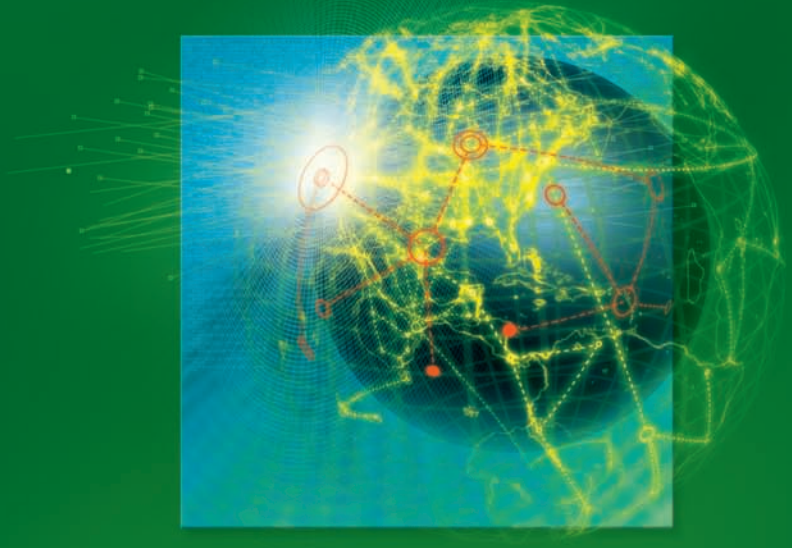
ADMINISTRACE

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,