapování lokalit je odlišné a zcela nezávislé na logických komponentách adresářové struktury, takže není nutné spojovat fyzickou strukturu sítě a logickou adresářovou strukturu.
- **Domény** – *doména* (Domain) je logické sdružení objektů, které sdílí stejnou adresářovou databázi. V adresářové struktuře je doména reprezentována jako kontejner objektů. V rámci domény lze zakládat uživatelské účty, skupiny a počítače, ale i sdílené zdroje jako tiskárny a složky. Přístup k objektům domény je řízen bezpečnostními oprávněními.
- **Organizační jednotky** – *organizační jednotka* (Organizational Unit, OU) je kontejner určený k udržování skupiny objektů uvnitř domény pohromadě. Protože organizační jednotka je nejmenší rámec, kterému lze delegovat oprávnění, může pomáhat při správě uživatelských účtů, skupin a počítačů i jiných zdrojů, například tiskáren či sdílených složek. Přidáním jedné organizační jednotky k jiné vzniká hierarchie uvnitř domény. Každá doména má svou vlastní hierarchii, nezávislou na hierarchii jakékoli jiné domény.

Objektů GPO lze založit mnoho. Jejich svázáním s místy v adresářové struktuře Active Directory je zajištěna aplikace odpovídajících nastavení těm uživatelům a počítačům, kteří se vyskytují v dané komponentě Active Directory.

Díky hierarchii Active Directory se standardně nastavení GPO na nejvyšší úrovni automaticky propagují i na nižší úrovně. Když je tedy nějaké nastavení v GPO uplatněno například na doménu dmn.cz a tato doména obsahuje organizační jednotku Obchodní oddělení, bude dané nastavení uplatněno také na uživatele a počítače v Obchodním oddělení. Pokud nemá být nastavení zásady aplikováno v Obchodním oddělení, je třeba jej na nižší úrovni přepsat nebo blokovat. To se dá zajistit s pomocí objektů GPO umístěných na nižší úrovni.

Poznámka: Při použití zásad skupiny založených na doméně se může zdát, že úroveň fungování doménové struktury nebo domény ovlivňuje, jak se zásady skupin používají. Avšak není tomu tak. Doménová struktura ani doména nemusí být v žádném zvláštním režimu, aby se zásady skupiny uplatnily.

Při založení domény se v Active Directory vždy automaticky vytvoří dva objekty GPO:

- **Default Domain Controllers Policy GPO** – výchozí objekt GPO propojený s organizační jednotkou Domain Controllers, která standardně obsahuje všechny řadiče dané domény. Tento objekt GPO se tedy vztahuje na řadiče domény, dokud jsou součástí této organizační jednotky.
- **Default Domain Policy GPO** – výchozí objekt GPO propojený s celou doménou v Active Directory.

Můžete pak vytvářet další objekty GPO podle potřeby a propojovat je s lokalitami, doménami a organizačními jednotkami. Lze například založit nový objekt GPO nazvaný Zásady Obchod a propojit jej s Obchodním oddělením. Zásady se pak aplikují právě na tuto organizační jednotku.

Lokální zásady skupiny

V malé síti nebo domácím prostředí lze použít podmnožinu zásad skupiny zvanou *lokální (místní) zásady skupiny*. Jak je z názvu patrné, lokální zásady skupiny dovolují ovládat nastavení zásad, které ovlivňují pouze uživatele přihlášené na místní počítač. Znamená to, že lokální zásady skupin se uplatní na uživatele nebo administrátora přihlášeného na počítač, který je členem nějaké pracovní skupiny, stejně jako na uživatele nebo administrátora přihlášeného lokálně na počítač, který je členem nějaké domény. Lokální zásady skupiny se ukládají na jednotlivých počítačích do složky %SystemRoot%\System32\GroupPolicy.

Podobně jako v případě doménových zásad, také lokální zásady skupiny se skládají z objektů GPO. Takovým GPO se říká Lokální objekty zásad skupiny (Local Group Policy Objects, LGPO). Na systémech Windows Vista a novějších, které podporují vícenásobné LGPO, se dodatečné LGPO specifické pro uživatele či skupiny ukládají do složky %SystemRoot%\System32\GroupPolicyUsers.

Lokální zásady skupiny jsou podmnožinou všech zásad skupin, a tak je mnoho věcí, které s lokálními zásadami nelze provádět, zatímco na úrovni domény ano. Zaprvé, nejsou k dispozici předvolby zásad. Zadruhé, lze ovládat jen omezenou podmnožinu nastavení zásad. Obecně se dá říci, že nastavení zásad, která nelze použít lokálně, mají co do činění s Active Directory. Příkladem je instalace softwaru.

Kromě uvedených zásadních rozdílů mezi lokálními a doménovými zásadami skupiny všechno ostatní funguje v podstatě stejným způsobem. Ve skutečnosti se používají stejné nástroje na ovládání obou typů zásad. Klíčový rozdíl spočívá v objektech GPO; na lokálním počítači pracujete výhradně s LGPO, pokud je však nasazena technologie Active Directory, je možné navíc pracovat s objekty GPO v doméně, lokalitě nebo organizační jednotce.

Všechny počítače s Windows 2000 a novějšími znají LGPO. Objekty LGPO jsou zde vždy zpracovávány, mají však nejnižší prioritu. Jejich nastavení může být tedy potlačeno nastavením na úrovni lokality, domény nebo organizační jednotky. Přestože i řadiče

domény mají LGPO, zásady skupiny je pro ně vhodnější řešit prostřednictvím objektu Default Domain Controllers GPO.

Tip: Mějte na paměti, že zásady skupiny se uplatňují v rámci adresářové struktury. Nastavení se provádí v následujícím základním pořadí: nejdříve lokální, pak nastavení dle lokality, domény a nakonec podle organizační jednotky. Ve standardní konfiguraci (když se nepoužívá vynucování a blokování) je efektivně uplatněno poslední nastavení z uvedeného pořadí.

Správa zásad skupiny

Když nyní víte, jak se pracuje s objekty GPO, podívejme se na správu zásad skupiny. V této sekci probereme základní nástroje a techniky a také postup instalace dodatečných nástrojů, které mohou být užitečné. Důkladnější pojednání o práci se zásadami skupiny bude následovat v dalším textu.

Práce se zásadami skupiny

Když kvůli konfiguraci organizační infrastruktury nainstalujete Active Directory, budou pro vás vytvořeny standardní uživatelské účty a skupiny. Jejich účelem je usnadnění práce s adresářovou strukturou a konfigurace zabezpečení. Mezi standardními uživateli a skupinami se nachází:

- **Administrator** – standardní privilegovaný uživatelský účet s přístupem do celé domény. Ve výchozím nastavení domény je Administrator členem následujících skupin: Administrators, Domain Admins, Domain Users, Enterprise Admins, Group Policy Creator Owners a Schema Admins.
- **Administrators** – lokální skupina, která poskytuje plný přístup správce k jednotlivým počítačům nebo k doméně, podle umístění. Protože členové této skupiny mají všechna oprávnění, měli byste je přidávat jen velmi obezřetně. Když chcete někoho učinit správcem počítače nebo domény, stačí přidat danou osobou jako člena do této skupiny. Svůj účet mohou měnit jen členové skupiny Administrators. Mezi výchozí členy této skupiny patří Administrator, Domain Admins a Enterprise Admins.
- **Domain Admins** – globální skupina určená ke správě všech počítačů v doméně. Členové této skupiny mohou plně ovládat všechny počítače v doméně, protože jsou automaticky ve skupině Administrators na každém počítači v doméně. Chcete-li někoho učinit správcem domény, přidejte ho do této skupiny.
- **Enterprise Admins** – globální nebo univerzální skupina navržená ke správě všech počítačů v doméně nebo v doménové struktuře. Členové této skupiny mají plnou kontrolu nad všemi počítači v podniku, protože tato skupina je automaticky členem skupiny Administrators na každém počítači v organizaci. Určenou osobu učiníte správcem pro celý podnik tak, že ji přidáte do této skupiny.

- **Group Policy Creator Owners** – globální skupina, která pomáhá se správou zásad skupiny. Členové této skupiny mají oprávnění spravovat zásady skupiny.
- **Schema Admins** – globální skupina určená ke správě schématu Active Directory. Její členové mohou měnit toto schéma.

Kdykoli pracujete se zásadami skupiny, ujistěte se, že používáte uživatelský účet náležející k patřičné skupině nebo skupinám.

Nástroje pro správu zásad skupiny

Zásady skupiny lze spravovat prostřednictvím grafických i řádkových nástrojů. S grafickým rozhraním se pracuje lépe, ale pokud zvládnete řádkové příkazy, zjistíte, že s nimi často vyřešíte některé úkoly rychleji. Když řádkové nástroje zkombinujete s plánovačem úloh, můžete dokonce zautomatizovat některé rutinní úkony.

Poznámka: V příloze A „Instalace rozšíření a nástrojů pro zásady skupiny" najdete podrobný návod, jak nainstalovat rozšíření a dodatečné nástroje pro práci se zásadami skupiny. V příloze je uvedeno:

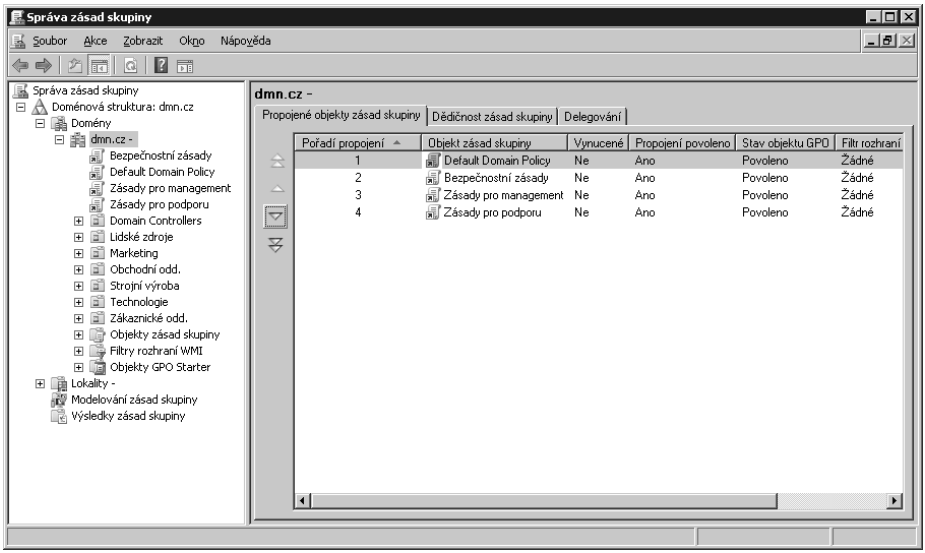
- Jak nainstalovat Remote Server Administration Tools na Windows Vista.
- Jak nainstalovat klientská rozšíření pro zásady skupiny na Windows XP, Windows Server 2003 a Windows Vista.
- Jak nainstalovat klientské a serverové komponenty pro Advanced Group Policy Management (AGPM).

Grafické nástroje pro správu

Grafické nástroje pro správu a práci se zásadami skupiny mají podobu přizpůsobených konzolí a modulů snap-in pro konzolu Microsoft Management Console (MMC). Tyto nástroje jsou dosažitelné přímo z nabídky Nástroje pro správu nebo je lze přidat k jakékoli konzole MMC, která se dá aktualizovat. Pokud jste na jiném počítači s přístupem k doméně Windows Serveru 2008, tyto nástroje nebudou k dispozici, pokud je zvlášť nenainstalujete. Jednou z možností instalace těchto nástrojů je Průvodce přidáním funkce (Add Feature Wizard).

Doménové zásady skupiny se ovládají v konzole Správa zásad skupiny (Group Policy Management Console, GPMC), kterou představuje obrázek 1.1. Konzolu GPMC lze přidat na jakoukoli instalaci Windows Serveru 2008 s pomocí Průvodce přidáním funkce (Add Feature Wizard).

Windows Server 2008 obsahuje aktualizovanou verzi konzoly Správa zásad skupiny. Jsou do ní zabudovány předvolby zásad skupiny, navíc tyto předvolby lze konfigurovat vzdáleně po instalaci Remote Server Administration Tools (RSAT) na počítač s Windows Vista SP1. V případě Windows Vista SP1 a novějších je verze konzoly Správa zásad skupiny obsažená v RSAT právě tou aktualizovanou verzí. Po instalaci na Windows Vista je konzola Správa zásad skupiny k dispozici v nabídce Nástroje pro správu.



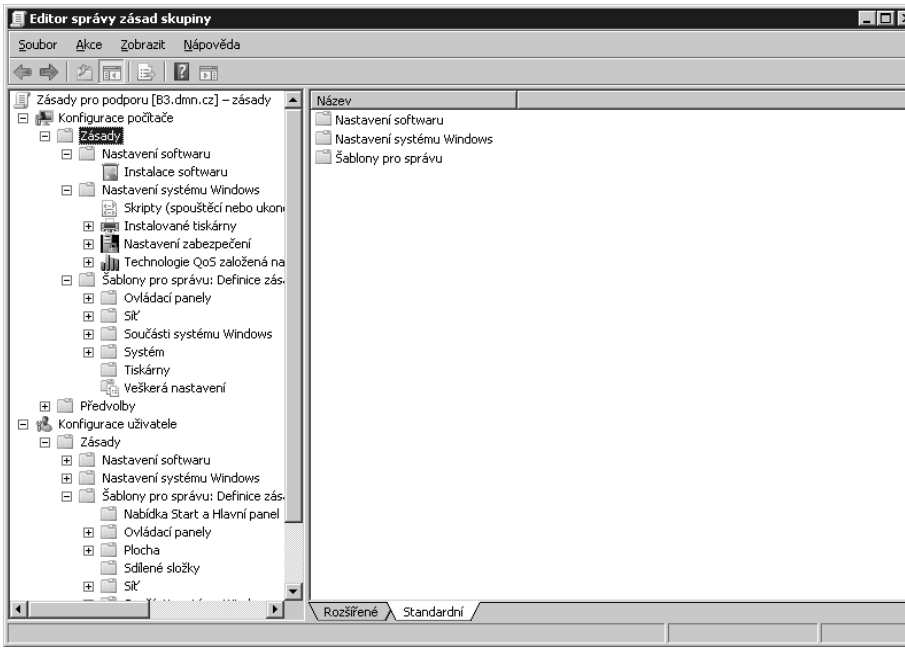
Obrázek 1.1: Konzola Správa zásad skupiny

V konzole Správa zásad skupiny (GPMC) je možné provádět následující operace:

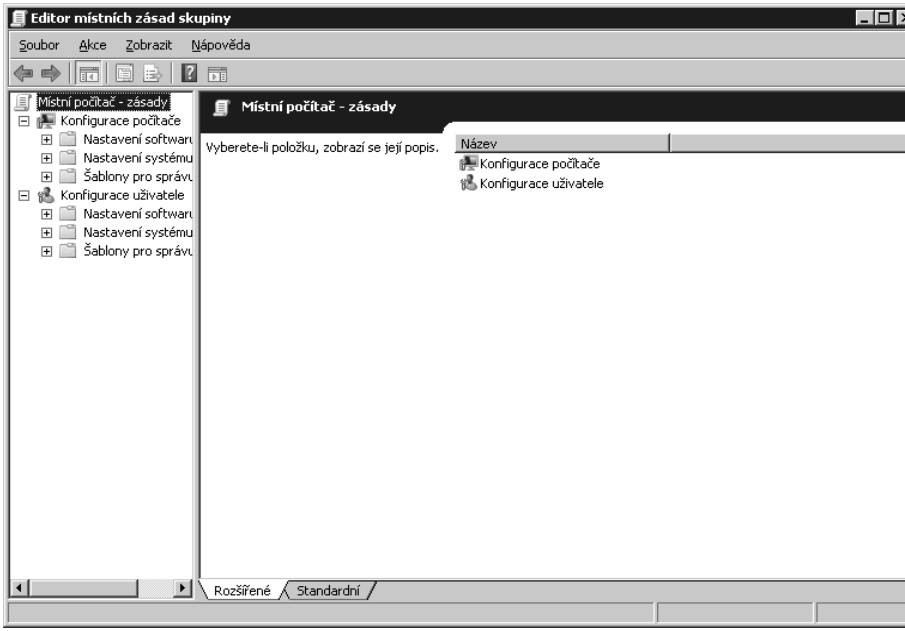
- Tvorba, úprava a mazání objektů zásad skupiny (GPO)
- Kopírování, import a export objektů GPO
- Zálohování a obnova objektů GPO
- Modelování objektů GPO před nasazením, takže je možné zjistit, jak nastavení ovlivní uživatele a počítače
- Modelování již aplikovaných objektů GPO ke zjištění způsobu, jakým ovlivňují uživatele a počítače

Když chcete v konzole Správa zásad skupiny upravit některý objekt GPO, otevře vám konzola v novém okně Editor správy zásad skupiny, který vidíte na obrázku 1.2. Editor slouží ke specifikaci nastavení a předvoleb zásad daného objektu GPO.

Další dva editory, které jsou k dispozici, se jmenují Editor objektu GPO Starter modulu snap-in Zásady skupiny a Editor místních zásad skupiny. Ten první z nich, Editor objektu GPO Starter modulu snap-in Zásady skupiny, slouží k vytváření a správě objektů GPO Starter. Jejich účelem je zjednodušení tvorby nových objektů zásad napříč vaším podnikem tím, že jsou jakýmsi startovním bodem pro nové objekty GPO. Když zakládáte nový objekt GPO, můžete uvést odkaz na některý objekt GPO Starter a na něm pak bude nový objekt založen. V Editoru místních zásad skupiny, který je ilustrován na obrázku 1.3, lze ovládat objekty zásad platné pouze na místním počítači, narozdíl od nastavení pro celou lokalitu, doménu nebo organizační jednotku.



Obrázek 1.2: Editor správy zásad skupiny



Obrázek 1.3: Editor místních zásad skupiny

Tip: Brána firewall systému Windows na platformách předcházejících Windows Vista může mít vliv na vzdálenou správu některými nástroji v konzole MMC. Pokud je brána firewall na vzdáleném počítači zapnuta a obdržíte chybové hlášení, že nemáte příslušná oprávnění, že síťová cesta nebyla nalezena nebo že přístup byl odepřen, bude možná nutné přidat na vzdálený počítač výjimku pro příchozí port 445 protokolu Transmission Control Protocol (TCP). S pomocí zásad vyřešíte nastavení brány firewall tak, že výjimku pro port 445 zadáte v cestě Konfigurace počítače\Zásady\Šablony pro správu\Síť\Síťová připojení\Brána Windows Firewall\Profil domény. Podrobnější informace k tomuto tématu najdete v článku Microsoft Knowledge Base číslo 840634 „How to Configure Windows firewall in Windows XP service Pack 2 to Allow Remote Administration Tools That Use WMI, RPC, or DOM" (*http://support.microsoft.com/kb/840634*).

Nástroje na příkazovém řádku

V konzole GPMC je k dispozici obsáhlá sada rozhraní pro Component Object Model (COM), která lze využít k tvorbě skriptů pro mnoho rozmanitých operací podporovaných v konzole. Příklady skriptů jsou dostupné v Centru stažení softwaru společnosti Microsoft (*http://www.microsoft.com/downloads*). Nenovější verze skriptů hledejte v tomto centru zadáním klíčových slov „Group Policy Management Console Sample Scripts". Mezi další nástroje příkazového řádku pro práci se zásadami skupiny patří:

- **ADPREP** – slouží k přípravě doménové struktury nebo domény na instalaci řadičů domény. Chcete-li připravit doménu před první instalací Windows Serveru 2008, spusťte na serveru, který má roli hlavního uzlu pro operace infrastruktury, příkaz *adprep /domainprep /gprep*.
- **GPFIXUP** – používá se k vyřešení závislostí v objektech zásad skupiny a jejich propojení po operaci přejmenování domény.
- **GPRESULT** – ukazuje, jaké zásady jsou v platnosti, a pomáhá řešit problémy se zásadami.
- **GPUPDATE** – ruční aktualizace zásad skupiny. Příkaz GPUPDATE nahrazuje nástroj SECEDIT /refreshpolicy známý z Windows 2000. Pokud na příkazovém řádku zadáte **gpupdate**, aktualizují se na místním počítači jak konfigurace uživatele, tak konfigurace počítače podle zásad skupiny.
- **LDIFDE** – poskytuje import a export informací z adresářové struktury. Tento nástroj využijete při provádění pokročilých úkonů souvisejících se zálohováním a obnovou nastavení zásad, která jsou uložena mimo GPO. Tento příkaz je zvláště užitečný při zálohování a obnově velkého množství filtrů rozhraní Windows Management Instrumentation (WMI) najednou (pro bližší informace viz blog týmu pro zásady skupiny na adrese *http://go.microsoft.com/fwlink/?linkid=109519*).
- **NETSH IPSEC** – prohlížení a změny konfigurace zabezpečení IPSec. Příkaz *netsh ipsec static show all* vypisuje statická nastavení a zásady pro IPSec, zatímco příkazem

netsh ipsec dynamic show all získáte informace o dynamických nastaveních a zásadách zabezpečení IPSec.

Z praxe: Příkaz NETSH IPSEC uvádíme v seznamu podstatných nástrojů pro zásady skupiny proto, že zálohy zásad skupiny vytvořené v konzole GPMC neobsahují nastavení IPSec. Ta jsou zálohována spolu se zálohami stavu systému. Proto budete možná potřebovat sledovat nastavení IPSec a jejich zásad a příkaz NETSH IPSEC vám v tom pomůže.

Nástroje pro správu zásad skupiny poskytují přístup k objektům GPO. Detailně popíšeme techniky práce s nimi v kapitole 2 „Nasazení zásad skupiny". Najdete zde několik rychlých a snadných postupů pro přímou práci s objekty GPO. Na příkazovém řádku s oprávněními správce se příkazem **gpedit** otevírá možnost práce s místními objekty GPO v programu Editor místních zásad skupiny. Je také možné otevřít editor pro místní zásady skupiny jiného počítače, a to příkazem s následující syntaxí:

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

Zde *NázevPočítače* reprezentuje jméno stanice nebo plně kvalifikované doménové jméno počítače. Jméno vzdáleného počítače musí být obklopeno uvozovkami, jako v tomto příkladě:

```
gpedit.msc /gpcomputer:"Server82"
```

nebo

```
gpedit.msc /gpcomputer:"Server82.dmn.cz"
```

Na příkazovém řádku s oprávněními správce lze otevřít dokonce i objekty GPO v Editoru správy zásad skupiny. Základní podoba příkazu je tato:

```
gpedit.msc /gpobject:"LDAP://CN=GPOID,CN=Policies,
CN=System,DC=JménoDomény,DC=cz"
```

Přitom *GPOID* je jedinečné ID objektu GPO tak, jak je uvedeno na kartě Podrobnosti v konzole Správa zásad skupiny, když je daný objekt GPO vybrán. *JménoDomény* je pak první složka názvu domény, ve které byl daný objekt GPO vytvořen. Celá LDAP cesta k objektu musí být obklopena uvozovkami. Zde je příklad:

```
gpedit.msc /gpobject:"LDAP://CN={BEC9EE90-EC28-42E8-850F-631AEBF97761},
CN=Policies,CN=System,DC=dmn,DC=cz"
```

V předchozím příkladě byl otevřen objekt GPO s jedinečným ID {BEC9EE90-EC28-42E8-850F-631AEBF97761} v doméně dmn.cz.

Příkaz otevírající editor specifického objektu GPO s pomocí jedinečného ID využijete v případě, že chcete rychlý přístup k často prohlíženému nebo upravovanému objektu GPO. Pokud takový příkaz uložíte například jako zástupce na Plochu nebo v nabídce Start, bude pro vás tento objekt GPO skutečně pohotově a snadno dostupný. V Příkazovém řádku můžete právě zadaný příkaz zkopírovat tak, že klepnete pravým tlačítkem na okno Příkazového řádku a zvolíte Označit. Když pak pře-

táhnete myší zadaný příkaz a stisknete Enter, zkopírujete příkaz do schránky Windows. Zástupce na ploše pak založíte klepnutím pravým tlačítkem na volné místo na ploše, výběrem volby Nový a Zástupce. Spustí se průvodce Vytvořit zástupce a stačí už jen stisknout Ctrl+V, aby se zkopírovaný příkaz vložil do pole Zadejte umístění položky. Klepněte na Další a zadejte název tohoto zástupce, například „GPO Zvýšené zabezpečení". Pak klepněte na Dokončit. Když potom poklepete na zástupce, spustí se Editor správy zásad skupiny a v něm bude otevřen požadovaný objekt GPO k prohlížení a editaci.

KAPITOLA 2

Nasazení zásad skupiny

V této kapitole:

Zásady skupiny přinášejí pohodlný a efektivní způsob správy předvoleb a nastavení pro počítače i uživatele. Se zásadami skupiny můžete ovládat předvolby a nastavení tisíců uživatelů nebo počítačů stejným způsobem, jakým měníte předvolby a nastavení u jediného počítače či uživatele, a to navíc bez opuštění vašeho pracovního místa. K tomu slouží několik nástrojů, kterým změníte předvolby či nastavení na požadované hodnoty, a tyto změny se uplatní po síti na cílovou skupinu počítačů a uživatelů.

Dříve bylo nutné všechny ty administrativní změny, které nyní zásady skupiny umožňují, dělat ručními úpravami registru Windows, a to zvlášť na každém cílovém počítači. Díky zásadám skupiny se s povolením nebo zakázáním nějaké hodnoty v registru vypořádáte tak, že uvedete předvolbu nebo nastavení zásady a tato změna se automaticky aplikuje ihned, jakmile se zásady skupiny na cílovém počítači aktualizují. V konzole Správa zásad skupiny je možné modelovat provedené změny ještě předtím, než se tyto změny uplatní. Díky tomu se můžete ujistit, jaký efekt budou požadované úpravy mít. Před zavedením změny můžete stav zásad skupiny uložit, a když se cokoli pokazí, můžete celý systém zásad skupiny vrátit do předchozího stavu. Jakmile obnovíte stav zásad skupiny, víte s určitostí, že po nejbližší aktualizaci zásad skupiny jsou všechny nechtěné změny vráceny zpět.

Před prvotním nasazením zásad skupiny či před provedením zásadních změn existujících zásad byste měli mít důkladné vědomosti v těchto oblastech:

- Jaké změny prodělal systém zásad skupiny s každou novou verzí operačního systému Windows.
- Jak aktualizovat zásady skupiny tak, aby obsahovaly nové předvolby a nastavení představené s novou verzí operačního systému Windows.
- Jak se zásady skupiny aplikují na místní počítač a jak se to děje v prostředí Active Directory.

- Jak se používají a kdy se uplatní výchozí sady zásad.
- Kdy jsou vhodnější předvolby zásad a kdy nastavení zásad.

Všechny tyto otázky jsou v této kapitole diskutovány.

Aktuálnost systému zásad skupiny

Zásady skupiny byly poprvé součástí operačního systému Windows 2000 a vztahují se proto pouze na počítače se systémy Windows 2000 a novějšími, ať už se jedná o servery nebo pracovní stanice. To znamená, že se zásady skupiny týkají jen systémů Windows 2000, Windows XP Professional, Windows Vista, Windows Server 2003, Windows Server 2008 a novějších verzí Windows. Každá nová verze operačního systému Windows s sebou přinesla změny ve fungování zásad skupiny, a tyto změny uvedeme v této sekci.

Podstatné změny ve zpracování zásad skupiny

Narozdíl od Windows 2000, systémy Windows XP Professional, Windows Server 2003, Windows Vista a Windows Server 2008 používají službu Klient zásad skupiny. Díky tomu jsou odděleny zprávy a zpracování zásad skupiny od procesu přihlášení do Windows. Separace zásad skupiny a přihlašování do Windows snižuje nároky na zdroje pro zpracování zásad na pozadí, a zároveň zvyšuje celkový výkon systému. Dává také možnost přenést a uplatnit nové zásady skupiny jako součást procesu aktualizace, aniž by byl nutný restart.

Windows Vista a Windows Server 2008 nepoužívají funkčnost podrobného protokolu událostí v Userenv.dll. Tyto systémy nezapisují podrobné události do protokolu aplikací, ale do protokolu systému Windows. Navíc operační protokol událostí zásad skupiny nahrazuje události, které byly dříve protokolovány do souboru %SystemRoot%\Debug\Usermode\Userenv.log. Proto když budete řešit nějaký problém se zásadami skupiny, nebudete hledat operační popisy událostí v souboru Userenv.log, ale v aplikačním protokolu. V Prohlížeči událostí (Event Viewer) najdete tyto záznamy pod Protokoly aplikací a služeb\Microsoft\Windows\GroupPolicy (Applications and Services Logs\Microsoft\Windows\GroupPolicy).

Windows Server 2008 navíc používá místo síťového protokolu ICMP (ping) systém Network Location Awareness. Díky němu je počítač obeznámen s typem sítě, do které je právě připojen, a může reagovat na změny stavu systému a konfigurace sítě. S pomocí Network Location Awareness může klient zásad skupiny zjistit stav počítače, stav sítě a dostupnou rychlost sítě. Tyto změny také dovolují aktualizaci zásad skupiny přes virtuální privátní sítě (Virtual Private Networks, VPN).

Změny v zásadách skupiny

Každá nová verze operačního systému Windows s sebou přináší změny v samotných zásadách. Někdy tyto změny spočívají v tom, že starší zásady jsou v novějších verzích Windows překonané. V tom případě tato zásada funguje jen na jistých verzích systému Windows, například jen na Windows XP Professional a Windows Serveru 2003. Obecně však naštěstí platí, že většina zásad skupiny je kompatibilní i v nových verzích Windows. Znamená to, že zásady pocházející z Windows 2000 budou většinou použitelné na Windows 2000, Windows XP Professional, Windows Serveru 2003, Windows Vista a Windows Serveru 2008. Méně příjemným důsledkem je to, že naopak zásady z Windows XP Professional z větší části nebudou použitelné na Windows 2000 a že zásady nově uvedené ve Windows Vista se nedají uplatnit na Windows 2000 ani Windows XP Professional.

Je-li zásada skupiny nekompatibilní s nějakou verzí Windows, nemůžete ji uplatnit na počítače, na kterých tato verze Windows běží. Zda je nějaká zásada podporována v jisté verzi Windows poznáte díky tomu, že je to u každé předvolby či nastavení výslovně uvedeno.

Také konzola Správa zásad skupiny (Group Policy Management Console, GPMC) se s novými verzemi operačního systému Windows proměňuje. Verze 1.0 této konzoly byla součástí Windows XP a Windows Serveru 2003. Původně byla součástí Windows Vista konzola GPMC verze 1.5. Když však nainstalujete balíček Remote Server Administration Tools (RSAT), jak je zmíněno v kapitole 1 „Úvod do zásad skupiny", a vyberete přitom GPMC jako jeden z nástrojů, získáte GPMC verze 2.0. Stejnou verzi 2.0 obdržíte spolu s Windows Serverem 2008.

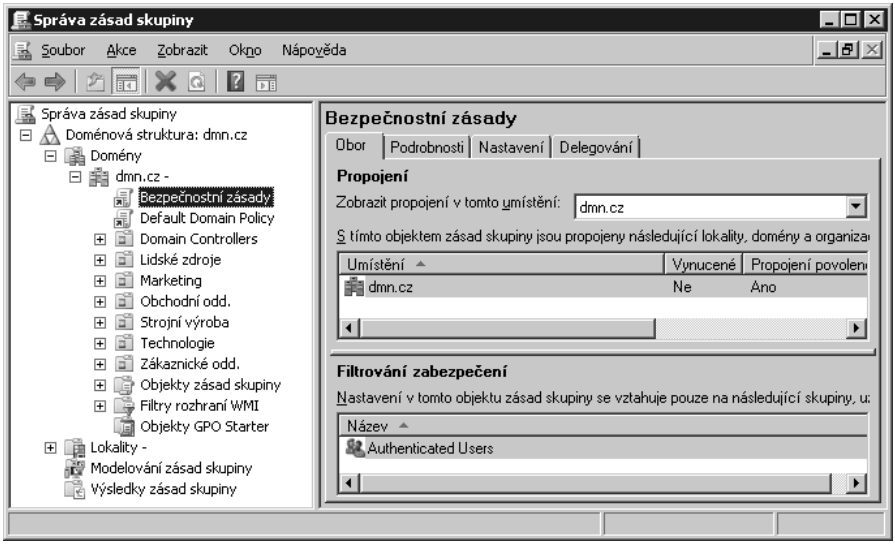
Jakmile v prostředí vaší domény začnete využívat GPMC verze 2.0 nebo novější, měli byste přestat používat předchozí verze GPMC. Konzola Správa zásad skupiny GPMC totiž od verze 2.0 přidává podporu pro funkce a formáty souborů. Tyto nové vlastnosti mohou být konfigurovány jen s verzí 2.0 nebo novější. Proto například zásady skupiny pro počítače se systémy Windows Vista a Windows Server 2008 mohou být ovládány opět jen ze stanic Windows Vista nebo Windows Server 2008, případně novějších verzí Windows.

Na Windows Vista, Windows Serveru 2008 a novějších verzích systému uvidíte v konzole Správa zásad skupiny GPMC 2.0 kromě standardních funkcí a zásad také již zmíněné nové funkce a zásady. Tyto novinky však nejsou automaticky součástí objektů zásad skupiny (Group Policy Objects, GPO). Nemějte žádné obavy, to se dá snadno napravit tak, že nakonec budete moci všechny tyto nové funkce a zásady používat v celé vaší doméně.

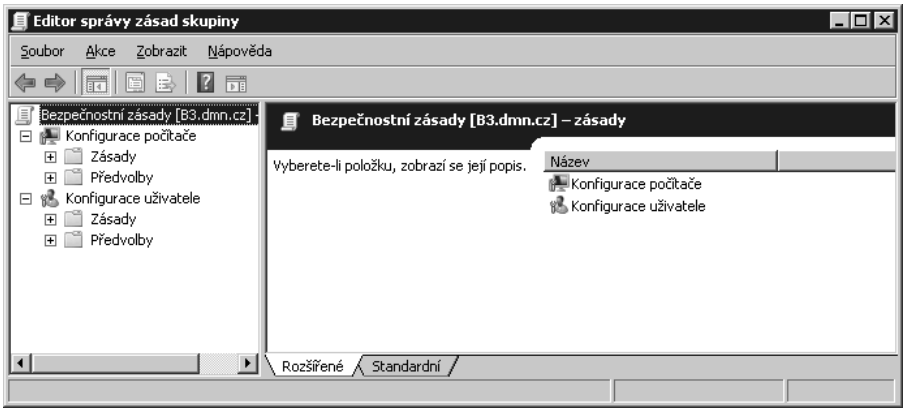
K propagaci nových funkcí a zásad do domény stačí, když aktualizujete příslušné objekty GPO. Jakmile tak učiníte, kompatibilní klienti si z nové sady zásad skupiny vyberou nová rozšíření a změní podle nich své chování, zatímco ostatní klienti budou nová nastavení, která nepodporují, prostě ignorovat.

Přidání nových funkcí a zásad do objektů GPO probíhá v následujících krocích:

1. Přihlaste se na Windows Vista nebo novější verzi Windows prostřednictvím účtu, který má oprávnění správce domény.
2. Otevřete konzolu Správa zásad skupiny (Group Policy Management Console, GPMC) klepnutím na Start, Nástroje pro správu (Administration Tools), a volbou Group Policy Management.
3. V konzole GPMC uvidíte uzel Doménová struktura (Forest), reprezentující aktuální doménovou strukturu, ke které jste připojeni (viz obrázek 2.1). Když uzel pro doménovou strukturu rozbalíte, uvidíte uzly Domény (Domains) a Lokality (Sites). Tyto uzly slouží k aplikaci objektů GPO tam, kde je to třeba.
4. Jakmile najdete objekt GPO, se kterým chcete pracovat, klepněte na něho pravým tlačítkem a zvolte Upravit (Edit). Otevře se Editor správy zásad skupiny (Group Policy Management Editor), který můžete vidět na obrázku 2.2.
5. V Editoru správy zásad skupiny klepněte na uzel Konfigurace počítače (Computer Configuration) a pak na uzel Konfigurace uživatele (User Configuration). Vždy když zvolíte tyto uzly, načtou a aplikují se do zvoleného objektu GPO aktuální šablony pro správu. Po aktualizaci zásad skupiny se uplatní změny v zásadách a předvolbách podle potřeby, a tyto změny se projeví ve vybraných lokalitách, doménách či organizačních jednotkách.
6. Opakujte tuto proceduru pro další objekty GPO, abyste aktualizovali také další lokality, domény a organizační jednotky.



Obrázek 2.1: Standardně se konzola Správa zásad skupiny (GPMC) připojí k místní doménové struktuře



Obrázek 2.2: Editace objektu GPO v Editoru správy zásad skupiny

Normálně se výše popsanou procedurou nezmění žádný další aspekt systému zásad skupiny. Avšak počítače s Windows Vista a novějšími verzemi Windows pracují s novým formátem souboru zvaným ADMX. Tento formát používá k popisu zásad XML a mění způsob, jakým se ukládají data v SYSVOL.

Změny v SYSVOL

Původní formát souboru pro popis zásad skupiny zvaný ADM znamenal, že soubory s definicemi zásad se ukládají společně s objekty GPO, na které se vztahují. Výsledkem je, že s každým objektem GPO se ukládá kopie všech definičních souborů příslušných zásad. Může se jednat až o několik megabajtů dat. Naopak s formátem ADMX nejsou standardně definiční soubory zásad ukládány spolu s relevantními objekty GPO. Místo toho se definiční soubory ukládají centrálně na doménovém řadiči a s objekty GPO se ukládají jen odpovídající nastavení. Jako důsledek jsou objekty GPO používající ADMX významně menší než tytéž objekty GPO založené na formátu ADM. Tak například objekt GPO s ADM o velikosti 4 megabajty se může zmenšit až na 4 kilobajty, pokud používá ADMX.

Formát ADMX se od původního formátu ADM podstatně liší. Soubory ADMX jsou rozděleny na jazykově neutrální soubory s příponou .admx a jazykově specifické soubory s příponou .adml. Jazykově neutrální soubory jsou zde proto, aby objekty GPO měly identické funkční jádro zásad skupiny. Jazykově specifické soubory zajišťují, že zásady mohou být prohlíženy a měněny v rozličných jazycích. Jelikož skutečné jádro funkčnosti zásad skupiny je uloženo v jazykově neutrálních souborech, je možné upravovat zásady skupiny v jakémkoli jazyce, který je na počítači nakonfigurován. Tak například jeden uživatel si může prohlížet a editovat zásady v angličtině, zatímco jiný tak může činit v jazyce českém. Mechanismus rozlišující jazyk, ve kterém probíhá editace zásad skupiny, je stejný jako pro všechny ostatní aplikace: je to nastavení jazyka v systému Windows.

Jazykově neutrální soubory ADMX se na počítačích s Windows Vista a Windows Serverem 2008 ukládají do složky %SystemRoot%\PolicyDefinitions, zatímco jazykově specifické soubory ADMX se instalují do složek %SystemRoot%\PolicyDefinitions*Jazyk-Kultura*. Podsložky *Jazyk-Kultura* jsou označeny podle odpovídajících standardů ISO (International Standards Organization) pro názvy jazyků a kulturních oblastí. Například pro americkou angličtinu bude mít podsložka název en-US, pro češtinu je to cs-CZ.

Pokud aktualizujte zásady na formát souboru ADMX, budou k nim mít od této chvíle přístup už jen editory zásad skupiny, které jsou s formátem ADMX kompatibilní. Takový kompatibilní editor si při svém spuštění automaticky načítá soubory ADMX ze složek pro definice zásad (%SystemRoot%\PolicyDefinitions). Když tedy chcete mít jisté definiční soubory při editaci nějakého objektu GPO dostupné, můžete je prostě do této složky nakopírovat. Pokud je v průběhu kopírování editor již spuštěn, musíte jej zavřít a spustit znovu, aby si načetl nové soubory ze složky.

V prostředí domény se definiční soubory zásad skupiny nemusí ukládat do složky na každém počítači, který používáte k editaci objektů GPO. Místo toho mohou být uloženy v centrálním úložišti, což přináší při práci se soubory ADMX značnou výhodu. S objekty GPO pak lze pracovat z jakéhokoli kompatibilního počítače v síti. Lépe se tak zvládají změny v obsahu i přidávání nových souborů ADMX.

Centrální úložiště pro soubory ADMX vytvoříte s pomocí účtu, který je členem skupiny Domain Admins, a to přímo na řadiči domény. Je třeba v rámci svazku SYSVOL vytvořit složku s názvem PolicyDefinitions, v níž budou ukládány jazykově neutrální soubory ADMX s příponou .admx, a také podsložky PolicyDefinitions pro jazykově specifické soubory pro všechny jazyky, které hodláte v souborech ADMX používat. Tyto soubory budou mít příponu .adml. Po vytvoření potřebných složek musíte zkopírovat jazykově neutrální i jazykově specifické soubory ADMX na správné místo v centrálním úložišti.

Standardní umístění svazku SYSVOL na řadiči domény je %SystemRoot%\Sysvol. Vytvoření a ustanovení centrálního úložiště pro soubory ADMX v tomto místě provedete následujícím postupem:

1. Přihlaste se na řadič domény se systémem Windows Server 2008 v cílové doméně prostřednictvím účtu, který je členem skupiny Domain Admins. Pak ve složce %SystemRoot%\Sysvol*JménoDomény*\Policies vytvořte podsložku PolicyDefinitions. Nahraďte řetězec *JménoDomény* skutečným jménem domény, jejíž je aktuální počítač řadičem a v níž chcete vytvořit centrální úložiště. Uvnitř složky PolicyDefinitions pak vytvořte podsložky pro všechny jazyky, ve kterých chcete mít soubory ADMX dostupné.

Z praxe: Jak se uvádí dále v této kapitole v sekci „Změny v replikaci", řadiče domény umí replikovat svazek SYSVOL buď s pomocí Služby replikace souborů (File Replication Service, FRS), nebo Distribuovaného systému souborů (Distributed File System, DFS). Standardní umístění SYSVOL je v případě, že řadiče domény používají k replikaci FRS, složka %SystemRoot%\Sysvol. Pokud je však mezi řadiči domény aktivní replikace DFS, je standardním umístění SYSVOL %System-

Root%\Sysvol_dfsr. Pokud tedy vaše řadiče domény replikují systémem DFS, vytvořte složku PolicyDefinitions i její jazykové podsložky uvnitř %SystemRoot%\Sysvol_dfsr*JménoDomény*\Policies a zkopírujte soubory sem.

2. Zkopírujte soubory ADMX i ADML z původního místa na řadič domény do odpovídajících složek v rámci SYSVOL.

   Windows Vista SP1 a Windows Server 2008 obsahují 146 výchozích souborů ADMX. Každý z nich má odpovídající soubory ADML umístěné v odpovídajících jazykových podsložkách, jakou je např. cs-CZ pro češtinu. Tyto soubory jsou standardně umístěny ve složkách %SystemRoot%\PolicyDefinitions, respektive %SystemRoot%\PolicyDefinitions*Jazyk-Kultura*. Pokud si založíte vlastní soubory ADMX, uloží se na stanici, na které byly vytvořeny. Na systémech novějších než Windows Vista SP1 nebo Windows Server 2008 RTM mohou být k dispozici také další soubory ADMX, dostupné pouze na počítačích se stejnou kombinací operačního systému a Service Packu.

Vytvoření centrálního úložiště pro všechny jazyky podporované na počítači, na kterém jste právě přihlášeni, je možné provést zkopírováním všech potřebných definičních souborů zásad v jednom kroku. Kopii všech souborů ADMX z vašeho počítače na doménový řadič zajistíte z příkazového řádku s oprávněními správce spuštěním následujícího příkazu:

```
xcopy /s /y %SystemRoot%\PolicyDefinitions \\ŘD\Sysvol\JménoDomény\Policies\
PolicyDefinitions\
```

Přitom *ŘD* je jméno cílového řadiče domény, a *JménoDomény* je plně kvalifikované DNS jméno domény, ve které je doménový řadič umístěn. V následujícím příkladu se kopírují soubory ADMX a ADML z místního počítače na řadič Server82 v doméně dmn.cz:

```
xcopy /s /y %SystemRoot%\PolicyDefinitions \\Server82\Sysvol\dmn.cz\Policies\
PolicyDefinitions\
```

Při práci s definičními soubory zásad jsou užitečné dvě proměnné prostředí: %UserDNSDomain% a %Logonserver%. První z nich, %UserDNSDomain%, uchovává aktuální doménu, do které je uživatel přihlášen, zatímco druhá proměnná, %Logonserver%, reprezentuje doménový řadič, který provedl autentizaci při přihlášení. S použitím těchto proměnných byste mohli zkopírovat všechny potřebné definiční soubory zásad zapsáním následujícího příkazu na příkazový řádek s oprávněními správce:

```
xcopy /s /y %SystemRoot%\PolicyDefinitions \\%LogonServer%\Sysvol\
%UserDNSDomain%\Policies\PolicyDefinitions\
```

Doporučujeme zachovávat zavedenou praxi, kterou je vytvoření centrálního úložiště na řadiči, jenž hraje roli emulátoru primárního řadiče v dané doméně (Primary Domain Controller Emulator, PDC emulátor). Standardně je totiž právě PDC emulátor tím řadičem domény, na který se systém zásad skupiny spoléhá při editaci objektů GPO. Když tedy vytvoříte centrální úložiště na PDC emulátoru, bude každý, kdo se pokusí o edi-

taci GPO, mít k dispozici ihned aktuální obraz definičních souborů zásad. V opačném případě by se mohlo stát, že na PDC emulátoru nejsou soubory aktuální, a uživatel by musel čekat na replikaci obsahu SYSVOL. Jako součást normální replikace svazku SYSVOL pak bude PDC emulátor šířit obsah centrálního úložiště na ostatní řadiče v doméně.

Pokud potřebujete zjistit, který z doménových řadičů ve vaší doméně má roli PDC emulátoru, spusťte na příkazovém řádku následující příkaz:

```
dsquery server -o rdn -hasfsmo pdc
```

Výstupem tohoto příkazu je název počítače s rolí PDC emulátoru v aktuální doméně. Jestliže vás zajímá jméno PDC emulátoru v jiné doméně, přidejte parametr -domain, jako v následujícím příkladě:

```
dsquery server -o rdn -hasfsmo pdc -domain tech.dmn.cz
```

V tomto případě obdržíte jméno PDC emulátoru v doméně tech.dmn.cz. Pokud je v doménové struktuře obsaženo více domén, můžete se zajímat také o jednotlivé doménové řadiče s rolí PDC emulátoru ve všech doménách. K tomu slouží parametr -forest, viz následující příklad:

```
dsquery server -o rdn -hasfsmo pdc -forest
```

Více informací o tom, proč se systém zásad skupiny obrací standardně na PDC emulátor, přináší sekce „Připojení a práce s GPO“ dále v této kapitole.

Změny v replikaci

Klíčovou změnou mezi dřívějšími implementacemi Active Directory a implementací ve Windows Serveru 2008 je způsob, jakým jsou zásady s příbuznými daty replikovány. Systémový svazek Active Directory SYSVOL (SYStem VOLume) obsahuje doménové zásady, přihlašovací skripty a skripty pro odhlášení, vypnutí systému a jeho restart, některé další relevantní soubory a soubory uložené v Active Directory. Zatímco v kapitole 7 „Správa a údržba svazku SYSVOL“ najdete velmi podrobné informace o SYSVOL, v této sekci se podíváme ve stručnosti na to, jak funguje replikace SYSVOL.

Způsob replikace svazku SYSVOL závisí na úrovni funkčnosti domény. Pokud běží doména na funkční úrovni Windows 2000 – nativní režim nebo Windows Server 2003, řadiče domény replikují SYSVOL prostřednictvím Služby replikace souborů (File Replication Service, FRS). Na úrovni funkčnosti Windows Server 2008 však replikace mezi doménovými řadiči probíhá s pomocí Distribuovaného systému souborů (Distributed File System, DFS).

Technologie FRS a DFS slouží obě k replikaci souborů a složek v systémovém svazku SYSVOL mezi doménovými řadiči v Active Directory. Funguje to tak, že replikační služba si kontroluje údaje s procesem Knowledge Consistency Checker (KCC), který běží na každém řadiči domény. Zjistí tak topologii pro replikaci generovanou pro danou

doménu Active Directory a pak tuto topologii použije pro replikaci souborů svazku SYSVOL na další doménové řadiče v dané doméně.

Techniky ukládání a replikační architektura jsou v případě DFS a FRS značně odlišné. Služba replikace souborů (FRS, proces Ntfrs.exe) ukládá topologii FRS a časový plán replikace do Active Directory a pravidelně kontaktuje Active Directory prostřednictvím protokolu LDAP (Lightweight Directory Access Protocol), aby získala aktualizované informace. Interně provádí FRS přímá volání systému souborů prostřednictvím standardních vstupních a výstupních operací. Když komunikuje se vzdálenými servery, používá k tomu FRS protokol pro vzdálená volání procedur (Remote Procedure Call, RPC).

FRS si uchovává konfigurační data v registru, ale ukládá také rozličné typy dat v souborovém systému NTFS. Tak například transakce skladuje FRS v souboru Jet databáze FRS (Ntfrs.jdb), události a chyby v souboru protokolu událostí FRS (NtFrs.evt) a ladicí protokol ve složce pro protokoly ladění (%SystemRoot%\Debug). FRS replikuje obsah tzv. replikačního stromu, kterým je v případě Active Directory svazek SYSVOL. Svazek SYSVOL obsahuje doménové, podpůrné a další složky.

V systému souborů NTFS existuje žurnál USN (Update Sequence Number), který slouží ke sledování informací o přidaných, smazaných a změněných souborech. FRS pak používá žurnál USN k určení změn, které byly v replikačním stromě učiněny, a následně replikuje tyto změny podle časového plánu v Active Directory.

Naproti tomu distribuovaný systém souborů DFS používá místo replikačních stromů koncept tzv. jmenných prostorů. Informace o samostatných jmenných prostorech se ukládají v registru, zatímco doménové jmenné prostory mají svoje údaje v Active Directory. Informace o samostatných DFS prostorech obsahují jejich konfiguraci a jsou k nalezení na kořenovém serveru v cestě HKLM\SOFTWARE\Microsoft\Dfs\Roots\Standalone. Doménové kořenové servery mají sice klíče registru pro všechny jmenné prostory v cestě HKLM\SOFTWARE\Microsoft\Dfs\Roots\Domain, ale nejsou zde uloženy konfigurační údaje DFS.

Při startu služby DFS na doménovém řadiči Active Directory, kde se DFS používá, probíhá kontrola uvedené cesty v registru. Služba hledá položky registru, které odpovídají doménovým kořenovým prostorům. Pokud takové položky existují, kořenový server kontaktuje PDC emulátor a snaží se od něho získat konfigurační DFS data pro všechny doménové jmenné prostory. Tato data si pak uloží do paměti.

V Active Directory se konfigurační data pro doménové jmenné prostory DFS uchovávají v objektu DFS. Objekt DFS je přitom vytvořen v Active Directory při založení domény s úrovní funkčnosti Windows Server 2008 nebo při povýšení domény na tuto úroveň funkčnosti. Active Directory pak replikuje celý tento objekt DFS na všechny doménové řadiče v doméně.

DFS používá architekturu klient-server. Řadič domény, na kterém se nalézá nějaký jmenný prostor DFS, obsahuje jak klientskou, tak serverovou komponentu DFS. Takový

řadič je pak schopen provádět vyhledávání ve svém vlastním datovém úložišti stejně jako ve vzdálených úložištích na ostatních řadičích domény. DFS využívá pro komunikaci mezi klienty DFS, kořenovými servery a doménovými řadiči protokol CIFS (Common Internet File System), který je rozšířením protokolu SMB (Server Message Block) pro sdílení souborů.

Mezi FRS a DFS je snadné si vybrat. FRS podporuje zpětnou kompatibilitu s prostředím Windows 2000 Server a Windows Server 2003, ale neumožňuje využít nejnovější vylepšení. DFS poskytuje zdokonalení výkonu a funkcí Active Directory, ale dá se využít jen v případě, že všechny řadiče domény jsou založeny na Windows Serveru 2008 a že doména běží na úrovni funkčnosti Windows Server 2008.

Mezi pokroky replikace, které DFS zavádí, patří replikace změn pouze uvnitř souborů, snížení nároku na šířku pásma a zlepšení replikační topologie. Když změníte objekt GPO a používá se FRS, zreplikuje se celý objekt GPO. Při stejné změně, pokud je aktivní DFS, se replikují jen změny objektu GPO, a nutnost replikovat celý objekt po jeho třeba jen malé změně je eliminována.

FRS používá pro replikaci starší, méně efektivní technologii zvanou Rsync. DFS nahrazuje Rsync technologií RDC (Remote Differential Compression), což zrychluje replikaci až o 300 procent a kompresi o 200 až 300 procent. S DFS je snížena i operační režie správy obsahu a jeho replikace, a to asi o 40 procent. Navíc DFS podporuje automatické zotavení po ztrátě nebo poškození dat a také plánování replikace. Všechny tyto novinky společně činí DFS výrazně lépe škálovatelné než FRS.

Aplikace a propojování objektů GPO

Předvolby a nastavení zásad skupiny se ukládají v objektech GPO (Group Policy Objects). V této sekci prozkoumáme základní principy při aplikaci zásad skupiny (úvodní zpracování) a při jejich aktualizaci (následné zpracování). V dalších kapitolách se pak dostaneme k nejjemnějším detailům zpracování zásad skupiny.

Sady zásad v rámci objektů GPO

V zásadách skupiny rozeznáváme dvě oddělené sady zásad:

- **Zásady počítače** – vztahují se na počítače a ukládají se v rámci objektů GPO do uzlu Konfigurace počítače (Computer Configuration).
- **Zásady uživatele** – vztahují se na uživatele a ukládají se v rámci objektů GPO do uzlu Konfigurace uživatele (User Configuration).

Konfigurace počítače i Konfigurace uživatele obsahují uzly pro Zásady (Policies) i Předvolby (Preferences). Použití je následující:

- Konfigurace počítače\Zásady (Computer Configuration\Policies) slouží k nastavení zásad pro jisté počítače.

- Konfigurace počítače\Předvolby (Computer Configuration\Preferences) obsahuje předvolby zásad pro dané počítače.
- Konfigurace uživatele\Zásady (User Configuration\Policies) řídí nastavení zásad pro specifického uživatele.
- Konfigurace uživatele\Předvolby (User Configuration\Preferences) je uzel s předvolbami zásad určenými konkrétnímu uživateli.

Prvotní zpracování odpovídajících zásad je spouštěno jednou ze dvou specifických událostí:

- **Zpracování zásad počítače se děje při spuštění počítače –** jakmile je počítač spuštěn a síťové připojení je inicializováno, aplikují se zásady počítače.
- **Zpracování zásad uživatele se odehrává jako reakce na přihlášení uživatele k počítači –** zásady uživatele se aplikují ihned po přihlášení.

Jestliže jsou zásady aplikovány, dochází k jejich automatickému obnovování, aby byla nastavení aktuální a odrážela všechny změny, které mohly být v systému zásad skupiny učiněny. Standardně se zásady skupiny obnovují na řadičích domény každých 5 minut, zatímco pro pracovní stanice a další servery probíhá obnovení standardně po 90 až 120 minutách. Navíc většina bezpečnostních nastavení se aktualizuje každých 16 hodin bez ohledu na změny v nastavení zásad v uplynulém období. Mezi další faktory, které mají vliv na aktualizaci zásad skupiny, patří způsob rozpoznání pomalého připojení – Rozpoznání pomalého připojení zásad skupiny v Konfigurace počítače\Zásady\Šablony pro správu\Systém\Zásady skupiny (Group Policy Slow Link Detection v Computer configuration\Policies\Administrative templates\System\Group Policy) a také různá nastavení zpracování zásad v Konfigurace počítače\Zásady\Šablony pro správu\Systém\Zásady skupiny (Computer configuration\Policies\Administrative templates\System\Group Policy). Jak rozvádí sekce „Určení nastavení zásad a poslední aktualizace“ v kapitole 7, můžete v konzole Správa zásad skupiny (Group Policy Management Console, GPMC) zkontrolovat, kdy proběhla poslední aktualizace.

Poznámka odborného korektora: Časový interval opětovného aplikování zásad je volen z intervalu 90 až 120 minut. Důvodem je snížení zátěže řadiče domény. Každá ze stanic k základnímu času 90 minut přičítá náhodně generovaný čas z rozmezí 0 až 30 minut.

Typy objektů GPO

Jak jsme uvedli v kapitole 1, rozeznáváme dva typy objektů zásad skupiny: doménové objekty zásad skupiny (objekty GPO) a lokální objekty zásad skupiny (objekty LGPO).

Active Directory podporuje tři stupně objektů GPO:

- **Objekty GPO pro lokality (Sites) –** tyto objekty GPO se aplikují na úrovni lokality, tedy pouze v dané lokalitě Active Directory.

- **Objekty GPO pro domény (Domains)** – objekty GPO uplatněné na úrovni domény, to znamená jen v jisté doméně Active Directory.
- **Objekty GPO pro organizační jednotky (Organizational Units)** – objekty GPO, které mají platnost v rámci organizační jednotky tak, jak je definovaná v Active Directory.

Díky dědičnosti se objekty GPO aplikované na nějaký rodičovský uzel v rámci Active Directory uplatní také v podřízených uzlech. Nastavení nebo předvolba zásady se tedy propagují ve struktuře domény do nižších pater. Když například aplikujeme nastavení zásady v doméně, je toto nastavení zděděno všemi organizačními jednotkami v této doméně. V tomto případě je objekt GPO pro doménu rodičovským objektem a objekty GPO v jednotlivých organizačních jednotkách jsou jeho dceřinými objekty GPO.

V prostředí Active Directory je v základním pořadí dědičnosti na prvním místě lokalita, pak doména a nakonec organizační jednotka. Předvolby a nastavení zásad skupiny pro lokalitu se tak propagují dále na domény v této lokalitě, a předvolby a nastavení pro doménu se předávají níže na organizační jednotky v této doméně.

Tip: Jak asi očekáváte, dědičnost se dá potlačit. Dělá se to specifickým nastavením nebo předvolbou zásady v dceřiném uzlu doménové struktury, které jsou v rozporu s nastavením nebo předvolbou v rodičovském uzlu. Pokud je povoleno takové přepsání zásad na nižší úrovni (tedy pokud není toto přepisování zablokováno), předvolba nebo nastavení zásady v dceřiném uzlu dostane přednost a uplatní se. Více se o přepisování a blokování objektů GPO uvádí v sekci „Dědičnost zásad skupiny" v kapitole 7.

Zatímco počítače se systémem Windows 2000 a staršími mají jen jeden objekt LGPO, Windows Vista, Windows Server 2008 a novější připouštějí více objektů LGPO na jednom počítači (pokud ovšem tento počítač není řadičem domény). Na počítačích, které to umožňují, existují tři stupně objektů LGPO:

- **Místní objekt zásad skupiny** – místní objekt LGPO je na vrcholu hierarchie zásad skupiny pro místní počítač. Tento objekt LGPO je jediným objektem LGPO na místním počítači, který dovoluje aplikaci konfigurace počítače i konfigurace uživatele na všechny uživatelské účty na tomto počítači.
- **Administrátorský objekt LGPO / Neadministrátorský objekt LGPO** – zda se uplatní administrátorský nebo neadministrátorský objekt LGPO, to závisí na tom, jaký uživatelský účet je aktivní. Pokud je účet členem skupiny Administrators na místním počítači, použije se administrátorský LGPO. V opačném případě přijde ke slovu neadministrátorský LGPO. V tomto objektu jsou obsažena pouze nastavení konfigurace uživatele.
- **Uživatelský objekt LGPO** – uživatelské objekty LGPO se vztahují pouze k vybranému uživatelskému účtu nebo skupině. Také tento objekt obsahuje pouze konfigurace uživatele.

Uvedené stupně objektů LGPO se zpracovávají v tomto pořadí: nejdříve místní objekt LGPO, dále administrátorský nebo neadministrátorský objekt LGPO, a nakonec uživatelský objekt LGPO.

Z praxe: V situaci bez domény, kdy všechny počítače mají pouze své vlastní místní nastavení, můžete shledat systém více stupňů LGPO velmi užitečný. Díky nim nemusíte vždy kvůli úkonům spojeným s administrací počítače explicitně povolovat a rušit nastavení, která ke správě potřebujete. Místo toho lze nasadit jeden lokální objekt zásad skupiny pro administrátory a druhý pro neadministrátory. V doméně však více lokálních objektů nebudete chtít používat. Pokud je totiž aktivní Active Directory, většina počítačů a uživatelů už má aplikováno více objektů GPO, a zavedení více než jednoho místního objektu LGPO k této již tak rozmanité směsi může být matoucí. Může se proto ukázat výhodné zpracování místních objektů LGPO zcela vyloučit, a přesně to se dá zajistit s pomocí zásad skupiny. Na počítačích s Windows Vista a novějšími potlačíte zpracování místních objektů LGPO tak, že povolíte nastavení Vypnout zpracování místních objektů Zásad skupiny (Turn Off Local Group Policy Objects Processing) v nějakém objektu GPO, který se aplikuje na daném počítači. Když takový objekt editujete v Editoru správy zásad skupiny, najdete toto nastavení pod uzly Konfigurace počítače\Zásady (Computer Configuration\Policies). Rozbalte Šablony pro správu\Systém\Zásady skupiny (Administrative Templates\System\Group Policy) a pak poklepte na položku Vypnout zpracování místních objektů Zásad skupiny (Turn Off Local group Policy Objects Processing).

Když to vše spojíme dohromady, pokud jsou aktivní doménové i místní zásady, uplatňují se v následujícím pořadí:

1. Místní objekty LGPO
2. Objekty GPO pro lokalitu
3. Objektu GPO pro doménu
4. Objekty GPO pro organizační jednotku
5. Objekty GPO pro podřízenou organizační jednotku

Předvolby a nastavení dostupné v jednotlivých objektech zásad skupiny jsou naprosto shodné. Proto předvolba nebo nastavení zásad skupiny může velmi snadno kolidovat s předvolbou či nastavením v jiném objektu GPO. Kompatibilní operační systémy řeší konflikty přepsáním předchozích předvoleb a nastavení takovou předvolbou či nastavením, které bylo zjištěno naposledy a je aktuálnější. Proto předvolba nebo nastavení, které bylo zapsáno jako poslední, je to, které systém Windows použije. Tak například zásady pro organizační jednotku mají standardně přednost před zásadami pro doménu. Jak možná tušíte, v pravidlech pro přednost předvoleb a nastavení jsou výjimky, které se diskutují v sekci „Dědičnost zásad skupiny“ v kapitole 7.

Propojení objektů GPO

V Active Directory může mít každá lokalita, doména a organizační jednotka k sobě přidružený jeden nebo více objektů GPO. Asociace mezi objektem GPO a lokalitou,

doménou nebo organizační jednotkou se nazývá *propojení*. Pokud je tedy například objekt GPO přidružen k doméně, říkáme, že jde o propojení mezi objektem GPO a touto doménou.

Zásady skupiny se ukládají do kontejnerů zvaných Objekty zásad skupiny (Group Policy Objects, GPO). Tyto kontejnery se replikují na všechny doménové řadiče v doméně, takže všechny objekty GPO se objeví na všech řadičích domény. Právě propojení (asociace) s doménou, lokalitou či organizační jednotkou aktivuje objekt GPO a způsobuje, že se v doméně, lokalitě nebo organizační jednotce aplikuje.

Propojení se realizuje dvěma způsoby:

- Můžete propojit objekt GPO s jistou lokalitou, doménou nebo organizační jednotkou. Pokud je tedy například objekt GPO propojen s doménou, vztahuje se na všechny uživatele a počítače v této doméně. Hlavním důvodem pro propojování objektů GPO s jednou lokalitou, doménou nebo organizační jednotkou je využití normálních pravidel dědičnosti.
- Objekt GPO může být také propojen s více úrovněmi v Active Directory. Jediný objekt GPO tak může být propojen s lokalitou, doménou a několika organizačními jednotkami. V tomto případě se objekt GPO vztahuje ke všem těmto úrovním Active Directory. Hlavní motivací pro takové propojení objektů GPO na více úrovních Active Directory je vytvoření přímých asociací mezi GPO a několika lokalitami, doménami a organizačními jednotkami, bez ohledu na standardní způsob, jakým se uplatňují pravidla dědičnosti.

Propojení objektu GPO s lokalitou, doménou nebo organizační jednotkou lze také zrušit. Odstraní se tím přímé spojení mezi objektem GPO a daným uzlem v Active Directory hierarchii. Pokud je tedy například objekt GPO propojen s lokalitou Ostrava i celou doménou dmn.cz, můžete chtít odstranit propojení s doménou, a přitom je ponechat u lokality. Objekt GPO pak zůstane propojen pouze s Ostravou, ale nikoli s doménou dmn.cz. Pokud později odstraníte i propojení s lokalitou, zůstane objekt GPO zcela bez propojení. Takový objekt, který není propojen s žádným uzlem Active Directory, zůstává stále součástí systému zásad skupiny, ale není aktivován.

Připojení a práce s GPO

Při práci s konzolou Správa zásad skupiny (Group Policy Management Console, GPMC) se za normálních okolností aplikují všechny změny na tom doménovém řadiči, který hraje úlohu emulátoru PDC. Emulátor PDC se tak stává centrálním místem, na kterém vznikají a zanikají objekty GPO a dochází tam také k jejich modifikacím. Důvodem pro toto chování Active Directory je nutnost zajistit, aby se změny ve struktuře objektů GPO děly na jediném, autoritativním řadiči domény a přístup k danému objektu GPO měl vždy jen jeden správce. Role emulátoru PDC se zavádí na úrovni domény, proto je v každé doméně jen jeden takový emulátor. Tudíž existuje jen jedno rozhodující místo, na kterém se změny v zásadách odehrávají. Pokud je ve chvíli, kdy chcete měnit zásady skupiny, emulátor PDC nedostupný, dostanete výzvu, zda chcete pracovat se zásadami

na tom doménovém řadiči, ke kterému jste připojeni, nebo na některém jiném dostupném řadiči domény.

Libovolný uživatel, jenž je členem jedné ze skupin Domain Admins nebo Enterprise Admins, má oprávnění procházet a pracovat s doménovými zásadami skupiny. Narozdíl od lokálních zásad skupiny jsou tvorba a propojování doménových zásad skupiny oddělené operace. Nejprve je nutné vytvořit objekt GPO a zadat jeho předvolby a nastavení zásad, které definují požadované chování. Následuje propojení objektu GPO s uzlem či uzly v Active Directory, kde má být aplikován, čímž se objekt GPO aktivuje.

Ačkoli definice a propojování objektů GPO jsou rozdílné věci, umožňuje konzola GPMC současné vytvoření GPO a jeho propojení s doménou nebo organizační jednotkou v Active Directory. Máte tedy dvě možnosti, jak založit a propojit objekt GPO:

- Nejprve vytvoříte objekt GPO a později jej propojíte s doménou nebo organizační jednotkou v Active Directory, nebo
- v jednom kroku vytvoříte nový objekt GPO a zároveň ho propojíte s doménou nebo organizační jednotkou v Active Directory.

Propojení s lokalitou nelze provést v jednom kroku, objekt GPO již musí před propojením existovat.

Právě propojení je mechanizmem, který určuje, že předvolby a nastavení uložené v objektu GPO budou uplatněny. Předpokládejme například, že vytvoříte objekt GPO s názvem „Hlavní objekt zásad domény dmn.cz“ a propojíte ho s doménou dmn.cz. Podle standardních pravidel dědičnosti a zpracování zásad se po propojení objektu GPO s uzlem v Active Directory toto propojení zdědí i ve všech jeho poduzlech v hierarchii Active Directory a projeví se zde odpovídající nastavení zásad. Propojený objekt GPO má tedy vliv na konfiguraci počítačů i uživatelů v celém podniku, nebo jen na nějakou podmnožinu těchto počítačů a uživatelů.

Používání výchozích zásad

Od Windows 2000 platí ve všech serverových operačních systémech Windows, že doména vzniká založením doménového řadiče pro novou doménu. Typicky to probíhá tak, že se správce přihlásí k samostatnému serveru jako místní administrátor a spustí Průvodce instalací služby Active Directory Domain Services (Domain Controller Installation Wizard, DCPROMO). V něm pak uvede, že chce zřídit novou doménu nebo doménovou strukturu. Po založení nové domény a jejího řadiče jsou automaticky vytvořeny dva objekty GPO:

- **Objekt Default Domain Policy** – objekt GPO vytvořený za účelem propojení s celou doménou v Active Directory. Propojení je také automaticky provedeno. Tento objekt GPO se používá k výběru základních nastavení zásad, která se uplatní na všechny uživatele a počítače v doméně.

- **Objekt Default Domain Controllers Policy** – objekt GPO automaticky vytvořený a propojený s organizační jednotkou Domain Controllers, která se vztahuje na všechny doménové řadiče dané domény (alespoň dokud nejsou odstraněny z této organizační jednotky). Tento objekt GPO se pak používá k ovládání bezpečnostních nastavení pro doménové řadiče.

Oba tyto výchozí objekty GPO jsou nepostradatelné pro správné fungování a zpracování zásad skupiny. Standardně má objekt GPO Default Domain Policy přednost před všemi ostatními objekty propojenými s doménou, a podobně má objekt Default Domain Controllers Policy přednost před všemi ostatními objekty GPO propojenými s organizační jednotkou Domain Controllers. Jak se dozvíte dále v této sekci, účel a použití obou těchto objektů GPO jsou poněkud jiné.

Poznámka: Výchozí objekty GPO se používají pro nastavení výchozích hodnot u omezené sady nastavení zásad. Tyto objekty se však nepoužívají pro specifikaci výchozích předvoleb.

Práce s objektem Default Domain Policy

Objekt GPO Default Domain Policy je kompletním souborem, který obsahuje nastavení pro správu všech oblastí zásad. Není však míněn pro všeobecné řízení zásad skupiny. Obvyklou praxí je, že se v objektu Default Domain Policy upravují jen výchozí nastavení zásad účtů (Account policies) a tři specifické oblasti týkající se uživatelských účtů:

- **Zásady hesla (Password policy)** – určuje výchozí zásady hesel pro doménové řadiče, jako je stáří hesel a minimální délka hesel.
- **Zásady uzamčení účtů (Account lockout policy)** – stanovuje výchozí zásady pro uzamčení účtů, jako jsou doba uzamčení účtu a prahová hodnota pro uzamčení účtu.
- **Zásady modulu Kerberos (Kerberos policy)** – definuje výchozí zásady modulu Kerberos pro doménové řadiče, například maximální toleranci synchronizace hodin počítače.

Chcete-li měnit jiné oblasti zásad, měli byste nejprve vytvořit nový objekt GPO a propojit jej s doménou nebo odpovídající organizační jednotkou v doméně. Přesto existuje několik výjimek z pravidla, že objekt Default Domain Policy (nebo jiný objekt GPO s nejvyšší předností propojený s doménou) se používá jen k ovládání zásad účtů. Mezi tyto výjimky patří následující zásady, jež jsou k nalezení v Editoru správy zásad skupiny (Group Policy Management Editor) pod cestou Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Místní zásady\Možnosti zabezpečení (Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options):

- **Účty: Přejmenovat účet správce (Accounts: Rename Administrator Account)** – Přejmenovává zabudovaný účet správce Administrator na všech počítačích v celé doméně a nastavuje nový název tohoto účtu, takže je lépe chráněn před zlovolnými

uživateli. Jedná se však jen o název účtu při přihlášení, nikoli zobrazované jméno. To zůstává nastavené stále stejně, tedy například Administrátor nebo Správce, pokud jste jej takto nastavili. I kdyby správce změnil přihlašovací název účtu v aplikaci Uživatelé a počítače služby Active Directory, vrátí se při příští aktualizaci zásad skupiny tento název na hodnotu podle nastavení zásad.

- **Účty: Stav účtu správce (Accounts: Administrator Account Status)** – vynucuje zákaz zabudovaného místního účtu správce na všech počítačích v doméně. Musíte si však uvědomit, že i když je účet správce zakázán, bude přesto povolen při nastartování počítače v nouzovém režimu.
- **Účty: Stav účtu hosta (Accounts: Guest Account Status)** – vynucuje zákaz zabudovaného místního účtu hosta Guest na všech počítačích v doméně. Při zákazu účtu Guest a současném nastavení Přístup k síti: Model sdílení a zabezpečení místních účtů na Pouze účet Guest (Network Access: Sharing And security Model For Local Accounts na Guest Only) selžou všechna přihlášení k síti.
- **Účty: Přejmenovat účet hosta (Accounts: Rename Guest Account)** – Přejmenovává zabudovaný účet hosta Guest na všech počítačích v celé doméně a nastavuje nový název tohoto účtu, takže je lépe chráněn proti zlovolným uživatelům. I v tomto případě nastavení ovlivňuje jen přihlašovací název účtu, nikoli zobrazované jméno, které zůstává v původním stavu (tedy Host nebo jakkoli jinak jste toto jméno nastavili). I když správce změní přihlašovací název účtu v aplikaci Uživatelé a počítače služby Active Directory, vrátí se při příští aktualizaci zásad skupiny tento název na hodnotu podle nastavení této zásady.
- **Zabezpečení sítě: Vynutit odhlášení, pokud vyprší časový limit pro přihlášení (Network Security: Force Logoff When Logon Hours Expire)** – Způsobí odpojení uživatele od domény ve chvíli, kdy vyprší jeho platné přihlašovací hodiny. Pokud tedy například nastavíte tomuto uživateli možnost přihlášení do domény mezi osmou hodinou ráno a šestou večer, bude úderem šesté hodiny tento uživatel automaticky odhlášen.
- **Zabezpečení sítě: Neukládat hodnotu hash programu LAN Manager při příští změně hesla (Network Security: Do Not Store LAN Manager Hash Value On Next Password Change)** – Určuje, zda bude při příští změně hesla uložena hodnota hash v programu LAN Manager pro nové heslo. Tato hodnota se ukládá lokálně v databázi zabezpečení, takže kdyby byla tato databáze napadena, mohlo by být heslo ohroženo. Na Windows Vista a novějších systémech je toto ve výchozím nastavení povoleno, na Windows XP zakázáno.
- **Přístup do sítě: Povolit anonymní překlad SID/názvu (Network Access: Allow Anonymous SID/Name Translation)** – Rozhoduje, zda anonymní uživatel může požadovat atributy bezpečnostního identifikátoru (security identifier, SID) jiného uživatele. V případě, že je toto nastavení povoleno, zlovolný uživatel by mohl použít dobře známý SID správce a získat skutečný název zabudovaného účtu správce, i když byl tento účet přejmenován. Pokud je nastavení zakázáno, počítače a aplikace běžící na doménách z doby před Windows 2000 mohou být neschopné komuniko-

vat s doménami Windows Serveru 2003. Tento komunikační problém se specificky týká:

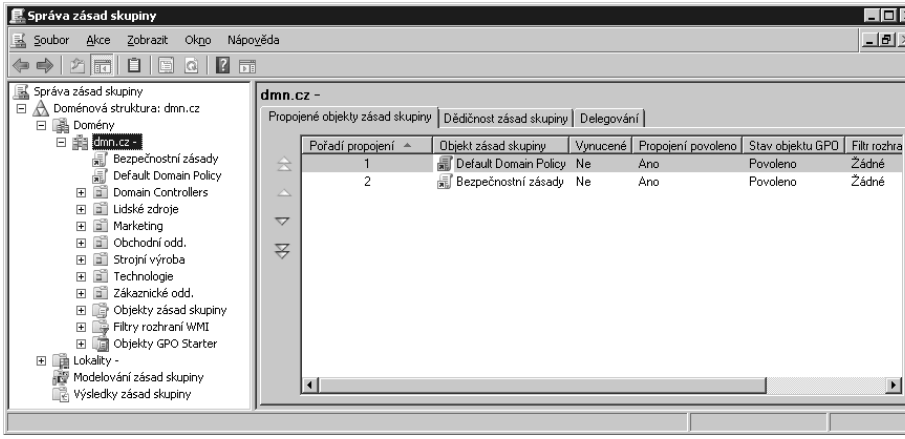
- Windows NT 4.0 serverů se službou vzdáleného přístupu (Remote Access Service)
- Microsoft SQL Serveru na počítačích s Windows NT 3.x nebo Windows NT 4.0
- Služby vzdáleného přístupu (Remote Access Service) běžící na počítačích s Windows 2000, které jsou umístěny v doménách Windows NT 3.x nebo Windows NT 4.0
- SQL Serveru běžícího na počítačích s Windows 2000, který je umístěn v doméně Windows NT 3.x nebo Windows NT 4.0
- Uživatelů v doménách Windows NT 4.0, kteří chtějí přidělit přístupová oprávnění k souborům, sdíleným složkám či objektům registru uživatelským účtům pocházejícím z domén, jež obsahují doménový řadič založený na Windows 2003 Serveru

Další výjimkou jsou certifikáty uložené jako nastavení zásad pro agenty obnovování dat v doméně. Tyto zásady jsou uloženy v cestě Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Zásady veřejných klíčů\Šifrování systému souborů (Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Encrypting File System). Typicky se tyto zásady ovládají právě v objektu GPO, který je propojen na úrovni domény a má nejvyšší prioritu. Stejně jako v případě zásad účtů je tímto objektem standardně Default Domain Policy.

Divíte se, proč je doporučenou praxí konfigurace zásad právě tímto způsobem? Nuže, když se zásady skupiny poničí a přestanou fungovat, můžete použít nástroj Dcgpofix a obnovit objekt Default Domain Policy do původního stavu (což znamená, že ztratíte veškerá vlastní nastavení, která jste v tomto objektu GPO učinili). Dále, některá nastavení zásad mohou být konfigurována pouze na úrovni domény, proto je rozumné zahrnout je do objektu Default Domain Policy (nebo do jiného objektu na úrovni domény, který má nejvyšší přednost).

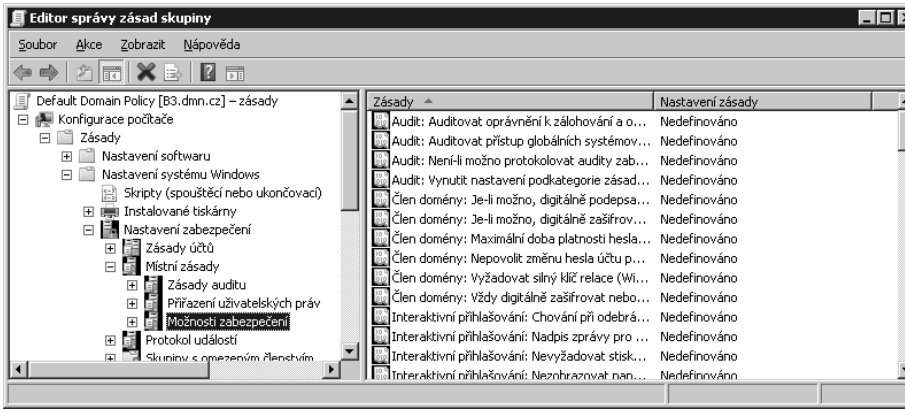
Poznámka: Sečteno a podtrženo, pokud nastavíte zásady účtu ve více objektech GPO propojených s doménou, budou tato nastavení sloučena podle pořadí propojení těchto objektů s doménou. Objekt GPO s pořadím propojení 1 bude mít vždy nejvyšší prioritu. Pořadí propojení diskutujeme v sekci „Změna pořadí propojení a priorita" v kapitole 7. Bližší informace o práci s nástrojem Dcgpofix najdete v sekci „Obnovení výchozích objektů GPO" v kapitole 8 „Údržba a obnovení zásad skupiny".

Přístup k objektu GPO Default Domain Policy získáte několika způsoby. Pokud používáte konzolu Správa zásad skupiny (GPMC), objeví se objekt Default Domain Policy po klepnutí na jméno domény ve stromu vlevo, jak ukazuje obrázek 2.3. Klepněte na uzel Default Domain Policy pravým tlačítkem a zvolte Upravit; získáte tak plný přístup k objektu GPO Default Domain Policy.



Obrázek 2.3: Přístup k objektu Default Domain Policy v konzole Správa zásad skupiny

V Editoru správy zásad skupiny, pod uzlem Konfigurace počítače (Computer Configuration), rozbalte Zásady\Nastavení systému Windows\Nastavení zabezpečení\Místní zásady (Policies\Windows Settings\Security Settings\Local Policies), jak ilustruje obrázek 2.4. Můžete pak podle potřeby pracovat s nastaveními v oblastech Zásady auditu, Přiřazení uživatelských práv a Možnosti zabezpečení.



Obrázek 2.4: Editace objektu Default Domain Policy

Práce s objektem Default Domain Controllers Policy

Objekt GPO s názvem Default Domain Controllers Policy byl navržen proto, aby bylo zaručeno shodné nastavení zabezpečení doménových řadičů v doméně. Je to důležité, protože všechny řadiče v dané doméně jsou si rovny. Kdyby měly rozdílné nastavení zabezpečení, mohly by se chovat odlišně, a to by bylo proti duchu a principu Active

Directory. Pokud jeden z doménových řadičů má specifická nastavení zásad, měla by být stejná nastavení uplatněna také na všechny ostatní řadiče v téže doméně, aby byla doména konzistentní.

Objekt Default Domain Controllers Policy je propojen s organizační jednotkou Domain Controllers. Díky tomu je aplikován na všechny doménové řadiče, dokud nejsou z této organizační jednotky vyřazeny. Ve výchozím nastavení jsou v organizační jednotce Domain Controllers automaticky všechny řadiče domény, a tak veškerá nastavení, která provedete v objektu Default Domain Controllers Policy, se standardně uplatní na všechny řadiče. Klíčové oblasti zabezpečení, které byste měli konzistentně ošetřit, obsahují:

- **Zásady auditu** – určuje výchozí zásady auditu pro doménové řadiče.
- **Přiřazení uživatelských práv** – stanovuje výchozí přiřazení uživatelských práv pro doménové řadiče.
- **Možnosti zabezpečení** – definuje výchozí možnosti zabezpečení pro doménové řadiče.

Microsoft doporučuje nedělat v objektu Default Domain Controllers Policy žádné další změny či úpravy. Mějte na paměti, že tento objekt GPO se vztahuje jen na řadiče domény, protože je propojen s organizační jednotkou Domain Controllers, a ve výchozí situaci jsou členy této organizační jednotky právě doménové řadiče.

Odstranění řadiče domény z organizační jednotky Domain Controllers může nepříznivě ovlivnit správu domény a vést k nekonzistentnímu chování v průběhu přihlášení a autentizace. Proč tomu tak je? Když přesunete nějaký doménový řadič pryč z organizační jednotky Domain Controllers, objekt Default Domain Controllers Policy se přestane na tento řadič aplikovat – pokud ovšem nepropojíte tento objekt s novou organizační jednotkou, do které jste řadič přesunuli. Dále, všechny další objekty GPO propojené s novou organizační jednotkou se začnou na řadič domény vztahovat.

Proto když se přece jen rozhodnete pro přesun doménového řadiče do jiné organizační jednotky, měli byste od té chvíle pečlivě sledovat jeho nastavení zabezpečení. Pokud totiž například učiníte změnu týkající se zabezpečení v objektu Default Domain Controllers Policy, musíte zajistit, že stejná změna bude aplikována také na ty doménové řadiče, které jsou součástí jiné organizační jednotky než Domain Controllers.

Přístup k objektu GPO Default Domain Controllers Policy získáte několika způsoby. Pokud používáte konzolu Správa zásad skupiny (GPMC), objeví se objekt Default Domain Controllers Policy po klepnutí na organizační jednotku Domain Controllers ve stromu vlevo. Klepněte na uzel Default Domain Controllers Policy pravým tlačítkem a zvolte Upravit. Získáte tak plný přístup k objektu GPO Default Domain Controllers Policy.

Z praxe: Oddělení produktové podpory firmy Microsoft neakceptuje přesunutí doménového řadiče z organizační jednotky Domain Controllers. Pokud jste tak učinili a máte potíže s doménovými řadiči, které by mohly mít souvislost s touto akcí, produktová podpora Microsoftu vás požádá o přesunutí doménového řadiče zpět do organizační jednotky Domain Controllers.

Jsou i další komponenty a produkty, které se spoléhají na to, že objekt Default Domain Controllers Policy existuje a je v doméně propojen s jejími řadiči. Například se může přihodit, že Exchange server bude hlásit chybové stavy se stížnostmi, že nemůže nalézt globální katalog. To se často děje právě proto, že nemáte objekt Default Domain Controllers Policy propojen s organizační jednotkou Domain Controllers, nebo když jste odstranili doménové řadiče z organizační jednotky Domain Controllers.

Používání nastavení a předvoleb zásad

Dosud jsme se zabývali proměnami zásad skupiny, tím, jak můžete zásady aktualizovat a jak se zásady aplikují. Zatím jsme však neuváděli postupy, kterými můžete nastavení a předvolby zásad využít k efektivnější správě sítě. Napravíme to nyní podrobným seznamem použití jak předvoleb, tak nastavení. Protože oblasti správy předvoleb a nastavení se do jisté míry překrývají, zmíníme v těchto případech také to, zda je pro daný úkon vhodnější nastavení či předvolba.

Používání nastavení zásad pro administraci

Nastavení zásad je řízené nastavení aplikovatelné na konfiguraci. Příkladem je omezení přístupu k dialogu Spustit (ke spouštění programů – dialog Run). Většina nastavení zásad má tři základní stavy:

- **Povoleno (Enabled)** – nastavení zásady je zapnuto a nastavení je aktivováno. Typicky povolujete nastavení zásady proto, že chcete danou konfiguraci vynutit. Některá nastavení zásad umožňují po povolení zadat dodatečné možnosti, které dále jemněji dolaďují aplikaci nastavení.
- **Zakázáno (Disabled)** – nastavení zásady je vypnuto a konfigurace se deaktivuje. Jedná se o vynucení stavu, kdy je nastavení vypnuto.
- **Nedefinováno (Not Configured)** – nastavení zásady se nepoužívá. Žádaná nastavení zásady nejsou aktivována ani deaktivována a cílové konfigurace nejsou touto zásadou nijak ovlivněny.

Samotné základní stavy jsou poměrně přehledné. Do hry však vstupuje dědičnost a blokování (o těchto mechanismech jsme se stručně zmínili a podrobně je probereme v kapitole 5 „Prohledávání a filtrování zásad skupiny“), což tyto stavy může ovlivnit. Když však budete mít na paměti následující dvě pravidla o dědičnosti a blokování, budete mít nakročeno na úspěšné zvládnutí zásad skupiny:

- Pokud jsou zděděná nastavení zásad striktně vynucena, nemůžete je potlačit. Zděděná nastavení jsou tedy aplikována bez ohledu na to, v jakém stavu je nastavení v aktuálním objektu GPO.
- Jestliže jsou nastavení zásad v aktuálním objektu GPO blokována a nejsou striktně vynucena, je zděděné nastavení potlačeno. Zděděné nastavení zásad tak není uplatněno a aplikuje se pouze nastavení zásad z aktuálního objektu GPO.

Když nyní přesně víte, jak se aplikují jednotlivá nastavení zásad, podívejme se na oblasti správy, ve kterých se zásady skupiny uplatňují. Prostřednictvím speciální sady zásad zvané šablony pro správu (Administrative Templates) máte možnost ovládat každý aspekt grafického rozhraní systému Windows, od nabídek přes pracovní plochu k hlavnímu panelu a další. Nastavení zásad v šabloně pro správu má vliv na vlastní nastavení registru, takže použitelné zásady jsou u místních zásad i u doménových zásad skupiny prakticky totožné. V šablonách pro správu lze ovlivnit:

- **Ovládací panely** – řízení přístupu k Ovládacím panelům a jejich volby. Lze také měnit konfiguraci komponent Přidat nebo odebrat programy, Tiskárny, Zobrazení a Místní a jazykové nastavení.
- **Plocha** – konfigurace plochy Windows, dostupnost a nastavení Active Desktop, a možnosti prohledávání Active Directory z plochy.
- **Síť** – konfigurace sítě a síťových klientů, včetně souborů offline, klienta služby DNS a síťových připojení.
- **Tiskárny** – volby zveřejnění a procházení tiskáren, ukládání do tiskových front a adresářové volby.
- **Sdílené složky** – povolení publikace sdílených složek a kořenových složek Distribuovaného systému souborů (Distributed File System, DFS).
- **Nabídka Start a Hlavní panel** – konfigurace nabídky Start a hlavního panelu, především odebíráním nebo skrýváním některých položek a možností.
- **Systém** – konfigurace zásad vztahujících se k obecným nastavením systému, diskovým kvótám, uživatelským profilům, možnostem napájení, obnově systému, hlášením chyb a dalším.
- **Součásti systému Windows** – ovládání, zda a jak lze používat rozličné komponenty systému Windows, jako jsou Prohlížeč událostí, Správce úloh a aktualizace Windows Update.

Z praxe: Další šablony pro správu týkající se Microsoft Office lze získat v Microsoft Download Center (http://download.microsoft.com). V nabídce Donwload Categories klepněte na Home & Office a hledejte v této kategorii „Office customization tool". Klepněte na odkaz pro nejnovější vydání, stáhněte a spusťte samorozbalovací program. Když budete dotázáni na přijetí licence, klepněte na Continue. Pak si budete moci vybrat cílovou složku pro příslušné soubory. Projděte si soubory, které jste právě rozbalili.

Použití šablon pro správu v konzole Správa zásad skupiny ve vašem počítači je možné tak, že zkopírujete soubory ADMX do složky %SystemRoot%\PolicyDefinitions a soubory ADML do odpovídajících jazykových podložek této složky. Chcete-li učinit nové šablony pro správu dostupné v celé doméně, zkopírujte soubory ADMX a ADML do odpovídajících složek SYSVOL na doménovém řadiči.

Tabulka 2.1 poskytuje vyčerpávající seznam oblastí správy, které lze řídit s pomocí zásad skupiny. Ať už pracujete s místními nebo doménovými zásadami skupiny, tyto oblasti jsou podobné. Můžete však docílit mnohem více s pomocí doménových zásad skupiny proto, že v rámci místních zásad skupiny nelze pracovat s vlastnostmi vyžadujícími Active Directory.

Tabulka 2.1: Klíčové oblasti správy ovladatelné nastaveními zásad skupiny

Kategorie zásad skupiny	Popis	Umístění v zásadách skupiny
Instalace ovladačů/zařízení	Konfigurace instalace ovladačů a zařízení	Konfigurace počítače\Zásady\Šablony pro správu\Systém\Instalace zařízení (Computer Configuration\Policies\Administrative Templates\System\Device Installation) Konfigurace počítače\Zásady\Šablony pro správu\Systém\Instalace ovladače (Computer Configuration\Policies\Administrative Templates\System\Drive Installation) Konfigurace uživatele\Zásady\Šablony pro správu\Systém\Instalace ovladače (User Configuration\Policies\Administrative Templates\System\Drive Installation)
Omezení pro instalaci zařízení	Omezení zařízení, která se mohou zapojit a používat	Konfigurace počítače\Zásady\Šablony pro správu\Systém\Instalace zařízení\Omezení pro instalaci zařízení (Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions)
Diskové kvóty	Konfigurace diskových kvót, a zda jsou kvóty vynucené nebo jen zaznamenané jako události nebo obojí	Konfigurace počítače\Zásady\Nastavení softwaru (Computer Configuration\Policies\Software Settings)
Agenti obnovování šifrovaných dat	Chování agentů pro obnovu šifrovaných dat a odpovídajících certifikátů pro použití v šifrovaném systému souborů	Konfigurace počítače → uživatele\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Zásady veřejných klíčů\Šifrování systému souborů (Computer → User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Encrypting File System)
Zabezpečení souborů a složek	Konfigurace bezpečnostních oprávnění pro soubory a složky	Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Systém souborů (Computer Configuration\Policies\Windows Settings\Security Settings\File System)
Přesměrování složky	Přesun uživatelských složek s kritickými daty na síťové disky, kde mohou být lépe spravovány a pravidelně zálohovány (pouze doménové zásady skupiny)	Konfigurace uživatele\Zásady\Nastavení systému Windows\Přesměrování složky (User Configuration\Policies\Windows Settings\Folder Redirection)

Kategorie zásad skupiny	Popis	Umístění v zásadách skupiny
Obecné zabezpečení počítače	Zavedení bezpečnostních nastavení pro účty, události, skupiny s omezeným členstvím, systémové služby, registr a systém souborů (v případě místních zásad skupiny lze ovládat jen zásady pro účty)	Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení (Computer Configuration\Policies\Windows Settings\Security Settings)
Prohlížení Internetu	Způsob používání prohlížeče Microsoft Internet Explorer a zavedení nastavení pro uzamčení síťového protokolu	Konfigurace počítače\Zásady\Šablony pro správu\Součásti systému Windows\Internet Explorer (Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer)
Údržba aplikace Internet Explorer	Konfigurace uživatelského rozhraní, zabezpečení, důležitých adres URL, programů, serveru proxy a další	Konfigurace uživatele\Zásady\Nastavení systému Windows\Údržba aplikace Internet Explorer (User configuration\Policies\Windows Settings\Internet Explorer Maintenance)
Zabezpečení protokolu IP (IPsec)	Ovládání zásad pro zabezpečení protokolu IP (IPsec) v režimu klienta, serveru nebo zabezpečeného serveru	Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Zásady zabezpečení protokolu IP (Computer Configuration\Policies\Windows Settings\Security Settings\IP security Policies)
Místní zásady zabezpečení	Zásady pro audit, přiřazení uživatelských práv a uživatelských privilegií	Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Místní zásady (Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies)
Soubory offline	Určení, zda a případně jak se mohou používat soubory offline	Konfigurace počítače → uživatele\Zásady\Šablony pro správu\Síť\Soubory offline (Computer → User Configuration\Policies\Administrative Templates\Network\Offline Files)
Technologie QoS založená na zásadách	Řízení síťového provozu se zajištěním kvality služby pro kritické aplikace	Konfigurace počítače → uživatele\Zásady\Nastavení systému Windows\Technologie QoS založená na zásadách (Computer → User Configuration\Policies\Windows Settings\Policy-based QoS)
Možnosti spotřeby a napájení	Řízení plánu a nastavení spotřeby pro zařízení (Windows Vista a novější)	Konfigurace počítače → uživatele\Zásady\Šablony pro správu\Systém\Řízení spotřeby (Computer → User Configuration\Policies\Administrative Templates\System\Power Management)
Instalace tiskáren	Konfigurace tiskáren, které lze používat (Windows Vista a novější)	Konfigurace uživatele\Zásady\Nastavení systému Windows\Instalované tiskárny (User Configuration\Policies\Windows Settings\Deployed Printers)
Zabezpečení veřejnými klíči	Konfigurace zásad pro veřejné klíče, jejich automatický zápis (enrollment), šifrování systému souborů (EFS), důvěryhodnost v rozlehlé síti a další	Konfigurace počítače → uživatele\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Zásady veřejných klíčů (Computer → User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies)
Zabezpečení registru	Nastavení přístupových oprávnění ke klíčům registru	Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Registr (Computer Configuration\Policies\Windows Settings\Security Settings\Registry)

Kategorie zásad skupiny	Popis	Umístění v zásadách skupiny
Skupiny s omezeným členstvím	Omezuje členství ve skupinách v doméně i na místním počítači	Konfigurace počítače → uživatele\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Skupiny s omezeným členstvím (Computer → User Configuration\Policies\Windows Settings\Security Settings\Restricted Groups)
Skripty	Konfigurace spouštěcích a ukončovacích skriptů pro počítače a přihlašovacích a odhlašovacích skriptů pro uživatele	Konfigurace počítače → uživatele\Zásady\Nastavení systému Windows\Skripty (Computer → User Configuration\Policies\Windows Settings\Scripts)
Instalace softwaru	Ovládání automatické instalace nového softwaru a nových verzí a aktualizací softwaru (pouze doménové zásady skupiny)	Konfigurace počítače → uživatele\Zásady\Nastavení softwaru\Instalace softwaru (Computer → User Configuration\Policies\Software Settings\Software Installation)
Omezení softwaru	Omezení softwaru, který může být nainstalován a používán (místní zásady skupiny nepodporují omezení softwaru pro uživatele, pouze pro počítače)	Konfigurace počítače → uživatele\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Zásady omezení softwaru (Computer → User Configuration\Policies\Windows Settings\Security Settings\Software Restriction Policies)
Nabídka Start	Definice dostupných možností a chování nabídky Start	Konfigurace uživatele\Zásady\Šablony pro správu\Nabídka Start a Hlavní panel (User Configuration\Policies\Administrative Templates\Start Menu And Taskbar)
Systémové služby	Konfigurace počátečního stavu služeb po startu systému a přístupových oprávnění k nim	Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Systémové služby (Computer Configuration\Policies\Windows Settings\Security Settings\System Services)
Pevná síť (IEEE 802.3)	Správa zásad pevné sítě, zejména autentizačních metod a režimů, které se uplatňují na klienty pevné sítě (pouze doménové zásady skupiny). Může se používat i pro ověření platnosti certifikátů serveru, povolení kontrol součásti Quarantine, vynucení pokročilých nastavení 802.1X a povolení mechanismu jednotného přihlášení (single sign on, SSO)	Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Zásady pevné sítě (Computer Configuration\Policies\Windows Settings\Security Settings\Wired Network Policies)
Bezdrátová síť (IEEE 802.11)	Konfigurace zásad bezdrátové sítě, zejména přístupových bodů, bezdrátových klientů a upřednostňovaných sítí (pouze doménové zásady skupiny). Může sloužit i k zadání povolených a zakázaných typů připojení.	Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Zásady bezdrátové sítě (Computer Configuration\Policies\Windows Settings\Security Settings\Wireless Network Policies)

Používání předvoleb zásad pro administraci

Předvolba zásad skupiny je jednorázové nastavení, kterým se nastavuje volba nebo konfigurace před jejím použitím pro uživatele. Příkladem je mapování síťové jednotky na místní jednotku. Většina předvoleb zásad vzniká jednou ze čtyř následujících metod:

- **Vytvořit (Create)** – vytvoří předvolbu pouze v případě, že již předvolba neexistuje.
- **Nahradit (Replace)** – odstraní předvolbu, pokud existuje, a pak ji vytvoří, nebo ji jen vytvoří, pokud neexistuje.
- **Aktualizovat (Update)** – změní předvolbu, pokud již existuje, jinak ji vytvoří.
- **Odstranit (Delete)** – odstraní předvolbu, pokud existuje.

Stejně jako v případě stavů nastavení zásad jsou tyto akce samotné poměrně zřejmé. Mohou však být ovlivněny dědičností a blokováním. Abyste se lépe orientovali v dědičnosti a blokování, pamatujte si, že:

- Pokud jsou zděděné předvolby zásad striktně vynuceny, nemůžete je potlačit. Zděděné předvolby jsou tedy aplikovány bez ohledu na to, v jakém stavu je předvolba v aktuálním objektu GPO.
- Jestliže jsou předvolby zásad v aktuálním objektu GPO blokovány a nejsou striktně vynuceny, je zděděná předvolba potlačena. Zděděná předvolba zásad tak není uplatněna a aplikuje se pouze předvolba zásad z aktuálního objektu GPO.

Narozdíl od nastavení zásad, předvolby zásad se používají pouze v prostředí domény. Pokud tedy pracujete s doménovými zásadami skupiny, máte k dispozici předvolby zásad uvedené v tabulce 2.2.

Tabulka 2.2: Klíčové oblasti správy ovladatelné předvolbami zásad skupiny

Konfigurační oblast	Soustřeďuje tvorbu, nahrazování, aktualizaci a odstraňování:	Umístění v zásadách skupiny
Aplikace	Nastavení aplikací, je dostupné po instalaci předvoleb pro některou aplikaci	Konfigurace uživatele\Předvolby\Nastavení systému Windows\Aplikace (User Configuration\Preferences\Windows Settings\Applications)
Zdroje dat	Zdroje dat ODBC	Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Zdroje dat (Computer → User Configuration\Preferences\Control Panel Settings\Data Sources)
Zařízení	Systémová zařízení, včetně USB portů, disketových jednotek a vyměnitelných médií	Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Zařízení (Computer → User Configuration\Preferences\Control Panel Settings\Devices)
Mapování jednotek	Síťové jednotky mapované na místní jednotky písmenem	Konfigurace uživatele\Předvolby\Nastavení systému Windows\Mapování jednotek (User Configuration\Preferences\Windows Settings\Drive Maps)
Prostředí	Systémové a uživatelské proměnné prostředí	Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Prostředí (Computer → User Configuration\Preferences\Windows Settings\Environment)

Konfigurační oblast	Soustřeďuje tvorbu, nahrazování, aktualizaci a odstraňování:	Umístění v zásadách skupiny
Soubory	Soubory mohou být kopírovány ze zdrojového do cílového umístění	Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Soubory (Computer → User Configuration\Preferences\Windows Settings\Files)
Soubory INI	Hodnoty obsažené v souborech s příponou .ini	Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Soubory INI (Computer → User Configuration\Preferences\Windows Settings\Ini Files)
Složky	Složky na určitém místě v systému souborů	Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Složky (Computer → User Configuration\Preferences\Windows Settings\Folders)
Místní uživatelé a skupiny	Uživatelské účty a jejich skupiny pro místní počítač	Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Místní uživatelé a skupiny (Computer → User Configuration\Preferences\Control Panel Settings\Local Users And Groups)
Možnosti sítě	Virtuální privátní sítě a vytáčení připojení k síti	Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Možnosti sítě (Computer → User Configuration\Preferences\Control Panel Settings\Network Options)
Sdílené síťové složky	Sdílené složky, skryté sdílené složky a administrativní sdílené složky	Konfigurace počítače\Předvolby\Nastavení systému Windows\Sdílené síťové složky (Computer Configuration\Preferences\Windows Settings\Network Shares)
Tiskárny	Konfigurace a mapování tiskáren	Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Tiskárny (Computer → User Configuration\Preferences\Control Panel Settings\Printers)
Registr	Klíče a hodnoty registru	Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Registr (Computer → User Configuration\Preferences\Windows Settings\Registry)
Naplánované úlohy	Úlohy naplánované pro automatické spuštění	Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Naplánované úlohy (Computer → User Configuration\Preferences\Control Panel Settings\Scheduled Tasks)
Služby	Systémové služby	Konfigurace počítače\Předvolby\Nastavení ovládacích panelů\Služby (Computer Configuration\Preferences\Control Panel Settings\Services)
Zástupci	Zástupci pro objekty systému souborů, adresy URL nebo skripty	Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Zástupci (Computer → User Configuration\Preferences\Windows Settings\Shortcuts)

Prostřednictvím zvláštních předvoleb pro Ovládací panely je možné řídit různé aspekty grafického uživatelského rozhraní Windows. Tyto speciální předvolby slouží k ovládání těchto položek:

- Možnosti složky, které odpovídají volbám dostupným v dialogu Možnosti složky v Ovládacích panelech. Jsou umístěny pod Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Možnosti složky (Computer → User Configuration\Preferences\Control Panel Settings\Folder Options).

- Nastavení Internetu, ekvivalent dialogu Možnosti Internetu z Ovládacích panelů. Naleznete jej pod Konfigurace uživatele\Předvolby\Nastavení ovládacích panelů\Možnosti Internetu (User Configuration\Preferences\Control Panel Settings\Internet Settings).
- Možnosti napájení, jež jsou totožné se stejnojmenným panelem v Ovládacích panelech. Hledejte v cestě Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Možnosti napájení (Computer → User Configuration\Preferences\Control Panel Settings\Power Options).
- Místní nastavení, ve kterém lze konfigurovat totéž jako v položce Místní a jazykové nastavení Ovládacích panelů. K nalezení pod Konfigurace uživatele\Předvolby\Nastavení ovládacích panelů\Místní nastavení (User Configuration\Preferences\Control Panel Settings\Regional Options).
- Nabídka Start, funkčně odpovídá dialogu Vlastnosti nabídky Start. Je umístěna v cestě Konfigurace uživatele\Předvolby\Nastavení ovládacích panelů\Nabídka Start (User Configuration\Preferences\Control Panel Settings\Start Menu).

Výběr mezi předvolbou a nastavením zásad

Některé oblasti správy se překrývají a může se stát, že některý úkol máte možnost splnit více než jedním způsobem. Například je možné s pomocí nastavení zásad určit přihlašovací skripty, které by se měly používat. V těchto skriptech pak provedete mapování síťových sdílených složek, konfiguraci tiskáren a vytvoření zástupců, zkopírujete soubory a složky a zajistíte další úkony. Avšak s předvolbami zásad byste mohli zařídit totéž, aniž byste se museli zabývat přihlašovacími skripty. Který způsob tedy použít? Pravda je taková, že neexistuje jediná správná odpověď. Záleží na tom, čeho chcete docílit. V následujícím textu popíšeme základní návod pro některé oblasti, ve kterých se předvolby a nastavení zásad překrývají.

Z praxe: Když se v jednom konkrétním objektu GPO vyskytne konflikt mezi nastavením zásad a předvolbami zásad, obvykle vítězí nastavení zásad umístěné v registru. V případě střetu mezi nastavením zásad, které není založeno na registru, a předvolbou zásad dostane přednost naposledy zapsaná hodnota. (Pořadí je určeno podle toho, jak se zpracovávají klientská rozšíření pro nastavení a předvolby zásad.) Zjistit, zda nějaké nastavení zásad používá registr, je snadné. Všechna nastavení zásad založená na registru jsou definována v šablonách pro správu.

Ovládání instalace zařízení

Prostřednictvím nastavení zásad můžete ovlivňovat instalaci zařízení a vynutit jistá omezení. Cílem je zabránit uživatelům v instalaci specifického typu hardwarového zařízení. Můžete říci, že jisté prověřené zařízení může být nainstalováno (podle hardwarového identifikátoru zařízení). Lze také zakázat instalaci konkrétného neprověřeného zařízení (opět na základě hardwarového identifikátoru). Tato nastavení zásad se uplatní pouze na Windows Vista a novějších a nacházejí se v Konfigurace počítače\Zásady\Šab-

lony pro správu\Systém\Instalace zařízení\Omezení pro instalaci zařízení (Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions).

Zatímco omezení blokují instalaci nového zařízení nebo předchází dalšímu připojení zařízení, které bylo odpojeno, nezabrání v používání existujícího zařízení. Proč? Ovladače zařízení jsou již nainstalovány a zařízení je již dostupné, a jelikož zařízení ani jeho ovladač nejsou znovu zkontrolovány, pokračuje nerušeně v práci.

S pomocí předvoleb zásad lze zakázat třídy zařízení, jednotlivá zařízení, třídy portů, individuální porty, ale nemůžete zabránit ovladači, aby se nahrál do paměti. Zařízení se zakazují zvolením třídy zařízení nebo konkrétního zařízení na počítači již nainstalovaného. Podobně port nebo třídu portů lze zakázat, když už je na počítači funkční. Odpovídající předvolby najdete pod Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Zařízení (Computer → User Configuration\Preferences\Control Panel Settings\Device).

I když prostřednictvím předvoleb zakážete zařízení a porty, nedojde tímto způsobem k zabránění v instalaci ovladače. Navíc uživatel s příslušnými oprávněními může příslušná zařízení a porty ve Správci zařízení opět povolit. Standardně však systém zásad skupiny aktualizuje předvolby stejně jako nastavení zásad v pravidelném intervalu, předvolba bude proto znovu uplatněna po uplynutí tohoto intervalu. Takže pokud u předvolby zvlášť neuvedete, že má být aplikována jen jednou, bude tato předvolba znovu uplatněna každých 90 až 120 minut.

Když nyní víte, jak obě technologie fungují, bude nejlepší řešení záviset na tom, čeho chcete dosáhnout. Jestliže máte v úmyslu kompletně zablokovat a nedovolit instalaci ani používání jistých zařízení, budete možná potřebovat kombinovat nastavení i předvolby zásad. Nastavení zásad zabrání instalaci specifických zařízení, pokud již nebyla nainstalována. Předvolby zásad pak zajistí, že již nainstalovaná zařízení nebudou moci být využívána. Musíte však předtím mít dané zařízení nainstalované na počítači, ze kterého systém spravujete, aby mohlo být vybráno.

Nakonec je důležité poukázat na to, že zmíněná nastavení zásad jsou platná jen pro Windows Vista a novější. Naopak odpovídající předvolby zásad se uplatní na libovolný počítač, na němž jsou nainstalována klientská rozšíření pro předvolby zásad skupiny.

Ovládání souborů a složek

Prostřednictvím nastavení zásad je možné řídit přístupová oprávnění k souborům a složkám. Účelem je zavést pro důležité soubory a složky specifické seznamy přístupových oprávnění (Access Control List, ACL). Tyto soubory a složky však musí na cílovém počítači již existovat, jinak nemohou být oprávnění uplatněna. Příslušná nastavení zásad najdete v cestě Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Systém souborů (Computer Configuration\Policies\Windows Settings\Security Settings\File System) a aplikují se na všechny počítače podporující zásady skupiny.

Předvolby zásad slouží ke správě souborů a složek. Přitom předvolby pro soubory fungují jinak než předvolby pro složky; je možné vytvářet, aktualizovat nebo nahrazovat soubory na cílovém počítači jejich zkopírováním ze zdrojové stanice. Stejně tak lze soubor na cílovém počítači smazat. Složky na jistém místě cílového počítače je možné vytvořit, aktualizovat, nahradit nebo odstranit. Pro tyto operace můžete navíc určit, zda mají být existující soubory a podsložky smazány.

Předvolby pro soubory a složky se uplatní na počítačích, které jsou vybaveny klientským rozšířením pro předvolby zásad skupiny. Odpovídající předvolby pro soubory najdete v Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Soubory (Computer → User Configuration\Preferences\Windows Settings\Files), zatímco předvolby složek hledejte v cestě Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Soubory (Computer → User Configuration\Preferences\Windows Settings\Files).

Tip: Zásady skupiny obsahují také speciální předvolby pro soubory INI a zástupce. Předvolby pro soubory INI se omezují na změny hodnot pro určené vlastnosti v jisté sekci souboru INI. Předvolby pro zástupce poskytují možnost vytvářet na jistém místě, například na Ploše, zástupce souborů, složek, adres URL a skriptů.

V případě souborů a složek vám kombinace nastavení a předvoleb přinese to nejlepší z obou kategorií. S pomocí předvoleb máte k dispozici snadný mechanismus pro kopírování souborů mezi počítači a práci se složkami. Nastavení zásad zase poskytují jednoduchý způsob aplikace požadovaných bezpečnostních opatření. Navíc, předvolby pro soubory a složky budete možná chtít aplikovat jen jednou. Jinak by při každé aktualizaci zásad skupiny mohly být operace typu vytvoření, změna, nahrazení nebo smazání souboru či složky zopakovány, a to nemusí být žádoucí.

Ovládání aplikace Internet Explorer

Systém zásad skupiny nabízí širokou sadu nastavení a předvoleb pro aplikaci Internet Explorer. Na tomto poli je tolik možností, že dokonce mnozí experti si nejsou vždy jisti, co která z nich znamená. Je důležité se soustředit na toto:

- Nastavení zásad pod Konfigurace počítače\Zásady\Šablony pro správu\Součásti systému Windows\Internet Explorer (Computer Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer) slouží především k ovládání chování aplikace Internet Explorer. Tato nastavení řídí bezpečnostní doplňky prohlížeče a umožňují blokovat jisté bezpečnostní zóny Internetu.
- Naproti tomu nastavení zásad v sekci Konfigurace uživatele\Zásady\Nastavení systému Windows\Údržba aplikace Internet Explorer (User configuration\Policies\Windows Settings\Internet Explorer Maintenance) se používá ke specifikaci důležitých adres URL, jako jsou domovská stránka, poskytovatel hledání, podpora, oblíbené položky a odkazy. Je zde také možné změnit uživatelské rozhraní

prohlížeče Internet Explorer, lze přidat vlastní logo, titulky, tlačítka, zavést výchozí hodnoty pro programy, nastavení proxy serveru a další.

- Předvolby v cestě Konfigurace uživatele\Předvolby\Nastavení ovládacích panelů\Nastavení Internetu (User Configuration\Preferences\Control Panel Settings\Internet Settings) umožňují nakonfigurovat možnosti dostupné v ovládacím panelu Možnosti Internetu (který obsahuje prakticky všechny uživatelsky nastavitelné volby prohlížeče).

Již víte, že nastavení zásad je vynutitelné, zatímco předvolby zásad se vynutit nedají. Budete tedy chtít použít nastavení zásad vždy, když mají být volby prohlížeče Internet Explorer prosazeny třeba proti vůli uživatelů. Přestože všechny konfigurační možnosti prohlížení Internetu je možné ovládat i s pomocí předvoleb, nejsou vynuceny a uživatelé je mohou změnit. To mějte na paměti, když budete aplikovat předvolby jako součást standardní aktualizace systému zásad skupiny; uživateli bude změněná konfigurace vždy znovu přepsána vašimi předvolbami.

K přizpůsobení prohlížeče Internetu používejte nastavení zásad v sekci Údržba aplikace Internet Explorer (Internet Explorer Maintenance). Tato nastavení dovolují měnit adresu URL domovské stránky, adresu poskytovatele hledání, adresu pro podporu, oblíbené položky a odkazy. Můžete zde také ovlivnit vzhled prohlížeče, zejména vlastní logo, titulky a tlačítka.

Ovládání možností napájení

Když chcete řídit s pomocí zásad možnosti napájení, volba mezi nastaveními a předvolbami zásad je snadná: pro Windows Vista a novější použijete nastavení zásad, zatímco pro Windows XP předvolby zásad.

Nastavení zásad napájení pro Windows Vista a novější najdete pod Konfigurace počítače → uživatele\Zásady\Šablony pro správu\Systém\Řízení spotřeby (Computer → User Configuration\Policies\Administrative Templates\System\Power Management).

Předvolby zásad napájení pro Windows XP jsou k dispozici v cestě Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Možnosti napájení (Computer → User Configuration\Preferences\Control Panel Settings\Power Options).

Ovládání tiskáren

S pomocí nastavení zásad lze zavést tiskárny na počítače podporující zásady skupiny, ať už jsou založeny na jakékoli verzi Windows. Touto technologií nastavíte připojení ke sdílené tiskárně, která je již funkční.

Pro instalaci tiskárny na počítače se systémem Windows Vista a novějším máte k dispozici nastavení pod Konfigurace uživatele\Zásady\Nastavení systému Windows\Instalované tiskárny (User Configuration\Policies\Windows Settings\Deployed Printers). V případě dřívějších verzí Windows probíhá instalace tiskárny přes zásady skupiny

zavedením programu PushPrinterConnection.exe jako přihlašovacího skriptu uživatele nebo spouštěcího skriptu počítače.

Předvolby zásad dovolují tiskárny mapovat a konfigurovat. Mezi předvolbami jsou možnosti konfigurace místní tiskárny i tiskáren na síti TCP/IP nebo sdílených z jiného počítače. Takové předvolby zásad se uplatní na všech počítačích, kde jsou nainstalována klientská rozšíření pro předvolby zásad skupiny.

Jelikož předvolby pro tiskárny jsou mnohem univerzálnější než odpovídající nastavení zásad, budete pravděpodobně dávat přednost předvolbám. Přesto pokud jste už zavedli konfiguraci tiskáren a použili jste k tomu nastavení zásad, není nutné ihned přecházet na předvolby a instalaci tiskáren měnit.

Ovládání klíčů a hodnot registru

Součástí nastavení zásad jsou přístupová oprávnění ke klíčům registru. Umožňují zavést pro významné klíče registru seznamy přístupových oprávnění. Aby se tento bezpečnostní mechanismus mohl uplatnit, musí na cílových počítačích již příslušné klíče existovat. Tato nastavení se aplikují na jakýkoli počítač podporující zásady skupiny a najdete je pod Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Registr (Computer Configuration\Policies\Windows Settings\Security Settings\Registry).

S pomocí předvoleb lze vytvářet, aktualizovat, nahrazovat a rušit klíče registru. Odpovídající předvolby jsou umístěny v cestě Konfigurace počítače → uživatele\Předvolby\Nastavení systému Windows\Registr (Computer → User Configuration\Preferences\Windows Settings\Registry). Ačkoli prostřednictvím předvoleb lze zcela ovládat prakticky jakýkoli klíč registru, rozsáhlé řízení obsahu registru předvolbami je kontraproduktivní. Proč? Nastavení zásad definovaná v šablonách pro správu nastavují hodnoty za vás, takže nemusíte modifikovat registr přímo. Ke změnám nastavení registru pro jiné aplikace slouží instalace dodatečných šablon pro správu. Pokud pro jistou aplikaci nejsou šablony dostupné, můžete si vytvořit vaše vlastní přizpůsobené šablony pro správu a ovládat jimi registr vaší aplikace.

Protože obě metody mají protikladné zaměření, doporučujeme používat předvolby zásad jen pro jednotlivé klíče registru a v omezené sadě situací. Jestliže pracujete s velkým množstvím klíčů, měli byste vzít zavděk již existující šablonou pro správu nebo zvážit vytvoření vašich vlastních šablon. Když už v případě registru zvolíte předvolby zásad, zamyslete se nad jejich aplikací pouze jedinkrát. Jinak by při každé aktualizaci zásad skupiny mohly být operace typu vytvoření, změna, nahrazení nebo smazání klíče registru zopakovány, a to nemusí být žádoucí.

Ovládání nabídky Start

Když přijde na nabídku Start, existuje mezi tím, jaké konfigurace lze zajistit nastaveními a předvolbami zásad, značný překryv. Navíc nastavení a předvolby zásad pracují s nabídkou Start mnoha různými způsoby.

S nastaveními zásad ovlivníte položky dostupné v nabídce Start a nadefinujete chování rozličných voleb této nabídky. Více než 70 nastavení v sekci Konfigurace uživatele\Zásady\Šablony pro správu\Nabídka Start a Hlavní panel (User Configuration\Policies\Administrative Templates\Start Menu And Taskbar) vám dává velký prostor. Můžete například uvést, že chcete vyčistit historii nedávno otevřených dokumentů ve chvíli, kdy se uživatel odhlásí, nebo že přetažení a upuštění položky je v nabídce Start zakázáno. Lze také uzamknout hlavní panel, odstranit systémové ikony a vypnout oznámení.

Předvolby zásad pracující s nabídkou Start se nacházejí pod Konfigurace uživatele\Předvolby\Nastavení ovládacích panelů\Nabídka Start (User Configuration\Preferences\Control Panel Settings\Start Menu). Tyto předvolby určují možnosti a chování nabídky Start stejně, jako byste to dělali v dialogu Vlastnosti Hlavního panelu a Nabídky Start. Máte k dispozici nabídku Start i klasickou nabídku Start, nejsou zde však žádné možnosti pro konfiguraci hlavního panelu.

Ovládání systémových služeb

Při zvažování, zda pro systémové služby využít nastavení nebo předvolby zásad, je výběr snadný. Nastavení zásad slouží ke:

- Konfiguraci typu spouštění služby
- Specifikaci přístupových oprávnění pro službu (ta řídí, kdo může spouštět, zastavovat a pozastavovat danou službu)

Nastavení zásad pro služby jsou umístěna pod Konfigurace počítače\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Systémové služby (Computer Configuration\Policies\Windows Settings\Security Settings\System Services).

Předvolby zásad jsou u služeb použitelné ke:

- Konfiguraci typu spouštění služby
- Konfiguraci akce služby, která je použitelná pro spuštění zastavené služby, zastavení spuštěné služby nebo k zastavení a restartování služby
- Uvedení účtu, pod nímž služba běží, a nastavení hesla tohoto účtu
- Specifikaci akcí obnovení, které určují, jak služba reaguje na selhání

Předvolby zásad pro služby najdete v sekci Konfigurace počítače\Předvolby\Nastavení ovládacích panelů\Služby (Computer Configuration\Preferences\Control Panel Settings\Services).

Nastavení zásad je vynutitelné, ale předvolby zásad se vynutit nedají. Jakmile má být typ spouštění služby či přístupových práv ke službě prosazen proti vůli uživatelů, zvolíte nastavení zásad. Přestože konfigurační možnosti služeb je možné ovládat i s pomocí předvoleb, nejsou vynuceny a uživatelé je mohou změnit. Když však budete aplikovat předvolby jako součást standardní aktualizace systému zásad skupiny, bude uživateli změněná konfigurace vždy znovu přepsána vašimi předvolbami.

Ovládání uživatelů a skupin

Ani v případě uživatelských účtů a jejich skupin není volba mezi nastaveními a předvolbami zásad nic těžkého. Nastavení zásad se dá použít pro omezení členství ve skupině definované buď v Active Directory, nebo na místním počítači. Pro danou skupinu lze uvést její členy a zároveň ty skupiny, jichž je daná skupina členem. Odpovídající nastavení máte k dispozici pod Konfigurace počítače → uživatele\Zásady\Nastavení systému Windows\Nastavení zabezpečení\Skupiny s omezeným členstvím (Computer → User Configuration\Policies\Windows Settings\Security Settings\Restricted Groups).

Předvolby zásad slouží k vytváření, aktualizaci a rušení uživatelských účtů a skupin na místním počítači. S místními účty lze provádět také tyto akce:

- Přejmenování existujícího uživatelského účtu
- Nastavení hesla účtu
- Specifikace možností účtů

Možnosti účtu nabízejí vyžadování změny hesla při příštím přihlášení, zablokování účtu nebo nastavení vypršení platnosti účtu.

S místními skupinami jsou k dispozici následující operace:

- Přejmenování existující skupiny
- Přidání nebo odebrání aktuálního účtu jako člena skupiny
- Odebrání člena skupiny, ať už se jedná o účet nebo skupinu

Předvolby zásad týkající se uživatelských účtů a skupin se nachází v sekci Konfigurace počítače → uživatele\Předvolby\Nastavení ovládacích panelů\Místní uživatelé a skupiny (Computer → User Configuration\Preferences\Control Panel Settings\Local Users And Groups).

ČÁST II

Ovládání zásad skupiny

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