

» Idź do

- Spis treści
- Przykładowy rozdział

» Katalog książek

- Katalog online
- Zamów drukowany katalog

» Twój koszyk

- Dodaj do koszyka

» Cennik i informacje

- Zamów informacje o nowościach
- Zamów cennik

» Czytelnia

- Fragmenty książek online

» Kontakt

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl
© Helion 1991-2008

Windows Server 2008 PL. Biblia

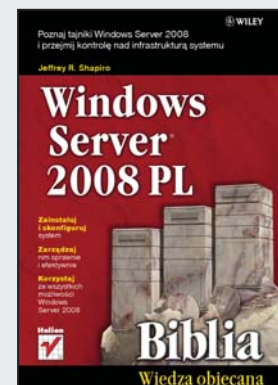
Autor: Jeffrey R. Shapiro

Tłumaczenie: Piotr Pilch

ISBN: 978-83-246-2117-0

Tytuł oryginału: [Windows Server 2008 Bible](#)

Format: 172×245, stron: 1072



Poznaj tajniki Windows Server 2008 i przejmij kontrolę nad infrastrukturą systemu

- Zainstaluj i skonfiguruj system
- Zarządzaj nim sprawnie i efektywnie
- Korzystaj ze wszystkich możliwości Windows Server 2008

Windows Server 2008 został zaopatrzony w mnóstwo nowych rozwiązań i opcji, między innymi rozbudowaną i udoskonaloną wersję usług Active Directory. Wyjątkową nowością jest także rewolucyjna edycja Server Core, umożliwiająca uruchomienie systemu operacyjnego bez użycia interfejsu graficznego, co oznacza, że można skonfigurować uproszczony serwer i przypisać mu rolę bardzo wydajnego serwera plików. Dzięki wprowadzonym udogodnieniom ten niezwykły system operacyjny nowej generacji zapewnia wszystkim użytkownikom organizacji dostęp do wszystkich usług sieciowych.

Książka „Windows Server 2008 PL. Biblia” zawiera pełen zestaw sprawdzonych i rzetelnych danych, dotyczących najlepszego wykorzystania tego systemu w każdej organizacji. Dowiesz się z niej m.in., jak poprawnie zainstalować i optymalnie skonfigurować Windows Server 2008. Poznasz tajniki tworzenia kont użytkowników i grup, a także konfigurowania udziałów plików czy limitów dyskowych. Nauczysz się w pełni wykorzystywać usługi Active Directory i zalety nowej rewolucyjnej edycji Server Core. Ten wyczerpujący podręcznik umożliwi Ci przejęcie kontroli nad infrastrukturą systemu i zoptymalizowanie wszelkich czynności administracyjnych.

- Strategia instalacji i konfigurowania
- Technologie sieciowe w systemie Windows Server 2008
- Protokół DHCP
- Routing i zdalny dostęp
- Archiwizowanie i odtwarzanie
- Rejestr
- Usługi plików, drukowania i magazynowania
- Zarządzanie magazynowaniem danych
- Bezpieczeństwo systemu
- Struktura usługi Active Directory
- Organizowanie struktury logicznej domeny
- Kontrola zmian i zarządzanie przestrzenią pracy

**Wszystko, czego potrzebujesz, aby optymalnie
korzystać z możliwości Windows Server 2008**

Spis treści

O autorze	23
Podziękowania	25
Wprowadzenie	27
Część I Windows Server 2008, instalacja Server Core, konfiguracja, usługi sieciowe i komunikacyjne	33
Rozdział 1. Instalowanie systemu Windows Server 2008	35
Wszystko na temat instalacji Server Core	35
Czym jest instalacja Server Core?	36
Strategia instalacji i konfigurowania	37
Przygotowanie do instalacji	38
Procedury serwerowe	38
Przegląd urządzeń	44
Zgodność sprzętu	44
Instalowanie systemu Windows Server 2008	45
Partycjonowanie dysków twardych	46
Przeprowadzanie instalacji Server Core	48
Przeprowadzanie bezobsługowej instalacji Server Core	48
Przeprowadzanie podstawowej instalacji	49
Instalowanie za pośrednictwem sieci	53
Role, funkcje i aplikacje	54
Serwery wolno stojące	54
Serwery członkowskie	54
Serwery ról	55
Serwer Windows Server 2008 w roli kontrolera domeny	58
Serwer Windows Server 2008 w roli serwera komunikacyjnego i serwera Microsoft Exchange	62
Integracja z oprogramowaniem Internet Information Services	62
Integracja z usługą Active Directory	62
Usługi rozproszone	63
Bezpieczeństwo	63
Administrowanie z jednego miejsca i z wykorzystaniem zasad	63
Routing wiadomości przy użyciu protokołu SMTP	64
Zawartość internetowej wiadomości pocztowej	64
Monitorowanie systemu przy użyciu narzędzia Windows Management Instrumentation	64

Zastosowanie systemu Windows Server 2008 na potrzeby usług bazodanowych bazujących na serwerze SQL Server	65
Współpraca systemu Windows Server 2008 z serwerem IIS i środowiskiem ASP.NET	66
Użycie systemu Windows Server 2008 na potrzeby usług aplikacji	67
Zastosowanie systemu Windows Server 2008 na potrzeby usług tłumaczących nazwy	68
DNS	68
DHCP	69
WINS	70
Podsumowanie	71
Rozdział 2. Konfigurowanie systemu Windows Server 2008	73
Zastosowanie konsoli Microsoft Management Console	73
Funkcja konsoli MMC	74
Uruchamianie konsoli MMC	76
Zastosowanie przystawek	77
Korzystanie z obszarów zadań	79
Inne dodatkowe narzędzia	82
Dostosowywanie konsoli MMC do własnych wymagań	83
Porównanie panelu sterowania i konsoli MMC	84
Zmiany dotyczące narzędzi konsoli MMC spowodowane przez zaporę firewall systemu Windows	85
Zastosowanie narzędzi konsoli MMC	85
Urząd certyfikacji	86
Zarządzanie klastrem pracy awaryjnej	86
Usługi składowe	86
Zarządzanie komputerem	88
Podgląd zdarzeń	89
Niezawodność i wydajność	89
Foldery udostępnione	89
Zastosowanie przystawki Podgląd zdarzeń	102
Rozszerzenia serwerowe	107
Zastosowanie narzędzia Kreator konfiguracji zabezpieczeń	108
Praca ze źródłami danych (ODBC)	111
Definiowanie nazw źródeł danych	112
Sprawdzanie informacji o sterowniku	117
Śledzenie	117
Pula połączeń	117
Aplety panelu sterowania	117
Aplet Centrum ułatwień dostępu	118
Aplet Dodaj sprzęt	118
Aplet Programy domyślne	119
Aplet Narzędzia administracyjne	120
Aplet Windows Update	120
Aplet Data i godzina	121
Obiekt Ekran apletu Personalizacja	122
Aplet Opcje folderów	122
Aplet Opcje internetowe	122
Aplet Centrum sieci i udostępniania	123
Aplet Opcje zasilania	123
Aplet Drukarki	123
Aplet System	124
Windows PowerShell	130
Podsumowanie	131

Rozdział 3. Technologie sieciowe w systemie Windows Server 2008	133
Protokół TCP/IP systemu Windows Server 2008	133
Podstawy protokołu TCP/IP (IPv4)	135
Adresowanie IP	135
Podsieci	137
Bezklasowy routing międzydomenowy	139
Uzyskiwanie adresów IP	139
Bramy i routing	140
Protokół DHCP	141
Domeny i rozwiązywanie nazw	142
Przygotowanie do instalacji	144
Określanie ustawień protokołu TCP/IP	144
Konfigurowanie protokołu TCP/IP	145
Zastosowanie protokołu IPv6	150
Terminy i pojęcia związane z protokołem IPv6	150
Zastosowanie protokołu IPv6 w systemie Windows Server 2008	154
Rozwiązywanie problemów z protokołem TCP/IP	157
Typowe zagadnienia związane z rozwiązywaniem problemów	157
Program ping	159
Narzędzie ipconfig	162
Program netstat	162
Program hostname	163
Narzędzie tracert	164
Program arp	165
Narzędzie route	167
Program nbtstat	168
Starsze protokoły	168
NetBEUI	169
IPX/SPX	169
DLC	170
SNMP	170
Zasady funkcjonowania protokołu SNMP	170
Instalowanie i konfigurowanie protokołu SNMP	171
Konfigurowanie zapory firewall systemu Windows i zarządzanie nią	176
Przegląd zmian wprowadzonych w zaporze firewall systemu Windows	176
Konfigurowanie zapory firewall systemu Windows	178
Zarządzanie zaporą firewall systemu Windows za pomocą zasad grupy	180
Zarządzanie zaporą firewall systemu Windows z poziomu konsoli	181
Zapora systemu Windows z zabezpieczeniami zaawansowanymi	181
Podsumowanie	183
 Rozdział 4. Protokół DHCP	 185
Przegląd protokołu DHCP	185
Usługa DHCP systemu Windows Server	186
Obsługa dynamicznej usługi DNS	187
Klasy dostawców i użytkowników	188
Przypisywanie adresów transmisji grupowej	188
Wykrywanie nieautoryzowanego serwera DHCP	188
Automatyczne konfigurowanie klientów	189
Monitorowanie i raportowanie	189

Instalowanie i konfigurowanie serwera DHCP	190
Instalowanie usługi DHCP	190
Zastosowanie konsoli DHCP	190
Tworzenie zakresów	190
Ustawianie ogólnych opcji zakresu	192
Konfigurowanie globalnych opcji DHCP	195
Tworzenie rezerwacji	196
Ustawianie globalnych właściwości zakresu	197
Aktywowanie i wyłączanie zakresu	198
Autoryzowanie serwera	198
Definiowanie i wdrażanie klas dostawców i użytkowników	199
Klasy dostawców	199
Klasy użytkowników	201
Konfigurowanie klienta pod kątem zastosowania identyfikatorów klas	202
Tworzenie i stosowanie superzakresów	203
Tworzenie superzakresu	203
Aktywowanie i wyłączanie superzakresu	204
Usuwanie zakresów z superzakresu	205
Usuwanie superzakresów	205
Tworzenie zakresów transmisji grupowej	205
Konfigurowanie globalnych właściwości serwera DHCP	207
Zarządzanie bazą danych serwera DHCP	209
Archiwizowanie i odtwarzanie bazy danych serwera DHCP	209
Przenoszenie bazy danych serwera DHCP do innego serwera	210
Konfigurowanie klientów DHCP z systemem Windows	211
Konfigurowanie opcji usługi DNS związanych z protokołem DHCP	212
Ochrona dostępu do sieci	213
Podsumowanie	213
Rozdział 5. Usługi nazewnicze systemu Windows	215
Usługa DNS	215
Nazwy domen	216
Dzisiejsze oblicze usługi DNS	218
Programy wysyłające zapytania, serwery nazw i wyszukiwanie do przodu	219
Rekordy domeny i pliki strefy	221
Wyszukiwanie wstecz	224
Delegowanie	226
Buforowanie, węzły przekazujące i węzły podrzędne	227
Rekursja, iteracja i odwołania	228
Microsoft DNS	230
Instalowanie usługi DNS	231
Przegląd konsoli DNS	231
Tworzenie stref wyszukiwania do przodu	232
Tworzenie stref wyszukiwania wstecz	233
Tworzenie rekordów zasobów	233
Konfigurowanie właściwości strefy	236
Zarządzanie opcjami i działaniem serwera DNS	239
Konfigurowanie wielu adresów w obrębie serwera DNS	239
Zastosowanie węzła przekazującego	240
Konfigurowanie ustawień zaawansowanych	241

Konfigurowanie głównych wskazówek	243
Konfigurowanie rejestrowania	244
Monitorowanie i testowanie	245
Zastosowanie zabezpieczeń	246
Zarządzanie serwerem i buforem	247
Konfigurowanie domen podrzędnych i delegowanie	247
Tworzenie domen podrzędnych	248
Delegowanie domeny podrzędnej	248
Usługi DNS i Active Directory	249
Usługa Dynamic DNS	250
Konfigurowanie usługi DDNS	251
Konfigurowanie procesu oczyszczania	252
Usługa WINS	253
Zasady działania usługi WINS	255
Proces rejestrowania przez serwer WINS	256
Odnawianie mapowania	257
Wieczna usługa WINS	257
Trwałe połączenia	258
Ręczne oznaczanie rekordu do usunięcia	259
Instalowanie i konfigurowanie usługi WINS	259
Instalowanie usługi WINS	259
Konfigurowanie usługi WINS	260
Konfigurowanie klientów Windows pod kątem usług DNS i WINS	262
Zastosowanie plików Hosts i LMHOSTS do rozwiązywania nazw	264
Zastosowanie pliku Hosts do rozwiązywania nazw	265
Zastosowanie pliku LMHOSTS do rozwiązywania nazw	266
Podsumowanie	268
Rozdział 6. Routing i dostęp zdalny	269
Usługi RAS i Telefonia systemu Windows Server 2008	269
Przegląd usługi RRAS systemu Windows Server 2008	270
Nowe funkcje usługi RRAS systemu Windows Server 2008	272
Konsola zarządzania usługi Routing i dostęp zdalny	275
Typy połączeń RAS i protokoły	276
Protokół PPP	276
Protokoły PPMP i BAP	276
Protokół PPTP	277
Protokół L2TP	277
Protokoły transportowe	278
Włączanie i konfigurowanie usługi RRAS	278
Routing IP	279
Przegląd routingu IP	279
Routing z wykorzystaniem usługi RRAS	282
Konfigurowanie prostego routera	283
Dynamiczny routing	289
Dodawanie i konfigurowanie protokołu RIP	289
Agent przekazywania DHCP	293
Protokół IGMP — przekazywanie transmisji grupowej	294
Translacja adresów sieciowych	297
Konfigurowanie mechanizmu NAT	298

Konfigurowanie usług i portów	300
Konfigurowanie usługi RAS pod kątem połączeń przychodzących	301
Uaktywnianie usługi RRAS	302
Konfigurowanie modemów i portów	304
Konfigurowanie protokołów	305
Konfigurowanie uwierzytelniania	308
Wyłączanie routingu (dotyczy tylko serwera zdalnego dostępu)	313
Rejestrowanie i monitorowanie usługi RRAS	314
Konfigurowanie serwera VPN	316
Konfigurowanie portów VPN	317
Uaktywnianie protokołu L2TP dla połączeń VPN	317
Zastosowanie protokołów Multilink i BAP	319
Serwer zasad	321
Tworzenie nowej zasady	321
Określanie priorytetu zasad	325
Zastosowanie usługi RADIUS	325
Konfigurowanie usługi RADIUS	326
Konfigurowanie monitorowania	326
Konfigurowanie wychodzących sieciowych połączeń telefonicznych	327
Tworzenie połączenia	327
Konfigurowanie właściwości połączenia	327
Konfigurowanie połączenia telefonicznego w celu połączenia się z internetem	331
Podsumowanie	332

Rozdział 7. Archiwizowanie i odtwarzanie 333

Dlaczego archiwizuje się dane?	334
Co jest archiwizowane?	334
Archiwizowanie danych	335
Bity archiwizacji	335
Czym jest kopia zapasowa?	335
Czym jest odtwarzanie?	337
Działanie procesu archiwizacji	337
Wymienne magazyny danych i pule nośników	338
Usługa Magazyn wymienny	338
Baza danych usługi Magazyn wymienny	340
Fizyczne lokalizacje	340
Pule nośników	342
Węzły Kolejka pracy i Żądania operatora	344
Korzystanie z zestawów roboczych i magazynujących	346
Określanie mierników jakości wsparcia technicznego związanego z archiwizowaniem i odtwarzaniem danych	347
Określanie jakości przechwytywania danych	351
Najlepsza pora dnia na archiwizowanie danych	352
Czas trwania archiwizacji	352
Archiwizowanie serwerów i stacji roboczych	354
Dylemat dotyczący otwartych plików	355
Procedura archiwizacji	357
Przeprowadzanie archiwizacji	359
Tworzenie puli nośników	359
Prawa i uprawnienia	360

Lokalizacja źródłowa i docelowa	361
Ustalanie harmonogramów	362
Schematy rotacji	362
Odtwarzanie danych	365
Lokalizacja taśm	366
Przepustowość procesu archiwizacji	367
Zastosowanie kopii woluminów w tle	368
Podsumowanie	372
Rozdział 8. Przywracanie danych po awarii	373
Planowanie przywracania po awarii	373
Zasada i protokół	374
Dokumentacja	374
Szkolenie z zakresu przywracania po awarii i planowanie działań	376
Identyfikowanie zasobów	376
Przygotowywanie planów interwencji	377
Testowanie planów interwencji	377
Programy symulujące awarie	379
Odporność na błędy	380
Identyfikowanie słabych punktów	381
Przywracanie danych z kopii zapasowej	382
Odtwarzanie bazowych systemów operacyjnych	382
Przywracanie konfiguracji	383
Powielanie usług, danych i sprzętu	383
Przywracanie kluczowych usług	383
Usługa Active Directory	383
DNS	384
Rejestr	384
Analiza awarii	384
Podsumowanie	385
Rozdział 9. Rejestr	387
Zastosowanie rejestru	387
Struktura rejestru	389
Pliki gałęzi rejestru	392
Klucze i wpisy	394
Edytor rejestru	394
Regedit.exe	395
Modyfikowanie rejestru	395
Importowanie i eksportowanie kluczy	396
Edytowanie zdalnego rejestru	398
Wczytywanie i usuwanie gałęzi	398
Zabezpieczanie rejestru	399
Uniemożliwianie dostępu do rejestru	399
Stosowanie uprawnień dla kluczy rejestru	399
Inspekcja dostępu do rejestru	400
Zabezpieczanie dostępu do zdalnego rejestru	401
Podsumowanie	402

Rozdział 10. Inspekcja systemu Windows Server 2008	403
Przegląd funkcji inspekcji	403
Konfigurowanie inspekcji	405
Uaktywnianie zasad inspekcji	405
Inspekcja dostępu do obiektów	407
Analizowanie raportów inspekcji	408
Zastosowanie narzędzia Podgląd zdarzeń	409
Zastosowanie innych narzędzi	409
Strategie inspekcji	411
Rezygnacja z inspekcji	411
Pełna inspekcja	411
Inspekcja problematycznych użytkowników	411
Inspekcja administratorów	412
Inspekcja krytycznych plików i katalogów	412
Podsumowanie	412
Rozdział 11. Usługi .NET Framework	415
Wprowadzenie do środowiska .NET Framework	416
Obsługa platformy 64-bitowej	417
Lista kontroli dostępu	417
ADO .NET i LINQ	417
Przetwarzanie asynchroniczne	417
Inicjatywa .NET	418
Środowisko CLR	418
System CTS	419
Zabezpieczenia technologii .NET	420
Domeny aplikacji	420
Mechanizm zwalniania pamięci	421
Porównanie technologii .NET i JVM	422
Konfigurowanie bufora GAC	422
Podsumowanie	422
Część II Usługi plików, drukowania i magazynowania	425
Rozdział 12. Usługi drukowania	427
Usługi drukowania	428
Usługi drukowania systemu Windows Server	429
Usługi drukowania — logiczne środowisko	429
Usługi drukowania — środowisko fizyczne	438
Strategia związana z usługami drukowania	441
Drukarkowa taksonomia	441
Tworzenie grup drukowania	443
Instalowanie drukarki sieciowej	443
Aktualizowanie sterowników	444
Instalowanie i konfigurowanie drukarek	444
Instalowanie lokalnej drukarki	445
Publikowanie drukarek	449
Lokalizowanie drukarek	449
Ukrywanie drukarek	451
Pule drukarek	451
Ładowanie portów drukarkowych	452

Administrowanie drukarkami	454
Zarządzanie drukarką	454
Zarządzanie zadaniami wydruku	457
Zaawansowane opcje buforowania	459
Kontrola dostępu	461
Rozwiązywanie problemów	464
Problemy z drukowaniem po stronie serwera	465
Problemy z drukowaniem po stronie klienta	467
Zastosowanie funkcji drukowania dwukierunkowego	467
Inspekcja dotycząca wykorzystania drukarek i zarządzania nimi	468
Podsumowanie	468
Rozdział 13. Zarządzanie magazynowaniem danych	469
Przegląd usług magazynowania	470
Zarządzanie magazynowaniem	470
Wydajność i pojemność	470
Wysoka dostępność	474
Przywracalność	474
Kwestie związane ze starszymi systemami	475
Narzędzie Zarządzanie dyskami	475
Style partycjonowania	477
Dyski MBR	477
Dyski GPT	477
Wymienne magazyny danych	478
Zdalne magazyny danych i rozwiązanie HSM	479
Przystawka Zarządzanie dyskami	480
Podstawowe magazyny danych	481
Partycje podstawowe	481
Partycje rozszerzone	481
Woluminy podstawowe	481
Dynamiczne woluminy i odporność na błędy	482
Dyski dynamiczne	482
RAID-1 — dublowanie dysków (mirroring)	485
RAID-5 — odporne na błędy paskowanie z parzystością	486
Sprzętowa macierz RAID	488
Zarządzanie dynamicznymi magazynami danych	489
Konwertowanie dysków podstawowych na dynamiczne	489
Tworzenie woluminów prostych	491
Rozszerzanie woluminów prostych i łączonych	492
Tworzenie woluminów RAID-0 (rozłożonych) i zarządzanie nimi	494
Tworzenie woluminów RAID-1 i zarządzanie nimi	494
Tworzenie woluminów RAID-5 i zarządzanie nimi	495
Importowanie dysków	496
Zarządzanie magazynami z wykorzystaniem przydziałów dyskowych	497
Dlaczego trzeba używać przydziałów dyskowych?	497
Konfigurowanie przydziałów dyskowych	501
Rozsądne zarządzanie przydziałami dyskowymi	502
Rozwiązywanie problemów	504
Statusy dysków i woluminów	505
Radzenie sobie z problemami dotyczącymi redundancji woluminów RAID	505
Eksplorator magazynu	508
Podsumowanie	508

Rozdział 14. Systemy plików systemu Windows Server 2008	509
Przegląd struktury dysku	509
Systemy plików FAT16 i FAT32	512
System plików NTFS	514
Struktura systemu plików NTFS	515
Przydziały dyskowe	519
Punkty połączenia	519
System szyfrowania plików EFS	520
Hierarchiczne zarządzanie magazynowaniem	520
Złącza katalogów (Directory junctions)	520
Podłączane woluminy	521
Transakcyjny system plików NTFS	522
Wybór systemu plików	522
Optymalizowanie pojemności magazynu danych	524
Optymalizowanie rozmiaru klastra	524
Defragmentowanie woluminów	525
Użycie dla dysków kompresji systemu plików NTFS	525
Zarządzanie rozproszonym systemem plików (DFS)	527
Struktura systemu DFS i związana z nim terminologia	528
Porównanie domenowych i niezależnych przestrzeni nazw DFS	530
Obsługa klienta	531
Replikacja z wykorzystaniem systemu DFS	531
Replikacja z wykorzystaniem składnika DFS-R	532
Buforowanie po stronie klienta	533
Praca z konsolą Zarządzanie systemem plików DFS	533
Praca z podłączanymi woluminami	539
Podłączanie woluminu	540
Odłączanie woluminu	541
Oprogramowanie Services for Network File System	541
Przegląd systemu NFS	543
Podsumowanie	549
 Rozdział 15. Udostępnianie i zabezpieczanie plików i katalogów	 551
Udostępnianie i zabezpieczanie danych	552
Prawo właściciela	553
Konfigurowanie roli serwera plików	554
Konsola Menedżer zasobów serwera plików	555
Publikowanie udziałów w usłudze Active Directory	560
Tworzenie udziału	561
Udostępnianie lokalnego katalogu	561
Tworzenie udziałów za pomocą konsoli Zarządzanie udziałami i magazynowaniem	563
Atrybuty udziału	568
Blokowanie uprawnienia	570
Sumowanie uprawnień udziału	571
Przenoszenie lub kopiowanie katalogów	572
Udziały w obrębie domeny	572
Kto może udostępniać katalogi?	572
Ukryte udziały	572
Łączenie się z udziałami	573
Podłączanie użytkowników do opublikowanych udziałów	574
Mapowanie dla użytkowników przestrzeni nazw DFS	575

Udziały administracyjne	577
Rozsądne strategie udostępniania katalogów	580
Ograniczanie udziałów	580
Konfigurowanie udziałów aplikacji	581
Konfigurowanie udziałów danych	581
Dostęp w trybie offline (buforowany)	582
Atrybuty trybu offline	583
Synchronizowanie buforowanych zasobów	583
Zabezpieczanie plików i katalogów z wykorzystaniem uprawnień	584
Typy uprawnień	586
Atrybuty uprawnień	588
Dziedziczenie	589
Przejmowanie prawa właściciela	590
Kopiowanie i przenoszenie	591
Strategie zarządzania uprawnieniami	591
Zabezpieczanie plików za pomocą systemu EFS	593
Funkcjonowanie systemu EFS	594
Możliwości odzyskiwania zaszyfrowanych danych i zasada przywracania	596
Zastosowanie systemu EFS	597
Kopiowanie, przenoszenie lub zmiana nazwy zaszyfrowanych plików	601
Zdalne uzyskiwanie dostępu do zaszyfrowanych danych	602
Udostępnianie zaszyfrowanych danych	602
Szyfrowanie plików dla wielu użytkowników	605
Archiwizowanie i przywracanie zaszyfrowanych danych	606
Konfigurowanie i stosowanie zasady przywracania	608
Podsumowanie	612

Część III Bezpieczeństwo oraz usługa Active Directory 613

Rozdział 16. Bezpieczeństwo systemu Windows Server 2008 615

Przegląd zabezpieczeń systemu Windows Server 2008	615
Potrzeba zabezpieczeń	616
Wprowadzanie danych	617
Transportowanie danych	617
Dlaczego istnieje zagrożenie?	617
Wywiązywanie się z zadań dotyczących zabezpieczeń	620
Usprawnienia zabezpieczeń w rolach serwera	621
Usługa kontrolera domeny Active Directory	622
Rola serwera DHCP	622
Rola serwera DNS	623
Podstawy szyfrowania	623
Wprowadzenie do kryptografii	624
Kryptografia nowej generacji	625
Klucze	626
Klucze prywatne	627
Klucze publiczne	627
Klucze sesyjne	627
Certyfikaty kluczy	628
Podpisy cyfrowe	628

Protokół Kerberos	629
Współpraca między protokołem Kerberos a rejestracją jednokrotną	630
Pst! Tak działa protokół Kerberos	631
Uwierzytelnianie za pomocą czasu	632
Rozpowszechnianie klucza	632
Bilety sesyjne	633
Protokół Kerberos a relacje zaufania	634
Lokalizowanie centrów dystrybucji kluczy	634
Wprowadzenie do protokołu IPSec	635
SSL/TLS	637
Wprowadzenie do usług certyfikacyjnych Active Directory	638
Infrastruktura klucza publicznego	638
Certyfikaty cyfrowe	638
Tworzenie PKI przy użyciu usług certyfikacyjnych Active Directory	639
Obsługa starszej wersji NTLM	639
Karty inteligentne	640
Domeny	641
Logowanie oraz uwierzytelnianie	641
Logowanie w systemie Windows Server 2008	642
Uwierzytelnianie dwuczynnikowe oraz jednoczynnikowe	642
Relacje zaufania	643
Kontrola dostępu	645
Audytowanie	646
Planowanie bezpieczeństwa	646
Zapory	646
Zasady zabezpieczeń Active Directory	647
Bezpieczne gniazda	648
Zapory, serwery proxy oraz bastiony	648
Wprowadzenie do infrastruktury klucza publicznego	649
Instalowanie oraz konfiguracja usług certyfikacyjnych Active Directory	649
Usługi certyfikacyjne Active Directory	650
Instalowanie oraz konfigurowanie urzędu certyfikacji	651
Wdrażanie infrastruktury PKI	652
Model zaufania	654
Podsumowanie	663

Rozdział 17. System Windows Server 2008 a usługa Active Directory 665

Wszelchwidząca usługa Active Directory	666
Dlaczego katalogi są potrzebne?	667
Czym jest usługa Active Directory?	670
Dziadek nowoczesnego katalogu — specyfikacja X.500	670
Ojciec współczesnego katalogu — protokół LDAP	673
Po protokole X.500	675
Otwarta usługa Active Directory	676
Gdzie tu miejsce dla rejestru?	676
Elementy usługi Active Directory	678
Przestrzenie nazw oraz schematy nazewnictwa	679
Usługa Active Directory a internet	679
Wszędzie usługa Active Directory	680

Wewnątrz usługi Active Directory	681
Jeżeli chodzi tak jak kaczka	681
Struktura bazy danych w usłudze Active Directory	683
Obiekty Active Directory	684
Schemat usługi Active Directory	686
Atrybuty obiektu	687
Poruszanie się po usłudze Active Directory	687
Konwencje nazewnictwa	688
Obiekty domenowe	690
Jednostki organizacyjne	691
Drzewa	692
Lasy	692
Relacje zaufania	693
Wykaz globalny	694
Mój aktywny katalog	695
Łączenie rozdzielonego — starsze wersje systemu Windows a Windows Server 2008	696
Pojedynczy punkt dostępu oraz administracji	698
Coraz więcej domen	699
Wewnątrzdomenowe relacje zaufania	700
Listy kontroli dostępu oraz tokeny dostępowe	700
Podsumowanie	701
Rozdział 18. Planowanie usługi Active Directory	703
Ogólny zarys usługi Active Directory	703
Podstawowe reguły planowania	704
Struktura usługi Active Directory	704
Plan domeny	705
Topologia lokacji	707
Plan lasu	708
Plan relacji zaufania	709
Planowanie jednostki organizacyjnej	710
Planowanie usługi Active Directory dla przedsiębiorstwa	711
Planowanie strategii nazewnictwa	711
Planowanie domeny oraz jednostek organizacyjnych	712
Plan oddziałów	714
Planowanie administrowania	718
Delegowanie administracji	718
Delegowanie lasów, drzew oraz jednostek organizacyjnych	719
Implementowanie zabezpieczeń obiektu	719
Role administracyjne	720
Planowanie migracji	721
Plan uaktualniania	721
Plan restrukturyzacji	722
Narzędzia służące do migracji	723
Plan laboratorium testowego	723
Plan tworzenia kopii zapasowej oraz przywracania	724
Wdrażanie planu	726
Podsumowanie	726

Rozdział 19. Organizowanie struktury logicznej domeny	727
Strażnicy nowego porządku	728
Planowanie infrastruktury Active Directory	728
Planowanie struktury logicznej domeny	729
Kwestia przygotowania psychicznego	729
Zebranie zespołu	730
Komitet do spraw planowania domen	730
Zarządzanie domeną	731
Zarządzanie zmianą kontroli	731
Bezpieczeństwo domeny	732
Komunikacja wewnątrzdomenowa	732
Informacje i szkolenie	733
Poznananie przedsiębiorstwa	733
Analiza przedsiębiorstwa	734
Środowiska przedsiębiorstwa	735
Praca ze schematami organizacyjnymi	738
Identyfikacja kluczowych jednostek zarządzania	739
Strategiczne motywacje	739
Identyfikowanie jednostek logicznych	741
Identyfikowanie jednostek fizycznych	742
Dokumentacja	742
Modele administracyjne	743
Struktura logiczna domeny — schemat	746
Domena najwyższego poziomu	746
Mechanizmy nazewnictwa DNS	754
Domeny drugiego poziomu	755
Partycjonowanie domeny	760
Jednostki organizacyjne	762
Praca z grupami	764
Zabezpieczenie partycji	765
Podsumowanie	766
 Rozdział 20. Architektura fizyczna usługi Active Directory	 767
Przeszłość, teraźniejszość i przyszłość	767
Lasy i relacje zaufania	769
Konsekwencje wyboru lasu związane z projektem	773
Kontrolery domen i wykazy globalne	774
Kontrolery domen	774
Wykazy globalne	777
Usługi lokalizacyjne kontrolera domeny i wykazu globalnego	779
Decyzje przy projektowaniu	781
Lokacje	782
Replikacja w lokacjach	783
Łączy lokacji	784
Mostki łączy lokacji	785
Obiekty połączeń pomiędzy lokacjami	786
Replikacja w usłudze Active Directory	786
Jak działa replikacja?	788
Synchronizacja katalogu	789

Projektowanie i konfiguracja lokacji Active Directory	790
Topologia	791
Tworzenie lokacji kontrolerów domeny	791
Rozmieszczanie kontrolerów domeny	793
Zabezpieczanie kontrolerów domeny	794
Rozmieszczanie serwerów wykazu globalnego	797
Rozmieszczanie serwerów DNS	797
Architektura DDNS	799
Centrale	799
Rozmieszczanie serwerów WINS	799
Rozmieszczanie serwerów DHCP	801
Architektura lokacji	804
Architektura	806
Koszt łączy lokacji	807
Czas	812
Architektura usługi czasu	813
Podsumowanie	814
Rozdział 21. Instalacja i rozmieszczanie usługi Active Directory	817
Przygotowanie do wdrożenia	817
Plan wdrożenia usługi Active Directory Firmy ABC	818
Streszczenie	818
Sieć FIRMAABC	818
Domena GENEZA	819
Domena CENTRUM	821
Domena DITT	823
Domena OCHRONA	823
Instalowanie i testowanie kontrolerów domeny Active Directory	823
Instalowanie kontrolera domeny	824
Wypromowanie do funkcji kontrolera domeny	825
Ustawianie domeny w systemie DNS (WINS)	832
Tworzenie lokacji	834
Tworzenie jednostek organizacyjnych	837
Delegowanie administrowania jednostek OU	838
Zabezpieczanie kontrolera domeny i postępowanie zgodnie z protokołem przywracania danych	839
Implementacja	840
Instalacja	841
Rezerwacje adresu IP	841
Instalacja domeny głównej — FIRMAABC.PL	841
Kontrola jakości	846
Podsumowanie	847
Rozdział 22. Zarządzanie usługą Active Directory	849
Instalowanie nowych usług katalogowych w istniejącej infrastrukturze	849
Zarządzanie replikacją	850
Instalowanie nowych kontrolerów domeny	850
Instalowanie nowych serwerów katalogowych	852
Ochrona usługi Active Directory przed uszkodzeniami	852
Defragmentacja bazy danych w trybach online i offline	852
Zapewnianie integralności bazy danych	855

Przenoszenie usługi Active Directory	856
Integrowanie bazy Active Directory z innymi usługami	857
Usługa Active Directory a SQL Server	857
Usługa Active Directory a Microsoft Exchange	857
Logowanie bez używania wykazu globalnego	857
Usługa Active Directory a system DNS	858
Architektura administracji usługi Active Directory	859
Architektura	863
Członkostwo w grupie systemu Windows Server 2008	864
Administrowanie usługami sieciowymi	865
Administrowanie serwerami usług przedsiębiorstwa	868
Architektura administrowania zdalną stacją roboczą	868
Zasady usług terminalowych	869
Bezpieczne administrowanie	870
Podsumowanie	877

Część IV Kontrolowanie zmian i zarządzanie przestrzenią roboczą 879

Rozdział 23. Zarządzanie użytkownikami i grupami 881

Konto w systemie Windows Server 2008 — zasób użytkownika	882
Czym jest użytkownik?	882
Czym są kontakty?	883
Użytkownicy lokalni a „użytkownicy lokalni”	883
Czym jest grupa?	883
Przegląd narzędzi zarządzania użytkownikami i komputerami	886
Konta użytkowników systemu Windows Server 2008	888
Zasady konta	893
Wystawcy zabezpieczeń i proces uwierzytelniania logowania	893
Identyfikatory zabezpieczeń	894
Menedżer SAM i uwierzytelnianie za pomocą urzędu LSA	895
Konta użytkowników w akcji	896
Aplikacja RunAs	896
Nazywanie kont użytkowników	897
Hasła	898
Logowanie	899
Przydzielanie zdalnego dostępu	900
Tworzenie konta użytkownika	900
Zmienianie nazw kont użytkowników	908
Usuwanie i wyłączanie kont użytkowników	908
Kopiowanie kont	908
Konta komputera	909
Konta grupy	909
Zakresy grup	910
Elementy grup	913
Instalowanie predefiniowanych grup	913
Grupy na serwerach członkowskich	916
Zagnieżdżanie grup	917
Tworzenie grupy	917

Zarządzanie grupami	920
Prawa i uprawnienia	920
Tryb mieszany kontra tryb natywny	923
Sztuka zen zarządzania użytkownikami i grupami	924
Delegowanie odpowiedzialności	926
Strategie zarządzania użytkownikami i grupami	928
Kontrolowanie kosztu TCO	928
Określanie potrzebnego dostępu i przywilejów	929
Określenie poziomu zabezpieczeń	930
Ochrona zasobów i zmniejszanie obciążenia przez używanie grup lokalnych	930
Ostrożne delegowanie	930
Ograniczanie zmian do minimum	930
Podsumowanie	931

Rozdział 24. Kontrola zmian, zasady grupy

i zarządzanie przestrzenią roboczą	933
Czym jest kontrola zmian?	934
Zarządzanie zmianami	935
Użytkownik	940
Komputer	940
Obejmowanie kontroli	942
Aplikacje	942
Zabezpieczenia	944
Środowisko systemu operacyjnego	944
Blokowanie stacji roboczej	945
Przygotowanie do zasad kontroli zmian	945
Zasady grupy	946
Typy zasad grupy	949
Elementy zasad grupy	951
Gdzie znajdują się obiekty GPO?	953
Jak działają zasady grupy?	955
Lokalne lub nielocalne obiekty zasad grupy	956
Wprowadzanie zasad grupy	957
Filtrowanie zasad	959
Delegowanie kontroli nad zasadami grupy	959
Zabezpieczenia w lokalnych obiektach zasad grupy	960
Jak są przetwarzane zasady grupy?	960
Zaprzęganie zasad grupy do pracy	965
Zasady oprogramowania	965
Zasady zabezpieczeń	966
Zasady grupy i zarządzanie zmianami — składanie wszystkiego w całość	966
Nie należy akceptować domyślnych zasad	968
Ustanawianie planu wdrażania zasad grupy	968
Zarządzanie kontami komputerów	969
Rozpoczynanie	970
Dostosowanie logowania i wylogowywania	970
Blokowanie pulpitu	970
Kontrolowanie menu Start	971
Przekierowywanie katalogu	971
Starsze wersje systemu Windows	972

Zarządzanie kontrolą zmian zasad grupy	973
Od projektowania do środowiska produkcyjnego z zasadami grupy	974
Kontrola zmian w zasadach grupy	974
Rozwiązywanie problemów związanych z zasadami grupy za pomocą kreatora wyników zasad grupy	975
Tworzenie architektury zasad grupy	976
Zasady haseł	979
Zasady blokady konta	979
Zasady inspekcji	981
Dziennik zdarzeń	985
Blokowanie administratorów domeny	985
Podsumowanie	988
Rozdział 25. Poziom usług	989
Poziom usług	989
Poziom usług — przykład 1.	990
Poziom usług — przykład 2.	990
Pisemna gwarancja jakości	991
Zarządzanie poziomem usług	992
Wykrywanie problemów	992
Zarządzanie wydajnością	992
Dostępność	992
Konstrukcja zarządzania SLM	993
Zarządzanie SLM a system Windows Server 2008	994
Architektura monitorowania systemu Windows Server 2008	995
Pojęcie szybkości i przepływności	996
Pojęcie kolejek	996
Pojęcie czasu odpowiedzi	997
W jaki sposób działają obiekty wydajności?	997
Narzędzia monitorowania systemu	998
Menedżer zadań	999
Konsola niezawodności i wydajności	1000
Monitor wydajności	1001
Dzienniki wydajności i alerty	1004
Tworzenie zestawów modułów zbierających dane	1006
Zapoznanie się z serwerami	1007
Monitorowanie wąskich gardeł	1008
Obciążenie robocze serwera	1010
Obciążenie powodowane przez monitorowanie wydajności	1011
Poziom usług w aplikacji Microsoft Systems Center Operations Manager	1012
Podsumowanie	1013
Skorowidz	1015

Rozdział 2.

Konfigurowanie systemu Windows Server 2008

W tym rozdziale:

- ◆ Użycie konsoli Microsoft Management Console
- ◆ Zapoznanie z narzędziami konsoli MMC
- ◆ Więcej informacji o narzędziu *Menedżer serwera*
- ◆ Zastosowanie narzędzia *Kreator konfiguracji zabezpieczeń*
- ◆ Praca ze źródłami danych ODBC
- ◆ Aplety panelu sterowania

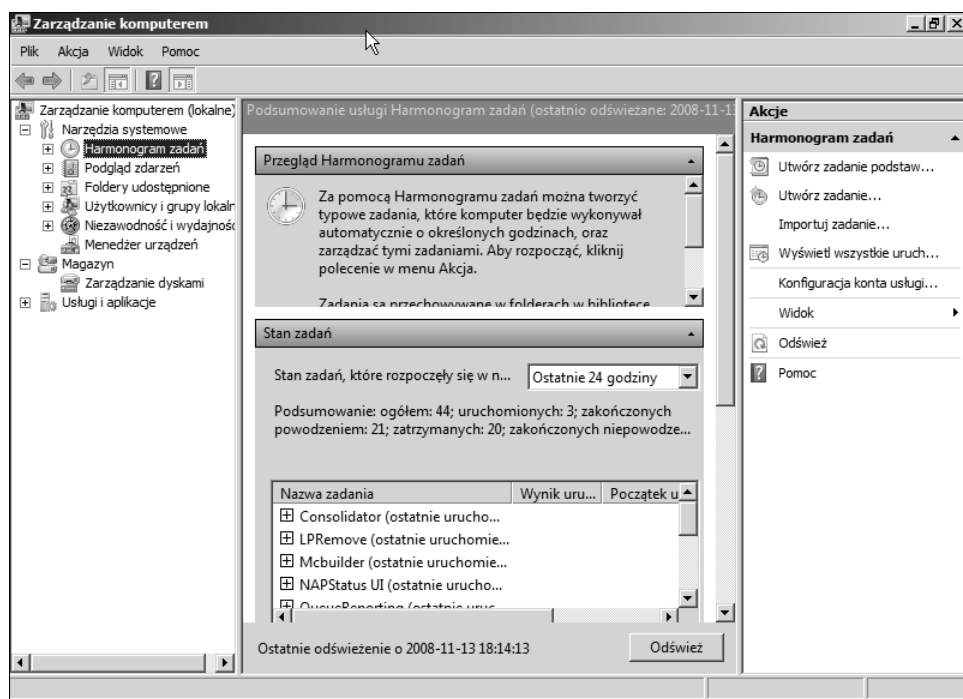
W rozdziale omówiono wiele narzędzi służących do konfigurowania systemu i zarządzania nim oraz użytkownikami, a także kontrolowania innych aspektów związanych z Windows Server 2008.

Zastosowanie konsoli Microsoft Management Console

Jedną z wielu zmian, które w porównaniu z systemem Windows NT pojawiły się w Windows 2000 i zostały rozwinięte w interfejsach i strukturze zarządzania systemów Windows 2003 i Windows Server 2008, jest większe ujednolicenie narzędzi administracyjnych. Choć wiele ustawień systemu w dalszym ciągu jest kontrolowanych z poziomu panelu sterowania, większość funkcji administracyjnych przeniesiono do konsoli *Microsoft Management Console* (MMC). Konsola MMC obsługuje różnego rodzaju tak zwane przystawki, które służą do zarządzania mnóstwem ról, funkcji i aplikacji serwera. Konsolę można uruchomić w systemach Windows Server 2008, Windows 2000, Windows Server 2003, Windows 9x, a także Windows XP i Windows Vista. W niniejszym podrozdziale przyjrzymy się konsoli MMC i wchodzącym w jej skład narzędziom przeznaczonym dla systemu Windows Server 2008.

Funkcja konsoli MMC

Sama konsola MMC pełni rolę szkieletu, w obrębie którego znajdują się różne narzędzia administracyjne nazywane przystawkami. W szczególności konsola MMC zapewnia narzędziom administracyjnym jednolity interfejs. Oznacza to, że po poznaniu struktury jednego narzędzia wykorzystanie tej wiedzy będzie możliwe w przypadku reszty podobnie wyglądających narzędzi (zakres podobieństwa jest ograniczony przez różnice w funkcjonowaniu różnych narzędzi). Rysunek 2.1 pokazuje okno konsoli MMC z załadowaną przystawką Zarządzanie komputerem (więcej na temat przystawek zamieszczono w dalszej części rozdziału). Jak się dalej okaże, przystawki Zarządzanie komputerem używa się w przypadku większości aspektów związanych z konfigurowaniem sprzętu i oprogramowania komputera.



Rysunek 2.1. Konsola MMC pełni rolę szkieletu dla bogatej gamy narzędzi administracyjnych

Być może od jednolitego interfejsu ważniejszy jest fakt, że konsola MMC umożliwia łączenie narzędzi administracyjnych w celu stworzenia własnej konfiguracji konsoli. Konfiguracji takiej można następnie nadać nazwę i zapisać ją na dysku. Gdy później trzeba będzie skorzystać z tej konfiguracji, z menu *Start* należy wybrać skrót konsoli MMC lub dwukrotnie kliknąć jej ikonę. Założmy, że chcesz skonfigurować niestandardową konsolę służącą do zarządzania serwerem internetowym Windows Server 2008. Istnieje możliwość zintegrowania narzędzi umożliwiających zarządzanie w obrębie jednego interfejsu serwerem DNS, serwerem DHCP, serwerem aplikacji i serwerem IIS. Taka dostosowana konsola pozwala szybko uzyskać dostęp do większości ustawień, które trzeba regularnie konfigurować dla serwera.

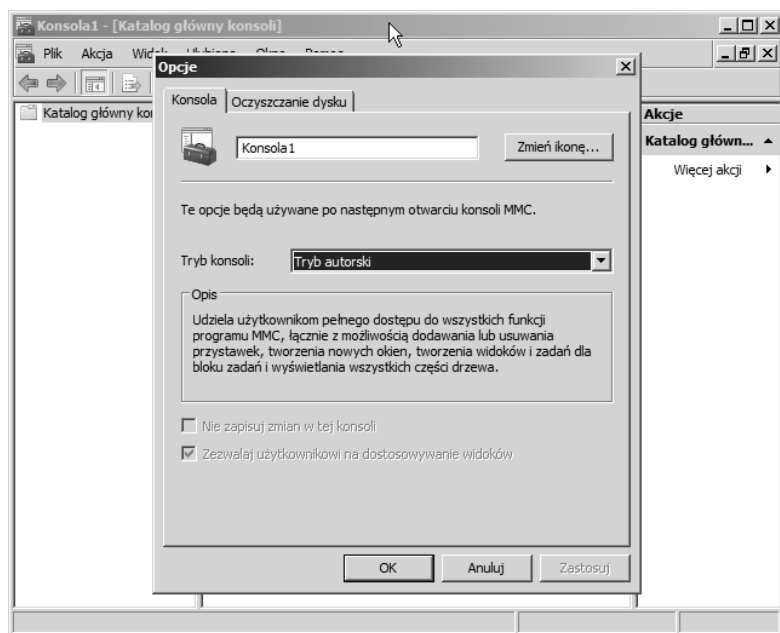
Choć zwykle okno konsoli MMC składa się z dwóch paneli, wiele przystawek systemu Windows Server 2008 dysponuje jednym oknem podzielonym na trzy panele. Lewy panel zazwyczaj zawiera kartę drzewa, która przeważnie prezentuje hierarchiczną strukturę zarządzanych obiektów. Gdy na przykład zastosuje się przystawkę Użytkownicy i komputery usługi Active Directory, drzewo będzie zawierać kontenery usługi Active Directory, które są powiązane z użytkownikami, grupami i komputerami.

W prawym panelu są wyświetlane szczegóły. Zawartość tego panelu jest zależna od pozycji zaznaczonej w obrębie drzewa. Jeśli na przykład w drzewie wybierzesz węzeł *Usługi*, w panelu szczegółów pojawi się lista zainstalowanych usług. Panel szczegółów zwykle udostępnia dwa widoki — pojedynczy panel i rozszerzony panel *Akcje*, który zazwyczaj prezentuje różne zadania. Rozszerzony widok uwzględni dodatkowy obszar, który przeważnie oferuje instrukcje lub informacje dotyczące zaznaczonej pozycji.

Konsola MMC zapewnia dwa różne tryby — użytkownika i autora. W trybie użytkownika korzysta się z istniejących konsoli. Można wyróżnić kilka odmian trybu użytkownika, które oferują różny poziom dostępu, od pełnego do ograniczonego. Tryb autora pozwala tworzyć nowe konsole lub modyfikować istniejące. Rysunek 2.2 przedstawia konsolę *Usługi* otwartą w trybie użytkownika. Rysunek 2.3 prezentuje konsolę uaktywnioną w trybie autora. Jak widać na rysunku, tryb autora oferuje dostęp do poleceń i funkcji niedostępnych w trybie użytkownika.

Rysunek 2.2.

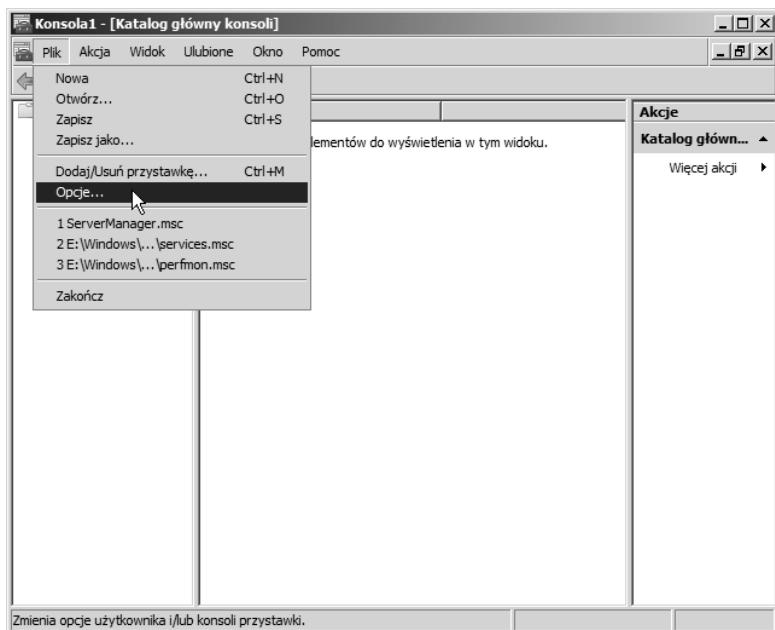
Widoczny tryb autora pozwala tworzyć nowe konsole, a tryb użytkownika ogranicza operacje, które użytkownik może wykonać w obrębie konsoli



Tryb użytkownika oferuje trzy różne opcje — pełny dostęp, ograniczony dostęp z wieloma oknami i limitowany dostęp z pojedynczym oknem. W przypadku pełnego dostępu użytkownik konsoli MMC może skorzystać z wszystkich jej poleceń zarządzających oknami. Jednak nie ma możliwości dodawania lub usuwania przystawek bądź zmieniania właściwości konsoli. Opcje ograniczonego dostępu zawężają zakres zmian konfiguracji okien konsoli, a także użycie pojedynczego okna lub wielu okien (zależnie od trybu). Tryb konsoli

Rysunek 2.3.

Tryb autora zapewnia możliwość modyfikowania opcji konsoli i dodawania nowych przystawek



jest zapisywany w jej obrębie i uaktywniany po otwarciu okna konsoli. Tryby konsoli mogą być zmieniane za pośrednictwem okna właściwości *Opcje* (z menu *Plik* wybierz pozycję *Opcje*). Ustawianie opcji konsoli omówiono w dalszej części rozdziału.



W systemie Windows Server 2008 domyślnym trybem jest tryb użytkownika (ograniczony dostęp z pojedynczym oknem).

Jak wcześniej wspomniano, za pomocą trybu autora tworzy się nowe konsole lub modyfikuje istniejące. W trybie autora można dodawać i usuwać przystawki, zmieniać opcje okien i konfigurować ustawienia konsoli.

Uruchamianie konsoli MMC

W celu załadowania konsoli MMC z menu *Start/Narzędzia administracyjne* wybierz odpowiedni skrót lub dwukrotnie kliknij ikonę konsoli w obrębie okna narzędzia *Eksplorator Windows*. Konsolę można również uruchomić z poziomu wiersza poleceń. Format polecenia jest następujący:

```
MMC ścieżka\plik.msc /a
```


Poniższa lista objaśnia opcje tego polecenia.

- ♦ *ścieżka\plik.msc*. W miejsce łańcucha *ścieżka* wstaw ścieżkę pliku konsoli o nazwie identyfikowanej przez *plik.msc*. Można zastosować ścieżkę bezwzględną lub użyć zmiennej środowiskowej `%systemroot%`, żeby odwołać się do ścieżki katalogu systemu Windows Server 2008 lokalnego komputera. Zmienna ta przydaje się podczas tworzenia skrótów konsoli wykorzystywanych w przypadku innych komputerów, których główny katalog systemowy może mieć inną ścieżkę.

- ♦ /a. Użyj tego parametru, żeby uaktywnić tryb autora i umożliwić wprowadzanie zmian w konsoli. Otwarcie istniejącej konsoli z tym parametrem spowoduje nadpisanie jej trybu zapamiętanego dla bieżącej sesji.
- ♦ /32. Parametr uaktywnia 32-bitową wersję konsoli MMC. Parametr ten jest konieczny tylko wtedy, gdy 32-bitową wersję trzeba uruchomić w obrębie 64-bitowej wersji systemu Windows.
- ♦ /64. Parametr uaktywnia 64-bitową wersję konsoli MMC. Parametr działa tylko w przypadku 64-bitowej wersji systemu Windows.

Żałujemy, że konsolę usługi DNS chcesz załadować w trybie autora, żeby dodać do niej przystawkę DHCP. Aby konsolę usługi DNS uaktywnić w trybie autora, wykonaj następujące polecenie:

```
MMC %systemroot%\System32\dnsmgmt.msc /a
```



Prawym przyciskiem myszy możesz kliknąć plik *.msc* i z menu kontekstowego wybrać pozycję *Autor*. W efekcie plik zostanie otwarty w trybie autora.

Po uruchomieniu konsoli usługi DNS konsolę DHCP możesz dodać za pomocą polecenia *Dodaj/Usuń przystawkę* menu *Plik*. Przystawki omówiono w następnym punkcie.



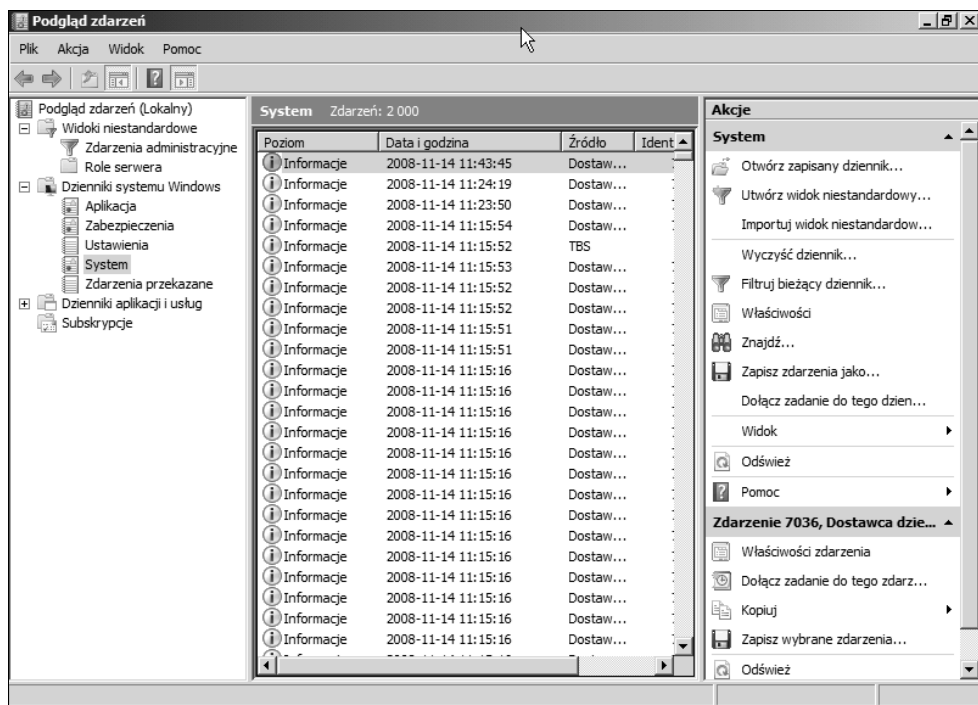
W razie potrzeby konsolę MMC można załadować w trybie autora, a następnie obie przystawki dodać przy użyciu polecenia *Dodaj/Usuń przystawkę* menu *Plik*.

Windows Server 2008 zapewnia kilka prekonfigurowanych konsol służących do realizowania różnych zadań administracyjnych. Większość plików tych konsol jest przechowywana w katalogu `%systemroot%\System32` i ma rozszerzenie *.msc* (skrót od Microsoft Console). Skróty dla kilku z tych konsol system Windows Server 2008 umieszcza w katalogu *Narzędzia administracyjne*, do którego można uzyskać dostęp z poziomu menu *Start/Wszystkie programy/Narzędzia administracyjne*. Zasadniczo każda z prekonfigurowanych konsol zawiera jedną lub więcej przystawek przeznaczonych do wykonania konkretnego zadania administracyjnego.

Wyraźnie starając się uprościć menu *Start*, w katalogu *Narzędzia administracyjne* Microsoft umieścił tylko niektóre skróty konsol. Jednakże można uruchomić dowolną konsolę przez dwukrotne kliknięcie jej pliku. Gdy się tak postąpi, najpierw zostanie załadowana konsola MMC, a następnie otwarte okno konsoli. Można również uaktywnić konsolę MMC i do własnych konsol dodać przystawki. Umożliwia to utworzenie niestandardowej konsoli zawierającej dowolne grupy przystawek, które są najczęściej używane lub przeznaczone do realizowania konkretnych zadań administracyjnych.

Zastosowanie przystawek

Choć konsola MMC tworzy szkielet dla zintegrowanych narzędzi administracyjnych systemu Windows Server 2008, same narzędzia są nazywane przystawkami. Każda przystawka konsoli MMC umożliwia realizowanie określonego zadania administracyjnego lub grupy zadań. Przykładowo przystawka Podgląd zdarzeń zajmuje miejsce niezależnego narzędzia o tej samej nazwie (rysunek 2.4). Z kolei podlegająca przystawce Zarządzanie komputerem



Rysunek 2.4. Przystawki realizują określone funkcje administracyjne i zastępują niezależne narzędzia, takie jak Podgląd zdarzeń

przystawka Zarządzanie dyskami zastępuje program Administrator dysków. Przystawka Użytkownicy i komputery usługi Active Directory zajęła miejsce narzędzia Zarządzanie użytkownikami dla domen itd.

Można wyróżnić dwie odmiany przystawek — niezależne i rozszerzające. Niezależne przystawki zwykle są nazywane po prostu przystawkami. Z kolei przystawki rozszerzające zazwyczaj określa się mianem rozszerzeń. Przystawki funkcjonują samodzielnie i można je wybiórczo dodawać do konsoli. Rozszerzenia są powiązane z przystawkami i dołącza się je do niezależnej przystawki lub innego rozszerzenia w obrębie drzewa konsoli. Rozszerzenia funkcjonują wewnątrz struktury niezależnej przystawki i przetwarzają obiekty będące docelowymi dla przystawki. Przykładowo przystawka Usługi uwzględnia cztery rozszerzenia — *Widok rozszerzony*, *Wysyłanie komunikatu konsoli*, *Zależności usługi* i *Rozszerzenie przystawki Snmp*.

Przystawki i rozszerzenia można dodać po załadowaniu konsoli w trybie autora. Choć domyślnie wszystkie rozszerzenia powiązane z przystawką są uwzględniane w momencie dodawania jej, dla przystawki można wyłączyć niektóre rozszerzenia.

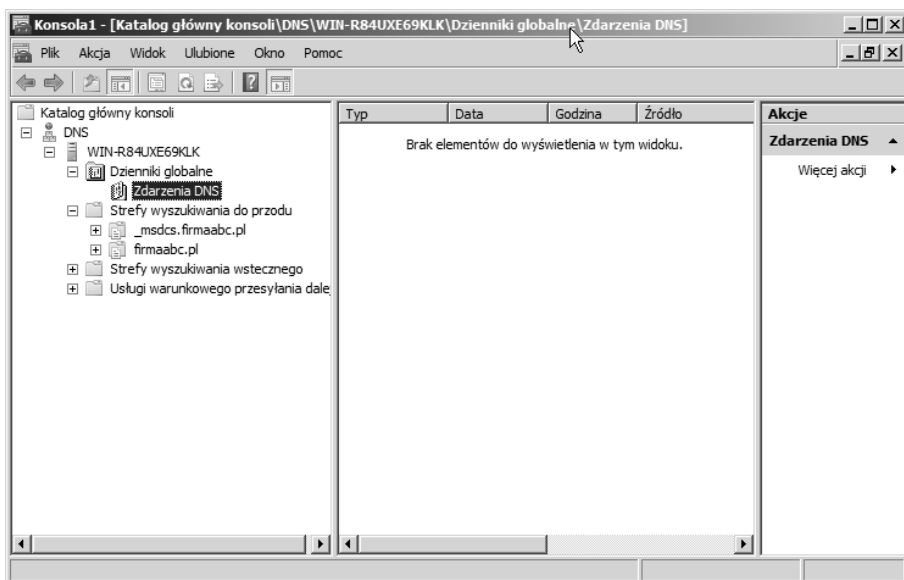
W celu dodania przystawki uruchom konsolę MMC w trybie autora i z menu *Plik* wybierz polecenie *Dodaj/Usuń przystawkę*. Sekcja *Wybrane przystawki* okna właściwości *Dodawanie lub usuwanie przystawek* zaprezentuje aktualnie wybrane przystawki. Przycisk *Edytuj rozszerzenia* udostępnia listę rozszerzeń dla aktualnie wybranej przystawki i pozwala dodać wszystkie rozszerzenia lub selektywnie wyłączyć bądź włączyć tylko niektóre z nich.

Okno dialogowe *Dodawanie lub usuwanie przystawek* wyświetla dostępne przystawki. Zaznacz przystawkę, która zostanie dołączona, i kliknij przycisk *Dodaj*. Zależnie od przystawki możesz zostać poproszony o doprecyzowanie wyboru. Gdy na przykład dodajesz przystawkę Menedżer urządzeń, możesz zdecydować się na zarządzanie lokalnym komputerem lub innymi znajdującym się w sieci. Podczas dodawania przystawki Zarządzanie zasadami zabezpieczeń IP możliwe jest dokonanie wyboru między lokalnym komputerem, domeną komputera, inną domeną lub komputerem.

Gdy skonfigurujesz przystawki i rozszerzenia w żądany sposób, zapisz konsolę, żeby później mieć możliwość szybkiego skorzystania z identycznej konfiguracji. W tym celu z menu *Plik* wybierz polecenie *Zapisz* lub *Zapisz jako* i określ nazwę konsoli. Domyślnie system Windows Server nową konsolę umieści w katalogu *Narzędzia administracyjne*, którego skrót znajduje się w menu *Start/Wszystkie programy*. W razie potrzeby można zmienić położenie tego katalogu.

Korzystanie z obszarów zadań

Obszar zadań jest kartą, w obrębie której można dodawać widoki panelu szczegółów i skróty do różnych funkcji zlokalizowanych wewnątrz i na zewnątrz konsoli. Skróty umożliwiają wykonywanie poleceń, otwieranie katalogów, wyświetlanie strony WWW, wywoływanie poleceń menu itp. Zasadniczo obszary zadań pozwalają utworzyć kartę uporządkowanych zadań, co ułatwia wykonanie pracy szybciej niż w przypadku istniejącego menu oferowanego przez przystawkę. Choć w konsoli można zdefiniować wiele obszarów zadań, musi ona zawierać przynajmniej jedną przystawkę. Rysunek 2.5 przedstawia obszar umożliwiający realizowanie różnych zadań wewnątrz przystawki usługi DNS.



Rysunek 2.5. Za pomocą obszarów zadań można wykonywać specyficzne czynności, takie jak związane z usługą DNS



W celu utworzenia obszarów zadań konsolę trzeba uruchomić w trybie autora.

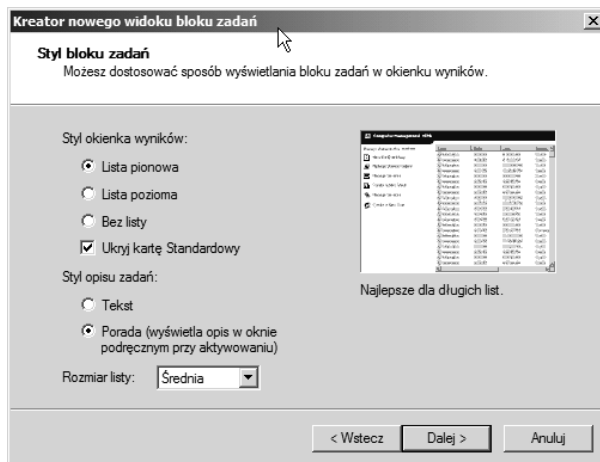
Obszar zadań może zawierać listę pochodzącą z panelu szczegółów, która jest ustawiona w poziomie lub w pionie. Pozioma orientacja sprawdza się dobrze w przypadku list wielokolumnowych (dla każdej pozycji przypada wiele pól), natomiast pionowe ułożenie przydaje się, gdy używa się długich list (każda pozycja dysponuje niewieloma polami). Można też skonfigurować obszar zadań, który nie będzie prezentował żadnych list. Oprócz listy obszar zadań dla każdego zadania zawiera ikonę z opisem zadania w postaci tekstowej lub wyskakującego okienka. W celu wykonania zadania trzeba kliknąć jego ikonę.

Tworzenie obszaru zadań

W celu utworzenia obszaru zadań kliknij prawym przyciskiem myszy obiekt w drzewie, dla którego obszar ma istnieć, i z menu wybierz pozycję *Nowy widok bloku zadań*. Konsola MMC uruchamia kreator, który ułatwia tworzenie obszaru zadań. Wewnątrz drugiej karty kreatora (rysunek 2.6) pojawiającej się tuż po karcie powitalnej określa się wygląd obszaru zadań. W trakcie dokonywania ustawień kreator pokazuje wyniki, żeby pomóc w ocenie efektów zmian.

Rysunek 2.6.

Karta kreatora pomaga skonfigurować wygląd obszaru zadań



W kolejnej karcie kreatora określa się pozycje, których obszar zadań będzie dotyczył. Poniższa lista zestawia dostępne opcje:

- ♦ **Wybrany element drzewa.** Opcja powoduje użycie obszaru zadań tylko dla pozycji zaznaczonej w drzewie. Gdy na przykład w przypadku przystawki usługi DNS obszar zadań utworzy się dla węzła *Strefy wyszukiwania do przodu* i użyje tej opcji, obszar zadań pojawi się wyłącznie po kliknięciu węzła *Strefy wyszukiwania do przodu*. Obszar nie będzie widoczny, jeśli zostanie uaktywniony węzeł *Strefy wyszukiwania wstecznego*.
- ♦ **Wszystkie elementy drzewa, będące tego samego typu co wybrany element drzewa.** Opcja sprawia, że obszar zadań dotyczy wszystkich obiektów drzewa, które są tego samego typu co wybrany obiekt. Zastosowanie tej opcji w przypadku

powyższej przykładowej przystawki usługi DNS spowodowałoby wyświetlenie obszaru zadań w momencie kliknięcia węzła *Strefy wyszukiwania do przodu* lub *Strefy wyszukiwania wstecznego*.

- ♦ **Użyj jako domyślnego bloku zadań dla tych elementów drzewa.** Użyj tej opcji, żeby konsola MMC automatycznie uaktywniała widok obszaru zadań, gdy użytkownik kliknie w drzewie obiekt powiązany z tym obszarem. Wyłącz opcję, żeby konsola MMC domyślnie wyświetlała standardowy widok.

W następnej karcie kreatora pojawi się prośba o wprowadzenie nazwy i opisu obszaru zadań. Nazwa pojawia się na samej górze obszaru zadań i w dolnej części jego karty. Opis jest widoczny w górnej części obszaru zadań poniżej jego nazwy.

W ostatniej karcie kreatora możesz kliknąć przycisk *Zakończ*, żeby utworzyć obszar zadań. Zaznaczenie opcji *Dodaj nowe zadania do tego bloku zadań po zamknięciu kreatora* spowoduje uruchomienie narzędzia *Kreator nowego zadania* po kliknięciu przycisku *Zakończ*. Kreator ten, który opisano w następnym podpunkcie, pomaga utworzyć zadania obszaru zadań.

Tworzenie zadań

Po wygenerowaniu obszaru zadań oczywiście trzeba utworzyć dla niego zadania. Jeśli realizujesz proces tworzenia obszaru zadań, zaznacz opcję *Dodaj nowe zadania do tego bloku zadań po zamknięciu kreatora*. Alternatywnie prawym przyciskiem myszy kliknij węzeł drzewa powiązany z obszarem zadań i z menu wybierz pozycję *Edytuj widok bloku zadań*, a następnie uaktywnij kartę *Zadania* i kliknij przycisk *Nowe*.

Pierwsza przydatna karta kreatora zażąda określenia typu dodawanego zadania. W tym przypadku dostępne są następujące opcje:

- ♦ **Polecenie menu.** Wybierz tę opcję, żeby wywołać polecenie menu. W następnej karcie kreatora określa się źródło polecenia i samo polecenie. Dostępne polecenia nawiązują do wybranego źródła. Zaznacz obiekt, a następnie wybierz żądane polecenie.
- ♦ **Polecenie powłoki.** Użyj tej opcji w celu uruchomienia programu, wywołania skryptu, załadowania obiektu WWW, uaktywnienia skrótu lub zrealizowania dowolnego innego zadania, które można zainicjować z poziomu wiersza poleceń. Kreator żąda wprowadzenia polecenia, jego parametrów lub przełączników, ścieżki katalogu startowego i statusu okna (zminimalizowane, normalne lub zmaksymalizowane).
- ♦ **Nawigacja.** Zastosuj tę opcję, żeby dodać ikonę dla istniejącej pozycji listy *Ulubione*.

Kreator żąda też podania nazwy i opisu zadania, określenia ikony, która zostanie powiązana z każdym zadaniem, a także na końcu pracy oferuje opcję pozwalającą ponownie uruchomić kreator w celu utworzenia kolejnego zadania.

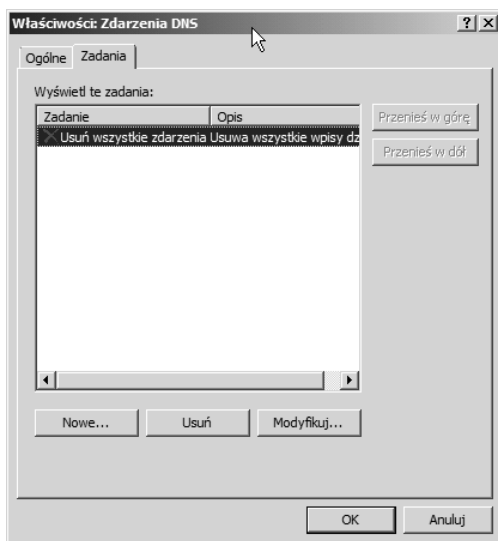
Modyfikowanie obszaru zadań

Istnieje możliwość zmodyfikowania istniejącego obszaru zadań w celu dodania lub usunięcia zadań bądź zmiany opcji widoku obszaru. Prawym przyciskiem myszy w obrębie drzewa kliknij obiekt powiązany z obszarem zadań i z menu wybierz polecenie *Edytuj widok bloku zadań*. Konsola MMC wyświetli okno właściwości obszaru zadań. Karta *Ogólne* prezentuje te same właściwości (między innymi typ i rozmiar listy), które określono podczas tworzenia obszaru zadań. W razie potrzeby zmodyfikuj opcje.

Karta *Zadania* widoczna na rysunku 2.7 wyszczególnia istniejące zadania i umożliwia utworzenie nowych. Kliknięcie przycisku *Nowe* powoduje uruchomienie narzędzia *Kreator nowego zadania*, a przycisku *Usuń* usunięcie zaznaczonego zadania. Przycisk *Modyfikuj* pozwala zmienić nazwę zadania, jego opis i ikonę, lecz nie umożliwia zmodyfikowania samego zadania. Aby to zrobić, trzeba usunąć zadanie i ponownie je utworzyć. Można też użyć przycisków *Przenieś w górę* i *Przenieś w dół*, żeby zmienić kolejność zadań na liście. W rezultacie inaczej będą uporządkowane zadania widoczne w obszarze zadań.

Rysunek 2.7.

Karta *Zadania* umożliwia dodawanie, usuwanie i modyfikowanie zadań



Inne dodatkowe narzędzia

Przystawki to tylko jeden z typów obiektów, które można dodawać do konsoli MMC. Do innych obiektów zaliczają się kontrolki ActiveX, odnośniki do stron WWW, katalogi, widoki obszaru zadań i zadania. W poprzednim punkcie omówiono widoki obszaru zadań i zadania. Poniższa lista podsumowuje dodatkowe obiekty.

- ♦ **Kontrolki ActiveX.** Kontrolki ActiveX można dodać do konsoli jako widok szczegółów lub wyników (prawy panel) dla zaznaczonego węzła drzewa. Przykładem takiej kontrolki jest kontrolka System Monitor Control, która w oknie narzędzia *Monitor wydajności* wyświetla status dotyczący wydajności systemu. Z menu *Plik* wybierz polecenie *Dodaj/Usuń przystawkę*, w obrębie listy zaznacz kontrolkę ActiveX,

a następnie kliknij przycisk *Dodaj*. Konsola MMC zapewnia kreator ułatwiający osadzenie kontrolki ActiveX. W razie konieczności kreator zażąda dodatkowych informacji.

- ♦ **Odnosiniki do stron WWW.** W oknie konsoli można umieścić łącza z dowolnymi adresami URL, których docelowe zasoby (witryna WWW, witryna FTP itp.) mogą być wyświetlone za pomocą przeglądarki.
- ♦ **Katalogi.** W obrębie konsoli można wstawić foldery pełniące rolę kontenerów innych obiektów. Katalogi mogą zostać wykorzystane do zorganizowania narzędzi konsoli.



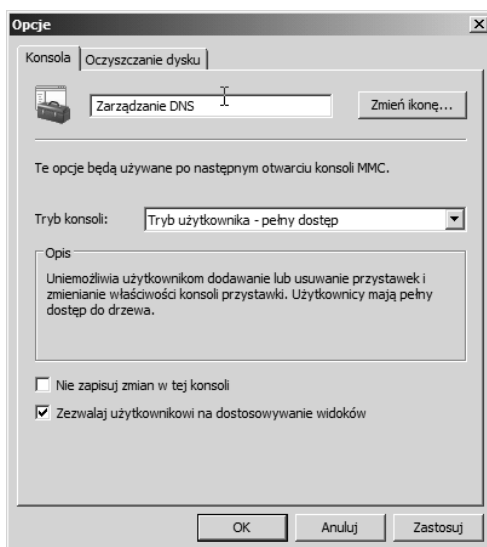
Czy chciałbyś dodać do konsoli lokalny lub sieciowy katalog? W tym celu po prostu użyj obiektu *Łącze do adresu w sieci Web* i zamiast do internetowego adresu URL odwołać go do katalogu.

Dostosowywanie konsoli MMC do własnych wymagań

Jak w przypadku większości aplikacji, również konsolę MMC można dostosować do własnych wymagań lub preferencji. Przede wszystkim w trybie autora można skonfigurować ustawienia konsoli tak, żeby określić sposób, w jaki będzie prezentowała się w kolejnych sesjach. Można na przykład skonfigurować konsolę z myślą o trybie użytkownika z limitowanym dostępem i pojedynczym oknem, żeby ograniczyć działania, jakie użytkownik może podejmować w obrębie konsoli. W celu skonfigurowania konsoli trzeba najpierw otworzyć ją w trybie autora. Z menu *Plik* wybierz pozycję *Opcje*, żeby otworzyć okno dialogowe *Opcje* (rysunek 2.8). Określ ustawienia, a następnie zapisz konsolę. Zmiany zostaną uwzględnione przy kolejnym uruchomieniu konsoli.

Rysunek 2.8.

Okno dialogowe
Opcje umożliwiający
skonfigurowanie
konsoli z myślą
o przyszłych sesjach



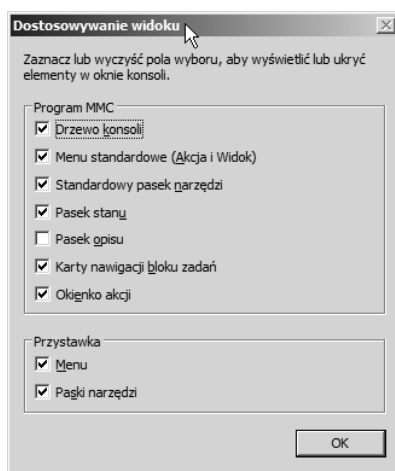
Poniższa lista objaśnia dostępne opcje.

- ♦ **Zmień ikonę.** Kliknij opcję, żeby zmienić ikonę powiązaną z plikiem `.msc`. W pliku `%systemroot%\system32\Shell32.dll` znajduje się kilka ikon.
- ♦ **Tryb konsoli.** Określ tryb, w którym konsola ma zostać uruchomiona w następnej sesji. Do wyboru jest tryb autora i jeden z trzech wcześniej omówionych trybów użytkownika.
- ♦ **Nie zapisuj zmian w tej konsoli.** Uaktywnij tę opcję, żeby uniemożliwić użytkownikowi zapisywanie zmian w konsoli. Oznacza to, że opcja ta chroni przed zapisem.
- ♦ **Zezwalaj użytkownikowi na dostosowywanie widoków.** Zaznacz tę opcję, żeby zezwolić użytkownikom na dodawanie okien przeznaczonych dla pozycji konsoli. Wyłącz opcję w celu uniemożliwienia użytkownikom dodawania okien.

Wewnątrz konsoli MMC można również kontrolować opcje widoku. W tym celu z menu *Widok* wybierz polecenie *Dostosuj*, żeby otworzyć okno dialogowe *Dostosowywanie widoku* widoczne na rysunku 2.9. Opcje zawarte w tym oknie nie wymagają objaśnienia.

Rysunek 2.9.

Okno dialogowe Dostosowywanie widoku umożliwia ustawienie właściwości widoku konsoli MMC



Porównanie panelu sterowania i konsoli MMC

Nawet pomimo tego, że obecnie konsola MMC stanowi centrum uwagi w przypadku wielu zadań administracyjnych, które będą regularnie wykonywane, panel sterowania nie odszedł w zapomnienie. Panel sterowania nadal istnieje, ma się dobrze i zawiera kilka obiektów służących do konfigurowania sprzętu i funkcji komputera. Narzędzia stworzone dla konsoli MMC nie zastępują obiektów panelu sterowania i odwrotnie. Jednakże w panelu sterowania znajdzie się kilka narzędzi konsoli MMC zlokalizowanych w katalogu *Narzędzia administracyjne*.

Panel sterowania systemu Windows Server 2008 działa podobnie jak panele sterowania systemu Windows Server 2003 i starszych wersji systemu Windows. Okazuje się, że wiele obiektów jest identycznych lub podobnych. W dalszej części rozdziału objaśniono obiekty panelu sterowania. Dalej omówiono podstawowy zestaw narzędzi konsoli MMC służących do zarządzania systemem Windows Server 2008.

Zmiany dotyczące narzędzi konsoli MMC spowodowane przez zaporę firewall systemu Windows

Przed zapoznaniem się z konkretnymi narzędziami konsoli MMC wchodzącymi w skład systemu Windows Server 2008 powinno się zrozumieć kilka ograniczeń narzuconych przez zmiany wprowadzone w zaporze firewall tego systemu. Zmiany mają wpływ na możliwość zdalnego zarządzania komputerem Windows Server 2008 z wieloma narzędziami konsoli MMC.

Domyślnie zaporę firewall systemu Windows blokuje ruch sieciowy przychodzący do portu 445. Port ten jest wykorzystywany przez wiele narzędzi zdalnego zarządzania. Jeśli przy próbie zdalnego administrowania pojawi się jeden z poniższych komunikatów o błędzie, oznacza to, że winnym tego może być wyżej przedstawiona zasada zapory firewall.

- ♦ Nie można uzyskać dostępu do komputera *NazwaKomputera*.
- ♦ Nie można otworzyć obiektu zasad grupy na komputerze *NazwaKomputera*. Być może nie masz odpowiednich uprawnień.
- ♦ Szczegóły: Nie można odnaleźć ścieżki sieciowej.
- ♦ Nie można odnaleźć obiektu (komputera) o następującej nazwie: „*NazwaKomputera*”. Sprawdź, czy wybrane typy i lokalizacja obiektów oraz wpisana nazwa obiektu są prawidłowe, lub usuń zaznaczenie tego obiektu.
- ♦ Nie można zarządzać komputerem *\\NAZWA_KOMPUTERA.PRZYKLAD.COM*. Nie można odnaleźć ścieżki sieciowej. Wybierz polecenie „Podłącz do innego komputera” z menu Akcja, aby zarządzać innym komputerem.
- ♦ Wystąpił błąd systemowy 53. Nie można odnaleźć ścieżki sieciowej.

Aby zaradzić temu problemowi, po stronie zdalnego serwera skonfiguruj zaporę firewall systemu Windows tak, żeby nie blokowała portu 445. Można to zrobić przy użyciu graficznego interfejsu zapory firewall, z poziomu wiersza poleceń lub za pomocą zasady grupy (w rozdziale 24. zamieszczono szczegóły dotyczące konfigurowania zapory firewall z wykorzystaniem zasady grupy).

Zastosowanie narzędzi konsoli MMC

Jak wcześniej wspomniano, Windows Server 2008 zawiera kilka predefiniowanych konsol przeznaczonych do realizowania różnych zadań zarówno w obrębie lokalnych komputerów, jak i za pośrednictwem sieci. W poniższych punktach dokonano przeglądu tych narzędzi. Jeśli Czytelnik szuka niektórych z tych przystawek i nie może ich znaleźć, powodem takiego stanu rzeczy może być to, że na serwerze nie zainstalowano odpowiednich funkcji lub ról.

Urząd certyfikacji

Konsola Urząd certyfikacji pojawiająca się w katalogu *Narzędzia administracyjne* pod nazwą *certification authority* jest instalowana tylko wtedy, gdy serwer skonfiguruje się jako urząd certyfikacji. Urząd certyfikacji można przygotować po zainstalowaniu roli *Usługi certyfikatów* w usłudze Active Directory. Usługi certyfikatów umożliwiają serwerowi tworzenie certyfikatów dla siebie, a także innych serwerów, stacji roboczych i użytkowników sieciowych (lokalnie lub za pośrednictwem internetu). Jeżeli na przykład trzeba skonfigurować serwer WWW tak, żeby na potrzeby sporządzania materiałów wymagał protokołu SSL, trzeba w tym celu na serwerze zainstalować certyfikat (aby serwer WWW obsługiwał protokół SSL, w jego obrębie nie muszą zostać zainstalowane usługi certyfikatów, lecz jedynie certyfikat). Urząd certyfikacji systemu Windows Server 2008 może wygenerować certyfikat, dzięki czemu eliminuje się konieczność nabywania go od komercyjnego urzędu, takiego jak Thawte lub VeriSign. Jeśli jednak osoby przeglądające zasoby witryny nie dodadzą urzędu certyfikacji do swojej listy zaufanych źródeł, w momencie wyświetlenia stron witryny ujrzą ostrzeżenia dotyczące certyfikatu.

Konsola Urząd certyfikacji służy do zarządzania usługami certyfikatów lokalnego i zdalnego serwera. Możliwe jest skonfigurowanie ustawień zasad certyfikatów, przeglądanie przetwarzanych i nieudanych żądań dotyczących certyfikatów, a także wydanych i wycofanych certyfikatów. Konsola pozwala też zarządzać ogólnymi właściwościami urzędu certyfikacji, takimi jak na przykład możliwość publikowania certyfikatów w strukturze usługi Active Directory, określanie sposobu odpowiadania serwera na żądanie dotyczące certyfikatu i kontrolowanie zabezpieczeń urzędu.



Kilka podrozdziałów rozdziału 16., w tym podrozdział „Usługi certyfikacyjne Active Directory”, szczegółowo objaśnia usługi certyfikatów, a także omawia zarządzanie nimi z wykorzystaniem konsoli Urząd certyfikacji.

Zarządzanie klastrem pracy awaryjnej

Konsola Zarządzanie klastrem pracy awaryjnej jest dostępna w wersji Enterprise Edition systemu Windows Server 2008. Jest podstawowym narzędziem umożliwiającym skonfigurowanie klastra. Klaster pozwala grupie serwerów funkcjonować jako pojedynczej logicznej jednostce zapewniającej możliwość przełączania po awarii.

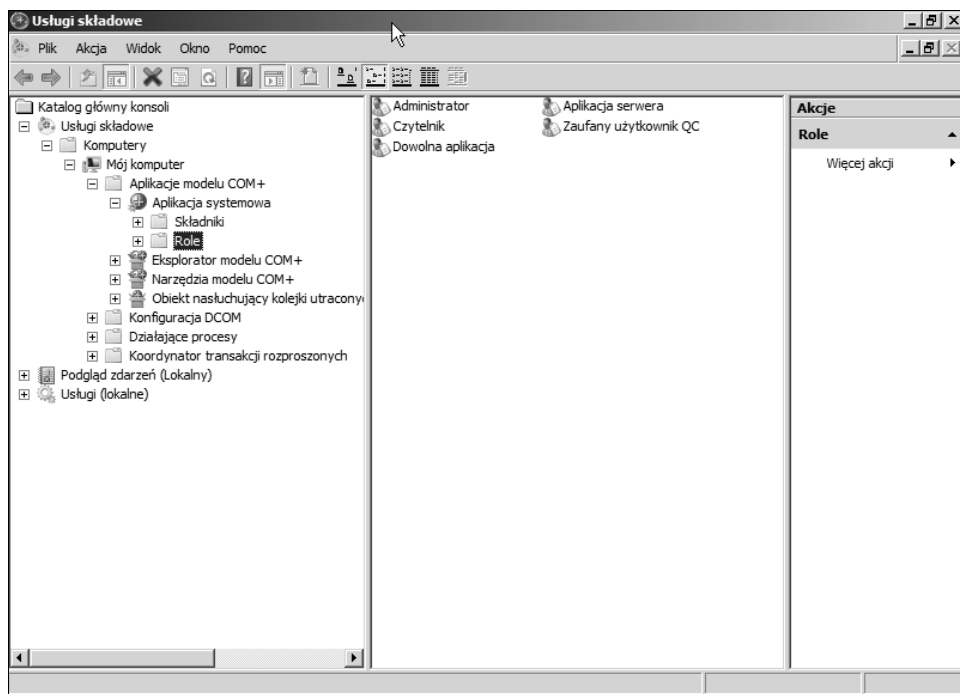


Wersje Standard Edition i Web Edition systemu Windows Server 2008 nie obsługują klastra.

Konsoli Zarządzanie klastrem pracy awaryjnej można użyć do utworzenia i skonfigurowania klastra, a także zrealizowania takich typowych zadań, jak dodawanie węzłów klastra, konfigurowanie węzła i właściwości klastra oraz wstrzymywanie usługi klastrowania.

Usługi składowe

Podstawowym zadaniem konsoli *Usługi składowe* (rysunek 2.10) jest zapewnienie narzędzi zarządzających aplikacjami COM+. Technologia COM+ oferuje strukturę na potrzeby projektowania aplikacji rozproszonych (aplikacje klient-serwer). Konsola *Usługi składowe*



Rysunek 2.10. Za pomocą konsoli Usługi składowe można skonfigurować aplikacje COM+, jak również ogólne usługi systemu Windows Server 2008

umożliwia skonfigurowanie systemu pod kątem usługi Usługi składowe i początkowych ustawień usługi, a ponadto instalację i konfigurację aplikacji COM+ oraz monitorowanie i dostrajanie komponentów.



Konfigurowaniu aplikacji COM+ towarzyszy ich projektowanie. Z tego powodu w książce nie zamieszczono dokładnego omówienia konfigurowania tego typu aplikacji.

Oto podstawowe węzły konsoli *Usługi składowe*:

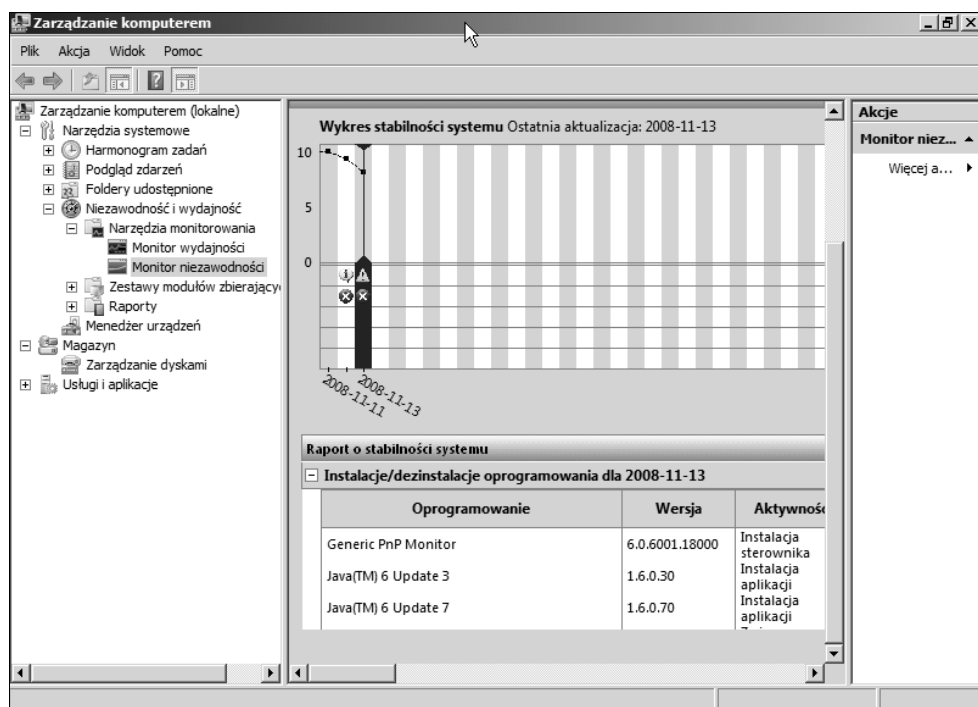
- ♦ **Aplikacje modelu COM+.** Przy użyciu tego węzła można skonfigurować właściwości składników i ról, a także ustawienia komponentów COM+.
- ♦ **Konfiguracja DCOM.** Węzeł ten pozwala skonfigurować komponenty DCOM (*Distributed COM*), włącznie z ich ustawieniami zabezpieczeń.
- ♦ **Koordynator transakcji rozproszonych.** Węzeł ten umożliwia przeglądanie listy transakcji DTC i monitorowanie statystyk dotyczących transakcji.
- ♦ **Działające procesy.** Za pomocą tego węzła można monitorować i debugować aktywne procesy. Prawym przyciskiem myszy kliknij aplikację i z menu wybierz pozycję *Zrzucić*, żeby na potrzeby debugowania i analizy zapisać w pliku stan aplikacji.



Czytelnik zauważy, że konsola *Usługi składowe* dołączona do systemu Windows Server 2008 zawiera węzły dla przystawek Podgląd zdarzeń, Użytkownicy i komputery usługi Active Directory i Usługi. Przystawki te są też dostępne jako oddzielne konsole. Więcej informacji można znaleźć w dalszej części rozdziału, w punkcie „Podgląd zdarzeń”, w podpunkcie „Usługi” i w punkcie „Zastosowanie przystawki Podgląd zdarzeń”. Omówienie usługi Active Directory znajduje się w rozdziałach od 17. do 23.

Zarządzanie komputerem

Konsola Zarządzanie komputerem (rysunek 2.11) zapewnia narzędzia służące do zarządzania kilkoma aspektami związanymi z komputerem. W celu załadowania tej konsoli kliknij prawym przyciskiem myszy ikonę *Mój komputer* i z menu wybierz polecenie *Zarządzaj* lub z menu *Start/Wszystkie programy/Narzędzia administracyjne* wybierz pozycję *Zarządzanie komputerem*. Konsola Zarządzanie komputerem oferuje trzy podstawowe węzły — *Narzędzia systemowe*, *Magazyn* i *Usługi i aplikacje*. Węzeł *Narzędzia systemowe* zapewnia rozszerzenia pozwalające przeglądać informacje o systemie, konfigurować urządzenia, sprawdzać dzienniki zdarzeń itp. Węzeł *Magazyn* oferuje narzędzia zarządzające fizycznymi i logicznymi dyskami oraz przenośnymi magazynami danych. Węzeł *Usługi i aplikacje* daje możliwość skonfigurowania telefonii, składnika Windows Management Instrumentation, usług, usługi indeksowania i serwera IIS. Zależnie od konfiguracji systemu w obrębie tego węzła mogą również pojawiać się inne aplikacje.



Rysunek 2.11. Konsola Zarządzanie komputerem integruje kilka przystawek w celu ułatwienia zarządzania systemem, jego urządzeniami magazynującymi dane i usługami

Konsoli Zarządzanie komputerem można użyć do administrowania lokalnym lub zdalnym komputerem. Prawym przyciskiem myszy kliknij węzeł *Zarządzanie komputerem* i z menu wybierz polecenie *Podłącz do innego komputera*, żeby zarządzać zdalnym komputerem. Choć zadania, które można wykonać, zwykle są takie same, niezależnie od tego, czy ma się do czynienia z lokalnym, czy ze zdalnym komputerem, część zadań można zrealizować wyłącznie w przypadku lokalnego systemu. W niniejszym rozdziale założono, że narzędzia *Zarządzanie komputerem* używa się do administrowania lokalnym komputerem.



W tym punkcie omówiono przystawki rozszerzające konsoli Zarządzanie komputerem. Jednakże wiele z tych rozszerzeń może być zastosowanych niezależnie w obrębie ich własnych konsol. Przykładowo do skonfigurowania usług można użyć przystawki *Services.msc*, a nie węzła *Usługi* konsoli Zarządzanie komputerem. Dostępnych przystawek (pliki z rozszerzeniem *.msc*) można szukać w katalogu `%systemroot%\System32`.

Podgląd zdarzeń

Narzędzie *Podgląd zdarzeń* umożliwia przeglądanie zdarzeń dzienników *Aplikacja*, *Zabezpieczenia* i *System*, a także konfigurowanie dzienników (rozmiar, wypełnianie danymi itp.). Więcej informacji zamieszczono w dalszej części rozdziału, w punkcie „Zastosowanie przystawki Podgląd zdarzeń”.

Niezawodność i wydajność

Węzeł *Niezawodność i wydajność* przystawki Zarządzanie komputerem zapewnia narzędzia konfiguracyjne monitorowanie wydajności. Możliwe jest skonfigurowanie dzienników liczników, dzienników śladu i alertów. Węzeł ten przydaje się tylko w przypadku sprawdzania lub modyfikowania ustawień, gdyż nie pozwala na przeprowadzenie żadnej operacji monitorowania wydajności. W tym celu trzeba skorzystać z przystawki *Niezawodność i wydajność* konsoli MMC. W rozdziale 25. znajdują się szczegółowe informacje dotyczące konfigurowania dzienników wydajności i alertów, a także monitorowania wydajności systemu.

Foldery udostępnione

Węzeł *Foldery udostępnione* przystawki Zarządzanie komputerem pozwala przeglądać udostępnione katalogi, połączenia i otwarte pliki i zarządzać nimi. Węzeł *Udziały* umożliwia sprawdzanie udziałów wybranego komputera. Ponadto dwukrotne kliknięcie udziału daje możliwość przeglądu i zmiany jego właściwości i uprawnień. W rozdziale 15. można znaleźć informacje o udostępnianiu katalogów w strukturze usługi Active Directory.



Udostępnione katalogi można tworzyć i zarządzać nimi za pośrednictwem interfejsu programu Eksplorator Windows. Zaletą użycia węzła *Foldery udostępnione* zamiast tego interfejsu jest to, że od razu można zobaczyć wszystkie udziały komputera.

Czytelnik zauważy, że domyślnie w obrębie systemu znajduje się kilka udziałów, z których większość jest ukrytych (na początku nazwy mają znak \$). Do udziałów tych zaliczają się następujące:

- ♦ *dysk\$*. Na potrzeby administracyjne system Windows Server 2008 udostępnia główny katalog każdego dysku jako ukryty udział. Można połączyć się z udziałem przy użyciu ścieżki UNC postaci `\\serwer\dysk$`, gdzie łańcuch *serwer* identyfikuje nazwę komputera, a łańcuch *dysk* literę dysku (na przykład `\\appsrvd`). Członkowie grup Administratorzy i Operatorzy kopii zapasowych mogą nawiązać połączenie z udziałami administracyjnymi systemów Windows 2000 Professional, Windows XP i Windows Vista. Z kolei członkowie grupy Operatorzy serwera mogą korzystać z udziałów administracyjnych komputerów z systemem Windows Server 2008. To samo dotyczy członków grup Administratorzy i Operatorzy kopii zapasowych.
- ♦ *ADMIN\$*. Ten udział administracyjny wskazuje na główny katalog systemu operacyjnego (zwykle jest to katalog `\Windows` lub `\WINNT`). Udział jest wykorzystywany przez system podczas zdalnego zarządzania.
- ♦ *IPC\$*. Udział służy do udostępniania potoków nazwanych i jest stosowany podczas zdalnego administrowania oraz przeglądania udziałów komputera.
- ♦ *PRINT\$*. Udział umożliwia zdalne zarządzanie drukarkami i domyślnie wskazuje na katalog `%systemroot%\System32\spool\drivers`.
- ♦ *NETLOGON*. Udział jest wykorzystywany do obsługi logowania użytkowników (zwykle sprowadza się to do przechowywania skryptów i profili związanych z logowaniem). W domenach Windows Server 2008 i Windows Server 2003 udział *NETLOGON* wskazuje na katalog `sysvol\domain\Scripts` kontrolerów domeny.



Obszerne omówienie udostępniania i zabezpieczania, dostępu do katalogów w trybie offline i powiązanych zagadnień zamieszczono w rozdziale 15.

Węzeł *Sesje* pozwala zapoznać się z listą użytkowników aktualnie połączonych z systemem. W celu odłączenia użytkownika kliknij go prawym przyciskiem myszy i z menu wybierz polecenie *Rozłącz*. Rozłączenie użytkownika może spowodować utratę przez niego danych. W związku z tym można najpierw przesłać do użytkownika komunikat wyświetlany w obrębie konsoli. Aby to zrobić, prawym przyciskiem myszy kliknij węzeł *Udziały* lub *Foldery udostępnione* i z menu *Wszystkie zadania* wybierz polecenie *Wyślij komunikat konsoli*.



W przypadku przeglądania sesji zdalnego komputera połączenie pojawia się jako otwarty potok nazwany, którego nie można zamknąć.

Węzeł *Otwarte pliki* umożliwia przejrzanie plików otwartych przez zdalnych użytkowników. W celu zamknięcia konkretnego pliku kliknij go prawym przyciskiem myszy i z menu wybierz polecenie *Zamknij otwarty plik*. Aby zamknąć wszystkie pliki, prawym przyciskiem myszy kliknij węzeł *Otwarte pliki* i z menu wybierz polecenie *Odlącz wszystkie otwarte pliki*. Ponieważ odłączanie użytkowników i zamykanie plików może spowodować utratę danych, powinno się wcześniej podjąć próbę wysłania komunikatu do konsoli użytkownika.

Menedżer urządzeń

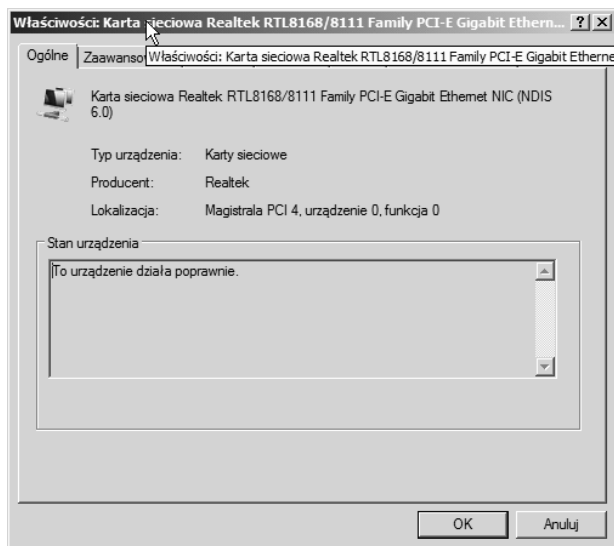
Menedżer urządzeń zapewnia jednolity interfejs służący do przeglądania urządzeń i ich zasobów (kanałów DMA, pamięci, przerwań IRQ itp.) i zarządzania nimi. Przystawka Menedżer urządzeń wyświetla urządzenia z wykorzystaniem struktury drzewiastej. Aby

zobaczyć urządzenia znajdujące się w obrębie gałęzi, rozwiń ją. Brak ikony obok urządzenia oznacza, że działa ono poprawnie. Ikona żółtego wykrzyknika wskazuje na potencjalny problem z urządzeniem, taki jak konflikt zasobów. Ikona czerwonego znaku X identyfikuje urządzenie, które jest odłączone, wyłączone lub niewykorzystywane w bieżącym profilu sprzętowym.

Menedżer urządzeń jest podstawowym narzędziem używanym do konfigurowania sprzętu komputera. W celu sprawdzenia urządzenia lub zarządzania nim zlokalizuj je w panelu szczegółów i dwukrotnie kliknij (lub kliknij prawym przyciskiem myszy i z menu wybierz pozycję *Właściwości*). Spowoduje to otwarcie okna właściwości urządzenia. Zawartość okna zmienia się w zależności od typu urządzenia. Rysunek 2.12 przedstawia typowe okno właściwości karty sieciowej.

Rysunek 2.12.

Za pomocą okna właściwości urządzenia można sprawdzić i skonfigurować ustawienia związane na przykład z wykorzystaniem zasobów



Karta *Ogólne* widoczna na rysunku 2.12 zapewnia ogólne informacje o urządzeniu, takie między innymi jak jego typ i producent.

Z praktycznego punktu widzenia nie ma zbyt większego sensu omawiać w rozdziale każdego możliwego ustawienia dla wszystkich istniejących typów urządzeń. W poniższych podpunktach objaśniono zadania typowe dla większości zadań — zmienianie sterowników i modyfikowanie przydziałów zasobów.

Zmiana sterownika

Karta właściwości *Sterownik* umożliwia sprawdzenie szczegółów dotyczących sterownika, a także odinstalowanie i zaktualizowanie sterownika urządzenia. Kliknij przycisk *Szczegóły sterownika*, żeby wyświetlić listę plików tworzących sterownik urządzenia. Lista przydaje się w przypadku sprawdzania wersji pliku lub sterownika w celu uzyskania pewności, że korzysta się z konkretnej wersji. Użyj przycisku *Odinstaluj*, aby usunąć zaznaczony sterownik urządzenia.

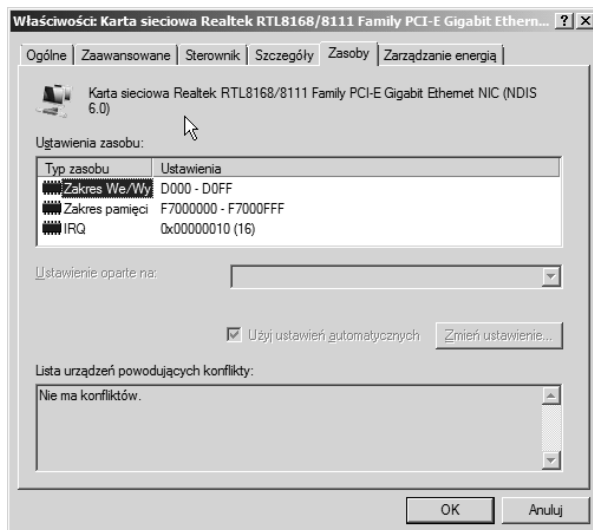
Przycisk *Aktualizuj sterownik* uruchamia narzędzie *Kreator aktualizacji sterowników*. Kreatora tego użyj do zainstalowania zaktualizowanego sterownika urządzenia. Kreator umożliwia przeszukanie dyskiety i dysku CD-ROM, określenie innej lokalizacji (lokalny lub zdalny udział) lub skorzystanie z witryny Microsoft Windows Update. W celu ukończenia aktualizacji wystarczy postępować zgodnie z instrukcjami. W określonych sytuacjach zmiana sterownika wymaga zrestartowania komputera.

Przydział zasobów

Ponieważ Windows Server 2008 obsługuje technologię *Plug and Play* (PnP), może automatycznie przydzielać zasoby sprzętowe, takie jak kanały DMA, przerwania IRQ, bazowe adresy wejścia-wyjścia i pamięć UMA. W określonych przypadkach (dotyczy to zwłaszcza starszych urządzeń nieobsługujących technologii PnP) trzeba będzie ręcznie skonfigurować przydzielanie zasobów. W tym celu otwórz okno właściwości urządzenia i uaktywnij kartę *Zasoby*. Jeśli karta nie udostępnia żadnych zasobów, które można zmodyfikować, wyłącz opcję *Użyj ustawień automatycznych*, żeby uaktywnić tryb ręcznej konfiguracji ustawień (rysunek 2.13).

Rysunek 2.13.

Karta Zasoby okna właściwości urządzenia daje możliwość skonfigurowania wykorzystywania przez nie zasobów



W większości sytuacji system Windows Server 2008 zapewnia wiele predefiniowanych konfiguracji urządzeń, takich jak kombinacja przerwania IRQ i zakresu adresów wejścia-wyjścia. Wyłącz opcję *Użyj ustawień automatycznych*, a następnie z listy rozwijanej wybierz inny zestaw konfiguracyjny. W celu zmodyfikowania poszczególnych ustawień w obrębie listy *Ustawienia zasobu* kliknij najpierw zasób, który ma być zmieniony, po czym kliknij przycisk *Zmień ustawienie*. W otwartym oknie dialogowym określ żądaną wartość ustawienia i kliknij przycisk *OK*.

Użytkownicy i grupy lokalne

Węzeł *Użytkownicy i grupy lokalne* przystawki Zarządzanie komputerem pozwala tworzyć lokalne konta użytkowników i grup wolno stojących i członkowskich serwerów Windows Server 2008 oraz zarządzać nimi. Węzła tego brakuje w przypadku kontrolera domeny, gdyż

do tworzenia kont użytkowników i grup usługi Active Directory wykorzystuje się przystawkę Użytkownicy i komputery usługi Active Directory.



Użytkowników i grupy szczegółowo omówiono w rozdziale 23.

Jeśli Czytelnik jest zaznajomiony z tworzeniem kont użytkowników i grup w poprzednich wersjach systemu Windows Server, nie będzie miał żadnego problemu z generowaniem kont za pomocą narzędzia *Użytkownicy i grupy lokalne*. W przeciwnym razie trzeba się zapoznać z obszernym omówieniem procesu tworzenia kont użytkowników i grup, które zamieszczono w rozdziale 23. Podstawową różnicą między tworzeniem lokalnych użytkowników i grup a tych samych obiektów w strukturze usługi Active Directory jest to, że usługa ta udostępnia dodatkowe właściwości kont użytkowników i grup. Ponadto tworzenie kont użytkowników i grup wymaga znajomości uprawnień, praw, zasad grupy i profili użytkowników (więcej na ten temat można znaleźć w rozdziale 23.).

Zarządzanie dyskami

Węzeł *Zarządzanie dyskami* przydaje się, gdy trzeba zarządzać fizycznymi dyskami i woluminami. Przystawka Zarządzanie dyskami zastępuje narzędzie *Administrator dysków* systemu Windows NT. W przeciwieństwie do tego programu przystawka Zarządzanie dyskami pozwala od razu zrealizować większość zadań. W przypadku narzędzia *Zarządzanie dyskami* większość zadań wymaga zatwierdzenia zmian (na przykład tworzenie lub usuwanie partycji). Jeśli Czytelnik jest doświadczonym administratorem systemu Windows NT, o tej ważnej uwadze musi pamiętać podczas modyfikowania magazynów danych za pomocą przystawki Zarządzanie dyskami.

Część zadań można wykonać przy użyciu narzędzia *Zarządzanie dyskami*, w tym zarządzanie partycjami, konwertowanie dysków podstawowych na dynamiczne, tworzenie woluminów (proste, łączone, rozłożone, lustrzane, RAID-5), tworzenie i usuwanie fizycznych woluminów i formatowanie dysków.



Obszerne omówienie urządzeń magazynujących dane i zarządzania nimi (z wykorzystaniem również przystawki Zarządzanie dyskami) zawarto w rozdziale 13.

Defragmentator dysków

Wraz z upływem czasu dane na używanym dysku są porozrzucane w nieciągłych klastrach. Doprowadza to do defragmentacji dysku. Wydajność dysku jest największa, gdy dane nie uległy defragmentacji. Wynika to stąd, że do odczytania danych potrzeba mniej czasu (główki napędu nie muszą tak bardzo się przemieszczać, żeby skompletować żądane dane). Węzeł *Defragmentator dysków* przystawki Zarządzanie komputerem pozwala przeanalizować dysk pod kątem fragmentacji, a następnie poddać go defragmentacji.



W rozdziale 13. opisano narzędzie *Defragmentator dysków* i inne opcje zwiększania wydajności dysków.

Magazyn wymienny

Węzeł *Magazyn wymienny* zapewnia narzędzie służące do konfigurowania wymiennych urządzeń i nośników danych i zarządzania nimi. Za pomocą przystawki Magazyn wymienny można monitorować takie nośniki jak taśmy i dyski optyczne, a także ich urządzenia (zmieniacz automatyczny, magazyn taśmowy itp.). Pod względem technologicznym przystawka Magazyn wymienny stanowi rozwiązanie podrzędne w stosunku do technologii *Hierarchical Storage Management* (HSM). Te nowe technologie zapewniają metody zautomatyzowanego archiwizowania danych i ich pobierania.

Węzeł *Magazyn wymienny* umożliwia tworzenie pul nośników i zarządzanie nimi, umieszczanie nośnika w napędzie i wyjmowanie go, podłączanie i odłączanie nośnika, sprawdzanie statusu nośnika i magazynu, inwentaryzowanie magazynów i przypisywanie uprawnień zabezpieczających nośnikom i magazynom.

Telefonia

Węzeł *Telefonia* oferuje scentralizowane narzędzie zarządzające w przypadku wybranego komputera ustawieniami związanymi z telefonią. Ustawienia uwzględniają dostawców telefonii i przypisywanie uprawnień użytkowników różnym dostawcom.

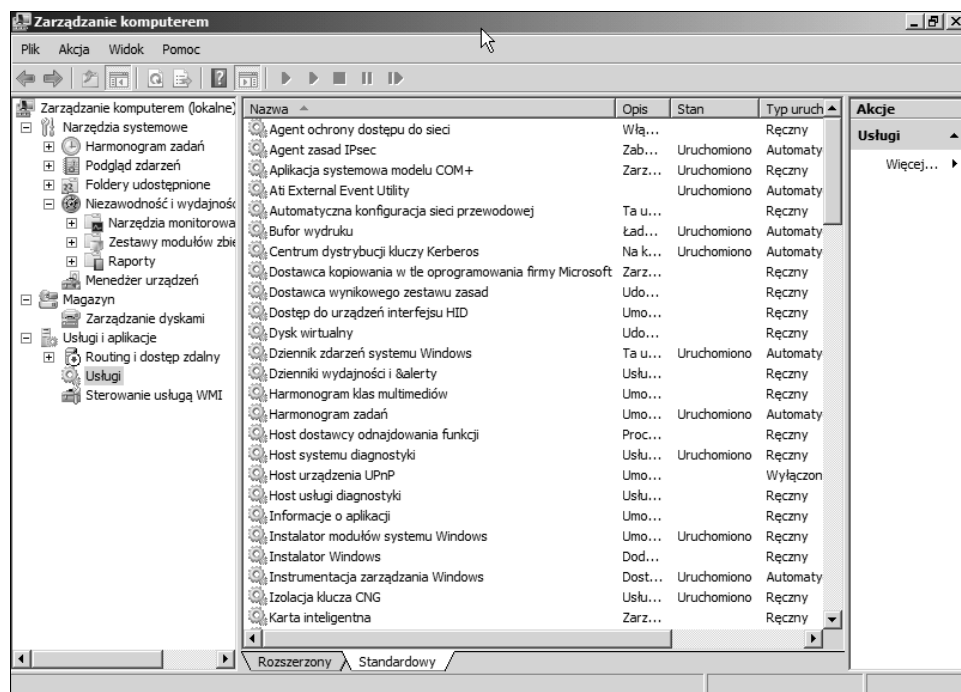
Sterowanie usługą WMI

Węzeł *Sterowanie usługą WMI* przystawki Zarządzanie komputerem zapewnia narzędzia przeznaczone do konfigurowania usługi *Windows Management Instrumentation* (WMI) komputera. W celu udostępnienia metod lokalnego i zdalnego gromadzenia danych o komputerach i ich składników sprzętowych usługa WMI działa w połączeniu z technologią *Web-Based Enterprise Management*. WMI funkcjonuje na poziomie sterowników urządzeń, zapewniając generowane przez nie powiadomienia o zdarzeniach i umożliwiając zbieranie danych na potrzeby analizy i administrowania. Usługa WMI jest kluczowym składnikiem w procesie zarządzania przedsiębiorstwem. Węzeł *Sterowanie usługą WMI* dostarcza środków pozwalających skonfigurować ogólne ustawienia, rejestrowanie, archiwizowanie i odtwarzanie repozytorium usługi WMI, a także zabezpieczenia kontrolujące dostęp do usługi WMI.

Usługi

W systemie operacyjnym Windows Server 2008 usługi są aplikacjami realizującymi określone funkcje, takie między innymi jak obsługa sieci, logowanie, kolejkovanie wydruków i zdalny dostęp. Usługi można traktować jak aplikacje dedykowane systemowi operacyjnemu, które działają samodzielnie lub w połączeniu z innymi usługami bądź aplikacjami użytkownika w celu zrealizowania określonych zadań lub zapewnienia w obrębie systemu specyficznych funkcji. Przykładowo sterowniki urządzeń funkcjonują jako usługi. Domyślnie system Windows Server 2008 zawiera kilka standardowych usług. Wiele zewnętrznych aplikacji pełni rolę usług lub dysponuje własnymi usługami. Dobrym przykładem możliwej zewnętrznej usługi jest działający w tle program skanujący wiadomości pod kątem wirusów.

W systemie Windows Server 2008 węzeł *Usługi* (rysunek 2.14) przystawki Zarządzanie komputerem (jak również samodzielnie jako konsola *Services.msc*) umożliwia zarządzanie usługami. Narzędzie *Usługi* wyświetla listę zainstalowanych usług docelowego komputera. Po uaktywnieniu widoku szczegółów zostanie udostępniony opis, status, typ uruchomienia i konto używane przez usługę do zalogowania się.



Rysunek 2.14. Węzeł *Usługi* umożliwia konfigurowanie, ładowanie, zatrzymywanie i wstrzymywanie usług, a także sprawdzanie zależności usług

Uruchamianie i zatrzymywanie usług

Aktywna usługa przetwarza zapytania i generalnie realizuje zadanie, do którego jest przeznaczona. Zatrzymanie usługi powoduje zakończenie przez nią pracy i usunięcie jej z pamięci. Proces ładowania usługi inicjalizuje ją i uaktywnia tak, żeby mogła wykonać powierzone zadanie lub funkcję. Przykładowo klient DNS działa jako translator DNS, który przetwarza zapytania dotyczące mapowania nazw na adresy obszaru nazw DNS. Jeżeli zatrzyma się usługę klienta DNS, klient nie będzie już obsługiwał zapytań DNS.

Windows Server 2008 obsługuje następujące trzy typy uruchamiania usług:

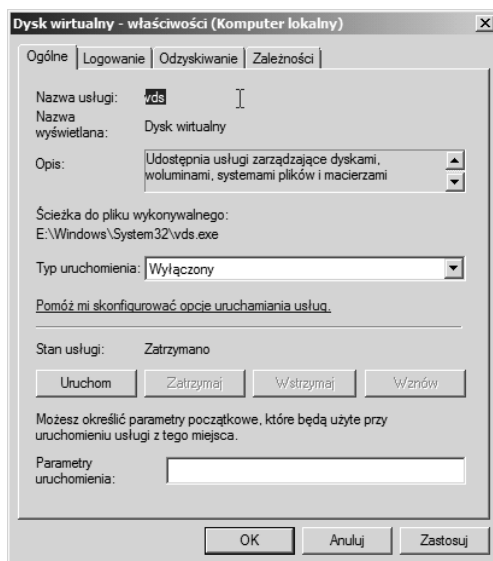
- ♦ **Automatyczny.** Usługa jest ładowana automatycznie podczas uruchamiania systemu.
- ♦ **Ręczny.** Usługa może być uruchomiona przez użytkownika lub zależną usługę. Usługa nie zostanie uaktywniona automatycznie w czasie ładowania systemu, jeśli zależnej usługi nie skonfiguruje się pod kątem samoczynnego uruchamiania (powodującego załadowanie usługi).

- ♦ **Wyłączony.** Usługa nie może zostać uruchomiona przez system, użytkownika lub zalezną usługę.

Typ uruchamiania usługi określa się w obrębie karty *Ogólne* okna właściwości usługi. Kliknij węzeł *Usługi* przystawki Zarządzanie komputerem (lub załaduj plik konsoli *Services.msc* znajdujący się w katalogu `%systemroot%\System32`), a następnie dwukrotnie kliknij usługę. Rysunek 2.15 pokazuje kartę *Ogólne* okna właściwości typowej usługi. Z listy rozwijanej *Typ uruchomienia* wybierz żądany typ uruchomienia i kliknij przycisk *OK* lub *Zastosuj*.

Rysunek 2.15.

Karta *Ogólne*
umożliwia
skonfigurowanie typu
uruchamiania usługi,
kontrolowanie jej
(ładowanie
i zatrzymywanie)
i określenie ogólnych
właściwości



Karta *Ogólne* pozwala również uruchomić, zatrzymać, wstrzymać lub wznowić działanie usługi. Ładowanie i zatrzymywanie omówiono wcześniej. Wstrzymanie usługi powoduje zawieszenie jej działania, lecz nie usuwa usługi z pamięci. Aby wstrzymana usługa kontynuowała pracę, trzeba ją wznowić. Uaktywnij kartę *Ogólne* okna właściwości usługi, po czym stosownie do potrzeb kliknij przycisk *Uruchom*, *Zatrzymaj*, *Wstrzymaj* lub *Wznów*.

Możliwe jest też uruchomienie i zatrzymanie usług z poziomu wiersza poleceń konsoli. Umożliwiają to polecenia `NET START` i `NET STOP` zawierające nazwę usługi, którą można znaleźć wewnątrz karty *Ogólne*, w polu *Nazwa usługi*. Użyj na przykład polecenia `NET START ALERTER`, żeby uaktywnić usługę Urządzenie alarmowe. Polecenie `NET STOP ALERTER` zatrzyma tę usługę.



Polecenia `NET START` i `NET STOP` bardzo przydają się do zdalnego kontrolowania usług. Jeśli w obrębie zdalnego komputera działa usługa Telnet, można nawiązać z nim połączenie, a następnie użyć poleceń `NET START` i `NET STOP` w celu załadowania i zatrzymania usług zdalnego komputera.

Określanie ogólnych właściwości usługi

Inne ustawienia zawarte w obrębie karty *Ogólne* okna właściwości usługi decydują o tym, w jaki sposób usługa będzie prezentowana w panelu szczegółów i jak będzie uruchamiana. Za pomocą pola *Nazwa wyświetlana* można określić nazwę usługi, która pojawi się w panelu

szczegółów poniżej etykiety kolumny *Nazwa*. W polu *Opis* wstaw opis usługi. Pole *Parametry uruchomienia* pozwala wprowadzić opcjonalne przełączniki lub parametry decydujące o sposobie załadowania usługi. Parametry te są takie same jak używane wierszu polecenia konsoli.

Konfigurowanie ustawień logowania usługi

Karta *Logowanie* okna właściwości usługi pozwala określić sposób logowania usługi i profile sprzętowe, w których usługa będzie używana. Choć większość usług loguje się za pomocą konta System, w niektórych sytuacjach na potrzeby usługi konieczne będzie zastosowanie innego konta. Określonego typu usługi administracyjne często korzystają z własnych kont, ponieważ wymagają uprawnień administracyjnych. A zatem trzeba utworzyć konto specjalnie dla usługi i dodać je do grupy Administratorzy lub zależnie od konkretnych wymagań usługi przypisać jej odpowiednie uprawnienia.



Trzeba unikać stosowania konta Administrator. Gdy zmieni się hasło dla tego konta (powinno się to robić często, jeśli korzysta się z konta), konieczne będzie również ponowne skonfigurowanie hasła w oknie właściwości każdej usługi, która używa konta Administrator. Zastosowanie dla takich usług specjalnego konta pozwala na zmianę hasła konta Administrator bez wpływu operacji na usługi. W rozdziale 16. wyjaśniono, jak chronić konto Administrator i zrezygnować z wykorzystywania go.

Karta właściwości *Logowanie* zawiera następujące kontrolki:

- ♦ **Lokalne konto systemowe.** Uaktywnij opcję, żeby usługa logowała się z użyciem lokalnego konta systemowego.
- ♦ **Zezwalaj usłudze na współdziałanie z pulpitem.** Zaznacz opcję, żeby umożliwić usłudze zapewnienie interfejsu użytkownika aktualnie zalogowanej osobie, aby mogła prowadzić z usługą interakcję. Ustawienie to nie ma żadnego wpływu, jeśli usługa nie jest w stanie udostępnić interfejsu użytkownika.
- ♦ **To konto.** Uaktywnij opcję i określ nazwę konta w polu tekstowym (lub przeszukaj listę kont), żeby usługa logowała się za pomocą konta innego niż lokalne konto systemowe.
- ♦ **Hasło, Potwierdź hasło.** Wprowadź hasło dwukrotnie dla konta określonego dla usługi.
- ♦ **Włącz, Wyłącz.** Z listy profili sprzętowych wybierz profil i kliknij przycisk *Włącz*, żeby dla profilu uaktywnić usługę. Kliknięcie przycisku *Wyłącz* spowoduje wyłączenie usługi dla profilu.

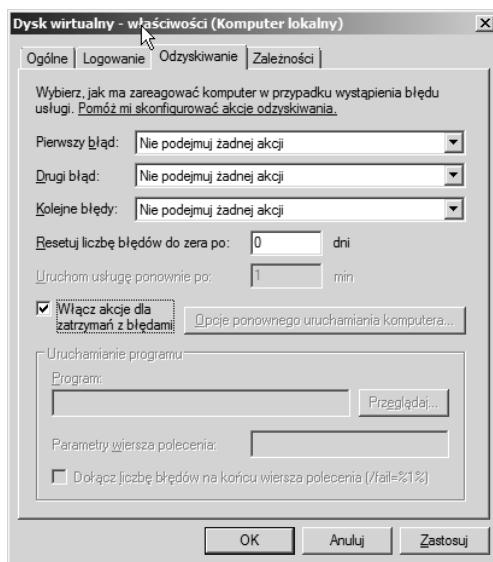
Konfigurowanie odzyskiwania usługi

Kolejną rzeczą, którą można skonfigurować w przypadku usług, jest działanie podejmowane, gdy usługa ulegnie awarii. Można tak skonfigurować usługę, żeby w przypadku awarii została ponownie uruchomiona, został załadowany plik lub zrestartowany komputer. Ponadto można użyć licznika błędów w celu rejestrowania liczby awarii usługi. Opcje odzyskiwania usługi ustawia się za pomocą karty *Odzyskiwanie* (rysunek 2.16).

Karta *Odzyskiwanie* zawiera następujące ustawienia:

Rysunek 2.16.

Konfigurowanie opcji odzyskiwania usługi w celu określenia operacji, jakie powinny zostać zrealizowane przez usługę, gdy ulegnie awarii



- ♦ **Pierwszy błąd, Drugi błąd, Kolejne błędy.** Te trzy listy rozwijane pozwalają wybrać czynność (lub zrezygnować z niej), która zostanie podjęta w przypadku konkretnej awarii. Można zdecydować się na niepodjęcie żadnych działań, zrestartować usługę, uruchomić plik lub ponownie uruchomić komputer.
- ♦ **Resetuj liczbę błędów do zera po.** W polu podaj liczbę dni, po upływie których licznik błędów zostanie wyzerowany.
- ♦ **Uruchom usługę ponownie po.** W polu określ liczbę minut, które upłyną między awarią i zrestartowaniem usługi. Wydłuż okres z domyślnej jednej minuty, jeśli system potrzebuje więcej czasu na stabilizację po wystąpieniu awarii usługi.
- ♦ **Uruchamianie programu.** Ta grupa ustawień pozwala zidentyfikować program lub skrypt, który zostanie wywołany po wystąpieniu awarii usługi. Można na przykład utworzyć skrypt, który do członków grupy Administratorzy wyśle komunikat z wartością licznika błędów i innymi informacjami. Użyj opcji *Dołącz liczbę błędów na końcu wiersza polecenia* w celu wstawienia bieżącej wartości licznika błędów na końcu wiersza polecenia (przekazanie poleceniu wartości licznika błędów na potrzeby wewnętrznego przetwarzania).
- ♦ **Opcje ponownego uruchamiania komputera.** Kliknij ten przycisk, żeby ustalić liczbę minut oczekiwania przed zrestartowaniem komputera i wprowadzić opcjonalny komunikat (na przykład ostrzeżenie o ponownym uruchomieniu), który za pośrednictwem sieci zostanie wysłany do użytkowników przed wykonaniem tej operacji.

Przeglądanie zależności

Za pomocą karty *Zależności* można zapoznać się z innymi usługami, od których zależy wybrana usługa, a także przejrzeć usługi od niej zależne. Ta karta właściwości wyświetla tylko informacje i nie pozwala skonfigurować lub zmodyfikować zależności. Zawartość karty nie wymaga objaśnienia.

Usługa indeksowania

W celu zachowania zgodności wstecz usługa indeksowania w dalszym ciągu jest dostępna w systemie Windows Server 2008. Usługa używa filtrów dokumentów do odczytywania i tworzenia wykazu dokumentów przechowywanych w obrębie komputera. Poza tym usługa zapewnia szybkie wyszukiwanie tekstowe dokumentów wykazu, które spełniają kryteria. Jeśli rozpoczyna się wyszukiwanie i po raz pierwszy indeksuje się dane w systemie Windows Server 2008, powinno się raczej skorzystać z nowej usługi Usługa wyszukiwania systemu Windows. Usługę tę omówiono w rozdziale 15. Nie można jednocześnie zainstalować zarówno usługi indeksowania, jak i nowej usługi Usługa wyszukiwania systemu Windows (w ramach roli *Usługi plików*). Podczas dodawania roli *Usługi plików* można wybrać tylko jedną z tych usług.

Filtr dokumentu wyodrębnia z dokumentu informacje i przekazuje je usłudze indeksowania w celu dołączenia ich do wykazu. Operację wyszukiwania można przeprowadzić przy użyciu pola wyszukiwania menu *Start*, węzła przeszukiwania katalogu, znajdującego się poniżej węzła *Usługa indeksowania* przystawki Zarządzanie komputerem, lub strony WWW. Wyszukiwać można z wykorzystaniem różnych kryteriów, takich jak nazwa dokumentu, autor i treść. Można na przykład za pomocą usługi indeksowania zbudować wykaz wewnętrznych dokumentów lub skatalogować zawartość witryny WWW organizacji. Usługa indeksowania poindeksuje następujące typy dokumentów:

- ♦ pliki HTML,
- ♦ pliki tekstowe,
- ♦ dokumenty pakietu Microsoft Office,
- ♦ internetowe wiadomości pocztowe i artykuły grup dyskusyjnych,
- ♦ inne dokumenty obsługiwane przez odpowiedni filtr (na przykład filtr zewnętrzny).



Usługa indeksowania przydaje się nawet w przypadku stacji roboczej, gdy trzeba poindeksować dokumenty użytkowników i przyspieszyć wyszukiwanie określonych dokumentów lub ich grup.

Za pomocą węzła *Usługa indeksowania* przystawki Zarządzanie komputerem można skonfigurować usługę indeksowania i przeszukać indeks pod kątem listy dokumentów spełniających kryteria zapytania. Węzeł ten pojawia się w oknie konsoli Zarządzanie komputerem nawet wtedy, gdy nie zainstalowano jeszcze usługi indeksowania. Aby ją zainstalować, otwórz okno panelu sterowania i dwukrotnie kliknij ikonę *Dodaj lub usuń programy*. Na pasku narzędzi położonym po lewej stronie kliknij ikonę *Dodaj/Usuń składniki systemu Windows*, z listy *Składniki* wybierz pozycję *Usługa indeksowania*, a następnie kliknij przycisk *Dalej* i postępuj zgodnie z instrukcjami procesu instalowania usługi.

Planowanie użycia usługi indeksowania

Przygotowując się do zastosowania usługi indeksowania, trzeba uświadomić sobie, że wydajność usługi jest zależna od konfiguracji systemu. Usługa indeksowania ma takie same minimalne wymagania sprzętowe co system Windows Server 2008. Jednak zwiększająca się liczba indeksowanych dokumentów spowoduje wzrost wymagań dotyczących pamięci. Dokładne zalecenia można znaleźć w pliku pomocy usługi indeksowania (wcisnij klawisz *F1* po zaznaczeniu węzła *Usługa indeksowania* w oknie przystawki Zarządzanie komputerem).

Ponadto trzeba zaplanować system plików, który będzie dostosowany do usługi indeksowania. Umieszczenie wykazu w obrębie woluminu FAT umożliwi użytkownikom uzyskanie do niego dostępu nawet wtedy, gdy nie będą dysponowali żadnymi uprawnieniami pozwalającymi przeglądać wybrane dokumenty wykazu. Zlokalizowanie wykazu wewnątrz woluminu NTFS oferuje najlepsze zabezpieczenia, ponieważ usługa indeksowania utrzymuje wszystkie listy kontroli dostępu ACL (*Access Control List*). Użytkownicy nie zobaczą na liście zwróconej dla zapytania żadnych dokumentów, jeśli nie będą mieć uprawnień niezbędnych do przeglądania dokumentów. Ponadto do logowania usługa indeksowania używa konta System. Jeżeli temu kontu zablokuje się dostęp do określonego katalogu lub pliku, usługa indeksowania nie będzie w stanie ich użyć i poddać indeksowaniu. Zaszzyfrowane dokumenty nigdy nie są indeksowane.

Istotne jest również miejsce przechowywania wykazu lub wykazów indeksu. Nie powinno się ich umieszczać w obrębie witryny WWW (w jej katalogu), gdyż serwer IIS (*Internet Information Services*) może zablokować wykaz i uniemożliwić aktualizowanie go. Poza tym trzeba unikać uruchamiania oprogramowania antywirusowego lub archiwizującego, które blokuje pliki wykazu. Coś takiego mogłoby spowodować przekroczenie przez usługę indeksowania czasu oczekiwania przy podejmowaniu próby zaktualizowania wykazów. Najlepszym rozwiązaniem jest utworzenie katalogu wewnątrz woluminu NTFS dedykowanego dla plików wykazu i zapisywanie każdego wykazu w jego własnym podkatalogu tego głównego katalogu.



Możliwa jest zmiana lokalizacji domyślnego wykazu. System tworzonego automatycznie podczas instalowania usługi indeksowania. Najpierw trzeba utworzyć katalog, który będzie przechowywał dane wykazu. W dalszej kolejności prawym przyciskiem myszy kliknij węzeł *Usługa indeksowania* i z menu wybierz polecenie *Zatrzymaj*, żeby wyłączyć usługę. Uruchom narzędzie *Edytor rejestru* i zmodyfikuj wartość `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ContentIndex\Catalogs\System\Location` tak, żeby wskazywała na żądane położenie. Zamknij edytor rejestru i zrestartuj usługę indeksowania.

Tworzenie i konfigurowanie wykazu

Możliwe jest utworzenie wielu dostosowanych do potrzeb wykazów indeksu. W celu wygenerowania nowego wykazu uruchom przystawkę Zarządzanie komputerem i prawym przyciskiem myszy kliknij węzeł *Usługa indeksowania*. Z menu *Nowy* wybierz pozycję *Wykaz*. Określ nazwę wykazu i jego położenie, a następnie kliknij przycisk *OK*. Wykaz pozostanie w trybie offline do momentu ponownego załadowania usługi indeksowania.

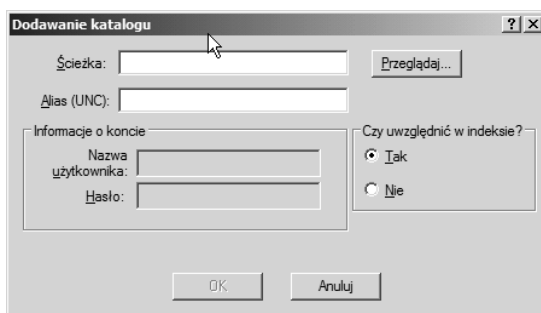
W obrębie węzła *Usługa indeksowania* przystawki Zarządzanie komputerem rozwiń nowo utworzony wykaz. Prawym przyciskiem myszy kliknij węzeł *Katalogi* znajdujący się poniżej węzła wykazu i z menu *Nowy* wybierz pozycję *Katalog*. Spowoduje to wyświetlenie okna dialogowego *Dodawanie katalogu* (rysunek 2.17). Określ opcje, korzystając z następującej listy:

- ♦ **Ścieżka.** Pole umożliwia określenie ścieżki katalogu, który zostanie dodany do wykazu. W celu odszukania katalogu można też kliknąć przycisk *Przeglądaj*.
- ♦ **Alias (UNC).** Jeśli identyfikujesz katalog zdalnego komputera, w polu wprowadź ścieżkę UNC w formacie `\\komputer\udział`, gdzie łańcuch *komputer* określa nazwę zdalnego komputera, a łańcuch *udział* reprezentuje udział, w którym zlokalizowano katalog.

- ♦ **Informacje o koncie.** W przypadku katalogu zdalnego komputera określ nazwę konta i hasło udzielające dostępu do komputera.
- ♦ **Czy uwzględnić w indeksie?** Kliknij opcję *Tak*, żeby dołączyć katalog, lub opcję *Nie* w celu wykluczenia go z wykazu. Opcja *Nie* umożliwia wyłączenie podkatalogu katalogu wchodzącego w skład wykazu. Dodaj nadrzędny katalog i ustaw dla niego opcję *Tak*, a następnie oddzielnie dołącz podkatalog i uaktywnij opcję *Nie*, żeby go wykluczyć.

Rysunek 2.17.

Okno umożliwia dodanie katalogów do wykazu w celu uwzględnienia ich zawartości w indeksie



Po wybraniu katalogów do wykazu zatrzymaj i ponownie załaduj usługę indeksowania, żeby uaktualnić wykaz. Węzeł *Właściwości* będzie pusty do momentu zatrzymania i zrestartowania usługi.

Wysyłanie zapytania do wykazu

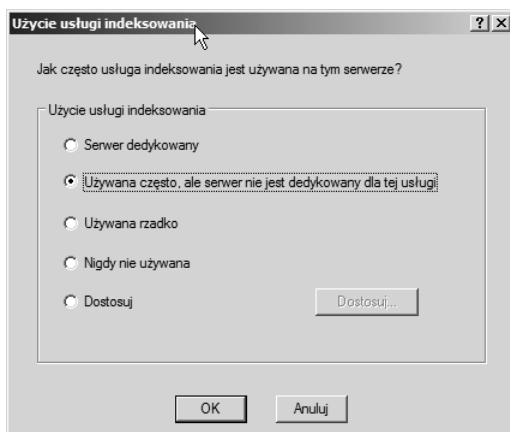
Jak wcześniej wspomniano, zapytanie do wykazu można wysłać za pośrednictwem pola szukania menu *Start*, strony WWW lub przystawki *Zarządzanie komputerem*. W celu wykonania zapytania za pomocą przystawki rozwiń węzeł *Usługa indeksowania* i kliknij pozycję przeszukiwania wykazu, znajdującą się poniżej żadanego wpisu wykazu. Windows Server 2008 zapewnia formularz zapytania, w którym można określić kryteria kwerendy i opcje, a także sprawdzić wyniki zapytania.

Dostrajanie wydajności

W przypadku komputera z dużą liczbą dokumentów w celu uzyskania najlepszej wydajności można się zdecydować na dostrojenie usługi indeksowanej. Prawym przyciskiem myszy kliknij węzeł *Usługa indeksowania* przystawki *Zarządzanie komputerem*, z menu wybierz polecenie *Zatrzymaj*, które spowoduje wyłączenie usługi. Ponownie prawym przyciskiem myszy kliknij węzeł *Usługa indeksowania* i w celu otwarcia okna dialogowego *Użycie usługi indeksowania* (rysunek 2.18) wybierz polecenie *Dostrajanie wydajności*. Opcje zawarte w tym oknie pozwalają określić, jak często usługa indeksowania ma być używana. System Windows Server 2008 automatycznie skonfiguruje usługę na podstawie ustawionych opcji. Uaktywnij opcję *Dostosuj*, a następnie kliknij przycisk *Dostosuj*, żeby dla operacji indeksowania i przetwarzania zapytań skonfigurować niestandardowe ustawienia. W przypadku indeksowania kontrolkę suwaka można ustawić między pozycjami *Z opóźnieniem* i *Natychmiastowe*. Pozycja *Z opóźnieniem* powoduje, że indeksowanie jest realizowane bardziej jako zadanie w tle, a pozycja *Natychmiastowe* przydziela operacji zasoby systemowe w maksymalnej ilości (w efekcie zasoby są odbierane innym

Rysunek 2.18.

Użycie okna dialogowego Użycie usługi indeksowania do optymalizacji wydajności usługi indeksowania



wykonywanym zadaniom). W przypadku przetwarzania zapytań kontrolkę suwaka można ustawić między niskim i dużym obciążeniem, zależnie od liczby zapytań, które komputer otrzymuje. Po ukończeniu konfiguracji trzeba pamiętać o zrestartowaniu usługi.

Zastosowanie przystawki Podgląd zdarzeń

Microsoft definiuje zdarzenie systemu Windows Server 2008 jako dowolne istotne wydarzenie w obrębie systemu operacyjnego lub aplikacji, które wymaga powiadomienia użytkowników (w szczególności administratorów). Zdarzenia są rejestrowane w dziennikach zdarzeń. Zdarzenia i dzienniki są ważnymi narzędziami administracyjnymi, ponieważ stają się nieodzowne podczas identyfikowania i rozwiązywania problemów, monitorowania dostępu kontrolowanego przez zabezpieczenia (logowanie, wylogowywanie, inspekcja zasobów itp.), a także śledzenia statusu systemu i jego aplikacji.



Niektóre funkcje są niedostępne, jeśli korzysta się z przystawki Podgląd zdarzeń konsoli Zarządzanie komputerem. W niniejszym punkcie przyjęto, że przystawka Podgląd zdarzeń jest wywoływana bezpośrednio z poziomu katalogu *Narzędzia administracyjne*.

Zdarzenia można zaklasyfikować do następujących ogólnych kategorii:

- ♦ **System.** W tej kategorii znajdują się zdarzenia systemowe związane z uruchamianiem i zatrzymywaniem usług, inicjalizowaniem sterowników i komunikatami ostrzegawczymi, a także zdarzenia sieciowe i inne dotyczące ogólnie systemu.
- ♦ **Zabezpieczenia.** Do tej kategorii zaliczają się zdarzenia powiązane z zabezpieczeniami, takie jak zdarzenia operacji logowania, wylogowywania i uzyskiwania dostępu do zasobów (inspekcja).
- ♦ **Aplikacja.** Zdarzenia tej kategorii są powiązane z konkretnymi aplikacjami. Przykładowo program skanujący wiadomości pod kątem wirusów może rejestrować w dzienniku *Aplikacja* zdarzenia dotyczące skanowania wirusów, operacji usuwania ich itp.
- ♦ **Ustawienia.** Zdarzenia tej kategorii mają związek z procesami konfiguracyjnymi, takimi jak dodawanie ról i funkcji.

- ♦ **Zdarzenia przekazane.** W tym dzienniku znajdują się wpisy pochodzące z systemu innego komputera. W przypadku tego dziennika tworzy się subskrypcję do dziennika zdarzeń innego komputera, a następnie filtruje ten dziennik w celu pobrania wyłącznie żądanych zdarzeń. Uzyskane zdarzenia są umieszczane w dzienniku *Zdarzenia przekazane*.



Oprócz trzech domyślnych dzienników zdarzeń inne usługi systemu Windows Server 2008 tworzą własne dzienniki. Usługi katalogowa, usługa DNS i usługa replikacji plików to kilka przykładowych usług, które tworzą własne dzienniki zdarzeń. Dzienniki te przegląda się za pomocą narzędzia *Podgląd zdarzeń*, tak jak trzy standardowe dzienniki.

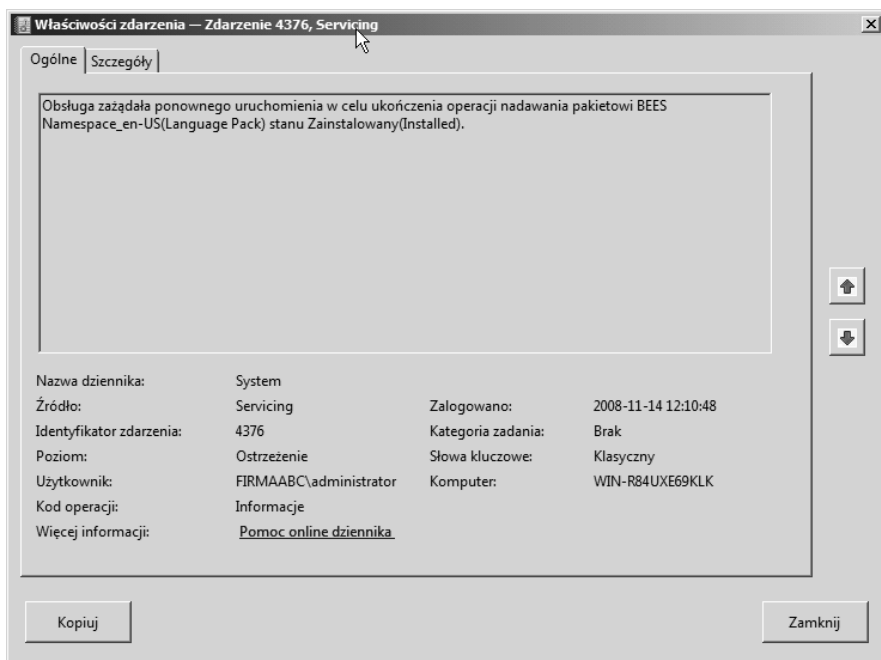
Istnieją zdarzenia będące tylko komunikatami informacyjnymi, jak również istotne zdarzenia dotyczące na przykład awarii usługi lub aplikacji. Do podstawowych kategorii zdarzeń zalicza się informacyjne i ostrzegawcze, a także związane z błędami, udaną inspekcją i nieudaną inspekcją. Ważność zdarzenia dziennika identyfikuje widoczna obok niego ikona. Przykładowo zdarzenia ostrzegawcze używają ikony z wykrzyknikiem, a zdarzenia błędów ikony ze znakiem X umieszczonym wewnątrz czerwonego okręgu. Z każdym zdarzeniem są powiązane następujące wspólne właściwości:

- ♦ **Data i godzina.** Data i godzina wystąpienia zdarzenia.
- ♦ **Źródło.** Identyfikuje źródło zdarzenia, takie jak usługa, sterownik urządzenia, aplikacja, zasób itp. Właściwość ta przydaje się w przypadku określania przyczyny wystąpienia zdarzenia (przyczyna i źródło zdarzenia nie są synonimami).
- ♦ **Kategoria.** Źródło określa kategorię zdarzenia. Przykładowo z kategorią zabezpieczeń są związane między innymi takie operacje jak logowanie, wylogowywanie, zmiana zasady i dostęp do obiektów.
- ♦ **Zdarzenie.** Każde zdarzenie zawiera identyfikator, czyli liczbę całkowitą generowaną przez źródło w celu jednoznacznej identyfikacji zdarzenia.
- ♦ **Użytkownik.** Właściwość identyfikuje użytkownika, który spowodował wygenerowanie zdarzenia (jeśli dotyczy).
- ♦ **Komputer.** Właściwość identyfikuje komputer, który spowodował wygenerowanie zdarzenia (jeśli dotyczy).

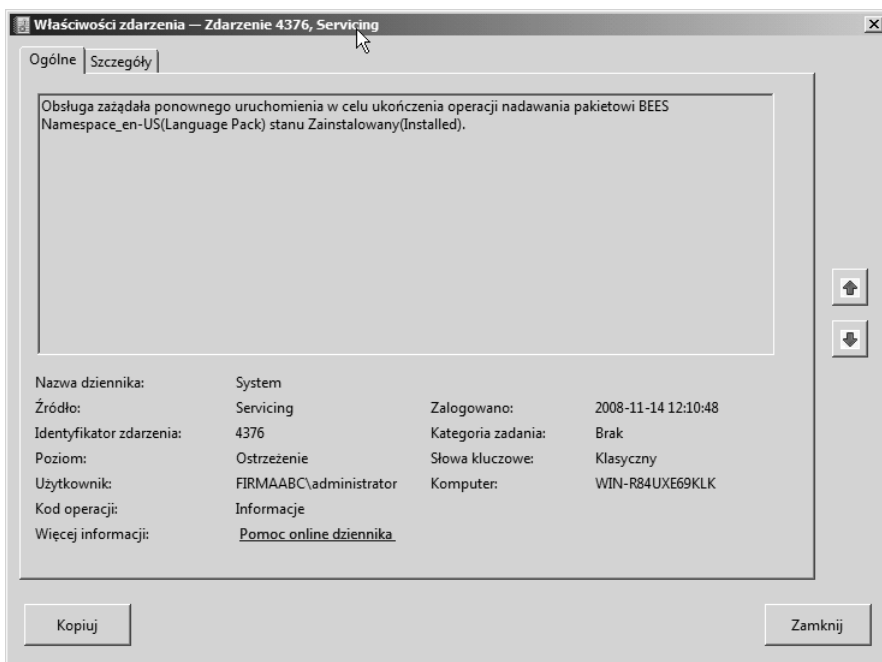
Przystawka Podgląd zdarzeń konsoli MMC jest narzędziem służącym do przeglądania dzienników zdarzeń i zarządzania nimi. Przystawka prezentuje dzienniki w panelu drzewa w postaci oddzielnych gałęzi. Po kliknięciu dziennika jego zdarzenia pojawiają się w panelu po prawej stronie (rysunek 2.19).

Przeglądanie i filtrowanie zdarzeń

Przeglądanie zdarzenia jest prostą operacją. Wystarczy uruchomić przystawkę Podgląd zdarzeń, zlokalizować zdarzenie i kliknąć je dwukrotnie (lub zaznaczyć je i wcisnąć klawisz *Enter*). Narzędzie *Podgląd zdarzeń* otworzy okno dialogowe z właściwościami zdarzenia (rysunek 2.20). Na samej górze okna znajdują się ogólne informacje o zdarzeniu, takie jak godzina i data utworzenia, typ itp. Tekst opisu zapewnia szczegółową prezentację zdarzenia, która zwykle (lecz nie zawsze) ma postać zrozumiałego objaśnienia znaczenia zdarzenia. W dolnej części okna dialogowego pojawiają się dodatkowe dane, jeśli zostały dołączone



Rysunek 2.19. Nowa, znacznie rozbudowana wersja przystawki Podgląd zdarzeń



Rysunek 2.20. Okno właściwości zdarzenia zapewnia szczegółowe informacje o zdarzeniu

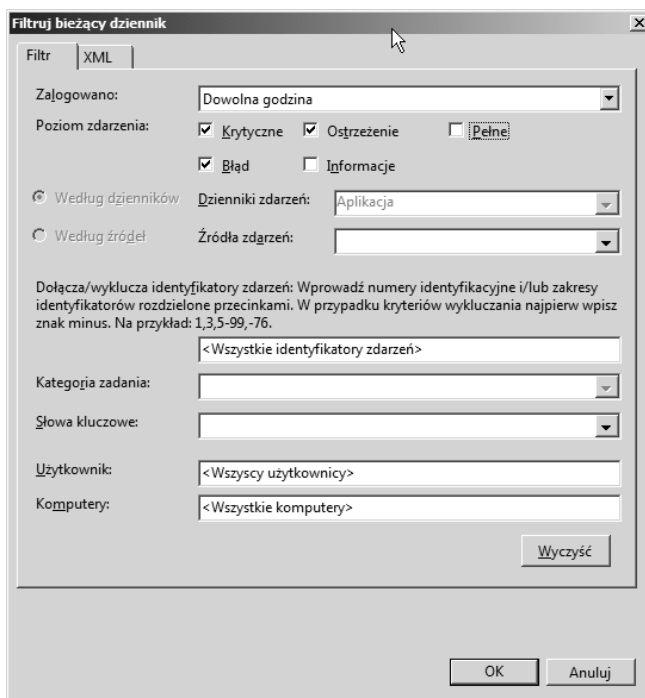
do zdarzenia. Dane można wyświetlić w formacie bajtowym (heksadecymalnym) lub DWORD. W większości przypadków dane takie musi przeglądać inżynier oprogramowania, gdyż do ich interpretacji jest niezbędne zrozumienie kodu generującego dane.

Użyj strzałek skierowanych w górę i w dół, zlokalizowanych z prawej strony okna dialogowego, żeby przejrzeć odpowiednio poprzednie i następne zdarzenia. Kliknij przycisk *Kopiuj* w celu skopiowania do schowka zaznaczonego zdarzenia.

Domyślnie przystawka Podgląd zdarzeń udostępnia wszystkie zdarzenia wybranego dziennika. W wielu sytuacjach pomocna będzie możliwość przefiltrowania widoku tak, żeby przystawka pokazała tylko zdarzenia spełniające określone kryteria. Aby zastosować filtr, kliknij dziennik i z menu *Akcja* wybierz pozycję *Filtruj bieżący dziennik*. W efekcie zostanie otwarta karta *Filtr* okna właściwości dziennika (rysunek 2.21).

Rysunek 2.21.

Karta *Filtr* pozwala określić, jakie zdarzenia zostaną wyświetlone w oknie przystawki Podgląd zdarzeń dla wybranego dziennika



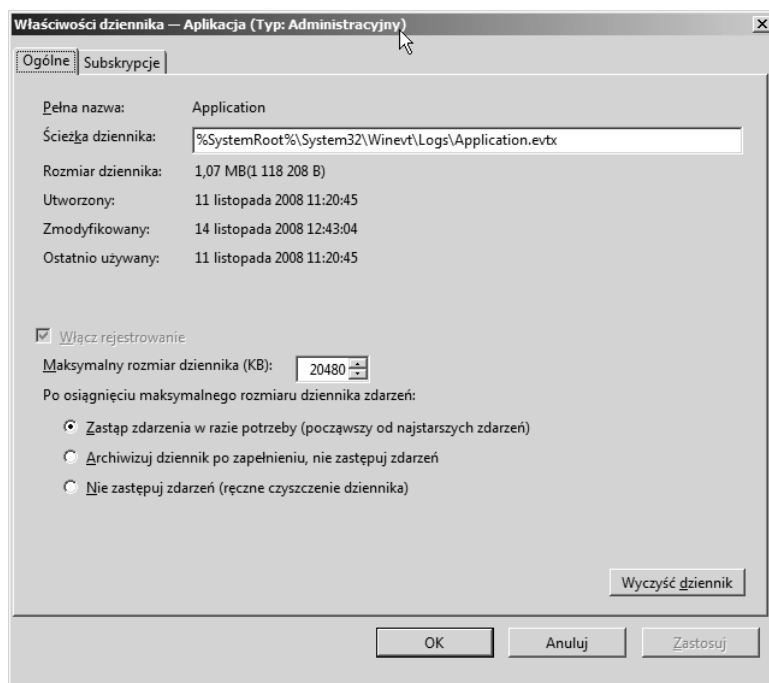
Zdarzenia można przeglądać według ich typu, źródła, kategorii, identyfikatora, użytkownika, komputera lub zakresu dat. Dla przykładu możliwe jest filtrowanie zdarzeń przy użyciu źródła, jeśli próbuje się rozwiązać problem związany z konkretną aplikacją, usługą lub sterownikiem. W celu utworzenia filtra w oknie dialogowym określ kryteria i kliknij przycisk *OK*. Z menu *Akcje* wybierz pozycję *Wyczyść filtr*, żeby usunąć filtr i przejrzeć wszystkie zdarzenia dziennika.

Ustawianie właściwości dziennika

Każdy dziennik dysponuje ogólnymi właściwościami, które między innymi decydują o tym, jak zostanie zaprezentowany w oknie przystawki Podgląd zdarzeń, a ponadto ustawiają rozmiar dziennika i pozwalają określić, co się stanie po osiągnięciu maksymalnego rozmiaru.

Zaznacz dziennik i kliknij go prawym przyciskiem myszy, żeby z menu wybrać pozycję *Właściwości* w celu wyświetlenia karty właściwości *Ogólne* (rysunek 2.22).

Rysunek 2.22.
Konfigurowanie
wewnątrz karty
właściwości *Ogólne*
wyglądu dziennika
i jego rozmiaru



Część informacji prezentowanych w obrębie karty *Ogólne* jest tylko do odczytu (na przykład położenie pliku dziennika). Można zmodyfikować właściwość *Pełna nazwa*, żeby zmienić nazwę dziennika, która pojawi się w panelu drzewa przystawki Podgląd zdarzeń.

Grupa kontrolki związanych z rozmiarem dziennika określa jego maksymalną wielkość i operację, jaka zostanie wykonana przez system Windows Server 2008, gdy dziennik osiągnie maksymalny rozmiar. Opcje te w zasadzie nie wymagają objaśnienia. Jednak trzeba mieć świadomość tego, że jeśli uaktywni się opcję *Nie zastępuj zdarzeń (ręczne czyszczenie dziennika)*, w momencie zapelnienia dziennika system Windows Server 2008 przestanie rejestrować w nim zdarzenia. Choć Windows Server 2008 powiadomi o zapelnieniu dziennika, trzeba będzie monitorować dziennik zdarzeń i okresowo czyścić jego zawartość w celu zapewnienia, że nie utraci się zdarzeń.



Zastosowanie wolnego połączenia uniemożliwi przystawce Podgląd zdarzeń pobranie wszystkich danych zdarzeń przed faktycznym zażądaniem ich. Jest to przydatne rozwiązanie, gdy dzienniki są zlokalizowane w obrębie innego komputera, który jest dostępny za pośrednictwem łącza sieciowego o niewielkiej szybkości (na przykład łącza telefonicznego).

Zapisywanie i czyszczenie dzienników

Sporadycznie pojawi się konieczność zapisania dziennika zdarzeń i (lub) wyczyszczenia jego zawartości. Operacja zapisu dziennika polega na skopiowaniu go do innego pliku zdarzeń o określonej nazwie. Czyszczenie zawartości dziennika powoduje usunięcie z niego

wszystkich zdarzeń. Można na przykład przed rozpoczęciem diagnozowania problemu zamierzać utworzyć test wydajności lub okresowo archiwizować dzienniki zdarzeń. W każdym przypadku zapisuje się dziennik, a następnie czyści go.

Aby zapisać dziennik, zaznacz go i z menu *Akcja* wybierz polecenie *Zapisz plik dziennika jako*. Alternatywnie kliknij dziennik prawym przyciskiem myszy i z menu wybierz pozycję *Zapisz plik dziennika jako*. Określ nazwę i położenie pliku dziennika, po czym kliknij przycisk *OK*. Po zapisaniu pliku dziennika można go otworzyć ponownie za pomocą przystawki *Podgląd zdarzeń*, żeby przejrzeć zawartość. Trzeba pamiętać o tym, że zapisany dziennik jest statyczny i nie trafiają do niego dodatkowe zdarzenia.

Gdy nadejdzie pora wyczyścić dziennik, uaktywnij kartę jego właściwości *Ogólne* i kliknij przycisk *Wyczyść dziennik*. Windows Server 2008 zażąda zatwierdzenia operacji.

Przeglądanie dzienników innego komputera

Za pomocą przystawki *Podgląd zdarzeń* można przeglądać plik dziennika innych komputerów zlokalizowanych w sieci (również za pośrednictwem internetu lub połączenia VPN). Aby wyświetlić dzienniki zdarzeń innego komputera, uruchom narzędzie *Podgląd zdarzeń*, a następnie prawym przyciskiem myszy kliknij węzeł *Podgląd zdarzeń* i z menu wybierz polecenie *Podłącz do innego komputera*. Określ nazwę komputera lub poszukaj go w sieci i kliknij przycisk *OK*. Uaktywnij opcję *Lokalny komputer*, żeby ponownie nawiązać połączenie z dziennikami zdarzeń lokalnego komputera.

Dostosowywanie widoku dziennika

Można dostosować panel wyników przystawki *Podgląd zdarzeń* przez wybranie kolumn, które będą widoczne i określenie kolejności ich wyświetlania. Jeśli na przykład rzadko przydaje się kolumna *Użytkownik* lub *Komputer*, można z nich zrezygnować.

W celu kontrolowania pokazywania kolumn kliknij dowolny węzeł przystawki *Podgląd zdarzeń* i z menu *Widok* wybierz polecenie *Dodaj/Usuń kolumny*. W efekcie pojawi się okno dialogowe *Dodawanie/usuwanie kolumn*. Stosownie do potrzeb dodaj i usuń kolumny, po czym za pomocą przycisków *Przenieś w górę* i *Przenieś w dół* zmień kolejność wyświetlania. Kliknij przycisk *OK*, żeby zastosować zmiany.



Kolejność wyświetlania kolumn w oknie przystawki *Podgląd zdarzeń* można zmienić przez przeciągnięcie ich.

Rozszerzenia serwerowe

Oprócz przystawek konsoli MMC opisanych wcześniej w rozdziale, Windows Server 2008 uwzględnił kilka innych przystawek służących do zarządzania określonymi usługami. Przykładowo usługi DNS, DHCP i IIS dysponują własnymi przystawkami. Ponieważ zapewniają one podstawową metodę kontrolowania tych usług, najlepiej zaprezentować je przy okazji omawiania usług. Przystawki tych trzech usług opisano w odpowiednich miejscach książki.

Zastosowanie narzędzia Kreator konfiguracji zabezpieczeń

Windows Server 2008 udoskonala narzędzie *Kreator konfiguracji zabezpieczeń* zaprezentowane w systemie Windows Server 2003, żeby ułatwić administratorom dostrajanie zabezpieczeń serwera. Kreator ten konfiguruje ustawienia zabezpieczeń na bazie ról serwerowych. W celu zapewnienia niezbędnego poziomu bezpieczeństwa kreator żąda informacji o serwerze i jego rolach, a następnie zatrzymuje wszystkie usługi niewymagane do pełnienia tych ról, w razie potrzeby blokuje porty, modyfikuje ustawienia rejestru, a także konfiguruje ustawienia serwera IIS i innych składników.



Zamiast omawiania każdego kroku kreatora objaśniono w niniejszym podrozdziale przeznaczenie tego narzędzia i jego ogólne działanie. Po zapoznaniu się z tymi podstawowymi informacjami nie powinno być problemu z korzystaniem z kreatora.

Obecnie narzędzie *Kreator konfiguracji zabezpieczeń* jest instalowane domyślnie. Nie trzeba już go dodawać tak jak w przypadku systemu Windows Server 2003.

Pierwszym krokiem kreatora jest określenie operacji związanej z zasadą, którą zamierza się zrealizować. Oto dostępne opcje:

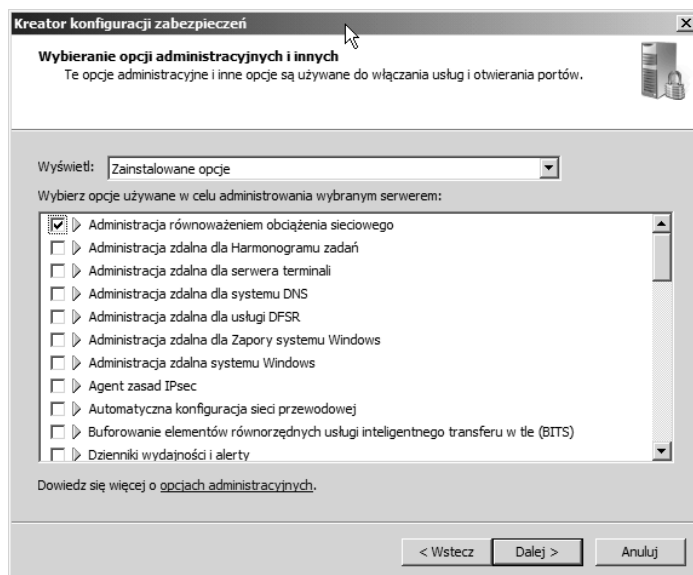
- ♦ **Utwórz nową zasadę zabezpieczeń.** Tworzy nową zasadę na podstawie ról serwera.
- ♦ **Edytuj istniejącą zasadę zabezpieczeń.** Modyfikuje zasadę utworzoną wcześniej dla lokalnego lub zdalnego serwera.
- ♦ **Zastosuj istniejącą zasadę zabezpieczeń.** Powoduje zastosowanie dla serwera wcześniej utworzonej zasady.
- ♦ **Wycofaj ostatnio zastosowaną zasadę zabezpieczeń.** Przywraca serwer do jego poprzedniego stanu sprzed ostatniego użycia zasady zabezpieczeń.

Po wybraniu operacji związanej z zasadą i określeniu serwera, który dla zestawu zasad będzie pełnił rolę punktu wyjściowego (można użyć lokalnego lub zdalnego serwera), narzędzie *Kreator konfiguracji zabezpieczeń* przeprowadza przez kilka następujących kluczowych obszarów:

- ♦ **Wybieranie ról serwerowych.** Na tym etapie pracy kreatora określa się role, które będą pełnione przez docelowy serwer. Jak wcześniej objaśniono w niniejszym podrozdziale, kreator nie dodaje ani też nie usuwa ról serwera.
- ♦ **Określanie roli klienta.** Każdy serwer spełnia kilka ról jako klient, takich między innymi jak automatyczna aktualizacja, klient DNS i członek domeny.
- ♦ **Wybieranie opcji administracyjnych i innych.** Określ opcje, które zostaną uwzględnione przez serwer, takie jak związane z metodami archiwizacji, specyficznymi usługami, opcjonalnymi aplikacjami i specjalnymi zadaniami (rysunek 2.23). Kreator używa wybranych ustawień do określenia, jakie porty powinny zostać otwarte i jakie usługi uaktywnione. Po kliknięciu przycisku *Dalej* kreator wyświetli listę wszystkich dodatkowych zewnętrznych usług, które znalazł na serwerze. Ma to na celu umożliwienie dołączenia lub wykluczenia tych usług z konfiguracji zabezpieczeń.

Rysunek 2.23.

Wybieranie opcji, usług
i zadań wymaganych
dla serwera

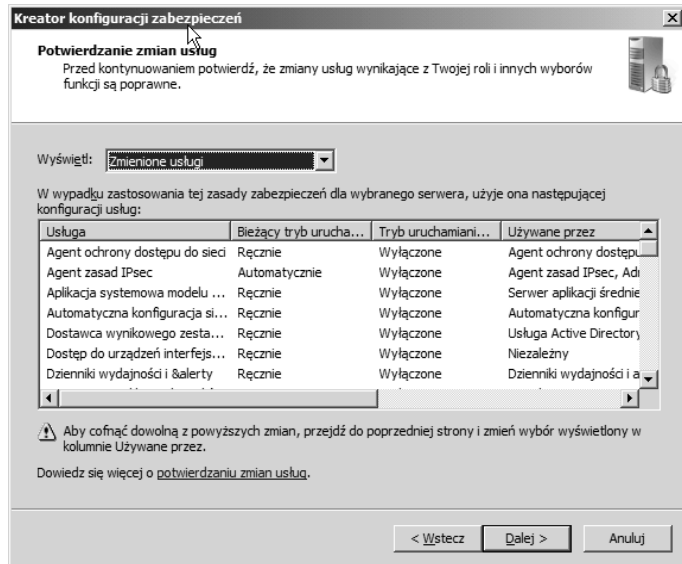


Aby zapoznać się z dodatkowymi informacjami o dowolnej pozycji kreatora, kliknij przycisk strzałki widoczny z lewej strony nazwy pozycji (rysunek 2.23).

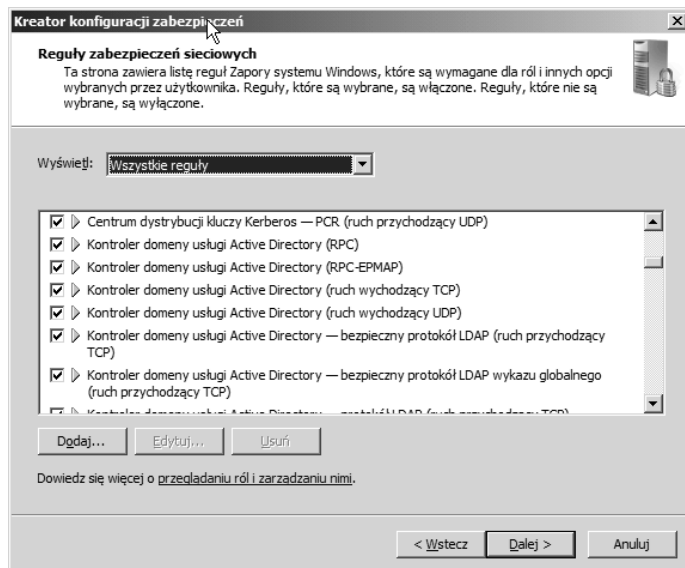
- ♦ **Określanie sposobu obsługi niewyszczególnionych usług.** Zdecyduj, jak będą obsługiwane usługi, których nie wyszczególnia zasada. Można wybrać wariant ustawienia dla usługi typu uruchamiania *Wyłączony* lub nakazać kreatorowi ignorowanie usług (bez modyfikowania typu uruchomienia).
- ♦ **Potwierdzanie modyfikacji usług.** Karta *Potwierdzanie zmian usług* kreatora (rysunek 2.24) po prostu wyświetla zmiany, które zostaną wprowadzone w poszczególnych usługach. Jeśli musisz zmodyfikować czynności, które kreator podejmie dla konkretnej usługi, zwróć uwagę na powiązaną z nią zawartość kolumny *Używane przez*. Kliknij przycisk *Wstecz*, żeby cofnąć się do odpowiedniej karty, w obrębie której można skonfigurować rolę lub role zidentyfikowane w kolumnie *Używane przez*. Wprowadź żądane zmiany i przejdź kolejne karty kreatora do momentu pojawienia się karty potwierdzenia i sprawdź, czy zmiany zostały uwzględnione.
- ♦ **Konfigurowanie ustawień zabezpieczeń sieciowych.** Na tym etapie pracy kreatora określa się, które porty zostaną przez firewall otwarte, a które zablokowane (rysunek 2.25). Kreator oferuje kilka opcji widoku, które ułatwiają identyfikację konkretnych portów. Można też kliknąć przycisk *Dodaj*, żeby dodać dodatkowe otwarte porty lub aplikacje niezablokowane przez firewall. Kreator wyświetla kartę potwierdzenia, żeby przed kontynuowaniem ułatwić sprawdzenie poprawności wybranych ustawień.
- ♦ **Konfigurowanie ustawień rejestru.** Kreator udostępnia kilka kart mających za zadanie uzyskanie informacji o protokołach używanych do komunikowania się z innymi komputerami, a także o stosowanych metodach uwierzytelniania i minimalnych wymaganiach systemu operacyjnego związanych z innymi

Rysunek 2.24.

Przed kontynuowaniem działań zatwierdź zmiany usług, a następnie stosownie do potrzeb zmodyfikuj rolę

**Rysunek 2.25.**

Określanie portów serwera, które będą otwarte



komputerami. Zgromadzone informacje kreator wykorzystuje do modyfikacji wybranych ustawień rejestru. Ma to na celu poprawienie zabezpieczeń i zapobiegnięcie konkretnym typom ataków. Kreator wyświetla kartę potwierdzenia, która pozwala zweryfikować docelowe zmiany.

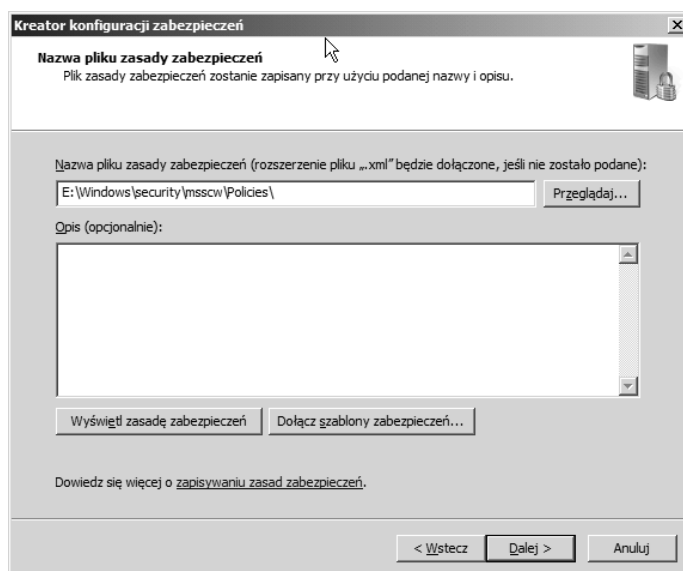
- ♦ **Konfigurowanie systemowej zasady inspekcji.** Karta *Zasady inspekcji systemu* kreatora ułatwia określenie zasady inspekcji dla zestawu zasad zabezpieczeń.
- ♦ **Konfigurowanie internetowych usług informacyjnych.** Jeśli użyto roli Serwer aplikacji, kreator wyświetli zestaw kart żądających skonfigurowania opcji rozszerzeń

usług WWW, wirtualnych katalogów i anonimowego uwierzytelniania serwera IIS. Przy użyciu tych kart można określić konfigurację serwera IIS dla zasady zabezpieczeń.

Na końcu kreator zażąda podania nazwy pliku zasady zabezpieczeń, w którym zapisze konfigurację zasady (rysunek 2.26). Kreator przechowuje ustawienia w pliku XML. *Plik* taki może być następnie wykorzystany do skonfigurowania innych serwerów.

Rysunek 2.26.

Określanie nazwy pliku XML, w którym będą przechowywane ustawienia zasady



Karta *Nazwa pliku zasady zabezpieczeń* zapewnia też dwa dodatkowe zadania, które można zrealizować. Jeśli klikniesz przycisk *Wyświetl zasadę zabezpieczeń*, kreator uruchomi aplikację Podgląd Kreatora konfiguracji zabezpieczeń (rysunek 2.27), która umożliwia przejrzanie ustawień zasady.

Do zasady można też dodać szablony zabezpieczeń. Domyślnie znajdują się one w katalogu `%systemroot%\security\templates` i mają postać zestawu plików INF. Szablony zabezpieczeń można przeglądać i modyfikować za pomocą przystawki Szablony zabezpieczeń konsoli MMC (a także tworzyć dodatkowe szablony). Aby do zasady zabezpieczeń dodać szablon, w obrębie karty *Nazwa pliku zasady zabezpieczeń* narzędzia *Kreator konfiguracji zabezpieczeń* kliknij przycisk *Dołącz szablon zabezpieczeń*. Spowoduje to otwarcie okna dialogowego *Dołączanie szablonów zabezpieczeń*, które stosownie do potrzeb pozwala dodać szablony do zasady lub usunąć je.

Praca ze źródłami danych (ODBC)

Interfejs ODBC (*Open Database Connectivity*) zapewnia szkielet dla mechanizmów bazodanowych komunikujących się z aplikacjami klienta. Sterowniki ODBC pełnią rolę pośrednika między bazą danych i aplikacją klienta, koordynując transakcje i przeprowadzając translację między klientem i bazą. W określonych sytuacjach sterowniki te mogą zastąpić

Rysunek 2.27.
Narzędzie Podgląd
Kreatora konfiguracji
zabezpieczeń
prezentuje ustawienia
zasady



mechanizm bazodanowy. Przykładowo serwer nie wymaga instalacji aplikacji Microsoft Access, żeby umożliwić klientom wysyłanie zapytań do pliku bazy danych Access przechowywanej w obrębie serwera. Jest to często praktykowane przez mechanizmy raportowania, takie jak Seagate Crystal Reports.

Aby aplikacje klienta skomunikowały się ze źródłem danych zlokalizowanym w obrębie komputera, trzeba skonfigurować odpowiedni sterownik ODBC i połączenie z docelowym serwerem. Jeśli na przykład aplikacja klienta wymaga dostępu do bazy danych Access, w pierwszej kolejności konieczne będzie skonfigurowanie sterownika ODBC Access dla komputera, który przechowuje bazę. Narzędzie administracyjne *Źródła danych* (ODBC) umożliwia skonfigurowanie sterowników ODBC i zarządzanie nimi, a także powiązanymi z nimi źródłami danych. W niniejszym podrozdziale wyjaśniono, jak konfigurować sterowniki ODBC.



Narzędzie *Źródła danych* (ODBC) jest jednym z kilku programów administracyjnych, które funkcjonują niezależnie, a nie jako przystawki konsoli MMC.

Definiowanie nazw źródeł danych

W celu udostępnienia źródła danych klientom należy utworzyć nazwę źródła danych DSN (*Data Source Name*). Można wyróżnić następujące trzy typy nazw DSN:

- ♦ **Nazwa DSN użytkownika.** Jest widoczna tylko przez użytkownika, który był zalogowany w momencie utworzenia nazwy DSN.
- ♦ **Systemowa nazwa DSN.** Jest widoczna przez wszystkie lokalne usługi komputera i każdego użytkownika zalogowanego lokalnie w obrębie komputera.

- ♦ **Plikowa nazwa DSN.** Może być dzielona przez wszystkich użytkowników, którzy zainstalowali te same sterowniki i dysponują uprawnieniami pozwalającymi uzyskać dostęp do nazwy DSN. W przeciwieństwie do nazw DSN użytkownika i systemowych nazw DSN, plikowe nazwy DSN są przechowywane w plikach tekstowych, a nie w rejestrze.

Nazwa DSN identyfikuje źródło danych, powiązany z nim sterownik i inne właściwości definiujące interakcję między klientem i źródłem danych, takie jak czas oczekiwania, tryb tylko do odczytu itp. W przypadku większości typów baz danych do tworzenia nazwy DSN używa się tego samego procesu. Wyjątkiem jest baza danych SQL Server, która zapewnia kreator konfigurujący źródło danych.

Definiowanie źródła danych

W celu utworzenia źródła danych trzeba najpierw otworzyć okno *Administrator źródeł danych ODBC*. W tym celu z menu *Start* wybierz pozycję *Wszystkie programy/Narzędzia administracyjne/Źródła danych (ODBC)*. W oknie *Administrator źródeł danych ODBC* uaktywnij kartę typu nazwy DSN, która zostanie utworzona, i kliknij przycisk *Dodaj*. Wybierz żądany typ źródła danych i kliknij przycisk *Zakończ*. Z wyjątkiem sterownika bazy danych SQL Server interfejs ODBC zażąda informacji, które zmieniają się w zależności od zaznaczonego sterownika. Określ wymagane ustawienia i kliknij przycisk *OK*, żeby utworzyć nazwę DSN.

Konfigurowanie źródła danych SQL Server

Sterownik ODBC bazy danych Microsoft SQL Server zapewnia kreator, który konfiguruje źródło danych SQL. W tym podpunkcie objaśniono opcje dostępne podczas konfigurowania tego sterownika. Pierwsza karta kreatora zawiera następujące opcje:

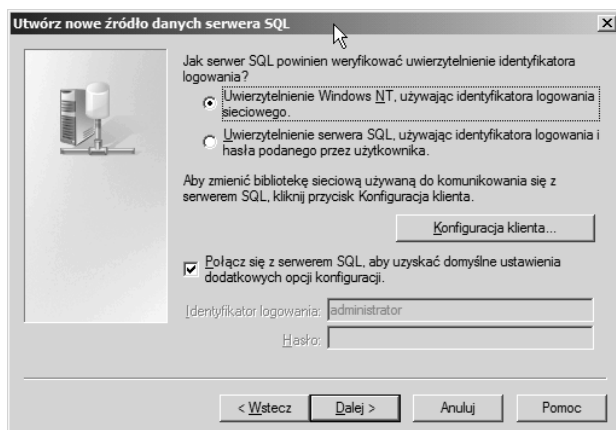
- ♦ **Nazwa.** Nazwa pojawia się dla źródła danych na liście źródeł danych w obrębie karty nazwy DSN.
- ♦ **Opis.** Opcjonalny opis jest wyświetlany dla źródła danych wraz z nazwą DSN w obrębie karty nazwy DSN.
- ♦ **Serwer.** Opcja umożliwia określenie adresu IP lub nazwy hosta serwera SQL Server.

Druga karta kreatora (rysunek 2.28) żąda określenia dla źródła danych opcji połączenia i uwierzytelniania. Oto lista zestawiająca opcje:

- ♦ **Uwierzytelnienie Windows NT, używając identyfikatora logowania sieciowego.** Uaktywnij tę opcję, żeby sterownik ODBC bazy danych SQL Server żądał bezpiecznego połączenia z serwerem. W celu uwierzytelnienia żądania przez serwer sterownik używa nazwy konta i hasła użytkownika aktualnie zalogowanego po stronie klienta. W przypadku usługi lub serwera WWW dane uwierzytelniające są kojarzone z usługą lub określane w kodzie tworzącym zapytanie. Określona nazwa konta i hasło muszą być powiązane z identyfikatorem logowania serwera SQL Server.

Rysunek 2.28.

Określanie opcji
połączenia
i uwierzytelniania

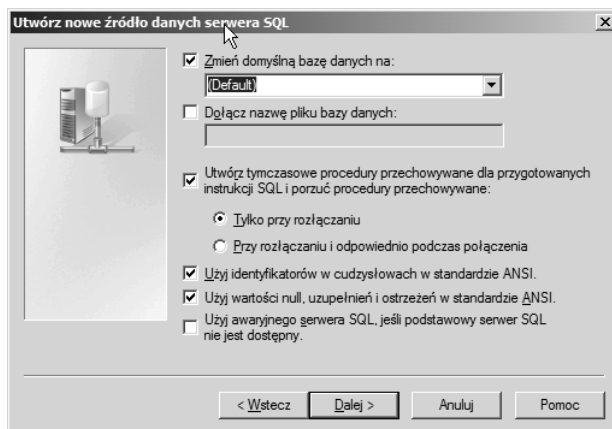


- ♦ **Uwierzytelnienie serwera SQL, używając identyfikatora logowania i hasła podanego przez użytkownika.** Zaznacz opcję, żeby w przypadku wszystkich połączeń żądań użytkownik musiał określić identyfikator logowania serwera SQL Server i hasło.
- ♦ **Połącz się z serwerem SQL, aby uzyskać domyślne ustawienia dodatkowych opcji konfiguracji.** Zastosowanie tej opcji spowoduje nawiązanie przez sterownik ODBC połączenia z serwerem SQL Server zidentyfikowanego w obrębie pierwszej karty kreatora w celu uzyskania poprawnych wartości opcji znajdujących się w pozostałych kartach kreatora. Kliknięcie przycisku *Dalej* po zaznaczeniu tej opcji sprawi, że sterownik połączy się z serwerem SQL Server i pobierze dane. Wyłączenie opcji umożliwi zastosowanie domyślnych ustawień zamiast łączenia się z serwerem SQL Server w celu uzyskania informacji.
- ♦ **Identyfikator logowania.** Określ nazwę użytkownika, który nawiąże połączenie z serwerem SQL Server, żeby pobrać ustawienia na potrzeby kolejnych kart kreatora (zapoznaj się z poprzednim punktem listy). Nazwa użytkownika i powiązane z nim hasło wstawione w polu *Hasło* po utworzeniu źródła danych nie są wykorzystywane w rzeczywistości do ustanawiania połączeń, a jedynie do pobierania informacji z serwera SQL Server w przypadku reszty kart kreatora.
- ♦ **Hasło.** Określ hasło, które będzie używane razem z nazwą użytkownika podaną w polu *Identyfikator logowania*.
- ♦ **Konfiguracja klienta.** Kliknij tę opcję, żeby móc skorzystać z okna dialogowego *Dodaj konfigurację biblioteki sieciowej*. Choć zwykle nie trzeba konfigurować klienta sieciowego pod kątem źródła danych, czasami może być konieczne określenie mechanizmu połączeń sieciowych i innych opcji, które zdefiniują sposób łączenia się klienta ze źródłem danych. Opcje sekcji *Parametry połączenia* są związane z typem połączenia sieciowego wybranego z listy opcji *Biblioteki sieciowe*.

W obrębie następnej karty kreatora (rysunek 2.29) określa się nazwę bazy danych i inne opcje źródła danych. Poniższa lista opisuje dostępne opcje.

Rysunek 2.29.

Określanie nazwy
bazy danych
i innych jej opcji



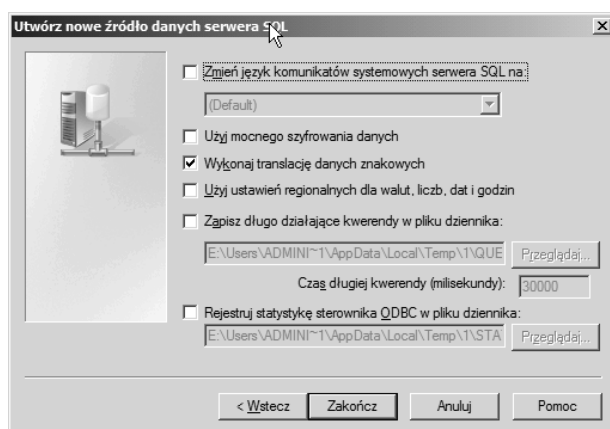
- ♦ **Zmień domyślną bazę danych na.** Z listy rozwijanej wybierz bazę danych, żeby dla źródła danych zdefiniować domyślną bazę danych. W efekcie zostanie zmieniona domyślna baza danych dla określonego identyfikatora logowania. Wyłącz opcję, żeby zastosować domyślną bazę ustawioną dla identyfikatora logowania.
- ♦ **Dołącz nazwę pliku bazy danych.** Określ pełną nazwę i ścieżkę podstawowego pliku dla możliwej do podłączenia bazy danych. Wybrana baza pełni rolę domyślnej dla źródła danych.
- ♦ **Utwórz tymczasowe procedury przechowywane dla przygotowanych instrukcji SQL i porzuć procedury przechowywane.** Zaznacz tę opcję, żeby w celu obsługi funkcji ODBC SQLPrepare sterownik utworzył tymczasowe procedury przechowywane, a następnie wybrał jedną z powiązanych opcji (zapoznaj się z poniższymi punktami listy). Wyłącz tę opcję, jeśli sterownik nie ma magazynować procedur.
- ♦ **Tylko przy rozłączaniu.** Opcja ta powoduje, że procedury przechowywane utworzone dla funkcji SQLPrepare zostaną usunięte tylko po wywołaniu funkcji SQLDisconnect. W ten sposób poprawia się wydajność przez zredukowanie obciążenia generowanego przez usuwanie procedur przechowywanych w czasie działania aplikacji. Jednak może to doprowadzić do wzrostu liczby tymczasowych procedur przechowywanych. Dotyczy to zwłaszcza aplikacji, które stosują kilka wywołań funkcji SQLPrepare lub bez rozłączania się działają przez długi okres.
- ♦ **Przy rozłączaniu i odpowiednio podczas połączenia.** Opcja ta sprawia, że procedury przechowywane zostaną usunięte po wywołaniu funkcji SQLDisconnect, wywołaniu funkcji SQLFreeHandle dla uchwytu instrukcji, wywołaniu funkcji SQLPrepare lub SQLExecDirect w celu przetworzenia nowej instrukcji SQL dla tego samego uchwytu lub po wywołaniu funkcji katalogu. Choć użycie tej opcji spowoduje większe obciążenie w czasie pracy aplikacji, pomoże w zapobiegnięciu wzrostowi liczby tymczasowo przechowywanych procedur.
- ♦ **Użyj identyfikatorów w cudzysłowach w standardzie ANSI.** Opcja ta wymusza reguły ANSI dla znaków cudzysłowu. Dzięki temu mogą one być stosowane tylko dla takich identyfikatorów, jak nazwy tabel i kolumn. Łańcuchy znakowe muszą być zawarte w pojedynczych cudzysłowach.

- ♦ **Użyj wartości null, uzupełnień i ostrzeżeń w standardzie ANSI.** Opcja ta powoduje, że opcje ANSI_NULLS, ANSI_WARNINGS i ANSI_PADDINGs są uaktywniane wtedy, gdy sterownik połączy się ze źródłem danych.
- ♦ **Użyj awaryjnego serwera SQL, jeśli podstawowy serwer SQL nie jest dostępny.** Opcja ta sprawia, że jest podejmowana próba połączenia w celu użycia serwera awaryjnego, jeśli pozwala na to podstawowy serwer SQL Server. Gdy połączenie zostanie przerwane, sterownik usuwa bieżące transakcje i próbuje ponownie połączyć się z podstawowym serwerem SQL Server. Sterownik podejmuje próbę nawiązania połączenia z serwerem awaryjnym, jeżeli ustali, że podstawowy serwer stał się niedostępny.

W ostatniej karcie kreatora, pokazanej na rysunku 2.30, trzeba określić różne opcje, które opisuje poniższa lista.

Rysunek 2.30.

Określanie różnych opcji bazy danych w obrębie ostatniej karty kreatora



- ♦ **Zmień język komunikatów systemowych serwera SQL na.** Opcja ta określa język służący do generowania komunikatów systemowych serwera SQL Server. Serwer może dysponować wieloma zestawami komunikatów systemowych prezentowanych w różnych językach. Opcja ta jest niedostępna, jeśli na serwerze zainstalowano tylko jeden język.
- ♦ **Użyj mocnego szyfrowania danych.** Opcja ta powoduje szyfrowanie danych z wykorzystaniem zaawansowanego algorytmu szyfrującego.
- ♦ **Wykonaj translację danych znakowych.** Uaktywnij tę opcję, żeby skonwertować łańcuchy ANSI przy użyciu standardu Unicode. Wyłącz opcję w celu zrezygnowania z translacji rozszerzonych kodów ANSI.
- ♦ **Użyj ustawień regionalnych dla walut, liczb, dat i godzin.** Zastosuj tę opcję, żeby ustawienia regionalne komputera klienta zostały wykorzystane do wyświetlenia waluty, liczb, dat i innych elementów regionalnych.
- ♦ **Zapisz długo działające kwerendy w pliku dziennika.** Opcja ta sprawia, że zostanie zarejestrowane każde zapytanie, którego czas działania przekracza określony w polu *Czas długiej kwerendy (milisekundy)*.
- ♦ **Czas długiej kwerendy (milisekundy).** Opcja ta określa maksymalną wartość progową na potrzeby rejestrowania długo wykonywanych zapytań.

- ♦ **Rejestruj statystykę sterownika ODBC w pliku dziennika.** Opcja ta rejestruje statystyki dotyczące sterownika w pliku dziennika, w którym rolę separatora pełni tabulator.

Component Checker

Niejednolity zestaw składników ODBC może doprowadzić do wszelkiego rodzaju dziwnych i trudnych do zidentyfikowania problemów. Przykładowo aplikacja WWW tworząca zapytania z wykorzystaniem połączenia ODBC może napotkać na błąd niezwiązany z serwerem, gdy podejmie próbę nawiązania połączenia w przypadku niezgodności wersji składników ODBC. Oznacza to, że bardzo ważne jest zsynchronizowanie składników.

Microsoft oferuje narzędzie o nazwie *Component Checker*, które pomaga skanować system i stwierdzić, czy są zsynchronizowane składniki *Microsoft Data Access Components* (MDAC). Narzędzie *Component Checker* jest dostępne pod adresem <http://www.microsoft.com/data>. Witryna ta udostępnia również najnowszą wersję składników MDAC, a także techniczne informacje dotyczące MDAC i interfejsu ODBC.

Sprawdzanie informacji o sterowniku

Karta *Sterowniki* okna *Administrator źródeł danych ODBC* umożliwia sprawdzenie informacji dotyczących zainstalowanych sterowników ODBC. Karta ta przydaje się podczas sprawdzania wersji sterownika, lecz nie zapewnia żadnych opcji, które można zmieniać.

Śledzenie

Karta *Śledzenie* narzędzia *Źródła danych (ODBC)* służy do konfigurowania opcji śledzenia, które ułatwiają rozwiązywanie problemów z połączeniem klienta. Po włączeniu śledzenia operacje związane z ODBC są rejestrowane w wybranym pliku dziennika, który można przeglądać za pomocą dowolnego edytora tekstu.

Pula połączeń

Karta *Pula połączeń* umożliwia określenie, czy sterowniki ODBC mogą, czy nie mogą ponownie korzystać z otwartych uchwytów połączeń z serwerem bazodanowym. Można zwiększyć wydajność przez wyeliminowanie konieczności ustanawiania przez aplikacje nowych połączeń z serwerem, gdyż zostanie skrócony czas i zmniejszone obciążenie generowane przez proces tworzenia połączenia. Dla baz danych Oracle i SQL pule połączeń są zapewniane domyślnie, a w przypadku innych baz nie.

Aplety panelu sterowania

Podobnie do innych wersji platformy Windows, panel sterowania systemu Windows Server 2008 pełni rolę centrum kontrolującego konfigurowanie ustawień urządzeń i systemu operacyjnego. Część apletów panelu sterowania nadzoruje dość proste zestawy opcji, a część stosunkowo złożone. W poniższych punktach omówiono bardziej skomplikowane aplety

panelu sterowania i ich funkcje. Pominęto aplety niewymagające żadnego objaśnienia (na przykład konfigurujące mysz i kontrolery gier). Ponadto trzeba zauważyć, że domyślnie nie są widoczne wszystkie aplety panelu sterowania. Przykładowo aplet *Łącze bezprzewodowe* pojawia się tylko w przypadku komputerów wyposażonych w porty podczerwieni lub podobne urządzenia bezprzewodowe.



Można skonfigurować menu *Start* tak, żeby uwzględniało skróty apletów panelu sterowania. Dzięki temu z poziomu menu *Start* uzyskuje się dostęp do poszczególnych apletów bez konieczności otwierania okna panelu sterowania. Aby wyświetlić w menu *Start* skróty apletów panelu sterowania, prawym przyciskiem myszy kliknij pasek zadań i z menu wybierz pozycję *Właściwości*. Uaktywnij kartę *Menu Start* i kliknij przycisk *Dostosuj* aktywnej opcji *Menu Start*, a następnie w otwartym oknie *Dostosowywanie menu Start* poniżej pozycji *Panel sterowania* zaznacz opcję *Wyświetl jako menu* i dwukrotnie kliknij przycisk *OK*.

W celu otwarcia panelu sterowania z menu *Start* wybierz pozycję *Panel sterowania*. Jeśli menu *Start* poszerzono o skróty apletów panelu sterowania i zamierza się otworzyć katalog *Panel sterowania*, trzeba kliknąć przycisk *Start*, a następnie prawym przyciskiem myszy kliknąć pozycję *Panel sterowania* i z menu wybrać polecenie *Otwórz*. Katalog ten można też otworzyć z poziomu okna *Komputer*.

Aplet Centrum ułatwień dostępu

Aplet ten umożliwia skonfigurowanie interfejsu, a także funkcji wejścia i wyjścia opracowanych w celu ułatwienia pracy użytkownikom o różnego rodzaju niepełnosprawności (na przykład mającym słaby wzrok). Można skonfigurować różne ustawienia i funkcje związane z wyświetlaniem, klawiaturą, myszą i dźwiękiem.

Aplet Dodaj sprzęt

Dwukrotne kliknięcie tego apletu spowoduje uruchomienie narzędzia *Dodawanie sprzętu*, które pomaga dodać nowe urządzenie, odłączyć sprzęt, a także rozwiązywać problemy z urządzeniami. Kreator sprawdza komputer pod kątem zmian i ułatwia zautomatyzowanie procesu instalowania sterowników obsługujących nowe urządzenia.

Jeśli zdecydujesz się dodać urządzenie lub zdiagnozować je, Windows Server 2008 automatycznie poszuka sprzętu *Plug and Play* (PnP). Jeżeli system znajdzie i rozpozna nowe urządzenie, krok po kroku przeprowadzi użytkownika przez proces instalacji sterownika urządzenia. Gdy system zlokalizuje sprzęt, lecz nie rozpozna go, kreator zażąda wybrania urządzenia z listy i ręcznego określenia sterownika.

W celu zdiagnozowania sprzętu zezwól systemowi Windows Server 2008 na wykrycie urządzenia, a następnie odszukaj je na liście umożliwiającej wybranie sprzętu i kliknij przycisk *Dalej*. Kreator pomoże wykonać kroki procesu diagnozowania urządzenia. Aby dodać nowe urządzenie, z listy wybierz pozycję *Dodaj nowe urządzenie* i kliknij przycisk *Dalej*. Gdy pojawi się odpowiednie żądanie, umieść w napędzie dysk DVD systemu Windows Server 2008 lub określ ścieżkę właściwych plików sterownika.

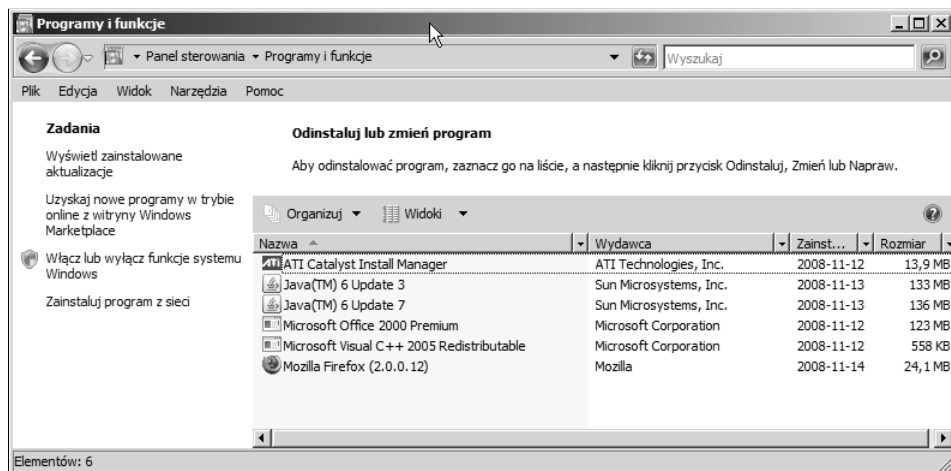
Jeżeli postanowisz odinstalować urządzenie, Windows Server 2008 zaprezentuje listę wszystkich urządzeń. Zaznacz urządzenie, które ma zostać usunięte, po czym kliknij przycisk *Dalej* i postępuj zgodnie z instrukcjami umożliwiającymi zakończenie procesu. Jeśli odłą-

czasz urządzenie, Windows Server 2008 udostępni listę sprzętu, który może zostać odłączony. Zaznacz urządzenie, a następnie kliknij przycisk *Dalej* i w celu ukończenia procesu zapewnij żądane dane (jeśli będzie to konieczne).

Aplet Programy domyślne

Nie jest już dostępny aplet *Dodaj* lub usuń programy. Większa część funkcjonalności tego starego apletu systemu Windows Server 2003 została zintegrowana z narzędziem *Menedżer serwera* (role i funkcje). Obecnie do dyspozycji jest aplet *Programy domyślne*. Składniki systemu Windows umieszczono w programie *Menedżer serwera*, rozdzielając je między role i funkcje (nie stosuje się też już określenia „składniki systemu Windows”).

W zasadzie aplet *Programy domyślne* jest niestandardowym lub zewnętrznym interfejsem służącym do instalowania oprogramowania i zarządzania nim. Jak widać na rysunku 2.31, na przykładowym serwerze zainstalowano kilka aplikacji. Nie trzeba robić nic szczególnego podczas instalowania aplikacji, żeby zapewnić, że będą zarządzane przez aplet *Programy domyślne*.



Rysunek 2.31. Za pomocą okna *Programy i funkcje* można dodać lub usunąć, a także przekonfigurować i zaktualizować programy

Podobnie do starszego apletu *Dodaj* lub usuń programy, aplet *Programy domyślne* pełni trzy podstawowe funkcje. Umożliwia modyfikowanie instalacji lub usuwanie istniejących programów, instalowanie nowych programów, a także włączanie lub wyłączanie funkcji systemu Windows. Dwie pierwsze z wymienionych możliwości zwykle mają zastosowanie w przypadku aplikacji użytkowników. Z kolei ostatnia z podanych możliwości pozwala dodawać do systemu Windows Server 2008 lub usuwać z niego takie funkcje jak usługa indeksowania, usługi certyfikatów, serwer IIS i dodatkowe narzędzia. Wielka różnica między systemami Windows Server 2008 i Windows Server 2003 polega na tym, że w przypadku drugiego w rzeczywistości z serwera usuwano aplikację, natomiast obecnie można ją wyłączyć bez konieczności usuwania jej składników i danych z serwera. Aby w dowolnym momencie dodać aplikację z powrotem, wystarczy ponownie uaktywnić opcję *Włącz*

lub wyłącz funkcje systemu Windows. Jednakże powinno się wiedzieć, że z opcji tej można skorzystać tylko w przypadku aplikacji, które obsługują nowy interfejs API bądź mają logo zgodności z systemem Windows Server 2008 lub Windows Vista.



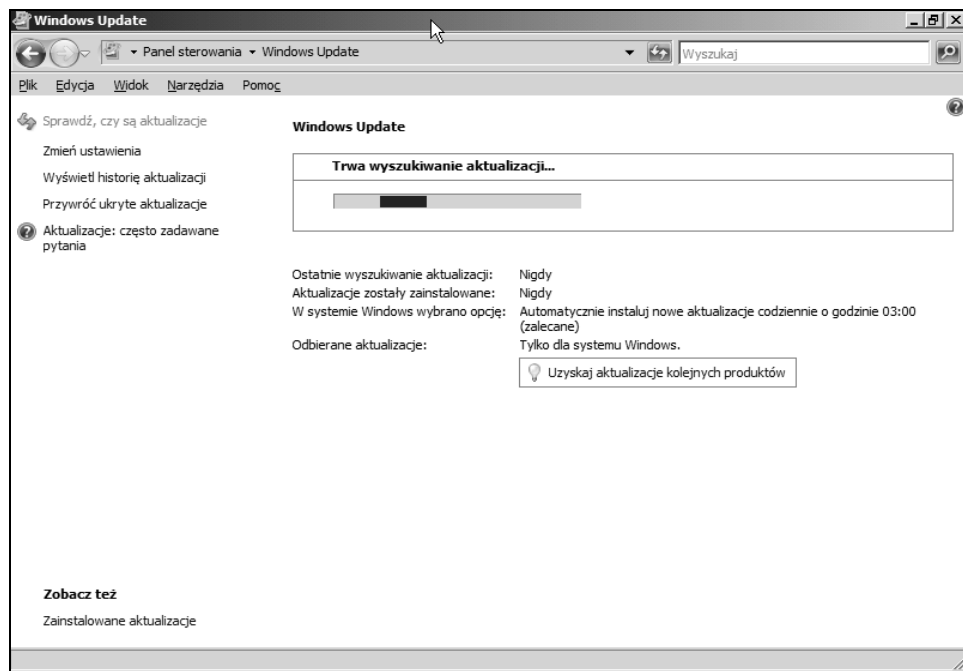
Domyślnie lista zainstalowanych aplikacji nie uwzględnia aktualizacji i poprawek. Aby zapoznać się z zainstalowanymi programami, kliknij opcję *Wyświetl zainstalowane aktualizacje* widoczną w oknie apletu pokazanego na rysunku 2.31.

Aplet Narzędzia administracyjne

Aplet *Narzędzia administracyjne* panelu sterowania pełni rolę kontenera dla różnych narzędzi administracyjnych, takich jak między innymi przystawki Zarządzanie komputerem, Usługi i Podgląd zdarzeń. Każde z tych narzędzi omówiono w odpowiednim miejscu niniejszego rozdziału lub w innych rozdziałach.

Aplet Windows Update

Aplet ten (rysunek 2.32) umożliwia określenie, w jaki sposób serwer korzysta z funkcji automatycznych aktualizacji. W większości sytuacji prawdopodobnie nie skorzysta się z automatycznego stosowania aktualizacji dla serwera, ponieważ wiąże się z tym wymóg testowania i weryfikowania aktualizacji przed ich wdrożeniem. W celu dokładnego kontrolowania tego, jak i kiedy automatyczne aktualizacje są stosowane dla serwerów i klientów, można użyć usługi *Windows Server Update Services* (WSUS) w połączeniu z zasadami grupy. Więcej informacji o usłudze WSUS można znaleźć pod adresem <http://technet.microsoft.com/en-us/wsus/default.aspx>.



Rysunek 2.32. Można skonfigurować funkcję automatycznych aktualizacji serwera

Aplet Data i godzina

Aplet ten jest tym samym, który pojawia się po dwukrotnym kliknięciu zegara w obrębie systemowego paska zadań. Otwarte okno dialogowe umożliwia ustawienie dla serwera daty, czasu i strefy czasowej — nie wymaga to objaśnień.

Zapewnianie przez serwer precyzyjnego czasu jest niezmiernie ważne nie tylko w przypadku uwierzytelniania, lecz również śledzenia błędów i zdarzeń, a także zabezpieczeń. Jeśli na przykład zostanie przeprowadzony atak DoS (*Denial-of-Service*) z wykorzystaniem konkretnego dynamicznego adresu IP, znajomość czasu, w którym atak miał miejsce, pozwoli wysledzić użytkownika stosującego ten adres w tym czasie. Dokładne znaczniki czasu są też istotne w celu zapewnienia niezawodnych operacji archiwizowania i odtwarzania danych.

Komputery należące do domeny przeprowadzają synchronizację we własnym zakresie. Stacje robocze i serwery członkowskie automatycznie synchronizują się z kontrolerem domeny pełniącym w niej rolę wzorca operacji. W przypadku tego kontrolera domeny okresowo powinna być sprawdzana dokładność czasu i w razie potrzeby ustawiana. Jednak lepszym rozwiązaniem jest takie skonfigurowanie kontrolera, żeby swój czas synchronizował z internetowym źródłem czasu, takim jak serwer time.nist.gov. W tym przypadku członkowie domeny uzyskają dokładny czas, gdy dokonają synchronizacji z kontrolerem.



Usługa Czas systemu Windows jest składnikiem odpowiedzialnym za synchronizację czasu. Domyślnie usługa jest automatycznie uruchamiana.

Ustawienia synchronizacji czasu można skonfigurować za pomocą zasady grupy. Zasady znajdują się w gałęzi *\Konfiguracja komputera\Szablony administracyjne\System\Usługa Czas systemu Windows*. Za pomocą zasady *Globalne ustawienia konfiguracji* można uaktywnić i skonfigurować wiele różnych właściwości, które określają sposób, w jaki serwer przetwarza próbki czasu otrzymywane od dostawców czasu.

Zasady zawarte w podgałęzi *Dostawcy czasu* kontrolują synchronizację czasu zarówno z poziomu klienta, jak i serwera. Oto te zasady:

- ♦ **Włącz klienta protokołu Windows NTP.** Uaktywnienie tej zasady pozwala serwerowi synchronizować swój czas z serwerem określonym w zasadzie *Konfiguruj klienta protokołu Windows NTP*. Aby serwer nie synchronizował własnego czasu, zasadę *Włącz klienta protokołu Windows NTP* trzeba wyłączyć.
- ♦ **Konfiguruj klienta protokołu Windows NTP.** Zasadę tę trzeba włączyć, jeśli swój czas serwer ma synchronizować ze zdalnym serwerem czasu. Po uaktywnieniu zasady uzyska się dostęp do kilku właściwości określających serwer czasu, częstotliwości aktualizacji, typ serwera i inne kwestie związane z synchronizowaniem czasu.
- ♦ **Włącz serwer protokołu Windows NTP.** Zasadę należy włączyć, jeżeli serwer ma pełnić rolę serwera czasu i obsługiwać żądania NTP pochodzące od innych komputerów zlokalizowanych w sieci.



Do uruchomienia własnego serwera czasu nie jest wymagane użycie systemu Windows Server 2008. Taką możliwość oferują też systemy Windows Server 2003, Windows XP i Windows Vista.

Obiekt Ekran apletu Personalizacja

Aplet *Ekran* nie jest już dostępny oddzielnie. Został przeniesiony do apletu *Personalizacja*. Jednak w dalszym ciągu aplet *Ekran* umożliwia konfigurowanie ustawień ekranu, takich jak tapeta, tło, schemat i głębia kolorów, a także rozmiar pulpitu (rozdzielczość). Możliwe jest również skonfigurowanie wygaszacza ekranu, włączenie i ustawienie efektów WWW, a także określenie ogólnych ustawień i efektów pulpitu. Jeśli komputer dysponuje wieloma kartami graficznymi, każdą można skonfigurować osobno, a ponadto określić, jak każda karta będzie wyświetlać obraz na pulpicie.

Aplet Opcje folderów

Aplet *Opcje folderów* panelu sterowania pozwala zdecydować, w jaki sposób będą się pojawiać i funkcjonować okna katalogów programu Eksplorator Windows. Za pomocą tego apletu można między innymi włączać lub wyłączać aktywny pulpit, określić typ okna używanego do wyświetlania katalogów (styl tradycyjny lub WWW) i zdecydować, czy nowe katalogi będą otwierane w tym samym oknie, czy w nowym. Istnieje też możliwość skonfigurowania innych opcji, takich jak powiązania plików i pliki trybu offline.

Aplet Opcje internetowe

Aplet ten oferuje kilka kart właściwości, które umożliwiają skonfigurowanie ustawień przeglądarki Internet Explorer i powiązanych z nią programów, takich jak Outlook Express i NetMeeting.

- ♦ **Ogólne.** Karta ta pozwala na określenie domyślnej strony głównej, usunięcie buforowanych plików, wyczyszczenie historii adresów URL, a także ustawienie ogólnych właściwości, takich jak czcionki, kolory, języki i funkcje dostępności.
- ♦ **Zabezpieczenia.** Karta ta umożliwia określenie poziomu zabezpieczeń dla różnych stref. Strefa jest grupą witryny WWW, które mają wspólny poziom zabezpieczeń. Zaznacz jedną z predefiniowanych stref i kliknij przycisk Witryny, żeby dodać witryny do strefy lub usunąć je z niej. Przy użyciu suwaka znajdującego się w obrębie karty *Zabezpieczenia* ustaw następnie dla strefy poziom zabezpieczeń lub kliknij przycisk *Poziom niestandardowy*, żeby określić niestandardowe ustawienia decydujące o sposobie przetwarzania plików *cookie* przez program Internet Explorer i powiązane z kontrolkami ActiveX i dodatkami, skryptami, pobraniami plików itp.
- ♦ **Prywatność.** Karta ta pozwala określić, jak przeglądarka Internet Explorer obsługuje pliki *cookie*, zarówno globalnie, jak i na poziomie wybranych witryny WWW.
- ♦ **Zawartość.** Karta ta umożliwia włączenie i skonfigurowanie klasyfikatora treści, który pomaga ograniczać dostęp do określonych witryn (na przykład z materiałami przeznaczonymi dla dorosłych). Karta *Zawartość* daje też możliwość skonfigurowania certyfikatów na potrzeby bezpiecznych witryn WWW i wiadomości pocztowych. Sekcja *Informacje osobiste* karty *Zawartość* umożliwia utworzenie profilu zawierającego personalia, adres, numer telefonu i inne informacje. Trzeba wiedzieć, że dane te będą dostępne dla odwiedzanych witryn WWW, jeśli nie uniemożliwi się to przez skonfigurowanie stref zabezpieczeń.

- ♦ **Połączenia.** Karta ta służy do konfigurowania połączeń internetowych i do określania, jak i kiedy Internet Explorer użyje funkcji automatycznego łączenia się z internetem. Kliknij przycisk *Ustawienia*, żeby uruchomić narzędzie *Połącz z Internetem*, które tworzy nowe połączenie internetowe. Aby skonfigurować ustawienia serwera proxy, kliknij przycisk *Ustawienia sieci LAN*.
- ♦ **Programy.** Karta ta umożliwia powiązanie konkretnych programów z zastosowaniami takimi jak poczta elektroniczna, grupy dyskusyjne itp.
- ♦ **Zaawansowane.** Karta zawiera kilka opcji decydujących o tym, jak program Internet Explorer obsługuje wersje protokołu HTTP, multimedia, drukowanie, zabezpieczenia i inne właściwości.

Aplet Centrum sieci i udostępniania

Aplet *Centrum sieci i udostępniania* panelu sterowania wyświetla okno *Centrum sieci i udostępniania*. Aplet ten zawiera ikonę dla każdego skonfigurowanego połączenia sieciowego (z uwzględnieniem połączeń LAN i telefonicznych). Kliknij odnośnik *Zarządzaj połączeniami sieciowymi*, żeby skonfigurować protokoły połączeń, dowiązania, klienty, usługi, udostępnianie i inne ustawienia.



Bardziej obszerne omówienie konfiguracji sieci można znaleźć w rozdziale 3.

Aplet Opcje zasilania

Aplet *Opcje zasilania* panelu sterowania kontroluje funkcje energooszczędne komputera, takie jak wyłączanie urządzeń peryferyjnych po upływie ustalonego czasu bezczynności i stan hibernacji (zapisanie danych na dysku). Możliwe jest skonfigurowanie ustawień zasilania i zapisanie ich w postaci schematu zasilania. Dzięki temu ułatwia się przełączanie między różnymi grupami ustawień.

Karta *Zasilacz UPS* okna *Właściwości: Opcje zasilania* nadzoruje usługę zasilacza awaryjnego UPS. Jeśli zasilacz UPS podłączono do komputera za pośrednictwem jednego z jego portów, w obrębie tej karty pojawi się status urządzenia informujący między innymi o szacunkowym czasie pracy i stanie baterii. Za pomocą karty *Zasilacz UPS* można skonfigurować zasilacz UPS lub wybrać inne tego typu urządzenie.

Aplet Drukarki

Aplet *Drukarki* otwiera okno *Drukarki*, w którym znajduje się ikona dla każdej zainstalowanej drukarki, a także kreator umożliwiający dodanie lokalnych lub zdalnych drukarek.



Szczegółowe informacje o oknie *Drukarki* i usługach drukowania zamieszczono w rozdziale 12.

Aplet System

Aplet *System* zapewnia dostęp do ogólnych właściwości systemu. Aplet ten można uruchomić przez kliknięcie prawym przyciskiem myszy skrótu *Komputer* i wybranie z menu pozycji *Właściwości*. Pierwsza karta apletu *System* oferuje podstawowe informacje o komputerze, włączając w to wersję systemu operacyjnego, zainstalowaną pamięć, typ procesora i dane o rejestracji.

Kliknięcie przycisku *Zaawansowane ustawienia systemu* spowoduje otwarcie okna dialogowego *Właściwości systemu*. Pierwsza karta nosi nazwę *Nazwa komputera*.

Karta Nazwa komputera

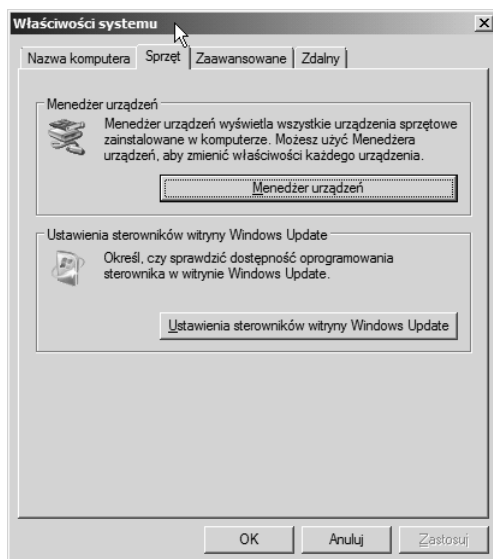
Karta *Nazwa komputera* umożliwia zmianę grupy roboczej lub domeny, do której należy komputer, a także modyfikację jego nazwy. Możliwa jest również zmiana dla komputera podstawowego sufiksu DNS i nazwy NetBIOS.

Karta Sprzęt

Karta *Sprzęt* oferuje kilka funkcji kontrolujących ustawienia urządzeń i zasobów komputera (rysunek 2.33). Wcześniej w rozdziale, w punkcie „Aplet Dodaj sprzęt”, omówiono narzędzie *Dodawanie sprzętu*. Z kolei narzędzie *Menedżer urządzeń* zaprezentowano wcześniej w podpunkcie „Menedżer urządzeń”.

Rysunek 2.33.

Karta *Sprzęt* umożliwia dodawanie, usuwanie i konfigurowanie urządzeń i profili sprzętowych



W systemie Windows Server 2008 sterowniki mogą być podpisane cyfrowo przez Microsoft w celu zapewnienia, że zostały przetestowane i spełniają określone kryteria zgodności zdefiniowane przez producenta systemu Windows. Kliknięcie przycisku *Ustawienia sterowników witryny Windows Update* spowoduje wyświetlenie okna dialogowego, które pozwala skonfigurować proces instalacji sterownika. Dostępne są następujące opcje:

- ♦ Wyszukaj sterowniki automatycznie (zalecane),
- ♦ Zapytaj mnie po każdym podłączeniu nowego urządzenia przed wyszukaniem sterowników,
- ♦ Nigdy nie wyszukuj sterowników, gdy podłączę urządzenie.

Podpisywanie sterowników można skonfigurować za pomocą zasady grupy.



Karta Zaawansowane

Przy użyciu tej karty apletu *System* panelu sterowania można ustawić opcje wydajności komputera, sprawdzić i określić zmienne środowiskowe, a także skonfigurować opcje związane z uruchamianiem i przywracaniem systemu.

Profil użytkownika

Profile użytkownika przechowują konkretne środowisko robocze, uwzględniające konfigurację pulpitu, mapowania napędów i drukarek, a także inne ustawienia. Gdy użytkownik loguje się, jego profil stosuje konfigurację pulpitu i inne właściwości. Profile użytkowników najbardziej przydają się do zapewnienia spójnego interfejsu każdemu użytkownikowi nawet wtedy, gdy inne osoby korzystają z tego samego komputera. Profile sprawdzają się również w sytuacji, gdy trzeba zagwarantować jednolity interfejs użytkownikom logującym się przy użyciu różnych komputerów (użytkownicy mobilni).



W celu uzyskania dostępu do profili użytkownika trzeba kliknąć przycisk *Ustawienia* znajdujący się w grupie *Profil użytkownika* karty *Zaawansowane* okna *Właściwości systemu*.

Profil użytkownika składa się z pliku rejestru i zestawu katalogów. Plik stosuje dla interfejsu użytkownika ustawienia związane z mapowanymi napędami, ograniczeniami, zawartością pulpitu, kolorami i czcionkami ekranu itp. Zawartość pliku jest buforowaną kopią gałęzi *HKEY_CURRENT_USER* rejestru. Wśród katalogów znajdują się takie jak *Moje dokumenty*, *Moje obrazy* i inne katalogi przechowywane dla użytkownika wewnątrz katalogu *Documents and Settings*.

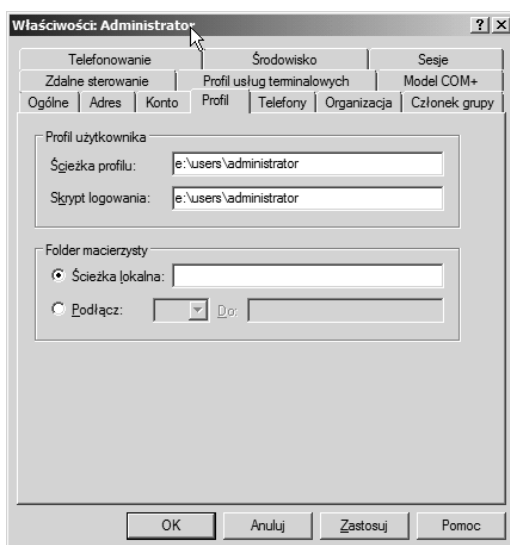
Można wyróżnić trzy typy profili — osobiste, obowiązkowe i domyślne. Profile osobiste umożliwiają użytkownikom modyfikowanie własnego środowiska roboczego i zachowywanie zmian między kolejnymi sesjami logowania. Profile obowiązkowe pozwalają na określone zmiany w konfiguracji (zależne od ograniczeń samego profilu), lecz nie są one zapamiętywane na potrzeby przyszłych sesji logowania. Jedyną różnicą między profilem osobistym i obowiązkowym jest rozszerzenie pliku profilu. Profile osobiste używają dla pliku rejestru rozszerzenia *.dat*, a profile obowiązkowe rozszerzenia *.man*.

Domyślny profil jest prekonfigurowany przez system Windows Server 2008 i stosowany dla nowych użytkowników, którzy logują się bez istniejącego jeszcze profilu. Profil jest następnie zapisywany dla użytkownika, który będzie z niego korzystał w przypadku późniejszych sesji logowania.

Profil użytkownika określa się w oknie właściwości konta podczas jego tworzenia lub modyfikowania. Przystawka Użytkownicy i grupy lokalne konsoli MMC służy do tworzenia i modyfikowania lokalnych kont. Z kolei w przypadku usługi Active Directory konsola *Użytkownicy* i komputery usługi Active Directory pozwala utworzyć i zmodyfikować konta domenowe. Karta *Profil* okna właściwości konta użytkownika (rysunek 2.34) określa ścieżkę profilu, skrypt logowania i inne ustawienia. Gdy użytkownik loguje się, system Windows Server 2008 stosuje profil położony w podanej ścieżce.

Rysunek 2.34.

Karta *Profil* określa ścieżkę profilu użytkownika



W rozdziale 24. zamieszczono więcej informacji na temat obiektów zasad grupy, a także wyjaśniono, jak są zintegrowane z usługą Active Directory.

Tworzenie profilu

Windows Server 2008 nie zapewnia żadnego konkretnego narzędzia, które umożliwiłoby utworzenie profilu użytkownika. Aby wygenerować profil, trzeba najpierw zalogować się jako docelowy użytkownik w systemie komputera z podobnym sprzętem wideo co w przypadku docelowej stacji roboczej użytkownika (ponieważ ustawienia wideo są przechowywane w profilu, trzeba zachować ich zgodność). Stosownie do potrzeb konfiguruje się środowisko robocze, mapuje napędy i drukarki, ustawia schematy pulpitu itp. Po wylogowaniu profil jest lokalnie przechowywany razem ze strukturą katalogów użytkownika.

Kopiowanie profilu

Aby profil użytkownika skopiować z jednego miejsca w drugie, używa się okna *Profile użytkownika* apletu *System* panelu sterowania. Otwórz okno *Profile użytkownika* w obrębie komputera, z którego profil zostanie skopiowany. Z listy profili przechowywanych w komputerze wybierz profil i kliknij przycisk *Kopiuj do*. Zaznacz lokalny katalog lub sieciowy udział, do którego profil ma być skopiowany i kliknij przycisk *OK*.

Obsługa mobilnych użytkowników

Profil mobilny różni się od lokalnego profilu osobistego tylko tym, że jest przechowywany w sieciowym udziale dostępnym dla użytkownika podczas logowania. Ponieważ w oknie właściwości konta użytkownika określa się ścieżkę UNC profilu, gdy użytkownik loguje się, profil może być zastosowany niezależnie od lokalizacji użytkownika. Jeśli profil istnieje w podanej ścieżce, system Windows Server 2008 użyje go w czasie logowania. Jeżeli w określonej ścieżce nie ma żadnego profilu, Windows Server 2008 automatycznie utworzy nowy profil, zapisze go w podanej lokalizacji i zastosuje w przypadku przyszłych sesji logowania.

Tworzenie profilu obowiązkowego

Choć profil obowiązkowy tworzy się w ten sam sposób co profil osobisty, konieczne jest wykonanie jednego dodatkowego kroku. Po wygenerowaniu profilu i skopiowaniu go w docelowe miejsce (na przykład może to być lokalny komputer użytkownika lub udział sieciowy w przypadku profilu mobilnego), nazwę pliku rejestru profilu trzeba zmienić z *ntuser.dat* na *ntuser.man*.

Opcje wydajności

W grupie *Wydajność* karty *Zaawansowane* kliknij przycisk *Ustawienia*, żeby otworzyć okno dialogowe *Opcje wydajności*. Karta *Efekty wizualne* pozwala skonfigurować różne opcje interfejsu, które mają wpływ na ogólną wydajność systemu. W domyślnej konfiguracji system Windows Server 2008 wyłącza wszystkie efekty wizualne z wyjątkiem stylów okien i przycisków. W zasadzie wszystkie efekty wizualne są jedynie miłe dla oka i nie dają żadnych znaczących korzyści. W związku z tym powinno się pozostawić je wyłączone.

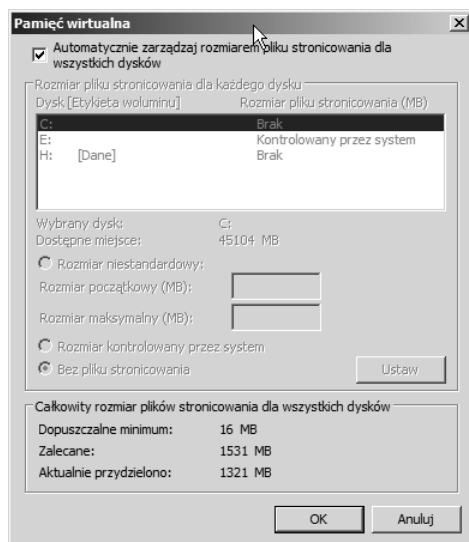
W obrębie karty *Zaawansowane* można uaktywnić opcje optymalizujące system pod kątem aplikacji lub usług działających w tle. W większości sytuacji wybiera się opcję *Programy* lub *Usługi działające w tle*.

Okno dialogowe *Opcje wydajności* pozwala też zmienić przydział pamięci wirtualnej (rozmiar systemowego pliku wymiany lub stronicowania) i przestrzeń przeznaczoną dla plików rejestru. Dlaczego warto zmodyfikować rozmiar pliku wymiany lub jego położenie? Plik wymiany służy do emulowania pamięci RAM (stąd pojęcie wirtualnej pamięci). Dzięki temu system wydaje się dysponować większą ilością fizycznej pamięci niż w rzeczywistości. Gdy pamięć RAM zapelnia się, system Windows Server 2008 przenosi jej strony do pliku wymiany, żeby dla nowych stron uwolnić miejsce w fizycznej pamięci. Jeśli potrzebna stanie się strona znajdująca się w pliku wymiany, zostanie ona przeniesiona z pamięci wirtualnej do fizycznej. Choć system Windows Server 2008 automatycznie ustala rozmiar pliku wymiany na podstawie pojemności pamięci fizycznej, w określonych sytuacjach można chcieć zwiększyć wielkość pliku w celu poprawienia wydajności. Można również plik wymiany przenieść z domyślnej lokalizacji na inny dysk o większej pojemności lub lepszej wydajności (na przykład przemieszczenie pliku z dysku IDE na dysk SCSI).

W obrębie karty *Zaawansowane* okna dialogowego *Opcje wydajności* kliknij przycisk *Zmień*, żeby uzyskać dostęp do okna *Pamięć wirtualna* (rysunek 2.35). Wybierz dysk dla pliku wymiany, określ początkowy i maksymalny rozmiar (w razie potrzeby Windows

Rysunek 2.35.

Za pomocą okna dialogowego *Pamięć wirtualna* można kontrolować wielkość pliku wymiany i rejestru



Server 2008 będzie zmieniał wielkość pliku w ustalonym zakresie), a następnie kliknij przycisk *Ustaw*. W udostępnionym polu podaj maksymalny rozmiar rejestru i kliknij przycisk *OK*, żeby zastosować dokonane zmiany.



Zmiana maksymalnego rozmiaru rejestru nie modyfikuje jego wielkości. Operacja ta narzuca maksymalny rozmiar rejestru, którego osiągnięcie powoduje wygenerowanie przez system Windows Server 2008 komunikatu ostrzegającego o tym fakcie.

Zmienne środowiskowe

W obrębie karty *Zaawansowane* kliknij przycisk *Zmienne środowiskowe*, żeby otworzyć okno dialogowe *Zmienne środowiskowe*, które umożliwia przeglądanie, usuwanie i dodawanie zmiennych środowiskowych. Zmienne definiowane w górnej części karty dotyczą aktualnie zalogowanego użytkownika. Z kolei zmienne środowiskowe ustawiane w dolnej części karty mają zastosowanie w przypadku wszystkich użytkowników.

Opcje uruchamiania i zamykania

Okno *Uruchamianie i odzyskiwanie* (rysunek 2.36) pozwala skonfigurować opcje rozruchu, sposób obsługi awarii systemu i metodę przetwarzania informacji dotyczących debugowania. Opcje grupy *Uruchamianie systemu* umożliwiają określenie domyślnie ładowanego systemu i czasu, przez jaki będzie wyświetlane menu rozruchowe. Ustawienia te są przechowywane w pliku *Boot.ini* znajdującym się w głównym katalogu dysku, w obrębie którego umiejscowiono program rozruchowy. W razie konieczności plik ten można poddać ręcznej edycji za pomocą edytora tekstu.

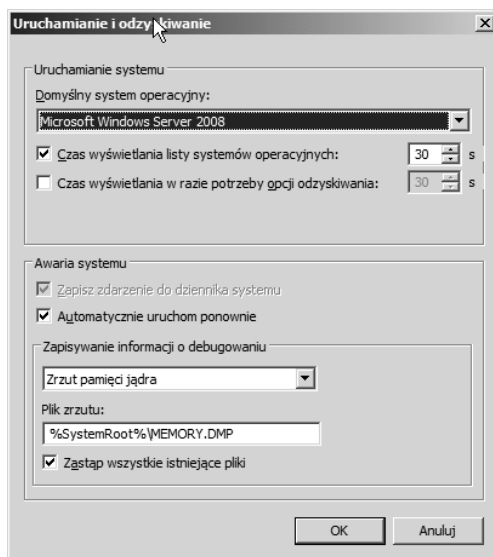


W celu wyświetlenia okna dialogowego *Uruchamianie i odzyskiwanie* kliknij przycisk *Ustawienia* zlokalizowany w grupie *Uruchamianie i odzyskiwanie* karty *Zaawansowane*.

Grupa kontrolki *Awaria systemu* decyduje, w jaki sposób zareaguje system Windows Server 2008, gdy wystąpi w nim awaria. Jeśli to możliwe, system zawsze próbuje zapisać zda-

Rysunek 2.36.

W oknie dialogowym *Uruchamianie i odzyskiwanie* można skonfigurować opcje związane z uruchamianiem, przywracaniem i debugowaniem



zenie w dzienniku. Jeżeli w celu zgromadzenia informacji na potrzeby diagnozowania systemu po wystąpieniu w nim awarii trzeba zapoznać się z zawartością niebieskiego „ekranu śmierci”, wyłącz opcję *Automatycznie uruchom ponownie*.

Grupa kontrolki *Zapisywanie informacji o debugowaniu* daje możliwość określenia czynności, którą system Windows Server 2008 podejmie w celu utworzenia pliku zrzutu pamięci po wystąpieniu awarii systemowej. Inżynierowie działu wsparcia Microsoftu mogą wykorzystać informacje o debugowaniu, żeby zidentyfikować przyczynę awarii, a następnie polecić rozwiązanie problemu lub przygotować je.

Karta Zdalny

Karta *Zdalny* widoczna na rysunku 2.37 kontroluje dostęp pulpitu zdalnego i usług terminalowych do serwera, a także narzędzie *Pomoc zdalna*.

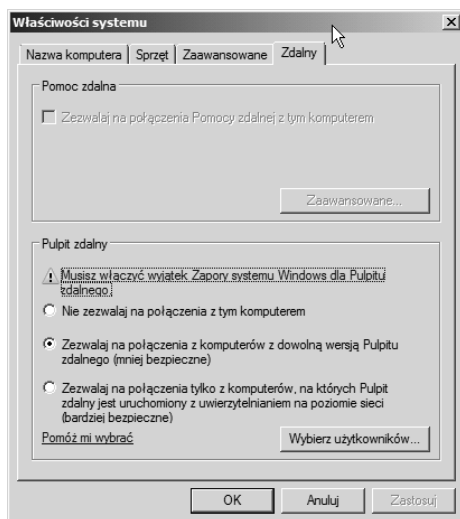
Grupa *Pomoc zdalna* umożliwia zezwolenie zdalnym użytkownikom na połączenie się z serwerem za pośrednictwem narzędzia *Pomoc zdalna*. Po kliknięciu przycisku *Zaawansowane* można włączyć lub wyłączyć opcję *Zezwalaj na zdalne sterowanie tym komputerem*. Gdy uaktywni się tę opcję, zdalny użytkownik będzie mógł zdalnie nadzorować serwer. Wyłączenie opcji pozwoli użytkownikowi przeglądać zasoby serwera, lecz nie kontrolować je. Można też ustawić okres, podczas którego zaproszenie narzędzia *Pomoc zdalna* może pozostać aktywne.

Żądania narzędzia *Pomoc zdalna* można wysłać za pomocą programu MSN Messenger lub poczty elektronicznej.

W zasadzie narzędzie *Pulpit zdalny* jest ograniczoną wersją usług terminalowych. Włączenie w grupie *Pulpit zdalny* opcji zezwalającej pozwoli zdalnym użytkownikom zainicjować z serwerem połączenie narzędzia *Pulpit zdalny* lub usług terminalowych. Kliknij przycisk *Wybierz użytkowników*, żeby wybrać użytkowników, którzy mogą zalogować się z wykorzystaniem narzędzia *Pulpit zdalny*.

Rysunek 2.37.

Przy użyciu karty
Zdalny można
skonfigurować
funkcje zdalnego
zarządzania



Systemy Windows XP i Vista dysponują wbudowanym klientem Pulpit zdalny, który może posłużyć do połączenia się z serwerem Windows Server 2008. Ponadto użytkownicy mogą zastosować klienta usług terminalowych do nawiązania połączenia z serwerem za pośrednictwem narzędzia *Pulpit zdalny*. Składnik ActiveX o nazwie *Remote Desktop Web Connection* pozwala użytkownikom przeglądarki Internet Explorer uzyskać dostęp do komputera obsługującego połączenia narzędzia *Pulpit zdalny*. Ten składnik ActiveX dołączono do systemów Windows XP i Windows Vista, a także można go pobrać z witryny internetowej Microsoftu.

Wprawdzie narzędzie *Pulpit zdalny* przydaje się w przypadku zdalnego kontrolowania i zarządzania, stanowi problem z punktu widzenia zabezpieczeń. Powinno się przeczytać rozdział 16., żeby mieć pewność, że przed uaktywnieniem po stronie serwera narzędzia *Pulpit zdalny* dobrze zrozumiano stwarzane przez nie zagrożenia.



Jeśli pojawiły się problemy z nawiązaniem przez klienty usług terminalowych połączenia z systemem Windows Server 2008 z włączonymi usługami terminalowymi, w obrębie karty *Zdalny* okna *Właściwości systemu* trzeba uaktywnić opcję *Zezwalaj na połączenia Pomocy zdalnej z tym komputerem*. Wyłączenie tej opcji uniemożliwi klientom usług terminalowych połączenie się nawet wtedy, gdy udzielono dostępu za pomocą zasady grupy.

Windows PowerShell

Nowym dodatkiem do serwerowych narzędzi administracyjnych systemu Windows Server 2008 jest Windows PowerShell, który został udostępniony przed pojawieniem się wersji produkcyjnej systemu. PowerShell jest nową powłoką trybu wiersza poleceń i językiem skryptowym, który umożliwia zautomatyzowanie lub zorganizowanie powtarzalnych serwerowych zadań administracyjnych.

Windows PowerShell znakomicie sprawdzi się w przypadku administratorów serwera, ponieważ nie trzeba być ekspertem od tworzenia kodu źródłowego, żeby pisać go tak jak

w systemie Windows Server 2003 z wykorzystaniem języków VB i JavaScript lub złożonego C#. Windows PowerShell wbudowano w system i umieszczono ponad środowiskiem .NET Common Language Runtime (CLR) i technologią .NET Framework. PowerShell odbiera i zwraca obiekty .NET, z którymi może prowadzić interakcję.

Windows PowerShell działa ze składnikiem określanym anglojęzycznym terminem *cmdlet*. Mianem *cmdlet* określa się jednofunkcyjne narzędzie wiersza poleceń wbudowane w powłokę. System wyposażono w ponad 130 standardowych składników *cmdlet*, które mogą być uaktywniane i przetwarzane stosownie do potrzeb. Z łatwością można również tworzyć własne składniki *cmdlet*. Składniki te mogą być użyte niezależnie lub w połączeniu z innymi w celu realizowania zadań serwerowych, które byłyby bardzo trudne do wykonania przy wykorzystaniu zwykłego wiersza poleceń lub za pośrednictwem apletów i funkcji panelu sterowania.

Za pomocą powłoki Windows PowerShell można zarządzać rolami systemu Windows Server 2008, takimi między innymi jak serwer IIS 7.0, serwer DNS, serwer DHCP i serwer terminali. Składniki *cmdlet* można też tworzyć dla serwerów biznesowych, takich jak Exchange Server 2007, SQL Server i Microsoft Operations Manager.

W celu zastosowania powłoki Windows PowerShell z menu *Start* wybierz pozycję *Wszystkie programy/Windows PowerShell 1.0/Documents*, a następnie odszukaj katalog przechowujący dokumentację *GettingStarted.rtf*. Jest to plik utworzony za pomocą edytora WordPad, który pozwoli szybko korzystać ze składników *cmdlet*. W tym samym katalogu umieszczono też między innymi przewodnik użytkownika i uwagi dołączone do wersji powłoki Windows PowerShell.

Podsumowanie

Windows Server 2008 zapewnia kilka narzędzi umożliwiających zarządzanie sprzętem komputera, właściwościami środowiska operacyjnego, użytkownikami i innymi obiektami. Choć większość funkcji administracyjnych wbudowano w przystawki lub rozszerzenia konsoli MMC, kilka (na przykład *Źródła danych* (ODBC)) istnieje w dalszym ciągu jako odrębne narzędzia. Panel sterowania pełni funkcję centrum nadzorującego konfigurowanie urządzeń, a także ustawień i właściwości systemu operacyjnego.

Zapoznanie się z dostępnymi narzędziami administracyjnymi stanowi ważny krok w przypadku konfigurowania i monitorowania komputera. W rozdziale przyjrano się większości narzędzi administracyjnych, które będą regularnie wykorzystywane. W innych rozdziałach omówiono dodatkowe programy zarządzające lub bardziej szczegółowo opisano niektóre wymienione tu narzędzia.