ADMINISTRACE

CHARLIE RUSSEL, SHARON CRAWFORD

MICROSOFT® WINDOWS SERVER 2008

VELKÝ PRŮVODCE ADMINISTRÁTORA

KOMPLETNÍ ZDROJ INFORMACÍ PRO PROFESIONÁLNÍ SPRÁVCE

INSTALACE A KONFIGURACE ROLÍ A JÁDRA SERVERU

SPRÁVA UŽIVATELŮ, SKUPIN, ZÁSAD SKUPINY A ACTIVE DIRECTORY

VIRTUALIZACE POMOCÍ HYPER-V

DOKONALÉ VYUŽITÍ REGISTRU A SKRIPTŮ

CPRESS Microsoft

Charlie Russel, Sharon Crawford

Microsoft Windows Server 2008
Velký průvodce administrátora

Computer Press, a. s.
Brno
2009

Microsoft Windows Server 2008
Velký průvodce administrátora

Charlie Russel, Sharon Crawford

Computer Press, a. s., 2009. Vydání první.

Překlad: Pavel Vaida, Pavel Paloncý, Jakub Hegenbart
Odborná korektura: Martin Babarík
Jazyková korektura: Alena Láníčková, Petra Láníčková
Vnitřní úprava: Jiří Matoušek
Sazba: Vladimír Ludva
Rejstřík: René Kašík

Obálka: Martin Sodomka
Komentář na zadní straně obálky: Libor Pácl
Technická spolupráce: Zuzana Šindlerová
Odpovědný redaktor: Libor Pácl
Technický redaktor: Jiří Matoušek
Produkce: Daniela Nečasová

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

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

ISBN 978-80-251-2115-3
Prodejní kód: K1608
Vydalo nakladatelství Computer Press, a. s., jako svou 3180. publikaci.

Stručný obsah

ČÁST V

Použití podpůrných služeb a funkcí

ČÁST VI

Ladění, údržba a oprava

Obsah

ČÁST II

Instalace a konfigurace

Poděkování

Žádná kniha takového rozsahu nevzejde jen z rukou autorů. Jsme velice zavázáni mnoha lidem pro jejich úsilí, kterým nám pomohli k úspěchu.

Roger Benes ze společnosti Microsoft v Kanadě hrál klíčovou a velmi cennou roli při navazování důležitých kontaktů – a kromě toho je to dobrý přítel.

Také jsme zavázáni Marku Dikinsonovi (rovněž ze společnosti Microsoft v Kanadě), který v navazování kontaktů učinil další krok, i Sashovi Krsmanovicovi, který byl k dispozici vždy, když jsme potřebovali odpověď.

Sestavení a spuštění hardwaru, který odvede svou práci při tvorbě takovéto knihy, je výzvou i při dnešních možnostech virtualizace. Společnost Hewlett-Packard v Kanadě byla natolik štědrá, že nám zapůjčila skvělý, plně vybavený server ML350G5. Jsme zavázáni i mnoha dalším: Gordonu Pellosovi a Alanu Rogersovi ze společnost HP v Kanadě, SanSanu Strozierovi z HP ve Spojených Státech, Sharon Fernandezové z Hill & Knowleton (což je firma pro komunikaci s veřejností společnosti HP, a hlavně Davidu Chinovi, také z firmy Hill & Knowleton) za umožnění zápůjčky a štědrost při nakládání s jeho časem a odborností.

Také jsme použili další vynikající server Hewlett-Packard DL380G5, a to díky Gregu Rankichovi ze společnosti Xtreme Consulting Group, Inc. a Danu Coxovi ze společnosti Hewlett-Packard v USA. Velmi si vážíme jejich pomoci.

Vytváření a testování úložišť Storage Area Networks (SAN) je bez SAN poněkud obtížné, děkujeme tedy Dylanu Locsinovi a Chrisi Carrierovi z firmy EqualLogic za velkorysé zapůjčení pole SAN PS3800XV. Je to výborně sestavené a výkonné úložiště SAN, které nám dobře posloužilo, a jsme za tuto pomoc velice vděční.

Všechny snímky obrazovek v této knize byly pořízeny pomocí programu HyperSnap firmy Hyperionics. Tvorba snímků obrazovek byla zvláštní výzvou zejména u jádra serveru, ale Greg Kochiniak z Hyperionics pro nás vytvořil pro jádro serveru zvláštní verzi HyperSnapu. Tomu se říká zákaznická podpora!

Při tvorbě této knihy jsme využili také pomoci dalších odborníků. Konkrétně pro tři kapitoly o bezpečnosti to byla Susan Bradley, držitelka ocenění Microsoft MVP a soudní účetní. Její pomoc byla neocenitelná, a navíc dodržovala termíny. Čtvrtá kapitola o bezpečnosti byla napsána Danou Epp, držitelkou ocenění MVP za oblast bezpečnosti a vývojářkou z firmy AuthAnvil, což je naše oblíbené řešení pro ověřování. Kapitola o clusterování je v prvé řadě prací Marka Coopera z Microsoftu; odvedl vynikající práci. Pro kapitoly týkající se Active Directory jsme nemohli mít lepšího autora než Stana Reimera, který souhlasil s téměř nesplnitelným termínem, dodržel jej, a navíc odvedl kvalitní práci. Marco Shaw, další MVP za oblast AdminFrameworks, ví o PowerShellu více, než my kdy vědět budeme, a přispěl do této knihy kapitolou o skriptování. Kurt Dillard odvedl vynikající práci na kapitole věnované IIS.

Velmi si vážíme skvělých lidí, díky kterým byla práce s Microsoft Learning skutečným potěšením. Počínaje Martinem DelRe, kterého známe již po mnoho let a který nás skutečně zachránil, když jsme ke konci potřebovali pomoc. Díky, Martine. Jsi skutečný pro-

fesionál. Redaktorem našeho projektu byla Melissa von Tschudi-Sutton, s níž byla radost spolupracovat během celého dlouhého procesu tvorby. Tato kniha je již druhou, na které jsme s Melissou pracovali, a doufáme, že není poslední. Hluboce si vážíme Melissina entuziasmu, zpětné vazby, nadhledu a trpělivosti. Zejména tu jsme občas zkoušeli velmi intenzivně.

Naším technickým redaktorem byl Randall Galloway a velmi oceňujeme jeho úsilí a komentáře v průběhu práce. Také náš indexer v Hyde Park Publishing Services a sazeč v Custom Editorial Productions, Inc. odvedli skvělou práci. Redakční tým Megan Smith-Creedové a Becky McKay provedl pečlivé a citlivé úpravy, za které jsme velice vděční. A nakonec bychom chtěli poděkovat i všem lidem v produkci i v oddělení podpory firmy Microsoft, bez kterých by tato kniha nemohla vzniknout. Je radost pracovat s týmem profesionálů takových hodnot. Děkujeme vám.

Jako obvykle i tentokrát děkujeme lidem, se kterými jsme spolupracovali v minulosti a jejichž přínos nemůžeme opomenout: Rudolphu S. Langerovi a Davidu J. Clarkovi.

Úvod

Abyste byli lepšími, musíte se změnit; být dokonalým znamená měnit se často.
– *Winston Churchill*

Změna je nevyhnutelná, stálá a nedá se před ní uniknout. Můžete se nad tím zamyslet, můžete mít na věc stejně optimistický pohled jako Winston Churchill (kdo jiný už by měl být optimistou, když ne on), ale v každém případě je nutné smířit se s tím, že zlepšení beze změny není možné. A i když upgradování serverů a klientských počítačů může být pro administrátory značnou výzvou, je to také příležitost k vylepšení vaší sítě. A můžete si být jistí, že operační systém Windows Server 2008 obsahuje mnoho nástrojů, které vaším změnám umožní nabrat ten správný směr.

Seznamte se s rodinou

Operační systém Windows Server 2008 je dostupný v pěti hlavních verzích. Tři z nich neobsahují Windows Server Hyper-V, což činí celkový počet edicí osm.

- Windows Server 2008 Standard
- Windows Server 2008 Enterprise
- Windows Server 2008 Datacenter
- Windows Server 2008 for Itanium-Based Systems
- Windows Web Server 2008
- Windows Server 2008 Standard bez Hyper-V
- Windows Server 2008 Enterprise bez Hyper-V
- Windows Server 2008 Datacenter bez Hyper-V

Edice	Jádro serveru	Služba pro nasazení systému Windows	Správce serveru	Terminálové služby, Brána TS a aplikace RemoteApps	Active Directory Rights Management	Network Access Protection (ochrana síťového přístupu – NAP)	Hyper-V	IIS 7.0
Standard	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Enterprise	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Datacenter	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Ano
Web	Ano	Ne	Ano	Ne	Ne	Ne	Ne	Ano
Itanium	Ne	Ne	Ano	Ne	Ne	Ne	Ne	Ano

Následující tabulka poskytuje obecná doporučení pro hardwarové požadavky. Skutečné požadavky se budou lišit podle toho, jaký systém a jaké aplikace konkrétně používáte. Výkon procesoru je závislý nejen na jeho frekvenci, ale také na počtu jader a velikosti vyrovnávací paměti procesoru. Požadavky na diskový prostor systémového oddílu jsou

přibližné. Operační systémy pro architektury Itanium a x64 se budou požadavkem na velikost disku mírně lišit. Pokud instalujete operační systém pomocí sítě, může být zapotřebí o něco více volného místa na systémovém oddílu.

Součást	Požadavek
Procesor	Minimum: 1 GHz (procesor x86) nebo 1,4 GHz (procesor x64) Doporučeno: 2 GHz a více
Paměť	Minimum: 512 MB RAM Doporučeno: 2 GB RAM nebo více Optimum: 2 GB RAM pro plnou instalaci nebo 1 GB RAM pro jádro serveru Maximum pro 32bitové systémy: 4 GB (Standard) nebo 64 GB (Enterprise a Datacenter) Maximum pro 64bitové systémy: 32 GB (Standard) nebo 2 TB (Enterprise, Datacenter a Itanium)
Místo na disku	Minimum: 10 GB Doporučeno: 40 GB nebo více Počítače s více než 16 GB RAM budou potřebovat více místa na disku pro stránkování, hibernaci a další soubory
Jednotka	DVD-ROM
Zobrazení	Monitor s rozlišením Super VGA (800x600) nebo vyšším
Další	Klávesnice Myš nebo jiné ukazovací zařízení

Poznámka: Pro systémy Windows Server 2008 Itanium je zapotřebí procesor Itanium 2.

Novinky v operačním systému

Operační systém Windows Server 2008 je samozřejmě plný nových funkcí, avšak některé z nich nemusí být na první pohled patrné. Ty hlavní z nich zahrnují:

- Správce serveru (Server Manager) jakožto rozšířená konzola Microsoft Management Console (MMC), poskytující jednotné rozhraní pro úlohy konfigurace a sledování serveru, společně s průvodci pro provádění běžných úkonů správy serveru.
- Prostředí Windows PowerShell, nový volitelně instalovaný interpreter příkazového řádku a zároveň skriptovací jazyk, který administrátorům umožňuje automatizaci rutinních úkolů na mnoha serverech.
- Rozšíření zásad skupiny formou předvoleb, jež umožňují konfigurovat tatáž nastavení, jaká se doposud prováděla převážně formou přihlašovacích skriptů.
- Monitor spolehlivosti a výkonu systému Windows poskytuje diagnostické nástroje, díky kterým můžete neustále sledovat prostředí serveru, ať už fyzického či virtuálního, a rychle tak identifikovat a vyřešit případné problémy.
- Optimalizovaná správa serveru a replikace dat zlepšují kontrolu nad servery v pobočkových sítích.

- Jádro serveru umožňuje minimalistickou instalaci operačního systému, kdy se instalují pouze ty role a funkce serveru, které skutečně potřebujete. Tím se snižuje potřeba údržby a také dostupná plocha pro útok na daný server.
- Průvodce pro konfiguraci clusteru s podporou převzetí služeb při selhání usnadňuje implementaci řešení vysoké dostupnosti i pro méně zdatné administrátory. Je také plně integrován protokol IPv6.
- Nový nástroj Zálohování serveru (Windows Server Backup) přináší rychlejší technologii zálohování a zároveň zjednodušení obnovy dat nebo systému.
- Windows Server 2008 Hyper-V umožňuje virtualizaci serverových rolí jakožto samostatných virtuálních počítačů, aniž byste museli kupovat software třetích stran.
- Mnoho operačních systémů – Windows, Linux a další – může být nasazeno zároveň na jediném serveru, na kterém běží technologie Hyper-V.
- Program RemoteApps Terminálových služeb a program TS Web Access umožňují vzdáleně otevřeným aplikacím, aby byly spuštěny jediným klepnutím myši a vypadaly stejně, jako by běžely na pracovní stanici koncového uživatele.
- Platforma firmy Microsoft pro publikování na webu sjednocuje technologie IIS 7.0, ASP.NET, Windows Communication Foundation a Windows SharePoint Services.
- Network Access Protection (ochrana síťového přístupu) pomáhá chránit sítě i systémy v nich proti počítačům s nevyhovujícím stavem – mohou být izolovány a/nebo jejich stav může být uveden do souladu s požadavky na zabezpečení.
- Řízení uživatelských účtů (User Account Control) poskytuje novou architekturu ověřování pro ochranu proti škodlivému softwaru.
- Doménové řadiče jen pro čtení (RODC – Read Only Domain Controllers) přinášejí bezpečnější způsob místního ověřování uživatelů ve vzdálených a pobočkových sítích s použitím repliky databáze Active Directory jen pro čtení.
- Program BitLocker Drive Encryption poskytuje rozšířenou ochranu proti krádežím a vyzrazení dat v případě, že je server fyzicky ukraden nebo ztracen. BitLocker Drive Encryption také poskytuje bezpečnější způsob smazání dat na serverech, které jsou určeny k vyřazení.

Co najdete v této knize

Kniha *Windows Server 2008 Velký průvodce administrátora* obsahuje 37 kapitol seřazených zhruba podle fází vývoje sítě založené na operačním systému Windows Server 2008.

Kapitoly 1 až 4 jsou o plánování. Možná jste zaslechli Edisonův slavný citát: „Genialita je jedno procento nadání a devadesát devět procent dřiny." Tuto větu můžete trošku upravit a dostanete dobré motto pro výstavbu sítě: Dobrá síť je jedno procento implementace a devadesát devět procent přípravy. První kapitola je přehledem operačního systému Windows Server 2008 a jeho součástí. Dále následují kapitoly o adresářových službách a plánování oboru názvů. Poslední kapitola této sekce se zabývá konkrétními problémy, které by měly být vyřešeny už při plánování nasazení.

Kapitoly 5 až 9 pokrývají instalaci a úvodní konfiguraci systému. Tyto kapitoly vás provedou procesem instalace operačního systému Windows Server 2008 a konfigurací hardwaru. Také jsou zde kapitoly věnované instalaci rolí a jádra serveru.

Kapitoly 11 až 21 se zabývají denními úkony správy systému včetně správy souborových prostředků a používání skriptů pro správu.

Kapitoly 22 až 26 jsou celé o bezpečnosti – jak vytvořit a implementovat plán zabezpečení.

Kapitoly 27 až 31 pokrývají další funkce včetně virtualizace a terminálových služeb

– každá z nich přidává operačnímu systému Windows Server 2008 skvělé nové možnosti.

Závěrečné kapitoly o ladění, údržbě a opravách se zabývají důležitými informacemi o stavu sítě. Je zde kapitola o nástroji Zálohování server (Windows Server Backup) a jiných z oblasti sledování výkonu. Také zde najdete kapitoly o důležitém tématu – plánování obnovy po havárii a prevenci. Pokud i přes vaše úsilí síť selže, toto je místo, kde najdete informace o řešení problémů a zotavení sítě. Navíc jsme přidali kapitolu o registrech – mozku systému Windows Server 2008 – a nějaké rady, pokud se chystáte podstoupit operaci tohoto mozku.

Na konci této knihy najdete doplňující materiály o změnách uživatelského rozhraní a podpůrných nástrojů.

V kapitolách samotných jsme se snažili učinit informace co nejdostupnější. Najdete zde popisné i teoretické informace, ale také mnoho postupů typu krok za krokem, které vás provedou procesem konfigurace jednotlivých funkcí. Tyto postupy jsou doplněny o obrázky, podle kterých byste měli být schopni snadno postupovat podle psaných instrukcí.

Také jsme intenzivně využili různých pomůcek pro čtenáře, které jsou společné všem knihám ze série *Velký průvodce administrátora*:

Poznámka: Poznámky obecně představují alternativní způsob, jak provést nějaký úkon, nebo informaci, která by měla být zdůrazněna. Poznámky mohou také obsahovat různá doporučení pro provádění daných úkonů rychleji nebo trošku jiným způsobem.

Důležité: Text zvýrazněný jako Důležitý byste vždy měli pečlivě přečíst. Tato informace vám může ušetřit čas nebo zabránit problému – nebo obojí.

Další informace: V těchto odstavcích se dozvíte další fakta o daném tématu.

Doporučené postupy: Nejosvědčenější postupy profesionálů.

Z praxe:

Všichni mohou mít prospěch ze zkušeností jiných lidí. Rámeček „Z praxe" obsahuje pojednání o konkrétním tématu nebo „dobrodružství" IT profesionálů, jako jste vy.

Pohled zevnitř:

Když čaroděj provádí své kouzlo nebo jinou proceduru mimo jeviště, sekce „Pohled zevnitř" vám popíše, co se děje v zákulisí.

Skripty na webu

Na adrese *http://knihy.cpress.cz/K1608* naleznete skripty z kapitol 9 a 15.

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/k1608*. Prostřednictvím uvedené adresy můžete též naší redakci zaslat komentář nebo dotaz týkající se knihy. Na vaše reakce se srdečně těšíme.

ČÁST I

Příprava

V této části:

KAPITOLA 1

Úvod do systému Windows Server 2008

Z názvu systému Windows Server 2008 je patrné, že tento operační systém přichází na svět pět let po systému Windows Server 2003. V lidských měřítkách to není dlouhá doba, ale v měřítkách počítačů je to prakticky věčnost.

Možná se teď sami právem ptáte: Proč to trvalo tak dlouho? Klidně byste toto zpoždění mohli připsat systému Windows Vista. Systém Windows Vista, uvedený na trh více než pět let po svém předchůdci, systému Windows XP, obsahuje mnoho nových a přepracovaných funkcí v oblasti sítí, správy a především zabezpečení, které vysvětlují jeho zpoždění. Systém Windows Server 2008, postavený na témže základě, nemohl těchto nových funkcí využít dříve, než byl dokončen samotný systém Windows Vista.

Čekání nikoli zbytečné

Systém Windows Server 2008 sice možná přichází s mírným zpožděním, čekání však bezpochyby stálo za to. Nový systém s sebou přináší příslib usnadnění práce oddělením informačních technologií, která jsou nucena odvádět stále více práce při současném neustálém omezování stavu zaměstnanců i rozpočtu. Nové vlastnosti a vylepšené funkce systému Windows Server 2008 se zaměřují na snížení nákladů na administraci a správu, aniž by tím utrpělo zabezpečení nebo snadné používání. Nejedná se o žádné okázalé změny – koneckonců, koho by okouzlily řadiče domény jen pro čtení, sítě založené na

zásadách, prostředí Windows PowerShell, nebo i výrazný upgrade Terminálové služby? Názvy těchto i mnohých dalších funkcí však uším přepracovaného správce znějí jako rajská hudba.

Virtualizace serverů

Přestože se virtualizace používá již řadu let, jsou virtuální servery horkým tématem posledních dní. Novinkou je zejména to, že systém Windows Server 2008 má virtualizaci vestavěnou. Nedokonalé využití serverů je jev mnohem častější, než byste mysleli. Servery jsou často vyhrazeny konkrétnímu účelu, který může využívat i jen deseti nebo dvaceti procent jejich skutečné kapacity. Po zbytek doby zůstávají nečinné, což se však nijak nepromítá do jejich pořizovacích a provozních nákladů. Virtualizací mnoha serverů na jediném počítači můžete snadno maximalizovat využití serveru a omezit přitom celkové náklady na správu. Všechny způsoby, kterými vám virtualizace pomůže efektivně využít hardwarové prostředky, jsou popsané v kapitole 29 (Práce se službou Windows Virtualization).

Jádro serveru

Používáte-li systém Windows Server 2008, můžete nainstalovat vysoce zabezpečené minimální prostředí s nízkou režií zvané *jádro serveru*. Pokud vyberete instalaci jádra serveru, nainstaluje se pouze omezená sada binárních souborů, které jsou nezbytné pro požadované role serveru, a zcela je vynecháno grafické rozhraní. Správci systému používají k místní správě takového serveru příkazový řádek nebo skripty. Nainstalované jádro serveru mohou spravovat také z jiného počítače se systémem Windows Server 2008 pomocí konzoly MMC (Microsoft Management Console), a to tak, že v konzole jako počítač ke správě vyberou počítač s jádrem serveru.

Servery bez grafického uživatelského rozhraní (GUI) také představují menší cíl pro hackery a vyžadují mnohem méně prostoru k instalaci (přibližně 1 GB). Virtualizovanou instalaci jádra serveru můžete nakonfigurovat pro takové role, jako je server DHCP, server DNS, Internetová informační služba 7, tiskový server, souborový server, služba Active Directory, služba AD LDS (Active Directory Lightweight Directory Services) a podobně. Instalaci a konfiguraci jádra serveru popisuje kapitola 9 (Instalace a konfigurace jádra serveru).

Poznámka: Jádro serveru není samostatná verze systému Windows Server 2008, ale volba instalace dostupná ve všech verzích s výjimkou verzí Web a Itanium.

Prostředí PowerShell

Dlouho očekávané prostředí Windows PowerShell je nové prostředí příkazového řádku jak pro interaktivní používání, tak i pro tvorbu skriptů, které lze používat samostatně nebo i společně. V prostředí Windows PowerShell se objevuje koncept *cmdletu* – jednoduchého, jednoúčelového nástroje příkazového řádku, vestavěného přímo do prostředí. Všechny cmdlety můžete používat i samostatně, jejich síla však tkví v možnosti je kom-

binovat. Prostředí Windows PowerShell obsahuje více než sto základních cmdletů, které můžete kombinovat a automatizovat tak složitější úlohy. Pro složitější vlastní skripty můžete dokonce psát i své vlastní cmdlety.

Prostředí PowerShell a jeho obměny jsou popsány v kapitole 15 (Konzistentní správa pomocí skriptů).

Řadiče domény jen pro čtení

Jedním z největších problémů, kterým pracovníci oddělení informačních technologií čelí, je správa a zabezpečení systémů na pobočkách firem. Kanceláře v pobočkách jsou často příliš malé, než aby měly vlastní IT oddělení, a často jsou příliš daleko na to, než aby se o ně správci mohli starat osobně. Kanceláře v pobočkách mohou být jen slabě fyzicky zabezpečené, ale přitom mohou přesto k provozu jedné nebo více důležitých aplikací potřebovat řadič domény. Řadič domény dokonce může být jediným serverem v pobočce, pak je po něm vyžadováno plnění hned několika rolí.

Mnoho problémů vlastních pobočkovým kancelářím řeší řadič domény jen pro čtení (RODC). Řadič RODC spravuje tytéž atributy a objekty služby Active Directory jako řadiče domény s možností zápisu. Rozdíl spočívá v tom, že změny v řadiči jen pro čtení nelze provádět přímo. Namísto toho musejí být změny provedeny v řadiči domény s možností zápisu a pak replikovány do řadiče RODC. Tím se předchází tomu, že by v pobočce mohly být provedené změny, které by se rozšířily do celé doménové struktury. A protože v řadičích RODC nelze data měnit, není zapotřebí změny při replikaci kontrolovat a poté je stahovat.

Mnohem více o řadičích domény jen pro čtení naleznete v kapitole 16 (Instalace a konfigurace adresářových služeb).

Služba Active Directory Domain Services

Ve službě AD DS (Active Directory Domain Services) došlo ke mnoha změnám, které správci mohou shledat nadmíru užitečnými. Několik z nich zde popíšeme.

Služba Active Directory Domain Services je restartovatelná

Většina správců bude s následující větou jistě souhlasit: Čím více funkcí, které omezují potřebu restartování řadiče domény, tím lépe. V systému Windows Server 2008 mohou správci instalovat aktualizace včetně bezpečnostních aktualizací i bez restartování systému – stačí jen zastavit službu Active Directory a pak ji zase spustit.

V systému Windows Server 2003 defragmentace offline vyžaduje restartování v režimu obnovení adresářové služby. V systému Windows Server 2008 můžete defragmentaci offline provést mnohem rychleji, stačí zastavit a pak zase spustit pouze službu Active Directory Domain Services.

Další informace naleznete v kapitole 17 (Správa služby Active Directory).

Podrobně nastavitelné zásady pro hesla

V systémech Windows 2000 a Windows Server 2003 bylo možné určit jen jednu zásadu hesla a jedna pravidla pro uzamčení účtu (v objektu zásad skupiny Default Domain Policy) a tyto zásady pak platily pro všechny uživatele v doméně. Pokud jste potřebovali různým skupinám uživatelů nastavit různé zásady hesla a uzamykání účtů, bylo nezbytné nějakým způsobem vytvořit filtry hesel nebo nasadit další domény. Tato řešení byla zdlouhavá, a tudíž i nákladná.

V systému Windows Server 2008 můžete pomocí podrobně nastavitelných zásad hesel určit různé zásady hesel i v rámci jediné domény. Můžete například nastavením přísnějších pravidel pro tvorbu hesel a přísnějších zásad pro uzamykání účtů lépe chránit konkrétní účty s rozsáhlejšími oprávněními.

Další informace o podrobných nastaveních hesel naleznete v kapitole 23 (Implementace zabezpečení).

Nástroj pro dolování dat

Obchodní analytici již dlouho získávají z dat informace prostřednictvím dolování dat. V systému Windows Server 2008 umožňuje nástroj Dolování dat porovnávat data ze snímků nebo záloh provedených v různých časech, abyste mohli lépe rozhodnout, jaká data je třeba obnovit.

Ve verzích systému Windows Server starších než Windows Server 2008 nebylo po odstranění objektů nebo organizačních jednotek možné zjistit rozsah a skutečný počet odstranění, aniž byste obnovili úplnou zálohu. To vyžadovalo restartování služby Active Directory v režimu obnovení adresářové služby. Kromě toho bylo v praxi téměř nemožné porovnat zálohy provedené v různých časech. Nástroj pro dolování dat neobnovuje odstraněné objekty, ale umožňuje prozkoumat změny a rozhodnout, co je třeba opravit.

Další informace o nástroji pro dolování dat naleznete v kapitole 34 (Použití zálohování).

Terminálová služba

I kdyby Terminálová služba nebyla zrovna ošklivá Popelčina nevlastní sestra, pozornost pohádkového prince by stejně asi neupoutala. V systému Windows Server 2008 jako by se z ní však náhle stala Popelka. Bylo přidáno mnoho nových funkcí, z nichž některé patří k nejhodnotnějším novinkám v systému Windows Server 2008, a stávající funkce byly vylepšeny.

Terminálová služba umožňuje přístup k serveru provozujícímu aplikace systému Windows nebo k plnohodnotné pracovní ploše systému Windows z téměř jakéhokoli výpočetního zařízení. Uživatelé se mohou připojovat k terminálovému serveru, spouštět na něm programy a používat jeho síťové prostředky.

Brána Terminálové služby

Brána Terminálové služby (Brána TS) je služba v rámci role Terminálová služba, která umožňuje uživatelům připojit se k serveru prostřednictvím sítě Internet pomocí šifro-

vaného připojení, aniž by bylo zapotřebí vytvářet připojení přes síť VPN. V předchozích verzích systému Windows Server se uživatelé nemohli ke vzdáleným počítačům připojovat přes brány firewall a hranice sítí, na kterých probíhal překlad NAT, protože port 3389 používaný protokolem RDP je obvykle z bezpečnostních důvodů zablokovaný. Při použití brány Terminálové služby je provoz RDP směrován na port 443, který je obvykle otevřený kvůli připojení k síti Internet, a tedy i pro vzdálená připojení.

Aplikace RemoteApp Terminálové služby

Funkce aplikace RemoteApp Terminálové služby (TS RemoteApp) je bezesporu nejpozoruhodnější novou funkcí systému Windows Server 2008. Pomocí funkce TS RemoteApp mohou počítače se systémy Windows Server 2008, Windows Vista, Windows XP (SP2) a Windows Server 2003 (SP1) přistupovat k jedné nebo více aplikacím systému Windows, které se zobrazují ve vlastních oknech proměnné velikosti s patřičnými tlačítky na hlavním panelu. Pokud program používá ikonu v oznamovací oblasti hlavního panelu, zobrazí se jeho ikona v oznamovací oblasti. Dialogová okna jsou také přesměrována na místní plochu. Uživatel může snadno spouštět několik programů současně. Pokud uživatel spustí více než jednu aplikaci RemoteApp na témže terminálovém serveru, budou všechny tyto aplikace sdílet jedinou relaci Terminálové služby.

Funkce Snadný tisk Terminálové služby, která je také novinkou systému Windows Server 2008, zajišťuje, že uživatelé mohou z aplikací RemoteApp nebo relací plochy terminálového serveru spolehlivě tisknout na tiskárně připojené k jejich klientskému počítači.

Funkce TS Web Access

Díky funkci TS Web Access mohou uživatelé přistupovat k seznamu dostupných aplikací RemoteApp navštívením webové stránky (jak ze sítě Internet, tak i ze sítě intranet). Jakmile uživatel spustí aplikaci RemoteApp, spustí se na terminálovém serveru hostujícím tuto aplikaci relace Terminálové služby.

Zprostředkovatel relací Terminálové služby

Zprostředkovatel relací Terminálové služby obsahuje novou funkci – Vyrovnávání zatížení služby Zprostředkovatel relací Terminálové služby. Tato funkce umožňuje rozložit relace mezi jednotlivé servery ve farmě serverů s vyrovnáváním zátěže. Toto řešení se používá snadněji než funkce Vyrovnávání zatížení sítě systému Windows a je optimální pro farmy se dvěma až pěti terminálovými servery.

Režim vyprazdňování Terminálové služby

Pokud budete využívat tyto nové funkce Terminálové služby, přijde okamžik, kdy budete muset server vypnout za účelem údržby, přestože k němu budou stále ještě připojeni uživatelé. V systému Windows Server 2003 jste sice mohli pomocí nástroje příkazového řádku zakázat vzdálená připojení, ale uživatelé se nemohli znovu připojit k již existujícím relacím, a přišli tak o všechnu neuloženou práci. To samozřejmě není žádoucí.

Systém Windows Server 2008 tento problém napravuje pomocí režimu vyprazdňování Terminálové služby. Ten novým uživatelům nedovolí připojit se k serveru, ale aktuálně

přihlášeným uživatelům umožní znovu se připojit k existujícím relacím. Nové žádosti o přihlášení jsou přesměrovány na jiný server. Režim vyprazdňování terminálové služby je integrován do Vyrovnávání zatížení služby Zprostředkovatel relací Terminálové služby, takže ve farmě serverů s vyrovnáváním zátěže můžete převést server do režimu offline, aniž by si toho uživatelé všimli.

Tato a další vylepšení Terminálové služby jsou podrobně popsána v kapitole 30 (Nasazení terminálových služeb).

Správce serveru

Správce serveru je nová integrovaná konzola, která zobrazuje přehledné informace o serveru, včetně informací o konfiguraci serveru, stavu nainstalovaných rolí a průvodců přidáváním a odebíráním rolí a funkcí. Ve Správci serveru naleznete nástroje Správce zařízení, Prohlížeč událostí a Sledování výkonu a můžete v něm provádět zálohování a konfigurovat služby. Tento nástroj se používá snadněji než funkce Správa serveru a také poskytuje více informací na dosah ruky. Nástroj Správce serveru nahrazuje nástroje Správa serveru, Průvodce konfigurací serveru a Přidat nebo odebrat součásti systému Windows. Mnoho použití nástroje Správce serveru popisuje kapitola 8 (Instalace rolí serveru a funkcí).

Zálohování serveru

Konečně byla novou a rychlejší funkcí zálohování nahrazena dnes již poněkud omšelá zálohovací technologie přítomná v dřívějších verzích systému Windows Server, která od dob systému Windows NT prakticky nedoznala změn. Nyní lze zálohovat na disky připojené pomocí rozhraní USB a FireWire, zálohy jsou založené na bitových kopiích a lze je provádět ručně nebo automaticky. Zálohováním všeho druhu se zabývá kapitola 37 (Řešení problémů a obnovení systému).

Korektní vypínání služeb

Pokud v systému Windows Server 2003 zahájíte vypnutí serveru, operační systém poskytne aplikacím dvacet sekund na to, aby se řádným způsobem samy ukončily. Pokud se aplikaci nepodaří ukončit se v tomto časovém intervalu, zobrazí se zpráva, která vám umožní ukončení aplikace vynutit. Vynucené ukončení může způsobit ztrátu dat. Systém Windows Server 2008 čeká na ukončení aplikací tak dlouho, dokud samy signalizují, že na řádné vypnutí potřebují více času.

Další funkce zabezpečení

Dosud popsané nové a vylepšené funkce se z velké části dotýkají zabezpečení. Následující části popisují některé funkce, které byly představeny v systému Windows Vista, ale v systému Windows Server 2008 hrají ještě důležitější roli.

Funkce Address Space Load Randomization

Funkce ASLR (Address Space Load Randomization) je další z nepříliš okázalých, ale nesmírně užitečných funkcí, kterými je systém Windows Server 2008 nabitý. V předchozích verzích systému Windows (až do systému Windows Vista a nyní i systému Windows Server 2008) byly spustitelné soubory operačního systému a knihovny DLL zaváděny stále do téhož místa v paměti, což malwaru umožňovalo snadno najít rozhraní API, nacházející se na pevné adrese. Funkce ASLR zajišťuje, že žádné dvě po sobě jdoucí instance operačního systému nezavedou tytéž systémové ovladače do téhož místa. Namísto toho správce paměti na začátku spouštění systému náhodně vybere umístění jako jednu z 256 adres zarovnaných na hranici 64 KB v 16MB oblasti na horní hranici uživatelského adresového prostoru. Knihovny DLL s novým příznakem dynamické relokace jsou načítány do paměti od náhodně vybrané adresy a následně jsou relokovány.

Zatímco dříve měl škodlivý software jistotu, že systémové služby nalezne vlastními prostředky, po této jednoduché a transparentní změně má v tomto směru skutečně již jen chabou naději.

Nástroj BitLocker Drive Encryption

Nástroj BitLocker je funkce zabezpečení představená v systému Windows Vista, která umožňuje chránit systémové svazky na klientských počítačích – a to především na přenosných počítačích – v případě ztráty nebo odcizení. Je-li disk zašifrovaný nástrojem BitLocker, nelze například obejít zabezpečení systému Windows tím, že disk vyjmete z jednoho počítače a vložíte do jiného.

V systému Windows Server 2008 je nástroj BitLocker obzvláště užitečný pro servery umístěné na pobočkách firem, ve kterých může být obtížnější zajistit fyzické zabezpečení. Nástroj BitLocker šifruje všechna data uložená na systémovém svazku (a na nakonfigurovaných datových svazcích) včetně operačního systému Windows, souboru režimu spánku, stránkovacího souboru, aplikací a aplikačních dat. Data jsou „uzamčena" tak, že zůstávají zašifrovaná i v případě, že je operační systém vypnut nebo je disk vyjmut z počítače.

Více informací o konfiguraci a používání nástroje BitLocker naleznete v kapitole 23 (Implementace zabezpečení).

Brána Windows Firewall

Nová brána Windows Firewall je součástí nového systému správy založeného na rolích. Brána Windows Firewall je založena na verzi použité v systému Windows Vista. Je obousměrná a ve výchozím nastavení je zapnutá bez ohledu na vybrané role. Když povolujete a zakazujete role a funkce serveru, brána Windows Firewall se automaticky konfiguruje tak, aby byly otevřené pouze nezbytné porty.

Další informace o používání nové brány firewall naleznete v kapitole 23 (Implementace zabezpečení).

Architektura Network Access Protection

Architektura NAP (Network Access Protection) je nová sada komponent operačního systému, které monitorují stav klientů pokoušejících se připojit k síti nebo jejím prostřednictvím komunikovat. Pokud je zjištěn klient nevyhovující požadavkům na zabezpečení, může být jeho přístup omezen na síť podléhající určitým omezením, dokud nebudou splněny požadavky na jeho stav.

Architektura NAP nechrání před uživateli se zlými úmysly. Pouze vynucuje dodržování zásad pro stav počítače, které určuje správce. Zásady stavu počítače mohou například vyžadovat, aby všechny počítače připojující se k síti měly nainstalovány nejnovější aktualizace systému Windows, aby byly vybaveny nejnovějšími virovými signaturami a tak dále. To je obzvláště důležité v případě přenosných počítačů nebo domácích počítačů, které jsou jinak po většinu času mimo kontrolu sítě. Je-li počítač při přihlášení vyhodnocen jako nevyhovující, může být přesměrován na omezenou síť, kterou obsluhují nápravné servery schopné uvést počítač do vyhovujícího stavu.

Všechny informace potřebné k co nejlepšímu využití funkce NAP naleznete v kapitole 24 (Správa architektury NAP (Network Access Protection)).

Verze systému Windows Server 2008

Systém Windows Server 2008 je k dispozici v následujících 32b a 64b verzích:

- Windows Server 2008 Web Edition,
- Windows Server 2008 Standard Edition,
- Windows Server 2008 Enterprise Edition,
- Windows Server 2008 Datacenter Edition.

Systém Windows Server 2008 bude poslední 32bitový serverový operační systém Windows. Protože prakticky všechny dnes prodávané servery podporují 64bitový režim, skutečně zvažte přechod na 64bitové prostředí. Zvětšení adresového prostoru má za následek výrazný nárůst výkonu. 64bitová verze také může využít hardware poskytující další funkce zabezpečení. Dostupnost ovladačů již v případě serverů nepředstavuje problém. Přestože na 64bitovém systému již nespustíte 16bitové aplikace, pokud je však z nějakého důvodu skutečně potřebujete, můžete je spustit ve virtuálním počítači a nikdo si toho nejspíš ani nevšimne.

Shrnutí

V této kapitole byla představena některá z vylepšení systému Windows Server 2008. Následující tři kapitoly se budou zabývat tématy důležitými při plánování nasazení systému Windows Server 2008. V příští kapitole budou popsány koncepty a struktura služby Active Directory Domain Services.

KAPITOLA 2

Představení adresářových služeb

Francis Bacon (1561–1626) byl pravděpodobně poslední člověk, který věděl vše. Jistě, byl to člověk s výjimečnými znalostmi všech vědních oborů, je ale nutné si uvědomit, že v sedmnáctém století toho lidstvo vědělo mnohem méně. Dnes si musíme udržovat přehled o takovém množství informací, že se musíme spoléhat na adresáře. Adresáře jsou definovány jako seznamy, které pomáhají najít různé položky – mohou mezi ně patřit například jízdní řády autobusů, rejstříky knih a telefonní seznamy. Dvě vyhledávací schopnosti nezbytné v počítačových adresářích jsou ve skutečnosti analogií právě k telefonním seznamům. Jedná se o vyhledávání typu „bílé stránky" pomocí atributu Hledat podle, kdy znáte jméno nebo nějaký jiný údaj o daném objektu a hledáte pomocí této informace. Druhý typ vyhledávání označený jako vyhledávání podle „žlutých stránek" je prováděn podle kategorií. Ať už používáte kterékoli z těchto dvou vyhledávání, nemusíte o daném objektu vědět mnoho informací, abyste jej vyhledali.

Adresáře jsou nezbytné pro správnou funkci počítačových sítí. Absence uceleného a přístupného adresáře se citelně projeví v síti libovolné velikosti. V sítích systému Microsoft Windows NT skutečné adresářové služby, tedy globální katalog síťových služeb a prostředků, chybějí. Přestože adresářové funkce dostupné ve verzi 4 zajišťují zcela nepostradatelné jednotné přihlašování a jediný bod pro správu, což je v podnikovém prostředí nezbytné, při vysokém počtu uživatelů se potýkají s vážnými problémy. Pokusy uspořádat dokumenty do složek a adresářů do jisté míry fungují, ale se vzrůstajícím počtem objektů se jejich správa stává složitou a náročnou.

Vysvětlení adresářových služeb

V typickém výpočetním prostředí systému Windows NT se uživatelé mohou přihlásit do sítě pomocí uživatelského jména, například *phora*, a hesla. Za předpokladu, že jsou správně udělena oprávnění, může uživatel phora klepnout na složku Okolní počítače nebo otevřít namapovanou jednotku a vyhledat potřebné soubory.

Vše pracuje jak má, dokud se nezmění rozsah služeb, které síť poskytuje. Společnost zapojí elektronickou poštu a uživatel phora rázem získá další identitu (*petrhora@scribes.com*). Stejnému uživateli musejí být přístupné další služby, databáze a nástroje pro správu, z nichž každý identifikuje Petra Horu mírně odlišně. Pokud uvážíte, že se jedná pouze o jednoho ze stovek, nebo dokonce tisíců uživatelů, brzy pochopíte, že může snadno dojít k velmi obtížně napravitelným chybám. A se vzrůstajícím počtem objektů v síti se adresářové služby – centrální úložiště dat potřebných ke správě celého počítačového systému – stávají nezbytnou součástí sítě.

Adresářové služby se liší od adresáře v tom, že sestávají jak z adresářového informačního zdroje, tak i ze služeb, které tyto informace zpřístupňují uživatelům. Jelikož jsou adresářové služby současně nástrojem pro správu i pro koncové uživatele, musejí plnit následující potřeby:

- Přístup ke všem serverům, aplikacím a zdrojům prostřednictvím jediného přihlášení. (Přístup je uživateli udělen nebo odepřen na základě jeho oprávnění.)
- Replikace typu multimaster. Veškeré informace jsou v systému distribuovány a replikovány na více serverech.
- Vyhledávání typu „bílé stránky“ na základě atributů, například podle názvu nebo typu souboru.
- Vyhledávání typu „žluté stránky“ na základě klasifikace, například všechny tiskárny ve třetím poschodí nebo všechny servery v kanceláři v Praze.
- Možnost odstranit vazbu objektů na fyzických umístěních za účelem snazší správy. To znamená, že by mělo být možné delegovat správu adresáře, a to buď částečně, nebo zcela.

Přestože společnost Microsoft již dříve v souvislosti se systémem Windows NT občas používala termín „adresářové služby“, tento systém skutečnou hierarchickou adresářovou službu neobsahoval. V systému Windows NT byly adresářové funkce rozděleny mezi množství služeb na základě domén. Server systému DNS (Domain Name System) překládal názvy do číselných adres IP a byl integrován se servery protokolu DHCP (Dynamic Host Configuration Protocol), které dynamicky přidělovaly adresy protokolu TCP/IP (Transmission Control Protocol/Internet Protocol). Služba WINS (Windows Internet Name Service) překládala názvy systému NetBIOS (Network Basic Input Output System) a v systému Windows NT byla vyžadována pro sdílení souborů a některé aplikace. Zabezpečení bylo implementováno prostřednictvím seznamů řízení přístupu (ACL), databáze SAM (Security Accounts Manager) a dalších služeb.

Systém Microsoft Windows Server 2000 byl prvním produktem, ve kterém služba Active Directory nahradila sbírku adresářových funkcí systému Windows NT integrovanou implementací, která zahrnuje systém DNS a protokoly DHCP, LDAP (Lightweight

Directory Access Protocol) a Kerberos. (Podrobnější informace o těchto součástech jsou uvedeny dále v této kapitole.)

Z praxe: Adresářové služby a standard X.500

X.500 je standard pro adresářové služby vytvořený Mezinárodní telekomunikační unií (ITU). Stejný standard vydává také organizace ISO/IEC. Standard X.500 definuje informační model používaný v adresářových službách. V tomto modelu jsou všechny informace v adresáři ukládány jako záznamy, z nichž každý patří do nejméně jedné třídy objektů. Skutečné informace v záznamu jsou určeny atributy obsaženými v daném záznamu.

Původní standard X.500 z roku 1988 se zaměřoval zejména na protokoly, které měly být implementovány. Protokol DAP (Directory Access Protocol) určuje, jakým způsobem přistupují uživatelské aplikace k informacím v adresáři. Protokol DSP (Directory Service Protocol) slouží k předání požadavků uživatelů na adresáře mezi adresářovými servery v případě, že místní adresářový server nemůže požadavek splnit.

Dosud neexistuje adresářová služba, která by standard X.500 implementovala v jeho úplnosti, všechny adresářové služby jsou však vystaveny na základních specifikacích modelu X.500, a služba Active Directory není výjimkou. Výborný úvod do adresářů a standardu X.500 naleznete na adrese *http://www.nlc-bnc.ca/9/1/p1-244-e.html*.

Služba Active Directory v systému Windows Server 2008

Služba Active Directory Domain Services (AD DS) má celou řadu výhod. Jednou z nejpodstatnějších je, že dokáže obsloužit jakoukoli velikost instalace, od jednoho serveru s několika sty objekty až po tisíce serverů a miliony objektů. Služba Active Directory také velmi zjednodušuje proces vyhledávání zdrojů v rozsáhlé síti. Díky rozhraní ADSI (Active Directory Service Interfaces) a novému režimu ADAM (Active Directory Application Mode) mohou vývojáři své aplikace přizpůsobit k využívání adresářových služeb a poskytnout tak uživatelům jednotný bod přístupu do více adresářů, ať již jsou založeny na protokolu LDAP, systému NDS nebo službě NTDS (NT Directory Services).

Sužba Active Directory integruje internetové pojetí oboru názvů s adresářovými službami operačního systému. Tato kombinace umožňuje sjednotit několik oborů názvů například ve smíšených hardwarových a softwarových prostředích podnikových sítí, a to dokonce mezi různými operačními systémy. Jelikož služba Active Directory umožňuje sloučit jednotlivé podnikové adresáře do jediného univerzálního adresáře, může do značné míry snížit náklady na správu více oborů názvů.

Služba Active Directory není adresář X.500. Místo toho jako protokol pro přístup používá protokol LDAP a podporuje informační model X.500, aniž by vyžadovala, aby byl systém zatížen režií celého standardu X.500. Protokol LDAP je založen na protokolu TCP/IP a je mnohem jednodušší než protokol DAP standardu X.500. Stejně jako v adresářích X.500 je adresářový model protokolu LDAP založen na záznamech, na které se lze odkazovat prostřednictvím jednoznačného rozlišujícího názvu (viz následující část). Namísto vysoce strukturovaného kódování dat používaného standardem X.500 však protokol LDAP reprezentuje adresářové záznamy pomocí jednoduchých řetězců. Protokol LDAP využívá mnoho technik adresářového přístupu specifikovaných ve standardu X.500 DAP,

ale vyžaduje méně klientských prostředků. Díky tomu je praktičtější pro běžné nasazení a připojení prostřednictvím protokolu TCP/IP.

Služba Active Directory také přímo podporuje protokol HTTP (Hypertext Transfer Protocol). Každý objekt adresáře Active Directory lze zobrazit jako stránku HTML (Hypertext Markup Language) ve webovém prohlížeči. Rozšíření služby IIS pro podporu adresářů překládá požadavky protokolu HTTP požadující adresářové objekty na stránky HTML, které lze zobrazit v libovolném klientu HTML.

Služba Active Directory umožňuje všechny publikované zdroje, mezi které mohou patřit soubory, periferní zařízení, hostitelská připojení, databáze, přístup na web, uživatelé, libovolné další objekty, služby atd., spravovat z jediného místa. Jako službu pro vyhledávání využívá internetovou službu DNS, objekty v doménách uspořádává do hierarchie organizačních jednotek a umožňuje propojit více domén do stromové struktury. Koncept primárního (PDC) a záložního (BDS) řadiče domény, který byl v systému Windows Server odstraněn, se znovu vrací – tentokrát ovšem v trošku jiné podobě. Roli řadiče BDC nyní plní řadič domény jen pro čtení (RODC), který je podrobně popsán v šestnácté kapitole (Instalace a konfigurace adresářových služeb). Počínaje systémem Windows Server 2003 R2 umožňují služby ADFS (Active Directory Federation Services) rozšířit službu Active Directory o funkci správy identit napříč organizacemi a platformami.

Terminologie a pojmy týkající se služby Active Directory

Některé termíny používané pro pojmy týkající se Active Directory se již nějakou dobu používají i v jiných souvislostech, takže je důležité vysvětlit si, co konkrétně znamenají v souvislosti se službou Active Directory. V této části jsou tyto základní pojmy a termíny vysvětleny.

Obor názvů a překlad názvů

Pojem „obor názvů“ vám možná na první pohled nic neříká, označuje však něco, co jistě velmi dobře znáte. Každá adresářová služba představuje *obor názvů* – omezenou oblast, ve které lze překládat názvy. Televizní program tvoří obor názvů, ve kterém lze názvy jednotlivých programů překládat na čísla kanálů. Systém souborů v počítači tvoří obor názvů, ve kterém lze názvy souborů překládat na samotné soubory.

Adresář Active Directory tvoří obor názvů, ve kterém lze název objektu v adresáři přeložit na objekt samotný. *Překlad názvů* je proces, který název objektu přeloží na nějaký objekt nebo na informaci, kterou tento název reprezentuje.

Atribut

Každá dílčí informace, která popisuje nějaký aspekt záznamu, se nazývá *atribut*. Atribut sestává z *typu atributu* a jedné nebo více *hodnot atributu*. Příkladem typu atributu může být „telefonní číslo“ a příkladem hodnoty atributu telefonní číslo může být „425 707 979“.

Objekt

Objekt je určitá sada atributů, které představují něco konkrétního, například uživatele, tiskárnu nebo aplikaci. Atributy obsahují data popisující to, co adresářový objekt identifikuje. Mezi atributy uživatele může patřit jeho křestní nebo rodné jméno, příjmení a e-mailová adresa. Klasifikace objektu určuje, jaké typy atributů budou použity. Například objekty klasifikované jako „uživatelé" mohou umožňovat použití takových typů atributů, jako je „běžný název", „telefonní číslo" a „e-mailová adresa", zatímco třída objektů „organizace" umožňuje používat takové typy atributů, jako je „název organizace" a „kategorie podnikání". Atribut může v závislosti na typu obsahovat jednu nebo více hodnot.

Každý objekt adresáře Active Directory má jedinečnou *identitu*. Objekty lze přesouvat a přejmenovávat, ale jejich identita se nikdy nemění. Objekty jsou interně známy na základě své identity, nikoli podle aktuálního názvu. Identitu objektu udává identifikátor GUID (Globally Unique Identifier), který je nově vytvářeným objektům přidělován agentem adresářového systému (DSA). Identifikátor GUID je uložen v atributu *objectGUID*, který je součástí každého objektu. Atribut *objectGUID* nelze změnit ani odstranit. Pokud ukládáte odkaz na objekt služby Active Directory do externího úložiště (například do databáze), použijte atribut *objectGUID*, protože se na rozdíl od názvu nebude měnit.

Kontejner

Kontejner se podobá objektu v tom, že také obsahuje atributy a také je součástí oboru názvů adresáře Active Directory. Na rozdíl od objektu však kontejner nepředstavuje nic konkrétního. Ukládají se do něj objekty a další kontejnery.

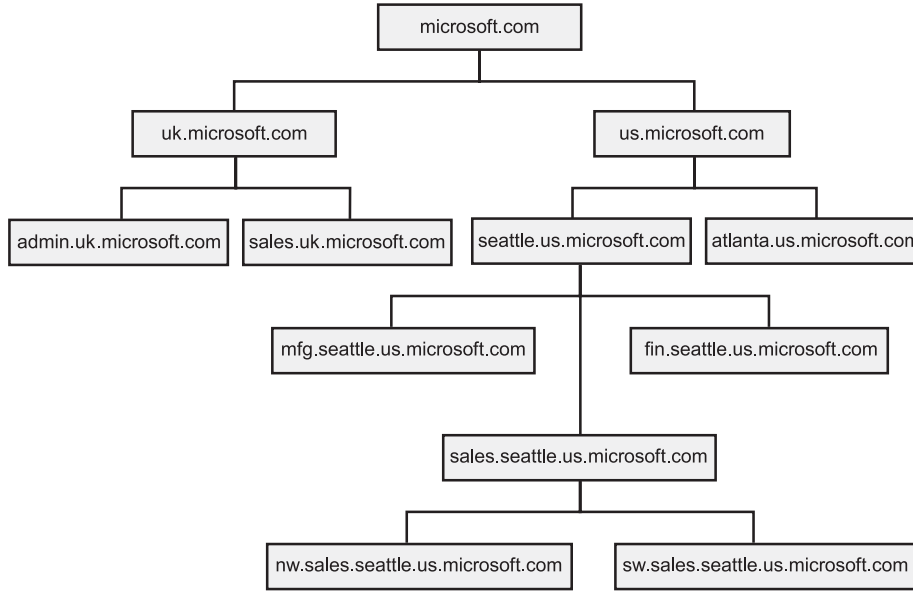
Strom a podstrom

Strom je v adresáři Active Directory pouhým rozšířením myšlenky adresářového stromu. Jedná se o hierarchii objektů a kontejnerů, která ukazuje, jak jsou objekty propojeny, nebo udává cestu z jednoho objektu do jiného. Koncové body stromu jsou obvykle objekty.

Podstrom je jakákoli nepřerušená cesta ve stromu, včetně všech členů jakýchkoli kontejnerů v dané cestě. Obrázek 2.1 znázorňuje stromovou strukturu domény microsoft.com. Jakákoli nepřerušená cesta (například cesta z objektu nw.sales.seattle.microsoft.com do objektu microsoft.com) představuje podstrom. Stromy a doménové struktury jsou podrobněji popsány v kapitole 3 (Plánování oborů názvů a domén).

Rozlišující názvy

Každému objektu adresáře Active Directory náleží takzvaný *rozlišující název* (DN). V této souvislosti slovo „rozlišující" označuje skutečnost, že se tento název něčím liší od všech ostatních. Rozlišující název identifikuje nejen doménu, ve které je objekt uložen, ale i úplnou cestu v hierarchii kontejnerů, po které se k objektu lze dostat. Typický rozlišovací název může vypadat následovně: CN=Petr Hora,OU=Technici,DC=example,DC=local. Tento název označuje objekt uživatele Petr Hora v organizační jednotce Technici v doméně example.local.



Obrázek 2.1: Stromová struktura s podstromy

Poznámka: Zkratka CN znamená běžný název (common name), OU organizační jednotku (organizational unit) a DC součást domény (domain component). Některé atributy jsou odvozeny z modelu X.500, další může definovat správce.

Služba Active Directory používá také *relativní rozlišující názvy* (RDN), což je součást rozlišovacího názvu, který je atributem objektu samotného. V předchozím příkladu je relativním rozlišujícím názvem objektu uživatele název CN=Petr Hora. Název RDN nadřazeného objektu je OU=Technici.

Část rozlišujícího názvu uvozená znaky „DC=“ umožňuje adresářům X.500 zapojit se do oboru názvů služby DNS, a služba Active Directory tak činí také. Kořen globálního oboru názvů pro adresář Active Directory je obor názvů služby DNS. Proto názvy domén DNS zapadají do jmenného schématu služby Active Directory. Název example.local je například platný interní název domény systému DNS, a současně to může být název domény služby Active Directory. Tato integrace se službou DNS znamená, že adresář Active Directory přirozeně zapadá do prostředí sítí Internet a intranet. Servery služby Active Directory můžete připojit přímo k síti Internet a zjednodušit tak bezpečnou komunikaci a elektronické obchodování se zákazníky a partnery.

Schéma

„Schéma“ je termín, který se obvykle používá v oblasti databází. V souvislosti se službou Active Directory *schéma* obsahuje definice jednotlivých objektů, ze kterých se váš adresář Active Directory skládá: objektů, atributů, kontejnerů atd. Výchozí schéma služby Active Directory definuje nejběžnější třídy objektů, jako jsou uživatelé, skupiny, počítače, organizační jednotky, zásady zabezpečení a domény.

Schéma služby Active Directory lze dynamicky aktualizovat. To znamená, že aplikace může rozšířit schéma o nové atributy a třídy a ihned je může začít používat. Schéma se aktualizuje vytvořením nebo změnou objektů schématu, také uložených v adresáři. Objekty schématu jsou chráněny prostřednictvím seznamů ACL, takže schéma mohou měnit pouze oprávnění uživatelé (členové skupiny Schema Admins).

Architektura služby Active Directory

Jak již bylo uvedeno výše, adresářová služba Active Directory není striktně řečeno adresářovou službou standardu X.500, i když je na něm jako všechny existující adresářové služby založena. V následujících částech je uveden výčet některých vlastností architektury služby Active Directory.

Agent adresářového systému

Agent DSA je proces, který zajišťuje přístup do fyzického úložiště adresářových informací, které se nachází na pevném disku. V systémech Windows Server 2003 a Windows 2000 je agent DSA součástí místního úřadu zabezpečení (LSA). Klienti mohou k těmto adresářovým informacím přistupovat pomocí některého z následujících mechanismů:

Klienti LDAP se připojují k agentu DSA pomocí protokolu LDAP. Služba Active Directory podporuje protokol LDAP v3 definovaný v dokumentu RFC 2251 a protokol LDAP v2 definovaný v dokumentu RFC 1777. Klienti systému Microsoft Windows 2000 a novějších se k agentu DSA připojují prostřednictvím protokolu LDAP v3.

- Klienti rozhraní MAPI, jako je například server Microsoft Exchange, se k agentu DSA připojují pomocí rozhraní vzdáleného volání procedur MAPI.
- Agenti DSA služby Active Directory se navzájem propojují pomocí vlastního rozhraní RPC, aby mohli svá data replikovat.

Formáty názvů

Aby služba Active Directory vyhovovala jak lidským uživatelům, tak i aplikacím, podporuje hned několik formátů názvů:

- **Názvy RFC 822** – tyto názvy jsou většině uživatelů sítě Internet známy jako e-mailové adresy, například *phora@example.local*. Služba Active Directory všem objektům poskytuje „uživatelsky přívětivy název" ve formátu RFC 822. Proto může uživatel snadno zapamatovatelný název používat současně jako e-mailovou adresu i jako přihlašovací jméno.
- **Adresy URL protokolu HTTP** – jsou známy většině uživatelů, kteří mají webové prohlížeče. Typická adresa URL má podobu *http://doména/cesta-ke-stránce*, kde doména odkazuje na server se spuštěnou službou Active Directory a cesta-ke-stránce představuje cestu hierarchií služby Active Directory k hledanému objektu. Adresa URL Petra Hory je *http://server.example.com/Divize/Produkt/inzenyri/petrhora*.
- **Názvy LDAP** – jsou složitější než názvy sítě Internet, ale jsou obvykle skryty uvnitř aplikace. Názvy LDAP používají konvenci s atributy standardu X.500. Adresa URL protokolu LDAP určuje server se službou Active Directory a název objektu určený

pomocí atributů – například ldap://server.examples.local/CN=petrhora,OU=Technici,OU=Produkt,OU=Divize,O=MegaIntl,C=US.

- **Názvy UNC** – jednotná konvence vytváření názvů používaná v sítích založených na serverech systému Windows Server 2008, která umožňuje odkazovat na sdílené svazky, tiskárny a soubory, například \\example.com\Divize.Produkt.Technici.Svazek\WordDokum\zpravazdubna.doc.

Datový model

Datový model služby Active Directory je založen na datovém modelu standardu X.500. V adresáři jsou uloženy objekty, které představují různé položky popsané atributy. Schéma definuje, které objekty lze do adresáře ukládat. Schéma pro každou třídu objektů definuje, jaké atributy musí instance třídy obsahovat, jaké další atributy může obsahovat a jaká třída objektů může být nadřazená aktuální třídě objektů.

Implementace schématu

Schéma adresáře Active Directory je implementováno jako sada instancí tříd objektů uložených v adresáři. Tímto přístupem se služba Active Directory značně liší od adresářů, které mají schéma, ale ukládají ho jako textový soubor, který je načítán při spuštění. Ukládání schématu do adresáře má mnoho výhod. Mohou jej například číst uživatelské aplikace, aby zjistily, jaké objekty a vlastnosti jsou k dispozici.

Model zabezpečení

Model zabezpečení služby Active Directory je součástí základu TCB (Trusted Computing Base) systému Windows Server 2000 a pozdějších verzí a plně se podílí na infrastruktuře zabezpečení. Distribuovaný model zabezpečení je založen na ověřovacím protokolu MIT Kerberos (verze 5). Ověřování Kerberos podporuje zabezpečení pomocí veřejných i soukromých klíčů a používá stejný model podpory seznamu řízení přístupu (ACL) jako operační systém Windows Server 2008, na kterém je provozováno. Seznamy ACL chrání všechny objekty v adresáři Active Directory. Určují, pro koho jsou objekty viditelné, jaké atributy jsou pro jednotlivé uživatele viditelné a jaké akce mohou jednotliví uživatelé s objektem provádět. Pokud není povoleno, aby byl objekt nebo atribut pro uživatele viditelný, uživatel se o jeho existenci nikdy nedozví.

Seznam ACL se naopak skládá z položek řízení přístupu (ACE), které se ukládají společně s objektem, který je tímto seznamem chráněn. V systémech Windows 2000 a pozdějších je seznam ACL ukládán jako binární hodnota zvaná *popisovač zabezpečení*. Každá položka ACE obsahuje identifikátor zabezpečení (SID), který identifikuje *zaregistrovaný objekt zabezpečení* (uživatele nebo skupinu), kterého se položka ACE týká, a poskytuje informace o typu přístupu, který položka ACE uděluje nebo odpírá.

Seznamy ACL adresářových objektů obsahují položky ACE, které platí pro objekt jako celek, a položky ACE, které platí pro jednotlivé atributy objektu. Díky tomu mohou správci řídit nejen to, pro které uživatele bude objekt viditelný, ale také to, které vlastnosti budou pro uživatele viditelné. Všem uživatelům může být například udělen přístup ke čtení atributů „e-mail“ a „telefonní číslo“ všech ostatních uživatelů, ale přístup k vlastnostem zabezpečení uživatelů může být odepřen všem kromě členů zvláštní skupiny správců

zabezpečení. Jednotlivým uživatelům může také být udělen přístup pro zápis osobních atributů, jako je telefon a e-mailová adresa jejich vlastních uživatelských objektů.

Služba Active Directory je úložištěm systému zabezpečení včetně uživatelských účtů, skupin a domén. Toto úložiště nahrazuje databázi účtů registru a je důvěryhodnou součástí místního systému LSA.

Delegování a dědičnost

Delegování je jednou z nejdůležitějších funkcí zabezpečení služby Active Directory. Správce může uživateli udělit oprávnění provádět určenou sadu akcí v označeném podstromu adresáře. To se označuje jako *delegovaná správa*. Delegovaná správa umožňuje přesně řídit, kdo může provádět jaké akce, a umožňuje správcům delegovat oprávnění bez udělování zvýšených oprávnění. Tím také odpadá potřeba udržovat správce domény, kteří by měli rozsáhlé pravomoce nad velkými skupinami uživatelů.

Administrátoři udělují práva pro konkrétní operace nad konkrétními třídami objektů přidáním položek ACE do seznamu ACL objektu kontejneru. Chcete-li například uživateli Petru Horovi udělit oprávnění spravovat organizační jednotku Technici, přidáte položky ACE na seznam ACL objektu Technici následujícím způsobem:

```
"Petr Hora";Povolit ;Create, Modify, Delete;Object-Class User
"Petr Hora";Povolit ;Create, Modify, Delete;Object-Class Group
"Petr Hora";Povolit ;Write;Object-Class User; Attribute Password
```

Nyní může Petr Hora v organizační jednotce Technici vytvářet nové uživatele a skupiny a nastavovat hesla stávajících uživatelů, nemůže ale vytvářet ostatní třídy objektů a ovlivňovat uživatele v jiných kontejnerech (pokud mu položky řízení přístupu neudělují tento přístup také pro jiné kontejnery).

Dědičnost umožňuje šířit danou položku ACE z kontejneru, ve kterém byla použita, do všech podřízených položek kontejneru. Kombinací dědičnosti a delegování lze udělit práva ke správě celého podstromu adresáře jedinou operací.

Názvové kontexty a oddíly

Adresář Active Directory sestává z jednoho nebo více názvových kontextů nebo oddílů. *Názvový kontext* je jakýkoli souvislý podstrom adresáře. Názvové kontexty jsou jednotkami rozdělování do oddílů. Jeden server vždy obsahuje nejméně tři názvové kontexty:

- schéma,
- konfiguraci (topologii replikace a související data),
- jeden nebo více uživatelských názvových kontextů (podstromy obsahující skutečné objekty v adresáři).

Globální katalog

Rozlišující název objektu obsahuje dostatek informací k vyhledání repliky oddílu, která objekt obsahuje. Častokrát však uživatel nebo aplikace nezná rozlišující název cílového objektu nebo údaj, který oddíl může objekt obsahovat. Globální katalog umožňuje uživatelům a aplikacím vyhledávat objekty ve větvi domény adresáře Active Directory s uvedením jednoho nebo více atributů cílového objektu.

Globální katalog obsahuje částečnou repliku všech názvových kontextů v adresáři. Obsahuje také názvové kontexty schématu a konfigurace. To znamená, že obsahuje repliku všech objektů v adresáři Active Directory, ale od každého objektu obsahuje pouze několik jeho atributů. V globálním katalogu se ukládají ty atributy, které se nejčastěji používají v operacích vyhledávání (například křestní jméno a příjmení uživatele, přihlašovací jméno atd.), a pak také atributy nezbytné k vyhledání úplné repliky objektu. Díky globálnímu katalogu mohou uživatelé rychle vyhledávat potřebné objekty, aniž by věděli, ve které doméně jsou uloženy, a aniž by byl vyžadován souvislý rozšířený obor názvů v organizaci.

Globální katalog je automaticky vytvářen systémem replikace adresáře Active Directory. Topologie replikace globálního katalogu je také generována automaticky. Vlastnosti replikované do globálního katalogu zahrnují základní sadu definovanou společností Microsoft. Správci mohou určit další vlastnosti a splnit tak potřeby vlastní instalace.

V systému Windows 2000 musel řadič domény při zpracovávání události přihlášení uživatele v doméně nativního režimu kontaktovat server globálního katalogu, aby bylo možné ověřit členství uživatele v univerzální skupině. To znamená, že u uživatelů ve vzdálené pobočce určité organizace může v případě odpojení zbývajících poboček docházet k chybám při přihlašování.

V systému Windows Server 2008 lze řadiče domény nakonfigurovat tak, aby při zpracovávání událostí přihlašování uživatelů ukládaly vyhledaná členství v univerzální skupině do mezipaměti, aby se uživatelé mohli přihlásit i v případě, že globální katalog není dostupný. Podrobnosti o správě a nasazení služby Active Directory naleznete v kapitole 16 (Instalace a konfigurace adresářových služeb) a v kapitole 17 (Správa služby Active Directory).

Shrnutí

Jak už jste jistě pochopili, služba Active Directory je nesmírně mocný nástroj – a jako většina mocných nástrojů může být zdrojem velkých potíží, pokud se s ním zachází nesprávně. Před jeho nasazením věnujte čas důkladnému promyšlení a plánování. Nejprve je třeba zvážit návrh tak, aby byl logický a účinný. Špatně navržený strom může negativně ovlivnit produktivitu sítě, a dokonce i její stabilitu. Kapitola 3 (Plánování oborů názvů a domén) popisuje, jak naplánovat obor názvů a domény tak, abyste z nich měli po co nejdelší dobu maximální užitek.

KAPITOLA 3

Plánování oborů názvů a domén

Plánování jako by snad v poslední době získalo nějakou špatnou pověst. Mnoho lidí si pod tímto pojmem představuje dlouhé nudné schůze, a dokonce ho vnímají jako způsob, jak se vyhnout činům. Přesto se však bez plánování a přípravy nelze obejít, ať již budujete počítačovou síť, nebo jen malujete pokoj.

Pokud se s pojmem *obor názvů* setkáváte poprvé, uděláte nejlépe, když nějaký čas a energii věnujete přípravě – vrátí se vám to později v podobě snížených nákladů na podporu, větší flexibility a menší potřeby reorganizace.

Plánování oboru názvů ve velké, nebo dokonce i ve středně velké organizaci je opakovaný proces. Napoprvé se vám to nepodaří, a možná se vám to nepodaří ani napodruhé. Přesto musíte někde začít. Pak plán projednáte s klíčovými osobami vaší organizace, potom plán vylepšíte a zase ho s nimi projednáte, dokud nezískáte obor názvů, který bude vaší organizaci vyhovovat. V průběhu této činnosti budete muset vyslechnout mnoho názorů ovlivněných firemní politikou a osobními zájmy účastníků. To může celý proces zkomplikovat nad nezbytně nutnou míru. Vaším úkolem je co nejlépe porozumět zájmům vaší organizace jako celku a jednat v souladu s nimi.

Analýza potřeb jmenných konvencí

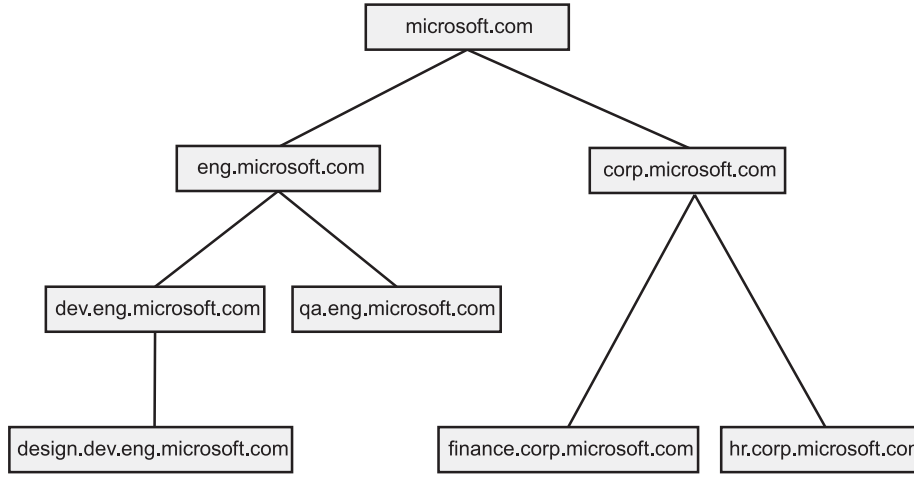
Abyste mohli naplánovat obor názvů a doménovou strukturu, musíte provést analýzu organizace a pokusit se porozumět jejím základním potřebám v souvislosti s přidělováním názvů. To vyžaduje jednak důkladné porozumění typu organizace, ve které pracujete, lidí, se kterými pracujete, a také opodstatněný odhad směru, kterým se organizace ubírá.

Stromy a doménové struktury

Existují dva základní typy oboru názvů – strom a doménová struktura. Pokud porozumíte rozdílům mezi těmito dvěma modely a tomu, jak tyto modely odpovídají či neodpovídají vaší organizaci, budete moci vybrat model, který nejlépe odráží její potřeby. Přestože můžete model změnit i později, vyžaduje takový zásah značné úsilí a měl by velký dopad na používané názvy v celém oboru názvů. Proto si v této fázi plánování nalezněte čas na porozumění potřebám vaší organizace. Ty se mohou lišit od toho, co si organizace sama myslí, že chce.

Stromy

Stromový obor názvů, jako například ten, který je znázorněn na obrázku 3.1, je jednoduchý, souvislý obor názvů, ve kterém je každý název přímo odvozen z jediného názvu kořene. Tento přímočarý návrh pojmenování je vhodný pro organizaci, která je v podstatě jednotná a má jediný název, pod který mohou být zařazeny její jednotlivé divize i různé obory podnikání. Celá řada malých až středně velkých podniků tomuto modelu odpovídá. Dokonce i pro velké organizace může být stromová struktura výhodou v případě, že je organizace dobře centralizovaná a má jednoduchý, snadno rozeznatelný název.

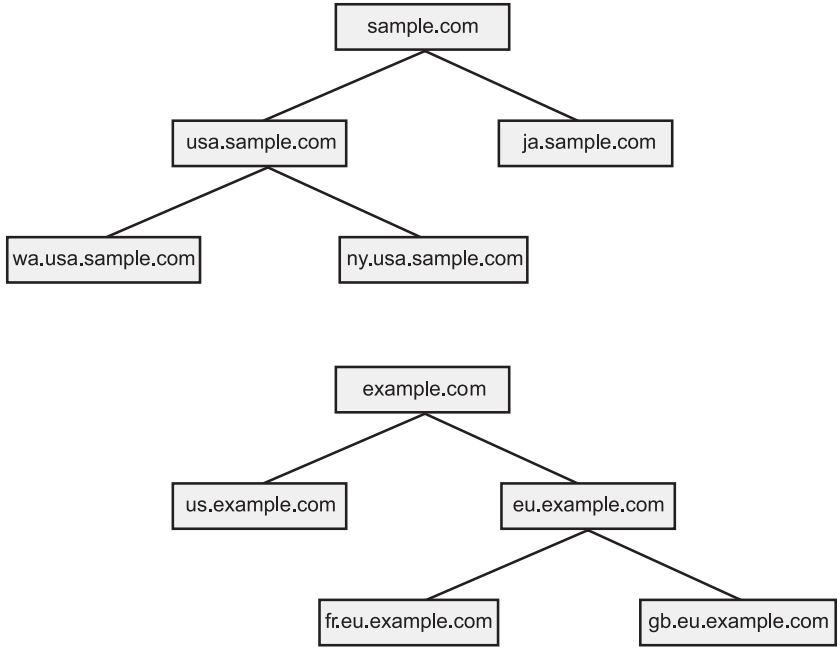


Obrázek 3.1: Stromová struktura představuje jediný souvislý obor názvů, ve kterém je vše odvozeno od jediného kořene

Jak je patrné z obrázku, který znázorňuje obor názvů se stromovou strukturou, každá větev stromu má název, který je přímo odvozen z kořene stromu. Díky tomu lze všechny listy nebo větve stromu nalézt procházením struktury od kořene podle jejich názvů.

Doménové struktury

Obor názvů doménové struktury, jako je například ten, který je znázorněn na obrázku 3.2, je skupina v zásadě rovnocenných stromů, které nesdílejí jediný společný kořen oboru názvů. Obor názvů doménové struktury je vhodný pro organizaci, která podniká ve více oborech a v každém z nich podniká pod samostatným identifikovatelným názvem. Jedná se obvykle o větší podniky, zejména o takové, které se rozrostly v důsledku akvizic. Obvykle nemají jediné centrální IT oddělení, které by spravovalo celou organizaci, a každá divize má zpravidla odlišnou identitu a infrastrukturu.



Obrázek 3.2: Doménovou strukturu tvoří několik samostatných stromů, které nejsou součástí souvislého oboru názvů

Jak je patrné z obrázku, doménovou strukturu tvoří skupina rovnocenných stromů, z nichž každý má vlastní souvislý obor názvů, ale zařadit všechny stromy do jediného souvislého oboru názvů by bylo obtížné. Jinak řečeno, názvy všech listů nelze přímo vysledovat do jediného kořene.

Definování konvence pojmenování

Ať již se chystáte jako celkový obor názvů používat jeden strom, nebo doménovou strukturu stromů, potřebujete se rozhodnout, jak pojmenujete jednotlivé větve stromu. To je pravděpodobně jedno z nejožehavějších a politicky nejcitlivějších rozhodnutí,

která musíte při návrhu celkové struktury pojmenování učinit. Buďte připraveni na to, že jakmile do rozhodovacího procesu přizvete nejdůležitější osoby v organizaci, budete muset vytrpět zdlouhavé a nepříjemné schůze. Přesto tento čas obětujte – ušetří vám to nezměrné množství pozdějších problémů.

Existují v podstatě dva typy konvencí pojmenování: organizační a zeměpisná. Obě mají své zastánce a je možné argumentovat ve prospěch kterékoli z nich. Nezapomeňte, že se lidé mohou nechat příliš strhnout svými emocemi, pokud dojde na pojmenování jejich divize nebo oddělení a na zhodnocení jeho relativního významu pro organizaci. Takové politické neshody nemusejí být jen nenávistné, ale mohou také trvat déle, než by kdokoli racionálně očekával.

Organizační konvence pojmenování

Pokud použijete organizační konvenci pojmenování, vytváříte obor názvů způsobem, jakým je společnost nebo organizace strukturována. Proto může být kořenem stromu například *microsoft.com* a první úroveň pod ním se může skládat z položek *admin.microsoft.com*, *finance.microsoft.com*, *mfg.microsoft.com*, *eng.microsoft.com* atd.

Následující seznam uvádí některé výhody a nevýhody organizačního modelu:

Výhody

- Odráží organizaci společnosti.
- Je srozumitelný.
- Může se přirozenou cestou rozrůstat.
- Umožňuje prostředky organizovat podle funkce, kterou v podniku zastávají.

Nevýhody

- Obtížně se přizpůsobuje změnám struktur a názvů uvnitř organizace.
- Může být politicky citlivý.
- Je obtížné ho podporovat v případě rozdělování a slučování divizí.
- Implementace může být obtížná v případě, že se jednotlivé pobočky nacházejí v několika zeměpisných umístěních.

Z praxe: Lokality

Lokality jsou funkcí poskytovanou službou Active Directory, která může omezit nebo vyloučit problémy, jež mohou vzniknout, pokud organizační strukturu pojmenování použijete v organizaci s divizemi, které se nacházejí na více zeměpisných umístěních. Společnost může vytvořit lokalitu pro každý ostrůvek počítačů propojených prostřednictvím místní sítě (LAN). Například sídlo firmy může představovat jednu lokalitu, zatímco pobočka může představovat jinou lokalitu. Všem doménám, které se rozprostírají přes více lokalit, se automaticky nastavují replikační parametry tak, aby se optimalizovalo využití pomalého propojení lokalit prostřednictvím sítí WAN. Klienti jsou také v případě požadavků na službu automaticky směrováni do místních řadičů domény, což dále snižuje vytížení sítě WAN.

Zeměpisná konvence pojmenování

Pokud použijete zeměpisnou konvenci pojmenování, modelujete obor názvů na základě toho, jak je vaše organizace geograficky rozložena. Pokud například použijete tentýž kořen microsoft.com, může první úroveň sestávat z podúrovní corp.microsoft.com, noram.microsoft.com, europe.microsoft.com, africa.microsoft.com atd. Pod touto první úrovní mohou být jednotlivé další položky rozděleny na jednotlivé země nebo státy či oblasti, v závislosti na velikosti a složitosti organizace. Zeměpisná konvence pojmenování může mít následující výhody a nevýhody:

Výhody

- Již ze své podstaty je apolitická.
- Používá názvy, které pravděpodobně budou trvalé.
- Nabízí vyšší flexibilitu a rozlišovací schopnost.

Nevýhody

- Neodráží povahu organizace.
- Může vyžadovat další domény, aby byly splněny potřeby zabezpečení.

Poznámka: V sítích využívajících zeměpisné konvence pro názvy mohou být lokality užitečné při optimalizaci využití pomalých připojení prostřednictvím sítí WAN. Přestože se v sítích využívajících zeměpisné konvence pojmenování obvykle nevyskytují domény, které překlenují více lokalit, může využití lokalit dále optimalizovat využití propojení pomocí sítí WAN, protože dochází k optimalizaci vzájemné replikace domén v adresáři Active Directory.

Smíšené konvence pojmenování

Nakonec můžete zvolit kombinaci organizační a zeměpisné konvence pojmenování, zejména u oboru názvů s doménovou strukturou, kde různé podnikové kultury vyrostly samostatně a každá sleduje vlastní zájmy. Potíž samozřejmě je, že to může vést ke zmatkům a obtížím při podpoře kvůli nekonzistenci firemních postupů. Pokud obor názvů právě vytváříte, snažte se za každou cenu navrhnout racionální strukturu. V konečném důsledku si tím usnadníte práci s podporou.

I v případě, že v celé organizaci použijete čistě zeměpisnou konvenci pojmenování, je možné, že na nejnižší úrovni stromu budete chtít vytvořit organizační jednotky nebo domény, které odrážejí různé funkce, jež v podniku zastávají. Důvodem je, že skupiny pracující v podobných oblastech nebo na příbuzných projektech mívají potřebu přistupovat ke zdrojům podobné povahy. Například potřeby výrobního oddělení jsou obvykle jiné než potřeby účetního oddělení. Tyto společné potřeby vymezují přirozené oblasti, ve kterých je třeba poskytovat podporu a řídit provoz.

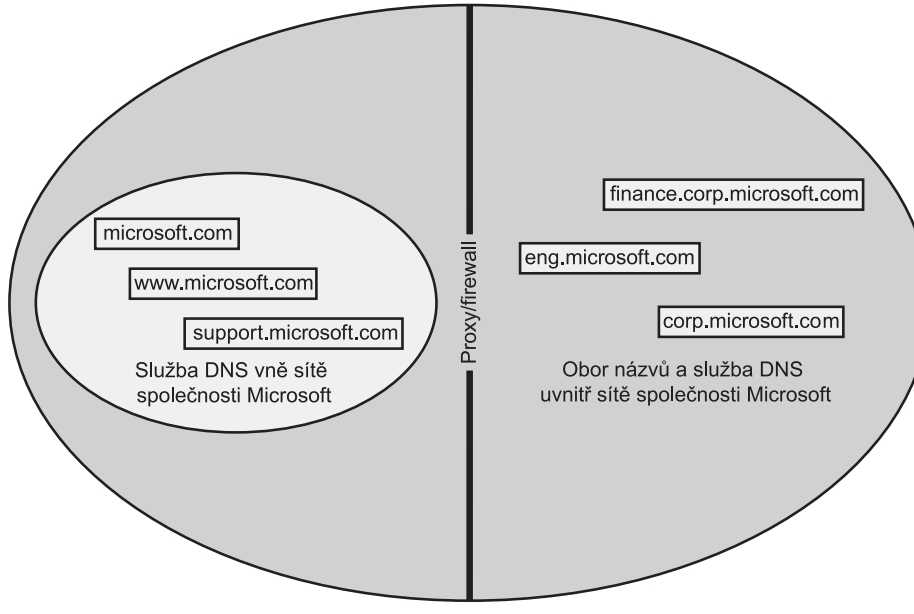
Určení překladu názvů

Jakmile definujete konvence pro názvy, musíte se dále rozhodnout, zda chcete, aby obor názvů používaný interně byl stejný jako ten, který prezentujete i vně vaší sítě. Ačkoliv si zpočátku můžete myslet, že by názvy měly být stejné, ve skutečnosti mohou existovat závažné důvody pro to, aby interní a externí obory názvů totožné nebyly.

Použití totožných interních a externích oborů názvů

Pokud používáte jediný obor názvů, máte vy a vaše počítače stejné názvy v interní síti jako ve veřejné síti Internet. To znamená, že od příslušné registrační autority na Internetu obdržíte jeden název a udržujete jediný obor názvů systému DNS (Domain Name System), ačkoliv je mimo společnost viditelná pouze část názvů. Konečná struktura sítě bude vypadat podobně jako na obrázku 3.3.

Pokud v interním i externím oboru názvů používáte tytéž názvy, musíte zajistit, aby mimo společnost bylo možné přeložit názvy pouze těch počítačů, které mají být pro vnější svět viditelné. Ujistěte se, že žádné servery služby Active Directory nejsou umístěny vně brány firewall. Je však také třeba se ujistit, že interní počítače mohou překládat názvy a přistupovat k prostředkům na obou stranách brány firewall.



Obrázek 3.3: Pokud jsou interní a externí obor názvů totožné, musí mít systém DNS různé zóny v závislosti na umístění, ze kterého přichází požadavek

Používání stejného interního a externího oboru názvů má následující výhody a nevýhody:

Výhody

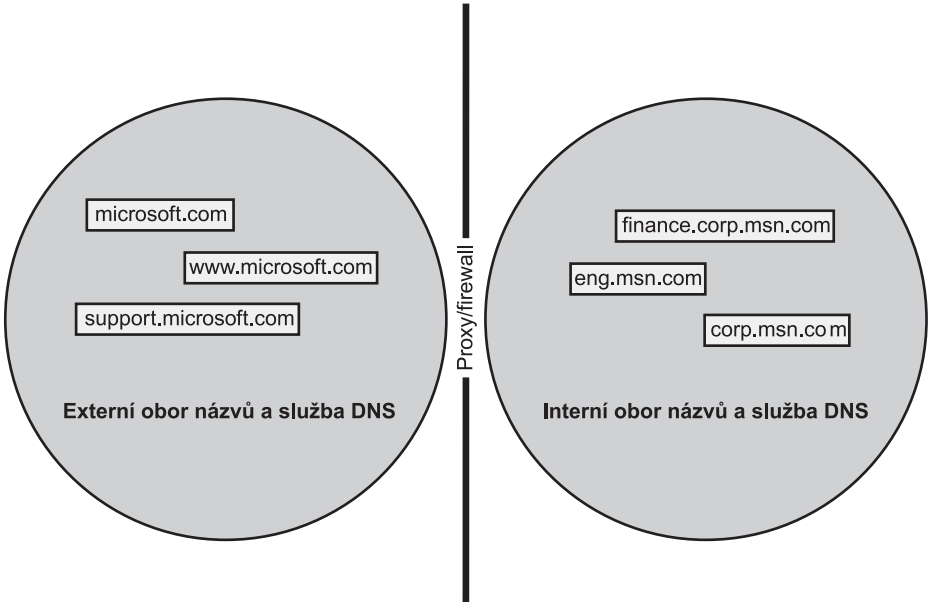
- Poskytuje konzistentní pojmenování interně i externě.
- Vyžaduje jen jedinou registraci každého názvu.
- Umožňuje uživatelům mít jedinou přihlašovací identitu a zároveň e-mailovou identitu.

Nevýhody

- Vyžaduje složitou konfiguraci serveru proxy.
- Vyžaduje spravování různých zón pro totožné názvy.
- Vyžaduje, aby uživatelé měli povědomí o tom, že jsou pro ně viditelné rozdílné prostředky v závislosti na to, odkud k nim přistupují.

Použití odlišných interních a externích oborů názvů

Pokud nastavíte odlišné interní a externí obory názvů, může být vaše jméno pro okolí *microsoft.com*, zatímco interně používáte *msn.com*. Všechny prostředky, které jsou umístěny vně sítě společnosti, používají názvy končící na *microsoft.com*, například *www.microsoft.com*. V rámci sítě společnosti však používáte samostatný obor názvů, které mají jako kořen *msn.com*, jak znázorňuje obrázek 3.4.



Obrázek 3.4: Veřejná a soukromá síť se samostatnými obory názvů

Používáte-li odlišné interní a externí obory názvů, jsou názvy DNS počítačů, které jsou veřejně dostupné, odlišné od názvů, které jsou viditelné pouze ze sítě za branou firewall. Při tomto scénáři nezapomeňte vzít v úvahu následující skutečnost: U příslušné registrační autority pro názvy v síti Internet je třeba zaregistrovat jak veřejné, tak i soukromé názvy. Možná se domníváte, že není nezbytné registrovat čistě interní názvy, které nechcete veřejně vystavit v síti Internet. Zajistíte tím však, že stejný název nebude používat nikdo jiný, což by vedlo k problémům při překladu názvů pro interní klienty.

Poznámka: Jedním ze způsobů, jak se vyhnout problémům s čistě interními názvy, zejména pokud máte problémy získat kontrolu nad názvem domény, protože je legitimně vlastněn někým jiným, je použití neexistujícího kořenového názvu domény, jako je .lan (například microsoft.lan). Touto strategií získáte interní název, který je pro danou část oboru názvů vhodný, aniž byste se dostali do konfliktu s názvem cizí domény. V systému Windows Server 2008 se jako výchozí interní kořenový název domény používá název .local. V celé této knize budeme jako primární doménu používat doménu example.local.

Použití odlišných interních a externích oborů názvů může mít následující výhody a nevýhody:

Výhody

- Poskytuje jednoznačné rozlišení, které prostředky jsou interní a které jsou externí.
- Nabízí snadnější správu a konfiguraci serveru proxy.
- Uživatelé díky němu mohou snáze porozumět rozdílům mezi interními a externími obory názvů.

Nevýhody

- Vyžaduje registrovat dvojí názvy.
- Znamená, že se přihlašovací jména uživatelů budou lišit od jmen používaných v e-mailové adrese.

Plánování doménové struktury

Po stanovení celkového návrhu oboru názvů je třeba navrhnout také doménovou strukturu, která ho bude podporovat. Každá větev doménové struktury může být buď doména, nebo organizační jednotka. To, zda je větev doménou, nebo organizační jednotkou, závisí na celé řadě faktorů, včetně potřeby replikace, zásad zabezpečení, dostupnosti zdrojů, kvality připojení atd.

Domény versus organizační jednotky

Stromy sítí systému Windows Server 2008 se skládají z domén a z organizačních jednotek. Jak domény, tak organizační jednotky vytvářejí z pohledu správy hranice mezi větvemi stromu, mají však různé implikace a požadavky na prostředky.

Domény

Základní jednotkou služby Active Directory systému Windows Server 2008 je doména, stejně jako v systémech Windows 2003 a Microsoft Windows NT 4. Všechny síťové objekty existují jako součást nějaké domény a v rámci domény platí jednotné zásady zabezpečení. Na rozdíl od systému Windows NT je v systémech Windows 2000, Windows Server 2003 a Windows Server 2008 zabezpečení založeno na protokolu Kerberos verze 5 a vztahy důvěryhodnosti jsou přenosné (tranzitivní). To znamená, že pokud doména A důvěřuje doméně B a doména B důvěřuje doméně C, důvěřuje také doména A doméně C.

Poznámka: I nadále je možné nastavit jednosměrné vztahy důvěryhodnosti, jaké se používaly v systému Windows NT 4. Ještě důležitější je, že vztahy mezi doménami systému Windows Server 2008 a staršími doménami systému Windows NT jsou založeny na jednosměrných a nepřenosných (netranzitivních) vztazích, které jsou systému Windows NT vlastní. Tyto vztahy je nutné vzít v úvahu při plánování doménové struktury.

S příchodem systému Windows 2000 se koncept primárního řadiče domény (PDC) a jednoho nebo více záložních řadičů domény (BDC) konečně stal historií. Systém Windows 2000 používal řadiče domény typu multimaster, které byly navzájem rovnocenné. Všechny řadiče domény měly v doméně stejnou autoritu, a pokud některý z řadičů přešel do režimu offline, ostatní řadiče doménu nadále spravovaly a ověřovaly. Jakýkoli

řadič domény mohl v doméně provést změnu a poté ji replikovat do ostatních řadičů v dané doméně.

Všimli jste si toho minulého času? Záložní řadiče domény se vrátily, pod novým názvem – řadiče domény jen pro čtení (RODC). Ale koncept se nemění – řadič domény jen pro čtení nemůže v adresáři Active Directory provádět změny. Více informací o řadičích domény jen pro čtení naleznete v kapitole 16 (Instalace a konfigurace adresářových služeb).

Poznámka: Přestože jsou v systému Windows Server 2008 všechny plnohodnotné řadiče domény stvořeny sobě rovné, může si být jeden řadič rovnější, pokud v doméně stále ještě podporujete počítače se systémem Windows NT (například pokud provozujete doménu nebo doménovou strukturu funkční úrovně, která podporuje řadiče domény systému Windows NT 4). V tomto zvláštním případě jeden řadič domény emuluje funkci primárního řadiče domény systému Windows NT 3.x a Windows NT 4. Ve výchozím nastavení tuto práci přebírá první řadič v doméně, ale v případě potřeby můžete roli emulátoru PDC přesunout na jiný řadič v doméně. Podrobné informace o této a dalších rolích hlavních operačních serverů získáte v kapitole 17 (Správa služby Active Directory).

Doména je ve službě Active Directory rovněž jednotkou replikace. Změny v doméně jsou replikovány do celé domény, a to i v případě, že se doména rozkládá přes několik lokalit nebo zeměpisných míst. Díky tomu mohou řadiče domény ve vzdálených lokalitách provádět v doméně změny a tyto změny replikovat po celé doméně. Pokud ve vzdálené lokalitě provozujete řadič domény jen pro čtení, ten samozřejmě změny provádět nemůže.

I když jsou přístupová práva přenosná přes hranice domény, jsou práva správce ve výchozím nastavení omezena na danou doménu. Díky tomu můžete práva ke správě udělit klíčovému uživateli konkrétní domény a nemusíte si dělat starosti s tím, že bude narušeno celkové zabezpečení organizace, protože tato práva končí na hranici domény, pokud nejsou explicitně udělena také pro jiné domény.

Organizační jednotky

Pojem organizační jednotky byl zaveden v systému Windows 2000. Organizační jednotky mají některé vlastnosti společné s doménami, nevyžadují však podobné režijní náklady na prostředky. Organizační jednotka je součástí domény a funguje jako kontejner objektů adresářové služby. Tvoří větev souvislého oboru názvů protokolu LDAP, přestože nemusí tvořit větev oboru názvů systému DNS, a sama může obsahovat další organizační jednotky. To znamená, že doména corp.microsoft.com může obsahovat další domény, například finance.corp.microsoft.com, a může obsahovat také organizační jednotky, jako je jednotka „hr“ domény corp.microsoft.com. Zde by jednotka měla název LDAP ve tvaru „OU=hr,DC=finance,DC=corp,DC=microsoft,DC=com“, ale název DNS by byl stále corp.microsoft.com, pokud byste ho explicitně nezměnili.

Organizační jednotka představuje vhodnou administrativní hranici a oprávnění a práva pro správu můžete uživatelům v organizační jednotce udělovat bez ohrožení zbytku domény. Organizační jednotka však nevyžaduje samostatný řadič domény ani se neúčastní replikace.

Návrh doménové struktury

Jakmile navrhnete obor názvů a všichni, kterých se to týká, s ním budou souhlasit, budete moci začít s návrhem a implementací doménové struktury. Návrh doménové struktury bude přesně odpovídat návrhu oboru názvů, i když se můžete rozhodnout, že některé hranice v oboru názvů vyžadují pouze organizační jednotky, nikoli celé domény. Založte svoji volbu mezi organizačními jednotkami a doménami na tom, zda pro entity v rámci hranice oboru názvů budete potřebovat samostatné zásady zabezpečení (například zásady určující složitost hesel a pravidla pro uzamykání účtů). Pokud konkrétní hranice oboru názvů nevyžaduje zásady zabezpečení, které by se lišily od zásad nadřazeného oboru názvů, bude pravděpodobně vhodné použít organizační jednotku, protože k implementaci vyžaduje méně prostředků.

Návrh struktury domén s jediným stromem

Pokud vytváříte jediný souvislý obor názvů, a tedy i čistě stromovou doménovou strukturu, vytvářejte domény v hierarchickém pořadí, počínaje vrcholem stromu. Tato nejvyšší doména představuje kořenovou doménu a obsahuje buď všechny uživatele v doméně (v případě malých modelů s jednou doménou), nebo vůbec žádné uživatele (pokud kořenovou doménu používáte jako strukturní). Pokud jste obeznámeni s modely domén v systému Windows NT4, tento systém zhruba odpovídá modelu domén typu „single-master“, ovšem s jedním důležitým rozdílem. Uživatelé se nemusejí a většinou by se ani neměli nacházet v doméně typu single-master, ale měli by se nacházet ve skutečně odpovídajícím umístění v doménové struktuře.

Jakmile začnete vytvářet větve stromu oboru názvů směrem dolů, budete vytvářet domény nebo organizační jednotky pro každou větev stromu. Rozhodnutí, zda vytvoříte organizační jednotku nebo řadič domény, závisí na celkovém modelu zabezpečení, kvalitě připojení k danému umístění a celé řadě dalších faktorů, včetně politických rozhodnutí, ke kterým došlo při prvotním plánování oboru názvů.

Poznámka: I zde popsaná struktura s jediným stromem je doménová struktura, přestože obsahuje jen jediný strom.

Návrh struktury domén s více stromy

Doménová struktura skládající se z více stromů se nejčastěji používá v případě, že se musíte přizpůsobit existujícímu oboru názvů, který není souvislý a nelze ho na souvislý snadno převést. Nakonec získáte několik kořenových domén, z nichž všechny jsou na stejné úrovni. Pod každou z těchto kořenových domén je souvislý obor názvů daného stromu. Každá větev oboru názvů protokolu LDAP je buď doména (s požadavkem na jeden nebo více řadičů domény), nebo organizační jednotka. Zpravidla vytváříte každý strom odshora dolů a každá větev stromu má automaticky přenosný vztah důvěryhodnosti s ostatními větvemi stromu.

Stromy ve struktuře sdílejí jediné schéma, konfiguraci a globální katalog a mezi všemi doménami ve struktuře existuje přenosný vztah důvěryhodnosti protokolu Kerberos. Hierarchie důvěryhodnosti v rámci každého stromu kopíruje hierarchii názvů systému DNS. Hierarchie důvěryhodnosti v doménové struktuře jako celku však odpovídá pořadí,

ve kterém jsou stromy připojeny do doménové struktury, přičemž se mezi každou dvojicí stromů v doménové struktuře vytváří obousměrný přenosný vztah důvěryhodnosti. Tyto vztahy jsou pro uživatele neviditelné, správci je však v případě potřeby mohou změnit, pokud potřebují zlepšit možnosti správy a odkazování.

Pokyny k zabezpečení domény

V rámci každé domény jsou požadavky na zabezpečení, zásady a konfigurace konzistentní. Pokud potřebujete změnit požadavky na zabezpečení a zásady pro podjednotku v rámci domény, vytvořte tuto jednotku jako doménu, nikoli jako organizační jednotku. Toto omezení mějte na paměti při plánování celého oboru názvů – abyste mohli používat oddělené zásady zabezpečení, potřebujete samostatné větve oboru názvů.

Co jsou zásady zabezpečení? Co s sebou přinášejí? Problematikou zabezpečení se zcela zabývá čtvrtá část této knihy, takže zatím uvedeme pouze souhrn toho, co zásady zabezpečení zahrnují:

- požadavky na přihlášení,
- certifikáty,
- stárnutí hesel a minimální požadavky na jejich délku,
- karty Smart Card nebo jiné doplňky pro ověřování,
- omezení na počítače a hodiny přihlášení.

Většina těchto bezpečnostních opatření bude v celé organizaci jednotná, ale mohou se vyskytnout oblasti, které vyžadují značně vyšší zabezpečení, než jaké je potřebné ve zbytku organizace. Pokud tomu tak je, naplánujte umístění oblastí vyžadujících tuto zvláštní péči do samostatné domény, aby jejich přísnější zabezpečení neovlivňovalo chod celé organizace.

Vytvoření organizačních jednotek

V případech, kdy nepotřebujete vytvářet samostatné domény z důvodů zabezpečení, ale chcete umožnit delegaci správy, vytvořte namísto podřízené domény samostatnou organizační jednotku. Můžete například mít doménu nazvanou *noram.example.com*, kterou chcete v rámci oblasti podle jednotlivých oddělení podniku rozdělit do jednotek. Mohli byste v doméně noram.example.com vytvořit podřízené domény pro oddělení prodeje, podpory, školení, lidských zdrojů, výroby a financí. Není však nutné vytvářet samostatné domény a jejich nezbytné řadiče pro každou z těchto jednotek, a to především proto, že všechny sdílejí jediné zásady zabezpečení. Takže stačí pro každé oddělení vytvořit organizační jednotku. Pokud budete později potřebovat jednu nebo více jednotek převést na doménu, můžete tak učinit, ačkoliv je tento proces složitější, než by musel být.

Organizační jednotky tvoří pro účely správy užitečné hranice. Správcům konkrétních organizačních jednotek můžete delegovat různá práva a úlohy správy, ulehčit tak správci domény a poskytnout organizačním jednotkám lokální kontrolu nad vlastními prostředky.

Plánování více domén

Pokud je vaše organizace natolik složitá, nebo i jen natolik velká, že již předem víte, že budete potřebovat více domén, věnujte více času předchozímu důkladnému naplánování jejich implementace. Čas strávený plánováním v předstihu se později mnohokrát vyplatí.

Nakreslete si plánovanou doménovou strukturu a porovnejte ji s plánovaným (nebo stávajícím) oborem názvů. Rozhodněte se, co musí být v každém případě doména a co může být bez problémů jen organizační jednotka. Určete servery, které budou sloužit jako řadiče domény. Mějte na paměti, že řadiče PDC a BDC známé ze systému Windows NT jsou zpět, nebo alespoň zčásti. Řadiče domény jen pro čtení nemohou v doméně provádět změny, ale všechny ostatní řadiče jsou rovnocenné. Změny provedené v jakémkoli řadiči domény s výjimkou řadičů jen pro čtení jsou šířeny do všech ostatních řadičů v doméně. Pokud jsou ve více řadičích provedeny změny současně, služba Active Directory k řešení případných konfliktů použije pořadová čísla aktualizací a časová razítka.

Plánování souvislého oboru názvů

Při plánování souvislého oboru názvů, a tedy i doménové struktury s jediným stromem nejprve vytvořte kořenovou doménu pro obor názvů. V tomto oboru názvů vytvořte primární účty správce, ale vytváření dalších účtů si ponechejte na později. Účty uživatelů a počítačů by měly být uloženy v listech těch stromů, ve kterých budou odvádět většinu své práce. Toto uspořádání kontrastuje se systémem Windows NT, kde bylo v případě provozování více domén často z důvodu povahy vztahů důvěryhodnosti nezbytné vytvářet všechny uživatelské účty na nejvyšší úrovni v doméně.

Pokud migrujete z existujícího prostředí systému Windows NT, mohli jste uživatele doposud spravovat v doméně typu single-master nebo multi-master. V tomto uspořádání můžete pokračovat, což může být nejsnadnější způsob, jak migrovat z existujícího prostředí. Podrobnější informace o upgradu domén naleznete v kapitole 6 (Upgrade na systém Windows Server 2008).

Určení potřeby doménové struktury s více stromy

Pokud již máte prostředí s více kořenovými doménami nebo bez souvislého oboru názvů, musíte místo prostředí doménové struktury s jediným stromem vytvořit doménovou strukturu s více stromy.

V prvním kroku se důkladně zamyslete nad nesouvislými obory názvů, které provozujete. Bylo by možné konsolidovat je do menšího počtu souvislých oborů názvů? Pokud to chcete učinit, učiňte tak teď. Konsolidovat je později by bylo daleko obtížnější a museli byste také svést náročnější politickou bitvu.

Vytvoření doménové struktury

Pokud dospějete k závěru, že neexistuje způsob, jak získat jediný souvislý obor názvů, což znamená, že budete muset vytvořit doménovou strukturu s více stromy, rozhodněte se, kde přesně bude kořen každého ze stromů doménové struktury umístěn. Popřemýšlejte o fyzickém umístění potenciálních řadičů domény, o rozložení sítě, o šířce pásma síťo-

vých linek do jednotlivých lokalit a o aktuálně existujících doménách a řadičích systému Windows NT. Jakmile budete mít kvalitní fyzickou a logickou mapu sítě, můžete začít plánovat strategii pro domény.

Nejprve vytvořte kořenové domény a poté začněte vytvářet stromy. Toto pořadí není zcela nezbytné – pokud zapomenete na některý strom nebo se něco změní, můžete se vrátit zpět a další strom do struktury přidat. Obecně je však lepší vytvořit nejprve kořeny, i kdyby mělo být důvodem jen dodržení správného pořadí vzájemné důvěryhodnosti stromů.

Doporučené postupy: Jakmile vytvoříte kořen stromu, neexistuje žádný snadný způsob, jak ho přejmenovat nebo odstranit. V systému Windows Server 2008 můžete měnit názvy domén pomocí programu Rendom.exe, ale to není něco, co byste chtěli provádět příliš často. Takže se stanovením doménové struktury moc nespěchejte – pokud ji naplánujete pečlivě, nepřipravíte se později o spánek.

Další informace: Podrobnější popis služby Active Directory a jejích principů naleznete v knize *Active Directory for Microsoft Windows Server 2003 Technical Reference*, kterou napsali Stan Reimer a Mike Mulcare (Microsoft Press, 2003), a v sadě *Microsoft Windows Server 2003 Deployment Kit* (Microsoft Press, 2003).

Shrnutí

Naplánování oboru názvů a struktury domén je klíčovým prvním krokem úspěšné implementace systému Windows Server 2008. Jedná se o opakovaný proces, který vyžaduje pečlivé plánování a důkladné porozumění politickým reáliím organizace. Obor názvů systému Windows Server 2008 může vytvářet jedinou souvislou hierarchickou stromovou strukturu, nebo může tvořit doménovou strukturu s několika stromy v nesouvislém oboru názvů. Všechny řadiče domény s výjimkou řadičů jen pro čtení mají v doméně stejnou autoritu a každá doména může obsahovat více organizačních jednotek za účelem delegace práv. Kapitola 4 (Plánování nasazení) je ještě zaměřena na plánování, v kapitole 5 (Začínáme) pak přejdeme od plánování instalace k její skutečné realizaci.

KAPITOLA 4

Plánování nasazení

Pracovali jsme se správci systémů, jejichž představa o nasazení spočívala ve vložení instalačního disku DVD do nového serveru a spuštění instalace. Jistě, takový postup je vždy zábavný, což je dobře, zvlášť když jej budete pravděpodobně používat donekonečna. Podle našich zkušeností je vložení disku DVD (nebo ať už instalaci provedete jakkoliv) posledním krokem celého procesu. Než začnete s instalací, už byste měli mít za sebou veškeré plánování, dojednání a přípravu všech nejdůležitějších částí úspěšného nasazení.

Zavedení předpokládá více než pouhou instalaci operačního systému, nebo dokonce síťového operačního systému. O specifikách nasazení – instalaci a konfiguraci aplikací, souborových a tiskových službách, službě Active Directory, komunikaci, zabezpečení a dalších funkcích – pojednávají další kapitoly. V této kapitole se zaměříme na veškerou práci, kterou je třeba provést, než vůbec vložíte první disk DVD do jednotky: na plánování infrastruktury hardwaru a softwaru, na které bude založena síť systému Windows Server 2008.

Úspěšné zavedení jakékoli sítě závisí v první řadě na plánování. Úspěšné plánování naopak závisí na shromáždění dat a jejich analýze i na určité míře předvídání a starém dobrém odhadu budoucnosti celé organizace. Rozhodnutí, která učiníte v prvních stádiích zavedení, ponesou vaše stopy, ať už v pozitivním nebo negativním slova smyslu. Vaše vize budoucnosti přetrvá roky, protože se bude podílet na chodu organizace, a vy budete nepochybně považováni za odpovědné v případě, že se tato vize ukáže být noční můrou. Čím více plánování tedy věnujete pozdějšímu nasazení, tím lepší to bude pro všechny strany.

Pro efektivní strategii informačních technologií jsou podstatné tři prvky:

- Analýza toho, jak možnosti IT infrastruktury splňují požadavky na provoz v současnosti. Kde je vaše technologická struktura adekvátní a v čem spočívají její nedostatky?
- Odhad obchodních a IT cílů. Potřebujete jednoleté, tříleté, pětileté a desetileté plány obchodních potřeb a IT vybavení, které bude splnění těchto potřeb nápomocno.
- Znázornění cesty k dosažení obchodních i IT cílů.

Tato kapitola pojednává o všech třech uvedených aspektech a zkoumá jejich vzájemné propojení.

V celé toto kapitole se zaměříme na otázky co, proč a jak. Záměrně jsme se vyhnuli uvádění některých z mnoha softwarových aplikací (ať už od společnosti Microsoft nebo od jiných výrobců), které jsou určeny k usnadnění celého procesu. To přenecháme obchodníkům. Myslíme si, že nejdůležitější věcí je správně pochopit související procesy. Určení nástrojů, které nám to mají usnadnit, by mělo být součástí tohoto procesu.

Fungování informačních technologií

Mluvíme-li obecně o IT odděleních, většina lidí by souhlasila s tvrzením, že účelem IT oddělení je sloužit aktuálním potřebám podniku a současně podporovat dlouhodobé cíle. Někteří by dokonce souhlasili i s tím, že IT oddělení by měla být klíčovým *aktivem* podniku, jakýmsi hnacím motorem podniku a pákou konkurenceschopnosti. Bohužel když titíž lidé začnou rozhodovat o svých vlastních IT odděleních, často se zdá, že k žádnému rozhodnutí nedošlo nebo se nad ním vůbec nezamysleli – síť působí dojmem, že se rozrostla jako houby po dešti bez přínosu čehokoli, co připomíná celkovou vizi. Změna situace je komplikovaná v mnoha faktorech:

- Zastaralý hardware a software
- Nekompatibilní operační systémy a aplikace, které byly přijaty k řešení specifických problémů pobočky nebo oddělení
- Rapidně se měnící technologie a požadavky uživatelů
- Negativní postoj ke změnám u těch, kterým se starší technologie zdají pohodlné
- Příliš málo zaměstnanců, času a peněz pro plánování a provedení inovace sítě

Poslední zmíněná položka je prakticky univerzální. Pokud však tyto faktory zatěžují vaši organizaci, je čas proti tomuto stavu začít bojovat. Situace se nemůže změnit přes noc a ani se nezmění, ale pečlivě promyšlené plánování s jasnými prioritami může věci rychle posunout kupředu.

Určení potřeb podniku

Určení potřeb podniku je téma, které se svým rozsahem může jevit jako ohromující. Vhodným výchozím bodem jsou jednotlivá oddělení nebo oblasti. Zvažte například potřeby oddělení prodeje, lidských zdrojů a marketingu. Co každá z těchto oblastí potřebuje už teď a jaké služby se vyplatí v budoucnosti?

Zvažte základní operace (jako pohledávky a vybavení), kterými je třeba se zabývat denně, a méně časté operace (zavedení nového produktu). Jaké druhy flexibility je třeba integrovat do systémů IT? Jaké druhy změn je třeba předvídat, aby bylo možné se vypořádat se zvýšenou činností sítě Internet nebo s rostoucím počtem přístupů uživatelů ve vzdálených oblastech?

Výzkum, který provedete u obchodních požadavků organizace, může také napomoci překonat odpor – a nějaký se vždycky najde – ke změnám v infrastruktuře. Když se lidé vašeho výzkumu účastní a sdílejí vaše porozumění aktuálním problémům a příležitostem organizace, bude jich čím dál více mít osobní zájem na podporování zavedení systému Windows Server 2008.

Specifika

Začněte seznamem podnikových funkcí sestavených podle důležitosti, které jsou nezbytné ke splnění podnikových cílů organizace. Tento seznam by měl obsahovat následující položky:

- Analýza celkových nákladů na vlastnictví identifikující možné oblasti, kde inovace infrastruktury IT mohou mít za výsledek snížení nákladů
- Analýza návratnosti investic označující finanční příležitosti, které mohou být důsledkem inovace infrastruktury IT
- Další podnikání, které může být důsledkem inovací infrastruktury IT
- Potenciální rizika vyplývající z toho, že infrastruktura IT nebude aktualizována

Tyto problémy jsou komplikované a v mnohém se překrývají, takže možná bude nutné tento seznam sestavit vícekrát. V závislosti na rozsahu operace může být snazší tento seznam rozdělit na spravovatelné části, z nichž každá představuje vlastní projekt s obsahy těchto menších seznamů tvořících celkový rámec plánování a opodstatnění pro celý podnik.

Pohled do budoucnosti

Chcete-li, aby vaše síť byla úspěšná, je třeba se důkladně zamyslet, jak bude vaše organizace vypadat za rok, tři, pět, či dokonce deset let. Bude více nebo méně centralizována? Rozšíří se její zeměpisná rozloha nebo bude spolupracovat se smluvními stranami? Budete mít více kvalifikovaných pracovníků, kteří vyžadují ke své práci volný tok informací v sítích? Budete potřebovat služby pracovníků „bez hranic“, kteří tráví čas v kanceláři, ale současně pracují z domu, patří k virtuálním týmům, nebo dokonce pracují v pobočkách klientů? Pracovníci s takovými potřebami mohou způsobit, že se běžně chápaný význam distribuce informací stane neadekvátním. Jak tito pracovníci získají, co potřebují? Jak zajistíte rovnováhu mezi mnohdy konfliktními požadavky na přístup a zabezpečení?

Samy počítačové sítě podléhají rychlým změnám, protože zkušenost s prací v síti mění vnímání uživatele, co je možné, a proto se mění také jejich pohled na to, co je potřebné. Jakmile bude možné získat přístup k údajům o prodeji nebo množství na skladě, roste poptávka po přístupu velmi rychle.

I ty nejmenší změny mohou mít značný vliv na vaši infrastrukturu IT. Předvídáním změn a důkladným plánováním zajistíte, že se vaše síť může vyvíjet tak, aby vyhovovala požadavkům na ni kladeným i v budoucnosti.

Odhad stávajících systémů

Je jen málo společností, které mají kompletní inventář softwaru a hardwaru. Ještě méně je takových, které znají rychlost, s jakou se mění jejich infrastruktura hardwaru a softwaru. Velké cíle pro budoucnost nelze splnit bez znalosti faktů o přítomnosti. I když jste si jisti, že chcete jet do Chicaga, máte jen malou naději, že se tam dostanete, pokud nevíte, zda jste zrovna v Savannah nebo v Seattlu. Následující části podrobně popisují kroky pro analýzu toho, co máte k dispozici, abyste mohli určit, co potřebujete a jak implementovat změny.

Dokumentace sítě

Znalost nasazeného hardwaru a softwaru a jejich využití je nezbytná pro rozvržení sítě a určení nejlepšího způsobu její implementace. Přece snad nerozbíjíte celou stávající síť a nenahrazujete ji zcela novým nejmodernějším zařízením! (A pokud ano, není to tak jednoduché, jak by se mohlo zdát.)

Místo toho budete raději postupně odstraňovat zastaralý hardware a software po dobu týdnů až měsíců, a možná dokonce let. Během této doby bude třeba nadále podporovat stávající hardware a software. Pečlivá a důkladná kontrola existující sítě se může vyplatit při určování toho, kde spočívají možné problémy (a příležitosti).

Organizační a fyzická infrastruktura

Udělejte si nákres fyzické sítě včetně pracovních stanic, serverů, směrovačů, elektrického rozvaděče a rozbočovačů. Tento nákres vám objasní, kde může být síť rozšířena (a kde naopak nemůže), ukáže optimální cesty směrování a umístění serverů a dalšího hardwaru. Současně může organizační graf znázornit všechny pracovníky oddělení IT a oblasti, za které jsou tito lidé zodpovědní. Díky tomu také uvidíte tok komunikace mezi těmito lidmi a slabá místa v něm. Ujistěte se, že jsou všechny důležité úlohy přiřazeny kompetentním osobám, a to ve všech sítích, organizačních jednotkách nebo lokalitách. Nechcete přece nasadit server ve vzdáleném umístění a mít tam někoho, kdo neumí nic víc než restartovat.

Vzorce dat síťového provozu

Abyste mohli stanovit optimální umístění směrovačů, rozbočovačů a přepínačů, požadavky na šířku pásma pro pracovní stanice a skupiny a budoucí potřeby na software pro správu sítí, potřebujete získat přehled o síťovém provozu. Nástroje analýzy sítí slouží k určení celkového (nebo zpětného) provozu sítí. Vzorce dat síťového provozu jsou také důležité při určování odpovídající rychlosti připojení sítě WAN nebo rychlosti, která bude použita ve vedení spojujícím podlaží v budově.

Síťové adresy

Během inovace sítě pomocí adresáře Active Directory budete pravděpodobně přiřazovat nové síťové názvy většině uzlů v síti. Přidáním adres uzlů k nákresu hardwaru, který jste pořídili dříve, můžete vyhodnotit, jaké adresy je třeba přiřadit a jaké kroky budou nutné k přechodu ze starého systému pojmenování k novému.

Konektivita operačního systému

Mnoho sítí je připojeno k jiným operačním systémům, jako je UNIX. Budete muset určit, které nástroje jsou nezbytné k udržování potřebného připojení nebo pro migraci těchto platforem na operační systém Windows Server 2008. Kromě toho může být umístění hardwaru – směrovače, přepínače a brány – velmi podstatné pro optimální připojení a rovněž může vyžadovat aktualizaci.

Poznámka: Sytém Windows Server 2008 obsahuje klientské a serverové součásti systému souborů NFS pro připojení platformy UNIX, společně se subsystémem SUA (Subsystem for UNIX Applications), který usnadňuje migraci aplikací platformy UNIX na platformu Windows. Další informace najdete v kapitole 27, „Spolupráce mezi systémy".

Externí připojení

Tak, jako většina společností neví, jaký hardware používají, může mít mnoho sítí nezdokumentované externí připojení. Většina společností ví o Internetu, síti WAN a faxových službách, ale často mají zcela nezdokumentované telefonní linky používané k telefonickému připojení nebo vzdálené správě sítí a často existují nezdokumentovaná (a obvykle neautorizovaná) bezdrátová připojení k síti. Vytvořte dokumentaci *všech* připojení. Proveďte důkladný úklid neautorizovaných přístupových bodů k bezdrátové síti. Nastal čas dostat je pod kontrolu.

Existující síťové operační systémy

Zdokumentování operačního systému na všech serverech a pracovních stanicích v síti je nezbytnou složkou úspěšné inovace nebo přenesení operačního systému. Měli byste určit, co musí inovace nebo migrace podporovat a jaké přípravné kroky jsou potřebné.

Existující aplikace a služby

Budete potřebovat soupis veškerého softwaru spuštěného na všech serverech a pracovních stanicích. Jakmile tento seznam budete mít, podívejte se podrobněji na typické i atypické požadavky každého programu na prostředky. Určitý program může například většinu času generovat mírné množství přenosu s výjimkou každotýdenního stahování 200 MB ze serveru WAN a požadavky účetního oddělení jsou diametrálně odlišné na konci roku než v čtvrtletí. V případě aplikací běžících na serverech nebo v operačních systémech, které budete přenášet, se ujistěte, že rozumíte migrační cestě pro danou aplikaci i pro operační systém.

Dále rozdělte a klasifikujte soupis aplikací a služeb do následujících kategorií:

- **Strategické** – software a služby, které jsou nezbytné pro obchodní operace a které jsou nejrelevantnější pro aktuální a budoucí cíle.
- **Taktické** – aplikace a služby, které mají hodnotu pro podnikání, ale které nepřinášejí optimální zisk.
- **Starší verze** – software a služby, které používají nějaké skupiny nebo oddělení, ale jejichž konec životnosti se blíží. Váš plán musí obsahovat požadavek na odstranění těchto součástí, než se dostanou do kategorie zastaralých.
- **Zastaralé** – aplikace a služby, které nemají přínos pro podnikání a jsou také překážkami. Cílem oddělení IT je odstranit je co nejdříve.

Každá součást patří do jedné z těchto kategorií a toto rozřazení vám může usnadnit přemýšlení a pomoci dát tvar vašemu plánu. Nepokoušejte se však provést tyto úkoly izolovaně. Zapojte součásti organizace, která danou aplikaci či službu používá v praxi. To je obzvlášť důležité, pokud si myslíte, že aplikace je buď starší verzí, nebo zastaralou aplikací. Důležitou součástí procesu pomoci vašim uživatelům opustit tyto starší verze aplikací je umožnit jim pochopit, kde se daná aplikace nachází v celkovém strategickém směřování organizace, a umožnit jim zapojit se do hledání lepších způsobů řešení problému, který má starší verze dané aplikace řešit.

Starší verze aplikací jsou mimořádně vhodní kandidáti pro virtualizaci. Jakmile odhalíte aplikaci, která spadá do této kategorie, přemýšlejte o tom, jak byste mohli efektivně zkombinovat a zracionalizovat využití serverů, které podporují virtualizaci těchto aplikací.

Zatížení serveru

Abyste vzali v potaz také efektivní zatížení serverů, budete potřebovat fyzický inventář serverů ve vaší síti. Ten vám pomůže odhalit kandidáty pro virtualizaci a konsolidaci serverů. Konsolidací zatížení na poddimenzovaných serverech a přesunutím celkového zatížení na virtualizované servery můžete významně snížit celkové zatížení administrací a můžete efektivněji využít vaše prostředky. Systém Windows Server 2008 obsahuje nové možnosti virtualizace, o kterých pojednává Kapitola 29, „Práce se službou Windows Virtualization".

Vytvoření přehledu

Studie, kterou společnost Microsoft realizovala před několika lety, zjistila šest vlastností úspěšných oddělení IT. Žádný z těchto závěrů není překvapivý, ale stojí za zopakování. Společnosti s úspěšným oddělením IT provádějí následující:

- **Přiřadí oddělení IT funkci řízenou podnikáním, nikoli funkci řízenou technologiemi** – jinými slovy: funkce zaměstnanců technologického oddělení musí být úzce spjata s podnikovými strategiemi a každodenní prací, která tyto strategie rozšiřuje.
- **Zakládají rozhodnutí o finančních prostředcích věnovaných do technologií na stejných rozhodnutích jako jakékoli jiné podnikové výdaje –** analýzy nákladů a návratnosti investic musí být stejnou součástí každého rozhodnutí o investování do IT jako v případě rozhodnutí o zakoupení nové budovy.

- **Trvají na jednoduchosti a flexibilitě v celém technologickém prostředí** – snižují počet zavedených technologií a platforem a snaží se získat maximální flexibilitu a snadnost zavedení.
- **Vyžadují krátkodobé obchodní výsledky z úsilí věnovaného do vývoje** – upřednostňuje se přírůstkové zavádění projektů, jako je například originální software nad vlastním softwarem. Pokud je nezbytný vlastní vývoj, zaměřte se na 20 procent funkčnosti, která obvykle doplňuje 80 procent hodnoty.
- **Vykazují konstantní každoroční vylepšení produktivity provozu** – měří výkon na základě interních a externích měřítek a standardů a snaží se o stálé zlepšování.
- **Mají za cíl mít takové oddělení IT, které je pohotové v oblasti podnikání, a takovou organizaci podnikání, která je pohotová v oblasti IT** – jednoduše řečeno: v lépe fungujících společnostech pracují oddělení IT a organizace podnikání společně. Mluví stejným jazykem, komunikují navzájem a rozumí vzájemně svým schopnostem a potřebám.

Toto jsou všechno velká prohlášení, kterým lze těžko oponovat na abstraktní úrovni, ale je obtížné je implementovat ve skutečném světě. Všichni však musíme někde začít, a pokud budete mít tyto cíle na paměti a pracovat na jejich implementaci, bude to mít přínos pro celou společnost.

Dalším krokem po vyhodnocení aktuální situace i podnikových cílů, kterých musíte dosáhnout, je naplánování postupu, který vás zavede, kam potřebujete. Tento postup bude obsahovat definici cílů, vyhodnocení rizik a plán implementace.

Definování cílů

Cíle zavedení musí být konkrétní, dosažitelné a změřitelné. A je nutno to zopakovat: cíle zavedení *musí být konkrétní, dosažitelné a změřitelné.* Konkretizujte a pojmenujte problémy, s kterými je nutné se utkat, a vyřešte, jak se vypořádáte s omezeními, jako jsou požadavky koncových uživatelů, náklady, plány a spolehlivost.

Váš plán pak musí konkrétně uvádět, čeho chcete v jednotlivých stádiích dosáhnout a jakým způsobem změříte, zda jste udělali, co jste si předsevzali. Při zavádění systému Windows Server 2008 v konkrétním oddělení přistupujte k úkolu jako dodavatel tohoto oddělení. Minimálně musíte provést následující:

- Určit, kdo musí odsouhlasit rámec projektu a kdo jej může zakončit.
- Určit rámec projektu: co je třeba nainstalovat, co je třeba nakonfigurovat a co budou uživatelé potřebovat být schopni dělat po ukončení projektu. Zapojte co největší možný počet lidí z oddělení.
- Dohodněte kritéria určující dokončení projektu. Projekt může být například považován za dokončený, pokud jsou všechny pracovní stanice připojeny k síti a je nainstalován určený software, všichni uživatelé se mohou přihlásit a data lze za všech podmínek získat v *n* sekundách nebo méně. Opět dbejte na konkrétnost a změřitelnost.
- Definujte metodu, která otestuje všechny oblasti projektu. Vyvoďte závěry. Vyhraďte si dostatek času na testování. Pravidelné okamžité testování vám později ušetří spoustu času a mrzutostí.

- Jakmile je projekt kompletní, považujte jej za dokončený. Dodatky a změny, které nejsou v původním rámci, chápejte jako nový projekt – další fáze nasazení. Je velmi důležité, aby každá fáze měla své dokončení.

Některé uvedené kroky se zdají zřejmé, ale je překvapující, jak často lidé netuší, zda jejich inovace systému skutečně k něčemu vedla, a pokud ano, zda byly výsledky tím, co bylo skutečně chtěné a potřebné. Dost často se stává, že pracovníci oddělení IT něco dokončí a navzájem si gratulují, zatímco skuteční „zákazníci" zdaleka nejsou spokojeni.

Z praxe: Nekonečný projekt

V časných dobách ve světě informačních technologií jsme pracovali na projektu migrace, který se značně nepovedl. Jedna velká společnost, která téměř výhradně používala sálové počítače a neměla téměř žádnou IT infrastrukturu nebo zkušenosti kromě sálových počítačů, se rozhodla do všech oddělení zavést osobní počítače. Ve stejnou dobu se v této společnosti instaloval velký podnikový softwarový balík, který měl změnit téměř všechny procesy, které v dané společnosti existovaly. Tento softwarový balík byl závislý na těchto osobních počítačích i na nových databázových serverech platformy UNIX.

Třebaže seznam problémů a lekcí, z kterých bychom se měli poučit díky naprostému neúspěchu projektu, by vydal na celou knihu, skutečné ponaučení spočívalo v cílech a rozsahu. Místo vytváření daného projektu po etapách s důkladným a dobře promyšleným testováním a plánem přezkoušení v každé etapě byl rámec projektu takový, že zasáhl celou společnost v podstatě najednou, bez jakýchkoliv jasných a předem odsouhlasených koncových bodů, které by umožnily ukončení projektu. Následkem toho nebyl projekt nikdy dokončen. Skončil překročením rozpočtu, s nešťastnými uživateli, nešťastnými zaměstnanci oddělení IT a nešťastným managementem – a drahou a špatně promyšlenou infrastrukturou, která nikdy nesplnila požadavky uživatelů společnosti. Nedopusťte, aby vaše projekty skončily jako tento. Udělejte vše, co je potřeba k tomu, abyste měli kontrolu nad rozsahem v každé fázi projektu a aby byly vaše cíle konkrétní, dosažitelné a změřitelné v každé etapě, s jasným a jednoznačným koncovým bodem, který tyto cíle *realisticky* splňuje.

Posouzení rizika

Nemůžete předpovídat, co všechno se může při zavádění pokazit, ale můžete si být jisti, že něco se stane. Mezi obvyklé problémy patří náhlá změna podnikových potřeb nebo požadavků uživatele, překročení nákladů nad očekávaný rámec a téměř nevyhnutelný časový skluz oproti plánu.

Rizika můžete zvládat proaktivně či reaktivně. Předvídání a zabránění problému je zřejmě lepší než reakce na potíže poté, co problém nastane. Věnujte čas určení prostředků a reakcí na všechna rizika, která jste odhalili. Potom udělejte totéž s riziky, která nemůžete určit předem, protože se vždy najde něco, co jste nepředvídali. Může to být nový server, který odpojil jistič elektrického obvodu, protože jste si neuvědomili, že je přetížený, nebo zastaralá aplikace, na kterou již všichni zapomněli, ale která stále podporuje klíčovou oblast vašeho podnikání. Může to být dokonce i klíčový člen vašeho týmu, který přijal nabídku práce dva týdny před datem implementace. Tento nepředvídatelný problém nebudete znát, dokud vám nepřeroste přes hlavu. Ale pokud si vyhradíte čas na identifikaci prostředků a reakcí na problémy, stále budete mít navrch oproti tomu, kde byste byli, kdybyste byli náhle překvapeni protože jste důkladně nepromysleli vhodné postupy.

Jsou ještě další věci, které vás při zavádění mohou zasáhnout více než nedokonale promyšlený plán. Plán, který zvažuje rizika, může urazit dlouhou cestu k minimalizaci pravděpodobnosti vážných problémů. Následující předběžná opatření vám pomohou minimalizovat rizika spojená s plánem:

- **Nejprve vytvořte vysoce rizikové součásti** – nejprve je třeba se samostatně věnovat již existujícím oblastem poskytujícím nepřetržité služby, jako jsou například servery pro zasílání zpráv nebo webový server. Nové součásti, které dříve nebyly součástí sítě, je také třeba samostatně otestovat a důkladně jim porozumět, než je nainstalujete někam, kde mohou ovlivnit důležité operace.
- **Zahrňte opravný faktor pro nepředvídané okolnosti** – nikdy nic nepracuje přesně tak, jak očekáváte. Z „pětiminutové instalace" se vyklube něco, co vyžaduje změnu hardwaru, aby vše fungovalo správně. Rychlá změna hardwaru vyžaduje půl hodiny konfigurace. Odhadněte, kolik času jednotlivé fáze zavedení zaberou, a tento čas zdvojnásobte.
- **Aktualizujte rozvrh a plán projektu** – jakmile se změní okolnosti a je dosaženo milníků, upozorněte všechny, kdo jsou do projektu zapojeni, aktualizací a rozesláním plánu a rozvrhu. Pokud zjistíte, že jste dva dny za první fází zavedení, neplánujte pouhé zrychlení práce, abyste to dohnali. Místo toho plán aktualizujte a určete, zda je zpoždění způsobeno nedostatkem v plánu (a proto ještě naroste), nebo pouhým jednorázovým selháním. Optimismus je dobrá vlastnost, ale důležitější je uvažovat realisticky.

Další informace: Správa rizik je komplexním tématem, nicméně je velmi důležité, aby mu zaměstnanci oddělení IT porozuměli, zejména v oblasti zabezpečení sítě. Průvodce Security Risk Management Guide společnosti Microsoft poskytuje expertní rady v této oblasti. Tohoto průvodce si můžete stáhnout z adresy: *http://www.microsoft.com/downloads/details.aspx?FamilyID=c782b6d3-28c5-4dda-a168-3e4422645459&displaylang=en*.

Shrnutí

Tyto první kapitoly určitě obsahují mnoho námětů k přemýšlení a také spousty námětů k realizaci. Přesto, bez ohledu na to, kolik základní práce jste provedli, byste možná měli převést některé ze svých plánů do praxe, třeba jen proto, abyste zjistili, jak je můžete vylepšit. Část 2 začíná další kapitolou, v níž zahájíte proces skutečné instalace a konfigurace systému Windows Server 2008.

ČÁST II

Instalace a konfigurace

V této části:

KAPITOLA 5

Začínáme

Instalovat systém Windows interaktivně na jediném počítači je zdlouhavé, instalovat ho interaktivně na pět počítačů je úmorné a instalovat dvacet serverů interaktivně už je vyloženě hloupé. Dokonce si myslíme, že instalovat ručně více než jeden nebo dva servery je nepříliš inteligentní plýtvání časem. V této kapitole popíšeme základní postup při instalaci systému Windows Server 2008 – a také to, jak ho zčásti nebo zcela zautomatizovat a usnadnit si tak život.

Kontrola požadavků na systém

Než se pokusíte systém Windows Server 2008 nainstalovat, měli bystě pečlivě zkontrolovat jeho požadavky na systém, abyste se přesvědčili, zda hardware vašeho počítače splňuje minimální požadované parametry. V tabulce 5.1 jsou uvedeny oficiální minimální požadavky systému Windows Server 2008 pro novou, čistou instalaci na „holé železo" – společně s našimi připomínkami k těmto požadavkům.

Tabulka 5.1: Hardwarové požadavky systému Windows Server 2008

Hardware	Požadavky	Komentář
Procesor	32bitový systém – 1 GHz 64bitový systém, x64 – 1,4 GHz 64bitový systém, Itanium – Itanium 2	Realističtější číslo je 2 GHz a více.
RAM	512 MB	Realističtější základ je 1 GB, doporučujeme 2 GB. K instalaci jádra serveru v běžném nasazení obvykle postačuje 1 GB RAM.
Disk	10 GB	Prosili bychom alespoň 40 GB prostoru na systémovém disku. A pokud je server vybaven více než 16 GB RAM, nejděte pod 50 GB.
Optická jednotka	DVD-ROM	Jednotka CD-ROM už nestačí, přestože je technicky stále možné získat speciální instalační média v podobě disků CD-ROM. K síťové instalaci nepotřebujete žádnou optickou mechaniku.
Grafická karta	800 × 600	1024 × 768 je realističtější údaj. Některé dialogy budou při rozlišení 800 × 600 jen stěží použitelné.
Další	Klávesnice a myš	
Síť	Není vyžadována	Dělají si z nás legraci? K připojení serveru k doméně, a vlastně k čemukoli, co budete se serverem chtít provádět, budete potřebovat podporovanou síťovou kartu.

Povšimněte si, co na seznamu vyžadovaného hardwaru chybí: Disketová jednotka! S příchodem systému Windows Server 2008 se konečně můžeme zbavit disketové mechaniky, a to i v případě, že potřebujeme načíst ovladače pro řadič pevného disku. Ovladače lze nyní zavádět z disků CD a DVD, z jednotky USB Flash a z diskety.

Z praxe: 64bitové systémy a podepsané ovladače

Velkou změnou v systému Windows Server 2008 je skutečnost, že všechny 64bitové verze systému vyžadují podepsané ovladače. To znamená, že se musíte předem přesvědčit, zda vaši dodavatelé hardwaru poskytují pro 64bitový systém Windows Server 2008 úplnou podporu. Pokud jde o poskytování podepsaných 64bitových ovladačů, neustále nás překvapuje liknavá odezva dokonce i předních dodavatelů, takže pokud používáte hardwarové karty či periferie, které nejsou součástí serveru objednaného od vašeho dodavatele, přesvědčete se před instalací 64bitové verze systému Windows Server 2008, že jsou pro ně k dispozici podporované a podepsané ovladače.

Pokud ovladač není dostupný, máte jen dvě možnosti: najít alternativního dodavatele hardwaru, který ovladač poskytuje, nebo provozovat 32bitovou verzi systému Windows Server 2008, pro kterou je ovladač k dispozici. Mezi námi, kdykoli narážíme na nedostatečnou podporu 64bitových ovladačů, raději měníme dodavatele. A nikdy nezapomínáme původním dodavatelům sdělit, proč se k nim obracíme zády.

Návrh prostředí pro nasazení

Pokud neprovádíte jen jedinou instalaci systému Windows Server 2008, je užitečné navrhnout prostředí pro nasazení systému, které vám umožní efektivněji nasadit systémy Windows na klientské i serverové počítače vaší organizace. V následujících částech bude popsáno, jak navrhnout takové prostředí pro nasazení systému, které umožní rychlé a přizpůsobené nasazení, aniž by přitom dosáhlo neúměrné složitosti.

Výběr metody instalace

Instalace systému Windows je nyní zcela založena na bitových kopiích. Nový instalační proces systému Windows Server 2008 nekopíruje na pevný disk jednotlivé soubory. Namísto toho pomocí souborů WIM (Windows Image) uloží na systémový disk cílového serveru úplnou bitovou kopii systému Windows Server 2008. Tento instalační postup založený na bitových kopiích se nemění, ať již používáte místní disk DVD nebo instalujete prostřednictvím sítě s použitím Služby pro nasazení systému Windows (WDS).
Přechod na instalaci založenou na bitových kopiích má několik výhod, mimo jiné:

- Skutečná doba instalace je podstatně kratší, bez ohledu na zdroj instalace.
- Přidávání a odebírání komponent systému nevyžaduje přístup k originálnímu instalačnímu médiu – všechny soubory se již nacházejí na médiu.
- Nasazení bitových kopií s předinstalovanými opravami nebo bitových kopií s přizpůsobenou sadou ovladačů je nyní jednodušší.

Pokud nasazujete systém Windows Server 2008 na jeden nebo dva servery, je snadné vzít instalační disk DVD a systém jednoduše nainstalovat. Pokud systém upgradujete, přejděte rovnou na kapitolu 6 (Upgrade na systém Windows Server 2008). Pokud instalujete nový server a používáte standardní médium DVD, přejděte k následující části s názvem Instalace systému Windows Server 2008. Podrobné informace o automatizaci nasazení systému Windows Server 2008 pomocí Služby pro nasazení systému Windows naleznete v části Automatizace nasazení serveru dále v této kapitole.

Instalace systému Windows Server 2008

Nainstalovat systém Windows Server 2008 ze standardního distribučního média na čistý server bez operačního systému znamená projít na samém začátku pouhých sedm obrazovek. Celý zbytek instalace proběhne bez jakýchkoli ručních zásahů. Nemusíte zadávat informace o síti, název počítače, název domény ani žádné další informace, s výjimkou skutečného kódu PID (Product Identification), který je přidružený k instalaci a k jazyku instalace.

Pohled zevnitř: Instalace bez zadání kódu PID

Systém Windows Server 2008 při instalaci obvykle vyžaduje zadání kódu Product ID. Zadání tohoto kódu však můžete vynechat. Budete pak muset vybrat přesnou verzi systému Windows Server 2008, který instalujete. Zobrazí se ještě několik dalších výzev a varování, pokud však chcete provozovat pouze demonstrační nebo zkušební prostředí po dobu nejvýše šedesáti dnů, jednoduše kód PID nezadávejte. Po těchto šedesát dnů budete mít k dispozici plně funkční instalaci systému Windows Server 2008. A dokonce i toto šedesátidenní období můžete až dvakrát prodloužit pomocí příkazu *slmgr –rearm*, pokaždé o dalších šedesát dnů.

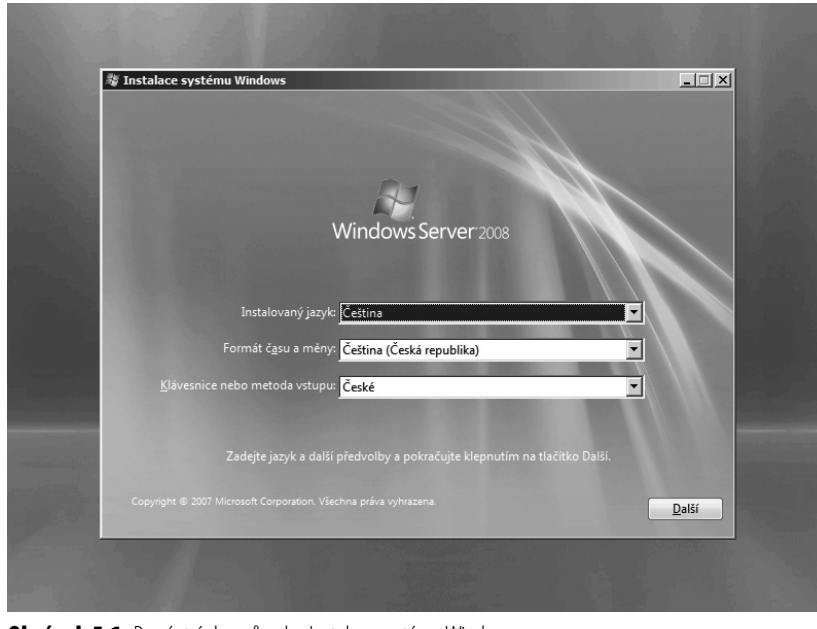
Pokud se rozhodnete server nainstalovaný bez kódu PID převést na plně aktivovaný server systému Windows Server 2008, zadejte kód PID *přesně* té verze systému Windows Server 2008, kterou jste vybrali při zahájení instalace. To znamená, že pokud jste k instalaci serveru použili médium retailové verze, musíte zadat klíč téže verze. Pokud jste vybrali systém Windows Server 2008 Standard, musíte zadat klíč retailové verze systému Windows Server 2008 Standard. Verzi nainstalovaného systému nelze změnit bez úplné přeinstalace systému Windows Server 2008.

Kód Product Key serveru nainstalovaného bez kódu PID zadejte pomocí příkazu *slmgr.vbs -ipk*.

Při instalaci systému Windows Server 2008 ze standardního média DVD na holý server postupujte následovně:

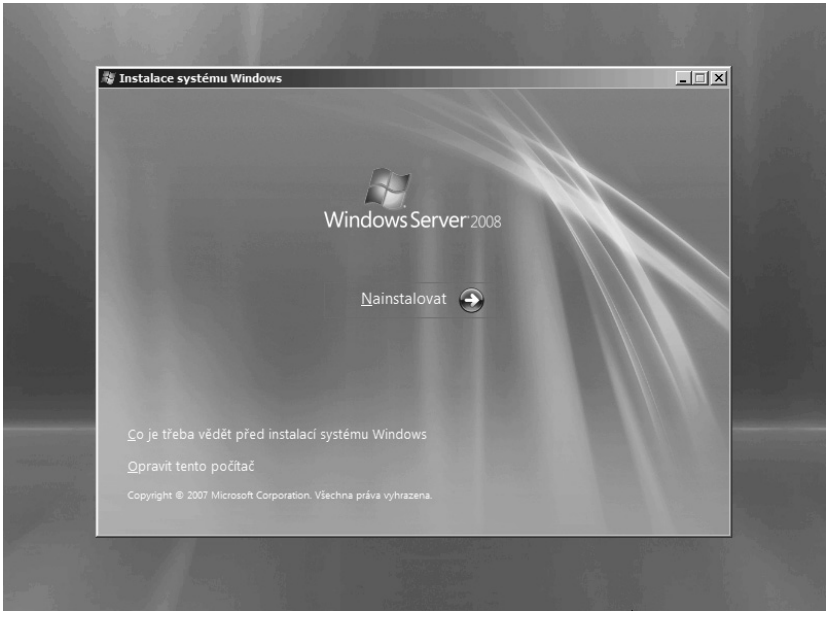
1. Zapněte server a okamžitě vložte disk DVD systému Windows Server 2008 pro architekturu systému Windows Server 2008, kterou chcete nainstalovat. Pokud se na primárním pevném disku nenachází spustitelný operační systém, bude ihned zahájen proces instalace systému Windows Server 2008. Pokud se na disku nachází spustitelný operační systém, budete vyzváni ke spuštění systému z disku CD nebo DVD stisknutím libovolné klávesy. V takovém případě stiskněte libovolnou klávesu.

2. Jakmile se zobrazí dialog Instalace systému Windows (Install Windows) znázorněný na obrázku 5.1, vyberte jazyk a další místní nastavení, která pro tuto instalaci budete chtít použít.



Obrázek 5.1: První stránka průvodce Instalace systému Windows

3. Klepnutím na tlačítko Další (Next) zobrazte dialog znázorněný na obrázku 5.2. Zde můžete vybrat, zda chcete opravit poškozenou instalaci systému Windows Server 2008 nebo zda před instalací chcete získat další informace.



Obrázek 5.2: Stránka Nainstalovat (Install Now) průvodce Instalace systému Windows

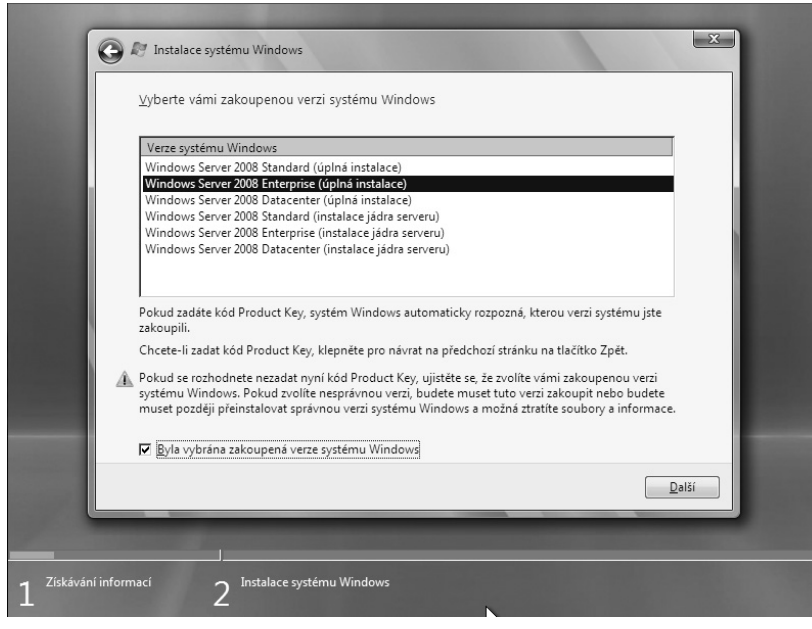
4. Klepnutím na tlačítko Nainstalovat (Install Now) zobrazte stránku Zadejte kód Product Key pro aktivaci (Type Your Product Key For Activation) průvodce Instalace systému Windows, znázorněnou na obrázku 5.3.

Obrázek 5.3: Stránka Zadejte kód Product Key pro aktivaci (Type Your Product Key For Activation) průvodce Instalace systému Windows

5. Zadejte kód Product Key pro tuto instalaci systému Windows Server 2008. (Informace o instalaci bez zadání kódu Product Key naleznete v rámečku Pohled zevnitř.)

6. Políčko Automaticky aktivovat systém Windows v režimu online (Automatically Activate Windows When I'm Online) ponechte zaškrtnuté, pokud nepotřebujete sami určit, kdy má k aktivaci dojít.

7. Klepnutím na tlačítko Další (Next) zobrazte stránku Vyberte operační systém, který chcete nainstalovat (Select The Operating System You Want To Install) průvodce Instalace systému Windows, znázorněnou na obrázku 5.4. Pokud instalujete bez zadání produktového klíče, zobrazí se mnohem delší seznam možných verzí.



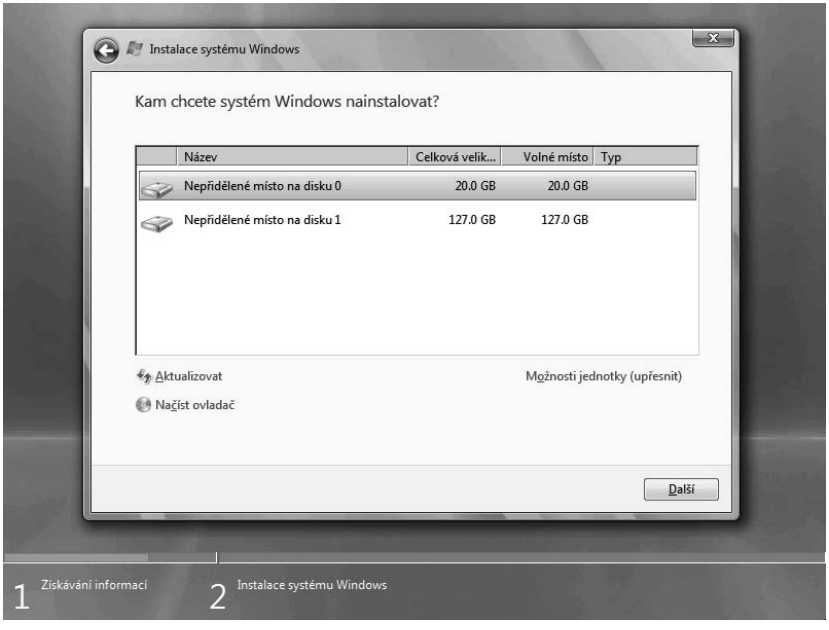
Obrázek 5.4: Stránka Vyberte operační systém, který chcete nainstalovat průvodce Instalace systému Windows

8. Vyberte buď úplnou instalaci (Full Installation), nebo instalaci jádra serveru (Server Core Installation). Tato možnost je nevratná: úplnou instalaci nelze později změnit na instalaci jádra serveru a naopak. (Podrobnosti o instalaci a konfiguraci jádra serveru systému Windows Server 2008 naleznete v kapitole 9 s názvem Instalace a konfigurace jádra serveru.)

9. Klepnutím na tlačítko Další (Next) zobrazte stránku Přečtěte si podmínky licenční smlouvy (Please Read The License Terms). Zaškrtněte políčko Souhlasím s licenčními podmínkami (I Accept The License Terms). Zde nemáte na výběr – pokud podmínky nepřijmete, instalace se ukončí.

10. Klepnutím na tlačítko Další (Next) zobrazte stránku Jaký typ instalace požadujete (Which Type Of Installation Do You Want). Při spuštění systému z disku DVD

můžete vybrat pouze možnost Vlastní (upřesnit) (Custom (Advanced)). Klepnutím na tuto možnost tedy zobrazte stránku Kam chcete systém Windows nainstalovat (Where Do You Want To Install Windows), znázorněnou na obrázku 5.5.



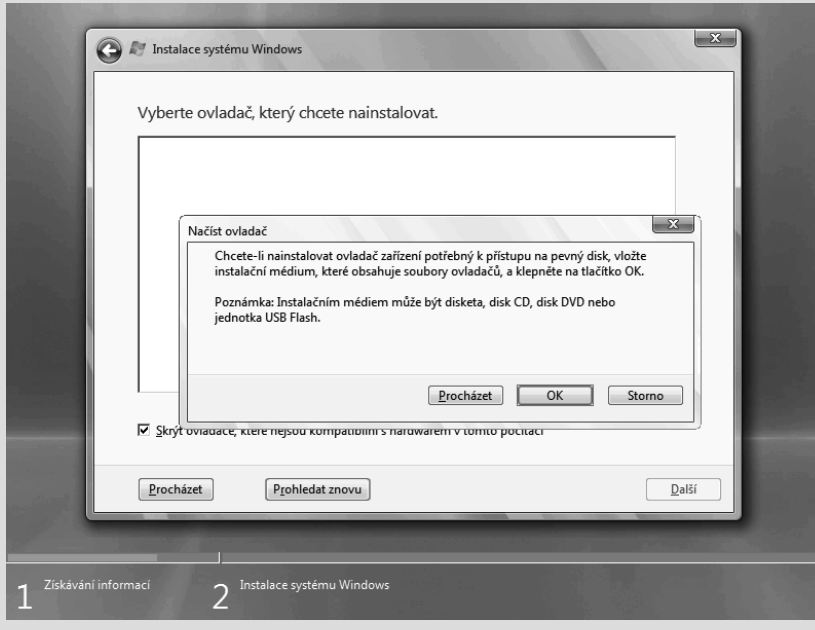
Obrázek 5.5: Stránka Kam chcete systém Windows nainstalovat průvodce Instalace systému Windows

11. První disk v počítači bude zvýrazněn. Můžete vybrat jakýkoli zobrazený disk, a pokud disk, do kterého chcete instalovat, není zobrazen, můžete po klepnutí na možnost Načíst ovladač načíst jakýkoli ovladač, který je k jeho použití zapotřebí. Po klepnutí na tlačítko Možnosti jednotky (upřesnit) (Drive Options (Advanced)) se zobrazí další možnosti, které vám umožní vybranou jednotku naformátovat nebo upravit její oddíly.

12. Jakmile vyberete jednotku k instalaci, klepněte na tlačítko Další (Next) a instalace bude zahájena. Od této chvíle bude instalace probíhat automaticky, až do okamžiku, kdy bude dokončena a kdy budete muset zadat heslo uživatele Administrator.

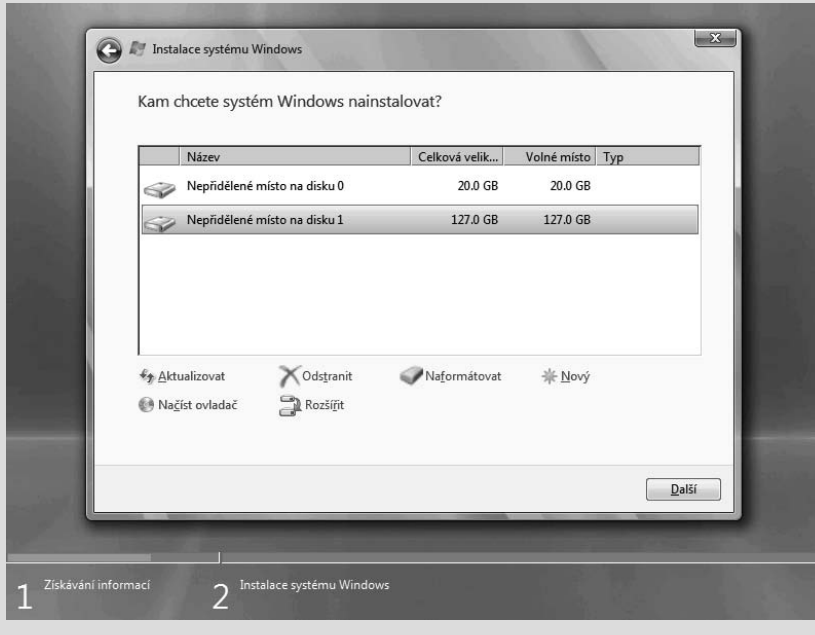
Pohled zevnitř: Možnosti jednotky

Výchozí jednotka, která je při instalaci systému Windows Server 2008 vybrána, je první jednotka v pořadí udaném operačnímu systému systémem BIOS. Pokud chcete instalovat na jinou jednotku, než jaká je vybrána, nebo pokud chcete přidat ovladače pro řadiče disků, které se nezobrazují, můžete výběr změnit. Pokud jste pracovali s dřívějšími verzemi systému Windows, jistě vás potěší, že systém Windows Server 2008 konečně podporuje načítání ovladačů paměťových zařízení i z jiného média, než je disketa. Jak ukazuje obrázek 5.6, můžete nyní načítat ovladače z diskety, disků CD a DVD a z disků USB Flash.



Obrázek 5.6: Systém Windows Server 2008 umožňuje načítat ovladače z disket, optických disků a z disků USB Flash

Pokud potřebujete změnit rozdělení disku na oddíly, naformátovat ho nebo i rozšířit oddíl o volný prostor, klepněte na tlačítko Možnosti jednotky (upřesnit) (Drive Options (Advanced)). Zobrazí se další možnosti správy a konfigurace disků při instalaci, znázorněné na obrázku 5.7.

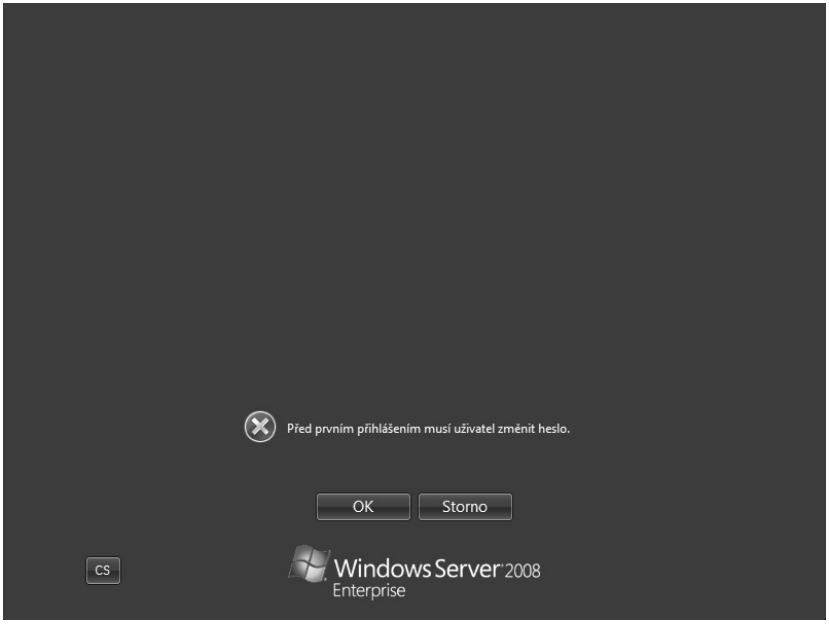


Obrázek 5.7: Při instalaci systému Windows Server 2008 je k dispozici volba Možnosti jednotky (upřesnit)

Důležitou novinkou mezi schopnostmi instalačního procesu systému Windows Server 2008 je možnost rozšířit existující oddíl. Přestože tato funkce při nové instalaci nehraje takovou roli, při recyklování starších počítačů může být užitečná. Oddíl můžete rozšířit o dostupné nevyužité místo na témže disku.

Poznámka: Pokud v průběhu instalace budete potřebovat zobrazit příkazový řádek, jednoduše stiskněte klávesu Shift+F10. Nyní můžete ručně spustit program diskpart.exe nebo jakýkoli jiný nástroj dostupný v této fázi instalace, ručně načíst ovladač nebo detailně upravit rozdělení disku na oddíly.

Po dokončení instalace se systém Windows Server 2008 restartuje a pokračuje zobrazením přihlašovací obrazovky. Budete muset zadat nové heslo uživatele Administrator, jak znázorňuje obrázek 5.8, a pak se budete moci přihlásit k novému serveru.



Obrázek 5.8: Nastavení počátečního hesla uživatele Administrator

Jakmile se přihlásíte, zobrazí se průvodce Úlohy počáteční konfigurace (Initial Configuration Tasks), který usnadňuje počáteční nastavení nového serveru. Všechny informace o tomto průvodci a o dalších počátečních krocích konfigurace serveru naleznete v kapitole 7 (Konfigurace nové instalace).

Instalace jádra serveru

Úžasnou změnou v systému Windows Server 2008 je možnost nainstalovat systém v režimu jádra serveru. Tato verze systému Windows Server 2008 s minimalistickým rozhraním podporuje méně rolí a funkcí a jen několik málo funkcí s grafickým rozhraním.

K instalaci vyžaduje výrazně méně diskového prostoru a má menší paměťovou režii. Co je ale nejdůležitější, představuje menší cíl pro útoky, a je tedy i bezpečnější. Protože také spouští méně služeb a instaluje méně komponent, vyžaduje méně údržby a menší objem aktualizací (a s nimi spojených rizik). Všechny podrobnosti a skripty pro instalaci a konfiguraci jádra serveru naleznete v kapitole 9 (Instalace a konfigurace jádra serveru).

Výchozí nastavení v počáteční konfiguraci

Protože se systém Windows Server 2008 při instalaci ptá na méně otázek, musí některé parametry nastavit na výchozí hodnoty, které můžete později nakonfigurovat pomocí průvodce Úlohy počáteční konfigurace. Tyto výchozí hodnoty uvádí tabulka 5.2.

Tabulka 5.2: Výchozí hodnoty instalace

Nastavení	Výchozí hodnota
Časové pásmo	(GMT+01:00) Praha, Bratislava, Budapešť, Bělehrad, Lublaň
Síť	Konfigurace pomocí protokolu DHCP
Název počítače	Vygenerovaný název
Doména nebo pracovní skupina	WORKGROUP
Automatické aktualizace	Nejsou nakonfigurovány
Nástroj Hlášení o chybách systému Windows	Vypnutý
Program CEIP (Zlepšování softwaru a služeb na základě zkušeností uživatelů)	Neúčastní se
Role	Žádné
Funkce	Žádné
Vzdálená plocha	Zakázaná
Brána Windows Firewall	Zapnuta

Automatizace nasazení serveru

Pokud instalujete pouze jeden nebo dva servery, má pravděpodobně smysl použít disk DVD a instalaci si před konzolou vysedět – obzvláště pokud se současně nepřipravujete na rozsáhlé nasazení klientů. Ale pokud jste právě dostali tucet serverů k instalaci a konfiguraci, určitě nebudete chtít sedět před konzolou. Budete chtít instalaci nějak zautomatizovat.

Z praxe: Standardizace informačních technologií

Mnohokrát jsme již slyšeli, že informační technologie standardizovat nelze. To ale vůbec není pravda. A pokud chcete mít sebemenší naději, že veškeré své IT procesy udržíte pod kontrolou, měli byste je začít standardizovat. Jsou k dispozici dobře zdokumentované metodologie pro standardizaci mnoha procesů v oblasti IT, včetně procesů ITIL (Information Technology Infrastructure Library) a MOF (Microsoft Operations Framework). A pokud nevíte, o čem je řeč, je už skoro pozdě na to, abyste si o nich něco přečetli. Dobrý výchozí bod je dokument *MOF: An Actionable and Prescriptive Approach to ITIL*, dostupný ke stažení na webových stránkách společnosti Microsoft (*http:// www.microsoft.com/tech-*

net/solutionaccelerators/cits/mo/mof/mofitil.mspx). Nasazování systémů je jedna z oblastí, ve kterých byste měli se standardizací začít. Pomocí nástrojů systému Windows Server 2008 můžete vytvořit standardizované bitové kopie pro servery i klienty a instalovat je automaticky.

Klíčová výhoda automatizovaného nasazování spočívá v tom, že každé automatické nasazení je zaručeně identické, což zjednodušuje průběžnou údržbu a aktualizaci.

V systému Windows Server 2008 jako mechanismus pro automatizaci nasazení slouží role Služba pro nasazení systému Windows neboli WDS (Windows Deployment Services). Služba WDS je rozšířený a vylepšený nástupce Služby vzdálené instalace (RIS) známé z předchozích verzí systému Windows Server.

Pohled zevnitř: Změny oproti službě RIS

Služba WDS je sice založena na službě RIS, nabízí však mnoho vylepšení a změn. Ve službě WDS serveru Windows Server 2008 přibyly oproti službě RIS mimo jiné následující funkce:

- podpora pro nasazení systémů Windows Vista a Windows Server 2008
- podpora prostředí Windows PE jako spustitelného operačního systému
- podpora souborů ve formátu .WIM (Windows Image)
- podpora nasazení systému pomocí vícesměrového vysílání
- nové grafické rozhraní

Služba WDS je dostupná i v systému Windows Server 2003, má tam však poněkud omezenější funkce. Nepodporuje všesměrové vysílání, server TFTP má méně funkcí a možnosti tvorby sestav jsou také omezenější.

Služba pro nasazení systému Windows se skládá ze tří skupin komponent:

- **Serverové komponenty** – nový server protokolu TFTP (Trivial File Transfer Protocol), vylepšený server PXE (Pre-Boot Execution Environment) a úložiště bitových kopií.
- **Klientské komponenty** – grafické rozhraní spouštěné jako součást prostředí Windows PE (Windows Pre-Installation Environment).
- **Komponenty pro správu** – různé nástroje používané ke správě serveru WDS a jeho komponent. Patří mezi ně grafická konzola Wdsmgmt.msc i nástroj příkazového řádku Wdsutil.exe.

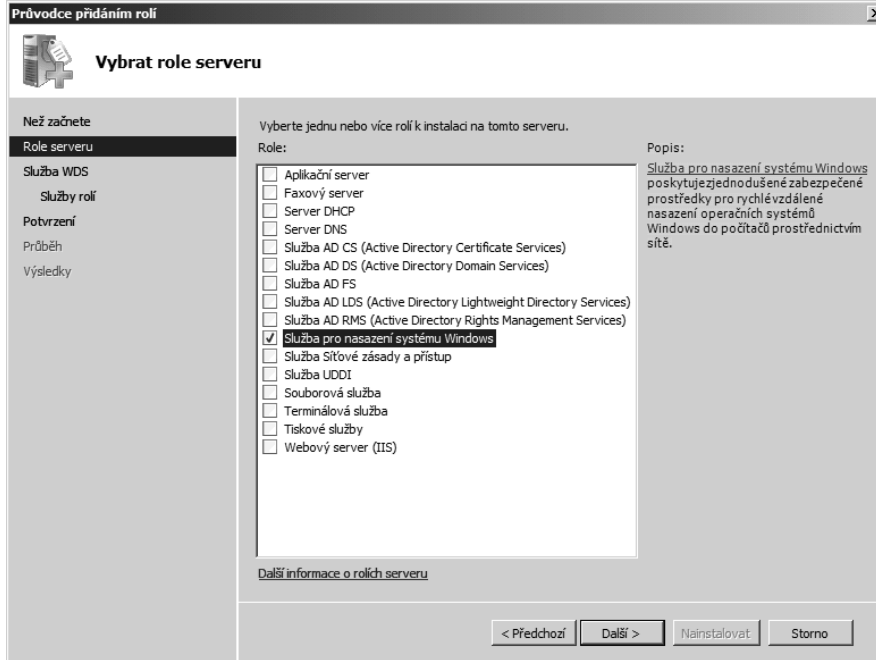
Instalace a konfigurace služby WDS

Role Služba pro nasazení systému Windows se instaluje pomocí téhož Průvodce přidáním rolí jako ostatní role serveru systému Windows Server 2008. Existují dvě služby rolí, ze kterých můžete vybírat: server služby pro nasazení a transportní server. Pokud chcete používat vícesměrové vysílání, ale nechcete úplnou sadu funkcí služby WDS, nainstalujte pouze transportní server. Ve většině případů však budete chtít nainstalovat oboje.

Postup při instalaci

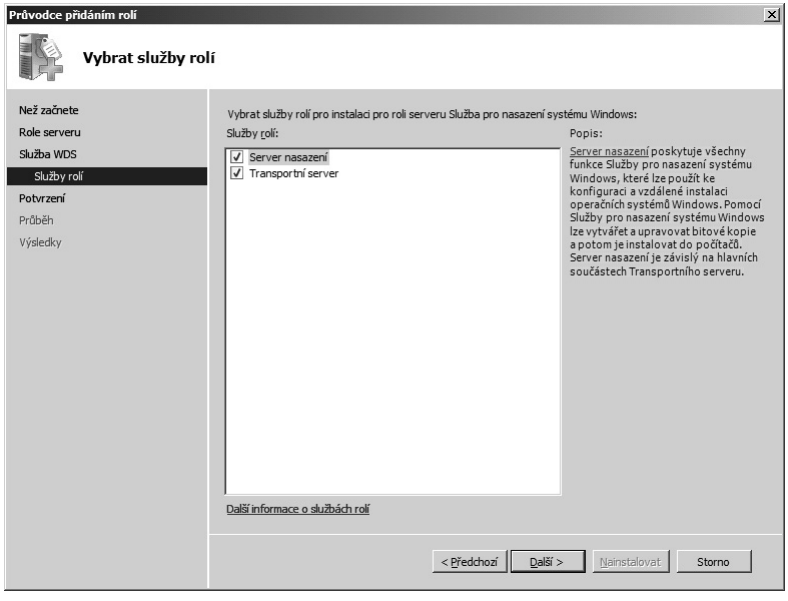
Roli Služba pro nasazení systému Windows nainstalujte následovně:

1. Spusťte nástroj Správce serveru (Server Manager), pokud již není spuštěný.
2. Označte položku Role (Roles) v levém podokně a v nabídce Akce (Action) klepněte na příkaz Přidat role (Add Roles). Zobrazí se Průvodce přidáním rolí (Add Roles Wizard).
3. Klepnutím na tlačítko Další (Next) zobrazte stránku Vybrat role serveru (Select Server Roles), znázorněnou na obrázku 5.9.



Obrázek 5.9: Stránka Vybrat role serveru Průvodce přidáním rolí

4. Vyberte položku Služba pro nasazení systému Windows (Windows Deployment Services) a klepnutím na tlačítko Další (Next) zobrazte stránku Přehled Služby pro nasazení systému Windows (Overview of Windows Deployment Services). Na této stránce naleznete některé základní informace o požadavcích služby WDS a odkazy na dokumenty týkající se konfigurace a správy služby WDS.
5. Klepnutím na tlačítko Další (Next) zobrazte stránku Vybrat služby rolí (Select Role Services), znázorněnou na obrázku 5.10. Pro většinu instalací vyberte obě služby této role, Server nasazení (Deployment Server) i Transportní server (Transport Server).



Obrázek 5.10: Stránka Vybrat služby rolí Průvodce přidáním rolí

6. Klepnutím na tlačítko Další (Next) zobrazte stránku Potvrdit vybrané možnosti instalace (Confirm Installation Selections).
7. Klepnutím na tlačítko Nainstalovat (Install) spusťte instalaci. Po dokončení instalace klepněte na tlačítko Zavřít (Close).

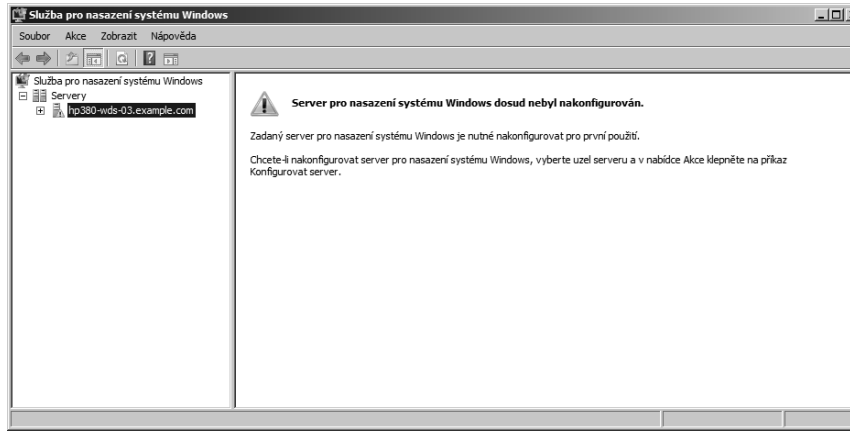
Počáteční konfigurace

Po instalaci služba WDS ještě vyžaduje základní konfiguraci, než je možné ji povolit. Než povolíte server PXE (Pre-boot Execution Enviroment) a služba WDS bude připravena nasazovat operační systémy, musíte nejprve provést počáteční konfiguraci a přidat bitové kopie, které mají být nasazovány. Službu WDS k nasazování verzí systému Windows Server 2008 nakonfigurujte následujícím postupem:

1. Spusťte konzolu Služby pro nasazení systému Windows, pokud již není spuštěna.

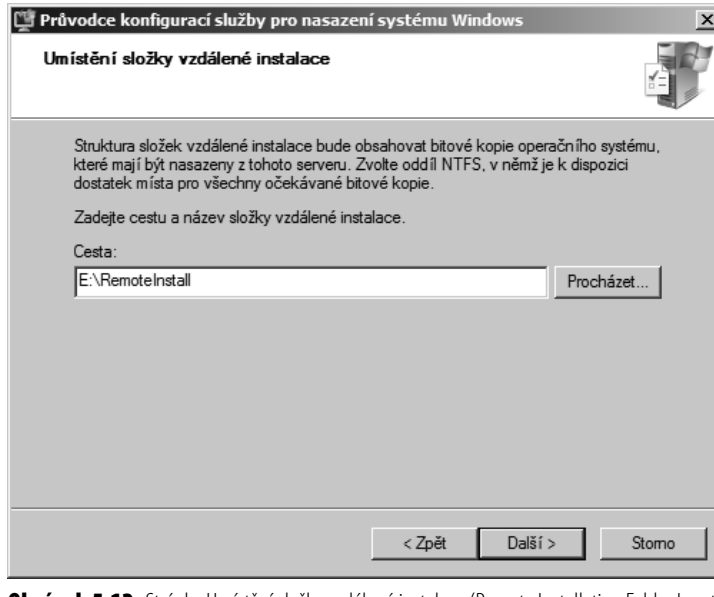
Poznámka: Konzolu Služby pro nasazení systému Windows otevřete zadáním příkazu *Wdsmgmt.msc* na příkazovém řádku.

2. Vyberte server, který chcete nakonfigurovat, jak znázorňuje obrázek 5.11, a pak v nabídce Akce (Action) vyberte příkaz Konfigurovat server (Configure Server).
3. Přečtěte si na úvodní stránce průvodce Služby pro nasazení systému Windows minimální požadavky pro službu WDS.



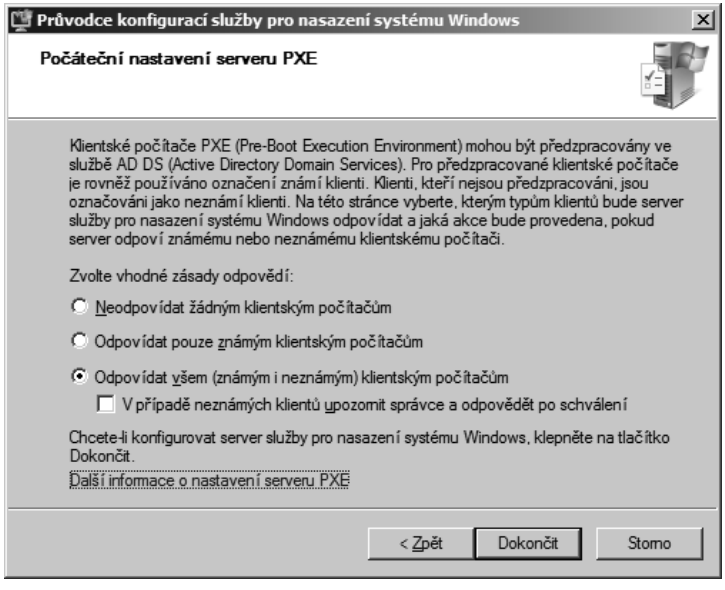
Obrázek 5.11: Konzola Služby pro nasazení systému Windows

4. Pokud vaše prostředí splňuje minimální požadavky, zobrazte klepnutím na tlačítko Další (Next) stránku Umístění složky vzdálené instalace (Remote Installation Folder Location), znázorněnou na obrázku 5.12. Zadejte umístění, do kterého mají být bitové kopie ukládány, nebo klepněte na tlačítko Procházet a umístění vyhledejte.



Obrázek 5.12: Stránka Umístění složky vzdálené instalace (Remote Installation Folder Location) průvodce Služby pro nasazení systému Windows

5. Klepnutím na tlačítko Další (Next) zobrazte stránku Počáteční nastavení serveru PXE (PXE Server Initial Settings), znázorněnou na obrázku 5.13. Ve výchozím nastavení server na požadavky PXE neodpovídá, což není nijak zvlášť užitečné. Pokud budete účty počítačů služby Active Directory vytvářet předem, vyberte možnost Odpovídat pouze známým klientským počítačům (Respond Only To Known Client Computers). Pokud předběžné vytváření účtů klientů neplánujete, vyberte možnost Odpovídat všem (známým i neznámým) klientským počítačům (Respond To All (Known And Unknown) Client Computers). Pokud účty počítačů předem vytvářet nebudete, můžete službu WDS nastavit tak, aby vyžadovala schválení neznámých klientů. (Známé klienty – ty, jejichž účty byly předem vytvořeny pomocí nástroje Uživatelé a počítače služby Active Directory – schválení nevyžadují.)

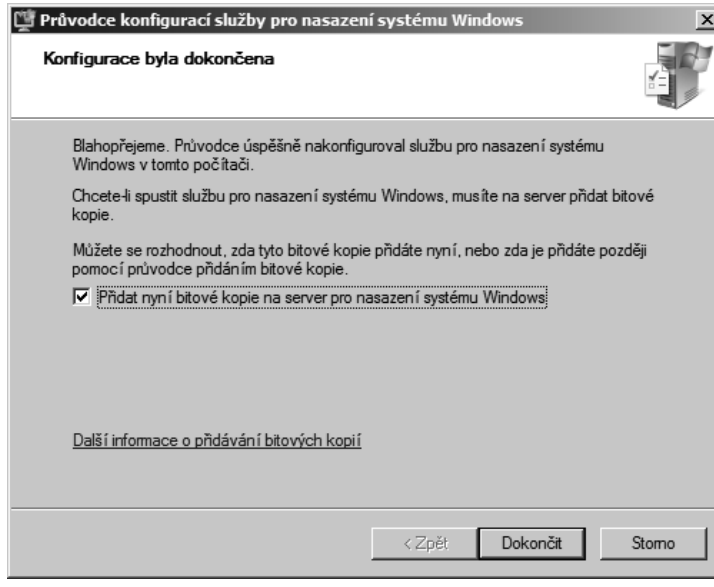


Obrázek 5.13: Stránka Počáteční nastavení serveru PXE průvodce Služby pro nasazení systému Windows

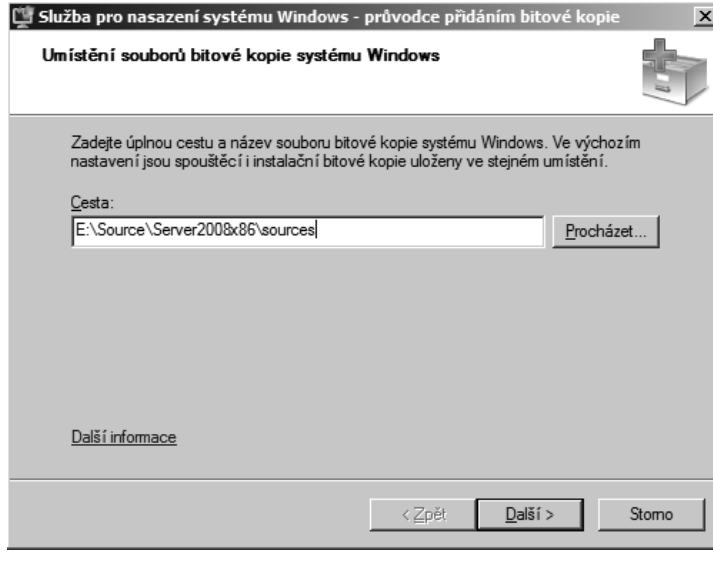
6. Klepnutím na tlačítko Dokončit (Finish) zobrazte stránku Konfigurace byla dokončena (Configuration Complete) průvodce Služby pro nasazení systému Windows, znázorněnou na obrázku 5.14.

7. Vyberte možnost Přidat nyní bitové kopie na server pro nasazení systému Windows (Add Images To The Windows Deployment Server Now) a klepnutím na tlačítko Dokončit spusťte průvodce přidáním bitové kopie (Add Image Wizard).

8. Na stránce Umístění souborů bitové kopie systému Windows (Windows Image Fines Location), znázorněné na obrázku 5.15, zadejte umístění bitových kopií systému Windows, které chcete používat. Toto umístění se musí nacházet na místním disku nebo v místním adresáři.



Obrázek 5.14: Stránka Konfigurace byla dokončena průvodce Služby pro nasazení systému Windows

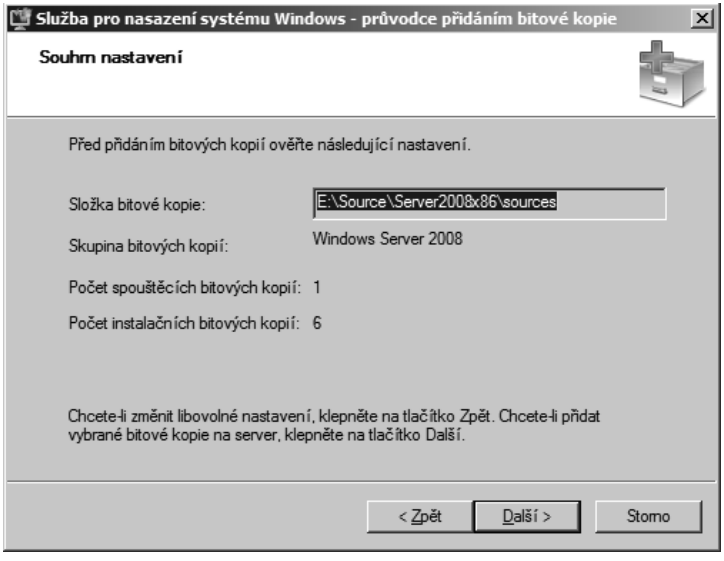


Obrázek 5.15: Stránka Umístění souborů bitové kopie systému Windows průvodce přidáním bitové kopie Služby pro nasazení systému Windows

Instalační a spouštěcí bitové kopie systémů Windows Server 2008 a Windows Vista se nacházejí v podadresáři Sources instalačního média.

9. Klepnutím na tlačítko Další (Next) zobrazte stránku Skupina bitových kopií (Image Group). Zadejte popisný název vaší první skupiny bitových kopií. (Výchozí název není zrovna dvakrát užitečný.)

10. Klepnutím na tlačítko Další (Next) zobrazte stránku Souhrn nastavení (Review Settings), znázorněnou na obrázku 5.16.



Obrázek 5.16: Stránka Souhrn nastavení průvodce přidáním bitové kopie Služby pro nasazení systému Windows

11. Klepnutím na tlačítko Další (Next) spusťte přidání bitové kopie. Jakmile budou přidány všechny bitové kopie, ukončete průvodce klepnutím na tlačítko Dokončit (Finish).

Nastavení dalších vlastností

Jakmile provedete základní konfiguraci serveru WDS, můžete nastavení serveru doladit. V konzole správy Služby pro nasazení systému Windows otevřete dialog Vlastnosti. Následující části popisují osm karet dialog Vlastnosti:

Obecné (General)

- Zde nejsou k dispozici žádná nastavení, ale zobrazují se zde základní informace o serveru, včetně jeho názvu, složky instalace a režimu nasazení.

Nastavení odezvy PXE (PXE Response Settings)

- Zásady odezvy PXE (PXE Response Policy)
- Neodpovídat žádným klientským počítačům (Do Not Respond To Any Client Computer)
- Odpovídat pouze známým klientským počítačům (Respond Only to Known Client Computers)

- Odpovídat všem (známým i neznámým) klientským počítačům (Respond to All (Known and Unknown) Client Computers)
- V případě neznámých klientů upozornit správce a odpovědět po schválení (For Unknown Clients, Notify Administrator And Respond After Approval)
- Zpoždění odezvy PXE (v sekundách) (PXE Response Delay (In Seconds)); výchozí hodnota je nula

Adresářové služby (Directory Services)

- Zásady pojmenování nových klientů (New Client Naming Policy). Upřímně, výchozí pojmenování klientů založené na uživatelském jméně je poněkud pošetilé. Pro nasazení skutečných serverů ho budete chtít změnit.

Důležité: Maximální délka názvu počítače je 15 znaků. Jsou-li použity výchozí zásady, může jako název být vygenerováno až 63 znaků, což při připojování k doméně způsobí potíže. Vyberte takové zásady pro pojmenování klientů, které zaručí, že názvy klientů nebudou delší než 15 znaků.

- Umístění účtu klientského počítače (Client Account Location). Doména nebo organizační jednotka, ve které jsou vytvářeny účty pro klientské počítače.

Spuštění (Boot)

- Výchozí spouštěcí program (volitelné) (Default Boot Program (Optional)). Umožňuje pro každou architekturu zadat jiný spouštěcí program, než jaký je pro danou architekturu výchozí.
- Výchozí spouštěcí bitová kopie (volitelné) (Default Boot Image (Optional)). Umožňuje pro každou architekturu zadat konkrétní výchozí bitovou kopii.

Klient (Client)

- Povolit bezobslužnou instalaci (Enable Unattended Installation). Je-li tato možnost zaškrtnuta, je možné provádět zcela bezobslužnou instalaci pomocí souborů bezobslužné instalace ve formátu XML.
- Vytvoření klientského účtu (Client Account Creation). Umožňuje zakázat automatické připojování k doméně.

DHCP

- Pokud je na serveru WDS místně spouštěna služba DHCP, použijte tuto kartu k její konfiguraci.

Nastavení sítě (Network Settings)

- Vícesměrová adresa IP (Multicast IP Addresses). Vyberte možnost DHCP, pokud to váš server DHCP podporuje, nebo zadejte rozsah adres IP, které mají být používány pro vícesměrové vysílání. (Výchozí hodnota je 239.0.0.1 – 239.0.0.254.)
- Rozsah portů UDP (UDP Port Range). Výchozí hodnota je 64001 – 65000. Tuto hodnotu neměňte.
- Profil sítě (Network Profile). Nastavte tuto možnost tak, aby odpovídala rychlosti vaší sítě.

Upřesnit (Advanced)

- Možnosti používané tímto serverem Služby pro nasazení systému Windows (Options Used By This Windows Deployment Services Server). Umožňuje zadat řadiče domény a servery globálního katalogu (nedoporučeno), nebo dovolí službě WDS zjišťovat servery dynamicky.
- Ověření DHCP (DHCP Authorization). Vyberte, zda tento server WDS chcete ověřit jako server DHCP.

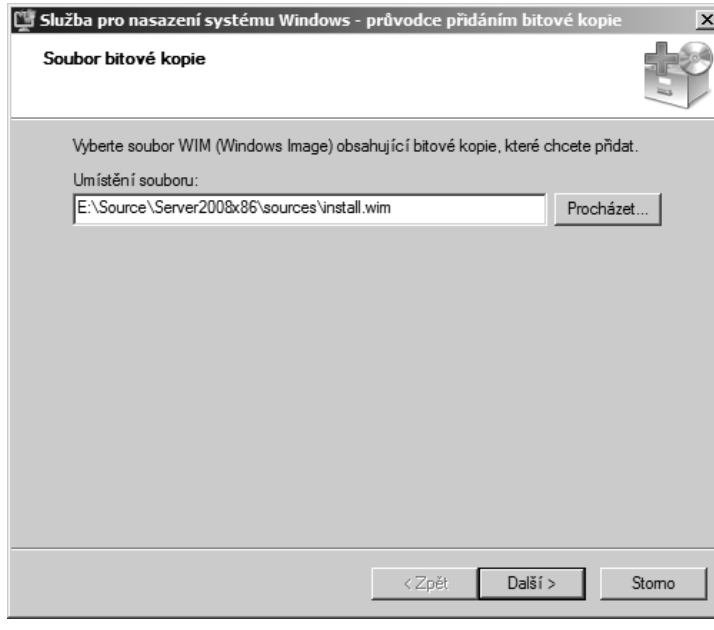
Přidání dalších bitových kopií

Počáteční konfigurace umožňuje určit bitové kopie, které má používat služba WDS, můžete však přidat také další bitové kopie pro jiné architektury a jiné operační systémy. Nebo můžete určit bitové kopie obsahující předinstalované aplikace a role serveru, které chcete používat ve velkém počtu různých klientů služby WDS.

Přidání standardních bitových kopií

Chcete-li přidat standardní bitové kopie operačního systému bez vlastních nastavení, postupujte následovně:

1. Spusťte konzolu Služby pro nasazení systému Windows, pokud již není spuštěna.
2. V levém podokně rozbalte název serveru WDS, do kterého chcete přidat bitové kopie, a vyberte položku Instalační bitové kopie (Install Images), pokud chcete přidat instalační bitové kopie, nebo Spouštěcí bitové kopie (Boot Images), pokud chcete přidat spouštěcí bitové kopie.
3. Chcete-li přidat spouštěcí bitovou kopii, klepněte v nabídce Akce (Action) na příkaz Přidat spouštěcí bitovou kopii (Add Boot Image). Chcete-li přidat instalační bitovou kopii, vyberte skupinu bitových kopií, do které chcete bitovou kopii přidat, a pak v nabídce Akce klepněte na příkaz Přidat instalační bitovou kopii (Add Install Image).
4. Na stránce Soubor bitové kopie (Image File) průvodce přidáním bitové kopie Služby pro nasazení systému Windows, znázorněné na obrázku 5.17, vyhledejte bitovou kopii, kterou chcete přidat, vyberte ji a klepnutím na tlačítko Otevřít (Open) se vraťte na stránku Soubor bitové kopie.
5. Klepnutím na tlačítko Další (Next) zobrazte stránku Seznam dostupných bitových kopií (List of Available Images). Zrušte zaškrtnutí všech bitových kopií, které instalovat nechcete.
6. Klepnutím na tlačítko Další (Next) zobrazte stránku Souhrn (Summary). Pokud vše vypadá podle vašeho očekávání, klepnutím na tlačítko Další (Next) přidejte bitové kopie, a jakmile průvodce akci dokončí, klepněte na tlačítko Dokončit (Finish).

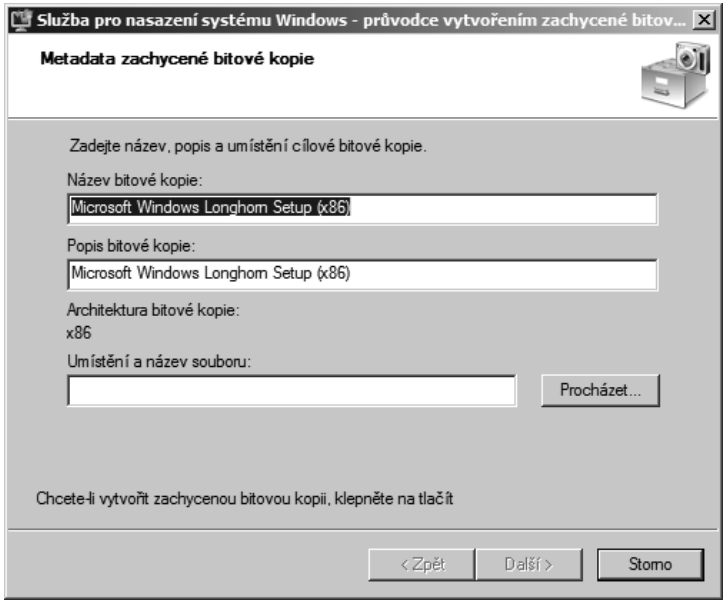


Obrázek 5.17: Stránka Soubor bitové kopie průvodce přidáním bitové kopie Služby pro nasazení systému Windows

Vytvoření zachycené bitové kopie

Zachycená bitová kopie je spouštěcí bitová kopie, která umožňuje vytvořit bitovou kopii konkrétního počítače a dovoluje tak vytvořit vlastní nasazovací (instalační) bitové kopie. Zachycenou bitovou kopii vytvořte následovně:

1. Spusťte konzolu Služby pro nasazení systému Windows, pokud již není spuštěna.
2. V levém podokně rozbalte název serveru WDS, do kterého chcete přidat bitové kopie, a vyberte položku Spouštěcí bitové kopie (Boot Images).
3. Označte spouštěcí bitovou kopii, kterou chcete použít k vytvoření zachycené bitové kopie, a v nabídce Akce (Action) klepnutím na příkaz Vytvořit zachycenou spouštěcí bitovou kopii (Create Capture Boot Image) spusťte průvodce vytvořením zachycené bitové kopie (Create Capture Image Wizard), jak znázorňuje obrázek 5.18.
4. Vyplňte pole na stránce Metadata zachycené bitové kopie (Capture Image Metadata) a klepněte na tlačítko Další (Next).
5. Jakmile je zachycená bitová kopie dokončena, klepněte na tlačítko Dokončit (Finish).
6. Označte položku Spouštěcí bitové kopie (Boot Images) a v nabídce Akce (Action) klepněte na příkaz Přidat spouštěcí bitovou kopii (Add Boot Image).
7. Vyhledejte zachycenou bitovou kopii, kterou jste právě vytvořili, a klepněte na tlačítko Další (Next).
8. Dokončete zachycení bitové kopie podle instrukcí průvodce přidáním bitové kopie.



Obrázek 5.18: Stránka Metadata zachycené bitové kopie (Capture Image Metadata) průvodce vytvořením zachycené bitové kopie

Poznámka: Abyste předešli problémům s duplicitními názvy a identifikátory SID, musíte počítače, ze kterých budete bitové kopie zachytávat, nejprve připravit pomocí programu Sysprep.exe. Nepodporovanou alternativou k programu Sysprep je program Newsid.exe, který můžete stáhnout z webových stránek společnosti Microsoft (*http://www.microsoft.com/technet/sysinternals/Utilities/NewSid.mspx*).

Přidání vlastních bitových kopií

Jakmile vytvoříte vlastní instalační bitovou kopii, můžete ji přidávat ke svým nasazením totožným postupem jako jakoukoli jinou bitovou kopii. Tato bitová kopie může obsahovat předinstalované ovladače pro neobvyklé síťové karty a předinstalované aplikace zjednodušující distribuci a nasazení standardních serverových bitových kopií.

Odstraňování potíží při instalaci

Instalace systému Windows Server 2008 je poměrně bezbolestný, ba i nudný proces. Pokud se však instalace z jakéhokoli důvodu nezdaří, jde nuda rychle stranou. Většina potíží při instalaci je způsobena vadným či nekompatibilním hardwarem, takže lze použít standardní techniky pro odstraňování potíží s hardwarem. Setkali jsme se mimo jiné s následujícími běžnými problémy:

- Nelze spustit systém z distribučního místa v síti.
- Při instalaci je zjištěn poškozený soubor.
- Nepodařilo se nalézt pevný disk.

- Vyskytla se chyba STOP.

V následujících částech popíšeme všechny tyto problémové scénáře a způsob jejich řešení.

Nelze spustit systém z distribučního místa v síti

Instalace systému Windows Server 2008 z distribučního místa v síti se spoléhá na schopnost kódu PXE síťové karty připojit se k distribuční sdílené složce a stáhnout do serveru prostředí WinPE (Windows Pre-Installation Environment), které následně do serveru zkopíruje spustitelnou bitovou kopii systému Windows Server 2008, kterou jste vybrali k instalaci. Celý tento proces závisí na síťovém prostředí a na ovladačích hardwaru v serveru, do kterého se pokoušíte systém nasadit. Při tom můžete narazit na následující problémy:

- Nelze se připojit k serveru PXE.
- Prostředí WinPE nelze načíst.
- Prostředí WinPE se nemůže připojit k distribučnímu serveru.
- Bitové kopie je poškozená.

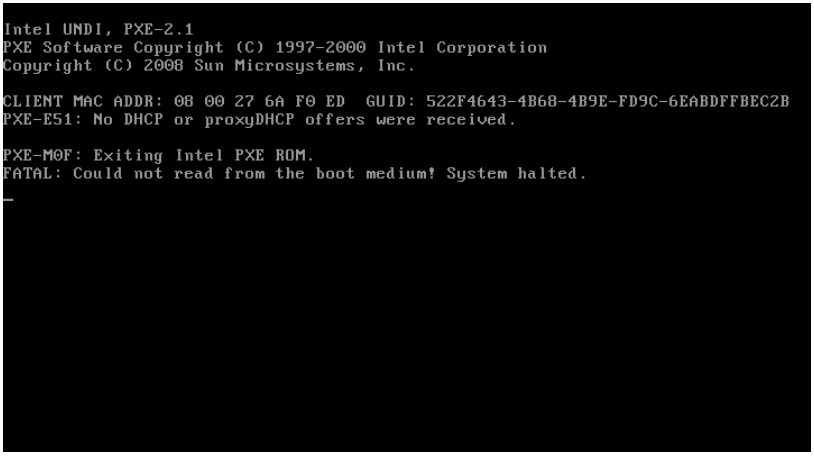
Nyní se zaměříme na tyto jednotlivé problémy a identifikujeme jejich možné příčiny.

Nelze se připojit k serveru PXE

Nejobvyklejší příčinou neúspěšného připojení k serveru PXE je skutečnost, že kód pro spouštění PXE není v systému BIOS povolen. To můžete rychle ověřit tak, že se podíváte, zda se síťová karta pokouší spustit systém ze sítě, jak znázorňuje obrázek 5.19. Přestože se výstup různých síťových karet při pokusu o spuštění systému pomocí protokolu PXE mírně liší, vypadají jejich zprávy v zásadě podobně. Pokud se vám podobný výstup nezobrazuje, zkontrolujte nastavení systému BIOS a ověřte, zda je povoleno spouštění systému ze sítě.

Obrázek 5.19: Pokus o připojení k serveru PXE při spouštění systému ze sítě

Dále možná příčina problému spočívá v nepřístupnosti serveru PXE prostřednictvím sítě. Obrázek 5.20 znázorňuje situaci, kdy se server pokusil o spuštění ze serveru PXE, ale neuspěl. Příčinou může být problém se síťovými kabely nebo mohly nastat potíže se samotným serverem PXE. Zkontrolujte síťové připojení a ověřte, zda server PXE pracuje správně.



Obrázek 5.20: Spuštění ze serveru PXE se nezdařilo

Prostředí WinPE nelze načíst

Jakmile se klient PXE v síťové kartě nového počítače připojí k serveru PXE, stáhne ze serveru soubory potřebné ke spuštění prostředí WinPE. Tato operace proběhne bez účasti jakýchkoli pevných disků: prostředí WinPE se celé načítá do paměti. Pokud počítač začne stahovat prostředí WinPE, ale pak se mu ho nepodaří úspěšně načíst, zkontrolujte, zda se nevyskytly problémy se sítí. Je také možné, že se jedná o projev vadné paměti počítače, ale taková chyba se v této fázi instalace projeví s menší pravděpodobností než v jiných fázích.

Prostředí WinPE se nemůže připojit k distribučnímu serveru.

Jakmile je prostředí WinPE zavedeno do počítače, jeho dalším úkolem je připojit se k serveru WDS a stáhnout příslušnou bitovou kopii systému Windows na pevný disk nového počítače. Pokud se připojení k serveru WDS nezdaří, má vinu pravděpodobně absence ovladače síťové karty v prostředí WinPE. Budete muset vytvořit vlastní spouštěcí bitovou kopii, která obsahuje potřebné ovladače síťové karty, nebo použít jinou síťovou kartu.

Poškození bitové kopie

Další možný způsob, jakým může instalace selhat, je následující: Všechny počáteční síťové kroky a kroky prostředí WinPE zdánlivě proběhnou správně a bitová kopie systému Windows Server 2008 se začne stahovat ze serveru WDS, ale k chybě dojde v průběhu jejího stahování nebo poté, co se počítač pokusí do stažené bitové kopie restartovat. To může být zaviněno špatnou bitovou kopií na serveru WDS nebo problémy se sítí, které způsobí poškození bitové kopie při přenosu.

Distribuce bitových kopií prostřednictvím sítě je náročný proces, který zatěžuje síťové komponenty po celé trase od serveru WDS až po počítač, do kterého je systém nasazován, a selhání v jakémkoli bodě může způsobit poškození dat. Zkontrolujte síťové komponenty a zjistěte, zda výrobce síťové karty neposkytuje aktualizovaný firmware.

Při instalaci je zjištěn poškozený soubor

I v případě, že instalujete z disku DVD, může dojít k selhání z důvodu poškozené bitové kopie. Není příliš pravděpodobné, že by disk DVD dodaný společností Microsoft byl vadný, přesto se to může stát a disk nemusí být čitelný. Pokud vypalujete disk DVD ze stažené bitové kopie ve formátu ISO, může dojít jak k chybnému stažení, tak i k chybnému vypálení disku DVD, a obojí způsobí poškození bitové kopie. Další možnou příčinou chyby, která se projevuje jako poškozený nebo chybějící soubor při instalaci, je vadný paměťový modul. Pokud dojde k chybě při instalaci z disku DVD, zkuste následující kroky:

1. Pokud použitý disk DVD byl sériově lisované médium, pokuste se o instalaci z jiného disku DVD.
2. Pokud jste si použitý disk vypálili sami, pokuste se o instalaci z lisovaného disku DVD nebo se pokuste disk vypálit znovu, a to poloviční rychlostí oproti rychlosti, kterou jste vypálili vadný disk.
3. Pokud jste si použitý disk vypálili sami a opětovné vypálení poloviční rychlostí problém nevyřešilo, stáhněte soubor ISO znovu.
4. Pokud žádná z těchto možností nepomohla, ověřte, zda jsou kabely ve skříni serveru správně usazené. Nahraďte jednotku disků DVD jinou jednotkou.
5. Proveďte důkladný test paměti.

Z praxe: Ověřování stažených souborů pomocí kódu CRC

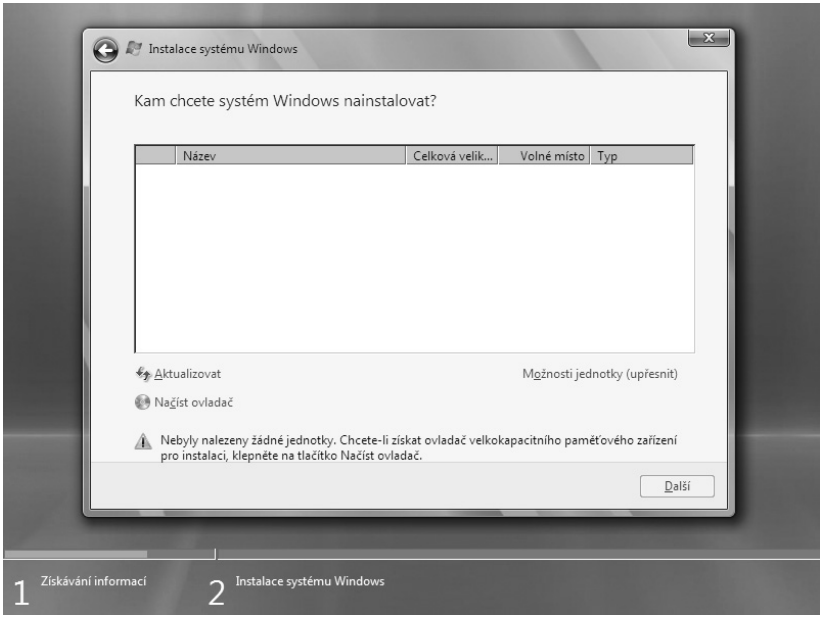
Kód CRC (Cyclic Redundancy Check) je způsob jednoznačné identifikace souboru. Mnoho zdrojů souborů ke stažení poskytuje kontrolní součet CRC, který můžete porovnat se staženým souborem na místním pevném disku. K výpočtu kódu CRC budete potřebovat nástroj, který se spouští se zadaným názvem souboru. Existuje mnoho volně dostupných nástrojů pro výpočet kódu CRC, například nástroj CRC305.exe, který si registrovaní uživatelé sítí MSDN a TechNet mohou stáhnout na stránce Tools, SDKs, and DDKs části Subscriber Downloads.

Nástroj CRC305 umožňuje kontrolovat jak soubory bitových kopií, tak i skutečné disky CD a DVD. Důrazně doporučujeme, abyste v případě použití disku DVD, který jste si vypálili sami, ověřili jeho kód CRC vůči známé referenční hodnotě, je-li k dispozici. Podle našich zkušeností jsou poškozené bitové kopie disků DVD zaviněné chybným stažením nebo chybným vypálením disku DVD nejčastější příčinou chyb při instalaci systému Windows Server 2008.

Nepodařilo se nalézt pevný disk

Systém Windows Server 2008 v průběhu instalace zkoumá počítač a pokouší se nalézt pevný disk, do kterého by se mohl nainstalovat. Pokud se mu nepodaří pevný disk nalézt,

znamená to, že pro řadič disku nemá potřebný ovladač, a budete vyzváni k poskytnutí ovladače v průběhu instalace, jak znázorňuje obrázek 5.21.



Obrázek 5.21: Pokud průvodce Instalace systému Windows nenalezne žádné jednotky, vyzve k načtení ovladačů

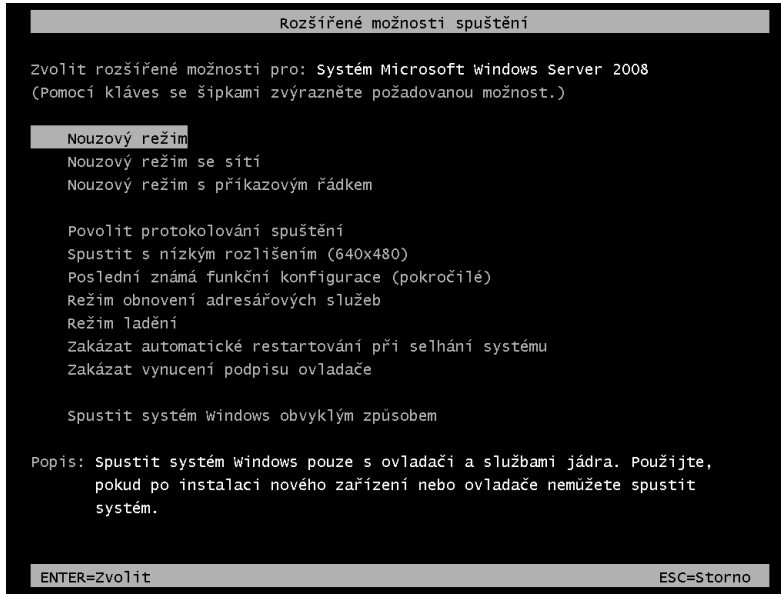
Systém Windows Server 2008 podporuje načítání ovladačů z paměťových zařízení připojených prostřednictvím sběrnice USB, z disků CD a DVD a z disket. To je velké zlepšení oproti starším verzím systému Windows Server, které podporovaly načítání ovladačů velkokapacitních paměťových zařízení pouze z disket.

Tuto techniku můžete použít také v případě, že se v počítači nachází více velkokapacitních paměťových zařízení a zařízení, do kterého chcete systém Windows Server 2008 nainstalovat, se v seznamu dostupných jednotek nenachází.

Vyskytla se chyba STOP

Někdy může závažná chyba při instalaci systému Windows Server 2008 způsobit, že se server začne nečekaně a opakovaně restartovat. Taková chyba se nazývá chyba STOP. Jednotlivé chyby STOP mají vlastní kódy, které umožňují odstranit jejich příčiny.

Pokud se chyba STOP zobrazí na obrazovce po příliš krátkou dobu a počítač se pak automaticky restartuje, můžete systém Windows přimět k tomu, aby se po chybě automaticky nerestartoval. Jakmile se systém restartuje, stiskněte okamžitě klávesu F8, která zpřístupní stránku Rozšířené možnosti spuštění (Advanced Boot Options), znázorněnou na obrázku 5.22.



Obrázek 5.22: Stránka Rozšířené možnosti spuštění (Advanced Boot Options)

Vyberte možnost Zakázat automatické restartování při selhání systému (Disable Automatic Restart On System Failure) a pak pokračujte ve spouštění počítače. Pokud nyní dojde k chybě systému, systém se na chybové zprávě zastaví, abyste si mohli chybu zapsat a vyhledat její popis.

Shrnutí

V této kapitole byla popsána instalace systému Windows Server 2008 do nového počítače, a to jak spuštěním systému z instalačního disku DVD, tak i pomocí spouštěcí bitové kopie a nasazením systému prostřednictvím sítě. Systém Windows Server 2008 používá instalaci založenou na bitových kopiích a jako standardní roli pro standardní i přizpůsobené nasazení systému prostřednictvím sítě poskytuje službu WDS.

V další kapitole bude popsán postup při upgradu starší verze systému Windows Server na systém Windows Server 2008.

KAPITOLA 6

Upgrade na systém Windows Server 2008

Nejjednodušším způsobem, jak nainstalovat systém Windows Server 2008 na určitý počítač a přesto zachovat informace o existující doméně, programy a nastavení počítače, je provést instalaci formou upgradu. Tento proces není nikterak složitý pro 32bitové členské servery a samostatné servery, ovšem pokud jsou přítomny i řadiče domény nebo pokud musíte změnit architektury, je třeba trocha pokročilého plánování.

Postup upgradu

Obecnou zásadou je, že můžete provádět upgrade počítače z libovolné edice systému Windows Server 2003 na odpovídající edici systému Windows Server 2008. Ovšem během upgradu nemůžete měnit architektury. Stejně tak neexistuje žádná přímá podpora upgradu pro systémy s procesorem Itanium – budete muset provést čistou instalaci. Tabulka 6.1 znázorňuje konkrétní podporované postupy.

Tabulka 6.1: Možnosti upgradu na systém Windows Server 2008

Stávající operační systém	Podporovaný upgrade
Windows Server 2003 Standard Edition (SP1) Windows Server 2003 Standard Edition (SP2) Windows Server 2003 R2 Standard Edition	Windows Server 2008 Standard (Úplná) Windows Server 2008 Enterprise (Úplná)
Windows Server 2003 Standard x64 Edition (SP1) Windows Server 2003 Standard x64 Edition (SP2) Windows Server 2003 R2 Standard x64 Edition	Windows Server 2008 Standard (Úplná, architektura x64) Windows Server 2008 Enterprise (Úplná, architektura x64)
Windows Server 2003 Enterprise Edition (SP1) Windows Server 2003 Enterprise Edition (SP2) Windows Server 2003 R2 Enterprise Edition	Windows Server 2008 Enterprise (Úplná)
Windows Server 2003 Enterprise x64 Edition (SP1) Windows Server 2003 Enterprise x64 Edition (SP2) Windows Server 2003 R2 Enterprise x64 Edition	Windows Server 2008 Enterprise (Úplná, architektura x64)
Windows Server 2003 Datacenter Edition (SP1) Windows Server 2003 Datacenter Edition (SP2) Windows Server 2003 R2 Datacenter Edition	Windows Server 2008 Datacenter (Úplná)
Windows Server 2003 Datacenter x64 Edition (SP1) Windows Server 2003 Datacenter x64 Edition (SP2) Windows Server 2003 R2 Datacenter x64 Edition	Windows Server 2008 Datacenter (Úplná, architektura x64)

Jak můžete vidět v tabulce, neexistuje žádná možnost upgradu na jádro serveru, pouze na úplné edice systému Windows Server 2008. A upgrade můžete provést pouze na stejnou architekturu, kterou právě používáte.

Obecné souvislosti s prováděním upgradu

Než se začneme zabývat podrobnostmi o samotném provedení upgradu, je třeba se seznámit s několika obecnými souvislostmi, které ovlivní většinu prostředí. Základní body, které je třeba vyřešit předem, jsou:

- Kroky předcházející upgradu
- Architektura
- Služba Active Directory
- Podpora hardwaru
- Podpora softwaru

V následujících částech se zmíníme o těchto bodech, abychom určili a naplánovali potřebné kroky ve vašem prostředí před a během upgradu stávajícího serveru.

Kroky předcházející upgradu

Před prováděním upgradu jakéhokoli serveru je ze všeho nejdříve potřeba provést úplnou, kompletní a ověřenou zálohu. Nezáleží na tom, jaký zálohovací program nebo jaká zálohovací média použijete. Ale ať už zvolíte jakoukoli možnost, ujistěte se, že jste zálohu ověřili jejím obnovením – ať už obnovením celé zálohy na stejný hardware nebo obnovením souborů ze zálohy do testovací oblasti původního serveru. Pokud jste vaši zálohu neotestovali, jednoduše ji nemůžete považovat za ověřenou zálohu. A to, k čemu se právě chystáte, může snadno vést k nutnosti čisté instalace serveru tzv. „na holé železo".

Několik upgradů jsme již provedli během psaní této knihy a zatím jsme nenarazili na žádnou zásadní chybu. Ovšem stále kontrolujeme, že máme ověřenou zálohu. Ověřená záloha je obzvláště důležitá v případě, že používáte specifickou sadu podnikových aplikací, jejichž reinstalace a obnova dat v těchto aplikacích by byla velkým problémem.

Takže ověřenou zálohu bychom měli. Které další kroky musíte provést před pokusem o provedení upgradu?

- **Převeďte svazky FAT** – systém Windows Server 2008 se nainstaluje pouze do oddílu NTFS. Svazky FAT jsou pro nesystémové disky stále podporovány, ale jejich použití není doporučeno.
- **Uvolněte místo na disku** – budete potřebovat alespoň 10 GB volného diskového místa na systémovém svazku, jehož upgrade provádíte. Upřímně si myslíme, že realističtějším minimem je alespoň 20 GB volného místa.
- **Aktualizujte firmware** – je vhodné aktualizovat firmware vašeho serveru na nejnovější verzi. Starší firmware může mít problémy s kompatibilitou se systémem Windows Server 2008, které jsou v novějších verzích firmwaru vyřešeny.
- **Získejte aktualizované ovladače** – získání aktualizovaných ovladačů je mimořádně důležité pro servery na platformě x64. Systém Windows Server 2008 podporuje pouze digitálně podepsané ovladače pro verze x64 systému Windows Server 2008.
- **Odpojte zařízení UPS** – mechanismus automatické detekce systému Windows Server 2008 může způsobit problémy s mechanismy automatického vypnutí zařízení UPS. Sériový kabel zařízení UPS můžete znovu připojit po dokončení instalace.
- **Vypněte antivirový software** – antivirový software může kolidovat v případě jakékoli instalace a v případě upgradů na systém Windows Server 2008 je tato pravděpodobnost ještě vyšší. V neposlední řadě antivirový software proces upgradu značně zpomalí a je velmi pravděpodobné, že bude příčinou chyby upgradu. Neaktivujte antivirový software, dokud si neověříte, že podporuje systém Windows Server 2008.
- **Připravte adresářovou službu Active Directory** – pokud provádíte upgrade řadiče domény, budete muset zajistit správnou připravenost adresářové služby Active Directory. Viz část o službě Active Directory dále v této kapitole.

Architektura

Naprostá většina serverů se systémem Windows Server 2003 obsahuje 32bitové verze systému Windows Server 2003. Ovšem mnoho z těchto serverů, pokud byly zakoupeny v posledních dvou letech, je zcela způsobilých ke spuštění verze x64 systému Windows Server 2008. Existuje spousta výhod, proč použít verze x64 systému Windows Server

2008, včetně podpory větší kapacity paměti RAM (32 GB ve verzi x64 systému Windows Server 2008 Standard a 2 TB ve verzi x64 systému Windows Server 2008 Enterprise a Datacenter). Pokud disponujete serverem se systémem Windows Server 2003, který je způsobilý k provozu verze x64, a máte 64bitové podepsané ovladače pro veškerý hardware, je vhodný okamžik pro přechod na 64 bitů. Věříme, že v mnoha případech shledáte verze x64 systému Windows Server 2008 rychlejší, stabilnější a bezpečnější než 32bitové verze.

Z praxe: Verze x64 a podepsané ovladače

Proč při instalaci verze x64 systému Windows Server 2008 klademe takový důraz na to, abyste se ujistili, zda máte digitálně podepsané ovladače? Protože společnost Microsoft se rozhodla, že s vydáním systému Windows Server 2008 nebude ani podporovat, ani povolovat spuštění nepodepsaných ovladačů v režimu jádra ve všech verzích x64 tohoto operačního systému. Dokonce i když jste provozovali verzi x64 systému Windows Server 2003, musíte ověřit, že máte aktualizované digitálně podepsané ovladače, jinak budete mít problémy.

Myslíme si, že tento posun je opravdu velmi dobrým krokem, díky němuž bude systém Windows Server 2008 bezpečnějším a stabilnějším operačním systémem. Stále bude možné, aby dodavatelé OEM napsali špatný ovladač a digitálně jej podepsali, ale alespoň budete mít jistotu, že všechny ovladače běžící ve vašem systému jsou podepsány a pochází od subjektu, který je v nich uveden.

Vlastně máme za to, že společnost Microsoft měla zvážit zavedení tohoto požadavku i u stávajících 32bitových serverů, které jsou upgradovány na systém Windows Server 2008, ale rovněž chápeme projevy nepochopení, se kterými by se toto opatření setkalo, a problémy, ke kterým by mohlo dojít u početné instalované základny stávajících 32bitových serverů. A s jasným prohlášením společnosti Microsoft, že tohle je *poslední* verze systému Windows Server, která bude mít 32bitové verze, toto rozhodnutí dává určitý smysl. Avšak rovněž jen dále zdůrazňuje náš postoj, že stávající 32bitové instalace systému Windows Server 2003, které mohou podporovat verze x64 systému Windows Server 2008, by měly být nyní převedeny.

Služba Active Directory

Pokud některé z vašich serverů se systémem Windows Server 2008 budou řadiči domény, adresářová služba Active Directory systému Windows Server 2008 bude vyžadovat novou verzi schématu služby Active Directory. Než se pokusíte přidat roli Active Directory Domain Services (AD DS) do systému Windows Server 2008 ve vaší existující adresářové službě systému Windows 2000 nebo Windows Server 2003, musíte si připravit adresářovou strukturu (a zřejmě i doménu) tak, aby akceptovala nový řadič domény se systémem Windows Server 2008. Pokud neinstalujete roli AD DS do žádného z počítačů se systémem Windows Server 2008, nemusíte schéma upgradovat.

Pro upgrade schématu služby Active Directory tak, aby podporovalo řadič domény se systémem Windows Server 2008, musíte provést následující kroky:

1. Přihlaste se k serveru, který je hostitelem role Schema Master Flexible Single Master Operations (FSMO). Musíte se přihlásit pomocí účtu, který je členem skupiny zabezpečení Schema Admins.

Poznámka: Pro rychlý způsob zjištění aktuálních vlastníků role FSMO pomocí prostředí PowerShell nahlédněte do části „Pohled zevnitř: Použití prostředí PowerShell ke zjištění vlastníků role FSMO".

2. Zkopírujte obsah složky \sources\adprep na disku DVD se systémem Windows Server 2008 na server.

Poznámka: Musíte použít stejnou verzi architektury příkazu adprep jako je verze serveru, který je hostitelem role hlavního serveru schémat. Takže pokud se aktuální hlavní server schématu nachází na 32bitovém systému Windows Server 2003, zkopírujte soubory z instalačního média 32bitové verze systému Windows Server 2008.

Poznámka: Adprep je jednorázový nástroj a v případě potřeby jej lze spustit přímo z disku DVD.

3. Otevřete okno příkazového řádku.
4. Najděte složku, do níž jste zkopírovali obsah složky adprep.
5. Spusťte následující příkaz:

   Adprep /forestprep

6. Pro prostředí, v nichž budete instalovat řadič domény jen pro čtení (RODC), rovněž spusťte následující příkaz:

   Adprep /rodcprep

7. Po dokončení operace a replikace můžete pokračovat s přípravou domény, aby podporovala řadič domény se systémem Windows Server 2008.
8. Přihlaste se k serveru, který je hostitelem role Infrastructure Master FSMO pro doménu, kterou připravujete. Musíte se přihlásit pomocí účtu, který je členem skupiny zabezpečení Domain Admins.
9. Zkopírujte obsah složky \sources\adprep na disku DVD se systémem Windows Server 2008 na server.

Poznámka: Musíte použít stejnou verzi architektury příkazu adprep jako je verze serveru, který je hostitelem role hlavního serveru schématu. Takže pokud se aktuální hlavní server schématu nachází na 32bitovém systému Windows Server 2003, zkopírujte soubory z instalačního média 32bitové verze systému Windows Server 2008.

10. Otevřete okno příkazového řádku.
11. Najděte složku, do níž jste zkopírovali obsah složky adprep.
12. Spusťte následující příkaz:

    Adprep /domainprep /gpprep

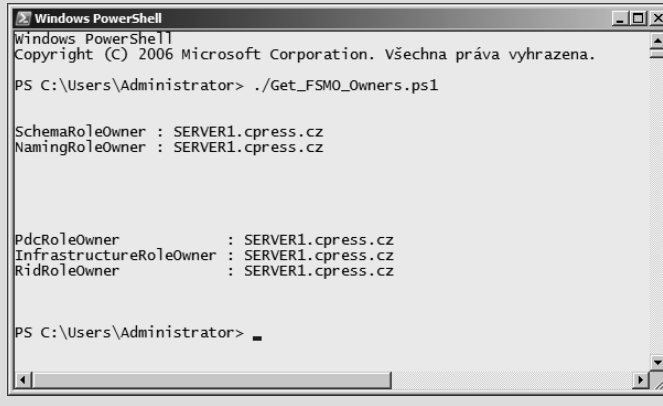
13. Po dokončení operace a replikace můžete přidat řadič domény se systémem Windows Server 2008 k vaší existující doméně.

Pohled zevnitř: Použití prostředí PowerShell ke zjištění vlastníků role FSMO

Existuje mnoho způsobů, jak zjistit role FSMO, ovšem jeden z nejjednodušších je učinit tak pomocí prostředí PowerShell. Následující kód lze spustit interaktivně na příkazovém řádku nebo jej lze zapsat jako skript a následně spustit v libovolném počítači v doméně, který obsahuje prostředí PowerShell.

```
# ScriptName: Get_FSMO_Owners.ps1
$Forest =
 [system.directoryservices.activedirectory.forest]::getcurrentforest()
$Domain =
 [system.directoryservices.activedirectory.domain]::getcurrentdomain()
$Forest | format-list SchemaRoleOwner, NamingRoleOwner
$Domain | format-list PDCRoleOwner, InfrastructureRoleOwner, RIDRoleOwner
```

Výsledek spuštění tohoto skriptu můžete vidět na obrázku 6.1.



Obrázek 6.1: Použití prostředí PowerShell ke zjištění aktuálních serverů spravujících roli FSMO

Podpora hardwaru

Systém Windows Server 2008 podporuje tři různé architektury: 32bitovou x86, 64bitovou x64 a 64bitovou ia64. Každá architektura má samostatné ovladače a podporovaný hardware. Není možno použít ovladače pro jednu architekturu v jiné architektuře. Kromě toho existují mnohem významnější omezení podporovaného hardwaru pro systémy architektury ia64, neexistuje žádná podpora pro většinu spotřebitelského nebo klientsky orientovaného hardwaru nebo funkcí, například zvukových karet či bezdrátových adaptérů. Systém Windows Server 2008 pro procesory Itanium je určen výhradně pro velké, škálovatelné serverové aplikace.

Jak již bylo řečeno, verze x64 systému Windows Server 2008 podporuje pouze digitálně podepsané ovladače pro veškerý hardware. Než se pokusíte provést upgrade edice x64 systému Windows Server 2003, ujistěte se, že máte podepsané ovladače pro veškerý důležitý hardware serveru.

Pokud stávající server obsahuje 32bitovou verzi systému Windows Server 2003 a podporuje pouze 32bitový systém Windows Server 2008, měli byste také ověřit, že pro veškerý důležitý hardware serveru existují aktualizované ovladače. Minimálním podporovaným procesorem je procesor řady x86 s frekvencí alespoň 1 GHz, dále je vyžadováno alespoň 512 MB paměti RAM. Tato čísla jsou významně vyšší než ta pro systém Windows Server 2003, který vyžadoval procesor s frekvencí pouze 133 MHz a 128 MB paměti RAM. Pokud stávající server se systémem Windows Server 2003 nesplňuje alespoň minimální požadavky, o upgrade se ani nepokoušejte. I když by byl upgrade úspěšný, použitelnost takového serveru by nebyla nikterak uspokojivá. Místo toho zvažte migraci rolí serveru na nový server. Nebo migraci serveru na virtuální počítač.

Z praxe: Použití virtualizace u starších verzí serveru

Skvělou novou technologií v systému Windows Server 2008 je Hyper-V. Tato nová nativní virtualizace na úrovni hypervisoru umožňuje migrovat stávající starší verze serverů, takže mohou běžet jako virtuální počítače systému Windows Server 2008. Bohužel technologie Hyper-V spatřila světlo světa pozdě a v čase uvolnění systému Windows Server 2008 do výroby nebyla k dispozici. O technologii Hyper-V a dalších možnostech virtualizace podrobněji pojednává kapitola 29, „Práce se službou Windows Virtualization".

Přestože technologie Hyper-V není součástí počáteční verze systému Windows Server 2008, můžete i tak využít virtualizaci k migraci vašich stávajících serverů se starším hardwarem, které nejsou dostatečně výkonné pro plnohodnotnou migraci na systém Windows Server 2008. Můžete použít aplikaci Microsoft Virtual Server 2005 R2 SP1 a převést fyzický server na virtuální počítač. Aplikace System Center Virtual Machine Manager 2007 podporuje přímé převody fyzických systémů na virtuální (P2V) a rovněž existují další nástroje od jiných výrobců, které dokáží usnadnit převod. Po převodu na virtuální počítač budou starší verze serverů, které nebyly způsobilé ke spuštění systému Windows Server 2008, ve skutečnosti rychlejší a budou moci využít dostatečnou rychlost procesoru a paměti RAM pro provedení upgradu. Nebo můžete pokračovat v používání starší verze systému Windows Server, pokud neexistuje naléhavá potřeba upgradu.

Pokud na aktuálním serveru běží edice x64 systému Windows Server 2003, pak již splňuje minimální požadavky na procesor a paměť RAM pro provedení upgradu na systém Windows Server 2008. Pokud server nedisponuje jednotku DVD-ROM, budete ji potřebovat (nebo budete muset objednat speciální distribuci systému Windows Server 2008 na discích CD). Rovněž budete potřebovat mnohem více místa na pevném disku. Kromě těchto změn byste však neměli mít žádné problémy, tedy za předpokladu, že jste aktualizovali digitálně podepsané ovladače k vašemu hardwaru.

Podpora softwaru

Software, který funguje se systémem Windows Server 2003, by měl rovněž fungovat i se systémem Windows Server 2008. Mohou se však vyskytnout problémy s kompatibilitou. Před provedením upgradu vždy ověřte, zda výrobce podporuje systém Windows Server 2008. Pokud migrujete z 32bitové verze systému Windows Server 2003 na verzi x64 systému Windows Server 2008, je třeba rovněž ověřit, zda všechny 32bitové aplikace, které fungují na serveru se systémem Windows Server 2003, podporují spouštění v 32bitové

emulaci systému Windows v architektuře Windows64 (WOW64), kterou používají verze x64 systému Windows Server 2008 k podpoře 32bitových aplikací.

Pohled zevnitř: WOW64

Hardwarová architektura x64 systému Windows je ve skutečnosti rozšířením existujícího hardwaru architektury x86 podporovaného 32bitovým systémem Windows. Jako taková obsahuje nativní podporu pro celou množinu 32bitových příkazů 32bitového systému Windows Server a skutečně umožňuje nativně spustit 32bitovou verzi systému Windows Server 2008. Při spuštění verze x64 systému Windows Server 2008 se tato nativní 32bitová podpora používá k zajištění velmi výkonného odlehčeného 32bitového operačního subsystému pro 32bitové aplikace. Pokud aplikace nevyžaduje ovladač hardwaru nebo používá nízkoúrovňová volání v režimu jádra, měla by běžet nativně v modulu WOW64 stejně rychle jako v 32bitovém systému Windows Server nebo ještě rychleji.

Aplikace napsané tak, aby při spouštění v 32bitovém systému Windows využily adresového prostoru většího než 2 GB virtuální paměti, automaticky uvidí celé 4 GB adresového prostoru virtuální paměti. To znamená, že aplikace, které nemají dostatek paměti ani v případě spuštění s přepínačem /3GB v systému Windows Server 2003, budou nyní mít 4 GB dostupné paměti v modulu WOW64. To je často dostačující pro podstatné zvýšení rychlosti pro aplikace náročné na paměť.

Aplikace běžící v modulu WOW64 vidí jiné zobrazení registru a části systému souborů operačního systému Windows, které jsou uchovány odděleně od 64bitových aplikací. To umožňuje následnou migraci na nativní 64bitové verze aplikací, jakmile budou k dispozici, neboť mohou běžet souběžně s 32bitovými verzemi.

64bitová verze systému Windows Server 2008 *vůbec* nepodporuje 16bitové aplikace. Pokud máte zastaralou verzi 16bitové aplikace (nebo 32bitovou aplikaci, která má 16bitový instalační program), je třeba buď zachovat stávající server, který tuto aplikaci podporuje, nebo migrovat server na fyzický nebo virtuální server s 32bitovou verzí systému Windows Server.

Bez ohledu na verzi systému Windows Server 2008, na kterou upgradujete, před provedením upgradu byste měli vždy ověřit, že vaše klíčové podnikové aplikace budou systémem Windows Server 2008 plně podporovány. Po dokončení upgradu je jedinou možností návratu k předchozí verzi systému Windows Server opakovaně provést novou instalaci.

Příprava domén a počítačů

Než budete moci provést upgrade řadiče domény na systém Windows Server 2008, měli byste postupovat podle pokynů popsaných v části „Služba Active Directory“ dříve v této kapitole, abyste připravili doménovou strukturu a doménu k přijetí řadiče domény se systémem Windows Server 2008. Pokud pouze provádíte upgrade na systém Windows Server 2008 na členském serveru (nebo provádíte upgrade samostatného serveru) není třeba doménu připravit. Ovšem je vhodné poznamenat, že správné upgradování doménové struktury a domény před samotnou instalací řadiče domény se systémem Windows Server 2008 nezpůsobí žádné problémy.

Před provedením upgradu proveďte základní vyčištění systémové jednotky počítače, který budete upgradovat. Odstraňte všechny dočasné soubory a vyčistěte adresáře se

soubory protokolů. (Pokud potřebujete protokoly uchovat, uložte je na jinou jednotku.) Proveďte defragmentaci jednotky. My používáme nástroj pro defragmentaci disku od jiného výrobce, a sice nástroj PerfectDisk od fy Raxco. Myslíme, že celkově odvádí lepší práci. Obsahuje možnost provedení defragmentace systémových souborů při spuštění systému, které by byly jinak používány a nebylo by možné je defragmentovat. Samozřejmě nic z toho nezabrání značné fragmentaci systémové jednotky během upgradu. Ale lépe něco, nežli nic. Dalším krokem, který je třeba provést po přípravě serveru k upgradu, je odstranit všechny soubory, které nezbytně nepotřebujete na systémové jednotce, aby bylo k dispozici maximum možného místa. K dokončení upgradu je třeba přibližně 15 GB volného diskového místa na jednotce.

Nakonec ukončete všechny nepotřebné služby nebo aplikace, zejména všechny antivirové programy nebo jakékoli služby provádějící monitorování v reálném čase. Odeberte všechna paměťová zařízení USB nebo jiná zařízení USB (kromě myši a klávesnice – je těžké se jich zbavit).

Upgrade klientů

Pokud máte v síti nějaké klientské počítače se systémem starším než Windows XP SP2, je nyní skutečně vhodný okamžik pro jejich upgrade. Podpora systémů Windows 95 a jeho předchůdců, Windows 98 a Windows ME byla ukončena a ze sítě by tyto systémy měly být odstraněny. Pokud jsou některé z počítačů poměrně nové a budou podporovat čistou instalaci systému Windows XP, měli byste tak učinit. Neprovádějte upgrade. Ano, v některých případech to technicky možné je. Opravdu to však není dobrý nápad.

Pokud máte klienty, kteří budou podporovat systém Windows Vista, rozhodně je upgradujte. Systém Windows Vista funguje se systémem Windows Server 2008 lépe, neboť sdílí společný síťový zásobník a další funkce. Systém Windows Vista rovněž podporuje Řízení uživatelských účtů (User Account Control – UAC) a obsahuje novou obousměrnou bránu Windows Firewall, což zvyšuje celkové zabezpečení.

Provedení upgradu

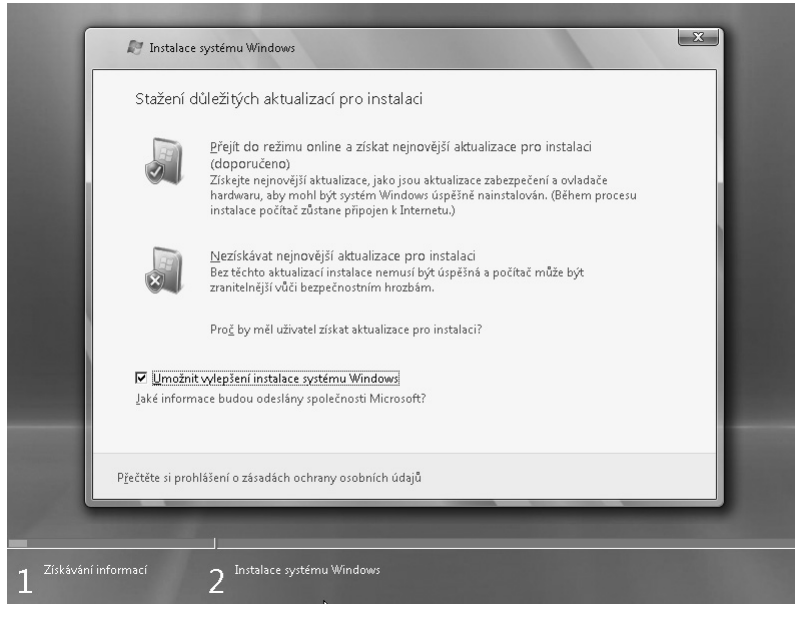
Nyní, když jste naplánovali upgrade a připravili pro něj doménu a doménovou strukturu, jste připraveni zahájit upgrade. Jedinými přímými podporovanými možnostmi upgradu jsou ty ze stejné architektury systému Windows Server 2003 na systém Windows Server 2008. Pokud máte systém Windows 2000 Server, který vyžaduje upgrade, bude třeba jej provést ve dvou krocích: nejprve provést upgrade na systém Windows Server 2003 a poté další upgrade na systém Windows Server 2008. Pokud tak učiníte, použijte média integrující *alespoň* aktualizaci Service Pack 1 (SP1) pro systém Windows Server 2003, ovšem upřednostňovaná je integrovaná aktualizace Service Pack 2 (SP2).

Důležité: Pokud na počítači, který hodláte upgradovat, běží systém Windows NT4, zvažte migraci služeb systému Windows NT4 na virtuální počítač a kompletní přestavění serveru. Opravdu nemáme rádi postupné upgrady od systému Windows NT4.

Upgrade na systém Windows Server 2008

Upgrade počítače se systémem Windows Server 2003 na systém Windows Server 2008 provedete podle těchto kroků:

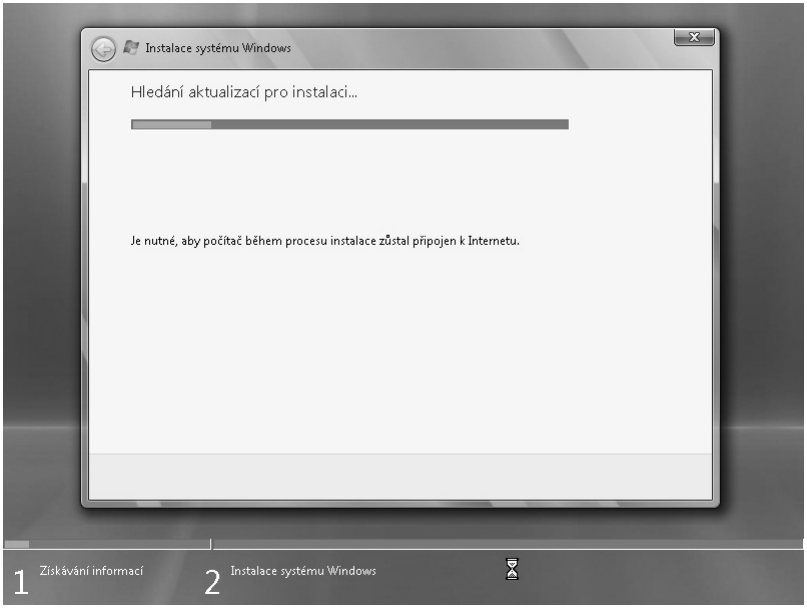
1. Proveďte upgrade serveru instalací nejnovější aktualizace Service Pack pro systém Windows Server 2003. (Nejnovější aktualizací je Windows Server 2003 SP2.)
2. Ukončete všechny otevřené programy, vypněte všechny antivirové programy a vložte do jednotky DVD disk DVD se systémem Windows Server 2008.
3. Pokud nedojde k automatickému spuštění instalačního programu systému Windows Server 2008, spusťte program setup.exe z disku DVD.
4. Na úvodní stránce průvodce Install Windows Wizard klepněte na tlačítko Install Now.
5. Na stránce Stažení důležitých aktualizací pro instalaci (Get Important Updates For Installation), znázorněné na obrázku 6.2, zvolte, zda chcete přejít do režimu online a získat nejnovější aktualizace, nebo zda chcete pokračovat bez aktualizací. Popis obou možností najdete v odstavci „Z praxe: Aktualizace během instalace?"



Obrázek 6.2: Stránka Stažení důležitých aktualizací pro instalaci průvodce Instalace Systému Windows

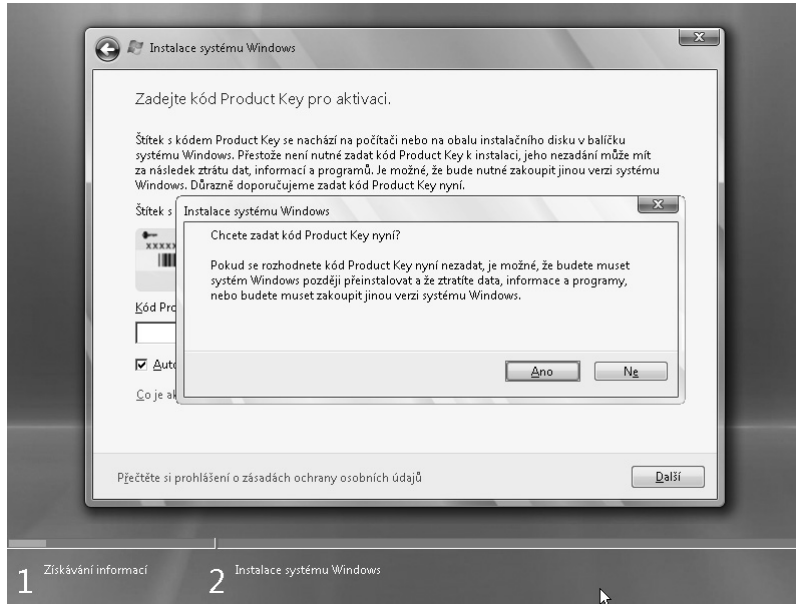
6. Pokud si přejete odeslat informace o výsledku instalace společnosti Microsoft, zaškrtněte políčko Umožnit vylepšení instalace systému Windows (I Want To Help Make Windows Installation Better). Myslíme, že tohle je dobrý nápad.

7. Zvolte, zda chcete instalovat aktualizace. Pokud zvolíte instalaci aktualizací, průvodce Instalace Systému Windows vyhledá aktualizace, viz obrázek 6.3.



Obrázek 6.3: Stránka Hledání aktualizací pro instalaci (Searching For Installation Updates) průvodce Instalace systému Windows

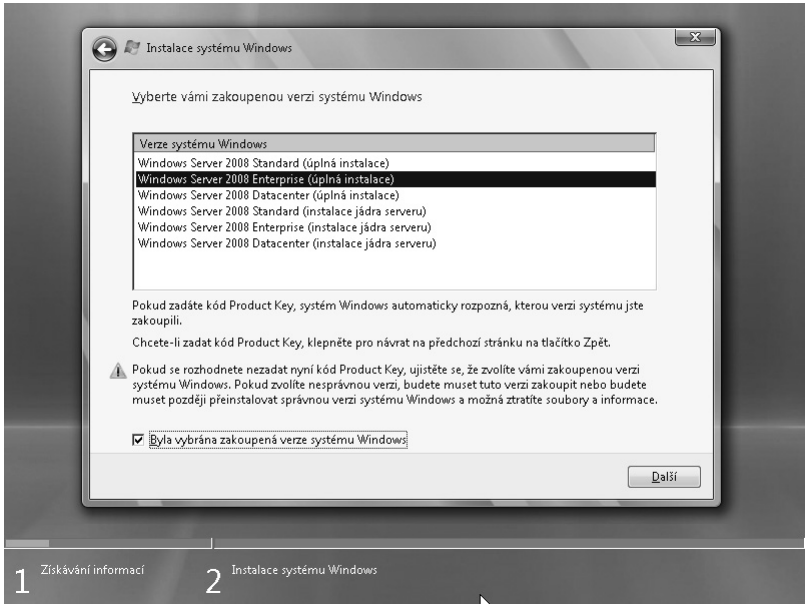
8. Na stránce Zadejte kód Product Key pro Aktivaci (Type Your Product Key For Activation) zadejte platný kód Product Key pro upgrade a klepněte na tlačítko Next. Zadání kódu můžete obejít – v takovém případě budete moci systém Windows Server 2008 používat 60 dní. Pokud kód nezadáte, zobrazí se upozornění znázorněné na obrázku 6.4. Klepnutím na tlačítko Ne (No) pokračujte bez zadání kódu, klepnutím na tlačítko Ano (Yes) se vraťte zpět na stránku Zadejte kód Product Key pro Aktivaci.



Obrázek 6.4: Pokud se pokusíte pokračovat bez zadání kódu Product Key, zobrazí se upozornění

9. Zvolte verzi systému Windows Server 2008, kterou chcete nainstalovat. Pokud jste zadali licenční klíč, budete mít k dispozici pouze verze, které jsou výslovně pokryty tímto licenčním klíčem. Pokud jste klíč nezadali, zobrazí se obrazovka znázorněná na obrázku 6.5.
10. Pro instalaci v podobě upgradu musíte zvolit verzi Úplná Instalace (Full Installation) systému Windows Server 2008 a musíte vybrat verzi systému Windows Server 2008, která je součástí dříve uvedené tabulky 6.1, obsahující možnosti podporovaného upgradu. Klepněte na tlačítko Další (Next). (Pokud provádíte instalaci bez licenčního klíče, budete muset potvrdit, že jste vybrali správnou edici systému Windows Server 2008.)
11. Na stránce Přečtěte si podmínky licenční smlouvy (Please Read The License Terms) zaškrtněte políčko Přijímám licenční podmínky (I Accept The License Terms). Nemáte žádnou jinou možnost na výběr, takže je dobré si tato licenční ujednání skutečně alespoň zběžně přečíst. Klepněte na tlačítko Další (Next).
12. Pokud jsou všechny podmínky upgradu splněny, uvidíte na stránce Jaký typ instalace požadujete (What Type Of Installation Do You Want) dostupnou možnost Upgrade.
13. Klepnutím na možnost Upgrade provedete instalaci v podobě upgradu. Zobrazí se zpráva o kompatibilitě. Tuto zprávu si pečlivě přečtěte a všimněte si jakýchkoli problémů, o nichž je ve zprávě zmínka. Pokud se žádné zásadní problémy nevyskytly, můžete klepnutím na tlačítko Další (Next) provést upgrade.

To je všechno. Instalační proces bude pokračovat a obvykle provede několikeré restartování počítače.



Obrázek 6.5: Stránka Vyberte vámi zakoupenou verzi systému Windows (Select The Edition Of Windows That You Purchased) průvodce Instalace systému Windows

Z praxe: Aktualizace během instalace?

Otázkou je, zdali provádět aktualizaci během instalace, či nikoliv. Pádné argumenty existují na obou stranách. Výhodou povolení aktualizací je, že všechny kritické opravy, které společnost Microsoft odhalí po vydání systému Windows Server 2008 a které by mohly ovlivnit úspěšnost vašeho upgradu, se automaticky stáhnou a zahrnou do instalace. Skvělé – to jistě zvýší šanci na úspěšnou instalaci.

Stinnou stránkou je, že musíte zachovat připojení serveru k Internetu po celou dobu instalace. V některých prostředích tento požadavek není problémem, ale v jiných se jedná o přímé porušení zásady, která spočívá v požadavku kompletního odpojení všech počítačů od vnějších sítí, dokud nejsou zcela připraveny včetně nainstalování všech aktualizací; to není vůbec špatná myšlenka, pokud máte prostředí, které takový postup podporuje, například prostředí se službou Windows Server Update Services (WSUS) nebo jiným mechanismem pro distribuci aktualizací.

Takže kterou možnost zvolit? Sami jsme nevěděli, jak se rozhodnout, ale nakonec jsme zvolili scénář se stažením aktualizací. Vaše volba závisí na vašich zásadách a prostředí.

Úrovně funkčnosti lesa a domény

Systém Windows Server 2008 podporuje tři úrovně funkčnosti domény, Windows 2000 Nativní, Windows Server 2003 a Windows Server 2008, a tři úrovně funkčnosti doménové struktury: Windows 2000, Windows Server 2003 a Windows Server 2008. Pokud provádíte upgrade řadiče domény v existující doméně a doménové struktuře služby Active Directory na systém Windows Server 2008, vaše doména i doménová struktura musí být na jedné z těchto úrovní. Veškerá podpora pro zastaralé a přechodné úrovně funkčnosti

domény, které umožňovaly další existence řadičů domény se systémem Windows NT4, je ukončena.

Podrobné informace o funkcích a omezeních jednotlivých úrovních funkčnosti domény a doménové struktury najdete v Kapitole 16, „Instalace a konfigurace adresářových služeb".

Shrnutí

Tato kapitola poskytla přehled o základních aspektech a krocích týkajících se upgradu počítače se stávajícím systémem Windows Server 2003 na systém Windows Server 2008. Řekli jsme si něco o podporovaných možnostech upgradu a krocích, které je třeba ve vašem prostředí provést před samotným upgradem. Upgrady jsou dobrým způsobem zachování vašich stávajících nainstalovaných aplikací a služeb a mají smysl pro klíčové podnikové aplikace, kdy by čistá instalace byla obtížná nebo by si vyžádala nepřiměřeně dlouhou odstávku počítače. Ovšem ve většině případů budete chtít provést čistou instalaci, kdykoliv to bude možné, neboť umožňuje dosažení vysoké flexibility při výběru typu a architektury instalace. V další kapitole se podíváme na kroky potřebné k provedení čisté instalace systému Windows Server 2008.

KAPITOLA 7

Konfigurace nové instalace

Po dokončení instalace systému Windows Server 2008 je třeba dokončit několik kroků, než bude server skutečně připraven k plnění své role ve vaší síti. Součástí procesu instalace není dokonce ani nastavení počátečního hesla správce, ani zadání názvu počítače. Nejsou nainstalovány žádné role, síť je uzamčena a všechny služby kromě těch nejzákladnějších a vyžadovaných jsou vypnuty. Nyní provedete základní konfiguraci serveru, než jej budete moci použít. Je třeba ověřit, zda instalační program nezaznamenal žádnou chybu, nastavit heslo administrátora a nakonfigurovat zbývající základní nastavení, včetně přidání služeb, nastavení názvu serveru a síťových nastavení a nastavení serveru tak, aby plnil svou životní úlohu (nebo alespoň svou úlohu ve vaší síti). Budeme předpokládat, že nastavujete nový server, ovšem pokud se jedná o upgrade z předchozí verze systému Windows Server, budete muset provést některé úlohy, třebaže jiné již byly provedeny jako součást upgradu.

Poznámka: Tato kapitola je zaměřena pouze na běžnou instalaci systému Windows Server 2008 v grafickém režimu. Nezabývá se instalací jádra systému Windows Server 2008, která je specializovanější instalací a jíž je vyhrazena celá kapitola. Další informace o konfiguraci jádra serveru najdete v kapitole 9, „Instalace a konfigurace jádra serveru“

Přehled úloh

Úlohy v této kapitole jsou většinou krátké a jednoduché, abyste mohli server po dokončení instalace rychle připravit a spustit. Minimálně bude u čisté instalace serveru potřeba provést následující úlohy:

- Nastavit počáteční heslo účtu administrátora
- Nastavit časové pásmo
- Nakonfigurovat síť
- Zadat název serveru.
- Připojit server k doméně nebo jej přiřadit do pracovní skupiny.
- Nakonfigurovat automatické aktualizace a nastavit automatické odesílání informací.
- Vyhledat aktualizace a nainstalovat je.

Průvodce Úlohy počáteční konfigurace (Initial Configuration Tasks Wizard) umožňuje snadný přístup k některým dalším krokům, které budete chtít zřejmě provést v rámci úvodních nastavení. Mezi tyto úlohy patří:

- Přidat role serveru
- Přidat funkce serveru
- Povolit vzdálenou plochu
- Nakonfigurovat bránu Windows Firewall

Na první a poslední z těchto úloh můžete pro tento okamžik zapomenout. O přidání rolí serveru se zmíníme v další kapitole a brána Windows Firewall je zapnuta automaticky. Podrobná konfigurace brány Windows Firewall je popsána v kapitole 23, „Implementace zabezpečení". Další dvě úlohy v tomto seznamu však vyžadují trochu pozornosti. Myslíme si, že na každém serveru by měla být okamžitě nainstalována alespoň jedna funkce – Windows PowerShell. Povíme si o ní v této kapitole. A rovněž máme za to, že dobrým nápadem je i opustit serverovnu, takže v této kapitole povolíme i vzdálenou plochu. Potom již můžete provádět další potřebné kroky z vaší pracovní stanice v pohodlí kanceláře.

Instalační program systému Windows Server 2008 je zcela nový a společnost Microsoft vynaložila veškeré úsilí na to, aby uživatel při počáteční instalaci musel odpovídat na co nejméně dotazů. Cenou za toto zjednodušení však je požádání uživatele o konfiguraci dalších nastavení po dokončení instalace. Myslíme si, že to je rozumný kompromis. Kdyby pro nic jiného, tak alespoň protože se nemusíte instalaci vůbec věnovat. Můžete zahájit novou instalaci, propracovat se přes několik málo úvodních obrazovek a jít pryč. Když se vrátíte, bude systém Windows Server 2008 nainstalován a vy můžete nyní začít s konfigurací podle vašich potřeb.

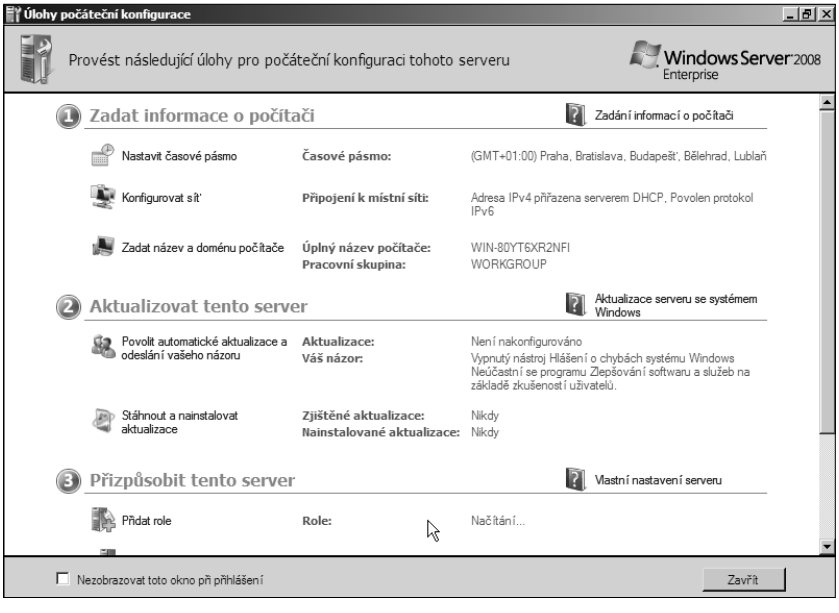
Společnost Microsoft používá interní výraz pro prostředí, které její zákazníci vidí při první instalaci softwarového balíku: prostředí prvního spuštění počítače (z ang. Out Of Box Experience, OOBE).

První přihlášení

V případě systému Windows Server 2008 začíná prostředí prvního spouštění počítače tak, že jste před prvním přihlášením vyzváni k zadání počátečního hesla správce, viz obrázek 7.1.

Obrázek 7.1: Nastavení počátečního hesla systému Windows Server 2008

Po nastavení počátečního hesla pro účet správce a po přihlášení ke konzole poprvé spatříte průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard), viz obrázek 7.2.

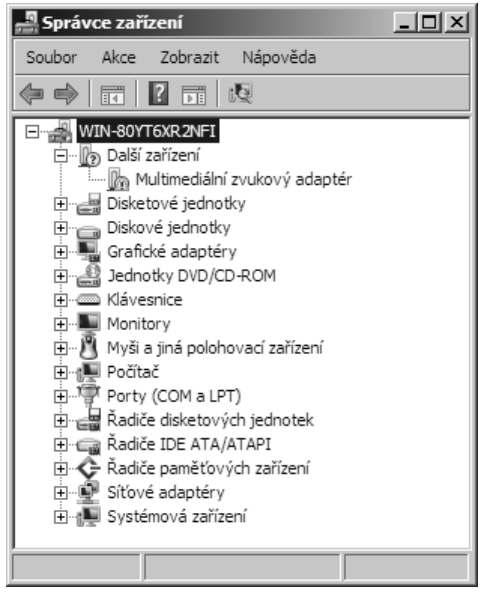


Obrázek 7.2: Průvodce Initial Configuration Tasks Wizard

Konfigurace hardwaru

Podle našeho názoru trpí průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) jedním neduhem, kterému opravdu vůbec nerozumíme. Myslíme si, že než budete moci začít s konfigurací serveru, měl by být váš hardware funkční. Jak můžete vidět na obrázku 7.2, nemáme moc možností na výběr – naše síťová karta není bez přidání ovladače podporována, takže průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) si myslí, že nemáme nainstalovány vůbec žádné síťové adaptéry. Společnost Microsoft vynakládá značné úsilí, aby na instalační médium DVD dostala co možná nejvíce ovladačů, ale realita je taková, že nový hardware bude vyvíjen i po uvolnění systému Windows Server 2008 do prodeje a některý hardware bude vyžadovat ovladače, které se na disku DVD nenachází.

Pro nás tedy bude prvním krokem otevření Správce zařízení (Device Manageru) a vyhledání zařízení, která nebyla detekována nebo nepracují. Budou jasně označena, jak můžete vidět na příkladu našeho síťového adaptéru na obrázku 7.3. Můžete nainstalovat ovladače nyní, nebo pokud se nejedná o zařízení, které byste potřebovali pro počáteční konfiguraci, můžete počkat na dokončení průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard).



Obrázek 7.3: Neznámé zařízení ve Správci zařízení

Jakmile se vám podaří hardware zprovoznit, můžete pokračovat v konfiguraci základního nastavení počítače v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard).

Konfigurace základních informací o počítači

První část průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) pokrývá základní konfiguraci počítače: časové pásmo, nastavení sítě, název počítače a připojení počítače k doméně. Tato část nastavení bude vyžadovat restart serveru po nastavení jeho názvu a případném připojení k doméně, takže s těmito úkony raději počkejte až na konec této části.

Nastavení časového pásma

Během počáteční instalace systém Windows zvolí časové pásmo (pravděpodobně ne to, v němž se nacházíte, pokud tedy nebydlíte na západním pobřeží Severní Ameriky) a rovněž nastaví aktuální datum a čas podle BIOSu vašeho počítače. Pro nastavení data a času, stejně jako pro nastavení aktuálního časového pásma, klepněte na odkaz v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard), čímž otevřete dialog Datum a čas (Date And Time) znázorněný na obrázku 7.4. Po nastavení času a časového pásma vašeho serveru klepněte na tlačítko Použít (Apply) a poté se klepnutím na tlačítko OK vraťte k průvodci Úlohami počátečního nastavení (Initial Configuration Tasks Wizard).

Obrázek 7.4: Dialog Datum a čas

Z praxe: Další hodiny

Systém Windows Server 2008 vám umožní nakonfigurovat dvoje další hodiny, které jsou součástí dialog Datum a čas. Zobrazení hodin v oznamovací oblasti je ve výchozím nastavení zapnuto, ovšem pokud je z nějakého důvodu vypnuto, můžete jej zapnout klepnutím pravým tlačítkem myši v oznamovací oblasti a výběrem položky Vlastnosti (Properties), čímž vyvoláte dialog Vlastnosti Hlavního panelu a nabídky Start (Taskbar And Start Menu Properties). Zde klepněte na kartu Oblast oznámení (Notification Area) a zaškrtněte políčko Hodiny (Clock). Tím zapnete zobrazení hodin. Pokud jste nakonfigurovali další hodiny, čas v těchto časových pásmech bude viditelný při najetí ukazatele myši na hodiny.

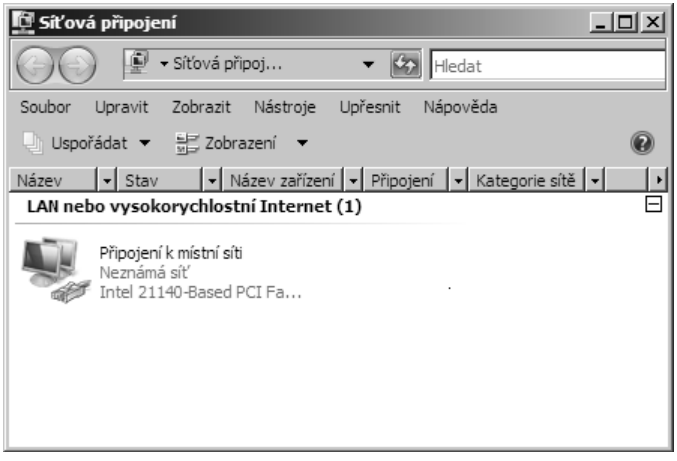
Pokud pravidelně pracujete s kolegy v jiném časovém pásmu, časem si na časový rozdíl zvyknete a další hodiny na vašem serveru nebudete potřebovat. A koneckonců ve většině případů byste stejně vůbec neměli sedět u konzoly serveru. Nicméně další hodiny mohou být užitečné, a jelikož relativně často pracujeme s lidmi z Evropy a Austrálie, máme zapnuty další dvoje hodiny: jedny nastaveny na Střední čas (GMT) a druhé na čas GMT+10:00 pro Sydney v Austrálii. Díky tomu máme jistotu, že když voláme ve zcela nevhodnou hodinu, nemáme pro to skutečně žádnou omluvu.

Konfigurace sítě

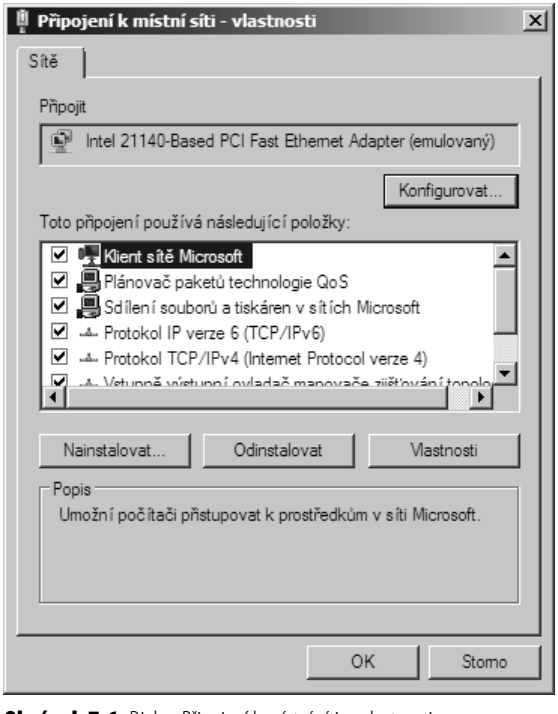
Dalším bodem v seznamu je konfigurace sítě. Ve výchozím nastavení má váš nový server zapnut protokol IPv4 i IPv6, a pokud v síti běží server DHCP, automaticky má nakonfigurovány adresy pro oba protokoly. Pokud nebyl žádný server DHCP dostupný, přidělil si server tzv. adresu *v link-local* (LLA) – IP adresa automatické konfigurace, která je v síti jedinečná, ale směrovače ji nemohou předat jiné síti. U serverů důrazně doporučujeme, aby alespoň adresa protokolu IPv4 adresa byla statickou adresou. Ve většině situací může být adresa IPv6 bezstavovou adresou automatické konfigurace nebo adresou LLA, poskytnutou serverem DHCP, jak je popsáno v kapitole 18, „Správa protokolu TCP/IP“,

Pro konfiguraci sítě a nastavení pevné IP adresy serveru postupujte podle následujících kroků:

1. Klepnutím na odkaz Konfigurovat síť (Configure Networking) v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) otevřete aplikaci Ovládacích panelů s názvem Síťová připojení (Network Connections), zobrazenou na obrázku 7.5. (Příkazem pro příkazový řádek je Ncpa.cpl.)
2. Klepněte pravým tlačítkem myši na připojení, které chcete konfigurovat, a zvolením položky Vlastnosti (Properties) v místní nabídce otevřete dialog Připojení k místní síti – vlastnosti (Local Area Connection Properties), znázorněný na obrázku 7.6.

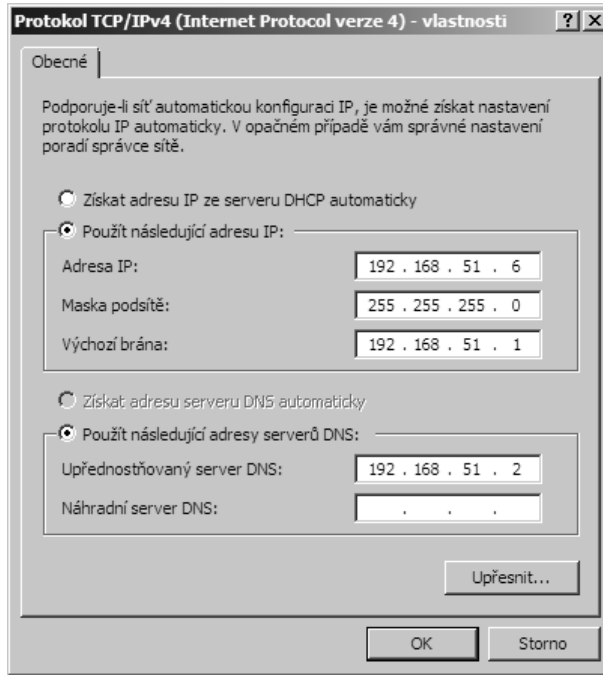


Obrázek 7.5: Aplikace Ovládacích panelů Síťová připojení



Obrázek 7.6: Dialog Připojení k místní síti – vlastnosti

3. Vyberte položku Protokol TCP/IPv4 (Internet Protocol verze 4) (Internet Protocol Version 4 (TCP/IPv4)) a klepněte na tlačítko Vlastnosti (Properties).
4. Zvolte možnost Použít následující adresu IP (Use The Following IP Address), viz obrázek 7.7.



Obrázek 7.7: Dialog Protokol TCP/IPv4 (Internet Protocol verze 4) – vlastnosti

5. Zadejte IP adresu, masku podsítě a výchozí bránu pro vaši síť.
6. Určete upřednostňovaný server DNS pro vaši síť. (Měl by jím být řadič domény, pokud používáte server DNS, který je součástí služby Active Directory.) Rovněž můžete zadat náhradní server DNS, pokud ve vaší síti existuje.
7. Na tlačítko Upřesnit (Advanced) klepněte pouze v případě, že potřebujete nastavit některé další vlastnosti tohoto síťového připojení. Můžete zadat další IP adresy, alternativní brány, další nastavení serverů DNS a nastavení serveru WINS. Výchozí hodnoty těchto pokročilých nastavení jsou ve většině sítí dostačující, zejména pro tuto počáteční konfiguraci. Klepnutím na tlačítko OK se vraťte na hlavní stránku vlastností.
8. Klepnutím na tlačítko OK zavřete dialog Protokol TCP/IPv4 (Internet Protocol verze 4 – vlastnosti (Internet Protocol Version 4 (TCP/IP) Properties), a poté klepnutím na tlačítko Zavřít (Close) dokončete konfiguraci tohoto připojení.
9. Okno Síťová připojení (Network Connections) zavřete klepnutím na tlačítko X v pravém horním rohu okna, čímž se vrátíte na stránku průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard).

Poznámka: Pokud váš server obsahuje více síťových karet, přejmenování na výstižnější názvy než Připojení k místní síti a Připojení k místní síti 2 může zjednodušit pozdější konfiguraci rolí serveru.

Nastavení názvu počítače a domény

Po konfiguraci sítě jste připraveni pojmenovat počítač a připojit jej k doméně. Pokud se jedná o první počítač v doméně, nebudete v tuto chvíli doménu nastavovat – k tomu dojde později po přidání a konfiguraci služby Active Directory Domain Services (AD DS).

Instalační program systému Windows Server 2008 novému serveru automaticky přiřadí náhodný a nic neříkající název. I když je tento název v síti jedinečný, nejedná se o vhodný konečný název, takže jej budete chtít změnit.

Z praxe: Pojmenování počítačů

Je vhodné použít název počítače, který je kompatibilní se službou DNS i s rozhraním NetBIOS, aby všechny typy klientů viděly stejný název počítače. (A ano, ještě nějaký čas budeme muset žít s rozhraním NetBIOS – existuje prostě příliš mnoho aplikací, včetně aplikací společnosti Microsoft, které bez něj zkrátka správně nefungují.) Proto dbejte na to, aby byl název počítače tvořen maximálně 15 znaky a nepoužívejte znaky hvězdičky nebo tečky. Nejvyšší kompatibility s aplikacemi docílíte použitím pomlček místo mezer a podtržítek.

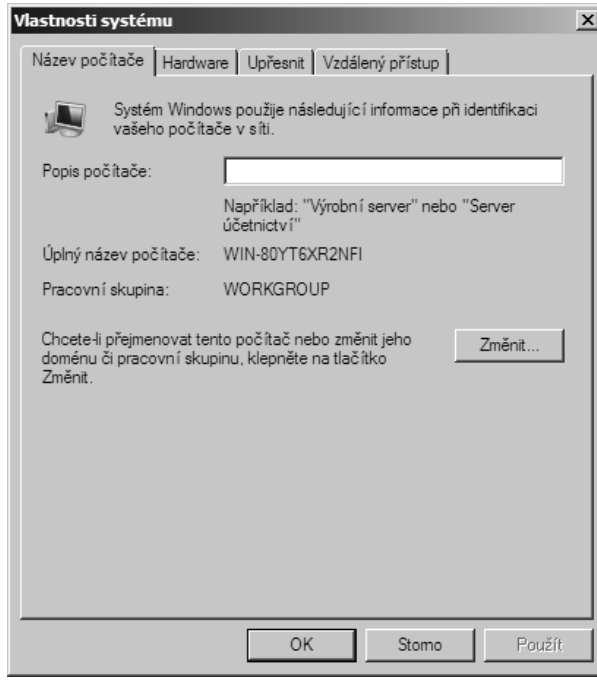
Kromě toho byste měli použít konvenci pro názvy, která je určitým způsobem vnitřně konzistentní. Už jsme viděli celou řadu konvencí pro názvy, od literárních obskurností, kdy se v názvu objevila jména romantických básníků nebo sci-fi postav, jména severských či řeckých bohů, až po barvy (kdy byla přední část serveru celá vybarvena tak, aby se shodovala s názvem serveru). Upřímně řečeno, líbí se nám názvy, z nichž je skutečně zřejmá funkce serveru, jeho umístění, adresa, hardware, doména nebo kombinace výše uvedeného. Naše vzorová síť zde proto obsahuje počítače s následujícími názvy:

- hp350-dc-02 (Server běží na hardwaru Hewlett-Packard ML350 G5, jedná se o řadič domény a jeho adresa IP je 192.168.51.2.)
- hp350-ts-05 (Terminálový server běžící na hardwaru Hewlett-Packard 350 s adresou IP 192.168.51.5.)
- dl380-core-08 (Hardwarem je Hewlett-Packard DL380 s instalací jádra serveru a adresou IP 192.168.51.8.)

Chápeme, že tato jmenná konvence je poněkud nudná, avšak máme za to, že to má větší smysl, než pokoušet se zapamatovat si, že Hermes je serverem Microsoft Exchange a Zeus je řadičem domény.

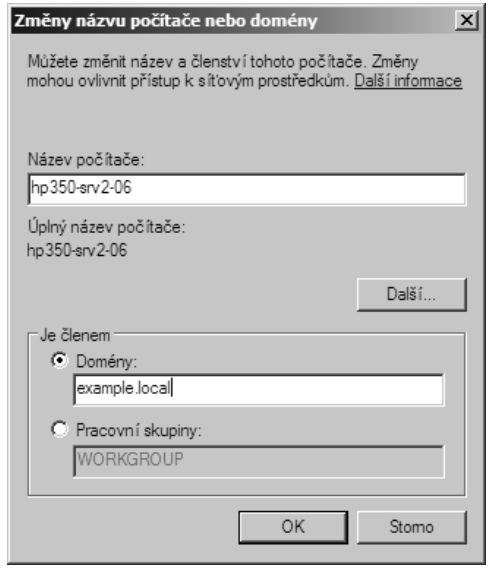
Pokud současně změníte název počítače a doménu, můžete si ušetřit jedno restartování počítače. Oba kroky vyžadují opětovné spuštění počítače, které zabrání dokončení jiných úloh, ovšem naštěstí lze tyto kroky sloučit. Název počítače a domény nastavíte podle následujících kroků:

1. Klepnutím na odkaz Zadat název a doménu počítače (Provide Computer Name And Domain) v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) otevřete dialog Vlastnosti systému (System Properties), znázorněný na obrázku 7.8.



Obrázek 7.8: Dialog Vlastnosti systému

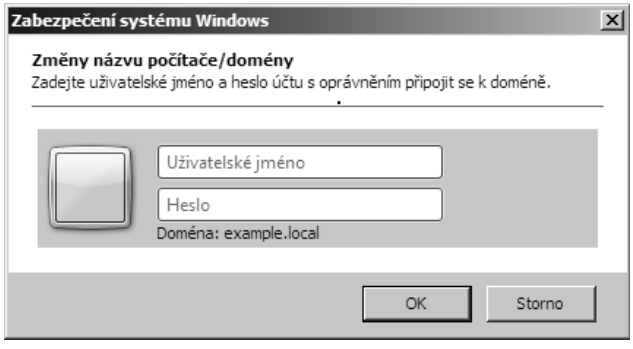
2. Pokud chcete, můžete zadat popis počítače, který však bude zobrazen jen zřídkakdy, takže to není nijak zvlášť užitečné.
3. Klepnutím na tlačítko Změnit (Change) otevřete dialog Změny názvu počítače nebo domény (Computer Name/Domain Changes), znázorněný na obrázku 7.9.



Obrázek 7.9: Dialog Změny názvu počítače nebo domény

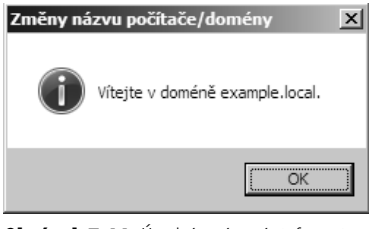
4. Zadejte název počítače, který je konzistentní s vaší konvencí pro názvy, a poté klepněte na tlačítko Domain, abyste zadali doménu, ke které chcete počítač připojit.

5. Klepněte na tlačítko OK, načež budete pravděpodobně požádáni o pověření k provedení změny, viz obrázek 7.10. K tomu budete potřebovat pověření na úrovni správce domény, ke které server připojujete, nebo účet, kterému bylo uděleno právo připojení počítače k doméně.



Obrázek 7.10: Je třeba zadat pověření pro správu domény, ke které chcete server připojit

6. Klepněte na tlačítko OK. Pokud se nevyskytnou žádné problémy, zobrazí se úvodní zpráva, podobná té na obrázku 7.11.



Obrázek 7.11: Úvodní zpráva vás informuje o tom, že jste nyní připojeni k doméně

7. Klepnutím na tlačítko OK potvrďte zprávu. Zobrazí se upozornění, že před provedením změn je třeba server restartovat. Znovu klepněte na tlačítko OK a poté několikerým klepnutím na tlačítko OK server restartujte.

Důležité: V tuto chvíli by vás to mohlo svádět k pokusu o odložení restartování počítače, abyste zjistili, zda můžete provést ještě nějaké kroky, než budete muset čekat na dokončení restartu serveru. To je pochopitelné – jsme zastánci minimalizování počtu nezbytného restartování a provedení co nejvíce možných kroků, když víme, že budeme muset počítač restartovat. Ovšem tohle je jediný případ, kdy si myslíme, že byste měli tomuto pokušení odolat. Potřebujete, aby se nový název a zabezpečení projevily co možná nejdříve.

Aktualizace a nastavení odesílání informací

Další skupina nastavení v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) se používá k nastavení zpracování aktualizací a odesílání informací společnosti Microsoft. Výchozím chováním je, že pokud neprovedete žádnou změnu, nebudou automaticky stahovány žádné aktualizace, nebudou odesílána žádná hlášení o chybách společnosti Microsoft, ale budou odesílány zprávy o nainstalovaných rolích na serveru. Věříme, že tohle není ve většině případů ideální nastavení, takže se pusťme do konfigurace.

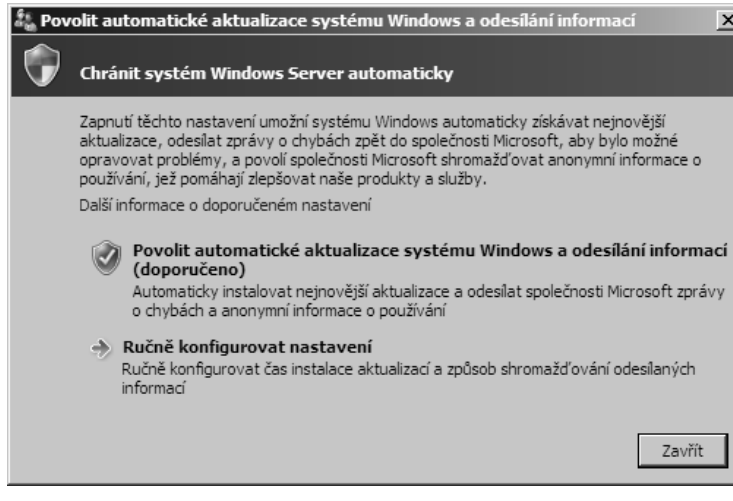
Zapnutí aktualizací a odesílání informací

Prvním nastavením této části průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) je nakonfigurovat ta nastavení, která souvisí s aktualizacemi a odesíláním informací. Po klepnutí na odkaz Povolit automatické aktualizace a odesílání vašeho názoru (Enable Automatic Updating And Feedback) v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) máte na výběr tři základní možnosti:

- Nastavení aktualizací systému Windows
- Nastavení nástroje Hlášení o chybách systému Windows
- Nastavení programu Customer Experience Improvement Program

Konfiguraci těchto nastavení provedete následujícím způsobem:

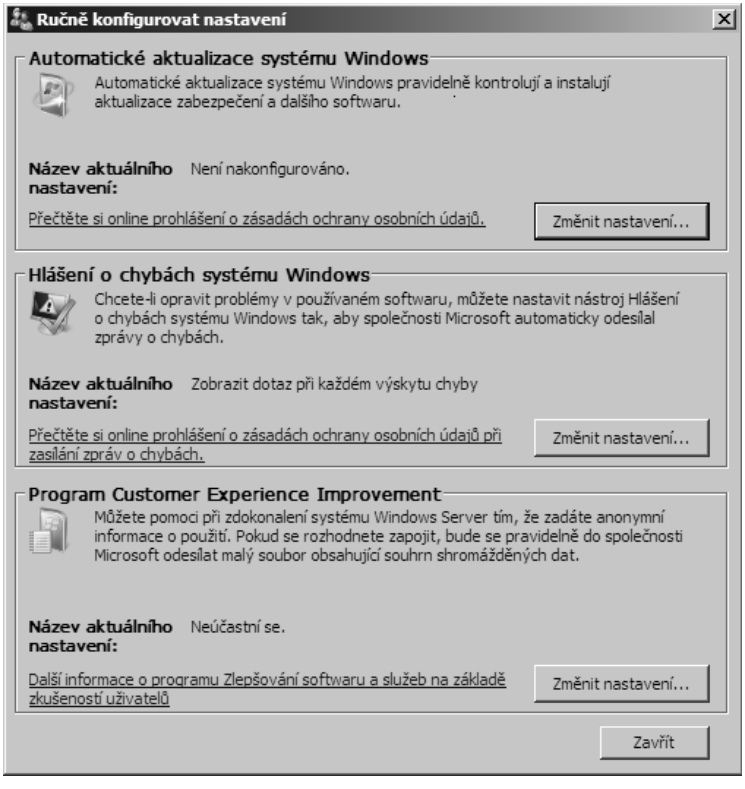
1. V průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) klepněte na odkaz Povolit automatické aktualizace a odesílání vašeho názoru (Enable Automatic Updating And Feedback), čímž otevřete dialog znázorněný na obrázku 7.12.



Obrázek 7.12: Dialog Povolit automatické aktualizace systému Windows a odesílání informací

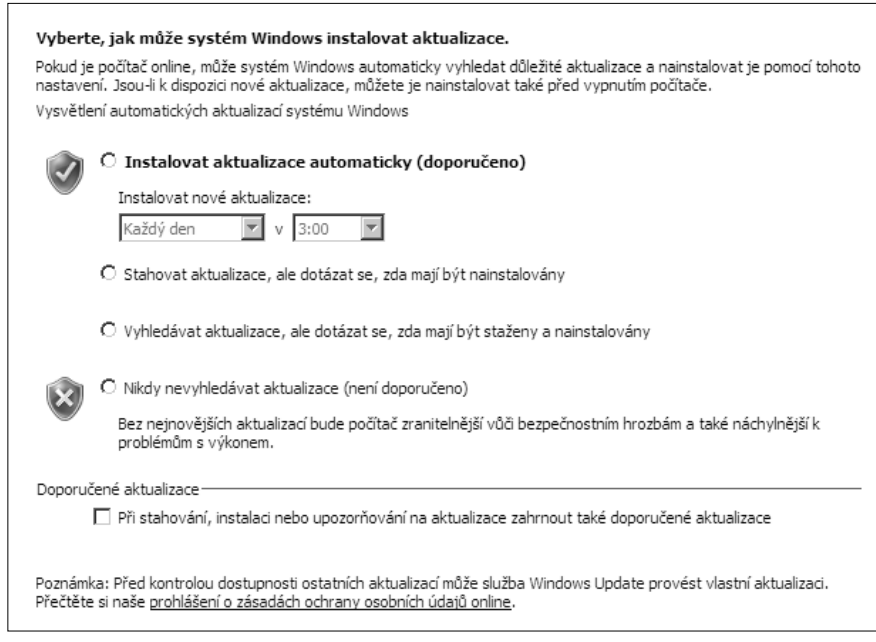
2. Pokud opravdu nechcete, aby váš server automaticky stahoval a instaloval aktualizace bez jakéhokoliv upozornění a automaticky bez upozornění prováděl restartování počítače, *nevolte* možnost Povolit automatické aktualizace systému Windows a odesílání informací (Enable Windows Automatic Updating And Feedback).

3. Klepnutím na tlačítko Ručně konfigurovat nastavení (Manually Configure Settings) otevřete dialog, znázorněný na obrázku 7.13.



Obrázek 7.13: Dialog Ručně konfigurovat nastavení

4. Abyste nakonfigurovali chování aktualizací systému Windows v tomto serveru, klepnutím na tlačítko Změnit nastavení (Change Settings) v části Automatické aktualizace systému Windows (Windows Automatic Updating) otevřete dialog znázorněný na obrázku 7.14.



Obrázek 7.14: Dialog Vyberte, jak může systém Windows instalovat aktualizace

5. Vyberte jednu z následujících možností:

- Instalovat aktualizace automaticky (doporučeno (Install Updates Automatically (Recommended))

  Tohle je možná doporučené nastavení společnosti Microsoft, nicméně my si myslíme, že na serveru je opravdu, opravdu nevhodné. Další informace najdete v odstavci Z praxe o automatických aktualizacích.

- Stahovat aktualizace, ale dotázat se, zda mají být nainstalovány (Download Updates But Let Me Choose Whether To Install Them)

  Toto nastavení doporučujeme. Stažení probíhá automaticky na pozadí v době nízkého vytížení sítě. Po stažení se při příštím přihlášení správce k serveru zobrazí výzva k instalaci aktualizace v oznamovací oblasti.

- Vyhledávat aktualizace, ale dotázat se, zda mají být staženy a nainstalovány (Check For Updates But Let Me Choose Whether To Download And Install Them)

  Pokud je dostupná aktualizace vhodná pro daný server, správce po přihlášení k serveru uvidí výzvu v oznamovací oblasti. Pokud je mezi aktualizacemi taková, kterou chcete nainstalovat, bude třeba ji před instalací stáhnout. Pokud není šířka pásma příliš drahá, tato možnost se nezdá být příliš efektivní.

- Nikdy nevyhledávat aktualizace (není doporučeno) (Never Check For Updates (Not Recommended))

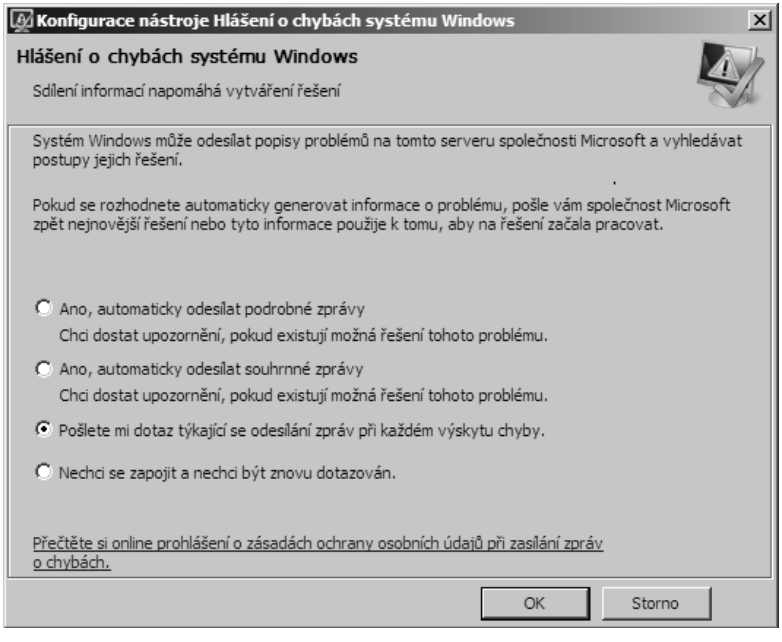
  Pokud vaše prostředí nepoužívá jiné řešení pro správu oprav než od společnosti Microsoft, máme za to, že toto nastavení opravdu není dobrým nápadem. Většina

urgentních a kritických aktualizací by měla být nainstalována včas, aby byl váš server ochráněn. Pokud používáte tato nastavení, budete se muset k webu Windows Update pravidelně připojovat ručně, abyste zjistili, zda jsou k dispozici nějaké aktualizace. Nebo budete muset použít řešení od jiného výrobce.

Můžete také zvolit možnost zahrnout doporučené aktualizace mezi aktualizace pokryté vaším nastavením. Tyto aktualizace jsou méně důležité než ty spadající do kategorie Kritické nebo Důležité, o které se stará služba automatických aktualizací.

6. Po výběru některé z možností se klepnutím na tlačítko OK vraťte k dialogu Ručně konfigurovat nastavení (Manually Configure Settings), znázorněnému dříve na obrázku 7.13.

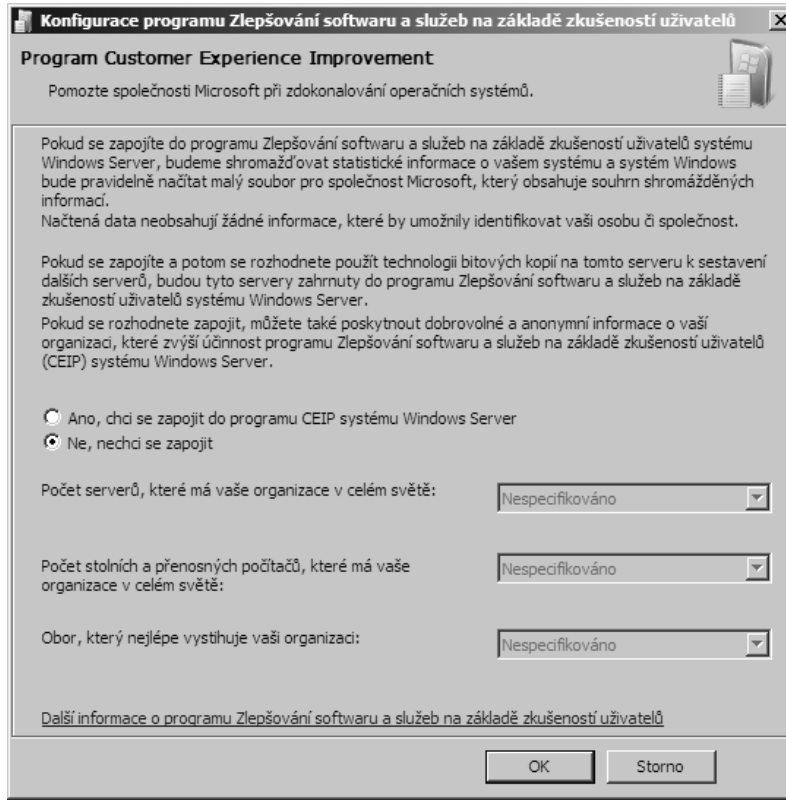
7. Klepnutím na tlačítko Změnit nastavení (Change Settings) v části Hlášení o chybách systému Windows (Windows Error Reporting) otevřete dialog Konfigurace nástroje Hlášení o chybách systému Windows (Windows Error Reporting Configuration), znázorněný na obrázku 7.15.



Obrázek 7.15: Dialog Konfigurace nástroje Hlášení o chybách systému Windows

8. Vyberte, jak chcete naložit s hlášeními o chybách. Myslíme si, že automatické odesílání alespoň souhrnných zpráv a možná i podrobných zpráv je dobré pro nás pro všechny. Další informace o tom, co se odesílá a proč by nás to mělo zajímat, najdete v části Pohled zevnitř. Po výběru některé z možností se klepnutím na tlačítko OK vraťte k dialogu Ručně konfigurovat nastavení (Manually Configure Settings), znázorněnému dříve na obrázku 7.13.

9. Klepnutím na tlačítko Změnit nastavení (Change Settings) v části Program Customer Experience Improvement (Customer Experience Improvement Program (CEIP)) otevřete dialog Konfigurace programu Zlepšování softwaru a služeb na základě zkušeností uživatelů (Customer Experience Improvement Program Configuration), znázorněný na obrázku 7.16.



Obrázek 7.16: Dialog Konfigurace programu Zlepšování softwaru a služeb na základě zkušeností uživatelů

10. Výchozí možností je automatické zapojení do programu CEIP. Společnosti Microsoft nejsou odesílány žádné osobní nebo podnikové údaje, které by vedly k identifikaci odesilatele. Žádné. Ovšem jsou shromažďovány informace o vašem hardwaru a rolích serveru, které jsou na serveru nainstalovány. A pokud uvedete podrobnosti o serverech, pracovních stanicích a oboru, který nejlépe vystihuje vaši organizaci, tyto informace se připojí k získaným datům.
11. Vyberte požadované možnosti a klepněte na tlačítko OK. Poté se klepnutím na tlačítko Close vraťte k průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard).

Z praxe: Automatické aktualizace na serveru

Pevně věříme v důležitost pravidelných a včasných aktualizací serverů vždy, když se objeví kritické aktualizace zabezpečení. Instalaci oprav věnujeme celou kapitolu (kapitola 25).

Rádi bychom si mysleli, že servery a pracovní stanice nebudou nikdy vyžadovat instalaci oprav nebo aktualizace, ale realita je jiná. Když se objeví nové hrozby v zabezpečení, jsou často ve velmi krátkém čase k dispozici i programy zneužívající toto slabé místo, které stanou se hrozbou pro vaši síť. Proč tedy máme tak intenzivní pocit, že společnost Microsoft dělá *chybu*, když výchozím nastavením je automatické použití aktualizací u systému Windows Server 2008? Protože si myslíme, že to, kde, kdy a jak se mají aktualizace použít, je *vaše* rozhodnutí, a nikoho jiného. A zejména si myslíme, že uživatelé mají právo vědět, kdy bude server restartován. Nejen že takový automatický restart by mohl být v rozporu s dodržováním smluvené úrovně vašich služeb (tzv. SLA), ale v tomto globálním světě, v němž všichni žijeme a pracujeme, proč by měly být tři hodiny ráno (výchozí čas instalace a restartování) místního času tím pravým časem na restartování v časovém pásmu vašich poboček nebo pro vaše obchodní zástupce, kteří mohou být kdekoliv na světě? Ti by mohli mít otevřeny důležité soubory, s nimiž právě pracují. Takže mějte aktualizace ve vašem prostředí pod kontrolou a plně automatickým aktualizacím řekněte ne. Aktualizace samozřejmě stáhněte, pokud to má s ohledem na cenu za šířku vašeho pásma smysl. Nebo nasaďte server Windows Server Update Services (WSUS) ve vaší síti a nakonfigurujte jej tak, aby ovládal to, jak a kde se aktualizace nabízí a na kterých serverech se použijí. Nebo pokud to má s ohledem na velikost vaší sítě opodstatnění, použijte System Center Configuration Manager. Nebo ke správě aktualizací použijte produkt od jiného výrobce, například aplikaci Shavlik NetChk Protect. Ale nenastavujte vaše servery tak, aby prováděly automatické aktualizace samy a restartovaly se, jak se jim zachce. To není dobré řešení.

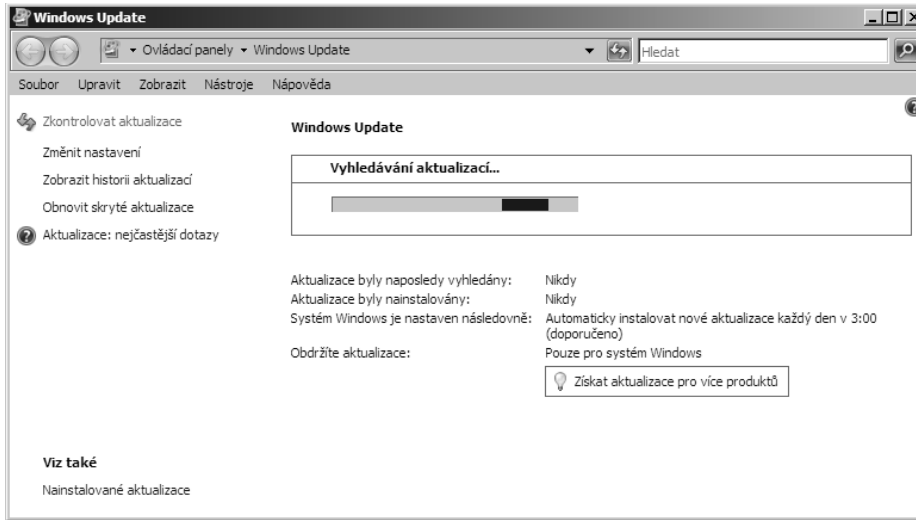
Pohled zevnitř: Hlášení o chybách systému Windows

Historie nástroje Hlášení o chybách systému Windows zasahuje až ke stařičkým chybám aplikace Dr. Watson, které jsme se všichni naučili v dřívějších verzích systému Windows nenávidět. Ovšem od té doby se již leccos zlepšilo. Jednou z hlavních změn, které spatřily světlo světa společně se systémem Windows XP, bylo odesílání výpisů stavu systému společnosti Microsoft po havárii nebo ukončení odezvy programu. (Tato funkce je označována jako Online Crash Analysis, zkráceně OCA, a již odhalila spoustu chyb!) Pokaždé jste byli dotázáni, zda chcete odeslat výpis stavu systému, a spousta lidí tak naštěstí učinila, neboť následkem toho byl stabilnější a bezpečnější systém Windows, společně s mnohem lepšími ovladači. Výkonný ředitel společnosti Microsoft Steve Ballmer prohlásil, že „asi 20 procent problémů v kódu způsobuje 80 procent všech chyb a – což mě samotného překvapuje – *jedno procento problémů v kódu způsobuje polovinu všech chyb*". Nalezením zmíněných 20 procent chyb v kódu a vyvinutím úsilí na jejich odstranění se budeme všichni těšit z výhod stabilnějšího, bezchybného softwaru.

Ovšem je třeba poznamenat, že výpisy stavu systému mohou obsahovat určitelné osobní údaje. Pokud dojde k chybě programu, v němž zrovna zadáváte číslo vaší kreditní karty, je možné, že číslo kreditní karty nebo jeho určitá část bude pravděpodobně ve výpise stavu systému. Společnost Microsoft nás opakovaně – a věříme, že důvěryhodně – ujišťuje, že nijak nezneužije žádné osobní údaje v takových výpisech stavu systému. Můžete si přečíst její prohlášení o zásadách ochrany osobních údajů na adrese *http://oca.microsoft.com/en/dcp20.asp*. Vlastně vás tímto vybízíme k přečtení tohoto prohlášení. Je srozumitelné a myslíme si, že maximálně jednoznačné, třebaže je dílem právníků. A shledali jsme jej uklidňujícím. Všichni profitujeme z ohlašování chyb tím, že pomáháme vytvářet lepší a spolehlivější aplikace.

Získání aktualizací

Poslední možností v této části průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) je přejít hned do režimu online a stáhnout aktualizace. Stačí klepnout na odkaz Download And Install Updates. Otevře se dialog Windows Update, znázorněný na obrázku 7.17.



Obrázek 7.17: Dialog Windows Update

Pokud jsou k dispozici nové aktualizace, zobrazí se a můžete je hned nainstalovat. Důležitým odkazem na této stránce však je odkaz Získat aktualizace pro více produktů (Get Updates For More Products). Klepnutím na tento odkaz můžete použít službu Microsoft Update Service místo služby Windows Update Service. Služba Microsoft Update Service zahrnuje více produktů společnosti Microsoft, včetně těch, které byste běžně nainstalovali v systému Windows Server. Pokud tuto možnost nevyužijete, mohli byste se sami vystavit riziku neošetřených oslabení zabezpečení serverových aplikací, které používáte. Takže pokud nepoužíváte nějaké jiné mechanismy zajišťující, že vaše ostatní aplikace společnosti Microsoft nainstalované na serveru jsou pravidelně aktualizovány, doporučujeme vám zvolit možnost použití služby Microsoft Update Services.

Přizpůsobení serveru

Poslední část průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) se používá k přidání rolí a funkcí na server, k povolení vzdáleného přístupu a ke konfiguraci brány Windows Firewall. Konečně se můžeme pustit do skutečného nastavení serveru a odvést tak nějakou práci. Všechno ostatní jsme již připravili.

Nehodláme se zabývat možností Přidat role (Add Roles) v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard), neboť instalaci a konfiguraci rolí serveru je věnována celá další kapitola. Rovněž instalaci funkcí bychom mohli nechat na další kapitolu, která se zabývá také jimi, ale myslíme si, že jedna funkce, kterou společnost

Microsoft ve výchozím nastavení neinstaluje, by měla být nainstalována na každém serveru – a sice prostředí Windows PowerShell. Proto si o její instalaci povíme už nyní.

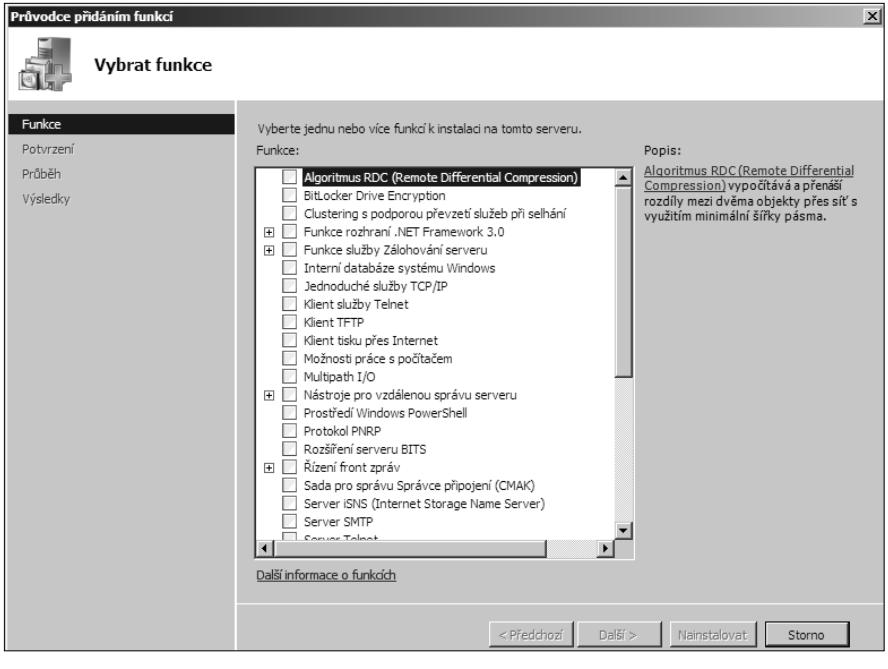
Přidání funkce Windows PowerShell

Windows PowerShell je nové prostředí příkazového řádku a skriptovací jazyk, vydaný společností Microsoft v roce 2006. Pro starší verze systému Windows je dostupný ke stažení na adrese *http://www.microsoft.com/technet/scriptcenter/topics/msh/download.mspx*, ovšem v systému Windows Server 2008 je přítomen jako funkce. (Tato funkce však není nainstalována automaticky.) A bohužel není vůbec přítomna v instalaci jádra serveru.

Prostředí Windows PowerShell zcela nahradilo Cmd.exe coby naše každodenní příkazové prostředí a zrovna tak byste to měli vnímat i vy. Třebaže hned nebudete psát hromadu skriptů prostředí PowerShell, můžete s prostředím PowerShell začít jako s vaším prostředím příkazového řádku.

Než však budete moci používat prostředí PowerShell, musíte na vaši novou instalaci systému Windows Server 2008 přidat funkci PowerShell. Průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) obsahuje odkaz Přidat funkce (Add Features), takže jej zrovna použijme k přidání funkce PowerShell, a to pomocí následujících kroků:

1. Klepnutím na odkaz Přidat funkce (Add Features) v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) otevřete Průvodce přidáním funkcí (Add Features Wizard), znázorněného na obrázku 7.18.



Obrázek 7.18: Stránka Vybrat funkce Průvodce přidáním funkcí

2. Posuňte se v seznamu dolů až téměř na konec seznamu Funkce (Features) a zaškrtnutím políčka vyberte funkci Prostředí Windows PowerShell.

3. Klepnutím na tlačítko Další (Next) otevřete stránku s potvrzením. Zobrazí se seznam funkcí, které hodláte nainstalovat, a upozornění, že tato operace může vyžadovat restartování systému. Žádné strachy, server neprovede restartování, pokud tohle bude jediná funkce, kterou nainstalujete.

4. Klepnutím na tlačítko Nainstalovat (Install) zahajte samotnou instalaci. Po jejím dokončení se zobrazí stránka Výsledky instalace (Installation Results). Pokud došlo k nějakým problémům, najdete na ní informace o nich, jinak jednoduše oznámí, že instalace byla úspěšná. Klepnutím na tlačítko Zavřít (Close) ukončete Průvodce přidáním funkcí.

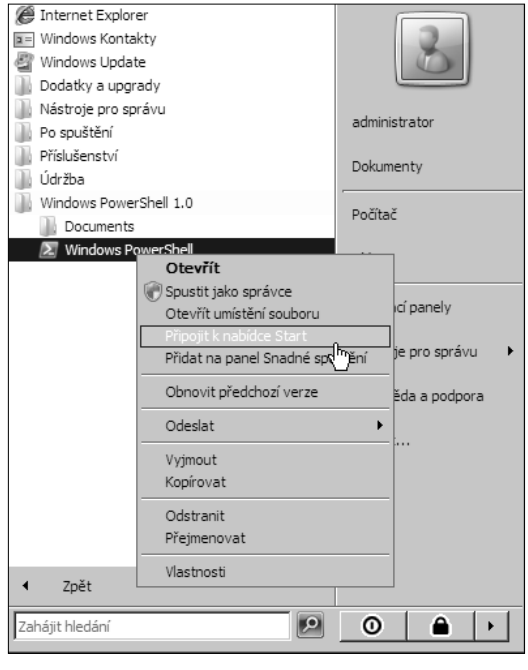
Už jste téměř hotovi. Ještě je třeba pár kroků konfigurace, které usnadní použití prostředí PowerShell, takže se do nich hned pusťme.

Nejprve umístěte zástupce prostředí PowerShell do nabídky Start, abyste jej lépe zpřístupnili. Koneckonců je tam i příkaz Cmd, tak proč by zde nemohl být zástupce prostředí PowerShell? Zástupce prostředí PowerShell umístíte do nabídky Start pomocí následujících kroků:

1. Klepněte na nabídku Start.

2. Klepněte na příkaz Všechny programy (All Programs) a poté klepněte na příkaz Windows PowerShell 1.0.

3. Klepněte pravým tlačítkem myši na příkaz Windows PowerShell a zvolte příkaz Připojit k nabídce Start (Pin To Start Menu), viz obrázek 7.19.



Obrázek 7.19: Přidání zástupce na prostředí Windows PowerShell do nabídky Start

4. Když už jste tady, přidejte zástupce na prostředí PowerShell i na panel Snadné spuštění (Quick Launch). Od této chvíle budete mít k prostředí PowerShell snadný přístup, aniž byste museli procházet nabídky, abyste se k němu dostali.

Ve výchozím nastavení se prostředí PowerShell nainstaluje nejbezpečnějším možným způsobem, přičemž vám znemožní spouštění veškerých skriptů nebo konfiguračních souborů. To vám umožní použít příkazový řádek, ovšem poněkud se tím omezí vaše možnosti vlastního nastavení nebo provádění téměř všeho v prostředí PowerShell místo prostých příkazů příkazového řádku.

Tato omezení jsou označována jako *zásady spuštění*. K dispozici jsou čtyři úrovně zásad spuštění:

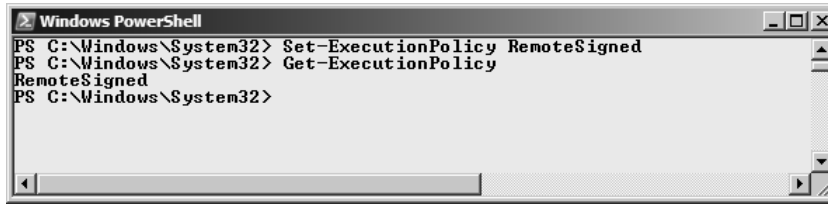
- **Restricted –** nepovolí spouštění žádných skriptů a nenačte konfigurační soubory. Jedná se o výchozí hodnotu.
- **AllSigned** – povolí spouštění skriptů nebo konfiguračních souborů podepsaných důvěryhodným vydavatelem. Dokonce i skripty, které si sami napíšete, musí být podepsány.
- **RemoteSigned** – povolí spouštění skriptů nebo konfiguračních souborů, které byly vytvořeny v místní síti, a to aniž by byly podepsány, ovšem všechny skripty, které byly staženy z Internetu, musí být podepsány důvěryhodným vydavatelem.
- **Unrestricted** – povolí spouštění všech skriptů nebo konfiguračních souborů bez ohledu na to, odkud pochází. Skripty nebo konfigurační soubory, které pochází z Internetu, vás ovšem před spuštěním na tuto skutečnost upozorní.

Myslíme si, že výchozí hodnota Restricted je poněkud přísná, a upřímně řečeno, nejsme ochotni vytvářet podepisovací certifikát jen proto, abychom mohli spouštět své vlastní skripty, takže i úroveň AllSigned je poněkud příliš restriktivní. Pro prostředí, které plně podporuje certifikáty pro podpis kódu a v němž chcete omezit skripty, které lze spouštět, jen na ty, které jsou schváleny a podepsány, má úroveň AllSigned smysl. Ovšem pro většinu umístění je dobrým kompromisem úroveň RemoteSigned. Zásadu spuštění na hodnotu RemoteSigned změníte pomocí následujících kroků:

1. Klepněte na nabídku Start, klepněte pravým tlačítkem myši na příkaz Windows PowerShell a poté zvolte příkaz Spustit jako správce (Run As Administrator).
2. Na výzvu Řízení uživatelských účtů (User Account Control) odpovězte klepnutím na tlačítko Pokračovat (Continue), čímž otevřete prostředí PowerShell s oprávněními správce.
3. V prostředí PowerShell spusťte následující příkaz:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

4. Abyste si ověřili, zda došlo k provedení změn, můžete použít příkaz `Get-ExecutionPolicy`, viz obrázek 7.20.



Obrázek 7.20: Nastavení zásad spuštění prostředí PowerShell

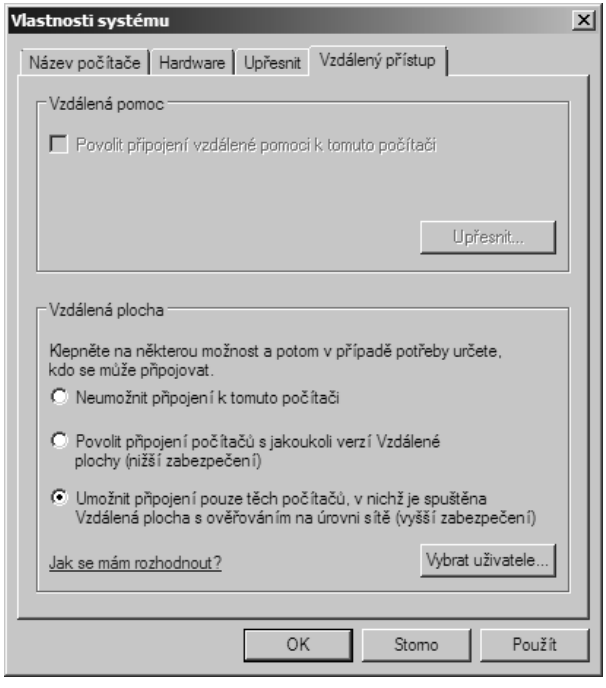
Povolení vzdálené plochy

Další položkou průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) je odkaz Povolit vzdálenou plochu (Enable Remote Desktop). Vzdálená plocha umožňuje správcům připojit se k serveru přímo, aniž by museli sedět u konzoly v serverovně. Systém Windows Server 2008 představuje verzi 6.1 protokolu Remote Desktop Protocol (RDP). Klient Remote Desktop Client verze 6.1 je součástí aktualizace Service Pack (SP) 1 pro systém Windows Vista a SP3 pro systém Windows XP a klienty verze 6 si můžete stáhnout z článku znalostní databáze Microsoft Knowledge Base 925876 na adrese *http://support.microsoft.com/kb/925876*.

Verze 6 a novější verze protokolu RDP obsahují oproti starším verzím mnohá vylepšení, včetně 32bitové barevné hloubky, ověření serveru, přesměrování prostředků, vyhlazování písma a Terminal Services RemoteApps. Pro vzdálenou správu serveru je nejdůležitějším vylepšením ověření serveru, které zajistí, že se skutečně připojujete k počítači, ke kterému si myslíte, že se připojujete.

Funkci vzdálené plochy na novém serveru povolíte pomocí následujících kroků:

1. Klepnutím na odkaz Povolit vzdálenou plochu (Enable Remote Desktop) v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) otevřete dialog Vlastnosti systému (System Properties). Ve výchozím nastavení by měla být vybrána karta Vzdálený přístup (Remote), viz obrázek 7.21.
2. Vyberte úroveň klienta Připojení ke vzdálené ploše, kterou chcete použít. Pokud bude na všech vašich klientech běžet alespoň systém Windows XP SP2 nebo novější, zvolte možnost Umožnit připojení pouze těch počítačů, v nichž je spuštěna Vzdálená plocha s ověřováním na úrovni sítě (vyšší zabezpečení) (Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication (More Secure)).
3. Po klepnutí na tlačítko OK se zobrazí oznámení, že kvůli funkci Vzdálená plocha byla povolena výjimka brány Windows Firewall. Po opětovném klepnutí na tlačítko OK se vraťte k dialog Vlastnosti systému.
4. Klepněte na tlačítko OK a funkce Vzdálená plocha je povolena.



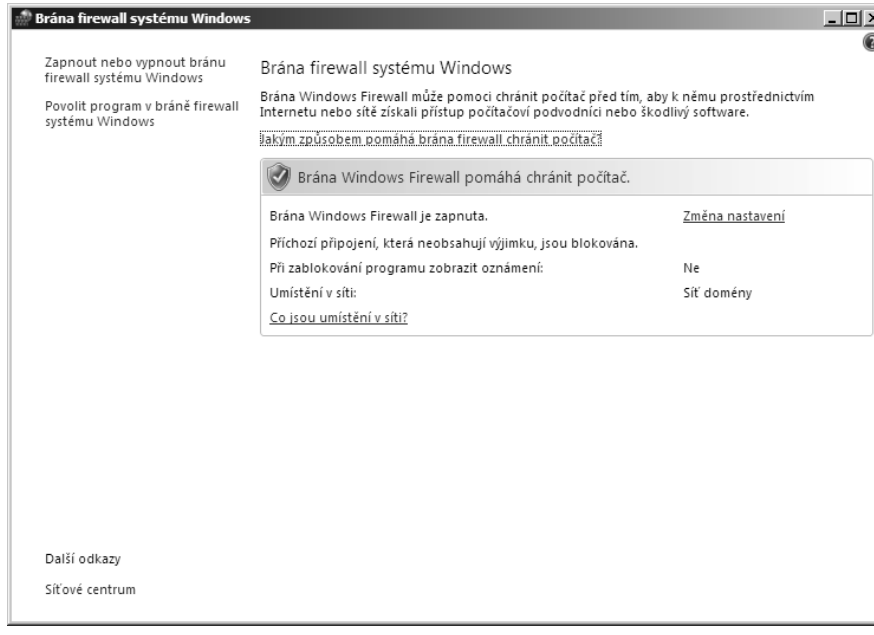
Obrázek 7.21: Karta Vzdálený přístup dialogu Vlastnosti systému

Konfigurace brány Windows Firewall

Posledním zastavením v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) je odkaz Konfigurovat bránu systému Windows (Configure Windows Firewall). Ve výchozím nastavení je na všech nových serverech brána Windows Firewall zapnuta. Jedná se o zcela odlišnou verzi brány Windows Firewall, než která byla součástí prvního vydání systému Windows Server 2003. Nová brána Windows Firewall je závislá na umístění a platí u ní různá pravidla pro provoz v rámci domény, privátní sítě a veřejné sítě. Kromě toho je obousměrná, tzn. kontroluje jak příchozí, tak i odchozí provoz. Podrobněji si o bráně Windows Firewall povíme v kapitole 23, „Implementace zabezpečení". Pro tuto chvíli je primárně důležité pouze vědět, že brána Windows Firewall je ve výchozím nastavení zapnuta. Všechny role nebo funkce systému Windows Server 2008, které povolíte prostřednictvím Správce serveru nebo průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard), bránu Windows Firewall v případě potřeby automaticky zaktualizují, ovšem pokud používáte sadu podnikových aplikací od jiných výrobců, které vyžadují povolení výjimek brány firewall, budete tak muset učinit ručně.

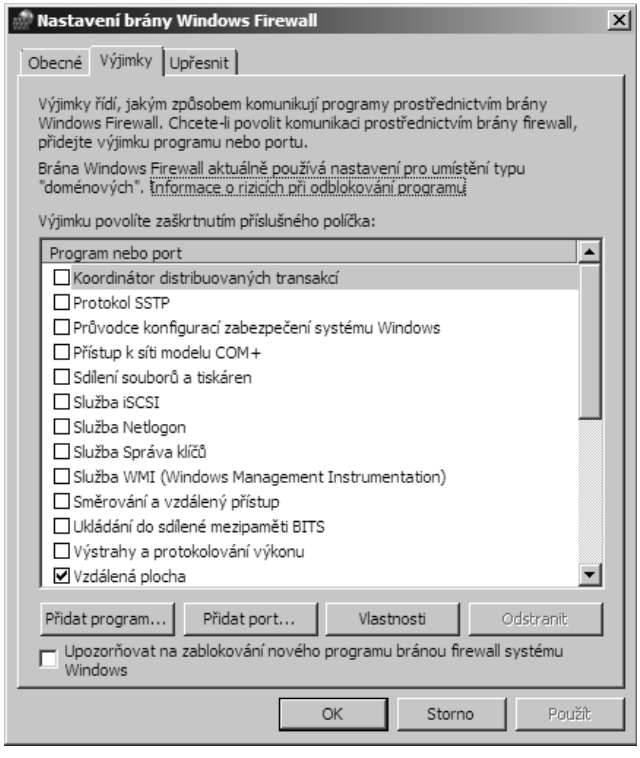
Konfiguraci brány Windows Firewall na novém serveru provedete pomocí následujících kroků:

1. Klepnutím na odkaz Konfigurovat bránu Windows Firewall (Configure Windows Firewall) v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) otevřete dialog Brána Firewall systému Windows, viz obrázek 7.22.



Obrázek 7.22: Dialog Windows Firewall

2. Klepnutím na odkaz Změna nastavení (Change Settings) otevřete kartu Obecné (General) dialogu Nastavení brány Windows Firewall (Windows Firewall Settings). Na této stránce můžete zapnout nebo vypnout bránu firewall nebo ji nastavit tak, aby blokovala veškerá příchozí připojení.
3. Klepněte na kartu Výjimky (Exceptions) dialogu Nastavení brány Windows Firewall (Windows Firewall Settings), abyste povolili konkrétním programům nebo funkcím komunikaci přes bránu Windows Firewall, viz obrázek 7.23.
4. Zaškrtnutím políčka u možnosti Vzdálená správa brány Windows Firewall (Windows Firewall Remote Management) povolte vzdálenou konfiguraci brány Firewall systému Windows na tomto serveru. Mezi další výjimky, které by vás mohly v tuto chvíli napadnout, patří Vzdálená správa systému Windows (Windows Remote Management) a Vzdálená správa služeb (Remote Service Management).
5. Klepnutím na tlačítko OK zavřete dialog Nastavení brány Windows Firewall (Windows Firewall Settings) a poté se zavřením dialogu Brána firewall systému Windows vraťte k průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard).



Obrázek 7.23: Karta Výjimky dialogu Nastavení brány Windows Firewall

Ukončení průvodce Úlohy počáteční konfigurace

Po dokončení všech kroků v průvodci Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) můžete zaškrtnou políčko Nezobrazovat toto okno při přihlášení (Do Not Show This Window At Logon) a klepnout na tlačítko Zavřít (Close). Tím ukončíte průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) a už se s ním nesetkáte. Po ukončení průvodce se otevře konzola Správce serveru (Server Manager), která vám umožní pokračovat v konfiguraci dalších rolí a služeb vašeho serveru a současně vám nabídne snadný přístup ke všem vašim denním úlohám správy na serveru.

Pokud si nejste zcela jisti, že jste s průvodcem Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) nadobro hotovi, doporučujeme vám ponechat políčko nezaškrtnuté a průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) ukončit. Díky tomu se sice dále automaticky otevře Správce serveru (Server Manager), ovšem při příštím přihlášení k serveru se zobrazí průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard).

Všechny funkce průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) jsou dostupné i jinde, ovšem myslíme si, že tento průvodce je užitečnou a dobře navrženou funkcí, která shrnuje všechny počáteční kroky, které zřejmě potřebujete

v případě nového serveru učinit, na jedno logické místo. Pokud jste průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard) ukončili a vypnuli jej a poté si uvědomili, že jej potřebujete použít, a nemůžete jej jednoduše najít, vždycky se k němu můžete vrátit zadáním příkazu Oobe.exe na příkazovém řádku.

Shrnutí

V této kapitole jsme se zmínili o základních úlohách počáteční konfigurace, které vás pravděpodobně neminou v případě většiny nových počítačů se systémem Windows Server 2008. Zaměřili jsme se na použití grafického průvodce Úlohami počáteční konfigurace (Initial Configuration Tasks Wizard), který se automaticky spustí na novém serveru, jelikož si myslíme, že se jedná o logického a promyšleného průvodce, nicméně všechny úlohy průvodce Úlohami počátečního nastavení (Initial Configuration Tasks Wizard) lze rovněž provést na příkazovém řádku nebo použitím jednotlivých průvodců. Pokud spouštíte instalaci jádra systému Windows, nemáte na výběr – k provedení počáteční konfigurace budete muset použít příkazový řádek nebo skripty a o instalaci jádra se zmíníme v kapitole 9. Mezitím si v kapitole 8 něco povíme o tom, jak pomocí nástroje Správce serveru přidat role serveru, služby serveru a funkce.

KAPITOLA 8

Instalace rolí serveru a funkcí

Dřívější verze systému Windows Server používaly volný způsob přidání a odebrání různých funkcí a možností systému Windows Server. Tento způsob mohl snadno umožnit zapnutí nepotřebných služeb, a vystavit tím server riziku. Stejně tak bylo možné vypnout kritickou funkci nebo možnost systému Windows Server, a způsobit tak nesprávnou funkčnost jiných služeb či funkcí. Řešení takových problémů bylo časově náročné a frustrující a celkové zabezpečení serveru mohlo být sníženo. Průvodce konfigurací serveru (Configure Your Server Wizard) a Průvodce správou serveru (Manage Your Server Wizard) systému Windows Server 2003 byli pokusem o řešení některých z těchto problémů nabídnutím jednoduchého rozhraní, které umožňovalo na jednom místě přidat nebo odebrat role a spravovat role, které již byly na serveru nainstalovány.

Systém Windows Server 2008 tyto staré průvodce zcela nahrazuje novým nástrojem Správce serveru (Server Manager). Jeho cílem je být jedním místem, kde můžete přidat nebo odebrat role, služby rolí a funkce na server a které vám umožní přístup k veškeré správě již nainstalovaných rolí a funkcí. Správce serveru (Server Manager) je centralizovaným místem pro všechny úlohy správy systému Windows Server 2008 – nebo alespoň taková je teorie. Upřímně řečeno, zjistili jsme, že Správce serveru (Server Manager) je značným vylepšením při přidání a odebrání rolí, služeb rolí a funkcí, ovšem pro každodenní správu zcela ideální není. I nadále budeme používat samostatné konzoly pro role, které potřebujeme spravovat. Je to rychlejší a navigace je v nich jednodušší, přesto však

budeme Správce serveru (Server Manager) používat pro některé úlohy správy. A pro přidání rolí, služeb rolí nebo funkcí je Správce serveru (Server Manager) docela užitečným nástrojem, ačkoliv existuje i alternativa v prostředí příkazového řádku.

Poznámka: Správce serveru (Server Manager) není dostupný v instalacích jádra systému Windows Server 2008. Instalace jádra používá ke konfiguraci jiné nástroje. Pro nastavení jádra serveru se systémem Windows Server 2008 přeskočte ke kapitole 9, „Instalace a konfigurace jádra serveru".

V této kapitole si něco povíme o tom, jak použít grafickou konzolu Správce serveru (Server Manager) a nástroj příkazového řádku ServerManagerCmd.exe k přidání a odebrání rolí, služeb rolí a funkcí.

Definice rolí serveru

Systém Windows Server 2008 rozlišuje mezi rolí serveru, službou role a funkcí. Role serveru jsou obecná seskupení běžných funkcí, které pomáhají definovat účel použití serveru. Proto by měl mít souborový server nainstalovánu roli Souborová služba (File Services) a terminálový server by měl mít nainstalovánu roli Terminálová služba (Terminal Services).

Každá z těchto všeobecně definovaných rolí má k dispozici jednu nebo více služeb rolí. Služba role je konkrétní funkčnost, který je dostupná pouze pro roli, pro niž slouží jako služba role. Pro souborový server s nainstalovanou rolí Souborová služba (File Services) jsou k dispozici následující služby rolí, které mohou být nainstalovány jako součást role Souborová služba (File Services): Souborový server (File Server), Systém souborů DFS (Distributed File System) (a její pomocné služby Obory názvů DFS (DFS Namespaces) a Replikace distribuovaného systému souborů (DFS Replication)), Správce prostředků souborového serveru (File Server Resource Manager), Services for NFS (Services for Network File System), Služba Windows Search (Windows Search Service) a Windows Server 2003 File Services (včetně jejích dvou pomocných služeb Služba replikace souborů (File Replication Service) a Služba indexování (Indexing Service)). Pro roli Terminálové služby (Terminal Services) jsou dostupné následující služby: Terminálový server (Terminal Server), Služba licencování TS (TS Licensing), Zprostředkovatel relací Terminálové služby (TS Session Broker), Brána TS (TS Gateway) a Program TS Web Access (TS Web Access).

Tabulka 8.1 obsahuje seznam rolí a služeb rolí, které jsou dostupné v systému Windows Server 2008.

Tabulka 8.1: Role a služby rolí systému Windows Server 2008

Role	Služba role	Instalační identifikátor
Služba AD CS (Active Directory Certificate Services)		AD-Certificate
	Certifikační autorita (Certification Autority)	ADCS-Cert-Authority

Role	Služba role	Instalační identifikátor
	Webový zápis k certifikační autoritě (Certification Authority Web Enrollment)	ADCS-Web-Enrollment
	Online odpovídací služby (Online Responder Service)	ADCS-Online-Cert
	Služba zápisu síťových zařízení (Network Device Enrollment Service)	ADCS-Device-Enrollment
Služba AD DS (Active Directory Domain Services)		Žádné (instaluje se společně s Dcpromo.exe)
	Řadič domény služby Active Directory (Active Directory Domain Controller)	ADDS-Domain-Controller
	Správa identit pro systém UNIX (Identity Management for UNIX)	ADDS –Identity-Mgmt
	– Server pro službu NIS (Server for Network Information Services)	ADDS-NIS
	– Synchronizace hesel (Password Synchronization)	ADDS-Password-Sync
	– Nástroje pro správu (Administration Tools)	ADDS-IDMU-Tools
Služba AD FS (Active Directory Federation Services)		
	Služba Federation Service (Federation Service)	ADFS -Federation
	Služba FSP (Federation Service Proxy)	ADFS-Proxy
	Weboví agenti služby AD FS (AD FS Web Agents)	ADFS-Web-Agents
	– Agent pracující s deklaracemi (Claims-Aware Agent)	ADFS-Claims
	– Agent pracující s tokeny systému Windows (Windows Token-Based Agent)	ADFS-Windows-Token
Služba AD LDS (Active Directory Lightweight Directory Services)		ADLDS
Služba AD RMS (Active Directory Rights Management Services)		
	Server AD RMS (Active Directory Rights Management Server)	
	Podpora Federace Identit (Identity Federation Support)	
Aplikační server (Application Server)		Application-Server
	Application Server Foundation	AS-AppServer-Foundation
	Podpora webového serveru (Web Server (IIS) Support)	AS-Web-Support
	Přístup k síti modelu COM+ (COM+ Network Access)	AS-Ent-Services
	Sdílení portu TCP (TCP Port Sparing)	AS-TCP-Port-Sharing

Role	Služba role	Instalační identifikátor
	Podpora služby WAS (Windows Process Activation Service Support)	AS-WAS-Support
	– Aktivace protokolem HTTP (HTTP Activation)	AS-HTTP-Activation
	– Aktivace službou Řízení front zpráv (Message Queuing Activation)	AS-MSMQ-Activation
	– Aktivace protokolem TCP (TCP Activation)	AS-TCP-Activation
	– Aktivace pojmenovanými kanály (Named Pipes Activation)	AS-Named-Pipes
	Distribuované transakce (Distributed Transactions)	AS-Dist-Transaction
	– Příchozí vzdálené transakce (Incoming Remote Transactions)	AS-Incoming-Trans
	– Odchozí vzdálené transakce (Outgoing Remote Transactions)	AS-Outgoing-Trans
	– Protokol WS-AT (WS-Atomic Transactions)	AS-WS-Atomic
Server DHCP (DHCP Server)		DHCP
Server DNS (DNS Server)		DNS
Faxový server (Fax Server)		Fax
Souborová služba (File Services)		
	Souborový server (File Server)	FS-FileServer
	Systém souborů DFS (Distributed File System)	FS-DFS
	– Obory názvů DFS (DFS Namespaces)	FS-DFS-Namespace
	– Replikace distribuovaného systému souborů (DFS Replication)	FS-DFS-Replication
	Správce prostředků souborového serveru (File Server Resource Manager)	FS-Resource-Manager
	Services for NFS (Services for Network File System)	FS-NFS-Services
	Služba Windows Search (Windows Search Service)	FS-Search-Service
	Souborová služba systému Windows Server 2003 (Windows Server 2003 File Services)	FS-Win2003-Services
	– Služba replikace souborů (File Replication Service)	FS-Replication
	– Služba indexování (Indexing Service)	FS-Indexing-Service
Hyper-V		Hyper-V
Služba Síťové zásady a přístup (Network Policy and Access Services)		NPAS
	Server NPS (Network Policy Server)	NPAS-Policy-Server

Role	Služba role	Instalační identifikátor
	Služba Směrování a vzdálený přístup (Routing and Remote Access Services)	NPAS-RRAS-Services
	– Služba vzdáleného přístupu (Remote Access Service)	NPAS-RRAS
	– Směrování (Routing)	NPAS-Routing
	Autorita pro registraci stavu (Health Registration Authority)	NPAS-Health
	Protokol HCAP (Host Credential Authorization Protocol)	NPAS-Host-Cred
Tiskové služby (Print Services)		Print-Services
	Tiskový server (Print Server)	Print-Server
	Služba LDP (LPD Service)	Print-LPD-Service
	Tisk přes Internet (Internet Printing)	Print-Internet
Terminálová služba (Terminal Services)		Terminal-Services
	Terminálový server (Terminal Server)	TS-Terminal-Server
	Služba Licencování TS (TS Licensing)	TS-Licensing
	Zprostředkovatel relací Terminálové služby (TS Session Broker)	TS-Session-Broker
	Brána TS (TS Gateway)	TS-Gateway
	Program TS Web Access (TS Web Access)	TS-Web-Access
Služba UDDI (UDDI Services)		
	Databáze služby UDDI (UDDI Services Database)	
	Webová aplikace služby UDDI (UDDI Services Web Application)	
Webový server (IIS) (Web Server (IIS))		Web-Server
	Webový server (Web Server)	Web-WebServer
	– Společné funkce protokolu HTTP (Common HTTP Features)	Web-Common-Http
	Statický obsah (Static Content)	Web-Static-Content
	– Výchozí dokument (Default Document)	Web-Default-Doc
	– Procházení adresářů (Directory Browsing)	Web-Dir-Browsing
	– Chyby protokolu HTTP (HTTP Errors)	Web-Http-Errors
	– Přesměrování protokolu HTTP (HTTP Redirection)	Web-Http-Redirect
	– Technologie Vývoj aplikací (Application Development)	Web-App-Dev
	– ASP.NET	Web-Asp-Net

Role	Služba role	Instalační identifikátor
	– Rozšiřitelnost rozhraní .NET (.NET Extensibility)	Web-Net-Ext
	– ASP	Web-ASP
	– CGI	Web-CGI
	– Rozšíření ISAPI (ISAPI Extensions)	Web-ISAPI-Ext
	– Filtry ISAPI (ISAPI Filters)	Web-ISAPI-Filter
	– Součást Začlenění na straně serveru (Server Side Includes)	Web-Includes
	– Stav a diagnostika (Health and Diagnostics)	Web-Health
	– Protokolování HTTP (HTTP Logging)	Web-Http-Logging
	– Nástroje protokolování (Logging Tools)	Web-Log-Libraries
	– Sledování požadavků (Request Monitor)	Web-Request-Monitor
	– Trasování (Tracing)	Web-Http-Tracing
	– Vlastní protokolování (Custom Logging)	Web-Custom-Logging
	– Protokolování pomocí rozhraní ODBC (ODBC Logging)	Web-ODBC-Logging
	– Zabezpečení (Security)	Web-Security
	– Základní ověřování (Basic Authentication)	Web-Basic-Auth
	– Ověřování systému Windows (Windows Authentication)	Web-Windows-Auth
	– Ověřování algoritmem Digest (Digest Authentication)	Web-Digest-Auth
	– Ověřování pomocí mapování certifikátu klienta (Client Certificate Mapping Authentication)	Web-Client-Auth
	– Ověřování pomocí mapování klienta služby IIS (IIS Client Certificate Mapping Authentication)	Web-Cert-Auth
	– Autorizace adres URL (URL Authorization)	Web-Url-Auth
	– Filtrování požadavků (Request Filtering)	Web-Filtering
	– Omezení podle adresy IP nebo domény (IP and Domain Restrictions)	Web-IP-Security
	– Výkon (Performance)	Web-Performance
	– Komprese statického obsahu (Static Content Compression)	Web-Stat-Compression
	– Komprese dynamického obsahu (Dynamic Content Compression)	Web-Dyn-Compression
	– Nástroje pro správu (Management Tools)	Web-Mgmt-Tools
	– Konzola pro správu služby IIS (IIS Management Console)	Web-Mgmt-Console

Role	Služba role	Instalační identifikátor
	– Skripty a nástroje správy služby IIS (IIS Management Scripts and Tools)	Web-Scripting-Tools
	– Služba správy (Management Service)	Web-Mgmt-Service
	– Kompatibilita správy služby IIS 6 (IIS 6 Management Compatibility)	Web-Mgmt-Compat
	– Kompatibilita metabáze služby IIS 6 (IIS 6 Metabase Compatibility)	Web-Metabase
	– Kompatibilita rozhraní WMI služby IIS 6 (IIS 6 WMI Compatibility)	Web-WMI
	– Nástroje pro skriptování služby IIS 6 (IIS 6 Scripting Tools)	Web-Lgcy-Scripting
	– Konzola pro správu služby IIS 6 (IIS 6 Management Console)	Web-Lgcy-Mgmt-Console
	– Služba Publikování FTP (FTP Publishing Service)	Web-Ftp-Publishing
	– Server FTP (FTP Server)	Web-Ftp-Server
	– Konzola Správa FTP (FTP Management Console)	Web-Ftp-Mgmt-Console
Služba pro nasazení systému Windows (Windows Deployment Services)		
	Server nasazení (Deployment Server)	WDS-Deployment
	Transportní server (Transport Server)	WDS-Transport

Funkce zajišťují funkčnost systému Windows Server 2008, která nevyžaduje nainstalování konkrétní role. Funkce jsou užitečné napříč širokým spektrem konfigurací rolí serveru. Funkce zahrnují obecné, univerzální funkce, například prostředí Windows PowerShell, stejně jako specializované funkce, nikoliv však specifické pro určitou roli, jako například Server iSNS (Internet Storage Name Server (iSNS)) nebo Řízení front zpráv (Message Queuing). Tabulka 8.2 obsahuje seznam funkcí dostupných v systému Windows Server 2008.

Tabulka 8.2: Funkce systému Windows Server 2008

Funkce	Instalační identifikátor
Funkce rozhraní .NET Framework 3.0 (.NET Framework 3.0 Features)	NET-Framework
– .NET Framework 3.0	NET-Framework-Core
– Prohlížeč XPS (XPS Viewer)	NET-XPS-Viewer
– Aktivace služby WCF (WCF Activation)	NET-Win-CFAC
– Aktivace protokolem HTTP (HTTP Activation)	NET-HTTP-Activation
– Aktivace jiným protokolem (Non-HTTP Activation)	NET-Non-HTTP-Activ

Funkce	Instalační identifikátor
BitLocker Drive Encryption	BitLocker
Rozšíření serveru BITS (BITS Server Extensions)	BITS
Sada pro správu Správce připojení (Connection Manager Administration Kit)	CMAK
Možnosti práce s počítačem (Desktop Experience)	Desktop-Experience
Clustering s podporou převzetí služeb při selhání (Failover Clustering)	Failover-Clustering
Správa zásad skupiny (Group Policy Management)	GPMC
Klient tisku přes Internet (Internet Printing Client)	Internet-Print-Client
Server iSNS (Internet Storage Name Server)	ISNS
Sledování portu LPR (LPR Port Monitor)	LPR-Port-Monitor
Řízení front zpráv (Message Queuing)	MSMQ
– Služba Řízení front zpráv (Message Queuing Services)	MSMQ-Services
– Server služby Řízení front zpráv (Message Queuing Server)	MSMQ-Server
– Integrace adresářové služby (Directory Service Integration)	MSMQ-Directory
– Aktivace řízení front zpráv (Message Queuing Triggers)	MSMQ-Triggers
– Podpora protokolu HTTP (HTTP Support)	MSMQ-HTTP-Support
– Podpora vícesměrového vysílání (Multicasting Support)	MSMQ-Multicasting
– Směrovací služby (Routing Service)	MSMQ-Routing
– Podpora klientů se systémem Windows 2000 (Windows 2000 Client Support)	MSMQ-Win2000
– Server proxy DCOM služby Řízení fronty zpráv (Message Queuing DCOM Proxy)	MSMQ-DCOM
Multipath I/O	Multipath-IO
Vyrovnávání zatížení sítě (Network Load Balancing)	NLB
Protokol PNRP (Peer Name Resolution Protocol)	PNRP
Služba qWave (Quality Windows Audio Video Experience)	qWave
Vzdálená pomoc (Remote Assistance)	Remote-Assistance
Algoritmus RDC (Remote Differential Compression)	RDC
Nástroje pro vzdálenou správu serveru (Role Server Administration Tools)	RSAT
Nástroje pro správu rolí (Role Administration Tools)	RSAT-Role-Tools
Nástroje služby AD CS (Active Directory Certificate Services)	Tools RSAT-ADCS
Nástroje certifikační autority (Certification Authority Tools)	RSAT-ADCS-Mgmt
Nástroje online odpovídajících zařízení (Online Responder Tools)	RSAT-Online-Responder
Nástroje služby AD DS (Active Directory Domain Services Tools)	RSAT-ADDS
Nástroje řadiče domény služby Active Directory (Active Directory Domain Controller Tools)	RSAT-ADDC
Nástroje serveru pro službu NIS (Server for NIS Tools)	RSAT-SNIS

Funkce	Instalační identifikátor
Nástroje služby AD LDS (Active Directory Lightweight Directory Services Tools)	RSAT-ADLDS
Nástroje služby AD RMS (Active Directory Rights Management Services Tools)	RSAT-RMS
Nástroje pro server DHCP (DHCP Server Tools)	RSAT-DHCP
Nástroje serveru DNS (DNS Server Tools)	RSAT-DNS-Server
Nástroje faxového serveru (Fax Server Tools)	RSAT-Fax
Nástroje souborové služby (File Services Tools)	RSAT-File-Services
Nástroje systému souborů DFS (Distributed File System Tools)	RSAT-DFS-Mgmt-Con
Nástroje správce prostředků souborového serveru (File Server Resource Manager Tools)	RSAT-FSRM-Mgmt
Nástroje Hyper-V (Hyper-V)	RSAT-Hyper-V
Nástroje služby Services for Services for Network File System (Services for Network File System Tools)	RSAT-NFS-Admin
Nástroje služby Síťové zásady a přístup (Network Policy and Access Services Tools)	RSAT-NPAS
Nástroje Tiskové služby (Print Services Tools)	RSAT-Print-Services
Nástroje Terminálové služby (Terminal Services Tools)	RSAT-TS
Nástroje Terminálového serveru (Terminal Server Tools)	RSAT-TS-RemoteApp
Nástroje brány Terminálové služby (TS Gateway Tools)	RSAT-TS-Gateway
Nástroje licencování TS (TS Licensing Tools)	RSAT-TS-Licensing
Nástroje služby UDDI (UDDI Services Tools)	RSAT-UDDI
Nástroje webového serveru (IIS) (Web Server (IIS) Tools)	RSAT-Web-Server
Nástroje služby pro nasazení systému Windows (Windows Deployment Services Tools)	RSAT-WDS
Nástroje pro správu funkcí (Feature Administration Tools)	RSAT-Feature-Tools
Nástroje BitLocker Drive Encryption (BitLocker Drive Encryption Tools)	RSAT-BitLocker
Nástroje rozšíření serveru BITS (BITS Server Extensions Tools)	RSAT-Bits-Server
Nástroje clusteringu s podporou převzetí služeb při selhání (Failover Clustering Tools)	RSAT-Clustering
Nástroje služby Vyrovnávání zatížení sítě (Network Load Balancing Tools)	RSAT-NLB
Nástroje serveru SMTP (SMTP Server Tools)	RSAT-SMTP
Nástroje serveru WINS (WINS Server Tools)	RSAT-WINS
Správce vyměnitelného úložiště (Removable Storage Manager)	Removable-Storage
Služba Vzdálené volání procedur prostřednictvím serveru HTTP Proxy (RPC over HTTP Proxy)	RPC-over-HTTP-Proxy
Jednoduché služby TCP/IP (Simple TCP/IP Services)	Simple-TCPIP
Server SMTP (SMTP Server)	SMTP-Server
Služba SNMP (SNMP Services)	SNMP-Services
Služba SNMP (SNMP Service)	SNMP-Service

Funkce	Instalační identifikátor
Zprostředkovatel rozrhaní WMI protokolu SNMP (SNMP WMI Provider)	SNMP-WMI-Provider
Správce úložiště pro sítě SAN (Storage Manager for SANs)	Storage-Mgr-SANS
Subsystém pro unixové aplikace (Subsystem for UNIX-based Applications)	Subsystem-UNIX-Apps
Klient služby Telnet (Telnet Client)	Telnet-Client
Server Telnet (Telnet Server)	Telnet-Server
Klient TFTP (TFTP Client)	TFTP-Client
Interní databáze systému Windows (Windows Internal Database)	Windows-Internal-DB
Prostředí Windows PowerShell (Windows PowerShell)	PowerShell
Služba WAS (Windows Process Activation Service)	WAS
Model procesu (Process Model)	WAS-Process-Model
Prostředí .NET (.NET Environment)	WAS-NET-Environment
Rozhraní API konfigurace (Configuration APIs)	WAS-Config-APIs
Funkce služby Zálohování serveru (Windows Server Backup Features)	Backup-Features
Zálohování serveru (Windows Server Backup)	Backup
Nástroje příkazového řádku (Command-line Tools)	Backup-Tools
Správce systémových prostředků (Windows System Resource Manager)	WSRM
Server WINS (WINS Server)	WINS-Server
Služba bezdrátové sítě LAN (Wireless LAN Service)	Wireless-Networking

Jak je zřejmé z tabulek 8.1 a 8.2, existuje celá řada rolí, služeb rolí a funkcí, které je možné nainstalovat. Všechny lze instalovat buď z konzoly Správce serveru (Server Manager), nebo z příkazového řádku se zvýšeným oprávněním (pomocí příkazu ServerManagerCmd.exe). Jedinou zvláštností je, že role Active Directory Domain Services (AD DS) se instaluje z konzoly Správce serveru (Server Manager), ovšem nedělá nic, dokud nespustíte příkaz Dcpromo.exe. Po jeho spuštění se nejprve zkontroluje, zda-li je role AD DS nainstalována, a pokud tomu tak není, nainstaluje roli a poté začne s povýšením serveru na řadič domény.

Přidání a odebrání rolí

Přidání a odebrání rolí na/ze sytému Windows Server 2008 lze provést buď z konzoly Správce serveru (Server Manager), nebo z příkazového řádku. Oba způsoby provádí stejné úlohy a při instalaci služeb postupují stejně. Ovšem mnohem jednodušší je k tomuto kroku použít grafické uživatelské rozhraní, takže pokud neprovádíte instalaci mnoha serverů, které jsou všechny stejně nakonfigurovány, vřele doporučujeme použít k tomuto úkolu konzolu Správce serveru (Server Manager). (Nemůžeme uvěřit tomu, že jsme to řekli – jsme totiž ortodoxní vyznavači příkazového řádku ve všech případech, kdy je to možné. Ovšem tohle je poprvé, kdy má použití grafického rozhraní smysl.)

Z praxe: Role – zbytečné omezení, nebo chytré vylepšení?

Když jsme poprvé narazili na nový požadavek vždycky použít k instalaci rolí, služeb rolí a funkcí konzolu Správce serveru (Server Manager), nebyli jsme z toho zrovna šťastni. Vlastně jsme si hlasitě a s notnou dávkou entusiasmu stěžovali více než tuctu uší ve společnosti Microsoft. Zřejmě v tu chvíli nepomohlo, že zmíněná funkce nebyla ještě dokončena; ještě neobsahovala alternativu příkazového řádku a nainstalovat jste mohli v jednu chvíli pouze jednu roli, službu role nebo funkci. Ovšem stále jsme tuto funkci považovali v systému Windows Server 2008 za zbytečnou a neproduktivní. Každý, komu jsme to řekli, nás nabádal k trpělivosti. No, *neradi* to přiznáváme, ale měli pravdu. Přidávání a odebírání rolí, služeb rolí a funkcí pomocí nové konzoly Správce serveru (Server Manager) je bezesporu mnohem lepší a chytřejší. Nejen že vždy správně určí *minimální* úroveň závislých služeb, ale rovněž automaticky nakonfiguruje správné výjimky brány Windows Firewall. A pokud instalujete role z konzoly Správce serveru (Server Manager), je přidání jen těch potřebných služeb rolí triviálně jednoduché. A navíc můžete přidat celou skupinu rolí a služeb rolí v jednom okamžiku nebo celou množinu funkcí najednou – a díky tomu je nastavení nového serveru podle vašich potřeb docela rychlé a snadné.

Nicméně jsme zjistili, že pokud přidáte najednou více než jednu roli nebo funkci, pravděpodobnost nutnosti restartování serveru patrně vzroste. To je jistě nepříjemné. A také není možno přidat funkce ve stejném kroku s přidáním rolí a služeb rolí – tedy další nepříjemnost, třebaže nijak velká.

A na závěr poslední nepříjemnost. Pokud přidáváte role nebo funkce jednu po druhé, téměř vždy se můžete vyhnout restartování systému. Ovšem při odebrání role nebo funkce budete muset s velkou pravděpodobností restartování provést.

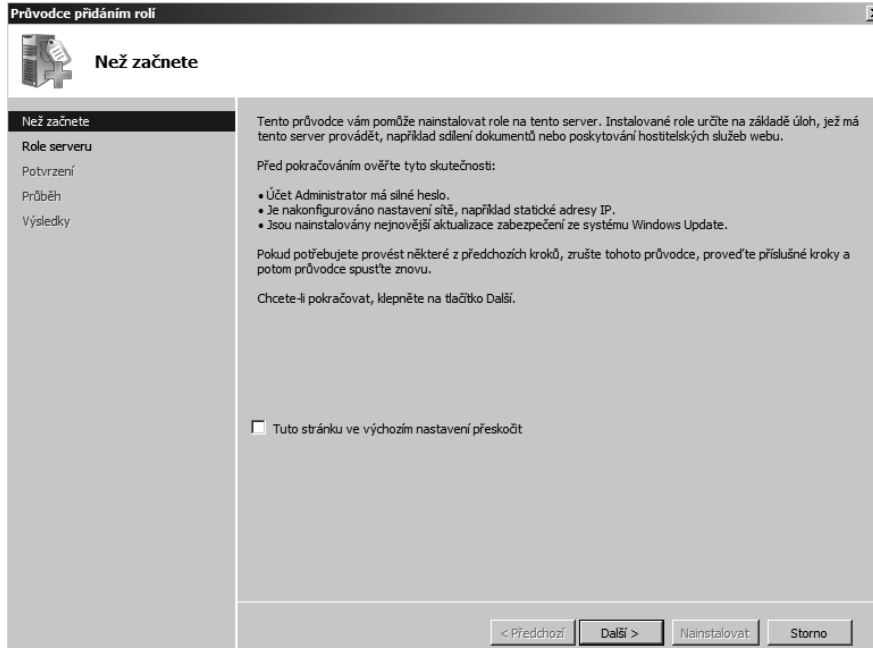
Přidání role

K přidání role můžete použít buď grafickou konzolu Správce serveru (Server Manager), nebo nástroj příkazového řádku ServerManagerCmd.exe.

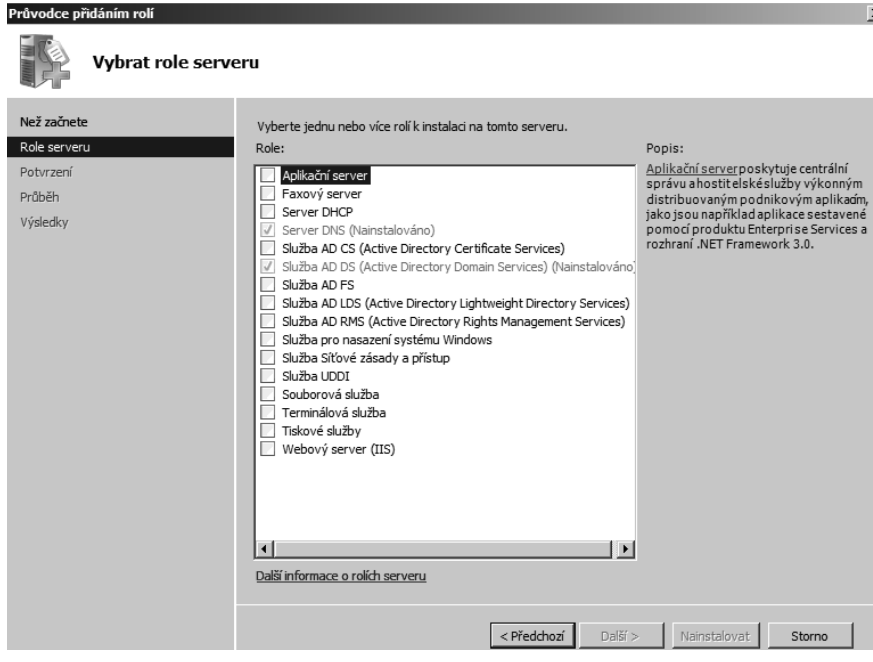
Použití konzoly Server Manager

Pro přidání role z konzoly Správce serveru (Server Manager) postupujte podle následujících kroků:

1. Otevřete konzolu Správce serveru (Server Manager), pokud již není otevřena.
2. Výběrem příkazu Přidat role (Add Roles) v nabídce Akce (Action) otevřete stránku Než začnete (Before You Begin) Průvodce přidáním rolí (Add Roles Wizard), viz obrázek 8.1.
3. Přečtěte si pokyny na stránce Než začnete (Before You Begin). Jsou to opravdu dobré rady, které je dobré si zapamatovat. Po přečtení této stránky a pochopení všech jejích důsledků ji už možná nebudete chtít znovu zobrazit, takže zaškrtněte políčko Tuto stránku ve výchozím nastavení přeskočit (Skip This Page By Default). (My jej nechávám raději nezaškrtnuto.)
4. Klepnutím na tlačítko Další (Next) otevřete stránku Vybrat role serveru (Select Server Roles), znázorněnou na obrázku 8.2.



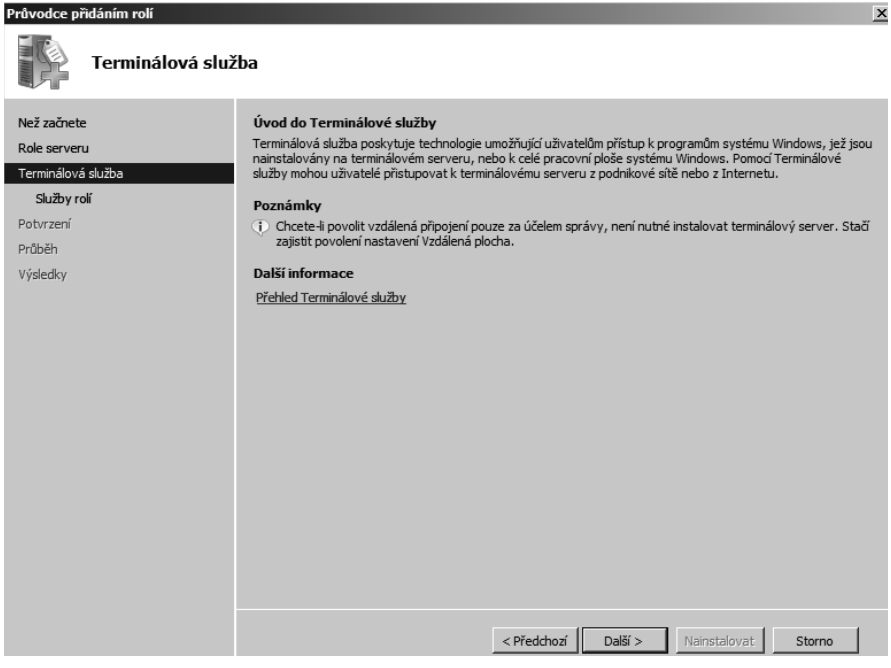
Obrázek 8.1: Stránka Než začnete (Before You Begin) Průvodce přidáním rolí (Add Roles Wizard)



Obrázek 8.2: Stránka Vybrat role serveru (Select Server Roles) Průvodce přidáním rolí (Add Roles Wizard)

5. Vyberte role serveru, které chcete přidat. Můžete vybrat víc než jednu, ovšem zvýšíte tím pravděpodobnost, že budete muset před dokončením instalace restartovat počítač.

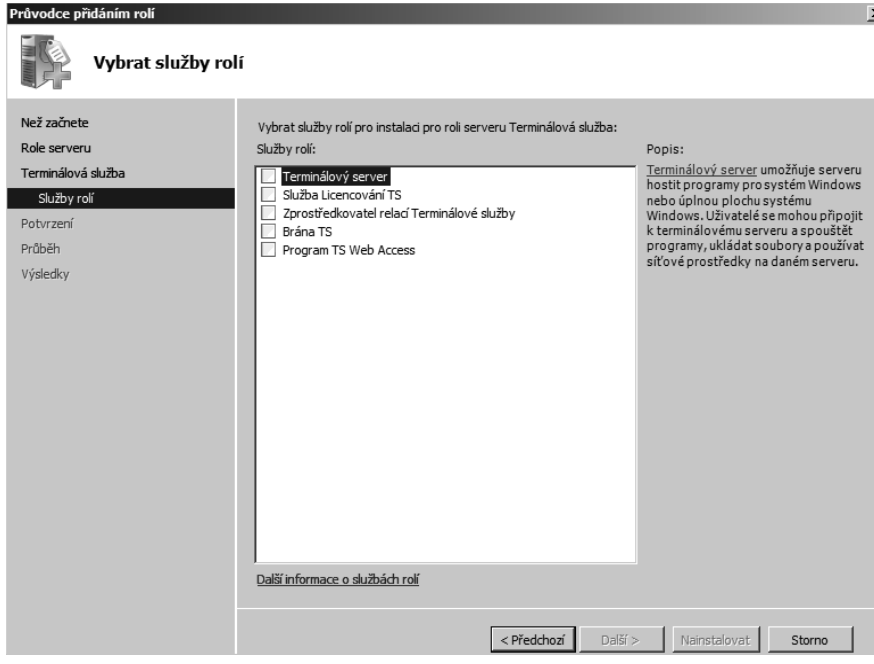
6. Klepnutím na tlačítko Další (Next) otevřete stránku první role, která se nainstaluje, viz obrázek 8.3 (pokud jste v předchozím kroku vybrali roli Terminálová služba (Terminal Services)). Tato stránka popisuje instalovanou roli a obsahuje i část Poznámky (Things To Note), která obsahuje upozornění nebo rady týkající se konkrétní instalované role. Rovněž je zde odkaz na stránku Další informace (Additional Information) s aktuálními informacemi o instalované roli.



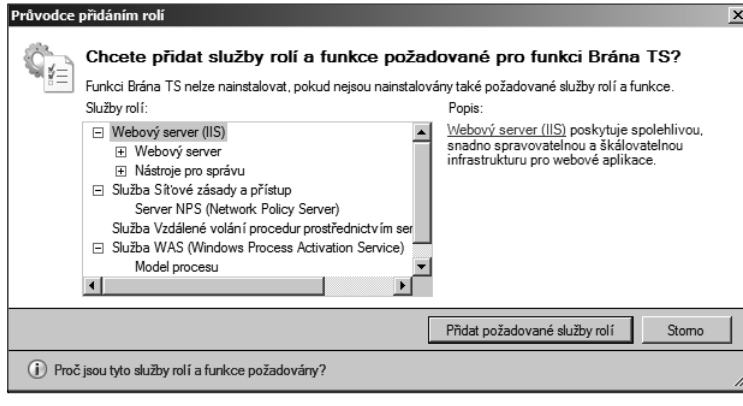
Obrázek 8.3: Stránka Terminálová služba (Terminal Services) Průvodce přidáním rolí (Add Roles Wizard)

7. Po přečtení všech informací v části Poznámky (Things To Note) klepnutím na tlačítko Další (Next) otevřete stránku Vybrat služby rolí (Select Role Services), znázorněnou na obrázku 8.4.

8. Vyberte služby rolí, které chcete v tuto chvíli přidat. Pokud vyberte služby rolí, které jsou závislé na jiné roli, službě role nebo funkci, automaticky se otevře dialog s popisem dalších služeb rolí, které budou nainstalovány, viz obrázek 8.5.



Obrázek 8.4: Stránka Vybrat služby rolí (Select Role Services) Průvodce přidáním rolí (Add Roles Wizard)



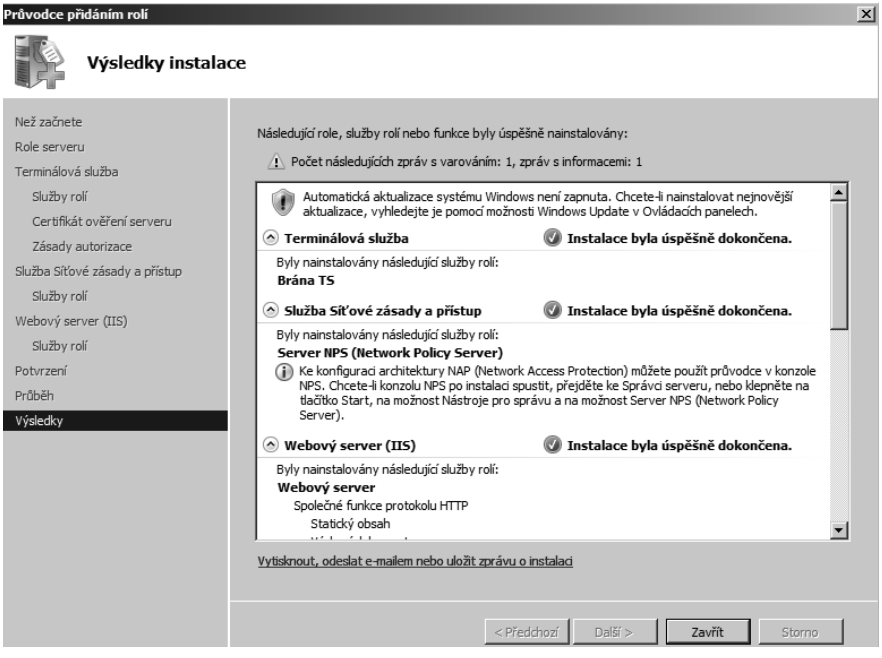
Obrázek 8.5: Stránka Chcete přidat služby rolí a funkce požadované pro funkci Brána TS? (Add Role Services And Features Required For TS Gateway) Průvodce přidáním rolí (Add Roles Wizard)

9. Pokračujte klepnutím na tlačítko Přidat požadované služby rolí (Add Required Role Services) a vraťte se na stránku Vybrat služby rolí (Select Role Services), nebo klepněte na tlačítko Storno (Cancel), pokud chcete změnit váš výběr služeb rolí.

10. Klepnutím na tlačítko Další (Next) otevřete další stránku v Průvodci přidáním rolí (Add Roles Wizard). Odsud až do konce průvodce se budou jednotlivé stránky lišit v závislosti na vámi vybraných rolích a službách rolí.

11. Když Průvodce přidáním rolí (Add Roles Wizard) zpracuje všechny potřebné informace, otevře stránku Potvrdit vybrané možnosti instalace (Confirm Installation Selections). Ta je posledním místem, kde můžete zkontrolovat, že jste vybrali potřebné role a služby rolí a nakonfigurovali všechna potřebná nastavení vhodná pro vaše prostředí. Pokud se vše zdá být v pořádku, klepnutím na tlačítko Nainstalovat (Install) zahajte instalaci.

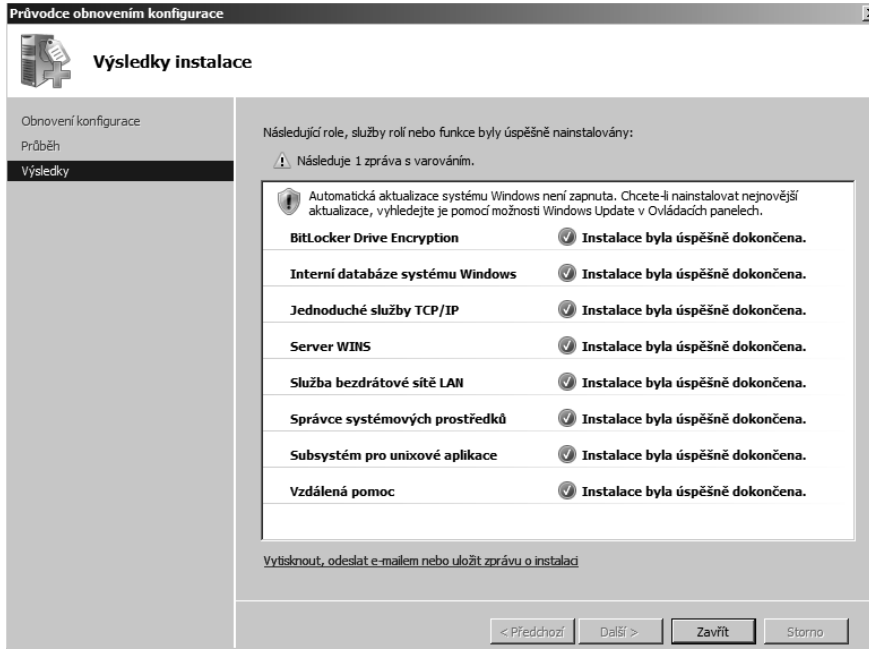
12. Po dokončení instalace se zobrazí stránka Výsledky instalace (Installation Results), znázorněná na obrázku 8.6. Pokud instalace bude vyžadovat restartování systému nebo pokud se vyskytnou nějaká jiná upozornění nebo chyby, zjistíte to na této stránce. Klepnutím na tlačítko Zavřít (Close) ukončete průvodce.



Obrázek 8.6: Stránka Výsledky instalace (Installation Results)

13. Pokud bude instalace vyžadovat restartování, budete vyzváni k restartování serveru. Rovněž tak můžete učinit hned, protože až do jeho provedení nemůžete instalovat nic jiného.

14. Pokud instalace vyžaduje restartování, nezapomeňte se opět přihlásit pomocí stejného účtu, který jste použili k přidání role. Instalace nemůže být dokončena, dokud se znovu nepřihlásíte pomocí téhož účtu. Otevře se Průvodce obnovením konfigurace (Resume Configuration Wizard) a dokončí instalaci vybraných rolí a služeb rolí, viz obrázek 8.7. Po dokončení instalace klepněte na tlačítko Zavřít (Close).



Obrázek 8.7: Stránka Výsledky instalace (Installation Results) průvodce Průvodce obnovením instalace (Resume Configuration Wizard)

Použití příkazového řádku

Pro přidání role pomocí příkazového řádku postupujte podle následujících kroků:

1. Otevřete okno příkazového řádku se zvýšeným oprávněním klepnutím pravým tlačítkem myši na zástupci Příkazový řádek (Command Prompt) v nabídce Start a výběrem příkazu Spustit jako správce (Run As Administrator).
2. Zadáním příkazu **ServerManagerCmd /?** zobrazte seznam možností příkazového řádku pro daný příkaz.
3. K instalaci role Terminálová služba (Terminal Services) se službou role Terminálový server (Terminal Server) použijte následující příkaz:

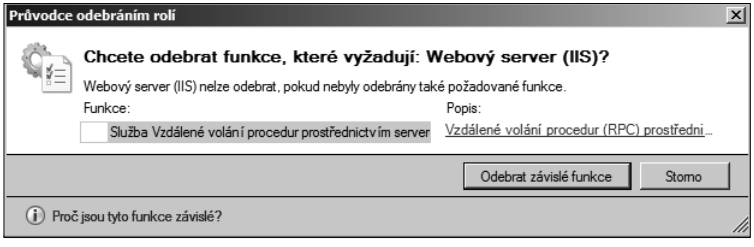
   ```
   ServerManagerCmd -install Terminal-Services TS-Terminal-Server -restart
   ```

4. Použijte-li parametr příkazového řádku *–restart*, server se v případě, že to instalace vyžaduje, automaticky restartuje (bez upozornění nebo prodlevy).

Odebrání role

K odebrání role můžete použít buď grafickou konzolu Správce serveru (Server Manager), nebo můžete použít nástroj příkazového řádku ServerManagerCmd.exe. Obě varianty plní stejnou funkci: odeberou pouze explicitně vybranou roli. Obvykle neodeberou žádné role nebo služby rolí, které byly přidány během počáteční instalace rolí podporujících odebíranou roli – pokud daná role, služba role nebo funkce *nevyžaduje* roli, kterou ode-

bíráte. To je poněkud matoucí, viďte? Dobrá, možná to více objasní konkrétní příklad: Řekněme, že jste nainstalovali roli Terminálová služba (Terminal Services) se všemi jejími službami role. Rovněž budete mít nainstalovánu roli Služby Síťové zásady a přístup (Network Policy And Access Services) a roli Webový server (IIS) (Web Server (IIS)). Nemůžete odinstalovat celou roli Terminálová služba (Terminal Services) a nedojde ani k odebrání rolí Služby Síťové zásady a přístup (Network Policy And Access Services) a Webový server (IIS) (Web Server (IIS)). Ovšem pokud odeberte roli Webový server (IIS) (Web Server (IIS)), rovněž se odebere funkce Služba Vzdálené volání procedur pomocí serveru HTTP Proxy (RPC over HTTP Proxy), viz obrázek 8.8.



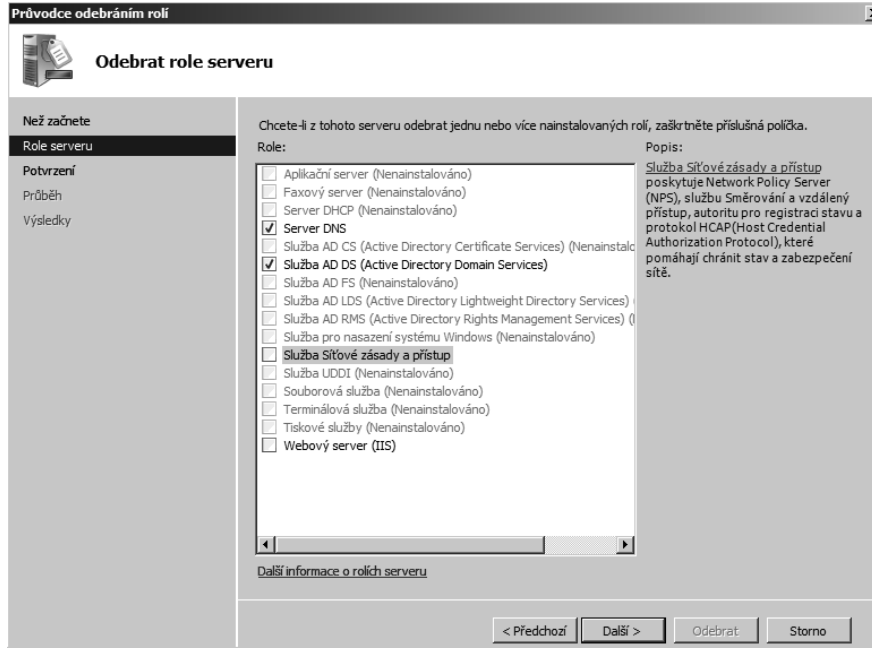
Obrázek 8.8: Odebrání role Webový server (IIS) (Web Server (IIS)) vyžaduje odebrání funkce role Služba Vzdálené volání procedur prostřednictvím serveru HTTP Proxy (RPC over HTTP Proxy)

Použití konzoly Správce serveru (Server Manager)

Použití konzoly Správce serveru (Server Manager) k odebrání role je obvykle lepším řešením než použití příkazového řádku. Při použití konzoly Správce serveru (Server Manager) můžete vidět, které další role a služby rolí se rovněž instalují, což usnadňuje odebrání všech rolí a služeb rolí, které nejsou potřeba, ale které nejsou automaticky odebrány.

K odebrání role pomocí konzoly Správce serveru (Server Manager) postupujte podle následujících kroků:

1. Otevřete konzolu Správce serveru (Server Manager), pokud již není otevřena.
2. Výběrem příkazu Odebrat role (Remove Roles) v nabídce Akce (Action) otevřete stránku Než začnete (Before You Begin) Průvodce odebráním rolí (Remove Roles Wizard).
3. Přečtěte si pokyny na stránce Než začnete (Before You Begin). Jsou to opravdu dobré rady, které je dobré si zapamatovat. Po přečtení této stránky a pochopení všech jejích důsledků ji už možná nebudete chtít znovu zobrazit, takže zaškrtněte políčko Tuto stránku ve výchozím nastavení přeskočit (Skip This Page By Default). (My jej nechávame raději nezaškrtnuto.)
4. Klepnutím na tlačítko Další (Next) otevřete stránku Odebrat role serveru (Remove Server Roles), znázorněnou na obrázku 8.9. Zrušte zaškrtnutí rolí, které chcete odebrat.

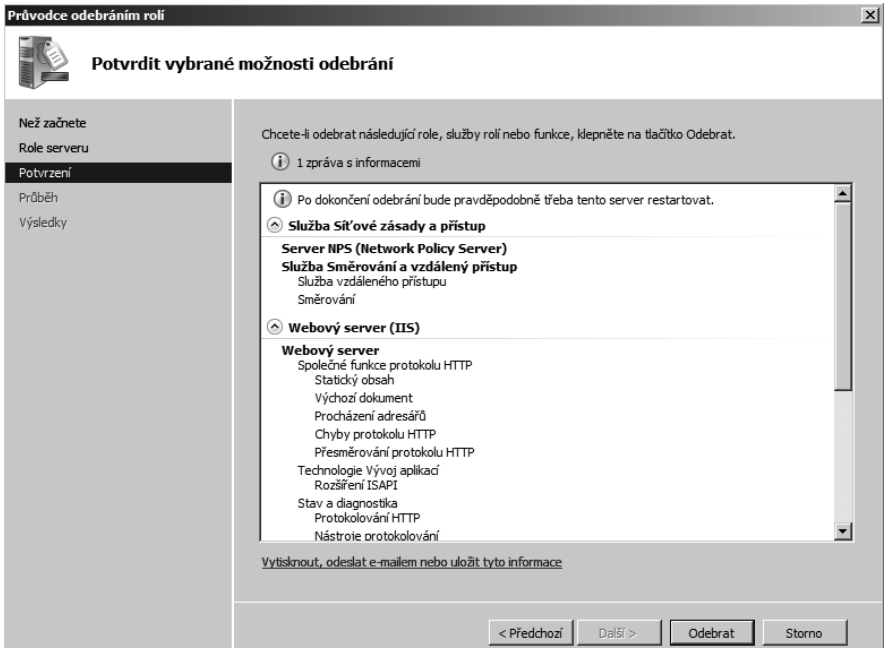


Obrázek 8.9: Stránka Odebrat role serveru (Remove Server Roles) Průvodce odebráním rolí (Remove Roles Wizard)

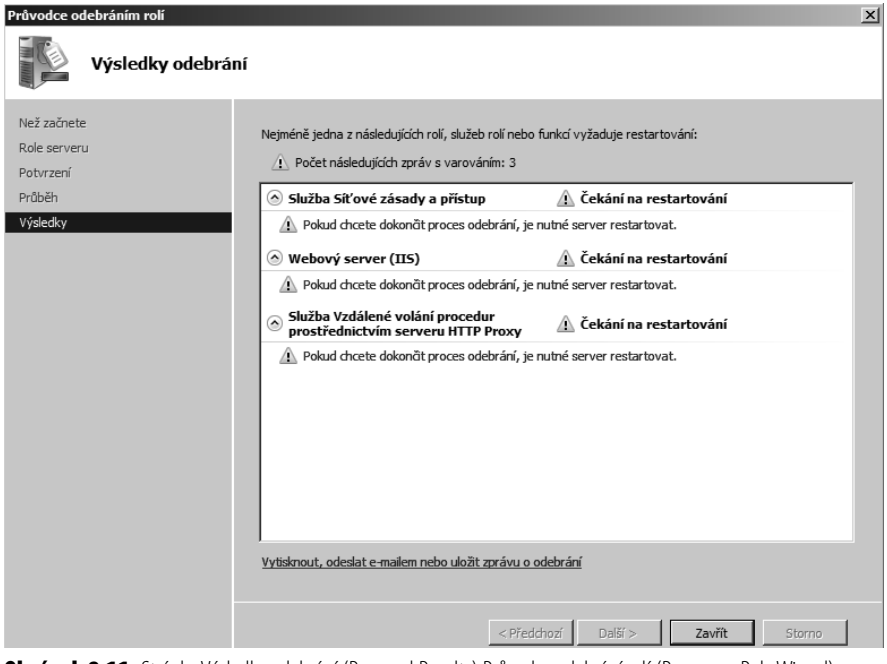
5. Pokud existují nějaké závislé funkce, budete rovněž vyzváni k jejich odebrání, jak znázorňuje dříve uvedený obrázek 8.8.
6. Po zrušení zaškrtnutí políček u všech rolí, které chcete odebrat, klepnutím na tlačítko Další (Next) otevřete stránku Potvrdit vybrané možnosti odebrání (Confirm Removal Selections), znázorněnou na obrázku 8.10. Tato stránka bude často obsahovat jednu nebo více informačních zpráv. Ujistěte se, že rozumíte všem následkům odebrání role nebo rolí.

Poznámka: Informace na stránce Potvrzení vybrané možnosti odebrání (Confirm Removal Selections) si můžete vytisknout, odeslat e-mailem nebo uložit klepnutím na odkaz pod informačním oknem.

7. Klepnutím na tlačítko Odebrat (Remove) zahajte odebrání.
8. Po dokončení odebrání se zobrazí stránka Výsledky odebrání (Removal Results), znázorněná na obrázku 8.11. Pokud některá z rolí či funkcí vyžaduje restartování systému, zobrazí se zpráva upozorňující vás na nutnost restartování počítače. Naše zkušenosti jsou takové, že restartování vyžaduje odebrání téměř čehokoliv.



Obrázek 8.10: Stránka Potvrdit vybrané možnosti odebrání (Confirm Removal Selections) Průvodce odebráním rolí (Remove Roles Wizard)



Obrázek 8.11: Stránka Výsledky odebrání (Removal Results) Průvodce odebrání rolí (Remove a Role Wizard)

9. Klepněte na tlačítko Zavřít (Close) a při výzvě k restartování počítače klepněte na tlačítko Ano (Yes).

10. Pokud odebrání vyžaduje restartování, nezapomeňte se opět přihlásit pomocí stejného účtu, který jste použili k odebrání role. Odebrání nemůže být dokončeno, dokud se znovu nepřihlásíte pomocí téhož účtu. Otevře se Průvodce obnovením konfigurace (Resume Configuration Wizard) a dokončí odebrání vybraných rolí. Po dokončení odebrání klepněte na tlačítko Zavřít (Close).

Použití příkazového řádku

Celkově si myslíme, že použití příkazového řádku k odebrání role není vůbec dobrým nápadem. Opravdu nijak nevidíte, co se stane, a existuje velmi málo případů použití hromadného odebrání rolí na tolika serverech, aby bylo zapotřebí nějakého automatizovaného řešení. Ovšem pokud na tom opravdu trváte, syntaxe příkazového řádku je naprosto stejná jako pro přidání role. K odebrání role pomocí příkazového řádku použijte následující příkaz:

```
ServerManagerCmd -remove <instalační_identifikátor> -restart
```

<*instalační_identifikátor*> všech rolí a služeb rolí najdete v tabulce 8.1.

Přidání a odebrání služeb rolí

V mnoha situacích budete přidávat nebo odebírat služby rolí jako součást přidání a odebrání rolí, pro které jsou tyto služby určeny. Ovšem poměrně často budete začínat s jednou sadou služeb rolí pro konkrétní roli a v určitou chvíli budete mít potřebu přidat nějakou službu role, nebo dokonce odebrat službu role, kterou již nadále nepotřebujete.

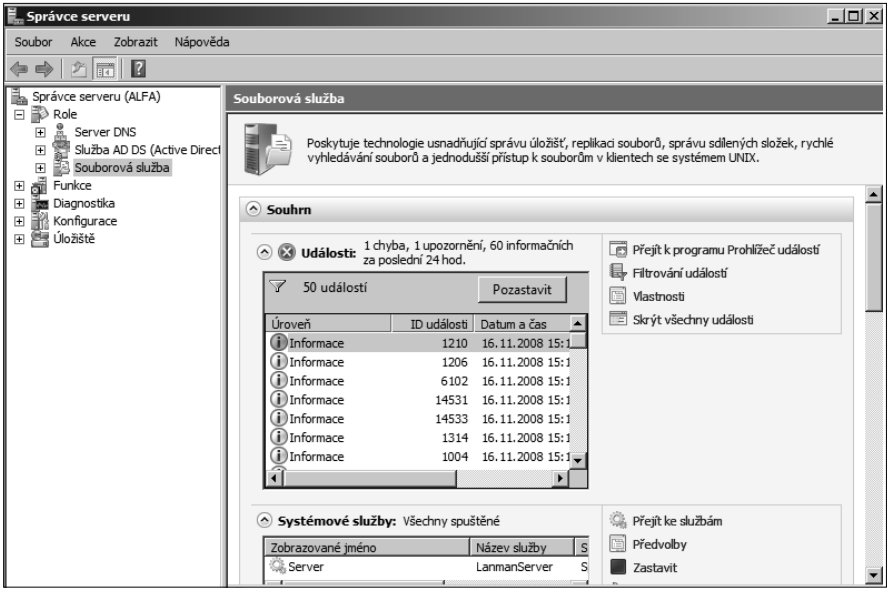
Proces přidání a odebrání služeb rolí je téměř stejný jako přidání a odebrání rolí a skládá se z mnoha stejných kroků. Nástroj příkazového řádku k přidání a odebrání služeb rolí je stejný jako v případě rolí: ServerManagerCmd.exe.

Přidání služeb rolí

Přidání služby role vyžaduje, aby byla role pro danou službu nainstalována. Nelze přidat službu role Services For Network File System, aniž by byla nainstalována role Souborová služba (File Services). (Samozřejmě můžete přidat službu role Network File System v rámci procesu přidání role Souborová služba (File Services). K přidání služby role můžete buď použít příkazový řádek, nebo grafickou konzolu Správce serveru (Server Manager). Chcete-li přidat službu role Services For Network File System k roli Souborová služba (File Services), postupujte podle následujících kroků:

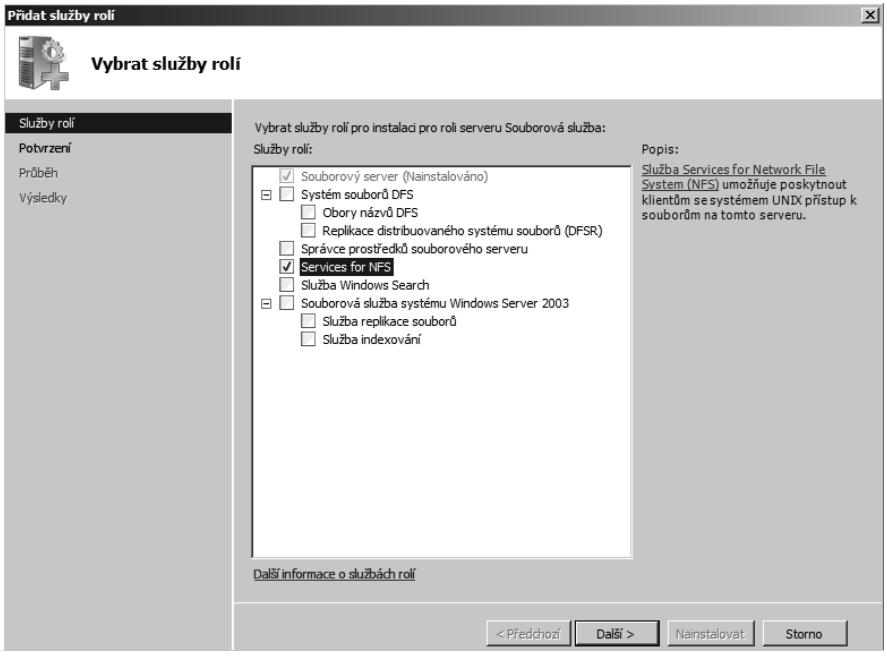
1. Otevřete konzolu Správce serveru (Server Manager), pokud není již otevřena.

2. V levém podokně konzoly Správce serveru (Server Manager) vyberte roli Souborová služba (File Services), viz obrázek 8.12.



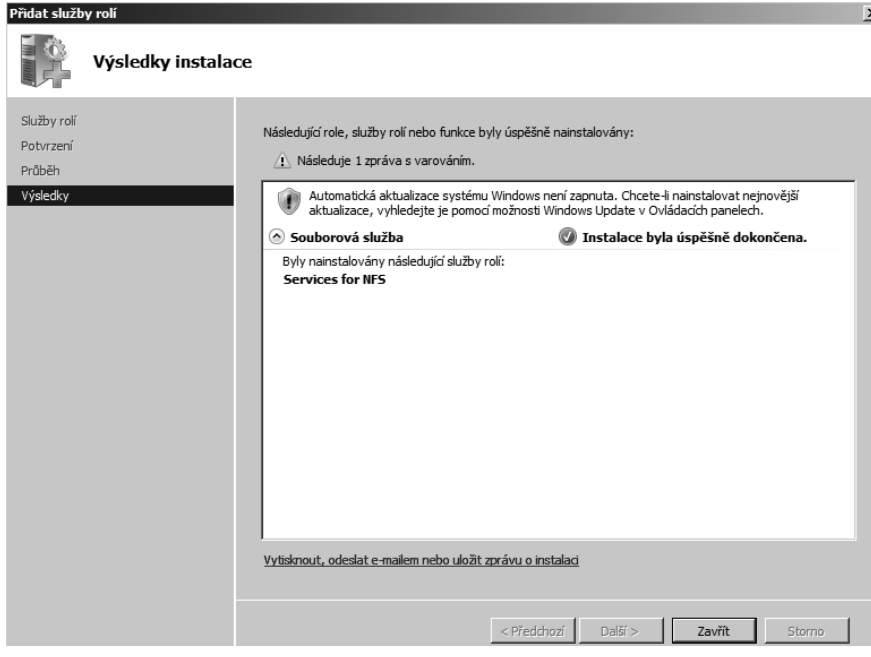
Obrázek 8.12: Konzola Správce serveru (Server Manager) znázorňující roli Souborová služba (File Services)

3. Výběrem příkazu Přidat služby rolí (Add Role Services) v nabídce Akce (Action) otevřete stránku Vybrat služby rolí (Select Role Services), znázorněnou na obrázku 8.13.



Obrázek 8.13: Stránka Vybrat služby rolí (Select Role Services) průvodce Přidat služby rolí (Add Role Services Wizard)

4. Klepnutím na tlačítko Další (Next) otevřete stránku Potvrdit vybrané možnosti instalace (Confirm Installation Selections).
5. Klepnutím na tlačítko Nainstalovat (Install) zahajte instalaci.
6. Po dokončení instalace se otevře stránka Výsledky instalace (Installation Results), znázorněná na obrázku 8.14. Pokud není vyžadováno žádné restartování systému, klepnutím na tlačítko Zavřít (Close) dokončete instalaci.



Obrázek 8.14: Stránka Výsledky instalace (Installation Results) průvodce Přidat služby rolí (Add Role Services Wizard)

Chcete-li provést stejnou instalaci služby role Services for NFS (Services For Network File System) pomocí příkazového řádku, použijte následující příkaz:

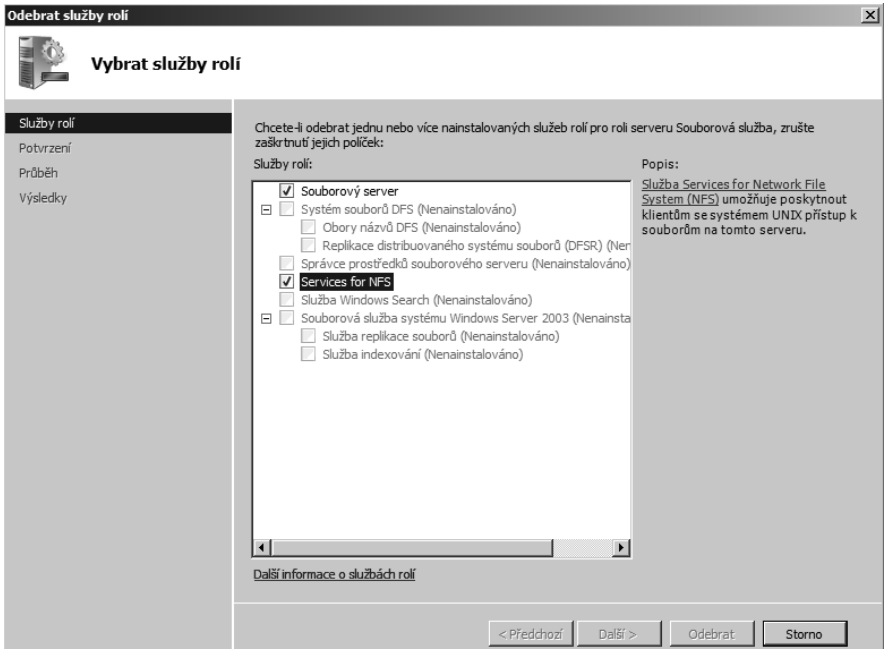
```
Servermanagercmd -install FS-NFS-Services
```

Odebrání služeb rolí

Odebrání služby role neznamená nutně odebrání i samotné role. Službu role Services for NFS (Services For Network File System) můžete odebrat, aniž byste ovlivnili jiné služby role Souborová služba (File Services).

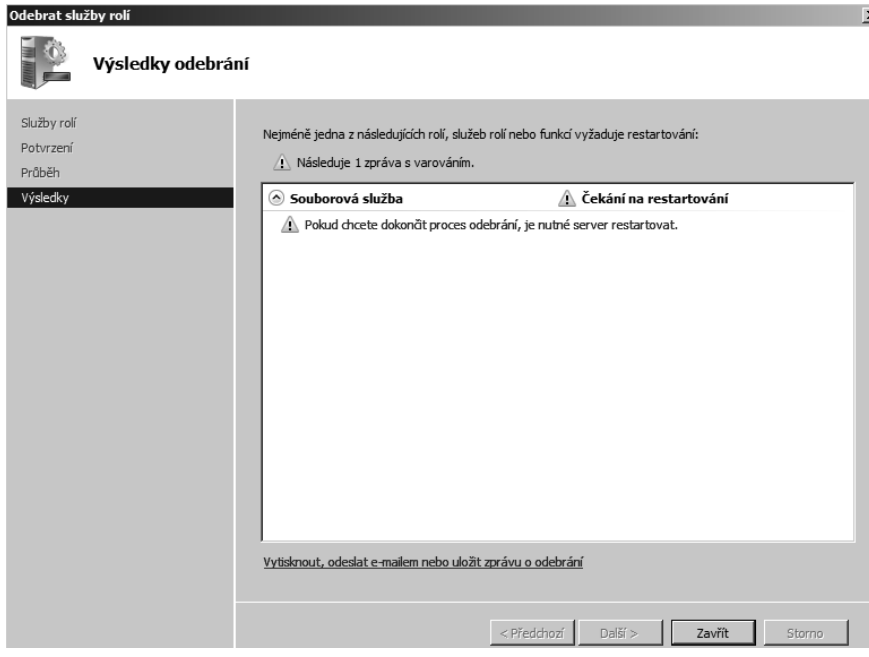
K odebrání služeb rolí můžete použít buď příkazový řádek, nebo grafickou konzolu Správce serveru (Server Manager). Podobně jako v případě odebrání rolí není snadné pochopit, proč by někdo chtěl k odebrání služby role použít příkazový řádek, ovšem neexistuje žádný konkrétní důvod, proč by ne. K odebrání služby Services for NFS (Services For Network File System) role Souborová služba (File Services) postupujte podle následujících kroků:

1. Otevřete konzolu Správce serveru (Server Manager), pokud není již otevřena.
2. V levém podokně konzoly Správce serveru (Server Manager) vyberte roli Souborová služba (File Services).
3. Výběrem příkazu Odebrat služby rolí (Remove Role Service) v nabídce Akce (Action) otevřete stránku Odebrat služby rolí (Select Role Services) průvodce Odebrat služby rolí (Remove Role Services Wizard), viz obrázek 8.15.



Obrázek 8.15: Stránka Vybrat služby rolí (Select Role Services) průvodce Odebrat služby rolí (Remove Role Services Wizard)

4. Zrušte zaškrtnutí u služby role Services for NFS (Services For Network File System) a klepnutím na tlačítko Další (Next) otevřete stránku Potvrdit vybrané možnosti odebrání (Confirm Removal Selections).
5. Klepnutím na tlačítko Odebrat (Remove) zahajte proces odebrání. Po jeho dokončení se zobrazí stránka Výsledky odebrání (Removal Results), znázorněná na obrázku 8.16.
6. Klepnutím na tlačítko Zavřít (Close) ukončete průvodce. Klepnutím na tlačítko Ano (Yes) restartujte server, jste-li k tomu vyzváni.
7. Pokud odebrání služeb rolí vyžaduje restartování serveru, nezapomeňte se znovu přihlásit pomocí stejného účtu, který jste použili k odebrání služby role. Odebrání nemůže být dokončeno, dokud se opět nepřihlásíte pomocí téhož účtu. Otevře se Průvodce obnovením konfigurace (Resume Configuration Wizard) a dokončí odebrání vámi vybrané služby role. Po dokončení odebrání klepněte na tlačítko Zavřít (Close).



Obrázek 8.16: Stránka Výsledky odebrání (Removal Results) průvodce Odebrat služby rolí (Remove Role Services Wizard)

K témuž odebrání služby role Services for NFS (Services For Network File System) pomocí příkazového řádku použijte následující příkaz:

```
Servermanagercmd -remove FS-NFS-Services -restart
```

Přidání a odebrání funkcí

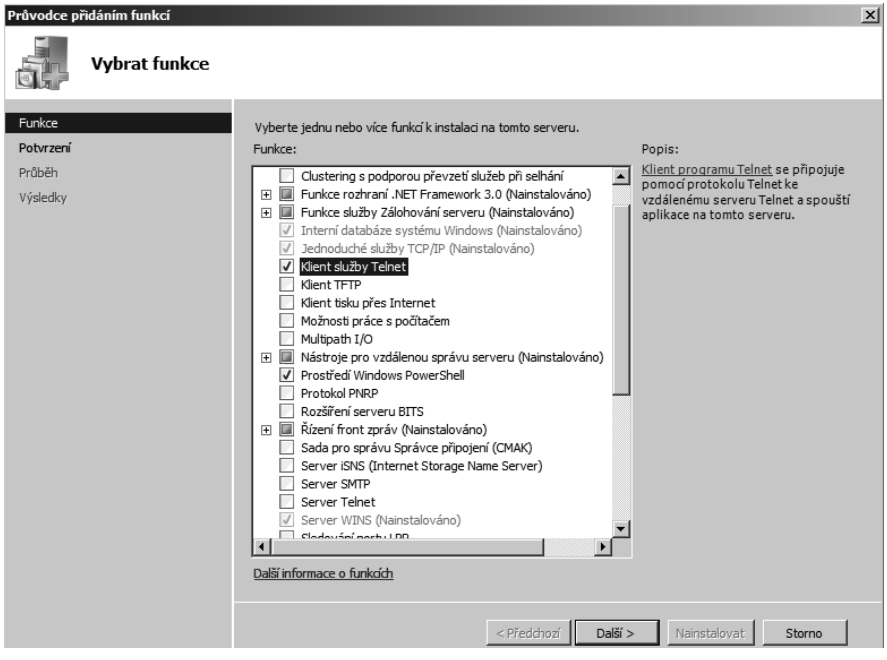
Funkce můžete přidat a odebrat pomocí stejných dvou nástrojů, které používáte i v případě rolí a služeb rolí. Rozdíl spočívá v tom, že funkce jsou obecně nezávislé na konkrétních rolích nainstalovaných na serveru. Jednou z prvních věcí, kterou provedeme s každým serverem, je instalace některých základních funkcí, které pokládáme za užitečné – nebo, v případě prostředí PowerShell, za nezbytné – na každém serveru, s nímž budeme pracovat. Základními funkcemi jsou Prostředí Windows PowerShell (PowerShell), Subsystém pro unixové aplikace (Subsystem for UNIX Applications (SUA)) a Klient služby Telnet (Telnet Client).

Přidání funkcí

Přidání určité funkce na systém Windows Server 2008 obvykle nevyžaduje jiné funkce nebo role, třebaže existují některé výjimky. Mezi ně patří funkce Message Queuing, která obsahuje několik pomocných funkcí, závislých na hlavní funkci Řízení front zpráv (Message Queuing), a Funkce rozhraní .NET Framework 3.0 (.NET Framework 3.0 Features), která rovněž obsahuje několik pomocných funkcí.

Chcete-li nainstalovat tři základní funkce, které máme na každém serveru, postupujte podle následujících kroků:

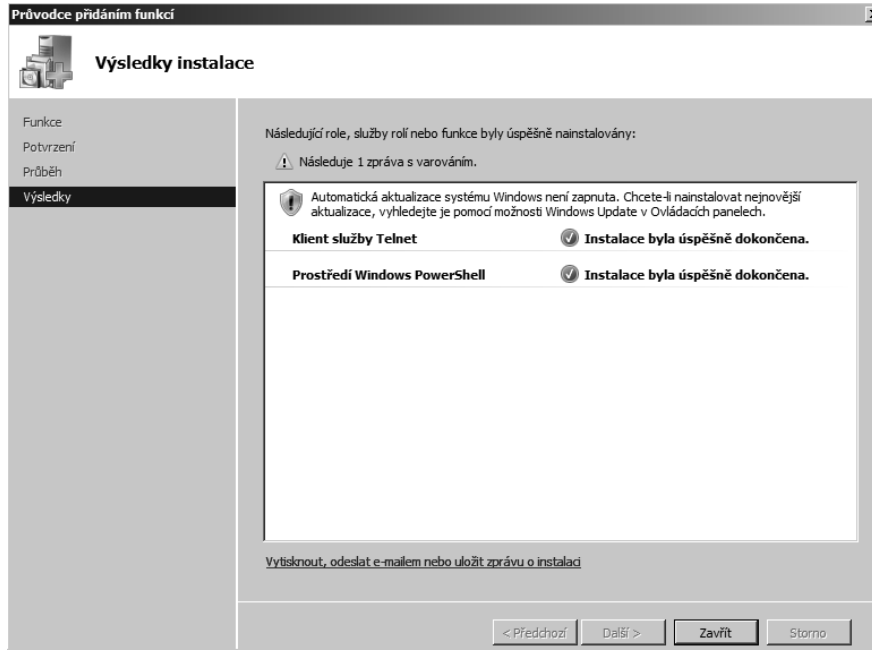
1. Otevřete konzolu Správce serveru (Server Manager), pokud není již otevřena.
2. V levém podokně konzoly Správce Serveru (Server Manager) zvolte příkaz Funkce (Features).
3. Výběrem příkazu Přidat funkce (Add Features) v nabídce Akce (Action) otevřete stránku Vybrat funkce (Select Features) Průvodce přidáním funkcí (Add Features Wizard), viz obrázek 8.17.



Obrázek 8.17: Stránka Vybrat funkce (Select Features) Průvodce přidáním funkcí (Add Features Wizard)

4. Vyberte funkce, které chcete nainstalovat, a klepnutím na tlačítko Další (Next) zahajte proces instalace.
5. Po dokončení procesu se zobrazí stránka Výsledky instalace (Installation Results) (viz obrázek 8.18). Pokud tato stránka obsahuje informaci o tom, že jedna nebo více funkcí vyžaduje restartování serveru, budete muset před pokračováním server restartovat.
6. Klepnutím na tlačítko Zavřít (Close) ukončete průvodce. Klepnutím na tlačítko Ano (Yes) restartujte server, jste-li k tomu vyzváni.
7. Pokud instalace vyžaduje restartování serveru, nezapomeňte se znovu přihlásit pomocí stejného účtu, který jste použili k odebrání služby role. Instalace nebude kompletní, dokud se opět nepřihlásíte pomocí téhož účtu. Otevře se Průvodce obnovením kon-

figurace (Resume Configuration Wizard) a dokončí instalaci vámi vybraných funkcí. Po dokončení instalace klepněte na tlačítko Zavřít (Close).



Obrázek 8.18: Stránka Výsledky instalace (Installation Results) Průvodce přidáním funkcí (Add Features Wizard)

Chcete-li nainstalovat tytéž tři funkce pomocí příkazového řádku, použijte následující příkaz:

```
servermanagercmd -install Telnet-Client PowerShell Subsystem-UNIX-Apps
```

Naše zkušenosti svědčí o tom, že tyto tři funkce lze nainstalovat společně, aniž byste museli restartovat server. Předchozí příkaz příkazového řádku jsme přidali do naší konfigurace standardního sestavení, abychom měli jistotu, že nástroje, které potřebujeme a s nimiž počítáme, budou dostupné na všech serverech.

Odebrání funkcí

Odebrání funkce ze systému Windows Server 2008 obvykle neovlivní jiné funkce nebo role, třebaže existují některé výjimky, například funkce Řízení front zpráv (Message Queuing), která obsahuje několik pomocných funkcí, které jsou závislé na hlavní funkci Řízení front zpráv (Message Queuing), a Funkce prostředí .NET Framework 3.0 (.NET Framework 3.0 Features), která rovněž obsahuje několik pomocných funkcí.

Chcete-li odebrat funkci Klient služby Telnet (Telnet Client), postupujte podle následujících kroků:

1. Otevřete konzolu Správce serveru (Server Manager), pokud není již otevřena.

2. V levé části konzoly Správce serveru (Server Manager) zvolte příkaz Funkce (Features) a poté označte funkci, kterou chcete odebrat.
3. Volbou příkazu Odebrat funkce (Remove Features) v nabídce Akce (Action) otevřete stránku Vybrat funkce (Select Features) Průvodce odebráním funkcí (Remove Features Wizard).
4. Zrušte zaškrtnutí políčka u funkce, kterou chcete odebrat, a klepnutím na tlačítko Další (Next) zahajte proces odebrání.
5. Po dokončení procesu se zobrazí stránka Výsledky odstranění (Removal Results). Pokud tato stránka obsahuje informaci o tom, že je třeba provést restartování serveru, budete muset před pokračováním server restartovat.
6. Klepnutím na tlačítko Zavřít (Close) ukončete průvodce. Klepnutím na tlačítko Ano (Yes) restartujte server, jste-li k tomu vyzváni.
7. Pokud odebrání vyžaduje restartování serveru, nezapomeňte se znovu přihlásit pomocí stejného účtu, který jste použili k odebrání funkce. Odebrání nemůže být dokončeno, dokud se opět nepřihlásíte pomocí téhož účtu. Otevře se Průvodce obnovením konfigurace (Resume Configuration Wizard) a dokončí odebrání vámi vybraných funkcí. Jakmile průvodce dokončí svoji práci, klepněte na tlačítko Zavřít (Close).

Chcete-li odebrat funkci Klient služby Telnet (Telnet Client) pomocí příkazového řádku, použijte následující příkaz:

```
servermanagercmd -remove Telnet-Client
```


Shrnutí

V této kapitole jsme si pověděli o základních krocích pro přidání a odebrání rolí, služeb rolí a funkcí na systém Windows Server 2008. V dalších částech knihy budeme tyto základní kroky používat k instalaci a konfiguraci funkcí, které budeme v systému Windows Server 2008 potřebovat. Výjimkou z tohoto procesu je nová možnost instalace jádra serveru systému Windows Server 2008. Instalace jádra serveru využívá jiné nástroje a obsahuje omezenější podmnožinu dostupných rolí a funkcí. V další kapitole se zmíníme o základních krocích při instalaci a konfiguraci jádra serveru a pro zjednodušení tohoto procesu si rovněž vytvoříme několik skriptů.

KAPITOLA 9

Instalace a konfigurace jádra serveru

Obvyklým způsobem existence operačního systému (nebo aplikace) je vyvíjet se a přidávat funkce, někdy i nad rámec toho, co kdokoliv z nás chce nebo potřebuje. Systém Windows Server 2008 převrací tento trend zcela novou možností instalace – instalace jádra. Při instalaci systému Windows Server 2008 – bez ohledu na to, jakou edici instalujete – máte možnost volby úplné instalace, se všemi funkcemi, nebo pouze části – můžete zvolit instalaci jádra.

Instalace jádra je pouze základem – s trochou grafického rozhraní, nebo dokonce žádným grafickým rozhraním. Poskytovatel přihlášení vypadá stejně, avšak po přihlášení je jediné okno příkazového prostředí znázorněné na obrázku 9.1 vším, co vidíte.

Poznámka: Kvůli lepší čitelnosti snímků obrazovky jsme ve zbývající části knihy změnili výchozí barvu schématu oken příkazového řádku na tmavě modrý text na bílém pozadí.

Obrázek 9.1: Plocha jádra systému Windows Server 2008

Výhody instalace jádra serveru

Všechny edice systému Windows Server 2008 podporují instalaci jádra serveru, kromě edice Compute Cluster Edition. Instalace jádra serveru vám však nijak neušetří náklady na licenci – jedná se o stejnou licenci a média jako v případě úplné instalace systému Windows Server 2008. Při instalaci jednoduše vyberete, kterou edici chcete nainstalovat. Pokud tedy nešetříte penězi, nemáte speciální médium a máte sníženou funkčnost, proč byste vůbec někdy měli volit možnost instalace jádra před úplným produktem? Důvod je opravdu prostý: zabezpečení a prostředky. Podívejme se na tyto dva aspekty poněkud zevrubněji, než se pustíme do výkladu o instalaci a konfiguraci jádra serveru.

Zabezpečení

Kdykoliv jste dříve instalovali systém Windows Server, automaticky se nainstaloval téměř se všemi funkcemi, které byly k dispozici, a zapnul všechny služby, o kterých se domníval, že byste je mohli potřebovat. Cílem bylo instalaci maximálně zjednodušit, což v dané době vypadalo jako dobrý nápad. Bohužel svět již není pro počítače přátelským místem a tento přístup už není bezpečný ani moudrý. Čím více služeb existuje a čím více služeb je zapnuto, tím více možností útoků skýtá pro zlé hochy. Kvůli zvýšení zabezpečení je zkrátka rozumné omezit možná místa útoku. V případě jádra serveru společnost Microsoft zcela odstranila veškerý spravovaný kód a celé rozhraní .NET Framework. Díky tomu se značně snižují možná místa útoku. Samozřejmě to přináší i určitá omezení v tom, co s instalací jádra serveru můžete a nemůžete provádět. A rovněž to znamená, že není k dispozici ani prostředí PowerShell, což je podle našeho názoru bezesporu největším omezením jádra serveru – ovšem omezení, které bude – doufáme – odstraněno v dalších verzích systému Windows Server.

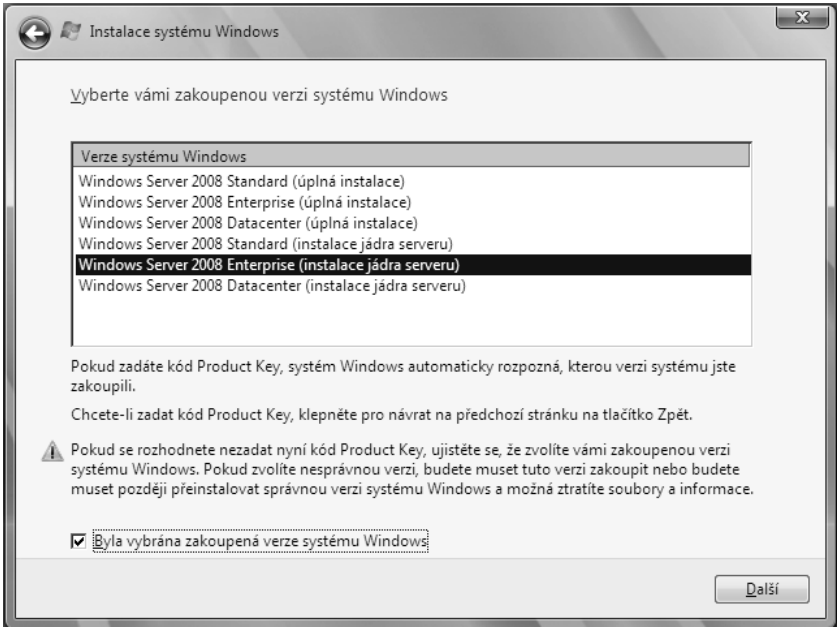
Výchozí instalace jádra serveru obsahuje méně než 40 spuštěných služeb. Typická úplná instalace systému Windows Server 2008 s jednou či dvěma přidanými rolemi obsahuje asi 60 až 70 i více spuštěných služeb. Nejen že nižší počet služeb snižuje možná místa útoku, která je třeba chránit, ale rovněž snižuje počet oprav, které budou možná potřebné po dobu životnosti serveru, což usnadňuje jeho údržbu.

Prostředky

Druhou hlavní výhodou jádra serveru je snížení prostředků potřebných pro samotný operační systém. Zatímco oficiální požadavky na instalaci systému Windows Server 2008 jsou stejné pro instalaci jádra jako pro úplnou instalaci, skutečná čísla jsou podle našich zkušeností o poznání menší – výjimkou je požadované místo na disku (pouze 2 až 3 GB místa na pevném disku pro spuštění instalace jádra). Přičteme-li k tomu omezenou podmnožinu úloh, které můžete provádět, myslíme si, že jádro serveru je ideální pro spouštění těch úloh infrastruktury, které spouští každý a které v průběhu času nevyžadují přílišnou interakci. Tedy úlohy jako DHCP, DNS a stále častěji i virtualizace. Kdybychom tak ještě měli k dispozici i prostředí PowerShell...

Instalace jádra serveru

Instalace jádra systému Windows Server 2008 je naprosto stejná jako instalace úplné grafické verze systému Windows Server 2008. Instalační modul je stejný a jediným rozdílem při instalaci je, že musíte zvolit, kterou verzi sytému Windows Server 2008 chcete nainstalovat, viz obrázek 9.2.



Obrázek 9.2: V počátku instalace provedete nevratnou volbu mezi serverovou verzí a instalací jádra

Po dokončení instalace se zobrazí počáteční přihlašovací obrazovka. Přihlaste se jako správce, bez hesla a ihned budete vyzváni ke změně hesla a poté přihlášeni k pracovní ploše, jak můžete vidět výše na obrázku 9.1. Veškerá počáteční konfigurace probíhá na příkazovém řádku, ačkoliv po nakonfigurování základních parametrů budete moci použít známé prostředí konzol pro vzdálenou správu.

K automatické počáteční instalaci a konfiguraci vaší instalace jádra serveru můžete použít soubor unattend.xml. Více informací o nastavení a syntaxi souboru unattend.xml najdete na adrese *http://go.microsoft.com/fwlink/?LinkId=81030*.

Konfigurace

Všechny konfigurační úlohy pro jádro serveru můžete provést na příkazovém řádku a všechny počáteční úlohy je třeba provést buď na příkazovém řádku, nebo jako součást instalačního procesu pomocí skriptu unattend.xml. Po provedení těchto úloh počáteční konfigurace můžete pro správu dalších nastavení použít klasické konzoly pro správu systému Windows. Bohužel pro dané úlohy neexistuje jediný příkaz pro příkazový řádek, nýbrž kolekce starých, oblíbených příkazů – každý s jiným chováním a syntaxí.

Počáteční konfigurace

Počáteční kroky, potřebné k instalaci jádra serveru, budou zčásti záviset na vámi zamýšleném použití instalace, nicméně si myslíme, že následující kroky jsou zřejmé:

- Nastavení pevné adresy IP.
- Změna názvu serveru takovým způsobem, aby odpovídal vašim vnitřním standardům.
- Připojení serveru k doméně.
- Změna výchozího rozlišení konzoly.
- Povolení výjimky v bráně Windows Firewall pro vzdálenou správu.
- Povolení vzdálené plochy.
- Aktivace serveru.

Uvedené kroky si společně projdeme a k dispozici vám necháme několik základních skriptů, které můžete upravit a zautomatizovat tak tyto úlohy pro vaše prostředí. Tabulka 9.1 obsahuje nastavení, která budeme používat v tomto scénáři instalace.

Tabulka 9.1: Nastavení počáteční konfigurace jádra serveru (příklad)

Nastavení	Hodnota
Adresa IP	192.168.51.4
Brána	192.168.51.1
Server DNS	192.168.51.2
Název serveru	Hp350-core-04
Doména, ke které se chcete připojit	example.local
Výchozí rozlišení plochy	1024x768
Vzdálená správa	Povolit pro profil domény
Aktivace systému Windows	Aktivovat

Nastavení adresy IP

K nastavení adresy IP serveru je třeba použít nástroj příkazového řádku `netsh`. Pro konfiguraci protokolu TCP/IP postupujte podle následujících kroků:

1. Z okna příkazového řádku použijte příkaz `netsh` k získání „názvu" (indexové číslo) síťové karty.

   ```
   netsh interface ipv4 show interfaces
   ```

2. Výsledek bude vypadat podobně jako v níže uvedeném výpisu:

   ```
   C:\Users\administrator>netsh interface ipv4 show interfaces
   Idx Met MTU Stav Název
   --- --- ----- ----------- -------------------
   2 10 1500 connected Připojení k místní síti
   1 50 4294967295 connected Loopback Pseudo-Interface 1
   ```

   V budoucích příkazech nástroje `netsh` se jako názvová hodnota vaší skutečné síťové karty použije hodnota Idx (v tomto případě 2).

3. Spusťte následující příkaz `netsh` s použitím hodnoty Idx z kroku 2:

   ```
   netsh interface ipv4 set address name="<Idx>" source=static
      address=<IP_adresa> mask=<maska_site>
      gateway=<IP_adresa_vychozi_brany>
   ```

Poznámka: Výše uvedené řádky a níže uvedené příklady příkazu `netsh` jsou ve skutečnosti jedním dlouhým příkazovým řádkem, ovšem museli jsme je rozdělit (a následující řádky odsadit) kvůli omezení tiskové stránky. A problémem není jen příkaz `netsh` – většina příkazů, které budete muset v případě jádra serveru použít, je dlouhých a budou v této kapitole uměle rozděleny.

4. Dále zadejte server DNS pro adaptér, opět pomocí příkazu `netsh`.

   ```
   netsh interface ipv4 add dnsserver name="<Idx>"
      address=<IP_adresa_serveru_DNS> index=1
   ```

5. V případě náhradních serverů DNS zopakujte příkaz v kroku 4, vždy se zvýšením hodnoty indexu o jedničku.

Přejmenování serveru a připojení k doméně

Dalším krokem počáteční konfigurace je přiřazení názvu serveru a připojení serveru k doméně. Během počáteční instalace systému Windows Server 2008 je serveru přiřazen automaticky vygenerovaný název a server je umístěn do pracovní skupiny WORKGROUP. Abyste sladili název počítače se zásadami pro pojmenování ve vašem podniku a připojili server ke správné doméně a organizační jednotce, budete chtít tyto údaje změnit. V našem případě se zásady pro pojmenování skládají ze tří částí: z modelu serveru, funkční role a čísla vyjadřujícího jeho adresu IP. Proto je počítač s jádrem serveru, který v této kapitole vytváříme, pojmenován jako hp350-core-04: jedná se o server společnosti Hewlett Packard, model ML 350 G5, je na něm jádro serveru a poslední oktet jeho IP adresy je číslo 4. Vaše zásady pro pojmenování serveru budou nepochybně jiné, nicméně je důležité zachovat jednotnost. Naší doménou pro tuto knihu je doména example.local.

Chcete-li změnit název serveru a připojit jej k doméně example.local, postupujte podle následujících kroků:

1. Na příkazovém řádku použijte příkaz `netdom` pro změnu názvu:

   ```
   netdom renamecomputer %COMPUTERNAME% /newname:<novy_nazev>
   ```

2. Po změně názvu musíte server restartovat:

   ```
   shutdown /t 0 /r
   ```

3. Po restartování serveru se přihlaste pomocí účtu správce.

4. Opětovným použitím příkazu `netdom` připojte počítač k doméně:

   ```
   netdom join %COMPUTERNAME% /DOMAIN:<nazev_domeny>
      /userd:<ucet_spravce_domeny> /password:*
   ```

5. Budete vyzváni k zadání vámi použitého hesla účtu správce domény. Zadejte heslo. Pokud bylo připojení k doméně úspěšné, opět bude třeba restartovat server:

   ```
   shutdown /t 0 /r
   ```

6. Po restartování serveru se opět přihlaste pomocí účtu správce domény. (Budete muset klepnout na tlačítko Přepnout uživatele (Change User), neboť server standardně použije místní účet správce.)

Pohled zevnitř: Skriptování počáteční konfigurace

Pokud nastavujete více než jeden či dva počítače s jádrem serveru, rychle vás tohle interaktivní zadávání příkazů na příkazovém řádku unaví. Mluvíme z vlastní zkušenosti. Máte možnost buď použít soubor unattend.xml k nastavení možností během instalace, nebo použít jednoduché skripty k automatizaci procesu. Oba způsoby fungují a oba mají své příznivce, nicméně my se kloníme spíše k použití skriptů. Následující tři skripty si můžete pozměnit pro vaše prostředí (rovněž si je můžete stáhnout z adresy *http://knihy.cpress.cz/K1608*) a zautomatizovat počáteční kroky nastavení protokolu TCP/IP, názvu serveru a připojení k doméně.

První skript nastaví adresu IP, nastaví server DNS a změní název serveru.

```
echo off
REM nazev souboru: initsetup1.cmd
REM
REM pocatecni nastaveni instalace jadra serveru Windows Server 2008.
REM soubor prikazu 1. ze 3
REM
REM Vytvoreno: 4. zari, 2007
REM Historie zmen: 5/9/07 - pouziti promennych (cpr)
REM
REM Copyright 2007 Charlie Russel a Sharon Crawford. Vsechna prava vyhrazena.
REM Tento skript muzete volne pouzit ve vlastnim prostredi
REM a upravovat jej tak, aby splnoval vase potreby. Ale nesmite jej znovu
REM publikovat bez predchoziho svoleni.

REM Nejdrive nastavte pevnou adresu IP. Musite znat indexove cislo
REM rozhrani, ktere nastavujete, ale v pripade vychozi instalace
REM jadra serveru
REM s pouze jednou sitovou kartou by mel mit index hodnotu 2.
REM Ke zjisteni indexu muzete spustit prikaz:
REM      netsh interface ipv4 show interfaces
```

```
SETLOCAL
REM Zmente nize uvedene hodnoty podle vasich potreb
SET IPADD=192.168.51.4
SET IPMASK=255.255.255.0
SET IPGW=192.168.51.1
SET DNS1=192.168.51.2
SET NEWNAME=hp350-core-04

netsh interface ipv4 set address name="2" source=static
   address=%IPADD% mask=%IPMASK% gateway=%IPGW%

REM Dale nastavte server DNS tak, aby ukazoval na server
REM DNS domeny example.local.
REM v tomto pripade na server 192.168.51.2
netsh interface ipv4 add dnsserver name="2" address=%DNS1% index=1

REM Nyni poterbujeme zmenit nazev pocitace.
REM Pote je treba server restartovat
REM a my muzeme pokracovat dalsi davkou prikazu.
REM Pouzitim prikazu s parametrem /force zabranime zobrazeni vyzev.
REM
netdom renamecomputer %COMPUTERNAME% /newname:%NEWNAME% /force

@echo Pokud se zda byt vse v poradku, je cas na restartovani serveru
pause
REM Nyni vypneme a restartujeme server. Neni nac cekat.
REM
shutdown /t 0 /r
```

Druhý skript, který použijeme, provede skutečné připojení serveru k doméně.

```
echo off
REM initsetup2.cmd
REM
REM pocatecni nastaveni instalace jadra serveru Windows Server 2008.
REM soubor prikazu 2. ze 3
REM
REM Vytvoreno: 4. zari, 2007
REM Historie zmen:
REM
REM Copyright 2007 Charlie Russel a Sharon Crawford.
REM Vsechna prava vyhrazena.
REM   Tento skript muzete volne pouzit ve vlastnim prostredi
REM a upravovat jej tak, aby splnoval vase potreby.
REM Ale nesmite jej znovu publikovat bez predchoziho svoleni.

SETLOCAL
SET DOMAIN=example.local
SET DOMADMIN=Administrator

REM Pripojeni k domene pomoci prikazu netdom join.
REM Zobrazi se vyzva k zadani vyse zadaneho hesla uctu spravce domeny,

netdom join %COMPUTERNAME% /DOMAIN:%DOMAIN% /userd:%DOMADMIN% /passwordd:*

REM Nyni vypneme a restartujeme server. Neni nac cekat a je to vse,
REM co muzeme v tuto chvili udelat

shutdown /t 0 /r
```

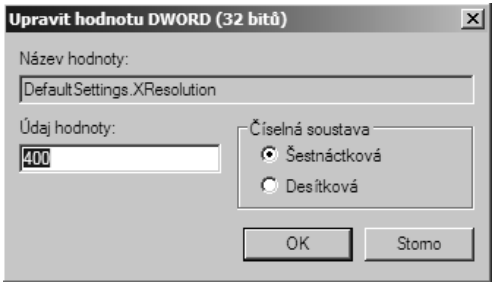
Nakonec použijte třetí skript, který povolí vzdálenou správu a provede aktivaci serveru.

```
echo off
REM initsetup3.cmd
REM
REM pocatecni nastaveni instalace jadra serveru Windows Server 2008.
REM soubor prikazu 3. ze 3
REM
REM Vytvoreno: 4. zari, 2007
REM Historie zmen:


REM
REM Copyright 2007 Charlie Russel a Sharon Crawford. Vsechna prava vyhrazena.
REM   Tento skript muzete volne pouzit ve vlastnim prostredi
REM a upravovat jej tak, aby splnoval vase potreby.
REM Ale nesmite jej znovu publikovat bez predchoziho svoleni.


REM Pouzijte prikaz netsh k povoleni vzdalene spravy
REM prostrednictvim brany firewall pro profil domeny.
REM Tohle je minimum, ktere je treba povolit pro pouziti
REM vzdalenych konzol MMC pro praci z jinych pocitacu v domene.

netsh advfirewall set domainprofile settings remotemanagement enable

REM Povolte skupinu pro vzdalenou spravu
netsh advfirewall firewall set rule group="Vzdálená správa" new
   enable=yes


REM Povolte vzdalenou spravu prostrednictvim brany firewall
REM (funguje take s parametrem group="Vzdálená plocha" misto name=)
netsh advfirewall firewall set rule name="Vzdálená plocha (TCP-In)" new
   enable=yes


REM Povolte Vzdalenou plochu pro spravu a povolte pripojeni
REM klientu nizsi urovne
cscript %windir%\system32\scregedit.wsf /AR 0
cscript %windir%\system32\scregedit.wsf /CS 0


REM Nyni spustte aktivacni skript
REM Zadny vystup znaci, ze vse funguje
Slmgr.vbs -ato
```

Nastavení rozlišení obrazovky

K nastavení rozlišení obrazovky plochy jádra serveru je třeba ručně upravit registr. My vám za tímto účelem nabízíme k dispozici skript, ten však závisí na správné identifikaci konkrétního identifikátoru GUID pro váš grafický adaptér. Ne všechno chceme zautomatizovat. Takže chcete-li změnit rozlišení plochy jádra serveru, postupujte podle následujících kroků:

1. Spusťte program `regedit`.
2. Najděte klíč HKLM\System\CurrentControlSet\Control\Video.
3. Pod klíčem Video je uveden jeden nebo více identifikátorů GUID. Vyberte ten, který odpovídá vaší grafické kartě. Tip: Každá grafická karta obsahuje popis zařízení pod klíčem 0000, což může někdy pomoci.
4. Pod identifikátorem GUID vaší grafické karty vyberte klíč 0000 a přidejte hodnotu DWORD s údajem DefaultSettings.XResolution. Upravte hodnotu na rozlišení osy X, které chcete použít. Pro šířku 1024 pixelů použijte hexadecimální hodnotu 400, viz obrázek 9.3.



Obrázek 9.3: Úprava hodnoty rozlišení obrazovky pro osu X

5. Přidejte hodnotu DWORD s údajem DefaultSettings.YResolution. Pro výšku 768 pixelů použijte hexadecimální hodnotu 300.

Poznámka: V některých případech již budou tyto klíče existovat. V takovém případě můžete jednoduše změnit jejich hodnotu.

6. Ukončete editor registru a odhlaste se pomocí následujícího příkazu:

```
shutdown /l
```

7. Jakmile se opět přihlásíte, nové nastavení zobrazení se uplatní.

Povolení vzdálené správy

Chcete-li povolit přístup k důvěrně známým grafickým nástrojům pro správu, je třeba povolit jejich funkci prostřednictvím brány Windows Firewall. K tomu je třeba další sada příkazů `netsh`. Pro povolení vzdálené správy a Vzdálené plochy (Remote Desktop) postupujte podle následujících kroků:

1. Na příkazovém řádku použijte příkaz `netsh` k povolení vzdálené správy:

```
netsh advfirewall set domainprofile settings remotemanagement enable
```

2. Nyní povolte skupinu pravidel Vzdálená správa brány firewall:

```
netsh advfirewall firewall set rule group="Vzdálená správa"
   new enable=yes
```

3. Život je koneckonců snazší, když se můžete připojit pomocí vzdálené plochy, takže ji taky povolme:

```
netsh advfirewall firewall set rule name="Vzdálená plocha (TCP-In)"
   new enable=yes
```

Nyní byste měli být schopni provádět další správu pomocí důvěrně známých grafických nástrojů z jiného serveru, kromě připojení k počítači s jádrem serveru.

Aktivace serveru

Posledním krokem základní konfigurace počítače s jádrem serveru je jeho aktivace. Ta vyžaduje použití skriptu v jazyce Visual Basic Script, který máte k dispozici. Použijte následující příkaz:

```
Slmgr.vbs -ato
```

Poznámka: Všechny příkazy základního, počátečního nastavení jádra serveru jsou obsaženy ve třech skriptech popsaných v části „Pohled zevnitř" a rovněž jsou dostupné na adrese *http://knihy.cpress.cz/K1608*.

Instalace rolí

Jádro systému Windows Server 2008 nepodporuje všechny dostupné role a funkce plně grafického systému Windows Server, ovšem podporuje nejdůležitější role infrastruktury. Myslíme si, že jedním z nejzajímavějších scénářů pro použití jádra serveru je server vzdálené sítě, nabízející základní funkčnost vzdálené sítě, v níž neexistuje nikdo, kdo by ji spravoval. Kombinací rolí Server DHCP (DHCP Server), Server DNS (DNS Server), Souborová služba (File Services) a Tisková služba (Print Services) s rolí Active Directory Domain Services jen pro čtení máte k dispozici řešení „pobočky v krabici" – stačí přidat zařízení pro vzdálený přístup, například VPN směrovač, a můžete začít podnikat.

Role Souborová služba (File Services) je přidána ve výchozím nastavení jako součást instalace jádra serveru, ovšem pro podporu další funkčnosti můžete přidat další služby rolí.

Příkazem, který se používá k instalaci role v případě jádra serveru, je Ocsetup.exe. Jedná se o stejný příkaz, který se používá k odinstalování role, ovšem s parametrem příkazového řádku */uninstall*. Úplná syntaxe příkazu `Ocsetup` je následující:

```
Ocsetup </?|/h|/help>
Ocsetup <soucast> [/uninstall][/passive][/unattendfile:<soubor>] [/quiet]
   [/log:<soubor>][/norestart][/x:<parametry>]
```

Důležité je zapamatovat si o příkazu `Ocsetup` to, že je docela nemilosrdný. Rozlišuje mezi velkými a malými písmeny a i drobná chybička v případě názvu součásti způsobí selhání příkazu.

Skript pro instalaci rolí by pro naše řešení, s výjimkou role řadiče domény, vypadal následovně:

```
@REM nazev souboru: SetupBranch.cmd
@REM
@REM Instalacni soubor pro instalaci roli pro pobockovy server
@REM
```

```
@REM Vytvotreno: 5. zari, 2007
@REM Historie zmen:
@REM
@REM Copyright 2007 Charlie Russel a Sharon Crawford. Vsechna prava vyhrazena.
@REM   Tento skript muzete volne pouzit ve vlastnim prostredi
@REM a upravovat jej tak, aby splnoval vase potreby.
@REM Ale nesmite jej znovu publikovat bez predchoziho svoleni.

@REM Pouziti prikazu "start /w" s nazvem ocsetup
@REM vynuti vyckani na dokonceni prikazu
@REM ocsetup, nez se prejde k dalsi uloze.

@REM Nainstalujte server DNS a DHCP
@echo Instaluji role DNS a DHCP...
start /w ocsetup DNS-Server-Core-Role
start /w ocsetup DHCPServerCore

@REM Nyni nainstalujeme souborove sluzby roli
@echo Instaluji souborove sluzby roli...
start /w ocsetup FRS-Infrastructure
start /w ocsetup DFSN-Server
start /w ocsetup DFSR-Infrastructure-ServerEdition

@REM u nasledujici dvou radku muzete zrusit komentar,
@REM chcete-li pridat podporu NFS
@REM start /w ocsetup ServerForNFS-Base
@REM start /w ocsetup ClientForNFS-Base

@REM Nainstalujte roli Print Server
@echo Instaluji roli Print Server
start /w ocsetup Printing-ServerCore-Role

@REM Zrusenim komentare nasledujiciho radku pridejte podporu sluzby LPD
@REM start /w ocsetup Printing-LPDPrintService
```

Poznámka: Do výše uvedeného skriptu nelze zahrnout příkaz DCPromo, neboť instalace role Print Server vyžaduje restartování serveru, což uzamkne příkaz DCPromo.

Příkaz DCPromo nelze k vytvoření řadiče domény použít interaktivně – musíte vytvořit soubor unattend.txt a použít tento příkaz v něm. Soubor unattend.txt musí obsahovat alespoň následující příkazy:

```
[DCInstall]
InstallDNS = Yes
ConfirmGC = yes
CriticalReplicationOnly = No
RebootOnCompletion = No
ReplicationSourceDC = hp350-dc-02.example.local
ParentDomainDNSName = example.local
ReplicaOrNewDomain = ReadOnlyReplica
ReplicaDomainDNSName = example.local
SiteName=Default-First-Site-Name
SafeModeAdminPassword = <heslo>
UserDomain = example
UserName = Administrator
Password = <heslo>
```

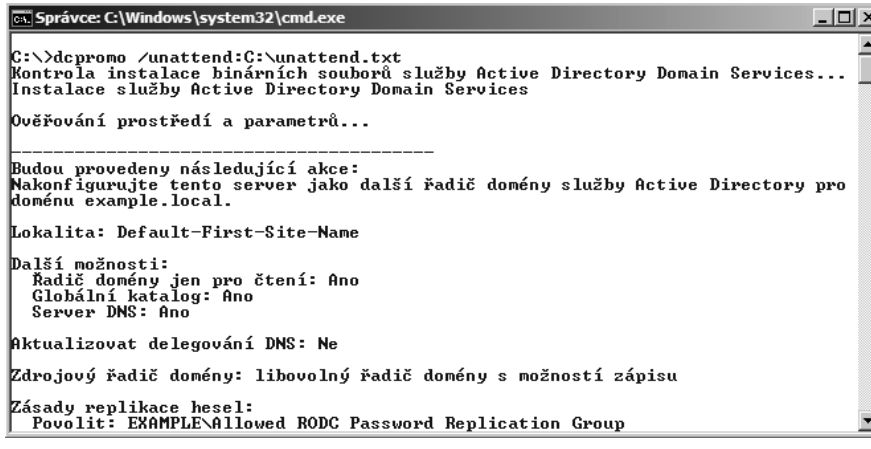
Důležité: Hesla musí být správně vyplněna a z bezpečnostních důvodů budou ze souboru automaticky odstraněna. V případě jádra serveru musíte zadat hodnotu *ReplicationSourceDC*. Parametr *ReplicaOrNewDomain* byste měli nastavit na zde uvedenou hodnotu – *ReadOnlyReplica* – abyste vytvořili řadič domény jen pro čtení.

Chcete-li nainstalovat roli Doménového řadiče v režimu jen pro čtení, postupujte podle následujících kroků:

1. Pomocí programu Notepad nebo vašeho oblíbeného ASCII textového editoru (my používáme GVim, který docela dobře funguje i v případě jádra serveru) vytvořte soubor unattend.txt s nezbytnými nastaveními domény, ke které se budete připojovat. Konkrétní název souboru bezobslužné instalace není důležitý, neboť jej uvedete na příkazovém řádku.
2. Přejděte do adresáře, který obsahuje soubor bezobslužné instalace. Pokud server čeká na restartování, musíte tak učinit ještě před převedením serveru na řadič domény.
3. Spusťte příkaz DCPromo s následující syntaxí:

   ```
   Dcpromo /unattend:<nazev_souboru_bezobsluzne_instalace>
   ```

4. Pokud se v souboru bezobslužné instalace nevyskytnou žádné chyby, příkaz DCPromo se provede a převede server na řadič domény jen pro čtení, viz obrázek 9.4.



Obrázek 9.4: Příkaz DCPromo použijte k vytvoření řadiče domény jen pro čtení s využitím souboru bezobslužné instalace

Výpis seznamu rolí

Příkaz Oclist.exe vypíše úplný seznam dostupných rolí jádra serveru, služeb rolí a funkcí i jejich aktuální stav. Pomocí příkazu `Oclist` získáte přesný seznam funkcí a rolí, které chcete nainstalovat, a to s dodržením velkých a malých písmen ve výpisu.

Správa počítače s jádrem serveru

Správa počítače s jádrem serveru je pro většinu správců systému neobvyklým zážitkem. Žádný z grafických nástrojů, které jste zvyklí používat, není *na serveru* k dispozici.

Ovšem po nakonfigurování počítače s jádrem serveru pro vzdálenou správu, jak je popsáno části „Počáteční konfigurace“ dříve v této kapitole, můžete vytvořit konzoly pro správu, které ukazují na počítač s jádrem serveru a které vám umožní provádět všechny úlohy z využitím grafické konzoly.

Další informace: Další podrobnosti o vytvoření vlastních konzol MMC najdete v kapitole 14, „Správa každodenních operací“.

Existují čtyři základní způsoby správy instalace jádra serveru:

1. Místní použití příkazového řádku.
2. Vzdálené použití Vzdálené plochy (Remote Desktop). Prostředí nástroje Vzdálená plocha (Remote Desktop) bude mít tutéž funkčnost (příkazový řádek) jako při místním přihlášení.
3. Vzdálené použití Windows Remote Shell.
4. Vzdálené použití modulu snap-in konzoly MMC z počítače se systémem Windows Vista nebo Windows Server 2008.

Některé úlohy jsou v případě jádra serveru poněkud rafinované – obvykle je provádíme výlučně z grafického uživatelského rozhraní. Samozřejmou úlohou je změna hesla k vašemu účtu. K tomu použijeme příkaz `net user <uzivatelske_jmeno> *`. Některé úlohy, které mohou představovat problém, a jejich řešení jsou vedeny v tabulce 9.2.

Tabulka 9.2: Řešení běžných úloh v jádru serveru

Úloha	Řešení/Postupy
Povolení automatických aktualizací	Cscript %windir%\system32\scregedit.wsf /AU [hodnota] Možné hodnoty jsou: 1 – zakáže automatické aktualizace 4 – povolí automatické aktualizace /v – zobrazí aktuální nastavení
Povolení Vzdálené plochy (Remote Desktop) pro správce	Cscript %windir%\system32\scregedit.wsf /AR [hodnota] Možné hodnoty jsou: 0 – povolí Vzdálenou plochu (Remote Desktop) 1 – zakáže Vzdálenou plochu (Remote Desktop) /v – zobrazí aktuální nastavení
Povolení klientů Terminal Server z verzí systému Windows předcházejících systému Windows Vista	Cscript %windir%\system32\scregedit.wsf /CS [hodnota] Možné hodnoty jsou: 0 – povolí předchozí verze 1 – zakáže předchozí verze /v – zobrazí aktuální nastavení

Úloha	Řešení/Postupy
Povolení vzdálené správy modulu IPSec Monitor	Cscript %windir%\system32\scregedit.wsf /IM [hodnota] Možné hodnoty jsou: 0 – zakáže vzdálenou správu 1 – povolí vzdálenou správu /v – zobrazí aktuální nastavení
Konfigurace váhy a priority záznamů SRV služby DNS	Cscript %windir%\system32\scregedit.wsf /DP [hodnota] Možné hodnoty priorit záznamů SRV služby DNS: 0-65535. (Doporučení hodnota = 200) /v – zobrazí aktuální nastavení Cscript %windir%\system32\scregedit.wsf /DW [hodnota] Možné hodnoty vah záznamů SRV služby DNS: 0-65535. (Doporučení hodnota = 50) /v – zobrazí aktuální nastavení
Aktualizace uživatelských hesel	Net user <uzivatelske_jmeno> [/domena] *
Instalace souborů .msi	Použijte přepínače /q nebo /qb na příkazovém řádku s úplným názvem souboru .msi. /q značí tichý režim; /qb značí tichý režim se základním uživatelským rozhraním
Změna časového pásma, data nebo času	timedate.cpl
Změna mezinárodních nastavení	intl.cpl
Použití konzoly Správa disků (Disk Management)	Na příkazovém řádku instalace jádra serveru: Net start VDS Poté vzdáleně spusťte nástroj Správa disků (Disk Management).
Získání informace o verzi systému Windows	Příkaz Winver není k dispozici. Místo něj použijte příkaz systeminfo.exe.
Získání nápovědy (obvyklá nápověda systému Windows; soubory podpory nelze v jádru serveru prohlížet)	Cscript %windir%\system32\scregedit.wsf /cli

Použití Windows Remote Shell

Windows Remote Shell můžete použít ke vzdálenému spouštění příkazů na počítači s jádrem serveru. Avšak než budete moci spustit Windows Remote Shell, musíte jej nejprve povolit na cílovém počítači s jádrem serveru. Windows Remote Shell povolíte použitím následujícího příkazu:

```
winrm quickconfig
```

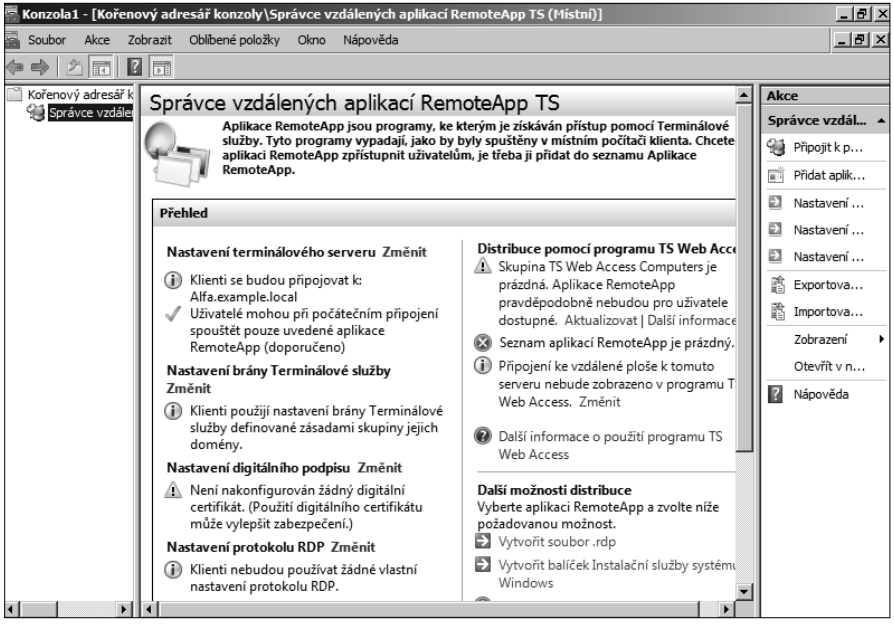
Ke vzdálenému spuštění příkazu použijte příkaz `WinRS` z jiného počítače s využitím následujícího příkazu:

```
winrs -r:<NazevServeru> <rezetec_prikazu_ke_spusteni>
```

Použití vzdálené aplikace RemoteApp TS

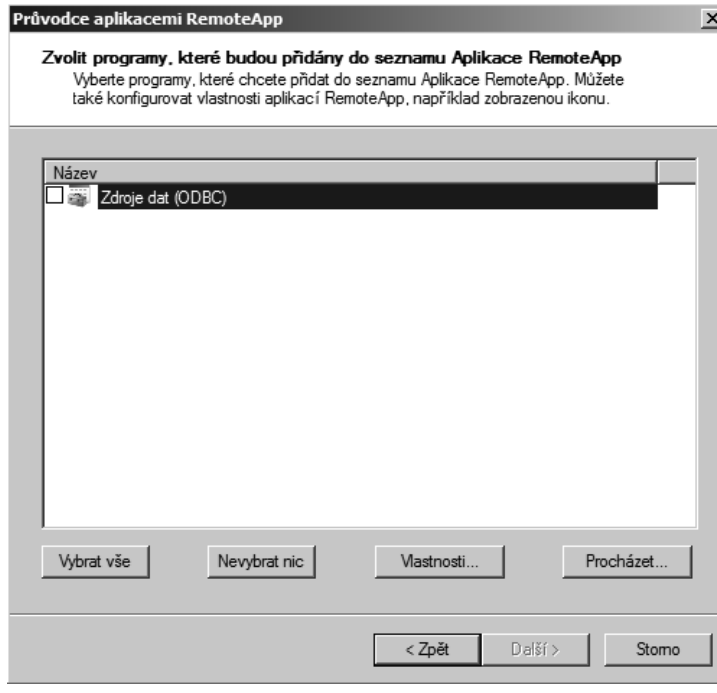
Jedním z hezkých triků je použití nové funkčnosti TS RemoteApp systému Windows Server 2008 k publikování okna příkazového řádku pro počítače s jádrem serveru přímo na naši plochu. Takové řešení je jednodušší a přímočařejší a ukládá obsah obrazovky, což je vždy výhodné. Chcete-li vytvořit balíček protokolu RDP, který můžete umístit na plochu, postupujte podle následujících kroků:

1. Na serveru se systémem Windows Server 2008, který má povolenu roli Terminal Services, otevřete Správce vzdálených aplikací RemoteApp TS (TS RemoteApp Manager), viz obrázek 9.5.



Obrázek 9.5: Pomocí modulu snap-in Správce vzdálených aplikací RemoteApp TS (TS RemoteApp Manager) vytvořte vzdálené okno příkazu cmd.exe

2. Připojte se k počítači s jádrem serveru, pro nějž chcete vytvořit balíček protokolu RDP.
3. Klepnutím na příkaz Přidat aplikace RemoteApp (Add RemoteApp) v podokně akcí otevřete Průvodce aplikacemi RemoteApp (RemoteApp Wizard).
4. Klepnutím na tlačítko Další (Next) otevřete stránku Zvolit programy, které budou přidány do seznamu Aplikace RemoteApp (Choose Programs To Add To The RemoteApp Programs List), znázorněnou na obrázku 9.6.
5. Klepnutím na tlačítko Procházet (Browse) najděte příkaz \\<*NazevServeru*>\c$\windows\system32\cmd.exe. Klepněte na tlačítko Otevřít (Open).
6. Klepněte na tlačítko Další (Next) a poté klepnutím na tlačítko Dokončit (Finish) přidejte vzdálený program a vraťte se do modulu snap-in Správce vzdálených aplikací RemoteApp TS (TS RemoteApp Manager).



Obrázek 9.6: Stránka Zvolit programy, které budou přidány do seznamu Aplikace RemoteApp (Choose Programs To Add To The RemoteApp Programs List) Průvodce aplikacemi RemoteApp (RemoteApp Wizard)

7. V podokně Aplikace RemoteApp (RemoteApp programs) vyberte příkaz cmd.exe a klepněte na příkaz Vytvořit soubor RDP (Create .rdp File) v podokně akcí.
8. Klepněte na tlačítko Další (Next) a zadejte další nastavení balíčku protokolu RDP. Poznamenejte si umístění, kam se balíček uloží.
9. Klepněte dvakrát na tlačítko Další (Next) a poté klepnutím na tlačítko Dokončit (Finish) vytvořte balíček protokolu RDP.
10. Zkopírujte balíček do počítače, v němž jej budete používat.

Nyní můžete otevřít okno příkazového řádku přímo na počítači s jádrem serveru prostým poklepáním na balíčku protokolu RDP, který jste uložili a vytvořili.

Shrnutí

V této kapitole jsme si pověděli o některých základních krocích nastavení a konfigurace nové možnosti instalace jádra serveru se systémem Windows Server 2008. Myslíme si, že se jedná o skvělý nový způsob vyždímání maxima výkonu ze systému Windows Server při zachování velmi vysokých úrovní zabezpečení a jednoduchosti správy. Víme, že to zní skoro jako marketingová fráze, nicméně opravdu si myslíme, že jádro serveru je důležitým krokem vpřed.

Další kapitola je zaměřena na správu a konfiguraci tiskáren pomocí konzoly Správa tisku (Printer Management).

KAPITOLA 10

Správa tiskáren

Zdá se, že než bude chtít téměř každý mít bezpapírovou kancelář, budeme všichni mnohem šedivější (nebo plešatější, případně oboje). Spotřeba papíru v kancelářích dosáhla vrcholu v roce 1999 a od té doby je množství odpadu v kancelářských skartovačkách papíru na stejné úrovni, a někde dokonce začalo i klesat. Ovšem třebaže méně lidí tiskne své e-maily předtím, než si je přečte, papír stále v mnoha obchodních operacích zastává důležitou roli.

Náklady na základní tiskárny dramaticky klesly, ale firmy investují do sofistikovaných vysokorychlostních tiskáren, které umožňují uživatelům realizovat úlohy, které kdysi vyžadovaly zpracování v klasické tiskárně. Avšak pořízení i provoz těchto sofistikovaných tiskáren jsou velmi nákladné. Proto zůstává sdílení tiskáren důležitou funkcí podnikových sítí. Nastavení sdílení tiskáren více uživatelům snižuje náklady a může zvýšit tiskový výstup. Můžete přesměrovat rutinní práci na tiskárny s nízkými náklady na stránku, naplánovat dlouhé tiskové úlohy mimo pracovní dobu a omezit přístup k nejmodernějším tiskárnám.

Plánování nasazení tiskáren

Plánujete-li nasazení tiskáren a tiskových serverů, důležité je zavést konvence pro pojmenování tiskáren a umístění, zvážit, zda upgradovat nebo migrovat existující tiskové servery, a připravit se na chyby tiskového serveru.

Doporučené postupy: Je-li to možné, připojte tiskárny k tiskovému serveru pomocí síťového připojení. Síťové tiskárny jsou rychlejší a vyžadují méně prostředků na tiskovém serveru než místně připojené tiskárny a rovněž můžete tiskárny umístit kamkoliv, kde můžete dovést síťový kabel (nebo bezdrátové připojení).

Zavedení konvencí pro pojmenování tiskáren

Efektivní konvence pro pojmenování tiskáren jsou důležité k tomu, aby uživatelé tiskárny v síti snadno rozpoznali. Při vytvoření konvencí pro pojmenování vezměte v potaz následující skutečnosti:

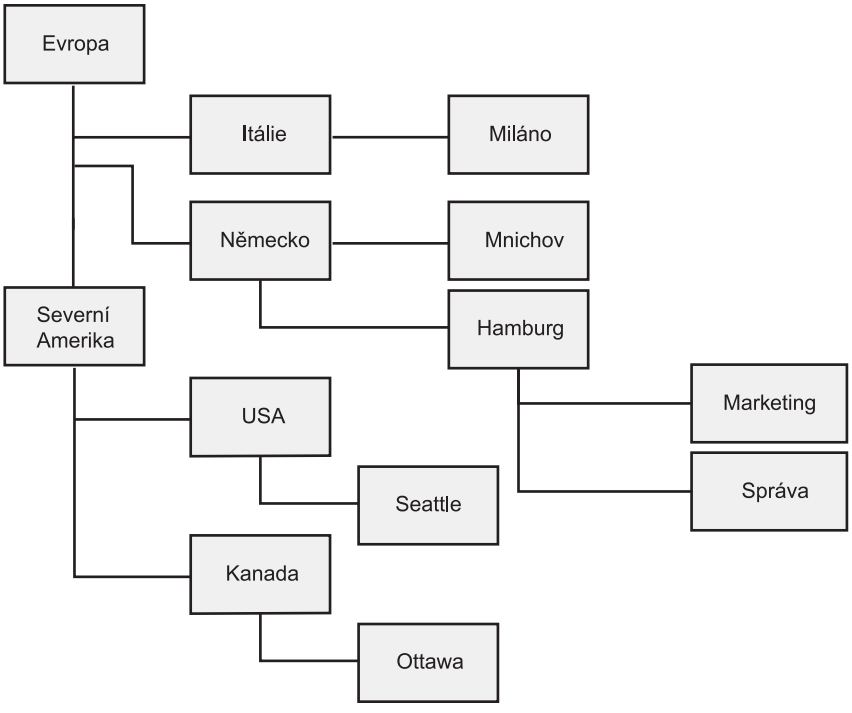
- *Název tiskárny* může být dlouhý maximálně 220 znaků, což je dostatek pro jakékoliv schéma, které vás napadne. Název by měl být samozřejmě co možná nejkratší, ovšem ne na úkor srozumitelnosti.
- *Název sdílené položky* je názvem, který vidí všichni klienti při vyhledání tiskárny, použití průvodce Přidat tiskárnu (Add Printer Wizard) nebo použití příkazu Net Use. Může mít délku až 80 znaků, ale opět by měl být kvůli čitelnosti co nekratší. Některé starší aplikace nemohou tisknout na tiskárnách s plně kvalifikovanými názvy sdílených tiskáren (takový název tvoří společný název počítače a název sdílené tiskárny), které jsou delší než 31 znaků, nebo na tiskových serverech, kde název sdílené výchozí tiskárny přesahuje 31 znaků. Rovněž klienti používající jiné operační systémy mohou mít problémy s názvy delšími než 31 znaků nebo názvy, které obsahují mezery nebo jiné speciální znaky. Nicméně ať už se musíte vypořádat s takovými aplikacemi či nikoliv, kratší název je obecně lepší.
- Před použitím konvencí pro pojmenování je nezbytná shoda týkající se správy.

Vytvoření konvencí pro pojmenování umístění

V malých organizacích je nalezení tiskárny snadné – stačí vstát a rozhlédnout se kolem nebo se zeptat osoby sedící vedle vás. Takhle to však nefunguje ve větších organizacích, kde jsou různé tiskárny, které mohou být různě rozptýleny. Za těchto okolností uživatelé musí mít možnost vyhledávání tiskáren v adresáři služby Active Directory podle požadovaných kritérií, včetně funkcí tiskárny a jejího umístění.

Názvy umístění jsou svým tvarem podobné názvům domén a používají syntaxi *název/název/název*... Začínají nejobecnějším názvem umístění a postupně se více zpřesňují. Například nadnárodní společnost by mohla mít strukturu pojmenování umístění podobnou té na obrázku 10.1. Každá část názvu je tvořena nejvíce 32 znaky a může obsahovat libovolné znaky kromě lomítka (/), které systém Windows používá jako oddělovač.

Podobně jako u volby názvů domén, i vytvoření schématu pojmenování umístění tiskáren je politickou záležitostí, takže získejte potřebný souhlas. Dbejte na to, aby byly konvence pro pojmenování jednoduché a snadno zapamatovatelné pro koncové uživatele – koneckonců oni musí být schopni při pohledu na název umístění odpovědět na letitou otázku: „Kde je můj vytištěný dokument?“ Příkladem názvu umístění je třeba Design/ArtStudio/HPDesignJet5500.



Obrázek 10.1: Vzorová struktura pojmenování umístění

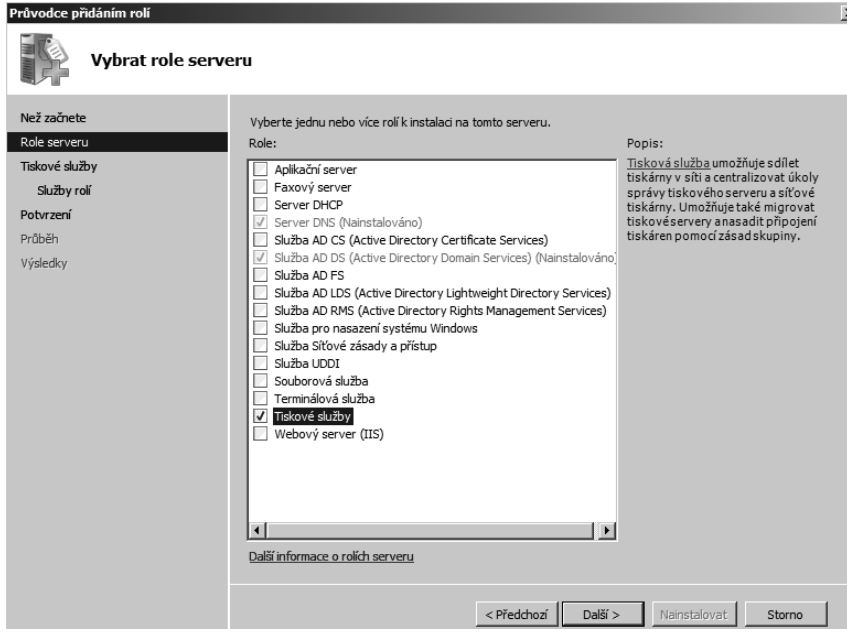
Po vytvoření konvencí pro pojmenování umístění tiskáren povolte sledování umístění tiskáren v adresáři služby Active Directory, jak je zmíněno v části „Zapnutí sledování umístění tiskáren" v této kapitole.

Pokud nepoužíváte funkci služby Active Directory sledování umístění tiskárny, stále můžete přidat informaci o umístění k tiskárně, ačkoliv toto řešení má některá omezení. Pro zadání informací o umístění zadejte název umístění na kartě Obecné (General) v dialogu s vlastnostmi tiskárny. Při zadávání názvů umístění buďte pečliví a konzistentní. Dbejte na to, aby všichni správci používali stejný název pro konkrétní umístění, a používejte krátké a snadno zapamatovatelné názvy: uživatelé musí při vyhledávání tiskáren znát přesný název umístění, pokud jsou funkce pro vyhledávání umístění služby Active Directory nedostupné.

Vytvoření tiskového serveru

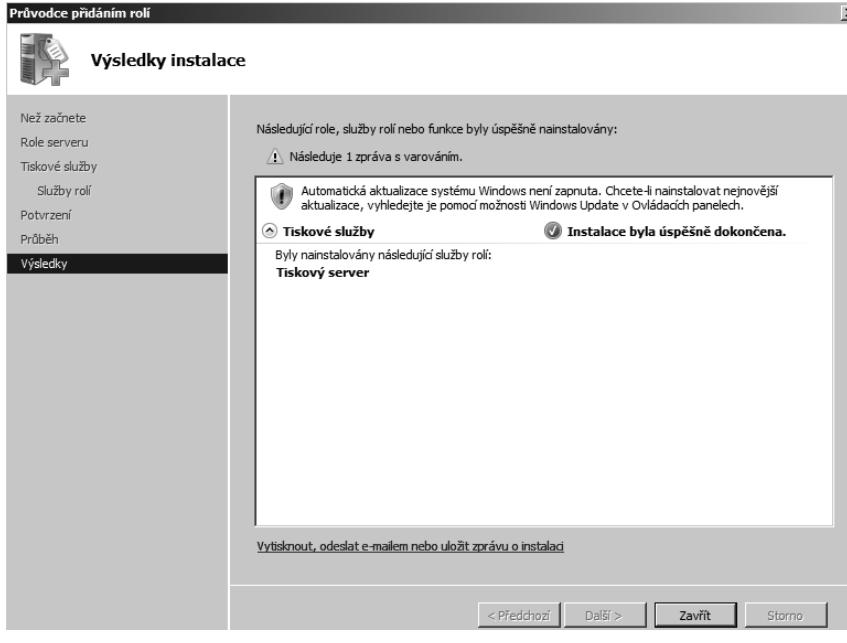
Roli Print Service můžete nainstalovat na kterýkoliv server, a to otevřením Server Manager, výběrem položky Roles ve stromu konzoly a poté pomocí následujících kroků:

1. V podokně s výsledky klepněte na příkaz Přidat role (Add Roles). Spustí se Průvodce přidáním rolí (Add Roles Wizard).
2. Klepejte na tlačítko Další (Next), dokud se nedostanete na stránku Vybrat služby rolí (Select Server Roles). (Viz obrázek 10.2.)



Obrázek 10.2: Výběr role Tiskové služby (Print Services)

3. Vyberte roli Tiskové služby (Print Services) a poté klepejte na tlačítko Další (Next), dokud se nezobrazí stránka Výsledky instalace (Installation Results). (Viz obrázek 10.3.)



Obrázek 10.3: Služba role Tiskový server (Print Server) je nainstalována

Zapnutí sledování umístění tiskáren

Chcete-li použít sledování umístění tiskáren, síť musí splňovat následující požadavky:

- Síť musí mít schéma adresování protokolu IP, které přibližuje fyzické rozvržení sítě.
- Struktura služby Active Directory musí obsahovat více než jednu lokalitu nebo více než jednu podsíť. Pokud nemáte více podsítí protokolu IP, můžete použít konzolu Lokality a služby Active Directory (Active Directory Sites And Services) k vytvoření podsítí z rozsahů adres v rámci podsítě, která odpovídá fyzickým umístěním.
- Klientské počítače musí být schopny odpovídat na dotazy služby Active Directory. (Musí podporovat protokol Lightweight Directory Access Protocol verze 2 nebo vyšší.)
- Každá lokalita je v samostatné podsíti.
- Každá podsíť, ke které klienti potřebují přistupovat, má svůj vlastní objekt podsítě v adresáři Active Directory.
- Síť používá konvenci pro pojmenování umístění tiskáren.

Další informace: Informace o instalaci adresářových služeb (Directory Services) a vytvoření odpovídajících podsítí pro daný podnik najdete v kapitole 16, „Instalace a konfigurace adresářových služeb".

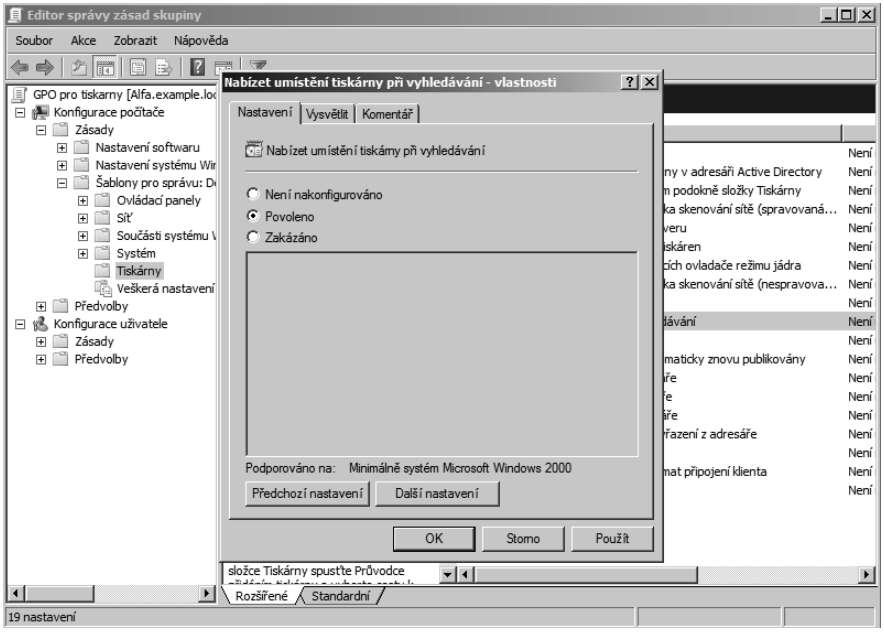
Doporučené postupy: Pokud očekáváte vysoký objem tisku, tiskárny a tiskové servery by se měly nacházet ve stejném segmentu sítě jako uživatelé dané tiskárny. Tento přístup minimalizuje dopad na uživatele v jiných částech sítě. V každém případě minimalizujte počet síťových směrování, která vyžaduje tisková úloha k tomu, aby se dostala od uživatelů k jejich výchozí tiskárně.

Chcete-li uživatelům povolit snadné vyhledávání tiskáren v adresáři Active Directory podle umístění, vytvořte konvence pro pojmenování umístění podle pokynů v části „Vytvoření konvencí pro pojmenování umístění" v této kapitole a poté podle následujících kroků nastavte sledování umístění tiskáren:

1. Ze Správce serveru (Server Manager), nabídky Nástroje pro správu (Administrative Tools) nebo zadáním příkazu **dssite.msc** do pole Zahájit hledání (Start Search) v nabídce Start otevřete modul snap-in Lokality a služby Active Directory (Active Directory Sites And Services).
2. V uzlu Sites klepněte pravým tlačítkem na první síti a z místní nabídky zvolte příkaz Vlastnosti (Properties).
3. Klepněte na kartu Umístění (Location) a zadejte název umístění sítě, viz obrázek 10.4, nebo klepnutím na tlačítko Procházet (Browse) vyberte umístění ze stromu umístění pro daný podnik.
4. Vyhledejte umístění ze stromu umístění pro daný podnik.

Obrázek 10.4: Zadání názvu umístění podsítě

5. Klepněte na tlačítko OK a zopakujte kroky 2 a 3 pro každou lokalitu a podsíť v dané síti.
6. Vytvořte nový objekt zásad skupiny (Group Policy), který platí pro všechny počítače, na nichž povolíte sledování umístění tiskáren: otevřete konzolu Správa zásad skupiny (Group Policy Management Console) z nabídky Nástroje pro správu (Administrative Tools) nebo zadáním příkazu gpmc.msc do pole Zahájit hledání (Start Search) v nabídce Start. Klepněte pravým tlačítkem myši na názvu domény a zvolte příkaz Vytvořit objekt zásad skupiny v této doméně a propojit jej sem (Create A GPO In This Domain, And Link It Here).
7. Pojmenujte objekt GPO a klepněte na tlačítko OK. Klepněte pravým tlačítkem myši na objektu GPO a volbou příkazu Upravit (Edit) otevřete Editor správy zásad skupiny (Group Policy Management Editor).
8. Ve stromu konzoly vyberte položku Konfigurace počítače (Computer Configuration), Zásady (Policies), vyberte složku Šablony pro správu (Administrative Templates) a poté vyberte Tiskárny (Printers).
9. Poklepejte na zásadě Nabízet umístění tiskárny při vyhledávání (Pre-Populate Printer Search Location Text) (viz obrázek 10.5.), zvolte možnost Povoleno (Enabled) a klepněte na tlačítko OK.



Obrázek 10.5: Zapnutí sledování umístění tiskáren

10. Zavřete konzolu Editor správy zásad skupiny (Group Policy Management Editor).

11. Otevřete konzolu Správa tisku (Print Management) nebo složku Tiskárny a faxy (Printers And Faxes) vašeho tiskového serveru, klepněte pravým tlačítkem myši na tiskárně, zvolte příkaz Vlastnosti (Properties) a poté do textového pole Umístění (Location) zadejte umístění; nebo klepněte na tlačítko Procházet (Browse) a vyberte umístění ze stromu umístění daného podniku. Zopakujte tento krok pro všechny tiskárny v adresáři Active Directory nebo použijte skript Prncnfg.vbs pro automatizaci tohoto postupu.(Zadáním příkazu **cscript %WINDIR%\system32\prncnfg.vbs /?** na příkazovém řádku zobrazte referenční informace příkazového řádku.)

Poznámka: V poli Umístění (Location) buďte při specifikaci tiskáren konkrétnější, neuvádějte jen umístění podsítě. Přidejte například číslo místnosti nebo název.

12. Otestujte sledování umístění tiskáren prohledáním adresáře Active Directory podle umístění z klientského počítače.

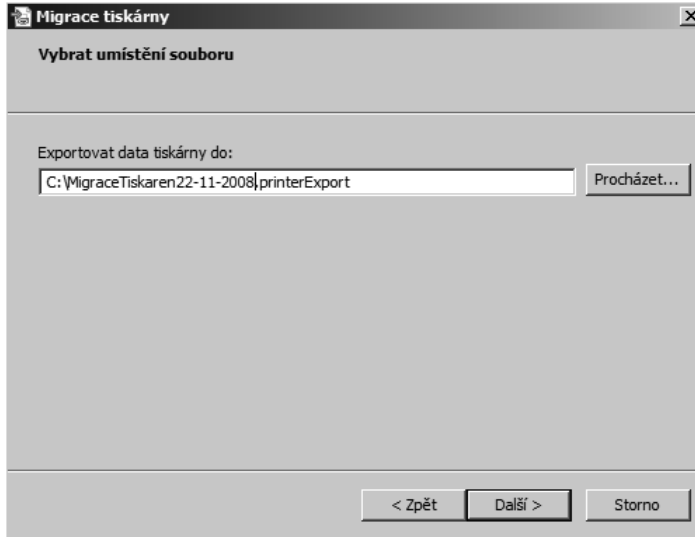
Migrace tiskových serverů

Pokud potřebujete nahradit starší tiskový server nebo sloučit více tiskových serverů do jednoho, můžete použít průvodce Migrace tiskárny (Printer Migration Wizard) nebo nástroj příkazového řádku Printbrm.exe. Je možné exportovat tiskové fronty, nastavení tiskáren, porty tiskáren a sledování jazyka a poté je importovat na jiném tiskovém serveru.

Použití průvodce Migrace tiskárny (Print Migration Wizard)

Chcete-li použít průvodce Migrace tiskárny (Print Migration Wizard), postupujte podle následujících kroků:

1. Z nabídky Nástroje pro správu (Administrative Tools) zvolte příkaz Správa tisku (Print Management).
2. Ve stromu Správa tisku (Print Management) klepněte pravým tlačítkem myši na počítači, který obsahuje tiskové fronty, které chcete exportovat, a poté klepněte na příkaz Export tiskáren do souboru (Export Printers To A File).
3. Prohlédněte si seznam souborů, které se mají exportovat, a poté klepněte na tlačítko Další (Next).
4. Na stránce Vybrat umístění tiskárny (Select The File Location) zvolte umístění, kam se mají uložit nastavení tiskárny (viz obrázek 10.6) a poté klepnutím na tlačítko Další (Next) uložte tiskárny. Po dokončení operace klepněte na tlačítko Dokončit (Finish).



Obrázek 10.6: Zadání místa pro uložení souborů tiskárny

5. Klepněte pravým tlačítkem myši na cílovém počítači, na nějž chcete importovat tiskárny, a zvolte příkaz Import tiskáren ze souboru (Import Printers From A File).
6. Na stránce Vybrat umístění souboru (The File Location) určete umístění souboru s nastavením tiskárny a poté klepněte na tlačítko Další (Next). Zkontrolujte objekty, které budou importovány, a klepněte na tlačítko Další (Next).
7. Na stránce Vybrat možnosti importu (Select Import Options) zvolte následující možnosti importu:
   - **Režim importu (Import Mode):** Co dělat, pokud konkrétní tisková fronta již na cílovém počítači existuje.

- **Uvést v adresáři (List In The Directory):** Zda mají být importované tiskové fronty publikovány ve službě Active Directory Domain Services.
- **Převést porty LPR na standardní sledování portů (Convert LPR Ports To Standard Port Monitors):** Zda mají být porty LPR v souboru s nastavením tiskárny při importu tiskáren převedeny na rychlejší standardní sledování portů.

8. Klepnutím na tlačítko Další (Next) importujte nastavení tiskárny.

Použití příkazového řádku

Migrace tiskových serverů je ještě jednodušší, pokud použijete příkazový řádek a následující kroky:

1. Klepněte na tlačítko Start, Všechny programy (All Programs), Příslušenství (Accessories), klepněte pravým tlačítkem myši na příkaz Příkazový řádek (Command Prompt) a poté zvolte příkaz Spustit jako správce (Run As Administrator).
2. Zadejte následující příkaz:

```
CD %WINDIR%\System32\Spool\Tools
Printbrm -s \\<nazev_zdrojoveho_pocitace> -b -f
   <nazev_souboru>.printerExport
```

3. Poté zadejte tento příkaz:

```
Printbrm -s \\<nazev_ciloveho_pocitace> -r -f
   <nazev_souboru>.printerExport
```

Základní syntaxe tohoto příkazu je následující:

<nazev_zdrojoveho_pocitace>*Název UNC zdrojového počítače.*

<nazev_souboru>*Název souboru s nastavením tiskárny. Použijte příponu souboru .printerExport nebo .cab.*

<nazev_ciloveho_pocitace>*Název UNC cílového počítače.*

Poznámka: Úplnou syntaxi tohoto příkazu získáte zadáním příkazu **printbrm /?** na příkazovém řádku.

Instalace tiskáren

Instalace tiskárny je známá úloha pro většinu uživatelů počítačů – pokud má tiskárna připojení USB nebo IEEE 1394 (Firewire), připojte ji k serveru a vložte do něj disk s ovladači. Chcete-li nainstalovat tiskárnu s využitím připojení k síti (což je nejlepší způsob připojení tiskárny), můžete přidat tiskárnu ručně, podle popisu v této části, nebo nechat modul Správa tisku (Print Management) automaticky detekovat všechny tiskárny, které se nachází ve stejné podsíti jako tiskový server.

Pro nastavení síťové tiskárny prostřednictvím standardního portu tiskárny TCP/IP připojte tiskárnu k síti a proveďte správné nastavení protokolu TCP/IP. Pokud konfigurujete tiskárnu tak, aby používala server DHCP, vytvořte pro danou tiskárnu rezervaci DHCP, aby se její adresa nezměnila, a poté postupujte podle následujících kroků:

1. Z nabídky Nástroje pro správu (Administrative Tools) otevřete konzolu Správa tisku (Print Management).
2. Vyberte požadovaný tiskový server, klepněte pravým tlačítkem myši na položce Tiskárny (Printers) a zvolte příkaz Přidat tiskárnu (Add Printer).
3. Na stránce Instalace tiskárny (Printer installation) vyberte způsob instalace z následujících možností:

   Vyhledat tiskárny v síti (Search The Network For Printers)

   a. Otevře se okno pro vyhledání síťové tiskárny a začnou se vyhledávat tiskárny.

   b. Po dokončení vyhledávání označte tiskárny, které se mají nainstalovat, a klepněte na tlačítko Další (Next).

Poznámka: Pokud nemůžete najít tiskárnu pomocí funkce pro vyhledávání, použijte jednu z dalších metod instalace v této části.

   Přidat novou tiskárnu TCP/IP nebo tiskárnu webových služeb zadáním adresy IP nebo hostitelského názvu (Add A TCP/IP Or Web Services Printer By IP Address Or Hostname)

   a. Zadejte síťový název tiskárny nebo IP adresu. Klepněte na tlačítko Další (Next) a průvodce vyhledá port.

   Přidat novou tiskárnu s použitím stávajícího portu (Add A New Printer Using An Existing Port)

   a. Vyberte existující port z rozevíracího seznamu a poté klepněte na tlačítko Další (Next).

   b. Určete stávající ovladač, který se má použít, nebo zvolte možnost Nainstalovat nový ovladač (Install A New Driver). Klepněte na tlačítko Další (Next).

Poznámka: Pokud zvolíte možnost instalace nového ovladače, budete muset zadat výrobce tiskárny a model tiskárny a poté v případě potřeby vložit instalační disk k tiskárně.

   c. V dialogu Nastavení názvu tiskárny a sdílení (Printer Name And Sharing Settings) můžete změnit název tiskárny a název sdílené položky, přidat umístění a další komentář a zvolit možnost publikování tiskárny v adresáři. Klepněte na tlačítko Další (Next).

   d. Tiskárna je připravena k instalaci. Zkontrolujte nastavení a klepnutím na tlačítko Další (Next) dokončete instalaci.

   Vytvořit nový port a přidat novou tiskárnu (Create A New Port And Add A New Printer)

   a. Vyberte typ portu, který se má vytvořit, a klepněte na tlačítko Další (Next).

   b. Zadejte název portu a klepněte na tlačítko OK.

c. Vyberte, zda se má použít stávající ovladač, nebo nainstalujte nový. Klepněte na tlačítko Další (Next).

d. V dialogu Nastavení názvu tiskárny a sdílení (Printer Name And Sharing Settings) můžete změnit název tiskárny a název sdílené položky, přidat umístění a další komentář a zvolit možnost publikování tiskárny v adresáři. Klepněte na tlačítko Další (Next).

e. Tiskárna je připravena k instalaci. Zkontrolujte nastavení a klepnutím na tlačítko Další (Next) dokončete instalaci.

Instalace tiskáren se zásadami skupiny

Tiskárny můžete pro uživatele nebo počítače automaticky nainstalovat s využitím zásad skupiny (Group Policy). Tento způsob instalace tiskárny je nejpraktičtější v situacích, kdy jsou stejné tiskárny používány většinou počítačů nebo uživatelů, například ve třídě nebo pobočce firmy.

Poznámka: V případě instalace připojení tiskárny pomocí zásad skupiny (Group Policy) musí vaše prostředí splňovat požadavek, aby schéma služby AD DS používalo verzi schématu pro systém Windows Server 2003 R2 nebo novější.

Klientské počítače se systémem Windows 2000, Windows XP nebo Windows Server 2003 musí použít nástroj PushPrinterConnections.exe buď ve spouštěcím skriptu (pro připojení vázaná na počítač), nebo v přihlašovacím skriptu (pro připojení vázaná na uživatele). Další informace najdete v části „Přidání příkazu PushPrinterConnections pomocí zásad skupiny (Group Policy)“ dále v této kapitole.

Pro automatickou instalaci tiskáren postupujte podle následujících kroků:

1. Z nabídky Nástroje pro správu (Administrative Tools) zvolte příkaz Správa tisku (Print Management).
2. U příslušného tiskového serveru klepněte na položku Tiskárny (Printers).
3. V podokně s výsledky klepněte pravým tlačítkem myši na tiskárně, kterou chcete nainstalovat, a poté zvolte příkaz Instalovat se zásadami skupiny (Deploy With Group Policy).
4. V dialogu Instalovat se zásadami skupiny (Deploy With Group Policy) klepněte na tlačítko Procházet (Browse) a poté vyberte objekt GPO pro uložení připojení tiskárny. Klepněte na tlačítko OK.
5. Určete, zda se mají připojení tiskárny nainstalovat pro uživatele, nebo pro počítače:
   - V případě instalace pro skupinu uživatelů (aby uživatelé mohli přistupovat k tiskárnám z libovolného počítače, ke kterému se přihlásí) zaškrtněte políčko Uživatelé, na které se tento objekt zásad skupiny vztahuje (vázáno na uživatele) (Users That This GPO Applies To (Per User)).
   - V případě instalace pro skupinu počítačů (aby všichni uživatelé daných počítačů mohli přistupovat k tiskárnám) zaškrtněte políčko Počítače, na které se tento

objekt zásad skupiny vztahuje (vázáno na počítač) (The Computers That This GPO Applies To (Per Machine)).

6. Klepněte na tlačítko Přidat (Add).
7. Opakováním kroků 4 až 6 přidejte v případě potřeby nastavení připojení tiskárny i pro další objekty
8. Klepněte na tlačítko OK.

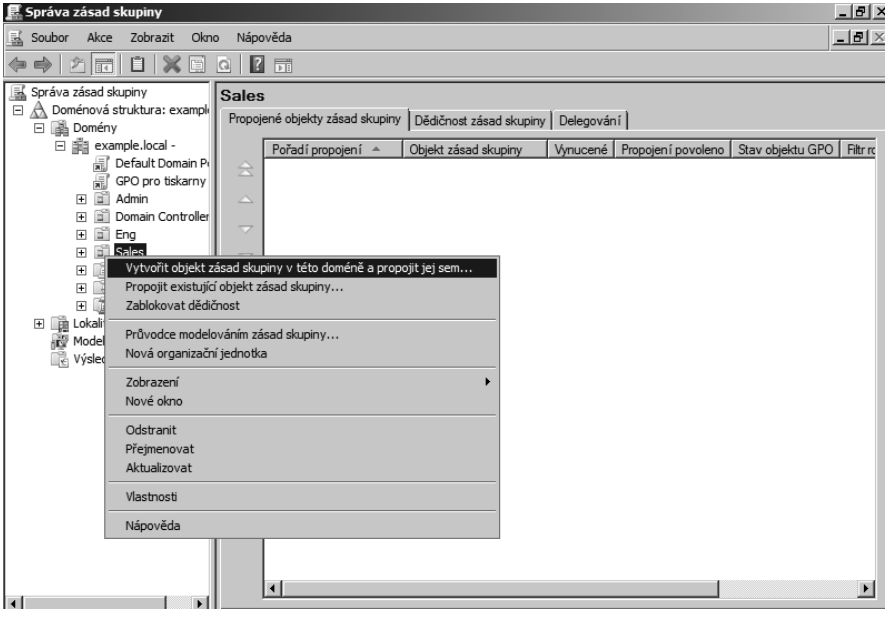
Poznámka: V případě připojení vázaných na uživatele systém Windows přidá připojení tiskárny po přihlášení uživatele. V případě připojení vázaných na počítač systém Windows přidá připojení tiskárny pouze po restartování klientského počítače. Pokud odeberete nastavení připojení tiskárny z objektu GPO, příkaz PushPrinterConnections.exe odstraní odpovídající tiskárny z klientského počítače při příštím restartování počítače nebo přihlášení uživatele.

Přidání příkazu PushPrinterConnections pomocí zásad skupiny (Group Policy)

Chcete-li nainstalovat připojení tiskárny k počítačům se systémem Windows XP, Windows 2000 nebo Windows Server 2003, musíte do spouštěcího skriptu počítače (v případě připojení vázaných na počítač) nebo do přihlašovacího skriptu (v případě připojení vázaných na uživatele) přidat nástroj PushPrinterConnections.exe. Zásady skupiny (Group Policy) jsou nejefektivnějším způsobem řešení téhle úlohy.

Chcete-li přidat soubor PushPrinterConnections.exe do spouštěcích nebo přihlašovacích skriptů, postupujte podle následujících kroků:

1. Z nabídky Nástroje pro správu (Administrative Tools) zvolte příkaz Správa zásad skupiny (Group Policy Management).
2. Ve stromu konzoly klepněte pravým tlačítkem myši na doméně nebo organizační jednotce, která obsahuje účty počítače nebo uživatelské účty, pro které chcete přidat nástroj PushPrinterConnections.exe, a zvolte příkaz Vytvořit objekt zásad skupiny v této doméně a propojit jej sem (Create A GPO In This Domain, And Link It Here) (viz obrázek 10.7). Zadejte název nového objektu GPO a poté klepněte na tlačítko OK.
3. Klepněte pravým tlačítkem myši na vámi vytvořeném objektu GPO a poté klepněte na tlačítko Upravit (Edit).
4. Ve stromu Editoru správy zásad skupiny (Group Policy Management Editor) najděte následující položky:
   - Pokud jsou připojení tiskárny nainstalována jako vázaná na počítač, přejděte k položce Konfigurace počítače (Computer Configuration), Zásady (Policies), Nastavení systému Windows (Windows Settings), Skripy (spouštěcí nebo ukončovací) (Scripts (Startup/Shutdown)).
   - Pokud jsou připojení tiskárny nainstalována jako vázaná na uživatele, přejděte k položce Konfigurace uživatele (User Configuration), Zásady (Policies), Nastavení systému Windows (Windows Settings), Skripty (pro přihlášení nebo odhlášení) (Scripts (Logon/Logoff)).



Obrázek 10.7: Vytvoření nového objektu GPO

Poznámka: Klientské počítače se systémem Windows 2000 nepodporují připojení vázaná na počítač.

5. Klepněte pravým tlačítkem myši na položce Po spuštění (Startup) nebo Přihlášení (Logon) a poté zvolte příkaz Vlastnosti (Properties).
6. V dialogu Přihlášení – vlastnosti (Logon Properties) nebo Po spuštění – vlastnosti (Startup Properties) klepněte na tlačítko Zobrazit soubory (Show Files), čímž otevřete okno Startup nebo Logon.
7. Zkopírujte soubor PushPrinterConnections.exe ze složky %WINDIR%\System32 do okna Startup nebo Logon. Tím tento nástroj přidáte do objektu GPO, odkud se bude replikovat na další řadiče domény společně se zbývajícími nastaveními Group Policy.
8. V dialogu Přihlášení – vlastnosti (Logon Properties) nebo Po spuštění – vlastnosti (Startup Properties) klepněte na tlačítko Přidat (Add). Zobrazí se dialog Přidat skript (Add Script).
9. Do pole Název skriptu (Script Name) zadejte název **PushPrinterConnections.exe**.
10. Chcete-li povolit přihlášení klientským počítačům se systémem Windows Server 2003, Windows XP nebo Windows 2000, zadejte do pole Parametry skriptu (Script Parametres) hodnotu **–log**. Soubory protokolů jsou zapsány do souboru %WINDIR%\temp\ppcMachine.log v případě připojení vázaných na počítač a do souboru %temp%\ppcUser.log v případě připojení vázaných na uživatele, a to v počítači, na který jsou zásady použity.

11. Klepněte na tlačítko OK v dialogu Přidat skript (Add Script) a poté klepněte na tlačítko OK v dialogu Po spuštění – vlastnosti (Startup Properties) nebo Přihlášení – vlastnosti (Logon Properties).

Konzolu Správa zásad skupiny (Group Policy Management Console) použijte k propojení objektu GPO, obsahujícího nástroj PushPrinterConnections.exe, s dalšími organizačními jednotkami nebo doménami.

Vyjmutí počítačů se systémem Windows Vista a Windows Server 2008 ze souboru PushPrinterConnections.exe

Soubor PushPrinterConnections.exe automaticky detekuje počítače se systémem Windows Vista nebo Windows Server 2008 a automaticky skončí, takže je bezpečné použít tento soubor v přihlašovacích nebo spouštěcích skriptech ve všech klientských počítačích vaší organizace. Pokud jsou časy pro přihlášení nebo spouštění klientských počítačů se systémem Windows Vista nebo Windows Server 2008 příliš pomalé, můžete tyto klienty vyloučit použitím filtrů rozhraní WMI.

Postupujte podle následujících kroků:

1. Z nabídky Nástroje pro správu (Administrative Tools) zvolte příkaz Správa zásad skupiny (Group Policy Management).
2. Ve stromu konzoly přejděte k doméně, klepněte pravým tlačítkem myši na položce Filtry rozhraní WMI (WMI Filters) a zvolte příkaz Nový (New).
3. Zadejte název a popis do příslušných polí a poté klepněte na tlačítko Přidat (Add).
4. Otevře se dialog Dotaz rozhraní WMI (WMI Query). Pro vytvoření filtru, který vyberte všechny klientské počítače se systémy Windows předcházející systému Windows Vista, zadejte do části dotazu následující příkaz:

```
Select * from Win32_OperatingSystem where BuildNumber < 6000
```

5. Klepněte na tlačítko OK v dialogu Dotaz rozhraní WMI (WMI Query) a poté klepněte na tlačítko Uložit (Save) v dialogu Nový filtr rozhraní WMI (New WMI Filter).
6. Vyberte objekt zásad skupiny, který obsahuje soubor PushPrinterConnections.exe, vyberte vámi vytvořený filtr rozhraní WMI ze seznamu Filtrování rozhraní WMI (WMI Filtering) a poté klepněte na tlačítko Ano (Yes).

Správa tiskových úloh ze systému Windows

Pro správu tiskových úloh otevřete konzolu Správa tisku (Print Management) z nabídky Nástroje pro správu (Administrative Tools) a poté postupujte podle pokynů k příslušným úlohám v následujícím seznamu.

Dočasné pozastavení tiskových úloh

Chcete-li dočasně pozastavit tisk *jednoho* dokumentu, klepněte pravým tlačítkem myši na odpovídající tiskárně a zvolte příkaz Otevřít tiskovou frontu (Open Printer Queue). Klepněte pravým tlačítkem myši na požadovaném dokumentu a z místní nabídky zvolte

příkaz Pozastavit (Pause). Pro pokračování v tisku klepněte pravým tlačítkem myši na požadovaném dokumentu a poté zvolte příkaz Pokračovat (Resume).

Chcete-li dočasně pozastavit tisk *všech* dokumentů, klepněte pravým tlačítkem myši na odpovídající tiskárně a zvolte příkaz Pozastavit tisk (Pause Printing). Pro pokračování v tisku všech dokumentů klepněte pravým tlačítkem myši na tiskárně a zvolte příkaz Pokračovat v tisku (Resume Printing).

Zrušení tiskových úloh

Chcete-li zrušit jednu nebo více tiskových úloh, klepněte pravým tlačítkem myši na odpovídající tiskárně a zvolte příkaz Otevřít tiskovou frontu (Open Printer Queue). Klepněte pravým tlačítkem myši na úloze, kterou chcete zrušit, a z místní nabídky zvolte příkaz Zrušit tisk (Cancel). (Tiskovou úlohu můžete zrušit také jejím výběrem a stisknutím klávesy Delete.)

Chcete-li zrušit *všechny* tiskové úlohy v tiskové frontě, z nabídky Tiskárny (Printer) zvolte příkaz Zrušit všechny úlohy (Cancel All Documents).

Restartování tiskové úlohy

Chcete-li tiskovou úlohu restartovat (to jest vytisknout dokument znovu od začátku), klepněte pravým tlačítkem myši na požadovaném dokumentu a z místní nabídky zvolte příkaz Tisknout znovu (Restart).

Poznámka: Někdy se zdá, že tisková úloha ve frontě „zamrzla" a nedaří se vám ji odstranit. Pokud se tak stane, vypněte tiskárnu a poté ji znovu zapněte nebo zastavte Službu zařazování tisku (Print Spooler) na tiskovém serveru a poté ji restartujte.

Změna priority tiskové úlohy

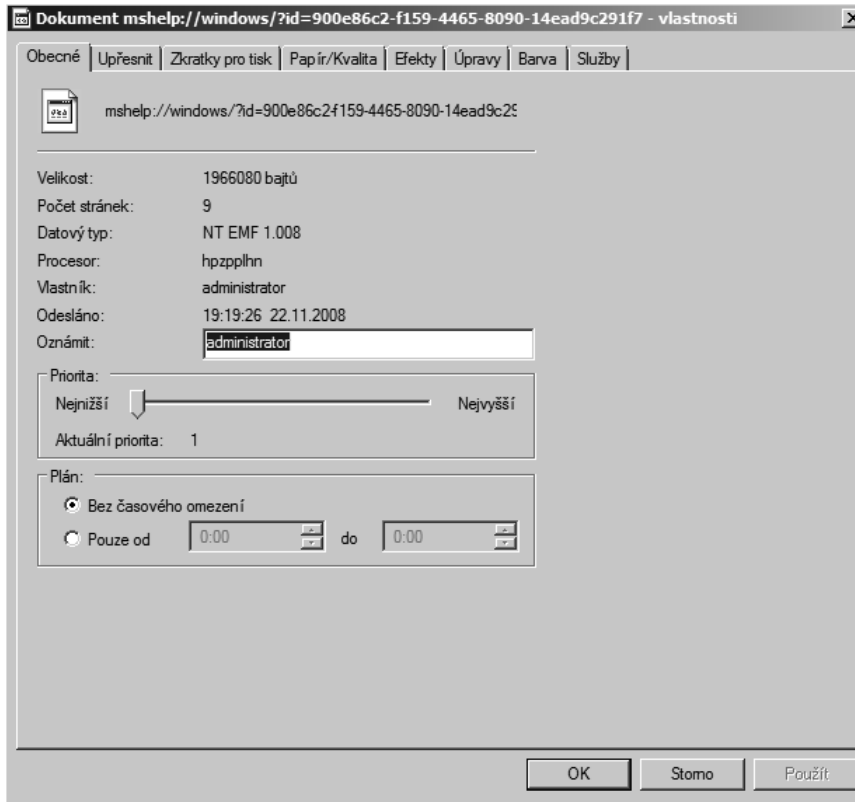
Chcete-li změnit prioritu nebo naplánování tiskové úlohy, klepněte pravým tlačítkem myši na tiskové úloze, zvolte příkaz Vlastnosti (Properties) a poté klepněte na kartu Obecné (General). Pomocí posuvníku Priorita (Priority) (zobrazeného na obrázku 10.8) upravte prioritu dokumentu; 1 značí nejnižší prioritu a 99 nejvyšší prioritu.

V případě, že chcete specifikovat, že dokument by měl být vytištěn pouze v určitém časovém rozmezí, zvolte možnost Pouze od (Only From) na téže stránce a vyberte časové rozmezí, kdy se může dokument vytisknout.

Poznámka: Funkce Plán (Schedule) je užitečná v případech, kdy máte velké tiskové úlohy, ale nechcete zatěžovat tiskárnu v nejvytíženější pracovní době.

Přesunutí tiskových úloh

Chcete-li přesunout všechny dokumenty z jedné tiskárny na jinou tiskárnu, která může použít stejný ovladač tiskárny, klepněte pravým tlačítkem myši na dané tiskárně, zvolte příkaz Vlastnosti (Properties), klepněte na kartu Porty (Ports), vyberte port, ke kterému je připojena druhá tiskárna, a poté zrušte zaškrtnutí políčka vedle původního portu.



Obrázek 10.8: Nastavení priority tiskové úlohy a konkrétního času vytištění

Poznámka: Tiskovou úlohu, která již zahájila tisk, nelze přesunout. Abyste ji přesunuli, musíte ji restartovat.

Správa tiskových úloh z příkazového řádku

Díky systému Windows Server 2008 je správa prováděná na příkazovém řádku pro správce systému Windows praktickou záležitostí. Na příkazovém řádku je možné provádět téměř všechny úlohy správy – včetně úloh, které se týkají tiskáren. Pro začátek použijte následující seznam příkazů a skriptů:

- **Print** – vytiskne určený textový server na určené tiskárně.
- **Lpr** – vytiskne určený textový soubor do určené tiskové fronty služby LPD.
- **Net print** – zobrazí informace o určené tiskové frontě nebo tiskové úloze. Rovněž může zablokovat, znovu aktivovat nebo odebrat tiskové úlohy.
- **Lpq** – zobrazí informace o určené tiskové frontě služby LPD.
- **Net start** – spustí určenou službu. Ke spuštění nebo zastavení služby zařazování můžete použít příkazy `Net start spooler` a `Net stop spooler`.

Poznámka: Chcete-li zobrazit seznam parametrů, zadejte příkaz následovaný parametrem /? na příkazovém řádku nebo použijte Nápovědu a podporu pro systém Windows (Help And Support Center).

- **Cscript %Windir%\System32\Prnmngr.vbs** – přidá, odstraní nebo zobrazí seznam tiskáren, které jsou nainstalovány na tiskovém serveru se systémem Windows.
- **Cscript %Windir%\System32\Prnjobs.vbs** – umožní vám zobrazit a spravovat tiskové úlohy sdílených tiskáren na tiskovém serveru se systémem Windows.
- **Cscript %Windir%\System32\Prncfg.vbs** – umožní vám zobrazit a změnit nastavení tiskáren na tiskovém serveru se systémem Windows.
- **Cscript %Windir%\System32\Prnqctl.vbs** – pozastaví tisk nebo opět pokračuje v tisku, odstraní tiskovou frontu nebo vytiskne zkušební stránky tiskárny.
- **Cscript %Windir%\System32\Prnport.vbs** – spravuje všechny úkony související s porty tiskáren.
- **Cscript %Windir%\System32\Prndrvr.vbs** – přidá, odstraní nebo zobrazí seznam ovladačů tiskárny na tiskovém serveru se systémem Windows.

Další informace o použití skriptů při správě na příkazovém řádku najdete v kapitole 15, „Použití skriptů ke konzistentní správě“.

Nastavení možností zabezpečení

Možnosti zabezpečení se dostávají ke slovu tehdy, když máte řadu tiskáren, které jsou samostatné, ale ne všechny stejné. Například byste mohli chtít, aby ne každý mohl tisknout na barevné, sublimační tiskárně s vysokými náklady na tiskovou stránku, kterou jste zakoupili pro umělecký tisk. Na základnější úrovni mohou nastavení zabezpečení zabránit neoprávněným změnám vlastností tiskárny nebo priorit tisku.

Chcete-li nastavit oprávnění k tiskárně, klepněte pravým tlačítkem myši na dané tiskárně, zvolte příkaz Vlastnosti (Properties) a poté na kartě Zabezpečení (Security) přidejte oprávnění pro skupinu uživatelů. Klepnutím na tlačítko Upřesnit (Advanced) získejte větší kontrolu nad oprávněními nebo povolte auditování. Výsledky nastavení auditování si můžete prohlédnout v protokolu zabezpečení.

Tiskárna má tři úrovně oprávnění: Tisk (Print), Správa dokumentů (Manage Documents) a Správa tiskáren (Manage Printers). Tyto úrovně jsou definovány následovně:

- **Tisk (Print)** – uživatelé nebo skupiny s oprávněním Tisk (Print) se mohou připojit k tiskárně, mohou tisknout dokumenty a pozastavit, restartovat nebo odstranit své vlastní dokumenty z tiskové fronty. Systém Windows ve výchozím nastavení udělí oprávnění Tisk (Print) členům skupiny Everyone.
- **Správa dokumentů (Manage Documents)** – uživatelům nebo skupinám s oprávněním Správa dokumentů (Manage Documents) je uděleno oprávnění Tisk (Print) společně s možností měnit nastavení všech dokumentů v tiskové frontě a pozastavovat, restartovat a odstraňovat z tiskové fronty dokumenty všech uživatelů. Systém Windows ve výchozím nastavení udělí oprávnění Správa dokumentů (Manage Documents) skupině Creator/Owner.

- **Správa tiskáren (Manage Printers)** – uživatelům nebo skupinám s oprávněním Správa tiskáren (Manage Printers) jsou udělena oprávnění Správa dokumentů (Manage Documents) a Tisk (Print) společně s možností měnit vlastnosti tiskárny, odstraňovat tiskárny, měnit oprávnění k tiskárnám a přebírat vlastnictví tiskáren. Úroveň oprávnění Správa tiskáren (Manage Printers) je ekvivalentní oprávnění Úplné řízení (Full Control) v systému Windows NT. Systém Windows ve výchozím nastavení udělí tuto úroveň oprávnění operátorům tiskáren, operátorům serverů a správcům.

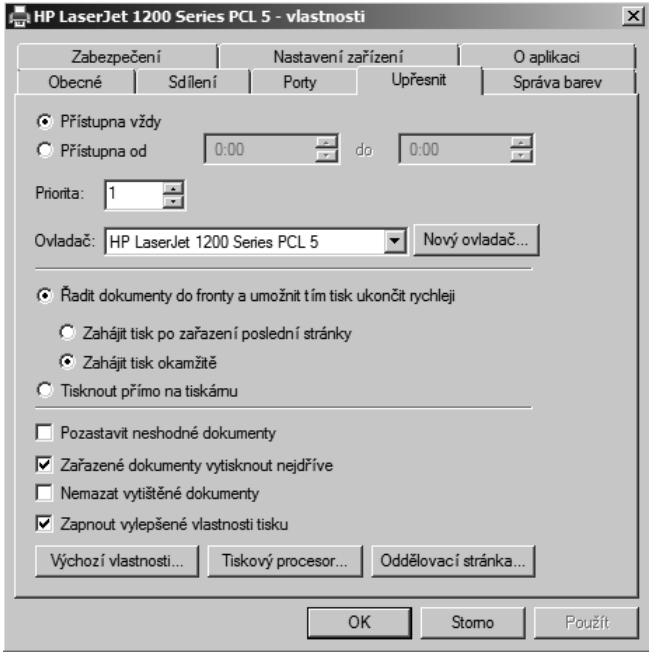
Změna dostupnosti tiskárny a priorit skupiny

Tiskárnu je možné nastavit tak, aby se tiskové úlohy odeslané některým z uživatelů vytiskly před úlohami odeslanými jinými uživateli; například můžete upřednostnit manažery nebo skupiny s krátkými termíny. Rovněž je možné rezervovat tiskárnu k výlučnému použití určitými skupinami v určitém období; například můžete rezervovat tiskárnu mimo běžnou pracovní dobu, aby mohly vámi určené skupiny tisknout velké, vysoce prioritní tiskové úlohy.

Chcete-li kontrolovat dostupnost nebo prioritu skupin, vytvořte dvě nebo více logických tiskáren pro jednu fyzickou tiskárnu, každé takové logické tiskárně nastavte různou prioritu a/nebo zpřístupněte ji v různém časovém rozpětí a nastavte různým skupinám uživatelů nebo skupinám oprávnění k tisku na jednotlivých logických tiskárnách.

Chcete-li provést tuto proceduru, postupujte podle následujících kroků:

1. Z nabídky Nástroje pro správu (Administrative Tools) zvolte příkaz Správa tisku (Print Management). Najděte tiskový server, na němž chcete vytvořit logickou tiskárnu, klepněte pravým tlačítkem myši na položce Tiskárny (Printers) a poté zvolte příkaz Přidat tiskárnu (Add Printer). Spustí se Průvodce instalací síťové tiskárny (Printer Installation Wizard).
2. Vyberte možnost Přidat novou tiskárnu s použitím stávajícího portu (Add A New Printer Using An Existing Port), vyberte port, ke kterému je fyzická tiskárna připojena, a poté klepněte na tlačítko Další (Next).
3. Zvolte možnost Použít stávající ovladač tiskárny v tomto počítači (Use An Existing Printer Driver On The Computer) a z rozevíracího seznamu vyberte ovladač. Klepněte na tlačítko Další (Next).
4. Zadejte výstižný popis tiskárny, z něhož bude zřejmá její funkce nebo kdo tiskárnu používá. Dvakrát klepněte na tlačítko Další (Next) a dokončete proces instalace.
5. Klepněte pravým tlačítkem myši na nové tiskárně v konzole Správa tisku (Print Management) a zvolte příkaz Vlastnosti (Properties).
6. Klepněte na kartu Zabezpečení (Security) a přiřaďte oprávnění skupinám nebo uživatelům, kteří budou mít k této tiskárně zvláštní přístup.
7. Klepněte na kartu Upřesnit (Advanced) (znázorněnou na obrázku 10.9). Pokud má být logická tiskárna dostupná pouze v určitou dobu, zvolte možnost Přístupna od (Available From) a nastavte požadované časy.



Obrázek 10.9: Karta Upřesnit (Advanced) dialogu s vlastnostmi tiskárny

8. Chcete-li změnit prioritu skupin a uživatelů, kteří budou tuto logickou tiskárnu používat, zadejte číslo do textového pole Priorita (Priority). Rozsah priorit je od 1, což značí nejnižší prioritu, až po 99, což značí nejvyšší prioritu.
9. Klepněte na tlačítko OK a zopakujte tento postup pro všechny logické tiskárny, které jste pro tiskárnu vytvořili.

Specifikace oddělovací stránky

Použití oddělovací stránky u vytížených tiskáren pomáhá zabránit jednomu uživateli v tom, aby kromě své vlastní tiskové úlohy vyzvedl i tiskovou úlohu dalšího uživatele. Systém Windows Server 2008 obsahuje čtyři výchozí oddělovací stránky, umístěné ve složce %WINDIR%\System32:

- **Pcl.sep** – přepne tiskárnu do jazyka Printer Control Language (PCL) a poté vytiskne oddělovací stránku.
- **Pscript.sep** – přepne tiskárnu do jazyka PostScript a nevytiskne oddělovací stránku.
- **Sysprint.sep** – přepne tiskárnu do jazyka PostScript a poté vytiskne oddělovací stránku.
- **Sysprintj.sep** – přepne tiskárnu do jazyka PostScript s podporou japonských znaků a poté vytiskne oddělovací stránku.

Pokud vaše tiskárna tyto jazyky nepodporuje, vytvořte si vlastní oddělovací stránku podle pokynů v odstavci „Vlastní oddělovací stránky“ dále v této kapitole. Chcete-li nastavit oddělovací stránku, postupujte podle následujících kroků:

1. V konzole Správa tisku (Print Management) klepněte pravým tlačítkem myši na tiskárně, kterou chcete upravit, a zvolte příkaz Vlastnosti (Properties).
2. Klepněte na kartu Upřesnit (Advanced).
3. Klepněte na tlačítko Oddělovací stránka (Separator Page) a vyberte stránku, která se má vložit mezi tištěné dokumenty a pomoci oddělit tiskové úlohy.

Vlastní oddělovací stránky

Chcete-li vytvořit vlastní oddělovací stránku, vytvořte textový soubor v Poznámkovém bloku nebo podobném textovém editoru, uložte jej s příponou .SEP a poté vytvořte svoji oddělovací stránku. Na prvním řádku zadejte řídicí znak, který se má použít (například \), a poté text, který se má objevit na oddělovací stránce. (Výpis příkazů, které můžete při vytvoření oddělovací stránky použít, najdete v tabulce 10.1.) Následující příklad představuje vzorovou tiskovou oddělovací stránku, která vytiskne uživatelské jméno, číslo úlohy, datum a čas tiskové úlohy; jako řídicí znak je použito zpětné lomítku (\):

```
\
\U\LUser Name: \N
\U\LJob : \I
\U\LDate: \D
\U\LTime: \T
\E
```

Tabulka 10.1: Příkazy oddělovací stránky

Příkaz	Funkce
\	Řídicí znak použitý interpretem souboru oddělovací stránky k oddělení příkazů. Může jím být libovolný znak, v této tabulce je pro příklad použito zpětné lomítko.
\Hn	Odešle do tiskárny řídicí sekvenci n. Správnou řídicí sekvenci, kterou můžete použít u vaší tiskárny, najdete v manuálu k tiskárně.
\Wn	Určí šířku oddělovací stránky, za níž systém Windows vynechá všechny znaky. Výchozí šířka je 80 a maximální šířka je 256.
\n	Přeskočí počet řádků zadaných číslem n. Platnými čísly jsou 0 až 9, kdy 0 slouží jako návrat na začátek dalšího řádku.
\Fnazevcesty	Vytiskne obsah souboru zadaného jako nazevcesty přímo na tiskárnu. Soubor musí být vyrenderován v příslušném jazyce pro danou tiskárnu.
\L	Vytiskne všechny znaky, které následují za příkazem \L až do výskytu dalšího řídicího znaku.
\N	Vytiskne uživatelské jméno uživatele, který odeslal tiskovou úlohu.
\I	Vytiskne číslo tiskové úlohy.
\D	Vytiskne datum vytištění tiskové úlohy; použitý formát data je shodný s formátem použitým tiskovým serverem.
\T	Vytiskne čas vytištění tiskové úlohy; použitý formát času je shodný s formátem použitým tiskovým serverem.

Příkaz	Funkce
\U	Zakáže blokování tisku znaků v souboru oddělovací stránky až do explicitního povolení.
\B\S	Vytiskne v bloku textu znaky s jednoduchou šířkou, dokud interpret souboru oddělovací stránky nenarazí na příkaz \U.
\B\M	Vytiskne v bloku textu znaky s dvojitou šířkou, dokud interpret souboru oddělovací stránky nenarazí na příkaz \U.
\E	Vysune aktuální stránku.

Změna zařazování tisku tiskárnou

Zařazování tisku nebo uložení tiskové úlohy na disk před jejím vytištěním jsou hlavní způsoby, pod kterými si uživatelé představují výkon tisku a skutečnou rychlost tisku. Způsob fungování zařazování tisku můžete změnit, chcete-li opravit problémy s tiskem nebo uchovat vytištěné dokumenty v tiskové frontě v případě, že uživatel potřebuje dokument vytisknout znovu.

Chcete-li změnit nastavení zařazování tisku pro určitou tiskárnu, klepněte pravým tlačítkem myši na tiskárně, u které tak chcete učinit, zvolte příkaz Vlastnosti (Properties) a poté pomocí následujících nastavení na kartě Upřesnit (Advanced) změňte nastavení zařazování tisku.

Řadit dokumenty do fronty a umožnit tím tisk ukončit rychleji (Spool Print Documents So Program Finishes Printing Faster)

Zařadí dokumenty do fronty tiskového serveru a uvolní prostředky klienta, aby mohl rychleji provádět jiné úlohy.

- Chcete-li zkrátit čas, který je třeba k vytištění dokumentu, zvolte možnost Zahájit tisk okamžitě (Start Printing Immediately).
- Chcete-li zajistit, aby byl celý dokument dostupný pro tiskárnu při začátku tisku, zvolte možnost Zahájit tisk po zařazení poslední stránky (Start Printing After Last Page Is Spooled). Tento krok může vést k odstranění některých problémů s tiskem a umožní vytištění dokumentů s vysokou prioritou před dokumenty s nízkou prioritou.

Tisknout přímo na tiskárnu (Print Directly To The Printer)

Vypne zařazování tisku, což ovlivní výkonnost serveru (může odstranit některé problémy s tiskem).

Pozastavit neshodné dokumenty (Hold Mismatched Documents)

Dokumenty, které nevyhovují aktuálnímu nastavení tiskárny, ponechá ve frontě (týká se to například dokumentů, které vyžadují papír velikosti Legal, přičemž v tiskárně je zrovna vložen papír velikosti Letter). Další dokumenty v tiskové frontě jsou ponechanými dokumenty neovlivněny.

Zařazené dokumenty vytisknout nejdříve (Print Spooled Documents First)

Nejprve vytiskne dokumenty s nejvyšší prioritou, které jsou již zařazeny ve frontě, a to i před dokumenty s vyšší prioritou, které se stále zařazují. Tento krok zrychlí celkovou propustnost tiskárny, neboť zabrání tiskárně v čekání na zařazování dokumentů.

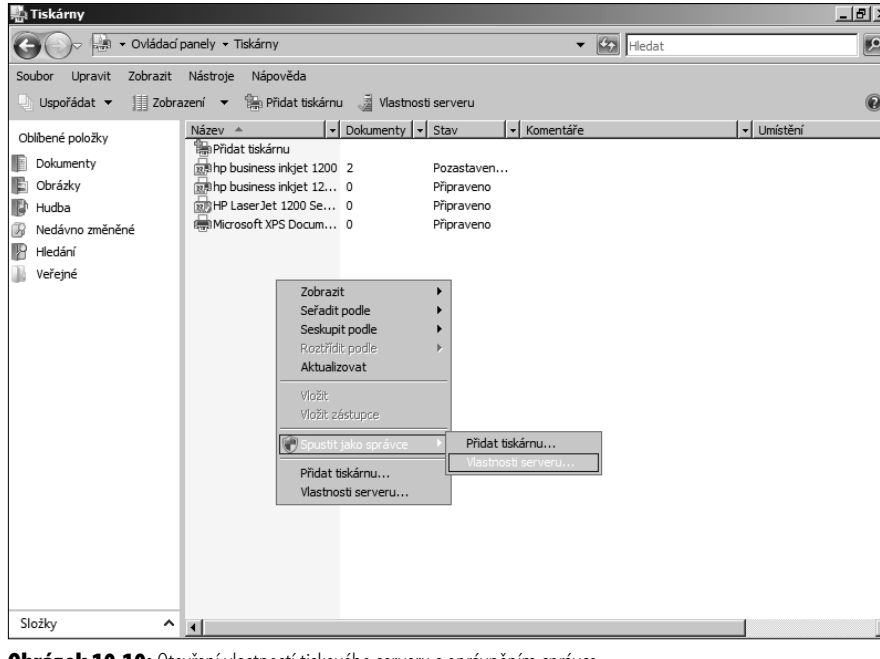
Nemazat vytištěné dokumenty (Keep Printed Documents)

Ponechá kopii tiskových úloh v tiskové frontě pro případ, že by uživatelé potřebovali vytisknout daný dokument znovu. V takovém případě může uživatel znovu odeslat dokument přímo z fronty, místo aby jej podruhé tiskl z příslušné aplikace.

Změna zařazování na tiskovém serveru

Ve výchozím nastavení se všechny události upozornění protokolují do souboru událostí (Event Log) na stránce Tiskové služby (Print Services) nástroje Správce serveru (Server Manager). Chcete-li protokolování těchto událostí zastavit, postupujte podle následujících kroků:

1. Otevřete Ovládací panel (Control Panel) a zvolte položku Tiskárny (Printers).
2. Ukažte myší na prázdné místo v okně a klepněte na něm pravým tlačítkem myši. Zvolte příkaz Spustit jako správce (Run As Administrator) a poté zvolte příkaz Vlastnosti serveru (Server Properties). (Viz obrázek 10.10.)



Obrázek 10.10: Otevření vlastností tiskového serveru s oprávněním správce

3. Klepněte na kartu Upřesnit (Advanced) a zrušte zaškrtnutí políčka Zobrazovat informační upozornění pro síťové tiskárny (Show Informational Notifications For Network Printers).
4. Operaci dokončete klepnutím na tlačítko OK.

Optimalizace výkonu tiskového serveru

Pro dosažení nejvyššího výkonu použijte rychlou, vyhrazenou jednotku nebo diskové pole pouze pro složku zařazování tisku a nepoužívejte tuto jednotku k umístění jakýchkoliv systémových souborů – zejména ne stránkovacího souboru. Sdílení souborů má vyšší prioritu než sdílení tiskáren, takže počítejte se snížením výkonu tisku, pokud na serveru používáte obě služby. Nezapomeňte umístit tiskové servery do stejného segmentu sítě, v němž jsou i uživatelé a tiskárny, a ujistěte se, že jednotka je dostatečně velká pro uložení všech dokumentů v tiskové frontě. (Pokud zvolíte možnost nemazat vytištěné dokumenty, možná budete potřebovat větší jednotku nebo diskové pole.)

Změna umístění složky zařazování tisku

Ve výchozím nastavení jsou tiskové úlohy zařazovány do složky WINDIR%\System32\Spool\PRINTERS, což není obvykle optimální umístění. Abyste jej změnili, postupujte podle následujících kroků:

1. Otevřete Ovládací panel (Control Panel)\Hardware a zvuk (Hardware And Sound) a vyberte položku Tiskárny (Printers).
2. Ukažte myší na prázdné místo v okně a klepněte na něm pravým tlačítkem myši. Zvolte příkaz Spustit jako správce (Run As Administrator) a poté zvolte příkaz Vlastnosti serveru (Server Properties).
3. Klepněte na kartu Upřesnit (Advanced) a zadejte nové umístění složky pro zařazování. Postup dokončíte klepnutím na tlačítko OK.

Správa ovladačů tiskárny

Při instalaci tiskárny systém Windows nainstaluje verzi ovladače, která odpovídá architektuře procesoru v serveru (x86, x64 nebo Itanium). Chcete-li použít tiskárnu z klientského počítače, který používá jinou architekturu procesoru, než která je na serveru, musíte nainstalovat další ovladače. Například pokud na serveru běží 32bitová verze systému Windows, ale na klientském počítači běží systém Windows XP Professional x64 Edition, musíte na server nainstalovat ovladače platformy x64 pro všechny tiskárny, z nichž mají mít klientské počítače možnost tisknout.

Rovněž možná bude třeba odebrat nebo přeinstalovat problematické ovladače nebo nastavit fond tiskáren, kdy dvě nebo více tiskáren slouží jako jedna tiskárna s cílem zvýšit rychlost a dostupnost.

Chcete-li nainstalovat ovladače tiskárny, které systém Windows automaticky stáhne do klientského počítače po připojení uživatele k tiskárně, postupujte podle následujících kroků:

1. Z nabídky Nástroje pro správu (Administrative Tools) vyberte položku Správa tisku (Print Management). V konzole Správa tisku (Print Management) klepněte pravým tlačítkem myši na složce Ovladače (Drivers) u příslušného tiskového serveru a zvolte příkaz Správa ovladačů (Manage Drivers).
2. Ke správě ovladačů použijte kartu Ovladače (Drivers) dialogu Tiskový server – vlastnosti (Print Server Properties):
   - Chcete-li nainstalovat ovladače, klepněte na tlačítko Přidat (Add) a poté pomocí Průvodce přidáním ovladače tiskárny (Add Printer Driver Wizard) nainstalujte ovladače pro příslušný operační systém a architekturu procesoru.
   - Chcete-li odebrat zastaralý nebo problematický ovladač, označte jej a klepněte na tlačítko Odebrat (Remove).
   - Chcete-li zobrazit podrobnosti o ovladači tiskárny, vyberte ovladač a klepněte na příkaz Vlastnosti (Properties).

Poznámka: Pokud instalujete nové ovladače pro více verzí operačního systému a/nebo architektury procesorů, použijte ovladače, které jsou určeny pro společnou práci, aby nastavení tiskárny, které provedete na tiskovém serveru, bylo použitelné na klientské počítače po jejich připojení k tiskárnám. Někteří výrobci tiskáren za tímto účelem nabízí balíčky ovladačů pro více platforem.

Systém Windows automaticky vyhledá nové ovladače

Systémy Windows Server 2008 a Windows Vista automaticky stáhnou ovladače tiskárny po připojení k sdílené tiskárně v systému Windows. Klienti se systémem Windows XP, Windows 2003 a Windows 2000 automaticky vyhledají aktualizované verze ovladačů tiskáren při spuštění a stáhnou novější verze z tiskového serveru, pokud existují.

Vytváření fondů tiskáren

Fond tiskáren je užitečný při zpracování velkého objemu tisku v jenom umístění, zejména v případě různých velkých a malých dokumentů. Například někdo, kdo potřebuje vytisknout jednu stránku s poznámkami, zřejmě nebude zrovna nadšený, když uvízne ve frontě za tiskovou úlohou, která svým rozsahem odpovídá románu *Vojna a mír*.

Pokud více tiskáren sdílí jeden ovladač, můžete takové tiskárny přiřadit do fondu tiskáren, který se uživatelům jeví jako jediná tiskárna. Výhodou použití fondu tiskáren je, že klienti jednoduše tisknou na jediné logické tiskárně nainstalované na tiskovém serveru, která poté odešle tiskovou úlohu první dostupné tiskárně. Pokud jedna tiskárna ve fondu tiskáren přejde do režimu offline, systém Windows odešle tiskové úlohy na jiné tiskárny ve fondu tiskáren, čímž sníží prostoje uživatelů. Fondy tiskáren rovněž zjednodušují správu, neboť všechny tiskárny spravujete ve fondu tiskáren s jednou logickou tiskárnou; pokud změníte vlastnosti jediné logické tiskárny, všechny fyzické tiskárny ve fondu tiskáren převezmou stejná nastavení.

Poznámka: Do fondu tiskáren umístěte fyzické tiskárny, které jsou vzájemně blízko, abyste snadno našli dokončenou tiskovou úlohu.

Chcete-li nastavit fond tiskáren, postupujte podle následujících kroků:

1. V nástroji Správa tisku (Print Management) klepněte pravým tlačítkem myši na logické tiskárně, na níž chcete povolit fondy tiskáren, a zvolte příkaz Vlastnosti (Properties).
2. Klepněte na kartu Porty (Ports).
3. Zaškrtněte políčko Umožnit fondy tiskáren (Enable Printer Pooling).
4. Chcete-li přidat další tiskárnu do fondu tiskáren, vyberte port, k němuž je daná tiskárna připojena.

   Pokud se jedná o síťovou tiskárnu a vy jste ji ještě nepřidali na tiskový server, klepnutím na tlačítko Přidat port (Add Port) přidejte pro danou tiskárnu nový port tiskárny Standard TCP/IP. (Další informace najdete v části „Instalace tiskáren“ dříve v této kapitole.)
5. Chcete-li změnit nastavení opakování přenosu pro daný port, vyberte port a klepněte na tlačítko Konfigurovat port (Configure Port).

Poznámka: Všechny tiskárny ve fondu tiskáren musí být schopny použít stejný ovladač tiskárny – pokud do fondu tiskáren přidáte nekompatibilní tiskárnu, dokument se nemusí správně vytisknout.

Příprava na chybu tiskového serveru

V případě, že je to vůbec možné, je rozumné mít druhý tiskový server pro zálohu primárního tiskového serveru. Pokud primární tiskový server selže, správce může uživatelům odeslat e-mail s pokyny, aby k tisku použili například server NahradniServer2. Tato možnost je pro správce nejjednodušším řešením, ale pro některé uživatele bude připojení k jiné tiskárně představovat problém. Pokud jste naplánovali odstavení tiskového serveru, můžete pomocí nástroje Správa tisku (Print Management) nainstalovat na záložní server připojení tiskáren a odebrat připojení k serveru, který je v režimu offline. Vytvořte alias na záložní tiskový server, aby klienti viděli záložní server místo primárního serveru. Záložní tiskový server musí být připojen ke stejným síťovým tiskárnám jako primární tiskový server a musí používat stejné názvy sdílených položek. Ke zkopírování konfigurace primárního serveru na záložní server použijte průvodce Migrace tiskárny (Print Migration Wizard). (Viz část „Použití průvodce Mirace tiskárny“ (Print Migration Wizard) dříve v této kapitole.) Pro přepnutí uživatelů postupujte podle následujících kroků:

1. Otevřete Editor registru (Registry Editor) (Regedit.exe) a najděte následující klíč registru:

   ```
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\
   Parameters
   ```

2. Vytvořte novou řetězcovou hodnotu s názvem **OptionalNames** a jako údaj hodnoty zadejte název primárního serveru.
3. Vytvořte novou hodnotu DWORD s názvem **DisableStrictNameChecking** a jako údaj hodnoty zadejte **1**.

Důležité: Hodnota registru DisableStrictNameChecking umožňuje všem uživatelům vnitřní sítě použít parametr *OptionalNames* k zosobnění počítače, třebaže by bylo rozlišení názvu nespolehlivé, pokud by zosobňující uživatel „nenakazil" také server DNS a/nebo WINS.

4. Vytvořte záznam DNS typu Alias (CNAME) mapující název DNS primárního serveru na název DNS záložního serveru.
5. Pokud v síti používáte službu WINS, vytvořte rezervaci DHCP pro záložní tiskový server, aby se jeho adresa IP nezměnila, a poté vytvořte nové statické mapování ve službě WINS, které bude mapovat název NetBIOS primárního tiskového serveru na IP adresu záložního tiskového serveru. (Další informace o správě služeb WINS, DHCP a DNS najdete v kapitole 18, „Správa protokolu TCP/IP".)
6. Restartujte server.
7. Chcete-li primární tiskový server přepnout zpět do režimu online, odstraňte nové hodnoty v registru, alias DNS a registraci ve službě WINS a poté restartujte server.

Poznámka: Pokud tiskárna na tiskovém serveru selže, ale server samotný nikoliv, můžete snadno přesunout uživatele na jinou tiskárnu, která umí použít stejný ovladač tiskárny. (Nové tiskárny ve stejné modelové řadě často dokáží použít stejný ovladač.) Pokud tak chcete učinit, klepněte pravým tlačítkem na tiskárně, zvolte příkaz Vlastnosti (Properties), klepněte na kartu Porty (Ports) a poté vyberte port tiskárny, na kterou chcete přesměrovat uživatele nefunkční tiskárny. Tento port může být místním portem, síťovým portem nebo sdílenou tiskárnou na jiném tiskovém serveru. Rovněž můžete vytvořit fond tiskáren pro automatické převzetí tiskových úloh jedné tiskárny jinou tiskárnou, která používá stejný ovladač. Pokud vaše síť vyžaduje mimořádně vysokou úroveň tiskového výkonu a spolehlivosti, nastavte cluster tiskového serveru. Ten poskytuje další kapacitu a automatické zabezpečení před selháním by mělo zabránit tomu, aby server přestal reagovat. Další informace o správě clusterů najdete v kapitole 21, „Použití clusterů".

Řešení problémů s tiskárnami

Při řešení problémů s tiskem, stejně jako při řešení jakýchkoli jiných problémů, je nejprve třeba problém izolovat a přijít na jeho příčiny a teprve poté je možné určit možný způsob nápravy. Tato část vám pomůže diagnostikovat problémy při tisku, pomůže vám najít tiskový subsystém, v němž chyba nastala, a nabídne některé konkrétní postupy pro řešení daného problému.

Problémy na straně serveru

Problémy s tiskem obvykle spadají do některé z následujících kategorií:

Fyzické problémy

Patří sem problémy se samotnou tiskárnou a s připojeními, tedy například zaseknuté papíry, nedostatek toneru nebo inkoustu atd.

Problémy s tiskovým serverem

Patří sem problémy s ovladači tiskárny, úrovněmi oprávnění a stav softwaru.

Problémy s připojením k síti

Sem patří komunikační chyby mezi servery a klienty pramenící z nesprávného nastavení protokolů nebo sítě. (Tyto problémy řešte buď na straně klienta, nebo na straně serveru, podle toho, kde se problém s připojením vyskytl.)

Problémy s klienty

Patří sem problémy s ovladači tiskárny, oprávněními a aplikacemi.

Je-li to možné, nejprve určete, ve které kategorii se daný problém nachází. Často můžete problém odstranit ze serveru a vyhnout se cestě ke klientskému počítači. To je mimořádně žádoucí v případě, že klientský počítač a tiskárna jsou několik podlaží, nebo dokonce několik budov vzdáleny. Vyzkoušejte alternativy, dokud problém co nejpřesněji neizolujete, a poté použijte nejčastější opravy, dokud problém neodstraníte. Pokud už víte, kde se problém nachází, přejděte rovnou k odpovídajícímu nadpisu v této části.

Další informace: Pokud nemůžete vyřešit problémy pomocí zde uvedených informací, použijte znalostní bázi Microsoft Knowledge Base na webových stránkách společnosti Microsoft na adrese *http://support.microsoft.com*.

Dokument se vytiskne nesprávně

Pokud se dokument vytiskne, ale je nečitelný nebo obsahuje jiné defekty, mezi klientem, ovladačem tiskárny a tiskárnou existuje problém s kompatibilitou. Ujistěte se, že klient používá správný klientský ovladač tiskárny a že server používá správný ovladač tiskárny. Pokud klient používá edici x64 systému Windows, obstarejte si nativní verzi x64 ovladače tiskárny pro konkrétní model používané tiskárny, místo abyste používali ovladač tiskárny napsaný pro podobný model.

Nainstalujte kopii logické tiskárny, abyste otestovali, zda je ovladač tiskárny poškozen. Pokud v tomto problém není, změňte nastavení zařazování u ovladače klienta. Pokud má stejný problém více klientů, změňte ovladač tiskárny na serveru. Přesněji řečeno, změňte následující možnosti na kartě Upřesnit (Advanced) dialogu s vlastnostmi tiskárny. (Podrobnější postup naleznete v části „Změna zařazování tisku tiskárnou“ dříve v této kapitole.)

- Abyste se ujistili, že při začátku tisku je pro tiskárnu dostupný celý dokument, zvolte možnost Zahájit tisk po zařazení poslední stránky (Start Printing After Last Page Is Spooled).

- Pokud i nadále máte problémy s tiskem, volbou možnosti Tisknout přímo na tiskárnu (Print Directly To The Printer) vypněte zařazování. Tento krok způsobí snížení výkonu na serveru.
- Zrušením zaškrtnutí políčka Zapnout vylepšené vlastnosti tisku (Enable Advanced Printing Features) na tiskovém serveru vypněte zařazování souboru ve formátu EMF, které znepřístupní některé možnosti tiskárny, například pořadí stránek, tisk brožury a počet stránek na list (pokud tyto možnosti tiskárna nabízí).

Poznámka: Pokud má tiskárna více zásobníků s různými formuláři, přidružte formulář k zásobníku, aby se dokumenty používající daný formulář vždy správně vytiskly. Pod nadpisem Formulář k přidružení zásobníku (Form To Tray Assignment) označte každý zásobník a vyberte formulář, který se k danému zásobníku přidruží. Pokud tiskárna podporuje funkci Page Protection a má k dispozici 1 MB nebo více volitelné paměti, klepněte na kartu Nastavení zařízení (Device Settings) a zvolte tuto možnost, čímž zajistíte, že se složité stránky správně vytisknou. Pokud tuto možnost zvolíte, tiskárna před začátkem tisku vytvoří každou stránku v paměti.

Tisk dokumentu selže

Pokud se dokument vůbec nevytiskne, postupně vyzkoušejte následující možnosti řešení problému:

- Pokud je z informace o chybě zřejmé, že vhodný ovladač tiskárny nelze stáhnout, nainstalujte na tiskový server ovladače tiskárny, které odpovídají operačnímu systému a architektuře procesoru klientského počítače. (Další informace naleznete v části „Správa ovladačů tiskárny“ výše v této kapitole.)
- Chyba informující o tom, že tiskové zařízení bylo nedostupné, může naznačovat problém s připojením k síti nebo uživatel nemusí mít oprávnění Tisk (Print) k dané tiskárně. (Další informace naleznete v části „Nastavení možností zabezpečení“ výše v této kapitole.)
- Pokud zaznamenáte mnoho přístupů na disk a tisk dokumentu selže, zkontrolujte, zda jednotka obsahující klientskou složku pro zařazování obsahuje dostatek volného místa na disku pro uložení zařazovaného dokumentu. (Další informace naleznete v části „Změna zařazování tisku tiskárnou“ výše v této kapitole.)
- Zjistěte, zda můžete tiskový server po síti zobrazit a připojit se k němu. Zkopírujte soubor na tiskový server, abyste zjistili, zdali můžete k tiskovému serveru přistupovat. (Obecně lze říci, že pokud nemáte k tiskovému serveru přístup, nemůžete přistupovat k žádné připojené tiskárně.)
- Vytiskněte testovací dokument z aplikace Poznámkový blok (Notepad) společnosti Microsoft. Pokud lze vytisknout dokument z této aplikace, ovladače tiskárny jsou správné a problém je pravděpodobně v aplikaci.
- Pokud nelze tisknout z aplikace Poznámkový blok (Notepad), zkuste tisknout na příkazovém řádku zadáním následujícího příkazu: `echo test> [nazev_portu_tiskarny]`, kde *nazev_portu_tiskarny* je název sdílené síťové tiskárny.

Tisk z konkrétní aplikace selže

Některé aplikace mohou mít problémy při tisku z prostředí systému Windows. Mezi některé z problémů, s nimiž se můžete setkat, patří:

- Chybová zpráva „Přístup odepřen“ při konfiguraci tiskárny z aplikace se zobrazí, pokud nemáte dostatečná oprávnění ke změně konfigurace tiskárny. K provedení změn pokročilého nastavení tiskárny potřebujete mít oprávnění Správa tiskáren (Manage Printers).
- Pokud program pro systém MS-DOS netiskne, program ukončete. Některé programy pro systém MS-DOS netisknout, dokud je neukončíte. Rovněž použijte příkaz `net use` k namapování místního portu na sdílenou tiskárnu. (Další informace najdete ve článku znalostní báze Microsoft Knowledge Base 314499 na webových stránkách společnosti Microsoft na adrese *http://support.microsoft.com/kb/314499*.)

Další informace: V případě jiných problémů nahlédněte do souboru Printer.txt na instalačním disku CD-ROM pro klientský operační systém, jedná-li se o systém Windows 2003, Windows XP nebo Windows 2000. Rovněž můžete nahlédnout do znalostní báze Microsoft Knowledge Base na adrese *http://support.microsoft.com*.

Odstranění uvíznutých dokumentů

Pokud se dokumenty nevytisknou nebo se vám nedaří odstranit dokumenty v tiskové frontě, zařazování tisku se může zastavit. To rovněž ovlivní všechny faxové služby běžící na serveru. Chcete-li restartovat Službu zařazování tisku (Print Spooler), postupujte podle následujících kroků:

1. Spusťte Správce serveru (Server Manager). Ve stromu konzoly vyberte položku Konfigurace (Configuration) a poté položku Služby (Services).
2. Klepněte pravým tlačítkem myši na odkaz Služba zařazování tisku (Print Spooler) v pravém podokně a zvolte příkaz Restartovat (Restart).
3. Dále je třeba určit proces obnovení, který se má provést v případě, že Služba zařazování tisku (Print Spooler) selže. To provedete poklepáním myší na položce Služba zařazování tisku (Print Spooler) a klepnutím na kartu Zotavení (Recovery). Klepněte na akci, kterou chcete provést, u možností První selhání (First Failure), Druhé selhání (Second Failure) a Další selhání (Subsequent Failures) a poté klepněte na tlačítko OK.
4. Chcete-li zobrazit služby (například Vzdálené volání procedur), na kterých je zařazování tisku závislé, poklepejte myší na Službě zařazování tisku (Print Spooler) a poté klepněte na kartu Závislosti (Dependencies). Tuto kartu můžete rovněž použít k zobrazení služeb, které závisí na správném fungování zařazování tisku.

Poznámka: Chcete-li restartovat zařazování tisku na příkazovém řádku, zadejte příkaz `net stop "print spooler"` a poté příkaz `net start "print spooler"`.

Zkontrolujte stav tiskového serveru

Stav tiskového serveru můžete zkontrolovat vzdáleně. Ke kontrole stavu tiskového serveru použijte následující seznam:

- Zkontrolujte, zda nedošlo k uvíznutí dokumentu nebo k chybovým zprávám v tiskové frontě nebo na webové stránce konfigurace tiskárny (pokud existuje). Pokud v tiskárně není papír nebo je v ní nedostatek toneru nebo pokud došlo k zaseknutí papíru, často se zde objeví chybová zpráva.
- Zkontrolujte, zda na jednotce, která obsahuje složku pro zařazování, je dostatek volného místa na disku.
- Pokud se dokument vytiskne nečitelný, tiskárna může používat špatný datový typ (EMF nebo RAW). Zkuste tento problém vyřešit použitím datového typu RAW. Zrušte zaškrtnutí políčka Zapnout vylepšené vlastnosti tisku (Enable Advanced Printing Features) na kartě Upřesnit (Advanced) dialogu s vlastnostmi tiskárny. (Další informace najdete v části „Změna zařazování tisku tiskárnou“ dříve v této kapitole.)
- Zjistěte, zda se vůbec nějaké dokumenty mají vytisknout. Pokud se v tiskové frontě nenachází žádné dokumenty, vytiskněte z tiskového serveru zkušební stránku nebo dokument, abyste zjistili, zda tiskový server tiskne správně.
- Pokud se některé dokumenty v tiskové frontě nevytisknou a vy je nemůžete odstranit, služba zařazování tisku se mohla zaseknout. Restartujte Službu zařazování tisku (Print Spooler), abyste zjistili, zda tím problém vyřešíte. Přidejte další logickou tiskárnu (ovladač tiskárny) pro danou tiskárnu, abyste vyloučili možnost poškozeného ovladače tiskárny

Poznámka: Abyste zabránili pomalému tisku dokumentů v určitých jazycích, nainstalujte na tiskových serverech fonty pro všechny jazyky, které budou klienti k tisku používat. To provedete zkopírováním fontů do složky %WINDIR%\Fonts na tiskovém serveru a otevřením složky Fonts (nebo restartováním serveru).

Problémy na straně klienta

Pokud není problém na tiskovém serveru, pokračujte na straně klientského počítače a tiskárny.

Problémy s tiskem z klientského počítače

Vyzkoušejte tisk z klientského počítače a všimněte si chybových zpráv. Tyto zprávy často odhalí příčinu problému nebo alespoň naznačí některé možnosti. Pokud se dokument vytiskne správně, může jít o prostou uživatelskou chybu. Jinak by mohl být problém s konkrétním programem nebo v kompatibilitě s ovladačem tiskárny.

Zkontrolujte tiskárnu

Pokud jste vyloučili klienty i server jako zdroj problému, ale stále nemůžete na tiskárně vytisknout žádné dokumenty, zaměřte se na tiskárnu. Pozastavte tiskovou frontu a poté zkontrolujte samotnou tiskárnu. Ohlašuje tiskárna nějaké chyby? Pokud zjistíte zasek-

nutí papíru nebo pokud je v tiskárně nedostatek toneru nebo tiskárna vyžaduje údržbu, tiskárna obvykle ohlásí chybovou zprávu. Zkontrolujte, že svítí kontrolka stavu připravenosti nebo zapnutí a že kabel tiskárny je správně připojen nebo že síťový kabel j správně připojen a že indikační dioda vedle síťového portu svítí (pokud se na adaptéru nachází).

Pokud na tiskárně stále není možno tisknout, vytiskněte zkušební stránku přímo z tiskárny. Většina tiskáren tuto možnost nabízí. Pokud se zkušební stránka vytiskne, proveďte konfiguraci tiskárny na jiném tiskovém serveru. Pokud z jiného tiskového serveru bude možné tisknout, problém je v původním tiskovém serveru. Ke zjištění adresy IP tiskárny použijte program Ping.exe.

Shrnutí

Téměř všechny sítě vyžadují komplexní a spolehlivé tiskové služby. Kromě chyby sítě nebo ztráty přístupu k Internetu není nic příčinou tolika obav a frustrací jako nemožnost tisku. Splnění požadavků na současný tisk a současně příprava na rozšíření a změny jsou zásadními faktory při vymýšlení životaschopné strategie tisku. V další kapitole se zaměříme na další kritickou oblast, jíž je správa skupin a uživatelských účtů.

KAPITOLA 11

Správa uživatelů a skupin

Počítačové sítě jsou dnes tak rozšířené, že je bereme již takřka za samozřejmost. A jen tehdy, pokud přestanou pracovat, si toho někdo všimne. A že si lidé všímají! Panické a zoufalé výkřiky lze v takovou chvíli slyšet na míle daleko, protože hlavní úlohou sítě je poskytovat uživatelům vše, co potřebují, a naopak jim odklízet z cesty vše, co by jim mohlo překážet v práci. Mezi to, co uživatelé potřebují, patří přístup k souborům, aplikacím, tiskárnám a připojení k Internetu, které jsou pro jejich práci nezbytné. Co nepotřebují, jsou potíže jakéhokoli druhu s přístupem k těmto prostředkům.

Správce sítě má další požadavky, např. ochranu materiálů, které nemusí znát každý, před těmi, kteří tyto informace znát nemusejí, ochranu sítě před uživateli se zlými úmysly nebo před uživateli nebezpečnými jiným způsobem, a ochranu uživatelů, aby neuškodili sami sobě. Abyste mohli uspět při plnění všech těchto úkolů, je důležité, abyste se seznámili s konfigurací organizačních jednotek, skupin, uživatelů a zásad skupiny. Tato témata jsou náplní této a následující kapitoly.

Principy skupin

Podle definice jsou skupiny v produktech řady Microsoft Windows Server 2008 objekty adresářové služby Active Directory Domain Service nebo místního počítače, které obsahují uživatele, kontakty, počítače či jiné skupiny. Obecně je však skupina obvykle kolekcí uživatelských účtů. Cílem skupin je zjednodušit správu, a to tak, že správci sítě mohou přiřazovat práva a oprávnění skupinám, a nikoli pouze jednotlivým uživatelům.

Systém Windows Server 2008 nabízí dva typy skupin: skupiny zabezpečení a distribuční skupiny. Téměř všechny skupiny používané systémem Windows 2008 Server jsou *skupinami zabezpečení*, protože oprávnění lze přiřazovat pouze prostřednictvím těchto skupin. Každé skupině zabezpečení je také přiřazen *rozsah skupiny*, jenž definuje způsob přiřazování oprávnění členům skupiny. Programy, které mohou službu Active Directory prohledávat, mohou skupiny zabezpečení používat i pro účely, které se zabezpečením spojeny nejsou, např. pro odeslání e-mailové zprávy skupině uživatelů. *Distribuční skupiny* funkci zabezpečení neplní a lze je používat pouze s e-mailovými aplikacemi k odesílání e-mailových zpráv většímu počtu uživatelů.

V pozdějších částech kapitoly naleznete části věnované uživatelským právům a způsobu, jak se definují a jak se přiřazují skupinám. Dvanáctá kapitola (Správa souborových prostředků) na toto téma navazuje popisem oprávnění a způsobu, jakým se přiřazují.

Přiřazení rozsahů skupin

Když je skupina vytvářena, je jí přiřazen rozsah skupiny, který následně definuje, jak jsou skupině přiřazována oprávnění. Tři možné rozsahy skupiny – globální, místní doménová a univerzální – jsou definovány v následujících oddílech.

Globální rozsah

Skupina s globálním rozsahem je skutečně globální v to smyslu, že jí lze přidělovat oprávnění k prostředkům umístěným v libovolné doméně. Nicméně členové mohou pocházet pouze z domény, v níž byla skupina vytvořena, a z tohoto pohledu skupina globální není. Do globálních skupin je nejlepší umisťovat adresářové objekty vyžadující častou údržbu, například uživatelské účty a účty počítačů. Globální skupiny mohou být členy univerzálních a místních doménových skupin v libovolné doméně a mohou mít tyto členy:

- jiné globální skupiny v téže doméně,
- individuální účty z téže domény.

Místní doménový rozsah

Místní doménová skupina je opakem globální skupiny – její členové mohou pocházet z libovolné domény, avšak jejím členům lze přiřadit oprávnění pouze pro prostředky v doméně, v níž je skupina vytvořena. Členové místní doménové skupiny často potřebují přistupovat k určitým prostředkům v konkrétní doméně. Místní doménové skupiny mohou mít jednoho či více členů z následujícího seznamu:

- jiné místní doménové skupiny v téže doméně,
- globální skupiny z libovolné domény,
- univerzální skupiny z libovolné domény,
- individuální účty z libovolné domény.
- libovolná kombinace výše uvedených členů.

Univerzální rozsah

Univerzální skupina zabezpečení může mít členy z libovolné domény a mohou jí být přiřazena oprávnění k prostředkům v libovolné doméně. Univerzální skupiny mohou mít následující členy pocházející z libovolné domény:

- další univerzální skupiny,
- globální skupiny,
- individuální účty.

Pomocí skupin s univerzálním rozsahem konsolidujte skupiny, které se rozprostírají přes více domén. To můžete provést tak, že účty přidáte do skupin s globálním rozsahem a tyto skupiny vložíte do skupin s univerzálním rozsahem. Univerzální skupiny musejí být používány s rozvahou, jelikož mohou mít negativní dopad na výkon sítě, jak je popsáno v poznámce s názvem Jak skupiny ovlivňují výkon sítě.

Jak skupiny ovlivňují výkon sítě

Důležitost plánování skupin vystoupí daleko více do popředí, pokud uvážíte negativní vliv, jaký může mít organizace skupin na výkon sítě. Když se uživatel přihlašuje k síti, řadič domény určuje, do jakých skupin uživatel patří, a přiřadí uživateli token zabezpečení. Součástí tokenu zabezpečení jsou kromě ID uživatelského účtu i identifikátory zabezpečení (SID) všech skupin, do nichž uživatel náleží. Počet skupin zabezpečení, do kterých uživatel patří, má přímý vliv na dobu, kterou trvá sestavení tokenu a proces přihlášení uživatele.

Kromě toho je token zabezpečení po sestavení odesílán do každého počítače, k němuž uživatel přistupuje. Cílový počítač porovnává všechny identifikátory SID v tokenu s oprávněními ke všem dostupným sdíleným prostředkům v počítači. Pokud velký počet uživatelů přistupuje k velkému počtu sdílených prostředků (včetně jednotlivých složek), může toto zpracování zabírat velký rozsah šířky pásma a trvat dlouhou dobu. Jedno z řešení spočívá v omezení členství ve skupinách zabezpečení. Pro kategorie uživatelů, které nevyžadují konkrétní oprávnění či práva, používejte distribuční skupiny.

Skupiny s univerzálním rozsahem mají negativní vliv na výkon i samy o sobě, jelikož všechny tyto skupiny jsou společně se svými členy uvedeny v globálním katalogu. Pokud je třeba změnit členství ve skupině s univerzálním rozsahem, musí být tato změna přenesena do každého serveru globálního katalogu ve stromu domén, což zvyšuje potřebu replikačních přenosů v síti. V globálním katalogu jsou také uvedeny skupiny s globálním rozsahem a rozsahem místní domény, nikoli však jejich jednotliví členové, takže řešením je omezit členství univerzálních skupin především na globální skupiny.

Plánování organizačních jednotek

Organizační jednotky (OJ) jsou, jak jejich název naznačuje, nástroje pro organizaci kolekcí objektů v rámci domény. Organizační jednotka může obsahovat libovolnou kolekci objektů služby Active Directory, např. tiskárny, počítače, skupiny, nebo i jiné organizační jednotky.

Překročí-li složitost domény určitou mez, spočívá jedno z možných řešení v rozdělení domény do několika domén. Organizační jednotky poskytují alternativní strukturu správy,

která je však podstatně pružnější. Mohou být v doméně hierarchicky uspořádány a řízení správy může být delegováno pro funkce v jediné OJ nebo pro celý podstrom organizačních jednotek. (Organizační jednotka je nejmenší entitou, které lze delegovat řízení správy nebo přiřadit nastavení zásad skupiny.) Přitom organizační jednotky lze snadno upravovat, přesouvat, přejmenovávat, a dokonce i odstraňovat. Další výhodou je, že podstrom organizačních jednotek na rozdíl od domény nevyžaduje samostatný řadič domény.

Organizační jednotky nebo nová doména?

Bohužel neexistuje pevné pravidlo, podle kterého by bylo možné rozhodnout, kdy má být rozrůstající se síť rozdělena do samostatných domén a kdy stačí vytvořit jen nové organizační jednotky. Pokud se ve vaší síti vyskytuje některá z níže uvedených situací, může být řešením vytvoření několika domén:

- Je zapotřebí decentralizovat správu.
- Síť zahrnuje soupeřící obchodní jednotky nebo podniky se společnou majetkovou účastí (joint ventures).
- Části sítě jsou odděleny velmi pomalými připojeními (například analogovými modemy), takže by úplná replikace zapříčinila vážné přenosové problémy. (Pokud je připojení pouze pomalé, můžete použít několik lokalit uvnitř jedné domény, protože replikace není tak častá.)
- Jsou vyžadovány různé zásady účtů. Jelikož jsou zásady účtů uplatňovány na úrovni domény, mohou velké rozdíly v požadovaných zásadách ospravedlnit zavedení samostatných domén.

V následujících situacích je naopak vhodné použít organizační jednotky:

- Je vyžadována soustředěná nebo přísně řízená správa.
- Struktura organizace vyžaduje uspořádání síťových objektů do samostatných kontejnerů.
- Struktura, kterou chcete rozdělit, se pravděpodobně v určitém okamžiku změní.

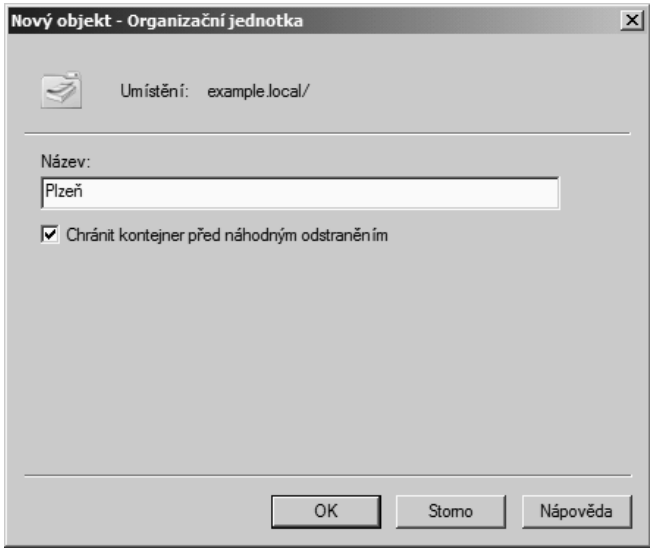
Obecně tedy lze říci, že pokud situace vyžaduje pružnou, či dokonce proměnlivou strukturu, vyplatí se vytvářet organizační jednotky.

Organizační jednotky jsou pouze kontejnery. Neudělují členství a nejsou registrovanými objekty zabezpečení. Práva a oprávnění jsou uživatelům udělována prostřednictvím členství ve skupinách. Po vytvoření skupin použijte organizační jednotky nebo uspořádejte skupinové objekty a přiřaďte nastavení zásad skupiny. Použití zásad skupiny je popsáno v kapitole 13 (Zásady skupiny).

Vytvoření organizačních jednotek

Organizační jednotky v doménové struktuře vystupují jako složky a jejich vytváření je snadné. Organizační jednotku vytvořte následovně:

1. V nabídce Nástroje pro správu (Administrative Tools) vyberte položku Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).
2. Pravým tlačítkem myši klepněte na doménu a vyberte příkaz Nová položka (New) a poté příkaz Organizační jednotka (Organizational Unit). Otevře se dialog uvedený na obrázku 11.1.



Obrázek 11.1: Vytvoření nové organizační jednotky

3. V dialogu Organizační jednotka (Organizational Unit) zadejte název jednotky a klepněte na tlačítko OK.

Poznámka: Políčko Chránit kontejner před náhodným odstraněním (Protect This Container From Accidental Deletion) je ve výchozím nastavení zaškrtnuté. Tato možnost aktualizuje popisovač zabezpečení objektu a případně i jeho nadřazeného objektu takovým způsobem, že odepře uživatelům této domény a tohoto řadiče domény možnost odstranit tento objekt. Nechrání však před náhodným odstraněním podstromu obsahujícího chráněný objekt. Objekt tedy můžete lépe ochránit tak, že tuto možnost nastavíte všem kontejnerům obsahujícím tento chráněný objekt až na úroveň hlavy názvového kontextu domény.

Přesouvání organizačních jednotek

Jednou z nejdůležitějších vlastností organizačních jednotek je, že mohou být přesouvány z jednoho kontejneru do druhého, a dokonce i z jedné domény do druhé. Organizační jednotku přesuňte následovně:

1. V nabídce Nástroje pro správu (Administrative Tools) vyberte položku Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).
2. Pravým tlačítkem myši klepněte na organizační jednotku, která má být přesunuta, a v místní nabídce vyberte příkaz Přesunout (Move).
3. V dialogu Přesunout (Move) vyberte nové umístění organizační jednotky a klepněte na tlačítko OK.

Důležité: Přesouvání organizačních jednotek je v systému Windows Server 2008 jednoduché, ale přesouvání organizačních jednotek s připojenými objekty zásad skupiny může mít nečekané následky. Pečlivě zvažte dopady přesunutí organizační jednotky na celkový návrh vašich zásad skupiny a po přesunutí ověřte výsledné chování.

Odstranění organizačních jednotek

Organizační jednotky lze také velmi snadno odstranit. Při odstraňování organizační jednotky nicméně buďte opatrní, protože odstraněn bude i obsah organizační jednotky. To znamená, že pokud budete jednat příliš spěšně, můžete nedopatřením odstranit veškeré účty prostředků a uživatelů obsažené v organizační jednotce. Organizační jednotku odstraňte následovně:

1. V nabídce Nástroje pro správu (Administrative Tools) vyberte položku Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).
2. Pravým tlačítkem myši klepněte na organizační jednotku a vyberte příkaz Odstranit (Delete).
3. Potvrďte odstranění – klepněte dvakrát za sebou na tlačítko Ano (Yes).

Plánování strategie použití skupin

Prozkoumáte-li síť a různé typy skupin a poté si přimyslíte konkrétní požadavky, nezřídka skončíte s pocitem, že pracujete na nějaké pekelné logické hádance: Klára žije v modrém domě, Lenka sbírá známky, Petr řídí dodávku a Karel jí sýr. Který z nich má zrzavé vlasy? Přesto je zde plánování, stejně jako u mnoha jiných aspektů týkajících se správy sítě, základním krokem.

Stanovení názvů skupin

Během plánování skupin určete schéma pojmenovávání vhodné pro vaši organizaci. Měli byste zvážit dva faktory:

- **Názvy skupin musejí být okamžitě rozpoznatelné** – správci prohledávající službu Active Directory by neměli být nuceni hádat, co názvy znamenají.
- **Srovnatelné skupiny musí mít podobné názvy** – jinými slovy: pokud existuje v každé doméně skupina konstruktérů, zadejte všem skupinám analogické názvy, např. Konstrukce Praha, Konstrukce Brno, Konstrukce BBystrica.

Použití globálních skupin a místních doménových skupin

Vypracujte strategii používání různých skupin. Například uživatelé se společnou pracovní odpovědností budou patřit do globální skupiny. Uživatelské účty pro všechny grafiky byste tedy měli přidat do globální skupiny s názvem Grafici. Ostatní uživatelé se společnými požadavky budou přiřazeni do jiných globálních skupin. Poté musíte identifikovat prostředky, ke kterým uživatelé potřebují přístup, a vytvořit pro tyto prostředky místní doménovou skupinu. Jestliže máte například k dispozici několik barevných tiskáren a plotrů používaných v určitých odděleních, můžete vytvořit místní doménovou skupinu s názvem Tiskárny_a_plotry.

Dále rozhodněte, které globální skupiny potřebují přístup k označeným prostředkům. Budeme-li pokračovat v příkladu, do místní doménové skupiny Tiskárny_a_plotry přidáte globální skupinu Grafici a také všechny ostatní globální skupiny, které k těmto

tiskárnám a plotrům potřebují přístup. Oprávnění k používání prostředků ve skupině Tiskárny_a_plotry jsou přiřazena místní doménové skupině Tiskárny_a_plotry.

Mějte na paměti, že globální skupiny mohou v prostředích s více doménami komplikovat správu. Globálním skupinám z různých domén musejí být oprávnění přidělována individuálně. Také platí, že přiřadíte-li uživatele do místních doménových skupin a udělíte-li oprávnění těmto skupinám, neposkytnete tím jejich členům přístup k prostředkům mimo doménu.

Použití Univerzálních skupin

Při použití univerzálních skupin mějte na paměti následující pravidla:

- Dbejte na to, aby do univerzálních skupin nebyly přidávány jednotlivé účty, omezíte tím replikační přenosy.
- Chcete-li členům globálních skupin z více domén poskytnout přístup k prostředkům ve více doménách, přidejte tyto globální skupiny do univerzálních skupin.
- Univerzální skupiny mohou být členy místních doménových skupin a jiných univerzálních skupin, ale nemohou být členy globálních skupin.

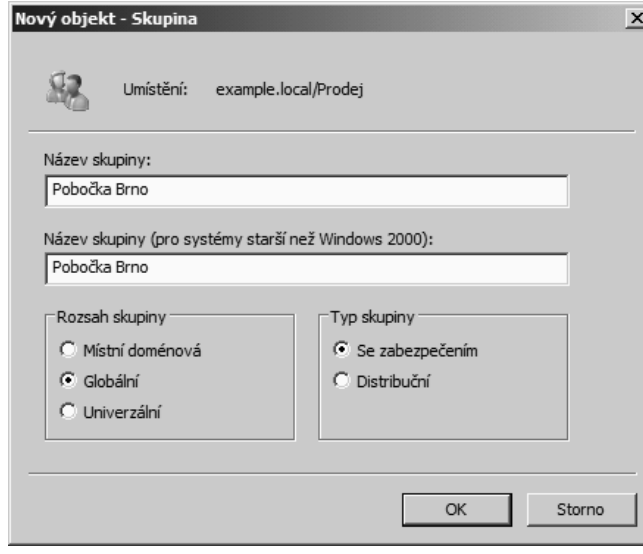
Implementace strategie použití skupin

Po naplánování strategie a jejím ověření pomocí různých scénářů jste připraveni začít s jejím budováním.

Vytvoření skupin

Skupiny je možné vytvářet a odstraňovat pomocí nástroje Uživatelé a počítače služby Active Directory. Skupiny vytvořte v kontejneru Users nebo v organizační jednotce vytvořené pro skupiny. Chcete-li vytvořit skupinu v organizační jednotce Prodej, postupujte následovně:

1. V nabídce Nástroje pro správu (Administrative Tools) vyberte položku Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).
2. Rozbalte doménu, ve které chcete skupinu vytvořit.
3. Pravým tlačítkem myši klepněte na kontejner Prodej, přejděte na příkaz Nová položka (New) a v místní nabídce zvolte příkaz Skupina (Group). Zobrazí se dialog znázorněný na obrázku 11.2.
4. Vyplňte požadované údaje:
   - Název skupiny musí být v doméně jedinečný.
   - Název skupiny v té podobě, v jaké je viditelný pro systémy starší než Windows 2000, je vyplňován automaticky. Mějte na paměti, že operační systémy starší než Windows 2000 již nejsou podporovány, ale přesto na ně lze ještě v některých situacích narazit.
   - Ve skupinovém rámečku Rozsah skupiny (Group Scope) klepněte na přepínač Místní doménová (Domain local), Globální (Global) nebo Univerzální (Universal).



Obrázek 11.2: Vytvoření nové místní skupiny

- Ve skupinovém rámečku Typ skupiny (Group Type) klepněte na přepínač Se zabezpečením (Security) nebo Distribuční (Distribution).

5. Nakonec klepněte na tlačítko OK. Nová skupina se zobrazí v organizační jednotce Prodej. Možná bude před přidáním členů do skupiny nutné několik minut vyčkat, než dojde k její replikaci do globálního katalogu.

Poznámka: Na skupiny vytvářené přímo v kontejneru Users (výchozí chování) nelze používat zásady skupiny. Pokud použijete organizační jednotky a své skupiny uspořádáte do nich, budete moci mnohem lépe řídit, jak budou zásady skupiny používány.

Odstraňování skupin

Nevytvářejte skupiny, které nejsou potřeba, a pokud již skupiny nejsou nezbytné, co nejdříve je ze systému odstraňte. Nepotřebné skupiny představují riziko v zabezpečení, protože není nic snazšího, než bezděčně přidělit oprávnění tam, kde by přidělena být neměla.

Každá skupina, podobně jako každý uživatel, má jedinečný identifikátor zabezpečení (SID). Identifikátor SID je používán k identifikaci skupiny a oprávnění, která jsou jí přidělena. Při odstranění skupiny je odstraněn i identifikátor SID a víckrát již není použit. Pokud odstraníte skupinu a později se rozhodnete ji znovu vytvořit, budete muset uživatele a oprávnění nakonfigurovat stejným způsobem, jako by se jednalo o novou skupinu.

Chcete-li skupinu odstranit, klepněte v nástroji Uživatelé a počítače služby Active Directory pravým tlačítkem myši na její název a v místní nabídce zvolte příkaz Odstranit

(Delete). Odstraněním skupiny odstraníte pouze skupinu a k ní přiřazená oprávnění. Odstranění skupiny nijak neovlivní účty uživatelů, kteří jsou členy této skupiny.

Přidání uživatelů do skupiny

Po vytvoření skupiny je nutné do ní přidat členy. Jak bylo v této kapitole zmíněno již dříve, skupiny mohou obsahovat uživatele, kontakty, jiné skupiny a počítače. Členy přidejte do skupiny následovně:

1. V nabídce Nástroje pro správu (Administrative Tools) vyberte položku Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).
2. Ve stromu konzoly klepněte na kontejner obsahující objekty, které chcete přidat do skupiny.
3. Označte účty, které mají být přidány. (Pomocí kláves Shift a Ctrl můžete vybrat více účtů.)
4. Pravým tlačítkem myši klepněte na označené účty a v místní nabídce zvolte příkaz Přidat do skupiny (Add To A Group). Zobrazí se dialog Vyberte objekt typu: skupiny (Select Groups). Omezte počet výsledků vyhledávání výběrem typů a umístění objektů.
5. Zadejte název skupiny, klepněte na tlačítko Kontrola názvů (Check Names) a pak klepněte na tlačítko OK.

Uživatele můžete do skupiny přidat také jiným způsobem, a to následovně:

1. Pravým tlačítkem myši klepněte na název skupiny a vyberte příkaz Vlastnosti (Properties).
2. Klepněte na kartu Členové (Members) a poté na tlačítko Přidat (Add). Ujistěte se, že pole Typy objektů (Object Types) a Umístění (Locations) odkazují na požadované pozice.
3. Klepněte na tlačítko Upřesnit (Advanced) a poté na tlačítko Najít (Find Now). V dolním podokně se zobrazí všichni potenciální členové skupiny.
4. Označte účty, které mají být přidány, a klepněte na tlačítko OK.

Poznámka: Kontakt je účet bez zabezpečovacích oprávnění a obvykle reprezentuje externí uživatele pro účely elektronické pošty. Není možné se připojit k síti jako kontakt.

Změna rozsahu skupiny

Během času možná zjistíte, že je u určité skupiny nutné změnit rozsah. Například budete chtít změnit globální skupinu na univerzální skupinu, aby součástí skupiny mohli být uživatelé z jiné domény. Typy změn, které lze u rozsahu skupiny provést, jsou však poměrně omezené a budete možná nuceni skupinu odstranit a vytvořit novou, abyste získali požadovanou konfiguraci.

Rozsah skupiny lze změnit po klepnutí pravým tlačítkem na název skupiny v nástroji Uživatelé a počítače služby Active Directory: v místní nabídce zvolte příkaz Vlastnosti (Properties), na kartě Obecné (General) proveďte nezbytné změny a poté klepněte na tlačítko OK. Pro změnu rozsahu skupiny platí následující pravidla:

- Globální skupina může být změněna na univerzální skupinu, pokud tato globální skupina není již členem jiné globální skupiny.
- Místní doménová skupina může být změněna na univerzální skupinu, pokud tato místní doménová skupina již neobsahuje jinou místní doménovou skupinu.
- Univerzální skupinu lze změnit na globální skupinu, pokud jejím členem není žádná jiná univerzální skupina.

Vytváření místních skupin

Místní skupina je kolekce uživatelských účtů v jednom počítači. Uživatelské účty v této skupině musejí být místní účty a členům místních skupin mohou být přiřazena pouze oprávnění k prostředkům v počítači, v němž byla místní skupina vytvořena.

Místní skupiny je možné vytvořit v libovolném počítači se systémem Windows Server 2000 a novějším s výjimkou řadiče domény. Obecně platí, že v počítači, který je součástí domény, by místní skupiny měly být používány střídmě. Místní skupiny se nezobrazují ve službě Active Directory, proto je nutné je spravovat samostatně v každém jednotlivém počítači. Místní skupiny lze vytvářet na konzole počítače nebo vzdáleně.

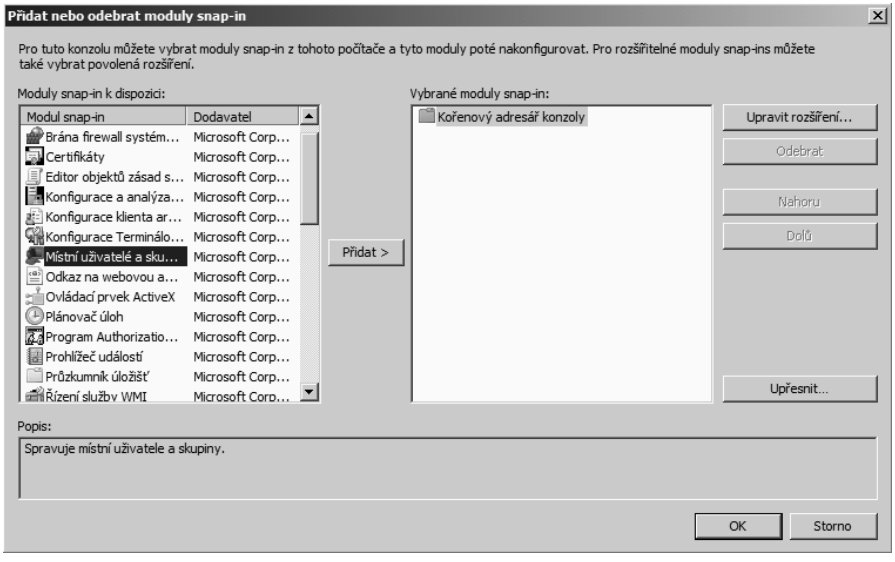
Vytvoření místní skupiny na konzole

1. V nabídce Start klepněte pravým tlačítkem myši na položku Počítač (Computer) a v místní nabídce vyberte příkaz Spravovat (Manage).
2. Ve stromu konzoly rozbalte položku Konfigurace (Configuration) a poté položku Místní uživatelé a skupiny (Local Users And Groups).
3. Pravým tlačítkem klepněte na složku Skupiny (Groups) a v místní nabídce vyberte příkaz Nová skupina (New Group).
4. V dialogu Nová skupina (New Group) zadejte název skupiny. Chcete-li, můžete zadat i popis skupiny.
5. Klepněte na tlačítko Přidat (Add) a přidejte členy do skupiny. (Členy můžete přidat nyní či později.)
6. Nakonec klepněte na tlačítko Vytvořit (Create). Nová skupina bude přidána do seznamu skupin v podokně podrobností.

Vzdálené vytvoření místní skupiny

1. Klepněte na tlačítko Start a pak klepněte na příkaz Spustit (Run). Zadejte příkaz **mmc /a** a klepněte na tlačítko OK.
2. V nabídce Soubor (File) klepněte na příkaz Přidat nebo odebrat modul snap-in (Add/Remove Snap-In).

3. V dialogu Přidat nebo odebrat moduly snap-in (Add or Remove Snap-ins), znázorněném na obrázku 11.3, označte modul Místní uživatelé a skupiny Místní uživatelé a skupiny (Local Users And Groups) a klepněte na tlačítko Přidat (Add).



Obrázek 11.3: Výběr modulu snap-in Místní uživatelé a skupiny (Local Users And Groups)

4. V dialogu Zvolit cílový počítač (Choose Target Machine) vyberte položku Jiný počítač (Another Computer) a zadejte název počítače nebo jeho adresu IP. Klepněte na tlačítko Dokončit (Finish) a pak klepněte na tlačítko OK.

5. Ve stromu konzoly klepněte na položku Místní uživatelé a skupiny (Local Users And Groups). Klepněte pravým tlačítkem na položku Skupiny (Groups) a vyberte příkaz Nová skupina (New Group).

6. Vytvořte skupinu.

Správa výchozích skupin a uživatelských práv

Když vytvoříte doménu služby Active Directory s jedním nebo několika řadiči domén se systémem Windows Server 2008, budou v kontejnerech Users a Builtin automaticky vytvořeny výchozí skupiny. Mnoho z těchto skupin má také práva, která jsou automaticky přiřazována členům skupiny. Výchozí skupiny v kontejneru Builtin mají rozsah předdefinované místní skupiny. Jejich rozsah skupiny ani typ skupiny nelze změnit.

V kontejneru Users se nacházejí skupiny definované s globálním rozsahem a skupiny definované s rozsahem místní domény. Skupiny v těchto kontejnerech lze přesouvat do dalších skupiny a organizačních jednotek v rámci domény, nelze je však přesouvat do jiných domén.

Předdefinované místní skupiny

Členské servery a samostatné servery se systémem Windows 2000 Server (aktualizace Service pack 3 či novější), Windows 2000 Professional (aktualizace Service Pack 3 či novější), Windows XP Professional (aktualizace Service Pack 1 či novější) a Windows Vista mají předdefinované místní skupiny, které udělují práva k provádění úloh v jednom konkrétním počítači. Konkrétní skupiny se v jednotlivých počítačích budou mírně lišit. V tabulce 11.1 je uveden přehled výchozích místních skupin v instalacích systému Windows Server 2008, které nejsou řadičem domény.

Tabulka 11.1: Výchozí místní skupiny

Místní skupina	Popis
Administrators	Členové mohou v počítači provádět všechny úlohy správy. Členem skupiny je výchozí účet Administrator vytvořený při instalaci operačního systému. Je-li k doméně připojen server (ne řadič domény) nebo klient se systémem Windows Vista, Windows XP Professional nebo Windows 2000 Professional, je do této skupiny přidána skupina Domain Admins (viz tabulka 11.3).
Backup Operators	Členové se mohou připojit k počítači, zálohovat a obnovovat data v počítači a vypnout počítač. Členové nemohou změnit nastavení zabezpečení, mohou je však za účelem zálohování nebo obnovy přepsat. Skupina nemá výchozí členy.
Cryptographic Operators	Členové mohou provádět kryptografické operace. Skupina nemá výchozí členy.
Event Log Readers	Členové mohou číst protokoly událostí místního počítače. Skupina nemá výchozí členy.
Guests	Členové mohou provádět pouze takové úlohy, ke kterým jim správce udělil práva. Členové mohou používat pouze ty prostředky, ke kterým jim správce specificky přidělil oprávnění. Výchozím členem skupiny je účet Guest.
Distributed COM Users	Členové skupiny mohou v tomto počítači spouštět, aktivovat a používat objekty modelu DCOM. Skupina nemá výchozí členy.
IIS_IUSRS	Tento účet používá služba IIS.
Network Configuration Operators	Členové mohou měnit nastavení protokolu TCP/IP a obnovovat a uvolňovat adresy. Skupina nemá výchozí členy.
Performance Monitor Users	Členové mohou místně nebo vzdáleně sledovat čítače výkonu v konkrétním serveru. Skupina nemá výchozí členy.
Performance Log Users	Členové mohou místně nebo vzdáleně spravovat výstrahy, čítače a protokoly výkonu v konkrétním serveru. Skupina nemá výchozí členy.
Power Users	Tato skupina existuje z důvodů zpětné kompatibility, ve výchozím nastavení však nemají její členové větší práva a oprávnění než standardní uživatelské účty. Pokud potřebujete pro tuto skupinu zachovat práva a oprávnění, která měla v předchozích verzích systému Windows, použijte šablonu zabezpečení, která tato práva a oprávnění udělí.
Print Operators	Členové mohou spravovat tiskárny a tiskové fronty v konkrétním serveru. Skupina nemá výchozí členy.
Remote Desktop Users	Členům je povoleno vzdálené připojení. Skupina nemá výchozí členy.

Místní skupina	Popis
Replicator	Do této skupiny nepřidávejte uživatelské účty skutečných uživatelů. Je-li to nutné, můžete do skupiny přidat fiktivní uživatelský účet, který vám umožní přihlásit se k replikační službě v řadiči domény a spravovat replikaci souborů a adresářů.
Users	Členové této skupiny se mohou přihlásit k počítači, přistupovat k síti, ukládat dokumenty a vypnout počítač. Členové nemohou instalovat programy ani provádět změny v systému. Je-li k doméně připojen členský server, počítač se systémem Windows 2000 Professional nebo Windows XP Professional, je do této skupiny přidána skupina Domain Users. Členy skupiny Users jsou také skupiny Interactive a Authenticated Users, takže členy skupiny Users jsou automaticky všechny uživatelské účty.

Poznámka: Pokud chcete, aby členové skupiny Domain Users neměli přístup k určité pracovní stanici nebo členskému serveru, odeberte v daném počítači skupinu Domain Users z místní skupiny Users. Podobně jestliže chcete, aby členové skupiny Domain Admins nemohli spravovat určitou pracovní stanici nebo členský server, odeberte skupinu Domain Admins z místní skupiny Administrators.

Předdefinované místní doménové skupiny

Výchozí místní doménové skupiny poskytují uživatelům práva a oprávnění potřebná k provádění úkolů v řadičích domény a ve službě Active Directory Domain Services. Tyto místní doménové skupiny mají předdefinovaná práva a oprávnění, která jsou přidělována uživatelům a globálním skupinám, které do těchto skupin přidáte jako členy. Tabulka 11.2 obsahuje nejběžněji používané výchozí místní doménové skupiny.

Tabulka 11.2: Běžné používané výchozí místní doménové skupiny

Místní doménová skupina	Popis
Account Operators	Členové mohou vytvářet, odstraňovat a spravovat uživatelské účty a skupiny. Členové nemohou upravovat skupiny Administrators, Domain Admins, Domain Controllers ani žádnou ze skupin Operators. Členové se mohou místně přihlásit k řadičům domény a vypnout je. Skupina nemá výchozí členy.
Administrators	Členům jsou automaticky přidělena všechna práva a oprávnění ke všem řadičům domény i vlastní doméně. Členy jsou účet Administrator a skupiny Domain Admins a Enterprise Admins.
Allowed RODC Password Replication Group	Členům v této skupině mohou být replikována hesla do řadičů domény jen pro čtení. Skupina nemá výchozí členy. Tato skupina se v seznamu Builtin objeví v okamžiku, kdy je v doméně vytvořen řadič RODC.
Backup Operators	Členové mohou zálohovat a obnovovat data ve všech řadičích domény, mohou se přihlásit k řadičům domény a vypnout je. Skupina nemá výchozí členy, členství by mělo být přidělováno s opatrností. Tato skupina není shodná s výchozí místní skupinou Backup Operators.
Certificate Service DCOM Access	Členové mohou publikovat certifikáty pro uživatele a počítače. Skupina nemá výchozí členy.
Cryptographic Operators	Členové mohou provádět kryptografické operace. Skupina nemá výchozí členy.

Místní doménová skupina	Popis
Denied RODC Password Replication Group	Členům této skupiny nesmějí být replikována hesla do řadičů RODC. Výchozími členy jsou skupiny Cert Publishers, Domain Admins, Domain Controllers, Enterprise Admins, Group Policy Creator Owners, Read Only Domain Controllers a Schema Admins. Tato skupina se v seznamu Builtin objeví v okamžiku, kdy je v doméně vytvořen řadič RODC.
Distributed COM Users	Členové skupiny mohou spouštět, aktivovat a používat objekty modelu DCOM. Skupina nemá výchozí členy.
Event Log Readers	Členové mohou číst protokoly událostí místního počítače. Skupina nemá výchozí členy.
Guests	Členové mají ve výchozím nastavení stejná přístupová práva jako člen skupiny Users, s výjimkou účtu Guest, který je ještě více omezen. Výchozími členy skupiny jsou skupina Domain Guests a účet Guest.
IIS_IUSRS	Vestavěná skupina používaná službou IIS.
Incoming Forest Trust Builders (objevuje se pouze v kořenové doméně doménové struktury)	Členové mohou povolovat příchozí vztah důvěryhodnosti doménové struktury, aby umožnili uživatelům z jiné doménové struktury přistupovat k prostředkům ve své domovské doménové struktuře. Skupina nemá výchozí členy.
Network Configuration Operators	Členové mohou obnovovat a uvolňovat adresy v řadičích domény a měnit nastavení protokolu TCP/IP. Skupina nemá výchozí členy.
Performance Monitor Users	Členové mohou místně nebo ze vzdálených klientů sledovat čítače výkonu v řadičích domény, aniž by museli být správci nebo členy skupiny Performance Log Users. Skupina nemá výchozí členy.
Performance Log Users	Členové mohou místně nebo vzdáleně spravovat výstrahy, čítače a protokoly výkonu v řadičích domény, aniž by museli být správci. Skupina nemá výchozí členy.
Pre–Windows 2000 Compatible Access	Poskytovaná pro zpětnou kompatibilitu s počítači se systémem Windows NT 4. Do skupiny přidávejte pouze uživatele systému Windows NT 4 nebo systému staršího. Skupina nemá výchozí členy.
Print Operators	Členové mohou provádět veškerou provozní správu a konfiguraci tiskáren v doméně. Skupina nemá výchozí členy.
Remote Desktop Users	Členům je povoleno vzdálené připojení k řadičům domény. Skupina nemá výchozí členy.
Replicator	Slouží pro podporu replikace souborů.
Server Operators	Členové mohou provádět většinu úloh správy v řadičích domény s výjimkou manipulace s možnostmi zabezpečení. Skupina nemá výchozí členy.
Terminal Servers License Servers	Členové mohou aktualizovat uživatelské účty ve službě Active Directory, aby mohli sledovat a vykazovat využití licencí klientského přístupu Terminálové služby vázaných na uživatele. Skupina nemá výchozí členy.
Users	Členové této skupiny se mohou přihlásit k počítači, přistupovat k síti, ukládat dokumenty a vypnout počítač. Členové nemohou instalovat programy ani provádět změny v systému. Výchozími členy jsou skupiny Authenticated Users a Domain Users.
Windows Authorization Access	Členové této skupiny mají přístup k vypočítanému atributu *tokenGroupsGlobalAndUniversal* objektů *User*.

Poznámka: V systému Windows NT jsou všichni uživatelé domény členy skupiny Everyone. Tato skupina je řízena operačním systémem a nachází se v každé síti se servery Windows NT. V systémech Windows 2000 Server a novějších má ekvivalentní skupina název Authenticated Users. Na rozdíl od skupiny Everyone neobsahuje skupina Authenticated Users žádné anonymní uživatele ani hosty. Skupina Everyone přetrvává jako *zvláštní identita*. Při správě skupin není zobrazována a nelze ji umístit do skupiny. Pokud se uživatel připojí k síti, je automaticky přidán do skupiny Everyone. Členství ve zvláštních identitách, mezi které patří také skupiny Network a Interactive, nelze zobrazit ani změnit.

Předdefinované globální skupiny

Výchozí globální skupiny mají za úkol obsáhnout běžné typy účtů. Ve výchozím nastavení nemají tyto skupiny vlastní práva, všechna práva musí skupině přiřadit správce. Nicméně někteří členové jsou do těchto skupin přidáni automaticky, další členy můžete přidávat na základě práv a oprávnění přiřazených skupinám. Práva lze přiřazovat přímo skupinám nebo přidáním výchozích globálních skupin do místních doménových skupin. Běžně používané výchozí globální skupiny jsou popsány v tabulce 11.3.

Tabulka 11.3: Běžné používané výchozí globální skupiny

Globální skupina	Popis
DnsUpdateProxy (instalována společně se službou DNS)	Členy jsou klienti DNS, kteří mohou provádět dynamické aktualizace DNS v zastoupení jiných klientů. Skupina nemá výchozí členy.
Domain Admins	Skupina je automaticky členem místní doménové skupiny Administrators, takže členové skupiny Domain Admins mohou provádět úlohy správy v libovolném počítači v doméně. Tato skupina je automaticky členem skupin Administrators a Denied RODC Password Replication Group. Výchozím členem skupiny je účet Administrator.
Domain Computers	Členy jsou všechny řadiče a pracovní stanice v doméně.
Domain Controllers	Členy jsou všechny řadiče domény v doméně. Tato skupina je automaticky členem skupin Administrators a Denied RODC Password Replication Group.
Domain Guests	Výchozím členem je účet Guest. Skupina je automaticky členem místní doménové skupiny Guests.
Domain Users	Členy této skupiny jsou účet Administrator a všechny uživatelské účty. Skupina Domain Users je automaticky členem skupiny místní domény Users.
Group PolicyCreator Owners	Členové mohou vytvářet a upravovat zásady skupiny pro doménu. Výchozím členem skupiny je účet Administrator. Skupina PolicyCreator Owners je automaticky členem skupin Administrators a Denied RODC Password Replication Group.

Poznámka: Pokud máte uživatele s menší úrovní práv a oprávnění, než jaká má typický uživatel, přidejte tyto uživatele do skupiny Domain Guests a odeberte je ze skupiny Domain Users.

Definování uživatelských práv

Akce, které uživatelé mohou či nemohou provádět, závisejí na právech a oprávněních, která jim byla přidělena. *Práva* jsou obecně platná pro systém jako celek. Právem je například možnost zálohovat soubory nebo se přihlásit k serveru. Správce může toto právo udělit a stejně tak ho může i odebrat. Práva lze přiřazovat individuálně, ale daleko častěji jsou vlastnostmi skupin a uživatelé jsou přiřazováni do konkrétních skupin na základě práv, která potřebují.

Oprávnění označují přístup, jenž má uživatel (nebo skupina) k určitým objektům, například k souborům, adresářům nebo tiskárnám. Oprávnění například určují, zda uživatel může zobrazit určitý adresář nebo přistupovat k síťové tiskárně. Oprávnění jsou podrobně popsána dále v této kapitole.

Práva se dále dělí do dvou typů: systémová oprávnění a přihlašovací práva. *Systémová oprávnění* zahrnují takové funkce jako možnost provádět audity zabezpečení nebo vynutit vypnutí počítače ze vzdáleného systému – zjevně se nejedná o úlohy, které by prováděla většina uživatelů. *Přihlašovací práva* není třeba vysvětlovat: jedná se o možnost připojovat se určitými způsoby k počítači. V systému Windows Server 2008 jsou práva automaticky přiřazována výchozím skupinám, i když mohou být přidělena i jednotlivým uživatelům a skupinám. Upřednostňováno je přiřazování podle skupin, proto kdykoli je to možné, přiřazujte práva podle skupin, abyste si správu zbytečně neztížili. Jsou-li práva definována členstvím ve skupině, můžete uživateli práva odebrat tak, že ho jednoduše odeberete ze skupiny. V tabulkách 11.4 a 11.5 jsou uvedena přihlašovací práva a systémová oprávnění a skupiny, kterým jsou ve výchozím nastavení přiřazena.

Tabulka 11.4: Přihlašovací práva přiřazená skupinám ve výchozím nastavení

Název	Popis	Skupiny s přiřazenými právy v řadičích domény	Skupiny s přiřazenými právy v pracovních stanicích a serverech
Přistupovat k tomuto počítači přes síť (Access This Computer From The Network)	Povoluje přistupovat k počítači přes síť	Administrators, Authenticated Users, Everyone, Pre-Windows 2000 Compatible Access, Enterprise Domain Controllers	Administrators, Backup Operators, Users, Everyone
Povolit místní přihlášení (Allow Logon Locally)	Povoluje interaktivní přihlášení k počítači	Administrators, Account Operators, Backup Operators, Print Operators, Server Operators	Administrators, Backup Operators, Users
Povolit přihlášení pomocí Terminálové služby (Allow Log On Through Terminal Services)	Umožňuje přihlásit se jako klient terminálové služby	Administrators	Administrators, Remote Desktop Users

Tabulka 11.5: Systémová oprávnění přiřazená skupinám ve výchozím nastavení

Systémové oprávnění	Popis	Skupiny s přiřazenými systémovými oprávněními ve výchozím nastavení
Slouží jako součást operačního systému (Act As Part Of The Operating System)	Umožňuje procesu projít ověřením jako libovolný uživatel. Proces vyžadující toto oprávnění musí používat účet LocalSystem, který již toto oprávnění zahrnuje.	Žádná
Přidat pracovní stanice do domény (Add Workstations To Domain)	Umožňuje uživateli přidávat do stávající domény nové pracovní stanice.	Skupina Authenticated Users v řadičích domény
Upravit příděly paměti pro proces (Adjust Memory Quotas For A Process)	Umožňuje uživateli nastavit maximální velikost paměti, která může být procesem využívána.	Administrators, Local Service a Network Service
Zálohovat soubory a adresáře (Back Up Files And Directories)	Umožňuje zálohování systému, potlačuje oprávnění k jednotlivým souborům a adresářům.	Administrators, Server Operators (v řadičích domény), Backup Operators
Vynechat kontrolu přecházení (Bypass Traverse Checking)	Umožňuje uživateli procházet adresářové stromy (struktury složek) i v případě, že nemá oprávnění pro přístup k procházeným adresářům.	Administrators, Authenticated Users, Everyone a Pre-Windows 2000 Compatible Access v řadičích domény; Administrators, Backup Operators, Users, Everyone, Local Service a Network Service v serverech a v pracovních stanicích
Změnit systémový čas (Change The System Time)	Umožňuje nastavení vnitřních hodin počítače.	Administrators a Server Operators v řadičích domény, Administrators v serverech a pracovních stanicích, Local Service
Vytvořit stránkovací soubor (Create A Pagefile)	Umožňuje vytvářet a měnit stránkovací soubor.	Administrators
Vytvořit globální objekty (Create Global Objects)	Umožňuje v relaci terminálové služby vytvářet globální objekty.	Administrators, Service, Local Service, Network Service
Ladit programy (Debug Programs)	Umožňuje uživateli připojit k procesu ladicí program.	Administrators
Povolit nastavení důvěryhodnosti pro delegování pro účty počítačů a uživatelů (Enable User And Computer Accounts To Be Trusted For Delegation)	Povoluje uživateli nastavit u objektu parametr Důvěryhodný k delegování (Trusted For Delegation).	Administrators v řadičích domény; v členských serverech a pracovních stanicích nepřiřazeno
Vynutit vypnutí ze vzdáleného systému (Force Shutdown From A Remote System)	Umožňuje vypnutí počítače ze vzdáleného místa v síti.	Administrators a Server Operators v řadičích domény; Administrators v členských serverech a pracovních stanicích

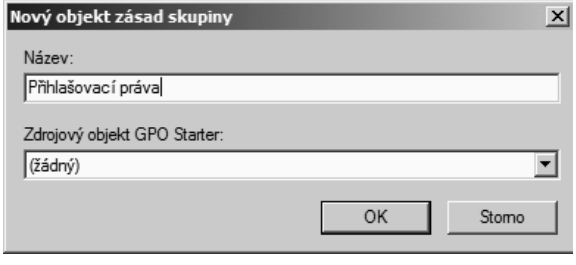
Systémové oprávnění	Popis	Skupiny s přiřazenými systémovými oprávněními ve výchozím nastavení
Zosobnit klienta po ověření (Impersonate A Client After Authentication)	Umožňuje účtu vydávat se za jiný účet.	Administrators
Zvýšit prioritu plánování (Increase Scheduling Priority)	Umožňuje pomocí programu Správce úloh (Task Manager) měnit plánovací priority procesů.	Administrators
Načíst a odstranit z paměti ovladače zařízení (Load And Unload Device Drivers)	Instaluje a odebírá ovladače zařízení plug-and-play.	Administrators a Print Operators v řadičích domény; Administrators v ostatních počítačích
Spravovat auditování a protokol zabezpečení (Manage Auditing And Security Log)	Umožňuje uživateli stanovit možnosti auditování a zobrazit nebo vymazat protokol zabezpečení v Prohlížeči událostí. U objektu, u něhož má být auditován přístup, musí být zapnuta funkce Auditovat přístup k adresářové službě (Audit directory service access). Protokol zabezpečení mohou vždy zobrazovat a mazat správci.	Administrators
Změnit hodnoty prostředí firmwaru (Modify Firmware Environment Variables)	Umožňuje měnit konfiguraci ve stálé paměti RAM v počítačích, které tuto funkci podporují.	Administrators
Profil jednoho procesu (Profile A Single Process)	Umožňuje vzorkování výkonu procesu.	Administrators; v členských serverech a pracovních stanicích Administrators a Users
Profil výkonu systému (Profile System Performance)	Umožňuje vzorkování výkonu systému.	Administrators
Vyjmout počítač z dokovací stanice (Remove Computer From Docking Station)	Povoluje vyjmutí přenosného počítače z dokovací stanice pomocí příkazu Vysunout PC (Eject PC) v nabídce Start.	Administrators a Users
Obnovit soubory a adresáře (Restore Files And Directories)	Umožňuje obnovení souborů a adresářů do systému, potlačuje oprávnění k jednotlivým souborům a adresářům.	Administrators, Backup Operators a Server Operators v řadičích domény; Administrators a Backup Operators v pracovních stanicích a serverech
Vypnout systém (Shut Down The System)	Umožňuje vypnout místní počítač.	Administrators, Backup Operators, Print Operators a Server Operators v řadičích domény; Administrators a Backup Operators v členských serverech; Administrators, Backup Operators a Users v pracovních stanicích.

Systémové oprávnění	Popis	Skupiny s přiřazenými systémovými oprávněními ve výchozím nastavení
Synchronizovat data adresářové služby (Synchronize Directory Service Data)	Umožňuje uživateli spustit synchronizaci služby Active Directory.	Žádná
Převzít soubory nebo jiné objekty (Take Ownership Of Files Or Other Objects)	Umožňuje uživateli převzít vlastnictví libovolného objektu zabezpečení včetně souborů a složek, tiskáren, klíčů registru a procesů.	Administrators

Přiřazení uživatelských práv skupině

Práva lze nejsnadněji přiřazovat a odebírat na úrovni domény pomocí zásad skupiny. Předpokládejme, že máte skupinu uživatelů, kteří by měli být schopni se místně přihlašovat k serverům se systémem Windows Server 2008, ale současně nechcete, aby byli členy skupin, které mají toto právo ve výchozím nastavení. Jeden ze způsobů, jak dosáhnout této situace, je vytvořit skupinu nazvanou Přihlašovací práva, přidat uživatele do skupiny a přiřadit skupině Přihlašovací práva právo k místnímu přihlášení. Práva konkrétní skupině přidělte následovně:

1. V nabídce Nástroje pro správu (Administrative Tools) zvolte položku Správa zásad skupiny (Group Policy Management).
2. Rozbalte název domény. Pravým tlačítkem klepněte na složku Objekty zásad skupiny (Group Policy Objects) a v místní nabídce vyberte příkaz Nový (New).
3. V dialogu Nový objekt zásad skupiny (New GPO) zadejte název nové zásady, jak znázorňuje obrázek 11.4. Klepněte na tlačítko OK.



Obrázek 11.4: Vytvoření nového objektu zásad skupiny

4. Klepněte pravým tlačítkem na nový objekt zásad skupiny a pak klepnutím na příkaz Upravit (Edit) spusťte Editor správy zásad skupiny (Group Policy Management Editor).
5. Rozbalte postupně položky Konfigurace počítače (Computer Configuration), Zásady (Policies), Nastavení systému Windows (Windows Settings), Nastavení zabezpečení (Security Settings), Místní zásady (Local Policies) a Přiřazení uživatelských práv (User Rights Assignment).

6. V podokně podrobností poklepejte na položku Povolit místní přihlášení (Allow Log On Locally).
7. Zaškrtněte políčko Definovat toto nastavení zásad (Define These Policy Settings) a klepněte na tlačítko Přidat uživatele nebo skupinu (Add User Or Group).
8. Zadejte název skupiny, které má být uděleno toto právo, případně klepněte na tlačítko Procházet (Browse) a skupinu vyhledejte. Klepněte na tlačítko OK. (Budete muset přidat také účet nebo skupinu s oprávněními pro správu.)
9. Klepněte na tlačítko OK a ukončete Editor správy zásad skupiny.

Stejným postupem můžete práva i odebrat, pouze v kroku 7 klepněte na tlačítko Odebrat. Tímto způsobem můžete práva přiřazovat také jednotlivým uživatelům.

Místní přiřazení práv

Práva mohou být přiřazována či odebírána i místně, ale je nutné si uvědomit, že zásady definované na úrovni domény potlačují nastavení místních zásad. Zásady můžete místně přiřadit následovně:

1. V nabídce Nástroje pro správu (Administrative Tools) zvolte položku Místní zásady zabezpečení (Local Security Policy).
2. Ve složce Nastavení zabezpečení (Security Settings) rozbalte položku Místní zásady (Local Policies) a klepněte na položku Přiřazení uživatelských práv (User Rights Assignment).
3. V podokně podrobností poklepáním na požadovanou zásadu otevřete okno s vlastnostmi dané zásady.
4. Po klepnutí na tlačítko Přidat uživatele nebo skupinu (Add User Or Group) můžete v dialogu Vyberte objekt typu: uživatelé nebo skupiny (Select Users, Computers, Or Groups) vybrat jednotlivce nebo skupinu. Ujistěte se, že pole Typy objektů (Object Types) a Umístění (Locations) odkazují na požadovaná umístění. Klepněte na tlačítko Upřesnit (Advanced) a poté na tlačítko Najít (Find Now). V dolním podokně se zobrazí všichni potenciální členové skupiny.
5. Označte účty, které mají být přidány, a klepněte na tlačítko OK.

Pokud tlačítka Přidat uživatele nebo skupinu a Odebrat nejsou v okně vlastností dostupná, znamená to, že zásada byla nastavena na úrovni domény a nelze ji přepsat místně.

Vytváření uživatelských účtů

Každá osoba, která má přístup k síti, musí mít uživatelský účet. Uživatelský účet umožňuje:

- ověřovat totožnost osoby připojující se k síti,
- řídit přístup k prostředkům domény,
- auditovat akce prováděné prostřednictvím účtu.

Systém Windows Server 2008 vytváří v řadiči domén pouze dva běžné předdefinované účty: účet Administrator, kterému jsou přidělena veškerá práva a oprávnění, a účet Guest,

jehož práva jsou omezena. V řadičích domény existuje také účet KRBTGT pro distribuci klíčů a v počítačích, které nejsou řadiči domény, existují speciální předdefinované účty pro účely funkcí Nápověda a podpora a Vzdálená pomoc. Všechny další účty vytváří správce a jedná se buď o účty doménové, které jsou ve výchozím nastavení platné v rámci celé domény, nebo o účty místní, které jsou použitelné pouze v počítači, v němž byly vytvořeny.

Pojmenovávání uživatelských účtů

Ve službě Active Directory má každý uživatelský účet své *hlavní jméno* (principal name). Toto jméno se skládá ze dvou částí: *názvu objektu zabezpečení* (security principal name) a *přípony hlavního jména* (principal name suffix). U stávajících uživatelských účtů systému Windows NT se ve výchozím nastavení název objektu zabezpečení shoduje se jménem používaným k přihlášení k doméně systému Windows NT. U nových uživatelských účtů systému Windows Server 2008 název objektu zabezpečení přiřazuje správce. Výchozí příponou uživatelského jména je název DNS kořenové domény větve domén. Uživatel označený v doméně Windows NT jako MarekS může mít v systému Windows Server 2000 a novějším například hlavní jméno *MarekS@autori.com*.

Možnosti účtu

Naplánováním možností účtů uživatelů si zjednodušíte proces tvorby účtů. Vezměte v úvahu následující možnosti účtů:

- **Přihlašovací hodiny (Logon Hours)** – ve výchozím nastavení se uživatel může během dne přihlásit v libovolném čase. Z důvodů zabezpečení možná budete chtít přístup omezit u některých nebo u všech uživatelů na konkrétní části dne nebo určité dny v týdnu.
- **Přihlásit se k (Log On To)** – ve výchozím nastavení se uživatelé mohou přihlásit ke všem pracovním stanicím. Z důvodů zabezpečení můžete uživatelům omezit přihlašovací přístup pouze na konkrétní počítač nebo počítače.
- **Vypršení platnosti účtu (Account expires)** – můžete rozhodnout, zda bude nastavena doba, po které vyprší platnost účtů. Ze zřejmých důvodů dává smysl nastavit pracovníkům s krátkodobým úvazkem datum vypršení platnosti účtu na datum ukončení jejich pracovní smlouvy.

U uživatelských účtů lze nastavit i další možnosti – mnoho dalších možností. Podrobně jsou popsány v tématu Nastavení vlastností uživatelských účtů v další části této kapitoly. Tři zmíněné možnosti však nejspíše použijete u velkého počtu uživatelů.

Z praxe: Vytvoření konvence pro pojmenovávání

Při přiřazování názvů objektů zabezpečení používejte jednotné konvence, aby si uživatelé mohli jména zapamatovat a snadno je nalezli v seznamech. Pro uživatelská jména zvažte následující možnosti:

- **Jméno plus iniciála příjmení** – příkladem může být MichalK nebo ZuzanaN. V případě duplicitních jmen můžete přidat čísla (MichalK1 a MichalK2) nebo dostatečný počet písmen, která umožní jejich identifikaci (IrenaNov a IrenaNat).

- **Jméno plus číslo** – příklady jsou David112 a David113. Tento přístup může způsobovat problémy zejména u lidí, jejichž jména se v populaci vyskytují častěji. Tento přístup vám značně ztíží zapamatování i vlastního uživatelského jména, natožpak jmen vašich kolegů.
- **Iniciála jména plus příjmení** – například Jnovak. Pokud jsou ve společnosti lidé se jména Jan Novák a Josef Novák, je možné použít JanNovak a JosNovak nebo JNovak1 a Jnovak2.
- **Příjmení plus iniciála** – toto pravidlo je užitečné ve velké síti. Pokud existují uživatelé se stejným příjmením, přidejte několik písmen, např. NovakJan a NovakJos.
- Bez ohledu na to, jaký přístup zvolíte, bude muset vyhovovat nejen stávajícím uživatelům sítě, ale musí být schopen pojmout také budoucí uživatele. Pak budete připraveni i na to, že se váš nový kolega může jmenovat třeba U Ti nebo Chomondely St. J. Montmorency-Glossup.

Hesla

Všichni uživatelé musejí mít dobře zvolená hesla a měli byste je vést k tomu, aby je pravidelně měnili. Hesla by měla být volena podle pokynů v poznámce Pravidla pro dobrá hesla. Nastavte účty tak, aby po zadání nesprávného hesla došlo k jejich uzamčení. (Ponechejte ale uživatelům prostor pro překlepy a povolte jim tři pokusy o zadání hesla.)

Z praxe: Pravidla pro dobrá hesla

Dobré heslo se vyznačuje následujícími vlastnostmi:

- Nevzniklo otočením znaků přihlašovacího jména, pokud možno nepoužívá znaky již použité v přihlašovacím jméně. (Kolik mozkových buněk je zapotřebí k uhodnutí takového hesla?)
- Obsahuje alespoň dva abecední znaky a jeden znak, který do abecedy nenáleží.
- Je alespoň osm znaků dlouhé.
- Není shodné se jménem uživatele ani jeho iniciálami, iniciálami dětí uživatele nebo jeho drahé polovičky, ani není kombinací libovolné z těchto položek s běžně dostupnými osobními daty, např. s datem narození, telefonním číslem nebo číslem SPZ.

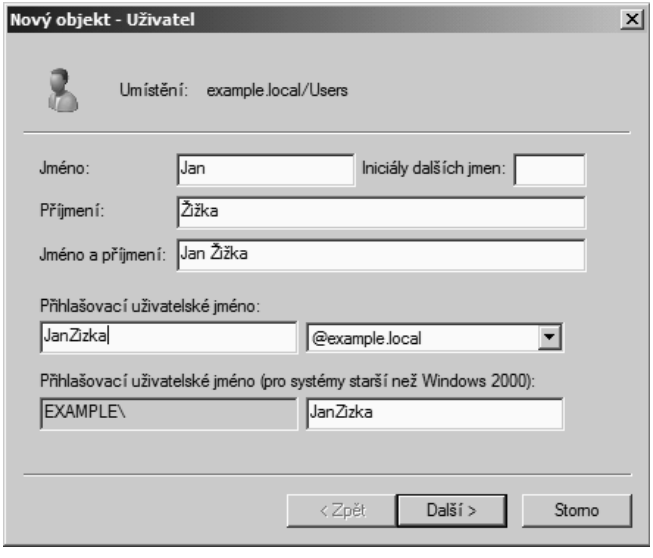
Mezi nejlepší hesla patří alfanumerické akronymy nebo fráze, které uživateli dávají smysl, ale není pravděpodobné, že byly známé ostatním lidem. Takové heslo je pro uživatele snadno zapamatovatelné, ale současně nesnadno uhodnutelné pro kohokoli cizího. Dobré heslo je také heslo, které není tvořené slovem, ale celou větou, i s mezerami a diakritikou.

Poučit uživatele o heslech a o jejich ochraně se vyplatí, především se však vyplatí dbát své vlastní rady: ujistěte se, že pro správu používáte kvalitní heslo a často ho měňte. Nebudete pak muset čelit následkům toho, že někdo vnikl do vašeho systému a způsobil v něm spoušť. Pokud se uživatelé připojují k síti z domova či vzdálených míst, mělo by být zabezpečení vyšší než jen autorizace heslem na úrovni domény.

Vytvoření účtu uživatele domény

Účty uživatelů domény můžete vytvořit ve výchozím kontejneru Users nebo můžete pro účty uživatelů domény vytvořit jinou organizační jednotku. Účet uživatele domény přidejte následovně:

1. V nabídce Nástroje pro správu (Administrative Tools) vyberte položku Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).
2. Pravým tlačítkem myši klepněte na kontejner, ve kterém chcete účet vytvořit, přejděte na příkaz Nový položka (New) a poté v místní nabídce zvolte příkaz Uživatel (User).
3. Zadejte uživatelovo jméno a příjmení, jak znázorňuje obrázek 11.5. Pole Jméno a příjmení bude vyplněno automaticky. V organizační jednotce, ve které účet vytváříte, musí být tato kombinace jména a příjmení jedinečná.



Obrázek 11.5: Vytvoření nového uživatele

4. Zadejte přihlašovací jméno uživatele, které jste vytvořili na základě konvencí pro pojmenovávání. Toto jméno musí být ve službě Active Directory jedinečné. Přihlašovací jméno pro systémy starší než Windows 2000 bude vyplněno automaticky. Jedná se o jméno, které se používá k přihlášení z počítačů se staršími operačními systémy Windows, jako je Windows NT. Klepněte na tlačítko Další (Next).
5. Zadejte heslo a nastavte zásady hesla. Klepněte na tlačítko Další (Next). Zobrazí se okno s výzvou k potvrzení údajů.
6. Pokud jsou údaje týkající se vytvářeného účtu správné, klepněte na tlačítko Dokončit (Finish). V opačném případě klepněte na tlačítko Zpět (Back) a údaje opravte.

V tomto okamžiku je nový uživatelský účet přidán do organizační jednotky za použití výchozích nastavení. Je nepravděpodobné, že toto výchozí nastavení splňuje vaše požadavky, takže budete nejspíše vlastnosti nového účtu muset upravit podle pokynů v tématu Nastavení vlastností uživatelského účtu v další části této kapitoly.

Vytvoření účtu místního uživatele

Místní účet nelze použít k přihlášení k doméně, poskytuje tedy pouze přístup k prostředkům v počítači, ve kterém je vytvořen a používán. V klientském počítači se systémem Windows Vista vytvořte účet místního uživatele následujícím postupem:

1. V nabídce Start klepněte pravým tlačítkem myši na položku Počítač (Computer) a v místní nabídce vyberte příkaz Spravovat (Manage).
2. Ve stromu konzoly klepněte na položku Místní uživatelé a skupiny (Local Users And Groups). Pravým tlačítkem myši klepněte na složku Uživatelé (Users) a v místní nabídce zvolte příkaz Nový uživatel (New User).
3. V dialogu Nový uživatel (New User) zadejte uživatelské jméno, jméno a příjmení a popis.
4. Zadejte heslo a nastavte zásady hesla. Klepněte na tlačítko Vytvořit (Create). V tomto bodě je vytvořen nový uživatelský účet s výchozím nastavením. Místní účty mohou být členy místních skupin (vytvořených v tomto jediném počítači).

Poznámka: V počítači se systémem Windows XP postupujte totožným způsobem, pouze v kroku 1 klepněte v nabídce Start pravým tlačítkem na položku Tento počítač (My Computer).

Nastavení vlastností uživatelského účtu

Dialog s vlastnostmi uživatele domény může mít v závislosti na nastavení domény až třináct karet. Tyto karty popisuje tabulka 11.6. Informace zadané do okna vlastností lze využívat jako základ pro hledání ve službě Active Directory. Můžete například vyhledat uživatelovo příjmení a zjistit jeho telefonní číslo nebo oddělení. Vlastnosti účtu uživatele domény nastavte následujícím postupem:

1. V nabídce Nástroje pro správu (Administrative Tools) vyberte položku Uživatelé a počítače služby Active Directory (Active Directory Users And Computers).
2. Otevřete organizační jednotku, ve které byl doménový uživatelský účet vytvořen.
3. Poklepáním na uživatelský účet otevřete okno s vlastnostmi.
4. Klepněte na kartu s vlastnostmi, které chcete nastavit. Proveďte požadované změny a poté klepněte na tlačítko OK.

Tabulka 11.6: Karty v okně s vlastnostmi účtu uživatele domény

Karta	Popis
Obecné (General)	Obsahuje jméno uživatele, popis, umístění kanceláře, telefonní číslo, e-mailovou adresu a adresy webových stránek.
Adresa (Address)	Obsahuje fyzickou adresu uživatele.
Účet (Account)	Obsahuje přihlašovací jméno, omezení pro přihlášení, možnosti hesla a zda vyprší platnost účtu.

Karta	Popis
Profil (Profile)	Zobrazuje cestu k profilu uživatele, cestu ke skriptu spouštěnému při přihlašování uživatele, cestu k domovské složce a všechna automatická připojení jednotek.
Telefony (Telephones)	Udává další telefonní čísla, například číslo operátoru, mobilního telefonu a telefonu IP.
Organizace (Organization)	Obsahuje titul uživatele, oddělení, společnost, nadřízeného pracovníka a přímé podřízené pracovníky.
Vzdálené řízení (Remote Control)	Slouží ke konfiguraci úrovně, na které může správce zobrazovat nebo řídit relace Terminálové služby uživatele.
Profil Terminálové služby (Terminal Services Profile)	Obsahuje profil Terminálové služby uživatele.
Model COM+ (COM+)	Obsahuje členství uživatele v sadách oddílů modelu COM+.
Je členem (Member Of)	Udává členství uživatele ve skupinách.
Telefonické připojení (Dial-in)	Obsahuje údaje o telefonickém připojení uživatele.
Prostředí (Environment)	Nastavení prostředí Terminálové služby platného pro uživatele.
Relace (Sessions)	Nastavení odpojení a obnovení Terminálové služby.

Poznámka: Pokud v nabídce Zobrazit (View) modulu Uživatelé a počítače služby Active Directory vyberete možnost Upřesňující funkce (Advanced Features), zobrazí se navíc karty Publikované certifikáty (Published Certificates), Objekt (Object) a Zabezpečení (Security).

Testování uživatelských účtů

Po vytvoření různých typů uživatelských účtů se doporučuje provést jejich testování. Vytvořte fiktivní účet s členstvím a omezeními, která plánujete používat. Poté se přihlaste ke klientskému počítači a provedením následujících akcí ověřte, zda se účet chová podle očekávání:

- Prověřte omezení doby povolené pro přihlášení a omezení hesla – pokuste se je obejít.
- Prověřte domovské složky a profily (popsané dále v této kapitole v tématu Použití domovských složek) a zjistěte, zda jsou skutečně vytvořeny.
- Přihlášením z různých počítačů prověřte cestovní profily.
- Prověřte členství ve skupinách – proveďte úlohu, kterou by členství v dané skupině mělo umožnit (nebo naopak nepřipustit), například přihlášení k serveru.

Nevhodné nastavení byste měli odhalit již v testovacím prostředí. Pomocí modulu snap-in Výsledná sada zásad popsaného v kapitole 13 (Zásady skupiny) prověřte nastavení zásad skupiny.

Správa uživatelských účtů

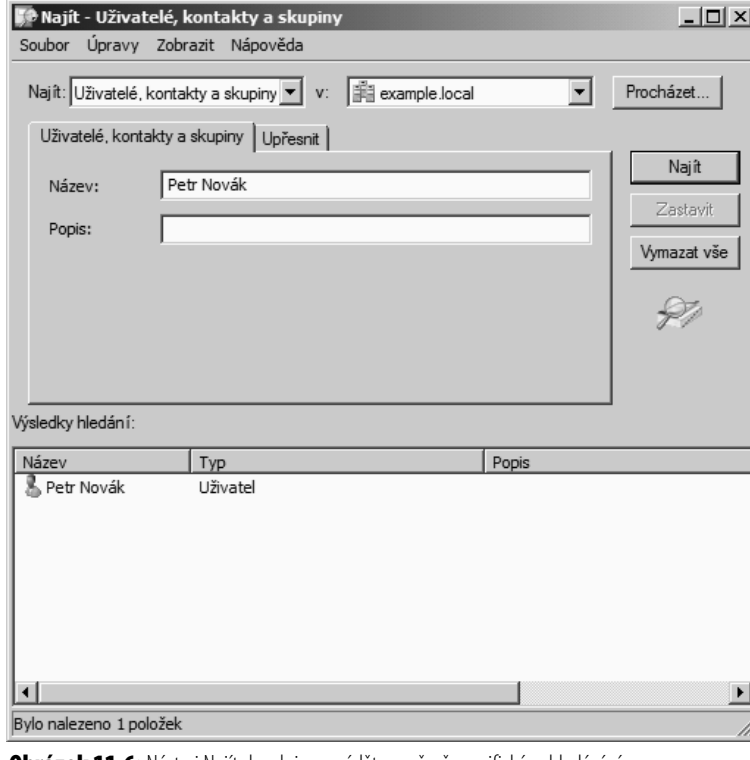
Ve velkých vytížených sítích je správa uživatelských účtů neustálým procesem přidávání, odstraňování a změn. I když tyto úlohy nejsou obtížné, mohou být časově náročné a vyžadují opatrnost.

Vyhledání uživatelského účtu

V malých sítích lze uživatele snadno vyhledat v modulu snap-in Uživatelé a počítače služby Active Directory. Ve větší síti je třeba použít rozšířené techniky hledání.

Chcete-li nalézt konkrétní uživatelský účet, zvolte v nabídce Nástroje pro správu (Administrative Tools) položku Uživatelé a počítače služby Active Directory (Active Directory Users And Computers) a na panelu nástrojů klepněte na ikonu Najít (Find), která vypadá následovně:

Otevře se dialog Najít – Uživatelé, kontakty a skupiny (Find Users, Contacts, And Groups). Klepněte na šipku rozevíracího seznamu Najít (Find). Zjistíte, že tento nástroj je možné použít také k vyhledání počítačů, tiskáren, sdílených složek, organizačních jednotek a dalších entit. (Viz obrázek 11.6.)

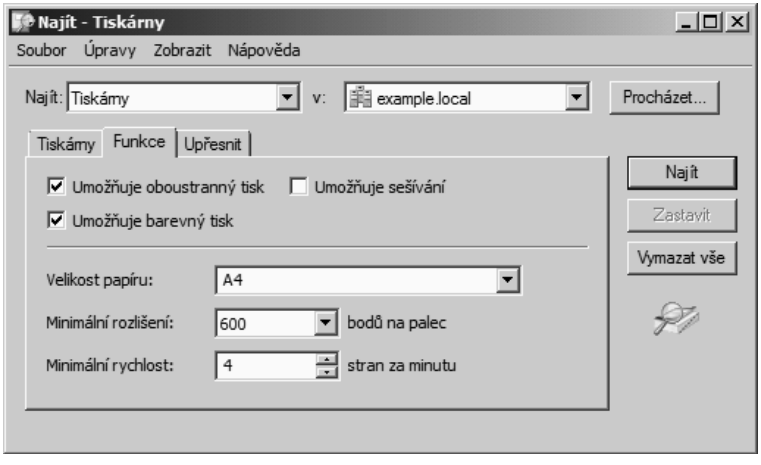


Obrázek 11.6: Nástroj Najít dovoluje provádět poměrně specifická vyhledávání

V poli V (In) vyberte oblast hledání. Zadejte jméno nebo část jména a klepněte na tlačítko Najít (Find Now). Hledání podle části jména vrátí všechny uživatele, kontakty a skupiny, které v názvu mají zadaný text.

V poli Najít zvolte jinou možnost a upravte možné parametry hledání. Vyberete-li v poli Najít například položku Běžné dotazy (Common Queries), můžete snadno vyhledat zakázané účty či uživatele s hesly bez nastavené doby platnosti.

Potřebujete-li provést podrobnější hledání, klepněte na kartu Upřesnit a pomocí tlačítka Pole zadejte požadovaná kritéria. Hledat lze podle prakticky každé informace uvedené v záznamu o uživateli, skupině nebo jiném objektu. Obrázek 11.7 ukazuje, jak vyhledat tiskárnu která umožňuje oboustranný barevný tisk na papír formátu A4 *a* tiskne rychlostí alespoň 4 stránky za minutu *a* má rozlišení 600 dpi nebo vyšší. Velké požadavky, ale pokud existuje, bude nalezena.



Obrázek 11.7: Hledání tiskárny ve službě Active Directory podle velmi specifických kritérií

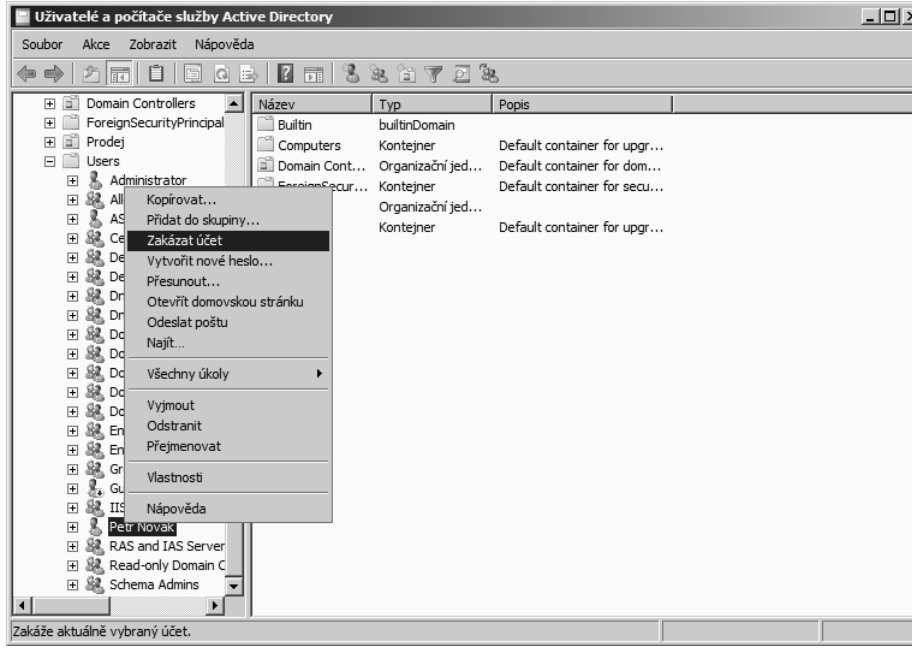
Zakázání a povolení uživatelského účtu

Pokud potřebujete na určité časové období doménový uživatelský účet deaktivovat, ale nechcete jej trvale odstranit, můžete jej zakázat. Vyhledejte uživatelský účet, pravým tlačítkem myši klepněte na uživatelské jméno a v místní nabídce vyberte příkaz Zakázat účet (Disable Account), jak znázorňuje obrázek 11.8.

Zobrazí se okno s informací o tom, že objekt byl zakázán. Chcete-li zakázaný účet opět povolit, zopakujte tento postup a v místní nabídce tentokrát vyberte příkaz Povolit účet (Enable Account).

Odstranění uživatelského účtu

Každý uživatelský účet v doméně má přidružen identifikátor SID, jenž je jedinečný a není nikdy použit znovu, což znamená, že odstraněný účet je odstraněn úplně. Odstraníte-li účet náležící Petrovi a později svůj úmysl změníte, musíte opět vytvořit nejen účet, ale také znovu nastavit oprávnění, nastavení, členství ve skupinách a další vlastnosti. Proto pokud existují jakékoli pochybnosti o tom, zda bude účet v budoucnosti ještě potřeba, je nejvýhodnější ho zakázat, nikoli odstranit.



Obrázek 11.8: Zakázání uživatelského účtu

Účty musejí být nicméně pravidelně odstraňovány. Vyhledejte uživatelský účet, klepněte pravým tlačítkem myši na uživatelské jméno a v místní nabídce zvolte příkaz Odstranit (Delete). Služba Active Directory zobrazí dialog s výzvou k potvrzení odstranění. Po klepnutí na tlačítko Ano bude účet odstraněn.

Přesunutí uživatelského účtu

Přesunutí uživatelského účtu z jednoho kontejneru do druhého je velmi snadné. Vyhledejte uživatelský účet ve službě Active Directory. Pravým tlačítkem myši klepněte na uživatelské jméno a v místní nabídce zvolte příkaz Přesunout (Move). V dialogu Přesunout (Move) vyberte cílový kontejner a klepněte na tlačítko OK. Účet také můžete jednoduše přetáhnout do cílového kontejneru. Pomocí kláves Ctrl a Shift můžete vybrat několik uživatelských účtů najednou.

Přejmenování uživatelského účtu

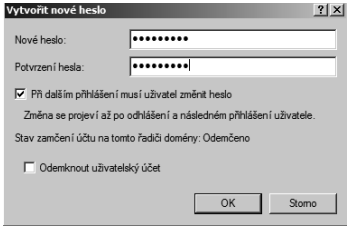
Příležitostně může být zapotřebí uživatelský účet přejmenovat. Je-li například účet nakonfigurován pro určitou pozici určitými právy, oprávněními a členstvím ve skupinách a tuto pozici převezme nová osoba, můžete změnit jméno, příjmení a přihlašovací jména uživatele a přizpůsobit je nové osobě. Existující uživatelský účet přejmenujte následovně:

1. Vyhledejte stávající uživatelský účet. Pravým tlačítkem myši klepněte na uživatelské jméno a v místní nabídce zvolte příkaz Přejmenovat (Rename). (Můžete také zvolna dvakrát klepnout na uživatelské jméno.)
2. Stiskněte klávesu Delete a poté klávesu Enter. Otevře se dialog Přejmenovat uživatele (Rename User).
3. Zadejte požadované změny a klepněte na tlačítko OK. Účet bude přejmenován, veškerá oprávnění a jiná nastavení zůstanou nezměněna. Další údaje v okně s vlastnostmi účtu, jako je například adresa, telefonní číslo atd., je také nutné změnit. Pokud k účtu existuje domovská složka, nebude přejmenována podle nového uživatele a bude potřeba ji vytvořit samostatně.

Nové nastavení hesla uživatele

Aby byla hesla účinná, nesmí být zřejmá a nesmí být možné je lehce uhodnout. Pokud však hesla nejsou zřejmá a nelze je snadno uhodnout, uživatelé je často zapomínají. Jestliže uživatel zapomene své heslo, můžete jej znovu nastavit. Nejvýhodnější je nastavit jednoduché heslo a stanovit, že jej uživatel musí při příštím přihlášení k síti změnit. Nové heslo nastavte následovně:

1. Vyhledejte uživatelský účet, jehož heslo je nutné opětovně nastavit.
2. Pravým tlačítkem myši klepněte na uživatelské jméno a v místní nabídce zvolte příkaz Vytvořit nové heslo (Reset Password).
3. V dialogu Vytvořit nové heslo (Reset Password), znázorněném na obrázku 11.9, zadejte dvakrát nové heslo. Pokud změnu provádíte, protože uživatel zapomněl své heslo a neuspěl při opakovaném pokusu o přihlášení, budete pravděpodobně muset zaškrtnout políčko Odemknout uživatelský účet (Unlock The User's Account). Klepnutím na tlačítko OK proveďte změny.



Obrázek 11.9: Nastavení nového hesla uživatele