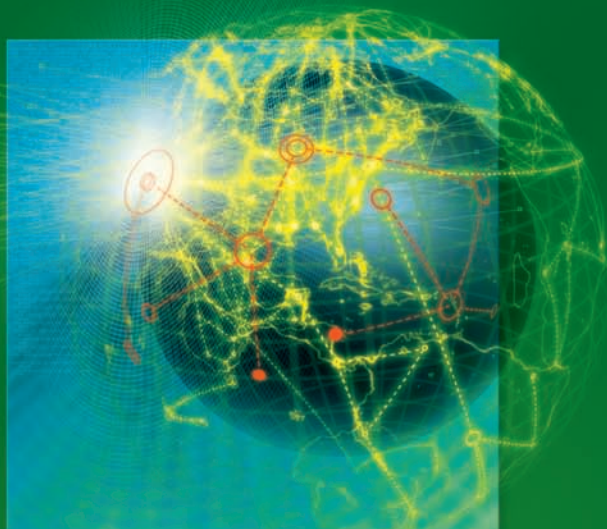


ADMINISTRACE

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

C PRESS *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

Authorized translation from English language edition Windows Server®2008 Administrator's Companion. Original copyright: © Charlie Russel, Sharon Crawford, 2008.

Translation: © Computer Press, a.s., 2009.

Autorizovaný překlad z originálního anglického vydání Windows Server®2008 Administrator's Companion. Originální copyright: © Charlie Russel, Sharon Crawford, 2008.

Překlad: © Computer Press, a.s., 2009.

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.

© Computer Press, a.s. Všechna práva vyhrazena. Žádná část této publikace nesmí být kopírována a rozmnožována za účelem rozšiřování v jakékoli formě či jakýmkoli způsobem bez písemného souhlasu vydavatele.

Stručný obsah

ČÁST I

Příprava

Kapitola 1	Úvod do systému Windows Server 2008	39
Kapitola 2	Představení adresářových služeb	47
Kapitola 3	Plánování oborů názvů a domén	57
Kapitola 4	Plánování nasazení	71

ČÁST II

Instalace a konfigurace

Kapitola 5	Začínáme	83
Kapitola 6	Upgrade na systém Windows Server 2008	109
Kapitola 7	Konfigurace nové instalace	123
Kapitola 8	Instalace rolí serveru a funkcí	149
Kapitola 9	Instalace a konfigurace jádra serveru	177
Kapitola 10	Správa tiskáren	193
Kapitola 11	Správa uživatelů a skupin	225
Kapitola 12	Správa souborových prostředků	263
Kapitola 13	Zásady skupiny	305

ČÁST III

Správa sítě

Kapitola 14	Správa každodenních operací	371
Kapitola 15	Důsledná správa pomocí skriptů	407
Kapitola 16	Instalace a konfigurace adresářových služeb	477
Kapitola 17	Správa služby Active Directory	541
Kapitola 18	Správa protokolu TCP/IP	577
Kapitola 19	Implementace správy disků	617
Kapitola 20	Správa úložišť	651
Kapitola 21	Použití clusterů	697

ČÁST IV

Zabezpečení sítě

Kapitola 22	Plánování zabezpečení	741
Kapitola 23	Implementace zabezpečení	755
Kapitola 24	Správa Architektury NAP	789

Kapitola 25	Správa oprav	823
Kapitola 26	Implementace strategií vzdáleného přístupu: SSTP, VPN a bezdrátový přístup.	837

ČÁST V

Použití podpůrných služeb a funkcí

Kapitola 27	Spolupráce mezi systémy	893
Kapitola 28	Správa softwaru	923
Kapitola 29	Práce se službou Windows Virtualization	949
Kapitola 30	Nasazení terminálových služeb	989
Kapitola 31	Internetová informační služba	1043

ČÁST VI

Ladění, údržba a oprava

Kapitola 32	Spolehlivost systému Windows a sledování výkonu	1087
Kapitola 33	Plánování pro případ havárie	1113
Kapitola 34	Použití zálohování	1127
Kapitola 35	Plánování odolnosti proti chybám	1153
Kapitola 36	Správa registru	1169
Kapitola 37	Řešení systémů a obnovení systému	1197
Příloha A	Změny v rozhraní oproti systému	1215
Příloha B	Volitelné komponenty	1221
Příloha C	Poznejte protokol TCP/IP verze 4	1231

Obsah

Poděkování	29
Úvod	31
Seznamte se s rodinou	31
Novinky v operačním systému.....	32
Co najdete v této knize.....	33
Skripty na webu	35
Poznámka redakce českého vydání	35

ČÁST I

Příprava

Kapitola 1 Úvod do systému Windows Server 2008	39
Čekání nikoli zbytečné	39
Virtualizace serverů	40
Jádro serveru	40
Prostředí PowerShell	40
Řadiče domény jen pro čtení.....	41
Služba Active Directory Domain Services	41
Služba Active Directory Domain Services je restartovatelná	41
Podrobně nastavitelné zásady pro hesla.....	42
Nástroj pro dolování dat	42
Terminálová služba	42
Brána Terminálové služby	42
Aplikace RemoteApp Terminálové služby	43
Funkce TS Web Access.....	43
Zprostředkovatel relací Terminálové služby	43
Režim vyprazdňování Terminálové služby	43
Správce serveru	44
Zálohování serveru	44
Korektní vypínání služeb	44
Další funkce zabezpečení.....	44
Funkce Address Space Load Randomization	45
Nástroj BitLocker Drive Encryption.....	45
Brána Windows Firewall	45
Architektura Network Access Protection.....	46
Verze systému Windows Server 2008.....	46
Shrnutí	46

Kapitola 2	Představení adresářových služeb	47
	Vysvětlení adresářových služeb	48
	Služba Active Directory v systému Windows Server 2008.....	49
	Terminologie a pojmy týkající se služby Active Directory	50
	Architektura služby Active Directory	52
	Agent adresářového systému	52
	Formáty názvů	53
	Datový model	53
	Implementace schématu	53
	Model zabezpečení	54
	Názvové kontexty a oddíly	55
	Globální katalog	55
	Shrnutí	56
Kapitola 3	Plánování oborů názvů a domén	57
	Analýza potřeb jmenných konvencí	58
	Stromy a doménové struktury	58
	Definování konvence pojmenování	59
	Organizační konvence pojmenování	60
	Plánování doménové struktury	64
	Domény versus organizační jednotky	64
	Návrh doménové struktury	66
	Pokyny k zabezpečení domény	67
	Vytvoření organizačních jednotek	67
	Plánování více domén	68
	Plánování souvislého oboru názvů	68
	Určení potřeby doménové struktury s více stromy	68
	Vytvoření doménové struktury	68
	Shrnutí	69
Kapitola 4	Plánování nasazení	71
	Fungování informačních technologií	72
	Určení potřeb podniku	72
	Specifika	73
	Pohled do budoucnosti	73
	Odhad stávajících systémů	74
	Dokumentace sítě	74
	Vytvoření přehledu	76
	Definování cílů	77
	Posouzení rizika	78
	Shrnutí	79

ČÁST II

Instalace a konfigurace

Kapitola 5	Začínáme	83
	Kontrola požadavků na systém.....	83
	Návrh prostředí pro nasazení	85
	Výběr metody instalace	85
	Instalace systému Windows Server 2008.....	85
	Automatizace nasazení serveru.....	92
	Instalace a konfigurace služby WDS.....	93
	Přidání dalších bitových kopií.....	101
	Odstraňování potíží při instalaci.....	103
	Nelze spustit systém z distribučního místa v síti	104
	Při instalaci je zjištěn poškozený soubor.....	106
	Nepodařilo se nalézt pevný disk.....	106
	Vyskytla se chyba STOP.....	107
	Shrnutí	108
Kapitola 6	Upgrade na systém Windows Server 2008	109
	Postup upgradu.....	109
	Obecné souvislosti s prováděním upgradu	110
	Kroky předcházející upgradu.....	111
	Architektura	111
	Služba Active Directory	112
	Podpora hardwaru.....	114
	Podpora softwaru	115
	Příprava domén a počítačů	116
	Upgrade klientů.....	117
	Provedení upgradu.....	117
	Upgrade na systém Windows Server 2008	118
	Úrovně funkčnosti lesa a domény.....	121
	Shrnutí	122
Kapitola 7	Konfigurace nové instalace	123
	Přehled úloh	124
	První přihlášení.....	125
	Konfigurace hardwaru	126
	Konfigurace základních informací o počítači	127
	Nastavení časového pásma.....	127
	Konfigurace sítě.....	128
	Nastavení názvu počítače a domény.....	131

	Aktualizace a nastavení odesílání informací	134
	Zapnutí aktualizací a odesílání informací	134
	Získání aktualizací	140
	Přizpůsobení serveru	140
	Přidání funkce Windows PowerShell	141
	Povolení vzdálené plochy	144
	Konfigurace brány Windows Firewall	145
	Ukončení průvodce Úlohy počáteční konfigurace	147
	Shrnutí	148
Kapitola 8	Instalace rolí serveru a funkcí	149
	Definice rolí serveru	150
	Přidání a odebrání rolí	158
	Přidání role	159
	Odebrání role	164
	Přidání a odebrání služeb rolí	168
	Přidání služeb rolí	168
	Odebrání služeb rolí	170
	Přidání a odebrání funkcí	172
	Přidání funkcí	172
	Odebrání funkcí	174
	Shrnutí	175
Kapitola 9	Instalace a konfigurace jádra serveru	177
	Výhody instalace jádra serveru	178
	Zabezpečení	178
	Prostředky	179
	Instalace jádra serveru	179
	Konfigurace	180
	Počáteční konfigurace	180
	Instalace rolí	186
	Správa počítače s jádrem serveru	188
	Použití Windows Remote Shell	190
	Použití vzdálené aplikace RemoteApp TS	191
	Shrnutí	192
Kapitola 10	Správa tiskáren	193
	Plánování nasazení tiskáren	193
	Zavedení konvencí pro pojmenování tiskáren	194
	Vytvoření konvencí pro pojmenování umístění	194
	Vytvoření tiskového serveru	195
	Zapnutí sledování umístění tiskáren	197

Migrace tiskových serverů	199
Použití průvodce Migrace tiskárny (Print Migration Wizard)	200
Použití příkazového řádku	201
Instalace tiskáren	201
Instalace tiskáren se zásadami skupiny	203
Přidání příkazu PushPrinterConnections pomocí zásad skupiny (Group Policy)	204
Správa tiskových úloh ze systému Windows	206
Dočasné pozastavení tiskových úloh	206
Zrušení tiskových úloh	207
Restartování tiskové úlohy	207
Změna priority tiskové úlohy	207
Přesunutí tiskových úloh	207
Správa tiskových úloh z příkazového řádku	208
Nastavení možností zabezpečení	209
Změna dostupnosti tiskárny a priorit skupiny	210
Specifikace oddělovací stránky	211
Změna zařazování tisku tiskárnou	213
Řadit dokumenty do fronty a umožnit tím tisk ukončit rychleji (Spool Print Documents So Program Finishes Printing Faster)	213
Tisknout přímo na tiskárnu (Print Directly To The Printer)	213
Pozastavit neshodné dokumenty (Hold Mismatched Documents)	213
Zařazené dokumenty vytisknout nejdříve (Print Spooled Documents First)	214
Nemazat vytištěné dokumenty (Keep Printed Documents)	214
Změna zařazování na tiskovém serveru	214
Optimalizace výkonu tiskového serveru	215
Změna umístění složky zařazování tisku	215
Správa ovladačů tiskárny	215
Vytváření fondů tiskáren	216
Příprava na chybu tiskového serveru	217
Řešení problémů s tiskárnami	218
Problémy na straně serveru	218
Problémy na straně klienta	222
Shrnutí	223
Kapitola 11 Správa uživatelů a skupin	225
Principy skupin	225
Přiřazení rozsahů skupin	226
Plánování organizačních jednotek	227
Vytvoření organizačních jednotek	228

Přesouvání organizačních jednotek	229
Odstranění organizačních jednotek	230
Plánování strategie použití skupin	230
Stanovení názvů skupin	230
Použití globálních skupin a místních doménových skupin	230
Použití Univerzálních skupin	231
Implementace strategie použití skupin	231
Vytvoření skupin	231
Odstraňování skupin	232
Přidání uživatelů do skupiny	233
Správa výchozích skupin a uživatelských práv	235
Předdefinované místní skupiny	236
Předdefinované místní doménové skupiny	237
Předdefinované globální skupiny	239
Definování uživatelských práv	240
Vytváření uživatelských účtů	244
Pojmenovávání uživatelských účtů	245
Možnosti účtu	245
Hesla	246
Vytvoření účtu uživatele domény	246
Vytvoření účtu místního uživatele	248
Nastavení vlastností uživatelského účtu	248
Testování uživatelských účtů	249
Správa uživatelských účtů	249
Vyhledání uživatelského účtu	250
Zakázání a povolení uživatelského účtu	251
Odstranění uživatelského účtu	251
Přesunutí uživatelského účtu	252
Přejmenování uživatelského účtu	252
Nové nastavení hesla uživatele	253
Odemknutí uživatelského účtu	254
Použití domovských složek	254
Vytvoření domovských složek v serveru	254
Poskytnutí domovských složek uživatelům	255
Správa uživatelských profilů	256
Místní profily	258
Cestovní profily	259
Přiřazení přihlašovacího skriptu k profilu uživatele	262
Shrnutí	262

Kapitola 12 Správa souborových prostředků	263
Oprávnění ke sdílení versus oprávnění k souborům	264
Oprávnění ke sdílení	264
Oprávnění k souborům	265
Oprávnění NTFS	266
Co znamenají oprávnění	266
Jak oprávnění fungují	268
Dědičnost	268
Konfigurace oprávnění ke složkám	269
Přiřazení oprávnění k souborům	270
Konfigurace zvláštních oprávnění	271
Vlastnictví a jak funguje	274
Sdílené složky	276
Použití nástroje Správa sdílených složek a úložišť (Share And Storage Management)	276
Použití příkazového řádku: příkaz Net Share	280
Publikování sdílení ve službě Active Directory	280
Systém souborů DFS	281
Terminologie systému souborů DFS	282
Požadavky serveru oboru názvů	284
Požadavky klientů oborů názvů	284
Služba Replikace distribuovaného systému souborů (DFS Replication)	285
Instalace modulu snap-in DFS Management	287
Vytváření nebo otevření kořene oboru názvů	288
Přidání serverů oborů názvů	290
Přidání složek DFS	290
Změna pokročilých nastavení	291
Zálohování a obnovení cílových složek DFS	294
Použití služby Replikace distribuovaného systému souborů (DFS Replication)	294
Shrnutí	303
Kapitola 13 Zásady skupiny	305
Co je nového v systému Windows Server 2008	305
Součásti zásad skupiny	306
Objekty zásad skupiny	306
Pořadí implementace	306
Pořadí dědičnosti	307
Vytvoření objektu zásad skupiny	308
Editace objektu zásad skupiny	308
Odstranění objektu zásad skupiny	308
Vyhledání objektu zásad skupiny	309

Použití objektů GPO Starter	309
Předvolby zásad skupiny	312
Použití předvoleb zásad skupiny v systému Windows.....	315
Konfigurace společných možností	328
Použití předvoleb zásad skupiny pro Ovládací panely.....	329
Delegování oprávnění na objekty GPO	359
Delegování oprávnění k vytvoření	359
Delegování oprávnění k propojování	359
Odebrání oprávnění k úpravě, odstranění nebo změně zabezpečení	360
Zakázání určité větve objektu GPO.....	360
Aktualizace zásad skupiny.....	361
Zálohování objektu zásad skupiny.....	362
Obnovení objektu zásad skupiny	362
Použití zásad skupiny k přesměrování složky.....	363
Přesměrování na jedno umístění.....	363
Přesměrování prostřednictvím členství ve skupině	364
Odstranění přesměrování.....	365
Použití výsledné sady zásad	365
Spuštění dotazu nástroje RSoP	366
Režim plánování nástroje RSoP	366
Režim protokolování nástroje RSoP.....	367
Shrnutí	367

ČÁST III

Správa sítě

Kapitola 14 Správa každodenních operací	371
Správa pomocí nástroje Řízení uživatelských účtů	371
Režim schválení správce (Admin Approval Mode (AAM))	372
Nástroj Řízení uživatelských účtů (User Account Control)	
a virtualizace registru	373
Stinné stránky nástroje Řízení uživatelských účtů	
(User Account Control).....	373
Vypnutí nástroje UAC.....	376
Použití konzoly Microsoft Management Console 3.0.....	377
Nastavení možností konzoly MMC 3.0	378
Vytvoření konzoly MMC pomocí modulů snap-in	378
Použití Průvodce vytvořením zobrazení panelu úloh (New Taskpad View Wizard).....	379
Distribuce a použití konzol	380
Použití konzoly MMC ke vzdálené správě.....	380
Nastavení zásad auditu	381

Kategorie auditu	382
Audit událostí adresářové služby	386
Povolení auditu objektů služby AD DS	387
Nastavení globálních zásad auditu	390
Povolení auditu	391
Použití nástroje Prohlížeč událostí (Event Viewer)	394
Správa protokolů událostí	399
Použití nástroje Plánovač úloh (Task Scheduler)	401
Použití příkazu AT	402
Delegování úloh	403
Shrnutí	405
Kapitola 15 Důsledná správa pomocí skriptů	407
Představení prostředí Windows PowerShell	408
Principy prostředí Windows PowerShell	408
Základy	409
Prostředí PowerShell jako příkazový řádek	413
Rutiny (Cmdlety)	416
Infrastruktura systému Windows	420
Rozhraní .NET Framework	420
Rozhraní WMI (Windows Management Instrumentation)	423
Služba WinRM (Windows Remote Management)	425
Model COM (Component Object Model)	425
Vytváření dialogových a vstupních oken	426
Objevujeme prostředí PowerShell	427
Get-Command	427
Get-Help	428
Get-Member	429
Zobrazení dat	430
Sady parametrů a poziční parametry	431
Načítání modulů snap-in	433
Základy tvorby skriptů v prostředí PowerShell	434
Vytváření skriptů .ps1	434
Komentáře	436
Proměnné	436
Obor platnosti	437
Řetězce	438
Řetězce typu Here String	439
Zástupné znaky a regulární výrazy	439
Pole	440
Asociativní pole	441
Operátory	442
Funkce	442

Podmíněné příkazy	443
Příkazy smyček	445
Importování ze souborů a exportování do souborů	446
Řízení toku	447
Formátovací rutiny	449
Ukončování skriptů, funkcí a smyček	450
Načítání skriptů pomocí tečky	450
Předávání argumentů	451
Příkaz param	452
Proměnné \$_ a \$input	453
Ošetření chyb	454
Operátory přesměrování	456
Akcelerátory typů	456
Uvozování znaků	456
Příklady z prostředí Windows PowerShell	456
Obvyklé úkoly při práci se systémem souborů	456
Testování existence souboru nebo adresáře	457
Rutiny pro zálohování systému Windows Server	458
Příklady správy jádra serveru	458
Podpora jazyka XML	459
Použití protokolu FTP (File Transfer Protocol)	459
Stáhnutí souboru prostřednictvím protokolu HTTP	459
Odesílání e-mailů prostřednictvím protokolu SMTP	460
Komprese souborů	461
Práce s daty	461
Čítače a odpočty	462
Čtení vstupu z konzoly	463
Zabezpečené ukládání informací	464
Kontrola služeb a procesů	464
Kontrola protokolu událostí systému Windows	466
Získání informací o paměti a procesoru	467
Přístup k čítačům výkonu	468
Kontrola využitého místa na disku	469
Práce s registrem	470
Rekurzivní kopírování souborů do jiného adresáře	471
Rotace protokolů	471
Přejmenování souborů	471
Plánování úloh	472
Spouštění kódu na více cílových počítačích	473
Vytváření dat ve formátu XML	473
Kontrola otevřených portů	474
Příkazy head, tail, touch a tee	474
Shrnutí	476

Kapitola 16 Instalace a konfigurace adresářových služeb	477
Služba Active Directory v systému Windows Server 2008	477
Služba AD DS (Active Directory Domain Services)	478
Služba AD LDS (Active Directory Lightweight Directory Services)	478
Služba AD RMS (Active Directory Rights Management Services)	479
Služba AD FS (Active Directory Federation Services)	481
Služba AD CS (Active Directory Certificate Services)	482
Instalace služby Active Directory Domain Services	483
Předpoklady pro instalaci služby AD DS	483
Instalace služby AD DS pomocí Průvodce instalací služby Active Directory Domain Services	485
Kompatibilita operačních systémů	486
Konfigurace nasazení	487
Pojmenování domény	488
Nastavení úrovně funkčnosti systému Windows Server 2008	489
Umístění souborů	491
Dokončení instalace	491
Přidání řadiče domény do existující domény	492
Kontrola instalace služby AD DS	492
Možnosti rozšířeného režimu	494
Instalace z média	495
Bezobslužná instalace	496
Odinstalace služby AD DS	497
Instalace a konfigurace řadičů domény jen pro čtení	500
Co jsou řadiče domény jen pro čtení?	500
Proč používat řadiče RODC?	501
Delegování instalace a správy řadičů RODC	501
Konfigurace zásad replikace hesel	503
Správa služby AD DS pomocí modulu Uživatelé a počítače služby Active Directory	505
Zobrazování objektů služby AD DS	506
Vytvoření objektu počítače	509
Konfigurace objektů počítačů	510
Použití vzdálené správy počítačů	510
Publikování sdílené složky	511
Publikování tiskárny	511
Přesouvání, přejmenování a odstraňování objektů	512
Správa služby AD DS pomocí modulu Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains and Trusts)	512
Spuštění modulu Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains and Trusts)	512
Správa vztahů důvěryhodnosti mezi doménami	513

Určení správce domény	516
Konfigurace přípon hlavních uživatelských jmen v doménové struktuře	516
Použití modulu Lokality a služby Active Directory	
(Active Directory Sites and Services)	516
Přehled domén služby AD DS	519
Principy replikace služby AD DS	519
Spuštění modulu Lokality a služby Active Directory (Active Directory Sites and Services)	521
Instalace a konfigurace služby Active Directory Lightweight	
Directory Services	528
Přehled služby AD LDS	528
Funkce služby AD LDS	528
Konfigurace instancí a oddílů adresáře aplikace	529
Správa služby AD LDS	532
Konfigurace replikace	536
Konfigurace synchronizace služeb AD DS a AD LDS	537
Shrnutí	539
Kapitola 17 Správa služby Active Directory	541
Správa databáze služby AD DS	541
Úložiště dat služby AD DS	542
Uvolnění mezipaměti	543
Online defragmentace	543
Služba Active Directory Domain Services s možností restartu	544
Offline defragmentace databáze služby AD DS	545
Přesunutí databáze a umístění protokolu transakcí	546
Zálohování služby AD DS	547
Potřeba záloh	548
Frekvence zálohování	549
Provádění zálohy služby AD DS pomocí programu	
Zálohování serveru (Windows Server Backup)	550
Obnovení služby AD DS	551
Odebrání řadičů domény ze služby AD DS pomocí nástroje Ntdsutil ..	551
Provádění neautoritativního obnovení služby AD DS	553
Provádění autoritativního obnovení služby AD DS	555
Správa schématu služby AD DS	557
Požadavky na změnu schématu služby AD DS	558
Spuštění schématu služby Active Directory	558
Změna schématu	559
Správa rolí hlavních operačních serverů	565
Přenos rolí hlavních operačních serverů	568
Převzetí rolí hlavního operačního serveru	570

Audit služby AD DS	571
Konfigurace zásad auditu.	571
Povolení auditu změn služby AD DS	574
Shrnutí	576
Kapitola 18 Správa protokolu TCP/IP	577
Použití protokolu DHCP	578
Navrhování sítí s protokolem DHCP	578
Přidání role serveru DHCP	580
Vytvoření nového oboru.	586
Autorizování serveru DHCP a aktivace oborů	593
Přidání rezervací adres.	594
Použití více serverů DHCP pro redundanci	595
Nastavení přenosového agenta DHCP	596
Správa serveru DHCP na příkazovém řádku	598
Použití serveru DNS	599
Nastavení serveru DNS.	599
Vytváření subdomén a delegování oprávnění	606
Přidání záznamů prostředků	608
Konfigurace přenosů zón	610
Spolupráce s jinými servery DNS	612
Nastavení serveru pro předávání.	612
Nastavení serveru WINS	615
Shrnutí	616
Kapitola 19 Implementace správy disků	617
Porozumění terminologii disků	618
Přehled správy disků	620
Vzdálená správa.	623
Dynamické disky.	623
Příkazový řádek	624
Přidání nového disku	624
Oddíly a svazky	627
Vytvoření svazku nebo oddílu.	627
Vytváření rozšířených oddílů a logických jednotek	632
Převod disku na dynamický disk	632
Převod disku na disk typu GPT	633
Změna velikosti svazku.	634
Přidání zrcadlení do svazku.	637
Nastavení diskových kvót	642
Povolení kvót na disku	642
Nastavení kvót pro uživatele	644
Import a export kvót.	646

Zapnutí šifrování souborů	647
Shrnutí	650
Kapitola 20 Správa úložišť	651
Použití Správce prostředků souborového serveru (File Server Resource Manager)	652
Instalace a počáteční konfigurace Správce prostředků souborového serveru (File Server Resource Manager)	652
Plánování sestav úložišť	655
Použití adresářových kvót	658
Blokování souborů	664
Úvod k nástroji SAN Manager	670
Koncepty a terminologie	671
Instalace nástroje Správce úložiště pro síť SAN (Storage Manager For SANs)	674
Použití konzoly Správce úložiště pro síť SAN (Storage Manager For SANs)	674
Správa připojení serveru	675
Správa cílů iSCSI	677
Správa zabezpečení iSCSI	678
Přihlašování k cílům iSCSI	680
Vytváření a instalace logických jednotek	680
Rozšíření logické jednotky (LUN)	686
Vyměnitelné úložiště	688
Koncepty a terminologie	688
Použití a správa	692
Shrnutí	696
Kapitola 21 Použití clusterů	697
Co je cluster	697
Clusterly služby Vyrovnávání zatížení sítě	698
Clusterly s podporou převzetí služeb při selhání	698
Nové funkce clusterů s podporou převzetí služeb při selhání	698
Jádro systému Windows Server 2008	700
Scénáře clusterů	700
Webový server	700
Terminálová služba	701
Rozhodující aplikace a služby	701
Požadavky a plánování	701
Označení a stanovení cílů	702
Označení a vyjádření rizik	702
Vytvoření seznamu	703

Clustery služby Vyrovnávání zatížení sítě (NLB)	703
Klíčové pojmy služby NLB.	703
Volba modelu clusteru NLB.	704
Vytvoření clusteru služby Vyrovnávání zatížení sítě (cluster NLB).	705
Plánování kapacity clusteru NLB	713
Zajištění odolnosti proti chybám	713
Optimalizace clusteru NLB	714
Clustery s podporou převzetí služeb při selhání.	714
Klíčové pojmy týkající se clusteru	
s podporou převzetí služeb při selhání	715
Typy prostředků.	716
Definování zásad převzetí služeb při selhání	
a navrácení služeb po obnovení (failover a failback).	719
Konfigurace clusteru s podporou převzetí služeb při selhání.	720
Plánování kapacity clusteru s podporou převzetí služeb při selhání	721
Vytvoření clusteru s podporou převzetí služeb při selhání	723
HPC clustery	735
Shrnutí	738

ČÁST IV

Zabezpečení sítě

Kapitola 22 Plánování zabezpečení	741
Základní principy zabezpečení	742
Důvěrnost.	742
Jednota	743
Dostupnost.	743
Osm pravidel zabezpečení	744
Pravidlo minimálních práv	745
Pravidlo správy změn	745
Pravidlo důvěry	745
Pravidlo nejslabšího článku	745
Pravidlo oddělování	745
Pravidlo trojdílného procesu	746
Pravidlo preventivních opatření	746
Pravidlo okamžité a řádné odpovědi	746
Šablona vyšší bezpečnosti	746
Uvažujte ve smyslu zón.	748
Vytvořte zachytňné body	749
Rozvrstvěte své zabezpečení	750
Pochopte zabezpečení vztahů	751
Rozdělte zodpovědnost.	753
Shrnutí	754

Kapitola 23 Implementace zabezpečení	755
Úvod	755
Zabezpečená instalace	756
Jádro serveru	759
Průvodci rolí a funkcí	761
Zabezpečení spouštění počítače: nástroj BitLocker	764
Nastavení funkce BitLocker	765
Zabezpečení účtů	771
Zakázání účtu správce (administrátora)	771
Zásady hesel na samostatných serverech	772
Zásady hesel v doménách	773
Brána firewall systému Windows Server 2008	776
Nastavení brány firewall pomocí Zásad skupiny	778
Základy pravidel brány firewall	780
Definice pravidel	780
Vytvoření zásady brány firewall	782
Brána firewall systému Windows přes příkazový řádek	784
Další změny zabezpečení	786
Nové skupiny	786
Auditování	787
Hash hodnoty nástroje LanMan a úroveň ověření	787
SMBv2	788
Řadiče domény jen pro čtení	788
Shrnutí	788
Kapitola 24 Správa Architektury NAP	789
K čemu je potřeba NAP?	789
Plánování nasazení	791
Co nakoupit pro architekturu NAP	791
Servery potřebné pro architekturu NAP	792
Výhody architektury NAP	793
Určení zásad stavu	793
Kontrolované zásady	794
Úrovně vynucení	795
Rozhodnutí o výjimkách	796
Testování vynucení IPsec NAP	797
Nastavení certifikačního serveru	798
Konfigurace serveru zásad stavu NAP	807
Nastavení klientů architektury NAP	808
Vynucení architektury NAP ve standardu IEEE 802.1x	817
Konfigurace vynucení standardu IEEE 802.xz	818
Konfigurace vynucení standardu 802.1X	818

Zásady nasazení	819
Shrnutí	822
Kapitola 25 Správa oprav	823
Proč je to důležité	824
Cyklus oprav	825
Ohodnocení	825
Identifikace	826
Odhadnutí a plánování	827
Nasazení	828
Opakování	828
Testování nasazení	828
Nasazení na testovací síť	828
Použití beta testovacích uživatelů	829
Plné nasazení	829
Získávání aktualizací	830
Automatické aktualizace	830
Služba WSUS (Windows Server Update Services)	830
Správce konfigurací SCCM (Systems Center Configuration Manager) ..	834
Produkty třetích stran	834
Shrnutí	835
Kapitola 26 Implementace strategií vzdáleného přístupu:	
SSTP, VPN a bezdrátový přístup	837
Úvod	837
Server NPS (Network Policy Server)	838
Plánování pro server NPS	838
Začněte zásadami	839
Definujte podporu	840
Protokol SSTP (Secure Sockets Tunneling Protocol)	840
Proces připojení pomocí protokolu SSTP	840
Konfigurace protokolu SSTP	842
Instalace ověřovacího certifikátu serverů (Server Authentication Certificate)	847
Instalace služby Směrování a vzdálený přístup (Routing And Remote Access)	857
Konfigurace klientů založených na protokolu SSTP	866
Tvorba spojení protokolu SSTP	870
Řešení problémů se spojením	873
Použití serveru NPS v systému Windows Server 2008	876
Konfigurace vzdáleného přístupu dle uživatelů	876
Konfigurace vzdáleného přístupu v zásadách sítě NPS	877

Bezdrátová nasazení	879
Požadavky	880
Přidání klientů RADIUS do sítě	882
Konfigurace Přístupových bodů	884
Konfigurace klientů k použití zabezpečeného bezdrátového připojení ..	885
Shrnutí	890

ČÁST V

Použití podpůrných služeb a funkcí

Kapitola 27 Spolupráce mezi systémy	893
Obecná spolupráce se systémem UNIX.	893
Koncepty oprávnění a zabezpečení.	894
Výpis souborů v systému UNIX	894
Symbolické odkazy	896
Úrovně práv	897
Základní konektivita	897
Protokol FTP (File Transfer Protocol)	898
Služba Telnet	898
Souborové systémy	899
Tisk	901
Systém souborů NFS (Network File System)	901
Starší verze služby Mapování uživatelských jmen	903
Server pro službu NFS	905
Správa identit pro systém UNIX	912
Instalace Správy identit pro systém UNIX	913
Subsystem pro unixové aplikace (SUA)	917
Spolupráce se systémy Macintosh	921
Shrnutí	921
Kapitola 28 Správa softwaru	923
Používáme rozšíření Zásad skupiny pro instalaci softwaru	924
Nalezení správné kombinace služeb	925
Balíčky instalační služby systému Windows	926
Soubory Zap.	926
Nastavení rozšíření Zásad skupiny pro instalaci softwaru	928
Vytváření bodu distribuce softwaru	929
Vytvoření objektu zásad skupiny (GPO) pro nasazení aplikací	929
Konfigurace rozšíření Zásad skupiny pro instalaci softwaru	932
Práce s balíčky	936
Přidání balíčku do Zásad skupiny.	936
Změna vlastností aplikace	939

Použití balíčků vylepšení	940
Použití modifikací balíčků	942
Odstranění a opětovné nasazení balíčků	943
Používání Zásad omezení softwaru	944
Jak fungují zásady omezení softwaru	945
Vytvoření Zásad omezení softwaru	945
Služba pro nasazení systému Windows (Windows Deployment Services)	948
Shrnutí	948
Kapitola 29 Práce se službou Windows Virtualization	949
Přehled funkce Hyper-V	950
Scénáře	951
Požadavky	952
Instalace	953
Instalace ve verzi jádra serveru	953
Instalace v systému Windows Server 2008	953
Počáteční konfigurace	956
Konfigurace sítí	957
Nastavení serveru	960
Vytvoření virtuálního počítače	961
Vytvoření základního virtuálního počítače	962
Nastavení počítače	966
Nastavení správy	980
Práce s virtuálním počítačem	982
Spouštění, zastavování, ukládání a snímkování	983
Schránka	984
Export/Import	985
Shrnutí	988
Kapitola 30 Nasazení terminálových služeb	989
Koncepty	991
Vzdálený přístup	992
Centrální správa	992
Požadavky	993
Paměť RAM	993
Procesor (CPU)	993
Využití sítě	994
Plánování kapacity	994
Instalace	995
Zlepšení možností uživatelů	1004
Povolení Vzdálené plochy pro režim správy	1007
Instalace programů	1008

Správa	1010
Správce Terminálové služby	1011
Konfigurace Terminálové služby	1020
Licencování Terminálové služby	1025
Instalace licencování Terminálového serveru	1025
Vzdálené aplikace RemoteApps	1028
Správce vzdálených aplikací RemoteApp TS	1029
Přidání vzdálené aplikace RemoteApps	1034
Nasazení vzdálených aplikací RemoteApps	1036
Webový přístup k TS	1039
Webové připojení vzdálené plochy	1040
Aplikace RemoteApp programu TS Web Access	1041
Shrnutí	1042
Kapitola 31 Internetová informační služba	1043
Architektura	1044
Komponenty	1044
Moduly	1045
Instalace služby IIS	1047
Instalace pomocí Průvodce přidáním rolí (Server Roles Wizard)	1047
Instalace pomocí Správce balíčků systému Windows	1048
Nástroje pro správu	1049
Správce Internetové informační služby (IIS)	1050
AppCmd.exe	1052
Nástroj Windows Management Instrumentation (WMI)	1054
Úkoly správy	1054
Správa serverů	1055
Správa webů	1065
Správa webových aplikací	1073
Správa virtuálních adresářů	1074
Porozumění delegováním a oprávněním	1074
Delegování správy stránek a aplikací	1075
Konfigurace oprávnění k prohlížení a správě obsahu	1077
Porozumění úložišti konfigurace	1078
Použití sdílené konfigurace	1079
Vzdálená správa	1079
Instalace a správa Služby publikování FTP	1080
FTP Current Sessions	1082
FTP Directory Browsing	1082
FTP Firewall Support	1082
FTP Messages	1082
FTP SSL Settings	1083

FTP User Isolation.	1083
Služba AD FS (AD FS – Active Directory Federation Services)	1083
Shrnutí	1084

ČÁST VI

Ladění, údržba a oprava

Kapitola 32 Spolehlivost systému Windows a sledování výkonu	1087
Používáme Zobrazení zdrojů	1088
Podrobnosti o jednotce CPU	1089
Podrobnosti o disku	1090
Podrobnosti o síti	1090
Podrobnosti o paměti	1090
Použití nástroje Sledování výkonu	1090
Přidávání čítačů v nástroji Sledování výkonu	1092
Změna zobrazení nástroje Sledování výkonu	1093
Uložení obrazovky nástroje Sledování výkonu	1094
Připojení ke vzdálenému počítači pomocí Sledování výkonu	1094
Použití nástroje Sledování spolehlivosti	1095
Prohlížení Sledování spolehlivosti na vzdáleném počítači	1095
Interpretace indexu stability systému	1096
Vytvoření sady kolekcí dat	1099
Vytvoření sady kolekcí dat ze šablony	1100
Vytvoření Sady kolekcí dat z nástroje Sledování výkonu	1102
Vytvoření Sady kolekcí dat ručně	1103
Vytvoření Sady kolekcí dat pro sledování výkonu Čítače	1105
Plánování shromažďování dat	1105
Správa shromážděných dat	1107
Práce s datovými soubory protokolu	1109
Prohlížení sestav	1110
Shrnutí	1111
Kapitola 33 Plánování pro případ havárie	1113
Plánování pro případ havárie	1114
Rozpoznání rizik	1114
Rozpoznání prostředků	1115
Vytvoření reakcí	1116
Vyzkoušení reakcí	1119
Opakování postupu	1120
Příprava na havárii	1121
Nastavení systému odolného proti chybám	1121
Zálohování systému	1121

Oprava systému	1121
Zadání možností zotavení	1123
Shrnutí	1125
Kapitola 34 Použití zálohování	1127
Instalace Služby zálohování	1127
Uživatelé nástroje Ntbackup	1128
Plánování zálohy	1129
Výběr svazků pro zálohování	1129
Určení místa úložiště	1129
Vytvoření plánu zálohy	1130
Implementace rotující sady záloh	1133
Změna plánování záloh	1135
Zastavení plánovaných záloh	1136
Použití Průvodce jednorázovým zálohováním	1136
Použití příkazu Wbadmin	1139
Wbadmin enable backup	1139
Wbadmin disable backup	1139
Wbadmin start backup	1139
Wbadmin stop job	1140
Wbadmin start recovery	1140
Wbadmin start systemstatebackup	1140
Wbadmin start systemstaterecovery	1140
Wbadmin start sysrecovery	1140
Prostředí zotavení systému Windows	1141
Wbadmin get versions	1141
Wbadmin get status	1141
Obnovení vašeho serveru	1144
Obnova svazků	1144
Obnova souborů složek z místního serveru	1145
Obnova souborů složek z jiného serveru	1147
Obnova aplikací a dat	1148
Obnova operačního systému	1150
Obnova katalogu záloh	1151
Shrnutí	1152
Kapitola 35 Plánování odolnosti proti chybám	1153
Střední doba poruchy a střední doba zotavení	1154
Ochrana napájecího zdroje	1155
Selhání místního napájecího zdroje	1156
Kolísání síťového napětí	1157
Krátkodobé výpadky napájení	1159
Dlouhodobé výpadky napájení	1160

Disková pole.....	1160
Hardwarová a softwarová řešení.....	1160
Úrovně polí RAID a odolnost proti chybám.....	1161
Systémy s disky hot-swap a hot-spare	1166
Distribuovaný souborový systém DFS	1167
Clustery.....	1167
Vyrovnávání zatížení sítě	1167
Clustery s podporou převzetí služeb při selhání.....	1167
Shrnutí	1168
Kapitola 36 Správa registru.....	1169
Úvod k registru	1169
Původ registru.....	1169
Jak se používají data registru	1171
Změny funkcí v systému Windows Server 2008	1171
Princip struktury registru	1173
Kořenové klíče	1176
Hlavní podklíče	1177
Způsob uložení dat	1180
Vytvoření položek registru pomocí Průvodce registrem (Registry Wizard) ...	1182
Použití editorů registru	1184
Rychlá prohlídka Editoru registru	1185
Rychlá prohlídka programu Reg.....	1192
Zálohování a obnovení registru	1193
Výběr metody zálohování	1193
Obnovení systému.....	1195
Shrnutí	1195
Kapitola 37 Řešení systémů a obnovení systému.....	1197
Určení priorit	1197
Obnova systému	1199
Určení možných příčin.....	1199
Vrácení změn ovladače zařízení	1200
Obnovení vašeho serveru.....	1200
Obnova svazků.....	1201
Obnova souborů složek z místního serveru	1202
Obnova souborů složek z jiného serveru.....	1203
Obnova aplikací a dat	1204
Obnova operačního systému	1206
Obnova stavu systému	1208
Použití systémových informací	1209

	Ověření stavu služeb.....	1209
	Použití nástroje Konfigurace systému	1212
	Použití nástroje System File Checker	1213
	Použití Přehledu událostí vypnutí	1213
	Shrnutí	1214
Příloha A	Změny v rozhraní oproti systému	1215
	Windows Server 2003	1215
Příloha B	Volitelné komponenty.....	1221
Příloha C	Poznejte protokol TCP/IP verze 4.....	1231
	Rodina protokolů TCP/IP	1231
	Protokol IP (Internet Protocol).....	1232
	Protokol TCP (Transmission Control Protocol).....	1232
	Protokol UDP (User Datagram Protocol)	1233
	Rozhraní Windows Sockets	1233
	Rozhraní NetBIOS.....	1234
	Dokumenty RFC (Requests for Comments).....	1234
	Adresy IP a co znamenají	1236
	Síť třídy A	1236
	Síť třídy B	1237
	Síť třídy C	1237
	Adresy třídy D a třídy E	1237
	Směrovače a podsítě.....	1238
	Co je to podsít?	1238
	Brány a směrovače.....	1240
	Směrovací protokoly a protokoly překladu adres.....	1240
	Překlad názvů	1241
	Služba DNS (Domain Name System).....	1242
	Protokol DHCP (Dynamic Host Configuration Protocol)	1246
	Služba WINS (Windows Internet Name Service)	1248
	Shrnutí	1250
0 autorech		1251
Rejstřík		1253

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 Dickinsonovi (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 společnosti HP v Kanadě, SanSanu Strozierovi z HP ve Spojených Státech, Sharon Fernandezové z Hill & Knowlton (což je firma pro komunikaci s veřejností společnosti HP, a hlavně Davidu Chinovi, také z firmy Hill & Knowlton) za umožnění zápůjčky a štedrost 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 první 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 vašim 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.

- Jádru 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 trochu 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 nejedostupnější. 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 trochu 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

Kapitola 2: Představení adresářových služeb

Kapitola 3: Plánování oborů názvů a domén

Kapitola 4: Plánování nasazení

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 okouzly 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 rajska 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 popsány v kapitole 29 (Práce se službou Windows Virtualization).

Jádro serveru

Používáte-li systém Windows Server 2008, můžete nainstalovat vysoce zabezpečené minimální prostředí s nízkou režii 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 směřován 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 téže 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 relo-kace 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).

Služba 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 režii 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,