

Správa Windows Serveru 2008

průvodce pokročilého
správce

Bohdan Cafourek

EDICE
PROFESIONÁL

GRADA

- Nové vlastnosti verze 2008 a jejich přínos pro správu sítě
- Konfigurace a optimalizace Active Directory
- Zálohování, obnova a záchrany systému
- Tajnosti skriptování a příkazového řádku
- Spolupráce Serveru 2008 a Windows Vista
- Využití Core edice a RODC

Upozornění pro čtenáře a uživatele této knihy

Všechna práva vyhrazena. Žádná část této tištěné či elektronické knihy nesmí být reprodukována a šířena v papírové, elektronické či jiné podobě bez předchozího písemného souhlasu nakladatele. Neoprávněné užití této knihy bude **trestně stíháno**.

Používání elektronické verze knihy je umožněno jen osobě, která ji legálně nabyla a jen pro její osobní a vnitřní potřeby v rozsahu stanoveném autorským zákonem. Elektronická kniha je datový soubor, který lze užívat pouze v takové formě, v jaké jej lze stáhnout s portálu. Jakékoliv neoprávněné užití elektronické knihy nebo její části, spočívající např. v kopírování, úpravách, prodeji, pronajímání, půjčování, sdělování veřejnosti nebo jakémkoliv druhu obchodování nebo neobchodního šíření je zakázáno! Zejména je zakázána jakákoliv konverze datového souboru nebo extrakce části nebo celého textu, umísťování textu na servery, ze kterých je možno tento soubor dále stahovat, přitom není rozhodující, kdo takovéto sdílení umožnil. Je zakázáno sdělování údajů o uživatelském účtu jiným osobám, zasahování do technických prostředků, které chrání elektronickou knihu, případně omezují rozsah jejího užití. Uživatel také není oprávněn jakkoliv testovat, zkoušet či obcházet technické zabezpečení elektronické knihy.



Copyright © Grada Publishing, a.s.



Copyright © Grada Publishing, a.s.



Copyright © Grada Publishing, a.s.

Obsah

Úvod.....	13
1. Vlastnosti a instalace.....	15
1.1 Vlastnosti Windows Serveru 2008	15
1.2 Požadavky na hardware.....	17
1.3 Rozdíly jednotlivých edicí.....	18
1.4 Postup instalace.....	19
1.4.1 Inovační instalace	21
1.4.2 Shrnutí instalačních fází	24
1.5 Parametry instalace	26
1.5.1 Parametry programu Setup	26
1.6 Bezobslužná instalace.....	27
1.6.1 Struktura bezdotazové instalace	28
1.7 Inovace Active Directory.....	29
1.8 Příprava pomocí Adprep	29
2. Active Directory.....	31
2.1 Návrh a design	31
2.1.1 Adresářové služby.....	31
2.1.2 Členění Active Directory.....	32
2.1.3 Logická a fyzická struktura	34
2.1.4 Česká terminologie	35
2.1.5 Funkční úrovně domény.....	36
2.1.6 Funkční úrovně pro forest	38
2.1.7 Typy vztahů důvěry	40
2.1.8 Ruční definování trustu	42
2.1.9 Dotazy při instalaci	43
2.1.10 Více řadičů.....	44
2.1.11 Rozmístění řadičů a jejich rolí	44
2.1.12 Problémy s operačními servery.....	45
2.1.13 Active Directory Sizer	46

2.2	Instalace řadičů domény	47
2.2.1	Průběh instalace	49
2.2.2	Vlastnosti serveru DNS	57
2.2.3	Problémy při instalaci řadiče.....	59
2.2.4	Instalace ze záložního média.....	59
2.2.5	Automatická instalace Active Directory.....	60
2.2.6	Druhý řadič do domény.....	62
2.3.	Organizační jednotky.....	63
2.3.1	Tři stupně administrace	63
2.3.2	Rozložení organizačních jednotek	64
2.3.3	Vytvoření organizační jednotky	64
2.3.4	Vytvoření organizační jednotky příkazem	66
2.3.5	Delegace oprávnění	67
2.3.6	Zobrazení delegací.....	68
2.3.7	Úprava delegovaných oprávnění	69
2.3.8	Přesná oprávnění.....	70
2.3.9	Neviditelnost objektů	71
2.4	Uživatelé a skupiny.....	72
2.4.1	Typy uživatelských účtů.....	72
2.4.2	Nový uživatel příkazem	75
2.4.3	Spolupráce příkazů	76
2.4.4	Výmaz uživatelů	76
2.4.5	Skupiny uživatelů	77
2.4.6	Skupiny a SID.....	78
2.4.7	Typy skupin a jejich rozsah.....	81
2.4.8	Příkazy pro skupiny.....	81
2.5	Údržba a zálohy.....	84
2.5.1	Automatická údržba.....	85
2.5.2	Mechanismus replikace	85
2.5.3	Manuální replikace	86
2.5.4	Replikační monitor	86
2.5.5	Údržba pomocí Ntdsutil	87
2.5.6	Kontrola Active Directory.....	89
2.5.7	Sekce Local Roles	89
2.5.8	Správce pro obnovu	90
2.5.9	Duplicitní SID	90
2.5.10	Odstranění poškozeného řadiče domény	90
2.5.11	Role hlavního operačního serveru	91
2.5.12	Změny rolí FSMO	93
2.5.13	Odinstalování řadiče.....	95
2.5.14	Stavy doménového řadiče	97

2.6	Speciální řadiče	98
2.6.1	RODC	98
2.6.2	Instalace RODC	99
2.6.3	Výroba instalačního média	100
2.6.4	Instalace AD DS z média.....	101
2.6.5	Příkazy ntdsutl ifm.....	101
2.6.6	Přípravná procedura	103
2.6.7	Restartovatelné služby AD DS.....	105
2.6.8	Server CORE	107
2.6.9	Administrace edice Server Core.....	108

3. Zásady skupiny 113

3.1	Mechanismus Group Policy	113
3.1.1	Objekty a nastavení zásad.....	115
3.1.2	Priorita zásad	119
3.1.3	Dědění zásad	121
3.1.4	Pokročilá ovlivnění priorit	123
3.1.5	Položky pro správce.....	126
3.1.6	Časování zásad	129
3.1.7	Ovlivnění chodu zásad.....	130
3.1.8	Ruční aktualizace zásad	130
3.1.9	Využití šablon	131
3.1.10	Šablony zabezpečení.....	132
3.1.11	Šablony pro správu	134
3.1.12	Export zabezpečení.....	134
3.1.13	Výsledné zásady	135
3.1.14	Resultant Set of Policy v GPMC	136
3.2	Group Policy Modeling v GPMC.....	139
3.2.1	Hledání v objektech GPO	140
3.3	Údržba objektů	142
3.3.1	Zálohování objektů GPO.....	142
3.3.2	Postup zálohy	142
3.3.3	Obnova objektů zásad.....	143
3.3.4	Kopírování zásad skupiny.....	144
3.3.5	Import objektu GPO	145
3.3.6	Upozornění k úplné obnově.....	145
3.3.7	Řešení problémů se zásadami.....	146

4. Bezpečnost	147
4.1 Principy zabezpečení	147
4.1.1 Autentikace a autorizace	147
4.1.2 Bezpečnost dat	148
4.1.3 Základní typy útoků	152
4.2 Šifrování	153
4.2.1 Šifrování EFS	153
4.2.2 Postup šifrování	155
4.2.3 Technologie BitLocker	159
4.3 Autentikace a síť	165
4.3.1 Způsoby autentikace	165
4.3.2 Problémy s autentikací	167
4.3.3 Řešení problémů se zabezpečením	167
4.4 Firewall	168
4.4.1 Útoky proti firewallu	168
4.4.2 Nastavení firewallu	169
4.4.3 Porty potřebné v síti	170
4.5 IPSec	171
4.5.1 Zabezpečení paketů IP	171
4.5.2 GPO a IPSec	174
4.5.3 Vytvoření vlastní zásady IPSec	175
4.5.4 Doporučení pro zavádění	179
4.6 Spolupráce komponent	179
4.6.1 Microsoft Baseline Security Analyzer	179
4.6.2 Vzdálená plocha	180
4.6.3 Software Update Services	182
4.6.4 Překlad adres a IPSec	184
4.6.5 Názvové služby	186
5. Zálohování	193
5.1 Co a proč zálohovat?	193
5.2 Windows Server Backup	194
5.2.1 Zadání opakovaného spouštění zálohy	199
5.2.2 Základní postupy obnovy	200
5.2.3 Nová pravidla zálohování	201
5.2.4 Zálohování a práva	203
5.2.5 Záloha a obnova Active Directory	203

5.2.6	Úplná obnova domény	203
5.2.7	Neautoritativní obnova AD DS	204
5.2.8	Obnova příkazem	205
5.2.9	Kontrola správné obnovy	206
5.2.10	Parametry startu systému	207
5.2.11	Instalační médium.....	207
5.2.12	Výmaz objektů v AD DS.....	208
5.2.13	Změna konfigurace AD DS	209
5.2.14	Zálohovací příkazy.....	210
5.2.15	Robocopy	211
6.	WMIC	215
6.1	Význam WMI a WMIC	215
6.2	Uživatelé a skupiny.....	218
6.2.1	Výpisy uživatelů.....	218
6.2.2	Výběr položek uživatelů.....	219
6.3	Počítač a zdroje	224
6.3.1	Informace a řízení operačního systému	224
6.3.2	Informace o počítači.....	226
7.	Skriptování.....	231
7.1	Úvod do WSH	231
7.1.1	Proč skripty?.....	231
7.1.2	Volání skriptů	232
7.1.3	Kompatibilita skriptů.....	232
7.1.4	Druhy skriptování.....	233
7.1.5	VBScript kontra Windows Script Host	233
7.1.6	WScript.....	234
7.1.7	CScript.....	235
7.1.8	Skripty WSF.....	235
7.2	Jak začít psát?	236
7.2.1	Základy syntaxe	236
7.2.2	Podmínky.....	237
7.2.3	Smyčky	239
7.2.4	První krůčky.....	240
7.2.5	Objekty	241
7.2.6	Skript využívající metodu	241
7.2.7	Object Browser.....	242

7.2.8	Zajímavé knihovny	244
7.2.9	Ovládací tlačítka a boxy	245
7.2.10	Informace o disku	246
7.2.11	Skripty pro všední den	247
7.3	Skripty pro správce	248
7.3.1	Licence Serveru 2008	248
7.3.2	Mapování složky a tiskárny	248
7.3.3	Otestujeme volné místo	249
7.3.4	Logon skript	249
7.3.5	Práce s daty	250
7.3.6	Podrobné informace o discích	251
7.4	ADSI	252
7.4.1	Nová organizační jednotka a uživatel	252
7.4.2	Hromadné vytvoření objektů	253
7.4.3	Vytvoření skupiny uživatelů	255
7.5	Změna místních účtů	256
7.5.1	Kam uživatel patří?	256
7.5.2	Odemčení účtu uživatele	257
7.5.3	Práce s rolemi FSMO	258
7.6	WMI	258
7.6.1	Skripty WMI	258
7.6.2	Informace o souborech	259
7.6.3	Identifikace startujícího systému	261
7.6.4	Výpis spořiče obrazovky	262
7.6.5	Informace o stránkovém souboru	263
7.6.6	Informace o procesoru	264
7.6.7	Přístup na instalované aplikace	264
7.6.8	Sdílené složky	267
7.6.9	Práce s registrem	268
7.6.10	Startup command	268
7.6.11	Výpis lokálních uživatelů	269
7.6.12	Start aplikace ve skrytém okně	270
7.6.13	Informace o službách	271
7.6.14	Zastavení služby	272
7.6.15	Seznam procesů včetně cesty a priority	273
7.6.16	Změna priority procesu	274
7.6.17	Ukončení procesu	275
7.6.18	Vyhodnocení vlastností počítače	276
7.6.19	Shutdown či restart	276
7.6.20	Převzetí vlastnictví	277

7.6.21	Komprese	278
7.6.22	Generátory skriptů	278
7.7	Zabezpečení skriptů	280
7.7.1	Odstranění souborů	280
7.7.2	Zrušení asociací	280
7.7.3	Nastavení oprávnění	281
7.7.4	Roztřídění skriptů	281
7.7.5	Digitální podepisování skriptu	281
7.7.6	Zásady softwaru	281
7.7.7	Antivirový software a blokování skriptů	281
7.7.8	Vzdálené spouštění a nejmenší oprávnění	281
7.7.9	Brány firewall	283
7.7.10	Závěrečná pravidla	283
Rejstřík		287

Úvod

Tato kniha se zaměřuje na středně pokročilé správce přecházející na Windows Server 2008. Takové, kteří již rok či více používají systémy Windows Server 2003. Jste v této situaci a potřebujete bezbolestně přejít na novou verzi? Nemáte na aktualizaci rok času, a tak potřebujete konkrétní a přesné informace. Nechcete mít v knize obrázky jen pro zpestření, ale nasnímané obrazovky, které budou přesně popisovat daný problém a budete je muset podrobně studovat? Pak je tato kniha pro vás vhodná.

Další podrobnosti (jistě víte, že na 300 stran se nevejde všechno...) budete těžit se znalostní báze či ze sady Resource Kit. Zaměření na středně pokročilé správce chápu tak, že nemusíme popisovat, proč je důležité mít nastaveny přísné zásady hesel, či jak vytvořit uživatelský účet a přihlásit se na něj. O tom by si chtěli přečíst začínající správci. Naproti tomu úplně pokročilí budou chtít optimalizovat své propojení VPN či generovat obrazy disků pro instalace RIS – a tak hluboko v této knize nepůjdeme. Budeme se tedy pohybovat mezi těmito mantinely. Budeme popisovat automatizované instalace Serveru 2008 i jeho Active Directory, konfigurovat zásady Group Policy a správcovské postupy si zefektivníme pomocí skriptovacího rozhraní.

Informace, které v této knížce najdete, lze rozdělit do tří kategorií:

- a) Úplné novinky Windows Serveru 2008,
- b) inovované a rozšířené komponenty Windows Serveru 2008,
- c) komponenty, jež jsou obdobné s minulou verzí, ale pravděpodobně je neznáte.

Novinek je ve Windows Serveru 2008 celá řada. BitLocker, RODC, AD DS či Core Edition. Budeme se jim věnovat převážně v kapitolách o instalaci, Active Directory, zálohování a zabezpečení.

Na inovované komponenty se zaměříme v kapitolách o vlastnostech systému a Group Policy.

Na části systému, které jsou podobné ve verzích 2008 a 2003, se podíváme v kapitolách o WMIC a skriptování. Ze své šestnáctileté praxe ve školení vidím, že to jsou komponenty, které mnohdy učiní ze správců skutečné profesionály. Mám za to, že je většina správců buď neumí používat, odsoudí je jako příliš složité, či v nich jen postupuje metodou „pokus – omyl“. A také mám dojem, že neexistuje česky psaná publikace, kde by se správce za jeden týden naučil skriptovat. O to jsem se pokusil v sedmé kapitole této knihy.

Mottem této knížky je tedy „Upgrade správce sítě!“. Tak, jako probíhá upgrade systému, pokusíme se tedy i upgradovat správce (tedy, no ... vlastně vás ... ☺) na ještě vyšší úroveň. A to ve všech klíčových součástech administrace Serveru 2008.

1.

Vlastnosti a instalace

Na úvod celé knihy si představíme souhrn nových vlastností Windows Serveru 2008.

1.1 Vlastnosti Windows Serveru 2008

Novinek je pochopitelně ještě více, než si zde představíme. Je to z toho důvodu, že tato kniha je věnovaná praktické administraci menší sítě. Nevěnuje se tématům pro velké mezinárodní realizace se strukturovanou úrovní šifrování, autentikací, Load Balancing a dalších pokročilých mechanismů. K tomu slouží MS Resource Kit s pěti tisíci stranami. To ovšem neznamená, že čtete knihu začátečnickou. Témata jako skriptování, WMIC nebo instalační média RODC takovými nejsou. Převážně se cílově věnujeme praktické administraci v menší síti s 50 klienty při přechodu na Server 2008. Podle praktické důležitosti pro takovou síť si seřadíme i novinky Windows Serveru 2008:

Server Core

Nová edice MS Serveru, a to bez grafického rozhraní! Získáme tím vyšší spolehlivost, výkon a zabezpečení. Také získáme nižší nároky na HW a práci správce.

1.1 Vlastnosti Windows Serveru 2008

Členění služeb Active Directory

Inovace v Active Directory jsou velmi rozsáhlé. Její komponenty jsou rozdělené podle typu využívání objektů na AD DS, AD FS či AD LDS, jak si popíšeme v oddílu o Active Directory.

Read Only Domain Controller

RODC je novým typem řadiče Active Directory. Takový řadič má pouze jednosměrnou replikaci objektů a správce nemůže jeho objekty editovat.

Restartovatelné AD DS

Služby Active Directory (AD) DS lze za běhu serveru zapínat, vypínat nebo restartovat podle potřeb údržby či zabezpečení.

Integrovaný ADSI Edit

Přímo z editace objektů v konzoli Active Directory je nyní možné upravovat atributy objektu podobně jako v samostatném modulu ADSI Edit. Přibyla totiž karta Attribute Editor ve vlastnostech objektu.

Spolupráce s Windows Vista

Systém Windows Vista pro klienty i systém Windows Server 2008 pro servery představují ideální kombinaci. Společně budou nabízet výhody z hlediska homogenity správy, produktivity a zabezpečení. Ovládání i volby v nabídkách jsou identické. Určité komponenty správy, jako jsou instalace správcovského balíku Adminpak, budou fungovat pouze při této spolupráci. Například funkce NAP (Network Access Protection) využije plně své možnosti také pouze při této serverové i klientské verzi; jen tak je dosaženo vyššího zabezpečení sítě.

BitLocker

Přibývá celá nová způsob šifrování dat na pevném disku. Pracuje na hlubší úrovni než tradiční EFS. Nemá tedy vazbu na jednotlivé uživatele a jejich účet, ale využívá klíčování na objekt operačního systému.

Zálohování a obnova

Inovované postupy zálohování a obnovy integrované do nového programu Windows Server Backup pro kompletní zálohy systémových svazků a systému.

Network Access Protection (NAP)

Pro vysoké zabezpečení síťových komunikací s bloky nastavení požadavků na klienty, jako je antivirový software či existence záplat. Rovněž pro zabezpečení bezdrátových komunikací 802.1x.

Inovace síťových komponent

Přeorganizované klíčové komponenty sítě pro úplnou duální adresační podporu IPv4 a IPv6. Podpora IPv6 pro DHCP, IPSec a PPP.

Internet Information Services

Nová verze webového serveru IIS 7.0 obsahuje škálu novinek především delegovatelnou správu, diagnostiku a aplikační přenosy xcopy.

Windows Firewall

Vyšší zabezpečení s podporou IPSec a protokolů IPv4 i IPv6.

1. Vlastnosti a instalace

Diagnostika

Nové programy pro diagnostiku spolehlivosti a výkonových charakteristik počítače, paměti a komponent.

Integrovaná virtualizace

Technologie Microsoft Hyper-V je Microsoftem realizovaná virtualizace. Jedná se o provoz různých softwarových produktů v různých operačních systémech na jednom fyzickém stroji. Hlavní přínosy tohoto řešení:

- Dynamické rozložení zátěže,
- bezpečnost a spolehlivost (celý disk v „jednom souboru“, jednoduchá obnova),
- testování, zkušební provoz, zaškolení,
- kompatibilita pro starší aplikace,
- virtuální funkčnosti složitějších domén a prostředí,
- různé systémy na jednom stroji.

Špatná zpráva... Tato komponenta virtualizace pravděpodobně není na vašem systému k dispozici! Tento nový virtuální server není součástí instalace systému Windows Server 2008 v okamžiku uvedení na trh. Bude uvolněn jako stábnutelná aktualizace na podzim roku 2008, tedy zhruba půl roku po uvedení systému na trh. Uvidíme, zda bude pak existovat i jako součást instalačních CD/DVD. Proto se v knize této velmi progresivní technologii nemůžeme věnovat.



1.2 Požadavky na hardware

Minimální požadavky na hardware pro Windows Server 2008 standardní edice jsou tyto:

Procesor minimálně	1 GHz (pro procesor x86) 1,4 GHz (pro procesor x64)
Paměť minimálně	512 MB RAM
Volné místo na disku minimálně	8 GB
Jednotka	DVD-ROM
Monitor	SuperVGA (800×600)

Tab. 1.1: Minimální hardwarové požadavky

Doporučené požadavky na hardware pro Windows Server 2008:

Procesor	2 GHz
Paměť	2 GB RAM
Volné místo na disku	40 GB

Tab. 1.2: Doporučený hardware

1.2 Požadavky na hardware

1.3 Rozdíly jednotlivých edicí

Jako všechny předchozí verze je i Windows Server 2008 tvořen několika škálovatelnými edicemi. Jedná se o edice Web, Standard, Enterprise a Datacenter – seřazeno od nejslabější k nejsilnější. Podle zaměření, nároků a možností naší organizace si vybereme tu nejvhodnější.

Role serveru Služba systému	Web	Standard	Enterprise	Datacenter
Web (IIS)	✓	✓	✓	✓
Print	✗	✓	✓	✓
Hyper-V	✗	✓	✓	✓
Active Directory Domain Services	✗	✓	✓	✓
Active Directory Lightweight Directory Services	✗	✓	✓	✓
DHCP Server	✗	✓	✓	✓
DNS Server	✗	✓	✓	✓
File	✗	✓	✓	✓
Server Core	✗	✓	✓	✓
Cluster Nodes	✗	✗	✓ 16 uzlů	✓ 16 uzlů
Network Access Connections (RRAS)	✗	✓ 250 připojení	✓ neomezeno	✓ neomezeno
Network Access Connections (IAS)	✗	✓ 50 připojení	✓ neomezeno	✓ neomezeno
Terminal Services Gateway	✗	✓ 250 připojení	✓ neomezeno	✓ neomezeno
BitLocker Drive Encryption	✗	✓	✓	✓
Telnet Server / Client	✓	✓	✓	✓
Windows PowerShell	✓	✓	✓	✓

Tab. 1.3: Poskytované služby systému

Vazba na vlastnosti hardwaru se u jednotlivých edicí rovněž liší. Celá škála produktu Windows Server 2008 je však ještě širší, než jak by vyplývalo z minulé tabulky. Každá edice (Web, Standard, Enterprise a Datacenter) totiž existuje ve dvou různých instalačních sadách podle toho, zda bude provozována na 32- nebo 64bitovém procesoru. A ještě existuje speciální sada pro 64bitovou verzi s instrukční sadou pro procesory třídy Itanium. Celkem tedy devět různých instalačních sad a výsledných možností. Základní odlišnosti ukáže následující tabulka.

Role serveru HW vlastnost	Web	Standard	Enterprise	Datacenter	Itanium
Přidání RAM za provozu (Hot Add Memory)	✗	✗	✓	✓	✓
Výměna RAM za provozu (Hot Replace Memory)	✗	✗	✗	✓	✓

1. Vlastnosti a instalace

Role serveru HW vlastnost	Web	Standard	Enterprise	Datacenter	Itanium
Přidání a výměna CPU za provozu (Hot Add/ Replace Processors)	x	x	x	✓	✓
Maximální adresovatelná RAM, 32 bitů	4 GB	4 GB	64 GB	64 GB	–
Maximální adresovatelná RAM, 64 bitů	32 GB	32 GB	2 TB	2 TB	2 TB
Maximálně CPU pro 32 bitů	4	4	8	32	–
Maximálně CPU pro 64 bitů	4	4	8	64	64

Tab. 1.4: Hardwarové vlastnosti systému

1.4 Postup instalace

Samotná instalace Serveru 2008 obsahuje překvapivě málo dotazů. Pokud bychom chtěli instalaci ovlivnit více, museli bychom použít režim odpovědního souboru nebo upravovat inicializační soubory pro instalaci, což by ale bylo příliš náročné. Po vložení instalačního DVD z něj *nastartujeme počítač*. Dostaneme se na *výběr národního prostředí*, který ale můžeme klidně ponechat ve výchozí angličtině a kdykoli v průběhu práce se serverem jej můžeme změnit.



Obr. 1.1: Zadání jazyka a národního prostředí instalace

Vlastní spuštění instalace se nám nabídne na následující obrazovce tlačítkem **Install Now**. Tímto způsobem bychom spouštěli klasickou instalaci Serveru 2008 nebo inovaci z minulé verze. Obrazovka pro výběr startu instalace nám nabídne i přístup k informacím, které byste měli vědět před instalací. Můžeme klepnout na text **What to know before installing Windows**. Dále je v nabídce přístup k možnostem zotavení, kde je i funkce pro diagnostiku.

Pokud tedy chceme použít instalaci opravnou (tedy již server 2008 máme instalovaný, ale obsahuje chybu), musíme zvolit nabídku **Repair** v levé dolní části obrazovky:



Obr. 1.2: Volba typu instalace

Pak se dostaneme do *zadávaní produktového klíče*. Zde je důležité upozornit na zaškrtnávací pole automatické aktivace produktu. Toto pole se nachází hned pod produktovým klíčem a je standardně zaškrtnuté. Znamená to, že jakmile se tímto systémem připojíme na Internet, bude zahájen proces automatické aktivace. Dejme si pozor na nastavení sítě a firewall, aby taková aktivace mohla proběhnout. Při zaškrtnutí se pokusí systém Windows Vista po třech dnech provést aktivaci automaticky. V opačném případě můžeme volbu **Automatically activate Windows when I'm online** potlačit. Zrušením zaškrtnutí potlačíme možnost automatické aktivace Windows po Internetu a necháme si možnost aktivovat Windows Server ručně. Nejdéle to smíme odkládat po dobu 30 dnů.

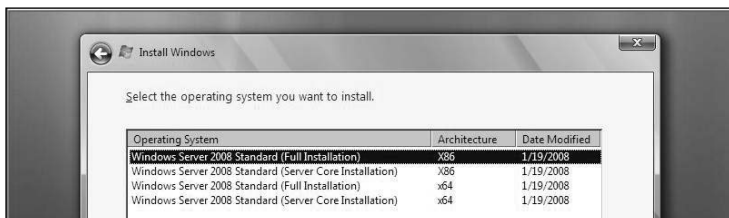


Obr. 1.3: Budeme vypisovat produktový klíč

Nyní se dostáváme ke zcela klíčové volbě – i když jsou zde pouze dva řádky na výběr, toto rozhodnutí *nemůžeme žádným způsobem vrátit zpět* a musíme si je tedy pečlivě promyslet. Vybíráme, zda náš server bude tvořen *plnou instalací nebo instalací Server Core*, která je

1. Vlastnosti a instalace

minimalizovaná a ovládaná z příkazového řádku. Nejsme-li si jisti, vybíráme vždy první možnost, což je klasický plnohodnotný server. Variantě Server Core je věnovaná část na závěr popisu Active Directory této knihy.



Obr. 1.4: Full nebo Server Core?

Pak budeme muset potvrdit, že souhlasíme s licenční smlouvou. Bez tohoto potvrzení v příslušném zaškrtnutém políčku nemůžeme v instalaci pokračovat. Všimněte si, že po celou dobu instalace je v dolní části obrazovky grafický přehled o tom, v jaké části instalační procedury se nacházíme a kolik nás toho ještě čeká. Jak instalace probíhá, zelená linka informující o dokončených činnostech se prodlužuje zleva doprava. Vidíme, že nyní jsme stále v části zaměřené na získávání vstupních informací.



Obr. 1.5: Potvrzení licenčních pravidel

1.4.1 Inovační instalace

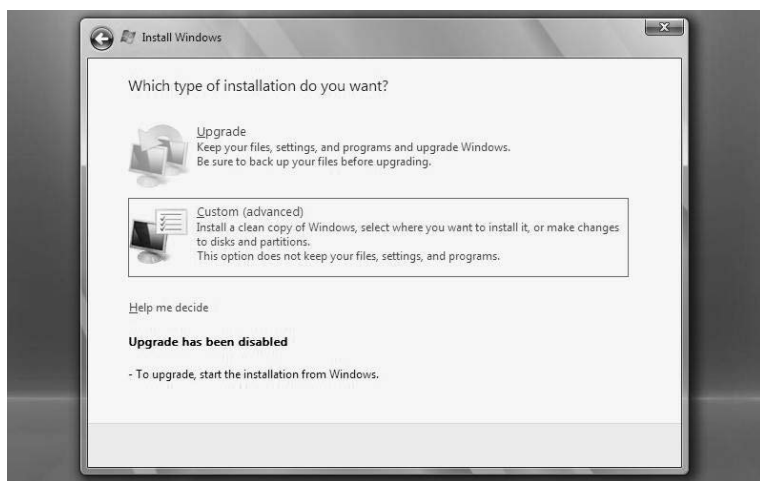
Máme-li na serveru minulou verzi operačního systému, která umožňuje inovaci na Windows Server 2008, bude nám tato inovace nabídnuta volbou **Upgrade** v následující části instalačního průvodce. Při čisté instalaci je dostupná pouze volba **Custom**. Upgrade je možný jen za určitých podmínek a je nutné takovou instalaci spustit přímo ze starší verze Windows Serveru! Budou tak zachovány soubory, nastavení a aplikace z předchozího staršího operačního systému. Konkretizujme si výhody inovace.

1.4 Postup instalace

Výboby inovované instalace jsou především tyto:

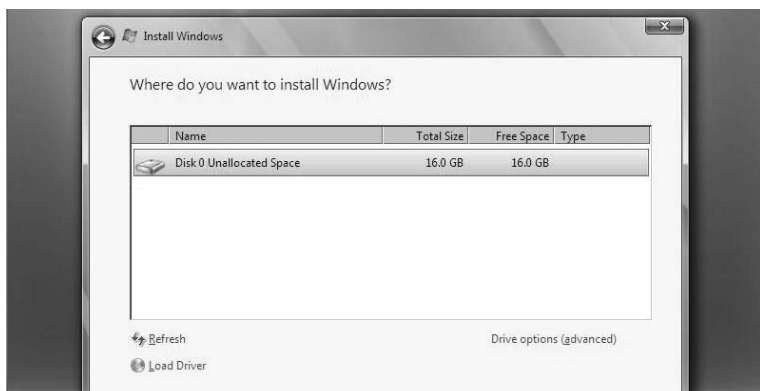
- Ponechání uživatelských účtů a jejich hesel a práv,
- ponechání uživatelských skupin a dalších systémových objektů,
- ponechání datových souborů a složek,
- ponechání dalších konfigurací systému, jako je národní prostředí či multimédia a asociace,
- ponechání nainstalovaných programů a to jak uživatelských, tak správcovských.

V našem případě však máme na počítači pouze klientský operační systém a *nabídka inovace tedy není dostupná*. Inovovat by šlo pouze z minulých verzí serverového systému. Budeme muset zvolit čistou instalaci.



Obr. 1.6: Volba Upgrade je pro nás nedostupná

Na další obrazovce instalačního průvodce zadáváme, *kam chceme náš systém nainstalovat*. Nezadává se název složky, ale pouze disková oblast. Jde takto instalovat na oblasti, které

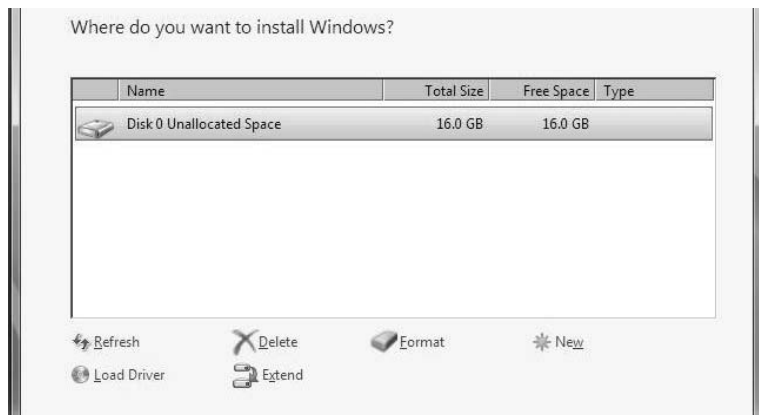


Obr. 1.7: Výběr instalačního disku

1. Vlastnosti a instalace

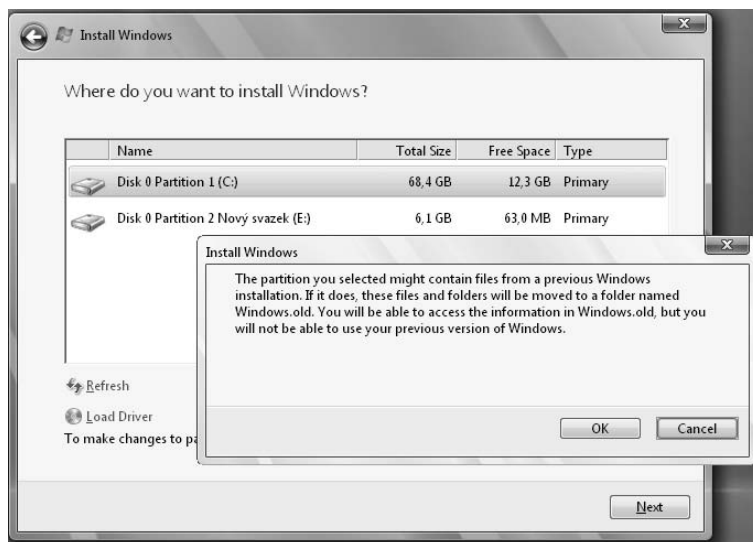
již existují, ovšem můžeme si vytvořit i oblast novou na nevyužitém místě disku. U každé oblasti (ať je existující, nebo prázdná) máme informaci o celkové velikosti a především o volném místě. Vidíme, že pro instalaci je zapotřebí alespoň 7 GB volného místa. Pokud si nemůžeme jednoduše vybrat ze tří nabízených oblastí, lze klepnout na volbu **Drive Options**.

Po stisku nabídky **Drive Options** zůstává přehled oblastí stejný, ale dole přibýly nové možnosti. Mohli bychom oblast na disku odstranit, přeformátovat ji, vytvořit novou oblast na nevyužitém prostoru disku, nebo oblast rozšířit. Vybereme si například první oblast pevného disku a pokračujeme tlačítkem **Next**.



Obr. 1.8: Upřesněné nabídky u diskových oblastí

V této chvíli se může objevit okno s upozorněním na chybu. Jak jsem říkal, v mém případě tato disková *oblast již obsahuje klientský operační systém*, a právě na to jsem upozorněn následující zprávou.



Obr. 1.9: Kolize se starším operačním systémem

1.4 Postup instalace

Jak na tuto kolizi instalace zareaguje? Předchozí operační systém bude přesunut včetně svých programů a dokumentů do složky s názvem `Windows.old`. Ovšem především nebude funkční! Budeme si tedy moci vzít jeho soubory, ale minulý systém spustit nepůjde. To může být velmi překvapivé, zejména když tímto systémem byly v mém případě Windows Vista. Minulá verze serveru (2003) si uměla s Windows XP na stejné diskové oblasti poradit lépe. Zde je u Windows Serveru 2008 situace velmi zjednodušená. *Na každé diskové oblasti může být pouze jeden funkční operační systém.* Výběr systému při startu počítače tu tedy existuje, ale dá na výběr z každé diskové oblasti maximálně jeden systém. Chceme-li tedy například z důvodu testování mít na počítači několik systémů, musíme tomu předem uzpůsobit diskové oddíly a pro každý systém naformátovat oddělenou oblast disku.



Tip

Sám mám na testování rozdělen disk na šest oblastí, každou o velikosti 20 GB. Na první oblasti jsou Windows XP, na druhé Windows Server 2003, na třetí oblasti Windows Vista a dalších oblastech různé edice Windows Server 2008, abych mohl zkoušet doménový řadič, členský či RODC server odděleně. Taková je možnost pro testování. V reálném provozu ale takhle uvažovat nebudeme a velmi pravděpodobně budeme chtít mít na celém serverovém počítači jenom jeden operační systém. Tudiž toto varování pravděpodobně neuvidíte.



Poznámka

Mobli jsme vidět, že dotyčná oblast v mém případě obsahovala pouze 5 GB volného místa, ale instalace psala, že potřebuje 7 GB. V tomto požadavku je již zahrnuta rezerva, která bude pro práci zatíženého serveru potřeba. V mém případě kvůli testování pracuje instalace i server funkčně v pořádku, i když je k dispozici pouze oněch 5 GB volného prostoru.

Toto zadání, kam chceme instalovat, je posledním krokem, jímž ovlivňujeme instalačního průvodce. Teď se již instalace rozbíhá ve své druhé části označené modrou linkou dole na obrazovce. Bude probíhat ještě přibližně 30 minut.

1.4.2 Shrnutí instalačních fází

V závěrečném přehledu o instalaci vidíme, že celý instalační proces je složen z následujících částí:

1. Kopírování instalačních souborů.
2. Rozbalování a třídění souborů na disku.
3. Instalace vybraných součástí a jejich nastavení.
4. Instalace inovačních balíčků.
5. Kompletace instalace.

Velice zjednodušeně můžeme říci, že každá z těchto částí trvá přibližně 10 minut. V průběhu instalace je počítač dvakrát restartován. Po druhém restartu je instalace již dokončena a objeví se okno vyzývající ke změně hesla administrátora.

Toto heslo se v průběhu instalace nezadávalo a budeme je muset vyplnit nyní. Je vyžadováno heslo složité, obsahující alespoň tři různé typy znaků. Po stisknutí tlačítka **OK** je budeme zadávat.

1. Vlastnosti a instalace



Obr. 1.10: Změna hesla administrátora při prvním přihlášení



Obr. 1.11: Heslo musíme vyplnit dvakrát

Rovněž zde máme možnost vytvoření disku, který slouží k obnově hesla, pokud bychom je zapoměli.

Vidíme, že celá instalace systému Windows Server 2008 je velmi zjednodušená a obsahuje polovinu dotazů minulé verze instalace. Hlavním důvodem je to, že všechny otázky týkající se konfigurace operačního systému byly z procesu instalace přesunuty až do momentu jeho prvního spuštění. Jakmile instalace skončí a počítač restartuje, jsme vyzváni k dalšímu zadávání, které bylo dříve součástí instalačního procesu. První je změna hesla lokálního administrátora. Hned poté se spouští nástroj Initial Configuration Tasks. Ten nám umožní provést ty nejzákladnější správcovské kroky, pomocí nichž dojde k nastavení základních parametrů operačního systému – např. adresy IP, časového pásma, nastavení Windows Update atd. Tím možností konfigurace ovšem nekončí. Po ukončení tohoto nástroje se automaticky spustí nástroj Server Manager. Tento nástroj se potom spouští po každém přihlášení uživatele, který je členem lokálních administrátorů (toto chování je možné samozřejmě potlačit). Tímto nástrojem budeme aktivovat role našeho stroje, které nebyly instalací zapnuty, například řadič domény, DHCP, server WINS či DNS.

1.4 Postup instalace



Obr 1.12: Aktivace rolí a funkcí programem Server Manager

1.5 Parametry instalace

Instalaci realizuje program Setup z kořenové složky instalačního DVD. DVD má jinou strukturu než v předchozí verzi serveru a jiné jsou i možnosti ovlivnění a parametrizace instalačního procesu. Není zde žádný program Winnt32 ani jeho obdoba. Bez specifikovaných prepínačů provede Setup.exe běžnou instalaci či upgrade (to v případě, že na disku najde existující systém) ze standardních souborů složky Sources. Můžeme provést následujícími ovlivnění.

1.5.1 Parametry programu Setup

- `/tempdrive:drive_letter` Volba diskové jednotky pro umístění dočasných instalačních souborů. Není-li specifikováno, instalační program vybere tento prostor sám, tedy použije první volný disk. Smí se napsat jen označení celé jednotky, bez názvu adresáře.
- `/unattend` Tento parametr spustí instalaci bez doplňujících dotazů. Nezadává se zde název skriptového souboru, protože se jedná o upgrade. Instalace nebude obsahovat žádné dotazy.
- `/unattend:answer_file` Slouží pro instalaci bez dotazů, použije se nastavení instalace ze zadaného souboru .xml, kde `answer_file` je název odpovědního souboru. Ten musí být umístěn ve zdrojovém adresáři.
- `/m:folder_name` S využitím tohoto prepínače lze použít instalační soubory z pomocné zdrojové složky. Pokud standardní instalační zdroj a tato složka obsahují stejný

1. Vlastnosti a instalace

soubor, přednost budou mít soubory uvedené v adresáři označeném /m. Teprve když se v něm příslušný instalační soubor nenachází, použije se ten na standardní zdrojové cestě. Lze tak inovovat a upravovat instalační sadu.

- /noreboot Potlačí restart počítače po úvodním kopírování souborů. Místo restartu lze potom zadat další příkazy.

Pokud znáte Windows Server 2003 a jeho parametrizaci instalační procedury, vidíte, že zde je možností podstatně méně. Většina přepínačů chybí a kdybychom se je zkusili zadat, budou označeny jako neznáme. Ty existující zjistíme pomocí Setup /?. Důvodem je úplné přepracování instalační procedury a nové vazby na parametrické soubory XML.



1.6 Bezobslužná instalace

Bezobslužná instalace způsobí, že *instalační proces bude klást uživateli méně otázek*; třeba vůbec žádné. Pak by to znamenalo plně bezobslužnou instalaci neboli automatizovanou instalaci.

Míru automatizace čili bezobslužnosti můžeme volit. Bezobslužná instalace Windows Serveru 2008 je zcela odlišná oproti Serveru 2003. Naopak je principiálně shodná s automatizovanou instalací systému Windows Vista.

Instalace a její základní přizpůsobení se zde provádí s pomocí odpovědního souboru `Autounattend.xml`. Tento odpovědní soubor vytvoříme a uložíme na sdílenou složku, disketu či flash-disk. Údaje v něm by měl instalační proces rozpoznat a použít, aby uživatel nemusel téměř nic zadávat. Pro vytvoření souboru automatické instalace a jeho dodatečnou úpravu je výhodné využít balíček Windows Automated Installation Kit (WAIK) stáhnutelný ze stránek Microsoftu. WAIK existuje již i v češtině.

Je však možné odpovědní soubor získat z Internetu přímo, popřípadě jej upravovat editorem XML. Možnosti přizpůsobení souboru neslouží jen pro základní instalaci. Soubor `Autounattend.xml` může být přizpůsoben pro čistou instalaci, kdy veškerá data na disku budou zničena. Můžeme jej ale vytvořit i pro instalaci jiného typu. Často správce nebude tuto automatickou instalaci používat pro servery (ty si raději ohlíká sám), ale pro stanice Windows Vista.

Windows AIK Documentation je elektronická dokumentace pro komponenty Windows Automated Installation Kit (Windows AIK). WAIK je sadou pro profesionální zavádění systémů MS Vista a MS Windows Server 2008 včetně automatizovaných instalací a správy obrazů disku – image. Celková *velikost* zabaleného souboru pro instalaci *WAIK činí na webu Microsoftu 1,1 GB*.

Kromě vlastního nástroje je součástí WAIK i rozsáhlá dokumentace, která má tyto hlavní součásti:

- `Getting_Started_ITPro.rtf` Úvodní informace, zavádění obrazů.
- `Windows AIK User's Guide (waik.chm)` Rozsáhlá nápověda pro celý životní cyklus nasazení WAIK v korporacích, včetně návrhu, výroby a správy image a akcí údržby.
- `Unattended Windows Setup Reference (Unattend.chm)` Zhužštěné informace o struktuře a volbách souboru `Unattend.xml` pro bezobslužnou instalaci.

1.6 Bezobslužná instalace

1.6.1 Struktura bezdotazové instalace

O proces bezdotazové instalace se starají služby Windows Deployment Services. Činnost se skládá ze dvou fází:

- Zpracování odpovědního souboru `Unattend.xml` službami Windows Deployment Services. Soubor je uložen ve složce `\WDSClientUnattend`.
- Zpracování parametrického souboru pro obraz disku – image. Ten bude pro moderní verze systému ve tvaru `Unattend.xml` a pro starší verze systémů ve formátu `Sysprep.inf`. Uložen bude v podsložce `$OEM$` nebo `\Unattend`. *Windows Server 2008 a Windows Vista* používají formát `Unattend.xml`. Systémy *Windows Server 2003 a Windows XP* používají starší formát `Sysprep.inf`

Jako ukázkou si zobrazíme sekci `DiskConfiguration` ze souboru `Unattend.xml` využitelnou jak pro Windows Server 2008, tak pro Windows Vista. Instalace vytvoří dvě nové oblasti na pevném disku pro instalaci Serveru 2008. První oblast pro vlastní instalaci bude primární o velikosti 100 GB a dostane písmeno jednotky C:

```
<DiskConfiguration>
  <Disk>
    <DiskID>0</DiskID>

    <CreatePartitions>
      <!--Create Partition 1-->
      <CreatePartition>
        <Order>1</Order>
        <Type>Primary</Type>
        <Size>100</Size>
      </CreatePartition>

      <!--Create Partition 2-->
      <CreatePartition>
        <Order>2</Order>
        <Type>Primary</Type>
        <Extend>true</Extend>
      </CreatePartition>
    </CreatePartitions>

    <ModifyPartitions>
      <!--Assign Drive Letter C to Partition 1-->
      <ModifyPartition>
        <Order>1</Order>
        <PartitionID>1</PartitionID>
        <Letter>C</Letter>
      </ModifyPartition>
    </ModifyPartitions>
  </Disk>
</DiskConfiguration>
```

Na závěr této části si ukážeme příklad spuštění bezobslužné instalace. Chceme provést síťovou instalaci z instalačního média H odpovědním souborem `Odpoved.xml` a umístěním pracovních souborů na disk D:

```
Setup /unattend:h:odpoved.xml /tempdrive:d
```

1. Vlastnosti a instalace

1.7 Inovace Active Directory

Samotná instalace se neptá, zda chceme mít roli doménového řadiče. Ta se zavádí dodatečně aktivací této role či programem Dcpromo. Případně se aktivuje automaticky, pokud provádíme upgrade z Windows Serveru DC.

Instalační program sám pozná případ, kdy se jedná o inovaci doménového řadiče, a po skončení instalačního programu se po restartu spustí program Dcpromo.exe, který konfiguruje funkci řadiče domény. Tento program tedy není nedílnou součástí instalace, ale její samostatnou procedurou. Programem Dcpromo lze provádět jak povyšování na doménový řadič, tak ponížení do role členského serveru. Pokud Dcpromo nenalezne fungující server DNS, nabídne nám jeho vytvoření na lokálním počítači.

Ovšem mezi instalací systému a instalací či inovací služeb AD DS jsou třeba přípravné procesy. Jedná se o přípravu schématu AD na vyšší funkční úroveň a na nové atributy, které například vyžadují řadiče RODC. Některé scénáře služeb Active Directory Domain Services tyto procesy vyžadují, pro jiné nejsou nezbytné. Jde o to, zda vytváříme nový forest, jaké máme verze řadičů a jaké funkční úrovně. Nikdy však těmito kroky situaci nezhoršíme, a tak je raději uděláme vždy. Tyto přípravné procesy *spouštíme ještě na původní strukturu Active Directory Windows Serveru 2000/2003*. Teprve po jejich dokončení budeme instalovat řadiče Serveru 2008 na další servery, inovovat je na existujících řadičích i instalovat na řadiče RODC.

Pro přesné rozlišení nutnosti procesů Adprep AD DS doporučuji studium Knowledge Base. Ovšem i sama firma Microsoft preferuje nevynucené volání procesu Adprep. Pozor na správnou verzi instalačního DVD. Musíme použít 32- a 64bitovou verzi Adprep přesně podle odpovídajícího mateřského systému!



1.8 Příprava pomocí Adprep

Příprava struktury forestu

- Přihlásíme se na řadič vlastníci roli FSMO Schema master. Uživatel musí být členem skupiny Enterprise Admins a Schema Admins.
- Zkopírujeme celou složku \sources\adprep z instalačního DVD pro systém Windows Server 2008 na místní disk.
- V příkazovém řádku přejdeme do složky Adprep na disku a spustíme program adprep /forestprep.
- Pokud plánujeme kdekoli ve forestu existenci RODC (Read-Only Domain Controller), provedeme navíc příkaz adprep /rodcprep.
- Provedeme ruční replikaci celého forestu.

Příprava domény a zásad

- Přihlásíme se na řadič vlastníci roli FSMO Infrastructure master. Uživatel musí být členem skupiny Domain Admins.
- Zkopírujeme celou složku \sources\adprep z instalačního DVD pro systém Windows Server 2008 na místní disk.